PLN-(I)SN09U-004

TDM and Carrier VoIP

(I)SN09U Release Change Reference Manual

(I)SN09U Standard 01.04 October 2006

NORTEL NETWORKS™

(I)SN09U Release Change Reference Manual
TDM and Carrier VoIP

Publication number: PLN-(I)SN09U-004
Product release: (I)SN09U
Document release: Standard 01.04
Date: October 2006

Copyright © 2006 Nortel Networks

All Rights Reserved.

Printed in the United States of America.

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

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

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

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

Publication history: North American

October 2006

(I)SN09U is an extension of the (I)SN09 software release and supersedes both (I)SN09 and (I)SN09FF for CVoIP applications. (I)SN09 continues to be supported for TDM-only applications. The (I)SN09U software release incorporates all capabilities of (I)SN09, (I)SN09FF, and additional corrective content delivered as part of Nortel's (I)SN09 software robustness program. (I)SN09, (I)SN09FF, and (I)SN09U are valid terms for use within the (I)SN09U software release.

Version 01.4 Standard release for (I)SN09U, combining content from SN09 and SN09FF.

Table of Contents

RelDoc Introduction **9**
(I)SN09FF Feature Subset Cross-Reference Tables: North American Features 11
Feature to Functional Group Cross Reference 11
Functional Group to Feature Impacts Cross Reference 20
Functional Descriptions List (FNs) 31
Functional Description (FN) A00007143 41
Functional Description (FN) A00007217 44
Functional Description (FN) A00007269 52
Functional Description (FN): A00007544 60
Functional Description (FN): A00007547 100
Functional Description (FN): A00007703 105
Functional Description (FN): A00007704 107
Functional Description (FN) A00007814 108
Functional Description (FN): A00008090 111
Functional Description (FN) A00008323 117
Functional Description (FN) A00008522 122
Functional Description (FN) A00008601 135
Functional Description (FN) A00008629 138
Functional Description (FN): A00008724 142
Functional Description (FN): A00008740 146
Functional Description (FN): A00008858 147
Functional Description (FN): A00008916 156
Functional Description (FN): A00008969 162
Functional Description (FN): A00009011 163
Functional Description (FN): A00009012 183
Functional Description (FN): A00009013 191
Functional Description (FN) A00009026 196
Functional Description (FN) A00009027 199
Functional Description (FN): A00009028 201
Functional Description (FN): A00009036 217
Functional Description (FN): A00009043 220
Functional Description (FN): A00009045 234
Functional Description (FN): A00009078 244
Functional Description (FN) A00009085 250
Functional Description (FN) A00009091 253
Functional Description (FN) A00009092 279
Functional Description (FN): A00009129 292
Functional Description (FN): A00009153 294
Functional Description (FN): A00009156 304
Functional Description (FN): A00009158 308
Functional Description (FN): A00009173 334
Functional Description (FN): A00009182 336
Functional Description (FN): A00009189 344
Functional Description (FN): A00009190 369
Functional Description (FN): A00009200 373

Functional Description (FN): A00009204 382
Functional Description (FN): A00009207 385
Functional Description (FN): A00009208 390
Functional Description (FN): A00009218 394
Functional Description (FN): A00009227 396
Functional Description (FN): A00009230 398
Functional description (FN): A00009235. 415
Functional description (FN): A00009239. 421
Functional description (FN): A00009241. 424
Functional description (FN): A00009252. 426
Functional description (FN): A00009280. 428
Functional description (FN): A00009282. 432
Functional description (FN): A00009289. 434
Functional description (FN): A00009292. 437
Functional description (FN): A00009294. 449
Functional description (FN): A00009310. 465
Functional description (FN): A00009311. 470
Functional description (FN): A00009313. 474
Functional description (FN): A00009315. 475
Functional description (FN): A00009316. 477
Functional description (FN): A00009320. 479
Functional description (FN): A00009332. 496
Functional description (FN): A00009337. 501
Functional description (FN): A00009339. 503
Functional description (FN): A00009353. 516
Functional description (FN): A00009359. 520
Functional description (FN): A00009361. 524
Functional Description (FN) A00009362. 563
Functional description (FN): A00009364. 574
Functional description (FN): A00009365. 589
Functional description (FN): A00009375 & A00009376 592
Functional description (FN): A00009378 616
Functional description (FN): A00009417 631
Functional description (FN): A00009418 635
Functional description (FN): A00009443 668
Functional description (FN): A00009446 682
Functional description (FN): A00009463 705
Functional description (FN): A00009470 711
Functional description (FN): A00009508 714
Functional description (FN): A00009513 719
Functional Description (FN): A00009514 721
Functional Description(FN): A00009515 769
Functional Description(FN): A00009520 797
Functional Description(FN): A00009530 800
Functional Description(FN): A00009532 807
Functional Description(FN): A00009550 810

Functional Description (FN) A00009576 816
Functional Description(FN): A00009610 822
Functional Description(FN): A00009611 825
Functional Description(FN): A00009612 828
Functional Description(FN): A00009614 830
Functional Description(FN): A00009616 832
Functional Description(FN): A00009651 847
Functional Description(FN): A00009655 855
Functional Description(FN): A00009711 882
Functional Description(FN): A00009726 903
Functional Description (FN): A00009777 904
Functional Description (FN): A00009822 907
Functional Description (FN): A00009823 909
Functional Description (FN): A00009828 913
Functional Description (FN): A00009829 960
Functional Description (FN): A00009830 983
Functional Description (FN): A00009831 1027
Functional Description(FN): A00009838 1037
Functional Description(FN): A00009839 1039
Functional Description(FN): A00009840 1040
Functional Description(FN): A00009865 1046
Functional Description(FN): A00009890 1050
Functional Description(FN): A00009893 1053
Functional Description(FN): A00009905 1059
Functional Description(FN): A00009950 1083
Functional Description(FN): A00009951 1086
Functional description (FN): A00010024 1104
Functional description (FN): A00010168 1106
Functional description (FN): A00010303 1114
Functional description (FN): A00010329 1131
Functional description (FN): A00010452 1133
Functional description (FN): A00010490 1136
Functional Description (FN) A00010567 1139
Functional description (FN): A00010617 1141
Functional Description (FN) A00010742 1143
Functional Description (FN) A00010880 1146
Functional Description (FN) A00011167 1148
Functional Description (FN) A00011281 1149
Functional Description (FN) A00011533 1150
Functional Description (FN) A00011740 1177
Functional description (FN): A00011746 1237
Functional Description (FN) A00011827 1240
Functional Description (FN) A00012001 1253
Functional Description (FN) A00012109 1266
Functional Description (FN) A00012183 1272
Functional Description (FN) A00012198 1278

Functional Description (FN) A00012199 1280
Functional Description (FN) A00012210 1283
Functional Description (FN) A00012215 1286
Functional Description (FN) A00012223, A00012217, A00012225 1289
Functional Description (FN) A00012242 1321
Functional Description (FN) A00012273 1393
Functional Description (FN) A00012308 1397
Functional Description (FN) A00012310 1400
Functional Description (FN) A00012315 1404
Functional Description (FN) A00012317 1411
Functional Description (FN) A00012321 1427
Functional Description (FN) A00012322 1430
Functional Description (FN) A00012323 1441
Functional Description (FN) A00012325 1447
Functional Description (FN) A00012326 1450
Functional Description (FN) A00012385 1452
Functional Description (FN) A00012386 1465
Functional Description (FN) A00012390 1467
Functional Description (FN) A00012402 1471
Functional Description (FN) A00012403 1482
Functional Description (FN) A00012410 1488
Functional Description (FN) A00012470 1490
Functional Description (FN) A00012478 1531
Functional Description (FN) A00012506 1553
Functional Description (FN) A00012526 1568
Functional Description (FN) A00012527 1581
Functional Description (FN) A00012528 1585
Functional Description (FN) A00012538, A00012537, A00012539 1588
Functional Description (FN) A00012569 1596
Functional Description (FN) A00012570 1626
Functional Description (FN) A00012571 1628
Functional Description (FN) A00012622 1698
Functional Description (FN) A00012635 1703
Functional Description (FN) A00012735 1721
Functional Description (FN) A00012843 1731
Functional Description (FN) A00012889 1736
Functional Description (FN) A00012893 1739
Functional Description (FN) A00012905 1783
Functional Description (FN) A00012974 1784
Functional Description (FN) A00013063 1787
Functional Description (FN) A00013457 1799
Functional Description (FN) A00013508 1851
Functional Description (FN) A00013935 1853
Functional Description (FN) A00014049 1855
CR Description Q01333369 1857
Fault Management List (FMs) 1859

Fault Management (FM): A00007544 1861
Fault Management (FM): A00007547 1881
Fault Management (FM): A00007703 1883
Fault Management (FM): A00007814 1884
Fault Management (FM): A00008740 1887
Fault Management (FM): A00009012 1890
Fault Management (FM): A00009013 1895
Fault Management (FM): A00009227 1900
Fault Management (FM): A00009235 1904
Fault Management (FM): A00009280 1924
Fault Management (FM): A00009282 1926
Fault Management (FM): A00009315 1932
Fault Management (FM): A00009353 1934
Fault Management (FM): A00009470 1936
Fault Management (FM): A00009515 1938
Fault Management (FM): A00009532 1940
Fault Management (FM): A00009610 1943
Fault Management (FM): A00009611 1953
Fault Management (FM): A00009614 1974
Fault Management (FM): A00009777 1982
Fault Management (FM): A00009822 1986
Fault Management (FM): A00009893 1991
Fault Management (FM): A00011827 1998
Fault Management (FM): A00012183 2005
Fault Management (FM): A00012199 2031
Fault Management (FM): A00012326 2033
Fault Management (FM): A00012403 2037
Fault Management (FM): A00012526 2039
Fault Management (FM): A00012622 2041
Fault Management (FM): A00012735 2044
Fault Management (FM): A00012905 2050
Configuration Management List (CNs) 2157
Configuration (CN): A00007217 2161
Configuration (CN): A00007544 2229
Configuration (CN): A00007547 2242
Configuration (CN): A00007814 2245
Configuration (CN): A00008090 2261
Configuration (CN): A00008522 2274
Configuration (CN): A00008601 2295
Configuration (CN): A00008629 2306
Configuration (CN): A00009011 2325
Configuration (CN): A00009012 2337
Configuration (CN): A00009013 2344
Configuration (CN): A00009036 2370
Configuration (CN): A00009078 2373
Configuration (CN): A00009085 2378

Configuration (CN): A00009091 2388
Configuration (CN): A00009129 2402
Configuration (CN): A00009189 2406
Configuration (CN): A00009190 2423
Configuration (CN): A00009200 2428
Configuration (CN): A00009207 2434
Configuration (CN): A00009218 2437
Configuration (CN): A00009227 2441
Configuration (CN): A00009235 2453
Configuration (CN): A00009280 2503
Configuration (CN): A00009282 2512
Configuration (CN): A00009339 2529
Configuration (CN): A00009375 & A00009376 2532
Configuration (CN): A00009463 2534
Configuration (CN): A00009470 2542
Configuration (CN): A00009520 2552
Configuration (CN): A00009532 2555
Configuration (CN): A00009576 2570
Configuration (CN): A00009611 2585
Configuration (CN): A00009655 2594
Configuration (CN): A00009822 2619
Configuration (CN): A00009839 2629
Configuration (CN): A00009840 2633
Configuration (CN): A00009890 2652
Configuration (CN): A000010303 2660
Configuration (CN): A000010742 2677
Configuration (CN): A000010880 2685
Configuration (CN): A000011167 2688
Configuration (CN): A00011281 2695
Configuration (CN): A00011827 2704
Configuration (CN): A000012001 2714
Configuration (CN): A00012183 2733
Configuration (CN): A00012198 2819
Configuration (CN): A00012199 2828
Configuration (CN): A00012215 2835
Configuration (CN): A00012223, A00012217, A00012225 2843
Configuration (CN): A00012526 2867
Configuration (CN): A00012527 2874
Configuration (CN): A00012570 2886
Configuration (CN): A00012889 2891
Performance Management List (PFs) 2909
Performance (PF): A00007544 2911
Performance (PF): A00007547 2919
Performance (PF): A00009515 2925
Performance (PF): A00009777 2938
Performance (PF): A00009893 2940

Performance (PF): A00012109 2944

RelDoc Introduction

TDM and Carrier VoIP SOFTWARE

PRODUCT COMPUTING MODULE LOAD RELEASE DOCUMENT

(PCL) Release Document

This release document is supplied for each Software Stream for the North American load. This release document provides software feature information pertinent to the new software load.

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

The release document consists of the following sections:

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

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

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

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

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

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

How To Use the Feature Content Section

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

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

A functional group is made up of several features.

- Table1: Feature to Functional Group Cross Reference

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

- Table 2: Functional Groups to Feature Impacts Cross Reference

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

(I)SN09U Feature Subset Cross Reference Tables: North American Features

Feature to Functional Group Cross Reference

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

Note: Features available in Nortel's FMDOC library show a version/issue number (i.e., AA05, etc.), while the features obtained from other sources do not have a version/issue number.

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

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of Base/TL, CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00007143.AB02	IPSec Integration with MS2010	Core23
A00007217	ITRANS Media Proxy Selection	CS2M09
A00007269.AB19	NGSS Backup and Restore	NGSS09
A00007544.AB06	NCAS Link and SIP NMS Support based on RFC 3842	NCGL8, NGSS09, Core22
A00007547.AB13	SIP Lines Core Call Processing Support	Core22
A00007703.AA08	SDM/CBM Log Capacity & Robustness	Core22, SDM22
A00007704.AB06	Table Access Manager Robustness	Core22, SDM22
A0007814.V3	REX testing for MG9000 (Media Gateway 9000) from Element Manager	MG9KEM09
A00008043	Refer to the FN under actid A00009189	CS2M09

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of Base/TL, CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00008090.AA14	SBA: Alternate Scheduled Closure of Billing Files	SDM22
A00008323.AA05	H.323 64k UDI	GC09
A00008522	SESM Support for SIP Lines	CS2M09
A00008601.AA03	IW-SPM-IP Fully Provisionable Codec Lists for G.711/G.729	Core22, MG4K22, SPSH22
A00008629.AA08	GEM-II AAL2 IW-SPM SN09 Core Preparation Work	Core22
A00008724.AA04	OMDD Enhancements and Robustness	SDM22
A00008740	SN09 Clock Sync Robustness	MG9K09
A00008858	CS2M and MG9KEM User Inactivity Time-out	SPFS09, CS2M09, MG9KEM09
A00008916.AA02	Gateway Controller Lines Density Increase	GC09
A00008969	ATM50 SSI Monitoring, Corrective	MG9K09
A00009011.AA02	TOPS Internet Protocol (IP) Security Enhancements	TOPS22, Core22, XPM22
A00009012.AA10	TOPS OSSAIN Service Enhancements	TOPS22
A00009013.AA09	TOPS announcements via UAS/AMS	TOPS22, Core22
A00009026.AA08	RMGC Security	GC09
A00009027.AA04	Global Network Product Support Trace Tool Enhancements	NGSS09, GC09
A00009028.AA12	CS2K MSM SIP Lines OAM Support	MCS09
A00009036.AA07	Table HOMELRN Option SITE Expansion	Core22
A00009043	CS2K SS SIP Lines Provisioning Support	MCS09
A00009045	CallP Checkpointing Support	MCS09
A00009078.AA11	ICM Dual CTI	Core22

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of Base/TL, CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00009085.AA06	ACD & ICM Capacity Expansion	Core22
A00009091.AA33	Equal Access (EA) LPIC Privilege Routing	Core22
A00009092	CS2K MSM SIP Lines Cisco 7960 Client	MCS09
A00009129.AA11	Controlled Hot Swact	Core22, NCGL09
A00009153.AA02	H.323 RLT Development	GC09
A00009156	USP-Compact Hardware	USP11
A00009158.AA05	M3UA over SCTP from Core to USP	Core22
A00009173.AA06	Linux <-> SOS Messaging	Core22
A00009182.AA02	Nortel Carrier Grade Linux Persistent Memory Application Programming Interface	NCGL8
A00009189	SESM support for 64 character FQDN	CS2M09
A00009190.AA23	Universal Carrier Protocol (UCP) C7UPTMR Enhancements	UCS22, GC09
A00009200.AA14	Packet Trunking Trunk Test: Milli-watt Tone Swap	Core22, GC09
A00009204.AA09	Siren Call Agent Customer Visible Capacity Tools	Core22
A00009207.AA05	DPT Trunk Testing Support	Core22
A00009208.AA12	SN09 180K Lines Support	Core22
A00009218	MG9K Data Audit Robustness	MG9KEM09
A00009227	NPM Robustness	MG9K09, CS2M09, MG9KEM09, GC09
A00009230	CS2000 Session Server Linux Support	MCS09
A00009235.AA09	TLS for SIP	NCGL8, NGSS09
A00009239.AA09	Services for SIP Lines	Core22, GC09
A00009241.AA06	NCAS and QSIP Development on CS2K SS	MCS09

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of Base/TL, CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00009252.A02	Multi-Time Zone AMA Enhancments	Core22
A00009280.v3	MG9K Line Circuit Enhancements	MG9KEM09
A00009282	Emergency Stand Alone (ESA) Multiple Level Precedence and Preemption (MLPP) for MG9KEM	MG9KEM09
A00009289	IEMS (Integrated Element Management System) - 10 Minute Default on User Inactivity Timer	IEMS09
A00009292	IEMS: UserID-based Partitioning by NE	IEMS09
A00009294.AA11	T.38 Annex D interworking with SIP	GC09
A00009310	SSPFS Restricted Access Shell	CS2M09, SPFS09
A00009311	SSPFS Dark Office backup	SPFS09
A00009313	SSPFS SN09 Upgrades and ESD Support	SPFS09
A00009315	Detect failures from syslog and generate alarms	SPFS09
A00009316	Backup and Restore Enhancements	SPFS09
A00009320, A00009336	Remote Ping and Traceroute for Gateway Controller and SSPFS Platforms	IEMS09, GC09
A00009332.AA14	P-Time and Codec Negotiation Selection Policy	CS2M09, GC09
A00009337.AA12	PacketCable 1.0, 1.1, and 1.5 Compliance	Base22, GC09
A00009339.AA16	Packet Cable T.38 Support	CS2M09, GC09
A00009353.AA10	GWC Unit Availability/ Health Monitoring	GC09
A00009359.AA06	HW Intro of MCPN905 for Compact Call Agent	NGCL8
A00009361	CICM: Enhancement to IP Phone 2001 CICM client	CICM9
A00009362	IP Phone 2007 User Interface support	CICM9
A00009364	CICM End-of-call QoS Reporting	CICM9
A00009365	Mid-call Session Description Protocol (SDP) renegotiation	CICM9

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of Base/TL, CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00009375 &A00009376	CICM Third-party Corrective Content Patching & CICM Selective Binary Component Patching	CICM9
A00009378.AA07	LI Support of SIP Lines	Core22, GC09
A00009417	Cold Cache Recovery	MCS09
A00009418	MCS as a 3G Application Server	MCS09
A00009443.AA07	T.38 Annex D for NGSS	GC09, NGSS09
A00009446.AA01	M2UA/SCTP Protocol for PVG SS7 backhaul support	USP11
A00009463.AA08	CBM to Support Centralized User Authentication with IEMS	SDM22
A00009470.AA09	SDM to support Security Assertion Markup Language (SAML) NSSwitch client	SDM22
A00009508.AA12	Automatic Message Accounting Session Initiation Protocol (SIP) Line Identification	Core22, SDM22
A00009513.AA07	PMA for SIP Lines	GC09
A00009514.AA25	CS2K-MCS Interop for SN09	NGSS09
A00009515.AA14	Out-of-Band Interop with MCS	NGSS09
A00009520.AA05	Trunk blocking tools for MG4K and GWC on SN09	Core22
A00009530.AA07	H248 & xUA NAT traversal for CPE Gateways	CS2M09, GC09
A00009532	Support host to host tunnels for all northbound OSS connections	IEMS09
A00009550.AA08	CBM-NPM Patching Convergence	SPFS09, SDM22
A00009576.AC04	H.323 RASLess Provisioning	CS2M09.1, GC09.2
A00009610	IEMS Calix Integration	IEMS09
A00009611	IEMS Keymile Integration	IEMS09

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of Base/TL, CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00009612	Restricted Shell Access	IEMS09
A00009614	Tamper-proof Key Storage and Event Generation	IEMS09, SPFS09
A00009616	IEMS Backward Compatibility and Upgrade	IEMS09
A00009651	Meet Me Web Collaboration Multilingual	MCS09
A00009655	BladeCenter-T RTP Media Portal	MCS09
A00009711	Multimedia Communication Server E911 Caller Hold	MCS09
A00009726	Addition of CALIX_C7 Gateway certificate	CS2M09
A00009777	IEMS Mediant 2000 Integration	IEMS09
A00009822	General Security Log When the User Logs Out	SPFS09
A00009823	Security Logging for SSPFS	SPFS09
A00009828	Granular Service Packaging	MCS09
A00009829	Subscriber Open Provisioning Interface Pro-ductization	MCS09
A00009830	Complete Re-IP Support	MCS09
A00009831	Patching	MCS09
A00009838.AA04	Removal of DCE from default install and install wizards	SDM22
A00009839.AA04	Ability to apply patches during ESUP upgrade	SDM22
A00009840.AA09	CBM IPSec Northbound Interface	SPFS09
A00009865	Add MCP820 supporting on SAM21 EM	CS2M09
A00009890	Provisioning for Media Proxy insertion for SIP lines	CS2M09
A00009893.AA12	Session Server Call Processing Overload	NGSS09
A00009905	Private and Public Name and Number Display	MCS09

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of Base/TL, CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00009950 (CICM) &A00010293 (GWC)	Media Portal Removal for Inactive CICM Clients	CICM9, GC09
A00009951	Introduction of 221X Wireless handset	CICM9
A00010024.AA01	Nortel Carrier Grade Linux kernel emergency pool	NGCL8
A00010168.AA06	H.323 support for COnnected Line Presentation/ COnnected Line Restriction (COLP/COLR)	GC09
A00010251.AA01	Support for SCTP (Simple control transmission protocol) security on GWC (Gateway controller	GC09
A00010303.AA22	Map Level Service Control Application Programming Interface	Base22
A00010329	Remove ASPEN protocol support on PVG	PVG09
A00010452	LANComm Multi-home Enhancements	Base22
A00010490	Adding Support MCPN905-270 card in SAM21 EM	CS2M09
A00010567	CS2M - G729 CODEC for AAL2	CS2M09.1
A00010617	Addition of NUERA_BTX4K and MGCP_IAD_40 Gateway certificates lines (Corrective)	CS2M09
A00010742	GWC EM Enhancements to Support SIREN	CS22M09.1
A00010880.AA08	ABI SMU Support	Core23
A00011167	MG9KEM Central Userid and Password Support	MG9KEM09
A00011281	MS2000 IPSec Configuration via IEMS	IEMS09
A00011740	Packet Cable Multimedia for CS2K	MCS09
A00011746	Addition of LGRP_TYPE field to GW profiles (Corrective)	CS2M09
A00011827.AB14	GWC Autonomous SWACT	CS2M09.1, GC09.2

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of Base/TL, CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00012001.V5	IEMS Call Server 2000 SIP Integration	IEMS09
A00012109.AA17	Session Server Shared Library Replacement (SLR) Patching	NGSS09.1
A00012183	Public Key Manager	MG9KEM09.1, IEMS09.1, SPFS09.1, CS2M09.1
A00012198.V2	GLC12 Coin Card Support from EM	MG9KEM09.1
A00012199	MG9K EM CPR Robustness	MG9KEM09.1
A00012210	Geo OA&M Automatic Backup and Accelerated Restore	SPFS09
A00012215	Global Line Card Field Programmable Gate Array	MG9KEM09.1
A00012223, A00012217, A00012225	SESM Support for SIP Lines, Part 2	CS2M09.1
A00012242	TME-CD with GSM Wireless Client, Ph-1	MCS09.1
A00012273.AA14	SIP Lines: Call Forwarding Indication	Core23, MCS09.1, GC09.1
A00012308.AA19	SIP Lines Services: PRK, DPRK, CPU	Core23, GC09.1
A00012310.AA04	Hunt, SCMP, and CWT variant support for SIP Lines	Core23, CS2M09.1
A00012315.AA07	Telemetry for SIP Lines	Core23, MCS09.1, GC09.1
A00012317.AA17	Session Initiation Protocol (SIP) Services - Automatic Call Back (ACB) and Automatic Recall (AR)	Core23, MCS09.1, GC09.1
A00012321.AB01	SIP Services: Long Distance Alerting (LDA)	Core23, MCS09.1, GC09.1
A00012322.AA07	Session Initiation Protocol (SIP) Services - Busy Line Verification (BLV)	Core23, GC09.1

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of Base/TL, CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00012323.AA13	Session Initiation Protocol (SIP) Services - Directed Call Pickup with Barge-in (DCBI) and Directed Call Pickup Barge-in Exempt (DCBX)	Core23, MCS09.1, GC09.1
A00012325.AA05	SIP Lines: Teen Line	Core23
A00012326.AA03	SIP Lines: Authentication and Authorization	Core23
A00012385.AA24	SIP Lines MADN Support	Core23, MCS09.1, GC09.1
A00012386	Media Gateway 9000 Public Key Infrastructure	MG9K09.1
A00012390.AA11	Call Transfer Screening for SIP Lines	Core23
A00012402.AA15	911 Hold/Ringback Support on SIP Lines	Core23, MCS09.1, GC09.1
A00012403.AA08	Data Protection for SIP Lines	Core23
A00012410.AA06	Support SIP lines for Malicious Call Hold	Core23
A00012470.AA08	Compact Call Agent - Support for NA/Intl Hybrid Market	CA09, SDM23
A00012478.AA14	Compact Call Agent: Geo Support for GigE	NCGL9, CA09
A00012506	Border Control Point (BCP) Operational Measurement (OM) Enhancements	MCS09.1
A00012526.AA12	TDM Call Recording Feature	Core23
A00012527.AA22	Provisioning of CS2K trunks on GW and Carrier basis	Core23
A00012528.AA16	ICM Queue Expansion	Core23
A00012538, A00012537, A00012539	SIP Lines Support - Part 2	MCS09.1
A00012569.AA22	NI2 PRI/ ISUP UUI over SCAI	Core23, GC09.1
A00012570	Disabling Non-secure Network Services in SSPFS	SPFS09.1

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of Base/TL, CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00012571	CBM User Group Improvements	SDM23
A00012622	Platform HW Alarm Reporting	MCS09.1
A00012635	Netra 240 146 GB Disk Drive Upgrade	SPFS09.1
A00012735.AA13	Session Server Fault Handling Enhancements	NCGL9, CA09
A00012766 (Refer to A00012470)	SDM/CBM800 connected with BRISC to CBM850 connected with CCA cutover	SDM23
A00012843	IEMS support for MDM security Interface changes	IEMS09.1
A00012889	Passphrase Protected Keys for SSH	SDM23
A00012893	BCP 7200 VLAN Tagging	MCS09.1
A00012905	ERS8600 Alarm Mapping Correction in IEMS	IEMS09.1
A00012974	Correct Execdata mismatch between GWC EM and Core	CS2M09.1
A00013063	PacketCable Multimedia for MCS and Carrier	MCS09.1
A00013457.AA01	Message Waiting Indication using SIP VM/UM based on RFC 3842	Core23
A00013508.V7	System Manager Auto-Failover Support	IEMS09.1
A00013935.AA04	PKMTA Extraction for DPT Calls	Core23, GC10
A00014049.AA02	GWC and SESM support for AAL2-G726-32 codec in IP Network	GC09.2, CS2M09.1
CR Q01333369	Triggering gateway capabillities audit while changing T.38 network option on CS2K with TGCP gateways	Core23

Functional Group to Feature Impacts Cross Reference

Table 2 is organized alphabetically by functional group. Within each group, the features are listed numerically. If a Feature belongs to more than one group, it

appears in each group to which it belongs. The table also indicates which sections are included for a given feature (for example, FN, FM, CN, PF, or ACC) in the release document.

Table 2 Functional Group to Feature Impacts Cross Reference

Functional Group (Stream and release)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
CA09	A00012478.AA14	Y				
CA09	A00012735.AA13	Y	Y			
CICM9	A00009361	Y				
CICM	A00009362	Y				
CICM9	A00009364	Y				
CICM9	A00009365	Y				
CICM9	A00009375 & 9376	Y	Y			
CICM9	A00009950	Y				
CICM9	A00009951	Y				
Core23	A00007143.AB02	Y				
Core22	A00007544.AB06	Y	Y	Y		Y
Core22	A00007547.AB12	Y	Y	Y		Y
Core22	A00007703.AA08	Y	Y			
Core22	A00008601.AA03	Y		Y		
Core22	A00008629.AA08	Y		Y		
Core22	A00009011.AA02	Y		Y		
Core22	A00009013.AA09	Y	Y	Y		
Core22	A00009036.AA07	Y		Y		
Core22	A00009078.AA11	Y		Y		
Core22	A00009085.AA06	Y		Y		
Core22	A00009091.AA33	Y		Y		

Functional Group (Stream and release)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
Core22	A00009129.AA11	Y		Y		
Core22	A00009158.AA05	Y				
Core22	A00009173.AA06	Y				
Core22	A00009200.AA14	Y		Y		
Core22	A00009204.AA09	Y				
Core22	A00009207.AA05	Y		Y		
Core22	A00009208.AA12	Y				
Core22	A00009239.AA09					
Core22	A00009252.A02	Y				
Core22	A00009378.AA07	Y				
Core22	A00009508.AA12	Y				
Core22	A00009520	Y		Y		
Core22	A00010303	Y		Y		
Core22	A00010452	Y				
Core23	A00010880.AA08	Y		Y		
Core23	A00012273.AA14	Y				
Core23	A00012308.AA19	Y				
Core23	A00012310.AA04	Y				
Core23	A00012315.AA07	Y				
Core23	A00012317.AA17	Y				
Core23	A00012321.AB01	Y				
Core23	A00012322.AA07	Y				
Core23	A00012323.AA13	Y				
Core23	A00012325.AA05	Y				
Core23	A00012326.AA03	Y	Y			

Functional Group (Stream and release)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
Core23	A00012385.AA24	Y				
Core23	A00012390.AA11	Y				
Core23	A00012402.AA15	Y				
Core23	A00012403.AA08	Y	Y			
Core23	A00012410.AA06	Y				
Core23	A00012526.AA12	Y	Y	Y		
Core23	A00012527.AA22	Y		Y		
Core23	A00012528.AA16	Y				
Core23	A00012569.AA22	Y				
Core23	A00013457.AA01	Y				
Core23	A00013935.AA04	Y				
Core23	CR Q01333369	Y				
CS2M09	A00007217	Y		Y		
CS2M09	A00008043	Refer to the FN under actid A00009189				
CS2M09	A00008522	Y		Y		
CS2M09	A00008858	Y				
CS2M09	A00009189	Y		Y		
CS2M09	A00009227	Y	Y	Y		
CS2M09	A00009310	Y				
CS2M09	A00009530	Y				
CS2M09	A00009726	Y				
CS2M09.1	A00009576.AC04	Y		Y		
CS2M09	A00009865	Y				
CS2M09	A00009890	Y		Y		
CS2M09	A00010490	Y				

Functional Group (Stream and release)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
CS2M09.1	A00010567	Y				
CS2M09	A00010617	Y				
CS2M09.1	A00010742	Y		Y		
CS2M09	A00011746	Y				
CS2M09.1	A00011827.AB14	Y	Y	Y		
CS2M09.1	A00012183	Y	Y			
CS2M09.1	A00012223, A00012217, A00012225	Y		Y		
CS2M09.1	A00012310.AA04	Y				
CS2M09.1	A00012974	Y				
CS2M09.1	A00014049.AA02	Y				
GC09	A00008323.AA05	Y				
GC09	A00008916.AA02	Y				
GC09	A00009026.AA08	Y				
GC09	A00009027.AA04	Y				
GC09	A00009153	Y				
GC09	A00009190.AA23	Y		Y		
GC09	A00009200.AA14	Y		Y		
GC09	A00009227	Y	Y	Y		
GC09	A00009239.AA09					
GC09	A00009294.AA11	Y				
GC09	A00009320, A00009336	Y				
GC09	A00009353.AA10	Y	Y			
GC09	A00009378.AA07	Y				

Functional Group (Stream and release)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
GC09	A00009443.AA07	Y				
GC09	A00009513.AA07	Y				
GC09	A00009530	Y				
GC09	A00010168	Y				
GC09	A00010251.AA01	Y				
GC09	A00010293	Y				
GC09.1	A00012273.AA14	Y				
GC09.1	A00012308.AA19	Y				
GC09.1	A00012315.AA06	Y				
GC09.1	A00012317.AA17	Y				
GC09.1	A00012321.AB01	Y				
GC09.1	A00012322.AA07	Y				
GC09.1	A00012323.AA13	Y				
GC09.1	A00012385.AA24	Y				
GC09.1	A00012402.AA15	Y				
GC09.1	A00012569.AA22	Y				
GC09.2	A00009576.AC04	Y				
GC09.2	A00011827.AB14	Y				
GC09.2	A00014049.AA02	Y				
GC10	A00013935.AA04	Y				
IEMS09	A00009289	Y				
IEMS09	A00009292	Y				
IEMS09	A00009320, A00009336	Y				
IEMS09	A00009532	Y	Y	Y		

Functional Group (Stream and release)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
IEMS09	A00009610	Y	Y			
IEMS09	A00009611	Y	Y	Y		
IEMS09	A00009612	Y				
IEMS09	A00009614	Y	Y			
IEMS09	A00009616	Y				
IEMS09	A00009777	Y	Y			Y
IEMS09	A00011281	Y		Y		
IEMS09	A00012001.V5	Y		Y		
IEMS09.1	A00012183	Y		Y		
IEMS09.1	A00012843	Y				
IEMS09.1	A00012905	Y	Y			
IEMS09.1	A00013508.V7	Y				
MCS09	A00009028.AA12	Y				
MCS09	A00009043	Y				
MCS09	A00009045	Y				
MCS09	A00009092	Y				
MCS09	A00009230	Y				
MCS09	A00009241.AA06	Y				
MCS09	A00009417	Y				
MCS09	A00009418	Y				
MCS09	A00009651	Y				
MCS09	A00009655	Y		Y		
MCS09	A00009711	Y				
MCS09	A00009828	Y				
MCS09	A00009829	Y				

Functional Group (Stream and release)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
MCS09	A00009830	Y				
MCS09	A00009831	Y				
MCS09	A00009905	Y				
MCS09	A00011740	Y				
MCS09.1	A00012242	Y				
MCS09.1	A00012273.AA14	Y				
MCS09.1	A00012315.AA07	Y				
MCS09.1	A00012317.AA17	Y				
MCS09.1	A00012321.AB01	Y				
MCS09.1	A00012323.AA13	Y				
MCS09.1	A00012385.AA24	Y				
MCS09.1	A00012402.AA15	Y				
MCS09.1	A00012506	Y				
MCS09.1	A00012538, A00012537, A00012539	Y				
MCS09.1	A00012622	Y	Y			
MCS09.1	A00012893	Y				
MCS09.1	A00013063	Y				
MG4K22	A00008601.AA03	Y		Y		
MG9K09	A00008740	Y	Y			
MG9K09	A00008969	Y				
MG9K09	A00009227	Y	Y	Y		
MG9K09.1	A00012386	Y				
MG9KEM09	A0007814.V3	Y	Y	Y		

Functional Group (Stream and release)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
MG9KEM09	A00008858	Y				
MG9KEM09	A00009218	Y		Y		
MG9KEM09	A00009227	Y	Y	Y		
MG9KEM09	A00009280.v3	Y	Y	Y		
MG9KEM09	A00009282	Y	Y	Y		
MG9KEM09	A00011167	Y		Y		
MG9KEM09.1	A00012183	Y				
MG9KEM09.1	A00012198.V2	Y		Y		
MG9KEM09.1	A00012199	Y	Y	Y		
MG9KEM09.1	A00012215	Y		Y		
NCGL8	A00007544.AB06	Y	Y	Y		Y
NCGL8	A00009129.AA11	Y		Y		
NCGL8	A00009182.AA02	Y				
NCGL8	A00009235.AA09	Y	Y	Y		
NCGL8	A00009359.AA06	Y				
NCGL8	A00010024	Y				
NCGL9	A00012478.AA14	Y				
NCGL9	A00012735.AA13	Y	Y			
NGSS09	A00007269.AB18	Y				
NGSS09	A00007544.AB06	Y	Y	Y		Y
NGSS09	A00009027.AA04	Y				
NGSS09	A00009235.AA09	Y	Y	Y		
NGSS09	A00009443.AA07	Y				
NGSS09	A00009514	Y				
NGSS09	A00009515.AA14	Y	Y			Y

Functional Group (Stream and release)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
NGSS09	A00009893.AA12	Y	Y			Y
NGSS09.1	A00012109.AA17	Y				Y
PVG09	A00010329	Y				
SDM22	A00007703.AA08	Y	Y			
SDM22	A00007704.AB06	Y				
SDM22	A00008090.AA14	Y		Y		
SDM22	A00008724.AA04	Y				
SDM22	A00009463.AA08	Y		Y		
SDM22	A00009470.AA09	Y	Y	Y		
SDM22	A00009508.AA12	Y				
SDM22	A00009550v1.1	Y				
SDM22	A00009838.AA04	Y				
SDM22	A00009839.AA04	Y		Y		
SDM23	A00012571	Y				
SDM23	A00012766 (Refer to A00012470)	Y				
SDM23	A00012889	Y		Y		
SPFS09	A00008858	Y				
SPFS09	A00009310	Y				
SPFS09	A00009311	Y				
SPFS09	A00009313	Y				
SPFS09	A00009316	Y				
SPFS09	A00009550v1.1	Y				
SPFS09	A00009614	Y	Y			
SPFS09	A00009822	Y	Y	Y		

Functional Group (Stream and release)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
SPFS09	A00009823	Y				
SPFS09	A00009840.AA09	Y		Y		
SPFS09	A00012210	Y				
SPFS09.1	A00012635	Y				
SPFS09.1	A00012183	Y				
SPFS09.1	A00012570	Y		Y		
SPSH22	A00008601.AA03	Y		Y		
TOPS22	A00009011.AA02	Y		Y		
TOPS22	A00009012.AA10	Y	Y	Y		
TOPS22	A00009013.AA09	Y	Y	Y		
UCS22	A00009190.AA23	Y		Y		
USP11	A00009156	Y				
USP11	A00009446.AA01	Y				
XPM22	A00009011.AA02	Y		Y		

Functional Descriptions List (FNs)

Introduction

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

Note: Features available in Nortel's FMDOC library show a version/issue number (i.e., AA05, etc.), while the features obtained from other sources do not have a version/issue number.

Featid	Title
A00007143.AB02	IPSec Integration with MS2010
A00007217	ITRANS Media Proxy Selection
A00007269.AB19	NGSS Backup and Restore
A00007544.AB06	NCAS Link and SIP NMS Support based on RFC 3842
A00007547.AB13	SIP Lines Core Call Processing Support
A00007703.AA08	SDM/CBM Log Capacity & Robustness
A00007704.AB06	Table Access Manager Robustness
A00007814.V3	REX testing for MG9000 (Media Gateway 9000) from Element Manager
A00008090.AA14	SBA: Alternate Scheduled Closure of Billing Files
A00008323.AA05	H.323 64k UDI
A00008522	SESM Support for SIP Lines
A00008601.AA03	IW-SPM-IP Fully Provisionable Codec Lists for G.711/G.729

A00008629.AA08	GEM-II AAL2 IW-SPM SN09 Core Preparation Work
A00008724.AA04	OMDD Enhancements and Robustness
A00008740	SN09 Clock Sync Robustness
A00008858	CS2M and MG9KEM User Inactivity Time-out
A00008916.AA02	Gateway Controller Lines Density Increase
A00008969	ATM50 SSI Monitoring, Corrective
A00009011.AA02	TOPS Internet Protocol (IP) Security Enhancements
A00009012.AA10	TOPS OSSAIN Service Enhancements
A00009013.AA09	TOPS announcements via UAS/AMS
A00009026.AA08	RMGC Security
A00009027.AA04	Global Network Product Support Trace Tool Enhancements
A00009028.AA12	CS2K MSM SIP Lines OAM Support
A00009036.AA07	Table HOMELRN Option SITE Expansion
A00009043	CS2K SS SIP Lines Provisioning Support
A00009045	CallP Checkpointing Support
A00009078.AA11	ICM Dual CTI
A00009085.AA06	ACD & ICM Capacity Expansion
A00009091.AA33	Equal Access (EA) LPIC Privilege Routing
A00009092	CS2K MSM SIP Lines Cisco 7960 Client
A00009129.AA11	Controlled Hot Swact
A00009153.AA02	H.323 RLT Development
A00009156	USP-Compact Hardware
A00009158.AA05	M3UA over SCTP from Core to USP
A00009173.AA06	Linux <-> SOS Messaging

A00009182.AA02	Nortel Carrier Grade Linux Persistent Memory Application Programming Interface
A00009189	SESM support for 64 character FQDN
A00009190.AA23	Universal Carrier Protocol (UCP) C7UPTMR Enhancements
A00009200.AA14	Packet Trunking Trunk Test: Milli-watt Tone Swap
A00009204.AA09	Siren Call Agent Customer Visible Capacity Tools
A00009207.AA05	DPT Trunk Testing Support
A00009208.AA12	SN09 180K Lines Support
A00009218	MG9K Data Audit Robustness
A00009227	NPM Robustness
A00009230	CS2000 Session Server Linux Support
A00009235.AA09	TLS for SIP
A00009239.AA09	Services for SIP Lines
A00009241.AA06	NCAS and QSIP Development on CS2K SS
A00009252.A02	Multi-Time Zone AMA Enhancments
A00009280.V3	MG9K Line Circuit Enhancements
A00009282	Emergency Stand Alone (ESA) Multiple Level Precedence and Preemption (MLPP) for MG9KEM
A00009289	IEMS (Integrated Element Management System) - 10 Minute Default on User Inactivity Timer
A00009292	IEMS: UserID-based Partitioning by NE
A00009294.AA11	T.38 Annex D interworking with SIP
A00009310	SSPFS Restricted Access Shell
A00009311	SSPFS Dark Office backup
A00009313	SSPFS SN09 Upgrades and ESD Support
A00009315	Alarm Logging Failure

A00009316	Backup and Restore Enhancements
A00009320, A00009336	Remote Ping and Traceroute for Gateway Controller and SSPFS Platforms
A00009332.AA14	P-Time and Codec Negotiation Selection Policy
A00009337.AA12	PacketCable 1.0, 1.1, and 1.5 Compliance
A00009339.AA16	Packet Cable T.38 Support
A00009353.AA10	GWC Unit Availability/ Health Monitoring
A00009359.AA06	HW Intro of MCPN905 for Compact Call Agent
A00009361	CICM: Enhancement to IP Phone 2001 CICM client
A00009362	IP Phone 2007 User Interface support
A00009364	CICM End-of-call QoS Reporting
A00009365	Mid-call Session Description Protocol (SDP) renegotiation
A00009375 & 9376	CICM Third-party Corrective Content Patching & CICM Selective Binary Component Patching
A00009378.AA07	LI Support of SIP Lines
A00009417	Cold Cache Recovery
A00009418	MCS as a 3G Application Server
A00009443.AA07	T.38 Annex D for NGSS
A00009446.AA01	M2UA/SCTP Protocol for PVG SS7 backhaul support
A00009463.AA08	CBM to Support Centralized User Authentication with IEMS
A00009470.AA09	SDM to support Security Assertion Markup Language (SAML) NSSwitch client
A00009508.AA12	Automatic Message Accounting Session Initiation Protocol (SIP) Line Identification
A00009513.AA07	PMA for SIP Lines
A00009514.AA25	CS2K-MCS Interop for SN09

A00009515.AA14	Out-of-Band Interop with MCS
A00009520.AA05	Trunk blocking tools for MG4K and GWC on SN09
A00009530.AA07	H248 & xUA NAT traversal for CPE Gateways
A00009532	Support host to host tunnels for all northbound OSS connections
A00009550.AA08	CBM-NPM Patching Convergence
A00009576.AC04	H.323 RASLess Provisioning
A00009610	IEMS Calix Integration
A00009611	IEMS Keymile Integration
A00009612	Restricted Shell Access
A00009614	Tamper-proof Key Storage and Event Generation
A00009616	IEMS Backward Compatibility and Upgrade
A00009651	Meet Me Web Collaboration Multilingual
A00009655	BladeCenter-T RTP Media Portal
A00009711	Multimedia Communication Server E911 Caller Hold
A00009726	Addition of CALIX_C7 Gateway certificate
A00009777	IEMS Mediant 2000 Integration
A00009822	General Security Log When the User Logs Out
A00009823	Security Logging for SSPFS
A00009828	Granular Service Packaging
A00009829	Subscriber Open Provisioning Interface Productization
A00009830	Complete Re-IP Support
A00009831	Patching
A00009838.AA04	Removal of DCE from default install and install wizards
A00009839.AA04	Ability to apply patches during ESUP upgrade

A00009840.AA09	CBM IPSec Northbound Interface
A00009865	Add MCP820 supporting on SAM21 EM
A00009890	Provisioning for Media Proxy insertion for SIP lines
A00009893.AA12	Session Server Call Processing Overload
A00009905	Private and Public Name and Number Display
A00009950 (CICM) &A00010293 (GWC)	Media Portal Removal for Inactive CICM Clients
A00009951	Introduction of 221X Wireless handset
A00010024.AA01	Nortel Carrier Grade Linux kernel emergency pool
A00010168.AA06	H.323 support for COnnected Line Presentation/COnnected Line Restriction (COLP/COLR)
A00010251.AA01	Support for SCTP (Simple control transmission protocol) security on GWC (Gateway controller
A00010303.AA22	Map Level Service Control Application Programming Interface
A00010329	Remove ASPEN protocol support on PVG
A00010452	LANComm Multi-home Enhancements
A00010490	Adding Support MCPN905-270 card in SAM21 EM (Corrective)
A00010567	CS2M - G729 CODEC for AAL2
A00010617	Addition of NUERA_BTX4K and MGCP_IAD_40 Gateway certificates lines (Corrective)
A00010742	GWC EM Enhancements to Support SIREN
A00010880.AA07	ABI SMU Support
A00011167	MG9KEM Central Userid and Password Support
A00011281	MS2000 IPSec Configuration via IEMS
A00011740	Packet Cable Multimedia for CS2K

A00011746	Addition of LGRP_TYPE field to GW profiles (Corrective)
A00011827.AB14	GWC Autonomous SWACT
A00012001.V5	IEMS Call Server 2000 SIP Integration
A00012109.AA17	Session Server Shared Library Replacement (SLR) Patching
A00012183	Public Key Manager
A00012198.V2	GLC12 Coin Card Support from EM
A00012199	MG9K EM CPR Robustness
A000012210	Geo OA&M Automatic Backup and Accelerated Restore
A00012215	Global Line Card Field Programmable Gate Array
A00012223, A00012217, A00012225	SESM Support for SIP Lines, Part 2
A00012242	TME-CD with GSM Wireless Client, Ph-1
A00012273.AA14	SIP Lines: Call Forwarding Indication
A00012308.AA19	SIP Lines Services: PRK, DPRK, CPU
A00012310.AA04	Hunt, SCMP, and CWT variant support for SIP Lines
A00012315.AA07	Telemetry for SIP Lines
A00012317.AA17	Session Initiation Protocol (SIP) Services - Automatic Call Back (ACB) and Automatic Recall (AR)
A00012321.AB01	SIP Services: Long Distance Alerting (LDA)
A00012322.AA07	Session Initiation Protocol (SIP) Services - Busy Line Verification (BLV)
A00012323.AA13	Session Initiation Protocol (SIP) Services - Directed Call Pickup with Barge-in (DCBI) and Directed Call Pickup Barge-in Exempt (DCBX)
A00012325.AA05	SIP Lines: Teen Line
A00012326.AA03	SIP Lines: Authentication and Authorization

A00012385.AA24	SIP Lines MADN Support
A00012386	Media Gateway 9000 Public Key Infrastructure
A00012390.AA11	Call Transfer Screening for SIP Lines
A00012402.AA15	911 Hold/Ringback Support on SIP Lines
A00012403.AA08	Data Protection for SIP Lines
A00012410.AA06	Support SIP lines for Malicious Call Hold
A00012470.AA08	Compact Call Agent - Support for NA/Intl Hybrid Market
A00012478.AA14	Compact Call Agent: Geo Support for GigE
A00012506	Border Control Point (BCP) Operational Measurement (OM) Enhancements
A00012526.AA12	TDM Call Recording Feature
A00012527.AA22	Provisioning of CS2K trunks on GW and Carrier basis
A00012528.AA16	ICM Queue Expansion
A00012538, A00012537, A00012539	SIP Lines Support - Part 2
A00012569.AA22	NI2 PRI/ ISUP UUI over SCAI
A00012570	Disabling Non-secure Network Services in SSPFS
A00012571	CBM User Group Improvements
A00012622	Platform HW Alarm Reporting
A000126235	Netra 240 146 GB Disk Drive Upgrade
A00012735.AA13	Session Server Fault Handling Enhancements
A00012766 (Refer to A00012470)	SDM/CBM800 connected with BRISC to CBM850 connected with CCA cutover
A00012843	IEMS support for MDM security Interface changes
A00012889	Passphrase Protected Keys for SSH

A00012893	BCP 7200 VLAN Tagging
A00012905	ERS8600 Alarm Mapping Correction in IEMS
A00012974	Correct Execdata mismatch between GWC EM and Core
A00013063	PacketCable Multimedia for MCS and Carrier
A00013457.AA01	Message Waiting Indication using SIP VM/UM based on RFC 3842
A00013508.V7	System Manager Auto-Failover Support
A00013935.AA04	PKMTA Extraction for DPT Calls
A00014049.AA02	GWC and SESM support for AAL2-G726-32 codec in IP Network
CR Q01333369	Triggering gateway capabillities audit while changing T.38 network option on CS2K with TGCP gateways

1: Functional Description (FN) A00007143

1.1 Feature name and Feature ID

A00007143: IPSec Integration with MS2010

1.2 Description

Media Server 2010, MS2010 is an audio server in the succession network and is responsible for announcements, lawful intercept, and conference ports. The MS2010 communicates its signalling messages via the audio Gateway Controller (GWC) which has one of the following profiles: AUDCNTL, AUDCNTLINTL, AUDCNTL_RMGC, AUDCNTL_RMGCINTL. The integrated element management system (IEMS) is the element manager for the MS2010 and is the supported interface for IPSec configuration on the MS2010.

This ICAF integrates the IPSec interactions between the audio GWC and the MS2010 as configured by the IEMS. There has been no additional development required on the GWC to support this feature as it relies on existing IPSec functionality and CS2M IPSec configuration tools. This integration tests that the new IPSec functionality on the MS2010 and the corresponding configuration interface on the IEMS work in conjunction with the existing functionality on the GWC and CS2M.

The documentation for using the IEMS graphical user interface for configuration and maintenance of the IPSec functionality on the MS2010 is in feature A00011281.

The documentation for general configuration and maintenance of the GWC IPSec functionality via the CS2M, is covered in the FCAP documentation NN10213-611 with the following considerations specifically for using this functionality for securing communication to the MS2010:

Key Exchange Method: The key exchange method used between the MS2010 and the audio GWC is IKE (internet key exchange).

IKE Cipher Algorithms: The MS2010 does not support AES encryption algorithm so the AES-CBC option should not be used on the GWC for IKE cipher algorithm.

IKE Diffie-Hellman key group: In order to properly match this value with the value configured on the MS2010 the user needs to know that Diffie-Hellman key group 1 on the GWC corresponds to dH-786-BIT setting on the MS2010 and Diffie-Hellman key group 2 on the GWC corresponds to dH-1024-BIT setting on the MS2010.

IPSec ESP Cipher Algorithms: The MS2010 does not support AES encryption algorithm so the option ESP-AES must not be used on the GWC for IPSec ESP cipher algorithm.

PFS: Diffie-Hellman key group: Perfect Forward Secrecy (PFS) is not supported on the MS2010 so this value must be set to NONE on the GWC

Fault Management: IPSec Fault management is covered in FCAP document NN10202-911 Gateway Controller Fault Management (no Kerberos logs would be applicable to this interface, only IKE management logs).

1.3 Hardware Requirements or Dependencies

None

1.4 Software Requirements or Dependencies

Depends on MS2010 support for IPSec and IEMS GUI for configuration and maintenance of IPSec for MS2010

1.5 Limitations and restrictions

None

1.6 Interactions

As with any other links that support IPSec, there is a performance degradation associated with applying security to the messaging link. The degradation for messaging to the MS2010 would be comparable to the degradation experienced on any of the other links that currently support IPSec.

1.7 Glossary

Term	Description
MS2010	Media Server 2010
IEMS	Integrated Element Management Server
IPSec	Internet Protocol Security
IKE	Internet Key Exchange
Diffie-Hellman	A key exchange method used in IKE phase 1 and perfect forward secrecy
PFS	Perfect forward secrecy

Term	Description
New term	**Definition**
no new terms	

2: Functional Description (FN) A00007217

2.1 Feature name and Feature ID

A00007217: ITRANS Media Proxy Selection

This feature is mapped to Actid A00007217 and A00009367. This FN covers the functionality added by both activities.

2.2 Description

Media Proxies (MPs) have been used in Internet Transparency features since SN06.2. They allow Media Streams to be sent to/from devices that are behind Network Address Translators (NAT).

Prior to this enhancement, the MPs were provisioned against Gateway Controllers (GWC). The MPs on the GWC were selected using a "round robin" approach when a call involving one of its subtending gateways required a MP. This did not completely satisfy customer requirements because a GWC could have Media Gateways (MG) from diverse locations. The round robin approach to MP selection could cause an MG to use a MP located a great distance from it. Another MP on the same GWC could have been a better choice because it was better located relative to the MG.

This SN09 activity will improve the method of selection of a MP by allowing customers to provision Media Proxy (MP) preferred groups. A MP preferred group will represent a subset of Media Proxies that are preferable for use in a particular part of the network configuration. For example a cluster of media Proxies in a particuar location could be put in a group to be used exclusively by a set of gateways in the same location. By enabling sub-division and restricted access of Media Proxies greater flexibility is given in the use of the MPs known to the GWC.

Media Proxy Groups can be allocated to Itrans Network Zones (Nats, LBLs and composite Nat/Lbl zones). The GWC will select the MP to use for the media stream at call setup time by finding the first Media Proxy Group in the Network Zone hierarchy linked to the Gateway and selecting an MP from that group on a round robin basis. Customers will be able to allocate MPs more efficiently (in terms of increased speed and cost savings) by grouping them according to location and reducing the distance travelled through the nextwork.

In addition to the capability to create preferred Media Proxy Groups, this feature will also retain the pre-SN09 capability to allow media proxies to be associated to GWCs. The media proxies associated to a GWC will be refered to as the GWC's default media proxies (see more detail below).

A Media Proxy may belong to more than one Media Proxy Group as well as a GWCs default media proxies. A Media Proxy Group may be associated with more than one Network Zone.

This feature also provides the capability to group Nat Itrans Network Zones into virtual private networks (VPNs). A VPN can contain one or more Nats. The VPN identifiers of the parties involved in a call will be used during call setup time to determine if a media proxy is required (see the call processing section below for more details).

Media Proxy Group (MPG) and Virtual Private Network (VPN) functionality will be included in the SN09 release and will be enabled in the CS2000 Management Tools User Interface. No additional action is required to enable this functionality.

This feature comprises provisioning enhancements and call processing enhancements.

2.2.1 Provisioning Enhancements

This enhancement will facilitate the creation, deletion and alteration of Media Proxy Groups (MPG) by means of a graphical user interface (GUI) incorporated into the CS2000 management Tools GUI. A MPG can consist of up to 5 MPs selected from a list of available MPs.

The pre-SN09 capability to provision media proxies against the whole GWC will remain. Media proxies that are provisioned against the GWC are referred to as the GWC's default media proxies, and can be used if no preferred Media Proxy Groups are provisioned. Thus, at provisioning time, a media proxy can be either:

1. Associated with one or more GWCs, but not be part of any preferred media proxy group. This is the retention of the SN08 functionality. This media proxy will be refered to as a default media proxy in SN09. And/or,

2. Made part of one or more preferred media proxy groups, And/or,

3. Made part of one or more preferred media proxy groups, and also be associated with one or more GWCs. I.e. a media proxy can be in one or more Media Proxy Groups, and also be a default media proxy for one or more GWCs.

A GWC may have none or several default media proxies associated to it.

The architecture is shown in Figure 1 below.

Figure 1 Functional Behaviour Diagram: Media Proxy Selection

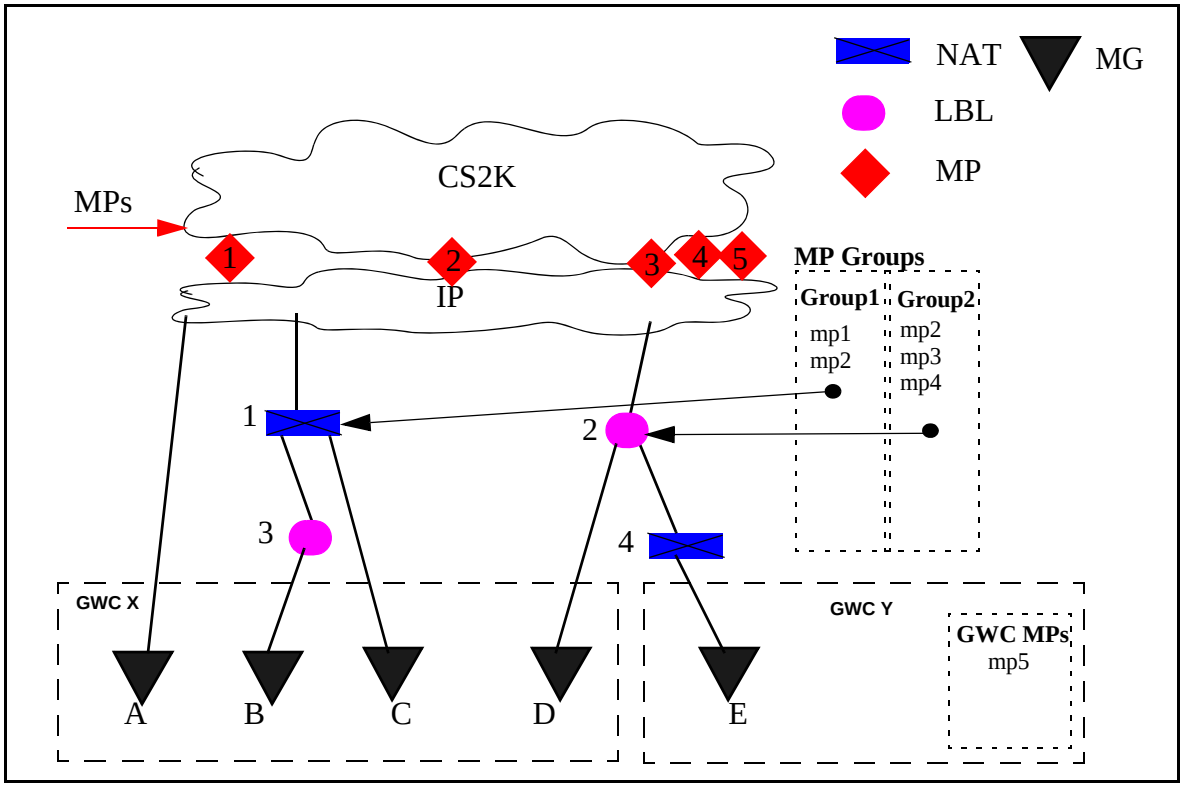


Figure 1 shows that MPs are assigned in MP Groups with some MPs being assigned as default MPs on a GWC. The MP Groups are then assigned to Nat, LBL and composite Nat/LBL Network Zones by the customer. If a call being set up on a MG requires a MP, the GWC would search the Itrans Middlebox hierarchy of the MG until it got to a NAT or LBL with a MP group. The MP would then be selected from the group on a round robin basis. If no MP Group was found in the hierarchy the GWC would select an MP from the default MPs provisioned on the GWC.

The following provisioning functionality will be added in this feature:

The capability to Provision a Media Proxy Group - a Media Proxy Group may be created with up to 5 Media proxies. A media proxy may be in more than one group and/or be one of the GWC's default media proxies.

The capability to modify a Media Proxy Group - The Media Proxies associated with a Media Proxy Group may be changed, and the number of media proxies in the group may be increased or decreased (subject to a maximum of 5 and minimum of 1). A Media Proxy Group that has been provisioned on a GWC(s) may not be modified unless it is first disassociated from the GWC(s). Disassociating the Media Proxy Group (s) from a GWC will affect call processing in that the Media proxies in the

group will not be available for selection for the duration of the modification operation.

The capability to query a Media Proxy Group - The Media Proxy Group may be queried as follows:

To return the media proxies in the group.

To return a list of all media Proxy Groups.

To return a list of GWCs that are provisioned with the Group.

To return a list of groups that have a particular Media Proxy.

The capability to delete a Media Proxy Group - The Media Proxy Group may be removed from the system. The Media Proxy Group must first be disassociated from any Itrans Network Zones that are present on any GWC.

The capability to associate a Media Proxy Group with an ITRANS Network Zone - A user may add a media proxy group to an Itrans Network Zone. A group may be associated with more than one Itrans Network Zone.

The capability to change the Media Proxy Group associated with an Itrans Network Zone - A user may change the Media Proxy Group that is selected for an Itrans Network Zone. This operation is likely to affect call processing and the availability of Media Proxies for the duration of the change.

The capability to associate a NAT Itrans Network Zone with a Virtual private network (VPN) - A NAT Network Zone may be assigned a VPN identifier. NAT Network Zones with the same VPN identifier are considered as being in the same VPN. Gateways may be moved to different network zones in a VPN even if the top-level network zones are different.

The capability to delete a VPN - A VPN may only be deleted if no NAT Network Zones are associated with it. This means that all Network Zones in a VPN must first be changed to remove the association with the VPN.

The capability to query a VPN - The NAT network Zones in the VPN may be queried.

The capability to Change a VPN - NAT Network Zones may be added or removed from a VPN by changing the VPN that a NAT Network Zone is associated with.

If any of the above listed actions fails to be executed on the server, the data will either be rolled back and the system restored to its original state or an alarm will be set to indicate a potential database mismatch. A message window will be displayed to alert the user to the provisioning fault.

2.2.2 Call Processing Enhancements

2.2.2.1 Media Proxy Selection During Call Processing.

During call setup, the GWC will determine whether or not the call requires a media proxy in order to facilitate call completion (see 2.2.2.2). If a media proxy is determined to be required, a media proxy is selected using the process in 2.2.2.3. If the selected media proxy is successfully contacted, it will be inserted into the media stream and call setup completed.

2.2.2.2 Criteria For Determining If A Media Proxy Is Required

Prior to SN09, whether or not a call required a media proxy to facilitate call completion depended on whether the parties involved in the call were behind NATs, and if so, whether the NATs of each party belonged to different Network Zones.

In SN09, whether or not a call requires a media proxy to facilitate call completion depends on whether the parties involved in that call are in the same virtual private network (VPN). A media proxy will be deemed to be required for call completion if either:

1. The two parties involved in the call belong to different VPNs. Or,

2. The call is an inter-domain SIP-T call, and the non-SIP-T media endpoint is not located in the common public domain. Or,

3. One of the endpoints is a SIP line.

2.2.2.3 Media Proxy Selection Process

At call setup time, if the GWC has determined that the call requires a media proxy to achieve call completion, a media proxy will be selected using the following process. At any point in the selection process, if a media proxy is successfully selected and contacted, then this media proxy selection process will stop and call processing will continue to insert the media proxy into the media stream, and set up the call.

MEDIA PROXY SELECTION PROCESS:

If it is determined that Early Slave Insertion of a media proxy is required, then the Slave GWC will "walk up" its Itrans Network Zone hierarchy, starting from the Itrans Network Zone adjacent to the Slave gateway, looking for a preferred media proxy group. It will select a media proxy, using a round-robin approach, from the first preferred media proxy group that it finds associated with a NAT, LBL or combined NAT-LBL zone. If none of the media proxies in that preferred media proxy group can be used, (e.g. all are out of capacity, or not active), then the Slave GWC will select a media proxy, using a round-robin approach, from its default media proxies.

If The Slave GWC does not have any default media proxies associated to it, or, if none of its default media proxies can be used (e.g. all are full to capacity),

then it means that the call required a media proxy, but no useable media proxy could be found. The call will then be taken down.

However, if Early Slave Insertion is not required, then the Master GWC will "walk up" its Itrans Network Zone hierarchy, starting from the Itrans Network Zone adjacent to the gateway, looking for a preferred media proxy group. It will select a media proxy, using a round-robin approach, from the first preferred media proxy group that it finds associated with a NAT, LBL or composite NAT-LBL zone. If none of the media proxies in that preferred media proxy group can be used, (e.g. all are out of capacity, or not active), then the Master GWC will select a media proxy, using a round-robin approach, from its default media proxies.

If the Master GWC does not have any default media proxies associated to it, or,if none of its default media proxies can be used (e.g. all are full to capacity), then the Master GWC will request the Slave GWC to perform media proxy insertion, provided that the Slave GWC has media proxies provisioned.

If Slave media proxy insertion is invoked by the Master GWC, the Slave GWC will perform a media proxy selection process that is the same as that described for Early Slave Insertion above.

2.2.2.4 Load Sharing Among Media Proxies

Load sharing among media proxies is implemented as follows:

1. Within each preferred media proxy group, media proxies are selected using a round-robin approach.

2. Selection of a default media proxy, from the default media proxies allocated to a GWC, is also performed using a round-robin approach

2.3 Hardware Requirements or Dependencies

There are no additional Hardware requirements for this feature.

2.4 Software Requirements or Dependencies

- The GWC should be running a software load of an equivalent stream to that of the SESM/GWC-EM, and should be running under a profile that enables ITrans functionality.
- The GWC should be running a software load that allows the use of a preferred Media proxy group.

2.5 Limitations and restrictions

A maximum of 5 Media Proxies may be assigned to a Media Proxy group.

A maximum of 20 Media Proxies are permitted on a GWC.

A maximum of 8 Media Proxy Groups are permitted on a GWC.

A maximum of 512 Media Proxy Groups can be provisioned in the system.

A maximum of 20 GWCs can be provisioned with a particular Media Proxy.

Only an Itrans Network Zone (Nat, LBL or composite Nat/LBL) may be assigned a Media Proxy group.

An Itrans Network Zone may be assigned only one Media Proxy Group.

A Media Gateway that does not have a media Proxy Group assigned via its Itrans Network Zone Hierarchy will use the default Media Proxies provisioned on the GWC.

Media Proxies must be provisioned before Media Proxy Groups can be created.

Media Proxy Groups must be provisioned before association with an Itrans Network Zone.

Only a Nat or Composite Nat Network Zone can be provisioned with a VPN.

A VPN cannot be deleted if it contains Nat Zones that are associated on a GWC.

A Media Proxy Group cannot be deleted if it is associated with a Network Zone that is on a GWC.

A Media Proxy cannot be deleted from the system if it belongs to a media proxy group.

A Media Proxy cannot be deleted from the system if it is a default media proxy on a GWC.

A Media Proxy Group cannot be changed if it is on a GWC. Changes to a Media Proxy Group and the Media Proxies in the group must be done in such a way that the Media Proxy Group is first removed from all GWCs. This can be done by disassociating the network zone with the group from GWCs or by changing the group associated with that network zone. Changes of this nature will affect the availability of Media Proxies (for call processing) for the duration of the change.

2.6 Interactions

Changes have been made to include the Media Proxy Group association with a Network Zone. These changes are, in part, on interfaces which are common to both the Call server 2000 Management Tools (CS2MT) and the Session Policy Controller (SPC). In particular the xml schemas used by the OSSGATE

interface for network Zones, are common to both systems. Therefore the changes made in the xml for the purposes of this feature are expected to be implemented in the SPC. The SPC implementation of the xml interface changes is not a part of this feature.

NAT traversal for CICM gateways is unchanged by this feature.

SIP line Provisioning is not affected by this feature. Any topology changes will flow through to the SIP GW to ensure that NAT traversal is correctly calculated. CS2K MP insertion will then proceed as normal. Media Proxy insertion by the SIP GW is unchanged and is done according to the existing SIP GW rules, using the common topology.

The provisioning of Media Proxy Group data brings changes to the following GUIs:

- GWC-EM Network Panel
- GWC Media Proxies Panel
- Add Itrans Network Zone Dialogs
- Change Itrans Network Zone Dialogs
- Itrans Network Zone Panels
- Network Devices Media Proxies Panel

See the GUI section in Configuration for full details of the changes to the GUIs.

See the OSS Gate section in Configuration for details of the xml changes.

See the Walkthrough section in Configuration for details of the provisioning use cases.

2.7 Glossary

Term	Description
Media Proxy Group	a group of Media Proxies

3: Functional Description (FN) A00007269

3.1 Feature name and Feature ID

A00007269 NGSS Backup and Restore

3.2 Synopsis

This activity enhances the backup functionality provided by the NGSS Session Server for SN09. These enhancements include creating a new directory to store the backed up files, backup additional files not previously backed up, and provide a mechanism for the customer to change the backup time. It also documents a restore procedure for the various backed up components.

3.3 Background Information

3.3.1 NGSS Pre-SN09 Backup Capability

In SN07 and SN08 the NGSS Session Server performs a daily backup of the Solid database files into the following directory on each NGSS unit:

```
/opt/apps/database/solid/backup
```

The database backup is performed by an automatic timed command at 1 AM daily. The backup time can not be configured. A single copy of the database backup is stored on the NGSS.

3.3.2 NGSS SN09 Backup Capability

For SN09, this activity backs up the Solid database, certificates, commish, and web files on the NGSS Session Server.

All backed up files are placed in a TAR file on the following directory:

```
/data/bkresmgr/backup
```

The backup mechanism is controlled by a cron job running on the NGSS. The backup time can be configured by the customer. The backup cron job is set to run at 1 AM as a default setting.

Customers need to ensure that NGSS backup times are synchronized with the times set for IEMS backups.

It is strongly recommended that customers transfer the backups to an external server or location daily to protect against system or office outages.

NOTE: In SN09, both units will be backed up. As some files are different between them, customers are recommended to store the backups taken from both units.

3.4 Description

3.4.1 NGSS Back up Directory

Backup files are stored locally on the NGSS. A new directory is created to store the backed up files. A directory is created for this purpose is:

`/data/bkresmgr/backup`[1]

All backed up files are placed in a TAR file in the backup directory. The name of the backup file is in the following format:

`<hostname>.backupfile.date_time.tgz`

For example:

`vm0.backupfile.2005-03-14_09-47.tgz`

3.4.2 NGSS Backed up Files

The following files are backed up on the NGSS for SN09:

- Solid Database files
  - /opt/apps/database/solid/backup/solid.db
  - /opt/apps/database/solid/backup/solid.ini
  - /opt/apps/database/solid/backup/solmsg.out
- certificate files
  - /opt/base/share/ssl/gen_cert.txt
  - /opt/base/share/ssl/server.crt
  - /opt/base/share/ssl/trusted.crt
- commish files[2]
  - etc/hosts[3]
  - etc/ntp.conf
  - etc/sysconfig/network-scripts/ifcfg-eth0[4]
  - etc/sysconfig/netnodes

[1]This backup directory naming convention was introduced by the A00006979 Synchronized Backup and Restore activity for Succession products.

[2]Note: files in the etc/ directory are identical to those in the /persist directory. They can be backed up from either directory.

[3]This is unit specific data.

[4]This is unit specific data.

- etc/group
- etc/passwd
- etc/shadow
- /opt/base/synch_local/common/etc/ssh/ssh_host_dsa_key.pub
- /opt/base/synch_local/common/etc/ssh/ssh_host_key.pub
- /opt/base/synch_local/common/etc/ssh/ssh_rsa_key.pub

• web files

- /opt/apps/webint/jakarta-tomcat-4.1.30/conf/server.xml
- /opt/apps/webint/jakarta-tomcat-4.1.30/webapps/prov/jsp/redirect.jsp
- /opt/apps/webint/jakarta-tomcat-4.1.30/webapps/prov/jsp/redirect_SSPFS.jsp
- /opt/apps/webint/jakarta-tomcat-4.1.30/webapps/prov/jsp/redirect_no-SSPFS.jsp
- /usr/local/apache/htdocs/redirect_apps.php

All backed up files are placed in a tar file on the following directory:

```
/data/bkresmgr/backup
```

3.4.3 Restoring NGSS Backed up Files

In general the backed up files simply need to be returned to their original directories as documented above “NGSS Backed up Files” on page 53. The files should be applied to their respective directories after the commish and SIPGW installation steps have been completed and prior to unsuspending the SIPGW application.

Perform these initial steps to start the restore process.

1. Log into NGSS as root.
2. Transfer backup TGZ file to /data/bkresmgr/restore
3. If image is stored locally, copy it from /data/bkresmgr/backup

   ```
   cp /data/bkresmgr/data/backupfile.tgz /data/
   bkresmgr/restore
   ```

4. If image is stored externally, use NFS, SFTP, SCP, or read it from a CD/DVD/tape drive.
5. Go to restore dir

   ```
   cd /data/bkresmgr/restore
   ```

6. Un-compress the backup image into the current dir.

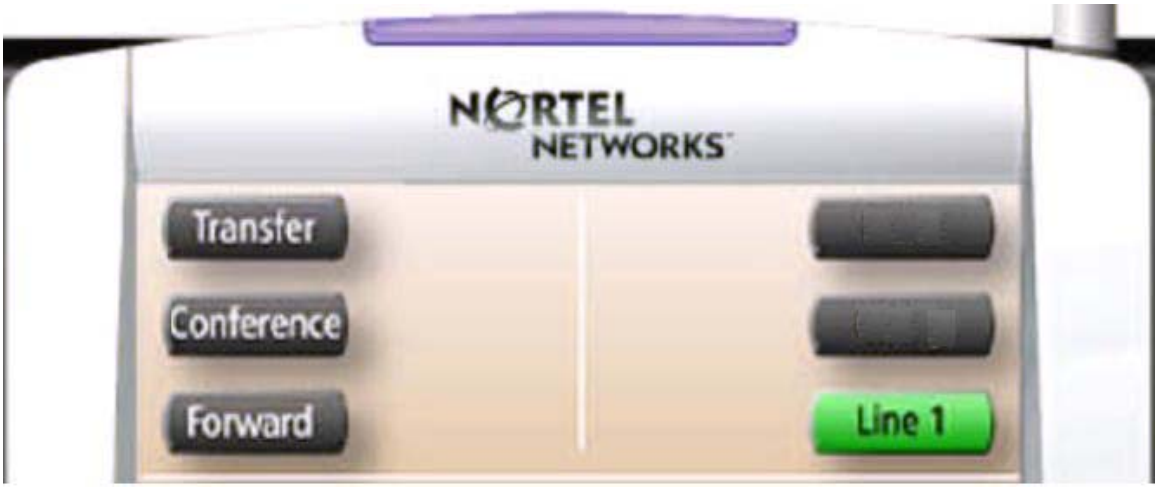
   ```
   tar -xzvf backupfile.tgz
   ```

The following sections provide a detailed procedure on how to restore files for each component that was backed up. Determine which components need to be restored. Follow the restore steps for that component if they are relevant to what needs to be restored. For instance, if the keys do not need to be restored, skip that step.

3.4.1.1 Restoring database from a backup copy

The following procedure is used to restore the database from the backup copy. The database is restored to its state when the backup was made. In general this procedure should only be followed when database corruption has occurred on both units of the NGSS. The database must be restored on the **active unit** of the NGSS.

1. Jam the Active Unit.
2. Suspend Call Processing
3. Copy over the database files[1]




```
chmod 700 /opt/apps/database/solid/backup/
solmsg.out
```

5. Run the restorebackup script as shown from the following directory:

```
cd /opt/apps/database/solid_install/

./restorebackup.sh
```

6. Unsuspend Call Processing
7. UnJam the Active Unit

Jamming the active unit is necessary to prevent the database from switching activity while its being restored. The database must be restored on the active unit. No action is needed to restore the database on the inactive unit. The database on the inactive unit is automatically updated by the active unit. Call processing should be suspended since the database will not be available.

[1]For each copy the system asks for confirmation. Please ensure the copy is correct before typing yes.

3.4.1.1 Restoring certificate

Stop the services which use the certificates and copy over the existing ones.

1. Restore **all** files

```
cp -i gen_cert.txt /opt/base/share/ssl/
cp -i server.crt /opt/base/share/ssl/
cp -i trusted.crt /opt/base/share/ssl/
cp -i server.xml /opt/apps/webint/jakarta-tomcat-4.1.30/conf/
```

2. Set the permissions on the files accordingly

```
chmod 644 /opt/base/share/ssl/server.crt
chmod 644 /opt/base/share/ssl/gen_cert.txt
chmod 644 /opt/base/share/ssl/trusted.crt
```

3. suspend the application
4. /opt/apps/webint/tomcatd stop
5. /usr/local/apache/bin/apachect1 stop
6. /usr/local/apache/bin/apachect1 start
7. /opt/apps/webint/tomcatd start
8. unsuspend the application

3.4.1.1 Restoring system data

Copy over and set permissions on the files that need to be restored.

1. Copy over the following files as needed

```
cp -i hosts /etc/
cp -i passwd /etc/
cp -i group /etc/
cp -i ntp.conf /etc/
cp -i shadow /etc/
cp -i ifcfg-eth0 /etc/sysconfig/network-scripts/
cp -i netnodes /etc/sysconfig
cp -i ssh_host_dsa_key.pub /opt/base/synch_local/common/etc/ssh/
cp -i ssh_host_key.pub /opt/base/synch_local/common/etc/ssh/
cp -i ssh_rsa_key.pub /opt/base/synch_local/common/etc/ssh/
```

2. Set the permissions on the restored files accordingly

```
chmod 755 /etc/hosts
chmod 755 /etc/passwd
chmod 755 /etc/shadow
chmod 755 /etc/group
chmod 755 /etc/sysconfig/netnodes
chmod 755 /etc/sysconfig/network-scripts/ifcfg-eth0
chmod 644 /opt/base/synch_local/common/etc/ssh/ssh_host_key.pub
chmod 644 /opt/base/synch_local/common/etc/ssh/ssh_host_dsa_key.pub
chmod 644 /opt/base/synch_local/common/etc/ssh/ssh_rsa_key.pub
```

3.4.1.1 Restoring web files

1. Copy over the following files

```
cp -i redirect*.jsp /opt/apps/webint/jakarta-tomcat-4.1.30/webapps/prov/jsp/
cp -i redirect_apps.php /usr/local/apache/htdocs/
```

Note: If additional web files need be restored then do a reinstall.

3.4.4 Configuring the backup time on the NGSS

The backup utility is run as a cron job. Cron is the name of a program that enables users to execute commands or scripts at specific times and dates. It is recommended that the backup utility be run daily on the NGSS during off peak hours. As a default setting the backup utility on the NGSS is scheduled to run at 1 AM daily.

Changing the scheduled time of the NGSS backup involves changing the cron programs configuration file: *crontab*. An entry in the crontab file is made up of a series of fields with each separated by a space. An example crontab entry follows:

0 1 * * * /opt/apps/database/solid_install/bkup_solprov.sh

A list of the fields follows:

minute hour day month weekday user cmd

minute: the minute of the hour the command will run on, range 0 to 59.

hour: thehour of the day the command will run on as specified on a 24 hour clock, range 0 to 23, where 0 is midnight.

day: the day of the month the command will run, e.g. to run a command on the 19th of each month, the day would be 19.

month: the month of the year the command will run on, range 0 to 12.

weekday: the day of the week the command will run, range 0 to 7.

cmd: the command/program to run.

To run a program daily set the minute and hour fields and place a ***** in the remaining fields (day, month, and weekday). In the previous example the bkup_solprov.sh program gets run at 1 AM daily.

Notes: Place a * in any unused fields. More than one value may be put into a field by separating the values with commas.

3.5 Hardware Requirements or Dependencies

N/A.

3.6 Software Requirements or Dependencies

N/A.

3.7 Limitations and restrictions

For security reasons *.key and *.keystore files are not backed up by this feature:

/opt/base/share/ssl/certificate.keystore
/opt/base/share/ssl/server.key
/opt/base/synch_local/common/etc/ssh/ssh_host_dsa_key
/opt/base/synch_local/common/etc/ssh/ssh_host_key
/opt/base/synch_local/common/etc/ssh/ssh_rsa_key

3.8 Interactions

N/A.

3.9 Glossary

Term	Description
CLI	Command Line Interface
CRONTAB	Cron Table
DB	Database
NGSS	Next Generation Session Server

3.10 References

A00006979 *Synchronized Backup and Restore Manager*
A00009266 *Siren[1] HLD Backup and Restore Framework*

[1]The NGSS may transition to the Siren platform at some future release.

4: Functional Description (FN): A00007544

4.1 Feature name and Feature ID

A00007544: NCAS Link and SIP NMS Support based on RFC 3842.

4.2 Description

This development includes following two separate but interdependent design:

- Non-Call Associated Signaling (NCAS) link development.
- Session Initiation Protocol (SIP) based network message waiting service (NMS) support based on RFC 3842.

4.2.1 NCAS Link Development

The NCAS Link provides a light weight switching control point (SCP) like functionality. The NCAS link provides a non-call associated link between the Communication Server 2000 (CS2K) Session Server (SS) (formally known as Next Gen Session Server (NGSS)) and the CS2K Core (Brisk/88K, XA-Core and Compact/3PC). The NCAS link is used by the SIP NMS support based on RFC 3842.

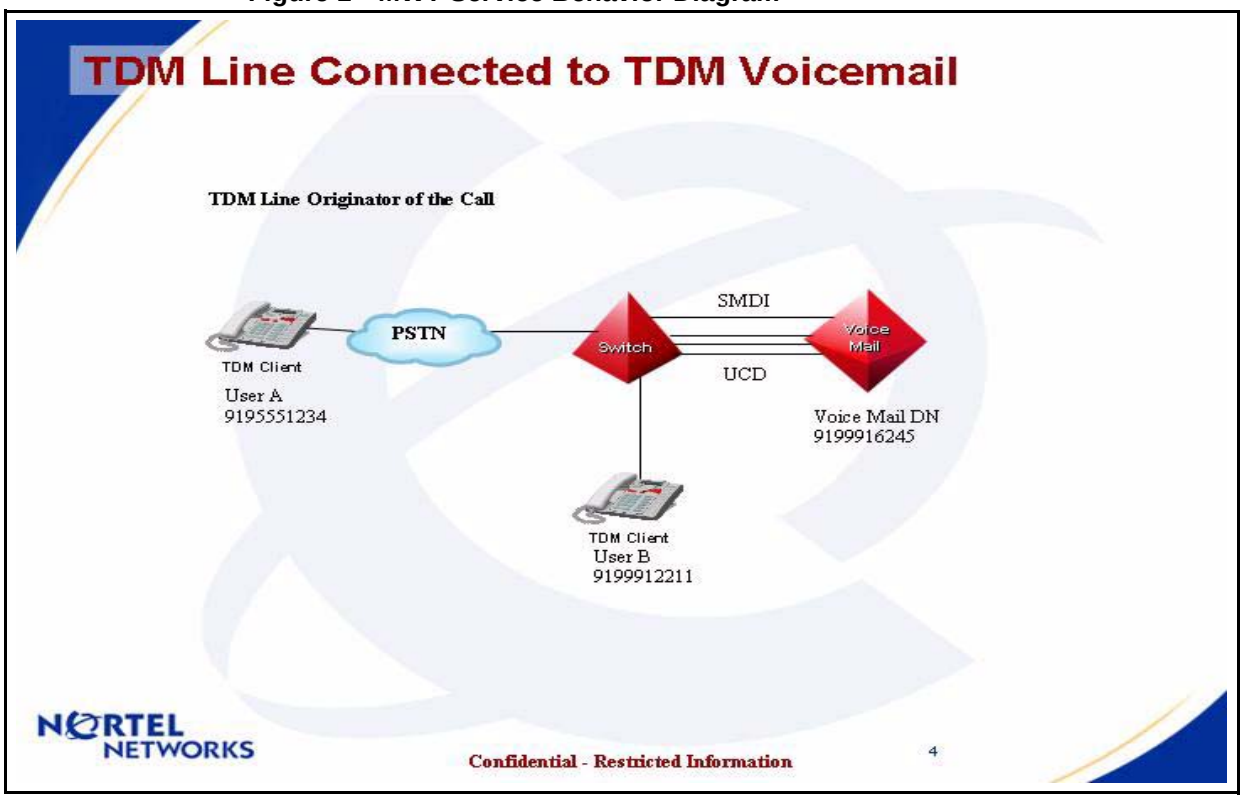
In the CS2K Core, NCAS link development is done under activity A00004500 in SN07. However, this development did not consider some internal drawback associated with Intelligent Network Access Point (INAP) signalling. Therefore, under this activity, the INAP drawback has been removed.

4.2.2 SIP NMS Support based on RFC 3842

The Message Waiting (MWT) service is a CS2K Core based service. The complete MWT service, includes Voicemail system (VM) to record voice messages and retrieve voice messages, communication link between CS2K Core and VM, the MWT service control in the CS2K Core, end user devices to provide MWT Indication (MWI) and CS2K Core based Redirection Services, such as Call Forward Do not Answer (CFD/CFDA) etc.

The following figure provides a pictorial view of how MWT service is provided to an end user and how an end user uses the service in traditional switching environment.

Figure 1 MWT Service Behavior Diagram



The following steps describe the functionality shown in Figure 1 above:

1. User A (In PSTN network) is calling User B (On serving End Office (EO))
2. User B does not answer (User B's CFDA is set to go to DN of VM). Call Forwarding happens and Call terminates to DN of VM.
3. VM answers the call and prompts user A for message. Message is recorded by User A. User A exits and call clears.
4. VM sends a turn on notification to EO for providing MWT functionality to User B.
5. EO sends appropriate message to User B's device to turn on the MWT Indication (MWI).
6. User B finds MWI, initiates call request for retrieval (CRR) functionality. The call terminates to DN of VM.
7. VM answers the call and prompts User B for User ID and Password for authentication. User B enters appropriate details. The VM play the message from User A to User B. User B can continue to interact with VM.
8. VM sends a turn off notification to EO for providing MWT functionality to User B.
9. EO sends appropriate message to User B's device to turn off the MWI.

The above functionality provides support for the traditional MWT service along with a traditional Voice Mail system. Increasingly, number of customers are deploying the VM connection with the CS2K Core or equivalent class 5 switches in a network mode. In this case, the customers have to maintain only one VM for mutiple customers servred via different class 5 switches (including CS2K). The existing software in CS2K Core already provide this service using NMS based on GR-866_core using SS7 network.

Due to advancement of Unified Messaging (UM) which combines all type of mail messages (e.g. Voice Message, E-mail, Paging etc.) and Voice over Internet Protocol (VoIP), an increasing emphasis to provide same functionality using SIP based on RFC 3842.

The MWT functionality to CS2K Core based SIP lines is developed under SIP lines development plan (Please refer to actid A0000 - for CS2K Core design, actid A0000 - for CS2K GWC design and actid A0000 - for CS2K SS design). The communication between CS2K SS and SIP Line is based on the RFC 3842.

Deployment of the SS7 network is expensive proposition in the VoIP network. While SIP based on RFC 3842 can provide similar network capability using SIP messages between two CS2K or a CS2K and SIP compliant remote node (e.g. MCS). This feature develop necessary software in CS2K SS to support RFC 3842 based message waiting SIP messages and expands existing NMS software in CS2K Core to use the SIP network to provide network message waiting service to/from remote CS2K or SIP compliant remote node.

This feature does not cover development needed in SIP clients, SIP compliant remote node and SIP compliant VM.

Based on the converged network needs and support for multiple interfaces following end user devices are supported:

- Traditional Phones (e.g POTS, RES, IBN, KSET etc.)
- CICM IP sets
- Traditional Lines off of a remote switch
- Traditional Lines off of a remote SIP domain
- Traditional Lines off of a PBX
- SIP lines served by MCP 5100/5200.

Also, following interfaces to a message server (Voicemail) system are supported:

- Traditional SMDI and UCD/HUNT group to VM.
- Traditional VM using public SS7 network for NMS.
- Traditional VM using SIP NMS based on RFC 3842.
- SIP NMS based on RFC 3842 for MCP 5100/5200 platform.

The combination of above user devices and VM interfaces are supported with following interoperatibility limitations.

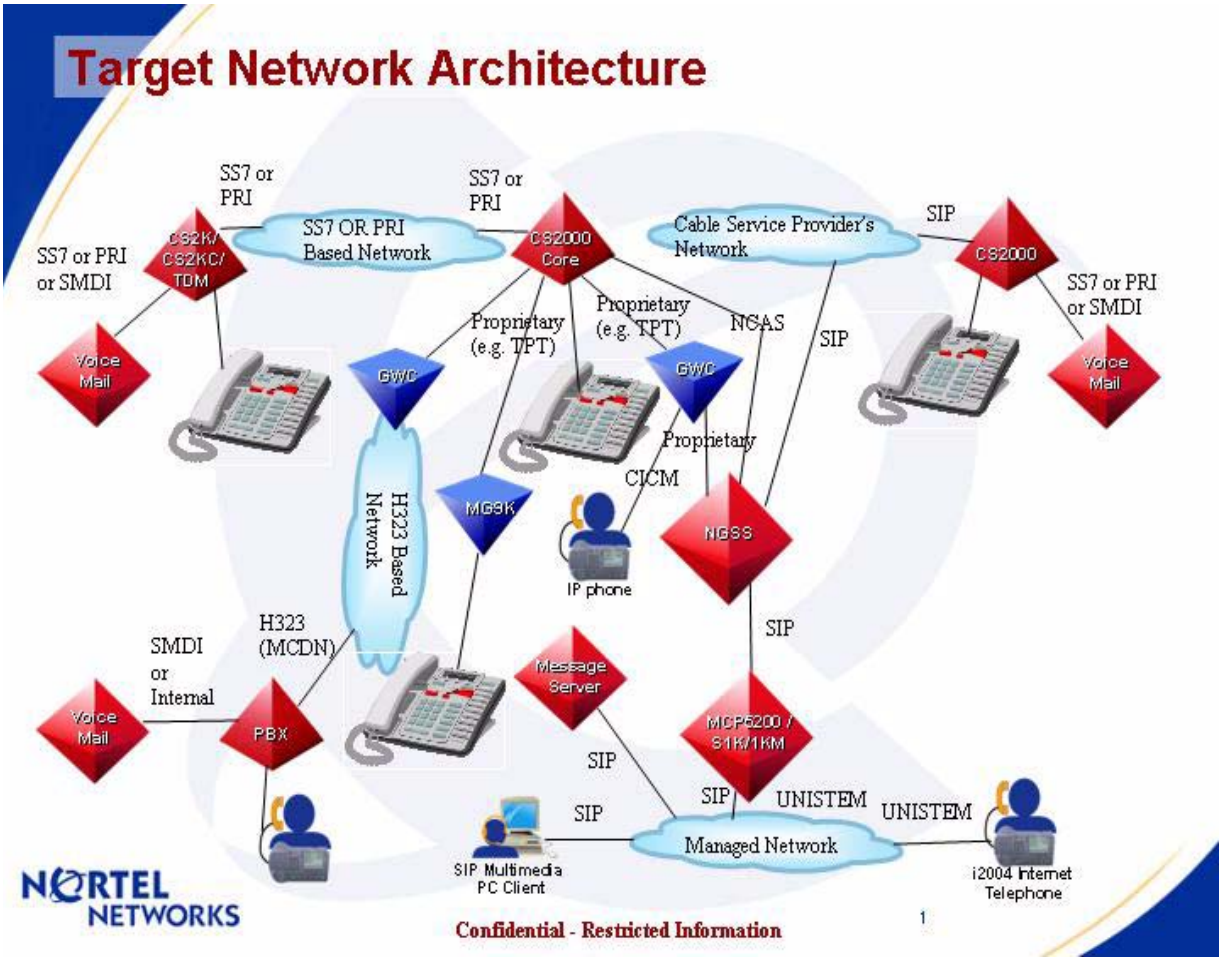
The design is generic and based on RFC 3842 standards, we are unable to test every possible interoperatibility using different handware and different vendor equipments. Therefore, we can only be able to claim the support for the tested networks. In order to make other hardware and different vendor equipment supported, proper interoperatibility testing must be done in Nortel approved interoperatibility lab. After the complete testing, appropriate support will be provided for them.

For Cable network support we need a design lab with appropriate Media Terminal Adaptors (MTAs). For design testing, no such lab identified yet. Without this testing, we can not claim the compatibility with cable specification for this feature.

4.2.3 Target Network Architecture

The feature develops a converge network architecture. In this architecture of the Message Waiting the VM or Message Server (MsgSrv) can resides any network and the user device can resides in any network. The communication required for MWT service is supported by this architecture. The following figure (Figure 2) is pictorial representation of the target architecture.

Figure 2 Target Architecture



With this development, MWT is provided across the different type of networks within Service Provider's network. The following are the advantages to the service provider:

- Support of MWI on user's choice of device
- Consolidation of the VM system in service provider's network
- Converged network support
- MWI to SIP clients or S1K/1KM

Other topologies and how MWT service provided are described in "Supported Configurations" on page 65.

4.2.4 Supported Configurations

The connection and communication bases the supported configurations are separated in two catagories. 1) Configurations of Voicemail or MsgSrv systems and 2) Configurations of Lines or clients.

The configurations described here are specific to MWT service and VM communications for MWT service. These configurations assumes that the call related communications and signalling are provoided prior to the MWT service and exists in the given configuration.

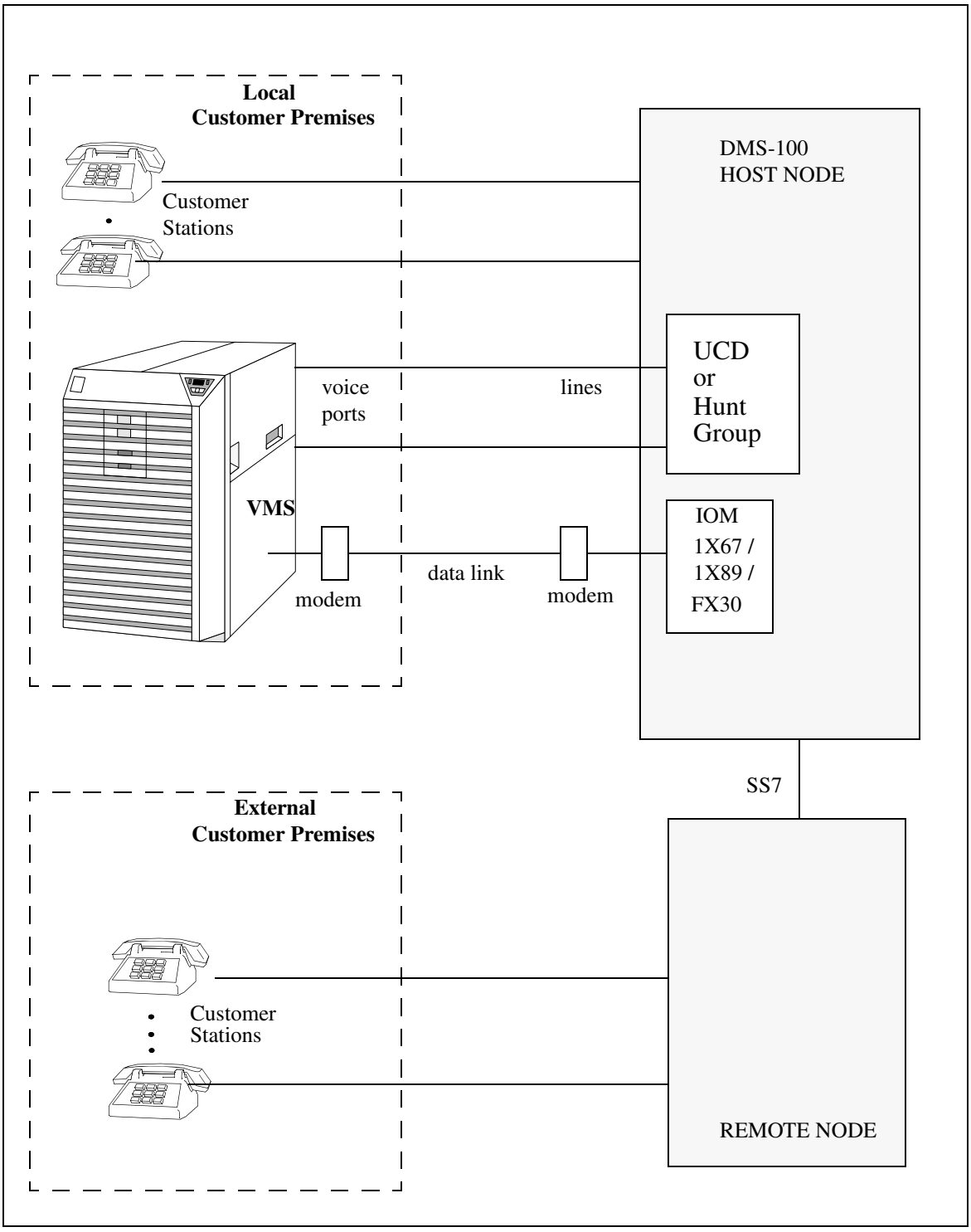
4.2.4.1 Configurations of Voicemail or MsgSrv Systems

The following configurations are separated by the protocol used for communication between CS2K and VM system:

4.2.4.1.1 Traditional VM communication using UCD/HUNT group and SMDI link

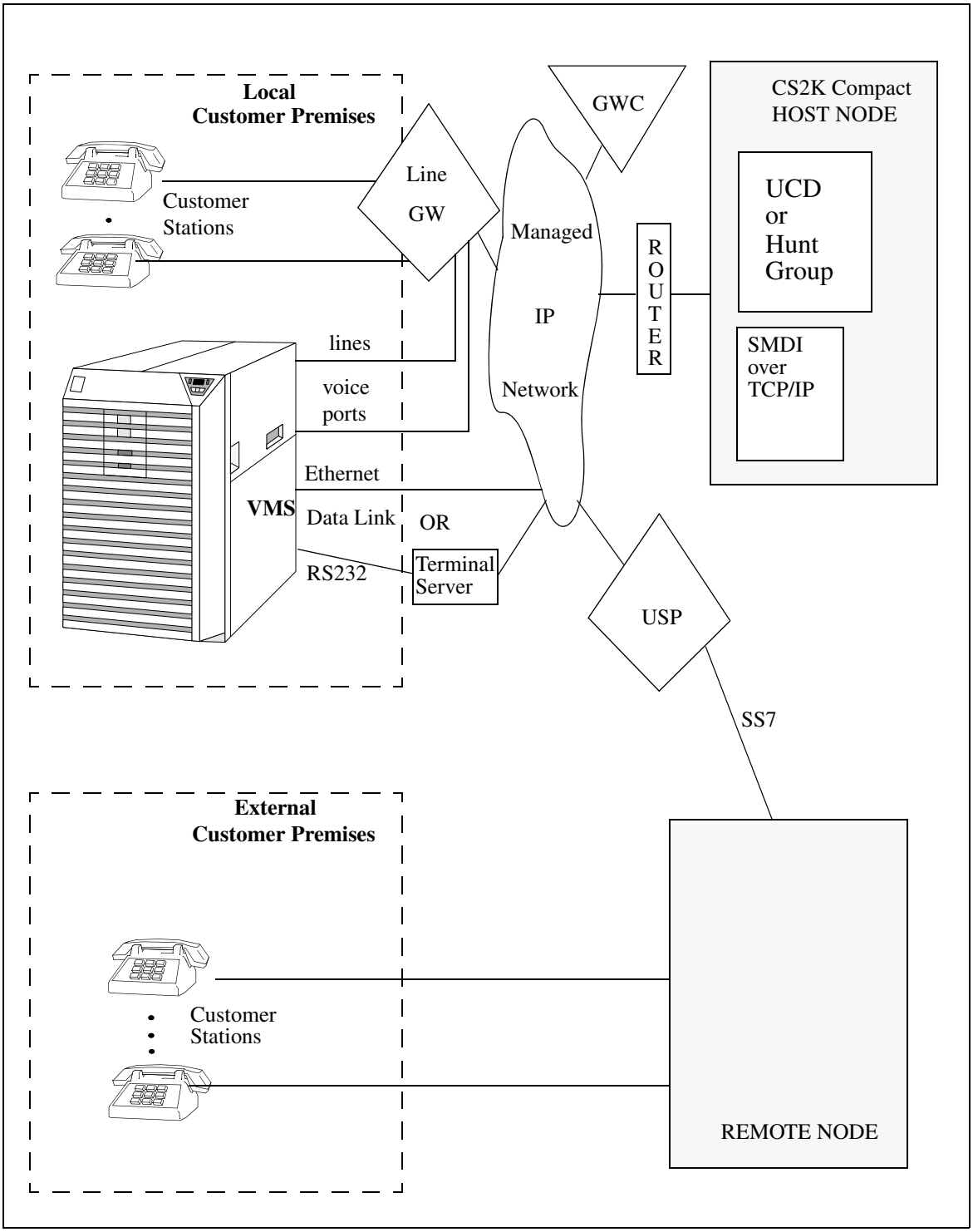
This is an existing and supported configuration in CS2K/DMS. For details on this configuration, please look in the NTP 297-2051-104- SMDI Setup and Operation. The following figure is a generic view of this configuration in DMS:

Figure 3 Simple VM Configuration in DMS



The data link in above Figure 3 is based on SMDI specifications described in the GR-283-Core. The following figure provides simple VM configuration in the CS2K Compact:

Figure 4 Simple VM Configuration is CS2K Compact



In Figure 4 , the communication between the CS2K Compact and VM is SMDI based on GR-283-Core. However, the transport medium is TCP/IP. The

details of this configuration can also be found in the NTP 297-2051-104 - SMDI Setup and Operation.

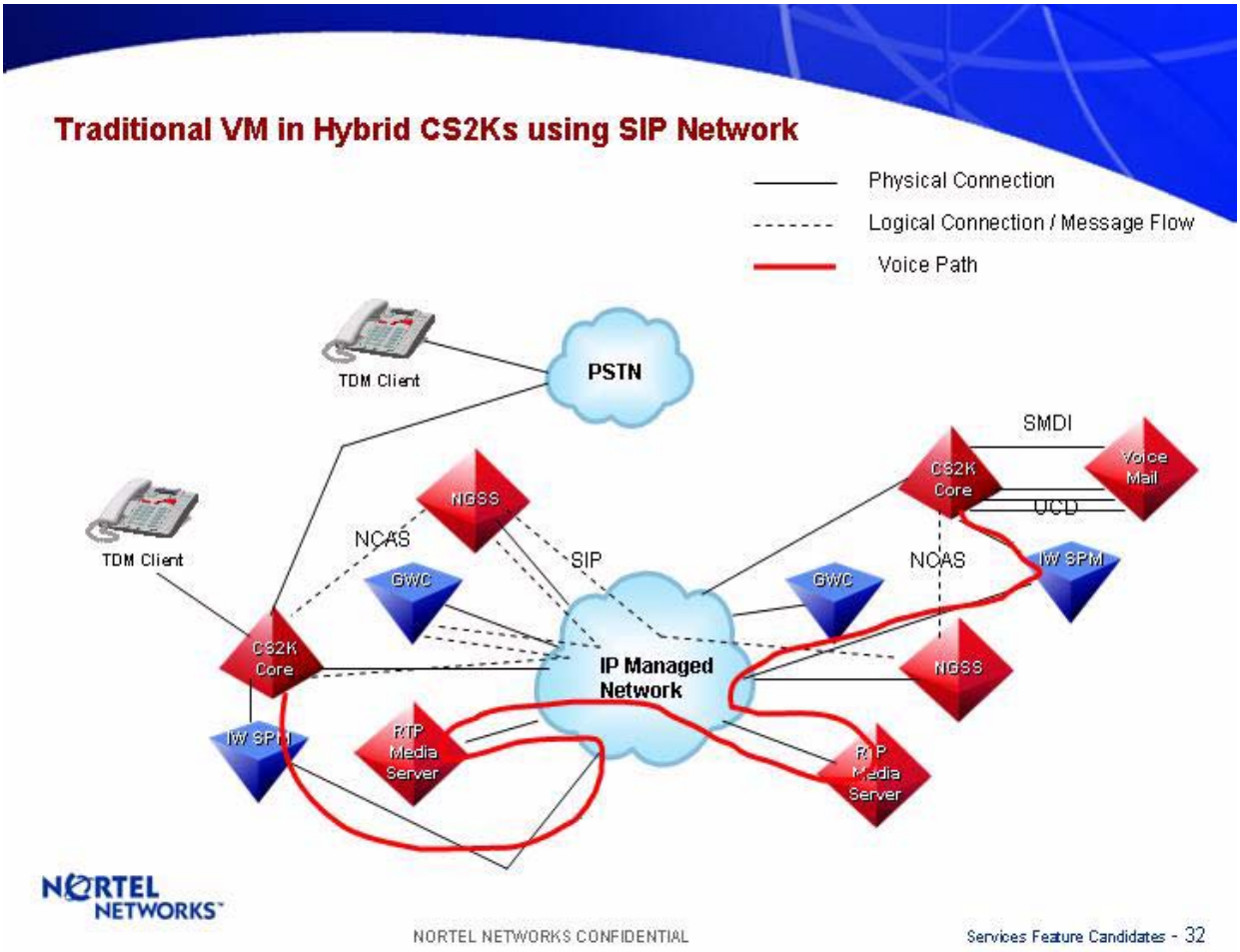
4.2.4.1.2 Network VM communication using SS7 network

The Figure 3 and Figure 4 also describe the configuration of the VM communication using SS7 network between host node and remore node. For details, please see NTP 297-2051-104 - SMDI Setup and Operation; and NTP 297-8021-350v13 - North American Translation Guide Volume 13 of 25.

4.2.4.1.3 Traditional VM communication using SIP network

This configuration, the VM is a traditional VM connected to one CS2K via SMDI and UCD/HUNT group. The line is on another CS2K. The RFC 3842 based SIP messages are used between two CS2K to pass MWI information for NMS.

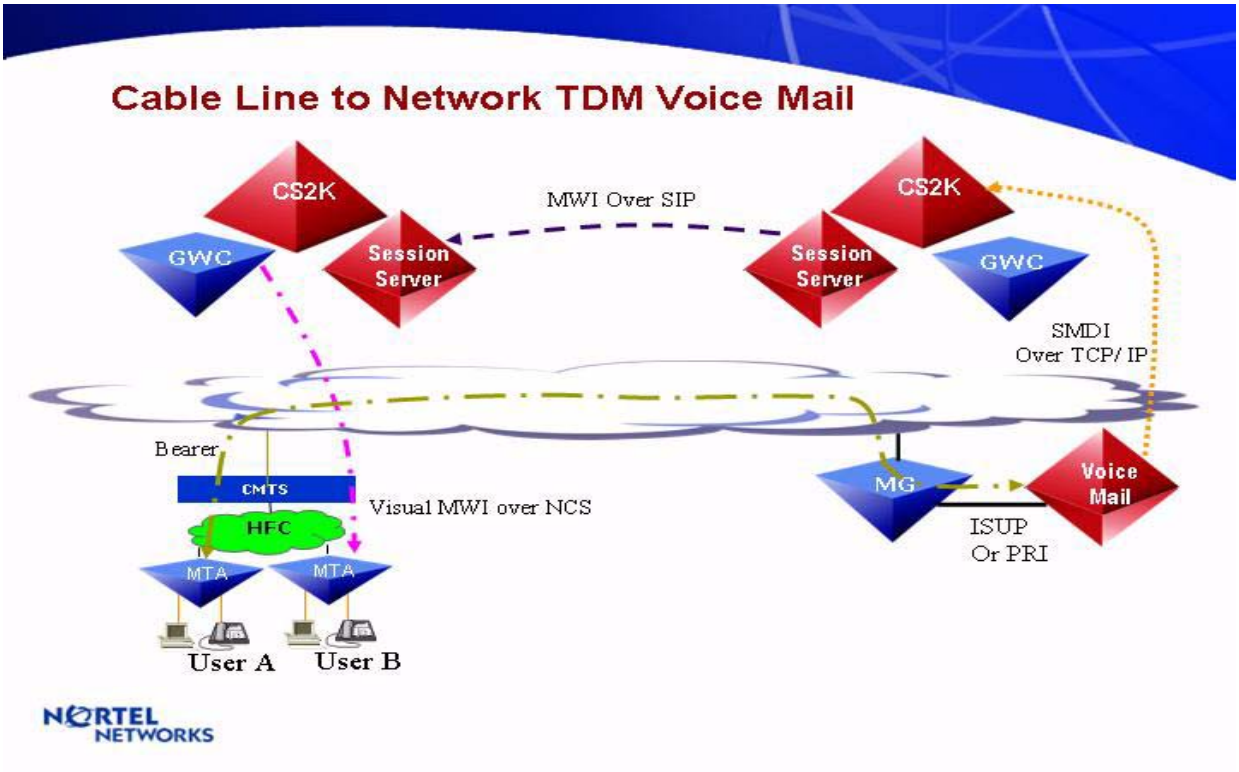
Figure 5 Traditional VM communication using SIP network



4.2.4.1.4 Network VM communication using SIP for Cable Service Providers

In cable service provider network, the VM is connected to a CS2K compact as described in previous section. However, the communication between two CS2K Compact is based on the managed IP network using SIP signalling.

Figure 6 VM in Cable Network

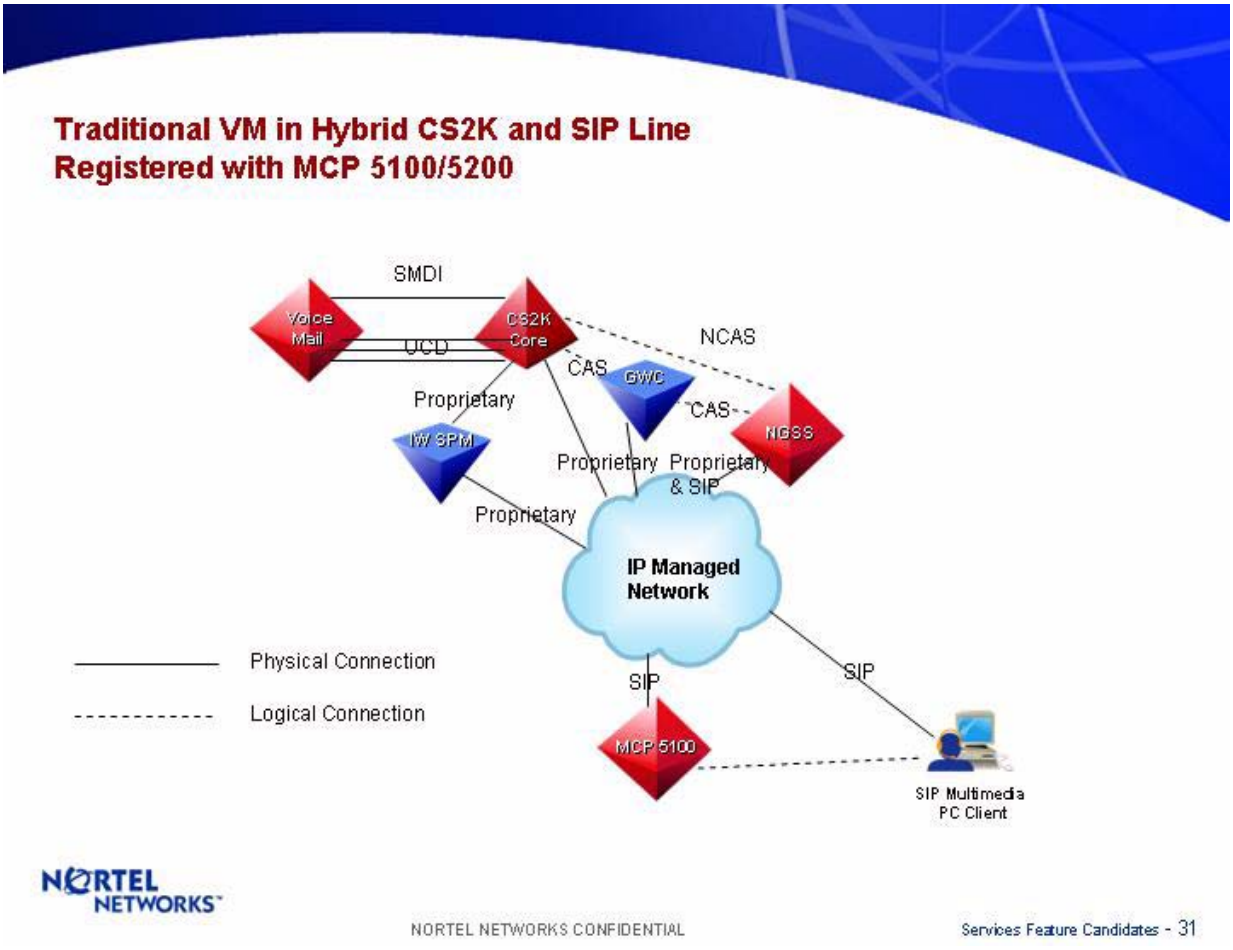


Note: The complete interoperatibility and compliance depends on the availability of the design lab. This configuration is quite similar to configuration describe by Figure 5 in previous section. The only major difference is the usage of MTA and conformance testing for cablelab specifications.

4.2.4.1.5 VM support for MCP 5100/5200 Platform using SIP network

This configuration, the VM is a traditional VM connected to one CS2K via SMDI and UCD/HUNT group. The SIP line is registered with the MCP 5100/ 5200 platform and SIP line is served by the traditional VM. The CS2K is sending RFC 3842 defined SIP messages to MCP 5100/5200 platform to provide network based MWI service.

Figure 7 VM support for MCP 5100/5200 using SIP network



4.2.4.2 Configurations of Lines or clients

The details of these configurations (datafill and setup) are described in the CN section of the feature. The following configurations are separated by the protocol used for communication between CS2K and line/client:

4.2.4.2.1 Lines connected via LCM/XPM

The phone line which is connected via LCM/XPM using PSTN network to the host node are supported today. In case of the SIP VM, these type of lines are considered as non-SIP lines and appropriate additional configuration is required in the Session Server.

4.2.4.2.2 Lines connected via Gateways

The phone lines which are connected via a MG9000 behave the same as traditional line connected to the CS2K via LCM/XPM. There is no change anticipated in this configuration. The CICM lines which are connected via an

IP gateway behave the same. There is no imapct to thier setup and operation. In case of the SIP VM, these type of lines are considered as non-SIP lines and appropriate additional configuration is required in the Session Server.

4.2.4.2.3 Lines connected to a remote node

The lines connected to a remote node (e.g. PBX, another switch, MCP etc.) are considered as networked lines. For these lines network message waiting (NMS) service is provided. The CS2K does not store any data associated with these remote lines.

4.2.4.2.4 Media Terminal Adaptor

The media terminal adaptor is used in the cable network to provide media (voice) services. From the CS2K perspective, the media terminal adaptor is same as a line in the CS2K supported via gateways and gateway controller. The MWT service is provided to the Media Terminal Adaptor same way as it is provided to lines connected via gateways.

> ***Note:*** The complete interoperatibility and compliance depends on the availability of the design lab. The availability of MTA will allow us to perform this cable network requirement. However, it will not be tested, if no lab or MTA available. If we assume that the MTA cable line is another line in the CS2K and behave same way as any other line with MWT service assignment, than this design will support the MTA.

4.2.4.2.5 Single Physical Line with Multiple VM Access

Current design of MWT service in the CS2K does not restrict a single physical line to have access to multiple VM systems. With this design, there is no change to such support. The support is provided using the datafill of the Call Forwarding on the single physical line. The following example explain how this works:

Line B is a KSET line with two different DN keys and has MWT service assigned to it.

The first key's DN is datafilled with call forwarding busy (CFB) and call forwarding do not answer (CFD) and call forwarding number to DN of VM 1.

The second key's DN is datafilled with call forwarding busy (CFB) and call forwarding do not answer (CFD) and call forwarding number to DN of VM 2.

Now let say first call to DN Key 1 encounters busy condition and forwards to the VM 1. The VM 1 records the message and send a message to CS2K to turn MWT light on for the DN Key 1. The MWT light is now lit for the first message from VM 1.

During the first call, a second call come to the DN key 2 and encounters no answer condition and forwards to the VM 2. The VM 2 records the message and send a message to CS2K to turn MWT light on for the DN Key 2. The request is now enqueued for the VM 2.

When user of Line B retrives the message from the VM 1, the MWT light will remain lit for the second message.

Please note that the MWT request from each VM will be treated as two separate requests in the MWT service.

4.2.4.2.6 Multiple Lines with Single VM Access

The multiple lines in a given CS2K are supported by a single VM. In this case the VM has each line provisioned as individual user. This is already supported functionality. This functionality is not changed by this feature.

If VM is capable to provide multiple MWT messages for multiple lines in a single mail box than it is also suppored because for each line CS2K receive a MWT message.

4.2.4.2.7 Multiple Lines with Multiple VM Access

This configuration is also supported in current design. The following example describes how this is supported.

Line A is a RES line with MWT service and datafilled with CFB and CFD forwarding to DN of VM 1. The VM 1 is on a remote node.

Line B is an IBN line with MWT service and datafilled with CFB and CFD forwarding to DN of VM 2. The VM 2 is on host node.

Line C is a SIP Line with MWT service and datafilled with CFB and CFD forwarding to DN of VM 3. The VM 3 is a SIP VM. The Line C is not registered.

Originator A calls Line A and Line A is busy. The call forwards to VM 1 on remote node. The VM 1 records the message from Originator A. The remote node sends a MWT message to the host node. The request of network MWT is now queued to Line A from VM 1.

Originator B calls Line B and Line B is busy. The call forwards to VM 2. The VM 2 records the message from Originator B. TheVM 2 sends a MWT message to the host node. The request of local MWT is now queued to Line B from VM 2.

Originator C calls SIP Line C and SIP Line C is not registered. The call forwards to VM 3. The VM 3 records the message from Originator C. TheVM

3 sends a MWT message to the host node. The request of network MWT is now queued to Line C from VM 3. The MWT notification is not sent to the Line C because it is not register. When the user of Line C sends a subscribe message for MWT after registration, the CS2K sends the current status of the MWT service in the CS2K to the line C.

4.2.5 Sample Message Details for SIP

The message details are based on the SIP Line configuration described above.

Step 1: The SIP Line SUBSCRIBE for MWT service.

Figure 8 SIP Line Register with CS2K - SUBSCRIBE Message

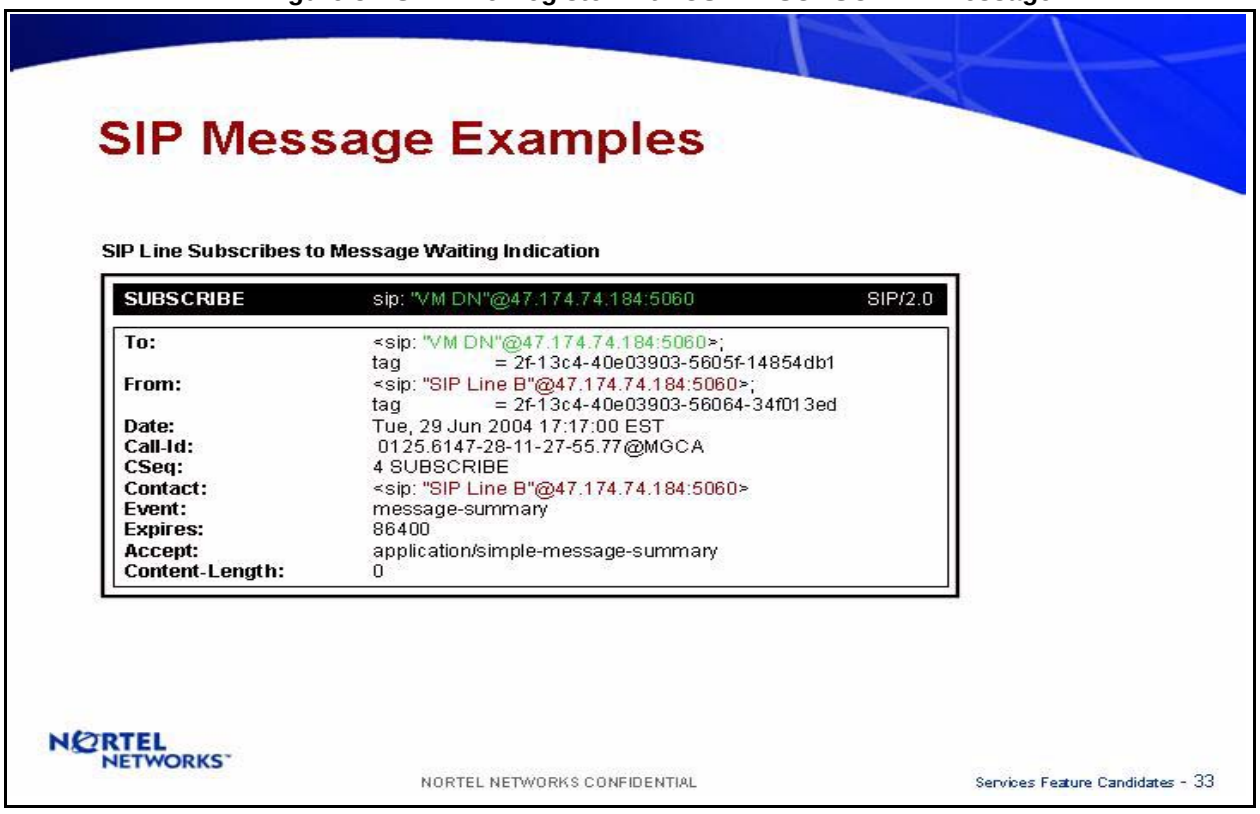


Figure 9 SIP Line Register with CS2K - OK Response

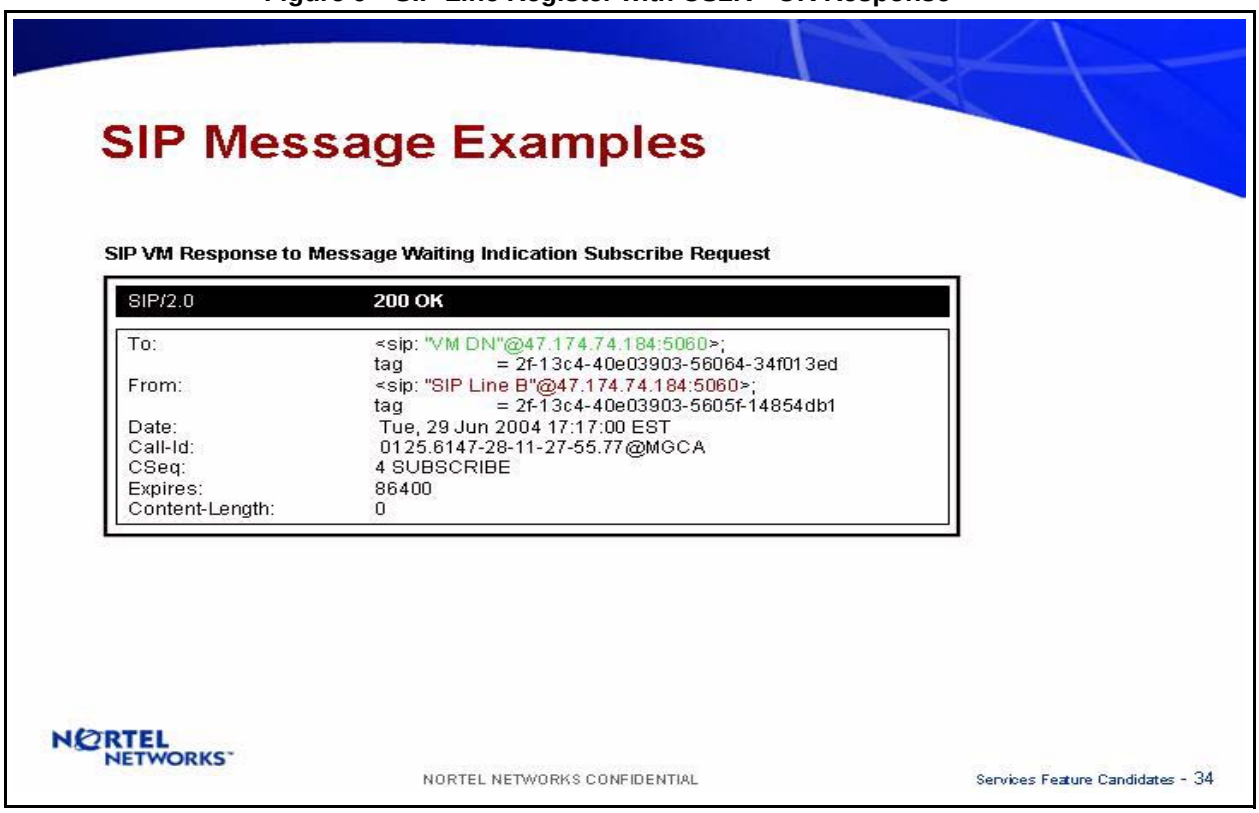


Figure 10 SIP Line Register with CS2K - NOTIFY Message

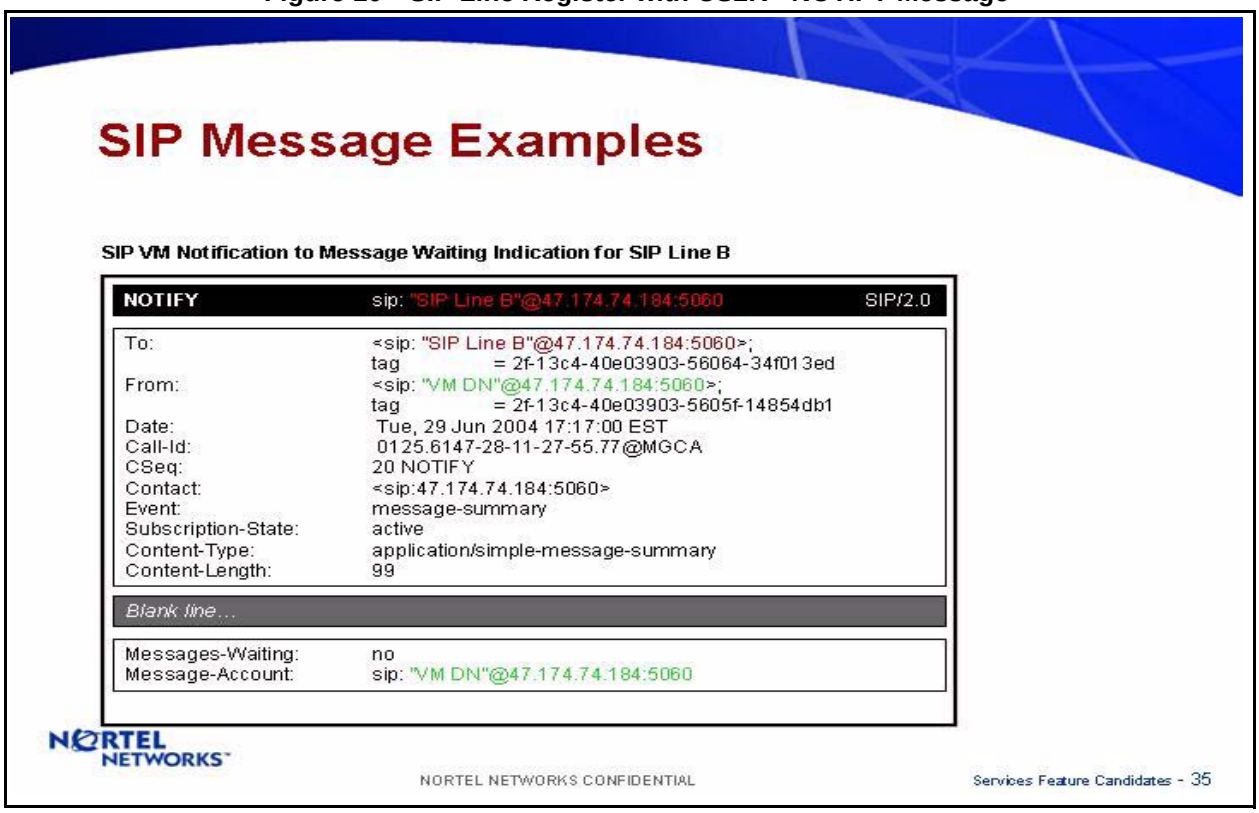
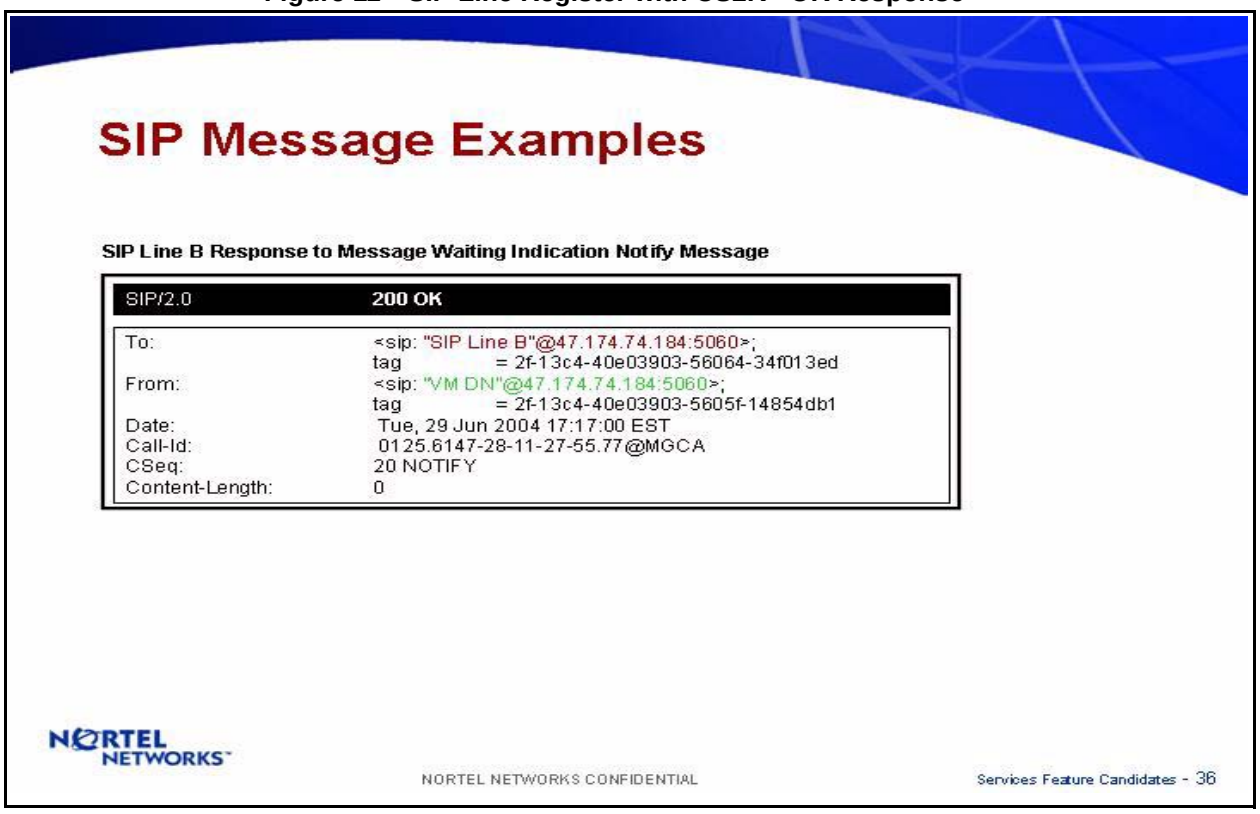


Figure 11 SIP Line Register with CS2K - OK Response



Step 2: Line A Calling SIP Line B and Forwarded to VM using SIP network

Figure 12 Call Termination to SIP VM DN - INVITE Message

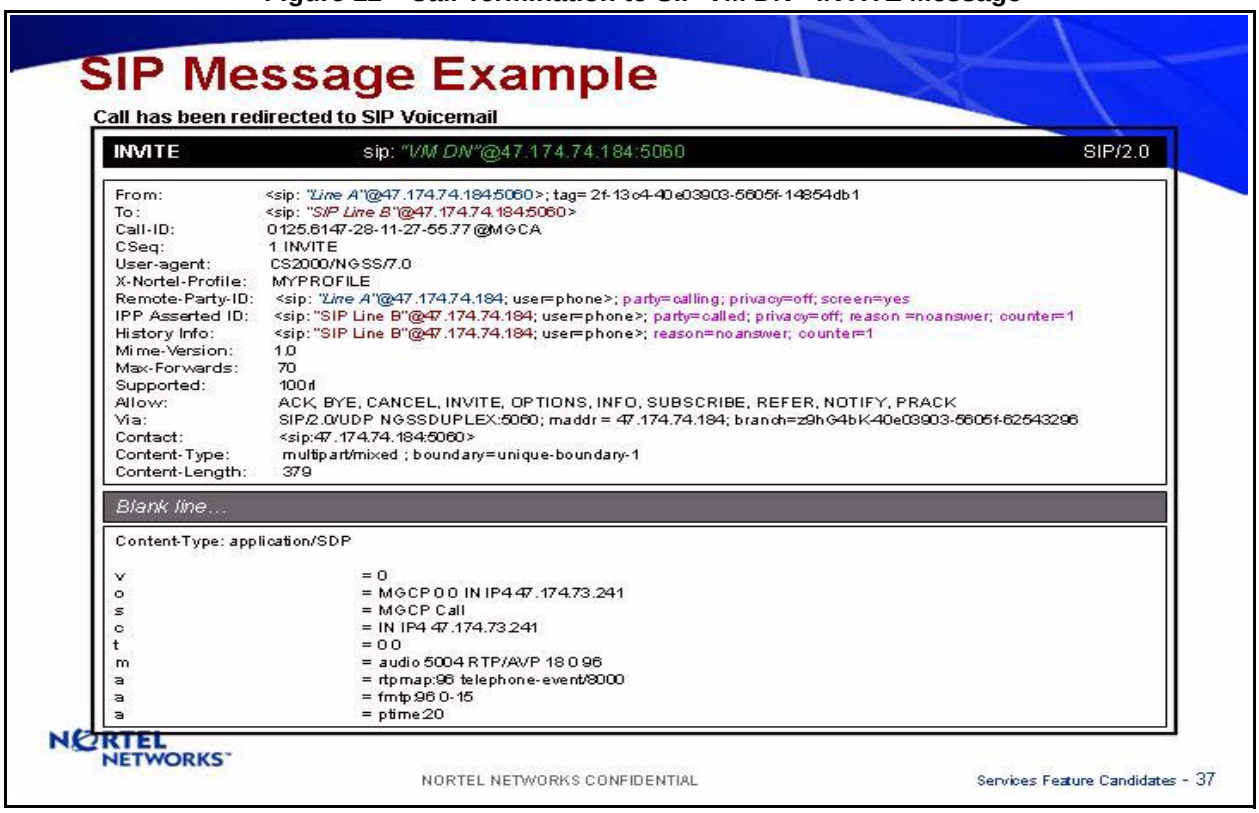


Figure 13 Call Termination to VM DN - 100 Trying Response

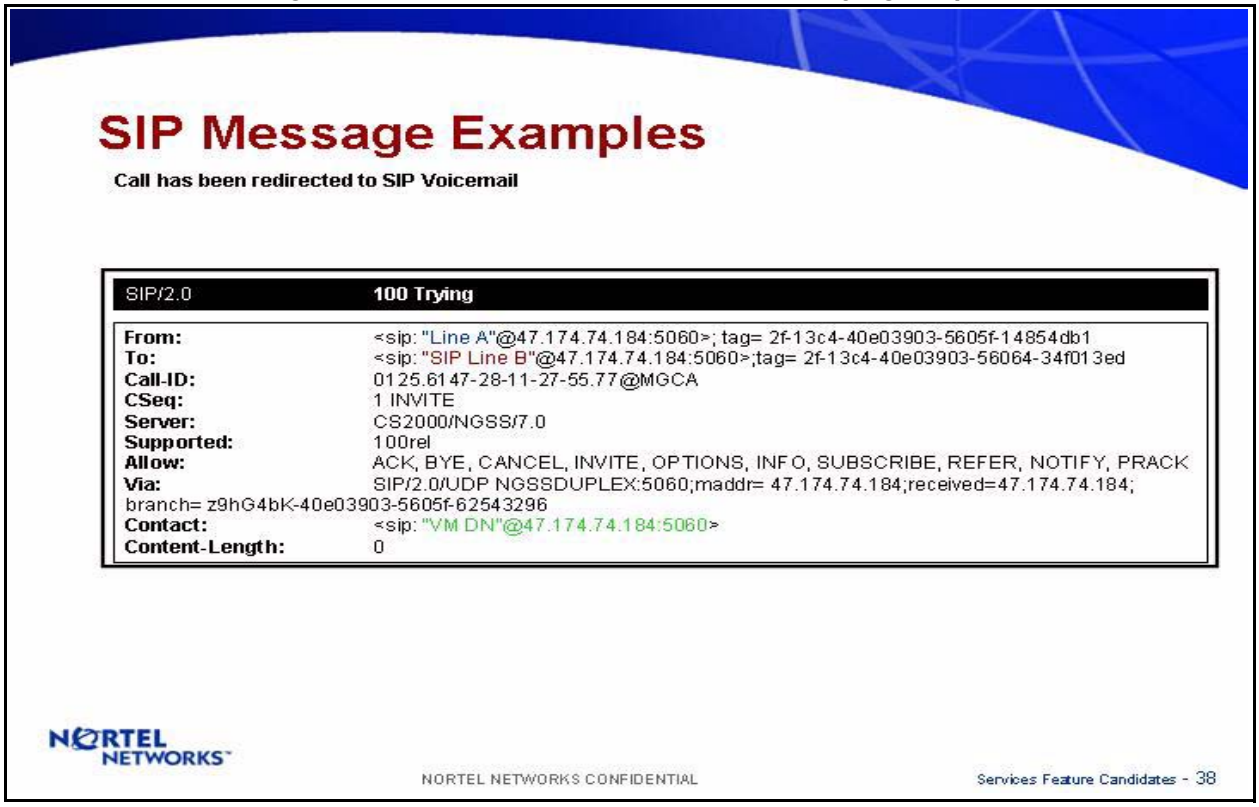


Figure 14 Call Termination to VM DN - 180 Ringing Response

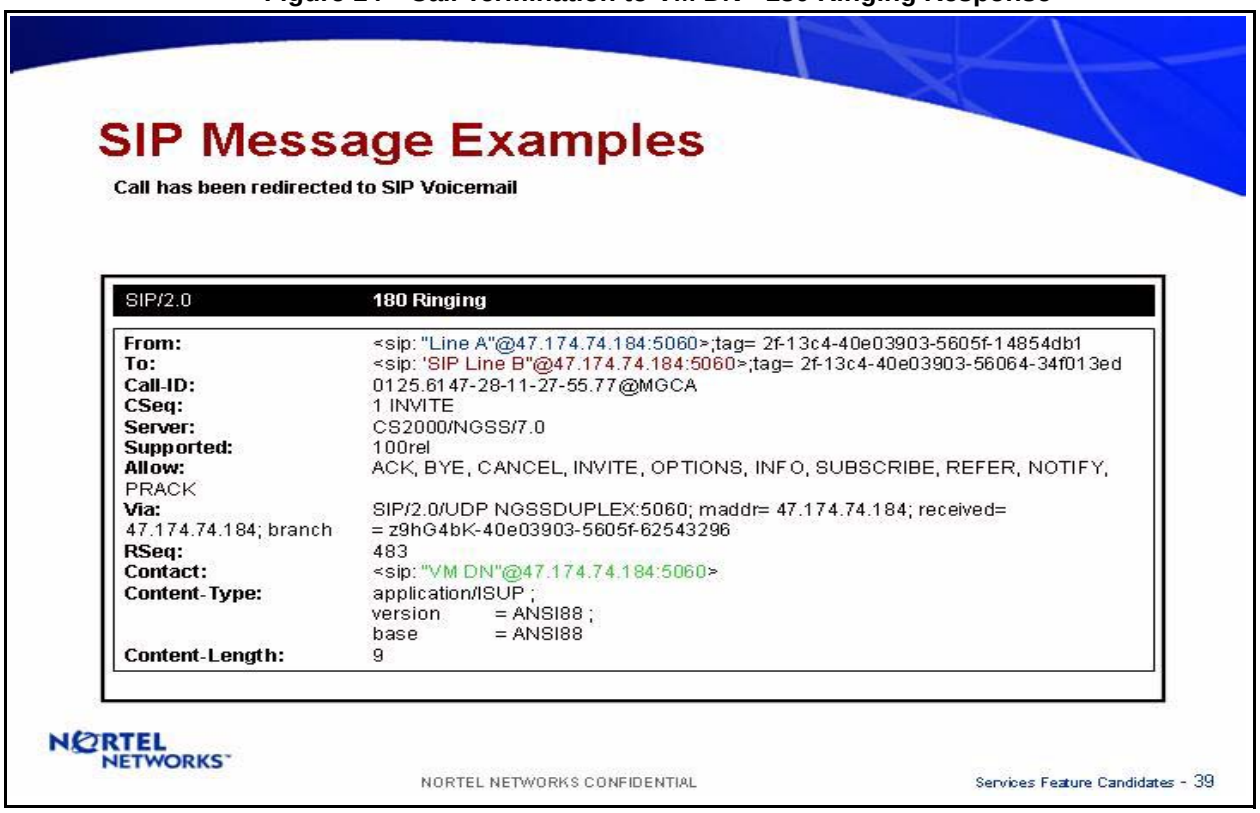


Figure 15 Call Termination to VM DN - 200 OK Response

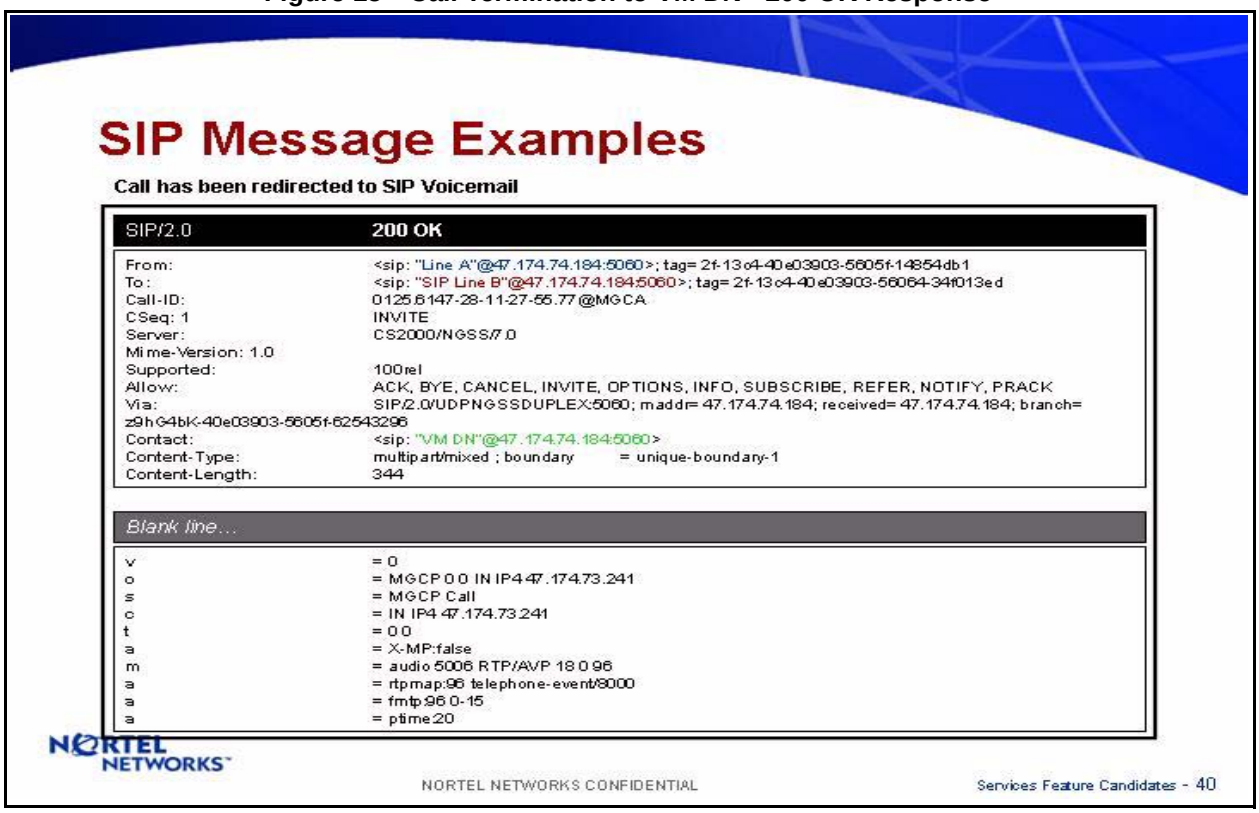
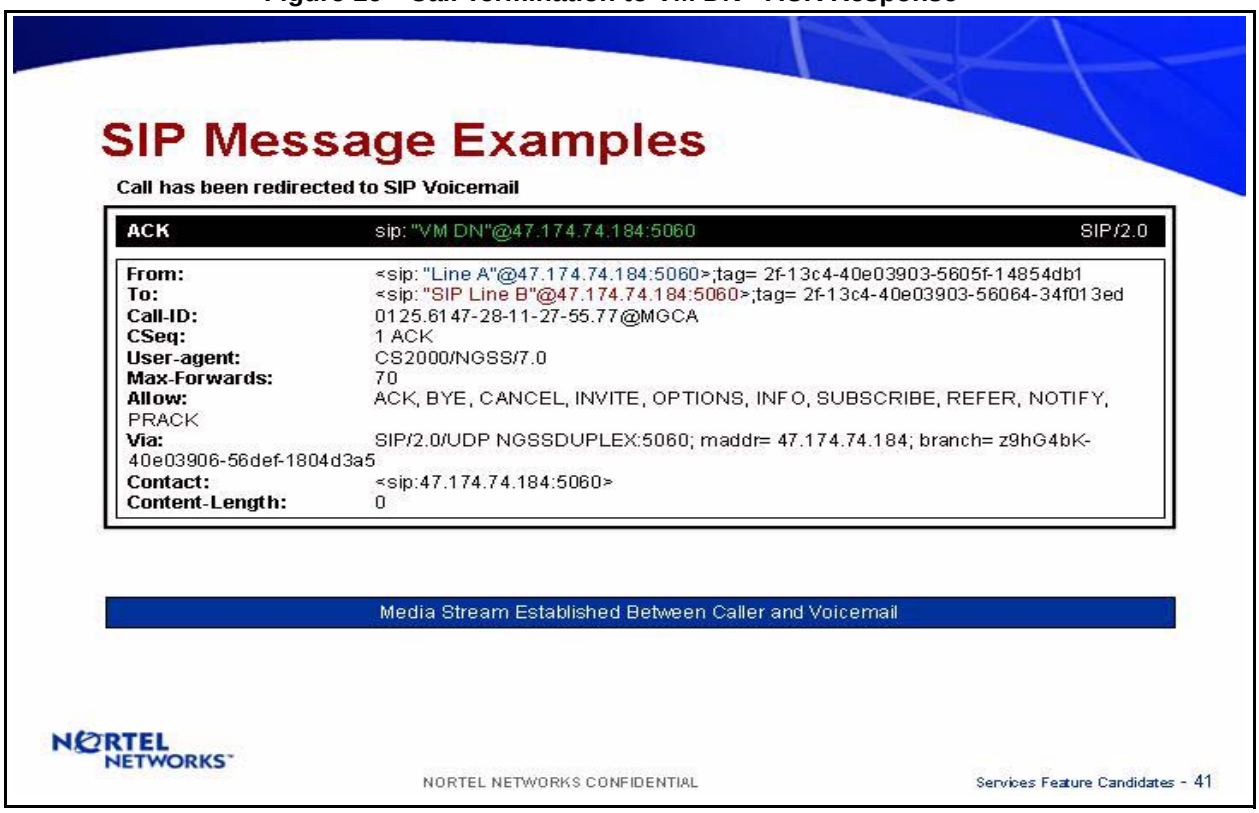


Figure 16 Call Termination to VM DN - ACK Response



Step 3: Caller Records Message and hang-up

Figure 17 Call Release from Caller - BYE Message

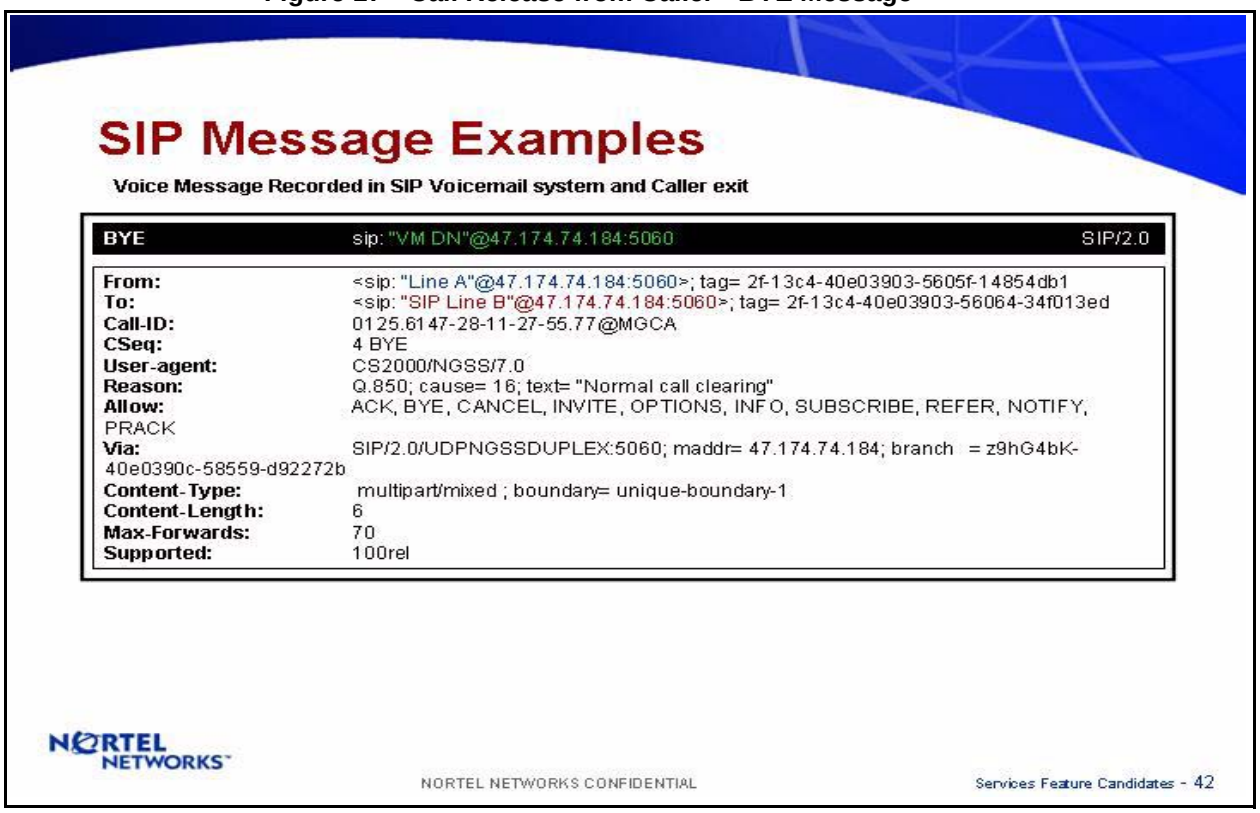
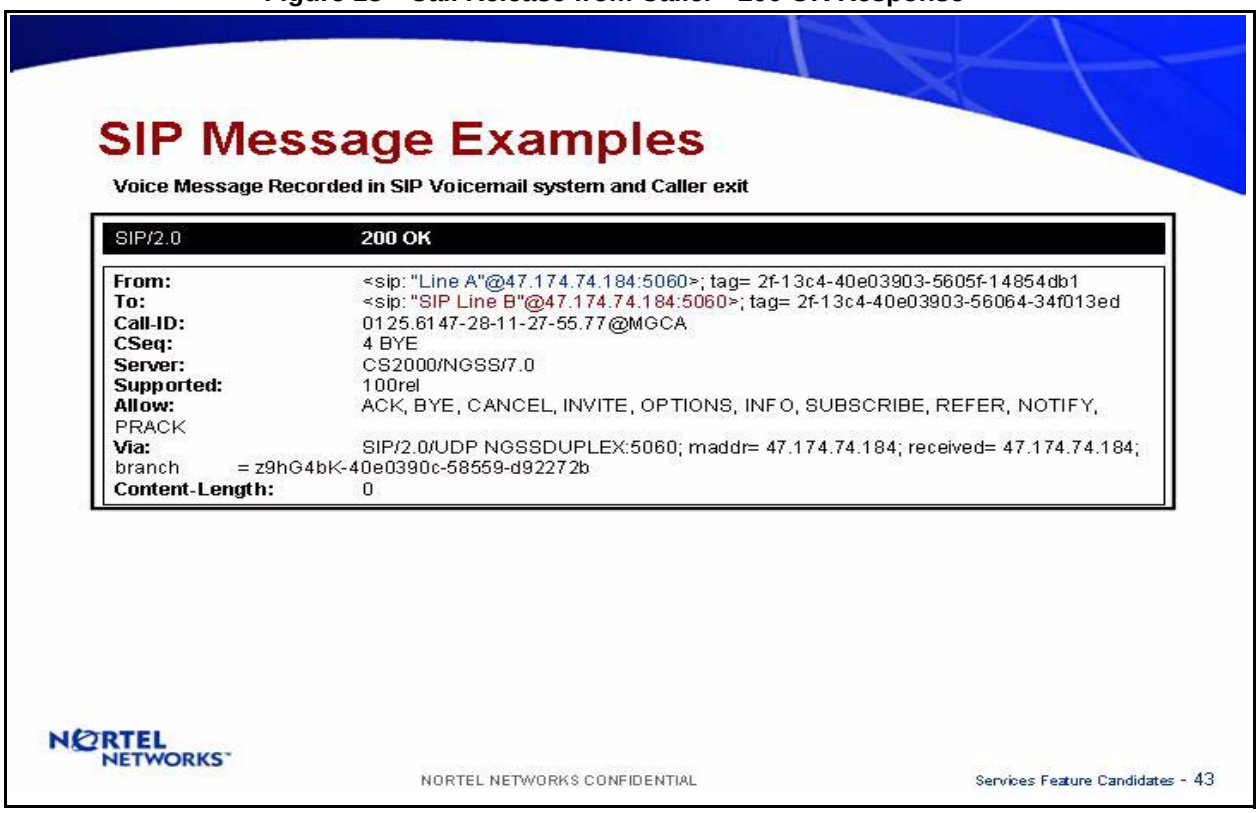


Figure 18 Call Release from Caller - 200 OK Response



Step 4: CS2K sends a NOTIFY Message

Figure 19 CS2K sends NOTIFY Message

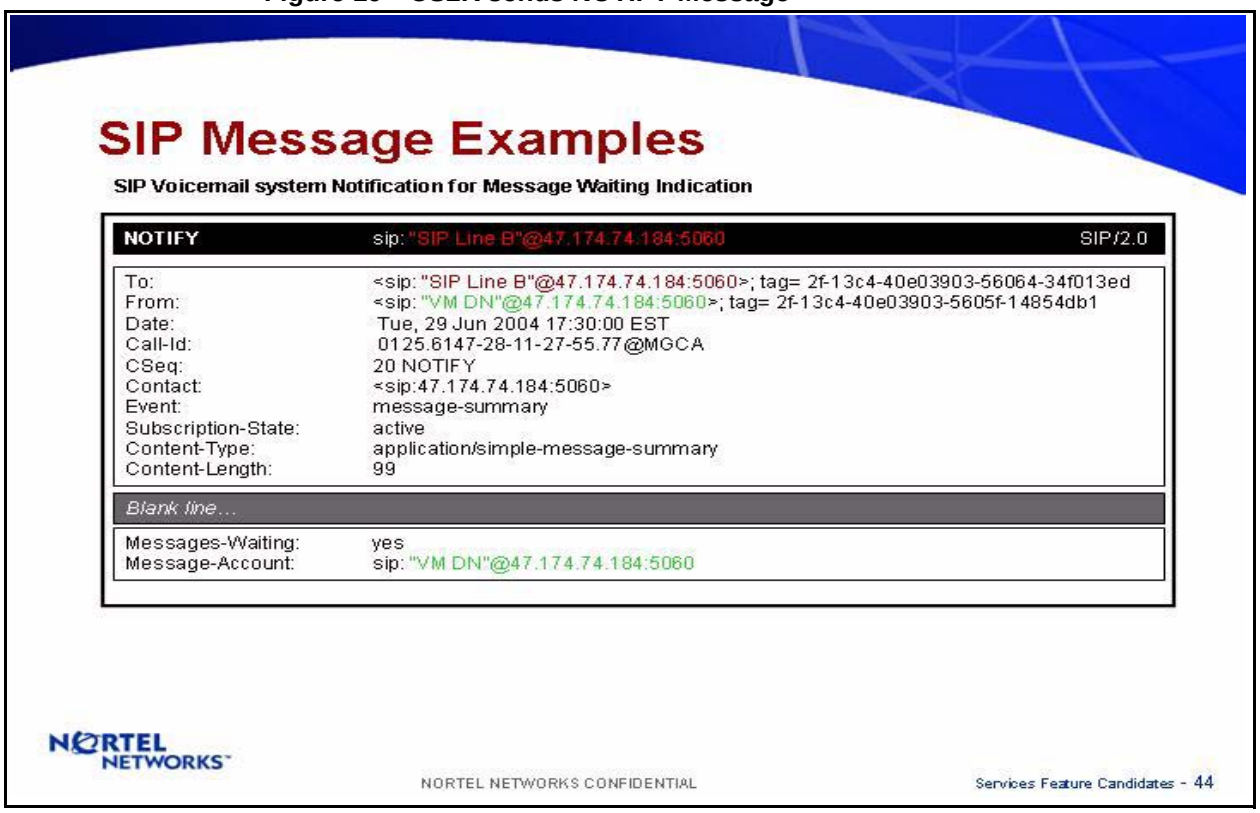
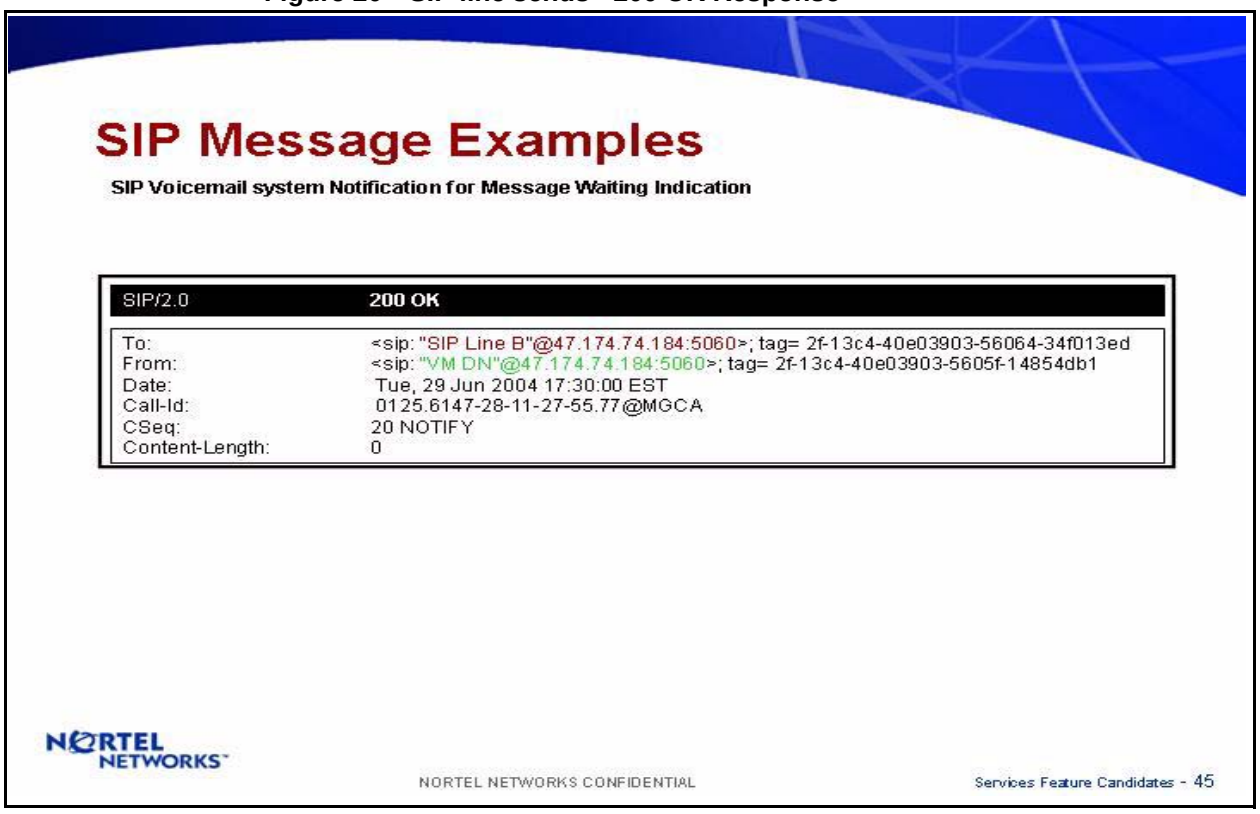


Figure 20 SIP line sends - 200 OK Response



Step 5: SIP Line retrieves the Messages from the VM using SIP network

Note: The SIP messages are related to basic SIP call.

Figure 21 SIP Line B Calling VM DN - INVITE Message

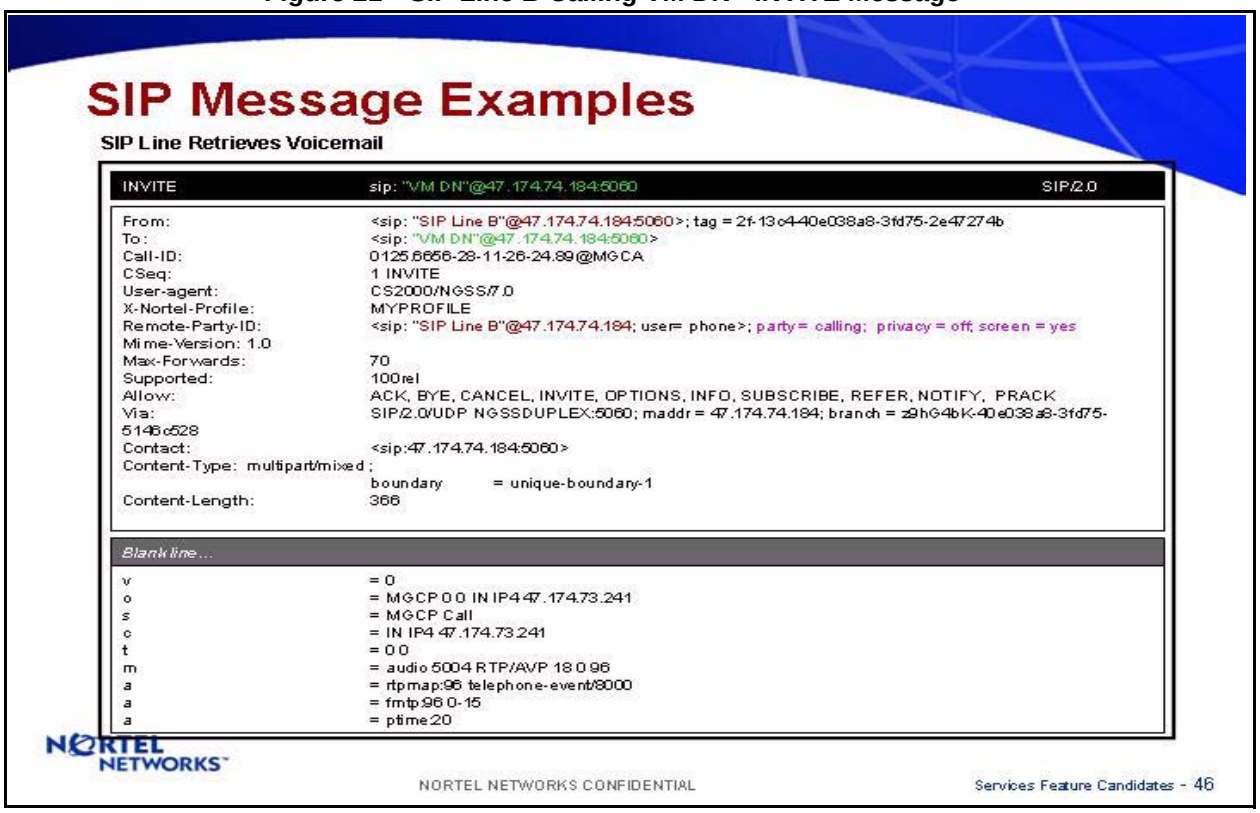


Figure 22 SIP Line B Calling VM DN - TRYING Message

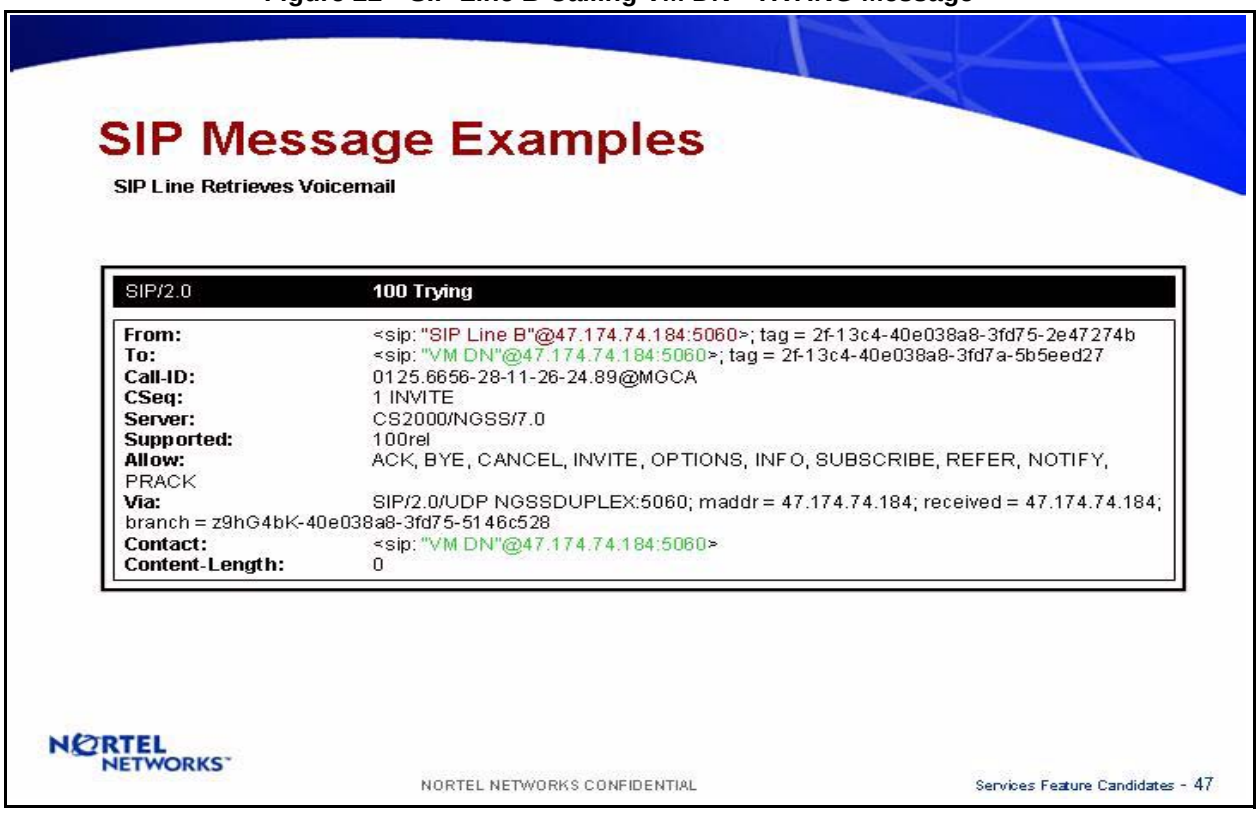


Figure 23 SIP Line B Calling VM DN - RINGING Message

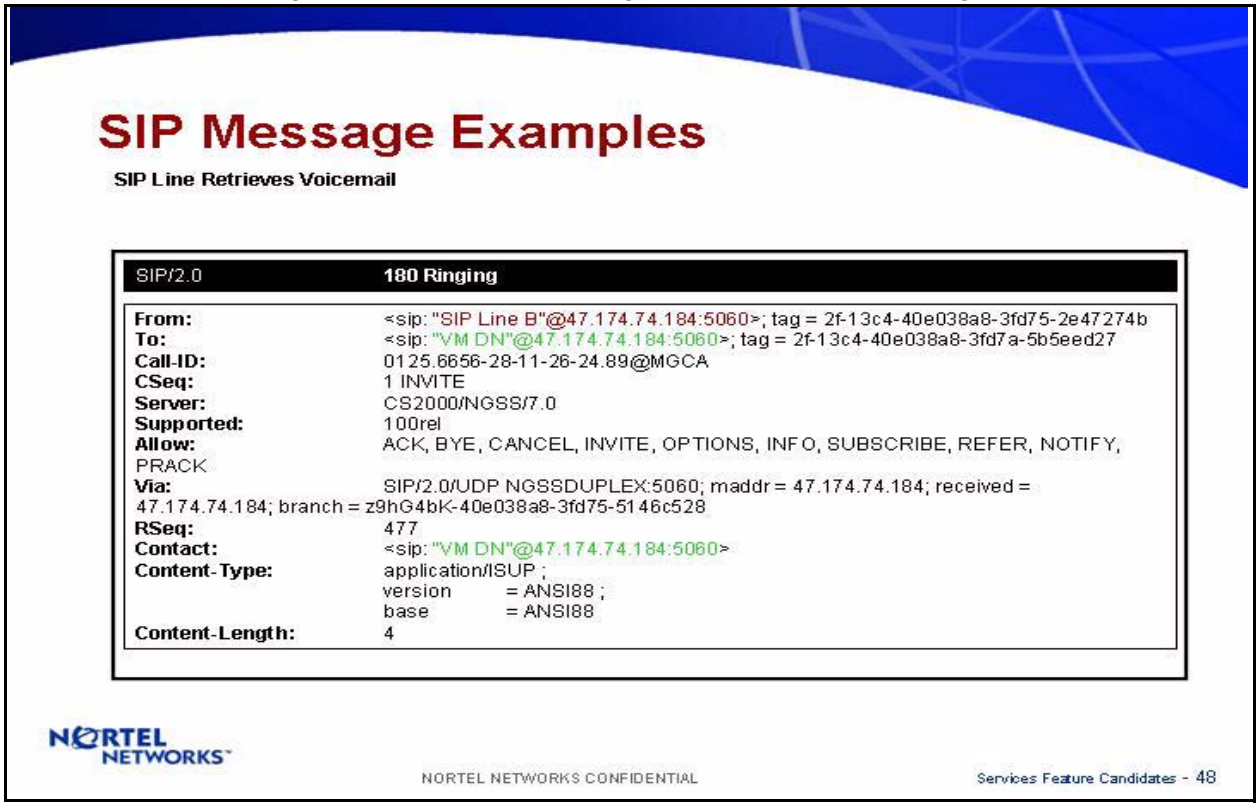


Figure 24 VM Answers - CS2K sends OK Response Message

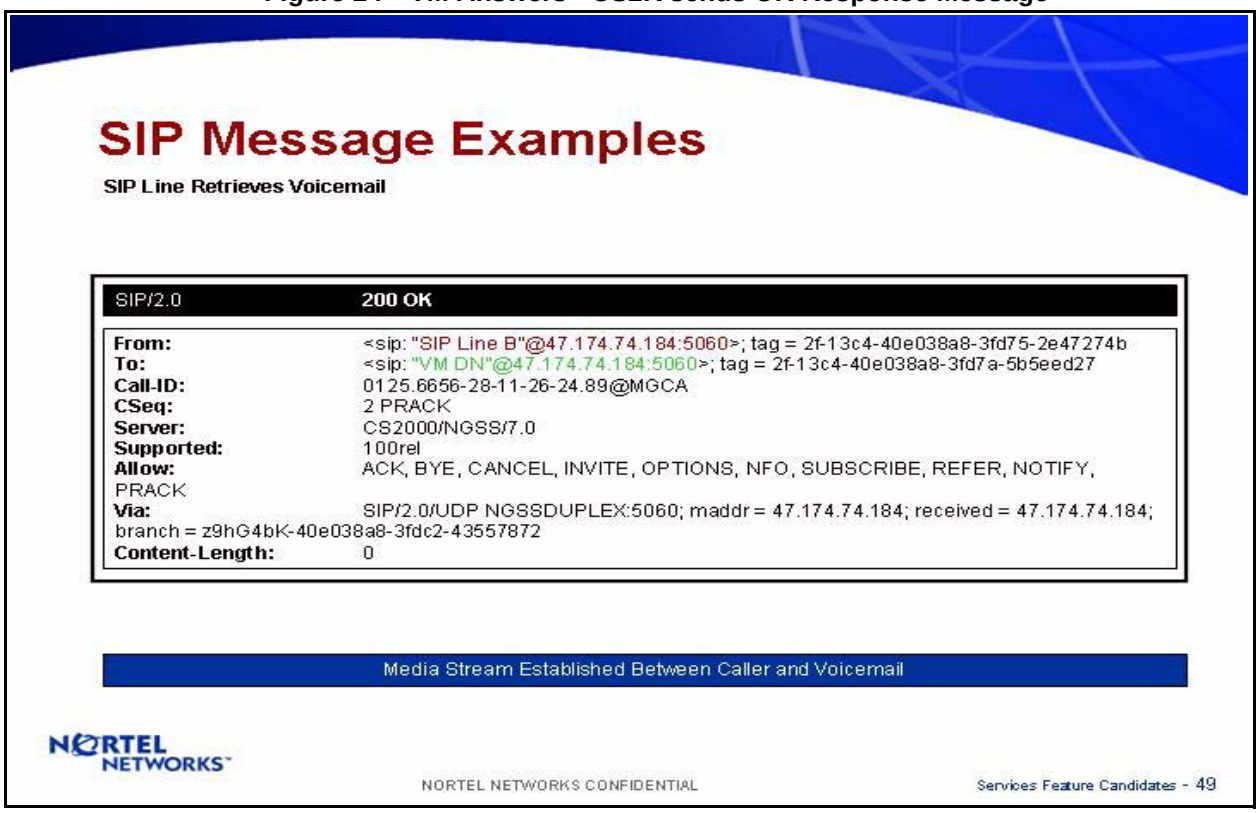


Figure 25 SIP Line B Accepts - ACK Response Message

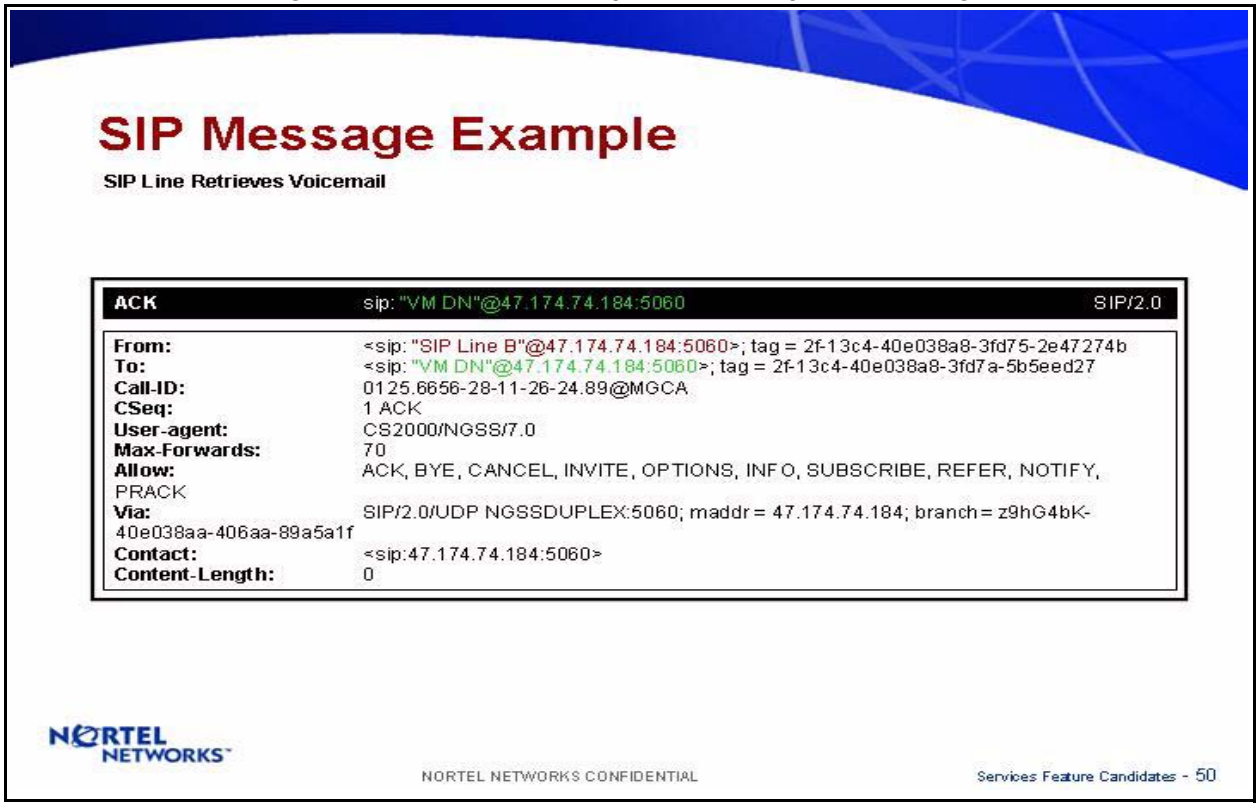


Figure 26 SIP Line B Exit from the Call - BYE Message

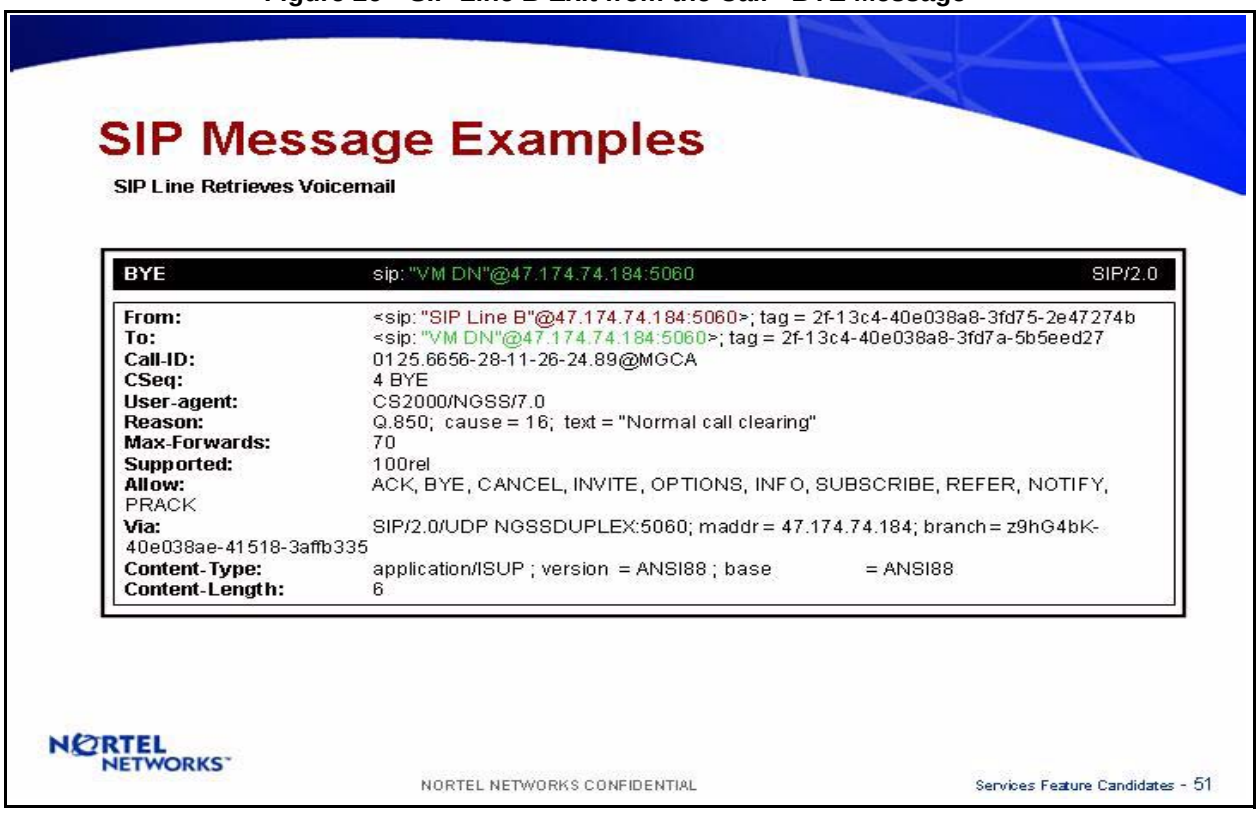
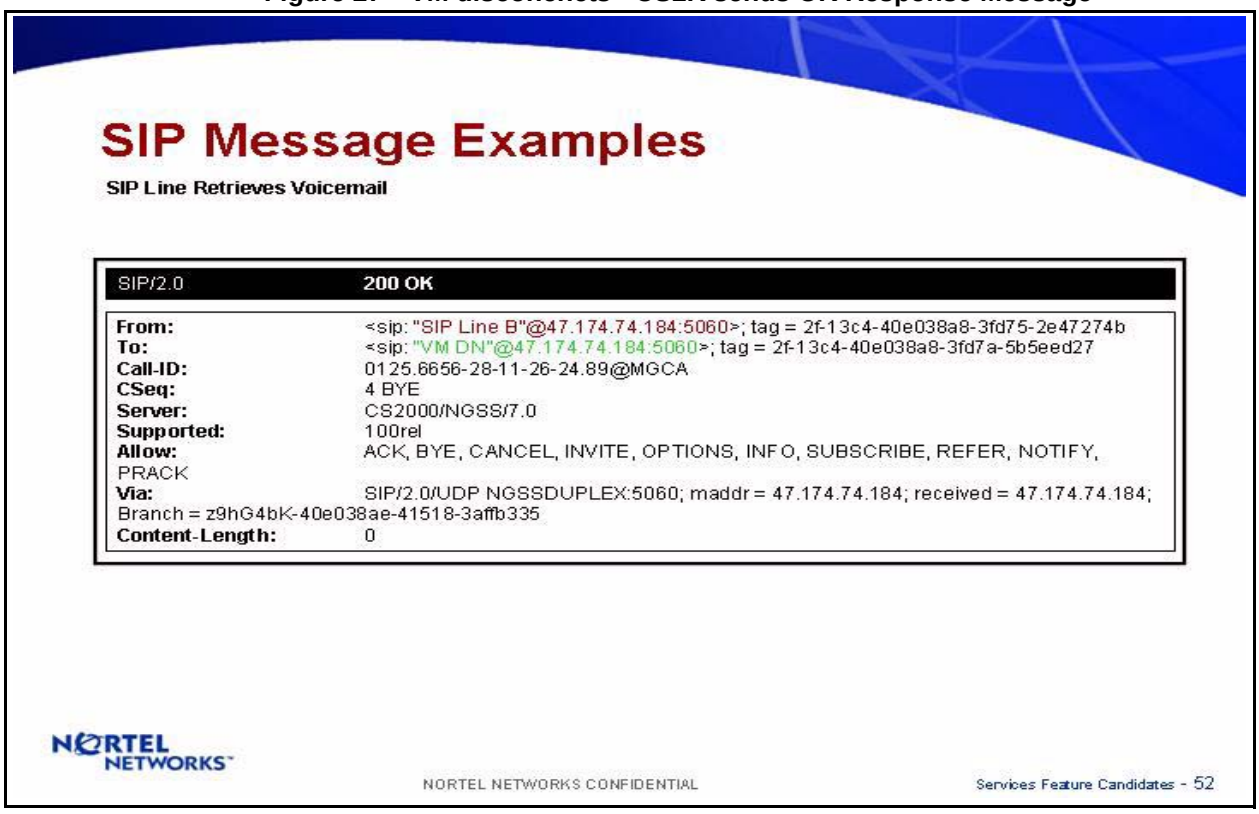


Figure 27 VM disconencts - CS2K sends OK Response Message



Step 6: CS2K sends NOTIFY message.

Figure 28 CS2K sends NOTIFY Message

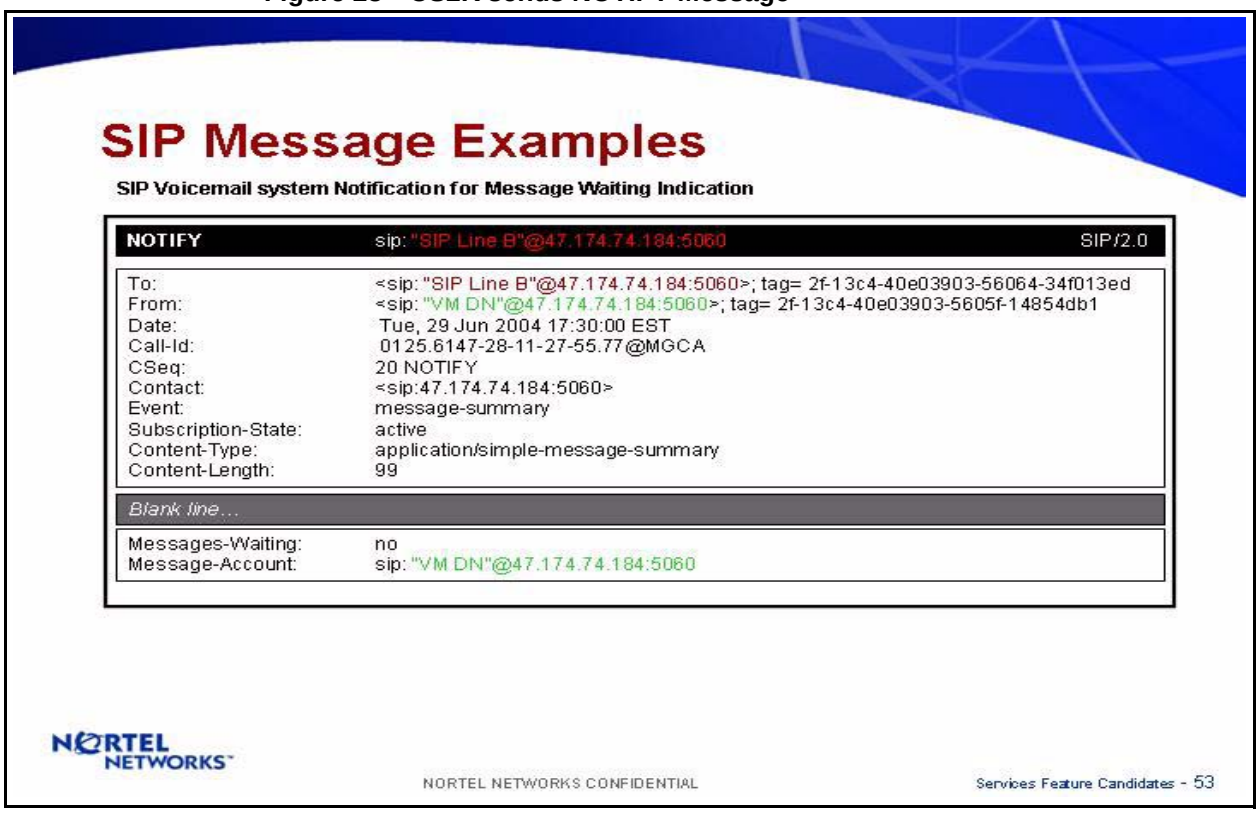
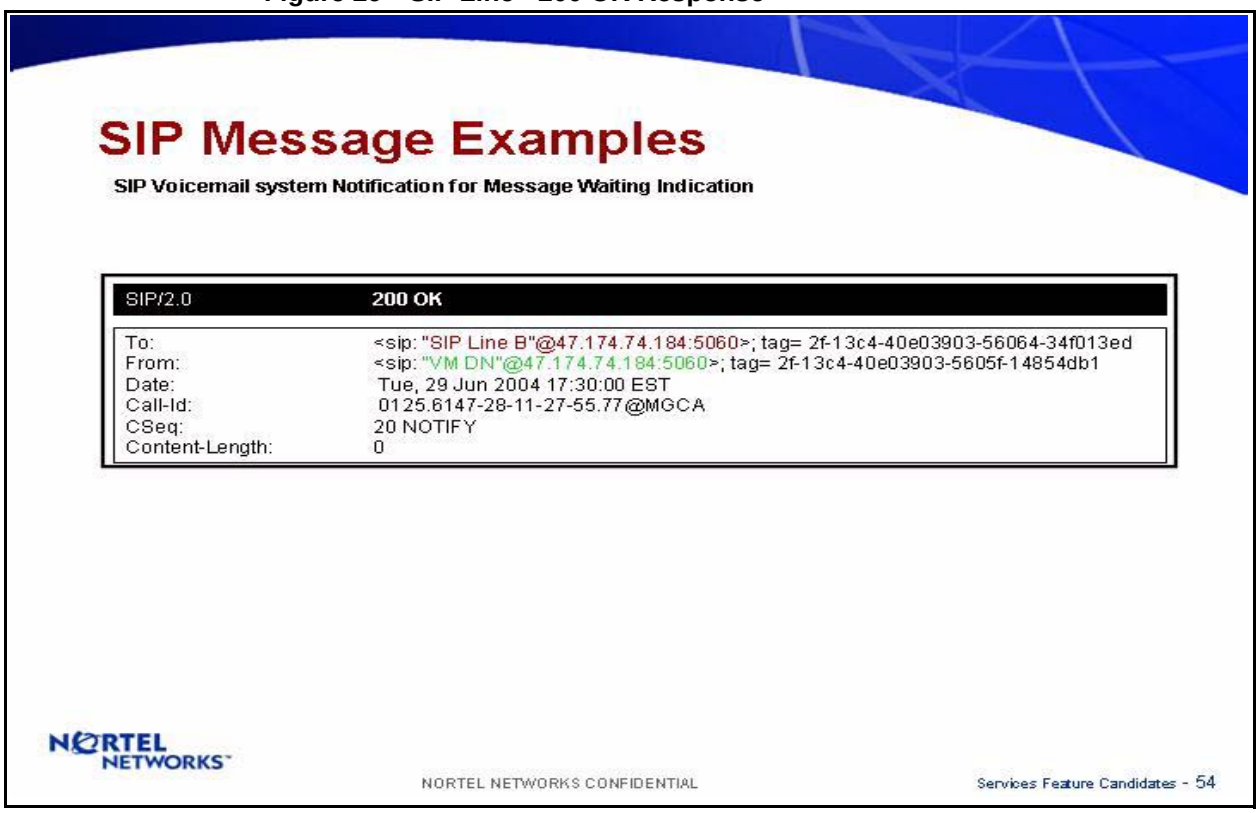


Figure 29 SIP Line - 200 OK Response



4.2.6 SOC Control

The new functionality is controlled by a SOC. This is a state controlled SOC. The following SOC is developed for this feature:

MDC00078 - NMS Over IP (SCTP)

4.3 Hardware Requirements or Dependencies

This feature uses the existing hardware of CS2K Core and Session Server. The Session Server provides standardized interface to SIP. Therefore, all 3rd party hardware and Voicemails are directly supported.

There is no new hardware dependency or requirement for this feature.

4.4 Software Requirements or Dependencies

The development depends on following 3rd party software currently exists in respective platform:

- SIP Stack from RADVISION in Session Server

4.5 Limitations and restrictions

The following limitations and restrictions apply to the feature:

- The NMS service sends MWI ON/OFF for the remote lines. It is assumed that the remote node or SIP Client will provide appropriate indication to end user for the MWI. The MWI indication can not be enforced.
- The Call Request Retrieval (CRR) functionality can not be invoked as second leg of Three way call (TWC). This limitation is for fraud prevention.
- The Call Request Retrieval (CRR) functionality can not be invoked as second or subsequent leg of a conference (CNF) call. This limitation is for fraud prevension.
- The MWT functionality is only provided to multiple appearance directory number (MADN) primary member.
- The MWT functionality is only provided to HUNT group primary member only.
- All existing MWT and NMS service limitations apply to this feature.
- The optional data defined in the RFC 3842 are not supported by this feature due to limited design scope. The support for the optional data can be developed in future releases.
- The direct SIP VM communication is not tested. Therefore, support for non-SIP lines using SIP VM can not be verified nor tested.
- In cases where a Line connected to a CS2K, the VM connected to a remote node (e.g. MCS) via SIP network and if G729 compatible codec is used for interconnect voice paths than remote node or device must support RFC 2833 for out of band DTMF signalling.
- When the line is connected to a remote node (e.g. MCS) via SIP network, VM is connected to a CS2K and if G729 compatible codec is used for interconnect voice paths than remote node or device must support RFC 2833 for out of band DTMF signalling.
- The design is generic and based on RFC 3842 standards. Testing limitations does not allow to test every possible interoperatibility using different handware and different vendor equipments in a network. Therefore, only tested network configurations are supported. In order to make other hardware and different vendor equipment supported, proper interoperatibility testing must be done in Nortel approved interoperatibility lab. After the complete testing, appropriate support will be provided.

4.6 Interactions

The service is controlled by the CS2K Core. The Session Server and GWC only provides access to various networks and protocol conversions. Therefore, CS2K Core interactions are applicable to this service.

The existing MWT and NMS service software is used for the development. Therefore, all existing interactions are apply to this expansion of service. There is no new interaction anticipated at the time of this writing.

4.7 Glossary

Term	Description
MWT	Message Waiting
MWI	Message Waiting Indication
CS2K	Communication Server 2000
VM	Voicemail System
CFD/CFDA	Call Forward Do Not Answer
CFB	Call Forward Busy
PSTN	Public Switched Telephony Network
EO	End Office
CRR	Call Request Retrieval
UM	Unified Messaging
SIP	Session Initiation Protocol
IP	Internet Protocol
SCTP	Session Control Transport Protocol
SDP	Session Description Protocol
NGSS	Session Server
VoIP	Voice over Internet Protocol
MsgSrv	Message Server
POTS	Plain Old Telephone Service
RES	Residential Line
IBN	Integrated Business Line
KSET	Key Set Line
ISDN	Integrated Services Digital Network
SS7	Signaling System No. 7
CICM	Centrex IP Line
IAD	IP Analog Gateway
PBX	Private Branch Exchange

Term	Description
SMDI	Simplified Message Desk Interface
UCD	Uniform Call Distribution
MCDN	Meridian Customer Defined Networking
MG9K	Media Gateway 9000
PVG	Packet Voice Gateway
S1K/1KM	Type of IP PBX
TDM	Time Division Multiplexing
NMS	Network Message Waiting
TCAP	Transaction Capabilities Application Part
GCP	Generic Call Protocol
GW	Gateway
GWC	Gateway Controller
DN	Directory Number
URI	Uniform Resource Identifiers
TEL URI	Telephony URI
TPT	Terminal Processing Task
CFU	Call Forwarding Unconditional / Call Forwarding Universal
NCAS	Non-Call-Associated Signaling
SOC	Software Optionality Control
PC	Personal Computer
DMS	Digital Multiplex Switch
MS	Message Switch

5: Functional Description (FN): A00007547

5.1 Feature name

A00007547: SIP Lines Core Call Processing Support

5.2 Description

This activity provides initial CS2K support for SIP (Session Initiation Protocol) lines basic call for SIP agents that interface to the CS2K via the GWC and CS2K Session Server. This includes the following components:

- Support for multiple call appearances for DPL lines
- CS2K call processing support for SIP basic call including signalling interface with the TPT in the GWC.

5.2.1 Multiple Call Appearances

Support for multiple call appearances relies on a new pool of resources (virtual terminal identifiers). This new pool has OMs and logs associated with it.

The new OM group DPLOM, has registers:

- DPLFNVA, DPLFBAL, DPLFREB, DPLRLOS
- DPLRCAL, DPLUSE, DPLFRE, DPLNOA, DPLNOD

DPL logs: DPL100, DPL101

The remainder of this section explains the rationale for these items and how they will be used when multiple call appearances are supported for SIP lines on the CS2K.

SIP allows devices to make multiple simultaneous call attempts, and actively engage in multiple simultaneous calls. The maximum number of such calls will be limited on a per-line basis, as part of the DPL SERVORD option, as described in feature A00008556. In order for the CS2K to handle these lines in a manner that preserves the way various line options work (as much as possible) and that makes efficient use of CS2K resources, a new resource pool is created. This section describes the resource pool and how it is controlled and monitored.

The new resource pool consists of “virtual terminal identifiers” (VIDs). VIDs are an existing resource on the CS2K. One VID is required for each appearance

of a SIP line in a CS2K call. The pool will be sized to the total of the maximum call appearances of all DPL lines (from the DPL SERVORD option) but capped at twice the maximum number of simultaneous calls (existing office parameter NCCBS in OFCENG).

5.2.1.1 Resource pool monitoring

There is a new OM group (DPLOM) defined that contains pegs and usage measurements of the resource pool. The registers are:

- DPLUSE - usage register (100 sec sampling, with extension register) that tracks the number of VIDs in use by call processing
- DPLFRE - usage register (100 sec sampling, with extension register) that tracks the number of VIDs on the resource pool free list.
- DPLNOA - peg register (with extension) that indicates the number of allocations from the resource pool.
- DPLNOD - peg register (with extension) that indicates the number of deallocations to the resource pool.
- DPLFNVA - peg register that indicates the number of times that a failure to allocate a VID happened because the resource pool free list was empty.
- DPLFBAL - peg register that indicates the number of times that a failure to allocate a VID happened because the resource pool free list was unavailable due to rebalancing (part of the rebuild process).
- DPLFREB - peg register that indicates the number of times that a failure to deallocate a VID happened (resulting in a “lost” VID) because the resource pool free list was being rebuilt.
- DPLRLOS - peg register that indicates the number of “lost” VIDs that were recovered .
- DPLRCAL - peg register that indicates the number of VIDs that were in use by call processing, but were not returned to the resource pool free list.

5.2.1.2 Resource pool recovery

As with any resource pool, there are recovery mechanisms. There is an audit which will recover “stranded” VIDs, that is, VIDs which are no longer in use, but have not been returned to resource pool free list. There is also a mechanism which detects corruption in the resource pool free list, and reconstructs it. A log will be output at the beginning of that reconstruction, and another at the end (DPL100 and DPL101, respectively).

5.2.2 Call Processing

The call processing component of this feature has very little customer visible impact to functionality. From the CS2K’s perspective, calls to and from DPL lines will function in the same manner that calls to and from standard IBN or RES lines function. Other than the VID allocation described in the previous

section, the CS2K will provide very little indication that the end user is in fact a SIP client.

The entire call progresses as a typical IBN or RES line call would progress. This will include any standard OMs and logs that apply to IBN and RES lines. Additional OMs and logs related to the DPL VIDs may be produced as described in the previous section.

The main exception to the IBN/RES call processing model is the fact that the DPL SIP line can have multiple call sessions active at any given time. This introduces 2 new concepts: 1) A maximum number of call appearances per DPL line can be defined, and 2) The presence of certain options on the line can dictate whether or not multiple terminations are allowed when the line is "busy".

5.2.2.1 Maximum Call Appearances

Each DPL SIP line defined in the core will be provisioned with a suboption called MAX_CALL_APPEARANCES. (See A00008556 for more information on provisioning the DPL line.) MAX_CALL_APPEARANCES will define the total number of VIDs that can be allocated for the line. Therefore, the total number of incoming and outgoing calls that involve the DPL line cannot exceed the value of MAX_CALL_APPEARANCES for that line.

Once the call appearance limit has been reached, any incoming call attempts will receive BUSY treatment, and any outgoing call attempts will receive NOSR (No Software Resources) treatment.

5.2.2.2 Allow Busy Terminations

The ability of a DPL line to have multiple active call sessions introduces some interaction problems with common CS2K features. For example, standard call waiting has no useful purpose if multiple calls can already be terminated on a DPL line.

To solve this problem, the concept of ALLOW_BUSY_TERMINATIONS is introduced. ALLOW_BUSY_TERMINATIONS is an internal bool that will be stored for every DPL line in the CS2K.

When the bool is set to N, incoming calls will not be presented to the DPL line if there is already at least one active call in progress. These calls will receive BUSY treatment instead. When the bool is set to Y, the only restriction on incoming calls being presented to the DPL line is the value of MAX_CALL_APPEARANCES.

Outgoing calls originated by the DPL line will not be restricted by the ALLOW_BUSY_TERMINATIONS bool at all.

ALLOW_BUSY_TERMINATIONS is not intended to be a provisionable value. It will be stored internally, and altered based on the addition or removal of certain options on the DPL line. For example: Initially the bool will be set to N, meaning that if one call is active, all subsequent incoming calls will receive busy treatment. The addition of the CWT option on the DPL line will cause the system to flip the internal bool to Y, and thus additional call terminations will be allowed as per the CWT feature function.

5.3 Hardware Requirements or Dependencies

5.4 Software Requirements or Dependencies

5.5 Limitations and restrictions

The DPL option will only be assignable to IBN and RES LCCs.

5.6 Interactions

Keyset and ISDN lines also make use of VIDs, but do so strictly based on provisioning. VIDs used for keyset and ISDN lines are separate from VIDs used in the resource pool defined by this activity. Thus, provisioning of keyset and ISDN lines will decrease the number of VIDs available for the resource pool defined by this activity, and vice versa.

5.7 Acronyms

Acronym	Description
ACD	Automatic Call Distribution
CS2K	Call Server 2000
DPL	Dynamic Packet Line
GWC	Gateway Controller
IBN	Integrated Business Network Line Type
ISDN	Integrated Services Digital Network
MADN	Multiple Appearance Directory Number

Acronym	Description
RES	Residential Line Type
SCMP	Series Completion
SIP	Session Initiation Protocol
VID	Virtual Identifier

5.8 Applicable customer facing sections.

Fault Management

- Logs __X__
- Alarms _N/A_

Configuration

- Data Schema _N/A_
- User Interface _N/A_
- Element Management _N/A_
- Security _N/A_
- Service Order _N/A_
- Office Parameters _N/A_

Accounting (includes AMA billing) _N/A_

Performance (includes operational measurements) __X__

6: Functional Description (FN): A00007703

6.1 Feature name and Feature ID

A00007703 SDM/CBM Log Capacity & Robustness

6.2 Description

A00007703 is intended to increase the log-flow capactity from the DMS Core to the SDM or CBM. Currently, the log rate is 10 logs/second (sustained) and 20 logs/second (2-minute burst) from the Core to the SDM or CBM. The sustained and burst rates are to be increased to 40 logs/second.

The increase in log throughput will be handled through one or two means. Firstly, a stream-lined LOGDEVP process will be implemented for the SDM and CBM log device, SDM_LOGDEV01. Currently, each LOGDEVP process communicates extensively with its associated LOGSLAVE process. The stream-lined process will bypass LOGSLAVE, thus removing the involvement of the middle-man and the inter-process communications overhead associated with it. This enhancement requires only changes to the Core software.

Optionally[1], the messaging scheme used to send the Core logs to the SDM or CBM will be made more efficient. The protocol iscurrently being used to send only one log at a time from the Core to the SDM or CBM, but it is capable of sending multiple logs at once. The implementation will be changed on both the Core and the SDM/CBM sides to allow the handling of multiple logs per message, and thus increasing log throughput.

This feature affects only the SDM_LOGEV01 log device, which is specifically used to send Core logs to an SDM or CBM for storage, downstream processing, etc. No other log devices will be affected.

The types of logs being handled by SDM_LOGDEV01 will not change as a result of this feature.

Logs handled by SDM_LOGDEV01 will still be visible on the Core as per normal handling, such as through LOGUTIL buffers and DLOGs. The logs will still be available to other log devices as required.

No new logs will be introduced by this feature.

[1]This option will be exercised if the LOGSLAVE bypass functionality does not increase Core-to-SDM/CBM log throughput to 40 logs/second.

6.3 Hardware Requirements or Dependencies

There are no specific hardware requirements or dependencies for A00007703. The feature is applicable to any DMS Core hosting an SDM or CBM.

6.4 Software Requirements or Dependencies

There are no new software requirements or dependencies for A00007703.

6.5 Limitations and restrictions

There are no restrictions or limitations associated with A00007703.

6.6 Interactions

This feature does not have any end-user-visible interactions.

6.7 Glossary

Term	Description
CBM	Core Billing Manager
SDM	SuperNode Data Manager

7: Functional Description (FN): A00007704

7.1 Feature name and Feature ID

A00007704: Table Access Manager Robustness

7.2 Description

This feature A00007704: Table Access Manager Robustness will allow the user/applications to make up to 5000 symbol changes and 1000 type info changes continuously without breaking the connection with SDM/CBM Table Access service. Prior to this feature, only less than 150 continuous DD changes were supported.

7.3 Hardware Requirements or Dependencies

None.

7.4 Software Requirements or Dependencies

The Table Access Service application is installed on the SDM/CBM and is in InSv state.

7.5 Limitations and restrictions

This activity does not prevent the SDM or CBM from re-downloading the Data Dictionary due to problems on the SDM/CBM side such as the DD file size exceeding 10 MB or the DD file being corrupted.

7.6 Interactions

None

7.7 Glossary

Term	Description
SDM	SuperNode Data Manager
CBM	Core & Billing Manager
DD	Data Dictionary

8: Functional Description (FN) A00007814

8.1 Feature name and Feature ID

REX testing for MG9000 (Media Gateway 9000) from Element Manager - A00007814

8.2 Description

Routine Exercise (REX) of intelligent card pairs is being introduced in SN09 release to perform the diagnostics of the inactive card. During REX, the inactive card of a card pair will be diagnosed. Followed by the inactive card, REX is executed on the active card, after a SWACT is initiated on the active card which now becomes inactive.

The need for a REX test stems from the fact that the inactive card (standby card) may be prone to latent faults, as it does not get exercised on a regular basis. Exercising it in a way that an active side operates during normal operation will provide a means to detect dormant failures. Moreover, the impact of incorrect or failed operation is in itself a means of detecting problems. Thus REX tests improve fault coverage of hardware and software, repair can take place during off-peak hours and the system re-instated into service before peak hour begins.

User will be able to input the schedule for REX on a particular NE. Intelligent card pairs considered for REX on MG9000 are SCO/SCI/SCG (DCC), ITP and ITX cards. User will be able to see the progress of the REX on a particular NE from the REX GUI of Subnet View and on NE Desktop View. Success/failure of the operations in REX for a given NE are also logged.

2.2.1 REX Scheduling

REX NE option is provided in the configuration menu of Desktop view. On clicking the REX NE menu, REX GUI will be opened. User will be able to initiate REX on NE(s) using REX GUI. REX GUI contains options to Add, Remove, Suspend, Resume an NE for REX. User can perform the following from the REX GUI:

1. REX on an NE can be scheduled for a particular day, time from the GUI or can be executed immediately. Scheduling of REX is similar to that of Audit.

2. An option is provided to remove an NE for which REX is already scheduled. On removing the NE, if the REX is in progress, it would be suspended.

3. User can suspend the already scheduled REX.

4. User can resume the suspended REX.

5. User will be able to view the results/progress details of REX executed on the selected NE.

2.2.2 REX Results

During REX, inactive card of the intelligent card Diagnosed. The results of all these operations are logged and progress of REX is shown on the progress details field of the REX GUI. Progress details are also shown on the REX tab of NE Desktop View. Success/Failure of SWACT and diagnostics are displayed to the user as part of the progress details and also in the Logs.

8.3 Hardware Requirements or Dependencies

None

8.4 Software Requirements or Dependencies

None

8.5 Limitations and restrictions

1. REX will not be supported on ABI cards. ABI cards behave as master-slave and hence SWACT is not possible on ABI cards.

2. REX will not be supported on DS1 cards as they adhere to 1:N protection scheme.

3. Any swact on ITPs should be followed by a wait period of at least 1 minute prior to locking the newly inactive card. Until ready for service calculations are handled on the inactive, the possibility remains that an ITP newly swacted to, may give up activity, shortly after the swact (as it discovers its not truly capable of providing service)

4. A critical datasync fault on the inactive card must not block Rex from locking/diagnosing/unlocking the inactive. A corollary to this restriction is that the card pairs exhibiting CPU overload alarms (or cards subtending a card with CPU overload alarms, like an ITP below an overloaded Supercore) must not be REX tested. A log should be output if a card pair is skipped due to CPU overload.

8.6 Interactions

None

8.7 Glossary

Term	Description
REX	Routine EXercise
MG9000	Media Gateway 9000
EM	Element Manager
SCG	SuperCore GigE
GigE	Gigabit Ethernet
SWACT	SWitch ACTivity
DCC	Data Control Card
SCO	SuperCore OC3
SCI	SuperCore IMA
ITP	Internet Telephony Processor
ITX	Internet Telephony Extender
CPU	Central Processing Unit

9: Functional Description (FN): A00008090

9.1 Feature name and Feature ID

SBA: Alternate Scheduled Closure of Billing Files: A00008090

9.2 Description

This feature facilitates the closure of billing files at the scheduled Interval as specified in the Stream Configuration and providing an additional functionality of Resetting the DIRP Billing File sequence number at Midnight. This feature does not impact the existing functionality of file closure based on time and other mechanisms like file closure based on file size or number of records in a file.

With this feature, all the open billing files are rotated exactly at scheduled interval without any drift or delay. Irrespective of the opening time of the billing File, the closure will take place at the exact scheduled interval. For e.g. if the scheduled interval for the ‘ Scheduled File Closure time options’ is ‘6 Hour’ then for the time frame 00:00 to 06:00,all the billing files which are in the open state will get closed at 06:00. In the time frame 06:00 to 12:00, all the billing files which are in the open state will get closed at 12:00. Similarly next file closure will be at 18:00 and 00:00 respectively.

If the billing files are closed by any other criteria such as BSY of SBA or issue of ‘closec’, prior to the scheduled rotation then additional file rotation occurs without impacting the scheduled closure of the next file. In the above example suppose that a closec command is issued for the scheduled stream at 04:00, but still the next file closure will happen at 06:00, if any open file exists.

This feature is introducing a new option in the Stream Configuration to schedule closure of billing files without any drift or delay. This option is mutually exclusive with the option of ‘Files Closure based on a time limit’ which means users can only turn on either ‘Files closed at scheduled intervals from midnight’ or ‘Files Closure based on a time limit’, but not both.

The functionality of file closure at scheduled intervals from midnight can be enabled at the time of configuring a Stream or at the time of changing the configuration of an existing stream. In the latter case, the functionality will be activated only for the billing files which are opened after enabling the functionality. Bsy/Rts of SBA application is not required to activate this functionality.

Following are the Options for the file closure of billing files at scheduled intervals from midnight.

1) Close billing files every 24 hours

2) Close billing files every 12 hours

3) Close billing files every 6 hours

4) Close billing files every 2 hours

5) Close billing files every 1 hour (Default Schedule Time)

6) Close billing files every 30 minutes

7) Close billing files every 15 minutes

7) Close billing files every 10 minutes

8) Close billing files every 5 minutes

Reset DIRP Sequence Number at Midnight:

This feature provides a facility to reset the DIRP Billing File sequence number at midnight. The first DIRP billing file which is opened after midnight (00:00 Hr) will have a sequence number 00, if there is no other file exists with the same name. If the same filename exists then increment the sequence number and rename the file with that Sequence Number.

This is introducing a new option in the Stream Configuration to enable the functionality of 'Reset DIRP Sequence Number at Midnight'. This option is mutually exclusive with the option of 'Files renamed with close date' which means users can only turn on either 'Files renamed with close date' or 'Reset DIRP Sequence Number at Midnight', but not both.

9.2.1 Desired Behavior of 'file closure based at scheduled intervals from midnight' with Respect to the Daylight Saving Time:

Since the proposed design uses RWTime, the 'file closed based at scheduled intervals from midnight' behaves in the similar way which is explained below with the help of an example.

Note: In the below examples consider that files are not closed by any other criteria such as BSY of SBA or closing the file with the command 'closec' or any other criteria other than the scheduled rotation.

Considering the US/Eastern TimeZone .

CASE1: On 04 April 2004, when Time Changes from 01:59:59 -> 03:00 (Time changes from EST to EDT)

Scheduled Interval : 05:00 Mins

SBA closes the file at intervals 00:05 hr, 00:10 hr,...,01:50 hr,01:55 hr(EST),03:00 hr(EDT),03:05 hr(EDT),...,23:50 hr,23:55 hr,00:00 hr.

Scheduled Interval : 10:00 Mins

SBA closes the file at intervals 00:10 hr, 00:20 hr,...,01:40 hr,01:50 hr(EST),03:00 hr(EDT),03:10 hr(EDT),...,23:40 hr,23:50 hr,00:00 hr.

Scheduled Interval : 15:00 Mins

SBA closes the file at intervals 00:15 hr, 00:30 hr,...,01:30 hr,01:45 hr(EST),03:00 hr(EDT),03:15 hr(EDT),...,23:30 hr,23:45 hr,00:00 hr.

Scheduled Interval : 30:00 Mins

SBA closes the file at intervals 00:30 hr, 01:00 hr,01:30 hr (EST),03:00 hr(EDT),03:30 hr(EDT),...,23:00 hr,23:30 hr,00:00 hr.

Scheduled Interval : 01:00 Hrs

SBA closes the file at intervals 01:00 hr(EST),03:00 hr(EDT),04:00 hr(EDT),...,22:00 hr,23:00 hr,00:00 hr.

Scheduled Interval : 02:00 Hrs

SBA closes the file at regular intervals 03:00 hr (EDT), 04:00 hr (EDT),06:00 hr,...,20:00 hr,22:00 hr,00:00 hr.

Scheduled Interval : 06:00 Hrs

SBA closes the file at intervals 07:00 hr (EDT), 12:00 hr ,18:00 hr,00:00 hr

Scheduled Interval : 12:00 Hrs

SBA closes the file at intervals 13:00 hr (EDT) and 00:00 hr

Scheduled Interval : 24:00 Hrs

SBA closes the file on April 5 2004(next day) at 01:00 hr and 00:00 hr

CASE 2: On 31 October 2004, when Time Changes from 01:59:59 -> 01:00 (Time changes from EDT to EST)

Scheduled Interval : 05:00 Mins

SBA closes the file at intervals 00:05 hr, 00:10 hr,...,01:50 hr,01:55 hr(EDT),01:00 hr(EST),01:05 hr(EST),...,23:50 hr,23:55 hr,00:00 hr

Scheduled Interval : 10:00 Mins

SBA closes the file at intervals 00:10 hr, 00:20 hr,...,01:40 hr,01:50 hr(EDT),01:00 hr(EST),01:10 hr(EST),...,23:40 hr,23:50 hr,00:00 hr.

Scheduled Interval : 15:00 Mins

SBA closes the file at intervals 00:15 hr, 00:30 hr,...,01:30 hr,01:45 hr(EDT),01:00 hr(EST),01:15 hr(EST),...,23:30 hr,23:45 hr,00:00 hr.

Scheduled Interval : 30:00 Mins

SBA closes the file at intervals 00:30 hr, 01:00 hr,01:30 hr (EDT),01:00 hr(EST),01:30 hr(EST),...,23:00 hr,23:30 hr,00:00 hr.

Scheduled Interval : 01:00 Hrs

SBA closes the file at intervals 01:00 hr(EDT),01:00 hr(EST),02:00 hr(EST),...,22:00 hr,23:00 hr,00:00 hr.

Scheduled Interval : 02:00 Hrs

SBA closes the file at intervals 01:00 hr (EST), 02:00 hr (EST),04:00 hr,...,20:00 hr,22:00 hr,00:00 hr.

Scheduled Interval : 06:00 Hrs

SBA closes the file at intervals 05:00 hr (EST), 06:00 hr ,12:00 hr,18:00 hr,00:00 hr

Scheduled Interval : 12:00 Hrs

SBA closes the file at regular 11:00 hr (EST) 12:00 hr and 00:00 h**r**

Scheduled Interval : 24:00 Hrs

SBA closes the file on 31st October 2004 at 23:00 hr and 00:00 hr

9.2.2 Desired Behavior of 'Reset DIRP Sequence Number at Midnight' with Respect to the Daylight Saving Time:

The functionality 'Reset DIRP Sequence Number at Midnight' does not have any impact if the time changes is happening in the same day. But if the time changes happens across the day following is the behavior.

for e.g. consider

CASE1: On 04 April 2004, suppose Time Changes from 22:59:59 -> 00:00 (Time changes from EST to EDT)

The resetting of DIRP Sequence number will happen when the new billing file opens on April 05 2004 after 00:00 hr.

CASE 2: On 31 October 2004, suppose Time Changes from 00:29:59 -> 23:30 (Time changes from EDT to EST)

In this case, resetting of DIRP sequence number will not happen again when the time changes from Oct 30 midnight(23:59 EST) to (00:00)Oct 31 , since the previously set date in Mib was of October 31.

i.e. The reset of DIRP Sequence number will occur only if current Date is greater than the date which was set in the Mib.

9.3 Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced by this feature

9.4 Software Requirements or Dependencies

None

9.5 Limitations and restrictions

- The option of 'Files closed at scheduled intervals from midnight' is mutually exclusive to the existing option of 'Files Closed based on a time limit'
- The Option of 'Reset DIRP Sequence Number at Midnight' is mutually exclusive to the existing option of 'Files renamed with close date'.
- This feature supports only Scheduled Rotation as '24 Hours','12 Hours','6 Hours','2 Hours','1 Hour','30 Minutes','15 Minutes', '10 Minutes' and'5 Minutes'
- If there are large numbers of billing files, then the file closure may get delayed since the OS not Real time
- File Closure may get delayed when SBAStreams is busy writing the billing records to the disk

- Billing File name does not guarantee that all the records are in line with the file closure time, in the event of any delay in transferring the call records from core to SBA
- During the event of BSY of SBA, prior to the scheduled closure of billing files all the open files will get closed.
- During Daylight Saving Time, the file closure does not happen at the exact schedule time.
- If the functionality is enabled by using Change command from CONFSTRM then the functionality will be activated only for the newly opened Files

9.6 Interactions

No

9.7 Glossary

Term	Description
SDM	Supernode Data Manager
CBM	Core & Billing Manager
SBA	SDM/CBM billing application
DIRP	Device Independent Recording Package (File format used by SBA to store billing records based on the DIRP billing file format on the DMS core)

10: Functional Description (FN) A00008323

10.1 Feature name and Feature ID

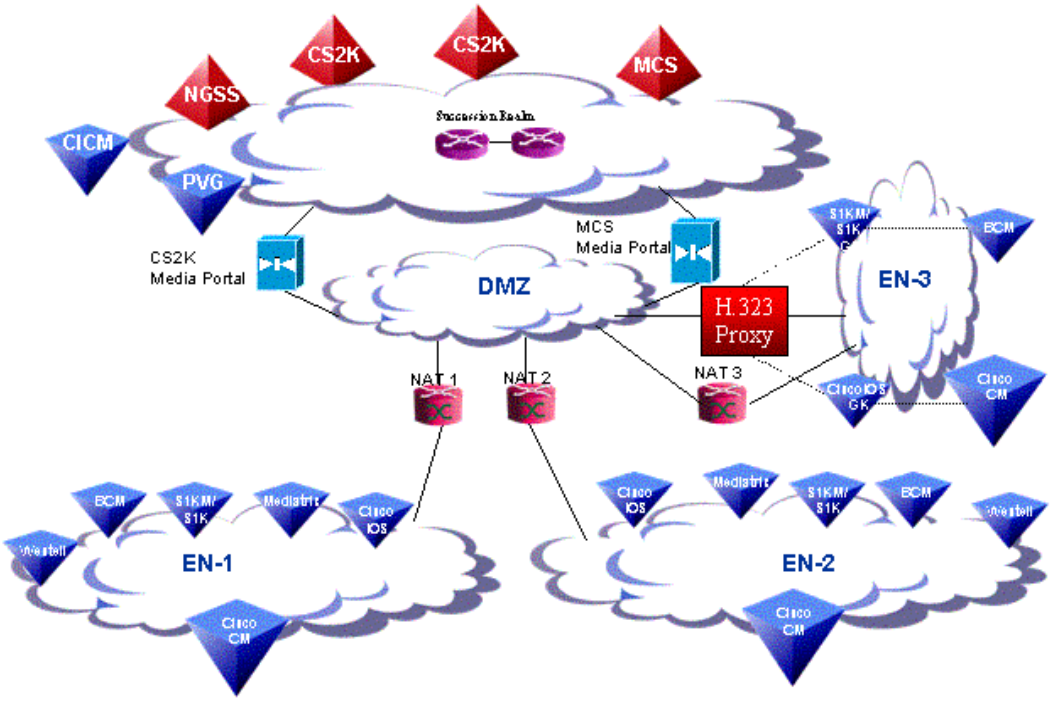
A00008323 H.323 64k UDI

10.2 Description

Besides packetization and depacketization, a VoIP media gateway performs additional processing on the media stream which it sends and receives. For example, the VoIP gateway may perform echo cancellation, DTMF detection, and encoding/decoding on the media stream.

However, there is a class of data streams that does not allow any data processing within the VoIP media gateway except for packetization and depacketization. ISDN data terminals, for example, will produce data streams that are not compatible with a non-linear encoding that is used for voice. For such applications, there exists a necessity for a bit-transparent relay of 64 kbit/s data streams in Real-time Transport Protocol (RTP) packets. This mode is often referred to as *Clear Channel Data* (CCD) or *64 kbit/s unrestricted data.*[1] No encoder or decoder is needed for CCD. However, a unique RTP payload type is necessary, and a related MIME type is to be registered for signaling purposes.

[1]CCD mode is not restricted to ISDN. It can be used by any application that does not need special encoding/decoding for transfer via an RTP connection.



CCD Mode in Succession CS2K

Existing VoIP vocoders (e.g. G.711, G.729) are not suitable to transmit a bit-transparent 64 kbit/s data stream. When processing a 64 kbit/s data stream, gateways should behave as follows:

- Gateways must turn off all voice processing features such as echo cancellation, DTMF detection, silence suppression, comfort noise insertion, A-law/u-law conversion, gain adjustment and packet loss concealment.
- Gateways should increase their jitter buffer size by 2 to reduce the possibility of buffer under-runs.
- Transport of the CCD stream through the gateway must be bit exact.

The H.323 standards (H.323, H.225 or H.245, H.323 implementation guide) do not provide stipulations for clear channel data within H.245 messages (for example in TCS, OLC). While the use of a bit-transparent 64 kbit/s channel can be signaled in the Bearer Capability information element of the H.225 SETUP message, it is not possible to advertise or negotiate the CCD capability in H.245 messaging. There is no standard codec defined in the industry to describe CCD data streams, so dynamic payload types must be used. In order to convey dynamic payload types in H.245, non-standard identifiers must be defined and agreed upon. Any solution based on this approach is therefore by default proprietary.

The Succession CS2K uses dynamic payload type 101, as specified in the SN07 IP Gateway InterOP Requirements, to indicate 64 kbit/s unrestricted data. The outgoing SDP for 64 kbit/s unrestricted data includes dynamic payload type 101 and rtpmap:101 X-CCD / clock-rate.

A sample outgoing SDP is illustrated below.

Figure 1 Example SDP: Gateway is requested to use 64 kbit/s unrestricted data

```
v=0
o=H323 0 0 IN IP4 172.29.224.26
c=IN IP4 172.29.224.26
m=audio 16398 RTP/AVP 101
a=rtpmap:101 X-CCD/8000
a=ptime:20
```

Succession CS2K CCD Interworking Requirements for H.323 Gateways

If the use of a bit-transparent 64 kbit/s channel is signaled in the Bearer Capability information element of the H.225 SETUP message (BC = UDI), the H.323 gateway should behave as follows.

Calls from H.323 gateway to CS2K:

- The H.323 gateway autonomously transitions to CCD mode.
- No requestMode commands are sent by the gatekeeper or by the H.323 gateway.
- Gateways shall use either 10ms or 20 ms packetization rate and signal this in the TCS.
- A non-standard CCD codec is not introduced. H.323 gateways may still use G.711 as codec in the TCS/OLC/Fast start element exchange, but the CS2K will ignore this information in case of UDI request in H.225 signaling.

- H.323 gateways must use dynamic payload type 101 for all CCD media streams.
- CCD calls cannot be converted to voice calls, and vice-versa.

Calls from CS2K to H.323 gateway:

- Upon receiving a H.225 SETUP with BC = UDI, the H.323 gateway must autonomously transition to CCD mode.
- No requestMode commands are sent by the GWC or by the H.323 gateway.
- CS2K shall signal the packetization rate from the far end in the TCS/OLC/Fast start element exchange (10 or 20 ms).
- H.323 gateway must expect and be able to handle dynamic payload type 101 for CCD media streams.
- CS2K signals G.711 as codec in the TCS/OLC/Fast start element exchange but the H.323 gateway must ignore this information in case of UDI request in H.225 signaling.
- CCD calls cannot be converted to voice calls, and vice-versa.

Note: There is no change to the gatekeeper functionality when interworking to non-H323 gateways that support CCD. The Session Descriptor is unchanged in this case as per the SN07 Succession Gateway Interoperability Requirements.

10.3 Hardware Requirements or Dependencies

There no CS2K hardware dependency, however needs customer provides devices to enable 64K UDI data transporting capabilities.

10.4 Software Requirements or Dependencies

This feature is sourced in SN09 and patched back to SN07 and SN08.

This feature requires H.323 Bearer Capability transparency which was sourced in SN07.

10.5 Limitations and restrictions

Not applicable.

10.6 Interactions

Not applicable.

10.7 Glossary

BC	**B**earer **C**apability
CCD	**C**lear **C**hannel **D**ata - the term used by Nortel Networks to denote data transmission over a bit-transparent 64 kbit/s channel
CS2K	**C**all **S**erver **2**000
ISDN	**I**ntegrated **S**ervices **D**igital **N**etwork
ISUP	**IS**DN **U**ser **P**art
OLC	**O**pen **L**ogical **C**hannel
RTP	**R**eal-time **T**ransfer **P**rotocol
SDP	**S**ession **D**escription **P**rotocol
TCS	**T**erminal **C**apability **S**et
UDI	**U**nrestricted **D**igital **I**nformation - the Bearer Capability used in ISDN and ISUP networks to characterize a bit-transparent 64 kbit/s channel

11: Functional Description (FN) A00008522

11.1 Feature name and Feature ID

A00008522, SESM Support for SIP Lines

11.2 Description

Feature A00008522 will deliver the lines flow through and pre-provisioning functionality in the Succession Element and Sub-element Manager (SESM) required for the Session Server (SS) integration with Succession. The design will be split into Nodes provisioning for SS virtual gateways (GWs), and lines provisioning for SIP terminations/users.

The Nodes provisioning feature component will provide for the provisioning of SS GWs. Nodes provisioning will also provide functionality to pre-provision the SIP terminations in the GWC-EM and to pre-provision LENs (Line Equipment Numbers) in XACore table LNINV. The Lines Provisioning component will provide flow through of service information entered at OSSGate (SERVORD+ commands). New line provisioning functionality will be delivered to allow line data to be transmitted to the SS Element Manager (SS-EM).

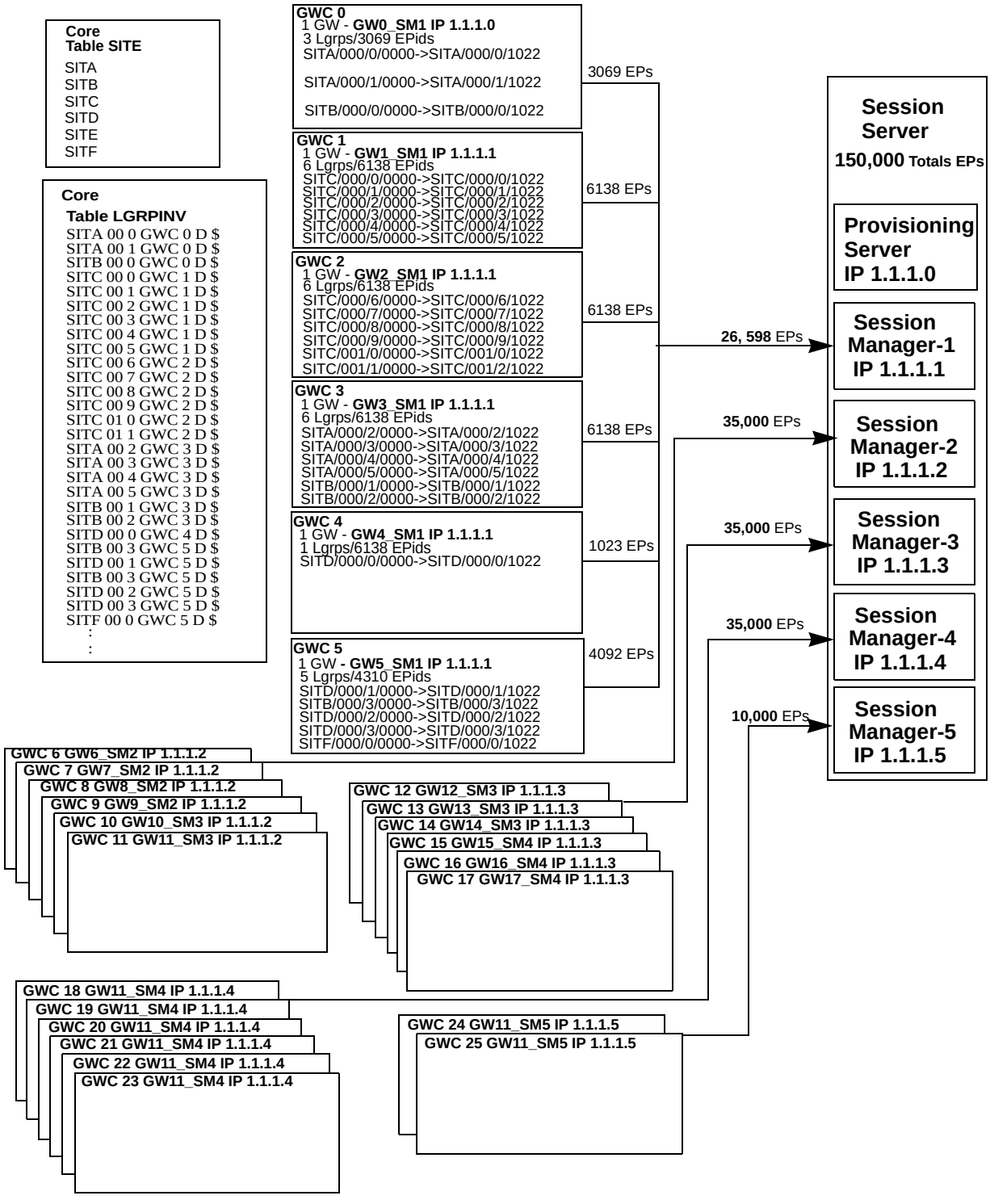
11.2.1 SS Provision Concepts

From figure 1, the interaction of various devices and tables is shown. Starting with the upper left is Table SITE in the CM. These site names are used to name line groups in the CS2KSS. This is performed during provisioning the GW.

From the example, GWC 0 has two GWs provisioned (also called a virtual gateway or VMG) called GW0_SM1 and GW1_SM2. More than GW is permitted on a GWC, as long as the GWs refer to different SS gateways. The GWC may support up to 12276 lines, or 12 LGRPs (12 LGRPs * 1023 endpoints per LGRP). These 12 LGRPs may be distributed over the 2 provisioned GWs in any fashion.

Note that multiple site names can be used in naming the LGRPs and the site names can span multiple GWs. The frame and group portions of the LGRP name are determined by the SESM/Nodes Provisioning and not by the user.

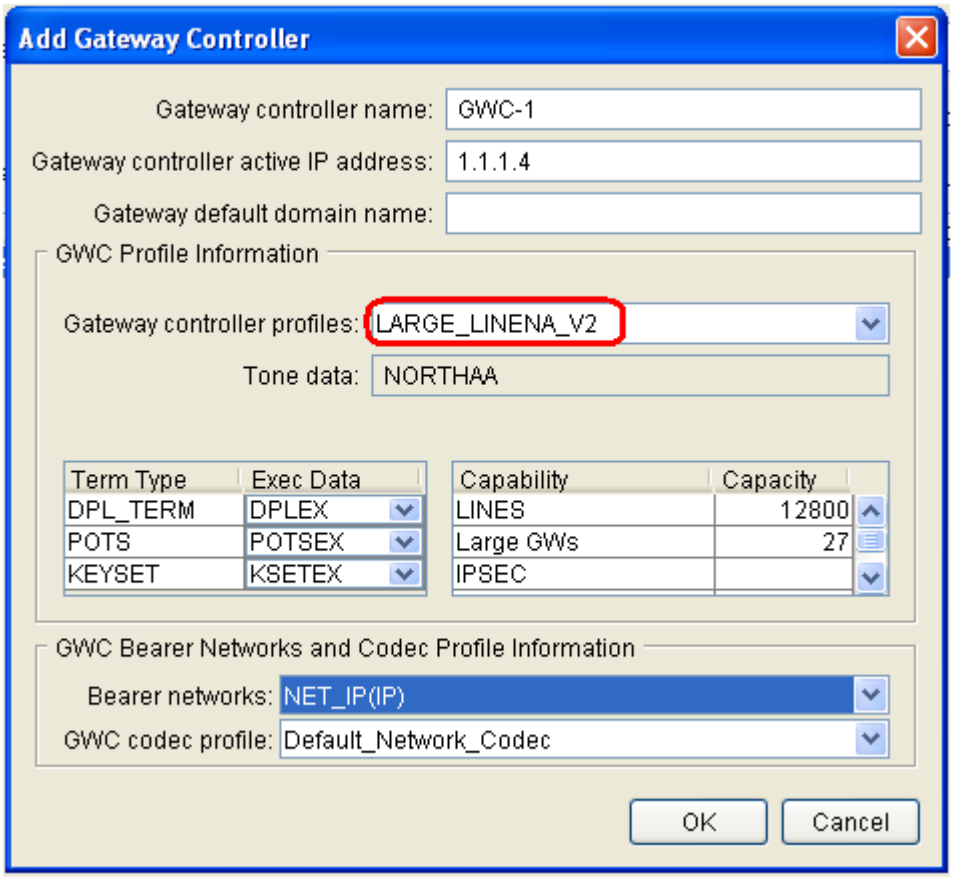
Figure 1 Example of MSM Provisioning Relationship


Core
Table SITE
SITA
SITB
SITC
SITD
SITE
SITF
Core
Table LGRPINV
SITA 00 0 GWC 0 D $
SITA 00 1 GWC 0 D $
SITB 00 0 GWC 0 D $
SITC 00 0 GWC 1 D $
SITC 00 1 GWC 1 D $
SITC 00 2 GWC 1 D $
SITC 00 3 GWC 1 D $
SITC 00 4 GWC 1 D $
SITC 00 5 GWC 1 D $
SITC 00 6 GWC 2 D $
SITC 00 7 GWC 2 D $
SITC 00 8 GWC 2 D $
SITC 00 9 GWC 2 D $
SITC 01 0 GWC 2 D $
SITC 01 1 GWC 2 D $
SITA 00 2 GWC 3 D $
SITA 00 3 GWC 3 D $
SITA 00 4 GWC 3 D $
SITA 00 5 GWC 3 D $
SITB 00 1 GWC 3 D $
SITB 00 2 GWC 3 D $
SITD 00 0 GWC 4 D $
SITB 00 3 GWC 5 D $
SITD 00 1 GWC 5 D $
SITB 00 3 GWC 5 D $
SITD 00 2 GWC 5 D $
SITD 00 3 GWC 5 D $
SITF 00 0 GWC 5 D $
GWC 0
1 GW - GW0_SM1 IP 1.1.1.0
3 Lgrps/3069 EPids
SITA/000/0/0000->SITA/000/0/1022
SITA/000/1/0000->SITA/000/1/1022
SITB/000/0/0000->SITB/000/0/1022
3069 EPs
GWC 1
1 GW - GW1_SM1 IP 1.1.1.1
6 Lgrps/6138 EPids
SITC/000/0/0000->SITC/000/0/1022
SITC/000/1/0000->SITC/000/1/1022
SITC/000/2/0000->SITC/000/2/1022
SITC/000/3/0000->SITC/000/3/1022
SITC/000/4/0000->SITC/000/4/1022
SITC/000/5/0000->SITC/000/5/1022
6138 EPs
GWC 2
1 GW - GW2_SM1 IP 1.1.1.1
6 Lgrps/6138 EPids
SITC/000/6/0000->SITC/000/6/1022
SITC/000/7/0000->SITC/000/7/1022
SITC/000/8/0000->SITC/000/8/1022
SITC/000/9/0000->SITC/000/9/1022
SITC/001/0/0000->SITC/001/0/1022
SITC/001/1/0000->SITC/001/2/1022
6138 EPs
GWC 3
1 GW - GW3_SM1 IP 1.1.1.1
6 Lgrps/6138 EPids
SITA/000/2/0000->SITA/000/2/1022
SITA/000/3/0000->SITA/000/3/1022
SITA/000/4/0000->SITA/000/4/1022
SITA/000/5/0000->SITA/000/5/1022
SITB/000/1/0000->SITB/000/1/1022
SITB/000/2/0000->SITB/000/2/1022
6138 EPs
GWC 4
1 GW - GW4_SM1 IP 1.1.1.1
1 Lgrps/6138 EPids
SITD/000/0/0000->SITD/000/0/1022
1023 EPs
GWC 5
1 GW - GW5_SM1 IP 1.1.1.1
5 Lgrps/4310 EPids
SITD/000/1/0000->SITD/000/1/1022
SITB/000/3/0000->SITB/000/3/1022
SITD/000/2/0000->SITD/000/2/1022
SITD/000/3/0000->SITD/000/3/1022
SITF/000/0/0000->SITF/000/0/1022
4092 EPs
Session Server
150,000 Totals EPs
Provisioning Server
IP 1.1.1.0
Session Manager-1
IP 1.1.1.1
Session Manager-2
IP 1.1.1.2
Session Manager-3
IP 1.1.1.3
Session Manager-4
IP 1.1.1.4
Session Manager-5
IP 1.1.1.5
26, 598 EPs
35,000 EPs
35,000 EPs
35,000 EPs
10,000 EPs
GWC 6 GW6_SM2 IP 1.1.1.2
GWC 7 GW7_SM2 IP 1.1.1.2
GWC 8 GW8_SM2 IP 1.1.1.2
GWC 9 GW9_SM2 IP 1.1.1.2
GWC 10 GW10_SM3 IP 1.1.1.2
GWC 11 GW11_SM3 IP 1.1.1.2
GWC 12 GW12_SM3 IP 1.1.1.3
GWC 13 GW13_SM3 IP 1.1.1.3
GWC 14 GW14_SM3 IP 1.1.1.3
GWC 15 GW15_SM4 IP 1.1.1.3
GWC 16 GW16_SM4 IP 1.1.1.3
GWC 17 GW17_SM4 IP 1.1.1.3
GWC 18 GW11_SM4 IP 1.1.1.4
GWC 19 GW11_SM4 IP 1.1.1.4
GWC 20 GW11_SM4 IP 1.1.1.4
GWC 21 GW11_SM4 IP 1.1.1.4
GWC 22 GW11_SM4 IP 1.1.1.4
GWC 23 GW11_SM4 IP 1.1.1.4
GWC 24 GW11_SM5 IP 1.1.1.5
GWC 25 GW11_SM5 IP 1.1.1.5

11.2.2 Adding a GWC

11.2.2.1 Add GWC

GWCs for CS2K Session Server gateways are provisioned using either the Large_LineNA_v2 or Large_LineINTL_v2 GWC profile. These GWC profiles will cause a GWC to be added to the CM, table SERVRINV, with the exec lineup of DPLEX/DPL, POTSEX/POT and KSETEX/KEYSET.

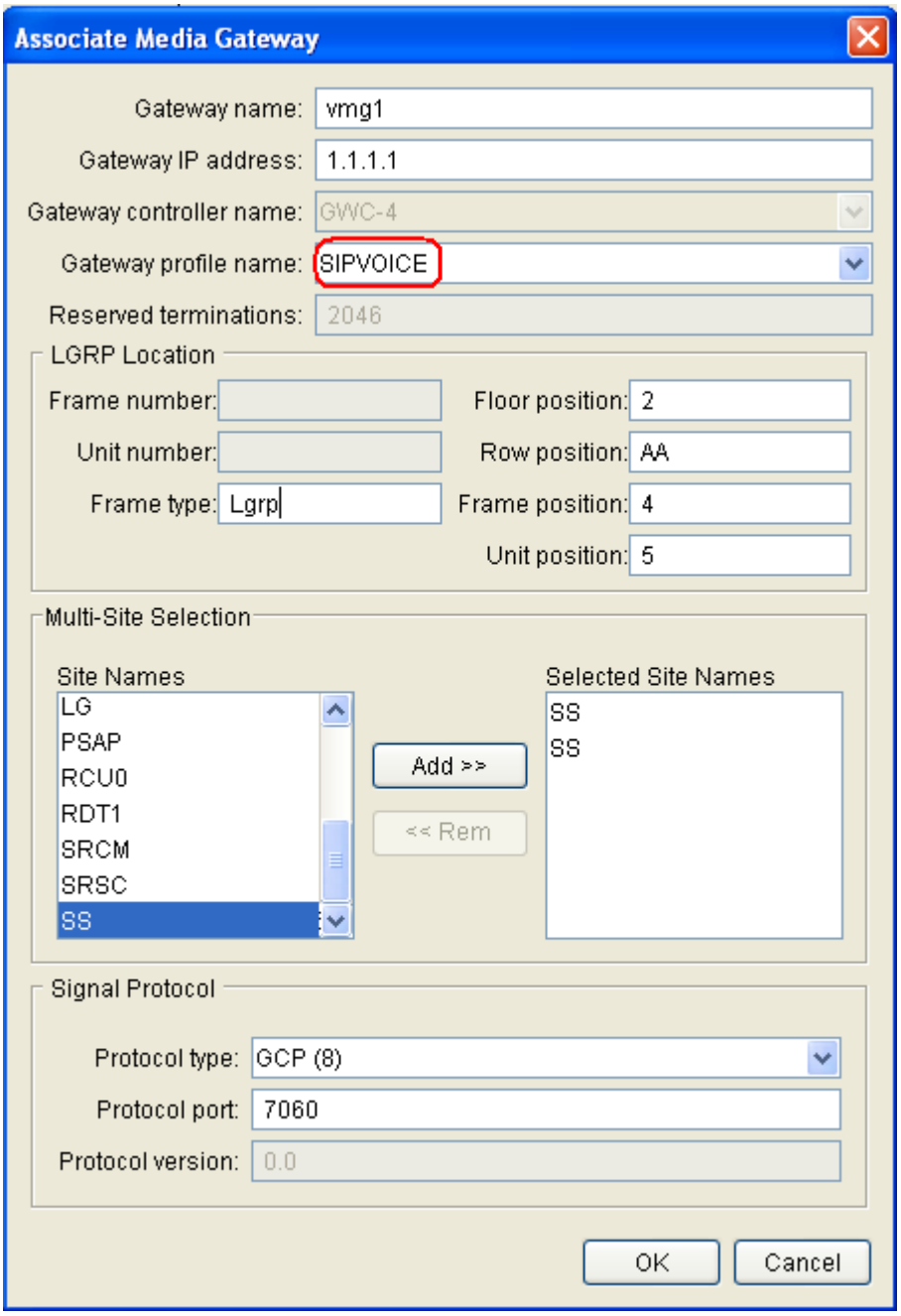


Also, the addition of these GWC profiles will update the GWC with a DPL enabled in the GWC configuration/capacity (GWC-PROFILE-MIB change).

11.2.2.2 Delete GWC

There are no changes required for this action.

11.2.2.3 Add GW



Adding a GW involves identifying a gateway name, IP address and selecting the SIPVOICE profile from the Gateway profile name list. The SIPVOICE selection causes an LGRP Location and Multi-Site Selection panel to appear.

The LGRP Location panel is used to provide the physical equipment location of the GW. LGRP_type is a string. Floor position, frame position and unit positions are all integers while row position is a char ‘A’ - ‘Z’, ‘AA’ or ‘AB’.

Below the LGRP Location panel is the Multi-Site Selection panel. Within this panel is a Site Names list and a Selected Site Names list. The Site Names list consists of all of the site names from table SITE in the CM. Site names are selected (placed in the Selected Site Name list) by simply clicking on the site name and selecting Add.

For SN09, a maximum of 12 site names can be selected. The same site name may be used multiple times by selecting Add several times.

Each site name represents one LGRP as defined by:

<site>/frame/group

Each LGRP is provisioned in table LGRPINV (CM) and represents 1023 endpoints. Each endpoint is added to table LNINV as:

<site> frame group terminal

where the terminal number ranges from 00 00 to 10 22.

The reserved termination field is updated as the Add button is selected.

The entries in the Signal Protocol panel are defaulted but can be changed.

Note: **Adding a fully provisioned CS2K SS GW will require approximately 10 minutes, or 2 minutes per LGRP.**

Note: Provisioning SIP GWs can only be performed one at a time. Attempts to provision multiple SIP GWs at the same time may cause all provisioning sessions to fail.

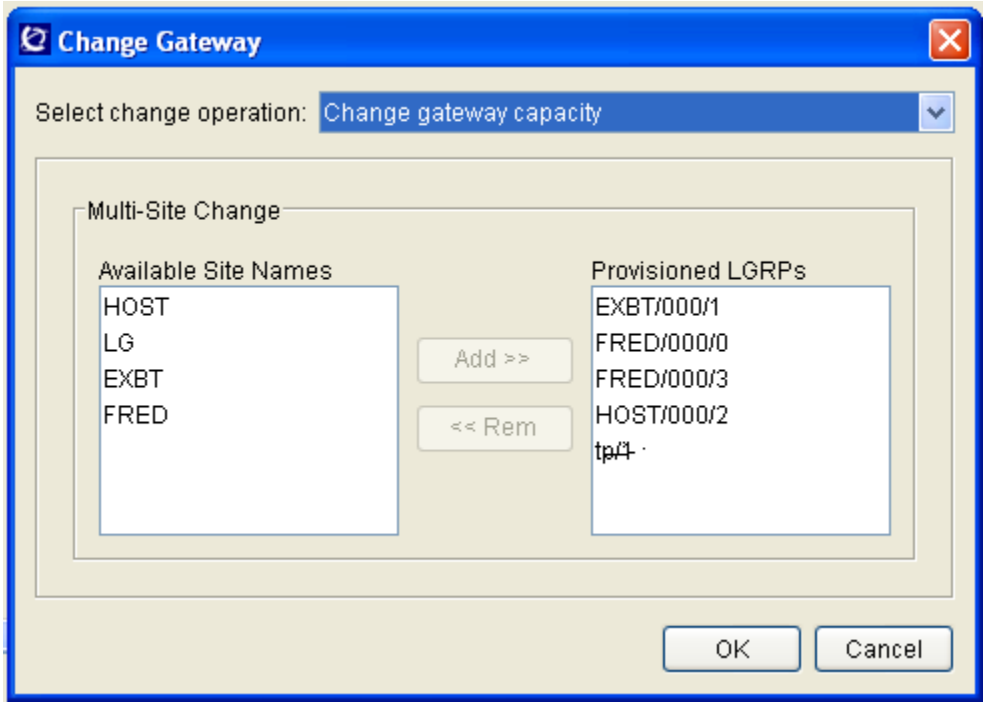
11.2.3 Design Solution / Module Flow Diagram

Addition of a GW includes (in order)

1. adding the GW to the GWC
2. adding one LGRP to LGRPINV (CM)
3. adding the associated endpoint groups (TN’s) for that LGRP to the GWC
4. adding the LENs to LNINV
5. Repeat steps 2-4 until all LGRPs have been added

11.2.3.1 Change GW

Figure 2 Change Gateway Capacity - Multi Site Dialog box



A gateway using the SIPVOICE profile will have the dialog box in figure 2 displayed. Similar to the AssocGW dialog box, this box contains two lists, Available Site Names on the left, which is a list of site names from the table SITE in the CM.

The second list, “Provisioned LGRPs”, is a list of site names already used and assigned. These site names have LGRPs and LENs assigned to it, therefore they show up with there respective frame and group numbers.

From this dialog box, the user can add additional site names (a maximum of 12 LGRP/Site names) are permitted in the Provisioned LGRPs list.

Additionally, the user can select to remove LGRP/Site names from the provisioned list simply by selecting them and the remove button.

Once the site names have been added, and OK selected, this diialog box will close and another panel will appear to display the progress and responses. The first item to display is the timeout value.

Cancel will close the box without executing any operation.

Note: Only single operations may be performed from the Change Gateway dialog; in other words, the user cannot add one site and remove another site in the same operation.

11.2.4 Configure

In the SESM, the /opt/nortel/NTsesm/admin/bin/configure tool should be used to configure SESM access to the Session Server Element Manager (SS-EM).

The configuration tool will prompt the user to enter the following:

- Transport protocol to SS-EM server (http/https - default is https). In SN09, only HTTPS is supported by the SS-EM, however flexibilty to choose HTTP is still provided to meet possible future needs.
- IP address / host name of primary SS-EM server
- IP address / host name of secondary SS-EM server. Some configurations may not include a secondary SS EM server. If so, configure the same information provided for the primary server (by default this should be the case).
- HTTP/HTTPS communication port to SS EM server (default 8080 for http, 8443 for https).
- The OPIClient version. This is mapped to the SS EM load version. In SN09, the appropriate value will be “9.0”. The OPIClient version should be incremented each release in steps of 1.0 i.e, 9.0, 10.0...15.0
- SS-EM Provisioning Manager administrator user name
- SS-EM Provisioning Manager administrator password

The IP address and port will be used to generate the SS-EM Provisioning Manager URL which in turn will be added to sesm.properties file.

As part of the configuration, the IP address will be validated for format, range and reachability. Other user entered data will be validated for format, range, values etc.

The user name will be added to sesm.properties as clear text.

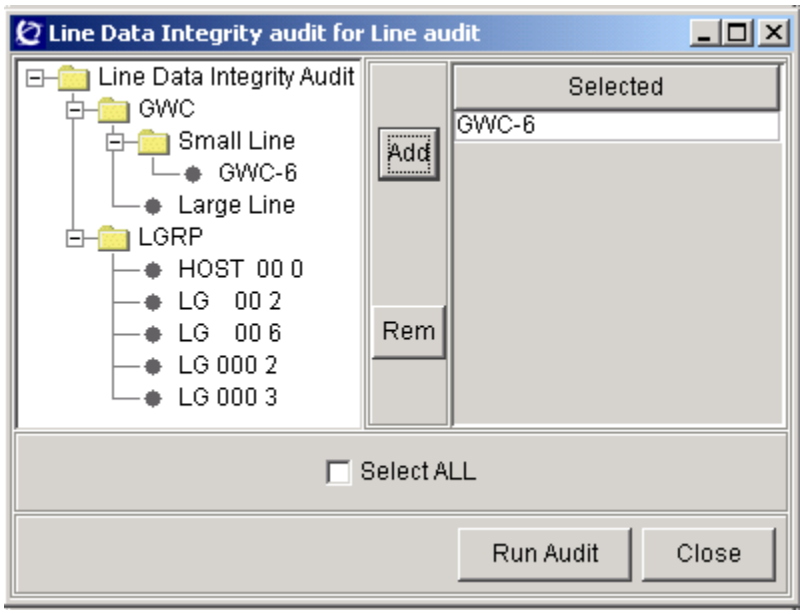
The password will be stored separately and accessible only to the root user.

All configuration information (url, username, etc.) except password can be displayed by using the SESM “/opt/nortel/NTsesm/admin/bin/configure” tool.

11.2.5 Audits

- Add a new gui to provide support for audit by GWCs, GWs or LGRPs. Only support Line Data Integrity audit now.

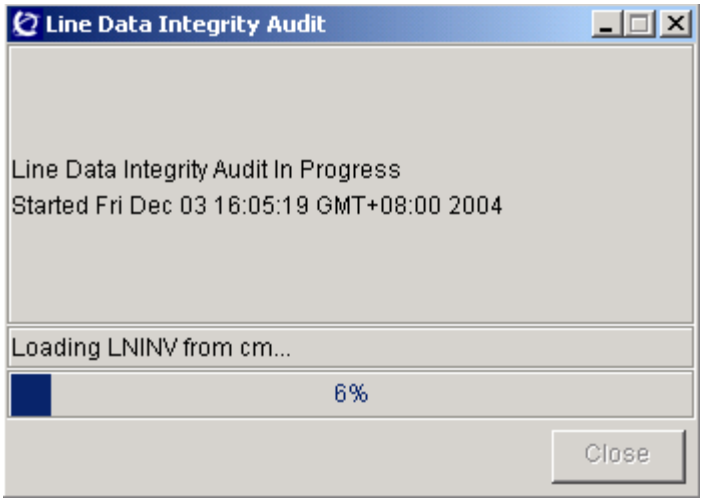
When users select “Line Data Integrity Audit” and press the “Run Audit” button in Audit System gui, the following gui will be displayed.



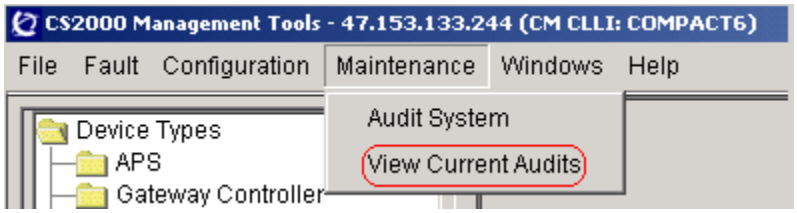
- User can select the gwc, gw or lgrp in the left tree and add them to the selected table by press the “Add” button.
- User can select the gwc, gw or lgrp in the right table and delete them from the table by press the “Rem” button.
- User can select all datas to do audit by select checkbox “Select All”. When user select the datas to do audit, the “Run Audit” button will be highlight.
- After user selected the data and press “Run Audit” button, the audit will be run as before.

- Add a progress bar in “Run Audit” gui to indicate the progress of the running audit.

Add a label to show current operation.

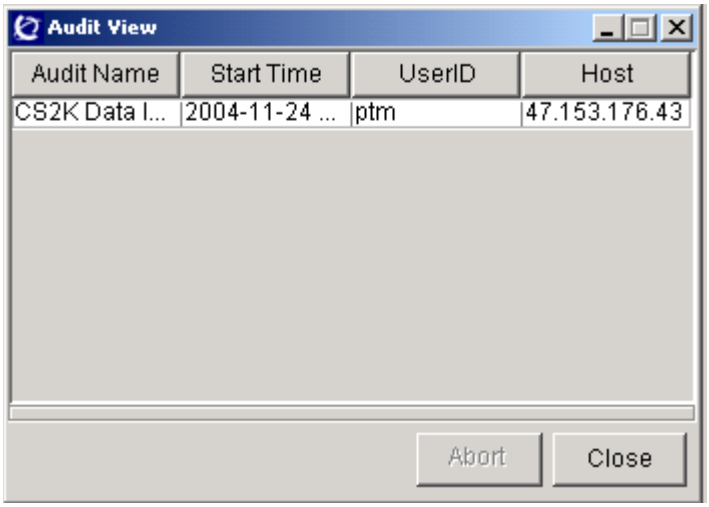


- Add a new menu in Maintenance of Cs2kmt to provide the new function “Abort Audit”.



When user selected the menu “View Current Audits”, another new gui will be displayed.

- Add a new gui to provide the new function “Abort Audit”.



The running audits will be displayed in this gui. The data of the audits include: Audit Name, Start Time, UserID, Host.

User can selected a running Audit and press the “Abort” button to abort the audit.

11.3 Hardware Requirements or Dependencies

Not applicable.

11.4 Software Requirements or Dependencies

This actrivity requires that the following components are loaded with SN09 or equalivalent loads.

CM, XAC or 3PC

GWC

MSM

11.5 Limitations and restrictions

None.

11.6 Interactions

This feature will integrate the SIP client provisioning with the existing Succession SERVORD+ system. SIP client commands/data are distributed to the SS-EM from the SERVORD+ system within the SESM. The following commands will trigger data distribution to the SS-EM from SESM SERVORD+ when SS vmgs/endpoints are found within the command: NEW, OUT, CHF

NOTE: CHF requires the use of gateway/termination names (or the equivalent LEN) in order to trigger flow through for SS lines. Use of DN will result in the command being processed only by the CM.

Query commands QLEN/QTP and QDN (which return formatted line/service information) will include the SIP_DATA options provisioned via the NEW/CHF commands in their output. The SIP_DATA option information will be appended to the end of the existing QLEN/QDN output, but prior to the dashed line (eg. “----------”) query output terminator line.

New data tags presented in query output with sample values:

END POINT DATA: *(This is the endpoint data header, no info/value associated with this tag)*

SIP_CLIENT_TYPE: SIP Line

SIP_EP_NAME: SCOT/000/0/0000

SIP_VMG_NAME: vmg1

SIP_DN: 6195209998

SIP_LOCATION: Nortel Networks.RTP.NC0

SIP_PACKAGE: SIP Lines

SIP_URI: slynch@mordor.com

See query examples in the next section for details on presentation and positioning within query output.

11.6.1 SERVORD+ Command Examples

See Configuration Section for SIP_DATA option format details and provisioning rules.

11.6.1.1 NEW command Examples:

NEW $ 6195209998 1FR LATA1 0 **SCOT 00 0 00 00** dgt SIP_DATA SIP_PACKAGE SIP Lines SIP_URI slynch@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD scott11 $ DPL Y 10 $

NEW $ 6195209998 1FR LATA1 0 **vmg1 SCOT/000/0/0000** dgt SIP_DATA SIP_PACKAGE SIP Lines SIP_URI slynch@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD scott11 $ DPL Y 10 $

11.6.1.2 CHF Command Examples

CHF $ SCOT 00 0 00 00 SIP_DATA SIP_PACKAGE siplines SIP_PASSWD scott11 SIP_CLIENT_TYPE IBN SIP_LOCATION IBM.RTP $ $

CHF $ **vmg1 SCOT/000/0/0000** SIP_DATA SIP_PACKAGE siplines SIP_PASSWD scott11 SIP_CLIENT_TYPE IBN SIP_LOCATION IBM.RTP $ $

11.6.1.3 OUT Command Examples

OUT $ 6195209998 SCOT 00 0 00 00 BLDN

OUT $ 6195209998 **vmg1 SCOT/000/0/0000** BLDN

11.6.1.4 Query Examples

```
> QLEN SCOT  00 0 00 00

------------------------------------------------------------------------------

LEN:     SCOT  00 0 00 00

END POINT: vmg1  SCOT/000/0/0000
```

```
TYPE: SINGLE PARTY LINE
SNPA: 619
DIRECTORY NUMBER:     5209998
LINE CLASS CODE:      1FR
SIGNALLING TYPE:  DIGITONE
LINE TREATMENT GROUP:     0
LINE ATTRIBUTE INDEX:     0
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: Y
PM NODE NUMBER     :    87
PM TERMINAL NUMBER :    1
OPTIONS:
DGT DPL Y 10
OFFICE OPTIONS:
SRA
END POINT DATA:
SIP_CLIENT_TYPE: SIP Line
SIP_EP_NAME: SCOT/000/0/0000
SIP_VMG_NAME: vmg1
SIP_DN: 6195209998
SIP_LOCATION: Nortel Networks.RTP.NC0
SIP_PACKAGE: SIP Lines
SIP_URI: slynch@mordor.com
--------------------------------------------------------------------------------

> qdn 5209998
--------------------------------------------------------------------------------
DN:     5209998
TYPE: SINGLE PARTY LINE
SNPA: 619   SIG: DT    LNATTIDX: 0
LINE EQUIPMENT NUMBER:     SCOT  00 0 00 00
END POINT: vmg1  SCOT/000/0/0000
LINE CLASS CODE:      1FR
LINE TREATMENT GROUP:     0
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: Y
PM NODE NUMBER     :    87
PM TERMINAL NUMBER :    1
OPTIONS:
DGT DPL Y 10
OFFICE OPTIONS:
SRA

END POINT DATA:
SIP_CLIENT_TYPE: SIP Line
SIP_EP_NAME: SCOT/000/0/0000
```

```
SIP_VMG_NAME: vmg1
SIP_DN: 6195209998
SIP_LOCATION: Nortel Networks.RTP.NC0
SIP_PACKAGE: SIP Lines
SIP_URI: slynch@mordor.com
--------------------------------------------------------------------------------
```

11.7 Glossary

Term	Description
New term	Definition

12: Functional Description (FN) A00008601

12.1 Feature name and Feature ID

ACT: A00008601, IW-SPM-IP Fully Provisionable Codec Lists for G.711/ G.729.

12.2 Description

This feature is to allow IW SPM IP's Codec list to be fully provisionable for G.711 and G.729.

The existing functionality of IW-SPM-IP supports the following two codec configurations.

1. G.711 Only

2. G.729 Preferred (1st Choice) and G.711 Supported(2nd Choice).

This feature extends the codec support of IW SPM IP by allowing codec list to be fully provisionable for G.711 and G.729. With this feature the following codec configuration can be provisionable in MNIPPARM table:

a. G.711 Only (G711 as default codec and NONE as preferred codec)

b. G.729 (preferred) / G.711(2nd Choice)

c. G.711 (preferred) / G.729(2nd Choice)

d. G729 Only (G729 as default codec and NONE as preferred codec).

The following codec list can be supported by IWIP SPM from SN09 for codec negotiation with the far end:

Table 1: Codec list supported by IWIP SPM from SN09

PRFCODEC **in MNIPPARM table**	**DFCODEC in MNIPPARM table**	Codec list supported by IWIP SPM
None	G711ALAW	G711ALAW, G711MuLAW
None	G711MuLAW	G711MuLAW, G711ALAW
None	G729	G729
G711ALAW	G729	G711ALAW, G711MuLAW, G729
G711MuLAW	G729	G711MuLAW,G711ALAW, G729
G729	G711ALAW	G729, G711ALAW, G711MuLAW

PRFCODEC **in MNIPPARM table**	**DFCODEC in MNIPPARM table**	Codec list supported by IWIP SPM
G729	G711MuLAW	G729, G711MuLAW, G711ALAW

Definitions for G711 and G729 codec are as follows:

G.711 is 64kbps codec. When G.711 is used, overall voice quality provided by IW-IP will have an ITU R Rating (G.107) of 90, which corresponds to a minimum average MOS of 4.3 (“Very Satisfactory” speech quality).

G.729 is 8kbps codec. When G.729A is used, overall voice quality provided by IW-IP will have an ITU R Rating (G.107) of 80, which corresponds to a minimum average MOS of 4.0 (“Satisfactory” speech quality).

Codec information is already provisionable in default codec[DFCODEC] and preferred codec[PRFCODEC] fields of MNIPPARM table. This feature only adds new values to support full provisioning of codec.

The default values of these fields remains same. The default value for DFCODEC filed is G711ULAW and the default value for PRFCODEC field is NONE.

Detailed information is available in Configuration Section.

12.3 Hardware Requirements or Dependencies

No new hardware required for this feature

12.4 Software Requirements or Dependencies

This functionality requires SN09 load in the Call Server, IW-IP CEM and GEM RM.

12.5 Limitations and restrictions

None

12.6 Interactions

None

12.7 Glossary

Term	**Description**
CEM	Common Equipment Module
GEM	Gigabit Ethernet (Resource) Module

Term	Description
IP	Internet Protocol
ITU	International Telecommunication Union
IW	Inter Working
MOS	Mean Opinion Score
RM	Resource Module
SPM	Spectrum Peripheral Module
TDM	Time Division Multiplexer

13: Functional Description (FN) A00008629

13.1 Feature name

GEM-II AAL2 IW-SPM SN09 Core Preparation Work

Notice a change in nomenclature. When referencing the original GEM card or GEM RM, GEM means “GigE Module” for IP applications. But when referencing the new GEM-II card, GEM means “Generic Equipment Module” since GEM-II can support either Gig-E (IP) and AAL2 applications.

13.2 Description

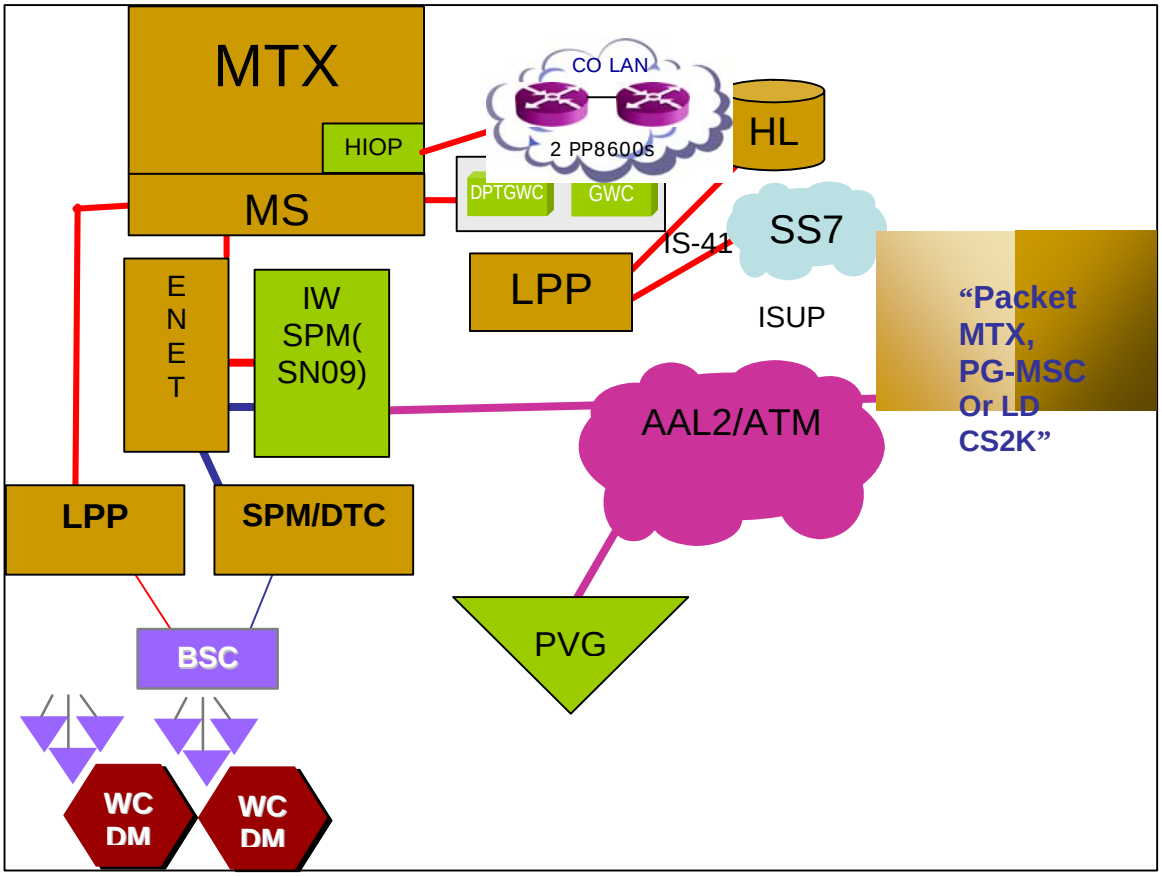
This activity implements all Core work in SN09 for the AAL2 ATM feature being delivered in MTX14. The AAL2 IW-SPM feature will allow customers of CDMA Wireless MTX switches to extend their ENET connected peripherals to ATM networks for voice and data call processing over AAL2 connections.

The ATM/AAL2 RM, based on the new ‘Generic Equipment Module 2’ (GEM-II) NTLZ20DA circuit pack, will be delivered as part of the Succession IW-SPM product offering beginning in the MG4K23 release. The GEM-II hardware is being introduced in SN09/MG4K22 as a replacement for the ‘Giga-bit Ethernet Module’ (GEM) RM which supports IP applications. The GEM-II RM has additional hardware capability of supporting ATM based applications over AAL2. The GEM-II runs on an IW-SPM configured as IP or AAL2. The GEM II provides PQII, TI DSPs (on board), winpath787, ECAN tone detection, generation, vocoding, etc.

Working AAL2 functionality will be delivered in MTX14, which is based on SN09 and MG4K23. The required AAL2 local code in the CEM and RM will be delivered in MG4K23. The A00008629 Core activity is being done in SN09 as a preparation activity to avoid later patching of the Core. With activity A00008629, the customer can datafill an IW-SPM as AAL2 bearer fabric with NTLZ20DA as an ATM RM. The customer can also datafill the AAL2 protocol parameters and the five required ATM carriers (same 5 that are required on AAL1 ATMs). A single office parm will control whether the AAL2 IW-SPM feature is active; this parm is “off” by default and should be enabled in MTX14 once the production MG4K23 loads become available.

Figure 1 below shows a network diagram of a wireless MTX switch with the AAL2 IW-SPM bridging calls from SPM/DTC over AAL2 to PVG.

Figure 1 Wireless Base Station Network using IW-SPM AAL2 solution. Note



that there is also a TDM bearer path connection between BSC and PVG.

13.3 Hardware Requirements or Dependencies

The new NTLZ20DA GEM-II circuit pack is being introduced in SN09 for IP applications running on a GEM-type RM. In MTX14, this same NTLZ20DA pack can be configured in software to work as an ATM RM providing AAL2 connectivity.

The GEM-II pack provides these external user interfaces on the faceplate, listed in top-down order:

1. Red triangular LED: works like standard SPM RM to indicate OOS status. When lit, card is OOS; when blank, card is InSv.
2. Green square LED: works like standard SPM RM to indicate activity status. When lit, card is active; when blank, card is in standby mode.
3. Green circular LED labeled "LINK": lights steady to indicate signal is being received; blank if no signal is being received. For AAL2 application, this signal would be the SONET signal from the far end. For IP application, this signal would be the Ethernet signal from the CS2K.

4. SFP (Small Form Pluggable) connector: for IP applications, this connector accepts a MT-RJ or LC plug that provides GigE (Gigabit Ethernet) interface for 1000B-SX or 1000B-LX. For AAL2 applications, this connector accepts a LC plug that provides OC3 SONET interface for SR (Short Reach), IM (Intermediate Reach), or LR (Long Reach). The SFP connector is compliant with specification SFF-8472 revision 9.3 (produced by the SFF Committee).

For AAL2, the transmit and receive SONET fibers are connected to an OC3 SONET plug inserted in the SFP. Note that the SFP interface is considered part of the cable and hence will not be ordered with the card.

The supported cable types for both SONET and GigE applications are:

a. single mode: good up to 5-6km and always uses a laser.

b. multi mode: good up 500m and can use LED instead of laser.

13.4 Software Requirements or Dependencies

A new GM2xxxx firmware load will be introduced in SN09/MG4K22 for the GEM-II configured as GEM RM for IP application.

In MG4K23, a new AL2xxxx load will be introduced to provide the AAL2 application on the GEM-II card. This new AL2xxxx load will only be supported on a GEM-II card configured as an ATM RM on a IW-SPM configured for AAL2 ATM fabric.

CEM changes are also required in MG4K23 for the IWSxxxx load to support AAL2 on the IW-SPM.

13.5 Limitations and restrictions

1. Attempts to load or RTS AAL2 ATM RM in SN09 are not permitted until the MG4K23 loads are available for the CEM and RM. Hence, AAL2 calls cannot be made until MTX14 when MG4K23 loads are available.
2. The GEM-II card can operate as IP or AAL2, but not both at the same time.

13.6 Interactions

Feature A00007926 was implemented in SN08 to introduce provisioning of the new NTLZ20DA PEC code for IP applications. In SN09, this same NTLZ20DA PEC code can be datafilled for AAL2 applications.

13.7 Applicable customer facing sections

Fault Management

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

13.8 Glossary

Term	Description
AAL2	ATM Adaption Layer 2
GEM	Gig-E Module (for IP applications)
GEM-II	Generic Equipment Module II (the NTLZ20DA)
PQII	Power Quick II processor
SFP	Small Form Pluggable

14: Functional Description (FN): A00008724

14.1 Feature name and Feature ID

A00008724: OMDD Enhancements and Robustness.

14.2 Description

This Activity address the following items:

1. Implementing a FTP retry mechanism for OMDD application: If FTP fails to send OM reports to any of the configured downstream machines for various reasons like downstream reboot, network congestion, password change and maintenance in downstream etc., those reports will be attempted to be sent to downstream at the next scheduled interval.
2. Improving OMDD audit mechanism: With current design there is a possibility of omdata filesystem getting filled up before the audit happens. Current audit period is every 6 hours. The improved audit mechanism will ensure that the omdata filesystem will not reach 100% at any instance for the currently supported OM capacity for SN09 release.
3. Enhancing file rotation mechanism: Currently there is a file rotation problem from *open* to *closedNotSent* directory when SDM/CBM and CM are not in sync with respect to time.This will result in configured downstream not receiving OM reports at scheduled time. This activity will make sure that all OM reports will be sent to downstream according to configured schedule.

14.3 Introducing ftp retry mechanism

Currently user can configure OMDD to send OM report to single/multiple downstream destinations. If the ftp fails for some reason, OMDD will not try to send the OM reports downstream again and the files are moved from *closedNotSent* to *closedSent* directory. To be specific, once ftp is attempted for an OM report file, OMDD will move the file to *closedSent* directory irrespective of the success or failure of the file transfer. On failure cases, log will be generated to notify the failure of the file transfer.

In case of failure to transfer the OM reports to downstream destination, this activity will ensure that reports are re-attempted to be sent.

If the OM report transfer fails for any destination, OMDD will keep track of the destination to which the report could not be transferred. At the next File Transfer Schedule, OMDD will attempt to send the report to the destination again. This will be done on every file transfer schedule until

- a successful transfer or
- this file exceeds the retention period of the *closedNotSent* directory or
- the file gets deleted during audit.

14.4 Improving OMDD Audit mechanism

OM reports are stored in omdata filesystem. Currently, this filesystem is audited every 6 hours. During the audit, if omdata filesystem usage is found to be more than 60%, then OMDD generates a warning log to the user stating *"ODM: WARNING omdata storage use exceeds 60 percent. Files will be deleted in next audit if the usage exceeds 70 percent"*.
In the next audit, if omdata filesystem usage is found to be more than 70%, then OMDD deletes all the files from *closedSent* directory. The filesystem usage will be calculated again and if is still more than 50%, files from *closedNotSent* directory will be deleted starting from the oldest file.This procedure is repeated till omdata filesystem usage is less than or equal to 50%. Customer will be notified on deletion of each file from *closedNotSent* directory through *Major* log.

With the current audit interval of 6 hours, there is still a high chance that omdata filesystem might get filled up in between two audits.

This activity will reduce the audit interval to 30 minutes with the following changes:

- Generate Major log when omdata filesystem usage reaches 60%.
- Generate Major Trouble log when omdata filesystem usage reaches 80%.
- Generate Info log and delete all files in *closedSent* directory on reaching 90% usage of omdata filesystem.
- If omdata filesystem usage does not fall below 80% after deletion of all the files in *closedSent* directory, files from *closedNotSent* directory will be deleted starting from the oldest file till the usage reaches 80% or less.
- Generate Info log for each file deletion from *closedNotSent* directory.
- Generate the corresponding Clear logs for all Major logs.

This activity will ensure that omdata filesystem usage will not reach 100% at any instance for the currently supported OM capacity for SN09 release.

1. The following log is generated when audit finds omdata filesystem usage exceeds 60%.
SDM338 MAJOR TBL SDM OM FILE RETENTION
ODM: Audit finds omdata usage exceeds 60 percent.OM files will be deleted in the next audit if the usage exceeds 90 percent.

2. The following clear log is generated when audit finds omdata filesystem usage goes below 60%.
SDM638 NONE INFO SDM OM FILE RETENTION
ODM: Audit finds omdata usage has gone below 60 percent.

3. The following log is generated when audit finds omdata filesystem usage exceeds 80%
SDM338 MAJOR TBL SDM OM FILE RETENTION
ODM: Audit finds omdata usage exceeds 80 percent.OM files will be deleted in the next audit if the usage exceeds 90 percent.

4. The following clear log is generated when audit finds omdata filesystem usage goes below 80%
SDM638 NONE INFO SDM OM FILE RETENTION
ODM: Audit finds omdata usage has gone below 80 percent.

5. The following log that is generated when audit finds omdata filesystem usage exceeds 90%
SDM639 NONE INFO SDM OM FILE RETENTION
ODM: Audit finds omdata usage exceeds 90 percent.All the OM files from closedSent directory will be deleted now

6. The following log is generated when a file in *closedNotSent* directory is deleted by audit to make morethan 80% available space in omdata filesystem.
SDM631 MINOR INFO SDM OM FILE RETENTION
ODM:The File<filename> from closedNotSent directory deleted by audit to free up space in omdata.

-where <filename> is the name of the file deleted from *closedNotSent* directory.

14.5 Enhancing File Rotation Timer

OM reports for an office transfer(OT) period will be sent from CM in either 15 or 30 minutes interval based on the CM configuration.When SDM and CM are out of sync by ~3 minutes OMDD fails to trigger the file rotation from *open* to *closedNotSent* directory in accordance with file rotation schedule[FRS]. This causes reports not reaching the downstream on time.

This activity will enhance the file rotation mechanism, so that files are rotated in accordance with FRS even when SDM/CBM and CM are not in sync.

14.6 Hardware Requirements or Dependencies

- SDM with basic configuration
- CBM with basic configuration

14.7 Software Requirements or Dependencies

Latest SDM22/CBM22 load with Table Access and OM Access services should be in service.

CM - SDM/CBM connectivity should be up.

14.8 Limitations and restrictions

None

14.9 Interactions

None

14.10 Glossary

Term	Description
CBM	Core and Billing Manager
CM	Computing Module
FTP	File Transfer Protocol
FRS	File Rotation Schedule
OM	Operation Measurement
OMDD	Operational Measurements and Data Delivery
OT	Office Transfer
SDM	Supernode Data Manager

15: Functional Description (FN): A00008740

15.1 Feature name and Feature ID

A00008740: SN09 CLOCK SYNC ROBUSTNESS.

15.2 Description

This Feature covers the software development on the Succession MG9000 (MG9K) node and specifically on the ABI card.

15.3 Hardware Requirements or Dependencies

15.4 Software Requirements or Dependencies

There are no software feature dependencies required by this feature. This feature is stand alone.

15.5 Limitations and restrictions

15.6 Interactions

15.7 Glossary

Term	Description
LCI	Local Craft Interface – A web based user interface
FITS	Fault Insertion TestS

16: Functional Description (FN): A00008858

16.1 Feature name and Feature ID

Feature A00008858: CS2M and MG9KEM User Inactivity Time-out

16.2 Description

This SN09 feature provides a standard and consistent design across MG9KEM and CallServer 2000 Management Tools (CMT) for client user inactivity time-out. There are three timers that will be configurable from the SSPFS CLI after the initial SSPFS installation. The three timers are:

- User Inactivity Timeout
- User Termination Timeout
- Reauthentication Disable Timeout

16.2.1 Configuration Behavior

Default Assignment - The default value of 10 minutes will be set on SSPFS installation for User Inactivity Timeout and User Termination Timeou. The default for Reauthentication Disable Timeout will be 30 seconds.

Accepted Values - The values for User Inactivity Timeout and User Termination Timeout can be entered in increments of full minutes(e.g 1, 2,3) The values can range from a minimum of 5 minute to a maximum of 1440 minutes(24 hours). The value ‘0’ will be used to indicate that no timeout implementation is desired, effectively turning this feature off.This applies to either value as follows. The accepted values for Reauthentication Disable Timeout are 0-300 in seconds.

- If the user wants to turn off the entire timeout feature, a value of ‘0’ for USER_INACTIVITY_TIMEOUT will indicate this.
- If the user wants the timeout feature to be activated but does not desire a USER_TERMINATION_TIMEOUT to be enforced, the value ‘0’ will indicate this

When the CLI is used to configure the timeout values, they will take effect immediately for all new client launches. No restart is required. The configuration access is located centrally to all supported applications and requires ‘root’ access to the SSPFS server.

16.2.2 CLUI Behavior

After user runs the CLUI, If there is no user input on the command line for the duration of the first timer, the process is killed and user exits from the session to the shell.

16.2.3 General GUI Behavior

When the User Inactivity Timeout expires for a given application, all application windows will be minimized, which prevents all users input and provides no data output to the user. Proper login authentication is required to release the application lock and make the application visible. Once the re-authentication occurs, the user's desktop view will be restored with no updates lost.If the application user does not re-authenticate within an acceptable time frame, as defined by the User Termination Timeout, the application user will be forced to exit the application before making another authentication request. Note that the User Termination Timeout does not start until the User Inactivity Timeout expires.

16.2.4 Re-authentication Behavior

The SSPFS Security Servlet enforces security limitations during re-authentication attempts. No userid will be displayed in the re-authentication window. If there are 3 failed authentication attempts, the re-authentication window will be locked for 30 seconds. After the 30 second timer, which is configurable, re-authentication will be allowed.

Table 1 Application Behavior Summary

Type	Name	Behavior
Launch Page	CS2M Launch Point	After user launches the Launch Page, If there are no user initiated mouse movements for the duration of the first timer, the client is iconizied and a dialog is popped up to prompt the user re-login. Only after successful re-authentication, the launch page is de-iconized. If there are no user initiated mouse movements on the screen for the duration of the second timer (At that time the client should be iconized and a login dialog is shown), a warning dialog is popped up which saying that the client is locked due to long time non-operation. When user confirm it, the client as well as the re-login dialog are both closed.

Type	Name	Behavior
Java GUI	CS2000 Management Tool GUI Line Maintenance Manager GUI GWC EM Independent GUI GWC EM Independent GUI launched from SAM21 EM Succession SAM21 Element Manager GUI SAM21 EM GUI launched from GWC EM Network Patch Manager GUI	After user launches the GUI, If there are no user initiated mouse movements for the duration of the first timer, the client is iconizied and a dialog is popped up to prompt the user re-login. Only after successful re-authentication, the GUI is de-iconized. If there are no user initiated mouse movements for the duration of the second timer (At that time the client should be iconized and a login dialog is shown), a warning dialog is popped up which saying that the client is locked due to long time non-operation. When user confirm it, the client as well as the re-login dialog are both closed.
Web GUI	Trunk Maintenance Manager Batch Configuration Monitor	After user launches the web client, If there are no user initiated **mouse clicks** on any html link/button/droplist for the duration of the first timer, when user mouse clicks, the Web Page will be redirected to the re-login page, on which it shows user "Application Session Invalid" and provide the link for re-login as well as the link for close current window. After user re-authenticated successfully, the page is re-direct to the original page. If there are no user initiated mouse clicks on the screen for the duration of the second timer, when user perform any mouse clicks, a warning message which says that the client is locked due to long time non-operation. Then the web client is closed directly after user confirm the message.
CLUI	GWCEM CLUI NPM CLUI SAM21 EM CLUI OSSGate CLUI BPT CLUI AMS CLUI	After user runs the CLUI, If there is no user input on the command line for the duration of the first timer, the process is killed and user exists from the session to the shell. If there is no user input on the command line for the duration of the shell time out value, user will exist from the shell automatically.

16.3 Hardware Requirements or Dependencies

None.

16.4 Software Requirements or Dependencies

None

16.5 Limitations and restrictions

Limitations and restrictions are:

1) The following CLUIs which run inside SSH/Telnet session, are not supported by this design. They are the SSPFS cli tool, SESM configure tool, App Start/Stop script and the Unix self-contained commands.

2) The UAS GUI is non-compliant with this design. There is no plan to support user inactivity timeout.

3) The APS GUI is partially compliant with this design. A fixed timeout is supported which logs the user out, but there is no re-login or minimization support planned

4) The Security Server Manager, used to configure secure IPSec connections between and SSPFS server and another destination(e.g. MG9000) is partially compliant to this design. A default 5 minute timeout exists and the user must initiate an action before being redirected to a page that will allow re-authentication. No changes were added to this functionality as a part of this feature.

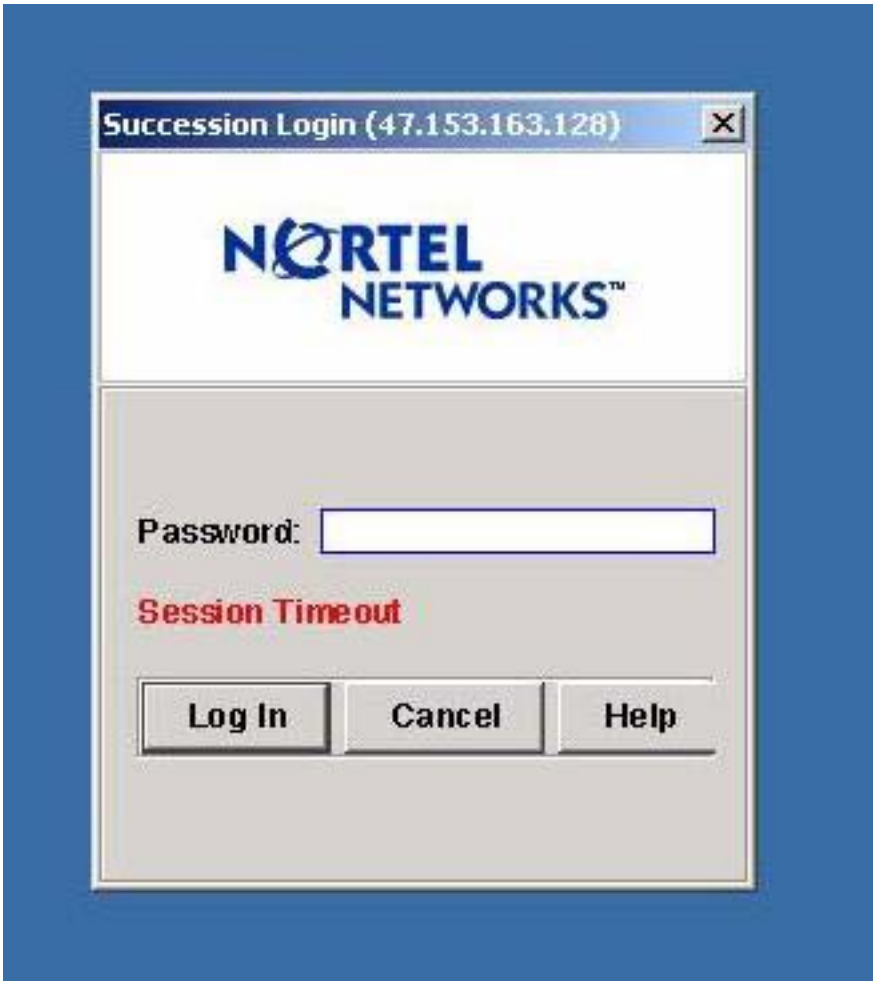
5) There may be some platform specific behavor in the GUI desktop. This applies strictly to the requirement to restrict all user access and provide no data output to the user when the timeout occurs. Based on the software platform the top-level view may be iconified or disappear all together.

6) Although the configuration is centrally located within the SSPFS platform, the craftsperson or system administrator must manually ensure that the timeout values across SSPFS servers are kept in sync between CMT and MG9KEM servers if this is the desired behavior. In other words, as long as the defaults are in place the CMT and MG9KEM applications will behave in exactly the same manner. Once the administrator makes a change on one SSPFS server there is not a design or expectation that this will be automatically synchronized.

Note: Though no specific design support is planned for the Unix shell applications as mentioned herein, the SSPFS does currently support a shell timeout that will kill a shell session if there is no activity within a specific time period. The value for this shell timeout is configured via the /etc/profile file as the TMOUT value

16.6 Screenshots

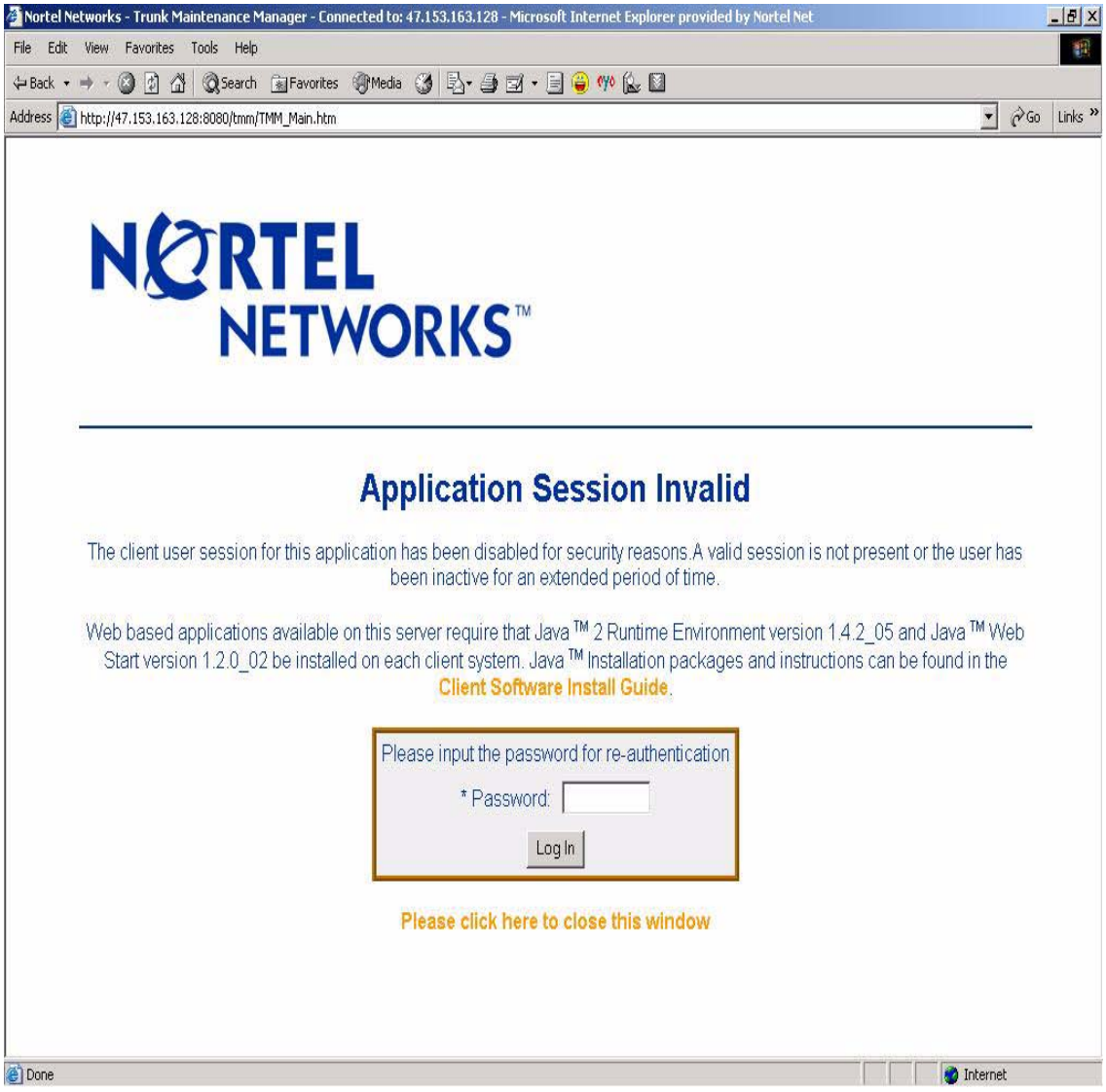
GUI Timeout



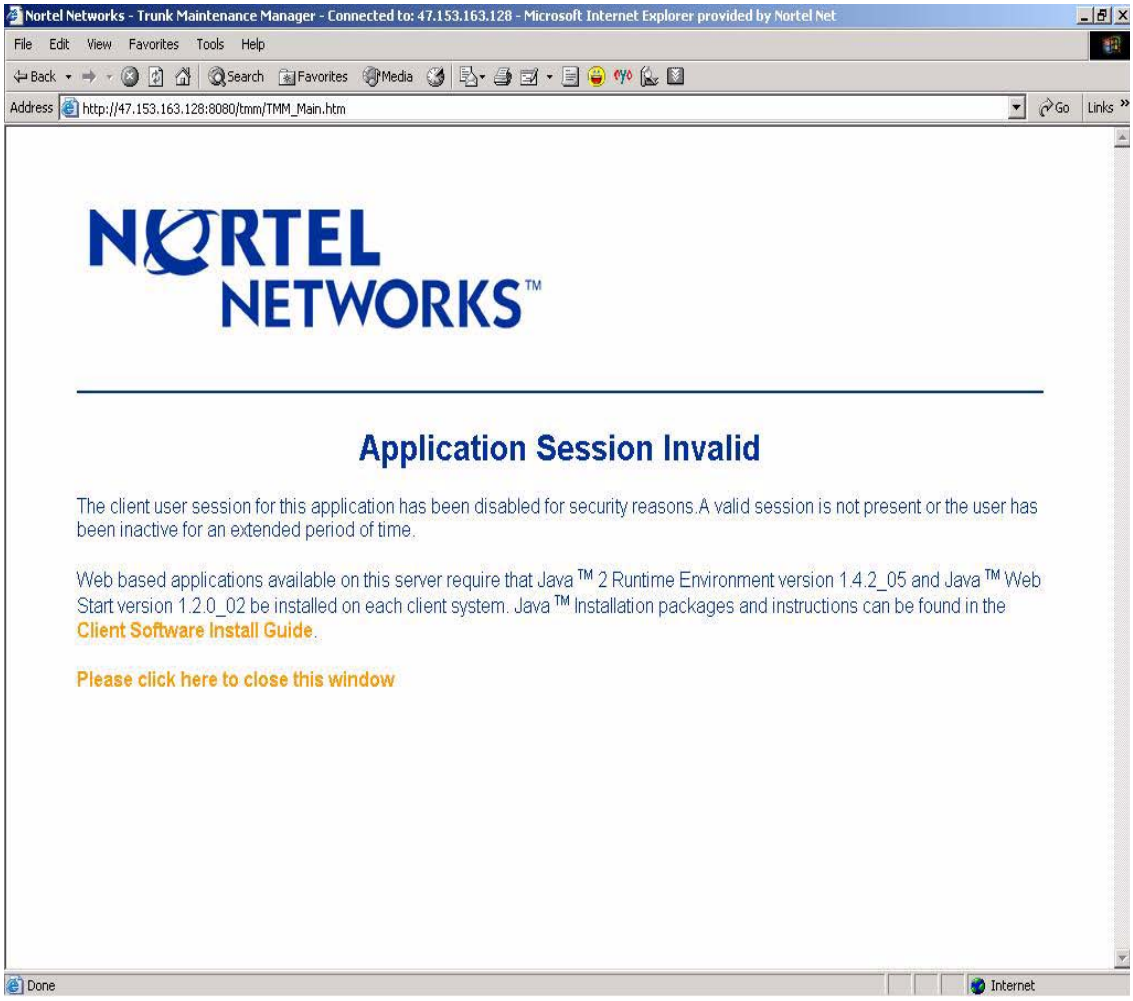
GUI Terminate Timeout

GUI After 3 Retries Fail

TMM Timeout


Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.163.128 - Microsoft Internet Explorer provided by Nortel Net
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://47.153.163.128:8080/tmm/TMM_Main.htm
Go Links
NORTEL NETWORKS™
Application Session Invalid
The client user session for this application has been disabled for security reasons.A valid session is not present or the user has been inactive for an extended period of time.
Web based applications available on this server require that Java ™ 2 Runtime Environment version 1.4.2_05 and Java ™ Web Start version 1.2.0_02 be installed on each client system. Java ™ Installation packages and instructions can be found in the Client Software Install Guide.
Please input the password for re-authentication
* Password:
Log In
Please click here to close this window
Done
Internet

TMM Terminate Timeout



16.7 Interactions

None

16.8 Glossary

MG9K EM Media Gateway 9000 Element Manager

CLUI Command Line User Interface

CS2M CS2000 Management Components

CMT CS2000 Management Tools

GWCEM Gateway Controller Element Manager

NPM Network Patch Manager

SSPFS Succession Server Platform Foundation Software

SESM Succession Element & Sub-element Manager

SAM21 EMCS2000 SAM21 Manager

17: Functional Description (FN): A00008916

17.1 Feature name and Feature ID

Feature A00008916: Gateway Controller Lines Density Increase

17.2 Description

With the introduction of the N905 Gateway Controller hardware there is now increased CPU speed and memory capacity. This enables increased port density and combined profiles. The new profiles introduced by this feature are only compatible with N905 GWC hardware and will not operate with MCP750 GWC hardware, therefore both GWC units MUST be loaded with N905 hardware before the GWC profile is migrated to one of the new N905 profiles.

The new profiles are forward compatible with certain existing profiles, allowing for in-service profile migrations. However, the new profiles are not backward compatible with previous profiles. In other words, once a N905 GWC is migrated to a new profile it cannot be migrated back to a previous profile. The only way to migrate backwards from high-density profile is to delete the GWC provisioning from the SESM database and re-provision the GWC.

17.2.1 Small Gateway Lines High Density Profiles

The High Density small line gateway profiles support 25,600 lines and small gateways without IPSEC turned on. If IPSEC is to be supported then the engineering limit is 12,800 gateways and lines. This is an engineering rule and is not enforced by the software, the software will allow up to 25,600 lines and gateways to be provisioned regardless of IPSEC. As noted above, once a GWC has been migrated to the high density profile it cannot be downward migrated to the previous profile without deleting the provisioning and re-provisioning with desired profile.

PROFILE NAME: SMALL_LINENA_V2

This profile is a high density version of the SMALL_LINENA profile. It enhances SMALL_LINENA by increasing line and gateway capacity from 6,400 to 25,600. This profile is compatible with SMALL_LINENA as part of an in-service upgrade.

TERM TYPE	EXEC DATA	TONEDATA
POTS	POTSEX	NORTHAA
KEYSET	KSETEX	

CAPABILITY	CAPACITY
Lines	25,600
Small Gateways	25,600
IPSEC	

Kerberos	
DQOS	80

PROFILE NAME: **SMALL_LINEINTL_V2**

This profile is a high density version of the SMALL_LINEINTL profile. It enhances SMALL_LINEINTL by increasing line capacity from 6,400 to 12,800 lines and gateways. This profile is compatible with SMALL_LINEINTL as part of an in-service upgrade.

TERM TYPE	EXEC DATA	TONEDATA
POTS	POTSEX	UKADSI
KEYSET	KSETEX	

CAPABILITY	CAPACITY
Lines	25,600
Small Gateways	25,600
IPSEC	
Kerberos	
DQOS	80

17.2.2 Large Gateway Lines High Density Profiles

The High Density large line gateway profiles support 12,800 lines and small gateways with or without IPSEC. This profile also supports SIP Lines [DPL] (see feature A00008522 for details). As noted above, once a GWC has been migrated to the high density profile it cannot be downward migrated to the previous profile without deleting the provisioning and re-provisioning with desired profile.

PROFILE NAME: **LARGE_LINENA_V2**

This profile is a high density version of the LARGE_LINENA profile. It enhances LARGE_LINENA by increasing line capacity from 6,400 to 12,800 lines. This profile is compatible with LARGE_LINENA as part of an in-service upgrade.

TERM TYPE	EXEC DATA	TONEDATA
POTS	POTSEX	NORTHAA
KEYSET	KSETEX	
DPL_TERM	DPLEX	

CAPABILITY	CAPACITY
Lines	12,800
Large Gateways	27
IPSEC	
DPL	

PROFILE NAME: **LARGE_LINEINTL_V2**

This profile is a high density version of the LARGE_LINEINTL profile. It enhances LARGE_LINEINTL by increasing line capacity from 6,400 to

12,800 large lines. This profile is compatible with LARGE_LINEINTL as part of an in-service upgrade.

TERM TYPE	EXEC DATA	TONEDATA
POTS	POTSEX	UKADSI
KEYSET	KSETEX	

CAPABILITY	CAPACITY
Lines	12,800
Large Gateways	27
IPSEC	
DPL	

17.2.3 Combined Lines, Trunks, and Audio Profiles

These profiles combine the SMALL_LINE, LARGE_LINE, TRUNK, and AUDCNTL profiles into one combined profile at MCP750 capacities. This profile also supports SIP Lines [DPL] (see feature A00008522 for details). All gateway types and capabilities that are supported on the individual profiles are supported in this combined profile with the following exceptions:

- 250 PTS and PRI trunk types are not supported on the combined profile (250 ISUP trunks are supported). 250 PTS and PRI trunks must be removed before migrating to the combined profile.

As noted above, once a GWC has been migrated to this profile it cannot be downward migrated to the previous profile without deleting the provisioning and re-provisioning with desired profile.

PROFILE NAME: **LINE_TRUNK_AUD_NA**

This profile is a combination of the SMALL_LINENA, LARGE_LINENA and TRUNK_NA profiles. This profile is compatible with SMALL_LINENA, LARGE_LINENA, and TRUNK_NA as part of an in-service upgrade.

TERM TYPE	EXEC DATA	TONEDATA
POTS	POTSEX	NORTHAA
KEYSET	KSETEX	
PRAB	DTCEX	
ABTRK	GWCEX	
DPL_TERM	DPLEX	

CAPABILITY	CAPACITY
Lines	6400
Trunks	4094
Audio	4096
DQOS	20
Small Gateways	6400
Large Gateways	51
Audio Gateways	16
BCT	
IPSEC	

KERBEROS	
Conferences	
Announcements	
DPL	

PROFILE NAME: **LINE_TRUNK_AUD_INTL**

This profile is a combination of the SMALL_LINEINTL, LARGE_LINEINTL and TRUNK_INTL profiles. This profile is compatible with SMALL_LINEINTL, LARGE_LINEINTL, and TRUNK_INTL as part of an in-service upgrade.

TERM TYPE	EXEC DATA	TONEDATA
POTS	POTSEX	UKADSI
KEYSET	KSETEX	
PRAB	DTCEX	
ABTRK	GWCEX	
DPL_TERM	DPLEX	

CAPABILITY	CAPACITY
Lines	6400
Trunks	4094
Audio	4096
DQOS	20
Small Gateways	6400
Large Gateways	51
Audio Gateways	16
BCT	
IPSEC	
KERBEROS	
Conferences	
Announcements	
DPL	

17.2.4 Profile Compatibility

The following table lists which new profiles are compatible with existing profiles. As noted above, once a GWC has been migrated to a N905 supported profile it cannot be downward migrated without deleting the provisioning and re-provisioning with desired profile.

Figure 1 Profile Compatibility Table

Existing Profile (SN08)	Compatible In-Service Upgrade To (SN09 Profile)
SMALL_LINENA	SMALL_LINENA_V2, LINE_TRUNK_AUD_NA
SMALL_LINEINTL	SMALL_LINEINTL_V2, LINE_TRUNK_AUD_INTL
LARGE_LINENA	LARGE_LINENA_V2, LINE_TRUNK_NA

LARGE_LINEINTL	LARGE_LINEINTL_V2, LINE_TRUNK_INTL
TRUNK_NA	LINE_TRUNK_AUD_NA
TRUNK_INTL	LINE_TRUNK_AUD_INTL
SIP_LINES_NA	LARGE_LINENA_V2, LINE_TRUNK_NA
SIP_LINES_INTL	LARGE_LINEINTL_V2, LINE_TRUNK_INTL

17.2.5 GWC Profile Migration Instructions

Once both GWC units have been upgrade to N905 hardware, the GWC profile can be migrated to one of the new N905 profiles using the SESM GUI. Following a successful GWC Profile change, both units of the Gateway Controller must be reloaded before the change takes affect, the GWC units are still running on previous profile until a lock/unlock is performed. An alarm is raised for each unit to indicate a data mismatch exists between the SESM server and the Gateway Controller. The alarm condition is displayed by the **Alarm Manager** accessed via the **Fault** menu. The alarm will be cleared once the GWC units have been reloaded.

1. Verify that both GWC units are N905 hardware.
2. Change Profile from SESM GUI (alarm will be generated).
3. (SESM GUI) **Busy** the inactive unit.
4. (SAM21 GUI) **Lock** and **Unlock** the associated card. The card is booted and provisioned data is downloaded following the unlock operation. The data mismatch alarm condition is cleared for this unit.
5. (SESM GUI) **RTS** the inactive unit.
6. (SESM GUI) **Warm Swact** the Gateway Controller.
7. Repeat steps 3 through 6 for the mate unit.

17.3 Hardware Requirements or Dependencies

This feature is dependent on the N905 GWC hardware.

17.4 Software Requirements or Dependencies

SN09 SESM, SAM-21 and GWC loads.

17.5 Limitations and restrictions

The new profiles are only supported on the N905 hardware. An MCP750 GWC will not come into service if it is provisioned with one of the new profiles. If the GWC card is pre-provisioned with a N905 profile and then loaded with MCP750 hardware and booted, an alarm will generated. This is

an unsupported configuration, both GWC units must be loaded with N905 hardware.

If an MCP750 profile is already in service (not a pre-provisioning case) the software will verify that N905 hardware exists before allowing the GWC profile change.

The new profiles are not backward compatible with any other profile. Therefore, the new N905 profile must be chosen carefully. Once the N905 GWC is in service on the new profile it cannot be changed without deleting provisioning on the GWC.

250 PTS and PRI trunk types are not supported on the combined profile (250 ISUP trunks are supported). 250 PTS and PRI trunks must be removed before migrating to the combined profile.

The N905 Small Gateway Lines profiles support 25,600 lines WITHOUT IPSEC. With IPSEC turned on 12,800 is the engineered limit. The limit is not enforced in provisioning however.

17.6 Interactions

None.

18: Functional Description (FN): A00008969

18.1 Feature name and Feature ID

Feature A00008969: ATM50 SSI Monitoring, Corrective

18.2 Description

This document defines and describes monitoring the rate of SSI(Signal State Change Interrupt) coming from the ATM ports and raising an alarm if the given threshold exceeded . This feature includes following parts:

- Collect the SSI event count from the all types of ATM ports.
- Decide that SSI alarm condition occurrence.
- Raise SSI alarm.

18.3 Problem Description

While investigating a recent ABI outage it was observed an exteremely high number of ATM50 SSI pegs occurred in the SCO & ITX cards. For this situation, monitor the rate of SSI (Signal State Change) indications from all types of ATM parts and alarm if the rate exceeds a given threshold. This feature will enable the detection of faulty hardware components in the field.

18.4 Adjustments made

Signal Condition Change Interrupts (SSI) are collected every minute for each port of the ATM50 device. Several variables are added to conduct counts and comparisons. If the SSI count is too high, an ATM50 SSI alarm is raised, called Hardware Port Unstable.

19: Functional Description (FN): A00009011

19.1 Feature name and Feature ID

Feature A00009011: Traffic Operator Position System (TOPS) Internet Protocol (IP) Security Enhancements

19.2 Description

This feature allows the customer to increase the security of the IP eXtended Peripheral Modules (IP-XPMs) in their TOPS-IP network. This feature introduces Succession core datafill which allows the customer to configure the following functions on the IP-XPM:

- Simple Network Management Protocol (SNMP): The customer can enable or disable SNMP, define an SNMP community name, and define an SNMP manager.
- Telnet: The customer can enable or disable Telnet.

These changes are discussed in more detail in the following sections.

19.2.1 Background

The implementation of TOPS-IP is based on the IP-XPM. The IP-XPM is a specialized Digital Trunk Controller (DTC) containing Ethernet-enabled SX05DA processor cards as well as 7X07AA Voice over IP (VoIP) gateway cards. The SX05DA and the 7X07AA each contain processor cards which can support various Internet applications including Ping, SNMP, Telnet, and more.

Nortel recommends that TOPS-IP be implemented on a secure network, not the public internet. A secure network contains subnets, firewalls, and routers which block unauthorized attempts to connect to a TOPS-IP node.

Security risks exist even if an IP-XPM resides on a secure network. For example, a malicious user could attempt to alter IP-XPM settings using SNMP. Another risk might be a user logging on to a 7X07AA card while the card is under heavy load. This action might cause the card to crash and calls to be lost.

This feature improves TOPS-IP security in the areas of SNMP and Telnet as described in the next sections.

19.2.2 SNMP

SNMP allows IP hosts to monitor, modify behavior, and receive unsolicited management information from other IP hosts. The monitoring host is termed the SNMP manager and the monitored host is termed the SNMP element. SNMP is described in several RFCs as follows:

- Version 1 (SNMPv1): RFCs 1155, 1157, 1212
- Version 2 (SNMPv2): RFCs 1441-1452, 1901-1910
- Version 3 (SNMPv3): RFCs 2271-2275

This feature proposes adding three new SNMP settings for TOPS-IP. The new SNMP settings are:

- **SNMP community name:** A character string which serves as a password when reading from or writing to an SNMP host.[1] This feature allows datafill of one community name up to 16 characters in length. The community name is used for reading and writing SNMP data. It is also used when the IP-XPM sends traps (unsolicited SNMP information) to an SNMP manager.

  This feature allows the community name to be set to some other value than "public." This increases security since hackers must guess the community name (through repeated attempts) or break into the secure network in order to use a sniffer to detect the SNMP community name.

  Many IP hosts allow configuration of different community names for SNMP reads, writes, and traps. For example, many users might need read access to a device while only a few need write access, so separate read and write names are defined. For TOPS-IP, SNMP support is limited, and it is not anticipated that many users will need access to SX05DAs and 7X07AAs. As a result only one community name can be defined.
- **SNMP manager:** An IP address specifying a remote host which is allowed to initiate SNMP requests to the IP-XPM. The SNMP manager is also called the trap manager, since it is the host to whom traps are reported. Allowing specification of an SNMP manager by IP address increases security, since the IP-XPM will reject SNMP write attempts from unauthorized remote hosts.
- **SNMP enable/disable:** A Y/N parameter indicating whether the IP-XPM supports any incoming SNMP requests, or sends out any traps.

The SX05DA and the 7X07AA support these settings as follows.

19.2.2.1 SNMP settings on SX05DA

The SX05DA supports limited SNMP capabilities, as detailed in "19.8 Appendix A: Supported SNMP objects on IP-XPM (SX05DA)" on page 170. The new SNMP settings apply to the SX05DA as follows.

- **SNMP community name:** The datafilled community name is validated for incoming read and write requests. The name is not sent in trap messages because the SX05DA does not send traps.

[1] In SNMP parlance, a read is a "get" and a write is a "set."

- **SNMP manager:** The SX05DA does not perform originating IP address validation when an SNMP write request is received. So there is no datafill for the SX05DA SNMP manager.
- **SNMP enable/disable:** By setting this parameter to N, the SX05DA will ignore all incoming SNMP requests. This parameter does not affect traps since the SX05DA does not send traps.

The SNMP community name and the SNMP enable/disable parameter are added as new fields in the tuples of existing Table XPMIPMAP. Table XPMIPMAP is used to configure the SX05DA cards on the IP-XPMs. Each tuple represents one IP-XPM. See the Configuration chapter of this document for the new field definitions.

The SNMP settings are datafilled in the Succession core, but the new settings do not take effect until the data is downloaded to the IP-XPM. The craftsperson must perform a LoadPM or Bsy/RTS on each unit to download the SNMP settings.

Dump and restore: Because SNMP is present on deployed IP-XPMs, the new fields are restored as follows when upgrading from an older TOPS Succession core load.

- **SNMP community name:** Restores as “public,” the default SNMP community name. “public” is also the name in use on currently deployed IP-XPMs.
- **SNMP enable/disable:** Restores to Y (SNMP enabled) since SNMP is enabled on currently deployed IP-XPMs.

19.2.2.2 SNMP settings on 7X07AA

The new SNMP settings apply to the 7X07AA as follows. These new settings apply only to TOPS 7X07AAs datafilled in existing Table IPINV (field `GW_TYPE` is set to `TOPS`).

- **SNMP community name:** The datafilled community name is validated for incoming read and write requests. The datafilled community name is also sent in trap messages.
- **SNMP manager:** Currently, up to 4 SNMP managers can be configured on a 7X07AA card. One is obtained via DHCP and up to three more can be configured using PMDEBUG on each card. This feature allows a fifth SNMP manager to be configured in the Succession core. When SNMP write requests arrive, the 7X07AA ensures the originating IP address is present in the allowed SNMP manager list. If not, the 7X07AA rejects the write operation.
- **SNMP enable/disable:** By setting this parameter to N, the 7X07AA will ignore all incoming SNMP requests and will not send any traps.

The new settings are added as individual office parameters in Table OFCENG. Each office parameter applies to all 7X07AAs in the office. See the Configuration chapter of this document for the new office parameter definitions.

The SNMP settings are datafilled in the Succession core, but the new settings do not take effect until the data is downloaded to the 7X07AA. The craftsperson must perform a PMRESET on each 7X07AA to download the SNMP settings.

Default values: These settings are implemented as office parameters which have default values of "public," no manager, and SNMP disabled, respectively.

Dump and restore: Because SNMP is present on deployed 7X07AAs, the new fields are restored as follows when upgrading from an older TOPS Succession core load with TOPS 7X07AAs present in Table IPINV.

- **SNMP community name:** Restores as "public," the default SNMP community name. "public" is also the name in use on currently deployed 7X07AAs.
- **SNMP manager:** Restores as N (no manager) since the 7X07AA currently has other methods of setting SNMP manager IP addresses.
- **SNMP enable/disable:** Restores to Y (SNMP enabled) since SNMP is enabled on currently deployed 7X07AAs. Note this differs from the default value of N.

19.2.3 Telnet (7X07AA only)

Telnet is a standard TCP-based service which allows a user to log on to a remote host and access the command line. Telnet is supported on the 7X07AA but not the SX05DA. Telnet is not recommended on a 7X07AA which is handling calls, since the use of Telnet or the use of CPU-intensive 7X07AA commands within a Telnet session can cause the card to crash, thus producing an outage.

Since Telnet is risky to use on an active 7X07AA, this feature allows Telnet to be disabled. This is done using a new office parameter in Table OFCENG. The parameter defaults to N meaning Telnet is disabled. See the Configuration chapter of this document for the new office parameter definition.

The new setting applies only to 7X07AAs datafilled for TOPS usage in existing Table IPINV (field `GW_TYPE` is set to `TOPS`).

The Telnet setting is datafilled in the Succession core, but the setting does not take effect until the data is downloaded to the 7X07AA. The craftsperson must perform a PMRESET on each 7X07AA to download the Telnet setting.

Dump and restore: Telnet is present and enabled on deployed 7X07AAs. But since it is such a risk, the new office parameter will restore to N (Telnet disabled) even if the TOPS-IP office has 7X07AAs defined in Table IPINV on the dump side. This is because it is likely that craftspersons do not use Telnet on a 7X07AA except for commissioning and debugging, and at other times Telnet presents the opportunity for an authorized craftsperson to cause an outage inadvertently.

19.3 Hardware Requirements or Dependencies

This feature does not introduce any new hardware requirements or dependencies.

19.4 Software Requirements or Dependencies

This feature requires new loads in the IP-XPM and in the NT7X07AA. These loads interpret and act on the SNMP and Telnet configuration data downloaded from the CM. The applicable loads are as follows:

- IP-XPM (SX05DA): QTP22
- 7X07AA: TGWYM004

19.5 Limitations and restrictions

19.5.1 IP-XPM (SX05DA) restrictions

The following existing IP-XPM restrictions are not changed by this feature.

- The SX05DA supports SNMPv1 and SNMPv2c only. The SX05DA does not support SNMPv2 or SNMPv3.
- The SX05DA does not validate the originating IP address of incoming SNMP write requests.
- The SX05DA does not send SNMP traps.
- The SNMP object values are not retained over a restart of the IP-XPM.
- The SX05DA does not support Telnet.

19.5.2 NT7X07AA restrictions

- The new parameters in Table OFCENG only have an effect on 7X07AA cards which are datafilled as TOPS cards in Table IPINV (field `GW_TYPE` is set to `TOPS`).
- The 7X07AA supports SNMPv1 and SNMPv2c only. The 7X07AA does not support SNMPv2 or SNMPv3. Please refer to the TOPS-IP User's Guide for further information concerning support of SNMP on the 7X07AA.

19.6 Interactions

Updated security settings do not take effect until they are downloaded to the SX05DA and 7X07AA using appropriate maintenance methods.

19.7 Glossary

Term	Description
7X07AA	VoIP cards which sit in an IP-XPM and act as a gateway between pulse code modulation (PCM) voice and packetized voice (VoIP)
Bsy	Busy, a maintenance command executed on DMS agents and peripherals
DHCP	Dynamic Host Configuration Protocol, an RFC2131-based method of configuring Internet hosts
DMS	Digital Multiplex System, the central Nortel switching processor
DTC	Digital Trunk Controller, an XPM for digital voice
IP-XPM	Internet Protocol eXtended Peripheral Module, a DTC-based XPM with Ethernet capability which provides the basis for TOPS-IP
LoadPM	Load Peripheral Module, a maintenance command executed on DMS peripherals
PMReset	Peripheral Module Reset, a maintenance command executed on DMS peripherals
RFC	Request For Comments, the standard method of documenting Internet applications
RTS	Return to Service, a maintenance command executed on DMS agents and peripherals
SNMP	Simple Network Management Protocol, described in “19.2.2 SNMP” on page 163
Succession core	An updated name for the DMS reflecting the addition of geographically diverse IP hosts serving a central processor (the core)
SX05DA	The processor card for the IP-XPM. Each unit of the IP-XPM has an SX05DA.
Telnet	A TCP-based tool for logging on to and executing commands on remote hosts
TOPS	Traffic Operator Position System, a system for providing operator services using operators and automation
VoIP	Voice over Internet Protocol, a method of sending voice over a packetized network

Term	Description
XPM	eXtended Peripheral Module, a device with its own processor sitting off the Succession core but providing essential services for the core

19.8 Appendix A: Supported SNMP objects on IP-XPM (SX05DA)

This section describes supported SNMP objects on the SX05DA.[1] The SX05DA supports Management Information Base II (MIB-II) as defined in RFC1213. The SX05DA also supports the User Security (USEC) basic group and USEC statistics from RFC1910 (User-based Security Model for SNMPv2).

The following two tables list SNMP objects supported by the SX05DA. MIB-II objects begin with the designation **iso.org.dod.internet.mgmt.mib-2** (numeric **1.3.6.1.2.1**). SNMPv2 objects begin with the designation **iso.org.dod.internet.snmpv2** (numeric **1.3.6.1.6**).

For definitions of these objects, refer to RFC1213 and RFC1910.

Read-write objects are check-marked in the R/W column. If there is no check mark, the object is read-only.

Restrictions apply as listed in section “19.5.1 IP-XPM (SX05DA) restrictions” on page 167.

Table 2: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
system.sysDescr	1.1		
system.sysObjectID	1.2		
system.sysUpTime	1.3		
system.sysContact	1.4	3	
system.sysName	1.5	3	
system.sysLocation	1.6	3	
system.sysServices	1.7		
interfaces.ifNumber	2.1		

[1]Supported SNMP objects on the 7X07AA are already defined in the TOPS-IP User’s Guide.

Table 2: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
interfaces.ifTable.ifEntry.ifIndex	2.2.1.1		
interfaces.ifTable.ifEntry.ifDescr	2.2.1.2		
interfaces.ifTable.ifEntry.ifType	2.2.1.3		
interfaces.ifTable.ifEntry.ifMtu	2.2.1.4		
interfaces.ifTable.ifEntry.ifSpeed	2.2.1.5		
interfaces.ifTable.ifEntry.ifPhysAddress	2.2.1.6		
interfaces.ifTable.ifEntry.ifAdminStatus	2.2.1.7	3	
interfaces.ifTable.ifEntry.ifOperStatus	2.2.1.8		
interfaces.ifTable.ifEntry.ifLastChange	2.2.1.9		
interfaces.ifTable.ifEntry.ifInOctets	2.2.1.10		
interfaces.ifTable.ifEntry.ifInUcastPkts	2.2.1.11		
interfaces.ifTable.ifEntry.ifInNUcastPkts	2.2.1.12		
interfaces.ifTable.ifEntry.ifInDiscards	2.2.1.13		
interfaces.ifTable.ifEntry.ifInErrors	2.2.1.14		
interfaces.ifTable.ifEntry.ifInUnknownPro-tos	2.2.1.15		
interfaces.ifTable.ifEntry.ifOutOctets	2.2.1.16		
interfaces.ifTable.ifEntry.ifOutUcastPkts	2.2.1.17		
interfaces.ifTable.ifEntry.ifOutNUcastPkts	2.2.1.18		
interfaces.ifTable.ifEntry.ifOutDiscards	2.2.1.19		
interfaces.ifTable.ifEntry.ifOutErrors	2.2.1.20		
interfaces.ifTable.ifEntry.ifOutQLen	2.2.1.21		
interfaces.ifTable.ifEntry.ifSpecific	2.2.1.22		
at.atTable.atEntry.atIfIndex	3.1.1.1	3	
at.atTable.atEntry.atPhysAddress	3.1.1.2	3	

Table 2: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
at.atTable.atEntry.atNetAddress	3.1.1.3	3	
ip.ipForwarding	4.1	3	
ip.ipDefaultTTL	4.2	3	
ip.ipInReceives	4.3		
ip.ipInHdrErrors	4.4		
ip.ipInAddrErrors	4.5		
ip.ipForwDatagrams	4.6		
ip.ipInUnknownProtos	4.7		
ip.ipInDiscards	4.8		Always 0
ip.ipInDelivers	4.9		
ip.ipOutRequests	4.10		
ip.ipOutDiscards	4.11		Always 0
ip.ipOutNoRoutes	4.12		
ip.ipReasmTimeout	4.13		
ip.ipReasmReqds	4.14		
ip.ipReasmOKs	4.15		
ip.ipReasmFails	4.16		
ip.ipFragOKs	4.17		
ip.ipFragFails	4.18		
ip.ipFragCreates	4.19		
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr	4.20.1.1		
ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex	4.20.1.2		
ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask	4.20.1.3		

Table 2: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
ip.ipAddrTable.ipAddrEntry.ipAdEntBcastAddr	4.20.1.4		
ip.ipAddrTable.ipAddrEntry.ipAdEntReasmMaxSize	4.20.1.5		
ip.ipRouteTable.ipRouteEntry.ipRouteDest	4.21.1.1	3	
ip.ipRouteTable.ipRouteEntry.ipRouteIfIndex	4.21.1.2	3	
ip.ipRouteTable.ipRouteEntry.ipRouteMetric1	4.21.1.3	3	
ip.ipRouteTable.ipRouteEntry.ipRouteMetric2	4.21.1.4	3	Not used
ip.ipRouteTable.ipRouteEntry.ipRouteMetric3	4.21.1.5	3	Not used
ip.ipRouteTable.ipRouteEntry.ipRouteMetric4	4.21.1.6	3	Not used
ip.ipRouteTable.ipRouteEntry.ipRouteNextHop	4.21.1.7	3	
ip.ipRouteTable.ipRouteEntry.ipRouteType	4.21.1.8	3	
ip.ipRouteTable.ipRouteEntry.ipRouteProto	4.21.1.9		
ip.ipRouteTable.ipRouteEntry.ipRouteAge	4.21.1.10	3	
ip.ipRouteTable.ipRouteEntry.ipRouteMask	4.21.1.11	3	
ip.ipRouteTable.ipRouteEntry.ipRouteMetric5	4.21.1.12	3	Not used
ip.ipRouteTable.ipRouteEntry.ipRouteInfo	4.21.1.13		
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaIfIndex	4.22.1.1	3	
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaPhysAddress	4.22.1.2	3	

Table 2: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaNetAddress	4.22.1.3	3	
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType	4.22.1.4	3	
ip.ipRoutingDiscards	4.23		Always 0
icmp.icmpInMsgs	5.1		
icmp.icmpInErrors	5.2		
icmp.icmpInDestUnreachs	5.3		
icmp.icmpInTimeExcds	5.4		
icmp.icmpInParmProbs	5.5		
icmp.icmpInSrcQuenchs	5.6		
icmp.icmpInRedirects	5.7		
icmp.icmpInEchos	5.8		
icmp.icmpInEchoReps	5.9		
icmp.icmpInTimestamps	5.10		
icmp.icmpInTimestampReps	5.11		
icmp.icmpInAddrMasks	5.12		
icmp.icmpInAddrMaskReps	5.13		
icmp.icmpOutMsgs	5.14		
icmp.icmpOutErrors	5.15		
icmp.icmpOutDestUnreachs	5.16		
icmp.icmpOutTimeExcds	5.17		
icmp.icmpOutParmProbs	5.18		
icmp.icmpOutSrcQuenchs	5.19		
icmp.icmpOutRedirects	5.20		

Table 2: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
icmp.icmpOutEchos	5.21		
icmp.icmpOutEchoReps	5.22		
icmp.icmpOutTimestamps	5.23		
icmp.icmpOutTimestampReps	5.24		
icmp.icmpOutAddrMasks	5.25		
icmp.icmpOutAddrMaskReps	5.26		
tcp.tcpRtoAlgorithm	6.1		
tcp.tcpRtoMin	6.2		
tcp.tcpRtoMax	6.3		
tcp.tcpMaxConn	6.4		
tcp.tcpActiveOpens	6.5		
tcp.tcpPassiveOpens	6.6		
tcp.tcpAttemptFails	6.7		
tcp.tcpEstabResets	6.8		
tcp.tcpCurrEstab	6.9		
tcp.tcpInSegs	6.10		
tcp.tcpOutSegs	6.11		
tcp.tcpRetransSegs	6.12		
tcp.tcpConnTable.tcpConnEntry.tcp-ConnState	6.13.1.1	3	
tcp.tcpConnTable.tcpConnEntry.tcp-ConnLocalAddress	6.13.1.2		
tcp.tcpConnTable.tcpConnEntry.tcp-ConnLocalPort	6.13.1.3		
tcp.tcpConnTable.tcpConnEntry.tcpCon-nRemAddress	6.13.1.4		

Table 2: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
tcp.tcpConnTable.tcpConnEntry.tcpConnRemPort	6.13.1.5		
tcp.tcpInErrs	6.14		
tcp.tcpOutRsts	6.15		
udp.udpInDatagrams	7.1		
udp.udpNoPorts	7.2		
udp.udpInErrors	7.3		
udp.udpOutDatagrams	7.4		
udp.udpTable.udpEntry.udpLocalAddress	7.5.1.1		
udp.udpTable.udpEntry.udpLocalPort	7.5.1.2		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsIndex	10.7.2.1.1		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsAlignmentErrors	10.7.2.1.2		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsFCSErrors	10.7.2.1.3		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsSingleCollisionFrames	10.7.2.1.4		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsMultipleCollisionFrames	10.7.2.1.5		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsSQETestErrors	10.7.2.1.6		

Table 2: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsDeferredTransmissions	10.7.2.1.7		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsLateCollisions	10.7.2.1.8		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsExcessiveCollisions	10.7.2.1.9		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsInternalMacTransmitErrors	10.7.2.1.10		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsCarrierSenseErrors	10.7.2.1.11		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsFrameTooLongs	10.7.2.1.13		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsInternalMacReceiveErrors	10.7.2.1.16		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsEtherChipSet	10.7.2.1.17		
transmission.rs232.rs232Number	10.33.1		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortIndex	10.33.2.1.1		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortType	10.33.2.1.2		

Table 2: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortInSigNumber	10.33.2.1.3		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortOutSigNumber	10.33.2.1.4		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortInSpeed	10.33.2.1.5		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortOutSpeed	10.33.2.1.6		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortInFlowType	10.33.2.1.7		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortOutFlowType	10.33.2.1.8		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortIndex	10.33.3.1.1		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortBits	10.33.3.1.2		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortStopBits	10.33.3.1.3		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortParity	10.33.3.1.4		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortAutobaud	10.33.3.1.5		

Table 2: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortParityErrs	10.33.3.1.6		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortFramingErrs	10.33.3.1.7		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortOverrunErrs	10.33.3.1.8		
transmission.rs232.rs232InSigTable.rs232InSigEntry.rs232InSigPortIndex	10.33.5.1.1		
transmission.rs232.rs232InSigTable.rs232InSigEntry.rs232InSigName	10.33.5.1.2		
transmission.rs232.rs232InSigTable.rs232InSigEntry.rs232InSigState	10.33.5.1.3		
transmission.rs232.rs232InSigTable.rs232InSigEntry.rs232InSigChanges	10.33.5.1.4		
transmission.rs232.rs232OutSigTable.rs232OutSigEntry.rs232OutSigPortIndex	10.33.6.1.1		
transmission.rs232.rs232OutSigTable.rs232OutSigEntry.rs232OutSigName	10.33.6.1.2		
transmission.rs232.rs232OutSigTable.rs232OutSigEntry.rs232OutSigState	10.33.6.1.3		
transmission.rs232.rs232OutSigTable.rs232OutSigEntry.rs232OutSigChanges	10.33.6.1.4		

Table 2: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
snmp.snmpInPkts	11.1		
snmp.snmpOutPkts	11.2		
snmp.snmpInBadVersions	11.3		
snmp.snmpInBadCommunityNames	11.4		
snmp.snmpInBadCommunityUses	11.5		Always 0
snmp.snmpInASNParseErrs	11.6		
snmp.snmpInTooBigs	11.8		Always 0
snmp.snmpInNoSuchNames	11.9		Always 0
snmp.snmpInBadValues	11.10		Always 0
snmp.snmpInReadOnlys	11.11		
snmp.snmpInGenErrs	11.12		Always 0
snmp.snmpInTotalReqVars	11.13		
snmp.snmpInTotalSetVars	11.14		
snmp.snmpInGetRequests	11.15		
snmp.snmpInGetNexts	11.16		
snmp.snmpInSetRequests	11.17		
snmp.snmpInGetResponses	11.18		Always 0
snmp.snmpInTraps	11.19		Always 0
snmp.snmpOutTooBigs	11.20		
snmp.snmpOutNoSuchNames	11.21		
snmp.snmpOutBadValues	11.22		
snmp.snmpOutGenErrs	11.24		
snmp.snmpOutGetRequests	11.25		Always 0
snmp.snmpOutGetNexts	11.26		Always 0
snmp.snmpOutSetRequests	11.27		Always 0

Table 2: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
snmp.snmpOutGetResponses	11.28		
snmp.snmpOutTraps	11.29		
snmp.snmpEnableAuthenTraps	11.30	3	IP-XPM (SX05DA) does not send traps.

Table 3: SX05DA support of SNMPv2

Object name	Numeric name	R/W	Notes
snmpModules.usecMIB.usecMIBObjects.usecAgent.agentID	3.6.1.1.1		
snmpModules.usecMIB.usecMIBObjects.usecAgent.agentBoots	3.6.1.1.2		
snmpModules.usecMIB.usecMIBObjects.usecAgent.agentTime	3.6.1.1.3		
snmpModules.usecMIB.usecMIBObjects.usecAgent.agentSize	3.6.1.1.4		
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsUnsupportedQos	3.6.1.2.1		
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsNotInWindows	3.6.1.2.2		Always 0
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsUnknownUserNames	3.6.1.2.3		
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsWrongDigestValues	3.6.1.2.4		
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsUnknownContexts	3.6.1.2.5		Always 0

Table 3: SX05DA support of SNMPv2

Object name	Numeric name	R/W	Notes
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsBadParameters	3.6.1.2.6		
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsUnauthorizedOperations	3.6.1.2.7		Always 0

20: Functional Description (FN): A00009012

20.1 Feature name and Feature ID

A00009012 - TOPS OSSAIN Service Enhancements

20.2 Description

This feature addresses a number of items to improve the OSSAIN functionality. It provides the following:

- The ability for an SN function to set the service of the call as it is being transferred or triggered.
- The ability for TOPSOPER and DASERV SN functions to indicate the call being transferred or triggered should be handled as a DA recall to increment the DA recall counter and populate operator messaging as needed.
- The removal of TOPSAUTO option AABS from table OAFUNDEF since AABS was EOL'd in a prior release.
- The support of MCCS for TOPSAUTO options in table OAFUNDEF to replace the default processing left by the AABS option. Since AABS could have still been datafilled, a call could route to AABS but fail since AABS was EOL'd - the call would then be routed to MCCS if available or operator if not.
- The replacement of ping usage in node audits and in the MAPCI command TST. Pings are not supported on certain platforms and are therefore replaced with an OAP message, Node Connectivity Test, as needed.
- The notification of OSSAIN Broadcast Announcements being EOL'd in SN10. The TEOL log will be generated whenever OSSAIN Broadcast Announcements are used.

Each of these areas is described in one of the following sections:

— SN Service for Transfers/Triggers

— DA Recall Support for OSSAIN

— AABS removal; MCCS support for OSSAIN functions

— OSSAIN Ping Replacement

— EOLing of OSSAIN Broadcast Announcements

— SOC and Table TOPSFTR for activation

20.2.1 SN Service for Transfers/Triggers

This portion of the feature enhances OSSAIN by allowing datafill to indicate what the service of the SN function should be for transfers and triggers.

20.2.1.1 Background

When an SN was allowed to offer DA service assistance, it was initially only designed to act like an ADAS/ADAS+ replacement to collect the city/name recording and perform the playback to an operator. The initial design did not anticipate a DA SN being able to fully automate a DA call nor provide service for DA recalls or transfers. Therefore, the switch assumes a DA call going from an operator to an SN must be going for call completion and switches the service to TA (along with cutting an AMA, changing the call origination, and resetting some billing parameters).

20.2.1.2 Enhancements

This feature provides datafill to override the switch assumptions in changing from DA to TA for operator to SN transfers. (If the service is not changed from DA to TA then the call origination will not change.) It also generalizes the ability of setting the proper service for an SN function to all transfers and triggers.

Table OAFUNDEF is enhanced to include two new options, one for the SN service and the other for generating AMA.

- The new SN service indicator datafill will be used for all transitions to an SN but not for initial call presentation. The scenarios include:
  - — Transfers from operator to SN
  - — Transfers from DAS to SN
  - — Transfers from SN to SN
  - — Triggers to SN
  - — Disposition Routing resulting in route to SN

20.2.1.3 Table OAFUNDEF: New Field USESERV

Note: The following illustrates the new look of table OAFUNDEF with this feature; however, each section will bold the new area it is discussing.

A new field, USESERV is added to table OAFUNDEF for calls transitioned to SN functions . When set to Y it indicates the service defined in ORIGSERV should be used for a call in transition (transfer, trigger, disposition routing).

Table 1 New Table OAFUNDEF

FUNCID	FUNCNAME	FUNCAREA
1	DA_SN	SN DASERV Y **N** N N N N Y CQ17 N
2	DA_TOPSOPER	TOPSOPER N OSSAIN_TO_DA_OPR N
3	TA_AUTO	TOPSAUTO MCCS 0_PLUS
4	TA_SN	SN TASERV **N** N N N Y Y CQ0 N
5	DA_SN_RCL	SN DASERV Y **Y** N N N N Y CQ17 N
6	DA_TOPSOPER_RCL	TOPSOPER Y OSSAIN_TO_DA_OPR N
7	TA_AUTO_RCL	TOPSAUTO MCCS 0_PLUS
8	TA_SN_RCL	SN TASERV **Y** N N N Y Y CQ0 N

- For a call in transition (transfer, trigger, disposition routing) to an SN function, the following processing occurs for the new field USESERV:if set to N, then existing functionality is maintained which means the service is maintained or switched DA to TA for operator to SN transfers
- if set to Y and the ORIGSERV is the same as the current service, then no changes are made to the call
- if set to Y and the ORIGSERV is different than the current service, then the service is changed and associated parameters reset as required with all service changes as noted in the OAP spec for service switches

Note: Whenever the OAFUNDEF option USESERV switches services, the same side effects occur as when an OAP Service Change Request is processed. Consult to OAP Specifications Document for details.

20.2.2 DA Recall Support for OSSAIN

This feature provides a datafillable means for OSSAIN to recognize a DA recall for calls which do not use the switch-based ARU structure for listing announcements. It will increment the DA recall counter and populate operator messaging as needed.

20.2.2.1 Background

A DA SN can offer listings via back-end announcements without using switch-based ARUs. The subscriber can initiate a recall from the announcement for an incorrect listing or for another listing. Transfers or triggers can be used to service the recall via an OSSAIN function. However, there is no mechanism provided for the SN or function to indicate this service is a recall service to mark recall counters to compare to switch limits as defined in table VROPT: maximum_da_recalls. Thus, if a call was serviced by an SN and then recalls to a TOPS operator, the call can exceed the maximum number of recalls defined in VROPT.

The vropt:maximum_da_recalls parameter was initially developed to limit the number of times a call can recall back to an operator to limit operator work time on one call. This parameter is not intended to track the number of listings. The maximum number of requested listings is datafillable in DATRKOPT field MULTREQ.

20.2.2.2 Enhancement

This feature provides datafill to note a DA recall via OSSAIN function to align SN and operator recall counts. It allows a method to count DA recalls processed by an operator and by an SN.

When the OSSAIN function is datafilled as a DA recall function, the DA recall counter is incremented and the OPP field, reason_for_operator, set to recall for proper processing at the position if the call routes to an operator.

The feature will also check if the maximum number of DA recalls has been reached prior to allowing the transition to the function. If the maximum DA recall limit has been reached and the call attempts to go to a DA recall function, then the call will be routed to treatment using the default_treatment of table OAINPARM, which is also used when the maximum number of transitions has been reached.

20.2.2.3 Table OAFUNDEF: New Field DARECALL

Note: The following illustrates the new look of table OAFUNDEF with this feature; however, each section will bold the new area it is discussing.

New field DARECALL is added in table OAFUNDEF to both TOPSOPER and DASERV SN functions. When set to Y, the count for DA recalls is incremented and, if going to an operator, the OPP field reason_for_operator is populated as recall.

Table 2 New Table OAFUNDEF

FUNCID	FUNCNAME	FUNCAREA
1	DA_SN	SN DASERV **Y** N N N N N Y CQ17 N
2	DA_TOPSOPER	TOPSOPER **N** OSSAIN_TO_DA_OPR N
3	TA_AUTO	TOPSAUTO MCCS 0_PLUS
4	TA_SN	SN TASERV N N N N Y Y CQ0 N
5	DA_SN_RCL	SN DASERV **Y** Y N N N N Y CQ17 N
6	DA_TOPSOPER_RCL	TOPSOPER **Y** OSSAIN_TO_DA_OPR N
7	TA_AUTO_RCL	TOPSAUTO MCCS 0_PLUS
8	TA_SN_RCL	SN TASERV Y N N N Y Y CQ0 N

Note: OAFUNDEF field DARECALL only applies to functions used in transfers and triggers. It is ignored for original services.

20.2.3 MCCS Support for OSSAIN Functions

This feature removes the AABS TOPSAUTO option from table OAFUNDEF datafill and adds the MCCS TOPSAUTO option.

Although AABS has been EOL'd, it was still possible for a call to route to the TOPSAUTO AABS datafill, fail AABS and then try to go to MCCS. Therefore, OSSAIN calls could route to MCCS in this manner. If the call was not eligible for MCCS then it was routed to an operator.

This feature maintains the existing functionality. Therefore, over an ONP, AABS will be replaced with MCCS and the call will route to MCCS instead of failing AABS first.

20.2.4 OSSAIN Ping Replacement

OSSAIN needs to replace ping (ICMP echo) functionality due to the following reasons:

— For security reasons, some customers may not allow ping in their Succession networks.

— Ping is not supported on some SOS platforms on which TOPS may be supported in the future.

SN07 activity A00005160 introduced the OAP Node Connectivity Test operation. The purpose of this operation is to verify application-layer connectivity between the switch and a service node. In SN07 and higher, OAP Node Connectivity Test messaging replaces ping in an OSAC remote in the RTS sequence for an OSN, if the OSN is at OAP 9 or higher and the OSAC host is at SN07 or higher.

This feature addresses the remaining situations in which OSSAIN has historically used pings - in audits and in the TST MAPCI command.

20.2.4.1 OSSAIN Audits

If an OSAC remote has not received a message from an in-service OSN for a datafilled time interval, it audits the OSN. Historically this audit has consisted of first a ping to the OSN and then, if a response is received, a Node Datafill Check Request to OSAC host. If the remote times out waiting for the ping reply, it retries a datafilled number of times.

With this feature, an OSAC remote at SN09 or higher uses the OAP Node Connectivity Test for the audit, rather than using ping, if the OSAC host is at SN07 or higher and the OSN is at OAP 9 or higher. Audit retries and time-outs are unchanged.

20.2.4.2 MAPCI TST Command

The `TST` command is available with an OSNM, OSN, or OSAC node posted at the MAP. A node must be ManB to be tested. The `TST` command has two variations which, prior to this feature, used pings - `TST` with no parameters and `TST` with the optional `PING` parameter.

- If `TST PING` is entered, the switch sends a ping request to the posted node and reports success on receipt of a valid reply. If it can't send the request or doesn't get a valid reply, it reports failure. This feature adds a new failure response, "Use TST without PING," which is displayed if the MAP user enters `TST PING` on a platform that does not support ping.

- If TST is entered with no parameters, the functionality prior to this feature depended on the kind of node being tested:
  - — OSNM - First did a ping test on the OSNM. Then if that succeeded, sent a Node Test Request to the OSNM.
  - — OSAC - First did a ping test on the OSAC node. Then if that succeeded, sent an OSAC Node Test Request to the OSAC node.
  - — OSN - First did a ping test on the OSN. Then if that succeeded, sent an OSN Node Datafill Check Request to the OSAC host.

  Notice that for OSNM and OSAC, the ping test was immediately followed by an OAP or OSAC message to the same node. The subsequent message also verifies connectivity. Therefore, this feature eliminates the redundant ping in the test sequence for OSNM and OSAC nodes.

  For OSN, the ping could not simply be removed from the test sequence because it is not followed by another message to the OSN. Therefore, for OSN nodes this feature substitutes a Node Connectivity Test request for the ping. This substitution occurs only if the OSAC remote is at SN09 or higher, the OSAC host is at SN07 or higher, and the OSN is at OAP 9 or higher.

20.2.5 EOLing of OSSAIN Broadcast Announcements

OSSAIN broadcast announcements will be EOL'd in SN10. A TEOL log will be generated in SN09 whenever OSSAIN Broadcast Announcements are used to indicate the functionality will be removed in SN10. The TEOL log will also be patched back to two prior releases.

20.2.6 SOC and Table TOPSFTR

A new entry in table TOPSFTR will control this feature's activation which will be tied to existing SOC option, OSAN0102: OSSAIN Enhancements. This new TOPSFTR entry will be called OSSAIN_RELEASE_22 to align with prior OSSAIN features.

The new entry will activate the call processing of the following portions of this feature (note datafill will be allowed regardless of this parameter):

- Transfer to SN function service
- DA Recall function

Table 3 Table TOPSFTR

FTRNAME	FTRENABL
OSSAIN_RELEASE_22	Y

20.3 Hardware Requirements or Dependencies

No new hardware requirements or dependencies.

20.4 Software Requirements or Dependencies

No special software requirements or dependencies.

Note: The OAP version is not increased by this feature since this feature does not change OAP.

20.5 Limitations and restrictions

- Although the DARECALL option in table OAFUNDEF could have been generalized to include TA recalls, TA recalls would apply to coin calls and since OSSAIN does not support coin at this time, this feature only supports DA recalls.
- Whenever the OAFUNDEF option USESERV switches services, the same side effects occur as when an OAP Service Change Request is processed. Consult to OAP Specifications Document for details.

20.6 Interactions

None

20.7 Glossary

No new terms are introduced with this feature.

21: Functional Description (FN): A00009013

21.1 Feature name and Feature ID

A00009013, TOPS announcements via UAS/AMS

21.2 Description

This activity provides the ability for Traffic Office Position System (TOPS) calls to use packet-based announcements. The functionality is available on Communication Server 2000 (CS 2000) with TOPS, in Succession hybrid offices with ENET and IP-based Succession solutions.

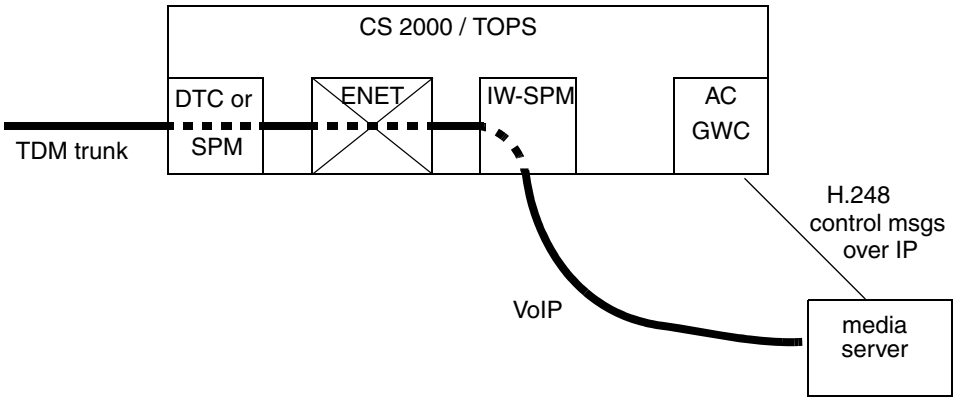
The packet announcement platforms that Nortel supports in SN09 for CS 2000 are the Media Server 2000 (MS 2000) Series and the older Universal Audio Server (UAS). The UAS is no longer sold, but this feature will work with it as long as Nortel supports it. The MS 2000 Series model used with IP bearer networks is the MS 2010.

In the Succession architecture, MS 2000 Series and UAS are special-purpose media gateways referred to as media servers. Each media server is controlled by a Gateway Controller (GWC) that is configured with the Audio Controller profile. An Audio Controller GWC can control multiple media servers, with the restriction that the same set of announcements must be provisioned on all the media servers that are controlled by the same GWC. The protocol between the GWC and the media server is H.248.

The operating company provides the voice recordings for packet-based announcements. Your Nortel or AudioCodes representative can refer you to professionals who provide this service. The web-based Audio Provisioning Server (APS) is used to provision the recordings on the media servers. Then CM datafill is entered in table ANNAUDID to associate the announcement phrase names known in the CM with the segment identifiers that were provisioned on the media servers. Other CM announcement tables are datafilled similarly for packet announcements as for legacy announcements.

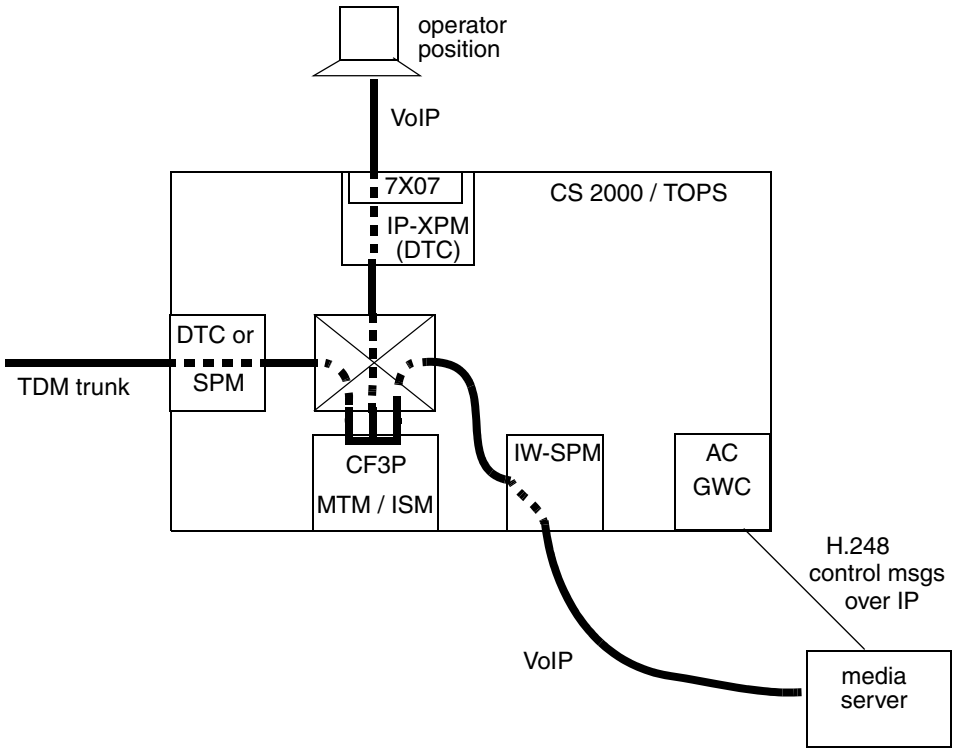
This activity does not change the restriction that calls can only enter the TOPS environment on legacy TDM trunks, and can only use legacy TDM conference resources. Therefore, an interworking bridge on an Interworking Spectrum Peripheral Module (IW SPM IP) is required for each TOPS call that connects to a packet announcement. The following figures show example topologies. The first example shows a TOPS call that has only the calling party connected to a packet-based announcement.

Figure 1 Legacy trunk connected to packet announcement



The next example shows a TOPS call that has an operator, a calling party, and a packet-based announcement.

Figure 2 Legacy conference connected to packet announcement



In both examples, the TDM trunk is any legacy PTS or ISUP trunk type that could originate calls to TOPS prior to this feature. It could be a looparound trunk, or it could connect to another office.

An announcement can have both legacy DRAM/EDRAM and packet members. If both legacy and packet members are available when a TOPS call needs an announcement, the CS 2000 automatically attempts to select a member whose network fabric matches that of the other agents on the call. Since all other agents on a TOPS call are connected to the ENET in SN09, this implies that legacy announcement members are always selected for TOPS calls if a legacy member is available. However, if only packet members are available, and if an interworking bridge is available, then a TOPS call will use a packet member and will automatically connect to it using the interworking bridge.

This activity supports TOPS use of packet announcements for the following functionalities:

- Branding
- Treatment
- Direct route to announcement via standard translations and routing
- Announcement segments of audio program for the Music and Announcement in Queue feature
- Automatic Coin Toll Service (ACTS)

  ACTS announcements are also used for the TOPS Time and Charges, Non-coin Notify, and ACTS Coin Tone Generation Test features. Those features can also use packet-based announcements.
- Mechanized Calling Card Service (MCCS)

  MCCS announcements are also used for the TOPS Sequence Calling, Account Code Billing, and Authorization Code features. Those features can also use packet-based announcements.

The functionality provided by this feature is automatically activated when packet members are brought into service for announcement groups that are used by TOPS calls.

This feature does not change the functionality of TOPS calls that use legacy DRAM/EDRAM announcements.

21.3 Hardware Requirements or Dependencies

This activity does not introduce new hardware. It uses hardware that is standard for CS 2000 IP hybrid with packet-based announcements.

21.4 Software Requirements or Dependencies

This functionality is first available in SN09. The software is also present in ISN09, but Nortel has tested it only with the North American load.

21.5 Limitations and restrictions

This activity does not add support for TOPS calls to connect directly with any kind of Succession agent other than announcements. Packet calls destined for TOPS in a CS 2000 must still arrive in the TOPS environment on legacy TDM trunks, using looparound facilities if needed to accomplish that.

This activity does not support packet-based announcements for TOPS custom announcement types TOPSVR and MDS. (TOPSVR is used for DRAM-based directory assistance and intercept announcements. MDS is used for the TOPS Message Delivery Service feature, also known as Audiogram Delivery Service. Note that most MDS functionality disappeared with end of life of the VSN.)

This activity does not support use of packet-based media servers for music segments of audio programs used by the Music and Announcement in Queue feature.

When packet-based announcements are used for MCCS and ACTS, the media server does not collect the DTMF or coin signals. Collection is still done by an MCCS or ACTS receiver card in an MTM/ISM.

An interworking bridge is required in SN09 for each TOPS connection to a packet-based announcement.

The functionality provided by this feature will not be supported in international (ISN) loads until it has been verified. At this time of this publication, Nortel planned to verify it only for North America.

The functionality provided by this feature will not be supported in ATM-based hybrid solutions until it has been verified. At this time of this publication, Nortel planned to verify it only with an IP network fabric.

This activity is subject to all of the limitations and restrictions that apply in general to CS 2000 use of packetized announcements. This includes the capacity limitations of media servers and Audio Controller GWCs. Some of the other important restrictions that this activity inherits from CS 2000 in SN09 are:

- Use of packet-based announcements is not supported if the CS 2000 connects two or more packet bearer networks. Note that a Trimodal CS 2000 connects two packet bearer networks, so packet announcements cannot be used on a Trimodal CS 2000. The restriction applies regardless of whether the two packet bearer networks have the same or different network fabrics.

- All of the media servers controlled by the same GWC must be provisioned with the same set of audio segments. Failure to follow this provisioning rule will result in call failures.

Please see the following section for additional interactions that could be viewed as limitations.

21.6 Interactions

The end user of a TOPS feature that uses announcements should detect virtually no difference in how the feature operates when packet-based announcements are used rather than legacy DRAM announcements. The one exception is that the media server may use different wording for certain variable phrases in custom announcements. The logic for the wording is in the media server, not in the switch. Specifically, when a time duration for ACTS is an even number of minutes, the switch instructs the DRAM to speak only "<x> minutes," but a packet media server may have logic to say "<x> minutes and zero seconds."

The MAXCYC field in CM table ANNS specifies the maximum number of times an announcement should repeat if the listening agent does nothing to terminate the connection. TOPS software has historically ignored the MAXCYC datafill for announcements played while a call is at an operator position or an OSSAIN service node. So, for example, if an operator requests to outpulse to a number and gets a treatment announcement, the announcement has historically continued to repeat itself until the operator keyed to release it. If the announcement member is a packet one, and if the operator does not key to release it before it has played the datafilled number of cycles, the announcement stops playing and the operator should key to release it at that time. The same is true for a packet announcement that is played to a call under control of an OSSAIN service node.

There are no interactions with the criteria by which an announcement is selected for a TOPS call. For example, the branding announcement CLLI for a TOPS call is selected based on criteria that may include the carrier or NBEC, the Service Provider ID (SPID), and datafill in several TOPS tables. All of this occurs before the announcement member is selected, and it happens independently of the network fabric of the member that will be selected.

21.7 Glossary

This activity does not introduce any non-standard terms or acronyms.

22: Functional Description (FN) A00009026

22.1 Feature name and Feature ID

RMGC Security.

Feature ID: A00009026

22.2 Description

The RMGC Security feature for the SN09 release will enable secure communications between the RMGC (or RMGC/Audio Controller) and the Multimedia Terminal Adapter (MTA).

Background

Small line gateways need to be provisioned with the address of their call processing (CallP) gateway controller (GWC) before they can provide service. Without an RMGC this must be done manually either in a configuration file downloaded to the gateway or directly on the gateway itself. This manual provisioning is difficult to manage and time consuming.

The RMGC serves as a registration agent that provides the gateways with a single location to obtain the fully qualified domain name (FQDN) (e.g., cms/gwc-08.iplab.gwsite-3.ny.net) of their associated CallP GWC. This simplifies the gateway provisioning. All gateways are provided with the RMGC FQDN. Each gateway will contact the RMGC before coming into service and the RMGC will redirect them to their controlling GWC.

Security

Many network deployments require the confidentiality, integrity, and authentication that is provided by Kerberos and IPSec services. When a Call Server 2000 (CS2K) network is deployed with security enabled, the components must all be secured. Prior to SN09 the RMGC (and Audio Controller (AC)/RMGC) combination were not secured.

In order to deploy an RMGC (or AC/RMGC) into a secure network it must be able to respond to requests from the MTA for secure associations (SAs). The method of establishing a SA is to use Kerberos for key management and Internet Protocol Security (IPSec) for secure connections.

The interaction between the MTA and the RMGC is straight-forward. Before coming into service the MTA will send an RSIP message to the RMGC. This RSIP message will initiate a SA negotiation with the RMGC. Kerberos will be used to negotiate an IPSec SA over which the RSIP is sent. The RMGC will respond with an RSIP redirect (over the SA) that contains the FQDN of it's associated CallP GWC. After this exchange the RMGC and MTA have no interaction until the next time that the MTA restarts.

Main Feature Items

The items that are addressed by this feature are:

- IPSec SA Management: The SAs that are used for the RSIP exchange between the RMGC and the MTA must have a short lifetime and must not be renewed. There are a large number of MTAs (maximum of 115,000) and the RMGC cannot maintain an SA database of that size.

- Memory Recovery: Even with the short lived SAs and no SA renewal enabled by this feature there is still a need to economize the memory usage since the high water mark for the SA storage is higher than that supported by the small lines profile.

- MTA Recovery: In order to maintain quick recovery times for the MTAs the CallP GWC must be modified slightly. In the case of a large restart event (like a power failure) the CallP GWC and restarting MTA must be able to re-establish contact without waiting for service from the RMGC, when possible.
The RMGC is modified to support multiple pools of SAs specifically to support the AC/RMGC combination profile. This ensures that the AC is able to setup secure connections when the RMGC is under heavy load.

To Provision an RMGC

The provisioning of the RMGC is very similar to that of a CallP GWC in that Kerberos and Connection Policies must be created. The only change is when a connection policy is created there is a limitation for the IPSec SA lifetime. This value must be between an upper and lower limit (10 seconds to 20 seconds). Any other value will not be accepted, the user will only be successful with the provisioning when this rule is conformed to.

22.3 Hardware Requirements or Dependencies

This feature can be deployed on the CEM-750 based GWC card in the SAM21 shelf.

This feature will function correctly on the CEM-905 GWC card as well. This configuration has not been tested but no issues are anticipated.

22.4 Software Requirements or Dependencies

This feature can be deployed in a dedicated (RMGC only) or combination (RMGC and Audio Controller) profile.

22.5 Limitations and restrictions

The user may only provision Kerberos-managed connection policies with a strict limit on the IPSec SA lifetime. If the user tries to create a connection policy with IPSec SA lifetimes that are outside of the range the connection policy will not be created and the user will be instructed to enter an acceptable lifetime.

22.6 Interactions

The behavior of the SA between the CallP GWC and it's associated MTAs will be different as a result of this feature. In a power failure or restart scenario the SA will be deleted from the CallP GWC in order to accelerate the recovery process. The user may detect this behavior if the number of SAs is being observed regularly.

22.7 Glossary

ACK	Acknowledgement
CallP	Call Processing
CS2K	Call Server 2000 (packet switching fabric)
DID	Design Intent Document
DSUM	Design Summary Document
FQDN	Fully Qualified Domain Name
GW	Gateway
GWC	Gateway Controller
IPSec	Internet Protocol Security
KDC	Key Distribution Center
KMP	Key Management Protocol
KRB	Kerberos
MTA	Multimedia Terminal Adapter
RMGC	Redirecting Media Gateway Controller
RSIP	Restart In Progress (NCS protocol message)
SA	Secure Association
DNS	Domain Name Server
ESP	Encryption Security Payload
SADB	Security Association Database

23: Functional Description (FN) A00009027

23.1 Feature name and Feature ID

Global Network Product Support Trace Tool Enhancements

23.2 Description

Currently, GNPS and customer ability to trace protocol expression in a robust, complete manner within the GWC is limited to a handful of protocol, and is inconsistent. In addition, some new protocols (SIP and H.323) lack the ability to do an onboard trace which is not to screen.

To address this, the existing TAPITRACE tool will be enhanced to include the SIP and H.323 protocols and allow for better filtering and redirection of output. In addition, it will be better integrated with the SIP-Trunking tracing feature to better restrict per call captures (per feature A00003698: Razor Gateway requirement for Trunking).

An additional CALLTRAK SELECT will be introduced to allow inclusion of the calling and/or called DN. Currently, the SELECT command only supports DPT + CLLI (for SIP-T) or DPT + CLLI + CICs (for non SIP-T), which restricts tracing to the given DPT trunk.

After the intended changes are made, the SELECT command will allow selection per digits, given that these are the digits AFTER translations have occurred within the core:

SELECT DPT SIPT CGN <cgn_digits>
SELECT DPT SIPT CDN <cdn_digits>
SELECT DPT SIPT CGN <cgn_digits> CDN <cdn_digits>

It will also modify the existing option for enabling tracing within calltrak to allow tapitrace to be include in the capture as well. The old format:

TRMTRACE

will be changed:

GWCTRACE

and allow an optional parm to enable/disable tapitrace inclusion:

GWCTRACE TRACEOPTS on

Within the GWC, the TAPITRACE PMDEBUG level will add commands to filter based on protocol messaging contents and redirect messaging to the screen or an offboard trace tool without affecting call processing. These commands will be documented within the PMDEBUG command and will be consistent with existing interface.

23.3 Hardware Requirements or Dependencies

None.

23.4 Software Requirements or Dependencies

None.

23.5 Limitations and restrictions

The additional trace functionality above needs to have SIP routed through a NGSS for full traceability of SIP messaging.

23.6 Interactions

Interacts with the changes made to CALLTRAK by A00003698: Razor Gateway requirement for Trunking.

23.7 Glossary

Term	Description
SIP	Session Initiation Protocol
SIP-T	Session Initiation Protocol - Trunking
NGSS	Next Generation Session Server

24: Functional Description (FN): A00009028

24.1 Feature name and Feature ID

A00009028 - CS2K MSM SIP Lines OAM Support

24.2 Description

This feature deals with meeting the OAM requirements on CS2K MSM for support of SIP Lines in release MCP 9.0. It is primarily concerned with the configuration of data corresponding to links to the CS2K and the maintenance on those links. All configuration will be done via the CS2K MSM Management Console; no flow through configuration is supported in this release. Once the link configuration is established the CS2K MSM components are responsible for initiating communication. Additionally, this feature provides for monitoring the registration state of SIP endpoints (CS2K MSM subscribers provisioned with a SIP Lines enabled service package) and performing a line test on the endpoint. This functionality will be accessible from the Management Console. Finally, Accounting will be disabled for the SIP Lines deliverable.

These requirements fall into the following work areas.

Non-Call Associated Signalling (NCAS) link for Querying SIP (QSIP)

Gateway Controller (GWC) link for Gateway Control Protocol (GCP)

Endpoint Maintenance

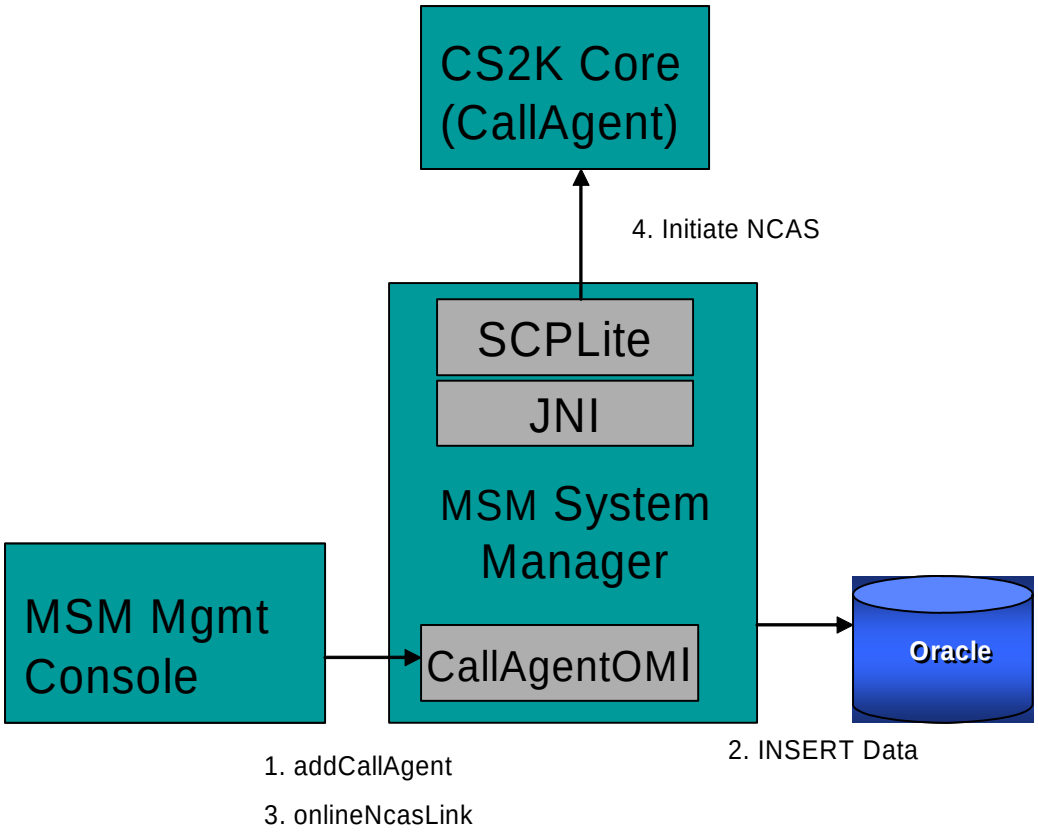
Disabling Accounting

24.3 NCAS Link for QSIP

This link will run between the CS2K MSM System Manager and the CS2K Core. Configuration of the link is provided via CallAgentData which contains a name (for database key purposes), an IP Address, and a port. Maintenance on this link will consist of setting a desired state to ONLINE or OFFLINE. The default state when the CallAgent data is added will be OFFLINE, requiring a manual maintenance action by the craftsperson at the Management Console to bring the link ONLINE. (See steps 1 and 3 in the diagram below.) In addition

to the desired state, the operational state of the link (CONNECTED or DISCONNECTED) will be reported at the Management Console.

Note: Screenshots of the Management Console will be made available in the Configuration section of this Design Document.



The OMI methods for configuring the CallAgentData are supported by the OMI service located at http://<sysMgrHost>:12121/axis/services/callagent as follows:

public void RuntimeResult addCallAgent(data CallAgentData)

public void RuntimeResult updateCallAgent(data CallAgentData)

public void RuntimeResult deleteCallAgent(key CallAgentNaturalKey)

public CallAgentData getCallAgent()

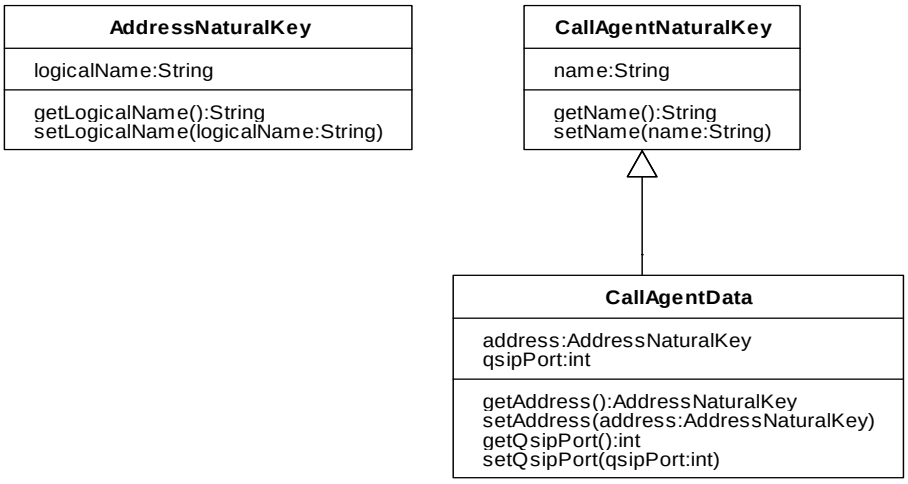


Table 1: CallAgent fields

Field Name	Description
AddressNaturalKey.logicalName	1-16 characters no spaces
CallAgentNaturalKey.name	1-32 characters [Aa-Zz][0-9][-.]
CallAgentData.qsipPort	Integer in the range 4900-4982

The local end of the NCAS link is defined at an offset of 25 from the base port of the System Manager. The address used will be the System Manager's Service Address, if configured, and if not, the Interface One address of the Server on which the System Manager resides.

Maintenance on the NCAS link is provided at the Management Console under the System Manager. The state of the link (CONNECTED, DISCONNECTED) is displayed. The actions to ONLINE or OFFLINE the link will be offered. Note that when the System Manager starts up, it will read the current desired state from the database to determine whether to initiate communication.

The OMI service is located at http://<sysMgrHost>:12121/axis/services/ncasmtc. The methods are are as follows:

public long startNcasLinkMonitor()

public RuntimeResult stopNcasLinkMonitor(long tid)

public NCASLinkStateData getNcasLinkNextState(long tid)

public String[] getNcasLinkAdminStates()

public String[] getNcasLinkOperationalStates()

public RuntimeResult rtsNcasLink()

public RuntimeResult offlineNcasLink()

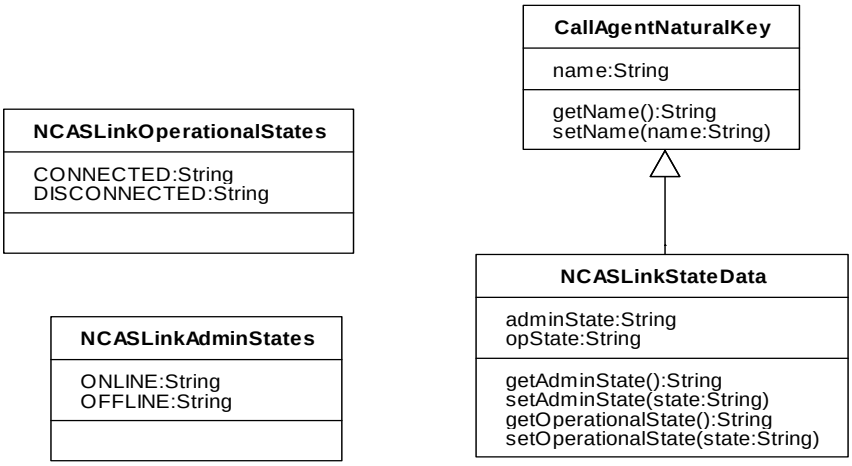


Table 2: NCAS Link State Data

Field	Description
adminState	String. Must be one of the values available from getNCASLinkAdminStates()
opState	String. Must be one of the values availabe from getNCASLinkOperationalStates()

Table 3: NCAS Link Operational States

Operational States
CONNECTED
DISCONNECTED

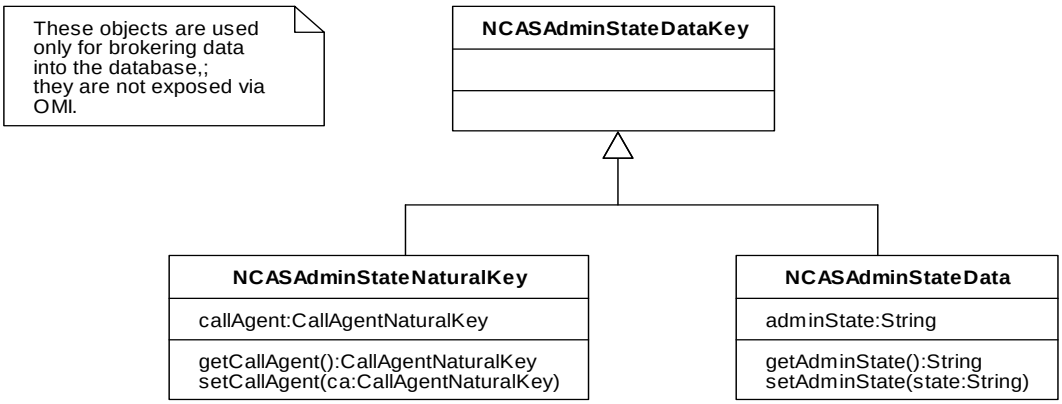
Table 4: NCAS Link Administrative States

Administrative States
ONLINE
OFFLINE

To support the additional data in the Oracle database, two new tables are added. The first contains the configuration data: CS2K_CALL_AGENT consists of three fields, NAME, ADDR and QSIP_PORT. NAME is a 32 character VARCHAR field, restricted to alphanumeric characters. ADDR is a reference to an Object Identification (OID) from the IP_ADDRESS table. QSIP_PORT is an integer field, restricted to the range 4900 and 4982.

> ***Note:*** All CS2K MSM configuration tables contain an implicit OID column created by the data access framework. This column will not be explicitly named for each table, but will be assumed to be present for foreign key use.

The second stores the administrative state: CS2K_CALL_AGENT_ADMIN_STATE consists of two fields. CALL_AGENT is a contextual foreign key into CS2K_CALL_AGENT. ADMIN_STATE is a 16 character VARCHAR, to contain “ONLINE” or “OFFLINE”.

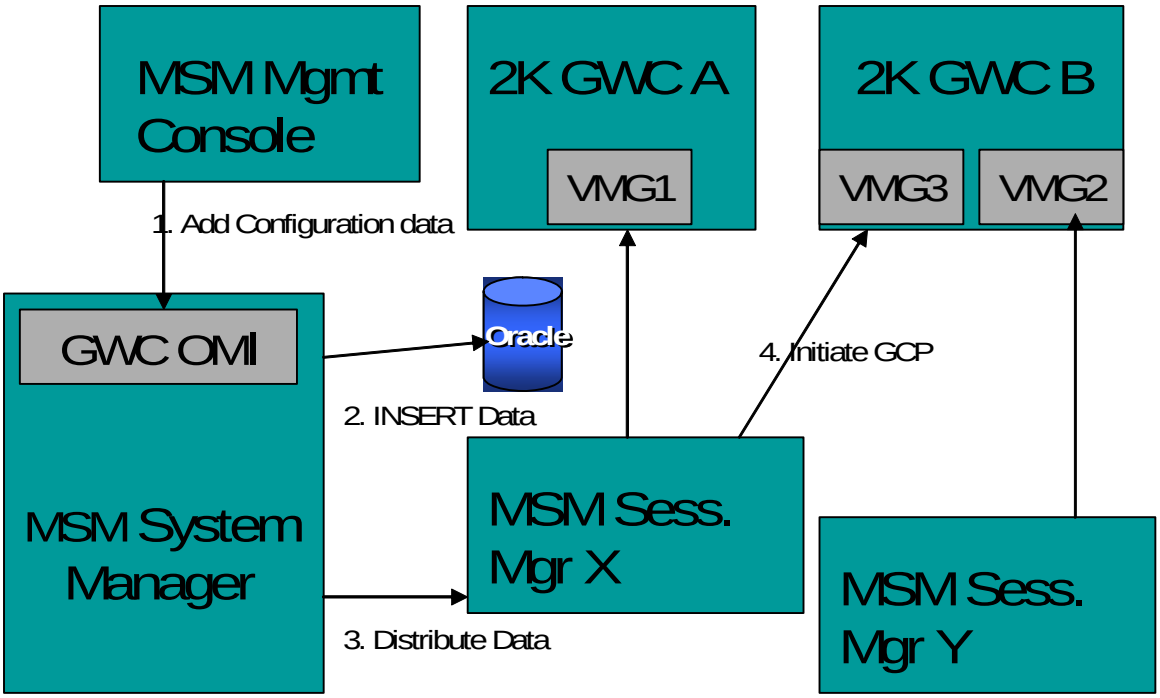


In addition to the configuration and maintenance of the link, enhancements to the Event Distribution framework allow the QSIP coming into the System Manager over NCAS to be answered by request to the active instance of the responding CS2K MSM Network Element (NE). A boolean indicating that only the active instance of an NE is to receive the request is added to the internal event, and is used by the Event Distribution system to determine destination.

24.4 GWC Configuration and Maintenance

A call processing link shipping Gateway Controller Protocol (GCP) over UDP exists between the CS2K MSM Session Manager and the CS2K Gateway Controller (GWC). It's configuration is somewhat more complex than that of the NCAS link, because the relationship between Session Manager and GWC may not be one to one, and further, the relationship is viewed from the GWC side through a Virtual Media Gateway (VMG), which is required for Subscriber provisioning (discussed in detail in A00009043 - SIP Lines Provisioning Support).

The diagram below describes an example of how GWCs and Session Managers might be associated via VMGs. The diagram depicts a configuration given GWCs A and B and Session Managers X and Y. Session Manager X appears as VMG1, tied to GWC A and Session Manager Y appears as VMG2, tied to GWC B. The flow shows the association of VMG3 with Session Manager X. When the association is made, Session Manager X initiates a GCP message to GWC B.



The GWC data is Network Level data shared across all Network Elements. VMG appearances are specific to the Session Manager, and appear only on the appropriate Session Manager. The GatewayControllerData is configured through the OMI service located at http://<sysMgrHost>:12121/axis/services/gwcconfig. The signatures of the OMI methods are as follows:

public void RuntimeResult addGatewayController(data GatewayControllerData)

public void RuntimeResult updateGatewayController(data GatewayControllerData)

public void RuntimeResult deleteGatewayController(key GatewayControllerNaturalKey)

public GatewayControllerData[] getGatwayControllers()

public GatewayControllerNaturalKey[] getGatewayControllerNaturalKeys()

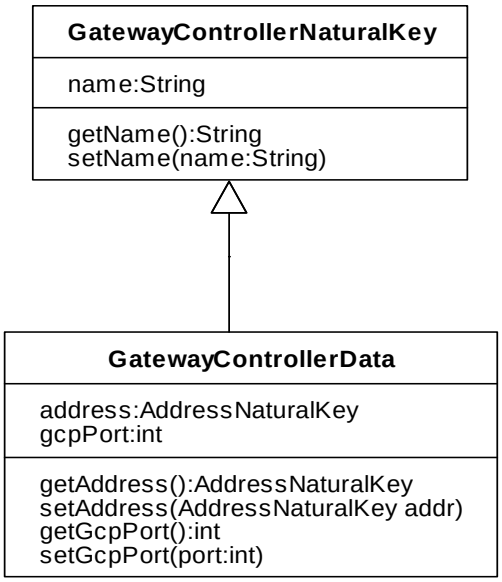


Table 5: Gateway Controller Data

Field	Description
name	Of the form gwc-### where ### may be any integer in the range 0-255, and the characters “gwc-” are fixed
gcpPort	Integer in the range 0-65534

For configuring the VMG the service at http://<sysMgrHost>:12121/axis/services/vmgconfig contains the following methods:

pubic void RuntimeResult addVmgAppearance(ctxt SessMgrNaturalKey, data VMGAppearanceData)

public void RuntimeResult deleteVmgAppearance(ctxt SessMgrNaturalKey, data VMGAppearance)

public VMGAppearanceData[] getVmgAppearances(ctxt SessMgrNaturalKey)

public VMGAppearanceNaturalKey[] getVmgAppearanceNaturalKeys(ctxt SessMgrNaturalKey)

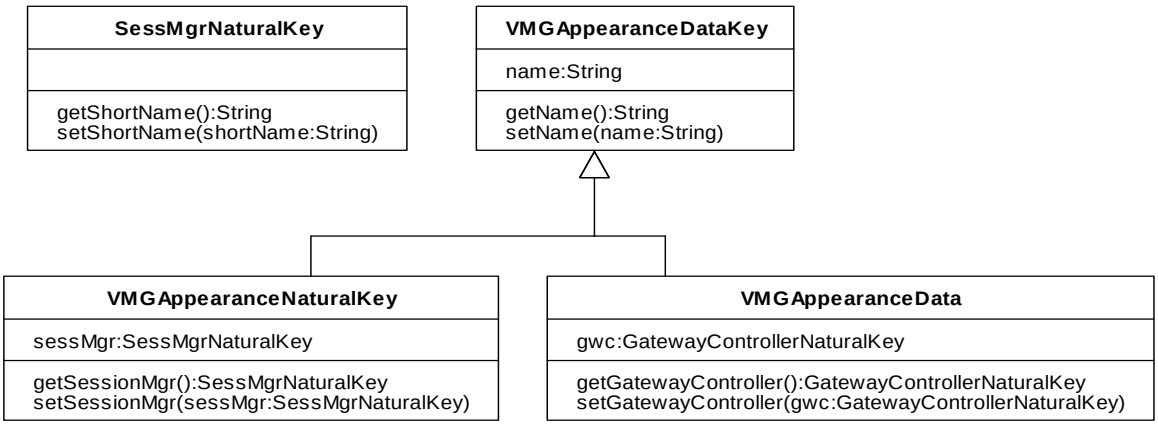


Table 6: VMG Appearance Data

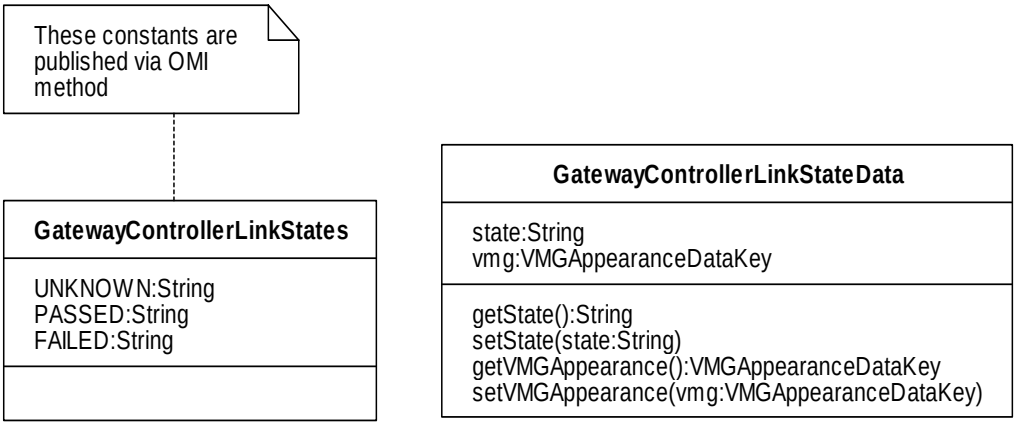
Field	Description
SessMgrNaturalKey.shortName	1-6 characters spaces, dots and underscores for-bidden
VMGAppearanceDataKey.name	1-32 characters [Aa-Zz][0-9][-.]

Maintenance on the links to GWC from Session Manager is available via the Management Console, under each Session Manager. Since the link is over UDP, the only available maintenance command is a line test.

The OMI methods for GWC link test are available through the service located at http://<sysMgrHost>:12121/axis/services/gwcmtc:

public GatewayControllerLinkStateData[]
testGatewayControllerLink(SessMgrNaturalKey ctxt,
VMGAppearanceDataKey[] keys)

public String[] getGatewayControllerLinkStates()



Starting the Gateway Controller Link State maintenance application at the Management Console for a given Session Manager will result in an initial test on the GWC links. Subsequent manual tests of each GWC link are allowed via a test button

Table 7: Gatway Controller Link State Data

Field	Description
state	String. Required to be one of the values available from getGatewayControllerLinkStates

.

Table 8: The displayed states of the GWC Link

Displayed States
NOT_RUN
TESTING
UNKNOWN

Table 8: The displayed states of the GWC Link

Displayed States
PASSED
FAILED

Table 9: The operational states of the GWC Link

Link States
UNKNOWN
PASSED
FAILED

The configuration requires the addition of two new tables to the Oracle database.The first allows the configuration of GWCs, the second the association of a Session Manager with a GWC via a VMG name.

The CS2K_GWC table contains three fields, NAME, ADDR, and GCP_PORT. NAME is of the form gwc-###, where ### is numeric from 0 to 255, giving a VARCHAR of length 7. ADDR is a reference to an Object Identification (OID) from the IP_ADDRESS table. GCP_PORT stored as an integer, between 0 and 65534.

The CS2KVMG_APPEARANCE table contains three fields, NAME, GWC and a contextual field SESSION_MGR. NAME is a VARCHAR(64) which is globally unique.This name will be used when the Subscriber association with the VMG. is made on the Provisioning Server. GWC is a reference to an OID from the CS2K_GWC table. SESSION_MGR is a reference to an OID from the SESS_MGR table.

Because the VMG is configured and the association of VMG with Subscriber is is provisioned, the use of a VMG associated with the correct server home (Session Manager) is enforced when a Subscriber is added or updated. VMGs may not be deleted while some subscriber is still associated with the VMG.

24.5 Endpoint Monitoring

This feature treats a CS2K MSM subscriber as a SIP Line. Subscribers have dynamic state: OFFLINE, IDLE, and CPB. This information (along with other subscriber data) will be available via a QSIP query over the NCAS link as discussed in section 2.3. Additionally, it will be available from the Management Console as a direct query to the Session Manager to which the subscriber is homed. Also from the Management Console, a maintenance ping can be sent to the subscriber endpoint via an OPTIONS message as a line test,

resulting in a line state. The line test functionality is available only through the Management Console. To limit network traffic, the number of lines which can be simultaneously monitored at a single Management Console is limited to five.

The state of a SIP Line is dynamic and is not stored in the Oracle database by the configuration system. Given this, a query must be made to find the subscribers before monitoring can be initiated. The query may be made by DN or by Subscriber name in the format name@domain. After a user is posted, it may have a line test done on it. The line test will test all devices provisioned against the subscriber in addition to all currently registered devices. The two sets of devices may overlap, and the result will contain data for the superset. The result will indicate for each client whether any response was received, as well as an overall indication of whether all clients responded, some clients responded, or no clients responded.

The OMI methods to monitor and maintain the SIP line are available at http://<sysMgrHost>:12121/axis/services/endpointmtc.

public SubscriberData[] getSubByDirectoryNumber(String dn)

public SubscriberData[] getSubByName(String name)

public long startEndpointStateMonitor(SubscriberNaturalKey[] keys)

public RuntimeResult stopEndpointStateMonitor(long tid)

public RuntimeResult updateEndpointStateMonitor(long tid, SubscriberNaturalKey[] keys)

public EndpointStateData[] getEndpointNextState(long tid)

public EndpointLineTestStateData[] testState(SubscriberNaturalKey[] keys)

public String[] getEndpointStates()

public String[] getEndpointLineStates()

The data returned by the subscriber queries:

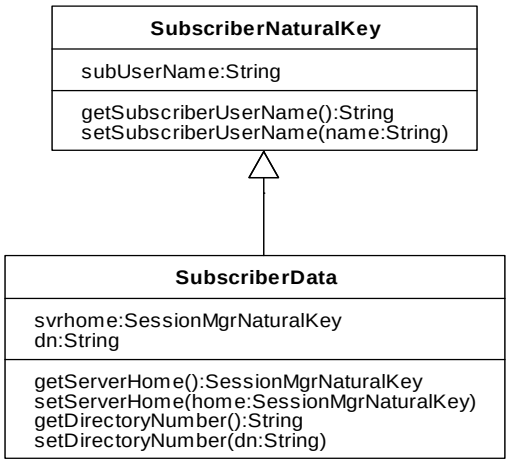


Table 10: Subscriber Data

Field	Description
userName	String of the form <user>@<domainname> where user and domain name each consist of 1-64 alphanumeric characters
dn	String containing 4-18 decimal digits.

The data returned by a line state monitor.

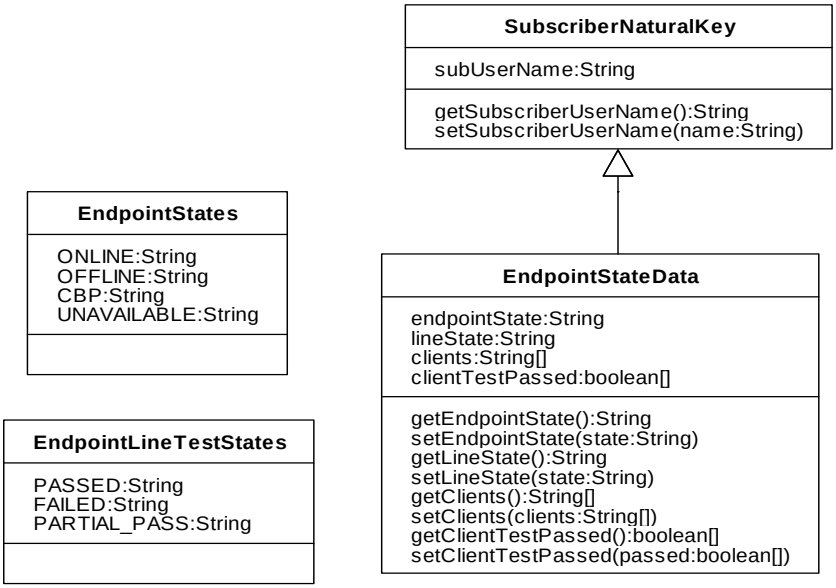


Table 11: Endpoint State Data

Field	Description
endpointState	String. Required to be one of the values available from getEndpointStates
lineState	String. Required to be one of the values available from getEndpointLineStates
clients	Array of strings describing the clients of the subscriber.
clientTestPassed	Array of booleans corresponding to the clients array, and indicating whether each client passed the line test (true=passed, false=failed)

Because acquiring the state of a line requires going to the Session Manager where the endpoint is homed, and that Session Manager may not be accessible from the System Manager, the UNKNOWN state is introduced to the list of displayed Additionally, since the line state is not automatically tested, it’s

initial displayed state is NOT_RUN. A PARTIAL_PASS exists when at least one, but not all of a subscriber's clients can be reached by the line test.

Table 12: SIP Line Endpoint States (displayed)

Subscriber States
UNKNOWN
OFFLINE
IDLE
CPB

Table 13: SIP Line Endpoint Line Test States (displayed)

Line Test States
UNKNOWN
NOT_RUN
TESTING
PASSED
FAILED
PARTIAL_PASS

24.6 Disable Accounting

This feature allows MCS accounting functionality to be disabled. When accounting is turned off, no Accounting Manager (AM_ will be configured against the Session Manager, and no billing records will be spooled. This feature changes the SESS_MGR table to allow NULL in the AM column. The Management Console provides a selection value of <none> in the AM combo box to support this configuration.

When the AM is set to null, no billing records will be spooled by the recording framework. When the AM is not set to null, billing records will be spooled and sent to the AM.

24.7 Hardware Requirements or Dependencies

Not Applicable.

24.8 Software Requirements or Dependencies

Dependant on SCPLite for NCAS link.

24.9 Limitations and restrictions

NCAS Link for QSIP

Support for a single NCAS link to a single CS2K Core at a time is provided. Therefore, only a single CallAgent can be configured at a time.

Updates to the IP address or port of the CallAgent are allowed only if the CallAgent is in the OFFLINE state.

GWC Link

VMG Appearances can only be added and deleted, not updated.

Global uniqueness is enforced across VMG names

Endpoint Monitoring

A maximum of 5 endpoints can be simultaneously posted from a single Management Console

24.10 Interactions

A00009043 SIP Lines Provisioning Support

A00007544 - NCAS link for service control

A00007545 - GCP to SIP conversation on FPF

24.11 Glossary

Term	Description
Accounting Manager	CS2K MSM component which formats and stores billing records from the Session Manager. Turned off in MSM 9.0
AM	Accounting Manager
CPB	Call Processing Busy. Used to indicate that a SIP Line Subscriber is in the middle of a call.
Endpoint	Refers to a SIP Line Subscriber. In the context of SIP Lines, an endpoint does not actually refer to an IP port pair, but to a subscriber who may have registrations at multiple locations.
GCP	Gateway Control Protocol. Used for communication with GWCs

Term	Description
GWC	Gateway Controller. CS2K component to which Session Managers communicate for call processing
MCS	Multimedia Communication Server
MSM	Multimedia Session Manager
NCAS	Non Call Associated Signalling
NE	Network Element. A managed component of CS2K MSM. Includes Accounting Manager, Session Manager, and System Manager.
OAM	Operations, Accounting, and Management.
OID	Object Identifier. Unique ID used in the CS2K MSM database as a primary key.
OMI	Open Management Interface
Provisioning Manager	CS2K MSM component which manages CS2K MSM provisioning, including subscribers.
Session Manager	CS2K MSM component which manages SIP Sessions and call processing
SIP	Session Initiation Protocol
System Manager	CS2K MSM component which manages CS2K MSM configuration and maintenance.
VMG	Virtual Media Gateway. CS2K view of the CS2K MSM Session Manager.

25: Functional Description (FN): A00009036

25.1 Feature name and Feature ID

SN09: A00009036 - Table HOMELRN Option SITE Expansion

25.2 Feature Background

Local Number Portability (LNP) allows users to change local service providers and yet retain their current 10-digit directory number (DN). Location Routing Numbers (LRNs), not DNs, are used to identify the switch serving a ported subscriber.

LRNs are used for routing and billing purposes and are associated with host and remote switching units via table HOMELRN. Table HOMELRN uses the SITE option to assign SITE (remote switching unit) names for a particular non-HOST LRN entry in the table.

To accommodate succession office collapse solutions there is a need to provision more than the current maximum of 10 SITE names that may be associated with a single LRN entry. This activity expands the maximum number of SITE names that can be assigned to the SITE option for an LRN entry in table HOMELRN from 10 to 256.

25.3 Feature Description

This activity affects the provisioning of LRNs for remote switching units in Table HOMELRN. Remote switching units are defined by entries in Table SITE. Prior to SN09, a maximum of 10 SITE names can be associated with a particular LRN entry in Table HOMELRN using the SITE option. This activity allows a maximum of 256 SITE names to be associated with a particular LRN entry in Table HOMELRN using the SITE option.

The option SITE enables multiple site names to be associated with a single LRN. The supported site names are valid names provisioned in Table SITE(i.e. HOST, REM1, REM2,. etc.). The maximum number of SITEs in one tuple is expanded to 256. Once the maximum number of SITE names has been entered for an LRN entry, HOMELRN table control stops prompting for additional SITE names as was done for the prior limit of 10. Other than the new (256) maximum limit for SITE names per HOMELRN entry, there are no other changes to the provisioning capabilities of table HOMELRN.

An external view of the table HOMELRN changes is shown in See “Table HOMELRN Option SITE Entry Changes” on page 218..

Figure 1 Table HOMELRN Option SITE Entry Changes

Old Maximum - Up to 10 SITE Names per LRN Example:

TABLE: HOMELRN
AREACODE OFCCODE STNCODE OPTIONS
---
312 858 $ (SITE (REM1) (REM2) (REM3) (REM4) (REM5) (REM6) (REM7) (REM8) (REM9) (REM10) $)**$**

New Maximum - Up to 256 SITE Names per LRN Example:

TABLE: HOMELRN
AREACODE OFCCODE STNCODE OPTIONS
---
312 858 $ (SITE (REM1) (REM2) (REM3) (REM4) (REM5) (REM6) (REM7) (REM8) (REM9) (REM10) **(REM11) (REM12) (REM13) (REM14) (REM15) (REM16) (REM17) (REM18) (REM19) (REM20) (REM21) (REM22) (REM23) (REM24) (REM25) (REM26) (REM27) (REM28) (REM29).....(REM57).....(REM127)..... ..... (REM208).....(REM256)** $)**$**

Note: This capability is NOT under Software Optionality Control (SOC). This capability is an enhancement to LNP00100 functionality.

25.4 Hardware Requirements or Dependencies

There are no hardware requirements or dependencies associated with this functionality.

25.5 Software Requirements or Dependencies

There are no software requirements or dependencies associated with this functionality.

25.6 Limitations and restrictions

No more than 256 SITE names can be associated with an LRN entry in table HOMELRN.

25.7 Interactions

None

25.8 Glossary

Term	Description
New term	Definition
DN	Directory Number
LNP	Local Number Portability
LRN	Location Routing Number
SOC	Software Optionality Control

26: Functional Description (FN): A00009043

26.1 Feature name and Feature ID

A00009043: CS2K SS SIP Lines Provisioning Support

26.2 Description

The SIP Lines product leverages existing CS2K SS SIP features and CS2K Centrex features. This feature provides the capability to provision data required by CS2K SS for the SIP Lines product for the MCP 9.0 release. Provisioning support that will be provided involves the ability to provision data such as subscriber or SIP end point information used by the Session Manager to provide SIP services.

The following items will be introduced into CS2K SS

- SIP Lines as a service called CS2000 SIP Line
- SIP Lines attributes to the subscriber

The Provisioning of the SIP Line data will be available via both the Provisioning Client and via OPI. OPI is the Open Provisioning Interface, a web service which gives the ability to provision data required on CS2K SS in return for services that it can provide. OPI's capabilities are available via a published WSDL using which the provisioning activities that are required can be determined. For more information on OPI, please refer to the OPI Specification document. Details on the Provisioning Client, which is a GUI based provisioning interface are available in the Provisioning Client User Guide.

26.3 SIP Line data

The data required for SIP Lines primarily consists of:

- End point id
- Virtual media gateway
- Client Type
- Directory Number

In addition to this on the CS2K SS, a new service will be introduced which will qualify a subscriber to be a SIP Line subscriber. All the above mentioned information in addition to a service package containing the new service will be associated to subscribers using which SIP Lines services will be processed.

A more detailed description of the data introduced is given below:

Field Name	Description
End Point Id	Format: <SITE>/<FFF>/<G>/<TTtt> <SITE> = 1-4 Alphanumeric characters. Corresponds to provisioned SITE name in the XACore. <FFF> = 000-511 Corresponds to the frame number used in the logical group name in the XACore. <G> = 0-9 Corresponds to the group number used in the logical group name in the XACore <TTtt> = 0000-1022 Corresponds to the circuit numbers (upper and lower) in the LENs defined against the logical group in the XACore. This is a globally unique field that the user is associated with Maximum length 15 characters; valid character set [Aa-Zz][0-9][/]
Virtual Media Gateway	Virtual gateway name used in GWC provisioning. Maximum Length 64 characters valid character set [Aa-Zz][0-9][-./]
Client Type	This is required for determining if the user has a device that can be queried. The supported client types are: Optical Network Terminator or ONT. If there is no client then the user will not be queried for a device on a line test
Directory Number	This is a globally unique number that is associated with a subscriber, similar to user aliases.

Note: Because of a restriction on the CS2K Session Server in the way the directory number is stored, the username part of the user, i.e. the string before the @domain, cannot be the same as the directory number. This restriction will be taken care of in future release, which will allow both to be same and hence easier to identify.

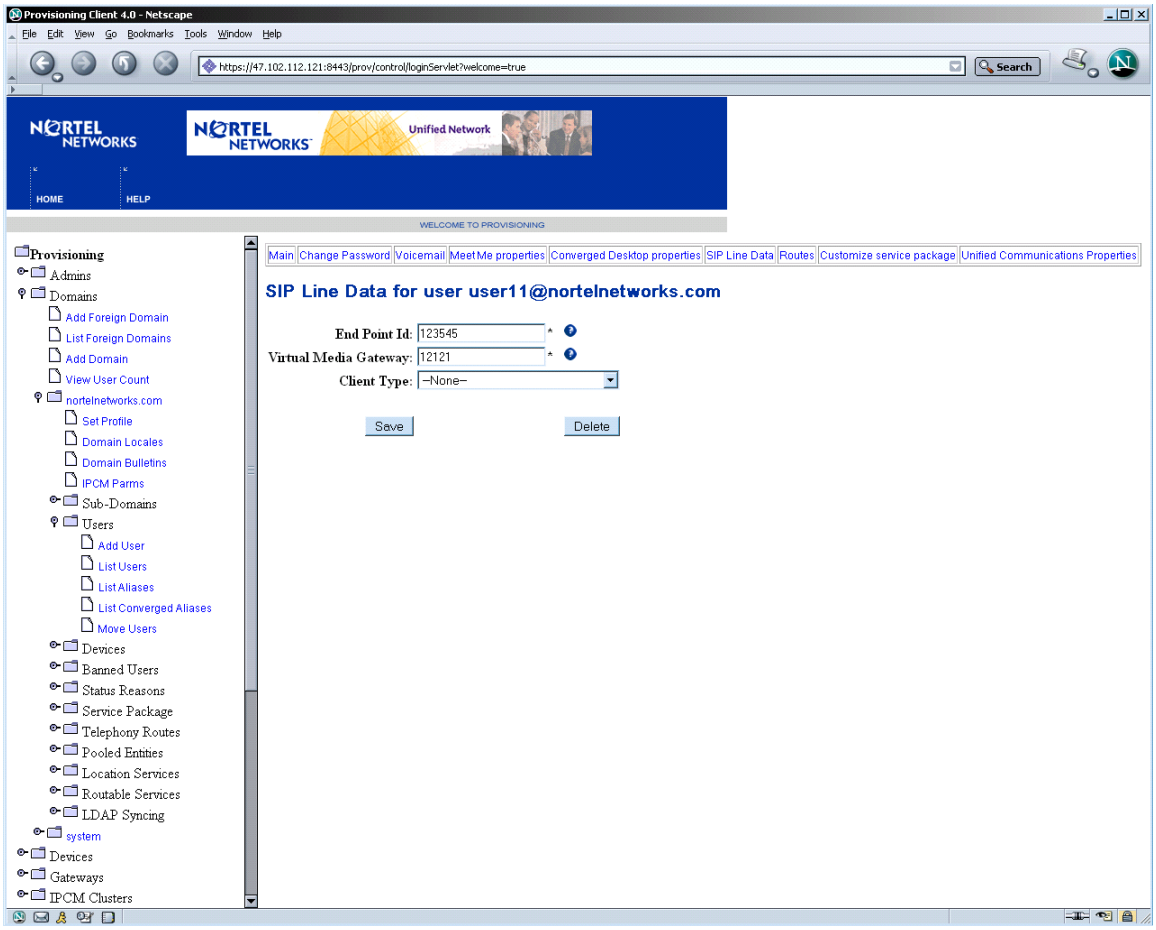


Figure 1 SIP Line Data provisioning for a user from Provisioning Client

Virtual Media Gateways are associated to Session Managers and also to a subscriber. Subscribers are homed on a session manager via the server home attribute associated to the domain that the subscriber belongs to. In case there is a change in the session manager of a domain, then the virtual media gateway information associated to a subscriber is no longer valid. In this scenario the following needs to be done to associate the subscriber to the correct virtual media gateway.

For each SIP Lines subscriber, going though SESM:

- change the end point id on the core
- change the end point id and the VMG via OPI

While changing the server home there will be no check to determine subscribers associated to it

Directory number is a new field associated to the subscriber which is exposed via OPI.

Additional types of clients supported for SIP Lines can be added to CS2K SS via OPI and the Provisioning Client. This interface is shown in the next figure.

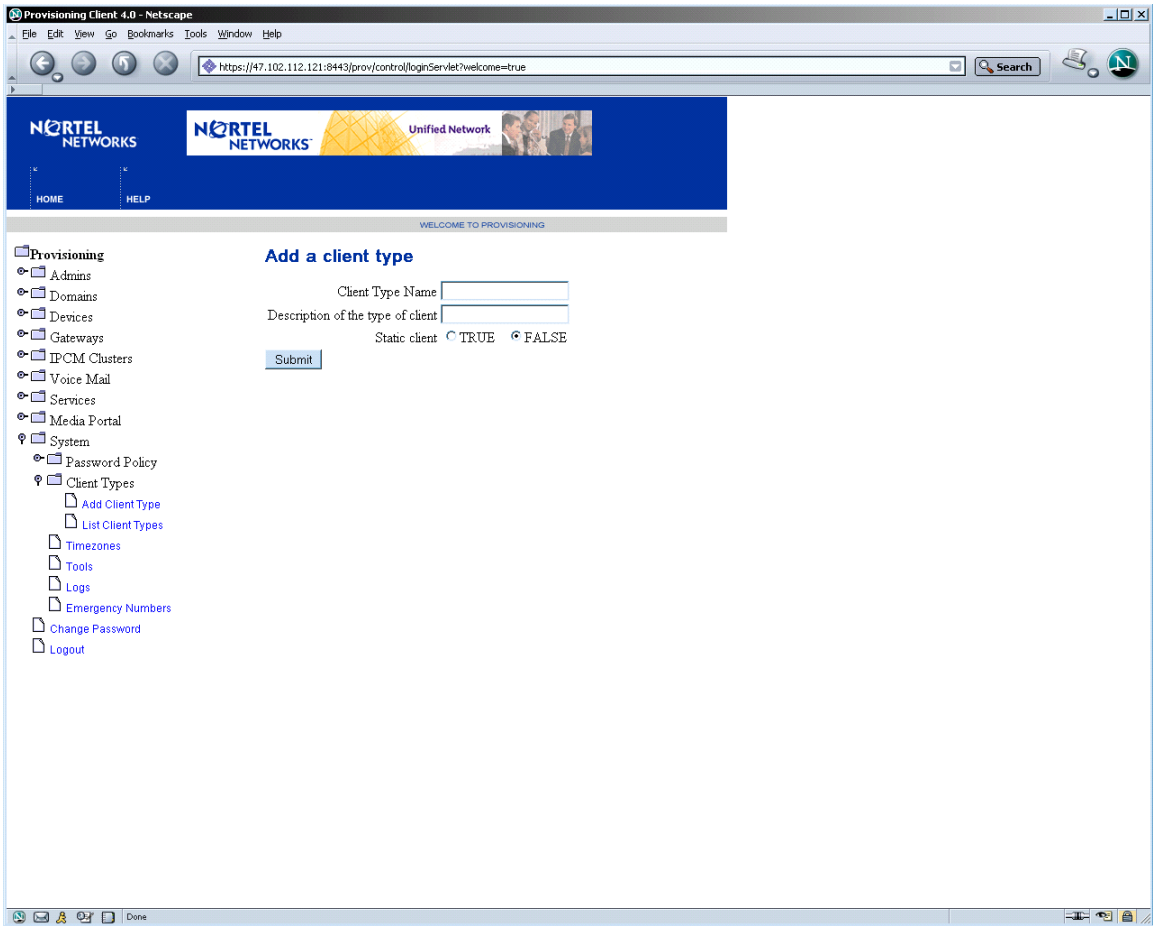


Figure 2 Client type provisioning interface

The OPI methods that can be used for Client Type provisioning are given below.

addClientType(ClientType clientType)
addClientTypes(ClientType[] clientTypes)
modifyClientType(String clientTypeName, ClientType clientType)
removeClientType(String clientType)
getClientTypeByName(String clientType):ClientType

All the client type operations need the administrator to have Full Domain Access privilege. The name of the Client Type information can be upto 60 characters long and the description can be upto 120 characters long.

The data model for the SIP Lines information and its association to the subscriber information is shown below in the figure.

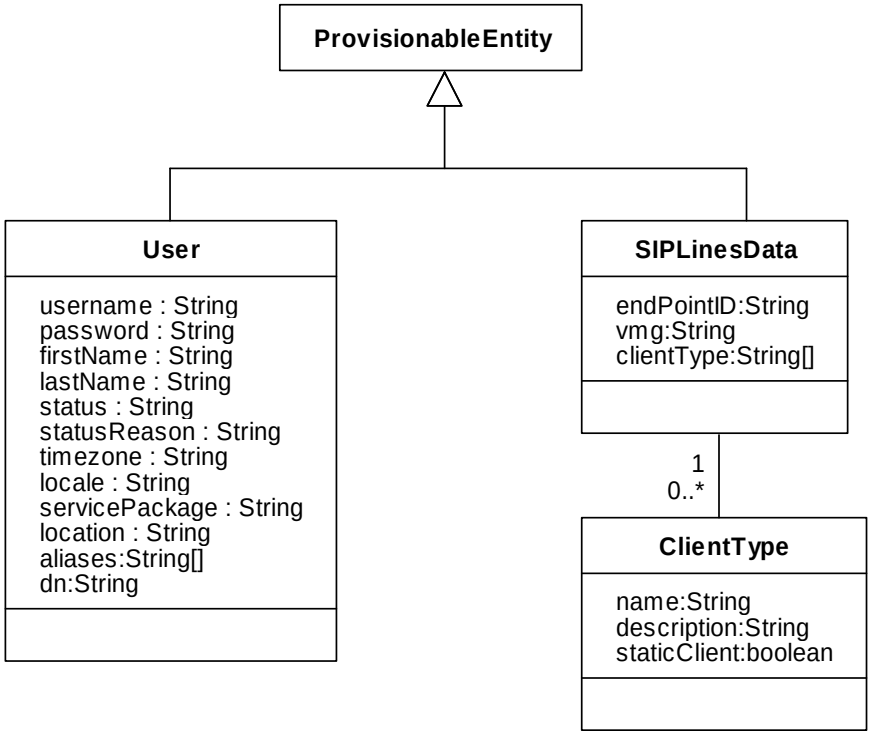


Figure 3 SIP Lines Data Model

The following table gives the required and optional field information for the above

Data	**Field Requirement**	
User	**Required**	Username,password,firstname/lastname,status, timezone, locale, service package, location
	Optional	Aliases, DN, status reason, first name/lastname (one of them)
SIPLineData	**Required**	End Point Id, VMG
	Optional	Client Type

26.4 Non SIP Line data

There is certain data that is required by OPI while adding subscribers which is not SIP Lines specific and hence can be set to a pre-defined value. Given below are three such fields and their valid values:

Field name	Possible Values
Status	ACTIVE, INACTIVE
Locale	French, English, Japanese, Simplified Chinese, Traditional Chinese, German, Spanish, Korean
Timezone	Pacific Standard Time, Mountain Standard Time, Central Standard Time, Eastern Standard Time, GMT-11:00, Hawaii Standard Time, Alaska Standard Time, GMT-04:00, Newfoundland Standard Time, GMT-03:00, Greenwich Mean Time, Central European Standard Time,G MT+02: 00, GMT+03 :00, GMT+03 :30, GMT+04 :00, GMT+05 :00, GMT+05 :30, GMT+06:00, GMT+07 :00, China Standard Time, Japan Standard Time, GMT+09 :30, GMT+10 :00, GMT+11 :00, GMT+12 :00

26.5 SESM and CS2K SS Provisioning

The SESM will be used to provision data onto the Core and CS2K SS in the SIP Lines Product. The data required on CS2K SS will be provisioned using both the Provisioning Client and also via OPI.

The following figure shows the function of the feature deliverables and its use by SESM in the product.

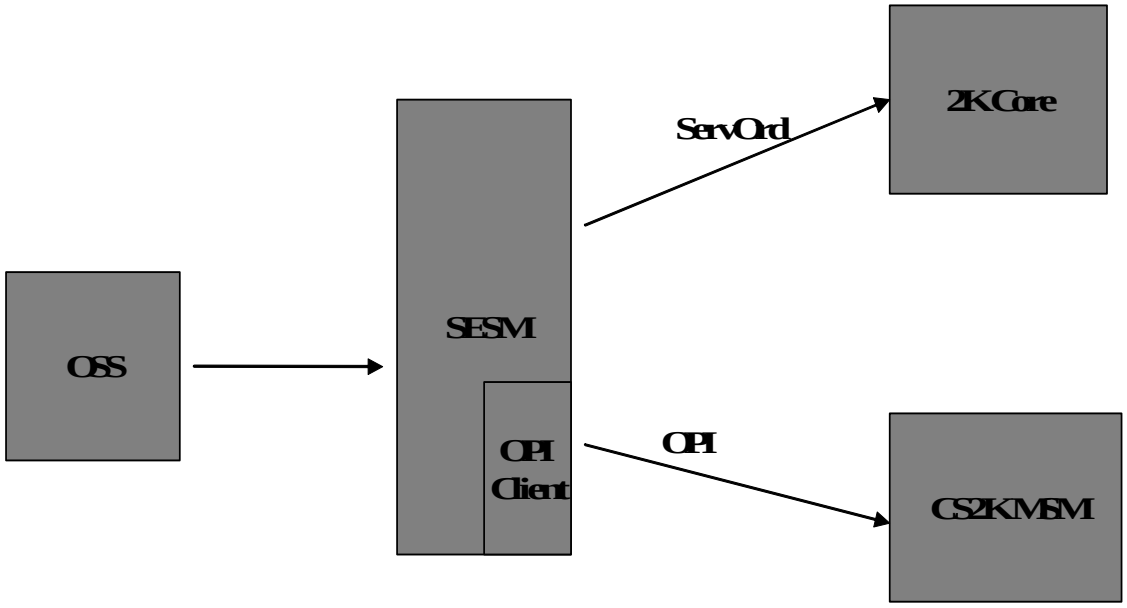


Figure 4 Flow through provisioning from and to CS2K SS in SIP lines

As mentioned above, provisioning of data for the first release of CS2K SS will involve two phases

- **Manual** - Provisioning Client will be used in this phase to provision data which would change rarely once the system is set up. This reduces the number of commands SESM has to carry out to do provisioning on CS2K SS.
- **Flow throug**h - the SESM using OPI carries out provisioning for adding subscriber and SIP Line specific information in this phase.

The existence of the following data is a pre-requisite for provisioning subscribers in CS2K SS:

- Administrator Role
- Administrator
- Root Domain
- Service Packages
- Locations
- Routability group

Figure 3 gives description of the information which can and needs to be Pre-provisioned before Flow through provisioning can take place.

The above data will be provisioned only once in CS2K SS as it will never be modified. The purpose of this data and other data that needs to be provisioned only once on CS2K SS is described below:

- **Administrator** - This is required for authentication and authorization of OPI calls during flow through provisioning from the SESM.
- **Domain** - This is where all the subscriber and end point information will be grouped under.
- **Service Package** - service packages containing the new CS2000 SIP Line service will be created. This will be assigned to all subscribers created from SESM, hence qualifying them as SIP Line subscribers.
- **Locations** - these are locations where the subscribers reside and are required for provisioning Routability groups for media portal insertion.
- **Routability Group** - This is required for the media portal insertion functionality via the zone information.

The following figure shows the data that will be manually provisioned in the CS2K SS system.

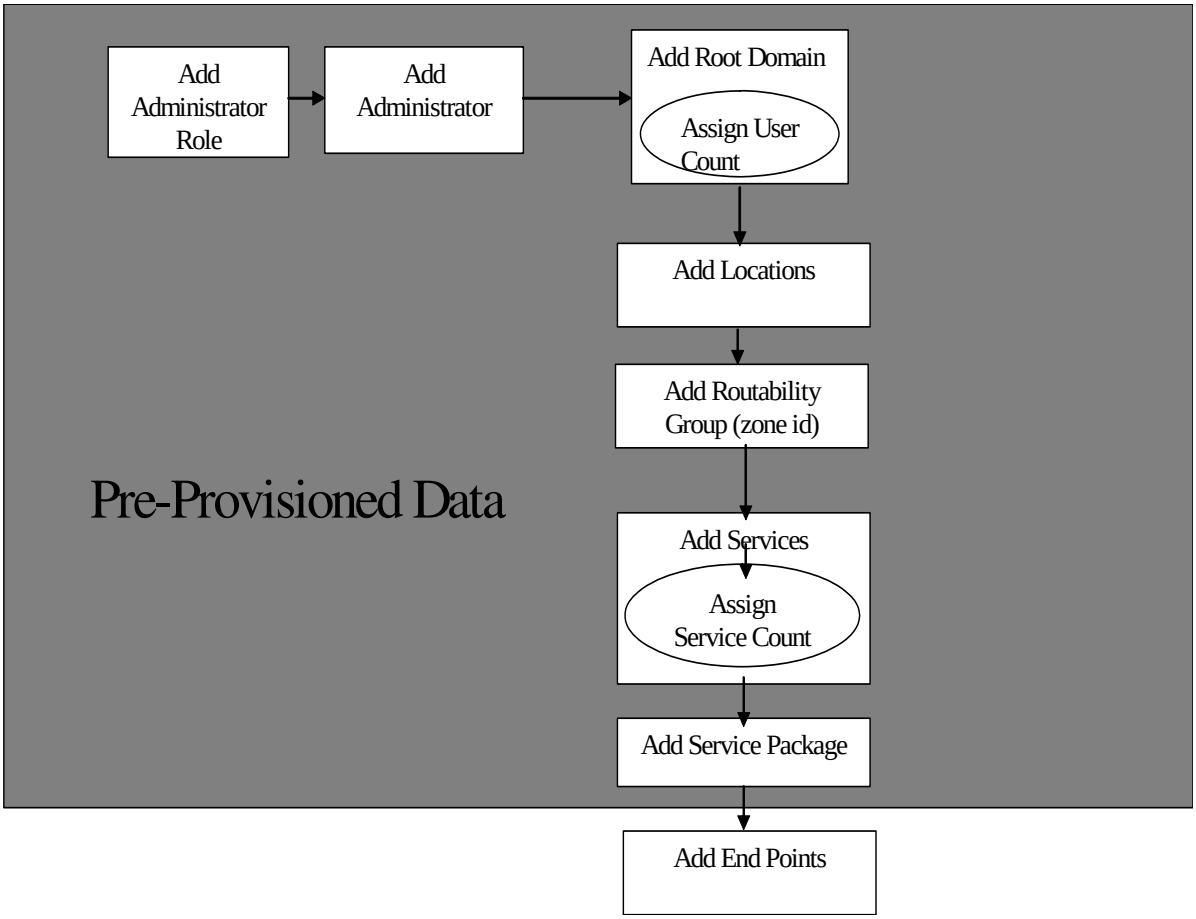


Figure 5 CS2K SS provisioning flow and pre-provisioned data information

Note:

For additional information on the provisioning client and operations please consult the Provisioning Client User Guide.

The next figure shows a sample service package with the CS2000 SIP Line service. Such a service package can be created with a mix of services which are supported on the Session Manager on CS2K SS.

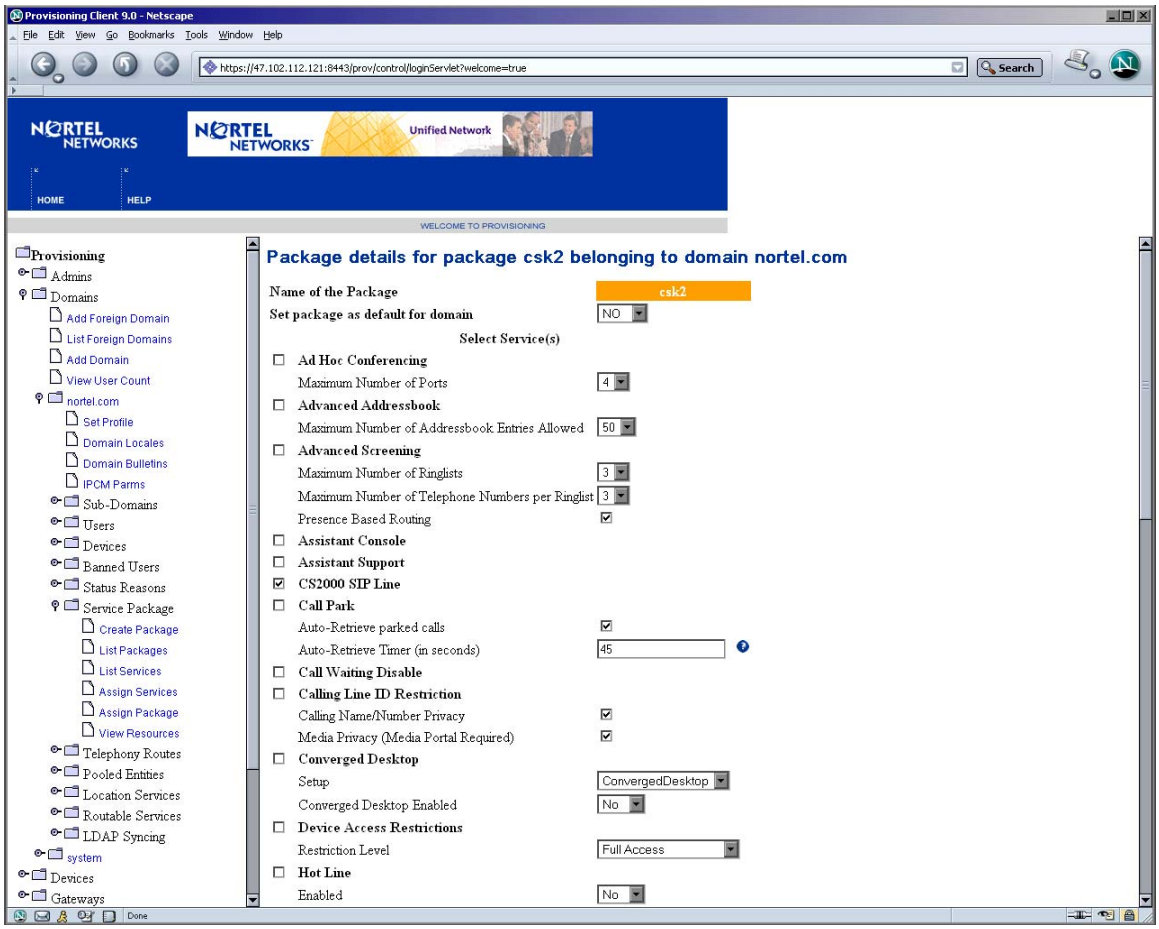


Figure 6 View of service package containing the CS2000 SIP Line service

26.6 Routability Group Information

To determine Media Portal insertion criteria by the Session Manager for services that require media portals for SIP Line calls, a new piece of data named Zone Id will be introduced as a part of the routability group information provisioned as a part of this feature. Following figure shows a view of this field

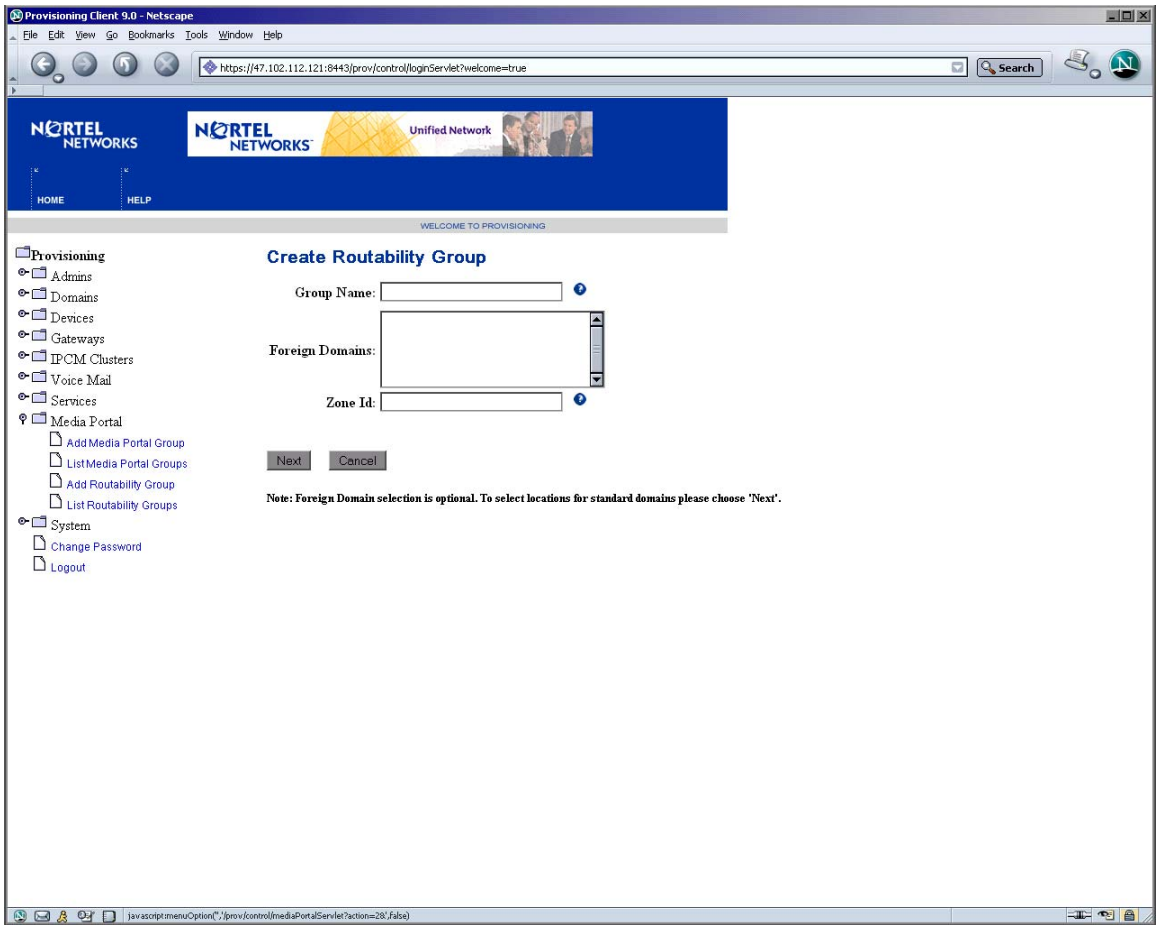


Figure 7 Zone Id information provisioning from Provisioning Client

26.7 SIP Line data provisioning using OPI

SIP Line data can be provisioned onto CS2K SS using both the Provisioning Client or OPI. The methods that are available via OPI for SIP Lines:

- Methods that will be used for user provisioning:

addUser (String domain, User user)
modifyUser (String username, User user)
removeUser (String username)
getUser (String username) : User

- new OPI methods introduced for provisioning SIP Line data

getUserByEndPoint (String endPointID):String
setSIPLineData(String userName, SIPLineData sipLineData)
getSIPLineDataByUserName(String userName):SIPLineData
removeSIPLineData (String userName)
getSIPLineData(String endPointID):SIPLineData
getSIPLineDataByDomain(String domain,int start, int stop):SIPLineData[]
getSIPLineDataByDomainByVMG(String domain, String vmg, int start, int stop):SIPLineData[]
getUserByDN(String dN):String

26.8 Hardware Requirements or Dependencies

The Provisioning Manager configuration in the SIP Lines product is as shown below. SESM will configure the Primary and secondary Provisioning Server Address and Port

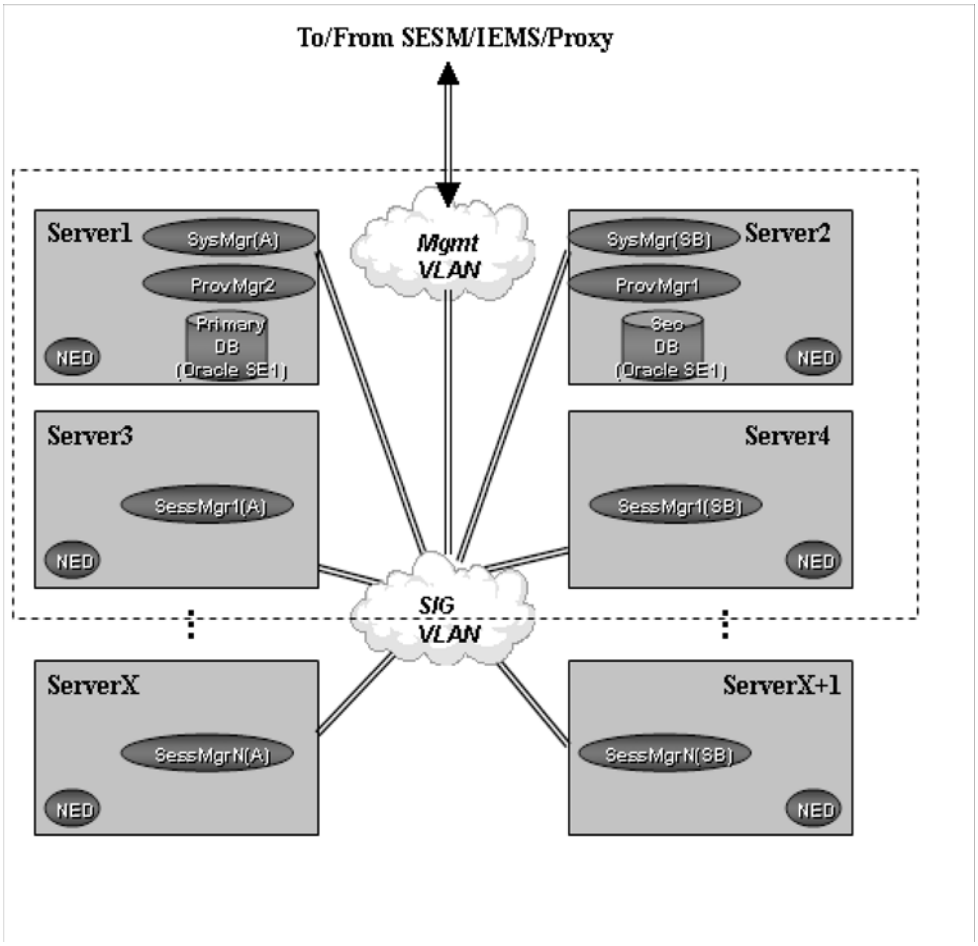


Figure 8 CS2K SS Core server hardware configuration

26.9 Software Requirements or Dependencies

The following software is required for building and using OPI on the SESM and will be delivered as a part of this feature.

- **Axis 1.1 final**: SOAP engine for OPI
- **passwdhash.jar**: contains a utility for hashing the administrator password for security reasons.
- **OPIStubs.jar**: contains the OPI client side stubs along with properties files containing error code and description mapping.
- **truststore**: for HTTPS/SSL based transactions using OPI.

The location of the software will be in the mcp_core_root and mcp_3rdparty vobs and can be accessed by the loadbuild process as needed.

26.10 CS2k SS Service Interaction

The following are services that cannot be provided from CS2K SS for a subscriber who has the CS2000 SIP Line service in the service package:

- Assistant Console
- Assistant Support
- Call Park
- Converged Desktop
- Device Access Restrictions
- Hot Line
- Music On Hold
- Net6 Support on i2004
- Wireless Client
- Voicemail
- Unified Communications
- Calling Line Id Restriction
- Call Waiting Disable
- PCClientSet Control

26.11 OPI Version and Release Information

There will be three new OPI methods introduced which will give current release and version information for OPI and MSM. The methods are:

Method Name	Purpose
getOPIVersion():String	current version of OPI
getOPISupportedVersion():String[]	List of OPI versions supported by the current release
getReleaseName():String	current release for MCP/ CS2K MSM

The information from these method calls can be used for the purpose of software upgrades based on release and OPI version that are compatible.

26.12 License key requirements and miscellaneous changes

The service CS2000 SIP Line at this time is not license keyed, meaning that the number of subscribers that can have this service is not controlled.

Also, as a part of this feature, the lengths of user name and the domain names are being increased to be 64 characters as opposed to the 60 character limit that enforced in earlier releases.

26.13 Glossary

Term	Description
OPI	Open Provisioning Interface
SESM	Succession Element and Sub-Element Manager
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP over SSL
SSL	Secure Sockets Layer
SIP	Session Initiation Protocol

27: Functional Description (FN): A00009045

27.1 Feature name and Feature ID

A00009045: CallP Checkpointing Support

27.2 Description

This feature adds the following capabilities to the CS2000 Multimedia Session Manager (MSM):

- The ability to checkpoint active calls to the standby instance of an MSM.

  For the purposes of this feature an active stable call is one that has been answered. Answering a SIP call means that the 200 OK response to the initial invite has been received or sent by the active session manager.

  Previously this information would have been lost on failover, but recreated, in part, by the long call audit and/or call clearing.

- The ability to checkpoint subscriptions to the standby instance of an MSM.

  Subscriptions refer to SIP SUBSCRIBE messages for a particular event package.Because if this checkpointing, subscription to service packages like presence , call park.. will be preserved after failover.

  Previously this information would have been lost on failover.

- The ability to checkpoint network call logs to the standby instance of an MSM.

  The call log information is preserved so that a user will be able to get a record of their calls from the Personal Agent even after a failover.

  Prior to this feature if the failover occurred before the call log was written to the DB the call log would have been lost. The database write occurs upon the completion or rejection of the call.

- Enhanced presence processing and recovery of “On the Phone” presence after failover.

  A number of enhancements have been made to presence processing. Additionally, after a failover, the newly active instance of the MSM is able to recover a user’s presence state to an “On the Phone” state if they are active in a call. Prior to this feature the user’s presence state would have been changed to “Connected” after failover.

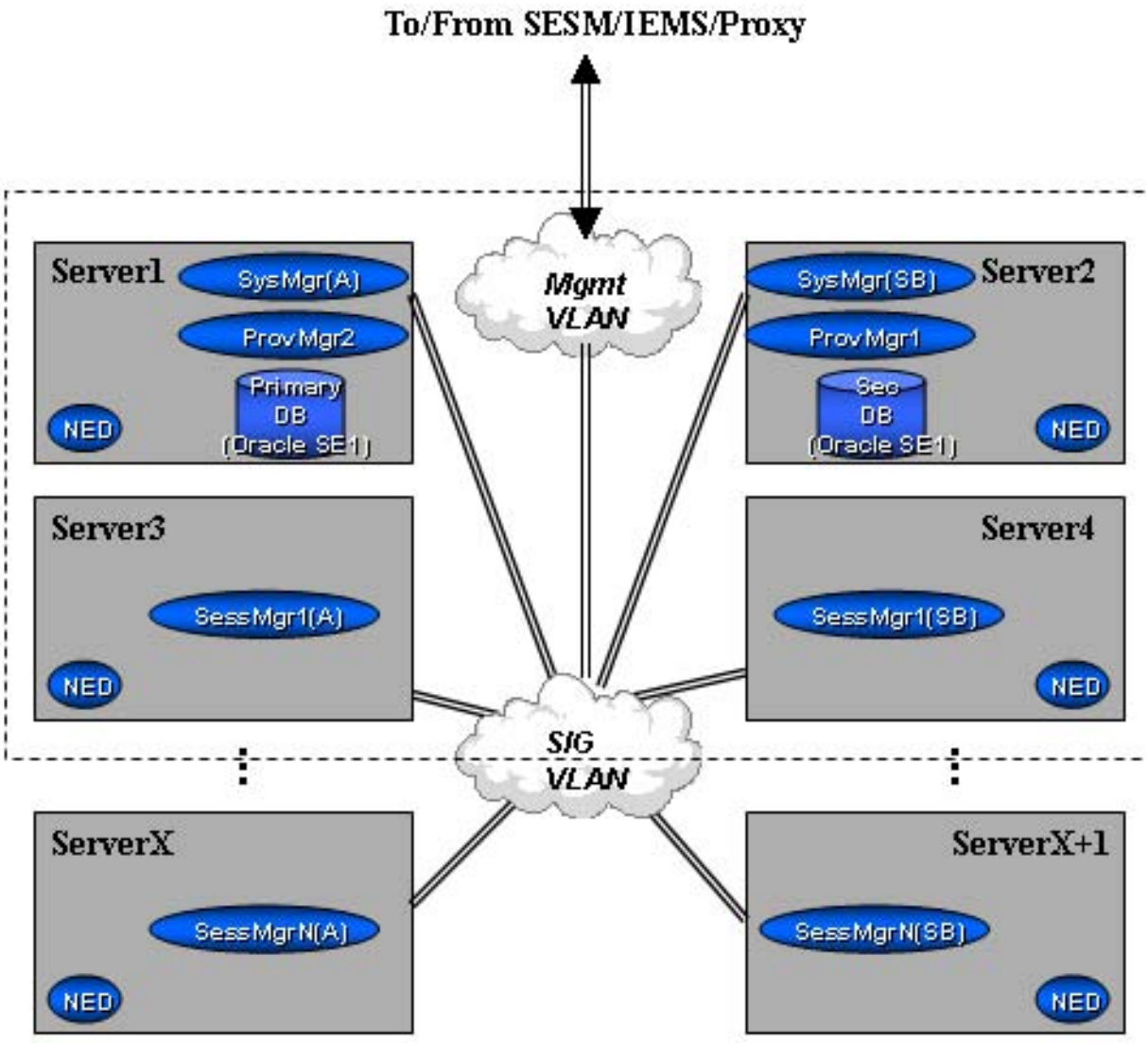
- This features adds 2 additional levels of overload to what was available in 3.0 and 4.0.

  In 3.0 and 4.0, there was only one level of overload, specified by 2 numbers, a "None" number and a "Severe" number. MCS would go into overload when the "Severe" number was exceeded. In the picture below, MCS would go into overload when the Call Queue exceeds 100. When in overload, alarms are raised, and all new sessions are blocked. Sessions that are already in progress would be allowed to continue. When the Call Queue goes below 70, the alarm is cleared, and all sessions are serviced.

27.3 Hardware Requirements or Dependencies

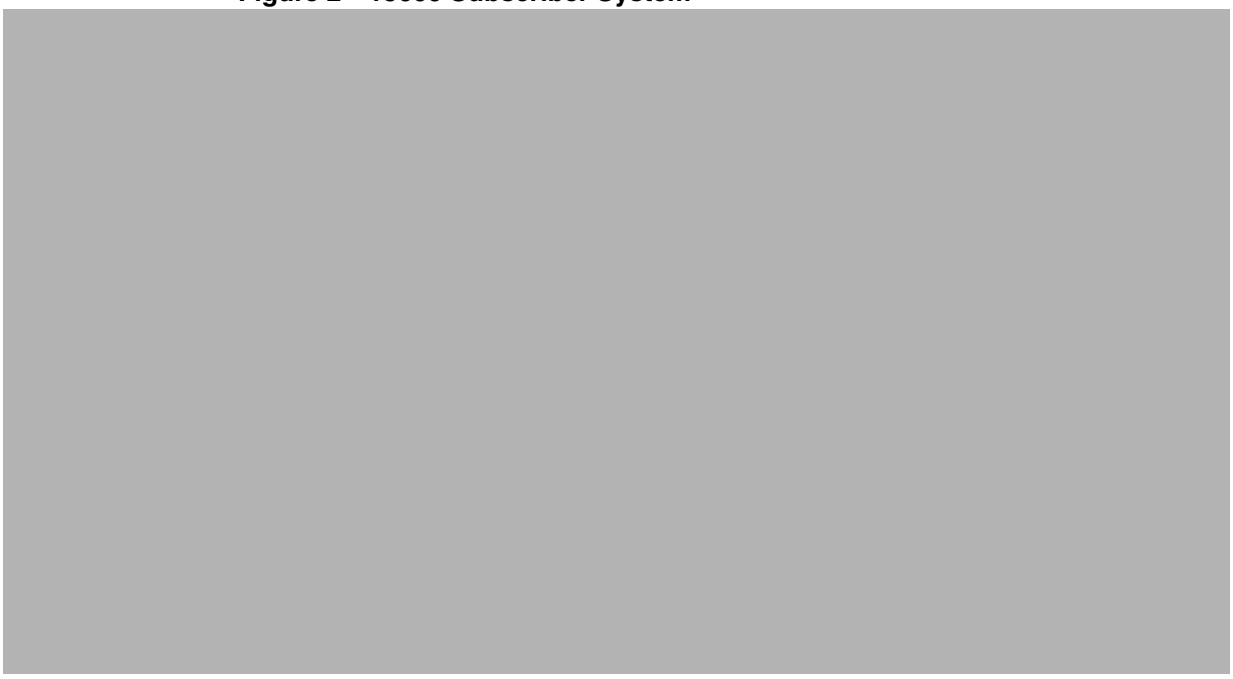
The diagram below represents the MSM configuration for 35000 subscribers. In this diagram, Server 3 and 4 represent an active/standby pair for Session manager instance 1 (SessMgr1). Server 3 is the active instance signified by the (A) and Server 4 represents the standby instance signified by (SB).

Figure 1 35000 Subscriber System



The following diagram represents the configuration for 15000 subscribers. In this diagram, SessMgr1(SB) represents the standby instance for SessMgr1(A), the active instance.

Figure 2 15000 Subscriber System



The diagrams above do not represent the only configuration possible.

27.4 Software Requirements or Dependencies

This feature is part of the MCP 9.0 release.

27.5 Limitations and restrictions

There are limitations in the processing for checkpointing. When a standby instance becomes active due to a failover there are two possible problems, both are due to the case where a Checkpoint is in process at the time the failover occurs. The newly active system can have calls active that were in the process of disconnecting and the checkpoint was not transferred before the failover occurred. In addition calls that were just setup prior to the failover will not appear on the newly active instance.This leads to inconsistent state information between the Sip Line clients, the MSM and the GWC. .

One audit goes active once the standby instance becomes the active instance to correct the inconsistencies. This audit causes the MSM to send a SIP message to all SIP Line clients the MSM thinks is active on a call to verify that they are actually on a call.

Due to the above limitations on checkpointing not all of the calls to a subscriber will be logged. Any entry in the local call log table in the process of being checkpointed at the time of the fail over will be lost. Unfortunately there is no way to mediate this loss of information.

Subscriptions have the same limitations as the call logs in that there is no way to audit them from the Session Manager. However any subscription that is lost will be refreshed by the client within one hour which is the expiration time returned by the session manager upon processing a subscription.

27.5.1 Removed Limitations and restrictions

A number of restrictions and limitations that were previously in effect have been lifted as a result of enhancements to the presence service operation.

Reporting of “On the Phone” presence is no longer limited to Nortel clients. Previously, only the Nortel IP Client Manager, Nortel Multimedia PC Client, and Nortel Multimedia Web Client were capable of reporting that they were “On the Phone” through signalling to the MSM. Now any subscriber that has an answered call going through the MSM will have their “On the Phone” presence tracked at the MSM itself. This allows third-party clients to be shown as on the phone regardless of their client’s capability set.

The MSM now detects dead clients much faster than in previous releases. This affects the scenario of a user’s client crashing or losing network connectivity and is unable to re-register with the MSM. In this case, their presence state will change to “Unavailable Offline” close to the time their last registration expires. In previous releases the interval between their last registration expiring and their presence state being updated was highly non-deterministic due to the auditing mechanism being used and system load. This mechanism has been improved to be less sensitive to system load and more timely than in previous releases.

The auditing mechanism to detect dead clients has also been applied to detecting stale clients that last reported that they are in an “Active Available” state. This is the case where a client reports that the user is actively using the PC. The MSM previously audited clients in this state by asserting that they were no longer in the active state. As a result this prompted the client to re-assert that the PC is actively being used to prevent users being shown as “Active Available” when network connectivity may have posed a challenge to accurately reporting their state. In previous releases the time period between audits was highly variable. The new mechanism reduces the variable lag time between the engineered activity auditing period and the audit being performed.

27.6 Interactions

Advanced services are not guaranteed to work after the fail over of the call. The only service guaranteed to work is the release of the call by either party in the call. Other messages will be sent a 500 service unavailable if the core is not able to process the message. Some of the services not guaranteed to work afte failover are MOH, Call Park, Boss/admin, unstable calls like consultative or blind transfers in progress , CD calls.

The presence service has been better integrated into the system overload controls. As a result, if the MSM is in a minor overload state, presence notifications will not be sent to people watching a particular user. Only the user's own self-subscriptions will be notified of presence state changes. If the MSM is in a major or severe overload state, presence notifications will not be sent to anyone. When the MSM returns to the minor overload state any postponed self-presence notifications are sent out as a background process. When the MSM is no longer in overload notifications return to normal and any postponed notifications are sent out as a background process.

Additionally, the presence service no longer processes presence events using the same processing queue as call processing. This reduces the processing time for registration requests and allows the system to handle presence processing at a different priority from call processing during overload conditions.

27.7 Operational Measurements

New OMs will be introduced with this feature.

27.7.1 Checkpoint OMs

One new OM is introduced relating to checkpointing: CheckpointedCalls.

The CheckpointedCalls OM can be used on the standby instance to monitor the number of calls that would be preserved in a case of a failover.

This OM will be reset in case of extensive connection loss between the active and standby instance, as all calls will be re-checkpointed when the connection is reestablished.

27.7.2 Presence OMs

A new OM group is introduced as part of the presence enhancements: Presence Event Report. This OM group is in addition to the OMs defined for presence in previous releases. This OM group tracks the behavior of the various presence events that are processed by the server.

For each of the rows in the report, which represent the eight presence event types: Activity, End Call, Inactive, Login, Logout, New Call, and Manual there are five columns:

- Created

  The number of events of that type that have been created in the system. This gives the operator an idea of the relative frequency of occurance for that presence event type.

  This OM is a counter register and is reset to zero after each office transfer period.

- Processed

The number of events of that type that have been processed by the presence event processor. Just because a presence event is created, does not mean that it is guaranteed to ever be processed. It may be eliminated from consideration because of an opposing presence event.

This OM is a counter register and is reset to zero after each office transfer period.

- Optimized

  The number of events of that type that have been optimized by the presence event processor. An event is optimized when it an opposing presence event is processed that nullifies the presence event change that would have taken place. For instance, if a new call event is processed, and the presence event processor sees that there is an opposing end call event in the queue or parked, there is no further point in processing either event, they cancel each other out.

  This OM is a counter register and is reset to zero after each office transfer period.

- Queued

  The number of events that are currently in the presence event processor queue waiting to be processed.

  This OM is a usage register. It increments and decrements according to the length of the processing queue and is unaffected by the office transfer.

- Parked

  The number of events that have been initially processed, but must wait for the presence guard timer to expire before being processed. These events are “parked” waiting for the guard timer to expire before being applied. They are frequently candidates for optimization.

  This OM is a usage register. It increments and decrements according to the length of the processing queue and is unaffected by the office transfer.

In addition to the new OM group, the following OMs are added to the existing “Presence” OM group:

- throttleNotifySelfOnly

  This OM is pegged every time the system does not send out a notifications to non-self subscriptions because of a presence state change during minor overload. This is pegged once for the entire state change, and does not reflect the actual number of notify messages that were not sent out.

This OM is a counter register and is reset to zero after each office transfer period.

- throttleNotifyAll

  This OM is pegged every time the system does not send out any notifications, including self-subscriptions because of a presence state change during major or severe overload. This is pegged once for the entire state change, and does not reflect the actual number of notify messages that were not sent out.

  This OM is a counter register and is reset to zero after each office transfer period.

27.8 System Manager Changes

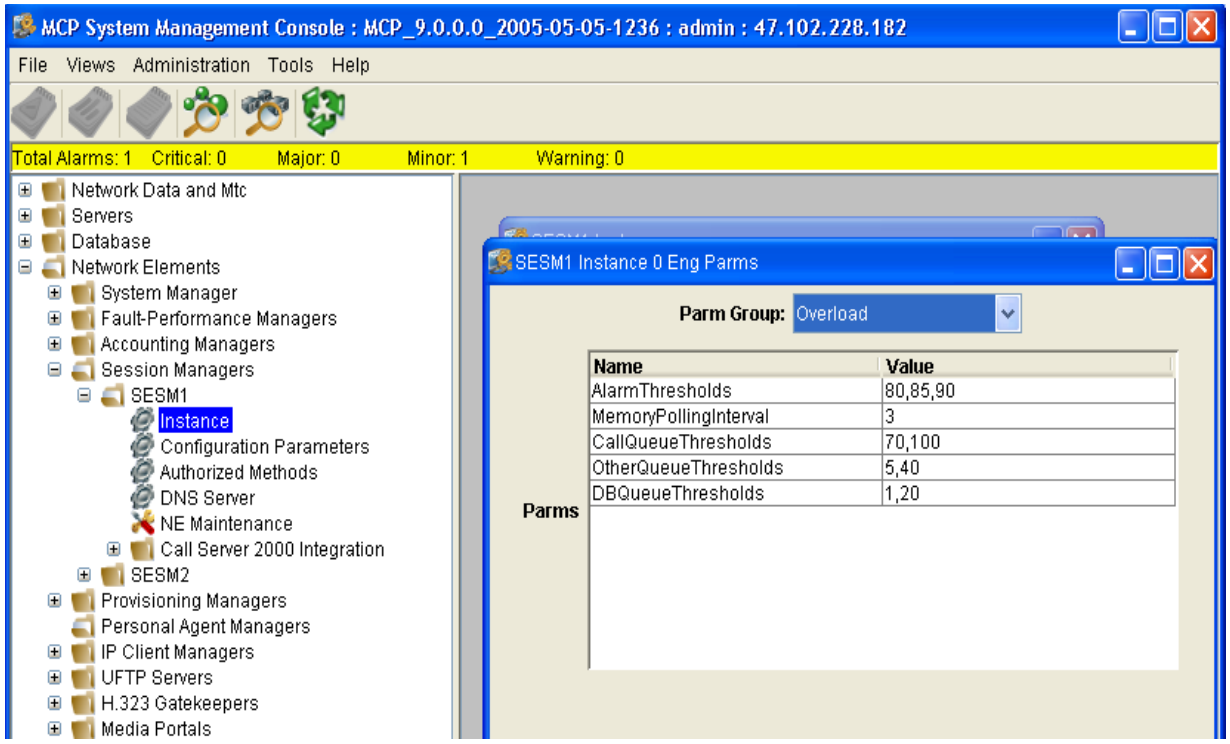
Instead of just having the Severe overload condition, there are 2 other overload conditions. They are:

- Minor -- presence notifications except to self and admins won't be generated.
- Major -- Same as in Minor, additionally, IM will be blocked.
- Severe -- Everything except in-session messages will be blocked.

To specify the additional levels, instead of just having the "None" and "Severe" numbers, the format is to accept 4 numbers: "None", "Minor", "Major", and "Severe".

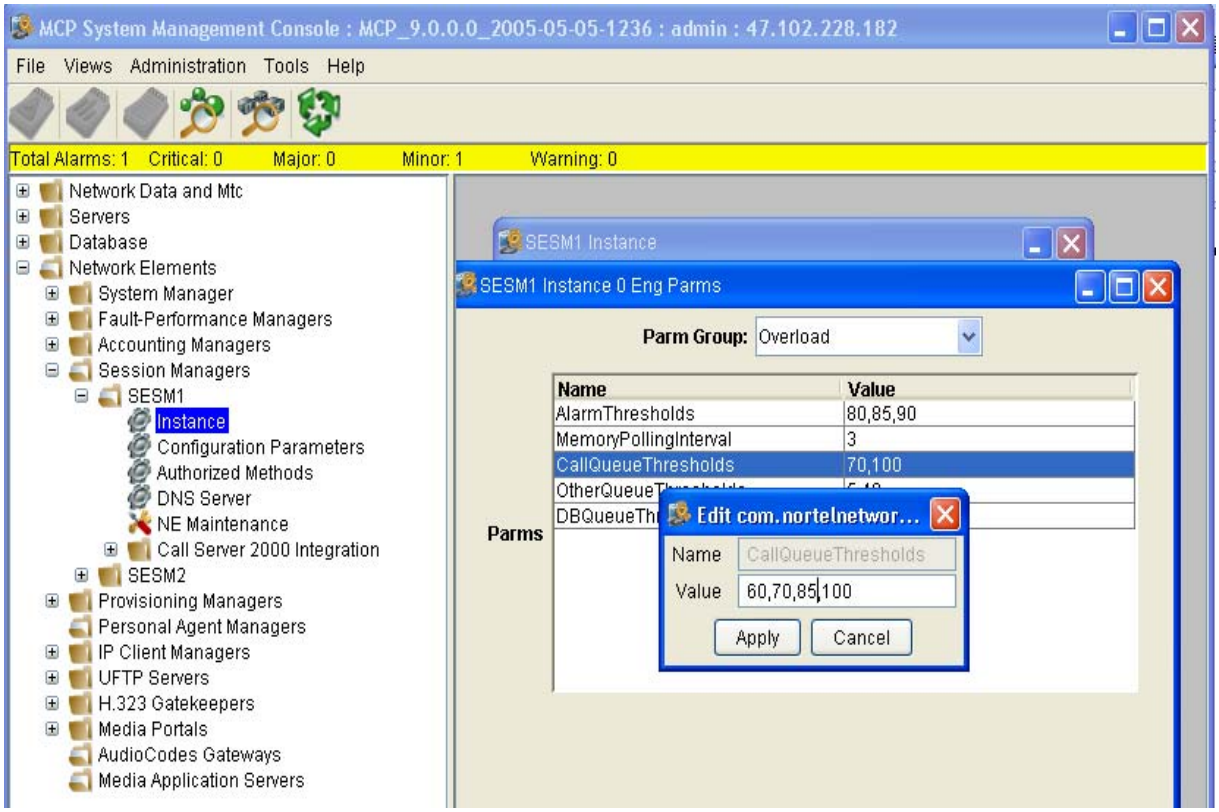
If only 2 levels are specified, such as after an upgrade, then the same behavior as in 3.0 and 4.0 is provided (see Figure 14, “Existing Overload Engineering Parameters,” on page 242).

Figure 14: Existing Overload Engineering Parameters



When four numbers are provided, the increased overload granularity is enabled. In the example below (Figure 15, “New Overload Engineering Parameters,” on page 243) if the Call Queue exceeds the Minor number (70), and stays at that level for a few seconds, MCS will stop generating presence notifications. If the Call Queue exceeds the Major number (85), then Instant Messages will be blocked. If the Call Queue exceeds the "Severe" number, then all new sessions will be blocked. For any of the overload conditions, the same alarm is raised, but different severities are assigned to those alarms.

Figure 15: New Overload Engineering Parameters



27.9 Glossary

Term	Description
Info Ping	A SIP INFO message sent without a message body. The proper response is a 200 Ok if the INFO is within a call and a 481 if outside of a call. Defined in RFC 2976
MSM	Multimedia session Manager
SIP	Session Initiation Protocol

28: Functional Description (FN): A00009078

28.1 Feature name and Feature ID

A00009078: ICM Dual CTI.

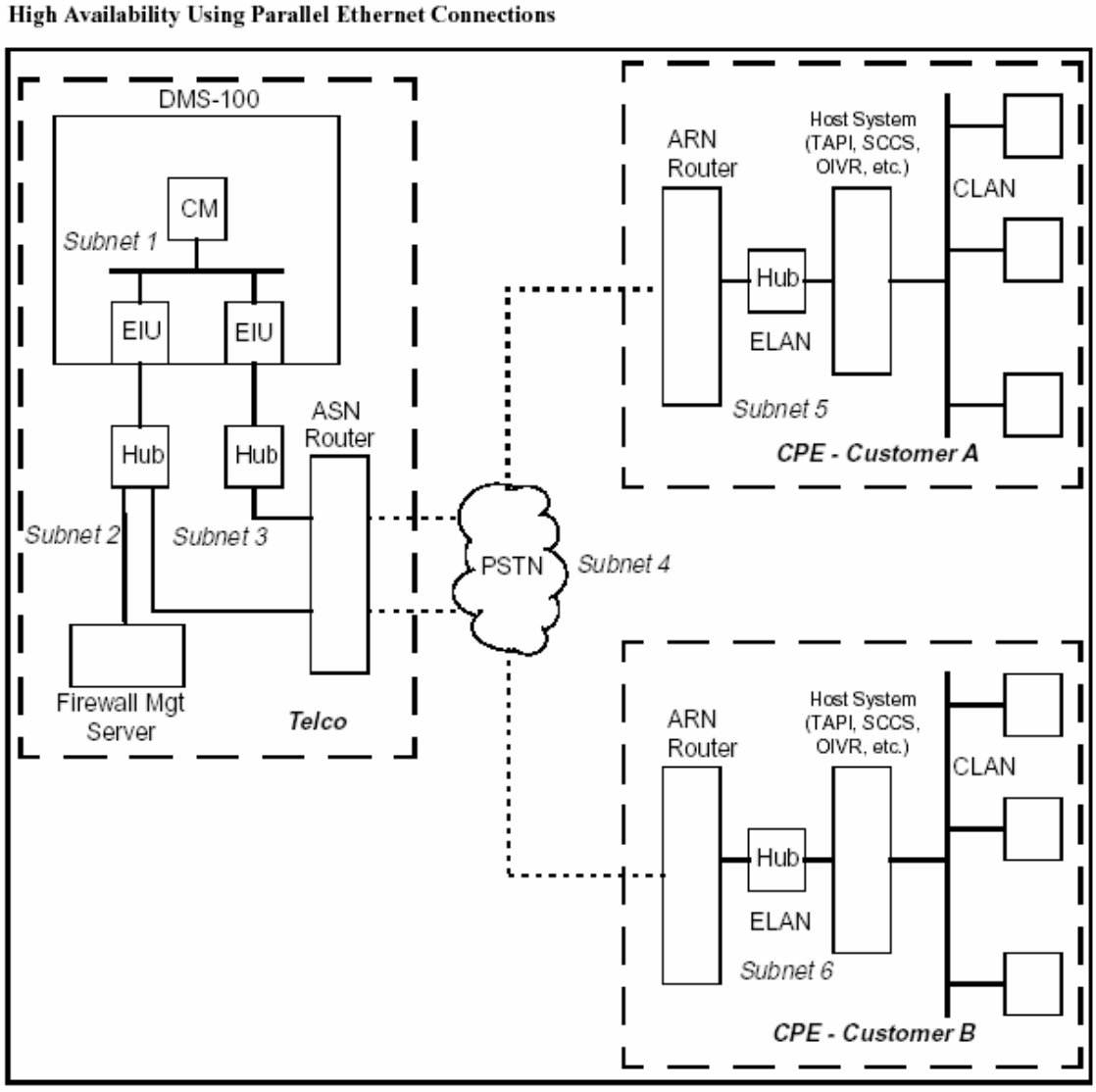
28.2 Description

Currently ICM only has one TCP/IP link per linkset. This feature will allow two TCP/IP connections to exist in one SCAI session. The second link will mirror the first link by broadcasting all switch to Host messages except the continuity test messages to both the TCP links. The switch would only expect a response where necessary from the Host through one of the TCP links within the linkset.

This feature does not need more than one EIU to function. The two TCP/IP links within the linkset can connect to a single EIU. It is the customer's responsibility to provide a reliable and properly configured network. For reliablity, Nortel recommends that the EIU's be configured on separate subnets and be configured in interface mode such that one TCP/IP link within the linkset connects to one EIU within one subnetwork and the other TCP/IP link within the linkset connects to the EIU in the other subnetwork. When EIU's are configured in the interface mode, the Host must use the IP address of the EIUs to connect to DMS-100.

For CS2Kc customers the connection will be made using one IP address for both ICM links within a linkset

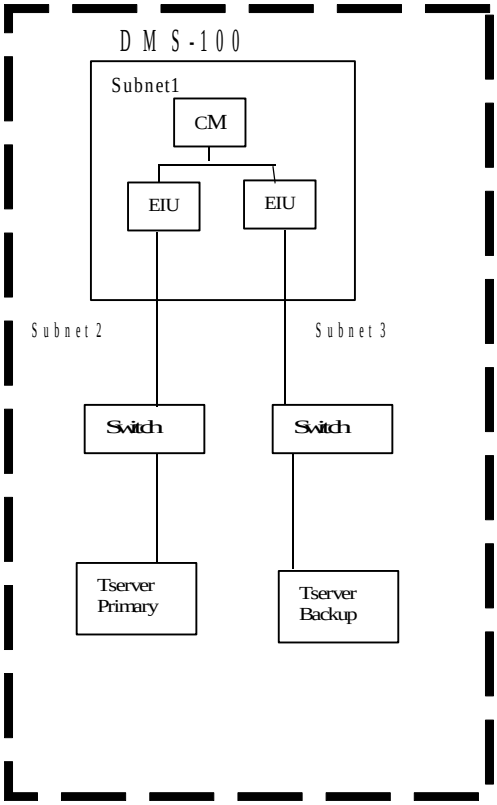
Figure 1 : High Availability Using Parallel Ethernet Connections



In the figure 1 above, the EIUs may be connected to either Eithernet hubs or switches. Hubs are blocking devices which will drop a packet when thereis a packet collision. Switches are non-blocking and should be utilised when there is a possibility of collisions(eg: When other Ehternet devices are connected).

Another simplified configuration can be used if the Tserver and the DMS-100 are co-located, meaning they are not far apart. The allowed distance between the Tserver and DMS-100 for this configuration depends on the hardware specification for each unit used.

Figure 2 Simplified Configuration for High Availability



Please refer to the CN section of this document for details on the datafill needed for this feature to work

28.2.1 Continuity Testing

The continuity test for the TCP links within a linkset will be enhanced to work as it does for multiple X.25 links within a linkset.

The continuity test message will be sent in a round robbin fashion to both links from the DMS. The DMS will wait for the response up to the datafilled response time before it will send it to the next link. DMS will expect a response from the corresponding link on the application. If the DMS does not receive the response to this test within the response time, the test would have failed for that link after the number of attempts has been exhausted.

If both links fail the test, then the session will be either taken down or not according to how the Terminet parm is datafilled per linkset. When the DMS detects that one of the link has failed, the broadcasting of messages to both links will stop and only the live link will be used to send the ICM messages.

When the continuity test is initiated from the Tservers, the DMS will respond to each of the continuity messages it receives by broadcasting the response to both links.

28.2.2 SOC

This feature uses Software Optionality Control (SOC). The SOC order code is ICM00081. Please refer to the CN section of this document for further details on SOC. This feature will not function if the SOC is not turned on.

28.2.3 OMs & Logs

Changes will be made to the OMs for TCP/IP linksets. The OM will now show the existing registers for each TCP/IP link as a separate tuple.
Example:

Existing tuple

16 TCP_AA

0 0 0 0

Will now appear as

16 TCP_AA **0**

0 0 0 0

If there a two links within a linkset it will appear as below:

21 TCP_BB **0**

0 0 0 0

23 TCP_BB **1**

0 0 0 0

The number next to the linkset name represents the link number within the linkset

No new logs or changes to the existing logs are needed for this feature.

28.2.4 Tools

SCIDBG13: This tools is used to debug the SCAI application. Changes will be made to the following commands in the tool to accommodate the second TCP/IP link within the TCP linkset.

- PRINT

-CLEAR
- RESET

SCAITCP: This is a MAP level tool to monitor the ICM application. The following commands of the tool will be enhanced to accommodate the addition of another TCP/IP link within the TCP linkset.

Query Linkset
Clear SessionID

Clear Linkset

Clear Invokes

Clear Transport

SCAItest Sanity.

28.3 Hardware Requirements or Dependencies

The TCP/IP transport uses the existing TLI interface to provide connectivity between the DMS-100 and a business computer. It also makes use of Local Area Network (LAN) and an internet router. The DMS is provided with LAN connectivity by an Ethernet Interface Unit (EIU). The EIU acts as an router between the DMS-100 and an internet router. If there are more than one link per linkset, the EIUs need to be in an interface mode for reliability. Messages originated from the business computer are routed through internet and finally terminates on a router which is connected to Ethernet LAN and are sent to the EIU which forwards the messages to the destination node on the DMS.

For CS2Kc, a primary and a backup 3PC card will be used to make the TCP/IP connections. Only a single IP address will be available for the Host to connect to the CS2Kc.

28.4 Software Requirements or Dependencies

The feature enhances already existing ICM software to handle the following areas:

Table Control mechanism to support additional TCP/IP link within a linkset.

Auditing for two TCP/IP link per linkset.

OMs and Logs changes for redundant TCP/IPlink per linkset.

SCAI tools, SCIDBG13 (CI tool) and SCAITEST (MAP level tool).

This feature also adds new code to support SOC for this feature.

28.5 Limitations and restrictions

Maximum number of TCP/IP connections are 96. No more than 96 service nodes and switches could be connected to a single switch. This is assuming no other applications are using TCP/IP connections from the CM. Therefore the maximum linksets available if all of the TCP/IP linksets are provisioned with two TCP/IP links will be 48.

CS2K will only provide one IP address for the Host to connect to it. Both links will use the same IP address to connect to the CS2K.

28.6 Interactions

This feature will interact with the existing SCAI X.25 transport due to enhancements made in the existing X.25 Table Control mechanism to support two TCP/IP links per linkset.

It will also interact with the current TCP/IP transport implementation that supports a single TCP/IP link per linkset.

28.7 Glossary

Term	Description
IP	Internet Protocol
TCP	Transmission Control Protocol
SCAI	Switch Computer Application Interface
TCP	Transmission Control Protocol

29: Functional Description (FN) A00009085

29.1 Feature name and Feature ID

A00009085: ACD & ICM Capacity Expansion

29.2 Description

Currently, the following limitations apply to the ACD and ICM capacities in a SL-100 or DMS-100 switch:

1. A maximum of 30,000 ACD Agents can be provisioned.
2. A maximum of 1,024 ACD Groups can be provisioned.
3. A maximum of 256 ACD Subgroups can be defined for a given ACD Group.
4. A maximum of 256 Supervisors can be defined for a given ACD Group.
5. A maximum of 1,024 ACD Agents can be associated with a given ACD Group.
6. A maximum of 511 calls can be simultaneously queued for a given ACD Group.
7. A maximum of 511 incoming overflowed calls can be simultaneously queued for a given ACD Group.
8. A maximum of 100 DNs can be associated with a given ICM Session.

This feature will expand these capacities to the following limits:

1. The maximum number of ACD Agents per switch will be increased to 99,999.
2. The maximum number of ACD Groups per switch will be increased to 5,000.
3. The maximum number of ACD Subgroups per Group will be increased to 2,500.
4. The maximum number of Supervisors per ACD Group will be increased to 2,500.
5. The maximum number of ACD Agents per Group will be increased to 10,000.
6. The maximum number of simultaneously queued calls per ACD group will be increased to 8,192.
7. The maximum number of simultaneously queued incoming overflowed calls per ACD Group will be increased to 8,192.
8. The maximum number of DNs that can be associated with a given ICM Session will be increased to 250.

29.3 Hardware Requirements or Dependencies

N/A

29.4 Software Requirements or Dependencies

This feature enhances the existing ACD and ICM software to provide the increased capacities. The following areas will be impacted by this feature:

- Table ACDGRP will be expanded to allow the provisioning of up to 5,000 ACD Groups per switch.
- Table ACDSGRP will be enhanced to allow provisioning of up to 2,500 ACD Subgroups per Group.
- Table ACDLOGIN will be expanded to hold a maximum of 99,999 tuples.
- Table ACDENLOG will be expanded to hold a maximum of 99,999 tuples per partition.
- SERVORD commands (NEW, ADO, NEWACD, CHF, etc.) will be enhanced to support position IDs up to 99999.
- A new ACDMIS protocol version (BCS57) will be defined to support the expanded login and position IDs.
- The ACDMIS load management/remote load management code will be enhanced to support the expanded login and position IDs.
- ACD and ICM Call Processing code will be enhanced to support the expanded login and position IDs.
- ACDDEBUG and ACDSHOW tools will be enhanced to support the expanded login and position IDs.
- Enhancements will be made to the ACD00101 SOC code to support the increase in the maximum number of ACD Agents per switch.

This feature also adds new code to provide the following SOCs to manage the various capacity increases:

- ACD00104 - to control the maximum number of ACD Groups per switch. This SOC will also control the maximum number of ACD Subgroups and Supervisors per Group.
- ACD00105 - to control the maximum number of ACD Agents per Group.
- ACD00106 - to control the maximum number of incoming and incoming overflowed calls per ACD Group.
- ICM00082 - to control the maximum number of DNs that can be associated per ICM Session.

29.5 Limitations and restrictions

It must be noted that all of the capacities described in this document can not be taken to the maximum simultaneously in a given switch.

29.6 Interactions

No changes are made to the existing interactions by this feature.

29.7 Glossary

Term	Description
ACD	Automatic Call Distribution
ACDMIS	ACD Management Information Systems
DMS	Digital Multiplex System
DN	Directory Number
ICM	Intelligent Call Management
SOC	Software Optionality Control

30: Functional Description (FN) A00009091

30.1 Feature name and Feature ID

SN09: A00009091 - Equal Access (EA) LPIC Privilege Routing

30.2 Introduction

This feature introduces two new capabilities to the SN09 release:

1. The capability to partition a DMS100/CS2000 into multiple Virtual End Offices (VEO) using a new translation attribute intended for public translation capabilities.
2. New LPIC Privilege Routing capability, which is the first functionality to make use of the new VEO partitioning.

Future releases may provide additional enhancements of public translation to utilize the new VEO partitioning capability.

30.3 Description

Two new capabilities are introduced by this feature. Please refer to the following sections for additional information:

- Section 30.3.1 “New Virtual End Office Capability” on page 253
- Section 30.3.2 “New LPIC Privilege Routing Functionality” on page 256

30.3.1 New Virtual End Office Capability

With this feature, a DMS100/CS2000 can be partitioned into two or more virtual end-offices. This provides a logical partitioning of originating agents on one DMS100/CS2000 into multiple VEOs.

Table VEONAME is introduced by this feature to provide an inventory of the VEO names. A VEO name is associated with valid “originating EO agent types” through new provisioning option VEONAME, in table XLAPLAN or table CXGRP.

The originating EO agent types that are supported by this activity include:

- All line types (e.g., RES, POTS, IBN, console) in the SN09 release except Line Class Codes (LCC) of *EOW* (Enhanced Outwats) and *ETW* (Enhanced Two-Way WATS).
- IBN trunks
- PRI trunks
- PX trunks (with exception of EWATS agents)

- virtual lines - RCF, RCFEA
- VFGs

VEO functionality is completely optional via provisioning in tables XLAPLAN and CXGRP.

For additional information please refer to the following sections:

- Section 30.3.1.1 “New Table VEONAME” on page 254
- Section 30.3.1.2 “New option VEONAME, Table XLAPLAN” on page 255
- Section 30.3.1.3 “New option VEONAME, Table CXGRP” on page 255

30.3.1.1 New Table VEONAME

New table VEONAME contains the list of VEO names. Each VEO name represents a virtual end office that is partitioned on the DMS100/CS2000.

Table VEONAME can provision up to a maximum of 999 VEO names, with an additional VEO name reserved as nil VEO name (NILV).

Refer to Table 1 for a Description of the key field of table VEONAME. The key field VEONAME is a string of up to 16 characters and is mapped to a string range.

Table 1 New Table VEONAME

Key	Values	Comments
Key: VEONAME	CHAR_VECTOR (16)	The table key specifies the Virtual End Office Name.

Following is a provisioning example for new table VEONAME.

Figure 1 Example of Table VEONAME

Table VEONAME:

```
VEONAME
--------------------
NILV
ENDOFFICE1
ENDOFFICE2
```

30.3.1.2 New option VEONAME, Table XLAPLAN

Table XLAPLAN provides an association between End Office (EO) originating agents and their translation types.

New option VEONAME is added to table XLAPLAN. Option VEONAME provides an association between the originating line/trunk agent and the Virtual End Office (VEO). This provides the flexibility to partition the DMS100/CS2000 into multiple virtual end offices.

Example datafill for table XLAPLAN is as follows.

Figure 2 Example datafill of Table XLAPLAN

```
Table XLAPLAN:

XLAPIDX  SCRNCLHSTS  PRTNMZEROMPOS RESINF  OPTIONS  ADMINF
-------------------------------------------------------------------------------------------
613_P621_0  FR01  613   P621  TSPS Y  RESGRP 0 2 VEONAME ENDOFFICE1   $
```

30.3.1.3 New option VEONAME, Table CXGRP

Table CXGRP (Customer Group Options) is required in local or combined local/toll switches to define the options associated with a PX digital trunk. The PX trunk agent tuple in table TRKGRP contains the field for PX Customer Group which is the index into table CXGRP.

New option VEONAME is added to table CXGRP. Option VEONAME provides an association between the originating PX trunk agent and the Virtual End Office (VEO). This provides the flexibility to partition the DMS100/CS2000 into multiple virtual end offices.

Note: Table CXGRP does not show up in Traver. See Figure 12.

Example datafill for table CXGRP is as follows:

Figure 3 Example datafill of Table CXGRP

```
Table CXGRP:

CUSTKEY SPB CTD FCTDNTER FCTDNTRA FCTDINT EWATS EWATSI
PXOPTION
-----------------------------------------------------------------------------------------------
50 N N N N N N N (LPIC CAR1 Y) ( VEONAME ENDOFFICE2 ) $
```

30.3.2 New LPIC Privilege Routing Functionality

The second capability introduced by this activity is LPIC Privilege Routing. When an LPIC is assigned to an originator, the DMS100/CS2000's behavior prior to this feature was to route all intraLATA toll calls to the LPIC. This feature introduces the ability to provision intraLATA toll NPANXX codes as exceptions to LPIC handling. Instead of routing to the LPIC, these NPANXX codes will be handled by the LEC.

A new table LPICPXLA is introduced to allow NPANXX LPIC privilege codes to be provisioned on a per VEO basis. New SOC EQA00032 is also introduced as a call processing and Traver control for the LPIC Privilege Routing capability.

For additional information please refer to the following sections:

- Section 30.3.2.1 "New Table LPICPXLA" on page 256
- Section 30.3.2.2 "New SOC EQA00032" on page 258
- Section 30.3.2.3 "Call Processing Enhancements" on page 259
- Section 30.3.2.4 "Traver Enhancements" on page 262
- Section 30.3.2.5 "Service Interactions with LPIC Privilege Routing" on page 271

30.3.2.1 New Table LPICPXLA

New table LPICPXLA is implemented to provision a list of NPANXX codes to be excluded from LPIC routing on per VEO basis. This table will be implemented using digilators for storing the NPNXX Codes and will be using 1 digilator pool of 32k 1-digits blocks.

Table LPICPXLA is accessed during call processing for an originating agent when the following is provisioned:

- VEONAME is provisioned in table VEONAME,

- table XLAPLAN entry for the originating agent's pretranslator has option VEONAME assigned (or for a PX trunk originator, option VEONAME is assigned in table CXGRP),
- and SOC EQA00032 'VEO LPIC Privilege' is turned ON.

Refer to Table 2 for a Description of table LPICPXLA. The key field PRIVCODE is made up of two parts:

- VEONM: Virtual End Office Name provisioned in Table VEONAME

- DIGITS: up to six NPANXX digits from the dialled number.

Table control enforcements:

— a VEONAME tuple can not be provisioned as nil VEO name (NILV),

— upto six-digit NPANXX codes are allowed to be provisioned as privilege codes in Table LPICPXLA.

Table 2 New Table LPICPXLA

Key	Values	Comments
Key 1: VEONM	VEO_NAME (String range 0 to 999)	Key 1 specifies the originating subscriber's Virtual End Office Name.
Key 2: DIGITS	DIGIT_REGISTER	Key 2 specifies NPANXX codes provisioned for each VEONAME.

Following is a provisioning example for new table LPICPXLA.

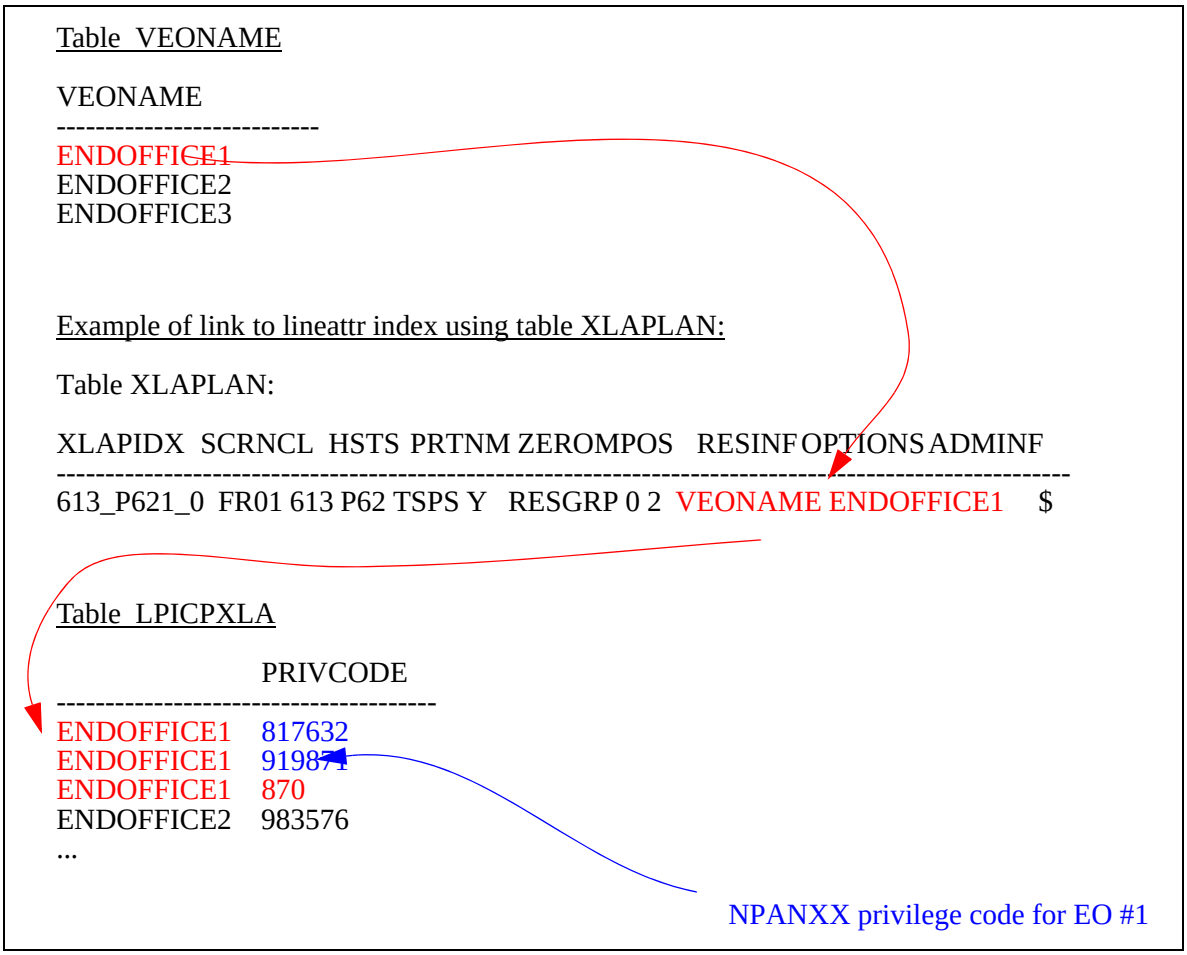
Figure 4 Example of Table LPICPXLA

Table LPICPXLA:

```
                PRIVCODE
----------------------------------
ENDOFFICE1      919484
ENDOFFICE2      212
```

The following figure illustrates the association between tables VEONAME, XLAPLAN, and LPICPXLA. For additional information please refer to Section 30.3.2.3 "Call Processing Enhancements" on page 259.

Figure 5 LPIC Exception Routing Datafill



30.3.2.2 New SOC EQA00032

A new state controlled SOC, EQA00032 ‘VEO LPIC Privilege’ is added by this activity. The SOC will have two states: IDLE, ON. This SOC, along with the assignment of the VEONAME option for the originating agent, controls both the call processing and Traver enhancements provided by this activity.

When SOC is in IDLE state:

- Table VEONAME can be provisioned.
- The new option VEONAME can be provisioned in table XLAPLAN and table CXGRP.
- The new option VEONAME can be provisioned in table LPICPXLA with NPANXX privilege codes.
- Table LPICPXLA is not accessed by call processing or by Traver. For further detail, refer to Section 30.3.2.3 “Call Processing

Enhancements” on page 259, and Section 30.3.2.4 “Traver Enhancements” on page 262.

When SOC is in ON state:

— Call processing and Traver will both access new table LPICPXLA if the originating agent has VEONAME assigned.

The functional group ordering code for EQA00032 is EQA00001, EQA Local.

All service interactions with SOC EQA00032, including EQA00024 ‘Override LPIC Priv’ feature, are described in Section 30.3.2.5 “Service Interactions with LPIC Privilege Routing” on page 271.

30.3.2.3 Call Processing Enhancements

The DMS100/CS2000 call processing software is enhanced to support the LPIC Privilege Routing capability. Figures 6 and 7 provide flowcharts of the enhanced call processing behavior. This feature is active only when SOC EQA000032 is set to ON and the originator has a VEONAME assigned.

Supplemental Information for the flowcharts.

1. Deriving LATA status of the call - There are no changes to the method of deriving the LATA status from Table LATAXLA. Existing behavior is to index Table LATAXLA with the originator’s LATA name and the dialed number. If the dialed number is a 7 digit dialplan then originator’s LATA name and the SERVING NPA[1](SNPA) plus the dialed number are used for the index into Table LATAXLA. Special considerations are required for some services. Please refer to Section 30.3.2.5 “Service Interactions with LPIC Privilege Routing” on page 271, for more details.
2. Performing Look-up in Table LPICPXLA - The index for the new Table LPICPXLA is the originator’s VEONAME and the terminating number. If the terminating number does not contain enough digits to determine if a match is found then more digits must be collected. As with Table LATAXLA, if the dialed number is a 7 digit dialplan then originator’s VEONAME and the SNPA with the dialed digits are used for the index into Table LPICPXLA. Special considerations are required for some services. Please refer to Section 30.3.2.5 “Service Interactions with LPIC Privilege Routing” on page 271 for more details.

[1]Serving NPA is the NPA of the originating party.

Figure 6 Equal Access Translations

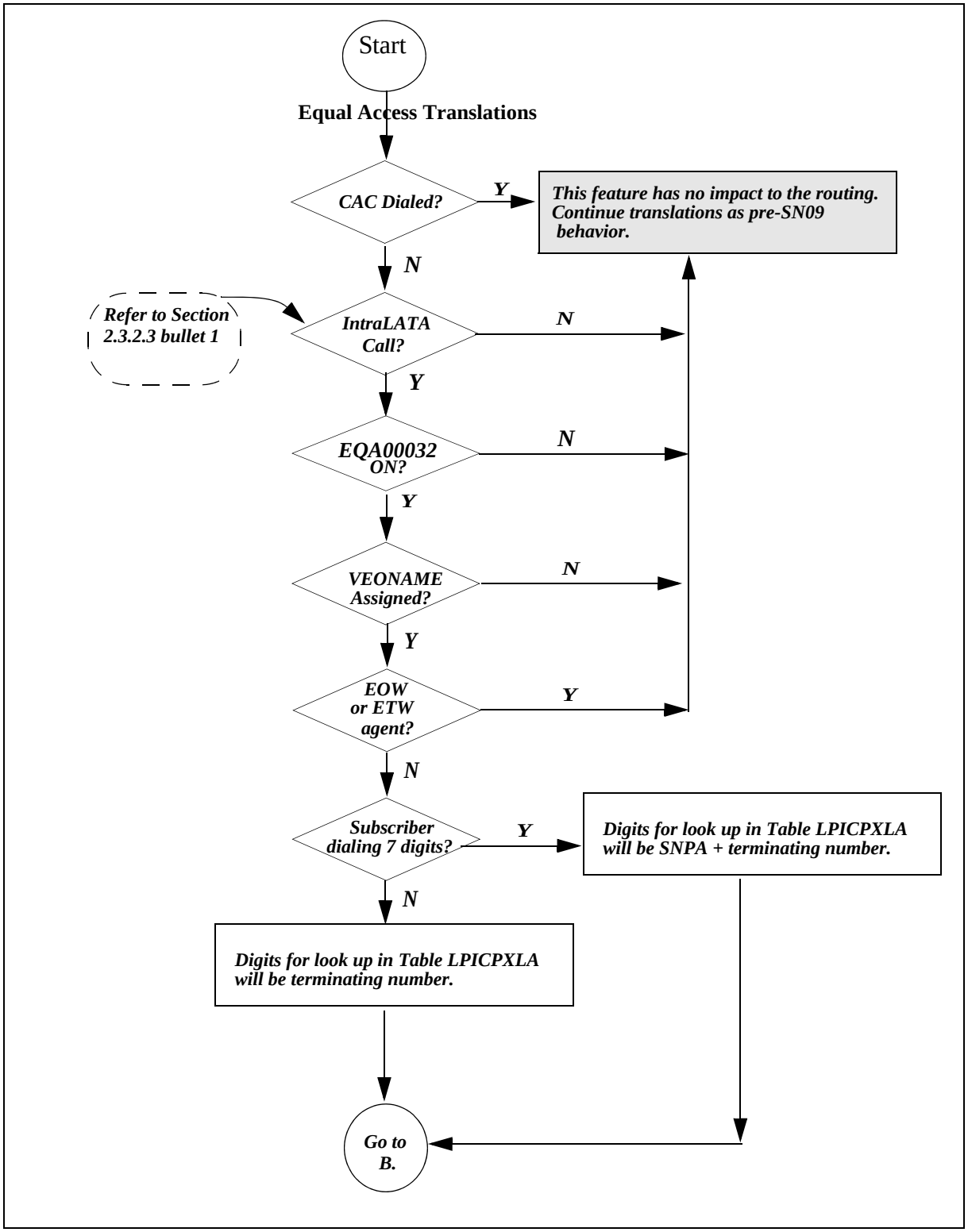
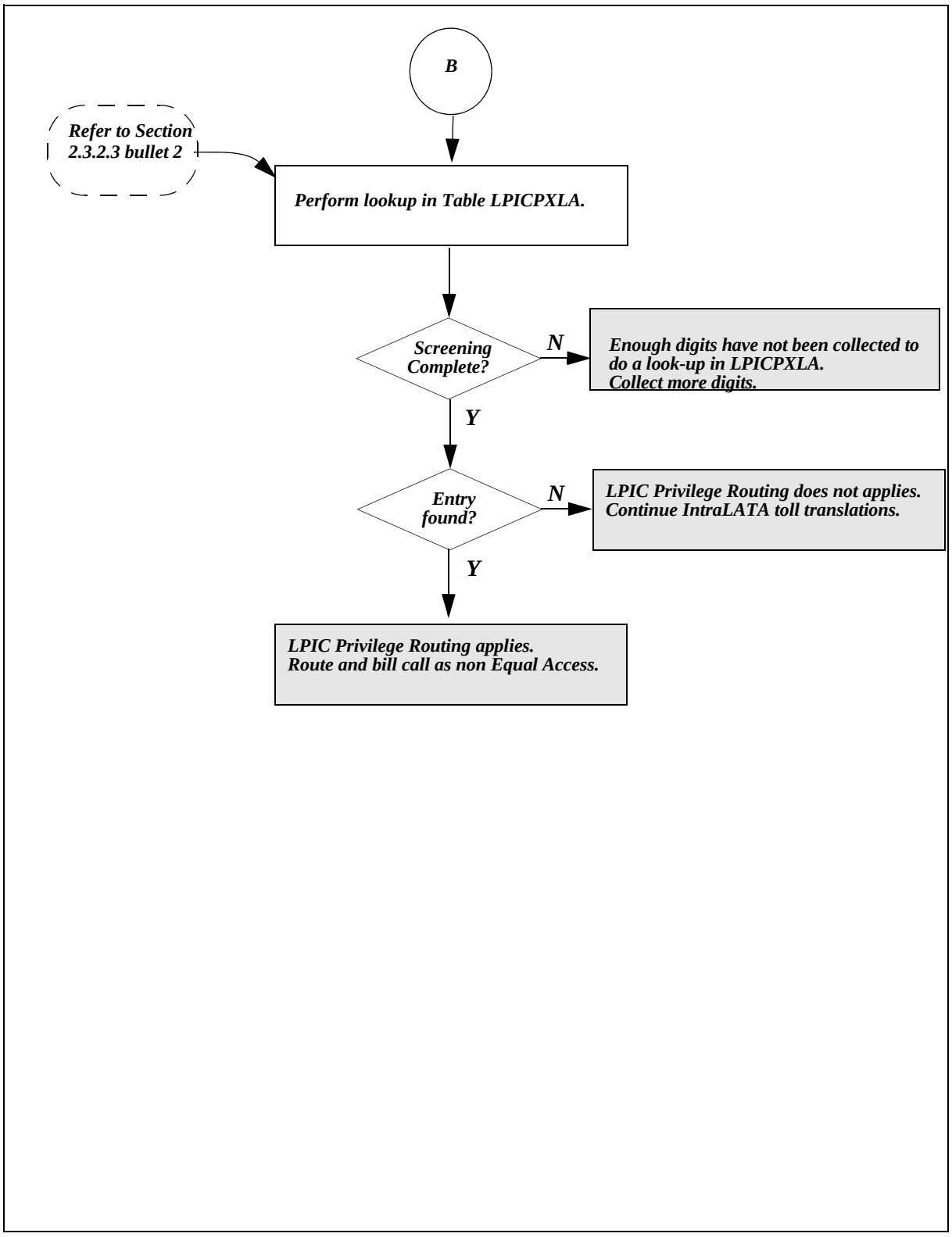


Figure 7 Continued - Equal Access Translations



30.3.2.4 Traver Enhancements

The DMS100/CS2000 EO Traver software is enhanced to support the display of new option VEONAME and to display the contents of new table LPICPXLA. The Traver enhancements are active only when SOC EQA00032 is set to ON and option VEONAME is provisioned for the originator. The following chart describes the Traver impact for the different combinations. Figures 8 through 11 are examples of the modified Traver output.

Table 3 Traver Impact

SOC State	VEONAME Assigned	LPICPXLA entry found?	Traver Impact
IDLE	No	N/A	There will be no new messages in the traver output.
IDLE	Yes	No	There will be no new messages in the traver output.
IDLE	Yes	Yes	There will be no new messages in the traver output.
ON	No	N/A	There will be no new messages in the traver output.
ON	Yes	No	New Message after displaying Table LATAXLA data: **'TABLE LPICPXLA** **TUPLE NOT FOUND '**
ON	Yes	Yes	New Message after displaying Table LATAXLA data: **'TABLE LPICPXLA** **VEO1 919528** ... **OPERATING TELCO WILL HANDLE THIS CALL'**

Figure 8 EQA00032 is ON & LPICPXLA datafilled

```
traver l 5206000 19195282112 b
TABLE LINEATTR
0 1FR NONE NT 0 0 NILSFC 0 NIL NIL 00 619_POT1_0 LPOT_L123_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
619_POT1_0 NSCR 619 POT1 RTE1 Y RES1 0 0 VEONAME VEO2$ $
TABLE RATEAREA
LPOT_L123_0 LPOT NIL L123 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE LENFEAT
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
AIN Orig Attempt TDP: no subscribed trigger.
TABLE STDPRTCT
POT1 ( 1) ( 1) 7
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . 1919 199 N DD 1 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE HNPACONT
619 Y 919 8 ( 114) ( 1) ( 0) ( 0) 1 $
 . SUBTABLE HNPACODE
 . 919 919 FRTE 919
 . SUBTABLE RTEREF
 .  919 N D ISUPIT4DIG 0 N N
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
LNP Info: Called DN is not resident.
LNP Info: HNPA results are used.
TABLE LCASCRCN
619 LPOT ( 29) OPTL N N Y
 . SUBTABLE LCASCRN
 . TUPLE NOT FOUND.  DEFAULT IS NON-LOCAL
TABLE PFXTREAT
OPTL DD N DD UNDT
TABLE LENFEAT
HOST 04 0 00 17 S LPIC LPIC CAR1 Y
TABLE LENFEAT
HOST 04 0 00 17 S PIC PIC CAR2 Y

<continued>
```

Figure 9 EQA00032 is ON & LPICPXLA datafilled

```
<continued>
TABLE LATAXLA
TUPLE NOT FOUND
ASSUMED TO BE DEFAULT INTRALATA, INTRASTATE, STD
TABLE LPICPXLA
VEO1 919528
TABLE OCCINFO
CAR1 6900 EAP Y Y Y Y Y N N  Y Y Y Y LONG 0 FGRPC Y N Y N N N N N N N N N N Y
TABLE EASAC
TUPLE NOT FOUND
OPERATING TELCO WILL HANDLE THIS CALL
AIN Info Collected TDP: no subscribed trigger.
AIN Info Analyzed TDP: no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 ISUPIT4DIG              9195282112                ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 ATB

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

Figure 10 EQA00032 is ON & LPICPXLA not datafilled

```
traver l 5206000 19195282112 b
TABLE LINEATTR
0 1FR NONE NT 0 0 NILSFC 0 NIL NIL 00 619_POT1_0 LPOT_L123_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
619_POT1_0 NSCR 619 POT1 RTE1 Y RES1 0 0 VEONAME VEO2$ $
TABLE RATEAREA
LPOT_L123_0 LPOT NIL L123 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE LENFEAT
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
AIN Orig Attempt TDP: no subscribed trigger.
TABLE STDPRTCT
POT1 ( 1) ( 1) 7
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . 1919 199 N DD 1 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE HNPACONT
619 Y 919 8 ( 114) ( 1) ( 0) ( 0) 1 $
 . SUBTABLE HNPACODE
 . 919 919 FRTE 919
 . SUBTABLE RTEREF
 .  919 N D ISUPIT4DIG 0 N N
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
LNP Info: Called DN is not resident.
LNP Info: HNPA results are used.
TABLE LCASCRCN
619 LPOT ( 29) OPTL N N Y
 . SUBTABLE LCASCRN
 . TUPLE NOT FOUND.  DEFAULT IS NON-LOCAL
TABLE PFXTREAT
OPTL DD N DD UNDT
TABLE LENFEAT
HOST 04 0 00 17 S LPIC LPIC CAR1 Y
TABLE LENFEAT
HOST 04 0 00 17 S PIC PIC CAR2 Y

<continued>
```

Figure 11 EQA00032 is ON & LPICPXLA not datafilled - continued

```
<continued>
TABLE LATAXLA
TUPLE NOT FOUND
ASSUMED TO BE DEFAULT INTRALATA, INTRASTATE, STD
TABLE LPICPXLA
TUPLE NOT FOUND
TABLE OCCINFO
CAR1 6900 EAP Y Y Y Y Y N N Y Y Y Y LONG 0 FGRPC Y N Y N N N N N N N N N N Y
TABLE EASAC
TUPLE NOT FOUND
OVERLAP CARRIER SELECTION (OCS) APPLIES
TABLE STDPRTCT
POT1 ( 1) ( 1) 7
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . 1016900 1016900 EA DD 7 P PCAR1 CAR1 Y OFRT 908 8 25 Y
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
 . . TABLE OFRT
 . .  908 CND EA INTNL SK 3
 . .     N D EATANDEMOG 15 D069 N
 . .     N D ISUPIT4DIG 15 D069 N
 . .     CND ALWAYS SK 2
 . .     N D EATANDEMOG 15 D169 N
 . .     N D ISUPIT4DIG 15 D169 N
 . . EXIT TABLE OFRT
 . TABLE STDPRTCT
 . PCAR1 ( 1) ( 0) 6
 . . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
  . . 19 19 EA DD 1 T NA CAR1 N
.TABLE HPCPATTN
TUPLE NOT FOUND
AIN Info Collected TDP: no subscribed trigger.
AIN Info Analyzed TDP: no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 EATANDEMOG          D069                  ST
2 ISUPIT4DIG           D069                  ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 ATB

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

Figure 12 PX trunks: EQA00032 is ON & LPICPXLA datafilled

EXAMPLE of PX trunk datafilled with LPIC and VEONAME in table CXGRP. Note that table CXGRP does not show up in traver.

Table CXGRP:
CUSTKEY SPB CTD FCTDNTER FCTDNTRA FCTDINT EWATS EWATSI PXOPTION
---
52 N N N N N N N **(LPIC CAR1 Y) (VEONAME VEO1)** $

> traver tr carypx 5414402502 b
TABLE TRKGRP
CARYPX PX 10 ELO NCRT IC NIL MIDL N P621 PBX1 613 613 LCL NONE TSPS L613 N N **52**
NIL 6211234 DIALTN N Y CAR2 Y LATA1 N $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE STDPRTCT
P621 (1) (0) 1
. SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO
DOCUMENTATION.
. 54 60 N NP 0 NA
. SUBTABLE AMAPRT
. KEY NOT FOUND
. DEFAULT VALUE IS: NONE OVRNONE N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE HNPACONT
613 Y 915 2 (85) (1) (0) (0) 2 $
. SUBTABLE HNPACODE
. 541 541 FRTE 541
. SUBTABLE RTEREF
. 541 N D 2WEAIT 3 276 N
. EXIT TABLE RTEREF
EXIT TABLE HNPACONT
LNP Info: Called DN is not resident.
LNP Info: HNPA results are used.
TABLE LCASCRCN
613 L613 (56) OPTL N N Y
. SUBTABLE LCASCR
. TUPLE NOT FOUND. DEFAULT IS NON-LOCAL
TABLE PFXTREAT
OPTL NP N DD UNDT
TABLE CLSVSCRC
KEY NOT FOUND
TABLE LATAXLA
TUPLE NOT FOUND
ASSUMED TO BE DEFAULT INTRALATA, INTRASTATE, STD
TABLE LPICPXLA
VEO1 541
TABLE OCCINFO
CAR1 6524 EAP Y Y Y Y Y N N Y N Y Y LONG 0 FGRPD N N N N Y N N N N Y N Y N N Y

<continued>

Figure 13 PX trunks: EQA00032 is ON & LPICPXLA datafilled - continued

<continued>

```
TABLE EASAC
TUPLE NOT FOUND
OPERATING TELCO WILL HANDLE THIS CALL
TABLE OFCVAR
AIN_OFFICE_TRIGGRP LNPOFFICE
AIN Info Collected TDP: no subscribed trigger.
TABLE TRIGGRP
LNPOFFICE INFOANAL
 . PODP ( DG PODPDIG)$ NIL
Trigger AIN PODP is applicable to office.
 . LNP ( DG LNPDIG) ( ESCEA ) ( ESCOP ) ( ESCDN ) ( ESCCN DD)$ NIL
Trigger AIN LNP is applicable to office.
AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 2WEAIT

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 T120

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Figure 14 PX trunks: EQA00032 is ON & LPICPXLA not datafilled

EXAMPLE of PX trunk datafilled with LPIC and VEONAME in table CXGRP. Note that table CXGRP does not show up in traver.

Table CXGRP:
CUSTKEY SPB CTD FCTDNTER FCTDNTRA FCTDINT EWATS EWATSI PXOPTION
---
52 N N N N N N N **(LPIC CAR1 Y) (VEONAME VEO1)** $

> traver tr carypx 5414402502 b
TABLE TRKGRP
CARYPX PX 10 ELO NCRT IC NIL MIDL N P621 PBX1 613 613 LCL NONE TSPS L613 N N **52**
NIL 6211234 DIALTN N Y CAR2 Y LATA1 N $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE STDPRTCT
P621 (1) (0) 1
. SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO
DOCUMENTATION.
. 54 60 N NP 0 NA
. SUBTABLE AMAPRT
. KEY NOT FOUND
. DEFAULT VALUE IS: NONE OVRNONE N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE HNPACONT
613 Y 915 2 (85) (1) (0) (0) 2 $
. SUBTABLE HNPACODE
. 541 541 FRTE 541
. SUBTABLE RTEREF
. 541 N D 2WEAIT 3 276 N
. EXIT TABLE RTEREF
EXIT TABLE HNPACONT
LNP Info: Called DN is not resident.
LNP Info: HNPA results are used.
TABLE LCASCRCN
613 L613 (56) OPTL N N Y
. SUBTABLE LCASCR
. TUPLE NOT FOUND. DEFAULT IS NON-LOCAL
TABLE PFXTREAT
OPTL NP N DD UNDT
TABLE CLSVSCRC
KEY NOT FOUND
TABLE LATAXLA
TUPLE NOT FOUND
ASSUMED TO BE DEFAULT INTRALATA, INTRASTATE, STD
TABLE LPICPXLA
TUPLE NOT FOUND
TABLE OCCINFO
CAR1 6524 EAP Y Y Y Y Y N N Y N Y Y LONG 0 FGRPD N N N N Y N N N N Y N Y N N Y

<continued>

Figure 15 PX trunks: EQA00032 is ON & LPICPXLA not datafilled - continued

<continued>

```
TABLE EASAC
TUPLE NOT FOUND
 TABLE STDPRTCT
P621 ( 1) ( 0) 1
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . 1016524 1016524 EA DD 7 P P524 CAR1 Y OFRT 889 3 20 Y
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
 . . TABLE OFRT
 . .  889 CND EA INTNL SK 3
 . .      S D OGEACAR1
 . .      S D ISUP2WCAR1
 . .      CND ALWAYS SK 2
 . .      N D OGEACAR1 15 D121 N
 . .      N D ISUP2WCAR1 0 D121 N
 . . EXIT TABLE OFRT
 . TABLE STDPRTCT
 . P524 ( 1) ( 0) 4
 . . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . . 5 9 EA DD 0 T NA C524 N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP LNPOFFICE
AIN Info Collected TDP: no subscribed trigger.
TABLE TRIGGRP
LNPOFFICE INFOANAL
 . PODP ( DG PODPDIG)$ NIL
Trigger AIN PODP is applicable to office.
 . LNP ( DG LNPDIG) ( ESCEA ) ( ESCOP ) ( ESCDN ) ( ESCCN DD)$ NIL
Trigger AIN LNP is applicable to office.
AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 OGEACAR1          5414402502          ST
2 ISUP2WCAR1        5414402502          ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 T120

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

30.3.2.5 Service Interactions with LPIC Privilege Routing

30.3.2.5.1 Interactions with Existing EA Translation Capabilities

The interactions between existing EA LPIC translation capabilities and the LPIC Privilege Routing are addressed below.

0+ Local Routing:

SOC EQA00015[1], "IntraLATA PIC Enhancements Phase 1," provides the flexibility to route 0+ local calls to the LEC, the subscriber's LPIC, or a designated carrier. Office parameter ZERO_PLUS_LOCAL_CARRIER in combination with SOC EQA00015 controls the switch behavior. If the 0+ local capability determines the call will route to the carrier provisioned for parameter ZERO_PLUS_LOCAL_CARRIER or to the LPIC, the call is handled as an LPIC toll call.

The LPIC Privilege Routing capability introduced by this activity adheres to the same behavior, and performs screening for the called NPANXX in table LPICPXLA when SOC EQA00032 is ON and the originator has the VEONAME option assigned. If the LPIC Privilege Routing applies, the call will route to the LEC as a non-EA call.

If SOC EQA00015 is OFF, the call will route to the LEC as a non-EA call (this behavior is unchanged by the functionality of this activity).

If NILC or USE_PREVIOUS is provisioned for parameter ZERO_PLUS_LCL_CARRIER, the call will route to the LEC as a non-EA call (this behavior is unchanged by this activity).

1+ Coin IntraLATA Routing Flexibility:

SOC EQA00015, "IntraLATA PIC Enhancements Phase 1," in combination with field INTRCOIN in table OCCINFO provides the ability to route 1+intraLATA toll *coin* originations to either the LEC, the subscriber's LPIC, or a designated carrier. If the coin 1+intraLATA toll capability determines the call will route to the carrier provisioned for INTRCOIN or to the LPIC, the call is handled as an LPIC toll call.

The LPIC Privilege Routing capability introduced by this activity adheres to this behavior and performs screening for the called NPANXX in table LPICPXLA when SOC EQA00032 is ON and the originator has the VEONAME option assigned. If LPIC Privilege Routing applies, the call will route to the LEC as a non-EA call.

If 'Y NILC' is provisioned for field INTRCOIN, the call will route to the LEC as a non-EA call (this behavior is unchanged by this activity).

If SOC EQA00015 is OFF, the call is handled as an LPIC toll call. The LPIC Privilege Routing capability introduced by this activity adheres to

[1]Introduced by feature AN1811.

this behavior and performs screening for the called NPANXX in table LPICPXLA when SOC EQA00032 is ON and the originator has the VEONAME option assigned. If the LPIC Privilege Routing applies, the call will route to the LEC as a non-EA call.

LATAXLA LPIC Privilege:

SOC EQA00024[1], "Override LPIC Privilege," provides the ability to mark intraLATA codes as privilege on a per LATA basis via table LATAXLA. When EQA00024 is ON, LPIC calls are handled by the LEC for those codes that are provisioned as privilege in table LATAXLA.

The LPIC Privilege Routing capability introduced by this activity provides the same capability as EQA00024, but on a per VEO basis. EQA00032 and EQA00024 are independent of each other. The LPIC Privilege Routing capability takes precedence when SOC EQA00032 is ON and VEONAME is provisioned on the originating agent. If the originator does not have VEONAME provisioned or SOC EQA00032 is IDLE, the new LPIC Privilege Routing capability does not apply. In this case SOC EQA00024 continues to be used to provide intraLATA privilege routing.

Table LATAXLA NON_EA Datafill:

Table LATAXLA allows NPA/NPANXX codes to be provisioned as a NON_EA calltype. If NON_EA calltypes, the call routes as a non-EA call. Casual access dialing to NON_EA codes is not permitted. This behavior takes precedence over the LPIC Privilege Routing feature. If the dialed number (NPA or NPANXX) is provisioned as NON_EA in table LATAXLA, the call will be routed as a non-EA call. In this case, table LPICPXLA is not referenced.

Alternate Service Provider:

An alternate service provider can be specified for any of the following services:

In-Session Activation (ISA): AQ1700

Special Delivery Service (SDS): AQ1335

Universal Voice Messaging (UVM): AQ1303

Virtual Call Framework (VCF): AJ4936

Who's Calling (WC): A59012655

These services specifically request an alternate carrier be used to complete the call.

With pre-SN09 behavior, privilege routing takes precedence over the alternate carrier. If table LATAXLA is provisioned as privilege, the call is handled by the LEC regardless of whether an alternate carrier is provided

[1]Introduced by feature AN1811.

by the service. This applies to both “Override LPIC Privilege” (SOC EQA00024), and interLATA privilege in table LATAXLA.

The LPIC Privilege Routing capability introduced by this feature is consistent with this behavior and takes precedence over alternate carrier. Screening will be performed for intraLATA toll NPANXX codes in table LPICPXLA when SOC EQA00032 is ON and the originator has the VEONAME option assigned. If LPIC privilege routing applies, the call will route to the LEC as a non-EA call.

30.3.2.5.2 Advanced Intelligent Networks (AIN)

This feature also interacts with AIN response translations. When AIN database response returns an intraLATA routing number, SOC EQA00032 is active, and VEONAME is associated, the new Table LPICPXLA is accessed to determine if LPIC privilege applies.

The routing number is always used as part of the index into LPICPXLA. The other part of the index is the VEONAME, which is retrieved as discussed below:

- When AIN response translation routes through a VFG the existing behavior is to retrieve the LATA name associated with the subscriber, and not the VFG. The LPIC feature is consistent with this behavior. The VEONAME is retrieved from the subscriber for intraLATA calls when the LPIC SOC EQA00032 is active. In these cases the LPICPXLA will be indexed using the subscriber’s VEONAME and the routing number returned in the AIN DB response.
- Using AIN it is possible to alter the translation through table XLAMAP and table PXLAMAP. Either the pretranslator name or the LINEATTR index can be altered. In this case deriving the VEONAME is dependent on whether the AIN translation specifies a new pretranslator name or a new LINEATTR index:
  - — If the AIN translation specifies a new pretranslator name, the VEONAME is derived from the subscriber.
  - — If the AIN translation specifies a new LINEATTR index, the VEONAME is derived based on the XLAPLAN associated to the new LINEATTR.
- The use of the LARP capability provides a method to override various translation attributes for the AIN response translation via option LARP in Table TRIGITM. These translation attributes include LINEATTR, XLAPLAN, and RATEAREA indices. LARP TRAVER option[1] and call processing derives the LATANAME associated with the LARP datafill in Table TRIGITM. This feature will adhere to this behavior and derive the

[1] Introduced by feature A59022554.

VEONAME associated with the XLAPLAN index provisioned in table TRIGITM.

- All other cases derive the VEONAME from the originating agent.

30.3.2.5.3 Local Number Portability (LNP)

LNP calls perform translations twice. The first one is referred to as the pre-query translation which occurs prior to the sending the query to the LNP database. The second one is referred to as the post-query translation which occurs after the receipt of the LNP database response.

If SOC NPE00005[1], "1000 Blk Nbr Pooling," is ON, the LPIC Privilege Routing capability introduced by this activity will use the LATAXLA results from the pre-query translation. Specifically, if the pre-query LATAXLA result determines the call is intraLATA, the LPIC privilege capability performs a lookup in table LPICPXLA if LPIC SOC EQA00032 is ON and the VEONAME is assigned to the originator. The ported DN is used for the look-up in table LPICPXLA.

IF NPE00005 is IDLE, the LPIC Privilege Routing capability uses the LATAXLA results from the post-query translation. Specifically, if the post-query LATAXLA result determines the call is intraLATA, the LPIC Privilege Routing capability performs a lookup in table LPICPXLA if the LPIC Privilege Routing SOC is ON and the VEONAME is assigned to the originator. The ported DN is used for the look-up in table LPICPXLA.

The LNP TRAVER option LNPAR provides the ability to simulate an SCP response containing an FLRN, HLRN, or ported DN. The LPIC Privilege Routing capability introduced by this activity requires the use of option LNPAR to correctly display the contents of table LPICPXLA. VEONAME is derived the same for TRAVER as with call processing but the NPANXX used to access LPICPXLA is derived differently. Specifically, the LNPAR option contains the ported DN which is used as the other part of the key to Table LPICPXLA. Thus, TRAVER is consistent with call processing.

The syntax for the LNPAR option is as follows:

TRAVER L 6215000 N CDN NA <routing #> AINRES R01 LNPAR <ported DN> B

Where an LRN or the ported DN can be entered as the <routing #> and a 10 digit DN or 'N' can be entered for <ported DN>.

[1]Introduced by activity A59012192.

30.3.2.5.4 In-Session Activation (ISA)

In-Session Activation (ISA)[1] is an originating line service that is activated when the originator places a call and the called party is either busy or a ringing timeout occurs. When either of these two conditions occur, the switch software performs *called party screening* to determine whether to offer the ISA service. The *called party screening* function looks at various call characteristics to determine whether to activate ISA. With pre-SN09 behavior, if the call is provisioned as privilege in table LATAXLA, the ISA service is offered. This applies to both intraLATA and interLATA privilege in table LATAXLA. The LPIC Privilege Routing capability will be consistent with this behavior and ISA service will be offered for intraLATA calls if SOC EQA00032 is ON, the originator has the VEONAME option assigned, and the NPANXX code is provisioned in table LPICPXLA. If the service redirects the call to a new number, LPIC Privilege Routing capability may apply.

30.3.2.5.5 Special Delivery Service (SDS)

Special Delivery Service (SDS)[2] is a feature that provides the originating line with the option to invoke message delivery when the called party is busy or does not answer within an office-defined interval. When either of these two conditions occur, the originating line is connected to a Voice Messaging System (VMS) either directly via an SMDI link or indirectly via an outgoing ISUP trunk.

Prior to terminating to VMS, the SDS features performs *call characteristics screening* to determine whether to offer the SDS service. The *call characteristics screening* function looks at various call characteristics to determine whether to activate SDS. With pre-SN09 behavior, if the call is provisioned as intraLATA privilege in table LATAXLA, the SDS service is offered. The LPIC Privilege Routing capability will be consistent with this behavior. The SDS service will be offered for intraLATA calls if the LPIC SOC EQA00032 is ON, the originator has the VEONAME option assigned and the NPANXX code is provisioned in table LPICPXLA. If the service redirects the call to a new number, LPIC Privilege Routing capability may apply.

30.3.2.5.6 Call Forwarding (CFW) Interactions

Call ForWarding (CFW) allows a subscriber to redirect a call to a new number. The LPIC feature interacts with CFW since it is possible to redirect a call to an IntraLATA number. For intraLATA calls LPIC privilege routing applies if the LPIC SOC EQA00032 is ON, the redirecting agent has the VEONAME option assigned, and the NPANXX code of the forwarding number is provisioned in table LPICPXLA.

[1]Introduced by activity AQ1700.

[2]Introduced by activity AQ1335.

30.3.2.5.7 IntraLATA Full Carrier Toll Denied (FCTDNTRA)

Subscribers may have option FCTDNTRA assigned to their phone. This option functionality is controlled by SOC EQA00015[1]. Subscribers assigned this option are either prohibited from making toll calls using any carrier, or are allowed to have access to a limited number of carriers. Since calls being handled by LPIC Privilege Routing feature will be terminated by the LEC, the FCTDNTRA functionality does not block the call.

30.3.2.5.8 Toll DeNied (TDN)

Subscribers may have the option Toll DeNied (TDN) assigned to their phone. This option restricts an originator from making toll calls. Since the privilege codes for LPIC Privilege Routing are treated as toll codes, originating agents with TDN shall be blocked from accessing privilege codes.

30.4 Hardware Requirements or Dependencies

Not applicable

30.5 Software Requirements or Dependencies

Not applicable

30.6 Limitations and restrictions

The following limitations and restrictions apply to Virtual End Office (VEO) partitioning capability:

- VEO capability is not supported by DMS200. It is only supported by DMS100/CS2000.
- VEO is only for public translations capabilities.
- VEONAME option can not be assigned in Table XLAPLAN or Table CXGRP with VEO name of NILV (NIL VEO name).
- Maximum 999 VEOs are supported.

The following limitations and restrictions apply to the LPIC Privilege Routing functionality:

- EOW (Enhanced Outwats) and ETW (Enhanced Two-Way WATS) originating agents are not supported.
- MDC EWATS which was introduced by feature AF1664 and AF7559 is not supported.
- CALEA is not supported.
- Up to six-digit (NPANXX) codes are allowed to be provisioned as privilege codes in table LPICPXLA.

[1]Introduced by activity AN1811.

- The maximum size of table LPICPXLA will be determined by the digits pattern used in the table LPICPXLA, and the total number of VEO names provisioned in table VEONAME.
- P2 trunks are not supported.
- AIN local trunk capability[1] allows a call to reroute to a carrier when incoming on local trunks (i.e. TI, T2, IT, ATC). AIN local trunk capability is not supported by this feature.
- Packet (X.25, X.75) translations are not supported.
- This feature is not supported on non-conforming end offices.

30.7 Interactions

Refer to Section 30.3.2.5 “Service Interactions with LPIC Privilege Routing” on page 271.

30.8 Glossary

Term	Description
AIN	Advanced Intelligent Network
CAC	Carrier Access Code
CALEA	Communications Assistance for Law Enforcement Act
CFW	Call Forwarding
EA	Equal Access
EO	End Office
EOW	Enhanced OutWats
ETW	Enhanced Two-Way WATS
FLRN	Foreign Location Routing Number
HLRN	Home Location Routing Number
ISA	In-Session Activation
LARP	Line Attribute Response Processing
LATA	Local Access and Transport Area
LCC	Line Class Code
LEC	Local Exchange Carrier
LNP	Local Number Portability

[1]Introduced by feature AJ3999.

Term	Description
LNPAR	LNP Analyze Route
LPIC	intraLata Primary Interexchange Carrier
MDC	Meridian Digital Centrex
NPA	Numbering Plan Area
SCP	Service Control Point
SDS	Special Delivery Service
SNPA	Serving Numbering Plan Area
SOC	Software Optionality Control
TDN	Toll Denied
UVM	Universal Voice Messaging
VCF	Virtual Call Framework
VEO	Virtual End Office
WC	Who’s Calling

30.9 References

1. Feature AN1811, IntraLATA PIC Enhancements, Phase 1

2. Feature AJ3999, AIN 0.1 FGC-FGD Interworking

3. Feature AQ1700, IN-SESSION ACTIVATION

4. Feature AQ1335, Special Delivery Services (SDS)

5. Feature A59022554, AIN:Line Attributes for PFC/TRAVER Support

6. Feature AQ1303, Universal Voice Messaging

7. Feature AJ4936, Virtual Call Framework

8. Feature A59012655, Who’s Calling

31: Functional Description (FN) A00009092

31.1 Feature name and Feature ID

A0009092: CS2K MSM SIP Lines Cisco 7960 Client

31.2 Description

This feature covers the integration of the Cisco 7960 SIP-enabled IP Phone with the CS2000 MSM SIP Lines program. This document details the functional requirements for the phone and CS2000 MSM 1.0 compliancy to the requirements.

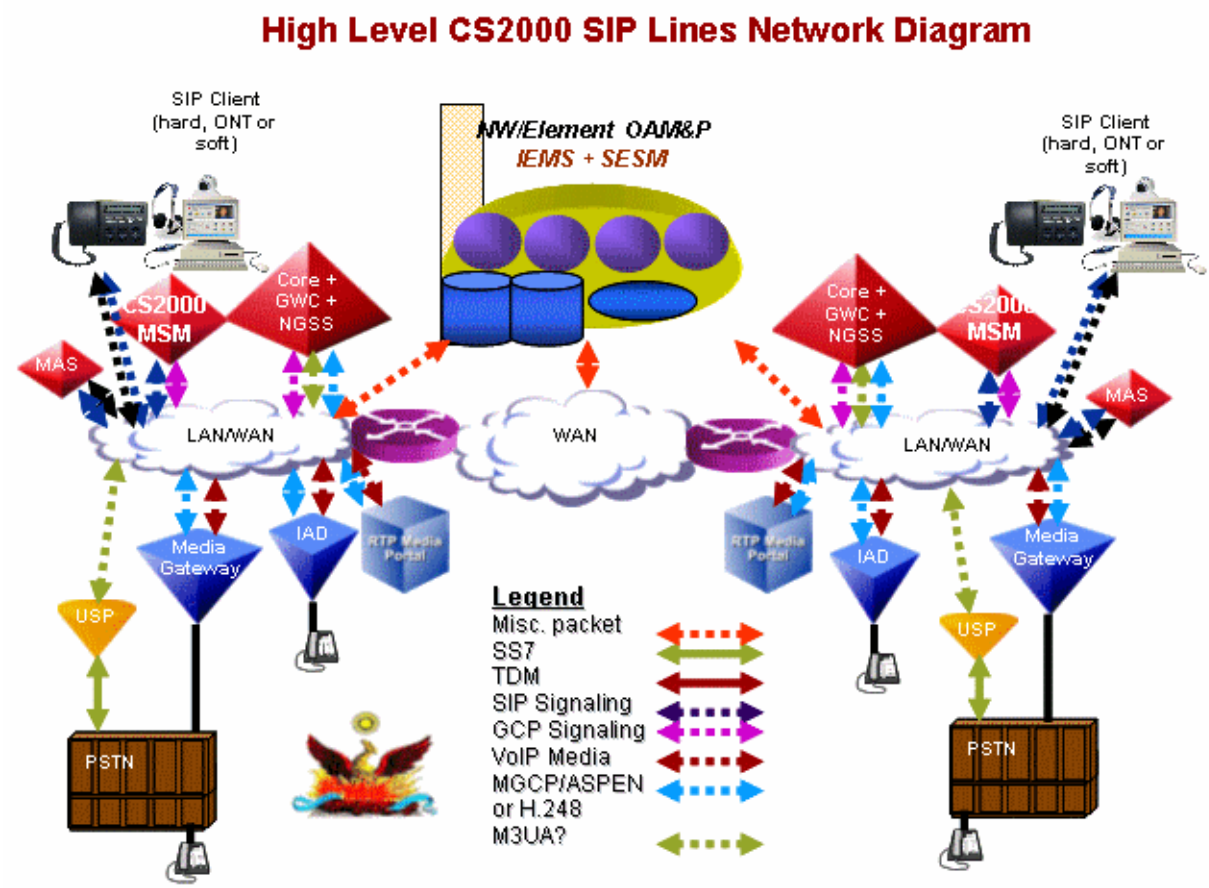
The Cisco 7960 requirements are broken into 3 categories:

1) Call Processing Services and Functionality

2) Software Download and configuration

3) NAT traversal

31.2.1 Hardware Requirements or Dependencies



31.2.2 Software Requirements or Dependencies

This feature is part of the MCP 9.0 Release. The Cisco Firmware release is POS3-07-4-00.sb2 (version 7.4)

The following requirements compliancy matrix lists both the feature requirements for the phone and which features are supported for CS2000 SS 1.0 in SN09.

Note: An asterisk (*) in the “Supported” column indicates the requirement is supported by the phone but requires development work on the CS2000 SS.

Feature/Capability	Supported on the Cisco 7960	Additional Notes
911	SN09	Routing provided by the core
Address book (personal)	No	

AIN services	n/a	
Analog signaling	n/a	
Answering Machine	n/a	
Assistant Console (Boss/ Admin)	n/a	
Audible voice identity delivery	n/a	
Basic inbound call delivery	SN09	
Bridged lines	n/a	
Bulletins	No	
Busy line verification	n/a	
Call back to busy line (ACBAR)	SN10	Done via feature activation on the core
Call forward locally on 7960	SN09	Programmed locally via softkeys on the phone
Call Forward via Personal Agent	SN09	
Call Forward via CS2000 Core	SN09* (if via FAC)	Handled by the core
Call Park	No	Not supported in SIP functionality on the phone – not available in standalone solution
Call rejection	n/a	
Call return	SN09 * (if via FAC)	Handled at the core
Call subjects	No	
Call tracing	SN09 * (if via FAC)	Handled at the core
Call waiting	SN09	User configurable on the phone
Call waiting disable	SN09	User configurable on the phone
Caller ID	SN09	User configurable on the phone
Click to call	n/a	Not initiated from the phone
Clipboard	n/a	
CODEC - G711	SN09	
CODEC - G729	SN09	
Conference (Ad hoc; 3-way calling only)	SN09	Phone provides the audio mixing at G.711 only – max 3-way call
6-way Adhoc conference	n/a	Not supported; max 3-way mixing
Converged Desktop	SN10	
Decline	n/a	Not supported by the phone
Device restrictions	n/a	
Direct connect	No	
Directory (global address via LDAP)	No	
Distinctive ringing	No	

Do Not Disturb	SN09	User configurable on the phone
File exchange	n/a	
Firewall support	SN09 *	Support for non-symmetric firewalls
Friends online	No	
Group alerting	n/a	
Hold (automatic hold)	SN09	Basic hold/retrieve performed on the phone
Hotline	n/a	
Ignore	n/a	
Import Outlook contacts	n/a	
Inbound call delivery to a group of lines	n/a	
Inbox	SN09	Phone has “Received Calls” and “Missed Calls” directories
Instant Message (IM)	No	Not supported by the phone
Lawful intercept (via Core)	SN09	Done by the core
Meet me Audio Conferencing	SN09 *	
Message Waiting Indicator (MWI)	SN09	
Multiple Lines/Users supported	SN09	Supports multiple users logged into the same device
Outbound call dialing	SN09	
Outbound call routing	SN09	
Outbound call screening	SN10	
Outbox	SN09	Phone has a “Placed Calls” directory
Outlook integration	n/a	
Picture ID	No	
Presence	n/a	SIP Presence not supported by the phone. “On the Phone” presence available via the SS
Profile manager	n/a	
Protocol - TCP	No	
Protocol - TLS	No	
Protocol - UDP	SN09	
Quality of Service (QoS) Reporting	n/a	
QoS Type Of Service (ToS) Marking	SN09	
Recursive calling (party line)	n/a	
Redirect	n/a	
Reject reasons	No	

Screening and routing (follow me, sequential ringing)	n/a	
Search options (address books)	No	
Server selection	SN09	Admin can provision a single Session Manager Address at the outbound proxy
Sharing	n/a	
Speed dialing	SN10	
Telemetry	n/a	
Transfer – Blind	SN09	Transfer failure cannot be retrieved
Transfer – Consult	SN09	Transfer failure cannot be retrieved
User configurable settings – requires user knowledge of phone configuration password	SN09 (See Section 2.5 below)	
User controlled codec selection – requires user knowledge of phone configuration password	SN09	
Video (video on demand)	n/a	
Voice mail	SN09	
Web push and co-browsing	n/a	
Whiteboard	n/a	

31.3 Limitations and restrictions

Certain call processing limitations of the 7960 result in the following services limitations:

- Calling Name/Number Blocking must be done via star-code activation on the core. The 7960 SIP implementation of this feature is not compatible with the CS2000 SS.
- Call Transfer is accomplished using the SIP REFER method. Transfers that fail cannot be retrieved due to the implementation on the 7960.
- Ad-hoc conferencing is accomplished as a 3-way call. The Cisco 7960 provides the audio mixing at the device itself. The 7960 only mixes G.711 packets, thus any existing legs negotiated to G.729 will attempt to be renegotiated to G.711. If a device does not support the G.711 codec then it cannot be included in a 3-way conference on the phone. The maximum ad-hoc conference size is 3. 6-way conferencing must be done via an external conferencing server.
- Presence is not supported from the phone. Therefore, all presence indications or updates must be derived from the active call state or registration state. By default, the CS2000 SS will support a presence state

of “connected” for a registered user, “unavailable offline” for a user who is not registered, and “On the Phone” for a user who is in an active call. Any additional presence states must be derived as if this device were a “Non SIP Lines device” by the core.

In addition, CS2000 SS SIP Lines will not support initiating a remote reset of the Cisco 7960 phone (via NOTIFY) for this release. Since reset remote is not supported, the phones cannot initiate a firmware upgrade without manual intervention. All firmware upgrades must be done manually via editing the configuration files located on the TFTP server and resetting the phone. Once the phone is reset, it will compare the current firmware load in flash with the load specified on the TFTP Server configuration file and initiate a download of the new firmware if the loads do not match. The network administrator is responsible for scheduling and initiating the reset of the phones for firmware upgrade. In addition, the TFTP server will not be integrated with the CS2000 SS solution, but rather a separate server from any other CS2000 SS component.

Note: Currently, there is no security mechanism in place to authenticate a remote reboot request via NOTIFY.

Likewise, provisioning of a CS2000 SS SIP Lines user will not automatically generate a phone specific configuration file on the TFTP server. The admin is responsible for creating and maintaining all the configuration files on the TFTP server for each phone in the network.

The Cisco phone does not provide a NAT traversal mechanism to indicate in SIP signaling the presence of a firewall between the client and the CS2000 SS. To compensate for this, the CS2000 SS will compare the UDP packet source IP address against the SIP Via Header IP address to determine whether or not to treat this client as a firewalled client and replace the contact IP address appropriately. The mechanism for keeping the firewall binding active will be a combination of the periodic maintenance audit via the OPTIONS message and a reduced registration expiry timer. However, if a NAT device dynamically re-binds a new IP and port to the Cisco 7960 after the phone is initially registered, a period of time will exist when calls can no longer terminate to the Cisco phone due to the stale NAT binding. This period of time can be up to the configured registration expiry timer. This firewall detection algorithm will not work for “symmetric” firewall solutions, where the IP address on both sides of the NAT device remain the same and only the port changes. Thus, symmetric firewall solutions are not supported for the first release.

31.4 Interactions

Where applicable, services initiated from the Cisco phone will use existing SIP service implementation to accomplish the desired feature. However, due to the

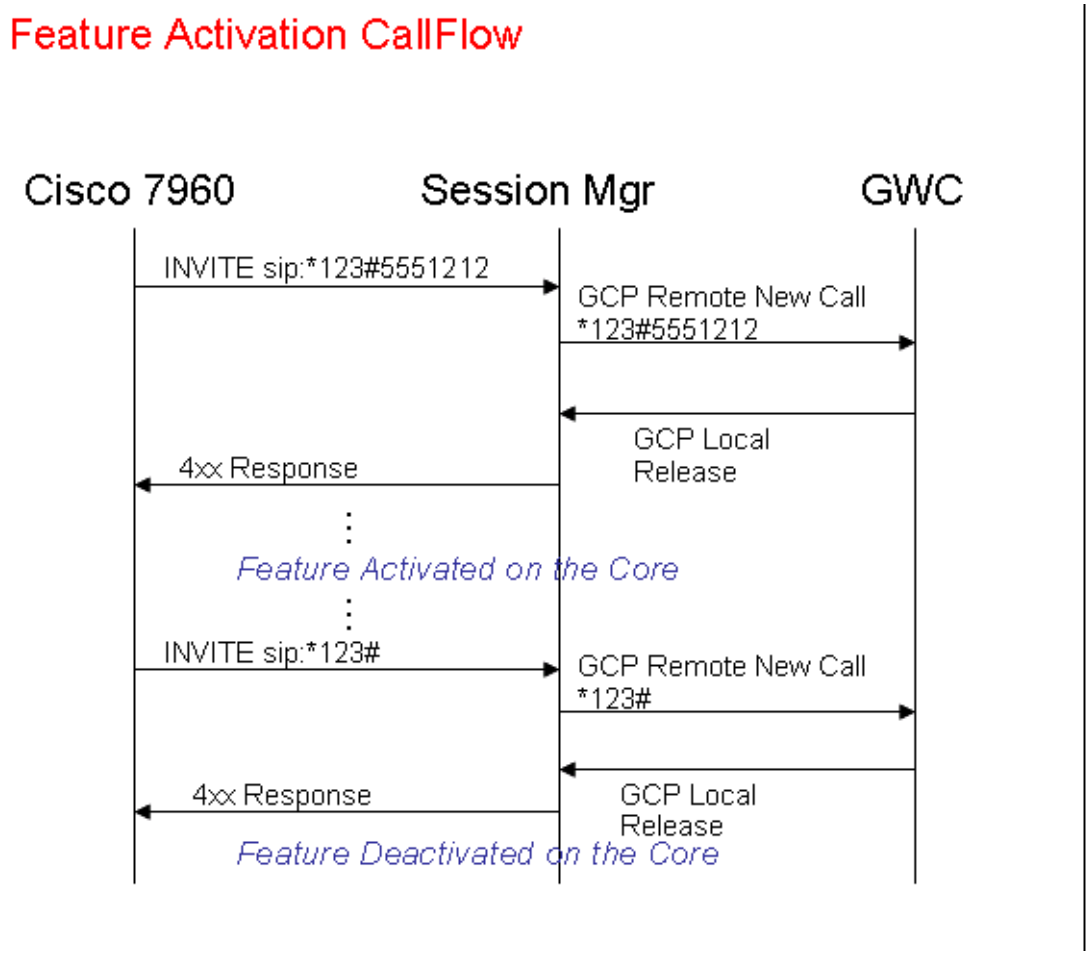
complex suite of services available to SIP Lines on the CS2000 Core, some feature activation will be done via star-code feature activation codes (FACs).

These services can be activated or deactivated by the phone via the configuration menu system:

- Do Not Disturb
- Auto-Completion of numbers
- Call Waiting
- Call Hold Ringback
- Stutter Message Waiting
- Auto-Answer (Intercom)
- Speed Dial (up to 5 numbers)
- Call Forward Unconditional

The services below will be permanently disabled on the phone and only available thru FACs. See the proposed call flow below for an indication of how the digits will be presented to the core.

- Caller ID Blocking
- Anonymous Call Reject



Call Forward is available on the phone (CFU) and also via FACs at the core.

31.5 Recommended Configuration

The following recommended settings should be used to assure interoperability between the 7960 and the CS2000 SS. The files reside in the root directory of an available TFTP server that all the 7960 phones are configured to use.

31.5.1 Common SIP Parameters

The SIPDefault.cnf file contains the common sip parameters needed by all the 7960 devices. These parameters control the default behavior of the phone and provide the phone the Session Server address and domain name that should be used. If these default parameters are not applicable to all 7960 phones in the network, then multiple TFTP servers should be used or duplicate parameters included in the phone-specific configuration file detailed in section 2.7.2. The file should be of this general format with only the domain name and IP Addresses highlighted in blue changed:

```
# SIP Default Generic Configuration File


# Image Version
image_version: P0S3-07-4-00

# Proxy Server
proxy1_address: "nortel.com" ; Can be dotted IP or FQDN
proxy2_address: ""           ; Can be dotted IP or FQDN
proxy3_address: ""           ; Can be dotted IP or FQDN
proxy4_address: ""           ; Can be dotted IP or FQDN
proxy5_address: ""           ; Can be dotted IP or FQDN
proxy6_address: ""           ; Can be dotted IP or FQDN

# Proxy Server Port (default - 5060)
proxy1_port: 5060
proxy2_port: 5060
proxy3_port: 5060
proxy4_port: 5060
proxy5_port: 5060
proxy6_port: 5060

# Proxy Registration (0-disable (default), 1-enable)
proxy_register: 1

# Phone Registration Expiration [1-3932100 sec] (Default - 3600)
timer_register_expires: 3600

# Codec for media stream (g711ulaw (default), g711alaw, g729a)
preferred_codec: g711ulaw

# TOS bits in media stream [0-5] (Default - 5)
tos_media: 5

# Inband DTMF Settings (0-disable, 1-enable (default))
dtmf_inband: 1

# Out of band DTMF Settings (none-disable, avt-avt enable (default), avt_always -
always avt )
dtmf_outofband: avt

# DTMF dB Level Settings (1-6dB down, 2-3db down, 3-nominal (default), 4-3db up, 5-6dB
up)
dtmf_db_level: 3

# SIP Timers
timer_t1: 500                ; Default 500 msec
```

```
timer_t2: 4000              ; Default 4 sec
sip_retx: 10                ; Default 10
sip_invite_retx: 6          ; Default 6
timer_invite_expires: 180   ; Default 180 sec

####### New Parameters added in Release 2.0 #######

# Dialplan template (.xml format file relative to the TFTP root directory)
dial_template: dialplan

# TFTP Phone Specific Configuration File Directory
tftp_cfg_dir: ""; Example:  ./sip_phone/

# Time Server (There are multiple values and configurations refer to Admin Guide for
Specifics)
sntp_server: ""             ; SNTP Server IP Address
sntp_mode: directedbroadcast ; unicast, multicast, anycast, or directedbroadcast
(default)
time_zone: EST              ; Time Zone Phone is in
dst_offset: 1               ; Offset from Phone's time when DST is in effect
dst_start_month: April      ; Month in which DST starts
dst_start_day: ""           ; Day of month in which DST starts
dst_start_day_of_week: Sun  ; Day of week in which DST starts
dst_start_week_of_month: 1  ; Week of month in which DST starts
dst_start_time: 02          ; Time of day in which DST starts
dst_stop_month: Oct         ; Month in which DST stops
dst_stop_day: ""            ; Day of month in which DST stops
dst_stop_day_of_week: Sunday ; Day of week in which DST stops
dst_stop_week_of_month: 8   ; Week of month in which DST stops 8=last week of month
dst_stop_time: 2            ; Time of day in which DST stops
dst_auto_adjust: 1          ; Enable(1-Default)/Disable(0) DST automatic adjustment
time_format_24hr: 1         ; Enable(1 - 24Hr Default)/Disable(0 - 12Hr)

# Do Not Disturb Control (0-off, 1-on, 2-off with no user control, 3-on with no user
control)
dnd_control: 0              ; Default 0 (Do Not Disturb feature is off)

# Caller ID Blocking (0-disbaled, 1-enabled, 2-disabled no user control, 3-enabled no
user control)
callerid_blocking: 2            ; Default 0 (Disable sending all calls as anonymous)

# Anonymous Call Blocking (0-disabled, 1-enabled, 2-disabled no user control, 3-enabled
no user control)
anonymous_call_block: 2         ; Default 0 (Disable blocking of anonymous calls)

# DTMF AVT Payload (Dynamic payload range for AVT tones - 96-127)
dtmf_avt_payload: 96            ; Default 101
```

```
# Sync value of the phone used for remote reset
sync: 1                         ; Default 1

####### New Parameters added in Release 2.1 #######

# Backup Proxy Support
proxy_backup: ""                ; Dotted IP of Backup Proxy
#proxy_backup_port: 5060        ; Backup Proxy port (default is 5060)

# Emergency Proxy Support
proxy_emergency: ""             ; Dotted IP of Emergency Proxy
#proxy_emergency_port: 5060     ; Emergency Proxy port (default is 5060)

# Configurable VAD option
enable_vad: 0                   ; VAD setting 0-disable (Default), 1-enable

####### New Parameters added in Release 2.2 ######

# NAT/Firewall Traversal
nat_enable: 1                   ; 0-Disabled (default), 1-Enabled
#nat_address: ""                ; WAN IP address of NAT box (dotted IP or DNS A record
only)
voip_control_port: 5060         ; UDP port used for SIP messages (default - 5060)
start_media_port: 16384         ; Start RTP range for media (default - 16384)
end_media_port: 32766           ; End RTP range for media (default - 32766)
#nat_received_processing: 0     ; 0-Disabled (default), 1-Enabled

# Outbound Proxy Support
outbound_proxy: "47.104.26.178" ; restricted to dotted IP or DNS A record only
outbound_proxy_port: 5060       ; default is 5060

####### New Parameter added in Release 3.0 #######

# Allow for the bridge on a 3way call to join remaining parties upon hangup
cnf_join_enable : 0             ; 0-Disabled, 1-Enabled (default)

####### New Parameters added in Release 3.1 #######

# Allow Transfer to be completed while target phone is still ringing
semi_attended_transfer: 0       ; 0-Disabled, 1-Enabled (default)

# Telnet Level (enable or disable the ability to telnet into the phone)
telnet_level: 2                 ; 0-Disabled (default), 1-Enabled, 2-Privileged

####### New Parameters added in Release 4.0 #######

# XML URLs
```

```
services_url: ""                ; URL for external Phone Services
directory_url: ""               ; URL for external Directory location
logo_url: ""                    ; URL for branding logo to be used on phone display

# HTTP Proxy Support
http_proxy_addr: ""             ; Address of HTTP Proxy server
http_proxy_port: 80             ; Port of HTTP Proxy Server (80-default)

# Dynamic DNS/TFTP Support
dyn_dns_addr_1: ""              ; restricted to dotted IP
dyn_dns_addr_2: ""              ; restricted to dotted IP
dyn_tftp_addr: ""               ; restricted to dotted IP

# Remote Party ID
remote_party_id: 0              ; 0-Disabled (default), 1-Enabled
```

31.5.2 Device Specific Parameters

The device-specific file of the filename format SIP<MACAddress>.cnf is used to specify parameters that apply only to a specific 7960 phone. In addition, parameters included in this file will take precedence over duplicate parameters in the SIPDefault.cnf file. The file should be of this general format with the each user-field matching what is provisioned:

```
# SIP Configuration Generic File

# Line 1 appearance
line1_name: user10

# Line 1 short name
line1_shortname: user10

# Line 1 Registration Authentication
line1_authname: "user10"

# Line 1 Registration Password
line1_password: "1234"

# Line 2 appearance
line2_name: user3

# Line 2 Registration Authentication
line2_authname: "user3"

# Line 2 Registration Password
line2_password: "1234"
```

```
####### New Parameters added in Release 2.0 #######

# All user_parameters have been removed

# Phone Label (Text desired to be displayed in upper right corner)
phone_label: "Phoenix SIP Lines         "; Has no effect on SIP messaging

# Line 1 Display Name (Display name to use for SIP messaging)
line1_displayname: "user10"

# Line 2 Display Name (Display name to use for SIP messaging)
line2_displayname: "user3"


####### New Parameters added in Release 3.0 ######

# Phone Prompt (The prompt that will be displayed on console and telnet)
phone_prompt:   "SIP Phone"      ; Limited to 15 characters (Default - SIP Phone)

# Phone Password (Password to be used for console or telnet login)
phone_password: "cisco" ; Limited to 31 characters (Default - cisco)

# User classifcation used when Registering [ none(default), phone, ip ]
user_info: none
```

31.5.3 Dialplan Definition

Finally, the dialplan.xml file should have the following entry to allow the proper handling of FAC star-code processing:

```
<DIALTEMPLATE>
    <TEMPLATE MATCH="\*.*#,*" Timeout="5"/>      <!-- Anything else -->
</DIALTEMPLATE>
```

31.6 Glossary

Term	Description
FAC	Feature Activation Code
NAT	Network Address Translation
TFTP	Trivial File Transfer Protocol
SS	Session Server

32: Functional Description (FN): A00009129

32.1 Feature name and Feature ID

A00009129: Controlled Hot Swact.

32.2 Description

This feature introduces a controlled hot SWACT capability for the CS 2000 - Compact Call Agent to the same load on the inactive side. A controlled swact is defined as being initiated from the linux CCAMTC map level or system initiated following a REX test.

Prior to this feature, a controlled Swact of the CS 2000 - Compact Call Agent utilizes a warm restart with an associated denial of origination period of approximately 25 seconds. Existing calls are preserved.

This new controlled hot Swact capability significantly reduces the denial of origination period to less than 3 seconds. Existing calls are preserved.

With the significantly reduced denial of origination period, this feature will now initiate a SWACT following a full REX test.

This feature will also provide the ability to set the day of the full REX test. Prior to this feature, the day of the full REX test was hardcoded to Thursday. The time of the REX test is still set via the NODEREXCONTROL tuple in table OFCVAR.

32.3 Hardware Requirements or Dependencies

N/A

32.4 Software Requirements or Dependencies

The minimum software baseline for this feature is a cPCI SOS image based on CSP22 as well a linux ramdisk based on NCGL8.

32.5 Limitations and restrictions

1. The controlled hot swact introduced in this feature is only initiated in two scenarios. From the CCAMTC map and after a REX test. It does NOT include the following.

- SWACT due to hardware/software failure.
- SWACT due to locking of active card on the SAM21EM.
- SWACT initiated by using the SWACT FORCE option in CCAMTC.

2. The CCAMTC map will not display whether the switch is in warm sync or hot sync. This will only be displayed from the CAPCI tool within SOS.

32.6 Interactions

A new SOS CI called CMREXFUL will be created to allow setting the day the full REX will occur.

The SOS CAPCI output will be modified to reflect warm or hot sync state.

The warning message when the swact command is initiated from the linux CCAMTC map level will be modified.

32.7 Glossary

Term	Description
REX	Routine Exercise
SAM21EM	SAM21 Element Manager
SWACT	Switch Activity

33: Functional Description (FN): A00009153

33.1 Feature name and Feature ID

Feature ID : A00009153, H.323 RLT Development

33.2 Description

Release Link Trunk (RLT) is used to free unused call signaling paths that result from call path changes such as call forwarding and call transfers. RLT is a proprietary function to Nortel that was originally developed for PRI trunks. Therefore, the RLT functionality will only be used by Nortel H323 gateways such as CS 1000 (CS1K).

Since this feature does not address any new functionality for the CS2000 or CS2100, for the remainder of this document, the term CS2K will imply functionality for both CS2000 and CS2100.

Note: A 3rd party H323 Gateway does not use the RLT functionality.

33.2.1 RLT Capability

The RLT functionality and provisioning for CS1K are described outside the scope of this document in "*CS 1000 RLT FS*". The following steps are needed to configure the "*RLT on NI-1 PRI"* capability in the CS2K.

SOC option can be set and verified as shown in the steps below:

```
>soc; soc debug; select option NI000024; (RLT on NI-1 PRI)

>assign rtu <Pass Code> to NI000024
>assign state on to NI000024
OPTION    NAME                                RTU   STATE
     USAGE  LIMIT   UNITS  LAST_CHG
NI000024  RLT on NI-1 PRI        Y     ON       -
     -        -             04/11/17
```

33.2.2 RLT Trunk Provisioning

Each trunk group may be provisioned for RLT capability using the existing MRLT option in the TRKGRP table that was developed for NTNA PRI.

Add the MRLT option to the TRKGRP table.

```
>table trkgrp; format pack ; pos <h323-clli> ; change
     (option set to MRLT)
```

```
<h323-clli> PRA 0 NPDGP NCRT ASEQ N (ISDN 100) $ (MRLT ) $
```

33.2.3 RLT of NTNA PRI trunks

The following section was taken from *NTNA PRI Specification* (NIS A211-1). The H323 RLT functionality is identical to the RLT functionality described in the NTNA PRI specification.

RLT is a feature available on an optional basis which optimizes the usage of NTNA PRI trunks. The following is a typical usage for RLT. Please note that many other scenarios are possible. In this scenario, User A calls User B. This call is referred to as Call 1. Call 1 is routed through the DMS-100 to the PBX. User B then forwards or transfers the call to User C, requesting RLT.

This call (Call 2) is routed through the same DMS-100 as shown in the following figure.

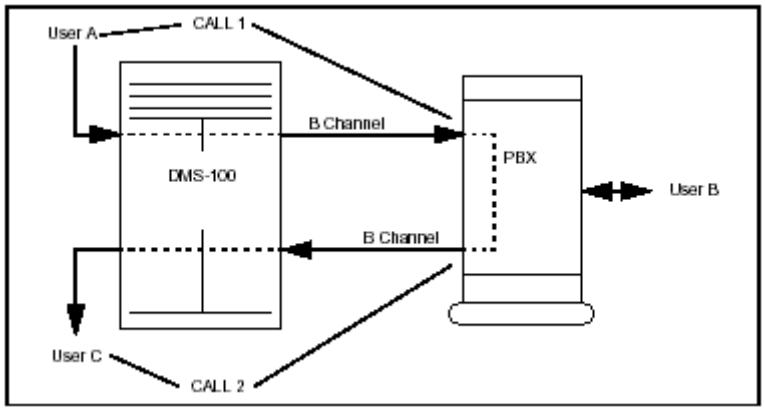


Figure 1: Typical Usage of RLT

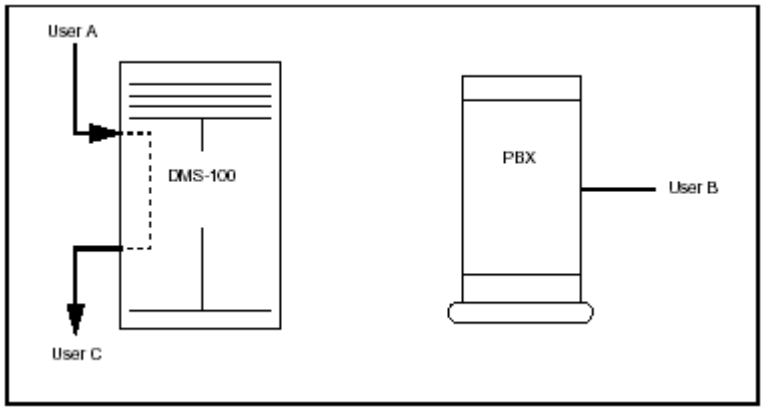


Figure 2: Result of Invoking RLT

When the call to User C is connected, RLT is invoked. The call is bridged between User A and User C at the DMS-100 and the PRI trunks to the PBX are released as shown in Figure 2: Result of Invoking RLT. Any CPE device may be used with this feature if it follows the same user side RLT protocol as described in "NTNA PRI Specification Chapter 5-12: Release Link Trunk (RLT)".

An example of the Q.931 message flow for RLT is shown in the following figure.

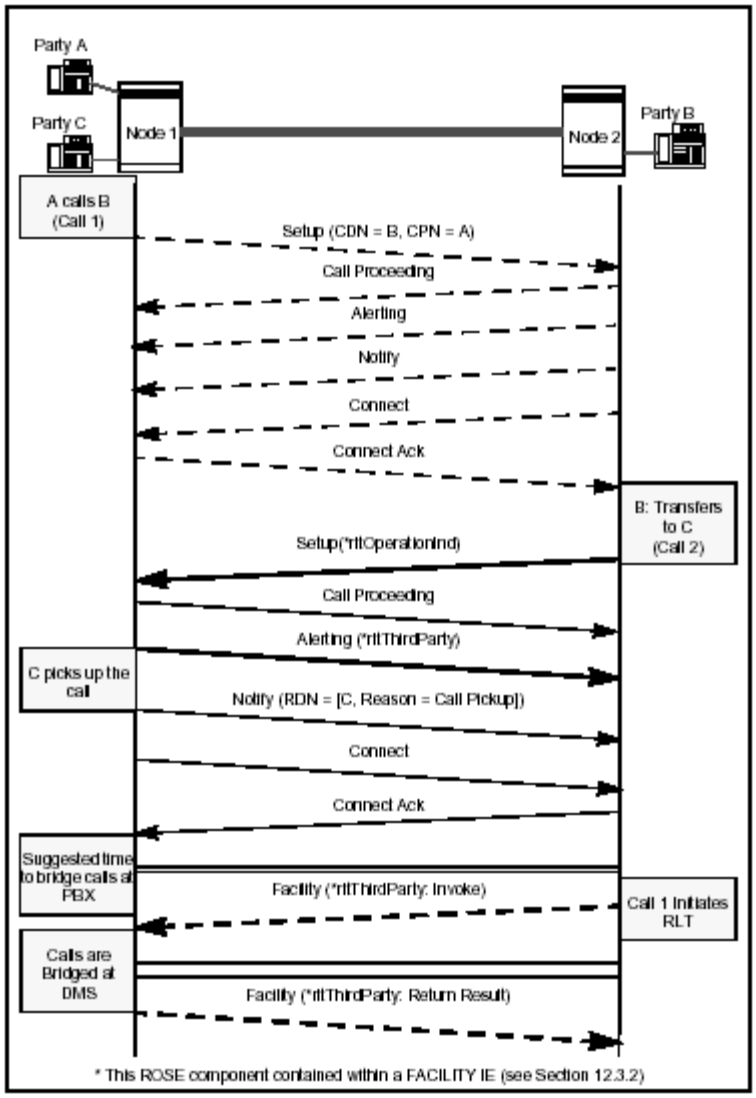


Figure 3: RLT with Call Transfer

33.2.4 Functional Behavior

Assuming RLT functionality has been provisioned in the CS2K and applied to all the H323 NTNA PRI trunk groups, there are two major behavior scenarios.

- "User Side" RLT capability
- "Network Side" RLT capability

33.2.4.1 User Side RLT

The first scenario is shown in the following figure. In this figure, CS1K A is calling CS1K B, and CS1K B call forwards to CS1K C. The invocation of RLT by CS1K B allows the CS2K to bridge the calls, making a new call from CS1K A through the CS2K to CS1K C. This invocation frees up the signaling path between CS1K B and the CS2K. Note that all signaling paths are through the CS2K, since it is the H323 Gate Keeper in this network.

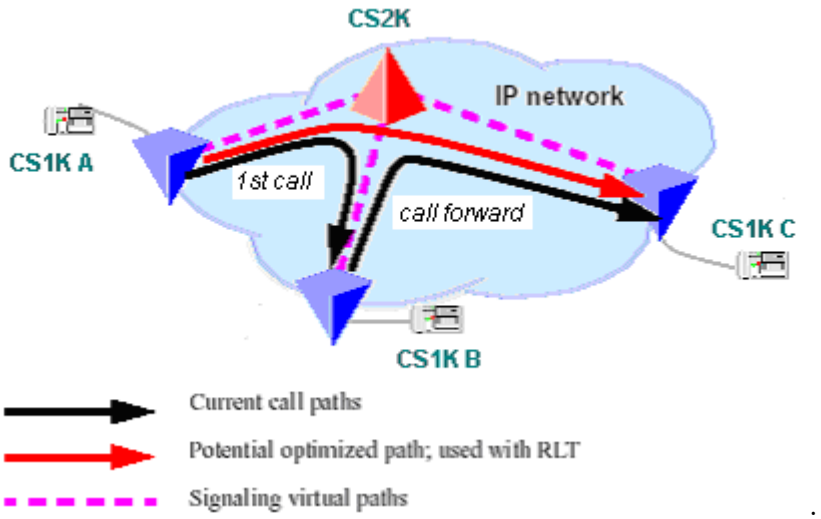


Figure 4 "User Side" RLT Functional Behavior

This scenario will also apply to call transfer in the CS1K. The CS2000 is only capable of processing RLT that is initiated by another H323 gateway such as CS1K; therefore, it is only capable of user side RLT.

33.2.4.2 Network Side RLT (CS 2100 only)

The second scenario is shown in the following figure. In this figure, CS1K A is calling an H323 gateway connected to the CS2100, and CS2100 call forwards to CS1K C. The invocation of RLT by CS2100 allows the CS1K A to bridge the call, making a new call from CS1K A to CS1K C. This invocation frees up the signaling path between CS2100 and the CS1K C.

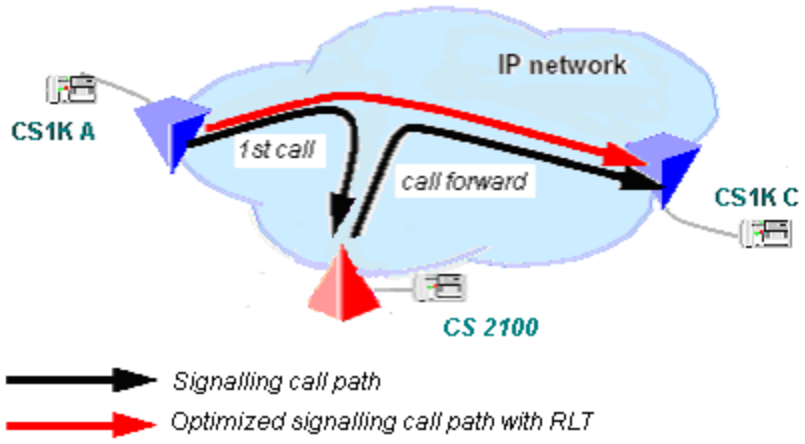
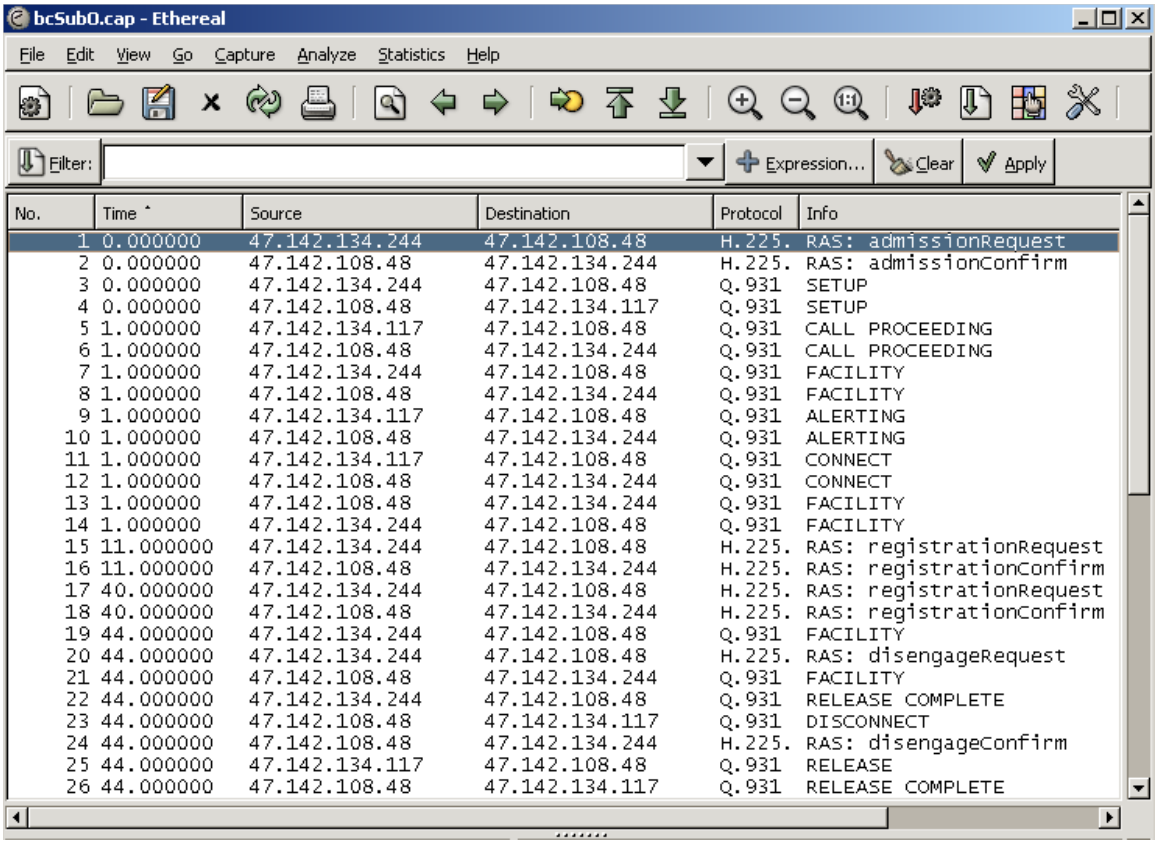


Figure 5 "Network Side" RLT Functional Behavior

This scenario will also apply to call transfer in the CS 2100. Since the CS2100 is the initiator of the RLT, it is performing the Network side RLT function.

33.2.5 H323 and Q.931 messaging

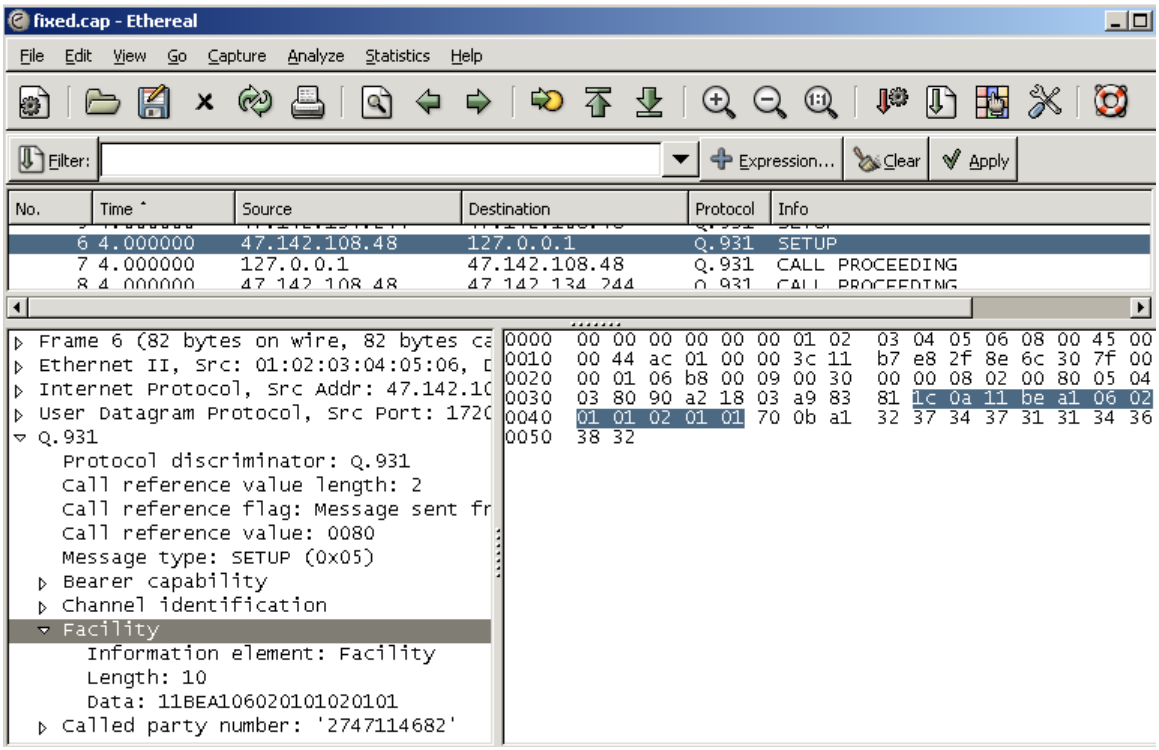
The H323 call processing messaging uses Q.931 within the H323 message. To demonstrate this, the packet capture tool in the GWC was used to capture packets from the H323 Gateway and packets formatted as Q.931 to send to CS2K. H323 Gateway: IP 47.142.134.244, GWC IP: 47.142.108.48 and CS2K IP: 47.142.134.117.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	47.142.134.244	47.142.108.48	H.225.	RAS: admissionRequest
2	0.000000	47.142.108.48	47.142.134.244	H.225.	RAS: admissionConfirm
3	0.000000	47.142.134.244	47.142.108.48	Q.931	SETUP
4	0.000000	47.142.108.48	47.142.134.117	Q.931	SETUP
5	1.000000	47.142.134.117	47.142.108.48	Q.931	CALL PROCEEDING
6	1.000000	47.142.108.48	47.142.134.244	Q.931	CALL PROCEEDING
7	1.000000	47.142.134.244	47.142.108.48	Q.931	FACILITY
8	1.000000	47.142.108.48	47.142.134.244	Q.931	FACILITY
9	1.000000	47.142.134.117	47.142.108.48	Q.931	ALERTING
10	1.000000	47.142.108.48	47.142.134.244	Q.931	ALERTING
11	1.000000	47.142.134.117	47.142.108.48	Q.931	CONNECT
12	1.000000	47.142.108.48	47.142.134.244	Q.931	CONNECT
13	1.000000	47.142.108.48	47.142.134.244	Q.931	FACILITY
14	1.000000	47.142.134.244	47.142.108.48	Q.931	FACILITY
15	11.000000	47.142.134.244	47.142.108.48	H.225.	RAS: registrationRequest
16	11.000000	47.142.108.48	47.142.134.244	H.225.	RAS: registrationConfirm
17	40.000000	47.142.134.244	47.142.108.48	H.225.	RAS: registrationRequest
18	40.000000	47.142.108.48	47.142.134.244	H.225.	RAS: registrationConfirm
19	44.000000	47.142.134.244	47.142.108.48	Q.931	FACILITY
20	44.000000	47.142.134.244	47.142.108.48	H.225.	RAS: disengageRequest
21	44.000000	47.142.108.48	47.142.134.244	Q.931	FACILITY
22	44.000000	47.142.134.244	47.142.108.48	Q.931	RELEASE COMPLETE
23	44.000000	47.142.108.48	47.142.134.117	Q.931	DISCONNECT
24	44.000000	47.142.108.48	47.142.134.244	H.225.	RAS: disengageConfirm
25	44.000000	47.142.134.117	47.142.108.48	Q.931	RELEASE
26	44.000000	47.142.108.48	47.142.134.117	Q.931	RELEASE COMPLETE

The GWC receives the H323 messages and creates new Q.931 messages to send to the CS2K. When the GWC receives the CS2K response, it will create a new H323 message from the content of the received message. Therefore, data does not pass from the H323 interface to the CS2K interface transparently. Every component of the Q.931 message is examined and a decision is made within the GWC whether to pass this data. For example, a CS2K DISCONNECT message is translated to a RAS message for H323.

For each message, the content can be viewed using the Ethereal built in decipher of Q.931 as shown in the example below for the SETUP message. In this example, the deciphered message contains the RLT Facility, being sent from the H323 Gateway, forwarded to the CS2K. It is also interesting to note that the call reference value is a 2 byte field on GWC to H323 messages but only one byte is used for the GWC to CS2K.

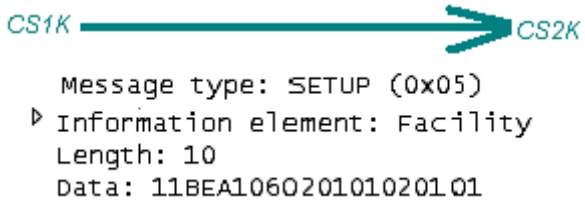


33.2.6 RLT message components

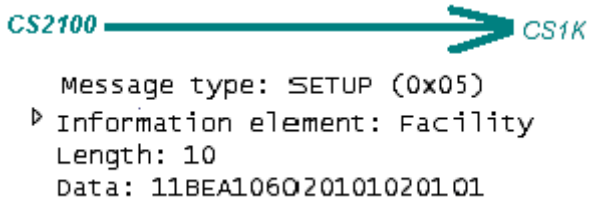
The RLT functionality is accomplished by adding a message component to the SETUP and ALERT messages and uses a new the FACILITY message to invoke RLT.

33.2.6.1 SETUP Message

CS1K SETUP messages for new calls will all contain the facility RLT.

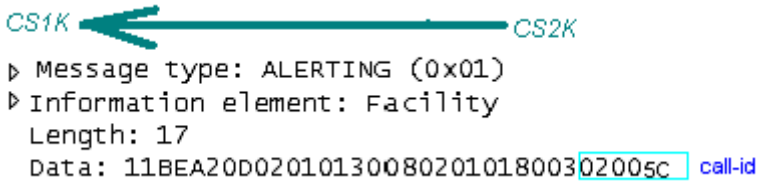


CS2100 SETUP messages for call forward or call transfer will contain the same facility RLT.

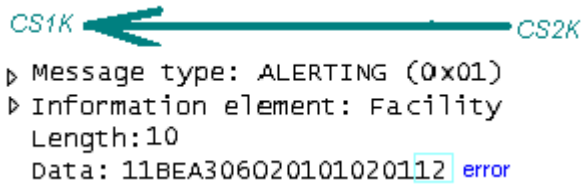


33.2.6.2 ALERT from CS2K

When CS2K is RLT provisioned and it receives an RLT Facility in the SETUP message, CS2K ALERT response messages will have the call-id in the facility RLT.

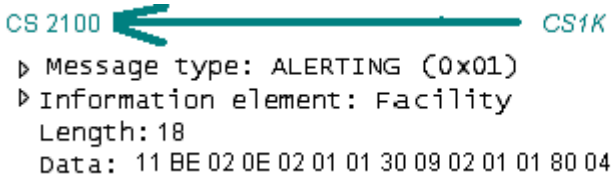


When CS2K is NOT RLT provisioned and it receives an RLT Facility in the SETUP message, CS2K ALERT response message will have and error indicating no RLT support.

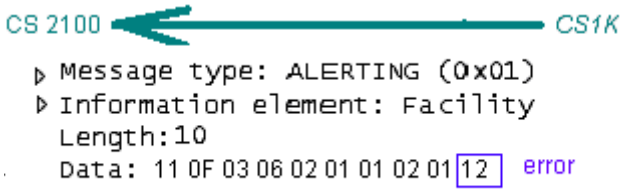


33.2.6.3 ALERT from CS1K

When CS2K sends an RLT Facility in the SETUP message, if CS1K is RLT provisioned, it will send an ALERT response messages with the call-id in the facility RLT.



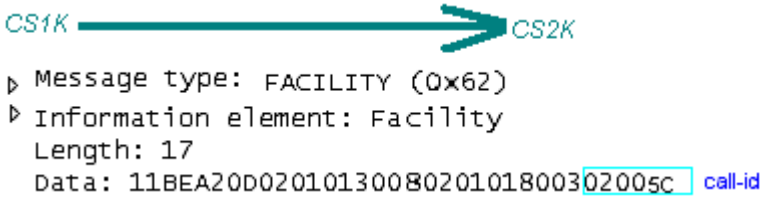
When CS2K sends an RLT Facility in the SETUP message but the CS1K is NOT RLT provisioned it will receive an ALERT response message with error indicating no RLT support.



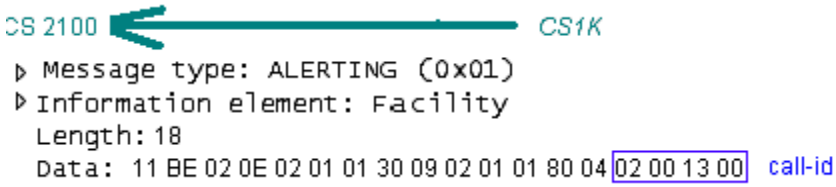
33.2.6.4 FACILITY RLT

After a successful call forward or call transfer, the FACILITY RLT message is used to free up the signaling links. The FACILITY RLT message contains the data returned in the ALERT message. Therefore, a FACILITY RLT message will can only be performed when the CS2K is properly provisioned for RLT on the particular trunk group.

The CS1K will send the FACILITY RLT message with the information it receives from the CS2K ALERT message.

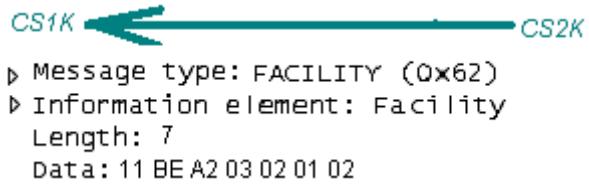


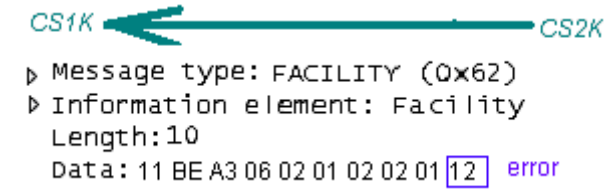
The CS 2100 will send the FACILITY RLT message with the information it receives from the CS1K ALERT message.



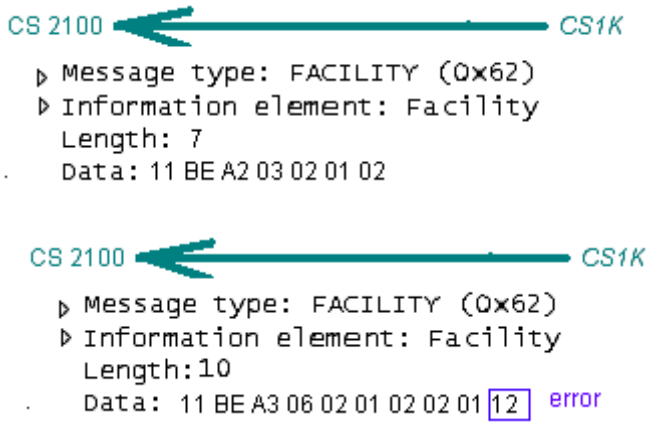
33.2.6.5 FACILITY RLT Response

The CS2K will send a response for the FACILITY RLT success or it will send an error indication.





CS1K response for FACILITY RLT message is the same as the CS2K.



33.3 Hardware Requirements or Dependencies

The H323 RLT capability is a software only component for GWC.

33.4 Software Requirements or Dependencies

The H323 RLT software requirements for the CS1K are described outside the scope of this document in CS1K feature DE2302. Since RLT is requested by the H323 Gateway, the GWC will not perform any RLT action without a Nortel H323 Gateway, such as the CS1K.

33.5 Limitations and restrictions

The CS2K will provide the RLT functionality described in *NTNA PRI Specification* (NIS A211-1).

33.6 Interactions

The RLT functionality is independent of the MCDN tunneling component of the H323.

34: Functional Description (FN): A00009156

34.1 Feature name and Feature ID

USP-Compact Hardware Feature ID : A00009156

34.2 Description

Each USP-Compact blade consists of two components the base card and the daughter card (PMC). The old base card and the old PMC are being phased out by the manufacturer; therefore it is necessary to adapt the USP-Compact software to run on the new replacement hardware.

This feature involves enabling the USP-Compact software that ran under the old hardware to now function on the new hardware. The USP-Compact functionality (from USPc9.0) is not changed by this feature, with the exception of possible performance increases resulting from the new cards (although this is not a required benefit). There are however minor provisioning changes as follows:

- introduction of a new hardware PEC which must be provisioned at commissioning time
- ability to provision the SS7 link interface type to be either T1 or E1 (previously required two separate PEC codes)

  Note: The SAM21 Element Manager is a support application used to provision bootp information queried by USPc at bootup time. It too will have to be modified so that it can support loads introduced by the new hardware.

34.3 Hardware Requirements or Dependencies

The old hardware consisted of two PECs (NTRX51FN and NTRX51FJ) which were selectable by the user and represent the base card and different PMC combo. Each of the two PECs corresponded to different t1-e1-mode in which the card combo would be running. For instance, selecting NTRX51FN automatically puts the cards in T1 mode of operation, while selecting the other PEC results in the cards running in E1 mode (proper PMC must be used for each mode). This is the mechanism employed by the user to change the operating mode of the cards (*see GUI screenshot Fig. 1*).

The addition of new hardware will add a new PEC **NTRX51TD** which the user can select. The new PMC card has the ability to function in either (T1 or E1) mode which is selectable through software (one PMC supports both modes). By default USP-Compact used to boot up with the NTRX51FN PEC

already provisioned which effectively set the card to T1 mode. However, with the introduction of the new PEC the default provisioned PEC is now NTRX51TD and the default t1-e1-mode is set to T1. This is now the default PEC whether running on new or old hardware and it's up to the user to match the PEC with the hardware that's being used. By selecting NTRX51TD PEC the t1-e1-mode becomes provisionable and at this point the user can select the mode he wants the cards to run in (*see GUI screenshot Fig. 2*).

Another minor change involves changing the PEC and/or port speed. In the old version of USP-Compact software *locking* the card was a sufficient prerequisite to make this modification. In the new version of the software the card must be taken *offline* before this provisioning will be allowed.

Figure 1 Fig. 1 Old hardware provisioning

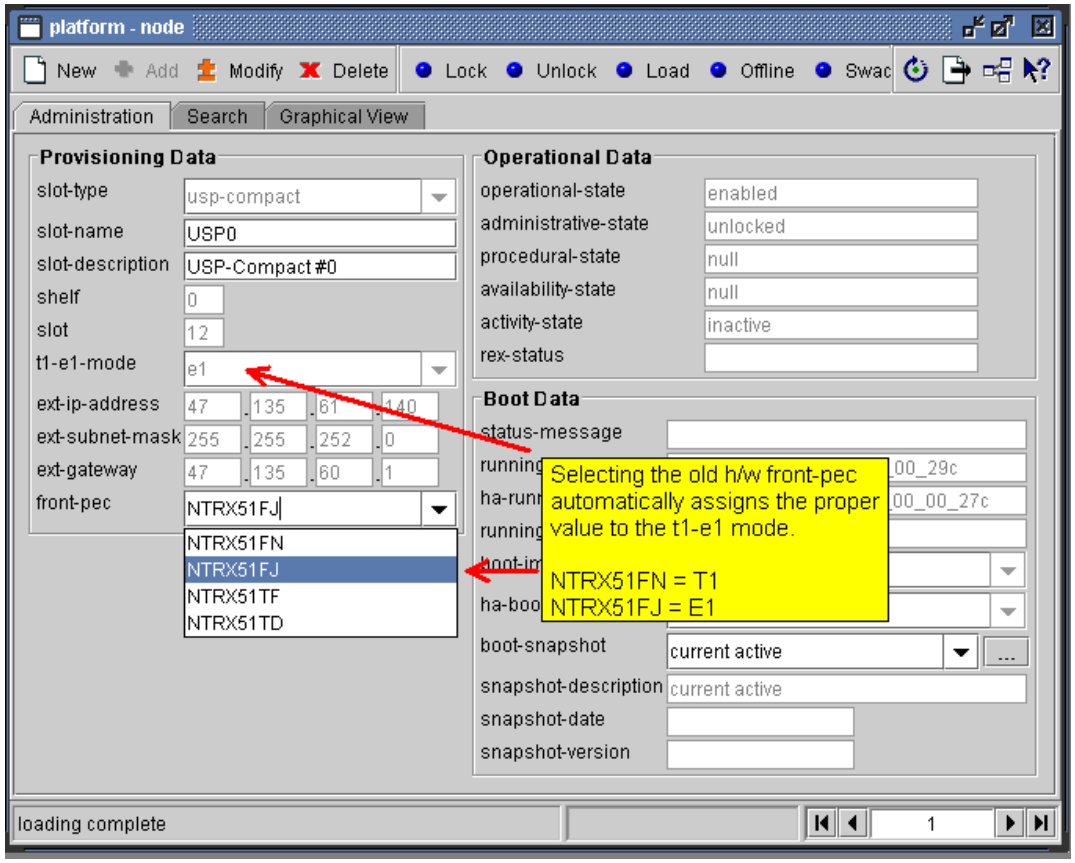
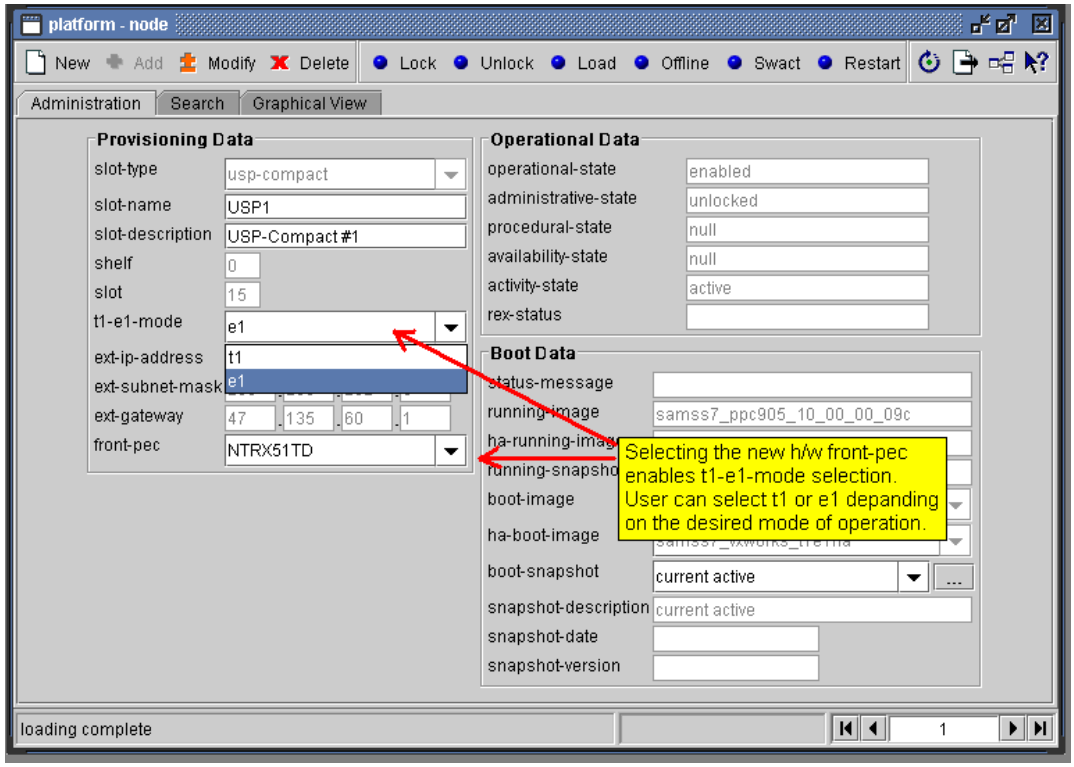


Figure 2 Fig. 2 New hardware provisioning



One other visible change introduced by this feature is that LED3 and LED4 are no longer present on the new hardware. On the old hardware LED3 would turn yellow whenever an alarm was received on the SS7 carrier port, but now LED1 takes that functionality and will turn yellow if this condition occurs. The condition normally indicated by LED4 on the old hardware is no longer an issue since the new hardware can handle it properly. Therefore LED4 is not longer needed and was removed.

34.4 Software Requirements or Dependencies

The SAM21 EM is used to provision bootup settings queried by USP-Compact at bootup time. EM is used to assign software loads to USP-Compact so that it knows what software to load when it boots up. This feature will result in a new USP-Compact software load. Therefore, when booting up USP-Compact on new hardware it is necessary to use the latest version of SAM21 EM application to be able to provisioning bootup information properly.

34.5 Limitations and restrictions

The main limitation is that base card and PMC software designed for the old hardware will only be able to run on that hardware. The same holds true for the software for the new hardware in that it will not function on the old hardware.

Also hardware mixing is not supported. This means that USP-Compact will run on either all old hardware or all new hardware. Only when upgrading hardware on USP-Compact both new and old hardware will be able to coexist for that short period of time.

34.6 Interactions

Not applicable.

34.7 Glossary

Term	Description
PMC	PCI Mezzanine Card
USPc	Universal Signaling Point - Compact
PEC	Product Engineering Code
SAM21 EM	SAM21 Element Manager

35: Functional Description (FN): A00009158

35.1 Feature name and Feature ID

Feature ID: A00009158
Feature name: M3UA over SCTP from Core to USP

35.2 Description

This activity implements M3UA RFC and SCTP RFC on CS2K core, supporting the following M3UA path type to USP.

- M3UA RFC over SCTP RFC client
- M3UA RFC over SCTP RFC server

This activity introduced changes on CS2K core but makes no changes to GWC platform.

This activity is based on the following specification on M3UA and RFC.

- RFC3332 Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA), September 2002
- M3UA Implementor's Guide, V7, February, 2004
- RFC2960 Stream Control Transmission Protocol, October 2000
- Stream Control Transmission Protocol (SCTP) Implementer's Guide, V12, October 15, 2004

Basically, without special mention, RFC2960 in this doc refers to the SCTP RFC2960 and SCTP Implementer’s Guide V12. RFC3332 in this doc refers to the M3UA RFC3332 and M3UA Implementor's Guide V7.

35.3 Support SCTP RFC on CS2K core

Activity A59023997 and A00003649 has implemented SCTP V5 [reference 6] on CS2K core. This activity will enhance the SCTP implementation based on SCTP RFC2960 [reference 3] and SCTP Implementer’s Guide V12 [reference 4].

35.3.1 SCTP chunk common header

In RFC2960, SCTP chunk common header is same as in SCTP V5. No change is introduced in this activity. Please refer to the following table for SCTP chunk common header format.

Table 1 SCTP chunk Common Header Format

Parameter	Type	Length(Octet)
Source Port Number	Mandatory	2
Destination Port Number	Mandatory	2
Verification Tag	Mandatory	4
Checksum	Mandatory	4

35.3.2 SCTP RFC chunks

This activity changes the following existing chunks to comply SCTP RFC version.

- SACK
- ABORT
- ERROR

This activity also adds a new chunk SHUTDOWN COMPLETE according to specification in RFC2960.

Other chunks are unchanged.

The following table shows the SCTP chunks supported by CS2K core. New and changed chunks are marked in BOLD.

Table 2 SCTP RFC chunks Supported by CS2K core

chunk Type	Value	chunk Explanation
DATA	0x0000	Payload Data
INIT	0x0001	Initiation
INIT ACK	0x0002	Initiation Acknowledgement
SACK	**0x0003**	**Selective Acknowledgement**
HEARTBEAT	0x0004	Heartbeat Request
HEARTBEAT ACK	0x0005	Heartbeat Acknowledgement

Table 2 SCTP RFC chunks Supported by CS2K core

chunk Type	Value	chunk Explanation
ABORT	**0x0006**	**Abort**
SHUTDOWN	0x0007	Shutdown Association
SHUTDOWN ACK	0x0008	Shutdown Acknowledgement
ERROR	**0x0009**	**Operation Error**
COOKIE ECHO	0x000A	State Cookie
COOKIE ACK	0x000B	Cookie Acknowledgement
SHUTDOWN COMPLETE	**0x000C**	**Shutdown Complete**

35.3.3 New and changed chunks

35.3.3.1 Selective Acknowledgement (SACK)

The chunk format of SACK is changed as below. Changed field is in BOLD.

Parameter	Type	Length(Octet)
Chunk Type	Mandatory	1
Chunk Flag	Mandatory	1
Chunk Length	Mandatory	2
Cumulative TSN Ack	Mandatory	4
Advertised Receiver Window Credit	Mandatory	4
Number of Gap Ack Blocks	Mandatory	2
Number of Duplicate TSNs	**Mandatory**	**2**
Gap Ack Block #1 - #N	Mandatory	n*4
Duplicate TSN 1-N	**Mandatory**	**n*4**

Two fields are introduced to this activity:

Number of Duplicate TSNs(16 bits): This field contains the number of duplicate TSNs the endpoint has received.

Duplicate TSN(32 bits): Every time a duplicate TSN is received before sending the SACK, it is added to the list of duplicates and appended to the end of the SACK. That is to say, if it is received n times(n>=1) before sending the SACK, it will be appended n-1 times. if it is received n times(n>=1) after sending the SACK for the TSN, it will be appended to SACK for current TSN n timers. The duplicate count is re-initialized to zero after sending each SACK.

35.3.3.2 Abort Association (ABORT)

The format of ABORT chunk is changed as below.

Parameter	Type	Length(Octet)
Chunk Type	Mandatory	1
Chunk Flag	**Mandatory**	**reserved (7 bits)** **T bit (1 bit)**
Chunk Length	Mandatory	2
zero or more Error Causes	Mandatory	4

When an endpoint is to close the association, ABORT chunk is sent with error causes.

The T bit is set to 0 if the sender filled in the Verification Tag expected by the peer. If the Verification Tag is reflected the T bit MUST be set to 1. Reflecting means that the sent Verification Tag is the same as the received one.

Refer to the following section for supported error codes on CS2K core.

35.3.3.3 Operation Error (ERROR)

An endpoint sends this chunk to its peer endpoint to notify it of certain error conditions. It contains one or more error causes. An Operation Error is not considered fatal in and of itself, but may be used with an ABORT chunk to report a fatal condition.

The below table shows the Cause Codes used in ERROR chunk, newly introduced Cause Codes are show in BOLD.

Cause Code	Cause	parameter of the Cause-specific Information	Description

1	Invalid Stream Identifier	Stream Identifier(16 bits) reserved (16 bits)	
2	Missing Mandatory Parameter	Number of missing parameters(32 bits) missing parameter type(16 bit)	
3	Stale Cookie Error	Measure of Staleness(32 bits)	
4	Out of Resource	None	
5	**Unresolvable Address**	**Unresolvable Address(32 bits)**	**Contains: complete Type, Length and Value of the address parameter. Indicates: the sender is not able to resolve the specified address parameter(e.g ,invalid transport address)**
6	**Unrecognized Chunk Type**	**Unrecognized Chunk(32 bits)**	**Contains: complete with Chunk Type, Chunk Flags and Chunk Length Indicates: the receiver does not understand the chunk (didn't defined)and the upper bits of the 'Chunk Type' are set to 01 or 11**
7	**Invalid Mandatory Parameter**	**None**	**Indicates: one of the mandatory parameters is set to a invalid value**
8	**Unrecognized Parameters**	**Unrecognized Parameters(32 bits)**	**Contains: contains unrecognized parameters copied from the INIT ACK chunk complete with TLV Indicates: returned to the originator of the INIT ACK chunk if the receiver does not recognize one or more Optional TLV parameters in the INITACK chunk.**
9	**No User Data**	**TSN value (32 bits)**	**Contains: the TSN of the DATA chunk received with no user data field Indicates: returned to the originator of a DATA chunk if a received DATA chunk has no user data**

10	**Cookie Received While Shutting Down**	**None**	**Indicates: A COOKIE ECHO was received while the endpoint was in SHUTDOWN-ACK-SENT state**
11	**Restart of an association with new addresses**	**New Address TLVs**	**Indicates: An INIT was received on an existing association. But the INIT added addresses to the association that were previously NOT part of the association. The New addresses are listed in the erro code.**
12	**User Initiated Abort**	**Upper Layer Abort Reason**	**Indicates: Upper Layer Abort Reason**
13	**Protocol Violation**	**Additional Information**	

35.3.3.4 Shutdown Complete (SHUTDOWN COMPLETE)

SHUTDOWN COMPLETE chunk is required to sent on reception of SHUTDOWN ACK at the completion of the shutdown process in SCTP RFC version. This activity introduced this new chunk type and supports related shutdown procedures.

The chunk format of new chunk SHUTDOWN COMPLETE is as below:

Parameter	Type	Length(Octet)
Chunk Type	**Mandatory**	**2**
Chunk Flag	**Mandatory**	**Reserved(7 bits)** **T bit (1 bit)**
Chunk Length	Mandatory	2

The T bit is set to 0 if the sender filled in the Verification Tag expected by the peer. If the Verification Tag is reflected the T bit MUST be set to 1. Reflecting means that the sent Verification Tag is the same as the received one.

35.3.4 Enhanced SCTP procedures

35.3.4.1 Normal Establishment of an Association

Association establishment procedures are modified to in RFC2960 section 5.1 comparing to SCTP v5. This activity enhances the existing SCTP implementation based on the specification in RFC2960 section 5.1.

35.3.4.2 Handle Duplicate or unexpected INIT, INIT ACK, COOKIE ECHO, and COOKIE ACK

New procedures are introduced to handle duplicate or unexpected INIT, INIT ACK, COOKIE ECHO, and COOKIE ACK in RFC2960 section 5.2. This activity enhances the existing SCTP implementation based on the specification in RFC2960 section 5.2.

The following scenarios are handled in this activity.

- Handle Duplicate INIT in COOKIE-WAIT or COOKIE-ECHOED States
- Unexpected INIT in States Other than CLOSED, COOKIE-ECHOED, COOKIE-WAIT and SHUTDOWN-ACK-SENT
- Unexpected INIT ACK
- Handle a COOKIE ECHO when a TCB exists
- Handle Duplicate COOKIE ACK

35.3.4.3 Path Verification

RFC2960 section 5.4 Path verification procedure is introduced to ensure all the address presented by the peer are in the fact belonging to the peer in SCTP implementor's guide V12. This activity enhances the existing SCTP implementation based on RFC2960 section 5.4.

35.3.4.4 User Data Transfer

User data transfer procedures are modified to enhance user data transfer reliability in RFC2960 section 6 comparing to SCTP V5. This activity enhances the existing SCTP implementation based on RFC2960 section 6.

35.3.4.5 Congestion Control

Congestion control procedures are modified in RFC2960 section 7 comparing to SCTP v5. This activity enhances the existing SCTP implementation based on RFC2960 section 7.

35.3.4.6 Fault Management

Fault management procedures are modified in RFC2960 section 8 comparing to SCTP v5. This activity enhances the existing SCTP implementation based on RFC2960 section 8.

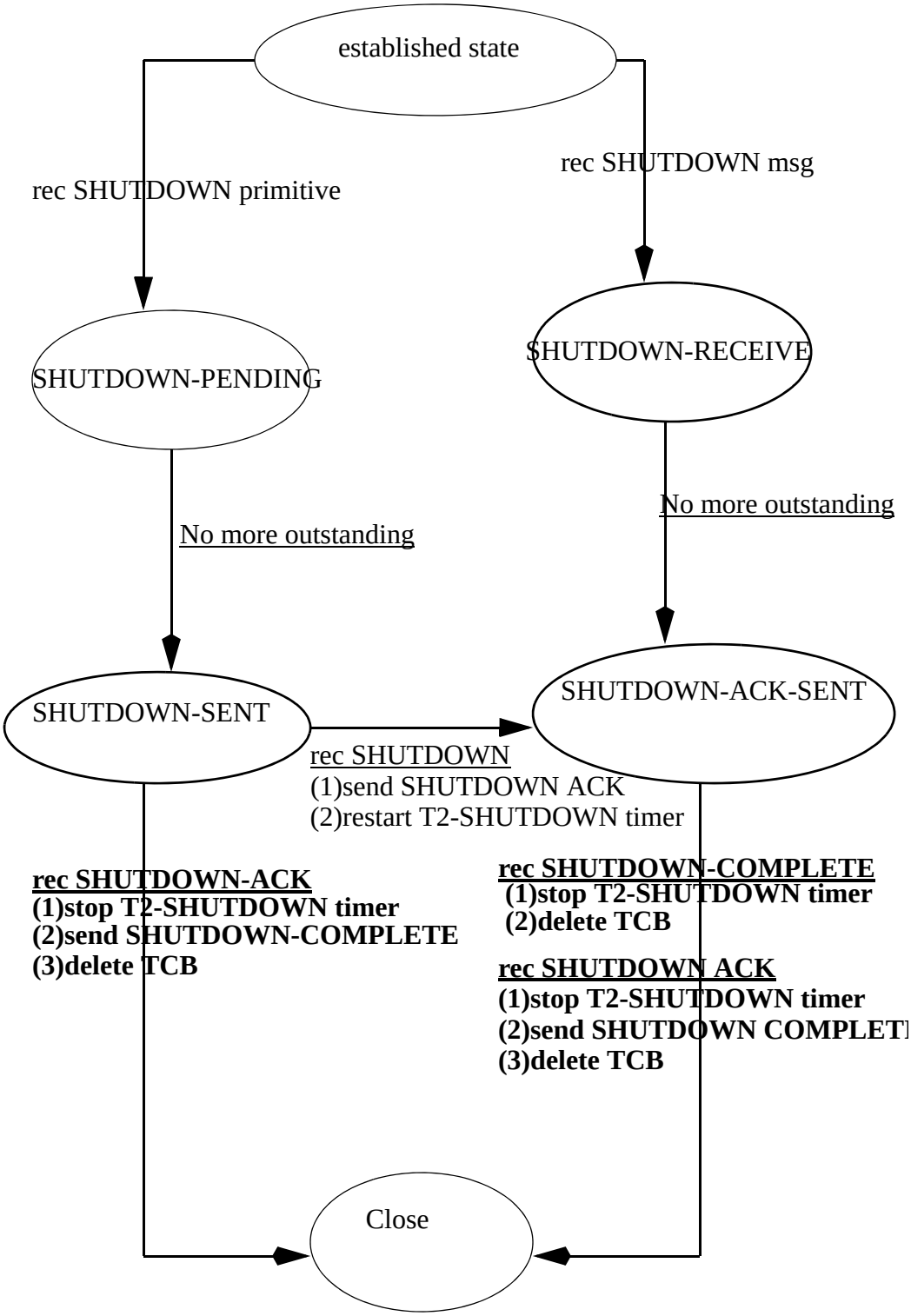
35.3.4.7 Abort of an Association

Association abort procedures are modified in RFC2960 section 9.1 comparing to SCTp V5. This activity enhances the existing SCTP implementation based on RFC2960 section 9.1.

35.3.4.8 Shutdown of an Association

SCTP RFC version has introduced new procedures to the termination of association (RFC2960 section 9.2). Refer to the following figure for the new procedures supported on CS2K core. The changes are marked in BOLD.

SCTP state diagram: termination of association



35.4 Support M3UA RFC on CS2K core

35.4.1 M3UA paths datafill

A new field PROTOCOL is added to table USPPATHS, to allow user to select the protocol of the path. The new field will have following 3 values:

- M3UA_V2_UDP - M3UA V2 over UDP
- M3UA_RFC_SCTP_CLIENT - M3UA RFC over SCTP CLIENT
- M3UA_RFC_SCTP_SERVER - M3UA RFC over SCTP SERVER

Normally, paths in the same pathset **SHOULD** be the same type. Warning message is displayed if customer try to datafill different path type in the pathset. But in-service cutover from M3UA V2 paths to M3UA RFC paths in one pathset is supported and Opposite cutover from M3UA RFC paths to M3UA V2 paths is not supported.

Please refer to section 2.4.11 and 2.4.12 for cutover and rollback procedures for M3UA V2 pathset to M3UA SCTP pathset.

The total message rate of all M3UA RFC paths over SCTP **SHOULD** be less than the max message rate that SCTP on core can support. Currently the max message rate that SCTP can support is 4500 msg/sec. Please refer to sction 2.4.10 and activity A00003649 “SCTP (Stream Control Transmission Protocol) Enhancements on XA-Core” for more detail.

One pathset on the CS2K core is configured as an ASP. IPSP configuration is not supported.

Refer to the following figure for datafill example of paths to USP.

Datafill example of M3UA paths to USP on CS2K core

Datafill for path to USP (M3UA V2 over UDP)
table usppaths
PATHNAME SRCPORT DESTIP DESTPORT PATHSEL **PATHPROT**
---
pathset_to_usp 0 4697 192 168 10 42 2905 0 **M3UA_V2_UDP**

Datafill for path to USP (M3UA RFC over SCTP client)
table usppaths
PATHNAME SRCPORT DESTIP DESTPORT PATHSEL **PATHPROT**
---
pathset_to_usp 0 4697 192 168 10 42 2905 0 **M3UA_RFC_SCTP_CLIENT**

Datafill for path to USP (M3UA RFC over SCTP server)
table pathset
PATHNAME SRCPORT DESTIP DESTPORT PATHSEL **PATHPROT**
---
pathset_to_usp 0 4697 192 168 10 42 2905 0 **M3UA_RFC_SCTP_SERVER**

As M3UA V2 path, the valid port number for M3UA RFC path is from 4697-4700 and 4710- 4721.

35.4.2 RFC M3UA message common header

Table 3 RFC M3UA message common header format

Field	Length (byte)	Description
Version	1 byte	it is set to 0x01, indicating M3UA release 1.0
Reserved	1 byte	it is set to 0x00
Message Group	1 byte	Refer to 2.4.3
Message Type	1 byte	Refer to 2.4.3
Message Length	4 byte	The Message Length defines the length of the message in octets, including the Common Header.

If version is not “0x01”, an ERROR message with error code “0x0001” is sent to USP.

35.4.3 RFC M3UA messages

"Table 4 M3UA RFC messages supported by CS2K" represents the set of messages that are required by M3UA RFC.

Table 4 RFC M3UA messages supported by CS2K

Message	Message Class and message type	Description
ERROR	0x0000	Error
NTFY	0x0001	Notify
DATA	0x0101	Payload data
DUNA	0x0201	Destination Unavailable
DAVA	0x0202	Destination Available
DAUD	0x0203	Destination State Audit
SCON	0x0204	Signalling Congestion
DUPU	0x0205	Destination User Part Unavailable
DRST	0x0206	Destination Restricted
ASPUP	0x0301	ASP Up
ASPDN	0x0302	ASP Down
ASPUP ACK	0x0304	ASP Up Acknowledgement
ASPDN ACK	0x0305	ASP Down Acknowledgement
ASPAC	0x0401	ASP Active
ASPIA	0x0402	ASP Inactive
ASPAC ACK	0x0403	ASP Active Acknowledgement
ASPIA ACK	0x0404	ASP Inactive Acknowledgement

If unsupported message class is received, ERROR message with error code 0x0003 is sent to USP.

If unsupported message type is received, ERROR message with error code 0x0004 is sent to USP.

Note: Since M3UA RFC is transported over SCTP, Heartbeat and Heartbeat ACK messages are not supported. SCTP has its own heartbeat mechanism to

detect loss of transport associations, Thus heartbeat procedure is not required when M3UA is transported over SCTP.

35.4.4 RFC M3UA Parameters

The following table represents the set of parameters that are required by RFC M3UA.

Table 5 RFC M3UA parameters supported by CS2K

Parameter	Parameter Id	Description
Traffic Mode Type	0x000b	Supported in ASP ACTIVE
Error Code	0x000c	Supported in ERROR
Status	0x000d	Supported in SCON
Affected Point Code	0x0012	Supported in DAVA, DUNA, DAUD, DRST, DUPU
Network Appearance	0x0200	Supported in SSNM messages and DATA message.
User/Cause	0x0204	Supported in DUPU
Congestion Indications	0x0205	Supported in SCON
Protocol Data	0x0210	Supported in DATA

When an optional parameter is received and not supported, the message is processed but the optional parameter is discarded silently.

35.4.5 RFC M3UA message format

35.4.5.1 ASPSM messages

No optional parameter is supported in the following messages.

ASP UP

ASP DOWN

ASP UP ACK

ASP DOWN ACK

35.4.5.2 ASPTM messages

The message format of ASP ACTIVE is as below:

Parameter	Type	Length (byte)

Traffic Mode Type	Optional	Tag(2 bytes) Length(2 bytes) Traffic Mode Type (4 bytes) 0x0001 - Override

If unsupported traffic mode type is received, ERROR message is sent to peer.

No optional message is supported in the following message.

ASP INACTIVE

ASP ACTIVE ACK

ASP INACTIVE ACK

35.4.5.3 SSNM messages

Message format for DAVA, DUNV, DRST and DAUD is as below.

Parameter	Type	Fields
Network Appearance	Optional	Tag(2 bytes) Length(2 bytes) Value(4 bytes)
Affected Point Code	Mandatory	Tag(2 bytes) Length(2 bytes) Mask 1 (1 bytes) Affected PC 1 (3 bytes) ..... Mask n (1 bytes) Affected PC n (3 bytes)

Message format for SCON is as below:

Parameter	Type	Fields
Network Appearance	Optional	Tag(2 bytes) Length(2 bytes) Value(4 bytes)
Affected Point Code	Mandatory	Tag(2 bytes) Length(2 bytes) Mask 1 (1 byte) Affected PC 1 (3 bytes) ..... Mask n (1 byte) Affected PC n (3 bytes)

Congestion Indications	Optional	Tag (2 bytes) Length (2 bytes) Reserved (3 bytes) Cong Level (1 byte)

Message format for DUPU is as below.

Parameter	Type	Fields
Network Appearance	Optional	Tag(2 bytes) Length(2 bytes) Value(4 bytes)
Affected Point Code	Mandatory	Tag(2 bytes) Length(2 bytes) Mask 1 (1 byte) Affected PC 1 (3 bytes) ..... Mask n (1 byte) Affected PC n (3 bytes)
User/Cause	Mandatory	Tag (2 bytes) Length (2 bytes) Cause (2 bytes) User (2 bytes)

35.4.5.4 DATA message

Message format for DATA is as below.

Parameter	Type	Fields
Network Appearance	Optional	Tag(2 bytes) Length(2 bytes) Value(4 bytes)
Protocol Data	Mandatory	Tag(2 bytes) Length(2 bytes) Protocol Data (variable length)

35.4.5.5 Error Message

Message format for Error is as below.

Parameter	Type	Fields

Error Code	Mandatory	Tag (2 bytes) Length (2 bytes) Error code (4 bytes)

Error Code supported by CS2K is as below.

Error Code	Description
0x01	Invalid Version
0x03	Unsupported Message Class
0x04	Unsupported Message Type
0x06	Unexpected Message
0x09	Invalid Stream Identifier
0x11	Invalid Parameter Value
0x12	Parameter Field Error
0x13	Unexpected Parameter
0x16	Missing Parameter

35.4.5.6 Notify Message

The Notify message used to provide an autonomous indication of M3UA events in USP to the CS2K.

Message format for Notify message is as below.

Parameter	Type	Fields
Status	Mandatory	Tag (4 bytes) Length (4 bytes) Status Type and Status Information (8 bytes) 0x0101 - Application Server State Change, inactive 0x0102 - Application Server State Change, active 0x0103 - Application Server State Change, pending

Notify message with unsupported status type and status information received is discarded silently.

35.4.6 RFC M3UA procedures

This activity implements the M3UA layer procedures based on the RFC3332 section 4.3, 4.5, 4.6.

35.4.6.1 Activate USP paths

Users can activate USP paths via ACT command in MAPCI CCS7 directory. If the path is the first activated path in the pathset, ASP UP and ASP ACTIVE procedure is started. The path is set to INSV after receive NTFY (AS ACTIVE) from USP. If the path is not the first activated path in the pathset, ASP UP and ASP ACTIVE procedure is not started. The path is set to INSV after SCTP association is established.

Refer to the following two figures for the message flow of activating USP path in pathset over SCTP.

Figure 1 Activate first path in the pathset when both paths are OFFL

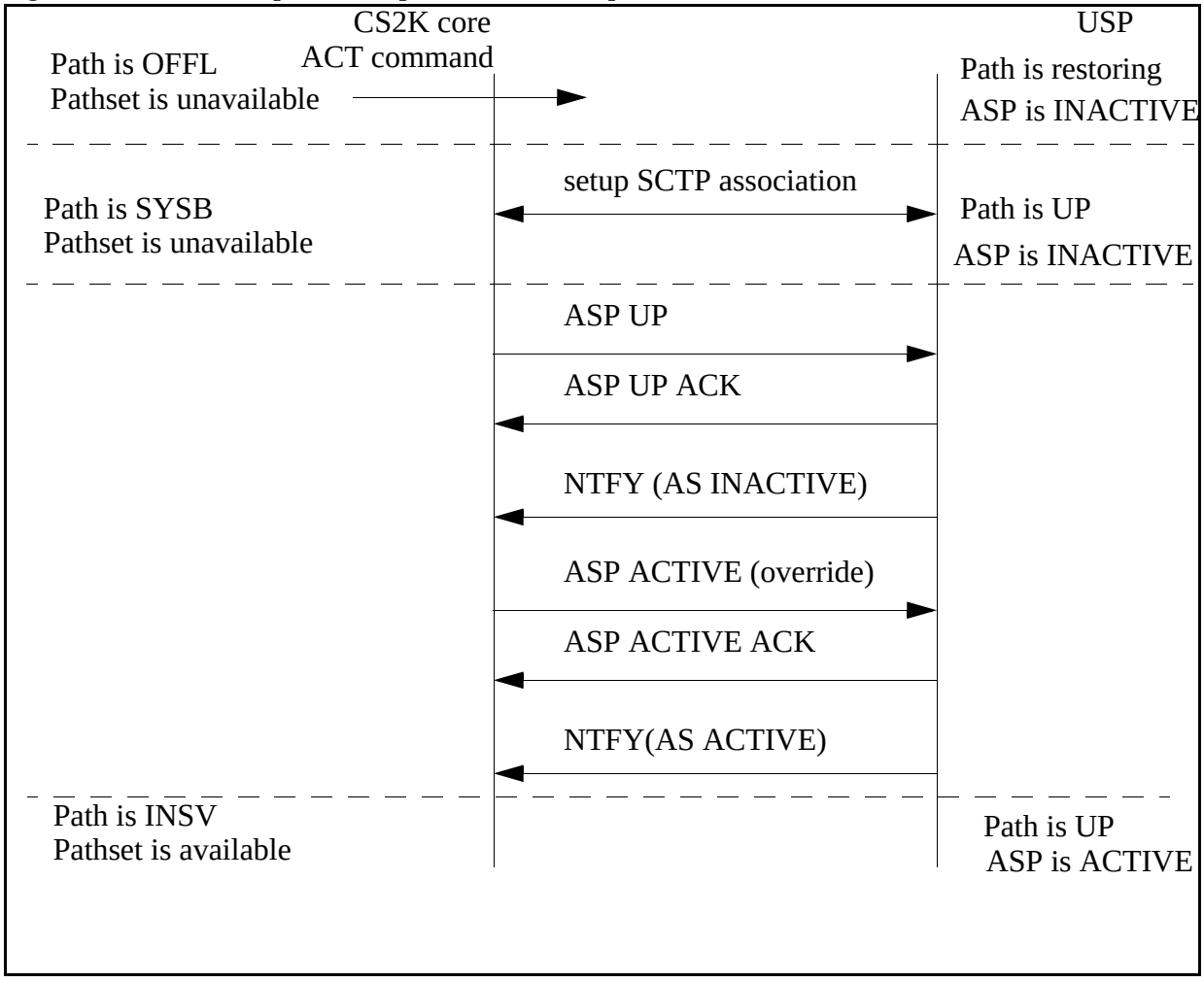
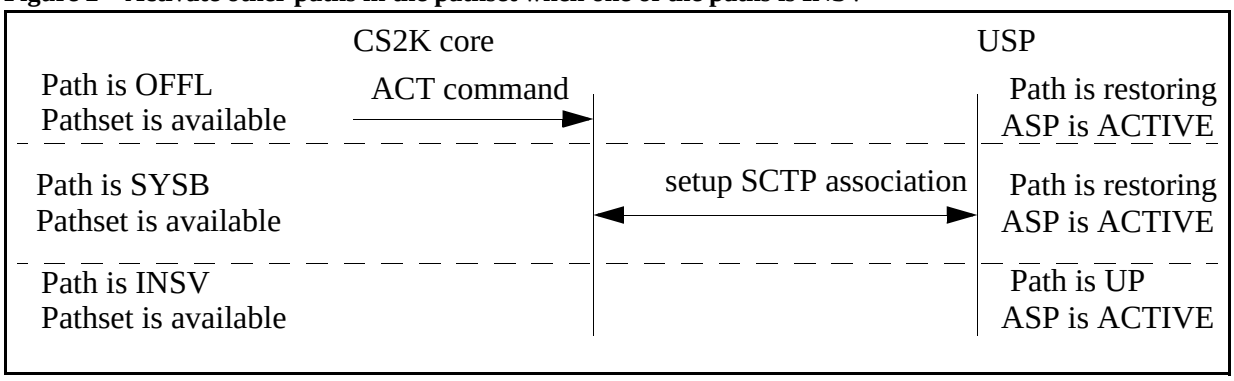


Figure 2 Activate other paths in the pathset when one of the paths is INSV



35.4.6.2 Deactivate M3UA path

Users can deactivate USP paths via DEACT command in MAPCI CCS7 directory. The path is set to OFFL when it is deactivated.

- Deactivate the last INSV path in the pathset

If the path is the last INSV path in the pathset, ASP INACTIVE and ASP DOWN procedure is started. and then the SCTP association is taken down.

After the path is deactivated, there is no more INSV path available. No more outgoing and incoming traffic is allowed immediately. ASPIA and ASPDN is sent to peer to update the ASP status.

In this case, the traffic received from peer ULP before ASPIA is received are discarded because no more outgoing and incoming traffic is allowed after the pathset is down.

- Deactivate INSV path (not the last INSV path in the pathset)

If the path is not the last INSV path in the pathset, ASP INACTIVE and ASP DOWN procedure is not started. SCTP association is taken down immediately.

After the path is deactivated, the path can not send outgoing traffic any more. SCTP SHUTDOWN chunk is sent to peer to take down the SCTP association.On reception of the SHUTDOWN chunk in the peer side, the traffic received from peer ULP before SHUTDOWN arrived are still sent out to the Core. To avoid traffic lost, the path will accept these incoming traffic and report to ULP.

- Deactivate SYSB path

If the path is in SYSB, if SCTP association is established, send SHUTDOWN to shutdown the association, otherwise, send ABORT to abort establishing SCTP association.

Please refer to the following three figures for the message flow of deactivating USP path in pathset over SCTP.

Figure 3 Deactivate a path in pathset if it is not last INSV path

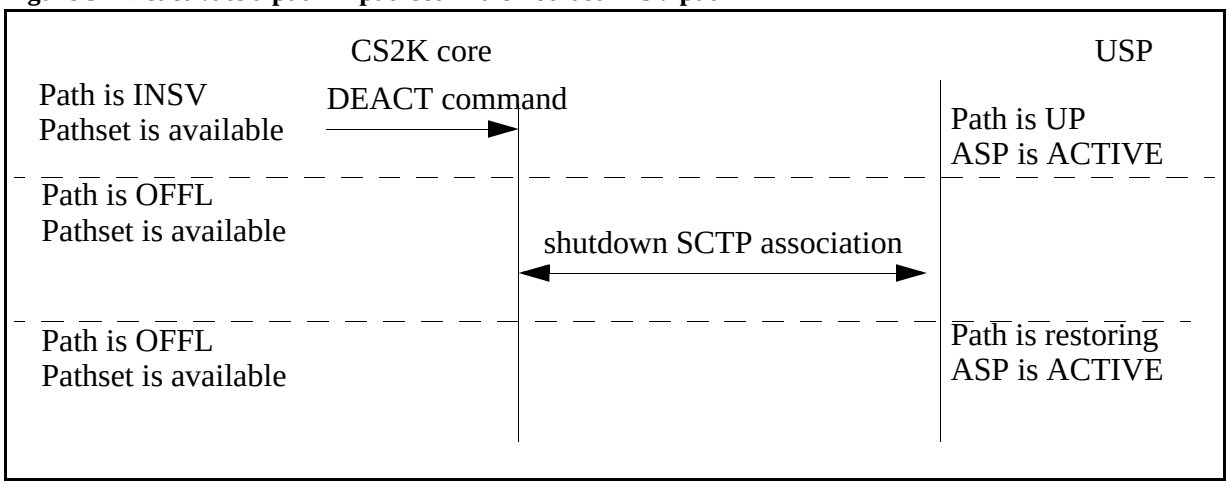


Figure 4 Deactive the last INSV path in the pathset

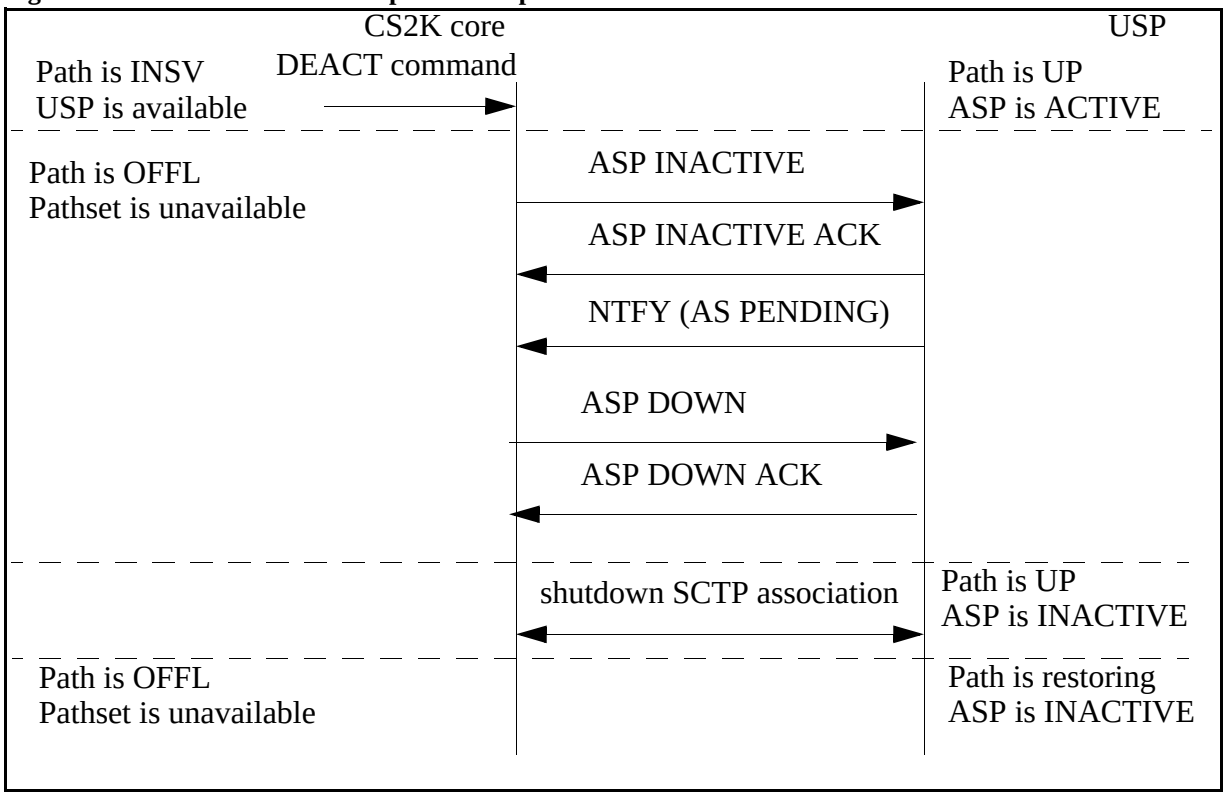


Figure 5 Deactivate a SYSB path if SCTP association is established

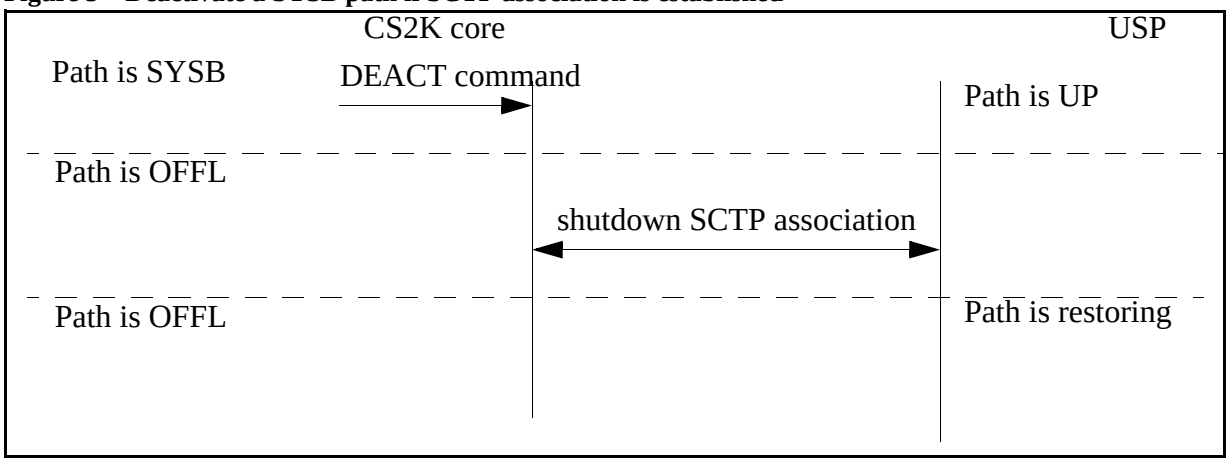
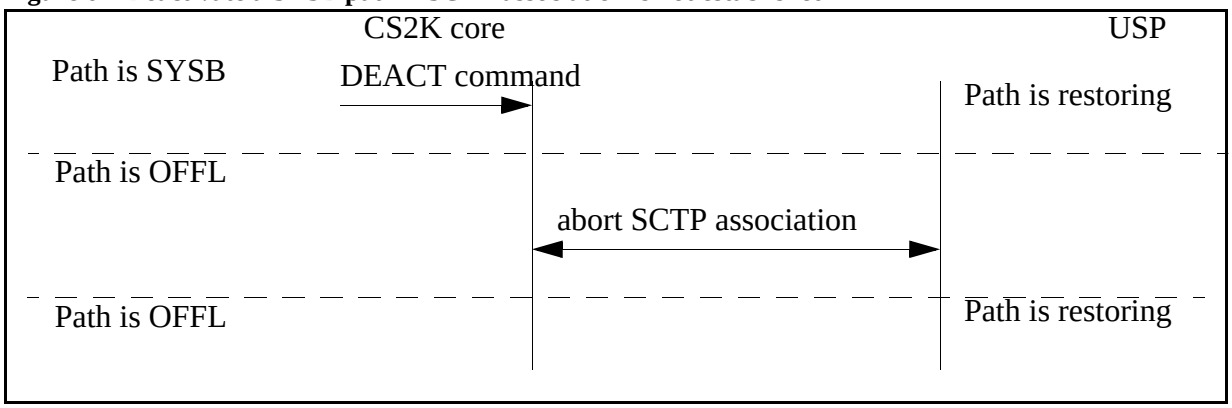


Figure 6 Deactivate a SYSB path if SCTP association is not established



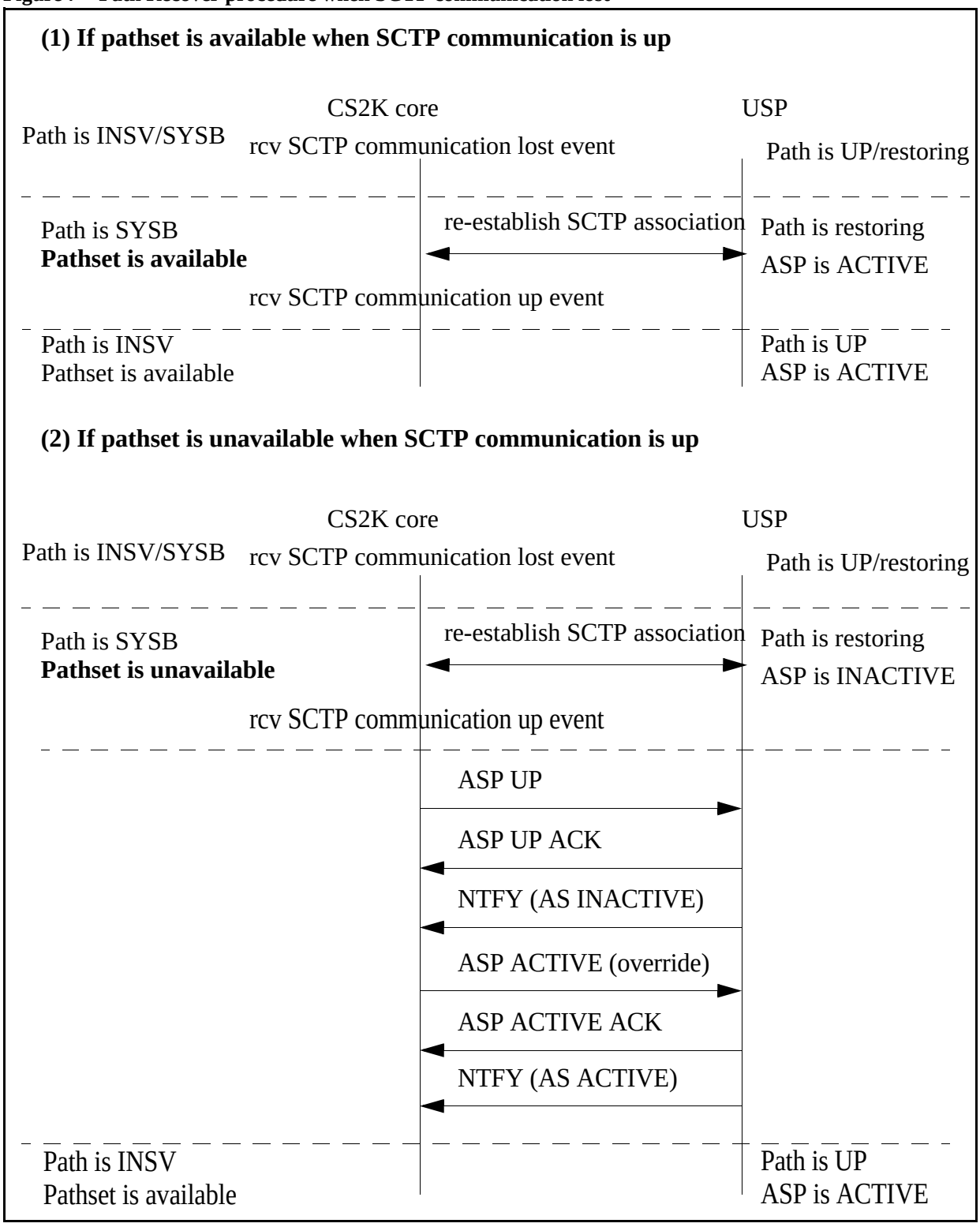
35.4.6.3 SCTP communication lost recovery

On reception of SCTP communication lost notify, M3UA management shall request the SCTP transport layer to re-establish the SCTP association.

If the pathset is unavailable when the SCTP communication is up, ASP UP and ASP ACTIVE procedure is started, otherwise, set the path to INSV.

Refer to the following figure for message flow of SCTP communication lost recovery.

Figure 7 Path Recover procedure when SCTP communication lost



35.4.6.4 SCTP congestion handling

Receiving SCTP STATUS CHANGE notification with congestion enter indication from one path in the pathset indicates that other paths in the pathset have the same situation because the paths are load sharing.

On reception of first path congestion indication, the pathset is regarded as congestion, M3UA layer notify the routeset management to update the status of the routeset related with pathset. The routeset status is updated as if received a SCON from USP. When all of the paths are out of congestion, the routeset management is notified. The routeset status related with the pathset is updated as if received a DAVA from USP.

35.4.6.5 SCTP stream mapping

M3UA RFC supports 2 outgoing SCTP streams.

- M3UA DATA message is sent over SCTP stream 1.
- ASPSM, MGMT messages are sent over SCTP stream 0.
- SSNM, ASPTM, BEAT ACK are sent over SCTP stream 0.

If the remote peer can not support 2 incoming streams, M3UA should take down the association.

35.4.6.6 Notify handling procedure

When receiving a Notify message reflecting a change in the AS state from USP, the CS2K core updates the local USP status and restart the ASP UP procedure if necessary. Please refer to the table below for Notify handling on CS2K core.

Table 6 Notify handling

Notify message	Status of paths	Action
AS ACTIVE	At least one path is INSV	No furthur action is taken.
AS ACTIVE	No path is INSV	Set the non OFFL paths to SYSB and start path activation procedure and sent out ASP UP message.
AS INACTIVE	In all cases	Set the non OFFL paths to SYSB and start path activation procedure and sent out ASP UP message.
AS PENDING	In all cases	Set the non OFFL paths to SYSB and start the path activation procedure and sent out ASP UP message

35.4.6.7 SSNM message handling procedure

DAUD is sent to USP periodly to audit the status of routesets. When the CS2K core receives DAVA, DUNA, SCON, application level is notified.

When the CS2K core receives DRST, application level is notified as if DAVA is received.

Please refer to activity A00009165-Offline Routesets w/o Alarms for more information on SSNM handling when the routeset is not activated on USP and Core.

35.4.7 M3UA RFC message extension

The PROVISIONING messages and MSC_UPDATE messages, which used as M3UA V2 extension on CS2K core to support communication between CS2K core and USP, will be used unchanged as M3UA RFC extension on CS2K core to support communication between core and USP.

35.4.8 Peg OM for M3UA RFC

The existing M3UA OMs are supported for M3UA RFC.

- TXMSG
- RXMSG
- LOSTMSG

M3UA RFC and M3UA V2 use the same OM counters.

35.4.9 M3UA timers for M3UA RFC

- ASPUP timer

When the status of pathset is changed from SYSB to INSV, ASPUP is sent to USP. ASPUP is resent to USP every 2s utill ASPUP ACK is received from USP.

- ASPAC timer

After received ASPUP ACK from USP, ASPAC is sent to USP. ASPAC is resent every 2s utill ASPAC ACK is received from USP.

- ASPIA timer

When the status of pathset is changed from INSV to SYSB or OFFL, ASPIA is sent to USP. ASPIA is sent for only once. If ASPIA ACK is not received from USP, the ASPIA is not sent again. ASPDN is sent out after ASPIA timer timeout.

- ASPDN timer

After received ASPIA ACK from USP or ASPIA timer timeout, ASPDN is sent to USP. ASPDN is sent for only once. If ASPDN ACK is not received from USP, the ASPDN is not sent again. SCTP association is taken down after ASPDN timer timeout.

35.4.10 Max message rate supported

The message rate that one M3UA RFC path can support is up to 1500 msg/sec.

The total message rate of all M3UA RFC paths over SCTP **SHOULD** be less than the max message rate that SCTP on core can support. Currently the max message rate that SCTP can support is 4500 msg/sec. Please refer to activity A00003649 “SCTP (Stream Control Transmission Protocol) Enhancements on XA-Core” for more detail.

35.4.11 Cutover from M3UA V2 pathset to M3UA SCTP pathset

This cutover procedure is used to change the in-service M3UA V2 pathset to M3UA SCTP pathset. This cutover MUST be done with low traffic.

1. Make sure at least **two** paths are provisioned in the M3UA V2 pathset. All of the paths are INSV.

2. Deactivate one of the M3UA_V2_UDP path in the pathset. The status of the path is OFFL now.

3. Change the pathprot from M3UA_V2_UDP to M3UA_RFC_SCTP_*. The pathprot M3UA_RFC_SCTP_* could be M3UA_RFC_SCTP_CLIENT or M3UA_RFC_SCTP_SERVER.

4. Activate the path in MAPCI. Verify the status of the path is INSV now and traffic are sent to the path.

5. Soak for some time. The time depends on customer’s decision.

6. Repeat step 2-5 for other M3UA_V2_UDP paths in the pathset.

Note: it is not recommended provisioning different type paths in one pathset. The cutover status should be regarded as a transient status. During cutover, there is no traffic change over between paths, which will cause traffic lost when the path is being deactivated.

35.4.12 Rollback from M3UA SCTP pathset to M3UA V2 pathset

This rollback procedure is used to restore the paths to M3UA_V2_UDP paths in case any problem during cutover.

1. Deactivate one of the M3UA_RFC_SCTP_* path in the pathset. The status of the path is OFFL now.

2. Change the pathprot from M3UA_RFC_SCTP_* to M3UA_V2_UDP. The pathprot M3UA_RFC_SCTP_* could be M3UA_RFC_SCTP_CLIENT or M3UA_RFC_SCTP_SERVER.

3. Activate the path in MAPCI. Verify the status of the path is INSV now and traffic are sent to the path.

4. Repeat step 1-3 for other M3UA_RFC_SCTP_* paths in the pathset.

Note: it is not recommended provisioning different type paths in one pathset. The cutover status should be regarded as a transient status. During cutover, there is no traffic change over between paths, which will cause traffic lost when one path is being deactivated.

35.5 Hardware Requirements or Dependencies

NA

35.6 Software Requirements or Dependencies

NA

35.7 Limitations and restrictions

1. This activity implements a basic functionality of M3UA RFC on CS2K core. Only those functionalities mentioned in this document are commited by this activity.

2. This activity doesn’t support dynamic register procedure (RFC3332 section 4.4) on CS2K core.

3. There is no changes introduced in the Core swact mechanism for SCTP and M3UA connections. The existing behavior is expected during SWACT after this activity.

4. There is no changes introduced into the path load sharing mechanism. The existing behavior is expected after this activity.

5. When the path is datafilled as SCTP server, the port used to listen for INIT chunk is not 2905, it can be from 4697-4700 to 4710-4721.

6. It is not recommended provisioning different type paths in one pathset. The cutover status should be regarded as a transient status.

7. There is no traffic change over between paths, which will cause traffic lost when one path is being deactivated.

8. SCTP CRC32 checksum is not supported in Core. Adler checksum should be used to establish SCTP association.

35.8 Interactions

NA

35.9 Glossary

Term	Description
ASPSM	ASP State Maintenance
ASPTM	ASP Traffic Maintenance
M3UA	Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) -User Adaptation Layer
OOTB	Out of Blue
SCTP	Stream Control Transmission Protocol
SCTP v5	SCTP version5
SG	Signaling Gateway
SSNM	SS7 Signalling Network Management
TCB	Transmission Control Block
TCP	Transmission Control Protocol
TLV	Type-Length-Value Coding Format
TSN	Transmission Sequence Number
UDP	User Datagram Protocol

35.10 Reference

1. RFC3332 Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) -User Adaptation Layer (M3UA), September 2002

2. M3UA Implementor's Guide, V7, February, 2004

3. RFC2960 Stream Control Transmission Protocol, October 2000

4. Stream Control Transmission Protocol (SCTP) Implementer's Guide, V12, October 15, 2004

5. <draft-ietf-sigtran-m3ua-02.txt> SS7 MTP3-User Adaptation Layer (M3UA)

6. <draft-ietf-sigtran-sctp-05.txt> Simple Control Transmission Protocol

7. A00009164- USP Supports Multiple CS 2000s
8. A00009159- USP Mated Pair Supporting Mult CS2000s (PREP)
9. A00009165- USP - Offline Routesets w/o Alarms

36: Functional Description (FN): A00009173

36.1 Feature name and Feature ID

A00009173: Linux <-> SOS Messaging

36.2 Description

1. Define a Linux CA process <-> SOS messaging framework that is data generic, fast, reliable, and expandable. Provide tools to verify correct operating behavior.
2. Convert existing ApplMan/APPLSOS HPTLI user to use the framework, in order to improve robustness and reduce HPTLI IO class process realtime used.

This feature includes a Compact Call Agent (CCA) and Siren Call Agent (SCA) phase. The SCA phase provides additional capabilities including:

1. TIPC support
2. Multiple service support
3. Siren Availability Management Framework (AMF) support

Functionality is always enabled, and cannot be disabled.
Password protected CI (SOS2CACI) is intended for designer/GNPS purposes only.

36.3 Hardware Requirements or Dependencies

No new H/W dependencies.
CCA phase runs on the CompactPCI hardware.
SCA phase runs on Siren/ATCA hardware.

36.4 Software Requirements or Dependencies

CCA phase delivers on NCGL8/SN09 release lineup.
SCA phase delivers on NCGL9/SN10 release lineup.

For lab purposes, NCGLx is coded to support earlier SOS image releases in addition to the intended lineups described above.

36.5 Limitations and restrictions

No limitations or restrictions visible to the user - it is an internal feature.

36.6 Interactions

No interactions with existing features.

36.7 Glossary

Term	Description
ATCA	Advanced Telecommunications Computing Architecture. Hardware Standard: Midplane/chassis/electrical etc.
CCA	Compact Call agent. AKA: CS2K, 3PC - compactPCI Hardware
SCA	Siren Call Agent ATCA Hardware/Software

37: Functional Description (FN): A00009182

37.1 Feature name and Feature ID

Nortel Carrier Grade Linux Persistent Memory Application Programming Interface.

37.2 Description

This feature will create a unified API to access all persistent memory in NCGL products. The API will exist in the kernel and will be exported to user space through a new persistent memory driver. Persistent memory users in the kernel and in user space in all products which have persistent memory will be updated to use the new API.

There are three methods for writing to persistent memory which are being supported. The first method, mmapping, is only used by user space applications. This allows any user space application to request a chunk of persistent memory and then write to it as if the memory was obtained through a malloc request. Users of this method include DSSAVE, VFOOT and the Neptune Persistent Memory API.

The second method is through a write request. When a user wants to write to persistent memory they will issue a write request. The API will then update persistent memory with the data according to the options configured during registration. Some of these options include writing to the active buffer, writing to per-cpu buffers, or writing fixed size logs. Users of this method include kernel fault handling, sanity timers, bigfoot, etc.

The final method is only available to the kernel. The kernel users will register a special handle with the API. The special handle contains pointers describing the region. The API will update the handle with the location of the desired region in persistent memory and store a pointer to the handle. Then the user can use the pointers in the handle to write logs. Since the API has a pointer to the handle, it is able to update the pointers when a rotation occurs. This method is being provided for users that need to be extremely fast and cannot wait on a spinlock for data synchronization. Users of this method include kernel scheduler history and kernel exception history.

The memory is divided up into user defined partitions, which may be divided further depending on the user specifications. If the user specifies one or more

blocks then the partition data is divided evenly into blocks. Only one block is written to at any given time and is considered active. Users can provision regions within the blocks to store data for a particular application. Each region exists at the same location in all blocks.

API users will be able to provision the following attributes for log regions:
- Fixed or variable size logs
- Separate logs areas for each processor or a single area (variable size logs must have a single area)

The API will provide the following functionality to the user:
- Register a partition: Reserve a section of persitent memory
- Register a log region: Reserve a section of a block in a partition
- Rotate a partition: Make an inactive block active
- Lock a block: Take block out of rotation
- Unlock a block: Allow block to be in rotation
- Read data: Read data from persistent memory
- Write log or data: Write a log or data to persistent memory
- Mmap memory: Mmap a section of memory to userspace
- Seek to location: Set the offset for reading
- Set reset flag: Reset persistent memory on next reboot

In order to use persistent memory, the user will have to register a partition with a unique partition string identifier. If the partition will be used for logs then the user will also have to register a region within the partition. Then the user will be able to use one of the three methods described above to begin writing to persistent memory.

In order to detect corruption, all element headers in persistent memory will have checksums. These checksums will only be validated during initialization.

During an upgrade from a release that does not support the API, the API will detect that the memory format is incorrect and will re-initialize persistent memory. Subsequent upgrades will not need to re-initialize persistent memory unless the format of peristent memory changes.

The persistent memory device driver will export the kernel API to userspace. It will keep track of any open handles for a user session and create buffers for copying data to and from userspace during reading and writing. When userspace wants to interact with persistent memory, they will have to open the persistent memory device, issue an IOCTL to set the area that they are interested in and then write or mmap to the device. The following is a list of file operations that are supported by the driver:
- read
- write
- ioctl

- mmap
- seek
- open
- release

The following is a list of persistent memory driver IOCTLs and their arguments:

- PMEMSETCB: Setup the device to perform operations on the control block
  No arguments
- PMEMSETPART: Setup the device to perform operations on a partition
  ```
  struct pmem_set_part
  {
     char desc[32];      // Partition string id
  };
  ```
- PMEMSETBLK: Setup the device to perform operations on a block. Device must be set to a partition.
  ```
  struct pmem_set_block
  {
     __s8;      // Block id
  };
  ```
- PMEMSETREG: Setup the device to perform operations on a region. Device must be set to a partition.
  ```
  struct pmem_set_region
  {
     char desc[32];      // Region string id
     __u8 block_id;
  };
  ```
- PMEMSETSHADOW: Setup the device to perform operations on the shadow copy of persistent memory.
  No arguments
- PMEMCLRSHADOW: Clear the shadow copy of persistent memory
  No arguments
- PMEMREGPART: Register a partition
  ```
  struct pmem_reg_log_part
  {
     char desc[32];         // Partition string id
     __u32 size;            // Size of partition data
     __u16 num_blocks; // Number of blocks in partition. 0 for mmap
     __u8 version;          // Version of partition
  };
  ```
- PMEMREGLOGREGION: Register a log region. Device must be set to a partition.
  ```
  struct pmem_reg_region
  {
  ```

```
    char desc[32];      // Region string id
    __u32 size;         // Size of region data
    __u32 flags;        // See below for flags
    __u32 fixed_size;  // Size of fixed size logs. 0 for variable size logs
   __u16 num_log_desc; // Number of variable size logs descriptors.
    __u8 version;       // Version of region
    __u8 block_id;      // Block id for resulting region handle.
};
```

PMEM_REGION_FLAG_PERPROC: Specifies that each processor writes to its own area in the region. Only valid for fixed size logs. PMEM_REGION_FLAG_STOP_FULL: Specifies that persistent memory will stop writing when the logs are full. Only valid for fixed size logs.

- PMEMROTATE: Rotate a log partition. Device must be set to a log partition.

```
__u8 lock;     // 0 to leave block unlocked, 1 to lock old block.
```

- PMEMLOCKBLK: Lock a log block. Device must be set to a block.

  No arguments
- PMEMUNLOCKBLK: Unlock a log block. Device must be set to a block.

  No arguments
- PMEMSETRESET: Sets the control block reset flag. Device must be set to the control block.

  No arguments
- PMEMCLRRESET: Clears the control block reset flag. Device must be set to the control block.

  No arguments
- PMEMGETCBINFO: Retrieves control block data. Device must be set to the control block.

```
struct pmem_cb_info
{
   __u32 size;
   __u32 avail_mem;
   __u16 num_partitions;
};
```

- PMEMGETPARTINFO: Retrieves partition data. Device must be set to a partition.

```
struct pmem_part_info
{
   __u32 size;
   __u32 avail_mem;
   __u16 num_blocks;
   __u16 num_regions;
};
```

In order to get logs, the user will have to decode the log structures in the region data. These structures contain the log data, as well as some information that

was obtained when the log was generated such as the timestamp and a log checksum. The structures are different for fixed size logs and variable size logs. The fixed size logs contain a small header for each cpu (or just one header if the logs are not per-proccessor), which describe the boundaries of the log area. Logs are then located one after the other.

The variable size log structures contain an array of log descriptors which describe the individual logs. Each log descriptor contains a time stamp, a checksum of the log data and the location of the log data in the region.

Table 1 Log Region Data With Log Descriptors Structure

Element	Type	Description
Region Description	char x[32]	Identifier for region
Last index	__u16	Index of last valid log
Current index	__u16	Index of current log
Checksum	__u32	Checksum of index information
Log 0 Offset	__u32	Offset of log from start of region data
Log 0 Size	__u32	Size of log data
Log 0 Time stamp	__u64	Time of log
Log 0 Log checksum	__u32	Checksum of log data
Log 0 Checksum	__u32	Checksum of log header data
...		
Log X Offset	__u32	Offset of log from start of region data
Log X Size	__u32	Size of log data
Log X Time stamp	__u64	Time of log
Log X Log checksum	__u32	Checksum of log data
Log X Checksum	__u32	Checksum of log header data
Log 0 data	raw	Log data
...	raw	Log data
Log X data	raw	Log data

Table 2 Log Region Data Without Log Descriptors Structure

Element	Type	Description
Region Description	char x[32]	Identifier for region
CPU 0 start offset	__u32	Offset of start of per cpu region from start of region
CPU 0 end offset	__u32	Offset of end of per cpu region from start of region
CPU 0 current offset	__u32	Offset from the start of the region to the current log
CPU 0 logs lost	__u32	Number of logs lost
...		Per cpu information
CPU X start offset	__u32	Offset of start of per cpu region from start of region
CPU X end offset	__u32	Offset of end of per cpu region from start of region
CPU X current offset	__u32	Offset from the start of the region to the current log
CPU X logs lost	__u32	Number of logs lost
CPU 0 Log record 0	struct	Log data
...	struct	Log data
CPU 0 Log record Y	struct	Log data
...	struct	Log data
CPU X Log record 0	struct	Log data
...	struct	Log data
CPU X Log record Y	struct	Log data

All users of persistent memory in the kernel and in userspace will be updated to use the new API. In the kernel this includes:

- Scheduler history
- Exception history
- Fault handling

- Sanity timers
- Persistent panic

In userspace this includes:
- DSSAVE
- VFOOT
- Neptune persistent memory API
- bigfoot
- bigfootd

A new userspace application will be created to manage persistent memory. This program will have the following features:
- Read persistent memory from a file or from the device driver
- Dump persistent memory to a file
- Read and decode all header information
- Read and decode any of the NCGL logging regions
- Lock or unlock a block
- Rotate a partition
- Set or clear the reset bit in the control block
- Read and clear the shadow copy of persistent memory

A program will be created to create backup copies of persistent memory on bootup. The program will check if a shadow copy of persistent memory exists and if so then it will copy the shadow copy to disk. If not then it will copy the entire persistent memory to disk instead. The last five copies of persistent memory will be maintained on disk.

37.3 Hardware Requirements or Dependencies

There are no new hardware requirements being introduced by this feature.

37.4 Software Requirements or Dependencies

There are no new software requirements being introduced by this feature.

37.5 Limitations and restrictions

This feature has the following limitations:
- The total size of persistent memory must be less than 4 GB
- All string identifiers must be less than 32 characters
- The maximum number of partitions is 32
- The maximum number of buffers in a log partition is 32
- The maximum number of regions in a log partition is 32
- The maximum number of variable size logs in a region is 65535
- Intel and MIPS64 architectures are not supported in this release

37.6 Interactions

This feature interacts with the following areas:

- Kernel scheduler history: This will be updated to use the new API for reading and writing logs.
- Kernel exception history: This will be updated to use the new API for reading and writing logs.
- Kernel fault handling: In addition to notifying hwmon that a fault has occurred, fault handling will now write logs to persistent memory.
- Kernel sanity timers: In addition to notifying hwmon that a sanity timeout has occurred, sanity timeout code will now write logs to persistent memory, and will rotate the log partition if a board reset is required.
- Kernel persistent panic: The panic code will no longer attempt to store scheduler and exception information in persistent memory.
- Bigfoot: This will use the new persistent memory driver to read logs from bigfoot.
- bigfootd: This will use the persistent memory driver to retreive bigfoot information. It will no longer initialize persistent memory with the bigfoot driver.
- DSSAVE: This will use the persistent memory driver to mmap memory instead of the dssave driver.
- VFOOT: This will use the persistent memory driver to mmap memory instead of the bigfoot driver.
- Neptune Persistent Memory API: This will use the persistent memory driver to mmap memory instead of the bigfoot driver.
- hwmon: This will no longer attempt to write logs to persistent memory when a sanity timeout or a fault occurs.

37.7 Glossary

Term	Description
New term	Definition

38: Functional Description (FN): A00009189

38.1 Feature name and Feature ID

A00009189 SESM support for 64 character FQDN. Related feature: A00008043 CS2K Support for 64 Character FQDN

38.2 Description

This feature makes enhancements on SESM & CS2K to make the whole system fully support Gateway FQDN up to 64 characters.

In SN07/SN08, FQDN support was introduced into CS2K system. But the solution had a number of limitations. The size of the gateway FQDN and domain name were restricted. Only a single domain name was supported per GWC, and only the hostnames were used in the CS2K-MT GUI, OSSGATE, TMM, and LMM.

This SN09 feature is intended to remove those limitations while still maintaining backwards compatibility:

- Multiple gateway domain names are supported per GWC as part of the Gateway Name field as long as default gateway domain name is not provisioned on the GWC. In this case, the Gateway Name represents a gateway FQDN and can be up to 64 characters.
- Only one default gateway domain name (up to 62 characters) can be provisioned per GWC. If provisioned, then the Gateway Name represents the gateway hostname. The FQDN is the concatenation of the Gateway Name and the default domain name, which together can contain up to 64 characters.
- The customer can use the Gateway Name as a hostname or a FQDN in CS2K-MT GUI, OSSGate (excepts SERVORD+ commands), TMM and LMM.
- When GWC has default gateway domain name provisioned, you must use only the gateway name in all OSSGate SERVORD+ commands. Use of FQDN will result in a command failure (eg. "Gateway not found").
- This feature allows Small Lines, TGCP trunks and third party Large Lines gateway to use a free-format, up to 64 characters gateway FQDN.
- Only cable solution gateways support usage of default gateway domain name. Please note provisioning 64 character FQDN using free-format is recommended for “packet cable” gateways.

Table 1 Gateway profiles which support default gateway domain name

Gateway Profile Name	Gateway Profile Name	Gateway Profile Name
MOTOROLAMTA_1	ARRIS_TOUCHTONE_NN01_4	TOUCHTONE_NN01_2
MOTOROLAMTA_2	ARRIS_TOUCHTONE_NN02_4	TOUCHTONE_NN01_3
MOTOROLAMTA_4	TOUCHTONE_NN01_1	TOUCHTONE_NN01_4

38.3 CS2K-MT GUI functionality modifications

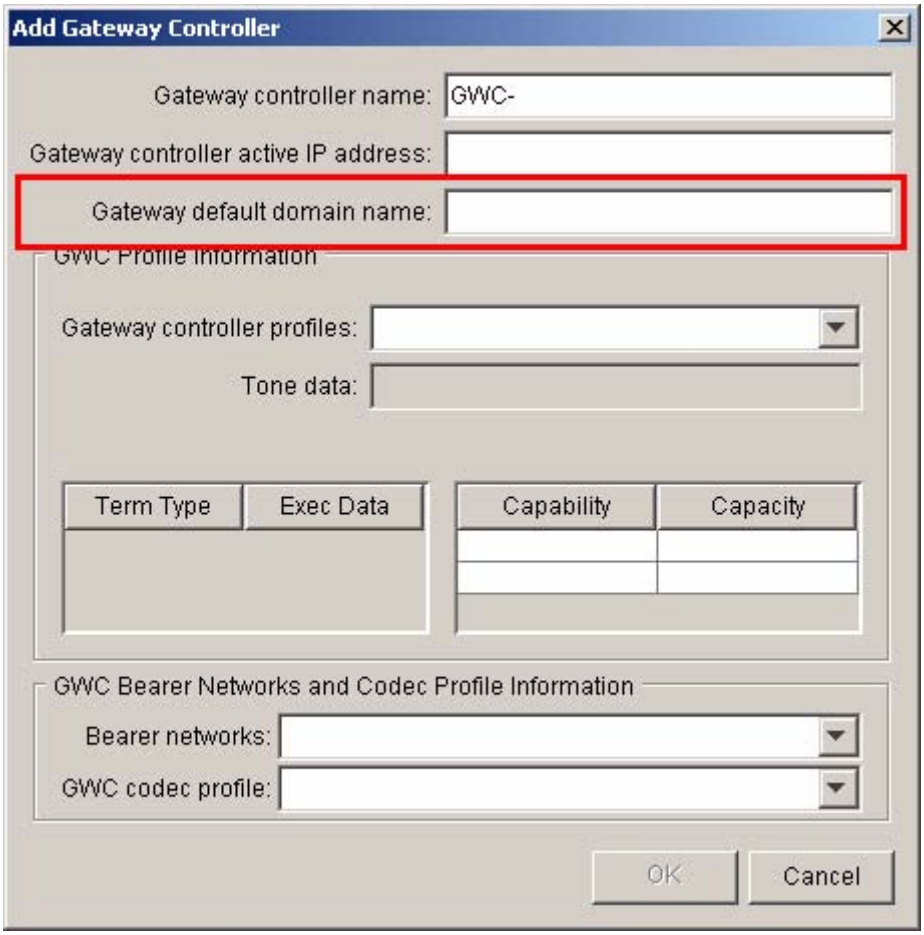
38.3.1 Add GWC node dialog

When adding GWC node, customer could set default gateway domain name. This name only can be used for cable solution gateways (refer to Table 1 on page 345).

If default gateway domain name is provisioned, only cable solution gateways can be associated on this GWC node. Any other gateway association will be rejected. Then the default gateway domain name will be applied to all associated cable solution gateways.

This field can be left empty if user don’t want to set default gateway domain name. In this case, not only cable solution gateways, but also other solution gateways can be associated.

Figure 1 Add GWC node dialog



Caution:

In SN09, only following GWC Profiles support cable solution gateways.

Table 2 SN09 GWC profiles which support cable solution gateways

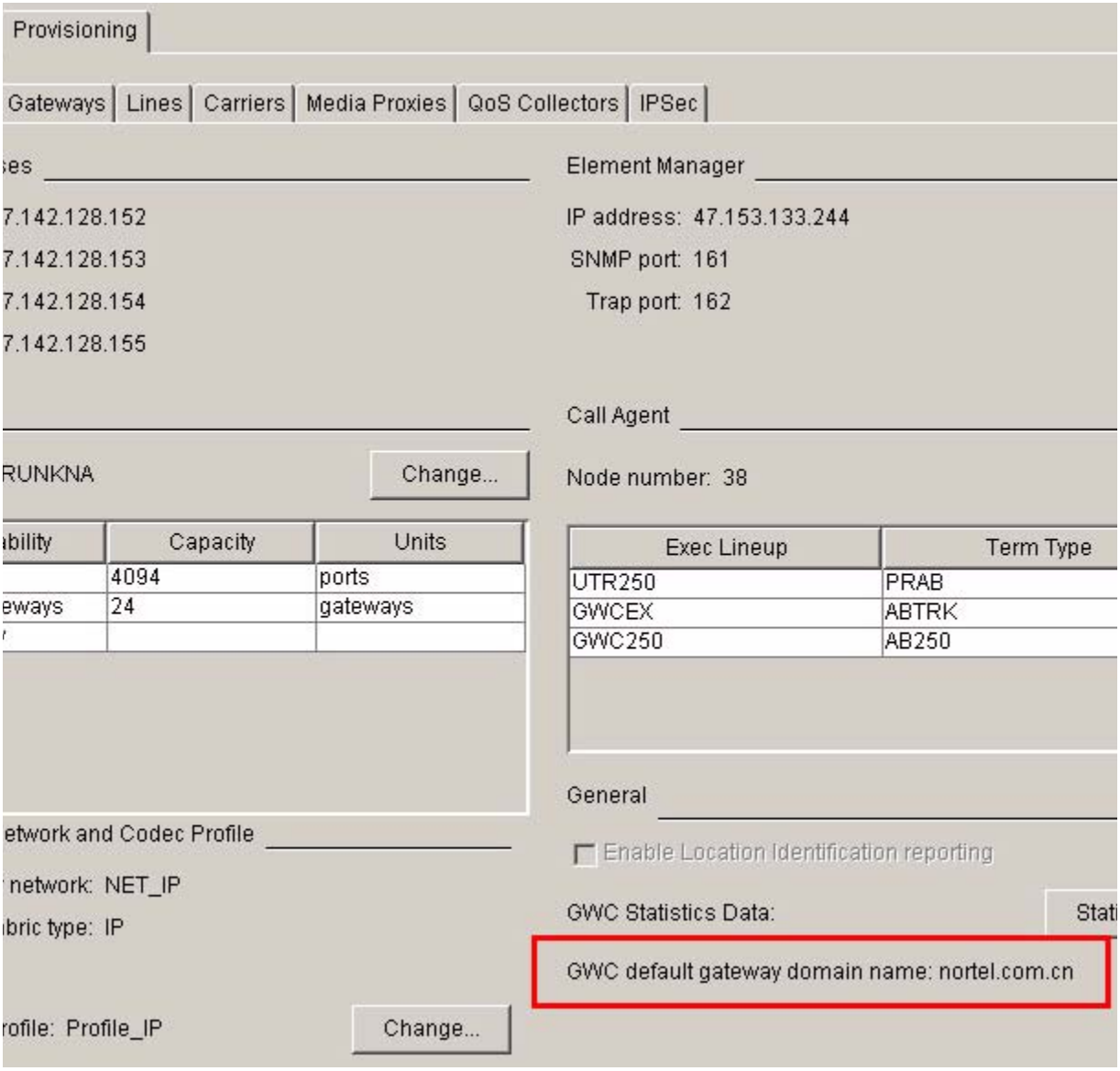
Gateway Contoller Profile Name
SMALL_LINESINTL
SMALL_LINESINTL_V2
SMALL_LINESNA
SMALL_LINESNA_V2

For other GWC Profiles, even if default gateway domain name can be provisioned, but any gateway association to this GWC will be rejected. Therefore, this field should be left empty if other GWC profiles are using, such as Packet Cable solution.

38.3.2 GWC provisioning display panel

If default gateway domain name was provisioned when adding GWC node, the domain name will be displayed on GWC provisioning display panel. If not provisioned, "<Not Configured>" will be displayed.

Figure 2 GWC provisioning display panel



38.3.3 Associate Media Gateway dialog

GUI layout of Associate Media Gateway dialog is not changed. But the usage of “Gateway Name” field is different than before.

38.3.3.1 Has default gateway domain name provisioned

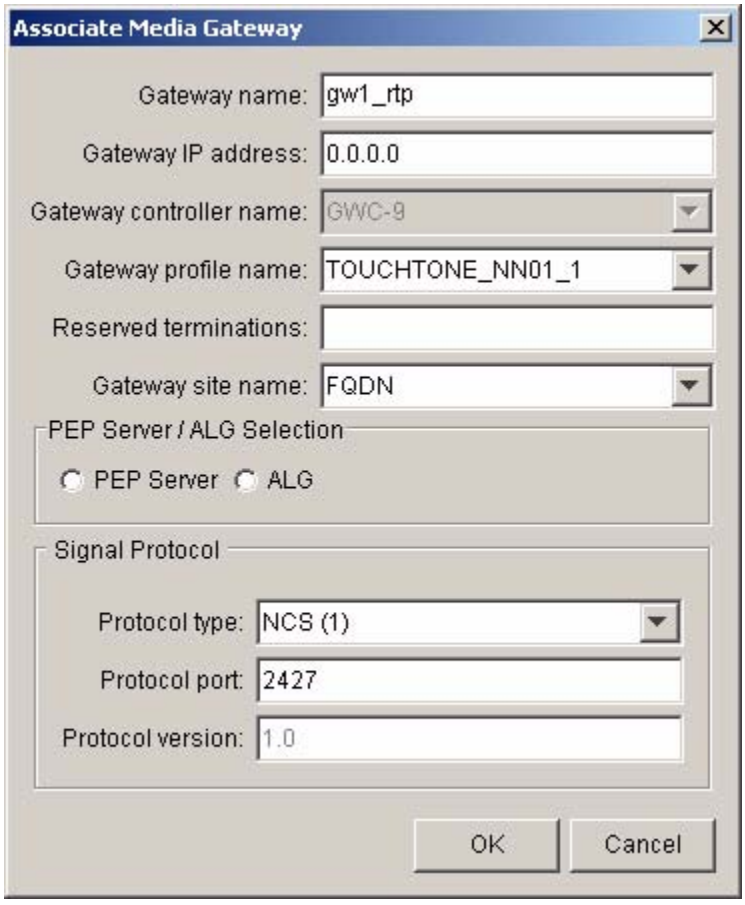
Since SN09, if a default gateway domain name is provisioned on the GWC, only cable solution gateways can be associated on this GWC (refer to Table 1 on page 345). Then the Gateway Name represents the gateway hostname. The FQDN is the concatenation of the Gateway Name and the default domain name, which together can contain up to 64 characters.

For example:

If the default domain name is “**nortel.com**”, And the user needs to provision a gateway with FQDN “**gw1_rtp.nortel.com**”, then input the Gateway Name field as the hostname “**gw1_rtp**”.

In this case, if the gateway is a PacketCable gateway, the Gateway Name "**gw1_rtp**" is downloaded to table LNENDPT on the Core, and it is also used for QoS record.

Figure 3 Associate Media Gateway Dialog



38.3.3.2 No default gateway domain name provisioned

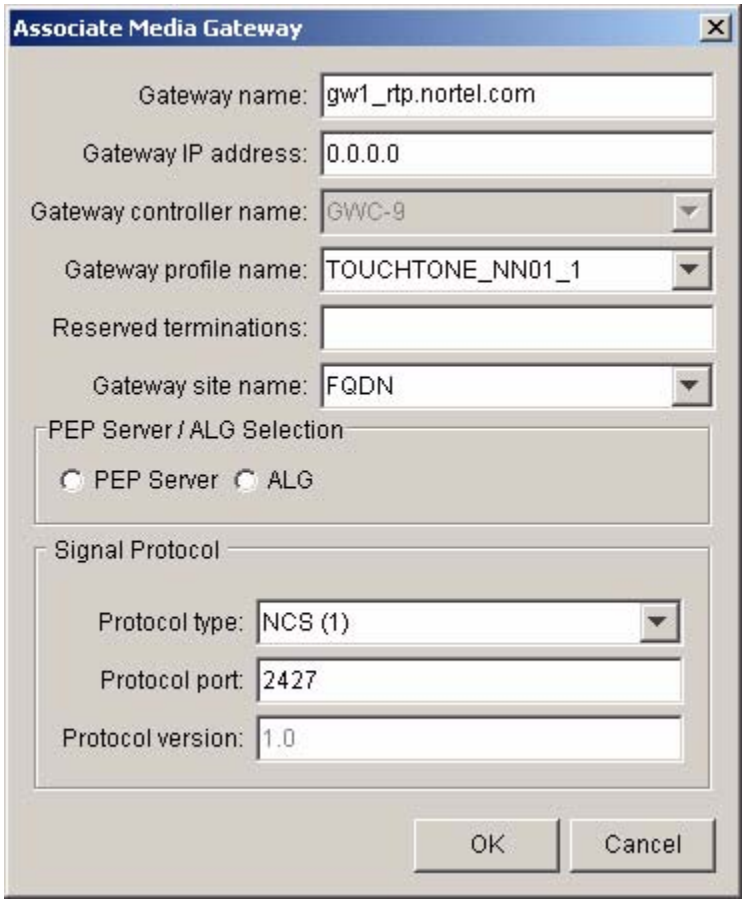
Since SN09, if default gateway domain name is not provisioned, then the Gateway Name represents the gateway FQDN, which can be free-format, up to 64 characters.

For example:

If the default domain name is not set and the user needs to provision a gateway with FQDN "**gw1_rtp.nortel.com**", then input the Gateway Name field as the FQDN "**gw1_rtp.nortel.com**".

In this case, if the gateway is a PacketCable gateway, the Gateway Name "**gw1_rtp.nortel.com**" is downloaded to table LNENDPT on the Core, and it is also used for QoS record.

Figure 4 Associate Media Gateway Dialog



38.3.4 Gateways display panel

On gateways display panel, gateway domain name or part of gateway FQDN can be used as retrieval criteria when querying gateway information. And gateway domain name will be displayed in separate column if provisioned.

38.3.4.1 Use default domain name

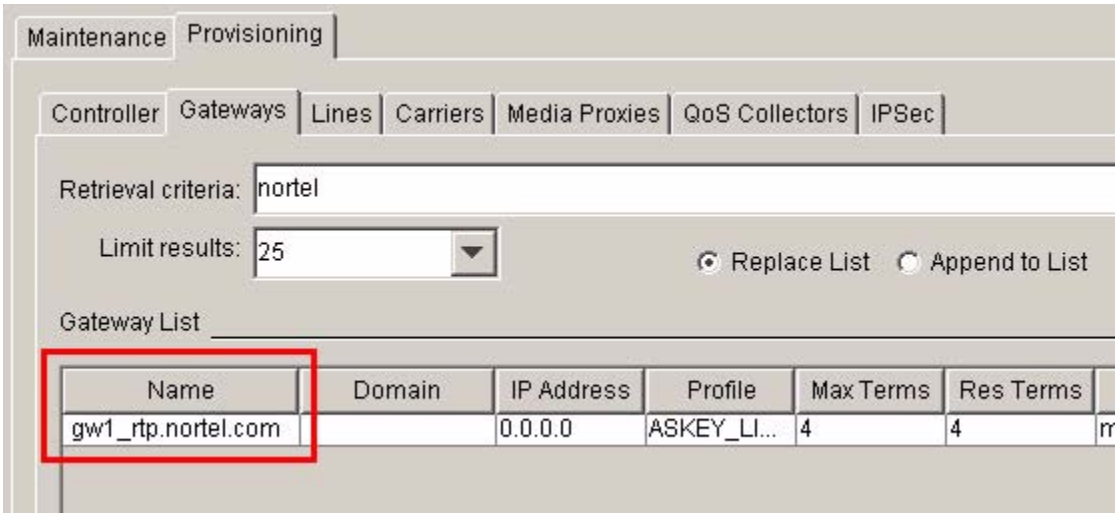
For those gateways using default gateway domain name, the gateway information will be displayed as following figure.

Figure 5 Gateways display panel - Case 1

38.3.4.2 No default domain name

For those gateways do not use default gateway domain name, the gateway information will be displayed as following figure.

Figure 6 Gateway display panel - Case 2



38.3.5 Lines display panel

On lines display panel, gateway domain name or part of gateway FQDN can be used as retrieval criteria when querying line information. And gateway domain name will be displayed in separate column if provisioned.

Figure 7 Lines display panel

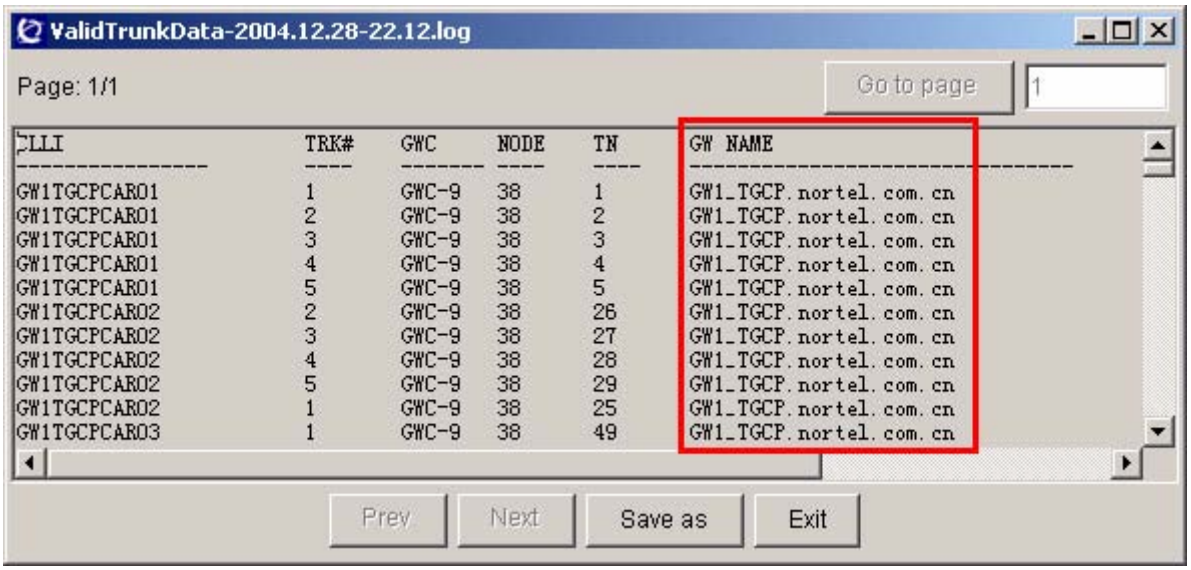
38.3.6 CS2K Audit

In all CS2K audit components (CS2K Data Integrity Audit, Line Audit and Trunk Audit), gateway FQDN can be recognized when running audit process.

If gateway domain name was provisioned, gateway FQDN will be displayed in audit report and possible correct action.

Figure 8 Line Data Integrity Audit report window

Figure 9 Trunk Data Integrity Audit report window



38.4 OSSGate functionality modifications

38.4.1 Nodes Provisioning interface

There are some changes on OSSGate Nodes Provisioning interface:

38.4.1.1 Add GWC node

A new parameter, gwDefaultDomainName, is added in the AddGWC xml command which is allowed user to input the gateway domain name if needed.

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <addGWCtoCS usn="1" version="1.0">
        <Parameters>
          <csUIName>COMPACT6</csUIName>
          <gwcUIName>GWC-10</gwcUIName>
          <profileName>SMALL_LINENA</profileName>
          <gwcActvIp>47.128.142.156</gwcActvIp>
          <gwcSnmpPort>161</gwcSnmpPort>
          <bearerNetworkName>NET_IP</bearerNetworkName>
          <bearerFabricType>IP</bearerFabricType>
          <codecProfileName>Profile_IP</codecProfileName>
          <termType>POTS</termType>
          <termType>KEYSET</termType>
          <execLineup>POTSEX</execLineup>
          <execLineup>KSETEX</execLineup>
          <gwDefaultDomainName>nortel.com.cn</gwDefaultDomainName>
        </Parameters>
      </addGWCtoCS>
    </Methods>
  </Command>
</CommandList>
```

38.4.1.2 Query GWC

The Query GWC OSSGate xml command doesn’t need to be changed, but the response will be changed to include the gateway domain name, if the queried GWC has no domain name, this field will be null.

The QueryGWC response will be like following:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
```

```
<Response>
<Interface>cs2kCfgMgrIf</Interface>
  <Methods>
    <queryGWC usn="1" version="1.0">
    <ReturnData>
      <Row>
        <gwcUIList>GWC-10</gwcUIList>
        <gwcIpList>47.142.128.156</gwcIpList>
        <callServerId>COMPACT6</callServerId>
        <nodeName>GWC 10</nodeName>
        <typeList>1</typeList>
        <typeList>6</typeList>
        <typeList>7</typeList>
        <typeList>15</typeList>
        <typeList>16</typeList>
        <xacNodeNumber>27</xacNodeNumber>
        <actvIpAddress>47.142.128.156</actvIpAddress>
        <snmpPort>161</snmpPort>
        <mktTones>NORTHAA</mktTones>
        <termTypes>POTS</termTypes>
        <termTypes>KEYSET</termTypes>
        <pmExecs>POTSEX</pmExecs>
        <pmExecs>KSETEX</pmExecs>
        <capacity>6400</capacity>
        <externalIP>NOT_YET_SUPPORTED</externalIP>
        <externalPort>0</externalPort>
        <bearerNetworkName>NET_IP</bearerNetworkName>
        <bearerFabricType>IP</bearerFabricType>
        <codecProfileName>Profile_IP</codecProfileName>
        <gwDefaultDomainName>nortel.com.cn</gwDefaultDomainName>
      </Row>
      <RC>0</RC>
      <MsgTxt>Query of a Single GWC was successful</MsgTxt>
    </ReturnData>
    </queryGWC>
  </Methods>
</Response>
</CommandList>
```

38.4.1.3 Query Media Gateway

Although the gateway might be associated with a default domain name, but in the OSSGate QueryMG response, only the gateway host name will be returned.

So no changes was made on QueryMG operation.

38.4.2 Other OSSGate interfaces

For all of other OSSGate interfaces, format of request/response messages are not modified. The only changes are:

- If gateway name is required in the request message, both of gateway name and gateway FQDN can be used.
- If gateway name is filled in request message, the same gateway name will be returned in the response message, no matter if default gateway domain name is provisioned.
- If gateway FQDN is filled in request message, the same gateway FQDN will be returned in the response message (excepts Query Media Gateway interface).

This applies to following OSSGate interfaces:

38.4.2.1 Nodes Provisioning

- disAssocGWC
- disAssocMG
- changeMG
- deleteGWCfromCS

38.4.2.2 Trunk Provisioning

- AddTuple
- DelTuple
- ReplaceTuple
- GetRange
- GetTuple

38.4.2.3 Carrier Provisioning

- AddCarrier
- DeleteCarrier
- GetCarrier
- GetEndpoint
- ListAllCarriers

38.4.2.4 Trunk Maintenance

- PostByGatewayName

- QESByGatewayName
- BSYByGatewayName
- RTSByGatewayName
- INBByGatewayName
- FRLSByGatewayName
- PostByCarrier
- QESByCarrier
- BSYByCarrier
- RTSByCarrier
- INBByCarrier
- FRLSByCarrier
- PostByTrunkClli
- BSYByTrunkClli
- RTSByTrunkClli
- INBByTrunkClli
- FRLSByTrunkClli
- PostGroupDChannelByTrunkClli
- GetTrunkCllisByGatewayName
- GetGatewayNames
- GetCarriers

38.4.2.5 Line Provisioning

All SERVORD+ commands which support GW/endpoint names will NOT support the use of a gateway name which contains the default domain name assigned to the gateway's hosting GWC. If the gateway is provisioned on a GWC which has a default gateway domain name assigned, only the gateway hostname (specified at gateway creation time) may be used in the SERVORD+ command. Examples of commands for such a gateway are as follows:

Gateway "testgwname" is provisioned on a GWC which has a default gateway domain name of "us.nortel.com" assigned.

Supported Hostname only:

EST $ DLH 5200999 1FR Lata1 0 ***testgwname*** aaln/1 ***testgwname.1*** aaln/1 $ DGT $ 3

QTP ***testgwname*** aaln/1

Unsupported FQDN:
EST $ DLH 5200999 1FR Lata1 0 ***testgwname.us.nortel.com*** aaln/1 ***testgwname.1.us.nortel.com*** aaln/1 $ DGT $ 3

QTP ***testgwname.us.nortel.com*** aaln/1

Query output will always provide FQDN information if available in the GWCEM if the gateway is initially provisioned with a FQDN (ie. does not use the a GWC's default gateway domain name). If the gateway is provisioned on a GWC which has a default gateway domain name assigned, then only the hostname entered at gateway provisioning time will be returned in the query output.

38.4.2.5.1 Limitations

Gateways which are provisioned with domain information imbedded within the user provided hostname and assigned to GWCs without a default gateway domain name, will always return the user-assigned, domain-imbedded name in queries and will always require the user-assigned, domain-imbedded name in non-query commands (eg. NEW, OUT, etc..).

Example 1:
A user associates gateway ***"testgwname.us.nortel.com"*** to GWC-0. GWC-0 is *not configured* with a default gateway domain name. When the gateway is provisioned in this manner, all SERVORD+ queries (QLEN/QDN/QTP/etc) will return ***"testgwname.us.nortel.com"*** in ouput and all SERVORD+ non-query commands (NEW/EST/OUT/etc) will require ***"testgwname.us.nortel.com"*** in the relevant command string.

Query command and output format:

```
> QTP testgwname.us.nortel.com aaln/4
------------------------------------------------------------------
---
LEN:     UAIP  00 0 00 03
END POINT: testgwname.us.nortel.com  aaln/4
TYPE: SINGLE PARTY LINE
SNPA: 613
DIRECTORY NUMBER:     6210003
LINE CLASS CODE:      1FR
IBN TYPE: STATION
CUSTGRP:           RES1     SUBGRP: 0  NCOS: 0
SIGNALLING TYPE:  DIGITONE
LINE TREATMENT GROUP:     77
LINE ATTRIBUTE INDEX:     77
XLAPLAN KEY :   613_PKDK_1            RATEAREA KEY :  L619_LATA1_20
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: N
PM NODE NUMBER     :    127
```

```
PM TERMINAL NUMBER :    4
OPTIONS:
DGT PIC 250CAR Y
RES OPTIONS:
CXR CTALL N STD
OFFICE OPTIONS:
SRA
------------------------------------------------------------------------
---
>
```

NON-Query Formats allowed:

EST $ DLH 5200999 1FR Lata1 0 ***testgwname.us.nortel.com*** aaln/1 ***testgwname.us.nortel.com*** aaln/2 $ DGT $ 3

Gateways which are provisioned without domain information imbedded within the user provided hostname and assigned to GWCs which specify a default gateway domain name, will always return the user-assigned host name in queries and will always require the user-assigned host name in non-query commands (eg. NEW, OUT, etc..).

Example 2:
A user associates gateway ***"testgwname.1"*** to GWC-0. GWC-0 is *configured* with a default gateway domain name ***"ibm.com"***. When the gateway is provisioned in this manner, all SERVORD+ queries (QLEN/QDN/QTP/etc) will return ***"testgwname"*** in output. Non-query SERVORD+ commands (NEW/EST/OUT/etc) will allow only ***"testgwname.1"*** in the relevant command string.

Query command and output format:

> QTP ***testgwname.1*** aaln/4
yields

```
------------------------------------------------------------------------
---
LEN:     UAIP  00 0 00 03
END POINT: testgwname  aaln/4
TYPE: SINGLE PARTY LINE
SNPA: 613
DIRECTORY NUMBER:     6210003
LINE CLASS CODE:      1FR
IBN TYPE: STATION
CUSTGRP:           RES1     SUBGRP: 0  NCOS: 0
SIGNALLING TYPE:  DIGITONE
LINE TREATMENT GROUP:     77
LINE ATTRIBUTE INDEX:     77
```

```
XLAPLAN KEY :   613_PKDK_1              RATEAREA KEY :  L619_LATA1_20
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: N
PM NODE NUMBER     :    127
PM TERMINAL NUMBER :    4
OPTIONS:
DGT PIC 250CAR Y
RES OPTIONS:
CXR CTALL N STD
OFFICE OPTIONS:
SRA
------------------------------------------------------------------------
---
>
```

NON-Query Formats allowed:

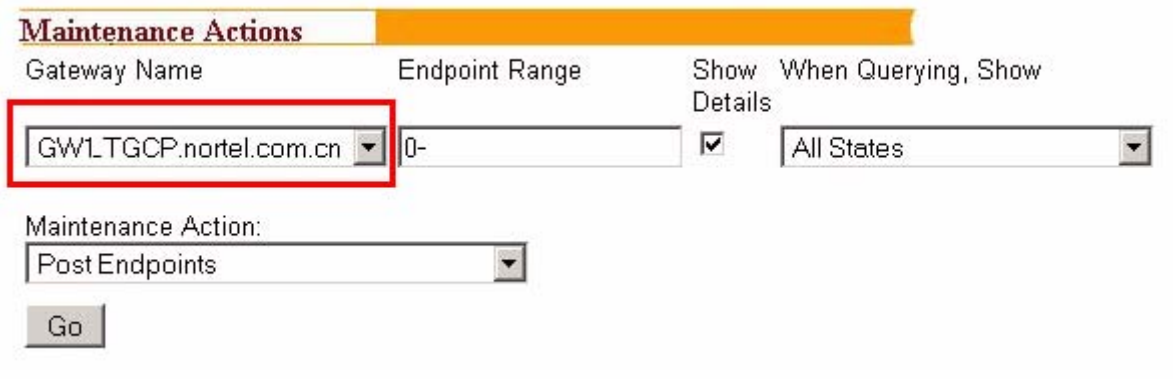
```
EST $ DLH 5200999 1FR Lata1 0 testgwname.1 aaln/1 testgwname.1 aaln/2
$ DGT $ 3
```

38.5 TMM functionality modifications

38.5.1 Maintenance By Gateway Name

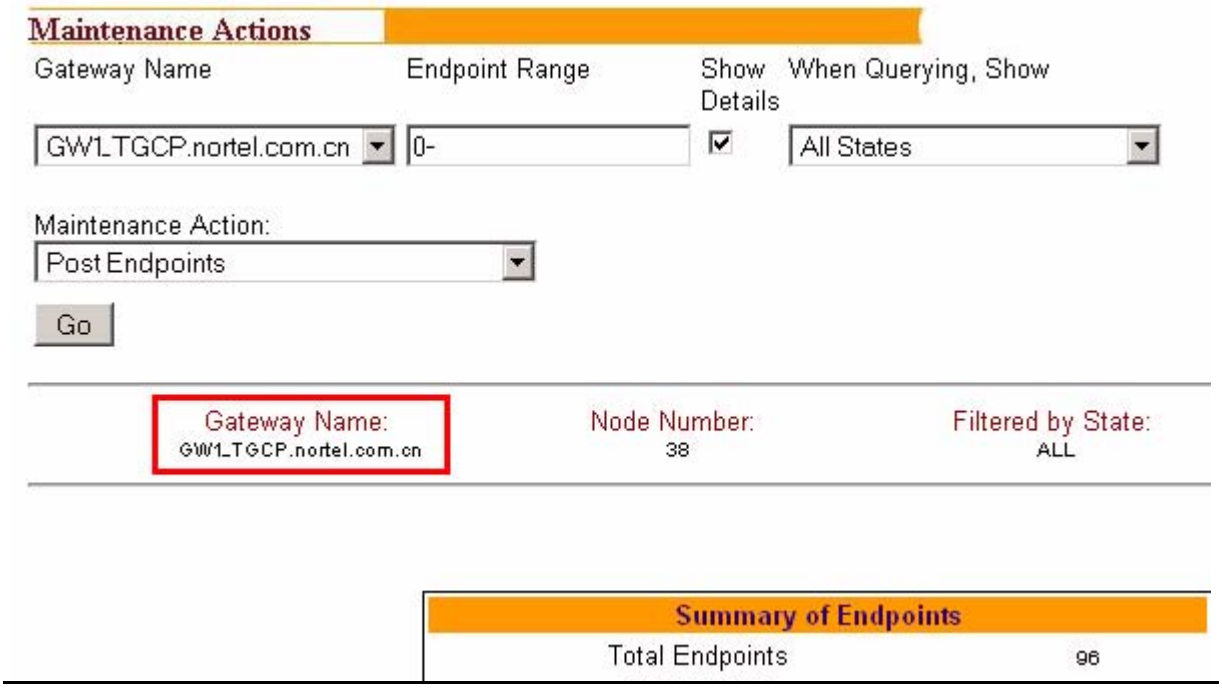
In SN09, gateway FQDN up to 64 characters will be automatically retrieved and displayed on TMM GUI.

Figure 10 FQDN gateway name retrieval - MtcByGatewayName



If user performs maintenance actions such as Post and Busy, Gateway FQDN will be displayed on state output.

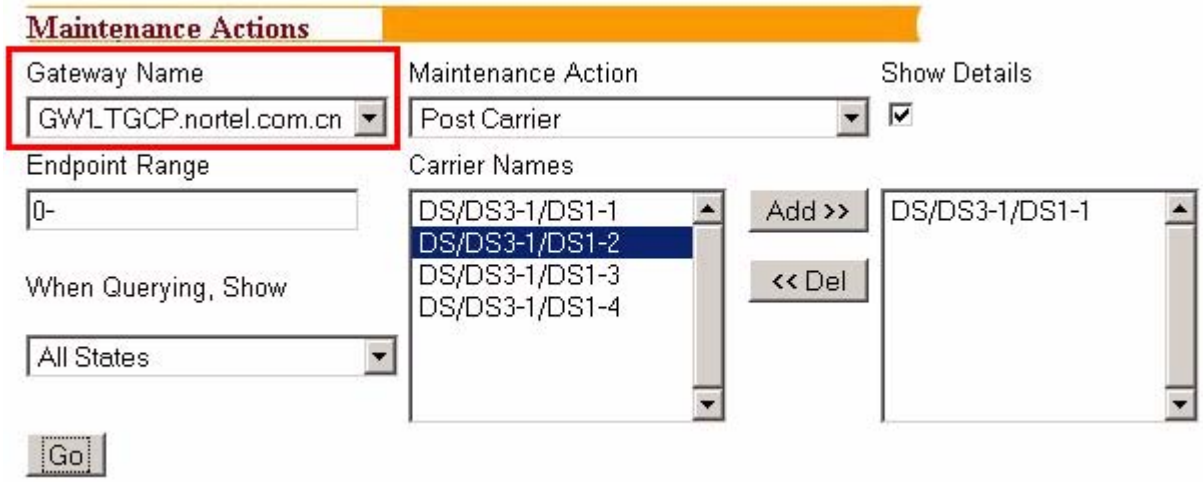
Figure 11 Mtc by Gateway Name state output



38.5.2 Maintenance By Carrier

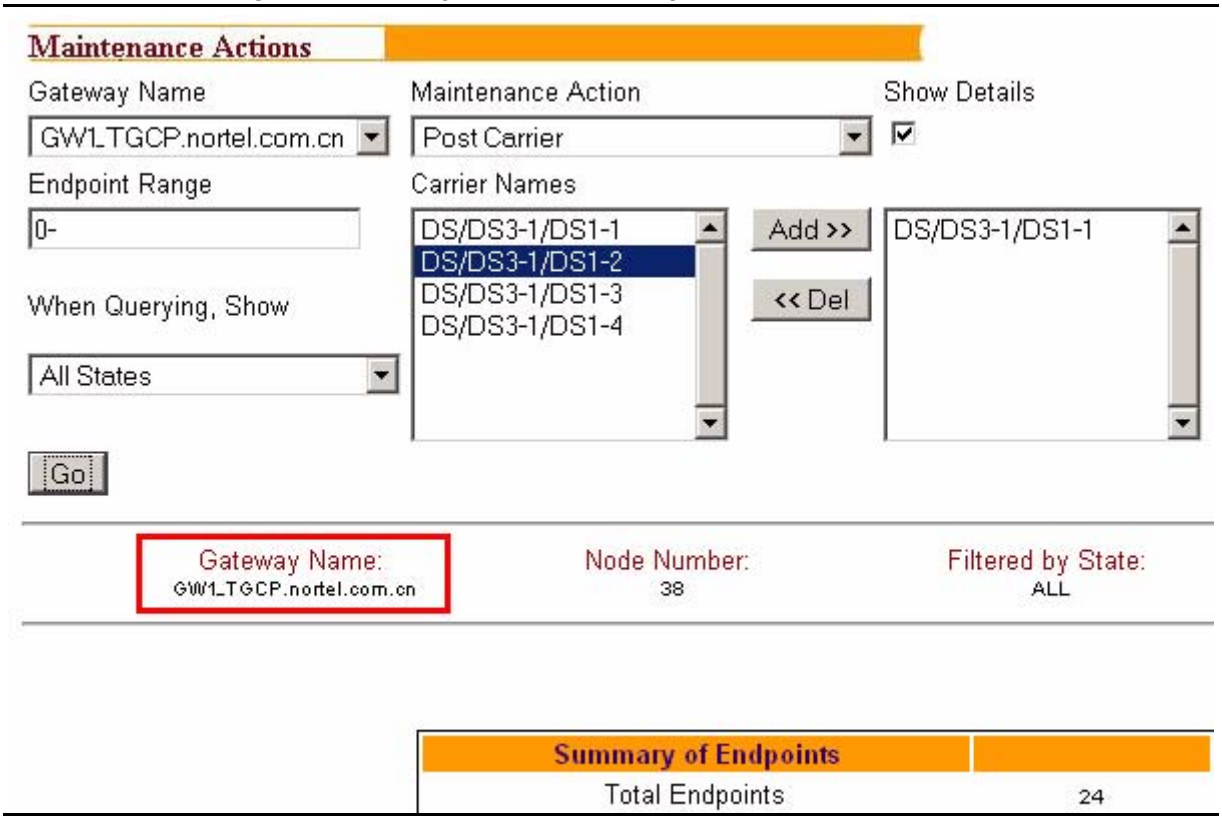
In SN09, gateway FQDN up to 64 characters will be automatically retrieved and displayed on TMM GUI.

Figure 12 FQDN gateway name retrieval - MtcByCarrier



If user performs maintenance actions such as Post and Busy, Gateway FQDN will be displayed on state output.

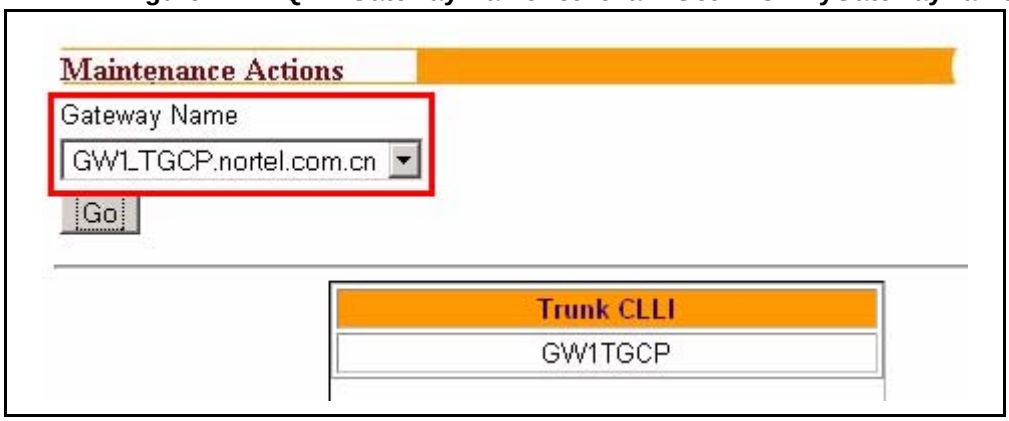
Figure 13 Mtc by Carrier state output



38.5.3 Get TrkCLLIs by Gateway Name

In SN09, gateway FQDN up to 64 characters will be automatically retrieved and displayed on TMM GUI.

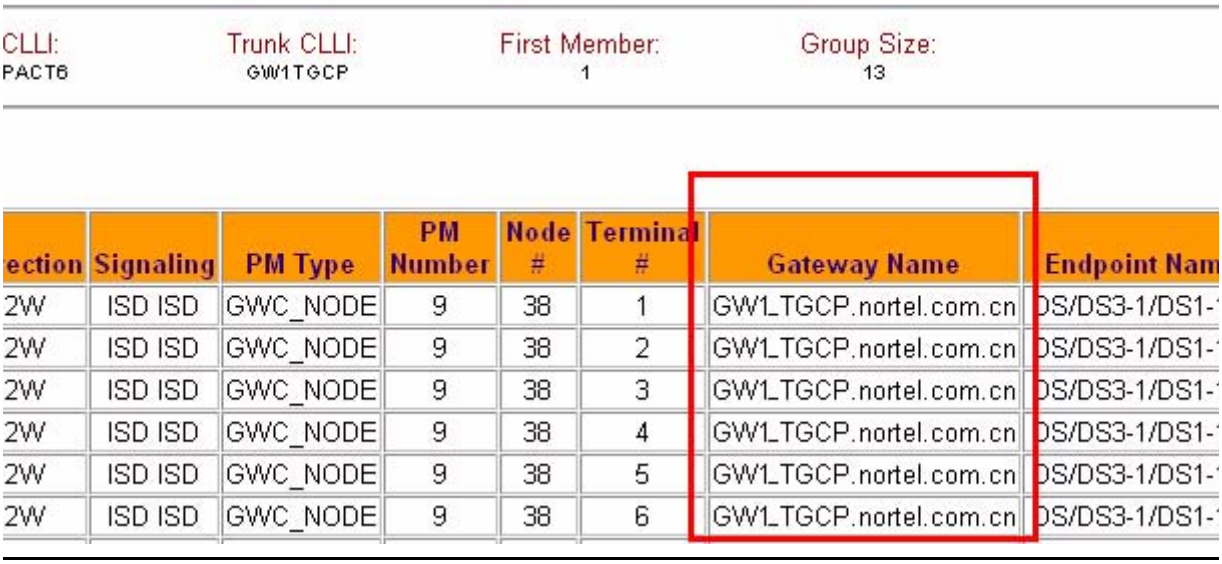
Figure 14 FQDN Gateway Name retrieval - GetTrkCliiByGatewayName



38.5.4 Maintenance By Trunk CLLI

If user performs maintenance actions such as Post and Busy, Gateway FQDN will be displayed on detailed trunk member information.

Figure 15 Mtc by Trunk CLLI



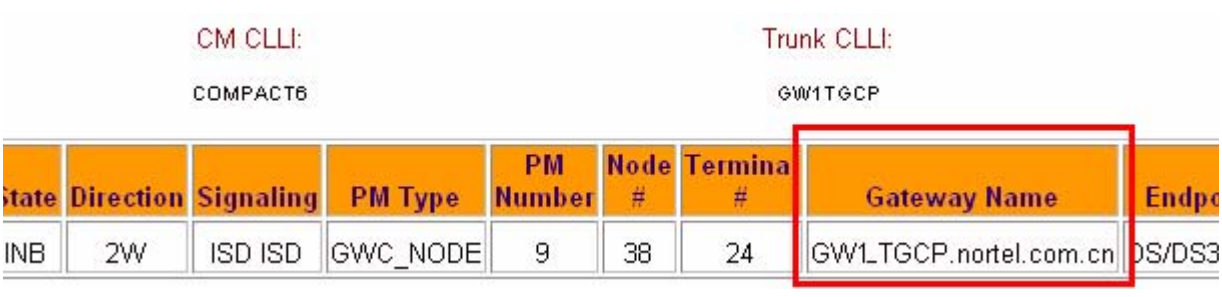
CLLI: PACT6 | Trunk CLLI: GW1TGCP | First Member: 1 | Group Size: 13

ection	Signaling	PM Type	PM Number	Node #	Terminal #	Gateway Name	Endpoint Nam
2W	ISD ISD	GWC_NODE	9	38	1	GW1_TGCP.nortel.com.cn	DS/DS3-1/DS1-
2W	ISD ISD	GWC_NODE	9	38	2	GW1_TGCP.nortel.com.cn	DS/DS3-1/DS1-
2W	ISD ISD	GWC_NODE	9	38	3	GW1_TGCP.nortel.com.cn	DS/DS3-1/DS1-
2W	ISD ISD	GWC_NODE	9	38	4	GW1_TGCP.nortel.com.cn	DS/DS3-1/DS1-
2W	ISD ISD	GWC_NODE	9	38	5	GW1_TGCP.nortel.com.cn	DS/DS3-1/DS1-
2W	ISD ISD	GWC_NODE	9	38	6	GW1_TGCP.nortel.com.cn	DS/DS3-1/DS1-

38.5.5 D-Channel Maintenance

If user post D-Channel by Trunk CLLI, Gateway FQDN will be displayed on detailed D-Channel trunk member information.

Figure 16 D-Channel Maintenance



CM CLLI: COMPACT6 | Trunk CLLI: GW1TGCP

State	Direction	Signaling	PM Type	PM Number	Node #	Termina #	Gateway Name	Endpo
INB	2W	ISD ISD	GWC_NODE	9	38	24	GW1_TGCP.nortel.com.cn	DS/DS3

38.6 LMM functionality modifications

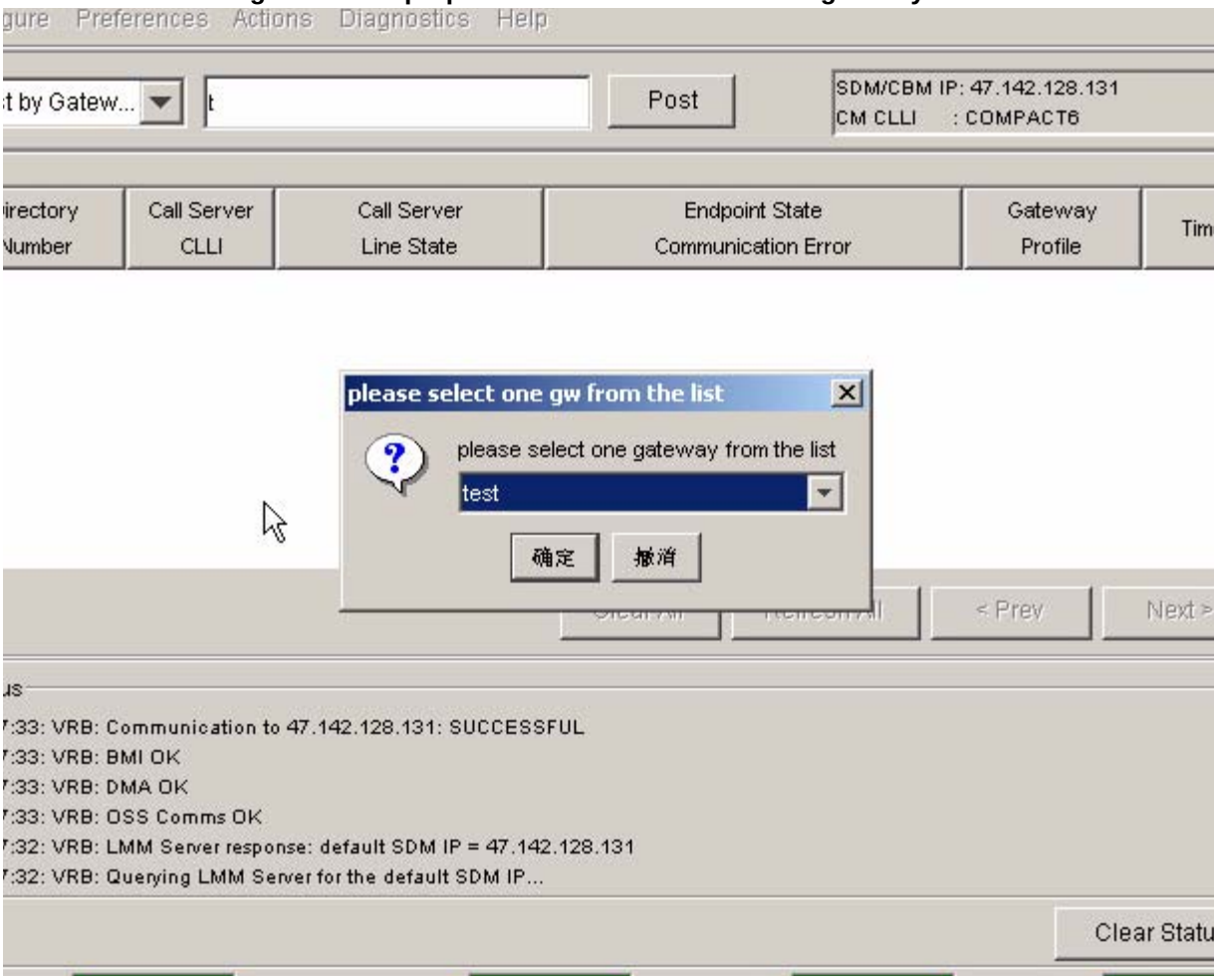
38.6.1 “Post by Gateways” operation

“Post By Gateways” can provide users the functionality to post all the DNs that is associated with the specific gateway, in SN08, all the gatways are hostname,

but in SN09, both gateway hostname and full FQDN name are all needed to be supported to post the DN.

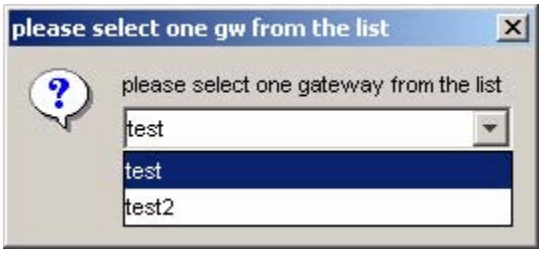
In SN09, the “Post by Gateway” can support the partial query, which means user can input only one part of the gateway name (either gateway hostname or full FQDN name), if there have more than one gateways which can match the partial string, a select box will be pop-uped to let user to choose one, if there is only one gateway to match the query string, it will be used to retrieve all the DNs and no box will be pop-uped.

Figure 17 Pop-up select box if more than one gateways are returned



User can select one gateway from the select box such like the following.

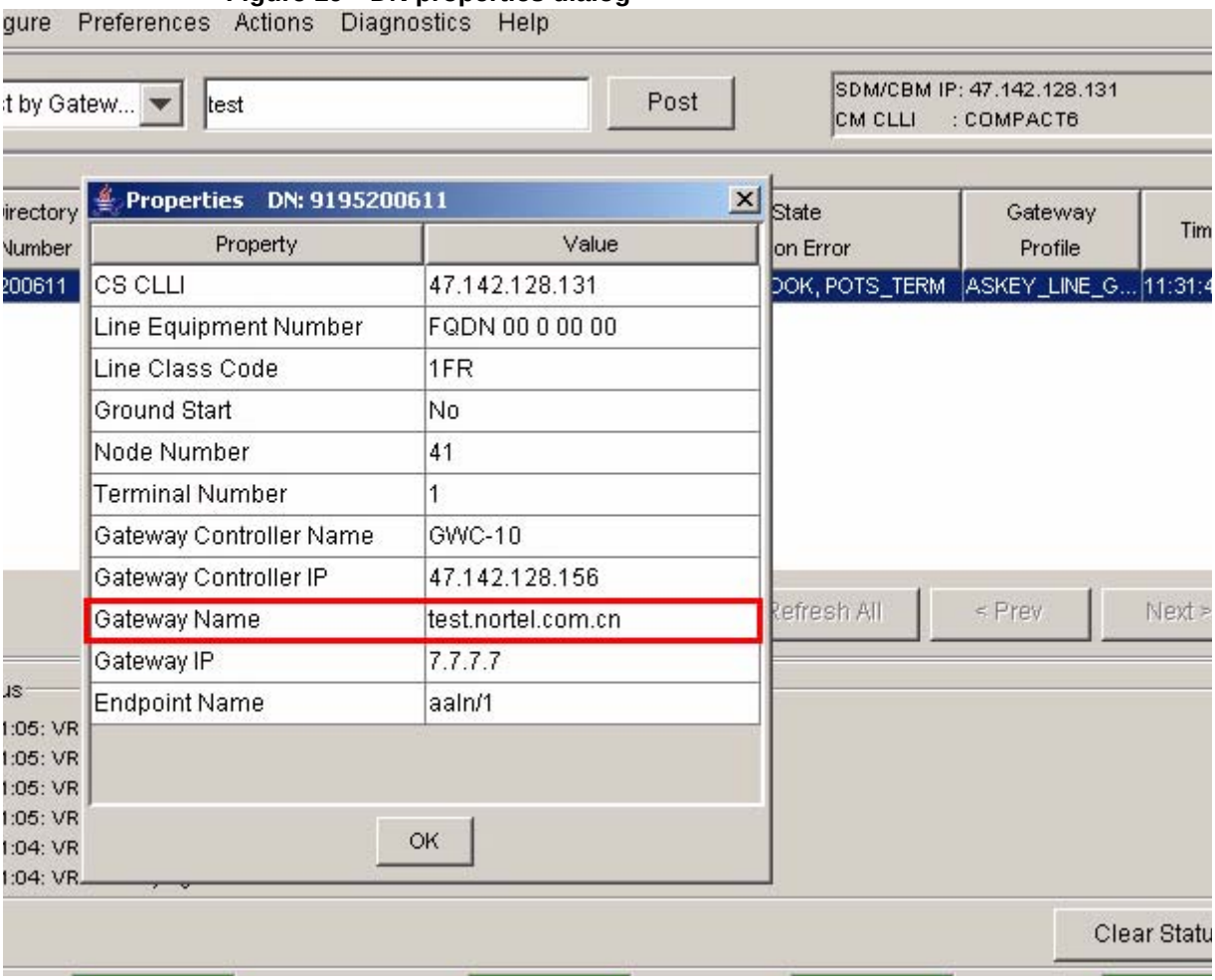
Figure 18 gateway select box



38.6.2 DN's properties dialog

When user right click on a DN and choose the "properties" menu, a DN's properties dialog will appear to show all the properties for the selected DN which includes a gateway name field. If the gateway is associated with a default domain name, the full FQDN name will be displayed in the gateway name field like following diagram.

Figure 19 DN properties dialog



38.7 Other Tools

38.7.1 QGW command on Core

Table LNENDPT is sorted by LENs and may contain up to 150,000 tuples. Therefore, finding all the LENs & Endpoints for a particular Gateway can be somewhat difficult.The Query Gateway Tool (QGW) is a tool on the CM that can be used to output all the LENs and Endpoints for the specified Gateway in table LNENDPT.

To use the command, enter the QGW command at the CM CI prompt, followed by a string denoting the Gateway name. Below is an example of the use of the command:

```
CI:
>qgw 'sbv-10.com6.net'
-------------------------------------------------------
--
LEN: LG    00 0 00 00     ENDPOINT: aaln/1
LEN: LG    00 0 00 01     ENDPOINT: aaln/2
-------------------------------------------------------
--
```

If the Gateway does not exist in table LNENDPT, the following error message is output:

```
>qgw 'sbbv-11.com6.net'
ERROR   - Gateway Name does not exist in table LNENDPT
```

38.8 Hardware Requirements or Dependencies

None.

38.9 Software Requirements or Dependencies

None.

38.10 Limitations and restrictions

1. When associating media gateway, gateway hostname and FQDN must be unique across whole office, otherwise it will be rejected.
2. If a default gateway domain name is provisioned, then together the Gateway Name and the default gateway domain name cannot exceed 64 characters. This rule only be applied to cable solution gateways. Refer to Table 1 on page 345.
3. If no default gateway domain name provisioned, Small line gateways, TGCP trunking gateway and third party gateway's max name length can up to 64 characters.

38.11 Interactions

None.

38.12 Glossary

Table 3 Glossary

Term	Description
CS2K	Call Server 2000
CS2K-MT	Call Server Management Tools
FQDN	Fully Qualified Domain Name
GUI	Graphic User Interface
GW	Gateway
GWC	Gateway Controller
GWCEM	Gateway Controller Element Manager
LMM	Line Maintenance Manager
TMM	Trunk Maintenance Manager
SESM	Succession Element and Subelement Manager
OSSDI	Operations Support System Data Interface

39: Functional Description (FN): A00009190

39.1 Feature name and Feature ID

A00009190: Universal Carrier Protocol (UCP) C7UPTMR Enhancements

39.2 Description

This activity in SN09 provides provisionable timer support on a per trunk basis for UCP Trunks. This is accomplished by

- Provisioning timers in table C7UPTMR for UCP protocol.
- Provisioning the C7UPTMR index in table TRKSGRP
- This feature will be tracked by Track SOC UCSB0001.

When there is no C7UPTMR index provisioned in table TRKSGRP, the default timer values are used.

Currently, the XPM patch XIX20, is used to hardcode the ACM timer value to 20 secs for UCS trunks. When the switch is upgraded to SN09 core load, this patch XIX20 will be Obsoleted. New patch, XHW10 for DTC should be applied to support provisionable timers on a per trunk basis for UCP Trunks. When trunks hosted on DTCs are used, this patch will allow the datafilled ISUP timer value to be used during CallP.

- Datafill table C7UPTMR for UCP Potocol with the required timer value.
- Datafill TRKSGRP to change the TMRNAME field to the datafilled C7UPTMR index.

39.2.1 Provisioning Table C7UPTMR

Table C7UPTMR provides the ability to provision various ISUP timer values on a per-protocol and direction basis. The ISUP (ISDN User Part) timer values that can be provisioned in table C7UPTMR are dependent on the protocol. This activity supports provisioning of timers for UCP protocol. The new UCP timer implementation is modeled after the existing provisionable timers for the Q764 protocol. Refer to the following figure for a sample UCP C7UPTMR datafill.

Figure 1 Examples of the C7UPTMR Datafill

```
TABLE C7UPTMR
UCP2W 2W UCP 13 2 30 6 60 10 180 20 200 13 60 2 $
UCPIC IC UCP 13 6 60 20 200 13 60 $
UCPOG OG UCP 2 25 6 60 10 180 13 60 2 $
```

Refer to the following table for a brief description of the UCP timers, range and default values.

Table 1: UCP Timer Description

Timer Name ANSI	Timer Name Bellcore	Table C7UPTMR Field Name	Timer Range (Secs)	Default Value (Secs)	Direction Applicable	Description
COT	$T_{ccr,r}$	COT	10 to 15	13	IC, 2W	When responding to a continuity check request (CCR), awaiting a Continuity Test message (COT) or Release (REL)
T21	T_{cot}	TONE	2 to 2	2	OG, 2W	When responding to a continuity check in an Initial Address Message (IAM), awaiting return of suitable tone
ACM	T_{iam}	ACM	20 to 30	25	OG, 2W	When sending Initial Address Message IAM, awaiting Address Complete Message (ACM), Answer (ANM) or Release (REL).
REL	T_{rel}	RLCSREL	4 to 15	6	IC, OG, 2W	When sending REL, awaiting Release Complete (RLC); shorter timer used for retransmission
RLC	$T_{rel,l}$	RLCLREL	60 to 60	60	IC, OG, 2W	When sending REL, awaiting RLC; longer timer used for abnormal procedures
T7	unnamed	IRETEST	1 to 10	10	OG, 2W	Wait before initial COT retest
T8	unnamed	SRETEST	60 to 180	180	OG, 2W	Wait before subsequent COT retest
T11	$T_{cot,r}$	ICCR	16 to 20	20	IC, 2W	When receiving first COT coded “failed”, awaiting receipt of CCR
T13	$T_{cot,l}$	SCCR	180 to 300	200	IC, 2W	When receiving subsequent COT coded “failed”, awaiting receipt of CCR
T15	T_{rsc}	RLCSRSC	4 to 15	13	IC, OG, 2W	When sending Reset Circuit message (RSC), awaiting RLC; shorter timer used for retransmission
T16	$T_{rsc,l}$	RLCLRSC	60 to 60	60	IC, OG, 2W	When sending RSC, awaiting RLC; longer timer used for abnormal procedures

Table 1: UCP Timer Description

Timer Name ANSI	Timer Name Bellcore	Table C7UPTMR Field Name	Timer Range (Secs)	Default Value (Secs)	Direction Applicable	Description
T20	T_{ccr}	LPA	2 to 2	2	OG, 2W	When sending a CCR, awaiting receipt of Loop Back Acknowledgement

This feature will be tracked by Track SOC UCSB0001.

39.2.2 Provisioning Table TRKSGRP

Table TRKSGRP provides the ability to provision C7UPTMR index per trunk subgroup basis in field TMRNAME. The provisioned timers values are used for UCP call processing.

Figure 2 Example of the TRKSGRP Datafill

```
TABLE TRKSGRP
LOOP3IMT2WS7A 0 DS1SIG C7UP 2W N N EXTERNAL NONE UCP THRH 0 DMSNODE
$ UCP2W CIC
```

Once TMRNAME field is updated in the Table TRKSGRP, BSY; RTS the trunk to make sure that the C7UPTMR INDEX for the trunk is reflected at the peripherals (GWC/XPM/SPM).

39.3 Hardware Requirements or Dependencies

None

39.4 Software Requirements or Dependencies

None

39.5 Limitations and restrictions

None

39.6 Interactions

None

39.7 Glossary

Term	Description
CCR	Continuity Check Request
COT	Continuity Test
IAM	Initial Address Message

Term	Description
ISUP	ISDN User Part
RLC	Release Complete Message
REL	Release Message
RSC	Reset Circuit Message
UCP	Universal Carrier Protocol

40: Functional Description (FN): A00009200

40.1 Feature name

Packet Trunking Trunk Test: Milli-watt Tone Swap

40.2 Description

The purpose of this feature is to provide the customer the capability to perform a function known as Milli-watt Tone Swap from the MAPCI TTP interface on a Gateway TDM trunk circuit in the Succession XA-Core non-hybrid and Compact CS2K platforms. The new command is supported for all fabrics where the AudioCodes Media Server 2000 series media servers are supported, which includes AAL2, AAL5, and IP. The AAL1 solution is not being considered at this time (as no AudioCodes Media Server is supported in that solution) and no verification is being planned. This feature utilizes the combined capabilities of the XA-Core, Audio Controller (AC) and AudioCodes Media Server (AMS).

Milli-watt Tone Swap is defined as passing a well known tone, the milli-watt tone of 1004 Hz., at a selectable power level, over a DS-0 trunk circuit on a Gateway TDM trunk, to a far-end switch wherein the amount of transmission loss can be measured. Simultaneously and independently, the far-end switch will pass the same 1004 Hz. tone back over the same trunk circuit wherein the amount of transmission loss can then be measured by the near-end switch. This operation permits the customer to ensure two-way voice path is present and verify trunk padding is set correctly.

This feature introduces a new command, MWTSwap, from the MAPCI TTP interface, available only on the Succession CS2K & Compact CS2K platforms. The hardware required to perform the test will reside in the AudioCodes Media Server 2000 Series products.

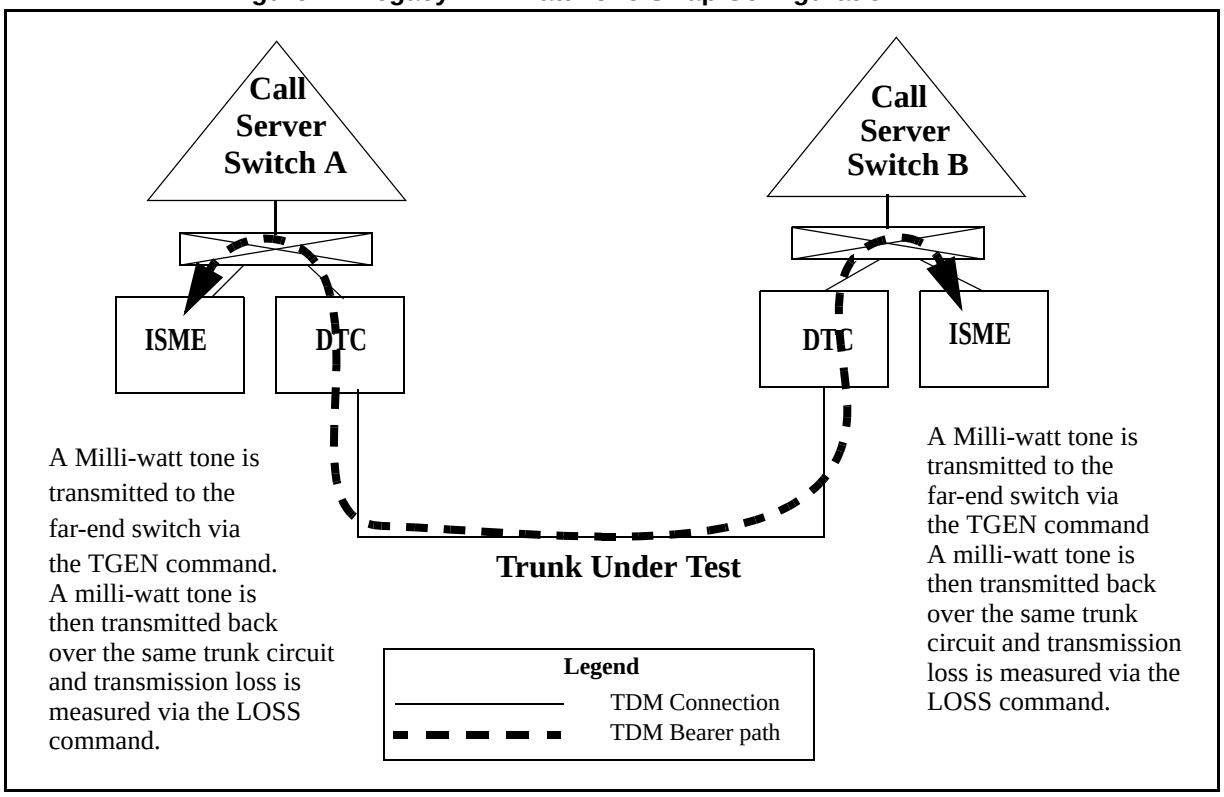
40.3 Configuration Overview

40.3.1 Legacy DMS Milli-watt Tone Swap Configuration

In a conventional DMS configuration Milli-watt tone swapping can be performed via the combination of the TGEN and LOSS commands located on the MAPCI TTP interface. The user must perform each function of the Milli-watt tone swap separately, once to generate the desired milli-watt tone with the TGEN command, followed by a loss measurement with the LOSS command while the far-end is generating the tone. This command implementation does not permit the user to perform both functions simultaneously. Milli-watt tone swap in legacy is executed using special hardware in the Integrated Service Module Equipment or ISME connected to the ENET. Both command requests

are originated by the user from the MAP interface. Connections are created between the Trunk Under Test and the appropriate trunk testing hardware resident on a local ISME. In order to perform Milli-watt tone swap a coordinated effort must be made between craft persons at both switches.

Figure 1 Legacy Milli-watt Tone Swap Configuration



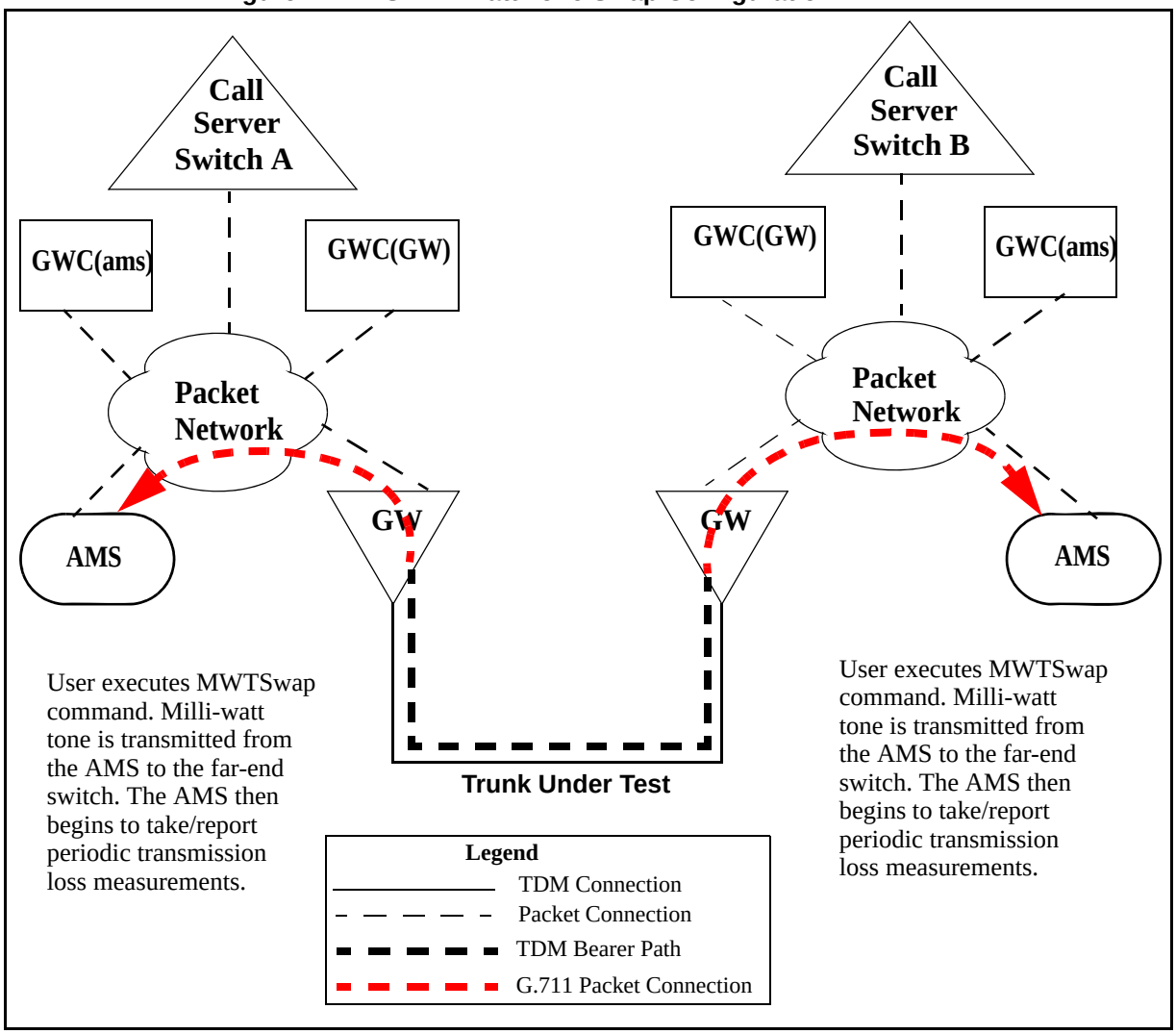
40.3.2 Packet Milli-watt Tone Swap Configuration

The implementation of this feature offers a new method of conducting milli-watt tone swapping via the DSP hardware resident in the AudioCodes Media Server (AMS) 2000 series products. This configuration has the capability of operating without the need for an ENET or ISME. A new command will be introduced at the MAPCI TTP interface called MWTSwap. This new command will perform both the tone generation and loss measurement functions simultaneously.

When the crafts-person invokes the new command, connections are established between the AMS and the Gateway TDM Trunk Under Test. A milli-watt tone is then generated towards the far-end switch. Simultaneously, transmission loss measurements will be taken, on a periodic basis, on the same trunk circuit and displayed on the MAP screen. In order to perform Milli-watt tone swap a coordinated effort must be made between craft persons at both

switches, but because the two functions are executed together the coordination required is less.

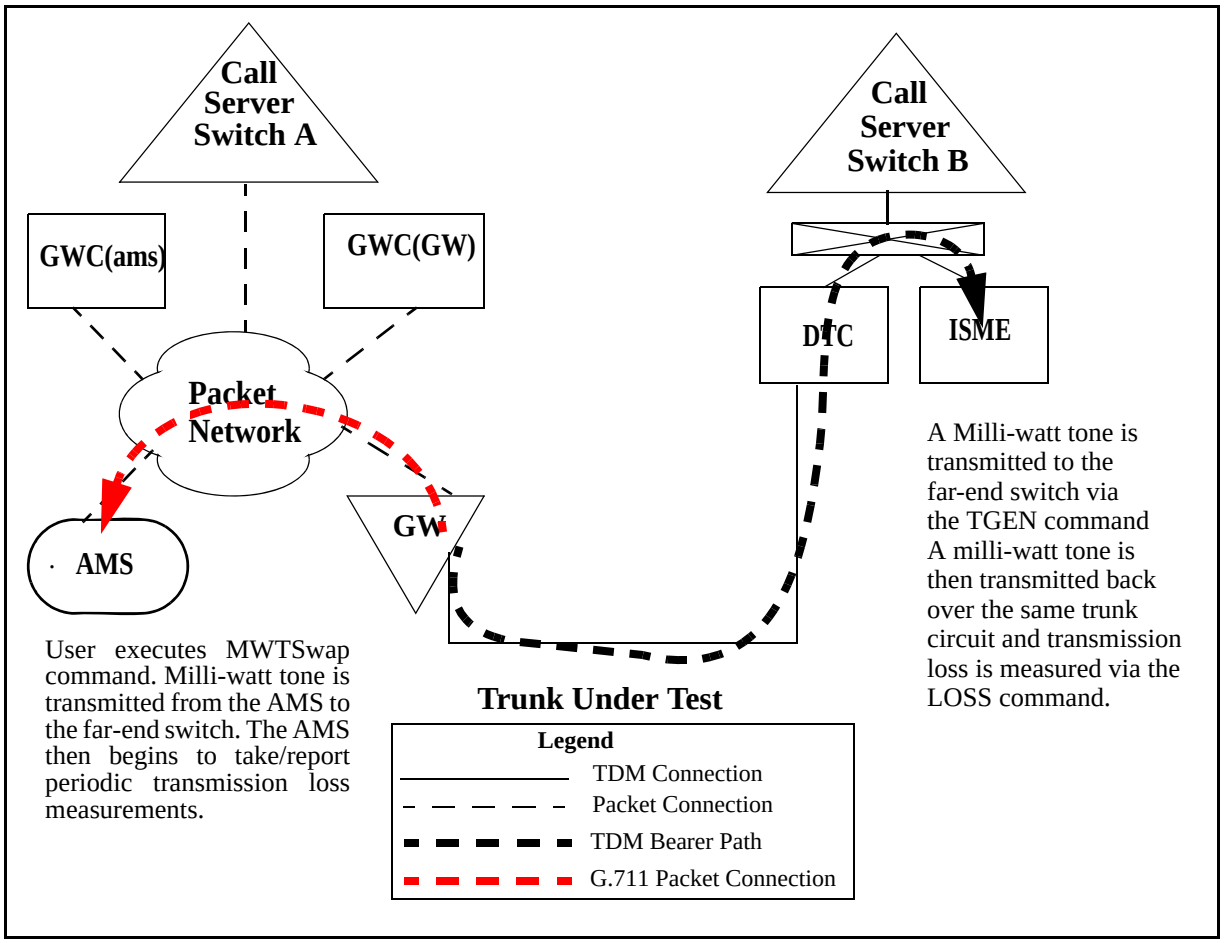
Figure 2 AMS Miili-watt Tone Swap Configuration



40.3.3 Packet Milli-watt To Legacy Tone Swap Configuration

The implementation of this feature also permits the user the ability to interoperate with legacy switches (either Nortel or other vendors). In this case if the user wishes to perform Tone Swap to an adjacent switch, which hosts non-AMS based test equipment, the user would simply issue the MWTSwap command and coordinate with the craftsperson at the adjacent switch to activate their hardware to perform tone swap. The above example shows Tone Swap between a packet-based switch and a DMS legacy switch..

When the crafts-person invokes the new command, connections are established between the AMS and the Gateway TDM Trunk Under Test. A milli-watt tone is then generated towards the far-end switch. Simultaneously, transmission loss measurements will be taken, on a periodic basis, on the same trunk circuit and displayed on the MAP screen. In order to perform Milli-watt tone swap a coordinated effort must be made between craft persons at both switches, but because the two functions are executed together the coordination required is less.



40.4 Functional Overview

As mentioned earlier this feature will introduce a new command at the MAPCI TTP level interface. The new command, MWTSwap, will appear on the TTP level screen only when the office parameter EXTERNAL_GATEWAY_TEST_LINES is set to ‘Y’ in table OFCVAR. This office parameter determines which test head will be used for hardware based TTP/ATT level trunk testing. The default is ‘N’ which indicates that tests will use the existing hardware located in the ISM/MTM peripheral. When set to

'Y', all testing currently supported will be performed via the AudioCodes Media Server (AMS) 2000 series products.

Please note: AMS based testing is only supported on Gateway TDM trunks. No support is currently available for legacy peripheral TDM trunks. Legacy peripheral TDM trunks can utilize the existing TTP Manual level command TGEN and Loss in combination to perform a Tone Swap.

The following is an example of the new command on the MAPCI TTP level interface.

```
 XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
Baseln  01SBPT  DLOG E   LOAD    1 DPT     .    SYSB     22C..   1Crit   SDM
  M                              *C*           *C*     *C*     *C*      M
  MANUAL
 0 QUIT      POST    23  DELQ            BSYQ         DIG
 2 Post_     TTP 27-0002
 3 MWTSwap   CKT TYPE     PM NO.          COM LANG     STA S R  DOT TE  RESULT
 4           2W S7 S7 GWC   9     1  H248ISUPITOG    1                   No Tn
 5 BSY                                                                  1004Hz
 6 RTS
 7 TST       EML  0.0 DB
 8 Noise     PAD PC 0 TE 0
 9 OP_
10 TDet
11 Hold      MWTSwap  f 1004 p 0 d 60
12 NEXT
13 RLS
14 HSet
15 Jack_
16 SGNL
17
18 CallTrf
  BRIAN
Time  10:46
```

When the ofcvar EXTERNAL_GATEWAY_TEST_LINES is activated the MWTSwap command will appear as a menu item to the crafts person. Note that the commands TGEN and Loss will be removed as menu items since they are currently not supported in the XA-Core non-hybrid and compact CS2K solution.

The following steps are performed to execute the command MWTSwap from the MAPCI TTP MANUAL level interface both on a Succession XA-Core non-hybrid or Compact CS2K platform.

1. Crafts person posts a trunk circuit which will be tested at the MAPCI TTP level interface.
2. The crafts person enters the MANUAL level.

3. The command MWTSwap is executed with the optional parameters to specify the tone frequency, power level, and test duration. If no optional parameters supplied, the default parameters are used, which are 1004 Hz. at 0 dB for 60 seconds.

   Please note although the command line interface provides for entering a tone frequency, only the 1004 Hz. frequency is supported for this feature. If a frequency other than 1004 Hz. is entered, the crafts person will be alerted with an error message.

4. Trunk is seized and connections established between the AMS and Gateway TDM trunk, the AMS is sent a request to perform the test.
5. Tone is generated on the outgoing Gateway TDM trunk, at the same time the AMS begins taking loss measurements and reporting them back to the CS2K.
6. The MAPCI TTP level interface is updated with the loss measurements on a periodic basis (every few seconds).
7. After the test duration completes the AMS will time out and release the connection and terminate the test.
8. The MAP screen will be cleared and the trunk revert to it's original state prior to the test being invoked.

Parameter	Range
Tone frequency	Currently only supports 1004 Hz.
Tone power level	-60 to 0 dB
Test Duration	1 to 240 seconds

40.5 MWTSwap frequency error message

This feature supports the generation of a tone frequency of 1004 Hz. If a crafts person enters any other frequency (1005 Hz in the example below) the following error message will be provided:

```
MWTSwap  f 1005
USING DEFAULT POWER LEVEL (0 DB)
USING DEFAULT DURATION (60 SECS)
Action not supported - invalid frequency entered.
Frequency is currently restricted to 1004 Hz for MWTSWAP command.
```

Other command level errors are documented in the CI section of this feature documentation as well as applicable Nortel NTP documentation.

40.6 Hardware Requirements or Dependencies

AudioCodes Media Server 2000 Series (MS2010, MS2020)

40.7 Software Requirements or Dependencies

This functionality will be available in SN09.

40.8 Limitations and restrictions

1. Tone frequency generation limited to 1004 Hz..
2. Loss measurement requires presence of Milli-watt tone. AMS will provide loss measurement data if 1004 Hz. tone is received. If no tone is present or if tone received is not 1004 Hz. the craftsperson will be alerted with an informational message of “No Tn” on the MAPCI display in place of the loss reading.
3. 32 Simultaneous MWTSwap commands can be conducted per AMS.
4. In SN09 only H.248 and TGCP ISUP and OP/ES PTS trunk types are supported for the MWTSwap command. All other PTS variants and PRI trunk types are blocked to prevent the command from being run on them.
5. PTS OP/ES trunk support is available on H.248 and TGCP based gateways.
   - TGCP OP trunk limited to OG and 2W non-verification trunk. This means that an OP PTS trunk data filled on a TGCP gateway with a direction of IC or 2W with an operator mode of either “verification”(VF) or “combined_verif”(CV)is not supported and blocked at the TTP level. Operator mode can be located in table TRKGRP, field Mode.
   - TGCP gateway (Nuera) support is limited to BTX-4K gateway, the BTX8 and BTX21 gateways are not supported.
   - MWTSwap command execution on supported GWC PTS trunks is recommended on trunk in a manual busy state.
   - MWTSwap command on a trunk in an idle state is supported with the following qualifications:
     - CS2Kc to CS2Kc testing is fully supported.
     - CS2Kc to PSTN requires that the PSTN trunk perform a “Loss” command first, followed by the CS2Kc MWTSwap command.
   - MWTSwap command on a trunk in the RMB state is supported with the following qualifications:
     - CS2Kc to PSTN must have the MWTSwap command complete before releasing the PSTN trunk connection to avoid trunk state mismatches between switches.

40.9 Applicable customer facing sections

Fault Management

Logs ___N___

Alarms ___N___

Configuration

Data Schema ___N___

User Interface ___Y___

Element Management ___N___

Security ___N___

Service Order ___N___

Office Parameters ___N___

Accounting (includes AMA billing) ___N___

Performance (includes operational measurements) ___N___

40.10 Glossary

Term	Description
AMS	AudioCodes Media Server
GWC	Gateway Controller
AC	Audio Controller
MTM	Maintenance Trunk Module
ISME	Integrated Services Module Equipment
PVG	Passport Voice Gateway

40.11 T105 NT Responder Variant Support

The purpose of this section is to reference an additional part of this feature to provide the additional sub-test called “NT” to the T105 responder test capabilities of the AudioCodes Media Server 2000 Series (AMS) products. Today, the AMS currently supports the Nortel standard T105 test which is comprised of the following sub-tests:

a. L - Two-way loss measurement at 1004 Hz. and 0 dBm.

b. N - Far-end noise measurement with C-msg filter.

c. RN - Near-end noise measurement with C-msg filter.

d. LSC - Far-end loss self check with 1004 Hz. and 0 dBm.

e. NSC - Far-end noise self check with C-msg filter.

This support is made available for the Compact CS2K and non-hybrid CS2K configurations in which there is no ISM/MTM present which houses the traditional DMS test trunk hardware. The AMS provides a limited replacement for trunk testing to the ISM/MTM in these configurations.

The “NT” test is defined via the AT&T Technical Advisory No. 17 section CB106 as:

NT - Two-way noise measurement C-msg filter with tone at 1004 Hz. and -16 dBM.

The AMS provides the “NT” sub-test to the T105 responder functionality in the AMS. A far-end switch signaling to perform an “NT” test as a part of aT105 request can now be handled by the AMS. No development was required by Nortel for this feature. All development effort was performed by AudioCodes. The AMS support for the “NT” sub-test is limited to the responder or terminating side. A T105 test originating on an AMS will not request an “NT” sub-test.

41: Functional Description (FN): A00009204

41.1 Feature name and Feature ID

Feature A00009204 - Siren Call Agent Customer Visible Capacity Tools

NOTE: Siren is not the official name that will be used; an official name has not yet been approved.

41.2 Description

This feature covers the changes required to the Customer Visible Capacity Tools for the SOS Call Agent blade on Siren. The Capacity Tools covered by this feature are:

- CAPCI tool
- CAPACITY MAP levels

41.2.1 CAPCI CI Command

The following figure is a prototype of the output of the CAPCI CI command.

Figure 1 CAPCI Command Output

```
>capci
CAPCI -- 2004/12/13 12:42:24.018
CATMP/HR UTIL ENGCATMP ENGLEVEL MAXCATMP SYNC OVRLD IDLE COMPLEX
 1200000  50%  2400000    BELOW  2600000 +HOT   OFF  YES    1140
```

```
>query capci
CAPCI -- Display status of switch activity
Parms: [<option> {PARMS,
                  SCHEDMAP,
                  ALL}]
```

The output of the CAPCI ALL CI will output all the options available for CAPCI. The order of the ouput is CAPCI + SCHEDMAP + PARMS.

The following figure is a prototype of the output of the CAPCI ALL CI command.

Figure 2 CAPCI ALL Command Output

```
 >capci all
CAPCI -- 2004/12/13 12:42:24.018
CATMP/HR UTIL ENGCATMP ENGLEVEL MAXCATMP SYNC OVRLD IDLE COMPLEX
 1200000  50%  2400000    BELOW  2600000 +HOT   OFF  YES    1140

SCHED  FORE  MAINT   DNC  AUXCP    OM  GTERM    BKG   NETM   SNIP
  87%   10%    80%   83%     0%   81%    66%    62%     0%    66%

    Guaranteed_Terminal_CPU_Share = 0.0%
    AUXCP_CPU_Share               = 1.0%
    CC_Englevel_Warning_Threshold = 100%
    NETM share setting            = 0.0%
    DNC share setting             = 0.0%
    SNIP share setting            = 0.0%
    1% CPU allocation             = 10581 CATMP/HR
```

41.2.2 CAPACITY Map Level

This MAPCI level is accessed from >mapci;mtc;capacity. The CAPACITY MAPCI level output has been modified to match the CAPCI command.

The following figure is a prototype of the CAPACITY MAPCI display.

Figure 3 CAPACITY MAPCI Display

```
 CAPACITY
 0 Quit      CATMP/HR UTIL ENGCATMP ENGLEVEL MAXCATMP SYNC OVRLD IDLE COMPLEX
 2 Parms      1200000  50%  2400000    BELOW   260000  HOT   OFF  YES    1140
 3 SchedMap
 4           CAPACITY:
 5
 6
 7
 8
 9
10
11
12
13
14
15
16
17
18
```

41.3 Hardware Requirements or Dependencies

None.

41.4 Software Requirements or Dependencies

This feature requires the Siren Release 1.0 Call Agent platform.

41.5 Limitations and restrictions

This feature requires the Siren Release 1.0 Call Agent platform.

41.6 Interactions

Changes are being made to the current CAPACITY MAPCI level

Changes are being made to the CAPCI CI command.

41.7 Applicable customer facing sections

Fault Management

- Logs __NA___
- Alarms __NA__

Configuration

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

Accounting (includes AMA billing) __NA__

Performance (includes operational measurements) __NA__

41.8 Glossary

Term	Description
New term	Definition

42: Functional Description (FN): A00009207

42.1 Feature name and Feature ID

A00009207: DPT Trunk Testing Support

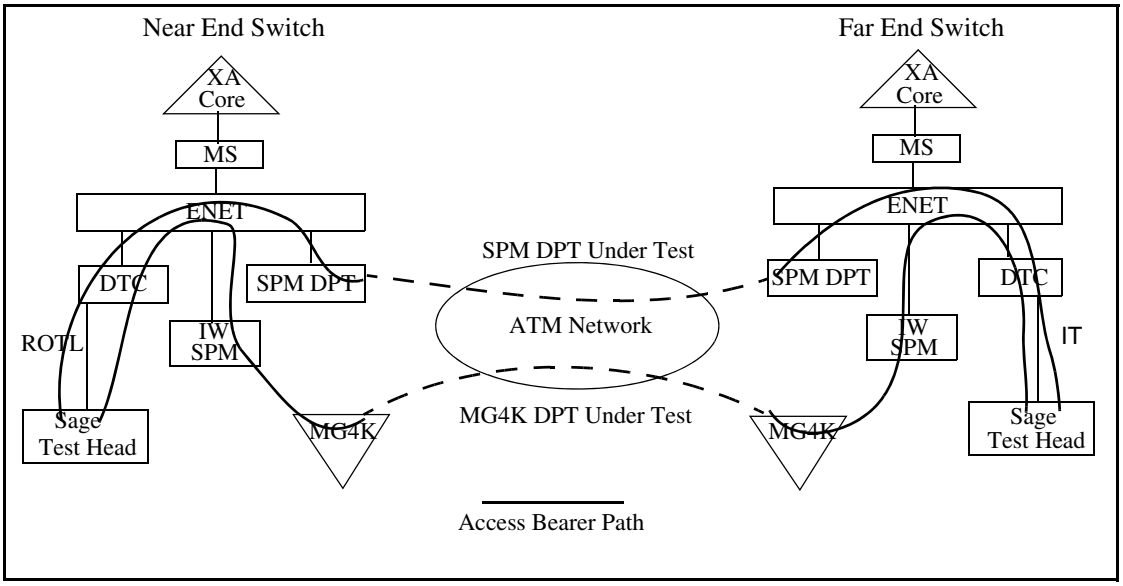
42.2 Description

This activity enhances the Digital Remote Office Test Line (ROTL) trunk interface to allow for the selection of a DPT node and Terminal Identifier (TID) if that DPT is hosted by a Spectrum Peripheral Module(SPM) or MG4K. In addition this feature allows the customer to select which SPM or MG4K to direct all incoming DPT test calls.

Digital ROTL is an existing DMS feature to remotely test trunks via a digital, four wire, E&M trunk. This CAS trunk interface permits a test head to be connected to the CS2K and, via a maintenance dial plan, select an outgoing trunk to be tested. A test head is connected to the CS2Kby a T1, on which several channels are provisioned with a ROTL trunk type. Test calls can then be outpulsed from the test head over the ROTL trunk members using a defined maintenance dial plan which instructs the CS2K software to select an outgoing trunk circuit and generate a test call to the far-end switch. A connection is then established between the test equipment and the trunk circuit being tested. Once all connections have been made the test head conducts the desired trunk test.

This feature enhances the Digital ROTL functionality to permit test connections over DPTs hosted by an SPM DPT or MG4K. The customer will be able to directly select the DPT group, node and TID to test.

Figure 1 Configuration Diagram



42.3 Digital ROTL Origination Feature Description

A test head in conjunction with the Digital ROTL feature permits the selection of an outgoing trunk to test via a maintenance dial plan outpulsed into the switch over a T1 interface. The group of digits in the dial plan which identify the outgoing trunk is known as the Port Identification Number. The current Digital ROTL Port Identification Number for TDM trunk selection is defined as the following:

KP + Test Line Id + ADNUM + Trunk Member + Testline Number + ST

KP - Key Pulse digit
Test Line Id - the code of the desired test (e.g. 05 = ROTL_105 testline id)
ADNUM - value from table CLLI represents the trunk group to be tested
Trunk Member - Member of the trunk from table TRKMEM
Testline Number - DN being outpulsed to the far end switch
ST - Stop or cut-through digit

With the introduction of DPT support by this feature, the existing TDM Port Identification Number portion of the maintenance dial plan is modified to select based on node and terminal number rather than trunk member. The new Port Identification Number will be defined as the following:

KP + Test Line Id + ADNUM + Node + Terminal + Testline Number + ST

KP - Key Pulse digit

Test Line Id - here new ids will be defined which will indicate trunk selection via the new node and terminal dial plan (#80 ROTL_100, #82 ROTL_102 and

#85 for ROTL_105)

ADNUM - ADNUM from table CLLI represents the trunk group the DPT terminal will be assigned to.

Node - the node which the DPT terminal is allocated

Terminal - the DPT which will be tested

Testline Number - DN being outpulsed to the far-end switch

The CS2K software will parse this new Port Identification Number and a selection of the desired outgoing DPT terminal will be performed. A connection between the selected DPT terminal and the test head will then be made. Once established the desired trunk test will be performed by the test head.

42.3.1 Find the node number of the SPM

The NODENO command provides the number of the node to dial for testing the outgoing call. The command also prints a reminder of the valid DPT terminal number range for the SPM. The valid terminal ranges are:

- DPT SPM: 1 to 2016
- MG4000: 2079 to 4094

42.3.1.1 Finding the node number

At the MAP terminal

1. Access the DPT info debug tools by typing
   ```
   >dptinfo
   ```
   DPTINFO:

Enter the node number command

```
>nn node_type device_class device_no
```

Note: The short form for the nodeno command is "nn". where
node_type--for any SPM, node_type is "spm"
device_class--for any SPM, device_class is "spm"
device_no is the SPM number found in table MNMODE.

Example:

```
> nn spm spm 1
NODENO=70
This node has DPT terminals 2079-4094
>
```

42.4 DPT Test Call Termination Feature Description

In conjunction with the design to provide DPT test support via the Digital ROTL interface, incoming DPT test calls will have the capability to be routed to a desired DPT node. This selection will be data fillable, and once set, all incoming DPT calls flagged as a test call will terminate on the provisioned SPM (either DPT SPM or MG4K).

42.4.1 New office parameter DPT_BICC_TEST_NODE

This activity introduces a new office parameter, DPT_BICC_TEST_NODE in the table OFCVAR which will identify the particular node to which all incoming DPT test calls will be routed to. This office parameter contains two fields, first PMTYPE and the second is SPM node number. Currently, the implementation of this office parameter will be limited to only the SPM node type. In addition, a check is place to ensure that the node number entered is supports DPT.

Note: During an ONP, if this new parameter exists in a previous software load, it will be propagated forward. If the office parameter does not exist in the previous load, the entry will be created in table OFCVAR with the default values of NIL_PMTYPE and '0'.

42.4.2 Set the CPC (Calling Party Category) in the ISUP IAM Message

A DPT test call IAM (Initial Address Message) initiated by the Digital ROTL feature is being modified to set the Calling Party Category (CPC) field to ISUP_CPC_TEST_CALL. At present this CPC field is set to the default of CPC_UNKNOWN. The CPC field will be used to identify if an incoming DPT call is considered to be a test call.

42.4.3 Move the incoming DPT Test Call to the provisioned terminating node

The incoming DPT test call will be moved to the desired SPM node based on the following:

- The call will be identified as a test call via the CPC field in the IAM message of ISUP_CPC_TEST_CALL.

- A look-up will be performed on the office parameter DPT_BICC_TEST_NODE and the provisioned SPM node will be returned.

- The incoming test call will then be moved to the desired node.

Note: Provisioning a desired terminating node effects test calls generated via the MAPCI;DPTTRKS level OP (Outpulse) command. Since a test call associated with this command sets the CPC of the IAM to ISUP_CPC_TEST_CALL.

42.5 Hardware Requirements or Dependencies

This feature enhances the existing Digital ROTL interface for trunk selection. A test head is required to perform the actual trunk test.

42.6 Software Requirements or Dependencies

Core: SN09 or greater.

SOC option BAS00050 56Kb/sTrk Tst prt must be activated.

42.7 Limitations and restrictions

1. The T1 interface to the test head equipment will not be supported on an MG4K node type because the MG4K does not currently support the ROTL trunk type.

2. This activity supports DPT terminals hosted by an SPM or MG4K. No official support is made for GWC DPT terminals. However, no enforcement will be provided by this feature.

42.8 Interactions

Not applicable

42.9 Glossary

Term	Description
DPT	Dynamic Packet Trunk
ROTL	Remote Office Test Line
TID	Terminal Identifier
PTS	Per Trunk Signaling
SPM	Spectrum Peripheral Module
MG4K	Media Gateway 4000
DMS	Digital Multiplex System
ONP	One Night Process
CPC	Calling Party Category
IAM	Initial Address Message
CS2K	Call Server 2000

43: Functional Description (FN): A00009208

43.1 Feature name and Feature ID

SN09 180K LINES SUPPORT - Actid A00009208

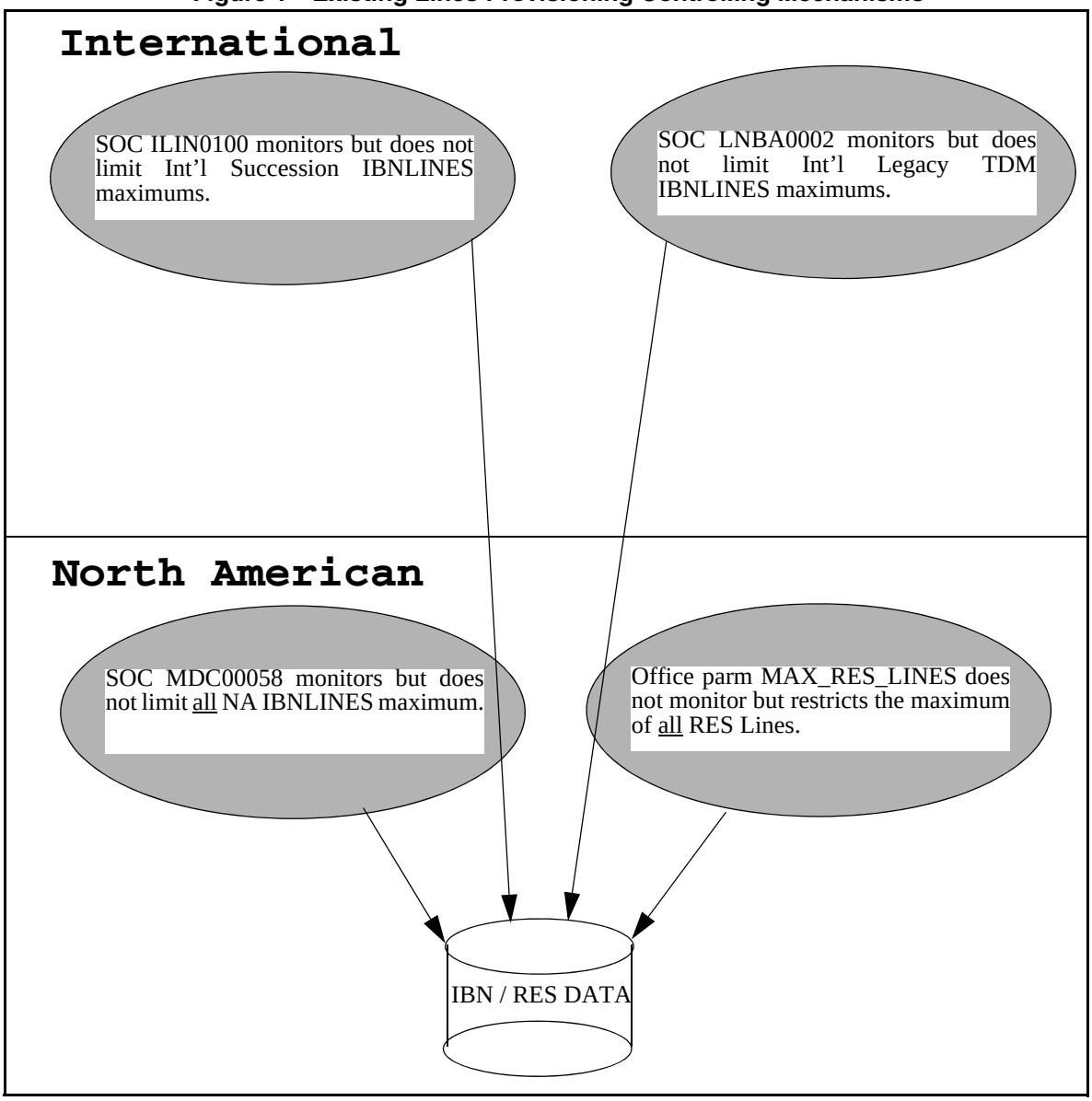
43.2 Description

The purpose of this feature is to increase the provisioning limits for lines globally from its current limit of 150k to 180k. The feature provides the ability to:

- provision a total of 180,000 RES lines for the North American market
- provision a total of 180,000 IBN lines for the International market
- perform Call Processing on each of these lines

There are no new SOCs or Office Parms introduced to activate the new provisioning limits. The capability is built into the SN09 load. The customer will use the existing mechanisms to allow provisioning of RES/IBN lines to these new limits. Refer to the following figure.

Figure 1 Existing Lines Provisioning Controlling Mechanisms



The specific SOCs mentioned in Figure 1 are soft SOCs which mean they monitor limits. Customers are allowed to go beyond their initial limit without Nortel intervention. For details on SOCs, please refer to the Maintenance and Operations Manual NTP 297-9881-500. This feature does not impact/change how these SOCs function.

The MAX_RES_LINES Office Parameter in Table OFCOPT does limit the maximum number of all RES lines provisioned. When this office parameter is changed to the new limits activation is immediate. For details on office parameters, please refer to the Office Parameters Reference Manual NTP-

297-8021-855. This feature does not impact/change how this office parameter functions.

43.3 Hardware Requirements or Dependencies

There are no hardware dependencies required to execute this feature.

43.4 Software Requirements or Dependencies

Software Dependencies:

— CORE - SN09 release or later

Firmware Dependencies:

— None

43.5 Limitations and restrictions

This feature is applicable to:

- North American and International software releases
- the CS2000 and CS2000-Compact configurations
- the AAL1 and IP solutions

This feature restrictions are:

- Does not change the Engineered maximum number of GWCs supported in an Office, currently at 60.
- Does not change the Engineered maximum number of lines supported per GWC, currently at 6400.
- Does not change or implement any new SOC controls for line capacities
- Does not increase current TDM limit of 150K lines
- Does not address the MG9000 Manager limit of 110K native lines. (ABI-based lines are not included in the 110,000 MG 9000 Manager limit)
- The current core BHCA capacity is not a limiting factor for the line access call models.
- Does not impact the ACD limit which is changing from 30K to 99,999 with SN09 feature A00009085.
- Does not increase Call Processing Feature limits:
  - — Current line service capacity limits apply (e.g., 50K Speed Call Long Lists)
  - — No more than 45% penetration of voice mail service (requiring CFW and MWT)
- Does not increase current Cable line capacity limit of 150K lines. 180K lines is possible with a combination of the current 150K Cable lines (with

a maximum of 115K MTAs when RMGC is employed) and 30K TDM or other allowable non-Cable packet lines.

43.6 Interactions

The following are the feature interactions for A00009208 feature:

- Features which A00009208 is dependant on:
  - — none
- Features which are dependant on A00009208:
  - — none

43.7 Applicable customer facing sections

Fault Management

Logs	___n/a___
Alarms	___n/a___

Configuration

Data Schema	___n/a___
User Interface	___n/a___
Element Management	___n/a___
Security	___n/a___
Service Order	___n/a___
Office Parameters	___n/a___

Accounting (includes AMA billing)	___n/a___
Performance (includes operational measurements)	___n/a___

43.8 Glossary

Term	Description
SOC	Software Optionality Control

44: Functional Description (FN): A00009218

44.1 Feature name and Feature ID

Activity A00009227 - MG9KEM Data Audit Robustness

44.2 Description

MG9KEM audits can currently only be run for an entire NE, even when data mismatches exist for only a small portion of the NE data. Experience in the field has shown that subsystem data corruption (e.g VMG data mismatch on a single shelf) is the most common type of data corruption. In these types of scenarios, the customer has to wait for lengthy NE audits to run to fix issues that in reality require only a small amount of time to run.This activity will enable subsystem audits. This capability was built in from the start, but has not been enabled in previous releases. This change offers both efficiency and robustness improvements as well as enhanced usability:

- ïRobustness improvements. The EM does not have to use unnecessary database resources and strain the MG9000 with unnecessary SNMP traffic, which has been known to affect call processing performance.
- ïUsability improvements. Selective audits will allow the user to quickly fix call processing affecting data mismatches. This will translate into significantly reduced outage times if data mismatches are call affecting. Also minimizing the audit times will in turn reduce the periods in which the GUI response of the EM is sluggish because the server is busy.

44.3 Hardware Requirements or Dependencies

No additional requirements are needed for this feature besides the standard MG9000 EM and the MG9000 Gateway.

44.4 Software Requirements or Dependencies

This is a standalone feature and has no special requirements or dependencies.

44.5 Limitations and restrictions

Subsystem audits will only be allowed for non-scheduled audits only.

44.6 Interactions

N/A

44.7 Applicable customer facing sections

Fault Management

Logs____

Alarms____

Configuration

Data Schema_____

User Interface_____

Element Management____

Security_____

Service Order_____

Office Parameters_____

Accounting (includes AMA billing)_____

Performance (includes operational measurements)_____

44.8 Glossary

Term	Description
EM	Element Manager
GUI	Graphical User Interface
MG9000	Media Gateway 9000
SNMP	Simple Network Management Protocol
WMG	Virtual Media Gateway

45: Functional Description (FN): A00009227

45.1 Feature name and Feature ID

Activity A00009227 - NPM Robustness

45.2 Description

The NPM Robustness feature addresses areas for improvement in the Network Patch Manager. Following is a list of items that this feature will provide:

- A New log will be provided as part of the NPM Customer logs indicating whether a GWC image was successful or not.
- Six new system defined reports will be added to the NPM as a result of this feature:
    - DEVICEINFO - lists the devices in the office, the date the devices registered, the loadname in the device and the date the load was discovered in the device.
    - LASTAPPLYACTION - A list of the patch, device, status and description of why the apply attempt failed for this patch device relationship.
    - PFRSSETTINGS - Lists the PFRS Dropbox, PFRS userid and status of if the delete patches is turned on.
    - SYSTEMPLANSETTINGS - Lists all the system plans in the office along with the tasks, enable status, and schedule for each plan
    - OFFICEINFOSETTINGS - Lists office information. Currently, only the GWC Auto imaging enabled setting is available in this report.
    - GWCLOADIMAGEREPORT - Lists the imaged load, the patches contained in the load, the time the image was taken and a list of patches available in the office that are not contained in the image.

All of these reports will be included in the inform report that is generated via the PFRSGENREPORT task in the NPM.

- The NPM CLUI will be able to accept patchids in lower case, upper case or a combination of thereof; except for one command, q PATCH.
- The majority of the NPM CLUI commands will be changed to ensure command naming consistency for commands that provide similar types of functions.

- A new alarm will be raised on the Media Gateway 9000 GUI (MG9K EM) after applying or removing a “restart required” patch to any of the Media Gateway 9000 patchable cards.
- The “restart required” patch alarms at the MG9K EM will be lowered after restarts are performed on MG9K patchable cards.
- Logs and alarms for “restart required” patches will be provided during application or removal of the patches.

45.3 Hardware Requirements or Dependencies

None.

45.4 Software Requirements or Dependencies

None.

45.5 Limitations and restrictions

None.

45.6 Interactions

None.

45.7 Glossary

Term	Description
NPM	Network Patch Manager
CLUI	Command Line User Interface
GUI	Graphical User Interface
MG9K EM	Media Gateway 9000 Element Manager

46: Functional Description (FN): A00009230

46.1 Feature name and Feature ID

Activity A00009230 - CS2000 Session Server Linux Support

46.2 Background

This activity provides the Linux support for the CS2000 Session Server in the SN09 / MCP9.0 release.

46.3 Overview

This feature continues the Linux porting work started by feature FTR399 in MCP3.1. In that feature, the MCP3.1 MCS-5100 (enterprise) system was ported to two IBM platforms: the IBM e-Server series x306 (small system) and BladeCenter (large system), both of which are based on Intel hardware. That porting effort based the MCP-5100 Linux systems on a distribution from RedHat called RedHat Enterprise Linux (RHEL) Application Server 3 (AS3), update 1.

In MCP9.0 the MCP product is being included into the CS2000 platform as the CS2000 Session Server, providing SIP functionality for the CS2000 platform. As the CS2000 platform is targeted for the carrier market, the porting effort focuses on the porting of the CS2000 Session Server onto carrier-class (NEBS certified) hardware.

The selected Linux distribution for CS2000 Session Server in SN09 / MCP9.0 remains RHEL AS3 (Update 3). Please refer to section Linux Operating System / Distribution3.1.1 for more information.

The network elements of the MCP architecture which are included for the CS2000 Session Server include the following, and are given the highest priority by this feature:

- Database
- System Manager
- SIP Session Manager
- Provisioning Manager

The following MCP network elements are also ported, but are given second priority as they are not required for the CS2000 Session Server:

- Fault Performance Manager

- Personal Agent Manager
- Accounting Manager
- IP Client Manager
- UFTP Server
- H.323 Gatekeeper

The following MCP network elements are not included in this porting feature:

- RTP Portal
- Audiocodes Gateway
- Media Application Server
- UAS Audio Server

The hardware platform chosen for the CS2000 Session Server is the HP CC3310 NEBS-compliant rack-mounted server.

46.4 Linux Operating System / Distribution

The selected Linux distribution for CS2000 Session Server in the SN09 / MCP9.0 release is RedHat Enterprise Linux Advanced Server 3 (RHEL AS3), Update 3. This distribution was used in earlier Linux porting work for MCP products and thus provides the least risk for this release of CS2000 Session Server.

Future CS2000 Session Server releases will deliver on NCGL (Nortel Carrier Grade Linux). Several basic requirements need to be satisfied before this can occur, however, including:

- Support for the Sun 1.4.x series of JVM must be available.
- Support for the Oracle 9.2.0.5 DBMS.
- Support for the SunONE web server must be available. An alternative to this is the transition, for the MCP product, away from SunONE to Apache Tomcat.
- SMP (Symmetrical Multiprocessor) support for the target hardware (IA32) must be provided.
- Transition to the 2.6 kernel to leverage enhanced threading (NPTL, Native Posix Thread Library), scheduler performance, and SCTP stack.

46.4.1 Platform Hardware

The hardware platform chosen for the CS2000 Session Server in this release is the HP CC3310 server. This is a NEBS-compliant rack-mounted server. The following table provides the key hardware characteristics of this platform.

Table 2: HP CC3310 (Model A9862A) Specifications for CS2000 Session Server

Item	Description
Processor	2 Xeon @ 2.4 GHz each
Memory	4 GB
L2 Cache	512 KB
Hard Disk	2 x 73 GB 15K Ultra 320 SCSI, hot swap
Optical Drive	CD-RW / DVD-ROM
Ethernet	4 x 10 / 100 / 1000 Base-T
RAID	Software RAID
NEBS	Level 3
Power	DC, redundant
Form factor	Rack
Dimensions (H x W x D)	3.45" x 17.11" x 20" (2U high)

46.4.2 CS2000 Session Server Product Configuration

There is only a single logical MCP configuration which is supported for CS2000 Session Server. Figure 1 CS2000 Session Server Product Configuration1 shows the mapping of the major MCP system components onto CC3310 server machines. The base system consists of four HP CC3310 servers deployed as two redundant pairs. Server pair 1 hosts the following MCP elements:

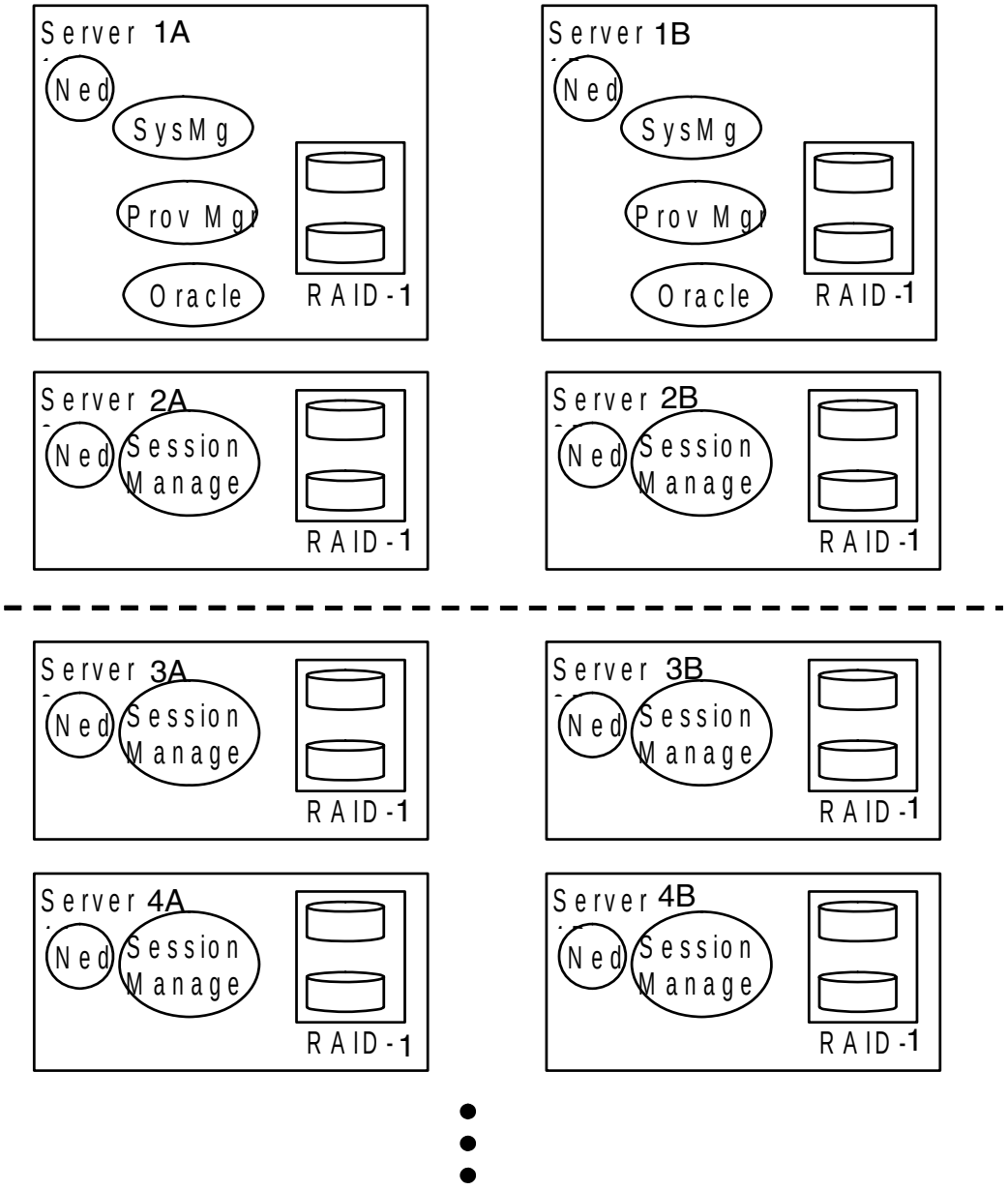
- SM (System Manager). This component configures, monitors, and maintains all MCP-based network elements. It also serves as the Fault-Performance Manager (FPM) which formats, stores, and forwards logs, alarms, and OMs. The backup system manager runs in a cold standby mode.
- Provisioning Manager. This network element provides the main provisioning interface into the system. It runs the SunOne web server through which client browsers connect to perform system-level provisioning actions. The provisioning managers run in load-sharing mode. Scaling of the Provisioning Manager is through additional provisioning managers.
- Database. This component provides the storage of persistent data for the system and is currently built on the Oracle DMBS. Redundancy is achieved through Oracle replication.
- Ned (Network Element Daemon). Ned is a process which runs on each server machine and which oversees the lifecycle of the MCP software components and cleans up logical network interfaces (where applicable) should a component die an unnatural death.

Server pair 2 hosts the following MCP components:

- SIP Session Manager. This network element runs the main SIP application portion of the CS2000 Session Server. The backup SIP Session Manager runs in hot standby. Scaling is through additional pairs.
- Ned. This is the same as previously discussed.

The server machines and components shown above the dashed line in Figure 1 CS2000 Session Server Product Configuration illustrate the base system (mandatory components). The server machines and components below the dashed line indicate an example of optional server machines and hosted MCP components used in system scaling. There is only a single (redundant pair of) SM / database / Prov in the system.

Figure 1 CS2000 Session Server Product Configuration



46.4.3 Installation and Commissioning (I & C)

There are four fundamental activities involved when performing an I&C on a CS2000 Session Server machine.

- Making BIOS-level settings and adjustments.
- Base-level software installation.

- Installation of the Oracle database on server machines which host the Database Module (if appropriate).
- Installation of MCP software loads in preparation for system deployment (if appropriate).

After completing the above steps, the system is then ready for the deployment of the MCP components and network elements.

46.4.3.1 BIOS-Level Settings

The CC3310 is an Intel based machine and comes with a BIOS familiar to any user who has previously used a PC or other Intel-based machine.

BIOS-level changes required during an I&C for this platform are TBD.

46.4.3.2 Base-Level Software

Installation of base level software typically includes the partitioning of disk drives, installation of the operating system and associated device drivers, installation of base system commands and utilities, and installation of MCP specific software packages used to support the MCP components and network elements to be deployed following the I&C process.

The core I&C mechanism used for this step of the I&C process is based on the RedHat kickstart framework.

The following basic steps are followed for this step of the I&C process:

1. Insert installation CD and reboot or power up the machine. Note that only a single CD is required for installation of the base system.
2. A Customer Information Questionnaire (CIQ) session is executed. The purpose of the CIQ is to specify key base-level configuration items for the server such as host IP settings (address, mask, gateway), the type of server being configured, IP addresses of other key machines, and time zone information.
3. The automated install of all the software mentioned at the start of this section is performed (no user intervention).
4. The system is rebooted.

The approximate installation time for base level software on the CC3310 platform is TBD minutes (expectation is roughly 15 minutes).

Note that this I&C mechanism is also used during system restore operations (recovering catastrophic server failures).

46.4.3.3 Oracle DBMS

If a Database Server machine is being I&C'd, the Oracle database is installed after the base level system install is finished. Installation methods for the

Oracle database follow the same CD install methods as is used for Solaris based MCP machines.

The approximate installation time for the Oracle DBMS on the CC3310 platform is TBD minutes (expectation is roughly 30 minutes).

46.4.3.4 MCP Software Installation

If a System Manager is being I&C'd, the MCP software load is installed after the base level system install is finished. Installation methods for these software loads follow the same CD install methods as is used for Solaris based machines.

The approximate installation time for the MCP load on the CC3310 platform is TBD minutes (expectation is roughly 5 minutes).

46.4.4 Backup and Restore

The objective of the backup and restore strategy is to provide a mechanism to completely recover a server machine, or a whole system, in the case of a catastrophic failure. A catastrophic failure typically means the loss of both disk drives (loss of all configuration).

The exact mechanism used for a backup and restore depends on the configuration of the server machine (see Figure 1 CS2000 Session Server Product Configuration). The following subsections outline specific backup and restore mechanisms for each configuration.

The backup and restore strategy employed here places no requirement for the use of tape drive units. In the cases where data must be persisted to external media, the customer has a choice on how this must be performed. Although a tape drive is one option, customers may also choose to perform this off-system storage through the use of CD-R's, CD-RW's, DVDs, or any other permanent external media.

46.4.4.1 Base System (Any Server Configuration)

When restoring a server machine, the first step in the process is always to recover the base system. Central to the restoration of the base of the system is the re-install and commissioning (re-I&C) of the machine from the original media. These server machines are relatively static in their configuration. Other than MCP component software, these machines do not undergo any other software installations which deviate from the original installation. Any base-level patches applied to an installed system are typically included in a new release of the I&C CD-ROM which is delivered as part of the maintenance release (MR). Re-installing from this new CD eliminates having to re-apply incremental patches from previous MRs.

This step of the restoration process, therefore, means the application of the I&C steps outlined in section BIOS-level Settings, if required, and section

Base-Level Software. The backup process for the latter (base system software) simply means the persistence, onto external storage, of the critical configuration data gathered during the CIQ (Customer Information Questionnaire) of the original I&C for that server machine. The restoration of the base level software, therefore, is optimized by making available this saved configuration information to the I&C mechanism during a restore, thus optimizing the time involved in the restoration process and drastically reducing the possibility of configuration errors.

46.4.4.2 SM + DB + Prov Configuration

All configuration information for the System Manager and Provisioning Managers are persisted in the database. There are no special actions required to perform backups of these components. For the database component, a nightly cron job executes on the hosting server machine, and which takes a snapshot of the primary database, storing it on the local hard drive. This backup image is then manually transferred to a remote backup server using secure FTP (SFTP). At the remote machine, this file is then written to persistent external media such as a CD-ROM, DVD, or tape drive. This protects against failures of the backup server. This storage mechanism is beyond the scope of this feature.

The following is the general procedure followed to restore a server machine configured with these components. This procedure assumes that the mated (redundant) server machine has taken over service for all of these components.

- The base level system is restored as described in section “Base System (Any Server Configuration).”
- The Oracle DMBS is installed using standard installation methods for I&C, but making use of the persisted configuration settings from the initial install (similar to how the base level software configuration systems are persisted).
- The MCP load is placed onto the server machine.
- The Database component is deployed manually using scripts from the MCP load. The “No files” option is specified such that no attempt is made to bring the database into service, or to start a database sync operation.
- A database re-sync operation is run to bring the two databases into sync and to allow the primary to take over execution (if this server machine in fact hosts the primary database).
- The System Manager component is deployed manually using scripts from the MCP load. The System Manager is left in the non-running state as the mate System Manager is currently running on the redundant machine.
- If necessary, the backup System Manager is taken down, and the primary System Manager is brought up.
- From the Management Console, the Provisioning Manager is re-deployed.

At this point, the server has been restored to full operation. In the event that both servers hosting these components have failed, the same procedure is followed above, except for the recovery of the first (primary) database. Instead of recovering the database contents from a re-sync operation, the snapshot from the last backup is transferred to the machine and local scripts are executed to restore the contents from that snapshot.

46.4.4.3 Session Manager Configuration

The restoration of the Session Manager server configuration shown in Figure 1 CS2000 Session Server Product Configuration is a simpler process than that required for the SM / DB / Prov configuration described earlier. The fundamental steps include:

- Restore the base system software as described in section “Base System (Any Server Configuration).”
- From the Management console, deploy and start the component(s) found on that server.

46.4.5 System Management

46.4.5.1 Core System Management

The core OAM (Operation, Administration, and Management) mechanism of the CS2000 Session Server remains as it is in MCP4.0. The System Manager (SM) continues to provide the following key management functions:

- Deploying, undeploying, starting, and stopping CS2000 Session Server network elements such as the Provisioning Manager and Session Manager.
- The collection and reporting of logs from the various network elements.
- The collection and report of Operation Measurements (OMs) from the various network elements.
- The collection and reporting of alarms from the various network elements.

The SM continues to provide a WSDL-based management interface through which clients such as the MCP Management Console can communicate. The default Management Console, accessed through the Apache Tomcat web server, remains.

46.4.5.2 Northbound Network Management System (NMS) Interfaces

A number of north-bound NMS interfaces are used with the CS2000 Session Server including:

- Management console
- Open Provisioning Interface (Bulk Provisioning)
- Secure FTP / SSH
- Nortel Reliable MIB.

46.4.5.3 Remote Server Management

Remote server management refers to the ability to power down, power up, and reset CS2000 Session Server network elements remotely from the System Manager. The typical interface for performing this function is via the CS2000 Session Server Management Console which interfaces to the System Manager via the WSDL-based OMI interface.

This capability is not a requirement for CS2000 Session Server in this release and is therefore not implemented for the CC3310 platform.

46.4.5.4 Serial Console

Serial console access refers to the ability to log into the system console through the serial port of the server machine. This is required in the event of loss of access through normal SSH login mechanisms, and for security reasons.

Connectivity is achieved by attaching the external serial port of the CC3310 to a terminal server. Access to the terminal server is typically through a management LAN and is therefore protected from general access.

The system console of the kernel is made available to the serial port both at I&C and during normal system run time. Serial console login is enabled for all provisioned users (“root”, “sysadmin”, and “nortel”).

Providing serial console access during I&C allows multiple systems to be I&C’d simultaneously from one remote station (e.g., PC).

46.4.5.5 SSH / SFTP

Telnet and FTP access to server machines is disabled as part of OS hardening (refer to that section). Instead SSH (Secure Shell) and SFTP (Secure FTP) access are provided.

46.4.6 Application-Level Components

46.4.6.1 SIP Stack

In this release of the CS2000 Session Server, the SIP stack is being migrated from Java to the Radvision C++ stack. For application components which are written in Java, JNI is used to interface to the C++ stack. The integration of this stack into the CS2000 Session Server is outside the scope of this feature and is being performed by [3].

46.4.6.2 Web Server

The CS2000 Session Server makes use of two different web servers.

- The Apache Tomcat web server is used to gain access to the System Manager’s Management Console, and makes use of the Java Web Start mechanism.

- The SUN Microsystem's SunONE web server is used on the Provisioning Manager. This web server is actually installed during I&C on all server machines but is only enabled on the machines which are deployed with the Provisioning Manager. Feature FTR460 [6] enabled SSL for the SunONE web server on Linux and provided a default Nortel self-signed certificate. This feature completes the integration of this functionality onto the target Linux platform used by this feature.

46.4.6.3 Java Virtual Machine

The CS2000 Session Server uses version 1.4.2_06 of the Sun MicroSystem's JVM.

46.4.7 IPSec

IPSec is used for encrypted connections (using transport mode) between the following components:

- RTP Portal and database server machine.
- RTP Portal and the System Manager (SM).
- RTP Portal and Session Manager.

Under the target Linux distribution, the IPSec policy database and encryption is performed within the kernel. The "ipsec-tools" RPM package is a BSD-licensed open source package which provides the following capabilities (refer to [7] for more information on open sources licenses):

- "libipsec", a PFKeyV2 library
- "setkey", a program to directly manipulate policies and SAs (Security Associations)
- "raccoon", an IKEv1 keying daemon

The API-level integration of IPSec into the CS2000 Session Server is implemented by [5]. This feature (A00009230) integrates the work of [5] into the I&C of the target systems.

46.4.8 Database

The database implementation used for CS2000 Session Server is Oracle 9i.

46.4.9 Fault Tolerance

There are several key areas regarding fault tolerance which are relevant to this feature. They are included in the following subsections.

46.4.9.1 Network (Ethernet) Interfaces

As with prior MCP releases, the dual ethernet interfaces to the server machine are grouped together in a port-bonded relationship using the port bonding driver functionality built into the linux kernel. The bonded interfaces are arranged in an active-backup mode. Upon initialization of a healthy system,

eth0 is made the active interface and eth1 the backup. When an active interface fails, the other interface takes over and remains active until it fails or the system is once again restarted.

Failure detection is through “miimon” which monitors link status. Upon failure of the link (e.g., link pull, failed network interface), failover actions are automatically taken by the port bonding driver, and remain unknown to application layer software.

46.4.9.2 Application Fault Tolerance

Check pointing and hot standby is added by [4] to the Session Manager’s fault tolerance functionality. The remainder of the MCP system’s application-level fault tolerance functionality remains the same as in prior MCP releases.

46.4.9.3 RAID (Redundant Array of Independent Disks)

RAID Level 1 (disk mirroring) is a hard requirement for the CS2000 Session Server machines. RAID-1 allows the continued operation of the system in the event one of the disk drives should fail.

The HP CC3310 server platform does not provide hardware RAID natively on the machine. Rather, an optional RAID controller (PCI card) from Intel is available, at additional cost, to provide this function. However, this additional cost and NEBS PI testing requirements make it infeasible to include this optional card into the product at this time. Given that the disk I/O traffic is relatively moderate for this type of system and does not pose a bottleneck, software RAID is an acceptable alternative and is implemented by this feature. Note, however, that software RAID requires a post-I&C period where the system synchronizes the two hard drives. During this time, the system runs in a degraded (non-protected, CPU overhead) mode.

This feature implements RAID-1 using the RAID functionality provided by either the “raid-tools” or “mdadm” GPL packages.

46.4.10 Kernel Features

46.4.10.1 SMP (Symmetric MultiProcessing)

The HP CC3310 platform uses dual 2.4 GHz Xeon processors. The kernel of the target Linux distribution fully supports SMP to allow the CS2000 Session Server to fully leverage this capability.

46.4.10.2 Hyper threading

The Xeon processors used on the HP CC3310 platform include support for hyper threading. The kernel of the target Linux distribution fully supports hyper threading to allow the CS2000 Session Server to fully leverage this capability.

46.4.10.3 NPTL

The target Linux distribution implements the NPTL (Native Posix Thread Library) enhancements which provide a much improved thread model than found in previous Linux distributions.

46.4.10.4 OS Hardening

This feature includes the changes required to provide a secure (hardened) system which is resistant to malicious or inadvertent attacks. These changes are implemented through a combination of elements including installation of software packages (e.g., ssh) and patches, changes to configuration files, and changes to system settings in the late stages of the automated installation procedure.

Areas which are affected by this hardening exercise include:

- Install patch for security and bug fix
- Minimize services
- Access control and authorization
- Logging
- Kernel tuning
- File and file system security
- Manage account on the server
- Secure Shell SSH
- Other miscellaneous actions

Please refer to [1] and [2] for a detailed discussion of the elements which go into the hardening of a system, and which are employed as part of this feature.

46.4.11 SCTP

The CS2000 uses SCTP as the transport protocol for the NCAS (Non Call-Associated Signalling) link between the CS2000 core and the CS2000 Session Server. This link is used for the relaying of line-maintenance related signalling.

The kernel of the target linux distrution does not currently support SCTP natively. The implementation of SCTP is therefore based on the open-source reference standard for SCTP available from “sctp.de” [8].

46.4.12 Software Management

46.4.12.1 Software Delivery

The processes for the naming, building, bundling, vaulting, and delivery of the CS2000 Session Server follows the same methods as used in prior MCP releases. Loadnames are based on MCP 9.0 version naming.

46.4.12.2 Software Upgrade and Maintenance Releases

The process to bring a system to a running state where it is able to process traffic involves two different stages of software installation. The first stage is the I&C of the server machine as is described in section “Base-Level Software.” The second stage is the deployment of the MCP component software onto the appropriate target machines.

Applying software updates and maintenance releases to the MCP component modules (second stage above) is performed in the same fashion as is done for MCP components on prior Solaris-based MCP systems. This essentially involves the creation and vaulting of new CD images of MCP software loads, distributing and installing these loads to customer systems, and using the system management console to apply the updated software to the necessary server machines.

Due to I&C differences, however, the methods for applying software upgrades and maintenance releases to the base platform are different for Linux based systems. The following outlines the steps performed for maintenance releases to this base software:

- At some point, it is determined that a new release of the base server software is required. Examples of such changes include patches to the base Linux kernel, corrections to MCP base software, and new base system utilities.
- Each of these updates is built into an RPM (RedHat Package Manager) package.
- The set of these RPM packages are collected and an MR (Maintenance Release) README file is created with instructions on how to apply the changes to an existing system.
- An ISO CD image is created with this update and is vaulted in the Nortel software distribution databases.
- A new I&C CD is created with these same updates included and is similarly vaulted.
- Both the MR and new I&C CD are delivered, or downloaded, to the customer site(s).
- The MR CD is used to apply the updates to any existing machines.

In addition to the base level software, it may also be necessary to upgrade the BIOS of the machine. BIOS upgrades are typically required due to unrecognized (new) hardware and therefore are usually required during initial system I&C (where the factory-installed BIOS may be an older revision). BIOS upgrades are typically performed using bootable media where, upon boot up, a program is launched through which the BIOS flashing process is performed. These boot media are vaulted and distributed to customers in the same manner as is done for system I&C CD’s.The I&C CD is used to install

any new servers which may be required and / or to restore any existing server which may fail in the future.

46.4.13 Re-IP Serviceability

The Linux-based MCP system has the ability to be re-IP'd through execution of a local script. Prior to the re-IP, the components on the server machine need to be undeployed and re-configured. The steps to recover the MCP components are similar to the steps used to restore MCP components as described in section "Backup and Restore."

46.4.14 Third Party Software Licensing and Support

The following are the major third party software components used by this feature:

- RedHat Enterprise Linux Advanced Server 3 (RHEL AS3). This includes a number of open source packages within the distribution.
- Oracle 9i
- Sun MicroSystems Java Virtual Machine 1.4.2_06
- SunONE web server

Additional dependencies on third party software and their licensing are TBD.

46.5 Dependencies

Not applicable.

46.6 Network Engineering

A Linux-based server requires two less IP address than a Solaris server configured with the same software components. This is due to the differences in NIC redundancy mechanisms between Solaris and Linux.

On Solaris-based machines, IPMP (IP MultiPathing) requires a physical IP address per NIC, as well as a logical IP address per IPMP group. Linux based machines use port bonding in place of IPMP. The port bonding driver re-uses the same IP address for both NICs as well as the bonding interface which is created to enslave these NICs. Therefore, on a public-only machine with two NICs (the only configuration supported for Linux-based servers), only a single IP address is required.

There are no differences in IP port usage between Linux and Solaris.

46.7 References

46.7.1 Internal Documents

1. MCP3.0LinuxHardening, MCP Livelink Site : MCP Technology Documentation -> MCP_3.0 -> PrepDocs.

2. MCP3.0Solaris8Hardening, MCP Livelink Site : MCP Technology Documentation -> MCP_3.0 -> PrepDocs
3. A00009046, Radvision Support, MCP Livelink Site : Technology Documentation -> MCS_9.0 -> Feature Documentation
4. A00009045, CallP Checkpointing Support, MCP Livelink Site : Technology Documentation -> MCS_9.0 -> Feature Documentation
5. A00009151, PKI Manual Key Management, MCP Livelink Site : Technology Documentation -> MCS_9.0 -> Feature Documentation
6. FTR460_FD_SSLWebSOAPIF.doc, MCP Livelink Site : Technology Documentation -> MCS_4.1 -> FDs

46.7.2 Other References

1. Open Source Org Licence Index, http://www.opensource.org/licenses/
2. http://www.sctp.de. (Open-source reference implementation of SCTP stack.)

46.8 Definitions & Abbreviations

API	Application Programming Interface
BIOS	Basic Input Output System
BSD	Berkely Software Distribution
CD	Compact Disc
CIQ	Customer Information Questionnaire
DBMS	DataBase Management System
DVD	Digital Video Disc
FPM	Fault Performance Manager
FSB	Front Side Bus
FTP	File Transfer Protocol
GA	General Availability
GHz	Giga Hertz
GNU	GNU's Not Unix (recursive definition)
GPL	GNU General Public Licence
I&C	Installation and Commissioning
IKE	Internet Key Exchange
IP	Internet Protocol
IPMP	IP MultiPathing
IPSec	IP Security
ISO	International Standards Organization
JNI	Java Native Interface
JVM	Java Virtual Machine
LOM	Lights Out Management
MCP	MultiMedia Communication Platform
MCS	MultiMedia Communication System
MIB	Management Information Base
MR	Maintenance Release
NCAS	Non Call-Associated Signaling
NCGL	Nortel Carrier Grade Linux
NEBS	Network Equipment Building Standard
NED	Network Element Daemon

NIC	Network Interface Card
NMS	Network Management System
NPTL	Native Posix Thread Library
OAM	Operation Administration and Maintenance
PCI	Peripheral Component Interconnect
PI	Product Integrity
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RHEL	RedHat Enterprise Linux
RHEL AS3	RedHat Enterprise Linux Advanced Server version 3
RPM	Release Package Manager
RTP	Real-Time Protocol
SCTP	Stream Control Transmission Protocol
SFTP	Secure File Transfer Protocol
SIP	Session Initiation Protocol
SM	System Manager
SMP	Symmetrical MultiProcessor
SN	Succession Networks
SSH	Secure Shell
SSL	Secure Sockets Layer
TBD	To Be Determined
UAS	Universal Audio Server
WSDL	Web Services Description Language

47: Functional description (FN): A00009235

47.1 Feature name and Feature ID

Activity A00009235 - TLS for SIP

TLS = Transport Level Security, a security protocol that enables secure data transmission between two communicating applications.

SIP = Session Initiation Protocol

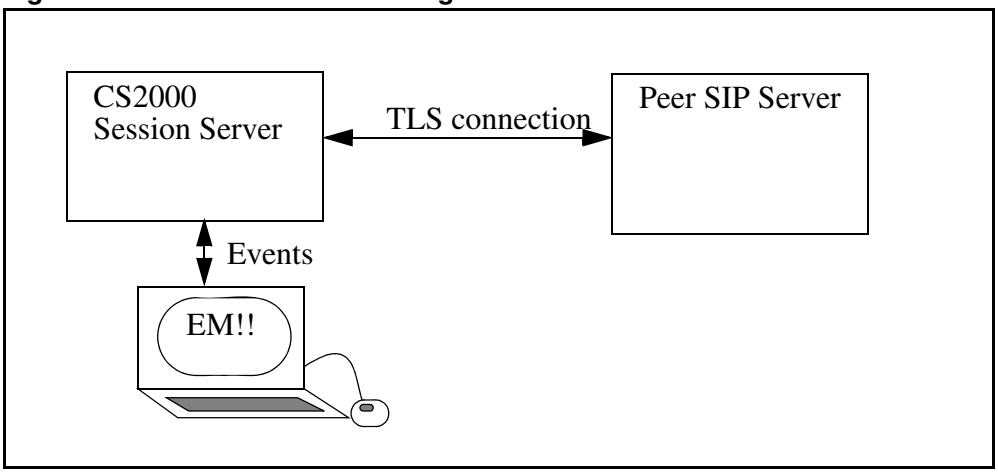
47.2 Description

The TLS for SIP feature will provide robustness improvements over the SN08 functionality, as well as provide compliance to specified Packet Cable requirements.

The peer-to-peer scenario is the focus of this feature. The peer SIP servers that the CS2000 Session Server connects to need to be authenticated, a TLS cipher must be selected, and the connection must be monitored, all to ensure the security of the connection and the validity of the messages being passed between the two peers. Most of this functionality has been delivered already, however some items remain (for example, FQDN/IP address mapping from the certificate, to ensure that FQDN's can be verified in the SIP messages).

Additional robustness improvements on the local CS2000 Session Server to alert the craft to issues in the system are required, and added flexibility to system/threshold settings are desired as well.

Figure 1 Functional Behavior Diagram



47.3 Hardware Requirements or Dependencies

No new hardware dependencies are introduced in SN09.

47.4 Software Requirements or Dependencies

This feature requires the standard SN09 load.

47.5 Limitations and restrictions

The following limitations exist for this feature:

Provisioning

- CS2000 Session Server Call Processing must be restarted anytime a new server certificate is provisioned (Call Processing is not required to be restarted if remote servers' certificates are provisioned).
- CS2000 Session Server Call Processing must be restarted for the following security parameters to take effect:
  ExitOnFailTLSInitialization
  MaxTLSSessions
  localTLSport
- Self-Signed Certificates from other servers must be data filled on the CS2000 Session Server in order to have the CS2000 Session Server recognize those certificates.
- Any Self-Signed Certificate from the current CS2000 Session Server must be data filled on other CS2000 Session Servers -- and other SIP servers in general -- in order to have the remote servers recognize those certificates.
- Restarting CS2000 Session Server Call Processing means restarting the SIP gateway application.

Performance

- Client-side session caching will be supported on the CS2000 Session Server. Server-side session-caching is already supported. However, the session cache exists only in memory. During a Dead-Office Recovery (DOR) new TLS sessions will require a full handshake.
- The maximum number of supported simultaneous TLS connections is limited to 400. The provisionable parameter 'MaxTLSSessions' controls this maximum number, and any connection attempts beyond the provisioned maximum will be rejected.

Cryptography

- Only RSA/DHE_RSA and AES/3DES ciphers will be enabled for use on the CS2000 Session Server by default. These will be the only ciphers supported by Nortel on the CS2000 Session Server. Specifi-

cally, the supported ciphers will be:
TLS1_TXT_RSA_WITH_AES_128_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS1_TXT_RSA_WITH_AES_256_SHA,
TLS_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA and
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.

- RSA keys used on the CS2000 Session Server will require a minimum of 1024 bits. RSA keys of smaller sizes are generally considered to be vulnerable to cracking.
- AES keys used on the CS2000 Session Server will require a minimum of 128 bits.
- Imported certificates will be expected to be in X509 version 3 PEM format,, in order to be imported for use by the CS2000 Session Server.

Licensing

- Licenses apply to certain open-source code (OpenSSL, Cryptlib) that are used in the CS2000 Session Server implementation of TLS. Terms of use require acknowledgement of the various authors in customer documentation materials etc. Please see appendix for full licenses of open-source code used within this product.

Certificate

- In this activity if the certificate and key files is changed in one NGSS, during initialization the mate host will be notified. If the mate host has not been updated with the new certificate and key files an alarm will raise. The limitation here is the application is not copying the certificate and key files over the mate host and by a craft person should do it.
- If the Common Name of the certificate contains an FQDN, it must match the Remote SIP Server name as provisioned in the Remote SIP Server web page. This FQDN must be less than 64 characters in length.
- Remote SIP Server Cluster configurations in which a single Remote SIP Server has been datafilled with multiple IP addresses must ensure that the Common Name of the certificate presented from any one of the IP addresses in the list matches either the IP address of the originator, or the FQDN as presented as the name of the Remote SIP Server.

47.6 Interactions

47.7 Glossary

Term	Description
TLS	Transport Level Security, a security protocol that enables secure data transmission between two communicating applications.
SIP	Session Initiation Protocol
DOR	Dead-Office Recovery, the term used to describe the complete loss, then recovery, of an entire office.

47.8 Appendix

- Open SSL license

```
//* ====================================================================
* Copyright (c) 1998-2004 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit.  (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
```

```
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
=====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).

*
*/
```

- Eric Young's License

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
```

- Brian Gladman's License

```
---------------------------------------------------------------------------
Copyright (c) 2002, Dr Brian Gladman <brg@gladman.me.uk>, Worcester, UK.
All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary
form is allowed (with or without changes) provided that:

  1. distributions of this source code include the above copyright
     notice, this list of conditions and the following disclaimer;

  2. distributions in binary form include the above copyright
     notice, this list of conditions and the following disclaimer
     in the documentation and/or other associated materials;

  3. the copyright holder's name is not used to endorse products
     built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product
may be distributed under the terms of the GNU General Public License (GPL),
in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties
in respect of its properties, including, but not limited to, correctness
and/or fitness for purpose.
---------------------------------------------------------------------------
Issue Date: 26/08/2003
```

- Peter Gutmann's License

```
/* The random pool handling code in this module and the misc/rnd*.c modules
   represent the cryptlib continuously seeded pseudorandom number generator
   (CSPRNG) as described in my 1998 Usenix Security Symposium paper "The
   generation of practically strong random numbers".

   The CSPRNG code is copyright Peter Gutmann (and various others) 1995-2002
   all rights reserved.  Redistribution of the CSPRNG modules and use in
   source and binary forms, with or without modification, are permitted
   provided that the following conditions are met:

   1. Redistributions of source code must retain the above copyright notice
          and this permission notice in its entirety.

   2. Redistributions in binary form must reproduce the copyright notice in
        the documentation and/or other materials provided with the distribution.

   3. A copy of any bugfixes or enhancements made must be provided to the
          author, <pgut001@cs.auckland.ac.nz> to allow them to be added to the
          baseline version of the code.

   ALTERNATIVELY, the code may be distributed under the terms of the GNU
   General Public License, version 2 or any later version published by the
   Free Software Foundation, in which case the provisions of the GNU GPL are
   required INSTEAD OF the above restrictions.

   Although not required under the terms of the GPL, it would still be nice
   if you could make any changes available to the author to allow a
   consistent code base to be maintained */
```

48: Functional description (FN): A00009239

48.1 Feature name and Feature ID

A00009239: Services for SIP Lines

48.2 Description

This feature expands the existing Message Waiting (MWT) service supported in the CS2K Core to SIP Lines.

The MWT service provides the activation/deactivation of the Message Waiting Indicator (MWI) on the line. In SIP Lines case, actual MWI is provided by the SIP Line or actual edge device (e.g. Optical Network Terminator (ONT)) when the SIP Notify message with Message Waiting header is received from the network and/or voice mail system.

The MWT service in SIP Lines case assumes that the Voice Mail is connected to Communication Server 2000 (CS2K) via existing Voice Mail connetivities (e.g. SMDI and UCD for Traditional Voicemail). The SIP Line is assigned with the appropriate Call Forwarding - Call Forward Do Not Answer (CFD) and Call Forward Busy (CFB) options.

When a call is terminated to SIP Line, the call is offered to the line. However, if end user is busy on another session/call on the SIP device or end user do not answer the call, the CFB or CFD occurs and call forwards to the Voicemail. The Voicemail as existing functionality answers the call and prompt with personalized greeting to the caller. The caller leave a message and end the call. The Voicemail sends the activation request to the serving CS2K for the SIP Line. This request is converted to a SIP Notify message by CS2K and sent to the SIP Line. The SIP Line than provide appropriate message waiting indication to the device for end user.

When end user observes the indication, make a call to Voicemail system. Upon answer, the voicemail prompts the end user for the userid and password. The end user connects to his/her voicemail box after userid and password authentication and starts listening the voice messages. When all new messages are listened by the end user, the Voicemail sends the deactivation request to the serving CS2K for the SIP Line. This request is converted to a SIP Notify message by CS2K and sent to the SIP Line. The SIP Line than remove appropriate message waiting indication to the device for end user.

48.3 Hardware Requirements or Dependencies

Not Applicable

48.4 Software Requirements or Dependencies

Not Applicable

48.5 Limitations and restrictions

The following are the restrictions and limitations of this service:

- Only Message-Waiting ON/OFF is supported in the SIP Notify message as per RFC 3842. Rest of the optional data required by the RFC 3842 are not supported.
- The existing MWT software in the CS2K only supports number upto 10 digits. This existing limitation apply to the MWT extension to SIP Lines.
- The direct communication with a SIP based Voicemail is not supported due to limitation of availability with the SIP based Voicemail during development.
- The DTMF tones required by the Voicemail system is assumed to be supported by appropriate Codec from the SIP Lines.
- This development only supports following form of the MWT service:
  - Message Waiting (MWT) option on the line.
  - Network Message Waiting (NMS) when Voicemail is networked to serving CS2K.
  - AIN (North American - NA) based MWT using AIN Update messages from Switching Control Point (SCP) to serving CS2K.
- For SIP Lines, only Message Waiting Lamp (MWL) notice is valid to datafill in the CS2K. The Stutter Dial Tone (STD), Periodic Ring Notification (PRN), etc. notice types are invalid for the SIP Lines because SIP Notify message does not allow to specify the notice type for SIP Line device. Also, the type of indication depends on the end user device in the SIP Lines case.
- Only following type of SIP Lines are supported by this design:
  - SIP Phone provided by CISCO
  - PC Client

48.6 Interactions

All existing MWT interactions works the same way with the SIP Lines. No new interaction anticipated.

48.7 Glossary

Term	Description
AIN	Advance Intelligent Network
CFB	Call Forward Busy
CFD	Call Forward Do Not Answer
CS2K	Communication Server 2000
DTMF	Digitone Multifrequency
MWI	Message Waiting Indicator
MWT	Message Waiting
NA	North American
NMS	Network Message Waiting
ONT	Optical Network Terminator
PC	Personal Computer
PRN	Periodic Ring Notification
SCP	Switching Control Point
SIP	Simple Internet Protocol
SMDI	Simplified Message Desk Interface
STD	Stutter Dial Tone
UCD	Uniform Call Distribution

49: Functional description (FN): A00009241

49.1 Feature name and Feature ID

A00009241 - NCAS and QSIP Development on CS2K SS

49.2 Description

The Non-call associated signalling (NCAS) Link on Communication Server 2000 (CS2K) Session Server (SS) platform with query SIP line data (QSIP) application feature provides a light-weight switching control point (SCP) like functionality (SCPLite). The NCAS link provides a non-call associated link between the CS2K SS and the core. At present the NCAS link is only used by the SIP Lines program for QSIP command interface (CI) command in the core to get the static and dynamic data snap shot from the CS2K SS platform related to the SIP line.

The display of the static and dynamic data is provided by QSIP CI command at CI increment.

49.3 Hardware Requirements or Dependencies

The development is on CS2K SS platform.

This activity does not require any new hardware.

49.4 Software Requirements or Dependencies

This activity uses SCTP library (SCTP.DE) developed in Germany for SCTP communication with the Core. The SCTP.DE is a generic SCTP library available from the web and it is not a NOTEL product.

The activity depends on the following two activities:

- QSIP CI Command development in the core under actid A00008556.
- OAM and GUI development in the CS2K SS platform under actid A00009028.

49.5 Limitations and restrictions

- Only one NCAS link is allowed for QSIP Application. When the link is active for QSIP application, subsequent QSIP application request to create another NCAS link will be ignored.

- QSIP application has lowest priority. Therefore, in case of high traffic and/or abnormal conditions, QSIP application will not response with the data within the timeout period.
- The T1 timer for the query and response is controlled by the office engineering parameter, Table OFCENG, AIN_T1_TIMER in the core.
- During failover cases, the NCAS link is disconnected with the core and re-established from the active side. All outstanding QSIP request prior to failover complete will be discarded and no response will be provided.

49.6 Interactions

The QSIP command from the core is a stand alone command. In the core, the QSIP CI increment send a request to CS2K SS platform. The software developed under this activity gathers the static and dynamic data associated with the specific SIP line, and sends an asynchronious response to QSIP CI in the core.

The QSIP request, data collection and sending response are independent from other activities/actions/events in the CS2K SS platform. Therefore, no specific interaction anticipated by this activity.

49.7 Glossary

Term	Description
CI	Command Interface
CS2K	Communication Server 2000
GUI	Graphical User Interface
NCAS	Non-Call Associated Signalling
OAM	Operation, Administration and Maintenance
QSIP	Query SIP Line data
SCP	Switching control point
SCPLite	SCP like functionality
SCTP	Steam Control Transport Protocol
SIP	Session Initiation Protocol
SS	Session Server

50: Functional description (FN): A00009252

50.1 Feature name

A00009252 Multi-Time Zone AMA Enhancments

50.2 Description

In order to support networks that span Multiple Time Zones (MTZ) features in the Succession/CS2K products must be enhanced. Feature A59038784 introduced a framework to support MTZ and DST (Daylight Savings Times) for subscriber visible services. Feature A00009120 (done in parallel with this feature) extends this framework.

This feature allows the customer to record a corrected timestamp for billing records that originate on agents with the MTZ line option. The connect timestamp will be modified to the agents time zone and this timestamps will be appended to the existing billing record in AMA using a module code and SMDR using an extension record.

Table AMAOPTS contains a new switch wide option (RECORD_MTZ) that will allow customers to use the MTZ option and decide whether or not they want to record the modified timestamp.

50.3 Software Requirements or Dependencies

SN09

50.4 Limitations and restrictions

The limitations and restrictions specified in activity A59038784 and A0009120 are also applicable to this activity.

In addition the following limitations and restrictions apply:

- This feature will not FORCE billing records, it will only append the information if a billing record exists.
- This Feature only modifies the Connect time stamp.
- Billable calls that terminate to an agent with the MTZ option will not generate a modified timestamp.

50.5 AMA

The addition of the MTZ line option and corresponding MULTITM datafill will append module code 611 (context ID 80200) that contains a modified connect time and date. The record will look as follows:

50.6 SMDR

50.7 Interactions

This feature interacts with the Multi-Time Zone feature, A59038784 and A0009120 Multi-Time Zone Enhancments.

50.8 Glossary

Term	Description
MTZ	Multi-Time Zone Enhancment
AMA	Automatic Message Accounting
SMDR	Station Message Detailed Recording

51: Functional description (FN): A00009280

51.1 Feature name and Feature ID

A00009280: MG9K Line Circuit Enhancements

51.2 Description

The MG9K EM Line Circuit Enhancements concentrates on the below requirements for SN09 release:

1> Color indication for alarms on the port ilog of the Card Display.

2> User can manually mark a port as faulty.

3> Color indication for faulty port on the port ilog of the Card Display.

4> Display of directory number in the LineCircuit view

5> Display of directory number at the Alarm Browser screen for alarms reported.

Also the associated directory number would get added in the line circuit alarm log.

6> Circuit Listing at the NE desktop level to list the faulty ports.

51.3 Alarms display at the Port level

The line circuit ilogs on a LineCard would be displayed with an appropriate alarm color (if any alarm exists on the line circuit). User can easily make out the ports with alarms without opening a Port View. Currently alarms show in color at many different levels in the EM such as the shelf and card but not at the port level. After the addition of this functionality EM would be consistent at all levels in displaying alarms. The existing port view would not be changed. WLC,XDSL,GLC and SAA card view currently displays a list of line circuits. Existing alarm colors would be used to indicate the appropriate alarms on the port ilog of a line card view.

say: Critical alarm: Red
Major alarm: Red
Minor alarm: Orange
Warning : Yellow

51.3.1 Manually marking a port as faulty from the Port view

The new Line Circuit view would enable a User to mark a port (line circuit) as faulty. User can mark a port as faulty only when it is locked. Authorization level for this method would be ‘ewsmtc’. Fault setting option would be disabled (greyed out) if the port is unlocked.

User would get a warning message when he tries to unlock a faulty port. But if User wishes to go ahead irrespective of the port being marked as faulty, the request would get submitted.

'Fault State' field would be added in the 'Circuit Status' section of a port view. This new variable will be persisted only on the EM. There is no associated MIB variable for this state.

51.3.2 Display of faulty ports with a specific color

Currently User has no indication of the port being faulty. This functionality would help User to indentify a faulty port/circuit from the Line Card View.

A faulty port would be displayed with magenta color. Faulty color indication on a port would take precendence over alarms color indication.
say: A port which has alarms and is also marked by the User as faulty would be displayed with magenta color.

51.4 Display of Directory number(DN) at the Line Circuit view

With every line circuit associated to a VMG, there can be an associated DN. The DN will be displayed in the 'Circuit Provisioning' section of the Line Circuit view.

This would help the User to be positive that he is on the correct port. Display of the directory number that is associated with a port ensures proper location.

If the DN is not yet created for a line circuit, then the field would have 'None' as the value.

Any subsequent changes to DN would get udpated on a open Line Circuit view.

51.5 Display of Directory number(DN) on Alarm Browser

Directory number(DN) associated with a particular Line Circuit would be displayed in the description part of the Line Circuit alarm on a Alarm Browser.

eg: The description part of a line circuit alarm would have an added entry
`DN Affected: 6195210102`
If no DN is associated with the line circuit, then the description part of the line circuit alarm would have an appended entry saying
`DN Affected: None`
DN associated when the alarm was reported would be displayed. Any subsequent changes to the DN would not get updated on the Alarm Browser.

Physical location and the directory number details for a line circuit alarms would be helpful in troubleshooting.

Alarm log would also reflect the DN associated with the line circuit alarm.

51.6 'Faulty Circuit Listing' view at the NE Desktop level

A new menu item would be added in Services Menu list, on NE desktop view, namely 'Faulty Circuit Listing'. Clicking this menu item would display the 'Faulty Circuit Listing' view which has the below

information:
1> Associated Frame number
2> Associated Shelf number
3> Associated Slot number
4> Port Number

'Faulty Circuit Listing' view at NE desktop level would have readonly values. This GUI would have an associated time stamp and a refresh button. Refresh button is used to refresh the GUI with the latest port being marked as faulty. Refresh button is used to avoid dynamic updates when the faulty status of the port changes.
Timestamp would reflect the last time when the 'Refresh' button was used to collect the latest faulty ports information.

51.7 Hardware Requirements or Dependencies

None

51.8 Software Requirements or Dependencies

None.

51.9 Limitations and restrictions

- User will be allowed to mark a port/line circuit as faulty only when it is locked.
- User would get an appropriate warning message when he tries to do unlock a faulty port.
- XDSL Data Circuits cannot be marked as faulty.
- Fault color display on a line circuit would take precedence over alarm color indication.
- No new color indication would be displayed for a port which is locked.
- Once the line circuit alarm is reported to the Alarm Browser, any subsequent changes to the DN of that particular Line Circuit would not get updated in the description part of the Alarm Browser for a line circuit alarm.
- Existing Circuit Listing GUI would not be changed. Line Card level circuit listing GUI will behave as before and would not undergo any changes as a part of this feature

51.10 Interactions

None.

51.11 Glossary

Term	Description
WLC	World Line Card
SAA	Service Adaptive Access
XDSL	X Digital Subscriber Line Card

Term	Description
MG9k	Media Gateway 9000
MG9K-EM	Media Gateway 9000 - Element Manager
GLC	Global Line Card
DN	Directory Number

52: Functional description (FN): A00009282

52.1 Feature name and Feature ID

A00009282: Emergency Stand Alone (ESA) Multiple Level Precedence and Preemption (MLPP) for MG9KEM

52.2 Description

MLPP is a Defense Switched Network (DSN) feature provided today in the Legacy environment. This feature provides MLPP off the MG9K for deployment of Succession to the United States Government. The MLPP feature provides a user with the ability to preempt a call in progress. If the originator dials a precedence level that is higher than the call which the terminator is involved, the call may be preempted. This feature is typically used in emergency situations and not during normal day to day phone calls.

MLPP in ESA will be supported on all platforms (ATM, IP, GigE) but only for Enhanced ESA. Enhanced ESA is required for the MG9K to receive the line and translation data necessary to support precedence dialing and preemption. As such, MLPP will interwork with the supported Enhanced ESA line services feature set across all nodes. This includes InterNodal ESA, AUL, Hunt Groups, and MADN.

Two attributes are provisioned for each Termination- if the line is preemptable, and its precedence.

The Element Manager receives this data from the Core in the form of an XML document, transferred using secure mechanisms. This data is not modified by the Element Manager, but is converted into a form for the MG9000. No editing of this data is done by the MG9000. However, these values are displayed at the appropriate views.

52.3 Hardware Requirements or Dependencies

None

52.4 Software Requirements or Dependencies

This ESA activity on the MG9K is dependent upon two additional activities for successful completion and will be integrated together under an ICAF:

Core -ESA MLPP (A00009119)

MLPP ESA on MG9K (A00009497)

ESA MLPP - ICAF (A00009423)

52.5 Limitations and restrictions

- The ESA data from the core will be autonomously downloaded to the MG9000 only once every 24 hours.
- ESA data can be manually downloaded from the core and sent to individual VMGs.
- MLPP is activated on the MG9K by the presence of precedence dialing for a termination. This can only be activated from a DSN switch provisioning precedence and preemption information per line on the MG9K.
- The MG9000 EM will not allow the modification of any ESA data retrieved from the core.
- Data and views relating to MLPP data will not be visible in non-MLPP offices.

52.6 Interactions

None

52.7 Glossary

Term	Description
ATM	Asynchronous Transfer Mode
DSN	Defense Switched Network
EM	Element Manager (MG9K)
ESA	Emergency Stand Alone
ITP	Integrated Telephony Processor
MEGACO	Media Gateway Control
MG9K	Media Gateway 9000
MLPP	Multiple Level Precedence and Preemption
POTS	Plain Old Telephone Service
SIP	Session Initiation Protocol
TID	Terminal Identifier
VMG	Virtual Media Gateway

53: Functional description (FN): A00009289

53.1 Feature name and Feature ID

A00009289 - IEMS (Integrated Element Management System) - 10 Minute Default on User Inactivity Timer

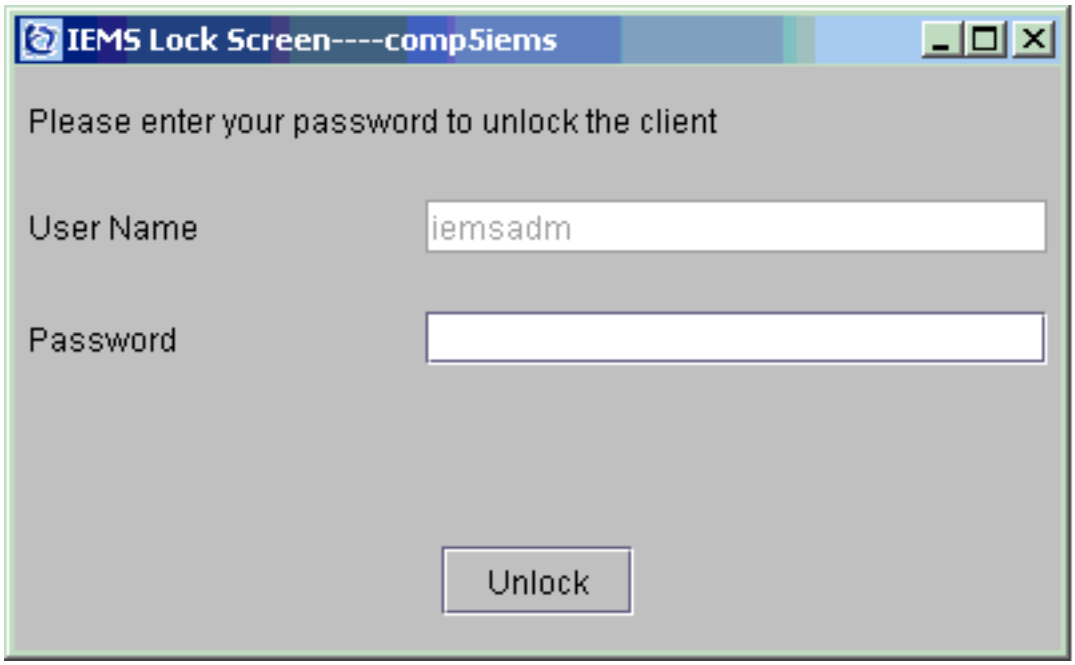
53.2 Description

In SN07, IEMS introduced a client inactivity timer that locked the client after a configurable period of time. Inactivity is defined as a lack of mouse actions - whether it be clicks or movements - on the IEMS screen. The inactivity timer functionality then locked the client until the user correctly entered his or her password. This basic security mechanism did not fully meet the customer requirements for security, so this feature further refines the existing IEMS client timeout to further meet those requirements.

With this feature, in addition to the existing locking of the IEMS client, the lockout timer will include the following:

- ability to change timeout value without requiring a restart of the server
- successive failed attempt lockout functionality to prevent multiple, rapid attempts to guess a password and unlock the client
- ability for the user to disable the client lockout will be removed

The new lock screen will look similar to the previous lock screen, without the option to disable it.



For more information on how to configure the timeout values, see the FN for A00008858 (http://ptm -> Documentation -> SN09).

When the user fails in 3 successive login attempts, they will be presented with a dialog box informing them that they will be unable to attempt to relogin again for a configured amount of time and the unlock button on the above window will be disabled. (Screen capture to be provided prior to IT declaration.)

The other additional functionality added this release is session termination after a specified inactivity timeout. The user will first see the GUI lock and then, if no action is taken before the user termination timer expires, the session will be terminated. This is consistent with other SSPFS based applications such as CMT and MG9KEM.

53.3 Hardware Requirements or Dependencies

No new hardware requirements or dependencies.

53.4 Software Requirements or Dependencies

This will require an SN09 or later version of SSPFS.

53.5 Limitations and restrictions

The IEMS HTML client will not timeout in this release. It will be supported in future IEMS releases.

53.6 Interactions

N/A.

53.7 Glossary

Term	Description
IEMS	Integrated Element Management System

54: Functional description (FN): A00009292

54.1 Feature name and Feature ID

IEMS: UserID-based Partitioning by NE, A00009292.

54.2 Configuring rules using the Custom View Scope

Using the Custom View Scope, rules can be set such that the view can be customized as per the customer's requirement. Rules can be set at various levels which allow filtering at different levels.

The partitioning rules that can be set on user groups such that a user belonging to a particular user group has a set of predefined access as governed by the rules. Note that Custom View Scopes cannot be added to the standard Carrier Voice over IP user groups.

The IEMS has 5 modules under which rules can be set. They are

1. Topology
2. Events
3. Alerts
4. Inventory
5. Stats Admin

Among these modules, Topology and Inventory modules are almost similar and rules set on any one of them is reflected to the user.

- Configuring Rules using the Topology / Inventory module
- Configuring Rules using the Event module
- Configuring Rules using the Alert module
- Configuring Rules using the Stats Admin module

Note: The terminology used for Maps is "**Topology**" and for Network Database is "**Inventory**".

54.3 Configuring Rules using the Topology / Inventory module

Integrated EMS administrator can add the authorized custom view scope to non-Carrier Voice over IP group using the Topology / Inventory module. This section describes Integrated EMS Security and Administration procedure to add the authorized custom view scope to a group using the Topology / Inventory module

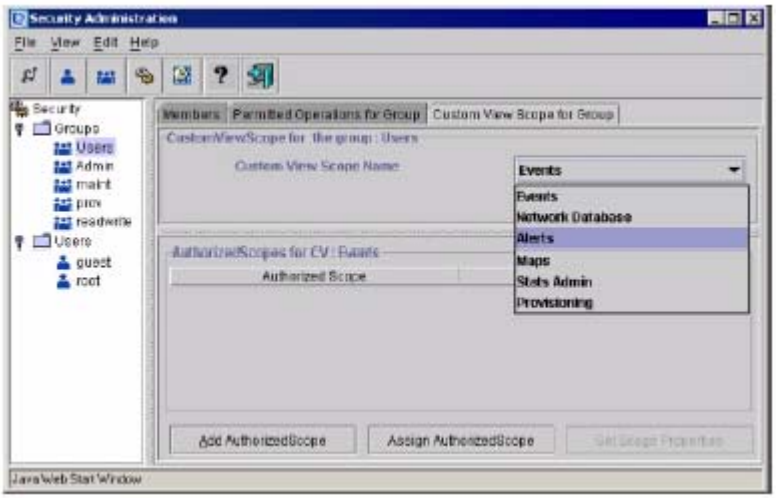
To add an authorized custom view scope to the group using the Topology/ Inventory module, follow these steps:

In the Security Administration tool of Integrated EMS

1 Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

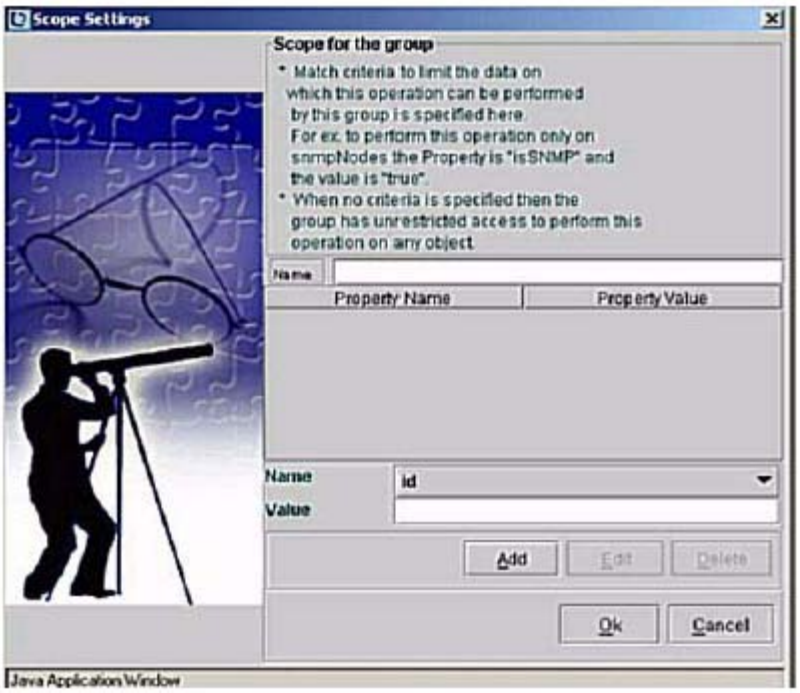
2 Select the required group under the Groups node in the Security tree.

3 Click the **Custom View Scope for Group** tab in the right-hand panel. The "Custom View Scope for the groups" window opens, as shown in the following figure.



4 Select the Topology / Inventory custom view scope name from the drop-down menu.

5 Click the **Add AuthorizedScope** button. The Scope Settings dialog opens, as shown in the following figure.



6 Specify a name for the created custom view in the **Name** text field. Then select a “Property Name” from *Name* drop-down box. This drop-down box lists the property names (which can be used for creating the authorized scopes) specific to each of the custom view scopes. The property names and the values for Topology/Inventory currently used in Integrated EMS are listed in the table below. List of all property names that can be use for partitioning, see Properties used in IEMS for CVS

Property Name	Property Value
DisplayName	Name assigned to the device added to IEMS Example (GWC*, CO*, MG*, etc)
Ipaddress	IP address of the devices added to IEMS Example (47.142.106.220, 47.142.*.* for particular subnet etc)
EmIpaddress	IP address of the Element Manager added to IEMS Example (47.142.122.200, 47.142.*.* for particular subnet etc)
Managed	True, False

Status	1(i.e., Critical), 2(i.e., Major), 3(i.e., Minor), 4(i.e., Warning), 5(i.e., Clear), 6(i.e., Info), 7(i.e., Unknown)
DeviceVersion	Version of the devices added to IEMS Example (7.0, 8.0, 9.0)

7 Click the **Add** button to add the Authorized Scope for the selected Custom View Scope of the group.

8 Click the **OK** button to update the scope details in the Integrated EMS Server.

Note: To identify more than one property value, separate each value using the appropriate operators (refer to the "Setting custom view scope properties"). Example: !GWC* -> This will show all the NEs except starting name with GWC

Note: The multiple criteria can be form by using the composite CVS rule. Example: Partitioning based on the set of Display Names and belonging to one subnet, this can be achieved by setting two rules in same module.

displayName as GWC*

IPaddress as 47.1.*.*

54.4 Configuring Rules using the Event module

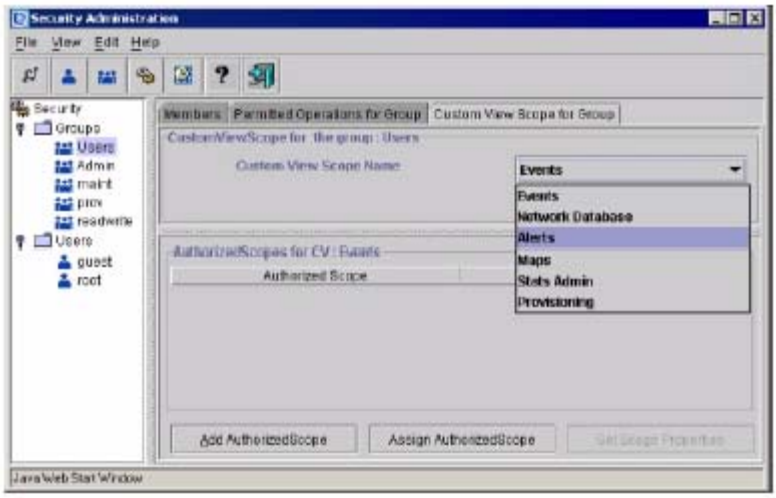
Integrated EMS administrator can add the authorized custom view scope to non-Carrier Voice over IP group using the Event. This section describes Integrated EMS Security and Administration procedure to add the authorized custom view scope to a group using the Event module

To add an authorized custom view scope to the group using the Event, follow these steps:

In the Security Administration tool of Integrated EMS

1. Launch the Security Administration tool (refer to the “Starting the Security Administration tool”).
2. Select the required group under the Groups node in the Security tree.
3. Click the **Custom View Scope for Group** tab in the right-hand panel.

The “Custom View Scope for the groups” window opens, as shown in the following figure.



4. Select the Event custom view scope name from the drop-down menu.
5. Click the **Add AuthorizedScope** button. The Scope Settings dialog opens, as shown in the following figure.

6. Specify a name for the created custom view in the **Name** text field. Then select a “Property Name” from *Name* drop-down box. This drop-down box lists the property names (which can be used for creating the authorized scopes) specific to each of the custom view scopes. The property names currently used in Integrated EMS and the values it can take are listed in the table below. List of all property names that can be use for partitioning, see Properties used in IEMS for CVS

Property Name	Property Value
Category	Category of Events Example (communication, processingError, qualityOfService, equipment, others etc)
LogName	Generated log name Example (IEMS, EMJS, PP etc)
LogNumber	Generated log number Example (398, 640, 641 etc)
LogKey	Combination of both LogName and LogNumber Example (IEMS398, EMJS640, PP318 etc)
EventType	Type of event Example (TBL, INFO, FLT etc)
ComponentId	Example (SAM21, STORM etc)
ProbableCause	Cause of event Example (communicationSubsystemFailure, underlyingResourceUnavailable etc)
EquipmentIdentifier	Identifier of devices added to IEMS Example (IpAddress of NE/EM etc)
EventLabel	Label on Event Example (Alarm set, IEMS OM collection job alarm etc)
Severity	1(i.e., Critical), 2(i.e., Major), 3(i.e., Minor), 4(i.e., Warning), 5(i.e., Clear), 6(i.e., Info), 7(i.e., Unknown)

7. Click the **Add** button to add the Authorized Scope for the selected Custom View Scope of the group.
8. Click the **OK** button to update the scope details in the Integrated EMS Server.

Note: To identify more than one property value, separate each value using the appropriate operators (refer to the "Setting custom view scope properties"). Example: IEMS* -> This will show all the Events starting with IEMS as a LogKey property .

54.5 Configuring Rules using the Alert module

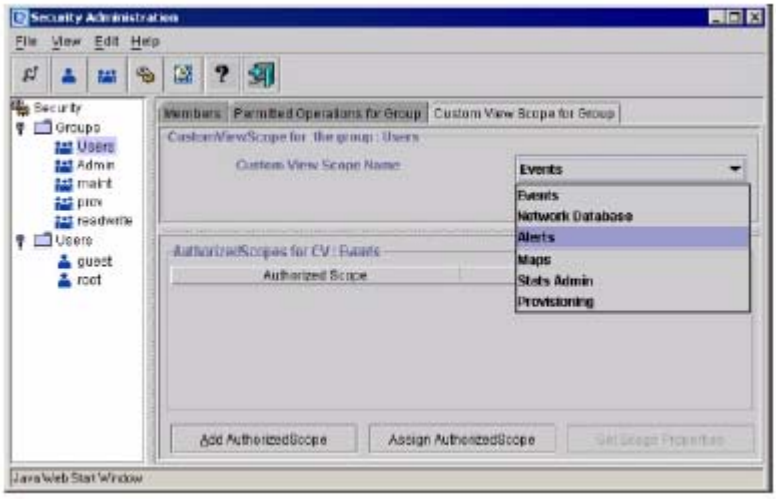
Integrated EMS administrator can add the authorized custom view scope to non-Carrier Voice over IP group using the Alert. This section describes Integrated EMS Security and Administration procedure to add the authorized custom view scope to a group using the Alert module

To add an authorized custom view scope to the group using the Alert, follow these steps:

In the Security Administration tool of Integrated EMS

1. Launch the Security Administration tool (refer to the "Starting the Security Administration tool").
2. Select the required group under the Groups node in the Security tree.
3. Click the **Custom View Scope for Group** tab in the right-hand panel.

The "Custom View Scope for the groups" window opens, as shown in the following figure.



4. Select the Alert custom view scope name from the drop-down menu.
5. Click the **Add AuthorizedScope** button. The Scope Settings dialog opens, as shown in the following figure.

6. Specify a name for the created custom view in the **Name** text field. Then select a “Property Name” from *Name* drop-down box. This drop-down box lists the property names (which can be used for creating the authorized scopes) specific to each of the custom view scopes. The property names currently used in Integrated EMS and the values it can take are listed in the table below. List of all property names that can be use for partitioning, see Properties used in IEMS for CVS

Property Name	Property Value
Category	Category of Events Example (communication, processingError, others etc)
EquipmentIdentifier	Identifier of devices added to IEMS Example (IpAddress of NE/EM, Display name of NE/EM etc)
LogKey	Combination of both LogName and LogNumber Example (IEMS398, EMJS640, PP318 etc)
ProbableCause	Cause of event Example (communicationSubsystemFailure, underlyingResourceUnavailable etc)
Severity	1(i.e., Critical), 2(i.e., Major), 3(i.e., Minor), 4(i.e., Warning), 6(i.e., Info), 7(i.e., Unknown)

7. Click the **Add** button to add the Authorized Scope for the selected Custom View Scope of the group.
8. Click the **OK** button to update the scope details in the Integrated EMS Server.

Note: To identify more than one property value, separate each value using the appropriate operators (refer to the "Setting custom view scope properties"). Example: IEMS* -> This will show all the Alerts starting with IEMS as a LogKey property

54.6 Configuring Rules using the Stats Admin module

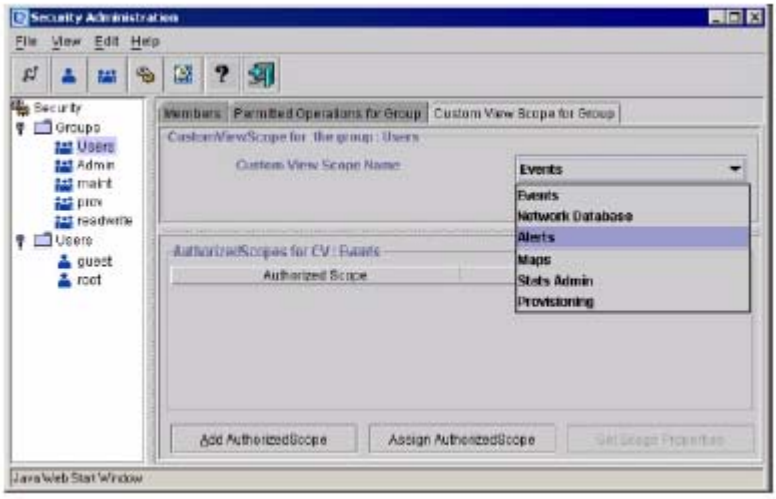
Integrated EMS administrator can add the authorized custom view scope to non-Carrier Voice over IP group using the Stats Admin. This section describes Integrated EMS Security and Administration procedure to add the authorized custom view scope to a group using the Stats Admin module. Stats Admin module is basically for partitioning the Performance Collection Data using supported properties.

To add an authorized custom view scope to the group using the Stats Admin, follow these steps:

In the Security Administration tool of Integrated EMS

1. Launch the Security Administration tool (refer to the “Starting the Security Administration tool”).
2. Select the required group under the Groups node in the Security tree.
3. Click the **Custom View Scope for Group** tab in the right-hand panel.

The “Custom View Scope for the groups” window opens, as shown in the following figure.



4. Select the Stats Admin custom view scope name from the drop-down menu.
5. Click the **Add AuthorizedScope** button. The Scope Settings dialog opens, as shown in the following figure.

6. Specify a name for the created custom view in the **Name** text field. Then select a “Property Name” from *Name* drop-down box. This drop-down box lists the property names (which can be used for creating the authorized scopes) specific to each of the custom view scopes. The property names currently used in Integrated EMS and the values it can take are listed in the table below. List of all property names that can be use for partitioning, see Properties used in IEMS for CVS

Property Name	Property Value
Name	Name of Job Example (CollectionJob*)
Agent	Name of component for which Collection is enable Example (GWC*)
DNSName	Name of DNS used (can use IP address also) Example (47.166.56.10)

ID	Poll ID Example (1, 2, 100 or 243 etc)
Protocol	Used Protocol Example (SNMP etc)
NumericType	1 for numbers and 2 for string
OID	Identifier for Object that is Data Identifier Example (.1.3.6.1.2.1.1.1.0)
Threshold	The value is set to true if the threshold value is set for the collection data and false if threshold value is not set
IsMultiplePolledData	True, False

7. Click the **Add** button to add the Authorized Scope for the selected Custom View Scope of the group.
8. Click the **OK** button to update the scope details in the Integrated EMS Server.

Note: To identify more than one property value, separate each value using the appropriate operators (refer to the "Setting custom view scope properties"). Example: !GWC* -> This will show all the Agent's Collection except starting name with GWC

54.6.1 Properties used in IEMS for CVS

All the property names currently used in Integrated EMS and the respective modules are listed in the table below.

Modules	Property Name
Topology	name, displayName, managed, status, isContainer, ipAddress, primaryIpAddress, secondaryIpAddress, timeZone, deviceVersion, FIState, SystemUnmanageState, platformAddress
Events	id, text, category, severity, time, source, node, logName, logNumber, logKey, sequenceNumber, eventType, componentId, probableCause, specificProblem, equipmentIdentifier

Alerts	entity, id, message, category, severity, modTime, createTime, who, source, logName, logKey, sequenceNumber, eventLabel, eventType, componentId, probableCause, specificProblem, equipmentIdentifier
Inventory	name, displayName, managed, status, isContainer, ipAddress, primaryIpAddress, secondaryIpAddress, timeZone, deviceVersion, FIState, SystemUnmanageState, platformAddress
Stats Admin	name, id, agent, oid, threshold, isMultiplePolledData, numericType, previouslySeverity, statsDataTableName, protocol, dnsName, lastTimeValue

55: Functional description (FN): A00009294

55.1 Feature name and Feature ID

T.38 Annex D interworking with SIP. It is covered activity ID A00009294.

55.2 Description

55.2.1 Overview

ITU-T Recommendation T.38 [T.38] describes the technical features necessary to transfer facsimile documents in real-time between two standard Group 3 facsimile terminals over the Internet or other networks using IP protocols. The Recommendation allows the use of either TCP or UDP depending on the service environment.

The annex D/T.38 describes system level requirements and procedures for Internet-aware facsimile implementations and Internet-aware facsimile gateways conforming to ITU-T Rec. T.38 to establish calls with other ITU-T T.38 implementations using the procedures defined in RFC 2543 (SIP) and RFC 2327 (SDP).

This activity intends to provide T.38 Annex D interworking support for SIP with a PVG on H.248.

This feature provides “Call Server controlled switch over to T.38” depending on T.38 network option:

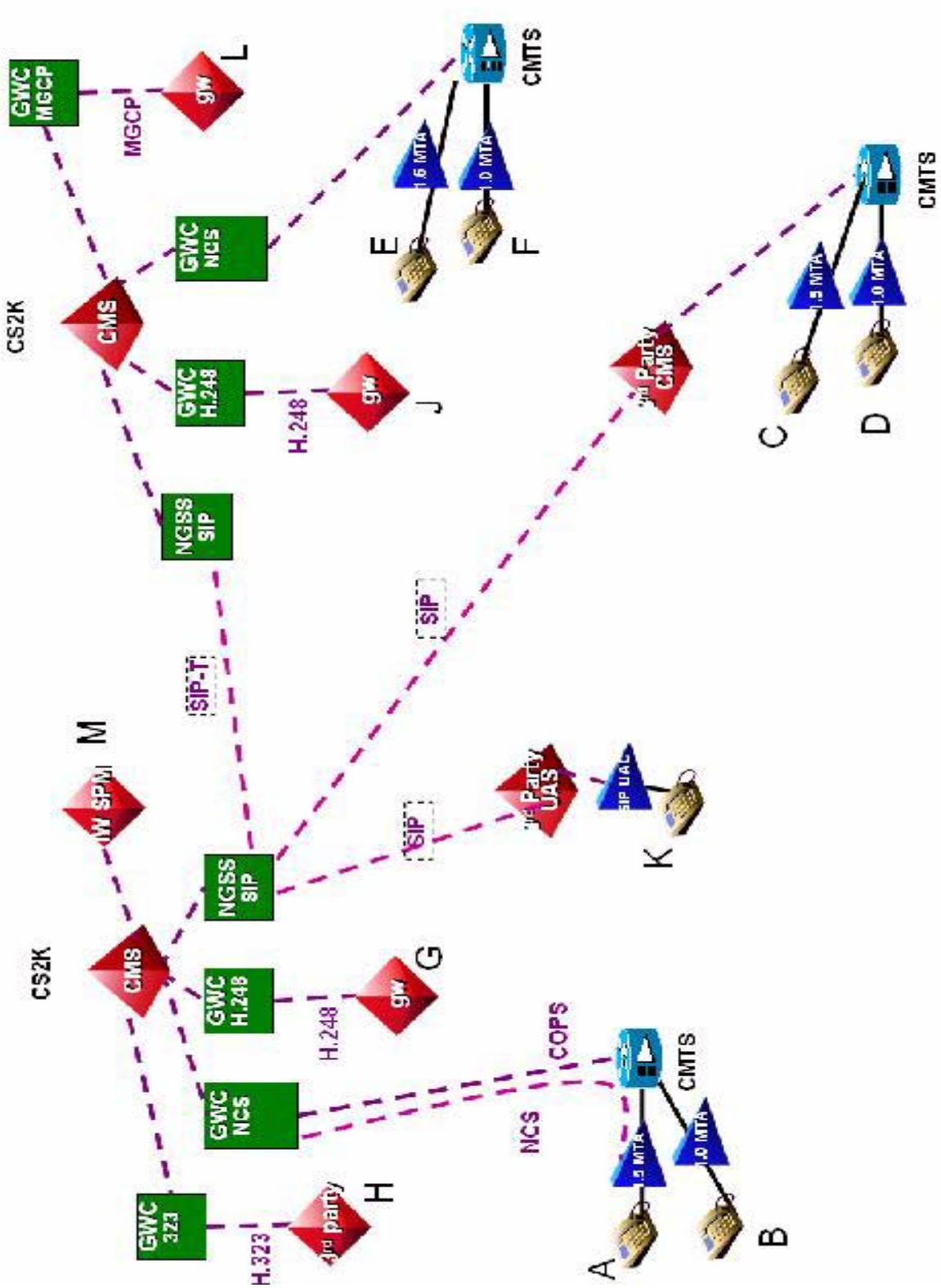
If in the Gateway controller configuration, **T.38 is enabled in the network codec profile provisioning** and H.248 GW supports T.38, then upon fax detection, switch over is done from G.729 (or G.711) to T.38 codec.

And if in the Gateway controller configuration, **T.38 is disabled in the network codec profile provisioning**, or the H.248 GW does not support T.38, then switch over to T.38 does not apply.

This activity is in parallel to the SN09 activity A00009443 which includes development on the DPT/GWC.

This feature does not impact the capability of a GW to do autonomous switch over to T.38.

55.2.2 Overall T.38 interop scenario



In SN07, T.38 is supported as follows:

- H.323 to/from H.248 PVG (G-H, G-J scenarios)
- PVG to/from MGCP IAD (G-L)
- PVG to/from IW SPM (J-M)
- IW SPM to/from MGCP IAD (M-L)
- AudioCodes M2K to/from IW SPM/MGCP IAD/ PVG

With this activity we are supporting a T.38 Interworking with 3rd Party SIP servers.

This is the G-K or J-K (CS2Ks in TANDEM) scenarios referring to the diagram above.

55.2.3 Communication between gateways

55.2.3.1 Call setup

Call setup for Annex D/T.38 compliant implementations is based on SIP (Session Initiation Protocol) defined in RFC 2543. The implementations may operate in two distinct compatible environments:

55.2.3.1.1 A facsimile-only over IP environment

The emitting gateway sends a SIP INVITE request (with the appropriate options set) for a T.38 facsimile connection with the receiving SIP server. The receiving server will likely be the receiving gateway; however, it may also proxy or redirect the SIP connection to the actual gateway through SIP or other means. In any case, a response will be sent to the emitting gateway indicating acceptance, redirection or failure of the request.

If accepted (or a redirected INVITE is accepted), the T.38 facsimile call proceeds. Once the call is completed, the call may be disconnected with a SIP BYE command.

55.2.3.1.2 A facsimile and voice over IP environment

A SIP INVITE is made to the called party requesting a voice connection per the requirements of RFC 2543. A voice connection is then established.

Upon detection of facsimile by the receiving gateway, a SIP INVITE request is sent to the emitting gateway (with the same Call-ID as the existing voice connection) for a T.38 facsimile connection. Upon completion of the facsimile

call establishment (noted in D.2.2.3), the T.38 facsimile call proceeds with a T.38 V.21 flags indicator packet.

Note that during this switch over and the facsimile call, it may be useful to mute the voice channel. The voice channel may be used again once the end of facsimile transmission is detected. Alternately, some implementations may choose to replace the voice channel with a facsimile channel.

This activity implements the facsimile and voice over IP environment where the voice call is first set-up and then a switch over to T.38 is triggered.

55.2.3.2 Basic call setup

Implementation of “Call Server controlled switch over to T.38 mode”, makes use of “Call Type Discriminator package” (ctyp) with event “Discriminating Tone detected” (dtone).

The GWC checks the GW capability to support T.38 via H.248 AuditValue command. If in the responded list of the packages of the H.248 GW, “ctyp-1” is present, then “Call Server controlled switch over to T.38 mode” is supported - see Figure 1, on page 452 .

If T.38 is enabled in the Network codec profile provisioning in Network Configuration, the H.248 GWC add the ephemeral termination with voice and T.38 codec - see Figure 4, on page 453 .

The H.248 SDP samples below display H.248 message as used in the call flow examples. See “Example Call Flows” on page 455.

Figure 1 Check supported H.248 packages

Transaction (GWC -> MG)	Reply (GWC <- MG)

MEGACO/1 [47.174.66.80]:2944
Transaction=62 {
Context=-{
AuditValue=Root{
Audit {Packages}
}}}
	MEGACO/1 [47.166.34.20]:2944
	Reply=62 {
	Context=-{
	AuditValue=Root{
	Audit {Packages {.., ctyp-1, ..}}
	}}}

Figure 2 Request fax event detection

Transaction (GWC -> MG)	Reply (GWC <- MG)

MEGACO/1 [47.174.66.80]:2944
Transaction=63 {
Context=$ {
Add=e1/03/05/1 {
M{O{MO=RC, tdmc/ec=ON }},
Events = 234 {ctyp/dtone}
}}}
	MEGACO/1 [47.166.34.20]:2944
	Reply=63 {
	Context= 1234{
	Add=e1/03/05/1
	}}

Figure 3 Notify fax event V.21 flag

Transaction (GWC <-MG)	Reply (GWC -> MG)

MEGACO/1 [47.166.34.20]:2944
Transaction=64 {
Context=1234 {
Notify=e1/03/05/1 {
ObservedEvents=234 {
20030924T14001201:ctyp/dtone{dtt=V21flag}
}}}}
	MEGACO/1 [47.174.66.80]:2944
	Reply=64{
	Context= 1234{
	Notify=e1/03/05/1
	}}

Figure 4 Add ephemeral with G.729 and T.38 codec”

Transaction (GWC ->MG)	Reply (GWC <- MG)

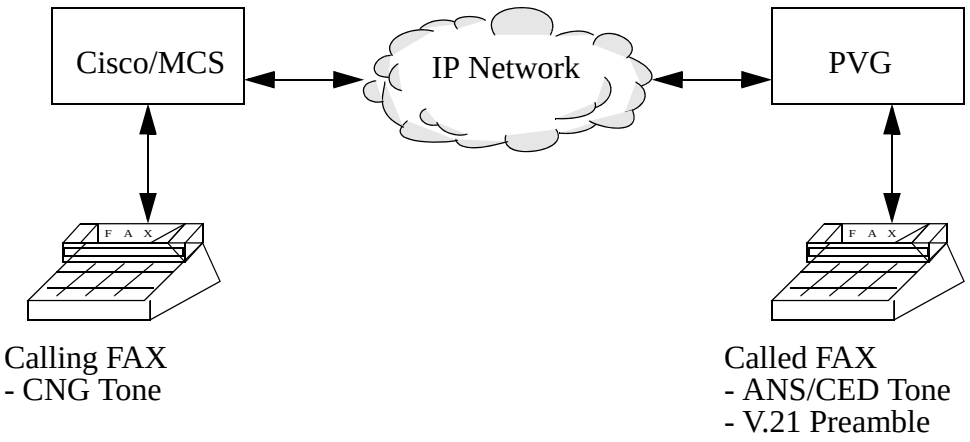
MEGACO/1 [47.166.34.20]:2944
Transaction=64 {
Context=1234 {
Add = $ {
Media {LocalControl {
v=0
c=IN IP4 $
m=audio$ RTP/AVP 18
a=ptime:20
m=image $ udptl t38
...
}}}}}
	MEGACO/1 [47.174.66.80]:2944
	Reply=64{
	Context= 1234{
	Add = rtp/34 {
	Media {Local {
	v=0
	c=IN IP4 47.174.66.14
	m=audio 1111 RTP/AVP 18 13 19
	a=ptime:20
	m=image 2222 udptl t38
	a=T38Fax ...
	a=T38Fax...
	...
	}}}}}

55.2.4 This activity accommodates two scenarios:

Assuming that there are no NACKs from either side of the connection, there are two possible scenarios: when the call is initiated form either end.

55.2.4.1 T.38 fax calls originating from SIP/NGSS and terminating at PVG.

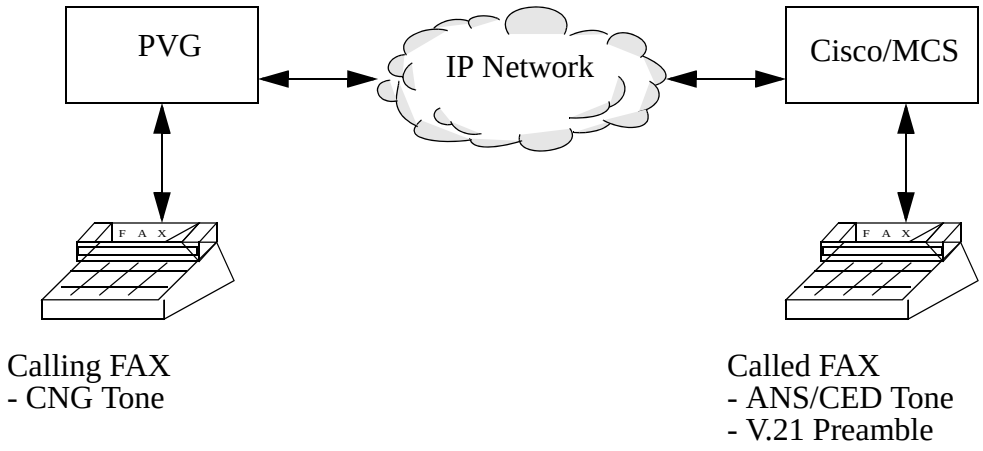
Figure 5



- A SIP Invite is sent to the CS2K by the CISCO/MCS requesting a voice connection.
- A voice connection is then established.
- Upon detection of fax tone by the receiving gateway i.e. the PVG, it sends a V.21notification to CS2K.
- CS2K then sends a SIP Re-Invite request to the emitting gateway (with the same Call-ID as the already existing voice connection) for a T.38 facsimile connection.
- Upon completion of the facsimile call establishment, the T.38 fax call proceeds with a T.38 V.21 flags indicator packet.

55.2.4.2 T.38 fax calls originating from PVG and terminating at SIP/ NGSS.

Figure 6



- For calls originating from the PVG end, a SIP Invite is sent to the CISCO/ MCS requesting for a voice connection.
- Then a voice connection is established.
- A V.21 notification is received by the CISCO/MCS.
- It sends a re-invite to the originating side (which is the PVG here). Then the switch-over to T.38 occurs.

55.2.5 Example Call Flows

Description of T.38 Annex D functionality is provided via call flows. The description of the first call flow is given in detail and may be applied to other subsequent call flows.

55.2.5.1 Basic Call Scenario: SIP to PVG interworking.

When the call is originated from the CISCO/MTS SIP endpoint:

Note 1: After receiving an INVITE from the SIP endpoint, a voice call is established. If in the Gateway controller configuration, T.38 is enabled in the network codec profile provisioning the ephemeral is added, and the PVG is asked to choose from m = audio $$$ m = image $$$..

Note 2: H248 GWC requests for all events on the ctyp/dtone package.

Note 3: The PVG replies with the intersection of the PVG capability and the offer from SIP, which is sent to the remote SIP end point. At this point voice call is established.

Note 4: The PVG then reports any detected ctyp/dtone event to the GWC.

Note 5: Upon detection of a CNG or a V.21 flag the GWC will send a modify to the PVG with the local descriptor m=image $ udptl t38.

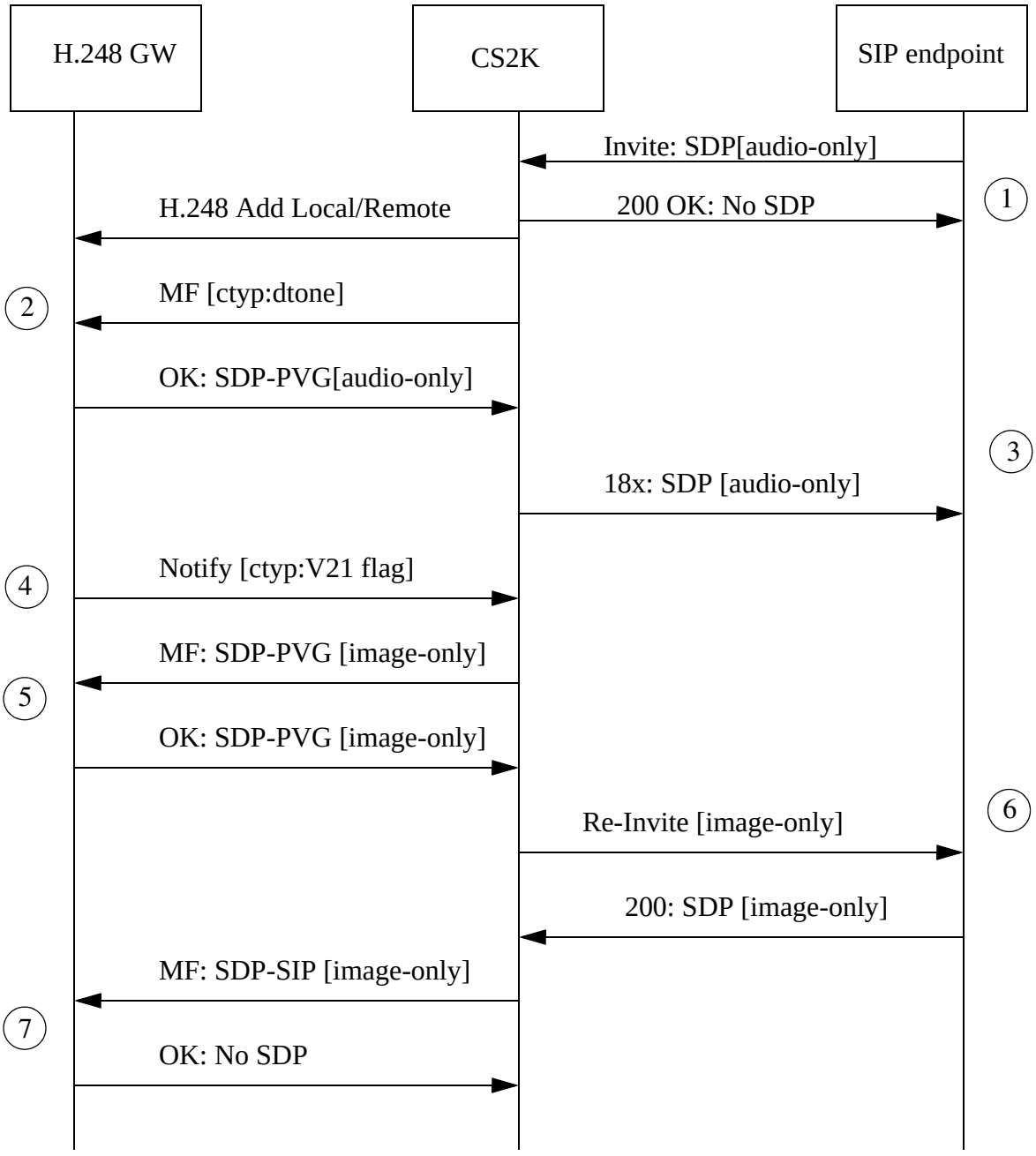
Note 6: CS2K sends image only SDP to the remote SIP end point in Re-INVITE message.

Note 7: Upon receipt of SDP(T.38) from remote SIP end point, CS2K sends an usual modify. At this point a fax call using T.38 is established.

Note 8: The content of SDP uses following abbreviation:

- SDP(audio) for processing of audio media stream.
- SDP(t38) for processing of t38 media stream.
- SDP(audio, t38) for simultaneous processing of audio and t38 media streams.
- SDP(audio, t38-cap) for processing of audio media stream and for t38 capability indication.

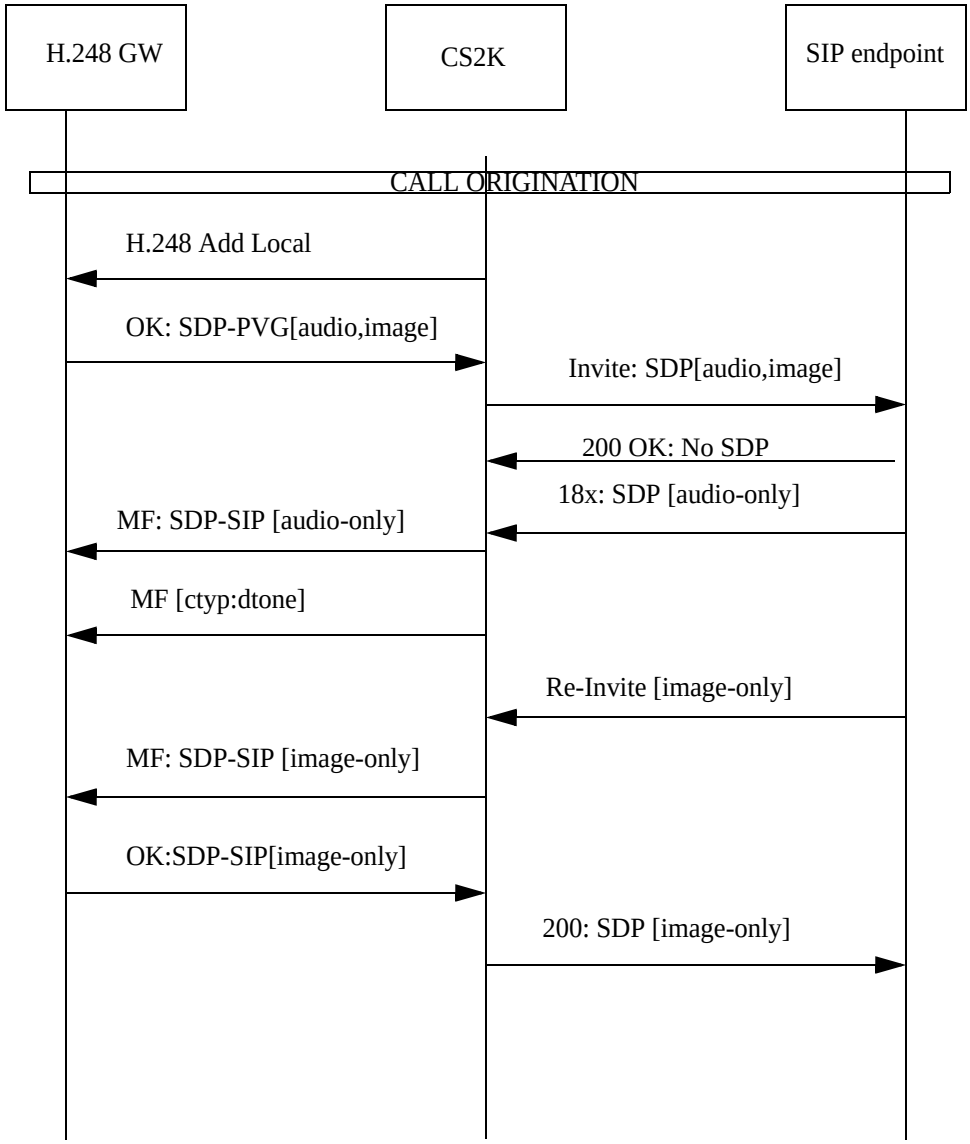
Figure 7 T.38 Calls originating from CISCO/MTS and terminating at PVG on CS2K



55.2.5.2 Basic Call Scenario: PVG to SIP interworking.

When a call is originating from PVG, a SIP INVITE is sent from CS2K to the SIP Endpoint which replies with its SDP. And a voice call is established successfully. After this a V.21 Fax notify is sent from the receiving gateway. This triggers a change in the codec from G.711 or G.729 to T.38 (If T.38 flag is set in netopts).

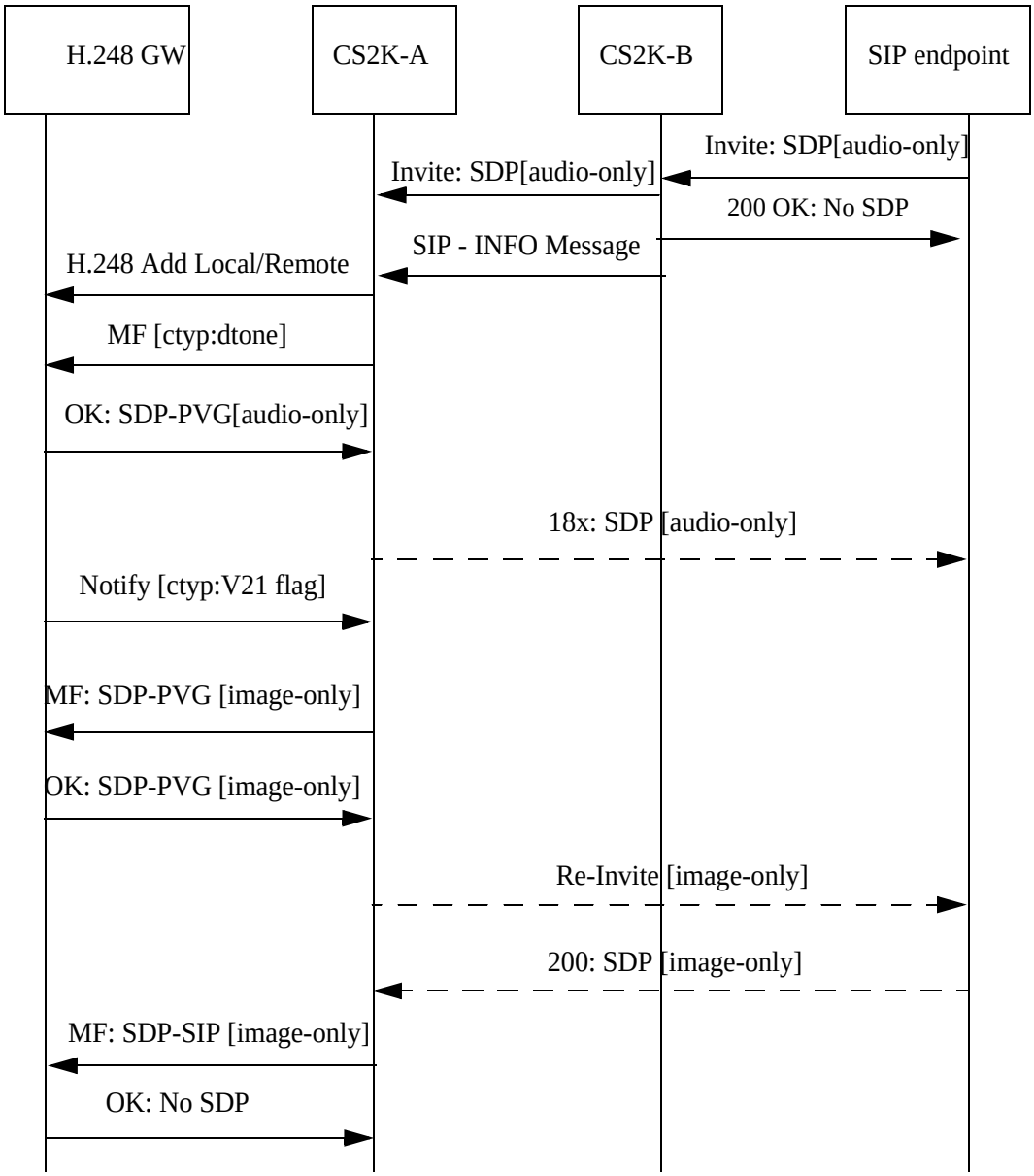
Figure 8 T.38 Calls originating from PVG on CS2K and terminating at CISCO/ MTS



55.2.5.3 Tandeming Support

SIP INFO message will be used when CS2Ks are in tandem to support T.38 Annex D interworking.In the figure below CS2K-B acts a TANDEM CS2K. If T.38 is provisioned on the NGSS of CS2K-B then it required to instruct CS2K-A to start scanning for fax tone from PVG. SIP INFO message will be used for this purpose.

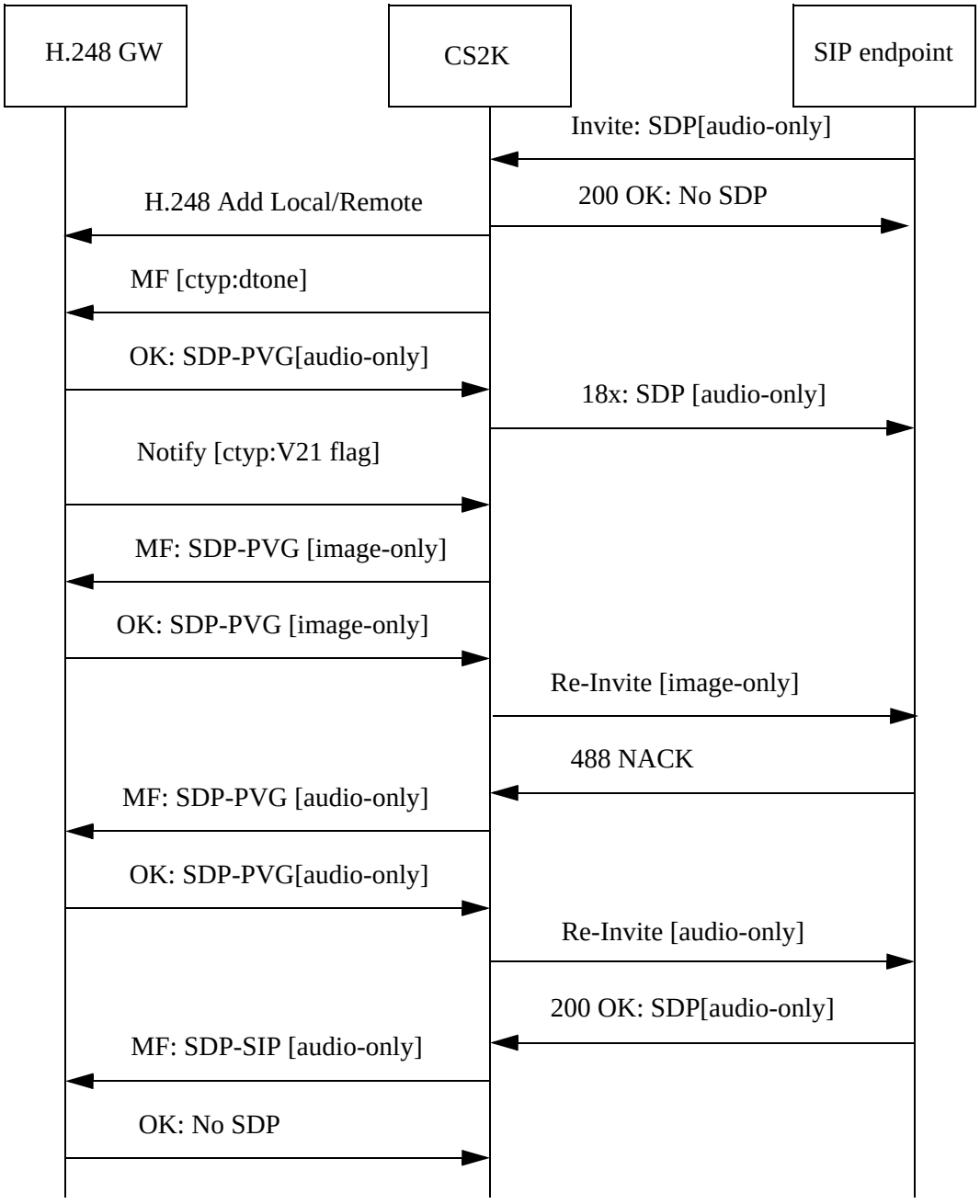
Figure 9 T.38 Fax calls spanning over more than one CS2K



55.2.5.4 Unsuccessful switch attempt

In a T.38 Fax call when the SIP Re-INVITE for the switch-over from voice to T.38 mode is NACKed, an attempt should be made to save the call by switching back the codec to voice. In such scenario, a SIP Re-INVITE is sent with voice only codec to switch the call back to voice.

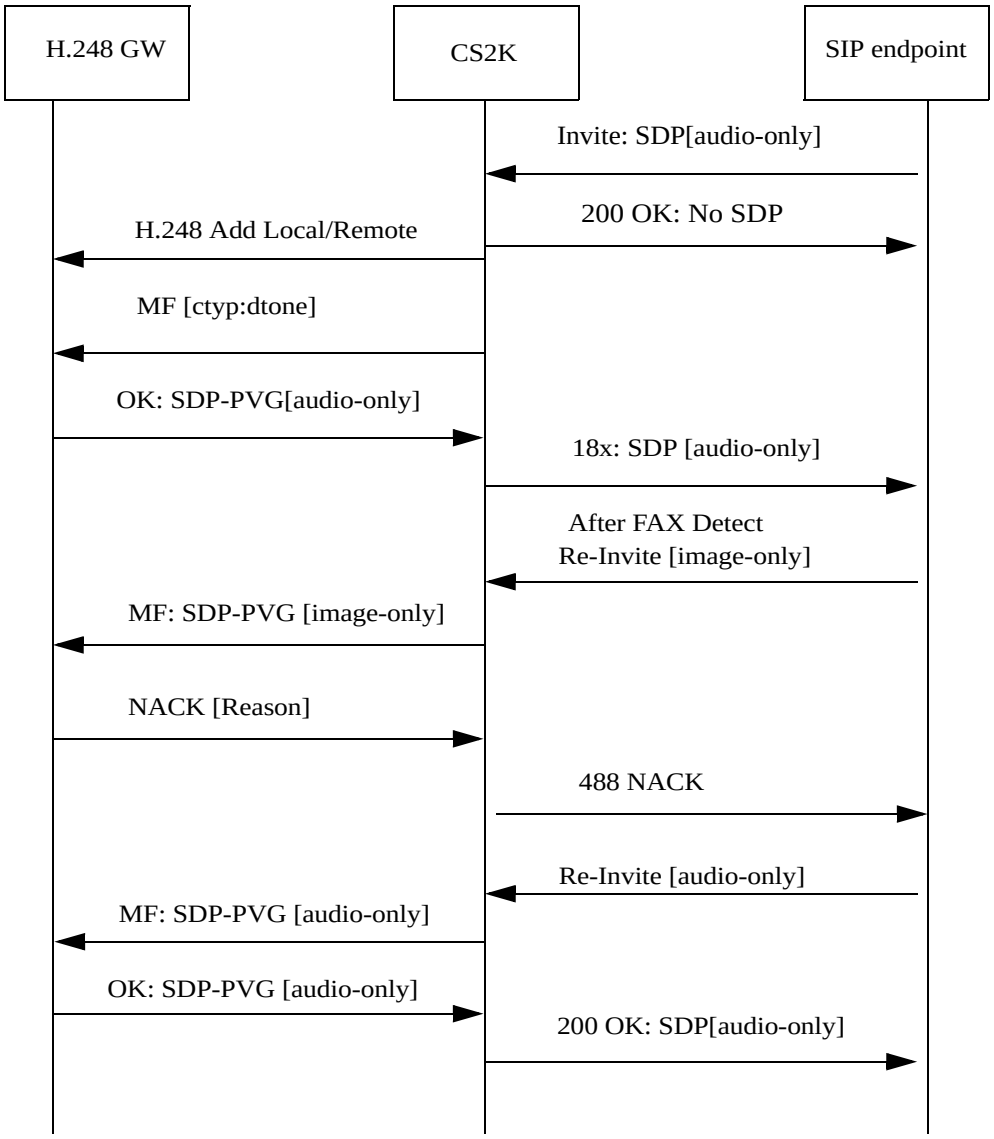
Figure 10 SIP endpoint rejects the Offer



55.2.5.5 Unsuccessful switch attempt

When the SIP Re-INVITE Fax offer for a switch to T.38 comes from the remote SIP side and the PVG NACKS it, the PVG sends the reason for the rejection to the SIP side which in turn sends a SIP Re-INVITE to change the SDPs to audio-only mode.

Figure 11 PVG Rejects Offer



55.3 Hardware Requirements or Dependencies

No New hardware is required.

55.4 Software Requirements or Dependencies

CM/GWC: SN09 load

H.248 GW: supporting H.248.1, H.248.2 ctyp package, T.38 mode.

T.38 should be provisioned both on the H.248 GW and remote SIP side.

55.5 Limitations and restrictions

- "Facsimile-only over IP environment" (T.38 Annex D.2.2.3) is out of scope for this feature. This feature addresses "Facsimile and voice over IP environment" (T.38 Annex D.2.2.4) in which first a voice call is established and then switch over to T.38 mode occurs.
- This feature verifies T.38 Annex D interworking for H.248 GW on one call leg and 3rd party SIP User Agent Server on other call leg. T.38 interworking with other GWs are out of scope for this feature and will not be tested in this feature.
- This feature uses the transport layer UDP/IP for T.38 packets (T.38 Annex D.2.3.2). Transport of T.38 packets via TCP/IP is not used by this feature.
- This feature is being tested only on H.248 PVG. Though it should work fine on H.248 supported gateways, we do not perform testing on other H.248 gateways such as M2K..

55.6 Interactions

Not Identified.

55.7 Glossary

Term	Description
CED	Called terminal identification answer tone of Fax device (2100 +/- 15 Hz, continuous tone, duration 2.6-4.0 sec.) see T.30 chapter 4.1
CM	Call Manager, Computing Modules
CNG	Calling tone of Fax device (1100 +/- 38 Hz, 0.5 sec. on, 3.0 sec. off, duration 60-120 sec.) see T.30 chapter 4.2.

Term	Description
CS2K	Call Server 2000
G3FE	Group 3 Facsimile Equipment G3FE refers to any entity which presents a communication interface conforming to ITU- T Recommendation T. 30, T. 4, and optionally T. 6. A G3FE may be a traditional G3 facsimile machine, an application with a T. 30 protocol engine or any other possibility mention in the network model for IP Facsimile mentioned in Recommendation T. 38.
GW	Gateway (Signalling Gateway and Media Gateway)
GWC	Gateway Controller
MCS	Multimedia Communication Server
PSTN	Public Switched Telephone Network.
PVG	Passport Packet Voice Gateway
RFC	Request For Comments (IETF)
RTP	Real-time Transport Protocol (IETF 1889, 3550)
SDP	Session Description Protocol (IETF RFC 3266)
SIP	Session Initiation Protocol (IETF RFC 3261)
UDP	User Datagram Protocol (IETF RFC 768)
UDPTL	Facsimile UDP Transport Layer protocol (ITU T.38)
V.21 Preamble	Series of flag sequences 01111110 for 1 sec +/- 15%.

56: Functional description (FN): A00009310

56.1 Feature name and Feature ID

SSPFS Restricted Access Shell - A00009310

56.2 Description

This feature's intention is to provide a hardened restricted shell for non-administrative CLUI functions on the SSPFS platform. It is expected that customers will use this environment when giving users access to CLUIs residing on SSPFS servers. The users will have a restricted command set and shell environment, unlike today whereas the user is given an unrestricted shell to run the CLUI utilities.

The restricted shell will use the Solaris resident rksh (restricted Korn shell). With a restricted Korn shell, the user cannot:

- Change the working directory.
- Set the value of SHELL, ENV, or PATH variables.
- Specify the pathname of a command with a '/' in it.
- Redirect output of a command with '>', '>|', '<>', or '>>'.

The only commands available to the user will be those in the PATH variable defined by the user's default .profile. The PATH variable will be made up of the restricted access shell bin directories. The default .profile will be contained in the restricted access shell skeleton directory (/etc/skel.rash).

The application CLUIs (i.e. npm, gwcadmin.sh) currently provide their own level of authentication via the existing login servlet when accessing the CLUI. Within the application, an additional level of command authorization may be used based on the group(s) of the CLUI user. This authorization/ authentication mechanism used by the application CLUIs is functionality that has been in use prior to SN09 and will not be changed by this new content.

At times, a restricted access shell user will need to perform system administrative tasks, which will require root (or other user) access. The restrcited access shell user will be required to 'su' to the new user. This feature provides an 'su' wrapper that verfies the user invoking su is a member of either emsadm or secadm group before gaining access to the Solaris resident 'su' command.

Creating Local Restricted Shell User Accounts

To obtain the functionality of this feature, specify the shell to be '/usr/bin/rash' and the skeleton directory to be./etc/skel.rash'. Restrcited access shell users

wil lhave their home directory created in /export/home/<user id>. If the user is to be created in the restricted shell environment using the Solaris 'useradd' command, specify the '-s' option for shell, '-d' option for home directory, and '-k' option for skeleton directory. The following is an example of creating restricted access user 'test6' using the Solaris useradd command:

useradd -gsuccssn -Gmgcadm,emsadm -s /usr/bin/rash -d /export/home/test6 -m -k /etc/skel.rash test6

From the example above, user id 'test6' will:

- Have a SHELL equal to restricted access shell (rash) which is ultimately rksh.
- Have a home directory at: /export/home/test6
- Home directory will contain the contents of /etc/skel.rash. This is where the user's .profile is obtained which will contain the limited PATH variable containing only restricted bin directories (i.e. /usr/rbin/basebin)..
- User's primary group is succssn.
- User's secondary groups are mgcadm and emsadm.

Creating Central Restricted Shell User Accounts

To grant restricted shell access to a central user account, the users's shell must be set to '/usr/bin/rash' and user's home directory to '/export/home/<usrname>'. If IEMS Security Server is used to manage the central user account, this is done by setting the user's login shell to 'restricted'.

The creation of user home directory /home/export/<usrname> and copying of user shell profile from skeleton directory /etc/skel.rash are automatically handled by a specialized PAM-MKHOMEDIR SPI.

Registering Restricted Access Shell Executables

Applications will use the Servman utility to register restricted access shell executables. Option '-rash' has been added to Servman which will handle creating the links and removing the links within servman.

To add single files, use the restricted access shell option as follows:

servman register -group newapp -*rash "fullpath;name"*

> ***Note:*** Where *name* is the symbolic link name in the restricted shell bin directory and *fullpath* is the path to the actual executable. Servman will create a symbolic link in the application restricted bin directory (i.e. /usr/rbin/appbin).

To add multiple files, us a similar command but delimit the entries with the ‘*’ character:

servman register -group oldapp -rash “fullpath1;name*fullpath2;name2”

Restricted Command Set

Much of what makes the restricted access shell restrictive is the limited command set. This command set will be split into base level commands and application level commands. Base level commands include Solaris resident commands and SSPFS delivered commands. Application commands includes commands installed after SSPFS, such as application CLUIs (i.e. gwcem, sam21em).

Table 1: Solaris and SSPFS Commands

Command	Comment/Usage
awk	pattern scanning
cat	concatenate and display files
cli	SSPFS command line interface, mainly for configuration changes.
cut	cut out selected fields of each line of a file
df	displays number of free disk blocks and files
grep	search a file for a pattern
iostat	report I/O statistics
ipcs	report inter-process communication facilities status
kill	terminate or signal processes
less	browse or page through a text file (
ls	list contents of directory
more	browse or page through a text file
netstat	show network status
ps	report process status

Table 1: Solaris and SSPFS Commands

Command	Comment/Usage
servquery	Query the status of SSPFS applications
sort	sort, merge, or sequence check text files
su	Wrapper that only allows users in group emsadm or secadm to access Solaris su.
top	provide system and process status
head	display first few lines of files
tail	display the last part of a file
vmstat	report virtual memory statistics

Table 2: Application (other) Commands

Command	Comment/Usage
npm	Network Path Manager CLUI
gwcad-min.sh	GatweWay Controller Element Manager CLUI
bpt	Bulk Provisioning Tool
sam21em	SAM21 Element Manager CLUI
?	SNMP Poller - executables needed not provided at this time.
?	OMPUSH - executables needed not provided at this time

Note: Currently, IEMS exposes the following commands to be executed on the SSPFS element in an unrestricted shell, logging in as root user via ssh: *servquery -status all, swact, servstart IEMS, init 6*. IEMS will continue to function in this manner for SN09 as the scope of this feature does not include changing existing “root only” commnads and having them execute in a restricted shell environemnt.

56.3 Hardware Requirements or Dependencies

Not applicable.

56.4 Software Requirements or Dependencies

Not applicable.

56.5 Limitations and restrictions

Not applicable.

56.6 Interactions

First interaction is the change to the shell environment users may get when they are given access to the SSPFS server to invoke maintenance CLUIs. Today, the user is granted an unrestricted shell to access the CLUIs, which gives the user access to other server resources which may not be the desired. This feature restricts the user's environment, limiting the server's exposure to only the user's home directory. In addition, the users PATH will also be limited to directories which contain a subset of available server executables.

56.7 Glossary

Term	Description
CLUI	Command Line User Interface
PAM	Pluggable Authentication Module
SSPFS	Succession Solution Platform Foundation Server

57: Functional description (FN): A00009311

57.1 Feature name and Feature ID

SSPFS Dark Office backup - A00009311

57.2 Description

There is a critical need to allow customers to re-write the image and data on to the DVD more than one time without ejecting the DVD tray as it currently is done today. This limits the number of times someone has to go to the central office every time when backing up data is required or to put a DVD into the DVD tray every time its blanked.

With this feature, full system backups are schedulable to both active and inactive units and can re-use the same physical media (DVD-RW only) to rewrite over them. Alarms are raised when backups fail. System image size is limited to 4 Gig. A backup image can be restored to a fresh installed machine. The original media is required for a restore. A restore will either leave the non backed-up filesystems intact or create them if they do not exist.

Figure 1 illustrates a typical backup scenerio of how this feature is used.

- User logs in either as a Super User or through the “Restricted Access Shell” feature in SN09 and be part of the “emsadm” group to have “su” access.
- User uses the SSPFS CLI (CLUI) to invoke the “Backup Configuration” settings menu and schedule a full system backup of the SSPFS box.
- On scheduled date and time, the bkfullsys backup command is called to backup the system and failures are reported northbound.

If the DVD disk is re-writable, no user intervention is required for this operation to happen and depending on what rules are defined for the DVD behavior, the DVD can be re-written over on the scheduled date and time automatically.

Three simple rules can be invoked through the “Backup Configuration” to define the backup behavior.

1 - When performing backup, eject DVD tray when done.

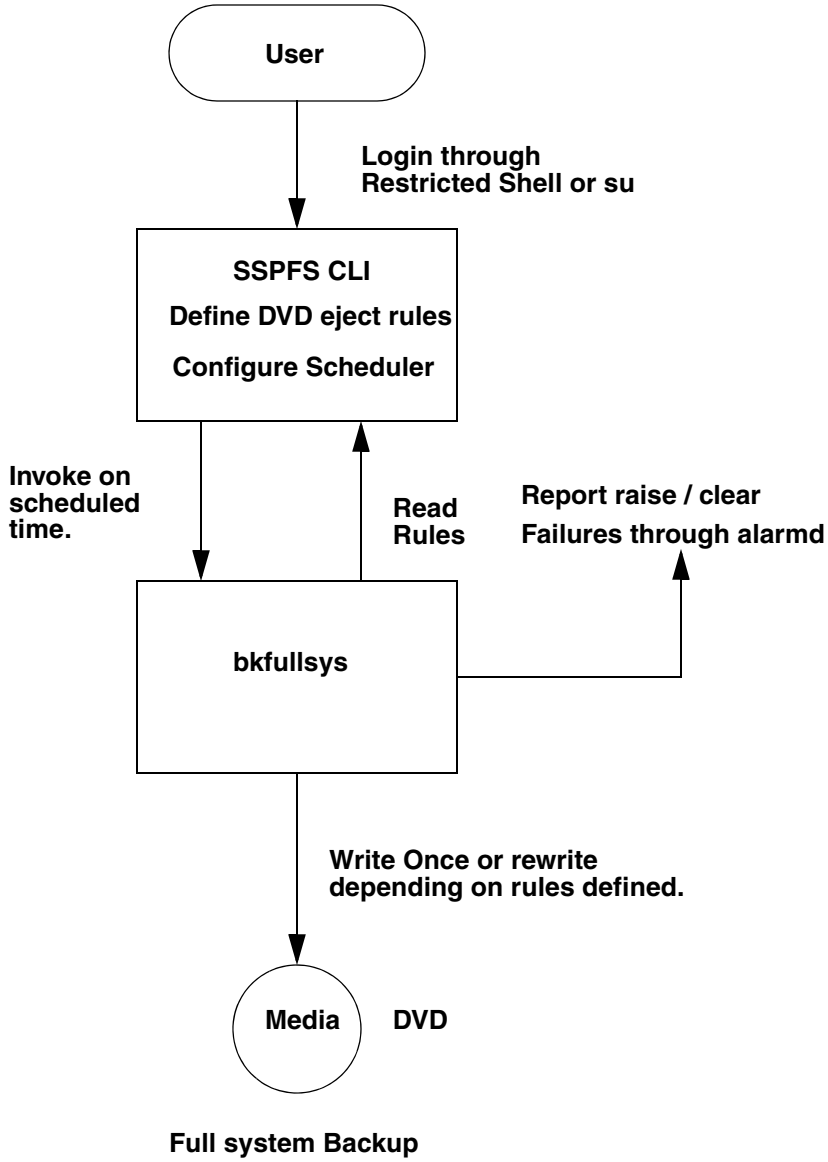
2 - When performing backup, do not eject DVD tray , subsequent backups will not overwrite previous data.

3 - When performing backup, do not eject DVD tray, subsequent backups will overwrite previous data.

The backup scripts (bkfullsys and bkdata) will also confirm to these rules if invoked manually, option 1 is default setting.

For backing up critical data which includes Oracle and critical application data, this feature provides you with an option that can be invoked through the "Backup Configuration" in SSPFS CLI called "***Copy last Oracle backup to DVD or tape".*** This option will copy the last good Oracle backup from the "Syncronized Backup Manager" and burn it to DVD or tape. The "Syncronized Backup Manager" has its own scheduler for backing up the critical data at scheduled intervals and writes to disk. This option does not do the backup itself, it simply copies what was written to disk by the "Syncronised Backup Manager".

Figure 1: Backup Flow Diagram



57.3 Hardware Requirements or Dependencies

Not applicable

57.4 Software Requirements or Dependencies

Not applicable

57.5 Limitations and restrictions

Backup and Restore time will dependent on the I/O speed to the target media whether it is hard drive, tape drive, or DVD / CD burner.

57.6 Interactions

This feature interacts with the SSPFS backup and restore scripts for doing a full system backup and backing up of oracle and critical data that are part of the" Backup and Restore Enhancements" feature in SN09 which is called at scheduled intervals by the "Syncronised Backup Manager" which was first introduced in SN08.

This feature also interacts with the "Restricted Access Shell" feature to be able to schedule backups in a restricted shell environment.

57.7 Glossary

Term	Description
New term	Definition
CLUI	Command Line User Interface
SSPFS	Succession Solution Platform Foundation Server
CLI	Command Line Interface

58: Functional description (FN): A00009313

58.1 Feature name and Feature ID

SSPFS SN09 Upgrades and ESD Support - A00009313

58.2 Description

This feature will cover the SSPFS upgrade from SN07, or SN08 to the SN09 SSPFS release. The goal of this feature is primarily two areas: ESD support and greater robustness. The intent is to upgrade SSPFS with a minimal of application downtime.

58.3 Design Component: ESD SSPFS SN09 Upgrade

It is very important to set the expectations of this feature. The goal of this feature is to provide SSPFS upgrades using electronic delivery of the ISO images instead of physical cdrom media.

The pre_upgrade.ksh upgrade script of SSPFS creates the location /Upgrade which is the repository for the iso images. After execution of the pre_upgrade script, the user is to place all 3 disk images in the /Upgrade directory. If they all exist, the user will be prompted as to whether or not they intend to perform an ESD upgrade. If they respond positively, then the upgrade will begin in a similar fashion to the normal upgrade. However, the main difference is that the user will never be prompted for the insertion of the SSPFS cdrom disks. Therefore, it will continue unassisted until near the end of the SSPFS upgrade. There will be one point on cbm profiles, where the SSPFS upgrade will stop and we will prompt the user to upgrade the CBM application. Lastly, the user must choose to accept the upgrade or fallback just like the normal upgrade.

58.4 Design Component: pre_upgrade.ksh improvements

This design component is just being developed to document changes which will be placed into the pre_upgrade.ksh script for robustness.The pre_upgrade.ksh upgrade script of SSPFS will be enhanced to check the following additional system states prior to full upgrade execution:

- Ensure the required SSPFS disk mirrors exist and have all sub-mirrors attached.
- Ensure that /var has enough free space to hold the package spooling during the upgrade execution.

These enhancements will allow pre_upgrade to catch more failure cases prior to execution of the main upgrade script. Therefore, the user has a chance to fix system errors before attempting the upgrade again.

59: Functional description (FN): A00009315

59.1 Feature name and Feature ID

Detect failures from syslog and generate alarms - A00009315

59.2 Description

Detect if the syslog system has failed to write logs and raise a major alarm. If and when the syslog system becomes operational, the alarm will be cleared.

Failure detection is not done on each write to the syslog stream, thus it's not 100% real-time. A ten minute audit is used instead. If the audit fails it will wait for one more failing audit before the alarm is raised.

The default timing interval for checking that the logs have stopped is 10 minutes. If a log was generated within the last 10 minutes then everything is working. If the log is older than 10 minutes the system will allow one more 10 minute interval to pass before rasing an alarm. The fastest that an alarm will be raised is 21 minutes and the slowest is 29 minutes.

Note, the timing interval is fixed and cannot be changed by the customer.

This facility will be provided on all profiles of SSPFS-based products, including CMT, MG9K EM, IEMS, MDM, and CBM.

The Fault Management section identifies the details of the new alarm.

59.3 Hardware Requirements or Dependencies

Not applicable.

59.4 Software Requirements or Dependencies

Not applicable.

59.5 Limitations and restrictions

Does not monitor each syslog write in real-time, and does not ensure reliable forwarding of syslog messages to a remote syslog daemon.

.

59.6 Interactions

Not applicable.

59.7 Glossary

Not applicable.

60: Functional description (FN): A00009316

60.1 Feature name and Feature ID

Backup and Restore Enhancements (A00009316)

60.2 Description

This feature's intention is to improve the speed of the SSPFS backup and restore of application data. This backup includes the data stored in the Oracle database and the files registered by applications for backup.

The end user backs up data to disk, tape, or DVD with the following two simple commands. Every effort will be made to preserve the same interface.

/opt/nortel/sspfs/bks/bkdata [-f filename]

/opt/nortel/sspfs/bks/rsdata [-f filename]

The introduction of IEMS to the Succession Solution has increased the amount of data stored in the Oracle database dramatically. The amount of data has made the restore take more than 30 minutes. The majority of the data is alarm, event histories, and peformance metrics. IEMS has made an effort to separate this data from the configuration data with the intention of only backing up the configuration data.

The current interface that applications use to register information in SSPFS is called SERVMAN. This feature will require changes to SERVMAN to allow applications to specify portions of data to exclude/include from the backup/ restore process.

New options in SERVMAN will allow the applications to register, deregister, and query a list of Oracle tablespace names to exclude from the backup/restore process. These commands are not intended for end users, they are intended to be called from application install scripts.

Use servman with register, deregister or query

servman register <-g Group> [-s startScript] [-t stopScript]

[-d dependsString] [-e healthScript]

[-p portInfo] [-f filesystem] [-k critData]

[-bem bkupEnableDataModsScript] [-bdm bkupDisableDataModsScript]

[-bcd bkupCritDataScript] [-bms bkupModeStatusScript]

[-bpc bkupPreCheckScript] [-tbs tablespace]

servman deregister <-g Group>

servman query <-registered | -status | -backup>

< <all | all -tbs | -group <groupName> | <-group <groupName> -bem | -bdm | -bcd | -bms | -bpc | -tbs> > <-v>

60.3 Hardware Requirements or Dependencies

No specific hardware requirements. But there will be a need for a new dedicated disk space for backups of the Oracle database and any files registered as critical files by applications. This space needs are bound by existing hardware specs for the Sun Netra T1400 and the Sun Netra 240.

60.4 Software Requirements or Dependencies

No new software requirements. However, a feature of Oracle called Recovery Manager (RMAN) may be utilitized for the first time.

60.5 Limitations and restrictions

Backup and Restore time will always be bound by I/O speed to the target media whether it is a hard drive, tape drive, or DVD/CD burner.

60.6 Interactions

The changes in this feature interacts with the “Synchronized Backup Manager”. This Backup Manager was introduced in SN08 and calls the SSPFS backup scripts at scheduled intervals.

60.7 Glossary

Term	Description
SSPFS	Succession Server Platform Foundation Software
RMAN	Recovery Manager (Oracle utility)
IEMS	Integrated Element Management System
SERVMAN	Services Manager: an SSPFS interface to manage starting, stopping, and gathering status from applications

61: Functional description (FN): A00009320

61.1 Feature name and Feature ID

A00009320, A00009336 - Remote Ping and Traceroute for Gateway Controller and SSPFS Platforms

61.2 Description

The purpose of this feature is to provide a centralized, graphical user interface on IEMS to allow users to launch ping and traceroute operations remotely on the Gateway Controller (GWC) and SSPFS platforms; including IEMS, CMT, MG9K Manager and CBM. This addresses the concerns of allowing non-root users access to these potentially harmful commands.

61.3 Hardware Requirements or Dependencies

This feature has no HA dependencies, so any customer-supported hardware configuration will provide a valid IT platform

IEMS Server: T1400, N240 (cluster or simplex)

CMT: T1400, N240 (cluster or simplex)

GWC - any supported hardware

61.4 Software Requirements or Dependencies

IEMS SN09 combo load week 11 or later

CMT - SN09

GWC - SN09 week 11 or later (gn090ap or later)

SSPFS - SN09 week 10 or later

61.5 Limitations and restrictions

This feature provides a centralized interface to the native ping and traceroute functionality on remote platforms. Command options and behavior for ping and traceroute may vary between remote launch points.

Central account users requiring SSPFS remote ping/traceroute capability must be granted restricted platform access (by setting their default shells to `restricted-access shell'.

61.6 Interactions

Remote command launch allows users to troubleshoot network connectivity problems from a single location using the same user interface. It initiates an operation on a remote platform or device as if the user had logged on to the device and issued the command himself. In SN09, remote ping and traceroute functionality has been provided through the IEMS GUI client. These remote operations are supported in this release for the GWC and SSPFS platforms.

This feature adds two new launch menu buttons to the GWC and the SSPFS platform managed objects in the IEMS GUI: one for remote ping, and one for traceroute.

61.6.1 Setup

The following configuration steps must be performed from the SAM21-EM to allow direct IEMS communications with GWCs:

1. Login to the SAM21-EM GUI
2. Click on the “Configuration” menu.
3. Select "Subnet Level Configuration"
4. Enter IEMS virtual IP in "MIB Reader (optional)" text box.
5. Click "Save"

Figure 1 SAM21-EM Configuration menu

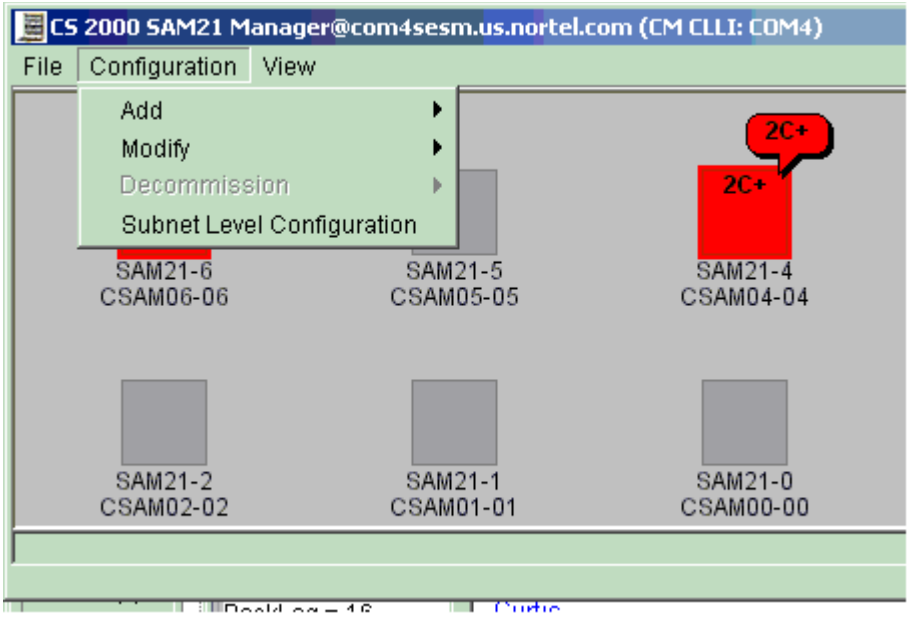
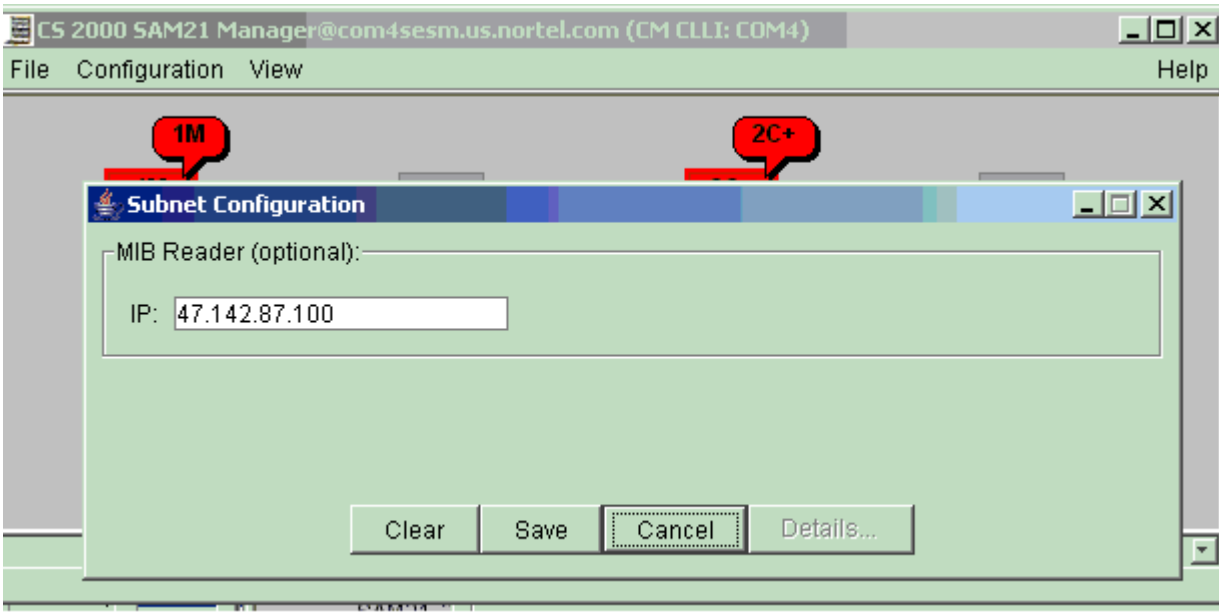


Figure 2 SAM21-EM Subnet Configuration menu



61.6.2 Launching:

This feature is accessed from the drop-down menu available when the a GWC or SSPFS unit managed object is right-clicked. Two new menu items have been added to the list:

- **“Launch Remote Ping”**
- **“Launch Remote TraceRoute”**

Figure 3 GWC Ping/Traceroute Launch Menu

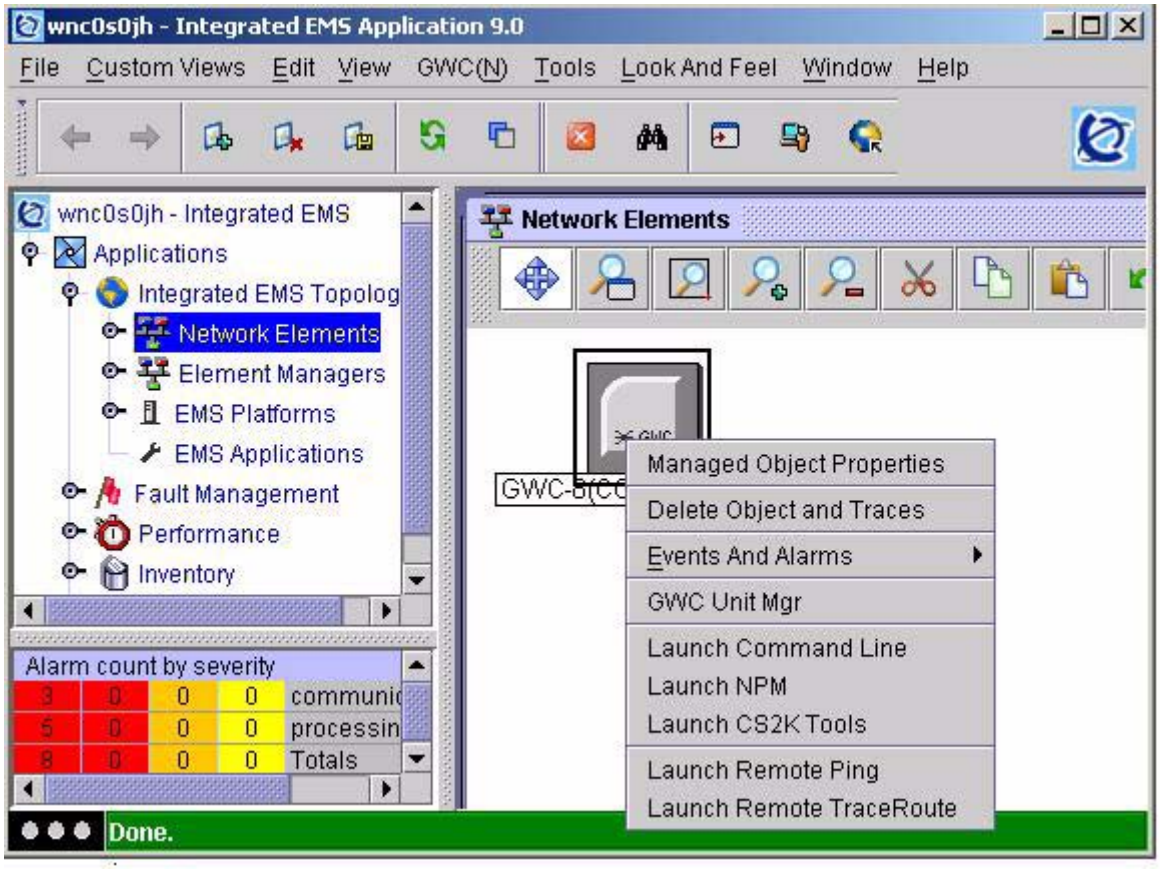
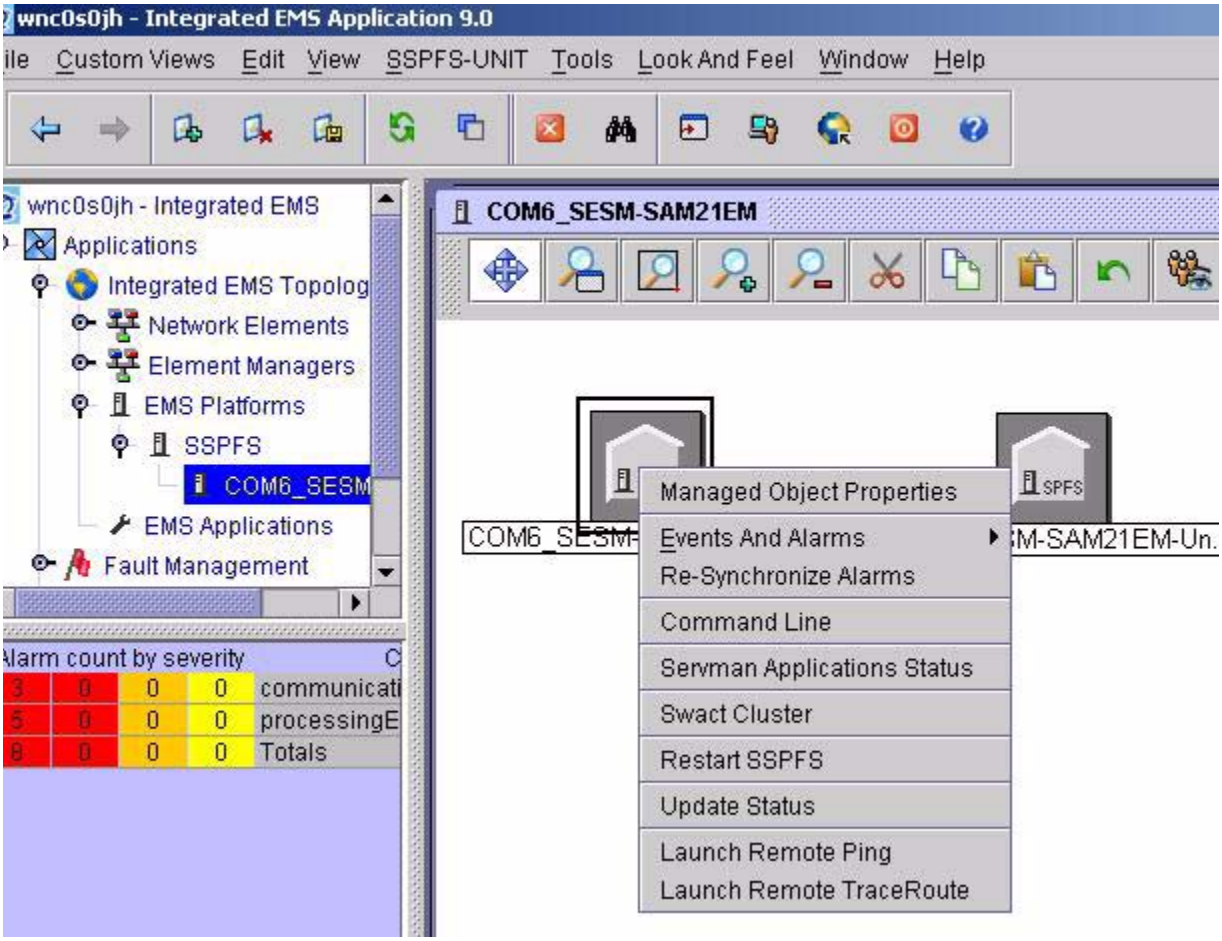


Figure 4 SSPFS Ping/Traceroute Launch Menu



The dialog for either operation is presented when selected from the menu. Each will be discussed in turn.

61.6.2.1 User Authorization

Remote operations are only available to a restricted set of users. For security purposes, only users belonging to one or more of the following groups for supported platforms will have access to these functions: ADM, MTC RW.

The following table lists the groups authorized for remote operations

Table 3: authorization groups for remote operations

SSPFS	GWC
emsadm	mgcadm
emsmtc	mgcmtc

Table 3: authorization groups for remote operations

SSPFS	GWC
emsrw	mgcrw

Remote launch menu options will not appear in the above drop-down menus for unauthorized users.

61.6.2.2 Single Sign-on Support

Once an authorized user has launched a remote operations GUI and entered the required parameters, the command should be sent to the remote host for execution without any further input required by the user. The client will use the security information obtained from the user at initial login , and use this to obtain access to the remote launch host. There is one exception to this rule:

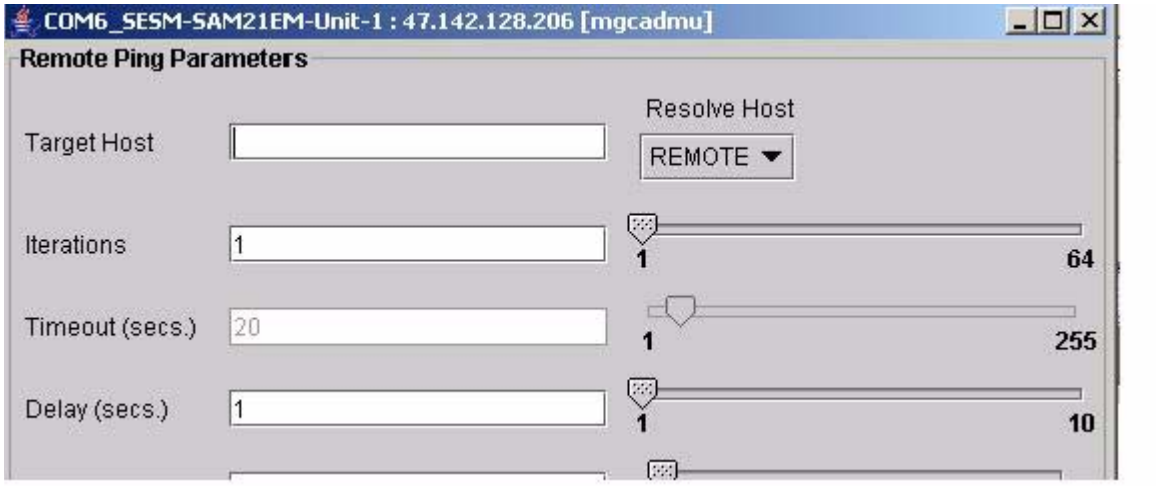
When configured for CBM, the SSPFS platform does not integrate its security with the central security services used to provide single sign-on capabilities to users. In this case, the user will be presented with a dialog prompting for a username and a password to allow remote execution of the ping/traceroute command on the CBM platform.

61.6.3 Notes on Remote Operations:

- only one remote operation (ping or traceroute) is permitted on each managed object at a time. This effectively denies concurrent requests on the same device or platform. For example, user A launches a ping command on GWC 13. User B will be unable to launch any command on GWC 13 until the command completes for user A.
- The RemoteOps interface is constrained by the actual ping and traceroute functionality provided by a remote device. The interface acts as a proxy and invokes the command from the remote host as if a user had logged on and run it manually. Supported values and their ranges may vary between devices. Although a generic set of options, defaults, and ranges have been defined to constrain these operations in the network, they may be constrained even further by the remote host. The supported parameters and ranges for each device will be shown on the client screens when presented for input. The user does not need to know about this. An example of this is packet size. SSPFS platforms support a range of 1-65507 bytes, while the GWC only supports 4-1472 byes. Each range will be automatically enforced on client invocation.
- Ping and traceroute user parameters are common across all device and platform types. If a parameter is unsupported or unconfigurable for a selected managed object, the option will be displayed as read-only with a default value specified (if supported). For example, the screen in Figure 3

displays the ***Delay*** parameter as Read-Only. The value shown will be used for the operation and cannot be changed by the user.

Figure 5 Read-Only Parameter example



Title Bar - The displayName and ipAddress properties of the managed object on the IEMS GUI are displayed in the top left corner of the screen. This is the source host for the remote operation (IP address of object right-clicked on GUI). Following the host infomation is the login user name enclosed in square brackets.

Figure 6 Remote Host Identifier

61.6.4 Remote Ping

The main screen for remote ping allows the user to set the following parameters:

Target Host:

This is the destination host to be ping'ed by the remote platform (GWC , for example). This value can be specified as a host name or IP address (see notes on DNS resolution).

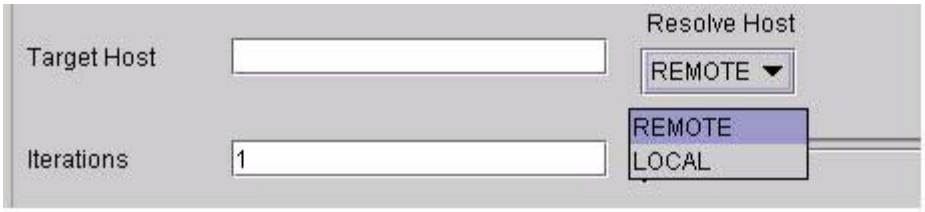
DNS Resolution

- specifies whether target address resolution should be attempted using the name service configured for IEMS server (*LOCAL*), or the name service of the remote launch host (*REMOTE*). This setting defaults to *REMOTE*.

Note: If DNS is not used in the network, then an attempt will be made to resolve the host name or IP using the default resolver on the IEMS server or remote device/platform.

Limitation: When using the "*REMOTE*" option on the GWC platform, target hosts MUST be entered as fully qualified domain names (FQDN). Host names provided without the full domain component will *fail* DNS resolution in the GWC. Target hosts can be specified this way by selecting "*LOCAL*" DNS resolution.

Figure 7 DNS Resolution Options



Iterations:

Specifies how many times to repeat the command.

Timeout:

Specifies the timeout for the remote host to use when running the remote operation. This value is given in seconds.

Delay:

Specifies the delay to use between each ping operation (ie: pause between iterations). This is given in seconds.

Packet Size:

Specifies (in bytes) the data size of each ping probe packet to use in the operation.

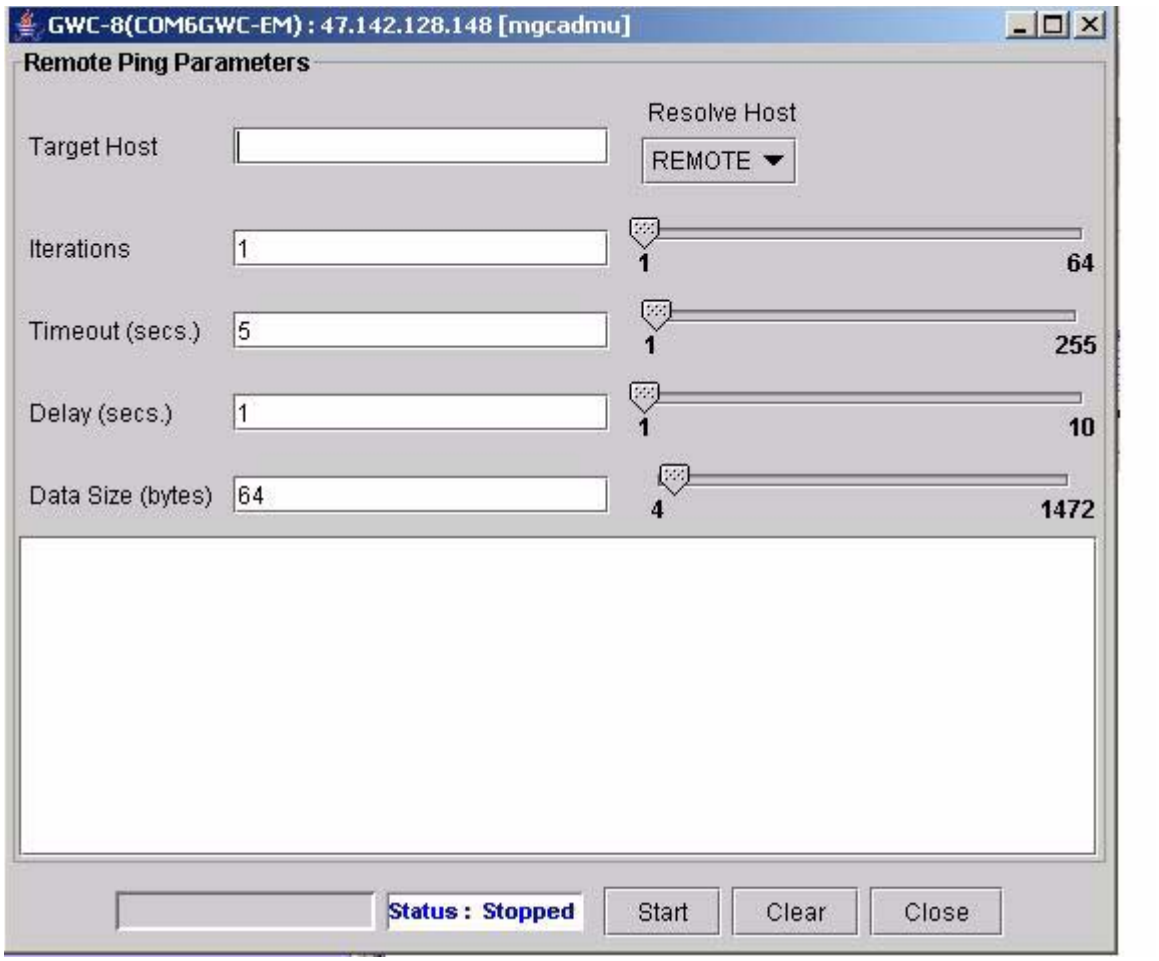
Table 1 Ping Dialog User Parameters

User Parameter	GWC Values	SSPFS Values	Default
Target IP	Host Name or IP address	Host Name or IP address	none
Iterations	1-64	1-64	1

Table 1 Ping Dialog User Parameters

User Parameter	GWC Values	SSPFS Values	Default
Delay (seconds)	1-10	1-10	1
Timeout (seconds)	1-255	1-255	5
DNS Resolution	local/remote	local/remote	remote
Packet size	4-1472 bytes	1-65507 bytes	64 bytes

Figure 8 Remote Ping Launch Screen

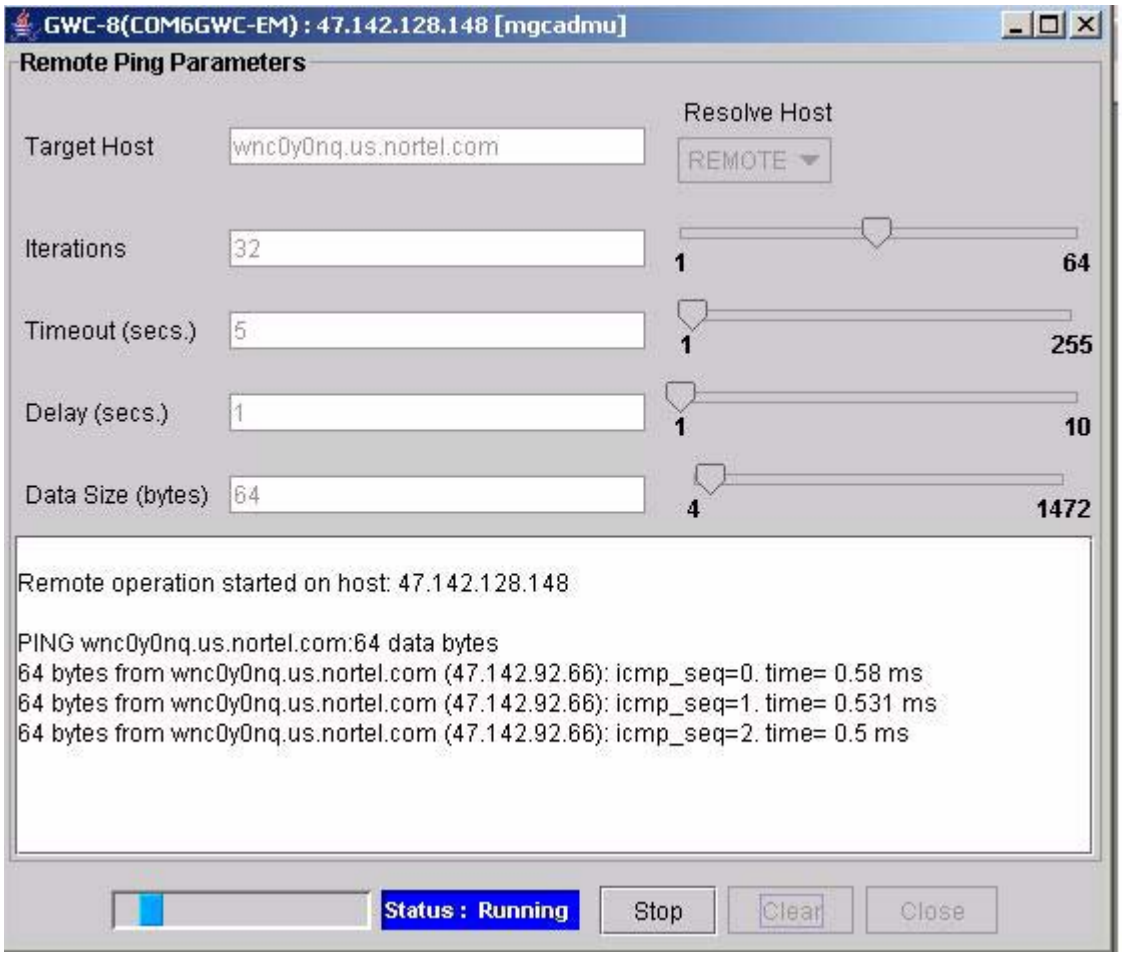


Start button

starts remote operation with entered user parameters. Once the operation is started, all user input is disabled and the Start button changes its function to

allow the command to be stopped (cancelled). This ensures that only operation can be launched at a time from the GUI. See Figure 9

Figure 9 Remote Ping while running



Clear Button

clears text screen

Close

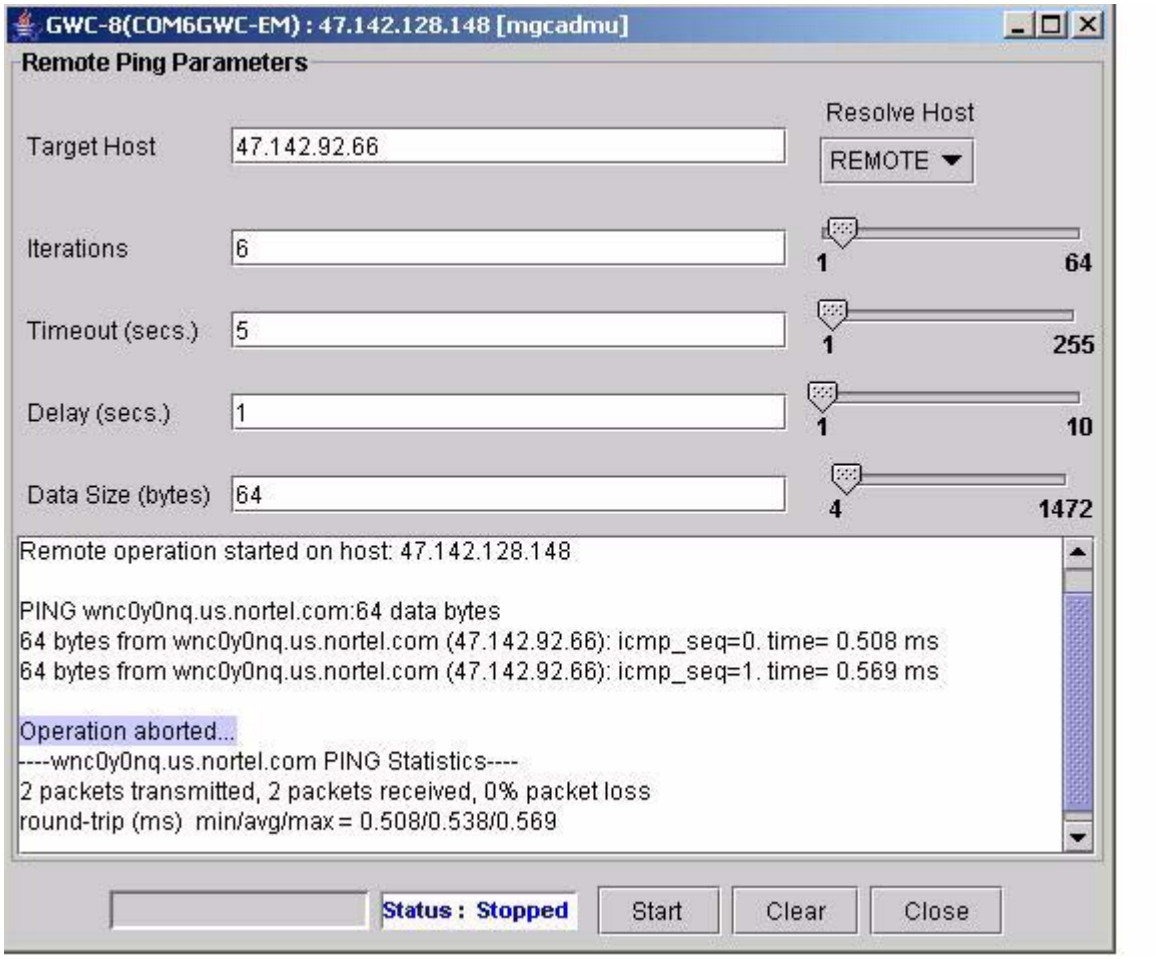
closes window

61.6.4.1 Command ABORT

Running commands can be cancelled by the user by clicking the “Stop” button while the status bar indicates “Running”. The command will terminate and provide statistics for the packets sent and received up to the point of

cancellation. The text output provides a message indicating the command was aborted.

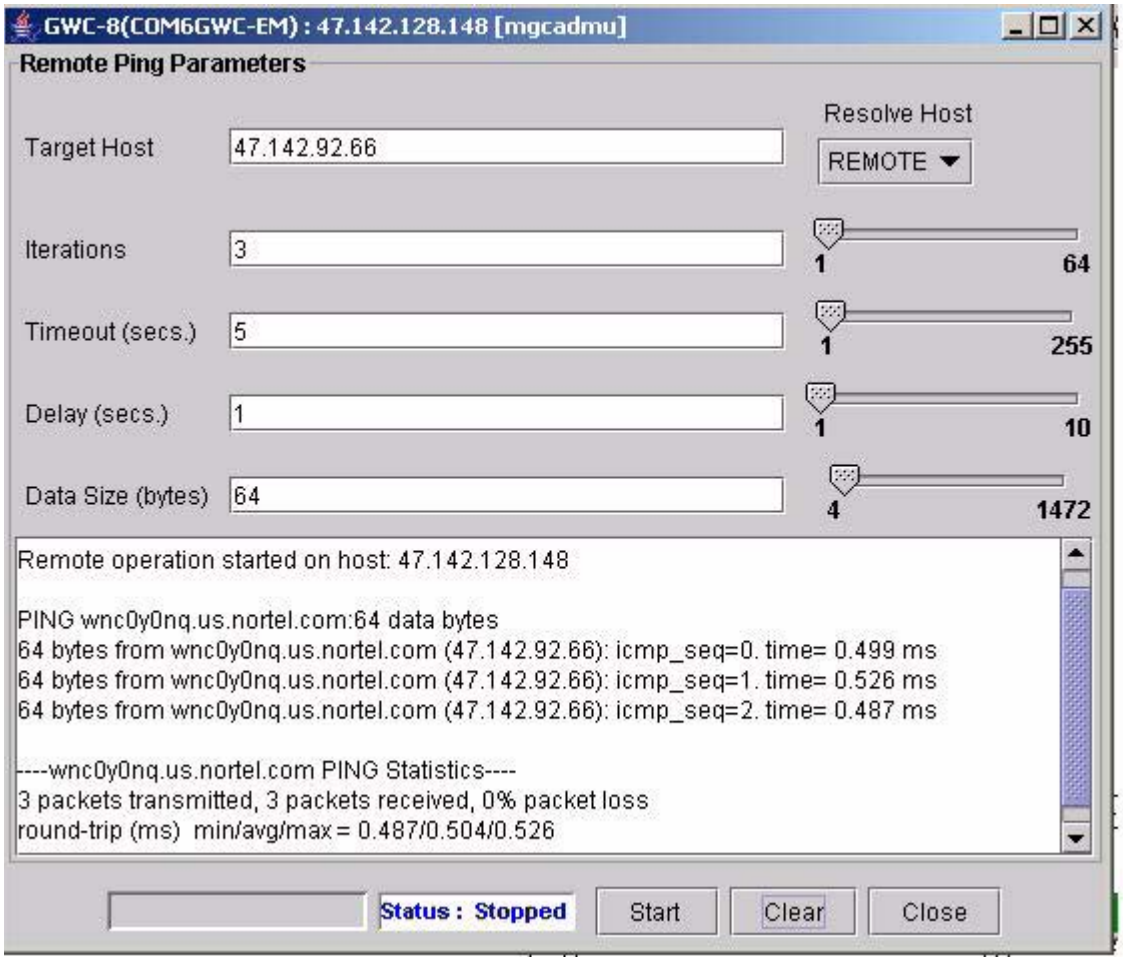
Figure 10 Cancel remote Ping Operation



61.6.4.2 Command output

The response output for the requested command will be output to the text window similar to that show shown in Figure 8. The application communicates with the GWC over SNMP and formats the results to appear similar to UNIX command line ping output :

Figure 11 Ping output Screen



61.6.5 Remote TraceRoute

The main screen for remote ping allows the user to set the following parameters:

Target Host:

This is the destination host to find a route by the remote platform (GWC , for example). This value can be specified as a host name or IP address (see notes on DNS resolution).

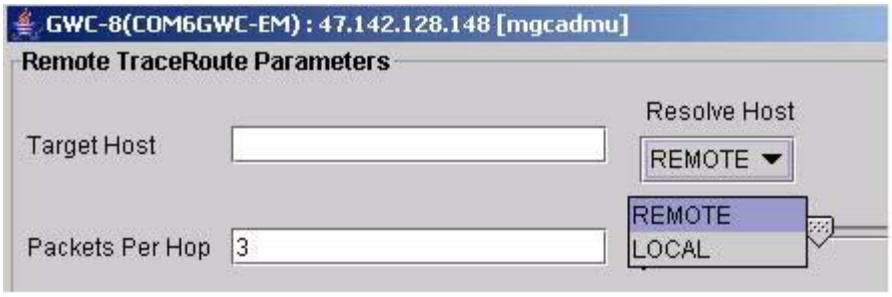
DNS Resolution

- specifies whether target address resolution should be attempted using the name service configured for IEMS server (*LOCAL*), or the name service of the remote launch host (*REMOTE*). This setting defaults to *REMOTE*.

Note: If DNS is not used in the network, then an attempt will be made to resolve the host name or IP using the default resolver on the IEMS server or remote device/platform.

Limitation: When using the "*REMOTE*" option on the GWC platform, target hosts MUST be entered as fully qualified domain names (FQDN). Host names provided without the full domain component will *fail* DNS resolution in the GWC. Target hosts can be specified this way by selecting "*LOCAL*" DNS resolution.

Figure 12 DNS Resolution Options



Timeout:

Specifies the timeout for the remote host to use when running the remote operation. This value is given in seconds.

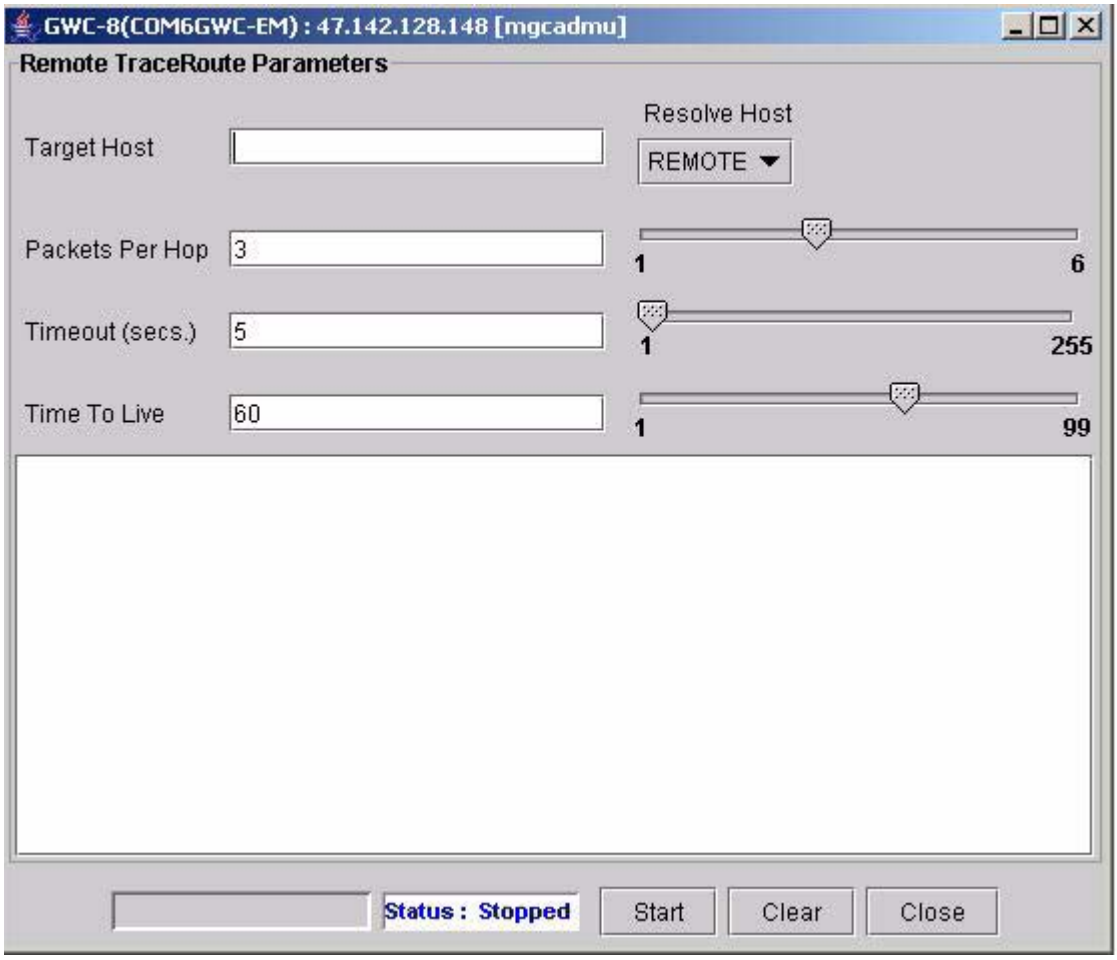
Packet Size:

Specifies (in bytes) the data size of each ping probe packet to use in the operation.

Table 2 Traceroute Dialog User Parameters

User Parameter	GWC Values	SSPFS Values	Default
Target IP	Host Name or IP address	Host Name or IP address	none
Probes per Hop	1-6	1-6	3
TTL (Time To Live)	1-99	1-99	60
Timeout (seconds)	1-255	1-255	5
DNS Resolution	local/remote	local/remote	remote

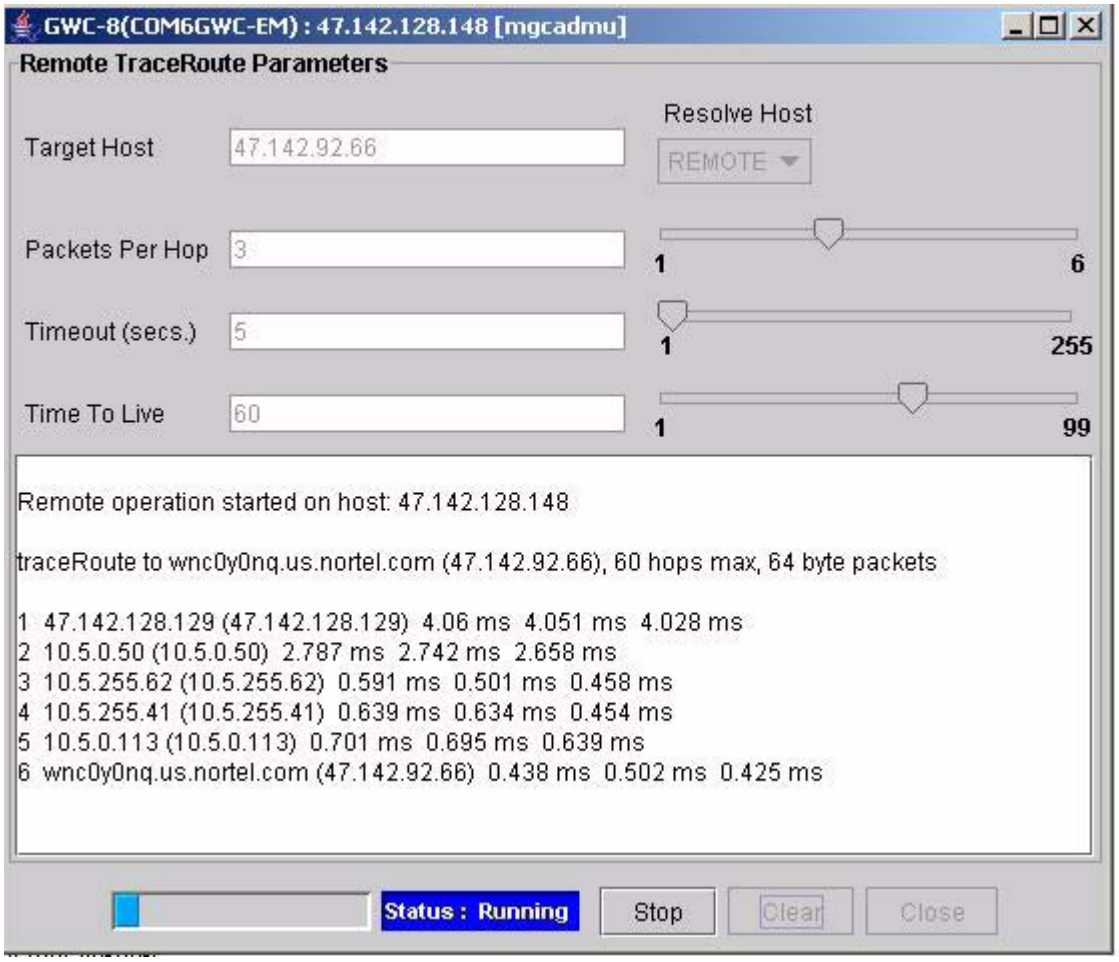
Figure 13 Remote Traceroute Launch Screen



Start button

starts remote operation with entered user parameters. Once the operation is started, all user input is disabled and the Start button changes its function to allow the command to be stopped (cancelled). This ensures that only operation can be launched at a time from the GUI. See Figure 14.

Figure 14 Remote TraceRoute in operation



Clear Button

clears text screen

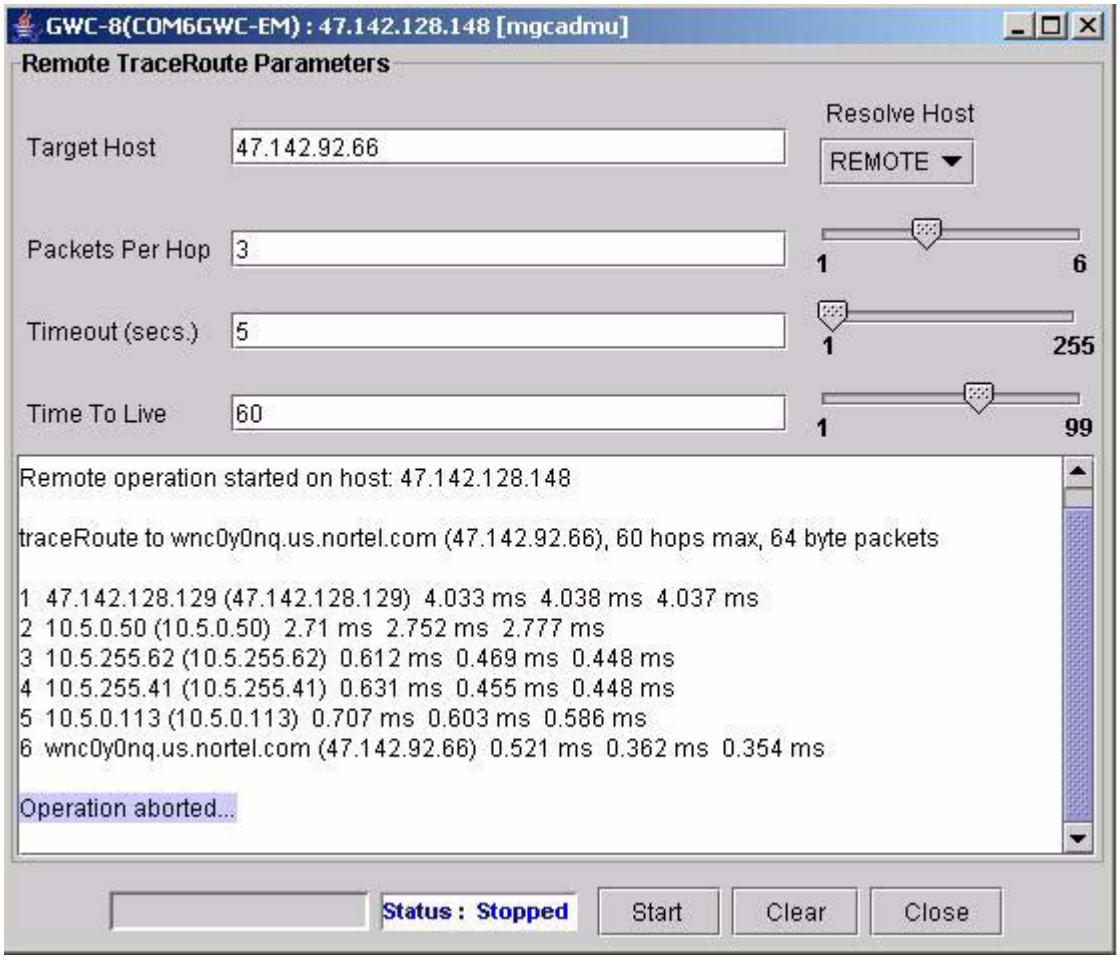
Close

closes traceroute window

61.6.5.1 Command ABORT

Running commands can be cancelled by the user by clicking the “Stop” button while the status bar indicates “Running”. The command will terminate and provide statistics for the packets sent and received up to the point of cancellation. The text output provides a message indicating the command was aborted.

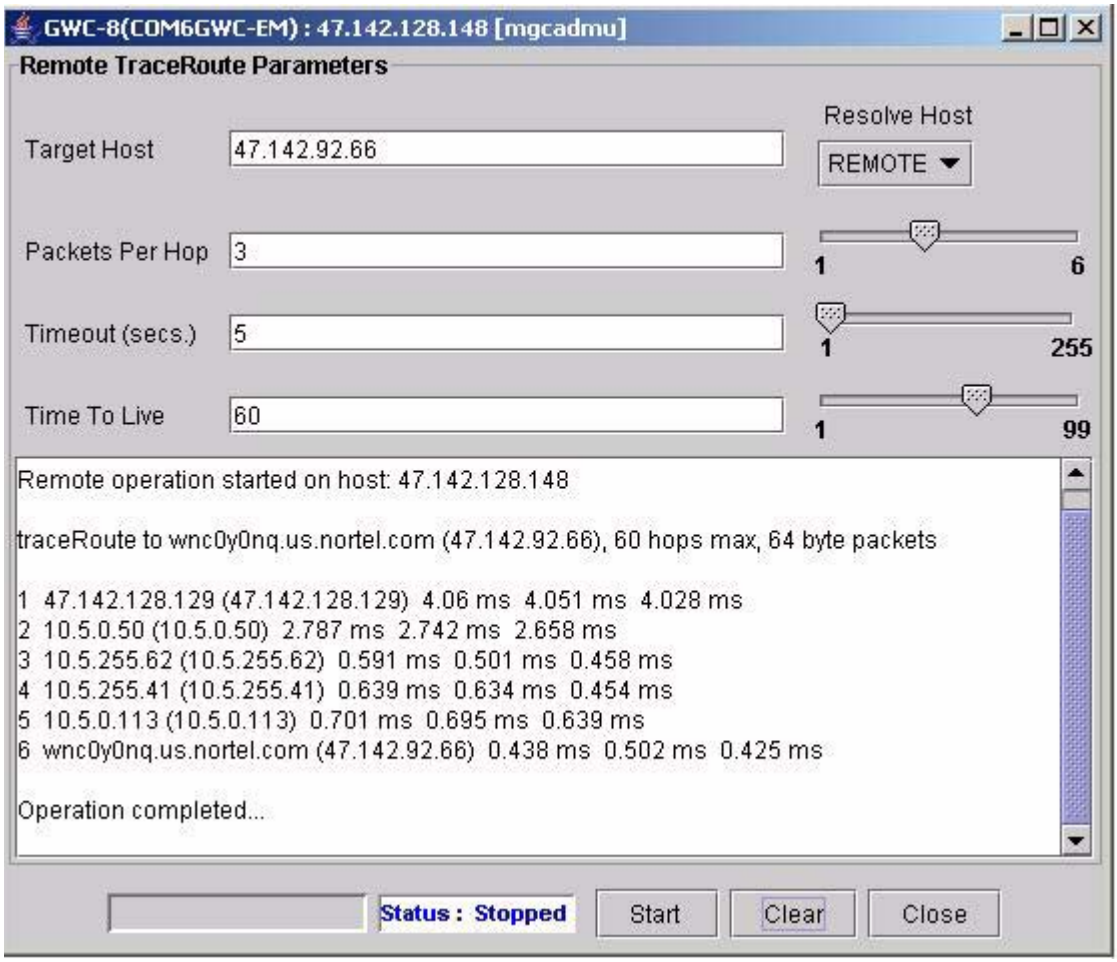
Figure 15 Cancel Remote Traceroute operation



61.6.5.2 Command output

The response output for the requested command will be output to the text window similar to that show shown in Figure 8. The application communicates with the GWC over SNMP and formats the results to appear similar to UNIX command line traceroute output :

Figure 16 Remote TraceRoute output



61.7 Glossary

Term	Description
IEMS	Integrated Element Management System
GWC	Gateway Controller
SSPFS	
MG9K	Media Gateway 9000
CBM	Core Billing Manager
CMT	
SNMP	Standard Network Management Protocol
SSH	Secure Shell

62: Functional description (FN): A00009332

62.1 Feature name and Feature ID

The name of the feature is “P-Time and Codec Negotiation Selection Policy”. The feature-ID is A00009332.

62.2 Description

This feature makes enhancements to the CS2M that allows the customer to choose codecs and packetization rates for IP and aal2 network bearer connections that were previously not available. The new P-times are p30ms and p40ms.

The CS2M now supports the following new codecs.

- G.723
- EVRC
- EVRC0
- G726-32
- ILBC
- BV16
- AMR
- G726-24

In addition to the above, further enhancements were made to the CS2M GUI. These enhancements were to display G.711A as PCMA and G.711U as PCMU.

Note: Codec ILBC should only be associated with packetization rates of 20ms or 30ms.

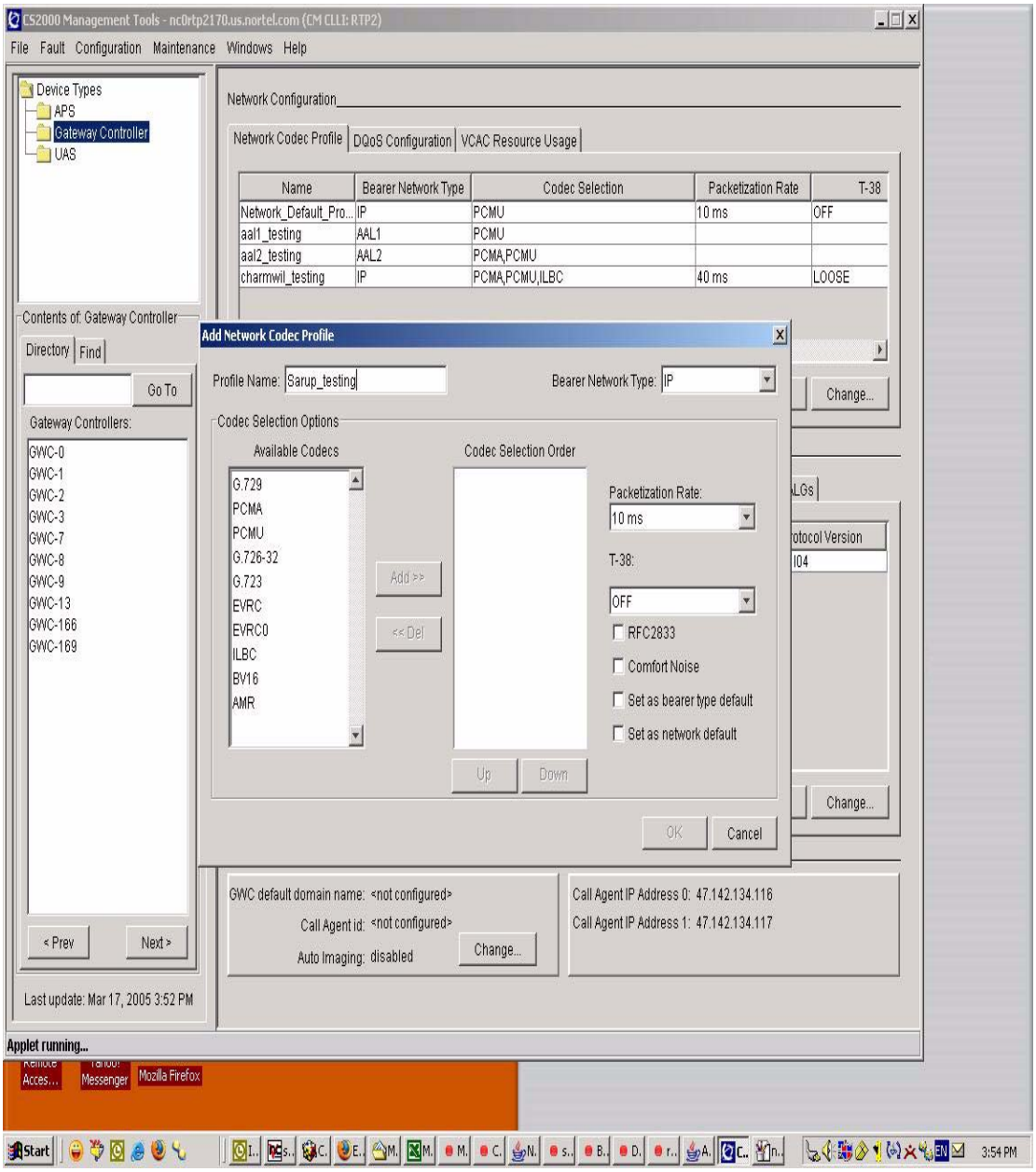
62.3 CS2M GUI Functionality Modifications

2.3.1 Add Network Profile Dialog

When adding a new network profile, the customer could choose three of the eleven codecs listed in the text area. Whatever combination of three that the customer chooses, that combination must include PCMA or PCMU.

The customer can choose from one to maximum of three codecs to provision within their network. Figure one shows the “Add Network Profile Dialog” screen that listed a subset of the codecs the CS2M support.

figure one: Add Network Profile Dialog

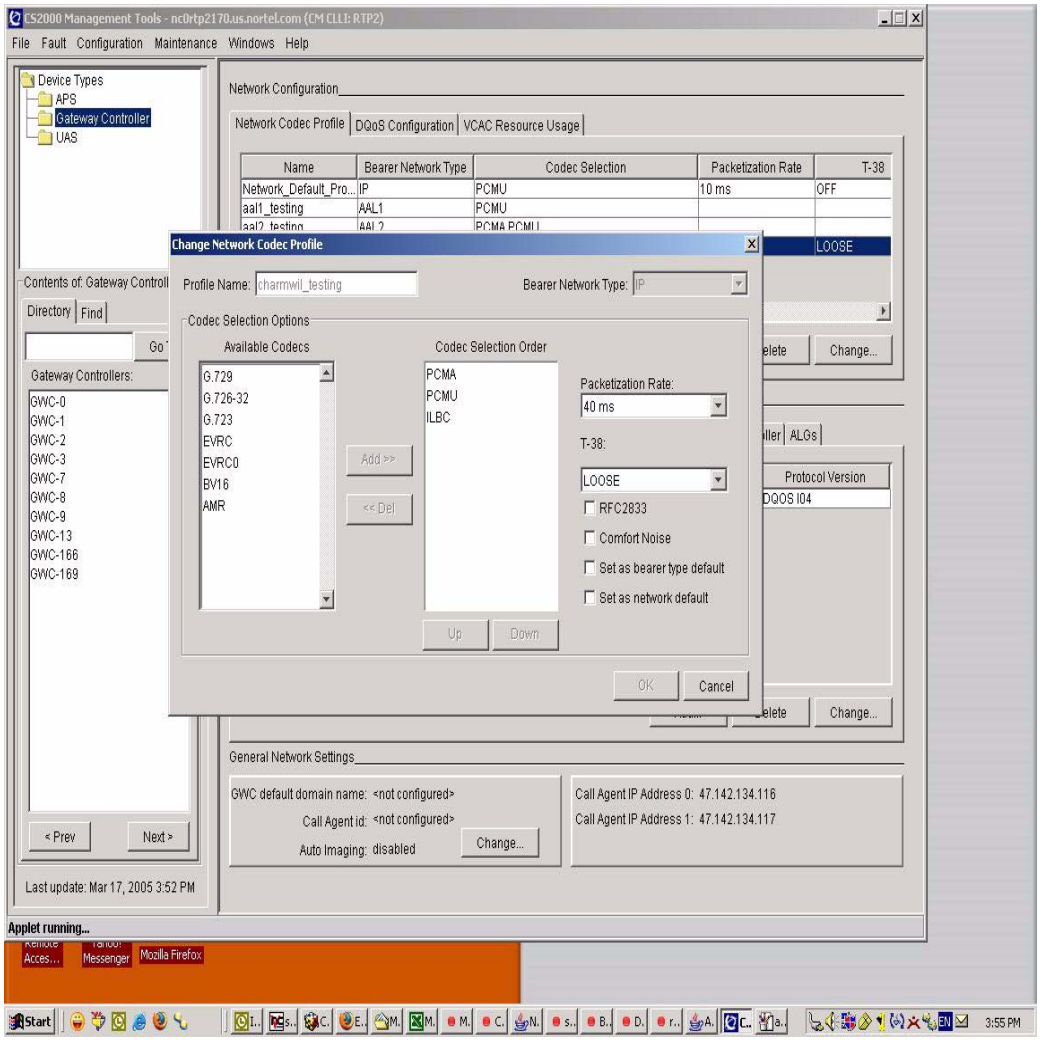


2.3.2 Change Network Profile Dialog

When changing the Network profile, the customer can now select from eleven codecs shown in the selection listing area. Figure two shows the “Change Network Profile Dialog” screen which allows the user to change their previous selection/s.

Note: The same restriction stated in “Add Network Profile Dialog” section applies here.

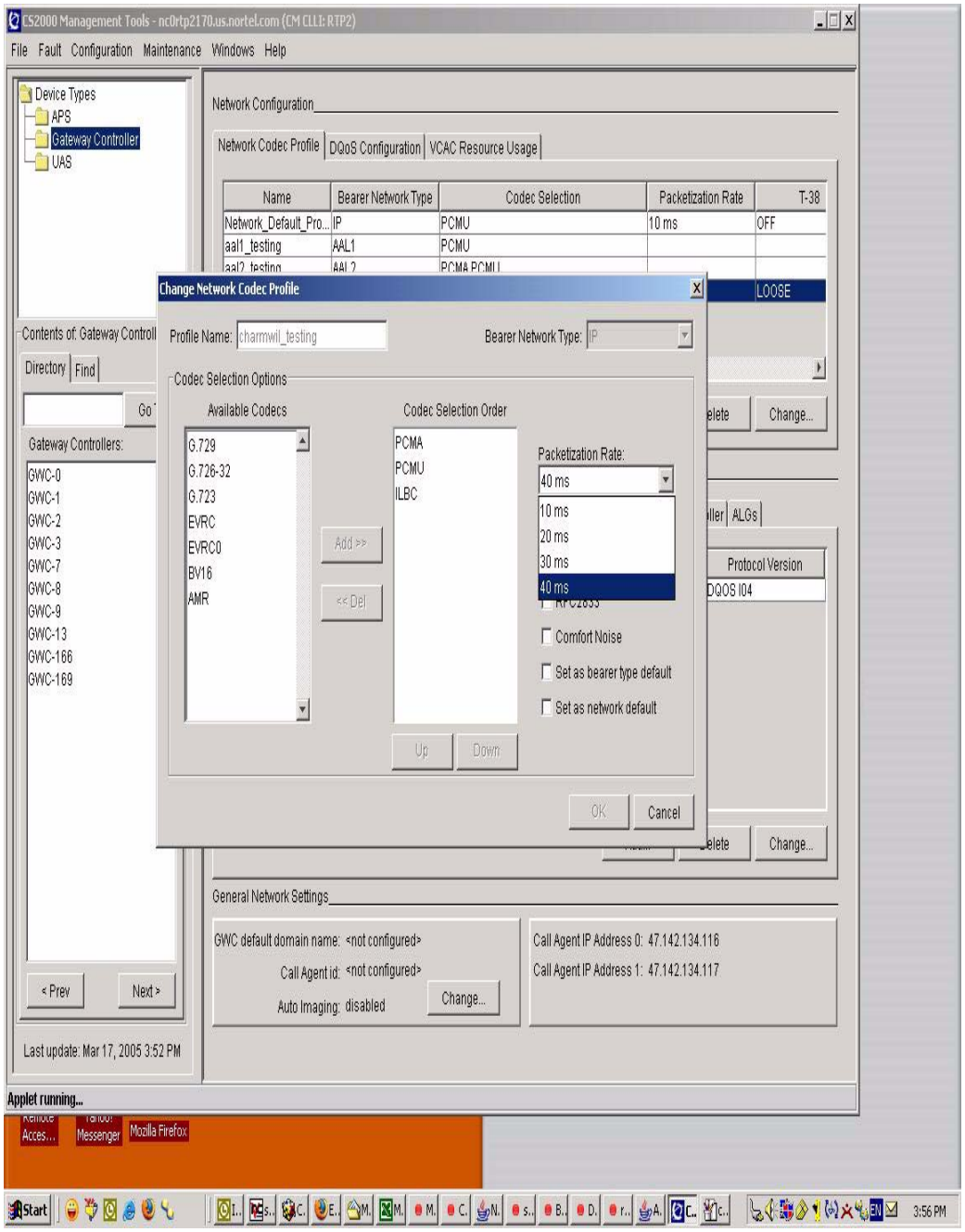
Figure 2: Change Network Profile Dialog



2.3.3 Add P-time Dialog

The customer can now select from four p-times. The p-times are p10ms, p20ms, p30ms and p40ms. Figure 3 shows the screen image of the P-time menu.

Figure 3: Add P-time Dialog Menu



62.4 Hardware Requirements or Dependencies

None.

62.5 Software Requirements or Dependencies

None.

62.6 Limitations and restrictions

- The maximum number of codecs the user is allowed to select is three.
- The user’s selection/s must always include PCMA or PCMU.

62.7 Interactions

None.

62.8 Glossary

Term	Description
P-Time	Packetization rate
CS2M	CS2K Mangement Tool

63: Functional description (FN): A00009337

63.1 Feature name and Feature ID

A00009337 PacketCable 1.0, 1.1, and 1.5 Compliance

63.2 Description

This activity addresses NCS and TGCP ECN support and development items for the Media Gateway Controller (MGC) to satisfy PacketCable1.5 Specifications PKT-SP-NCS1.5-I01-050128 and PKT-SP-TGCP1.5-I01-050128.

Excluded from this activity are:

- T.38 ECNs NCS1.5-S-I01.05-2-Atkinson and TGCP1.5-S-I01.04-2-Hancock, being addressed under activity A00009339 (PC 1.5 Support for T.38 Fax);

In addition, NCS and TGCP PacketCable 1.0 and 1.1 ECN compliance items and Succession solutions development items are included in the activity, and provide Certification Wave 37-aligned PacketCable specification compliance.

Some of the new items being developed in this feature are also being applied via ECN to the PacketCable 1.0 and 1.1 specifications. In these cases, the language is the same as the PC 1.5 ECN's, so the content being addressed in this feature will make the CS2K compliant to 1.0, 1.1, and 1.5 versions of these changes.

Operator services such as Operator Ringback, Operator Recall, Busy Line Verification (BLV), and Barge-In (BI) are now supported over TGCP OP trunks for hybrid office solutions.

For further information regarding MGC support of TGCP trunks, please refer to activities A00003630 (TGCP for the Cable Market) and A00007114 (TGCP Compliancy).

63.3 Hardware Requirements or Dependencies

Not Applicable

63.4 Software Requirements or Dependencies

- The PacketCable TGCP specification does not currently provide any explicit mechanism for an MGC to proactively acquire an endpoint's service state

(when it is necessary to distinguish between in-service and out-of-service endpoints). Until the TGCP specification allows such a mechanism, TGCP gateways MUST only include in-service endpoints within the EndPoint-IdList parameter in response to a CS2000 AuditEndpoint command.

63.5 Limitations and restrictions

- Operator recall over TGCP OP trunks provisioned with TERMHOLD is supported for both circuit-switched and packet-switched lines, if onhook/offhook (ie. suspend/resume) transition is performed via switchhook. Operator recall cannot be initiated with flash key for packet-switched lines.

63.6 Interactions

Not Applicable

63.7 Glossary

Term	Description
ECN	Engineering Change Notification
MG	Media Gateway
MGC	Media Gateway Controller
MTA	Multimedia Terminal Adapter
NCS	Network Control Protocol
RFC	Request For Change
TGCP	Trunking Gateway Control Protocol
VoIP	Voice over IP

64: Functional description (FN): A00009339

64.1 Feature name and Feature ID

Packet Cable T.38 Support, activity A00009339.

64.2 Description

This activity provides packet cable support for T.38 Fax based on PacketCable1.5 Specifications. It adds T.38 fax element into the LCO (for NCS and TGCP) which is sent to the gateway at the start of a call. The presence of this information triggers the gateway to include the T.38 into its SDP response. This is then used by the far end gateway to ensure that both gateways support T.38 before the functionality is used.

This activity provides T.38 support which is compliant with the PacketCable 1.5 Specifications.

The switch-over to T.38 is performed based on the MTA or MG sending a detection of the “t38 start” event. If the T.38 codec is supported by both gateways, the call switches to T.38 mode once the switching sequence completes.

This feature will implement T.38 strict and loose modes, as described in the PacketCable 1.5 Specifications. If strict mode is active, the attempt to switch to T.38 codec will only occur if both gateways in the call advertise T.38 capabilities in their SDP (refer to the CS2000 T.38 Gateway Interoperability Specification for details). If loose mode is active, the CS2000 will attempt to switch to T.38 even if one side does not advertise T.38 capabilities. In loose mode, when the codec switch is rejected by either end, an attempt will be made to preserve the call by switching back to G.711 codec.

> ***Note:*** Prior to SN09, the only choice for T.38 was enabled or disabled. The equivalent for “enabled” is “strict” mode in SN09.

Strict Mode is recommended to be used if all Gateways in a customer network support T.38. Due to increased messaging, Loose Mode is only recommended when there are gateways in the network that (1) support the T.38 codec, and (2) do not advertise this support in the SDP. This scenario is common when SIP trunks are being used, but is unlikely when a customer has exclusively PacketCable 1.5-compliant devices and/or a T.38-capable PVG.

Loose Mode is not recommended to be used during an SN09 upgrade while Gateways are being upgraded to T.38-capable loads. Instead, it is recommended to leave T.38 off until all Gateways have been upgraded, then turn it to “strict” or “loose” as appropriate.

The customer must configure T.38 in either “strict”, “loose”, or “off” mode via the GWC Element Manager in CS2M. Since this setting can be different for each GWC, there is a possibility of different modes being applied to each Gateway involved in a FAX call. It is recommended that customers choose the same T.38 mode across all GWC’s. If different modes must be used, the customer must select either “strict” or “loose” across all profiles. T.38 calls are not supported and will fail if any profiles have T.38 configured to the “off” setting.

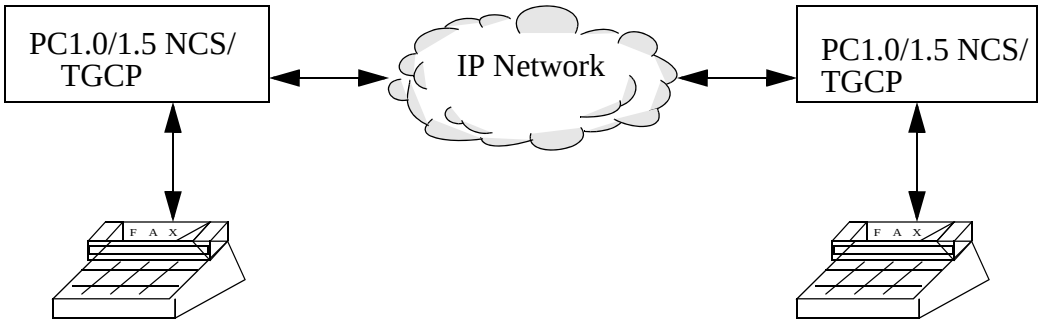
This feature requires that a non-compression codec (G.711) must always be an alternative in the codec list when one or more compression codecs are used. This provides an alternative to allow the FAX call to succeed in the event that one Gateway does not support T.38. If T.38 loose mode is active, one of the gateways in a call does not support T.38, and a compression codec is in use, the gateways must autonomously switch to G.711 without direction from the CS2K.

This feature is dependent on SN09 activity A00009294 and A00009443 for SIP/NGSS interworking.

64.3 Interworking and Scenarios

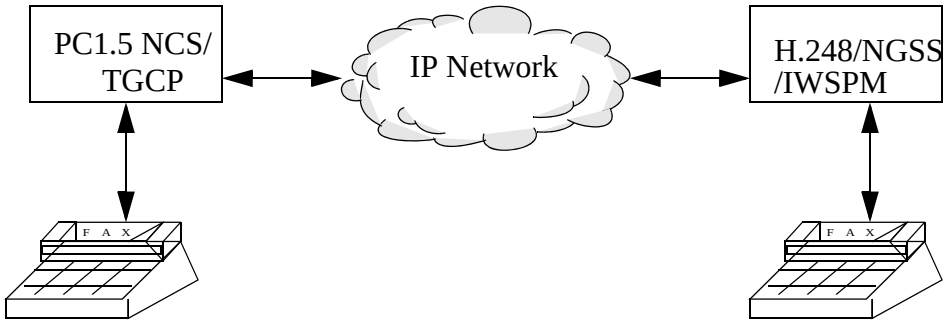
The feature covers FAX interworking between the following GWs in the Cable Solution:

- PacketCable 1.5 GW (MTA or MG)
- PacketCable 1.0 GW (MTA or MG)
- PVG (T.38 Annex D only)
- M2000 (T.38 Annex D only)
- SIP/SIPT
- IWSPM (G.711-only)



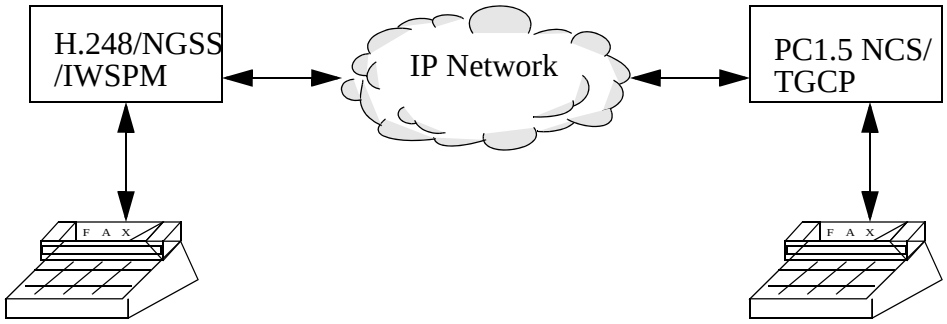
Calling FAX
- CNG Tone

Called FAX
- ANS/CED Tone
- V.21 Preamble



Calling FAX
- CNG Tone

Called FAX
- ANS/CED Tone
- V.21 Preamble



Calling FAX
- CNG Tone

Called FAX
- ANS/CED Tone
- V.21 Preamble

64.4 Software Requirements or Dependencies

The feature requires the following items in place for successful T.38 functionality:

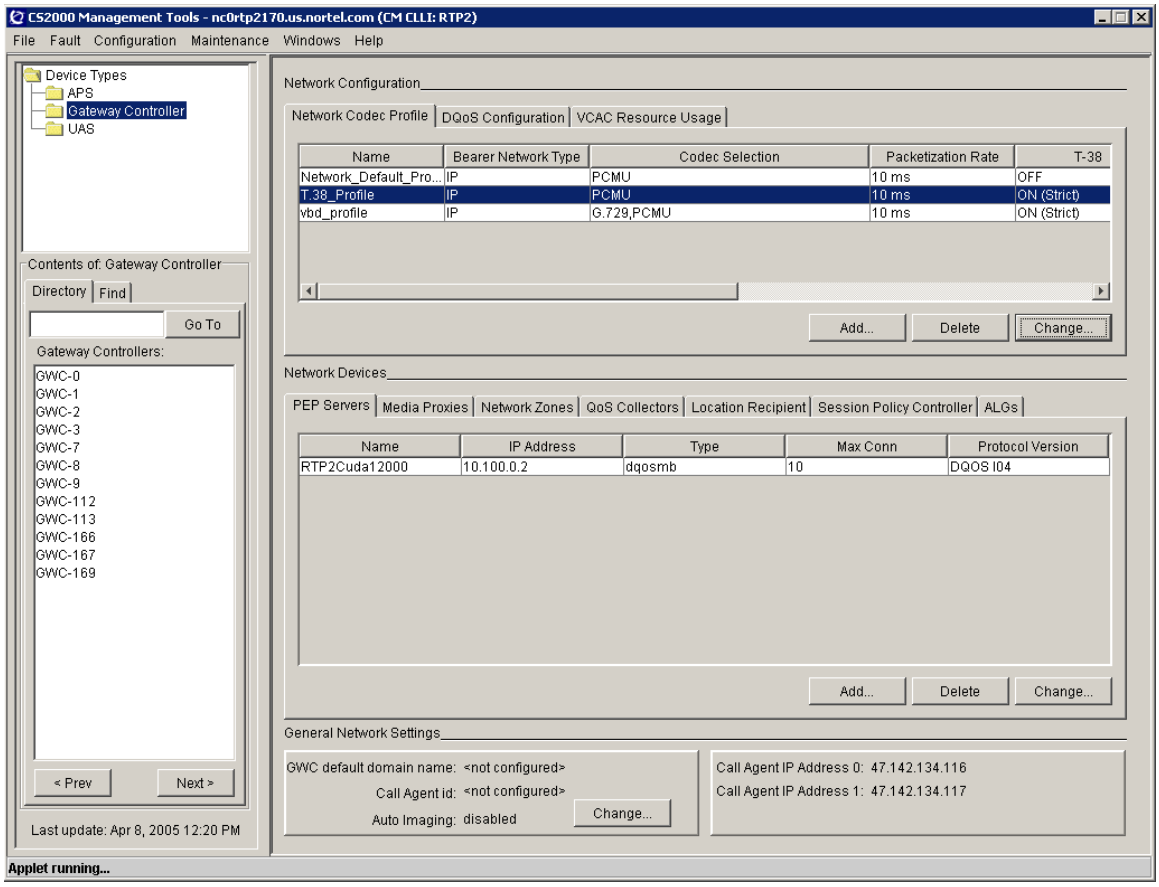
- SN09 SESM for setting up T.38 mode
- PacketCable 1.5 compliant GWs

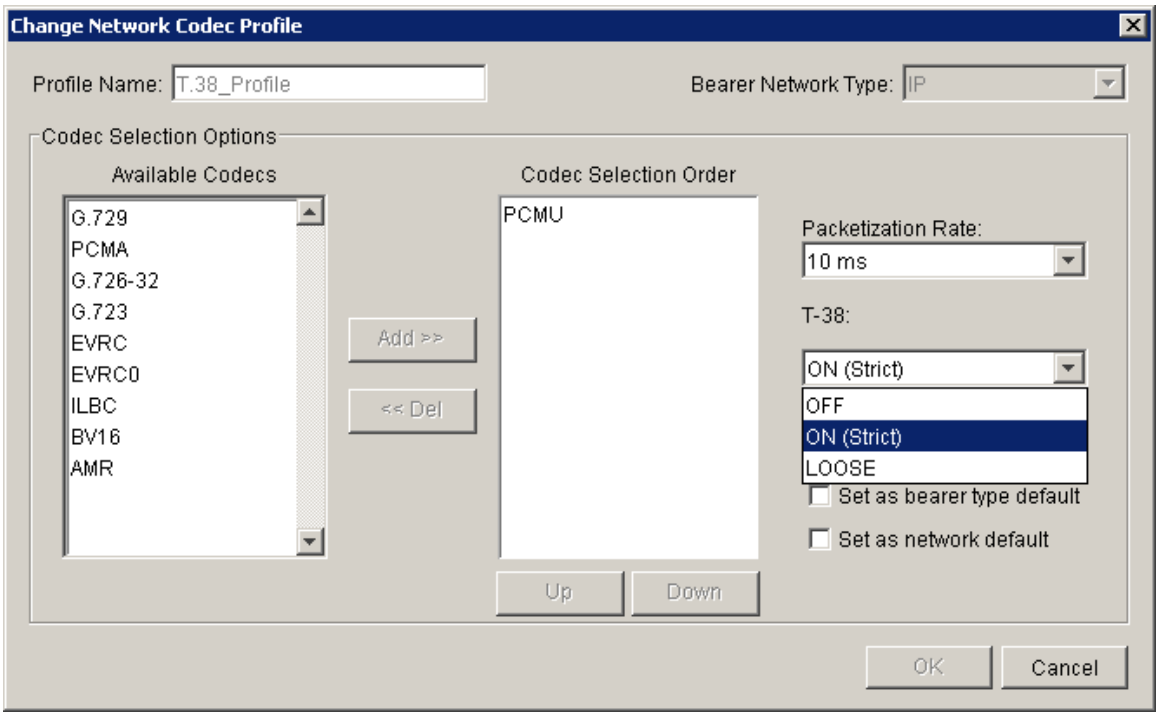
  Note: PacketCable GW's MUST advertise support for the FXR package in the Capabilities Audit response in order to use T.38.
- GWC load with all the feature related changes (including A00009294 and A00009443 content)

64.4.1 T.38 Provisioning from SESM

When adding a new network profile, the user could choose from one of three T.38 options currently provided on the CS2M GUI. The options are: “OFF, “ON (STRICT)”, and “LOOSE”. Prior to SN09 OFF was represented by disabled and ON(STRICT) was represented by enabled. The option “LOOSE” is used for packet cable. The figure below shows the T.38 options that the user may select from.

Figure one: Add network Codec Profile interface



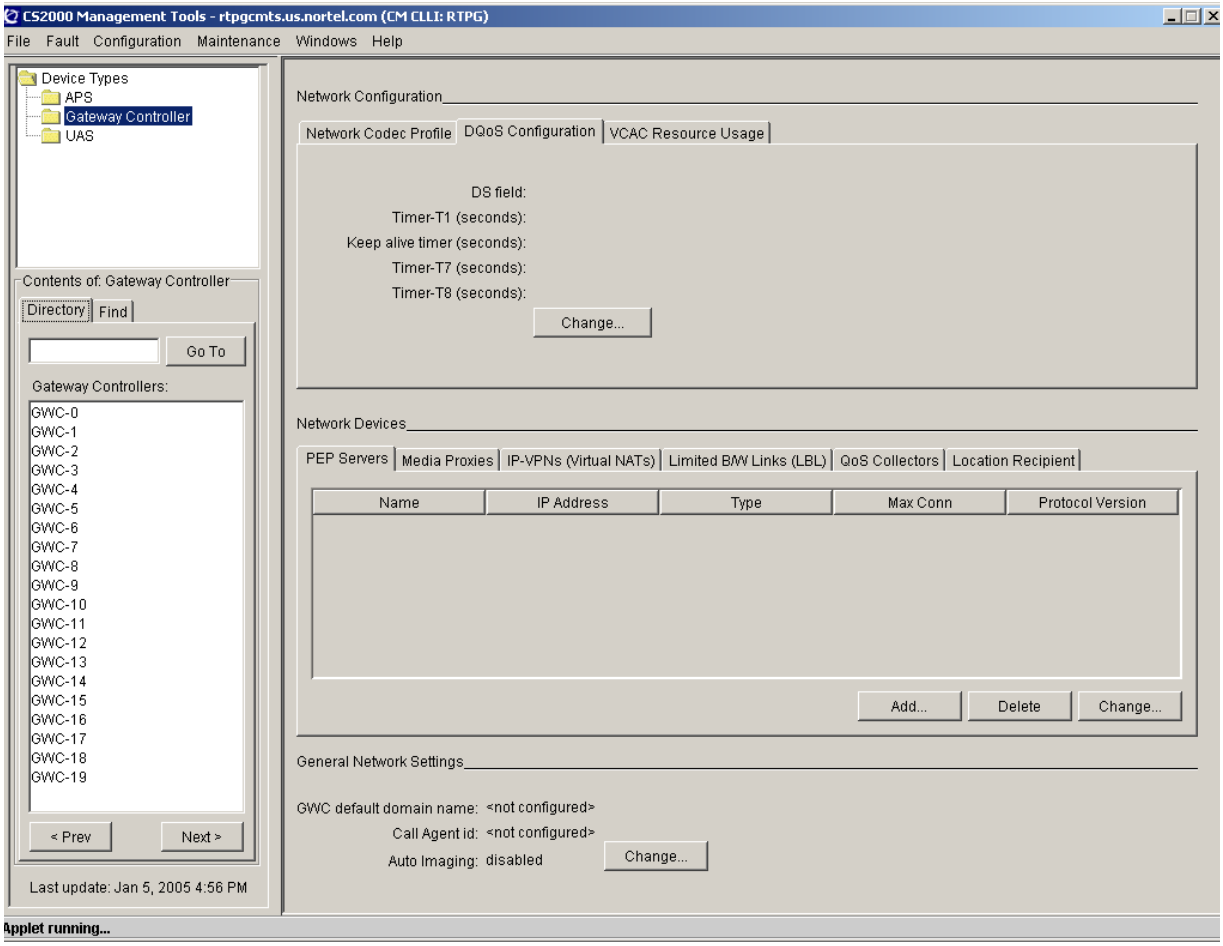


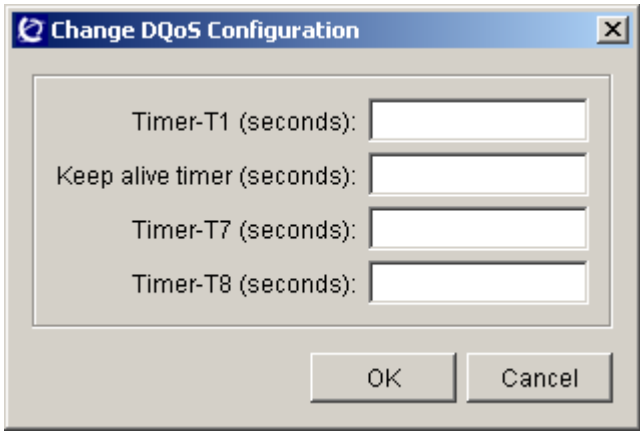
64.4.2 DSCP Provision in SESM

DS field is a fundamental value used for classification and marking of IP packets to achieve end-to-end QoS. This is a 8-bit value sent to CMTS from GWC via DQoS Signaling. This value will overwrite the TOS field in the IP header set by MTA. The media packet forwarding will then be prioritized according to the given DSCP, which is the most significant 6-bit value of the DS field. Prior to this feature, the DS field is hardcoded and set to 10111000 (184 in decimal) in SESM DQoS configuration GUI and it is displayed as “Expedited Fwding” after the user provisions the other DQoS values via “Change DQoS Configuration” dialog.

Figure 1 shows the DQoS configuration GUI display prior to this feature.

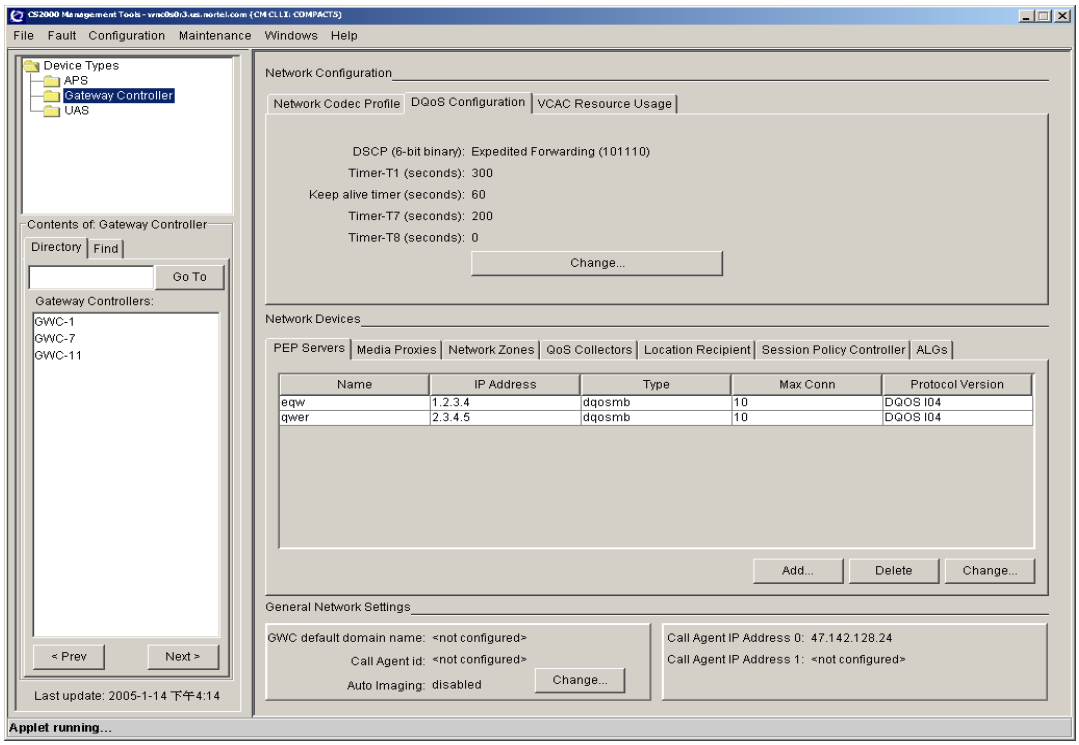
Figure 1 DQoS configuration GUI prior to this feature





Change from “DS field” to “DSCP (6-bit binary)” will be made to avoid any confusion between the 6-bit DSCP and an 8-bit DS Field value. On the “Change DQoS Configuration” dialog GUI, the “DSCP (6-bit binary)” field will be added. The pulldown menu containing predefined IP Service Class names will be provided for the selection (please refer to Table 1, “DiffServ Code Point Allocation,” on page 59). User could also input 6 binary stream. If the DSCP stream input is not one in the pulldown menu, the raw binary stream will be displayed.

Figure 2 Changed DQoS Configuration GUI



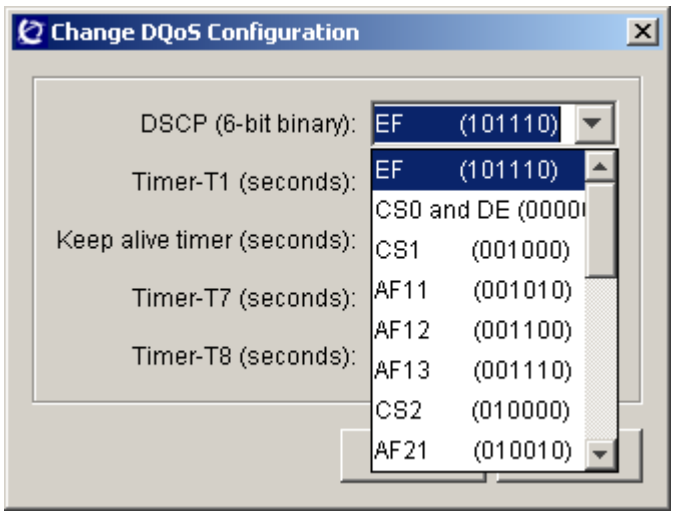


Table 1 DiffServ Code Point Allocation

DSCP	PHB	Status - Reference		DSCP	PHB	Status - Reference
000 000	CS0 and DE	RFC 2474		100 000	CS4	RFC 2474

Table 1 DiffServ Code Point Allocation

DSCP	PHB	Status - Reference		DSCP	PHB	Status - Reference
000 001	---	EXP/LU		100 001	---	EXP/LU
000 010	---	UASS		100 010	AF41	RFC 2597
000 011	---	EXP/LU		100 011	---	EXP/LU
000 100	---	UASS		100 100	FA42	RFC 2597
000 101	---	EXP/LU		100 101	---	EXP/LU
000 110	---	UASS		100 110	FA43	RFC 2597
000 111	---	EXP/LU		100 111	---	EXP/LU
001 000	CS1	RFC 2474		101 000	CS5	RFC 2474
001 001	---	EXP/LU		101 001	---	EXP/LU
001 010	AF11	RFC 2597		101 010	---	UASS
001 011	---	EXP/LU		101 011	---	EXP/LU
001 100	AF12	RFC 2597		101 100	---	UASS
001 101	---	EXP/LU		101 101	---	EXP/LU
001 110	AF13	RFC 2597		101 110	EF	RFC 2598
001 111	---	EXP/LU		101 111	---	EXP/LU
010 000	CS2	RFC 2474		110 000	CS6	RFC 2474
010 001	---	EXP/LU		110 001	---	EXP/LU
010 010	AF21	RFC 2597		110 010	---	UASS
010 011	---	EXP/LU		110 011	---	EXP/LU
010 100	AF22	RFC 2597		110 100	---	UASS
010 101	---	EXP/LU		110 101	---	EXP/LU
010 110	AF23	RFC 2597		110 110	---	UASS
010 111	---	EXP/LU		110 111	---	EXP/LU
011 000	CS3	RFC 2474		111 000	CS7	RFC 2474
011 001	---	EXP/LU		111 001	--	EXP/LU
011 010	AF31	RFC 2597		111 010	--	UASS
011 011	---	EXP/LU		111 011	--	EXP/LU

Table 1 DiffServ Code Point Allocation

DSCP	PHB	Status - Reference
011 100	AF32	RFC 2597
011 101	---	EXP/LU
011 110	AF33	RFC 2597
011 111	---	EXP/LU

DSCP	PHB	Status - Reference
111 100	--	UASS
111 101	--	EXP/LU
111 110	--	UASS
111 111	--	EXP/LU

This function has no impact to GWC because the DSCP value is converted to DS field (8-bit) by left-shift 2. This guarantees that bit 6 and 7 are set to zero.

64.5 Limitations and restrictions

In order to interworking with NGSS/SIP or SIPT, the NGSS software containing A00009443 content needs in place so that T.38 can be set properly. And for interworking with H.248 PVG, A00009294 GWC-related content is also required.

This feature will not support T.38 interworking with Gateways not included in the Cable Solution. This includes (but is not limited to) H.323 gateways, MGCP gateways, and other H.248-based gateways such as MG9K.

A PVG with a VSP3 card is required for T.38 interworking with PacketCable devices.

This feature will NOT support T.38 interworking with the IWSPM. G.711 will be used for all FAX calls involving the IWSPM.

This feature will only perform T.38 integration testing with Gateway vendors that can provide a T.38-capable load during the design phase of this feature. At the time of this FN, this only includes the Arris TTM. Currently, Motorola MTAs and Nuera Media Gateways are not planned for integration testing.

This feature will not make use of the fax tone "ft" or modem tone "mt" events in NCS or TGCP.

There is no impact to PacketCable Event Messaging due to T.38 behavior, with the exception of Electronic Surveillance. This feature will not support PacketCable 1.5 Electronic Surveillance, since there is other work required beyond the scope of this feature for full PC 1.5 ES compliance.
If the customer chooses to interwork with a Gateway (or SIP Client on the far end of a SIP trunk) that supports neither G.711 nor T.38, FAX calls will fail regardless of whether strict or loose mode is active.

T.38 functionality will not be supported for TGCP PTS trunks.

T.38 Annex D functionality is not supported between VRDN-based SIP Trunks and H.248 gateways (e.g. PVG). Therefore, if a PacketCable MTA/MG originates a call through a VRDN SIP trunk, terminating to a PVG, FAX calls will not be successful. This scenario will work with NGSS SIP trunks configured for T.38 support. Also, PacketCable MTA/MG to VRDN SIP to PacketCable MTA/MG calls will be supported using T.38.

64.6 Interactions

Not Identified.

64.7 Glossary

Term	Description
CS2K	Call Server 2000
CMTS	Cable Modem Termination System
MTA	Multimedia Terminal Adapter
GWC	Gateway Controller
MGC	Media Gateway Controller - refers to GWC/CS2K for trunks
PVG	Passport Packet Voice Gateway (Passport15000)
SDP	Session Description Protocol (IETF RFC 3266)
G3FE	Group 3 Facsimile Equipment G3FE refers to any entity which presents a communication interface conforming to ITU- T Recommendation T. 30, T. 4, and optionally T. 6. A G3FE may be a traditional G3 facsimile machine, an application with a T. 30 protocol engine or any other possibility mention in the network model for IP Facsimile mentioned in Recommendation T. 38.
SIP	Session Initiation Protocol (IETF RFC 3261)
SIP-T	Session Initiation Protocol - Telephony ITU-T based standard, that encapsulates ISUP messaging as payload within SIP messages.
UDP	User Datagram Protocol (IETF RFC 768)
UDPTL	Facsimile UDP Transport Layer protocol (ITU T.38)
CED	Called terminal identification answer tone of Fax device (2100 +/- 15 Hz, continuous tone, duration 2.6-4.0 sec.) see T.30 chapter 4.1

Term	Description
CNG	Calling tone of Fax device (1100 +/- 38 Hz, 0.5 sec. on, 3.0 sec. off, duration 60-120 sec.) see T.30 chapter 4.2.
V.21 Preamble	Series of flag sequences 01111110 for 1 sec +/- 15%.

65: Functional description (FN): A00009353

65.1 Feature name and Feature ID

A00009353 GWCUnit Availability/ Health Monitoring

65.2 Description

This feature addresses the prevention of GWC node outage caused by an improper SWACT to a GWC unit which appeared to be in good condition but was not.

This feature enhances the existing PreSwact audits and also create a new framework to monitor the health condition of the application resources like TAPI resource objects and Acceptor queues.

This feature will address the following:

1. Enhancement of the existing PreSwact audit.

2. Introduce a new alarm which will be raised whenever PreSwact audit fail.

65.2.1 Enhancement of the Existing PreSwact audit

Currently the PreSwact audit performs a set of checks to estimate the health of the inactive unit. This feature enhances the checks to consider additional fault conditions, such as

1. Datasync mismatch with the SESM
2. Invalid/Mismatch in some of GWC flash and GWC RAM data.
3. Application resource issues such as TAPI blocks (Transaction, Request and call)
4. Messaging resources (Acceptor queue on TAPI and Connection Broker).
5. Patching in progress in the inactive unit.However no alarm will be raised if the preSwact audit fails under this condition.

The PreSwact audit runs at a frequency of 40 seconds and with priority 6.

Swact force can still be used to force a manual warmswact when the preSwact audit fails and alarm raised.This existing functionality will not be changed.

65.2.2 New PreSwact alarm

This feature will introduce a new alarm which will be raised when ever PreSwact audit fails. An alarm will be raised with proper text which explains which component has led Preswact audit to fail. The PreSwact runs

periodically and raises alarm for PSA fail on error conditions.The specific problem displayed at the GWC level for the alarm raised will match with the swact failure reason at the SESM GUI.

65.2.2.1 Details of alarm

The details of the new alarm are as foll

Table 4: PreSwact Alarm details

Description	PreSwact Audit Failure
Severity or Level	Major
Category	QualityOfService
Probable Cause	resourceAtOrNearingCapacity
Component	NODEMTC
Specific Problem	Description about the component which caused the PreSwact audit failure.

Figure 1 Snap Shot of the Alarm Summary on GWC

```
ALARm> Print

==============================

 Alarms raised :
 Critical: 0  Major: 1  Minor: 0  Warning: 0

 AlarmTable length is : 1
 Critical: 0  Major: 1  Minor: 0  Warning: 0  Clear: 0
 Alarm raise/clear failures: 0

==============================

Print Alarm Element at index 1
-=-=-=
```

65.3 Hardware Requirements or Dependencies

None.

65.4 Software Requirements or Dependencies

None.

65.5 Limitations and restrictions

None

65.6 Interactions

This feature will interact with another activity A00009350 to get the health status of the flash data. An interface will be provided by the above activity for the preswact audit to query the status of flash-data.

65.7 Glossary

Table 5

Term	Description
EM	Element Manager
GWC	Gate Way Controller
PSA	PreSwact Audit
SWACT	Switch of Activity

66: Functional description (FN): A00009359

66.1 Feature name and Feature ID

A00009359 HW Intro of MCPN905 for Compact Call Agent

66.2 Description

66.2.1 Overview

This feature introduces the MCPN905-270 card for the Compact Call Agent application. The MCPN905 is being introduced to reduce recovery times on restarts as well as to increase overall capacity of the Compact Call Agent. It is expected the performance gain will be in the order of 1.6-1.7x faster than the MPCN765 card.

The MPCN765 card continues to be supported.

The MCPN905 is the next generation high performance hot swap CompactPCI Peripheral slot CPU board. It includes a new memory controller (MV64360) which is functionally equivalent to PMC280. .

As there is no persistent memory on the MCPN905 board, an 815 PrPMC has been added to the MPCN905 to add persistent memory. Each process running on the 905 that uses persistent memory accesses the memory on the 815 through the PCI bus.

66.2.2 Configuration

The MCPN905 card for the Compact Call Agent application is configured with the following:

- 815 PMC used for persistent memory
- Fiber Channel PMC used for Call Agent Sync
- 2.0 GB Memory

This configuration has been assigned the PEC code NTRX51HZ

A new transition module for the rear slot has the PEC code NTRX51HS.

66.2.3 Performance

The MCPN905 card for the Compact Call Agent application is being introduced for enhanced performance, specifically, call capacity and restart times.

Call Capacity: The expected performance gain is of the order of 1.6-1.7 x over the MPCN765 card. The committed BHCA capacity will be available at the First Customer Ship (FCS) timeframe.

Restart Times: Warm Restart times on the MCPN905 card will be less than 30 seconds. (It is expected that they will be less than 20 secs - to be confirmed).

66.2.4 Load naming convention

Due to differences between the MCPN765 and MCPN905, the ncgl cca loads are not binary compatible; a new platform load is introduced for the MCPN905 card. The load name is of the form:

- ncgl_cca_905_image_8.ww.rr.pp

In order to more clearly identify the loads, the load name for the MCPN765 card has been modified from the form:

- ncgl_cca_image_8.ww.rr.pp

to:

- ncgl_cca_765_image_8.ww.rr.pp

At the ccamtc map, sys level, the QryLD command shows the new loadnames, including the appropriate 765 or 905 indicator.

66.2.5 Load Delivery

For load delivery, the 905 cca load has been added to the existing RPM file

ncgl_cca_mc_images-8.ww-rr.pp.noarch.rpm

When the **platform_load_install.sh** script is used to install the RPM file, the mc and both 765 and 905 cca images are installed in the /swd/3pc directory on the bootp server.

66.2.6 Configuration of the 905 CCA card in the SAM21 EM GUI

Detection of the MCPN905-270 card version is done automatically in the EM when the card is inserted in the slot. After the card type is detected, the installer assigns the Call Agent service type.

On the Equip tab, the Card Type is shown as MCPN905, with a memory size of 2048.

The configuration data supplied at commissioning time is identical for the MCPN765 and MCPN905 cards with the exception of the load name. It is ncecessary to supply the correct 765 or 905 specific load name when setting the boot load name on the provisioning panel. Additionally, the Firmware version will appear different.

66.2.7 H/W Upgrades

In service upgrades of an office from an MCPN765 card to MCPN905 card is supported. The procedure uses the Norestartswact capability of the core to minimize the impact of the upgrade.

At a high level, the procedure is as follows:

- Drop Sync. Remove inactive CA card and transition module.
- Insert and commission new CA card and transition module. Run diagnostics.
- Boot new card (inactive). Soak.
- Perform onp/norestartswact procedure to switch activity to new card. Soak.
- Remove old CA card and transition module.
- Insert and commission new CA card and transition module. Run diagnostics.
- Boot new card. Soak.
- Sync.

Abort procedure is also provided .

This procedure is provided via Installation Method (IM).

66.3 Hardware Requirements or Dependencies

- MCPN905-270 card configured as above (PEC NTRX51HZ)

- MCPN905 compatible transition module (TM) (for rear slot) (PEC NTRX51HS)

66.4 Software Requirements or Dependencies

- NCGL_8 905 CCA load
- SN09 Shelf Controller and SAM21 Manager loads (including support for MCPN905 card)
- SN09 SOS (Callp Application) load

66.5 Limitations and restrictions

- Fiber Channel continues to be supported for sparing in SN09.
- For this release, the maximum amount of memory available for SOS (Callp Application) is the same as on the MCPN765 card.
- The MCPN765 and MCPN905 card versions cannot be mixed or synced except during the MCPN765 to MCPN905 upgrade procedure.
- An additional GigE port is available on the transition module, but is not used in this release.

66.6 Interactions

None.

66.7 Glossary

Term	Description
SC	Shelf Controller
CCA	Compact Call Agent
MC	Message Controller

67: Functional description (FN): A00009361

67.1 Feature name and Feature ID

A00009361 - CICM: Enhancement to IP Phone 2001 CICM client

67.2 Description

The IP Phone 2001 was introduced into the CICM portfolio of terminals in the SN07 CICM release in activity A00003951. The IP Phone 2001 was designed as a low cost alternative to the 2002 and 2004 terminals and with this cost reduction the IP Phone 2001 was designed without any feature keys.

The CICM supports the Centrex features and directory contacts by using the dedicated feature keys found on the IP Phone 2002 and 2004, however, with the 2001 not actually having any feature keys the approach was taken to provide a limited set of features using the 'Services Key' as a form of feature activation. The core provides the ability for terminals that do not support 'flash hooks' to use the 3WC or CXR features to trigger other features via * access codes. If 3wc/cxr was provisioned on the line that the 2001 terminal was connected to, the user could hit the 'services key' to perform a flash hook and dial the access code for the required feature.

The limitations in this approach meant that some of the features were not supported (a core restriction with using 3wc/cxr) and the user visible indications of the current state of the feature were not present, for example on the 2004 with Call Forward active you would have an icon next to the feature key showing its status, on the 2001 no sure indication was presented. This made the general ease of use not to the standard expected of an IP client.

The purpose of this feature is to provide a more manageable approach to feature interactions in the 2001 and emulations, such as the 2033.

67.3 Centrex Features on the IP Phone 2001 and emulations.

The real estate on the 2001 is limited and thus it is a challenge to provide the feature activation functionality that would put it on a par with the 2002 or 2004 terminals.

In previous terminal development on the CICM, an approach was adopted to limit the use of the soft keys. This was mainly driven by the lack of characters that can be assigned to a soft key and with CICM providing UI's for a number of nationalities this became an issue with regards to languages. The approach to limit the soft keys to just a small selection of Keywords (OK, Cancel, Menu, Yes, No, etc) was adopted. This leaves a number of the soft keys empty in a normal menu or call scenario.

On the IP Phone 200x, during idle state (and not active in a menu) only the far left hand soft key is used. This displays the option 'Menu' and provides the user with access to all the menus available.

For the IP Phone 2001 these soft keys will be used as feature keys, acting in the same manner as the features keys provided on the 2002/2004.

Feature Activation will also be made available to the user from an extra menu option,' Call Services' which has added to the main menu.

KEM features provisioned on the user's line will not be accessible to the 2001.

67.4 Assigning Features to Keys

Any features provisioned on the Users line will be made available to the user when they are logged into an IP Phone 2001 terminal. Two methods are available to the user for how these keys are assigned.

The first time a user logs into the IP Phone 2001, the softkeys will be automatically provisioned for them. The method for this provisioning is based on the numerical order of the feature keys on the core.

So for example if a user transfers from a 2004 to a 2001 for the first time, the features that the user has provisioned on features keys 2, 3 and 4 will be assigned to softkeys 2, 3 and 4.

Depending on the feature profile, more features may be automatically provisioned for the user. The following table provides an example of what the user may have provisioned and what they might expect when they log into the 2001 for the first time.

Key	Users features on a IP Phone 2004	Feature Profile	IP Phone 2001 Soft Key	Automatically provisioned on a IP Phone 2001
1	Three Way Call	Hide when Idle	1	Yes, Only displayed when the terminal is not idle.
2	Call Forward	Hide when Active	1	Yes, Only displayed when Terminal is Idle
3	Make Set Busy	Hide when Active	2	Yes, Only displayed when Terminal is Idle
4	Busy Override	Hide when Idle	2	Yes, Only displayed when the terminal is not idle.
5	Ring Again	Never Hide	3	Yes, This is displayed in both idle and no idle states
6	Call Waiting	Never Hide	NONE	All three soft keys are now allocated; this feature is not automatically provisioned.

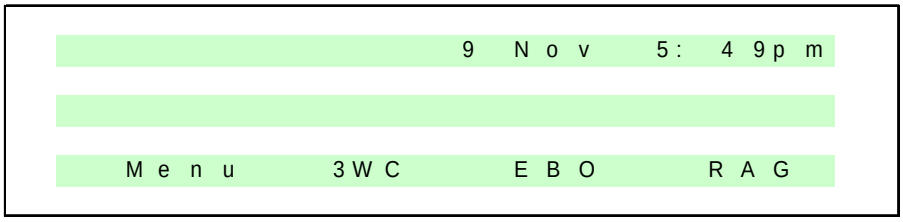
If all the feature profiles were set to never, only features assigned to keys 1, 2 and 3 would be automatically provisioned.

From the automatic provisioning described above the user does not have a dedicated key for Call Waiting. If the user feels that they use the feature more than one of the features that has been automatically provisioned then they can change the feature assignment manually on the terminal itself.

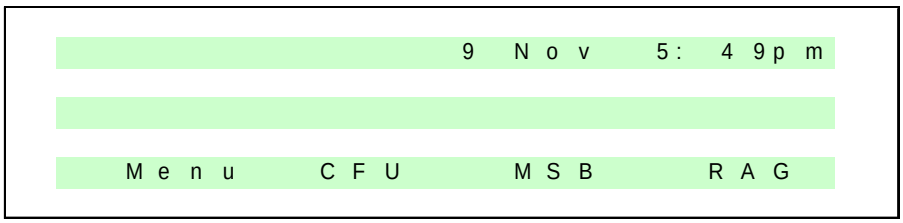
The new ‘Call Services’ menu will present the entire list of features that the user has assigned. From here they can either activate a feature by selecting it from the menu, or reassign it to one of the soft keys, this provides an interface suitable to them.

Using the example above, if the user wishes to allocate Call waiting to soft key 3, because they feel they use that feature more than Ring Again, then they may do so. If they wished to allocate Call waiting to key 1 then they will be replacing both 3WC and Call Forward, this is because the Call Waiting feature profile is set to never hide and is displayed when idle and non idle.

The following is an example of how the terminal will look based on the automatically configured softkeys from the users line configuration previously mentioned.



When a terminal transitions to an idle state, the ‘display when idle’ features will be available.

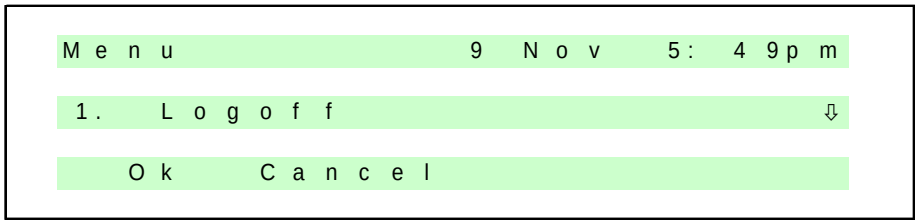


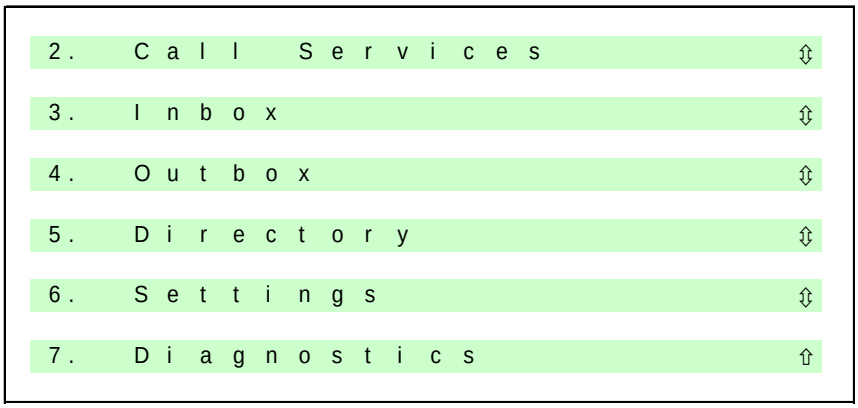
When assigning features the user will be prompted for confirmation, this confirmation will also display any features that will be unassigned from the soft key.

All this mapping will be transparent to the user, so when they log back into a 2004 terminal the keys will be displayed in their original assignment. Any subsequent times that the user logs into the 2001 will present the keys in the format that the user last used them. Only on the first time that the user connects to a 2001 will the automatic allocation occur.

67.5 Menu Map

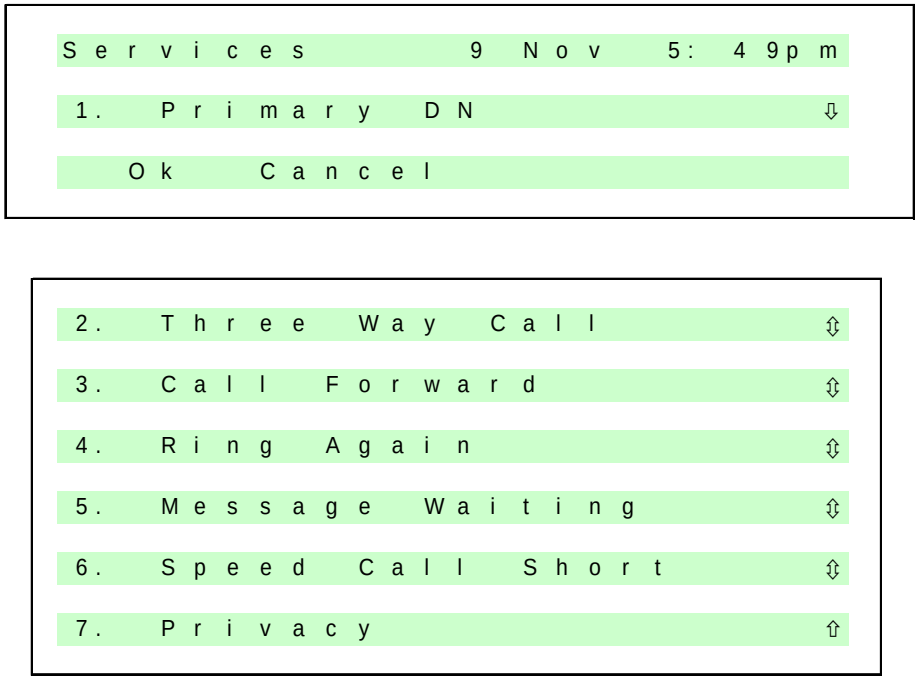
The following screen representations show what will be presented to the user when logging on to a gateway, and navigating the feature allocation menus of the i2001





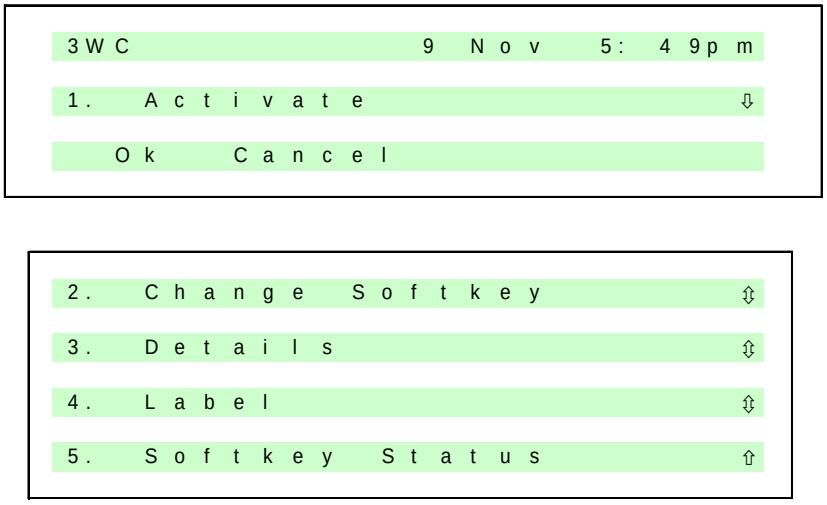
67.5.1 Call Services Menu:

Presents a list of the Features assigned on the user's line, this user has 7 features assigned; this is in the order in which they would be displayed on a 2004/2002 terminal.

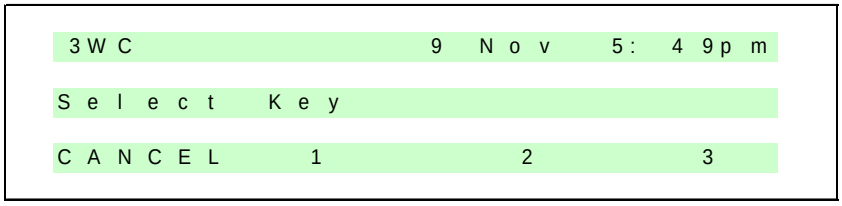


67.5.2 Assign / Activate Menu:

When Highlighting a feature from the list and selecting OK the user will be presented with a further menu. From here they can manually activate the feature or assign it to one of the soft keys.

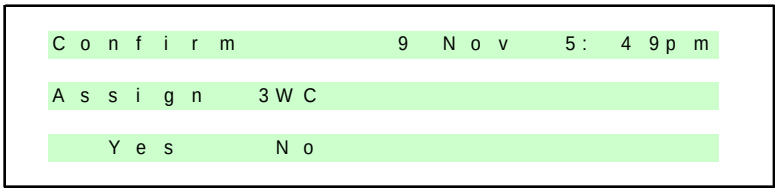


When assigning a feature to a soft key the user will be presented with the following screen.

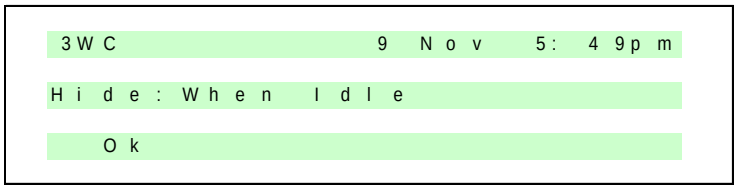


The user would then press the key that they wish to assign the feature to and a confirmation screen will be presented to the user.

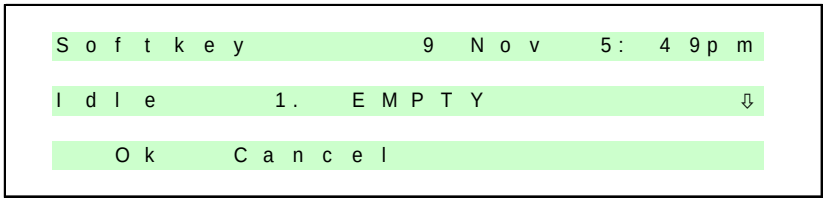
In the following example we are assigning three way call to soft key 1, when no features are currently assigned. So the user is just prompted with a confirm message.

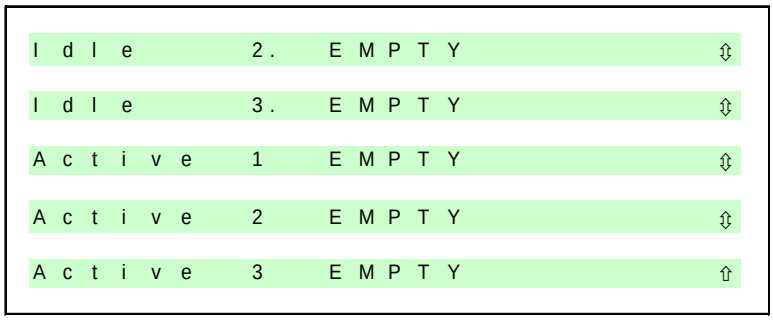


When selecting the Details option, the details of the feature are displayed to the user.

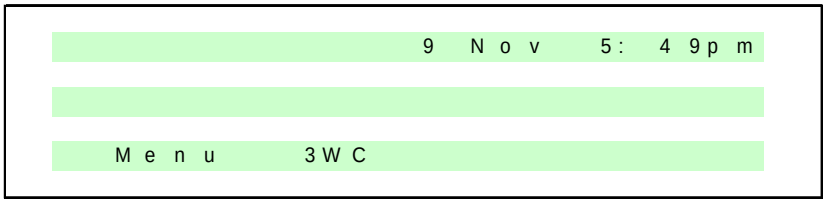


When selecting the Soft key Status, the following will be displayed.





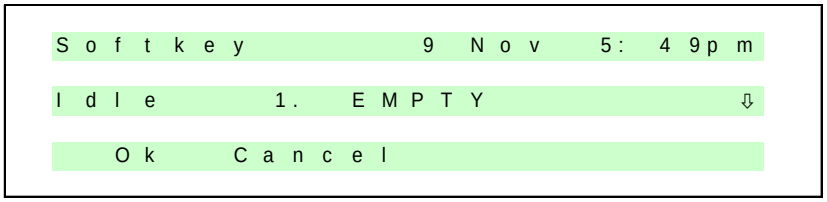
The list of currently assigned features is Empty. The user selecting ‘Yes’ to the assignment would result in 3WC being assigned to soft key 1 when the terminal is not idle

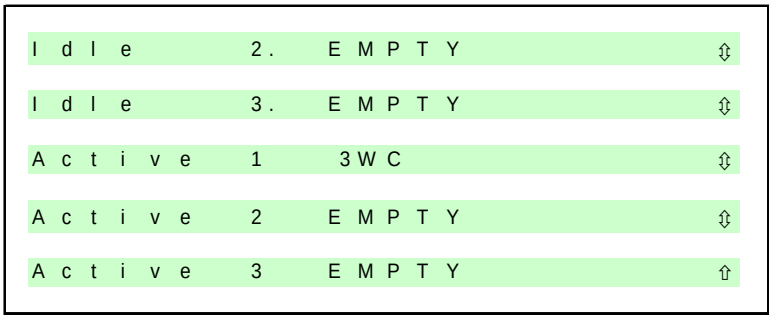


The users feature assignment would then look like this.

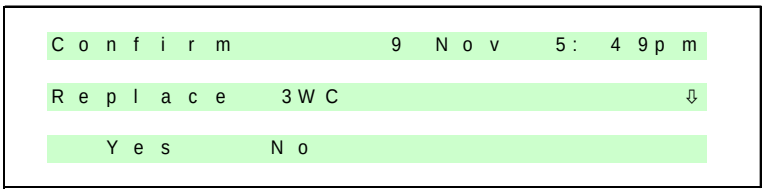
Key	Users features on a IP Phone 2004	Feature Profile	IP Phone 2001 Soft Key
1	Three Way Call	Hide when Idle	1
2	Call Forward	Hide when Active	None
3	Make Set Busy	Hide when Active	None
4	Busy Override	Hide when Idle	None
5	Ring Again	Never Hide	None
6	Call Waiting	Hide when idle	None

The soft key status page would now resemble.





If the user decides to replace 3WC with Call Waiting (Hide when idle) the confirmation would include the 3WC feature in the list of Currently Assigned features.

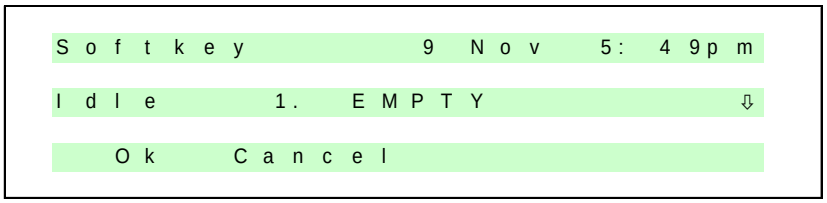


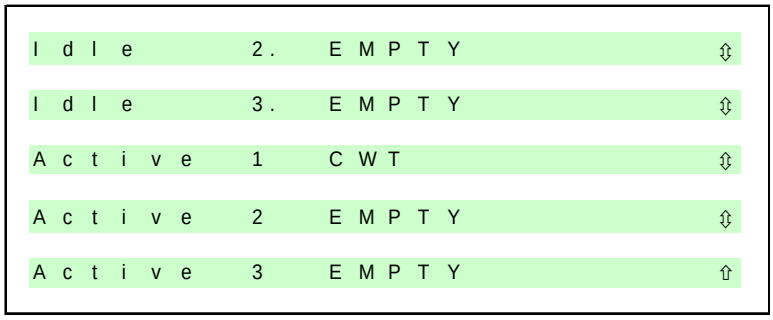
The users feature assignment would then look like this.

Key	Users features on a IP Phone 2004	Feature Profile	IP Phone 2001 Soft Key
1	Three Way Call	Hide when Idle	None
2	Call Forward	Hide when Active	None
3	Make Set Busy	Hide when Active	None
4	Busy Override	Hide when Idle	None
5	Ring Again	Never Hide	None

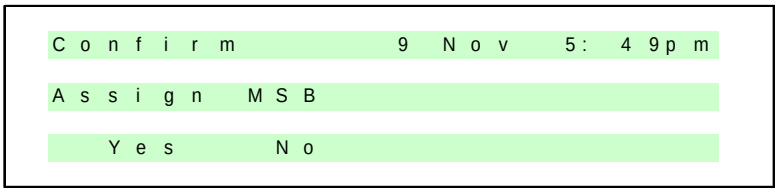
6	Call Waiting	Hide When Idle	1

The soft key status page would now resemble.

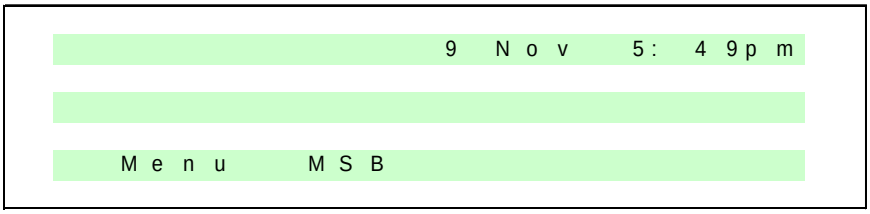




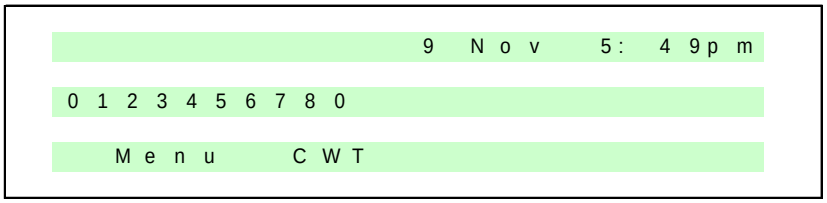
The user then wishes to assign Make Set Busy to Key 1 as well, Make Set Busy is configured as a Hide when DN is not idle feature, so it can be assigned to Key 1 without effecting any features already configured (only Call Waiting is assigned and because it is hidden when the feature is idle, there theoretically is a key available).



The list of currently assigned features to an idle soft key 1is Empty. The user selecting ‘Yes’ here would result in MSB being assigned to soft key 1 when the terminal is idle.



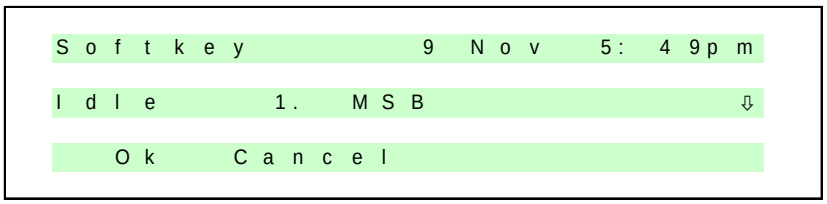
But still display Call Waiting when we are in a non idle state.

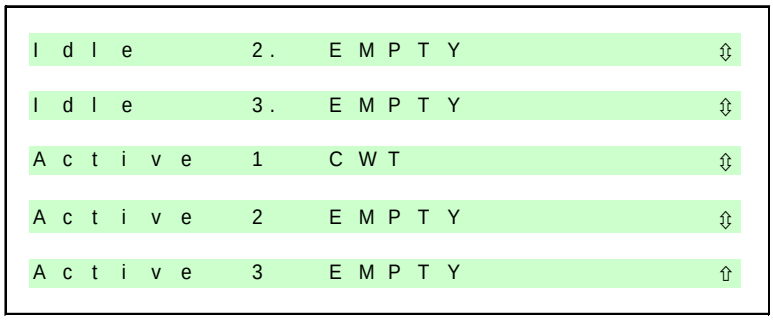


The users feature assignment would then look like this.

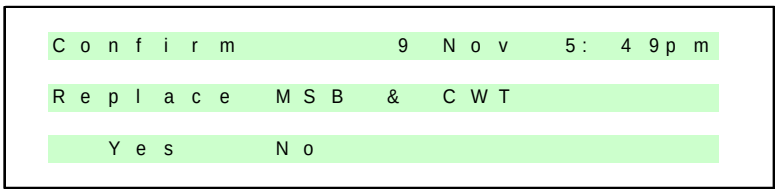
Key	Users features on a IP Phone 2004	Feature Profile	IP Phone 2001 Soft Key
1	Three Way Call	Hide when Idle	None
2	Call Forward	Hide when Active	None
3	Make Set Busy	Hide when Active	1 (shown when idle)
4	Busy Override	Hide when Idle	None
5	Secondary DN	Never Hide	None
6	Call Waiting	Hide When Idle	1 (shown when not idle)

The soft key status page would now resemble.

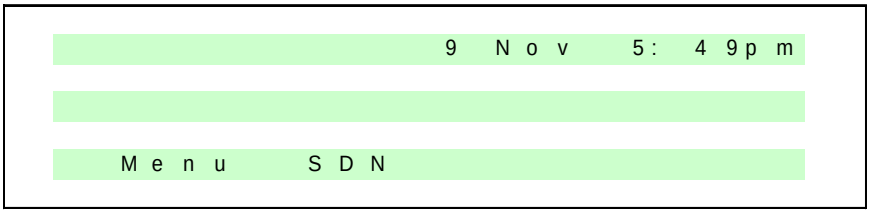




Now if the user wishes to assign a never hide feature, such as a secondary DN to soft key 1 they will be replacing Make Set Busy and Call Waiting.



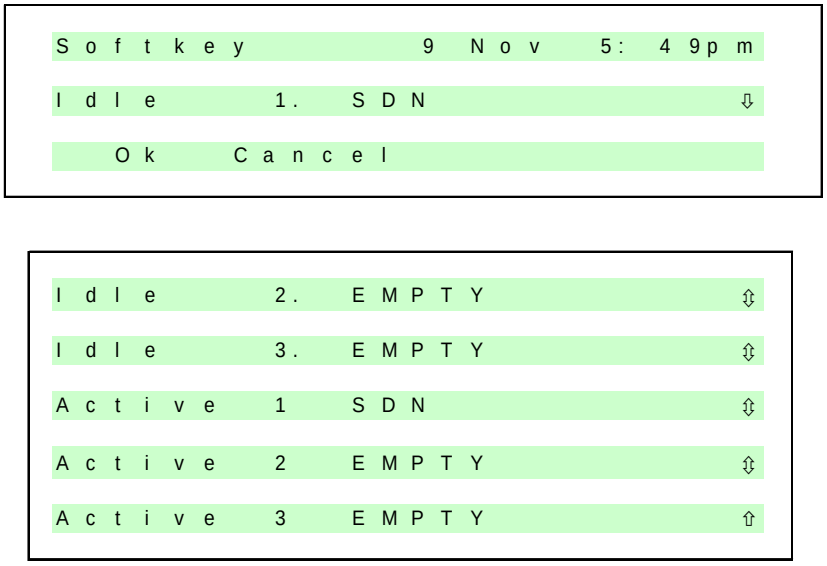
The fact that the secondary directory number feature is never to be hidden means that it will replace both the features assigned to key 1. Upon confirmation the user would see the following when idle and not idle.



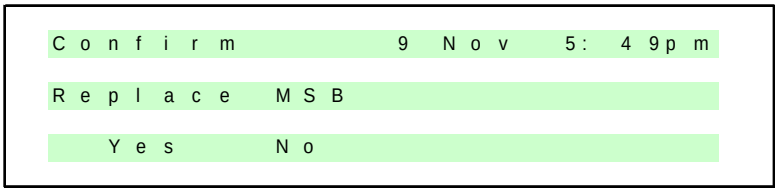
The users feature assignment would then look like this.

Key	Users features on a IP Phone 2004	Feature Profile	IP Phone 2001 Soft Key
1	Three Way Call	Hide when Idle	None
2	Call Forward	Hide when Active	None
3	Make Set Busy	Hide when Active	None
4	Busy Override	Hide when Idle	None
5	Secondary DN	Never Hide	1 (shown in both idle and non idle states)
6	Call Waiting	Hide When Idle	None

The soft key status page would now resemble.



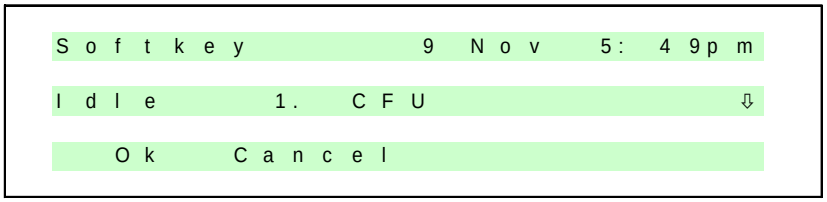
Alternatively, if the user wishes to replace MSB with another hide when not idle feature, only MSB will be replaced and not both assigned features. In this example CFU is being assigned to Key 1

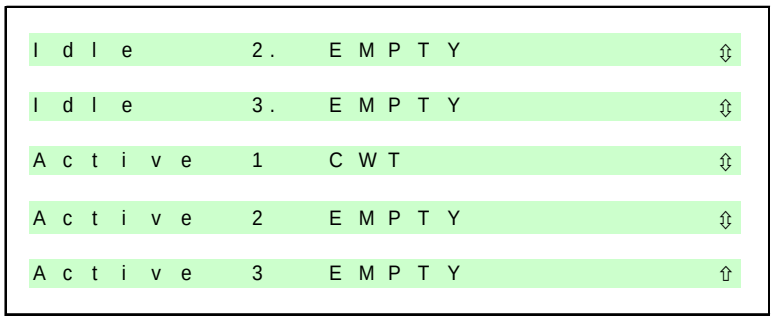


The users feature assignment would then look like this.

Key	Users features on a IP Phone 2004	Feature Profile	IP Phone 2001 Soft Key
1	Three Way Call	Hide when Idle	None
2	Call Forward	Hide when Active	1 (shown when idle)
3	Make Set Busy	Hide when Active	None
4	Busy Override	Hide when Idle	None
5	Secondary DN	Never Hide	None
6	Call Waiting	Hide When Idle	1 (shown when not idle)

The soft key status page would now resemble.



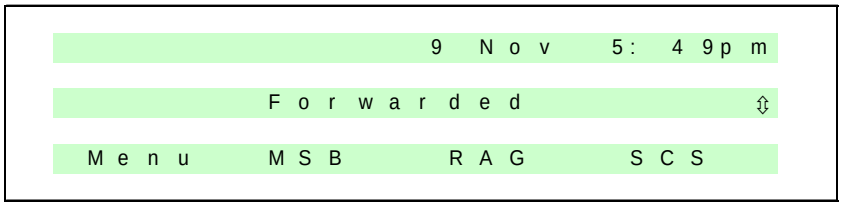


67.5.3 Feature Indication in the Call Services Menu / Terminal Display:

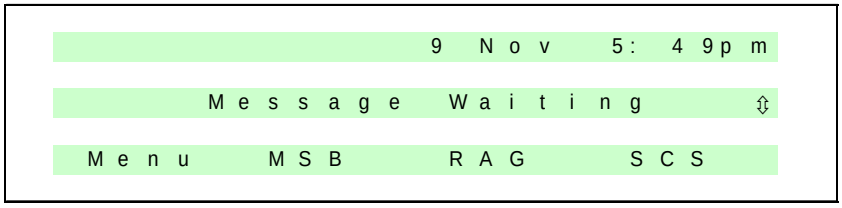
Features can also be activated via the menu system without necessarily having a dedicated softkey assigned; the status of the features will be indicated by a Message being displayed on the terminal when idle as well as an icon being placed next to the features name in the Call Services Menu

For features that are active on the terminal when the set is idle the user would use the navigational up and down arrows on the terminal to scroll through the list of features active.

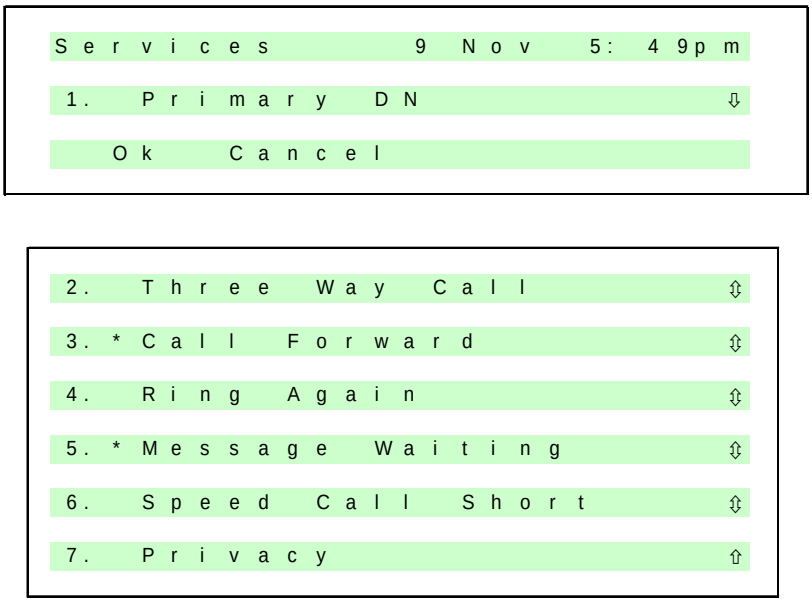
For example: This terminal has no feature keys assigned but Call Forward and Message Waiting are both active.



Then by pressing up or down on the navigational buttons it would display the next active feature in the list.



Alternatively, the Call Services Menu would also indicate their status.

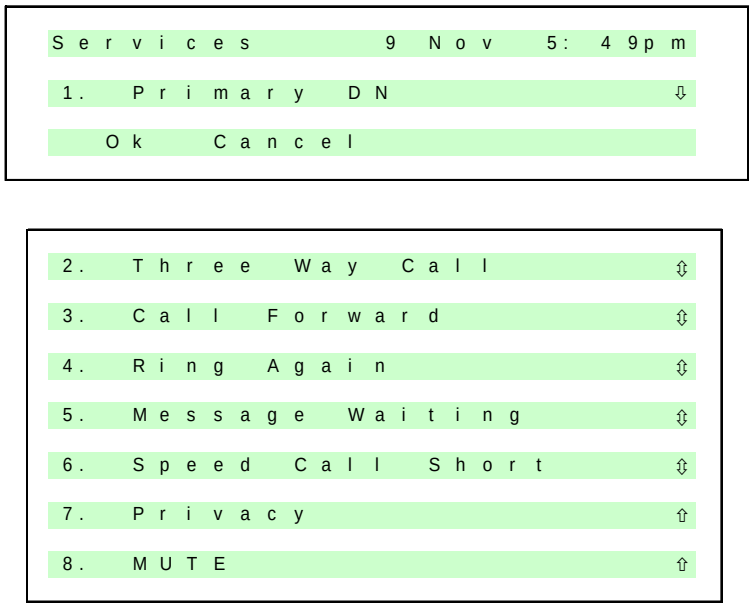


67.5.4 IP Phone 2001 MUTE functionality:

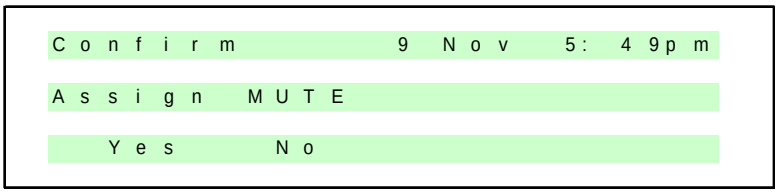
The IP Phone 2001 does not have a physical mute button, although the 2001 does not have an external microphone its necessary to provide such functionality when active in a call on the handset.

Mute is only applicable in a non idle state and can be assigned to any of the soft keys in the same manner as the Centrex features.

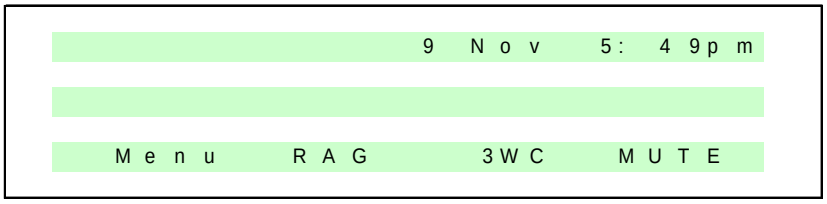
Independent of the features provisioned on the terminal the MUTE option will be displayed in the Call Services menu at the bottom of the list.



Select and assign the MUTE option in the same method as described earlier. This will occupy a Non idle soft key space, overwriting any current configuration on that key.



When assigned the MUTE button will be displayed against the relevant soft key.



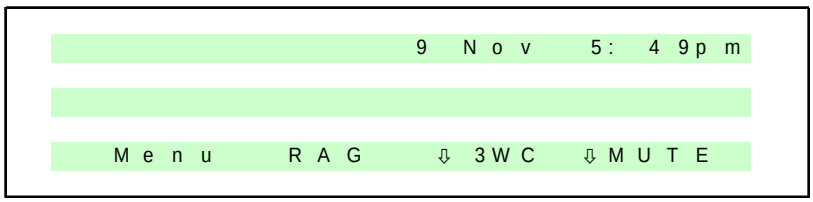
The IP Phone 2033 does actually have a physical mute button, where the majority of the functionality introduced by this feature is also applicable to the 2033, the mute option will not be displayed.

67.5.5 Indication of feature state on the Soft keys:

In the D91 phase 2 firmware stream we currently do not have the ability to perform reverse video on the softkey labels. A development activity is being discussed to provide this functionality with the firmware development team. Until the method for reverse video to be displayed on the terminals softkey is available we will be providing an alternative.

An Icon will be placed next to the Feature label on the softkey to provide a visual indication of the features state.

Currently an active feature will be represented by the following:

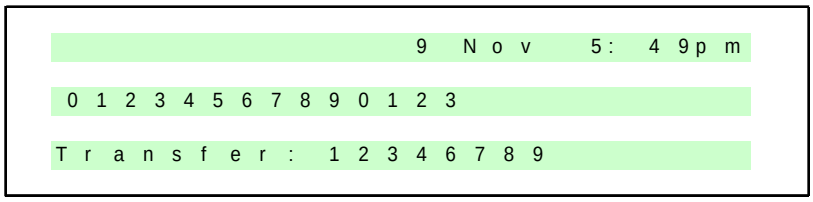


In this example the 3WC and the Mute functionality is activated. This extra icon occupies one character on the soft keys label. The result of this means that the text in the label will be moved one space to the right. When the label exceeds 4 characters and the feature is activated the label will be truncated and an ellipsis will be appended.

On the 2002 and 2004's feature keys icons are used to represent the stages that the features are in, usually by flashing the icon during provisioning. Its not possible to provide any form of flashing on the labels above the soft keys, so the tri states that features can be involved (on, off and provisioning) in is not represented The feature is either on (activated or provisioning) or off.

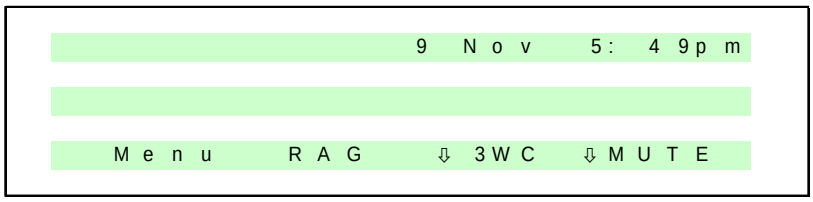
67.5.6 Displaying the soft key labels during a call:

When active on a call, the 2001 clears the two display lines and leaves the context line present. This is to enable the user to see the incoming DN, dialed digits, transfer details, etc. With these occupying the screen the soft keys are no longer visible.



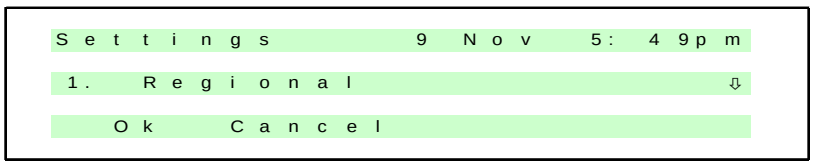
A timer is started while the labels are not visible on an incoming or outgoing call, after a set duration the labels will appear again.

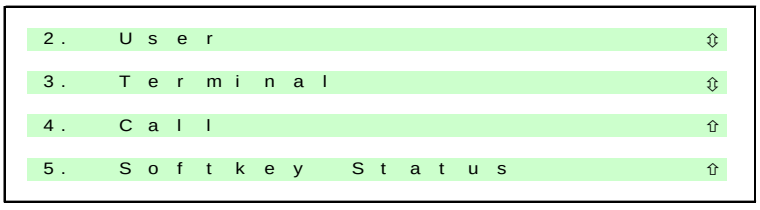
The soft key labels can be removed from the display at any time by pressing the ‘services key’. While hidden pressing the ‘services key’ will present the labels back onto the screen. The timer is not started when the user manually hides the soft key labels, only when active on a call.



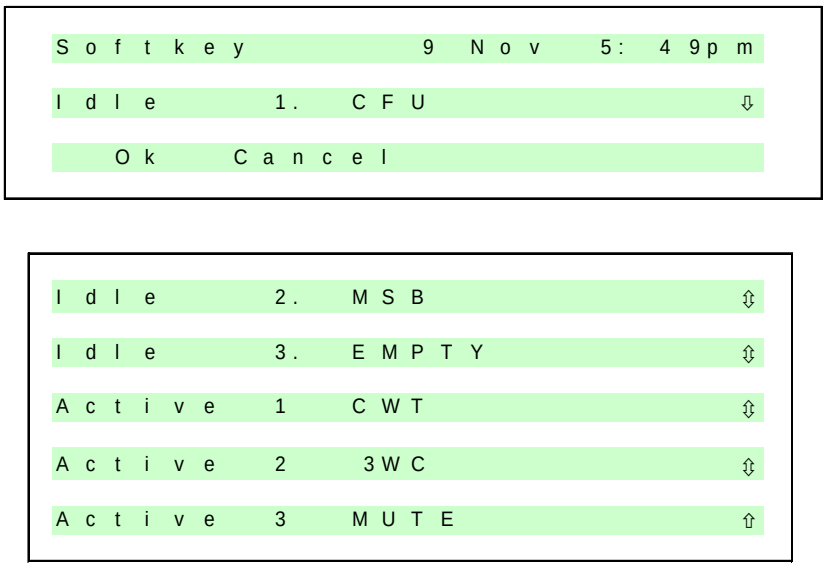
67.5.7 Displaying the configured soft keys:

The list of provisioned soft keys can be obtained by either selecting the Soft key Status while provisioning a feature or via the Settings menu located on the main menu.





Selecting option 5 will present the same information as during provisioning.



67.5.8 2033 compatibility:

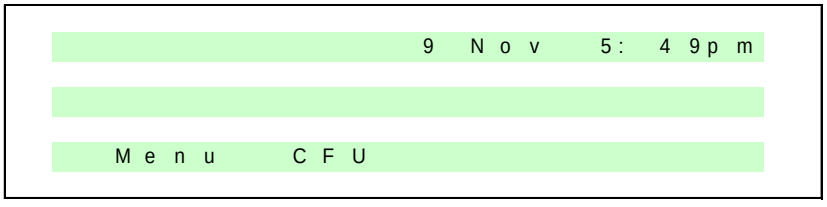
The functionality introduced by this feature is also intended for the 2033 conference phone.

Where the soft key driven functionality on the 2001 is distributed across 4 soft keys, the 2033 only has 3 but provides a ‘more’ option on the far right soft key.

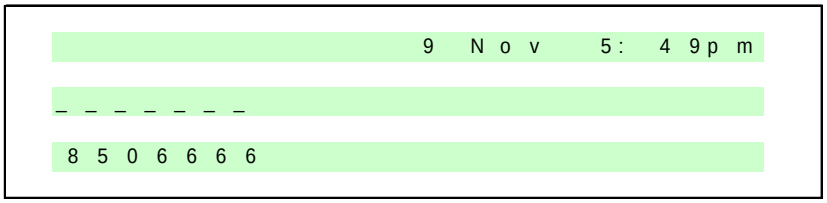
The normal display would consist of soft keys 1, 2 and more, selecting the more key will display soft keys 3, 4 and more. Selecting more this time will return to keys 1 and 2.

67.5.9 Example feature activation: Call Forward

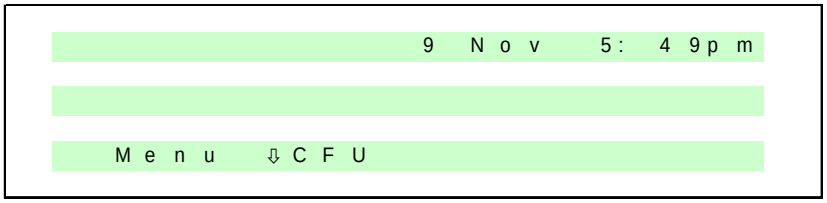
With Call Forward assign to soft key 1 and the terminal idle the user would press soft key 1.



The screen would prompt the user for the forwarding digits clearing the display of the soft keys labels. The user would enter the DN they wish to be forwarded to

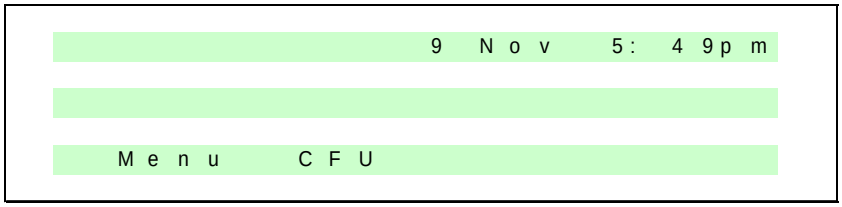


The user could then either press the service key to present the soft key labels again, or just press the soft key itself to confirm the operation.



After confirmation the terminal will place an icon next to the CFU key to indicate that its status is on.

Pressing the soft key again will return the CFU status back to off.



67.6 Feature Labels

The string interpretation for the features are available in long and short form, in Appendix A we list the features that currently have strings available on the CICM, in most cases the short form version of the feature is too long to fit in the soft keys structure. The 2001 can provide 6 characters per soft key but for aesthetics we try to use 5 for the first 3 keys and 6 for the last key, to ensure that we provide a gap between keys. The suggested soft key label will be new additions to the language strings and used as the representation for the features

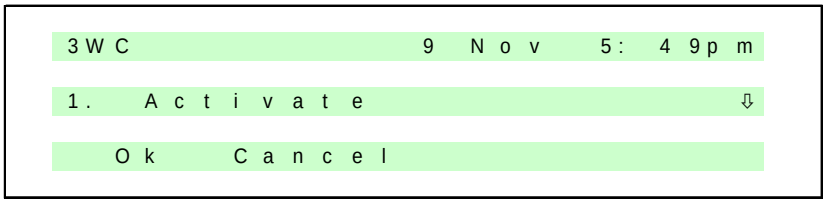
on the soft keys. Where possible the string has been limited to 5 characters but it's not possible for each feature.

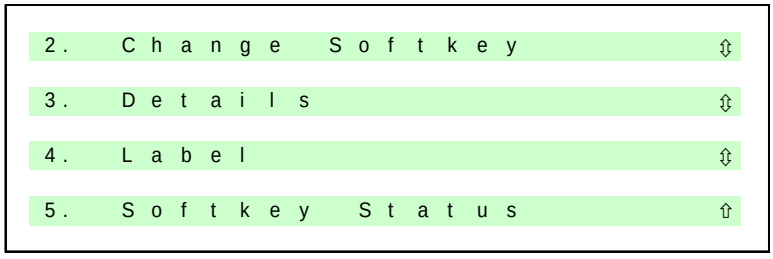
See Appendix A for details of each counties default labels.

67.7 Labeling the Softkeys

The user has the ability to re-label the soft key associated with a feature replacing the default label associated with that feature.

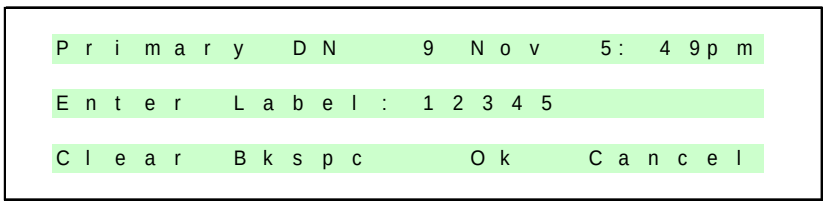
To re-label a feature the user should select the feature from the Call Services menu and select option 4 – Label.



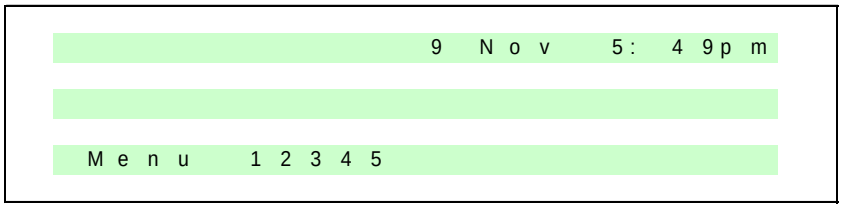


This will prompt the user to enter the label that they wish to be associated with that specific feature; all the alpha numeric characters are available including symbols.

The user is limited to entering only 5 characters.



In this example the user has assigned the numbers 12345 to their Primary DN, if the Primary DN is assigned to soft key 1 then this is how it will appear.



Use the Symbol key to enter special characters

When entering text into the soft key label the full character set is available. Each number on the key pad (except 1) has a range of symbols associated with it. Press the Symbols soft key after the keypad to obtain the special characters available.

Key 1 - Nothing

Key 2 - AÀÁÂÃÄÅÆBCÇaàáâãäåæbcç2

Key 3 - DEÈÉÊËFdeèéêëf3

Key 4 - GHIÌÍÎÏghìíîï4

Key 5 - JKLjkl5

Key 6 - MNÑOÒÓÔÕÖØmnñoòóôõöø6

Key 7 - PQRSpqrs7

Key 8 - TUÙÚÛÜVtuùúûüv8

Key 9 - WXYÝÞßZwxyýþÿz9

Key # - !"#$%&'()*+,-./0123456

67.8 Auto Labeling the Directory Numbers.

The auto propagation will not automatically assign Primary or Secondary DN's to soft keys, if the user wishes to assign a DN key to a soft key, the user should follow procedures detailed in this document.

When a DN key is assigned for the first time to a soft key, the label associated with that key will be the last 4 digits of the user DN which is configured via OSSGate.

This can then be relabeled if required by the user.

67.9 Element Manager

The Element Manager has no knowledge of a specific users soft key feature association.

67.10 Hardware Requirements or Dependencies

The IP phone 2001 is the main hardware requirement, however, for certain aspects of this feature there is a dependency on the terminals firmware. In the D91 phase 2 firmware we do not currently have the ability to Reverse Video the display above the terminals softkeys. Alternatives are presented in this FN for how we will display feature indication to the user.

Details of request to the firmware team will be documented in the Limitations and Restrictions section.

67.11 Software Requirements or Dependencies

The new firmware requirements as described earlier in the document are required.

67.12 Limitations and restrictions

The lack of the terminals firmware supporting:

- Reverse Video on soft keys.
- Context Line being used as a standard display line
- Bitmap downloading, as an alternative to using the icon or the reverse video we could send predefined bitmaps to the terminal to display. The 2001 has a fully bit mapped display but currently the Unistim protocol does not support it.
- Soft key Highlighting, as another alternative.

Configuration Limitation.

- The only supported method for provisioning LEN's and Users is via OSSGate and flow through provisioning. This ensures that all the users feature association on the CS2K and the CICM is in sync. Flow through provisioning will automatically create a label for the users DN keys and associate the correct features to keys. The Element Manager provides the ability to apply features to keys on the user’s line, but should only be used as a means to amend any inconsistencies that occurred during creation.
- No Predefined Assignments will be available; the automatic configuration will be used for the 1st time when connecting to 2001. Configuration changes will be stored and used from then on.
- The Auto configuration option is not configurable.

Possible Future Enhancements:

- Template Soft key Profiles.

67.13 Interactions

This feature has interactions with the original i2001 feature and the 2033 features from previous CICM releases,

67.14 Glossary

Term	Description
New term	definition

67.15 Appendix A: Language Strings

67.15.1 UK and US Default Soft key Labels

Feature Name	Default Softkey Label	Indication displayed when feature active and not assigned to a key.	Description
Forward	Fwd	Forwarded	Forward
Msg Wait	MsgWt	Message Waiting On	Message Waiting' short feature name
Transfer	Xfr	Call Transfer On	Call Transfer' short feature name
Ring Again	Rag	Ring Again On	Ring Again' short (and long) feature name
Speed Call	Scl	Speed Call Short On	Speed Call' short (and long) feature name
Primary DN	PDN	Primary DN On	The Most important DN. Usually assigned to feature key 1.
Time&Date	Qtd	Time and Date On	The 'Time and Date' short (and long) feature name
Agent	Agent	Agent Incalls On	Agent In calls' short feature name
DN	Dn	Directory Number On	Directory Number' short feature name
Make Busy	Busy	Busy Active	Make Set Busy' short feature name
3 Way Call	3wc	Three Way Call On	3 Way Call' short feature name
Dir. Park	DcPk	Directed Call Park On	Directed Call Park' short feature name
Not Ready	NtRdy	Agent Not Ready	Agent Not Ready' short feature name. This feature is part of the ACD family of features.
Emergency	Emerg	Emergency Active	Emergency' short (and long) feature name. This feature is part of the ACD family of features.
Supervisor	SpvIn	Supervisor Incalls On	Supervisor Incalls' short feature name. This feature is part of the ACD family of features.
Call Super	Supv	Call Supervisor On	Call Supervisor' short feature name. This feature is part of the ACD family of features.
Ans. Emerg	EmAns	Emergency Answer On	Answer Emergency' short feature name. This feature is part of the ACD family of features
Ans. Agent	AgnAns	Agent Answer Active	Answer Agent' short feature name. This feature is part of the ACD family of features.

Agent Stat	AgnSta	Agent Status On	Agent Status' short feature name. This feature is part of the ACD family of features.
Obs. Agent	AgObsv	Observe Agent On	Observe Agent' short feature name. This feature is part of the ACD family of features.
Conference	6wc	6 Party Conference	6 Party Conference' short feature name
Autodial	ADial	Automatic Dialing	Autodial' short (and long) feature name. To automatically dial the phone. Abbreviation for Automatic Dialing
Park	Park	Call Park Active	Call Park' short feature name.
Unknown	Unknwn	Unknown Feature On	This catch all feature is used when a feature is present on the feature key, but does not have its own assigned entry in this list.
Fast Xfer	Fxr	Fast Transfer On	Fast Transfer' short feature name.
Pickup	Cpu	Call Pickup Active	Call Pickup' short feature name.
Intercom	Icom	Intercom Active	Intercom (Business sets)' short (and long) feature name.
Call Wait.	Wait	Call Waiting	Call Waiting' short feature name
QryBusyStn	QBS	Query Busy Station On	Query Busy Station' short feature name.
AgtSummary	DASK	Display Agent Summary	Display Agent Summary' short feature name. This feature is part of the ACD family of features to display the summary of an agent's activities.
Q Status	DQS	Display Queue Status	Display Queue Status' short feature name. This feature is part of the ACD family of features and is used to display the status of the ACD queue.
QThreshold	DQT	Display Queue Threshold	Display Queue Threshold' short feature name. This feature is part of the ACD family of features and is used to display the threshold of the ACD queue.
FrcAgAvail	FAA	Force Availability On	Force Agent Availability' short feature name. This feature is part of the ACD family of features and is used by the supervisor to force the agent into becoming available.
Ctrl IFlow	Cif	Controlled Interflow	Controlled Interflow' short feature name. This feature is part of the ACD family of features.
SupNgtServ	NgtSrv	Night Service On	Supervisor Control of Night Service' short feature name. This feature is part of the ACD family of features.
Line Bus	Lob	Line of Business	Line of Business' short feature name. This feature is part of the ACD family of features.
Call Agent	Cag	Call Agent Active	Call Agent' short (and long) feature name. This feature is part of the ACD family of features.
Call Force	Force	Call Force Active	Call Agent with Call Forcing option. This feature is part of the ACD family of features.
ACB	Acb	Automatic Call Back	Automatic Call Back
BLF	Blf	Busy Lamp Field On	Busy Lamp Field
Call Back	Ccbs	Call Completion On	Call Completion To Busy Subscriber
CustTrace	Cot	Originated Trace On	Customer Originated Trace
CWD	Cwd	Dial Call Waiting	Dial Call Waiting
EMW	ExMw	Executive Msg Waiting	Executive Message Waiting
Inspect	Insp	Calling Name Inspect	Calling Name Inspect Key
LVM	Lvm	Leave Message Active	Leave Message
MCH	Mch	Malicious Call Hold	Malicious Call Hold
MRFM	MADNRF	MADN Active	Multiple Appearance Directory Number Ring Forward

MsgWaitInd	MwInd	Message Waiting Ind	Message Waiting Indication
MsgWaitQry	MwQry	Message Waiting Query	Message Waiting Query
PRL	Prel	Privacy Release On	Privacy Release
Privacy	Priv	Privacy Active	Privacy
SpdCalShrt	Scs	Speed Calling Short	Speed Calling Short List
SLQ	SLQ	Single Line Queuing	Single Line Queuing
UCD Login	Login	UCD Login Active	Uniform Call Distribution Login
MakeBusyI	MSBI	Make Set Busy Intra On	Make Set Busy Intragroup
GIC	GIC	Group Intercom Active	Group Intercom
GIAC	GIAC	Group Intercom All On	Group Intercom All Calls
Quick Conf	QCK	Quick Conference On	Quick Conference Key
Subcom	Subcom	Sub Community Active	Sub Community routing for Emergency Calls
AutoAnswer	AAB	Auto Answer Back On	Auto Answer Back
CallCover	Ccv	Call Covering Active	Call Covering
BsyOveride	Ebo	Executive Busy Override	Executive Busy Override
SupAgnDN	SAgnDN	Incalls (SupAgntDN) On	ACD Incalls (Sup + Agent + DN)
SupAgnPDN	SAgnPDN	Incalls (SupAgntPDN) On	ACD Incalls (Sup + Agent + PDN)
SupPDN	SupPDN	Incalls (Sup + PDN) On	ACD Incalls (Sup + PDN)
AgentPDN	AgPDN	Incalls (Agnt + PDN) On	ACD INCALLS (Agent + PDN)
CFK	CFK	Call Forwarding (Key)	Call Forwarding On A Per Key Basis
MBSCAMP	Camp	Station Camp On	Meridian Business Set Station Camp On
SBLF	SBLF	Set Based Lamp Field	Set Based Lamp Field

67.16 French Default Soft key Labels

Feature Name	Default Softkey Label	Indication displayed when feature active and not assigned to a key.	Description
Forward	Rnvoie	Renvoie	Forward
Msg Wait	EnAttn	Msg en attente	Message Waiting' short feature name
Transfer	Trns	Appel sur renvoie	Call Transfer' short feature name
Ring Again	Rappel	Comp. même num. actif	Ring Again' short (and long) feature name
Speed Call	ComAbr	Appel abbrègé actif	Speed Call' short (and long) feature name
Primary DN	PDN	Numéro principal actif	The Most important DN. Usually assigned to feature key 1.
Time&Date	Heure	Heure et Date actif	The 'Time and Date' short (and long) feature name
Agent	Agent	Appel pour agent actif	Agent In calls' short feature name
DN	DN	DN actif	Directory Number' short feature name
Make Busy	Occup.	Service Occupé actif	Make Set Busy' short feature name
3 Way Call	Conf3	Appel conférence actif	3 Way Call' short feature name

Dir. Park	GarDir	Garer appel dir. actif	Directed Call Park' short feature name
Not Ready	PasPrt	Agent pas prêt actif	Agent Not Ready' short feature name. This feature is part of the ACD family of features.
Emergency	Urgenc	Service d'urgence actif	Emergency' short (and long) feature name. This feature is part of the ACD family of features.
Supervisor	Supv.	Agent superviseur actif	Supervisor Incalls' short feature name. This feature is part of the ACD family of features.
Call Super	TelSup	Appellez superv. actif	Call Supervisor' short feature name. This feature is part of the ACD family of features.
Ans. Emerg	RepUrg	Rep. d'urgence actif	Answer Emergency' short feature name. This feature is part of the ACD family of features
Ans. Agent	RepAgt	Rep. agent ACD actif	Answer Agent' short feature name. This feature is part of the ACD family of features.
Agent Stat	SomAgt	Status d'agent actif	Agent Status' short feature name. This feature is part of the ACD family of features.
Obs. Agent	Obsv	Agent Observateur actif	Observe Agent' short feature name. This feature is part of the ACD family of features.
Conference	Conf6	Appel conférence à 6	6 Party Conference' short feature name
Autodial	CmpAut	Composition automatique	Autodial' short (and long) feature name. To automatically dial the phone. Abbreviation for Automatic Dialing
Park	Garer	Garer appel actif	Call Park' short feature name.
Unknown	Incnnu	Service Inconnue actif	This catch all feature is used when a feature is present on the feature key, but does not have its own assigned entry in this list.
Fast Xfer	TrnRpd	Transfer rapide actif	Fast Transfer' short feature name.
Pickup	RepAut	Rép appel d'autre actif	Call Pickup' short feature name.
Intercom	Intcom	Intercom actif	Intercom (Business sets)' short (and long) feature name.
Call Wait.	AppAtt	Appel en attente	Call Waiting' short feature name
QryBusyStn	Interg	Inter.du poste actif	Query Busy Station' short feature name.
AgtSummary	SomAgt	Sommaire de l'agent	Display Agent Summary' short feature name. This feature is part of the ACD family of features to display the summary of an agent's activities.
Q Status	F.Attn	Sommaire file d'attente	Display Queue Status' short feature name. This feature is part of the ACD family of features and is used to display the status of the ACD queue.
QThreshold	S.Attn	Seuil file d'attente	Display Queue Threshold' short feature name. This feature is part of the ACD family of features and is used to display the threshold of the ACD queue.
FrcAgAvail	Dispon	Forcer dispon. actif	Force Agent Availability' short feature name. This feature is part of the ACD family of features and is used by the supervisor to force the agent into becoming available.
Ctrl IFlow	GstCnt	Gestion controllé	Controlled Interflow' short feature name. This feature is part of the ACD family of features.
SupNgtServ	SvNuit	Service de nuit actif	Supervisor Control of Night Service' short feature name. This feature is part of the ACD family of features.
Line Bus	Dept	Departement	Line of Business' short feature name. This feature is part of the ACD family of features.

Call Agent	AgACD	Agent ACD est actif	Call Agent' short (and long) feature name. This feature is part of the ACD family of features.
Call Force	Forcer	Appel Forcer actif	Call Agent with Call Forcing option. This feature is part of the ACD family of features.
ACB	RpAuto	Rappel automatique	Automatic Call Back
BLF	VyOccp	Voyant d'occup. actif	Busy Lamp Field
Call Back	CmpApp	Completer l'appel actif	Call Completion To Busy Subscriber
CustTrace	ApMalv	appel malveillant actif	Customer Originated Trace
CWD	AtnDir	Appel att. Dirigé	Dial Call Waiting
EMW	AtnExe	Msg en attente executif	Executive Message Waiting
Inspect	InspNm	Verif du nom d'appel	Calling Name Inspect Key
LVM	LszMsg	Laisser Message actif	Leave Message
MCH	CnMalv	Cntl appel malveillant	Malicious Call Hold
MRFM	NAMU	NAMU actif	Multiple Appearance Directory Number Ring Forward
MsgWaitInd	IndAtt	Indic. Msg en attente	Message Waiting Indication
MsgWaitQry	VrfAtt	Verif Msg en attente	Message Waiting Query
PRL	DésPrv	Désengager appel privé	Privacy Release
Privacy	Privé	Appel Privé actif	Privacy
SpdCalShrt	CmpAbr	Comp. abrégée mini	Speed Calling Short List
SLQ	FdAttn	File d' attente	Single Line Queuing
UCD Login	Login	UCD Login	Uniform Call Distribution Login
MakeBusyI	Intra	Appel intra seulement	Make Set Busy Intragroup
GIC	Intcom	Intercom Groupe actif	Group Intercom
GIAC	IntcmT	Intercom Groupe Tous	Group Intercom All Calls
Quick Conf	CnfRpd	conférence rapide actif	Quick Conference Key
Subcom	TelUrg	Tel. d' urgence actif	Sub Community routing for Emergency Calls
AutoAnswer	RepAut	Réponse Automatique	Auto Answer Back
CallCover	Couvr	Couvrage actif	Call Covering
BsyOveride	PrioEx	Priorité Exécutif	Executive Busy Override
SupAgnDN	SAgnDN	ACD Agent, Supv., DN	ACD Incalls (Sup + Agent + DN)
SupAgnPDN	SAgnPDN	ACD Agent, Supv., PDN	ACD Incalls (Sup + Agent + PDN)
SupPDN	SupPDN	ACD Supv, PDN	ACD Incalls (Sup + PDN)
AgentPDN	AgPDN	ACD Agent, PDN	ACD INCALLS (Agent + PDN)
CFK	TchRen	Touche Renvoie d'appel	Call Forwarding On A Per Key Basis
MBSCAMP	Camp	Camper actif	Meridian Business Set Station Camp On
SBLF	VytTel	Voyant pour telephone	Set Based Lamp Field

67.17 German Default Soft key Labels

Feature Name	Default Softkey Label	Indication displayed when feature active and not assigned to a key.	Description
Forward	UML	Rufumleitung	Forward

Msg Wait	NchWrt	Nachricht wartet EIN	Message Waiting' short feature name
Transfer	WtrVrb	Weiterverbinden> EIN	Call Transfer' short feature name
Ring Again	Rckruf	Rückruf EIN	Ring Again' short (and long) feature name
Speed Call	KrzWhl	Kurzwahl EIN	Speed Call' short (and long) feature name
Primary DN	HptNr	Hauptnummer EIN	The Most important DN. Usually assigned to feature key 1.
Time&Date	Zt+Dat	Zeit und Datum EIN	The 'Time and Date' short (and long) feature name
Agent	Agent	Agent Ankommend EIN	Agent In calls' short feature name
DN	Dn		Directory Number' short feature name
Make Busy	Bstzt	Besetzt Aktiv	Make Set Busy' short feature name
3 Way Call	3-Konf	Dreierkonferenz EIN	3 Way Call' short feature name
Dir. Park	Parken	Gespräch Parken EIN	Directed Call Park' short feature name
Not Ready	AgtNAk	Agent nicht bereit	Agent Not Ready' short feature name. This feature is part of the ACD family of features.
Emergency	NotAkt	Notsituation Aktiv	Emergency' short (and long) feature name. This feature is part of the ACD family of features.
Supervisor	SpvAnk	Supervisor Ankom.d EIN	Supervisor Incalls' short feature name. This feature is part of the ACD family of features.
Call Super	SpvGeh	Anruf zu Supervisor EIN	Call Supervisor' short feature name. This feature is part of the ACD family of features.
Ans. Emerg	NotAtw	Notsituat.n Antwort EIN	Answer Emergency' short feature name. This feature is part of the ACD family of features
Ans. Agent	AgtAtw	Agent Antwort Aktiv	Answer Agent' short feature name. This feature is part of the ACD family of features.
Agent Stat	AgtSta	Agent Status EIN	Agent Status' short feature name. This feature is part of the ACD family of features.
Obs. Agent	AgtÜbw	Agent Überwachen EIN	Observe Agent' short feature name. This feature is part of the ACD family of features.
Conference	6-Konf	Sechserkonferenz	6 Party Conference' short feature name
Autodial	AutDl	Automatische Wahl	Autodial' short (and long) feature name. To automatically dial the phone. Abbreviation for Automatic Dialing
Park	GspPrk	Gespräch Parken Aktiv	Call Park' short feature name.
Unknown	UbekLM	Unbekanntes LM EIN	This catch all feature is used when a feature is present on the feature key, but does not have its own assigned entry in this list.
Fast Xfer	WtrVrb	Weiterverbinden>> EIN	Fast Transfer' short feature name.
Pickup	GspÜbn	Gespräch übernehmen EIN	Call Pickup' short feature name.
Intercom	Gegspr	Gegensprechanlage Aktiv	Intercom (Business sets)' short (and long) feature name.
Call Wait.	Ankl	Anklopfen	Call Waiting' short feature name
QryBusyStn	BzApAb	Bes. Apparat abfr. EIN	Query Busy Station' short feature name.
AgtSummary	AgtZus	Zusfsg.f.Agent anzgn	Display Agent Summary' short feature name. This feature is part of the ACD family of features to display the summary of an agent's activities.
Q Status	WrtSt	Wartschl.Status anzgn	Display Queue Status' short feature name. This feature is part of the ACD family of features and is used to display the status of the ACD queue.

QThreshold	WrtSw	Wartschl.Schwelle anzgn	Display Queue Threshold' short feature name. This feature is part of the ACD family of features and is used to display the threshold of the ACD queue.
FrcAgAvail	VfgErz	Verfügbkt erzwingen EIN	Force Agent Availability' short feature name. This feature is part of the ACD family of features and is used by the supervisor to force the agent into becoming available.
Ctrl IFlow		??	Controlled Interflow' short feature name. This feature is part of the ACD family of features.
SupNgtServ	NchMod	Nachtmodus EIN	Supervisor Control of Night Service' short feature name. This feature is part of the ACD family of features.
Line Bus	GesBR	Geschäftsbereich	Line of Business' short feature name. This feature is part of the ACD family of features.
Call Agent		??	Call Agent' short (and long) feature name. This feature is part of the ACD family of features.
Call Force		??	Call Agent with Call Forcing option. This feature is part of the ACD family of features.
ACB	AutRrf	Autom. Rückruf	Automatic Call Back
BLF	AnzBes	Anzeige für Besetzt EIN	Busy Lamp Field
Call Back	AnrBnd	Anruf Beenden EIN	Call Completion To Busy Subscriber
CustTrace	VerfAn	Verfolgung ankom.EIN	Customer Originated Trace
CWD	AnrWrt	Anruf warten wählen	Dial Call Waiting
EMW	WNR	Wichtige Nachr. Wartet	Executive Message Waiting
Inspect	NamDAR	Name d.Anrufers ansehen	Calling Name Inspect Key
LVM	NchAkt	Nachricht Aktiv lassen	Leave Message
MCH	BösHlt	Böswilligen Anr. halten	Malicious Call Hold
MRFM	MADNAk	MADN Aktiv	Multiple Appearance Directory Number Ring Forward
MsgWaitInd	AnzNch	Anzeige f.wart.Nachr.	Message Waiting Indication
MsgWaitQry	NchWrt	Wart.Nachr.abfragen	Message Waiting Query
PRL	??	??	Privacy Release
Privacy	??	??	Privacy
SpdCalShrt	KrzWhl	Kurzwahl	Speed Calling Short List
SLQ	??	??	Single Line Queuing
UCD Login	UCDAnm	UCD Anmelden Aktiv	Uniform Call Distribution Login
MakeBusyI	BesInt	Besetzt Intern EIN	Make Set Busy Intragroup
GIC	GGspr	Gruppengegenspr Akt	Group Intercom
GIAC	GGsprA	Gruppenggnspr alle Akt	Group Intercom All Calls
Quick Conf	AdHKnf	Ad-hoc Konferenz EIN	Quick Conference Key
Subcom	SubCom	Untergruppen Aktiv	Sub Community routing for Emergency Calls
AutoAnswer	AutRrf	Autom. Rückantwort Akt.	Auto Answer Back
CallCover	GsprSi	Gesprächsabsicherg Akt.	Call Covering
BsyOveride		??	Executive Busy Override
SupAgnDN		??	ACD Incalls (Sup + Agent + DN)
SupAgnPDN		??	ACD Incalls (Sup + Agent + PDN)
SupPDN		??	ACD Incalls (Sup + PDN)
AgentPDN		??	ACD INCALLS (Agent + PDN)
CFK	UML(T)	Rufumleitung(Taste)	Call Forwarding On A Per Key Basis

MBSCAMP		??	Meridian Business Set Station Camp On
SBLF		??	Set Based Lamp Field

67.18 Portuguese Default Soft key Labels

Feature Name	Default Softkey Label	Indication displayed when feature active and not assigned to a key.	Description
Forward	Fwd	Direccionado	Forward
Msg Wait	MsgWt	Mensagem em Espera	Message Waiting' short feature name
Transfer	Xfr	Transf. de Chamada ON	Call Transfer' short feature name
Ring Again	Rag	Toque Repetido ON	Ring Again' short (and long) feature name
Speed Call	Scl	Chamada rápida ON	Speed Call' short (and long) feature name
Primary DN	PDN	DN primário ON	The Most important DN. Usually assigned to feature key 1.
Time&Date	Qtd	Data e Hora ON	The 'Time and Date' short (and long) feature name
Agent	Agent	Chamadas de Agent ON	Agent In calls' short feature name
DN	Dn	Lista telefonica ON	Directory Number' short feature name
Make Busy	Busy	Ocupado activado	Make Set Busy' short feature name
3 Way Call	3wc	Chamada 3 vias ON	3 Way Call' short feature name
Dir. Park	DcPk	Parqueamento chamada ON	Directed Call Park' short feature name
Not Ready	NtRdy	Agente não disponível	Agent Not Ready' short feature name. This feature is part of the ACD family of features.
Emergency	Emerg	Emergência activada	Emergency' short (and long) feature name. This feature is part of the ACD family of features.
Supervisor	SpvIn	Chmd. do supervisor ON	Supervisor Incalls' short feature name. This feature is part of the ACD family of features.
Call Super	Supv	Chamar supervisor ON	Call Supervisor' short feature name. This feature is part of the ACD family of features.
Ans. Emerg	EmAns	Atender emergencia ON	Answer Emergency' short feature name. This feature is part of the ACD family of features
Ans. Agent	AgnAns	Atender Agente activo	Answer Agent' short feature name. This feature is part of the ACD family of features.
Agent Stat	AgnSta	Estado do Agente ON	Agent Status' short feature name. This feature is part of the ACD family of features.
Obs. Agent	AgObsv	Observar Agente ON	Observe Agent' short feature name. This feature is part of the ACD family of features.
Conference	6wc	Conferencia a 6	6 Party Conference' short feature name
Autodial	ADial	Marcação automática	Autodial' short (and long) feature name. To automatically dial the phone. Abbreviation for Automatic Dialing
Park	Park	Parqu. de chmds activo	Call Park' short feature name.
Unknown	Unknwn	Função desconhecida ON	This catch all feature is used when a feature is present on the feature key, but does not have its own assigned entry in this list.
Fast Xfer	Fxr	Transf. Rápida ON	Fast Transfer' short feature name.
Pickup	Cpu	Atender chamada activa	Call Pickup' short feature name.

Intercom	Icom	Intercom Activa	Intercom (Business sets)' short (and long) feature name.
Call Wait.	Wait	Chamada em espera	Call Waiting' short feature name
QryBusyStn	QBS	Questionar Est.Ocup. ON	Query Busy Station' short feature name.
AgtSummary	DASK	Mostrar Estado do Agent	Display Agent Summary' short feature name. This feature is part of the ACD family of features to display the summary of an agent's activities.
Q Status	DQS	Mostrar estado Fila	Display Queue Status' short feature name. This feature is part of the ACD family of features and is used to display the status of the ACD queue.
QThreshold	DQT	Mostrar Limite da Fila	Display Queue Threshold' short feature name. This feature is part of the ACD family of features and is used to display the threshold of the ACD queue.
FrcAgAvail	FAA	Forçar disponibil. ON	Force Agent Availability' short feature name. This feature is part of the ACD family of features and is used by the supervisor to force the agent into becoming available.
Ctrl IFlow	Cif	Fluxo controlado	Controlled Interflow' short feature name. This feature is part of the ACD family of features.
SupNgtServ	NgtSrv	Serviço nocturno ON	Supervisor Control of Night Service' short feature name. This feature is part of the ACD family of features.
Line Bus	Lob	Linha de negócio	Line of Business' short feature name. This feature is part of the ACD family of features.
Call Agent	Cag	Chmd de agente Activa	Call Agent' short (and long) feature name. This feature is part of the ACD family of features.
Call Force	Force	Chmd forçada activa	Call Agent with Call Forcing option. This feature is part of the ACD family of features.
ACB	Acb	Rechamada automática	Automatic Call Back
BLF	Blf	Campo Lamp ocupado ON	Busy Lamp Field
Call Back	Ccbs	Conclusão de Chamada ON	Call Completion To Busy Subscriber
CustTrace	Cot	Trace de Origem ON	Customer Originated Trace
CWD	Cwd	Chamar chmd em espera	Dial Call Waiting
EMW	ExMw	Msg Executiva em Espera	Executive Message Waiting
Inspect	Insp	Ver nome chamada	Calling Name Inspect Key
LVM	Lvm	Deixar mensagem activo	Leave Message
MCH	Mch	Hold de chamd maléfico	Malicious Call Hold
MRFM	MADNRF	MADN activa	Multiple Appearance Directory Number Ring Forward
MsgWaitInd	MwInd	Indicador Msg. Espera	Message Waiting Indication
MsgWaitQry	MwQry	Questionar Mng. Espera	Message Waiting Query
PRL	Prel	Libertar privacidade ON	Privacy Release
Privacy	Priv	Privacidade Activa	Privacy
SpdCalShrt	Scs	Chamada rápida	Speed Calling Short List
SLQ	SLQ	Fila em linha única	Single Line Queuing
UCD Login	Login	UCD Login activo	Uniform Call Distribution Login
MakeBusyI	MSBI	Definir ocupado ON	Make Set Busy Intragroup
GIC	GIC	Intercom Grupo Activo	Group Intercom
GIAC	GIAC	Intercom todo Grupo Act	Group Intercom All Calls
Quick Conf	QCK	Conferencia rápida ON	Quick Conference Key

Subcom	Subcom	Sub-comunidade ON	Sub Community routing for Emergency Calls
AutoAnswer	AAB	Atendimento auto ON	Auto Answer Back
CallCover	Ccv	Cobertura Chmd activo	Call Covering
BsyOveride	Ebo	Ignorar Exec. ocupado	Executive Busy Override
SupAgnDN	SAgnDN	Chd Entr.(SupAgntDN) On	ACD Incalls (Sup + Agent + DN)
SupAgnPDN	SAgnPDN	Chd Entr.(SupAgntPDN)On	ACD Incalls (Sup + Agent + PDN)
SupPDN	SupPDN	Chd Entr.(Sup + PDN) On	ACD Incalls (Sup + PDN)
AgentPDN	AgPDN	Chd Entr.(Agnt+PDN) On	ACD INCALLS (Agent + PDN)
CFK	CFK	Direccionamento (Tecla)	Call Forwarding On A Per Key Basis
MBSCAMP	Camp	Camp da estação ON	Meridian Business Set Station Camp On
SBLF	SBLF	Definir ampo Based Lamp	Set Based Lamp Field

67.19 Spanish Default Soft key Labels

Feature Name	Default Softkey Label	Indication displayed when feature active and not assigned to a key.	Description
Forward	TBD	TBD	Forward
Msg Wait	TBD	TBD	Message Waiting' short feature name
Transfer	TBD	TBD	Call Transfer' short feature name
Ring Again	TBD	TBD	Ring Again' short (and long) feature name
Speed Call	TBD	TBD	Speed Call' short (and long) feature name
Primary DN	TBD	TBD	The Most important DN. Usually assigned to feature key 1.
Time&Date	TBD	TBD	The 'Time and Date' short (and long) feature name
Agent	TBD	TBD	Agent In calls' short feature name
DN	TBD	TBD	Directory Number' short feature name
Make Busy	TBD	TBD	Make Set Busy' short feature name
3 Way Call	TBD	TBD	3 Way Call' short feature name
Dir. Park	TBD	TBD	Directed Call Park' short feature name
Not Ready	TBD	TBD	Agent Not Ready' short feature name. This feature is part of the ACD family of features.
Emergency	TBD	TBD	Emergency' short (and long) feature name. This feature is part of the ACD family of features.
Supervisor	TBD	TBD	Supervisor Incalls' short feature name. This feature is part of the ACD family of features.
Call Super	TBD	TBD	Call Supervisor' short feature name. This feature is part of the ACD family of features.
Ans. Emerg	TBD	TBD	Answer Emergency' short feature name. This feature is part of the ACD family of features

Ans. Agent	TBD	TBD	Answer Agent' short feature name. This feature is part of the ACD family of features.
Agent Stat	TBD	TBD	Agent Status' short feature name. This feature is part of the ACD family of features.
Obs. Agent	TBD	TBD	Observe Agent' short feature name. This feature is part of the ACD family of features.
Conference	TBD	TBD	6 Party Conference' short feature name
Autodial	TBD	TBD	Autodial' short (and long) feature name. To automatically dial the phone. Abbreviation for Automatic Dialing
Park	TBD	TBD	Call Park' short feature name.
Unknown	TBD	TBD	This catch all feature is used when a feature is present on the feature key, but does not have its own assigned entry in this list.
Fast Xfer	TBD	TBD	Fast Transfer' short feature name.
Pickup	TBD	TBD	Call Pickup' short feature name.
Intercom	TBD	TBD	Intercom (Business sets)' short (and long) feature name.
Call Wait.	TBD	TBD	Call Waiting' short feature name
QryBusyStn	TBD	TBD	Query Busy Station' short feature name.
AgtSummary	TBD	TBD	Display Agent Summary' short feature name. This feature is part of the ACD family of features to display the summary of an agent's activities.
Q Status	TBD	TBD	Display Queue Status' short feature name. This feature is part of the ACD family of features and is used to display the status of the ACD queue.
QThreshold	TBD	TBD	Display Queue Threshold' short feature name. This feature is part of the ACD family of features and is used to display the threshold of the ACD queue.
FrcAgAvail	TBD	TBD	Force Agent Availability' short feature name. This feature is part of the ACD family of features and is used by the supervisor to force the agent into becoming available.
Ctrl IFlow	TBD	TBD	Controlled Interflow' short feature name. This feature is part of the ACD family of features.
SupNgtServ	TBD	TBD	Supervisor Control of Night Service' short feature name. This feature is part of the ACD family of features.
Line Bus	TBD	TBD	Line of Business' short feature name. This feature is part of the ACD family of features.
Call Agent	TBD	TBD	Call Agent' short (and long) feature name. This feature is part of the ACD family of features.
Call Force	TBD	TBD	Call Agent with Call Forcing option. This feature is part of the ACD family of features.
ACB	TBD	TBD	Automatic Call Back
BLF	TBD	TBD	Busy Lamp Field
Call Back	TBD	TBD	Call Completion To Busy Subscriber
CustTrace	TBD	TBD	Customer Originated Trace
CWD	TBD	TBD	Dial Call Waiting
EMW	TBD	TBD	Executive Message Waiting
Inspect	TBD	TBD	Calling Name Inspect Key
LVM	TBD	TBD	Leave Message
MCH	TBD	TBD	Malicious Call Hold

MRFM	TBD	TBD	Multiple Appearance Directory Number Ring Forward
MsgWaitInd	TBD	TBD	Message Waiting Indication
MsgWaitQry	TBD	TBD	Message Waiting Query
PRL	TBD	TBD	Privacy Release
Privacy	TBD	TBD	Privacy
SpdCalShrt	TBD	TBD	Speed Calling Short List
SLQ	TBD	TBD	Single Line Queuing
UCD Login	TBD	TBD	Uniform Call Distribution Login
MakeBusyI	TBD	TBD	Make Set Busy Intragroup
GIC	TBD	TBD	Group Intercom
GIAC	TBD	TBD	Group Intercom All Calls
Quick Conf	TBD	TBD	Quick Conference Key
Subcom	TBD	TBD	Sub Community routing for Emergency Calls
AutoAnswer	TBD	TBD	Auto Answer Back
CallCover	TBD	TBD	Call Covering
BsyOveride	TBD	TBD	Executive Busy Override
SupAgnDN	TBD	TBD	ACD Incalls (Sup + Agent + DN)
SupAgnPDN	TBD	TBD	ACD Incalls (Sup + Agent + PDN)
SupPDN	TBD	TBD	ACD Incalls (Sup + PDN)
AgentPDN	TBD	TBD	ACD INCALLS (Agent + PDN)
CFK	TBD	TBD	Call Forwarding On A Per Key Basis
MBSCAMP	TBD	TBD	Meridian Business Set Station Camp On
SBLF	TBD	TBD	Set Based Lamp Field

67.20 Turkish Default Soft key Labels

Feature Name	Default Softkey Label	Indication displayed when feature active and not assigned to a key.	Description
Forward	Yönldr	Yönlendirildi	Forward
Msg Wait	BekMsj	Bekleyen Mesaj Açk	Message Waiting' short feature name
Transfer	Trnsfr	Çar Transferi açk	Call Transfer' short feature name
Ring Again	TkrÇal	Tekrar Çal Açk	Ring Again' short (and long) feature name
Speed Call	HzlAra	Hzl Arama Açk	Speed Call' short (and long) feature name
Primary DN	PDN	Birincil DN Açk	The Most important DN. Usually assigned to feature key 1.
Time&Date	ZmnTrh	Zaman ve Tarih Açk	The 'Time and Date' short (and long) feature name
Agent	Kllnc	Kullanc Çarlar Açk	Agent In calls' short feature name
DN	Dn	Rehber Numaras Açk	Directory Number' short feature name
Make Busy	Mesgul	Megul Aktif	Make Set Busy' short feature name
3 Way Call	3Konf	Üçlü Konferans Açk	3 Way Call' short feature name
Dir. Park	DcPk	Çar Park Açk	Directed Call Park' short feature name
Not Ready	HzDgil	Kullanc Hazr Deil	Agent Not Ready' short feature name. This feature is part of the ACD family of features.

Emergency	Acil	Acildurum Açk	Emergency' short (and long) feature name. This feature is part of the ACD family of features.
Supervisor	SpvIn	Supervisör Çar Açk	Supervisor Incalls' short feature name. This feature is part of the ACD family of features.
Call Super	Supv	Supervisör Arama Açk	Call Supervisor' short feature name. This feature is part of the ACD family of features.
Ans. Emerg	AclCvp	Acildurum Cevap Aktif	Answer Emergency' short feature name. This feature is part of the ACD family of features
Ans. Agent	KulCvp	Kullanc Cevap Aktif	Answer Agent' short feature name. This feature is part of the ACD family of features.
Agent Stat	KulDrm	Kullanc Durum Açk	Agent Status' short feature name. This feature is part of the ACD family of features.
Obs. Agent	KuGzlm	Kullanc Gözlem Açk	Observe Agent' short feature name. This feature is part of the ACD family of features.
Conference	6Konf	Altl Konferans	6 Party Conference' short feature name
Autodial	OtoÇvr	Otomatik Çevirme	Autodial' short (and long) feature name. To automatically dial the phone. Abbreviation for Automatic Dialing
Park	Park	Çar Park Aktif	Call Park' short feature name.
Unknown	Blnmyn	Bilinmeyen Özellik Açk	This catch all feature is used when a feature is present on the feature key, but does not have its own assigned entry in this list.
Fast Xfer	HTrnsf	Hzl transfer Açk	Fast Transfer' short feature name.
Pickup	ÇTpla	Çar Toplama Aktif	Call Pickup' short feature name.
Intercom	Icom	Intercom Aktif	Intercom (Business sets)' short (and long) feature name.
Call Wait.	Bekle	Bekleyen Çar	Call Waiting' short feature name
QryBusyStn	MsAbSr	Megul Abone Sorgu Açk	Query Busy Station' short feature name.
AgtSummary	KuOzet	Kullanc Özet Gösterme	Display Agent Summary' short feature name. This feature is part of the ACD family of features to display the summary of an agent's activities.
Q Status	KyrOzt	Kuyruk Durumu Gösterme	Display Queue Status' short feature name. This feature is part of the ACD family of features and is used to display the status of the ACD queue.
QThreshold	KyrSvy	Kuyruk Seviye Gösterme	Display Queue Threshold' short feature name. This feature is part of the ACD family of features and is used to display the threshold of the ACD queue.
FrcAgAvail	FAA	Zorlama Açk	Force Agent Availability' short feature name. This feature is part of the ACD family of features and is used by the supervisor to force the agent into becoming available.
Ctrl IFlow	Cif	Kontrollu Ak	Controlled Interflow' short feature name. This feature is part of the ACD family of features.
SupNgtServ	GceSrv	Gece Servis Açk	Supervisor Control of Night Service' short feature name. This feature is part of the ACD family of features.
Line Bus	Lob	Hatt	Line of Business' short feature name. This feature is part of the ACD family of features.
Call Agent	KulAkt	Kullanc Aktif	Call Agent' short (and long) feature name. This feature is part of the ACD family of features.
Call Force	Forc	Çar Zorlama Açk	Call Agent with Call Forcing option. This feature is part of the ACD family of features.
ACB	OtoAra	Otomatik Çar Yapma	Automatic Call Back

BLF	Blf	Megul Lamba Alan Açk	Busy Lamp Field
Call Back	ÇTmla	Çar Tamamlama Açk	Call Completion To Busy Subscriber
CustTrace	Cot	Aranan zleme Açk	Customer Originated Trace
CWD	BÇÇ	Bekleyen Çar Çevir	Dial Call Waiting
EMW	ExMsj	Üstdüzey Mesaj Bekliyor	Executive Message Waiting
Inspect	Arsm	Arayan sme Bakma	Calling Name Inspect Key
LVM	MsjBrk	Mesaj Brakma Aktif	Leave Message
MCH	MCH	Kötü amaçl Çar Tutma	Malicious Call Hold
MRFM	MADNRF	MADN Aktif	Multiple Appearance Directory Number Ring Forward
MsgWaitInd	BkMsjG	Bekleyen Mesaj Göster	Message Waiting Indication
MsgWaitQry	BkMsjS	Bekleyen Mesaj Sorgula	Message Waiting Query
PRL	ÖzlÇöz	Özel Çözme Açk	Privacy Release
Privacy	Özel	Özel Kullanm Açk	Privacy
SpdCalShrt	Scs	Hzl Arama Ksa Liste	Speed Calling Short List
SLQ	TkHtS	Tek Hat Sralama	Single Line Queuing
UCD Login	Giri	UCD Giri Aktif	Uniform Call Distribution Login
MakeBusyI	StMEt	Seti Megul Et Açk	Make Set Busy Intragroup
GIC	GIC	Grup Intercom Aktif	Group Intercom
GIAC	GIAC	Grup Intercom Açk	Group Intercom All Calls
Quick Conf	HzKonf	Hzl Konferans Açk	Quick Conference Key
Subcom	Subcom	Sub Community Aktif	Sub Community routing for Emergency Calls
AutoAnswer	OtoCvp	Otomatik Cevap Açk	Auto Answer Back
CallCover	ÇgrMhf	Çar Muhafaza Açk	Call Covering
BsyOveride	AraGir	Üstdüzey Araya Girme	Executive Busy Override
SupAgnDN	SAgnDN	Incalls (SupAgntDN) Açk	ACD Incalls (Sup + Agent + DN)
SupAgnPDN	SAgnPDN	Incalls (SupAgntPDN) Açk	ACD Incalls (Sup + Agent + PDN)
SupPDN	SupPDN	Incalls (Sup + PDN) Açk	ACD Incalls (Sup + PDN)
AgentPDN	AgPDN	Incalls (Agnt + PDN) Açk	ACD INCALLS (Agent + PDN)
CFK	ÇaYönl	Çar Yönlendirme (Tu)	Call Forwarding On A Per Key Basis
MBSCAMP	MNoBek	Megul No Bekleme Açk	Meridian Business Set Station Camp On
SBLF	SBLA	Set Bazl Lamba Alan	Set Based Lamp Field

67.21 Italian Default Soft key Labels

Feature Name	Default Softkey Label	Indication displayed when feature active and not assigned to a key.	Description
Forward	fwd	inoltrata	Forward
Msg Wait	MsgWt	messaggio in attesa	Message Waiting' short feature name
Transfer	Xfr	chiamata traferita	Call Transfer' short feature name
Ring Again	Rag	Ring Again	Ring Again' short (and long) feature name

Speed Call	Scl	Speed Call Short	Speed Call' short (and long) feature name
Primary DN	PDN	Primary DN	The Most important DN. Usually assigned to feature key 1.
Time&Date	Qtd	Data e ora	The 'Time and Date' short (and long) feature name
Agent	Agent	Agente Incall	Agent In calls' short feature name
DN	Dn	Directory Number	Directory Number' short feature name
Make Busy	Busy	Occupato	Make Set Busy' short feature name
3 Way Call	3wc	Chiamata 3 way	3 Way Call' short feature name
Dir. Park	DcPk	Directed Call Park	Directed Call Park' short feature name
Not Ready	NtRdy	Agent Not Ready	Agent Not Ready' short feature name. This feature is part of the ACD family of features.
Emergency	Emerg	emergenza	Emergency' short (and long) feature name. This feature is part of the ACD family of features.
Supervisor	SpvIn	Supervisor Incall	Supervisor Incalls' short feature name. This feature is part of the ACD family of features.
Call Super	Supv	chiamata supervisor	Call Supervisor' short feature name. This feature is part of the ACD family of features.
Ans. Emerg	EmAns	risposta emergenza	Answer Emergency' short feature name. This feature is part of the ACD family of features
Ans. Agent	AgnAns	risposta agente	Answer Agent' short feature name. This feature is part of the ACD family of features.
Agent Stat	AgnSta	stato agente	Agent Status' short feature name. This feature is part of the ACD family of features.
Obs. Agent	AgObsv	Observe Agente	Observe Agent' short feature name. This feature is part of the ACD family of features.
Conference	6wc	conferenza 6 Pty	6 Party Conference' short feature name
Autodial	ADial	Automatic Dialing	Autodial' short (and long) feature name. To automatically dial the phone. Abbreviation for Automatic Dialing
Park	Park	Call Park	Call Park' short feature name.
Unknown	Unknwn	feature sconosciuta	This catch all feature is used when a feature is present on the feature key, but does not have its own assigned entry in this list.
Fast Xfer	Fxr	trasfer veloce	Fast Transfer' short feature name.
Pickup	Cpu	Call Pickup Attivo	Call Pickup' short feature name.
Intercom	Icom	Intercom Active	Intercom (Business sets)' short (and long) feature name.
Call Wait.	Wait	chiamata in attesa	Call Waiting' short feature name
QryBusyStn	QBS	Richiesta Busy Station	Query Busy Station' short feature name.
AgtSummary	DASK	Display Agent Summary	Display Agent Summary' short feature name. This feature is part of the ACD family of features to display the summary of an agent's activities.
Q Status	DQS	Stato coda	Display Queue Status' short feature name. This feature is part of the ACD family of features and is used to display the status of the ACD queue.
QThreshold	DQT	stato soglia	Display Queue Threshold' short feature name. This feature is part of the ACD family of features and is used to display the threshold of the ACD queue.
FrcAgAvail	FAA	disponibilità force	Force Agent Availability' short feature name. This feature is part of the ACD family of features and is used by the supervisor to force the agent into becoming available.

Ctrl IFlow	Cif	Controlled Interflow	Controlled Interflow' short feature name. This feature is part of the ACD family of features.
SupNgtServ	NgtSrv	Night Service On	Supervisor Control of Night Service' short feature name. This feature is part of the ACD family of features.
Line Bus	Lob	Line of Business	Line of Business' short feature name. This feature is part of the ACD family of features.
Call Agent	Cag	call agente attivo	Call Agent' short (and long) feature name. This feature is part of the ACD family of features.
Call Force	Force	Call Force Attivo	Call Agent with Call Forcing option. This feature is part of the ACD family of features.
ACB	Acb	richiama automatico	Automatic Call Back
BLF	Blf	campo busy lamp	Busy Lamp Field
Call Back	Ccbs	Chiamata completata	Call Completion To Busy Subscriber
CustTrace	Cot	trace originato	Customer Originated Trace
CWD	Cwd	Dial Chiam in attesa	Dial Call Waiting
EMW	ExMw	exec msg in attesa	Executive Message Waiting
Inspect	Insp	Calling Name Inspect	Calling Name Inspect Key
LVM	Lvm	Leave Message Attivo	Leave Message
MCH	Mch	Malicious Call Hold	Malicious Call Hold
MRFM	MADNRF	MADN Attivo	Multiple Appearance Directory Number Ring Forward
MsgWaitInd	MwInd	Message Waiting Ind	Message Waiting Indication
MsgWaitQry	MwQry	Mess Waiting richiesta	Message Waiting Query
PRL	Prel	Privacy Release	Privacy Release
Privacy	Priv	Privacy Attivo	Privacy
SpdCalShrt	Scs	Speed Calling Short	Speed Calling Short List
SLQ	SLQ	accodamento Single Line	Single Line Queuing
UCD Login	Login	UCD Login Attivo	Uniform Call Distribution Login
MakeBusyI	MSBI	Make Set Busy Intra	Make Set Busy Intragroup
GIC	GIC	Group Intercom Attivo	Group Intercom
GIAC	GIAC	Group Intercom All	Group Intercom All Calls
Quick Conf	QCK	Quick Conference	Quick Conference Key
Subcom	Subcom	Sub Community Attivo	Sub Community routing for Emergency Calls
AutoAnswer	AAB	Auto Answer Back	Auto Answer Back
CallCover	Ccv	Call Covering Attivo	Call Covering
BsyOveride	Ebo	Executive Busy Override	Executive Busy Override
SupAgnDN	SAgnDN	Incalls (SupAgntDN)	ACD Incalls (Sup + Agent + DN)
SupAgnPDN	SAgnPDN	Incalls (SupAgntPDN)	ACD Incalls (Sup + Agent + PDN)
SupPDN	SupPDN	Incalls (Sup + PDN)	ACD Incalls (Sup + PDN)
AgentPDN	AgPDN	Incalls (Agnt + PDN)	ACD INCALLS (Agent + PDN)
CFK	CFK	Call Forwarding (Key)	Call Forwarding On A Per Key Basis
MBSCAMP	Camp	Station Camp	Meridian Business Set Station Camp On
SBLF	SBLF	campo Set Based Lamp	Set Based Lamp Field

68: Functional Description (FN) A00009362

68.1 Feature name and Feature ID

A00009362: IP Phone 2007 User Interface support

68.2 Scope

This document covers the functional description for the work required to support the IP Phone 2007 Internet Telephone. This document also covers the functional description for the work required to support a common User Interface for the IP Phone 2007.

68.3 Description

The IP Phone 2007 is a colour display telephone that offers innovative touch screen capability and a 5.7" diagonal display, delivering converged applications (voice, framed video and data such as customized web content) along with future SIP support via firmware download to a user's desktop. The IP Phone 2007 offers Bluetooth compatibility and USB support. The IP Phone 2007 is an extended functionality sibling of the IP Phone 2004. Refer to the following figure.

Disclaimer:

The Screenshot currently shows Incorrect labels: (i.e.) the Labels for the softkeys and f feature keys are swapped in a CICM environment.

Figure 1 IP Phone 2007

Figure 1 IP Phone 2007

IP Phone 2007 has an incorporated three-port hub, meaning that a desktop with an IP Phone 2007 and a computer requires only one connection to the network. In addition it is possible to draw power from the LAN.

This feature implements the screen displays to support basic functionality on the IP Phone 2007. Refer to the following table.

Table 1 IP Phone 2007 Configuration/menu matrix

Feature	**2007**
Display	
Pixels	240x320
Dimensions	5.7” diagonal
Backlight	CCFL
Technology	STN Colour
Greyscale/Colour	16-bit colour
Adjustable contrast	Yes

Adjustable backlight	Variable brightness
Touch panel	Yes
Keys & Indicators	
Number of LEDS	TBD
Mute Lamp	Yes Red
Headset lamp	Yes Red
Handsfree lamp	Yes Red
MW Lamp	Yes Orange/Red
Data Waiting Lamp	Yes blue
Link Lamp	Yes green
Feature Keys	Soft Defined
Nav Keys	4
Line Keys	Soft defined
Connectors	
Network Port	Gig
PC Port	Gig
10 pin KEM	Yes
Handset	Yes
Headset	Yes with detect
USB	Two
DC Power	Yes
Power Supply	
IEEE 802.3AF	Yes
Cisco Link Pulse	Yes
Cisco Mid-span	No
AC Adapter	Yes 48 volts DC
PowerDSine Mid-Span	Yes
Bluetooth	
Version	1.x
Profiles at GA time	Headset/HF
Audio	
Handsfree	Full Duplex
Headset	Yes

Handset	Yes
Wideband	Yes
USB	
Mouse	Yes
Keyboard	Yes
Flash Drive	Yes

68.3.1 Display

The IP Phone 2007 has a bit mapped and backlit 240x320 pixel colour STN display with 16 bit colour depth and integrated touch panel. The display of the IP Phone 2007 is not visible without the backlight.

Fonts are supported on this Display and the IP Phone 2007 has graphic capable displays and using a font representation of characters in place of the 5x7 dot matrix characters. The IP Phone 2007 sets are supporting a true font, Lucida Sans.

The contrast of this display is adjustable and On-off and brightness controls are provided.

The IP Phone 2007 is using cold cathode fluorescent lamp for backlit.

There is no reflected mode in the display of IP Phone 2007.

The CCFL is having the lifetime of 50,000 hours. To address Lifetime of CCFL, a firmware timer has been used to turn off the backlight after a period of inactivity. The user can customize the timeout period. The default timeout period is a long time and one more choice is no timeout.

The IP Phone 2007 doesn’t have any physical feature or soft keys but provide access to the functionality provided by the keys via the touch screen interface.

The display of the IP Phone 2007 looks same as the display of IP Phone 2004.

68.3.2 Keys

IP Phone 2007 supports the Key Expansion Module to provide access to an extended feature set.

The softkey and feature keys are not physically on the IP Phone 2007 but are available within the main screen display and are accessible by touching the screen. These keys provide access to the same functionality that is available on the IP Phone 2004.

68.3.3 Indicators

There are two Message Indicator Lamps on the IP Phone 2007, the amber indicator is intended to show when a voicemail message is waiting.

Message Waiting Indicator Orange/Red LED: Located at the top of the set. This LED indicates alerting and message waiting.

Data Waiting Indicator Blue LED: Located at the top of the set. This will be turned on while the user is on an active call.

Handsfree Indicator Red LED: Located on the front cover near the Handsfree key. Indicates when the handsfree is in use

Headset Indicator Red LED: Located on the front cover near the Headset key. Indicates when the headset is in use.

Mute Indicator Red LED: Located on the front cover near the Mute key. Indicates whether the terminal is on mute.

Link/Data Indicator Green LED: Located on the back cover near the Network Ethernet jack. Indicates when the Network etherport detects link and flashes for data activity.

68.3.4 Display Screens

The Following screen shots show some of Display screens of IP Phone 2007.

Figure 2 Services Key Panel

The above screen shot shows the services Key panel which is available in the IP Phone 2007. The services key panel offers various services. Example of such service is to view the Inbox and Outbox entries as well as gives facility to Transfer / forward the Call.

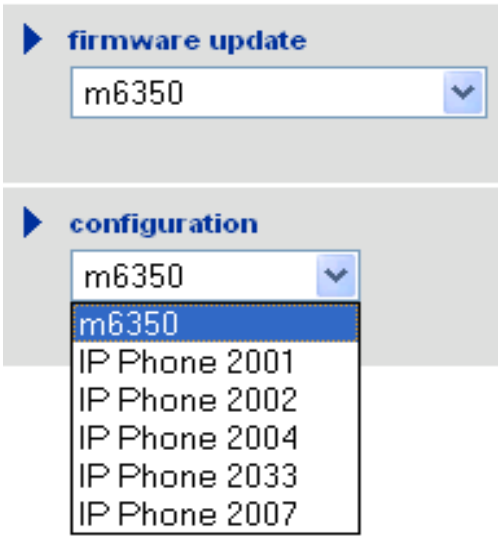
Figure 3 Navigation Key Panel

The Navigation keys provide us with the ability to use left and right keys during the text entry to navigate through the input string. The up and down arrow keys act as Home and End as found on the other IP Phone 2004.

Figure 4 Feature Key Panel

The feature keys are available via the touch screen and are used exactly the same manner as the IP Phone 2004.

68.3.5 Administration - Element Manager



The below screenshot provides the information of the firmware configuration e.g. firmware transfer protocol, Firmware load name and the version details of IP Phone 2007.

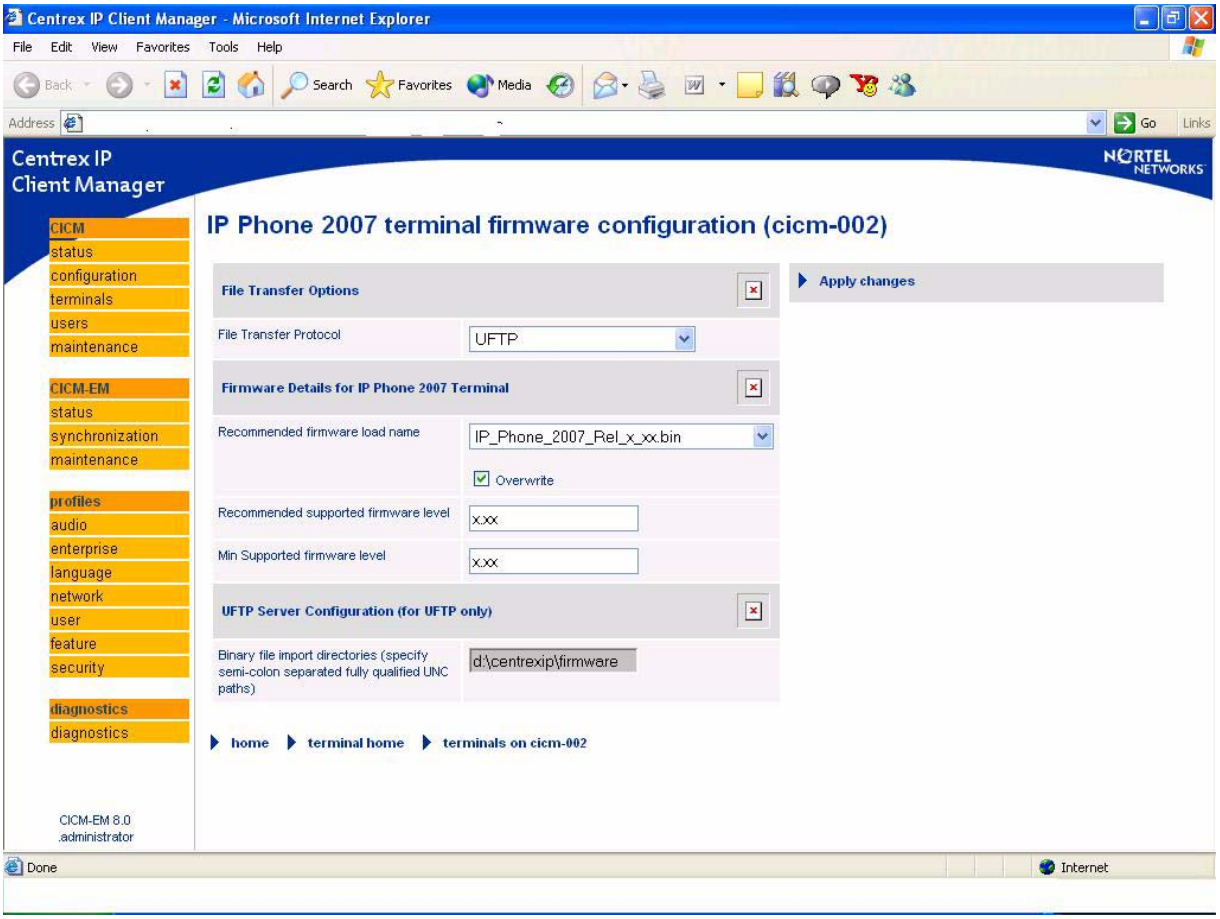


Figure 7 Terminal firmware upgrade page

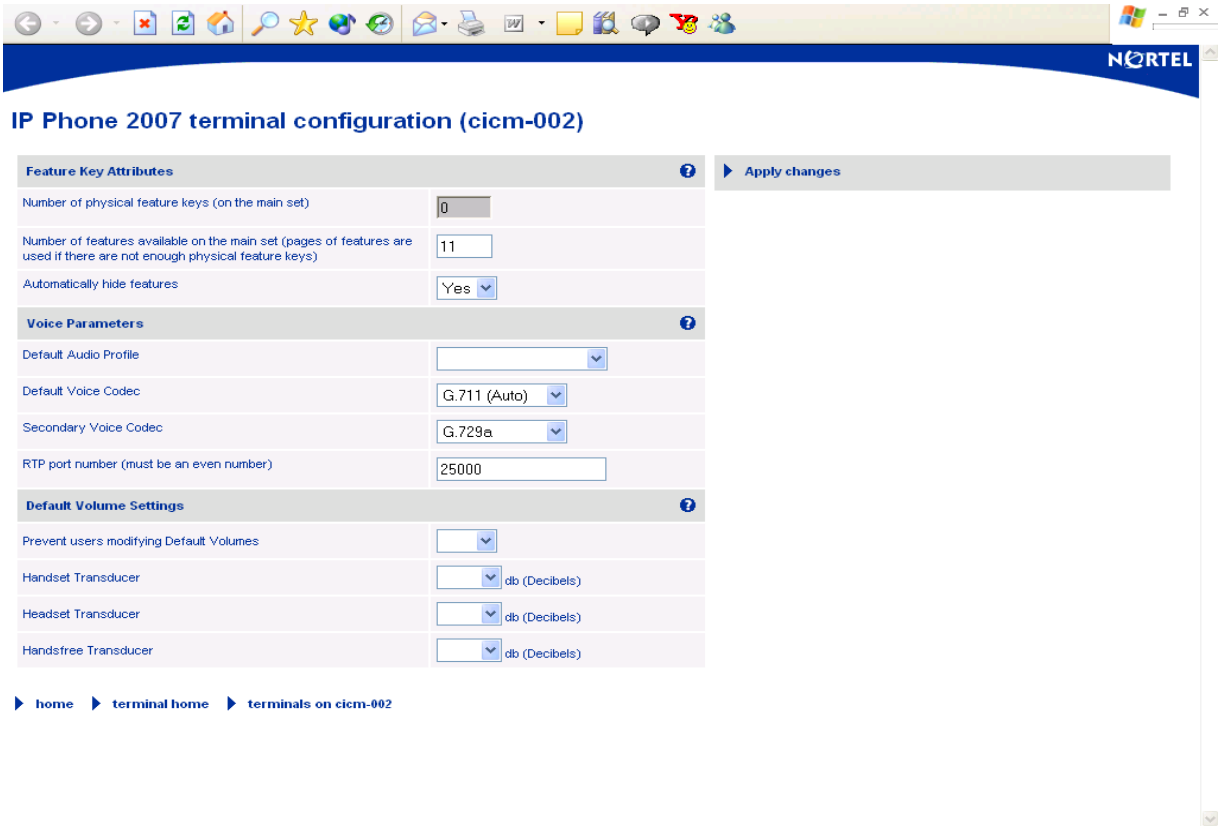


Figure 8 Terminal configuration page

The administration and configuration of the IP Phone 2007 use the same pages which are already provided for the IP Phone 2004 terminals. (See figure 7 and Figure 8.)

68.4 Interactions

68.4.1 Joint Sessions

The IP Phone 2007 is able to have a joint session with the m6350 Softclient. In this scenario, it will always adopt the master position in their master/slave relationship. In this case, the IP Phone 2007 will function in the same manner as the IP Phone 2004.

IP phone 2007 doesn’t support to have a joint session with another IP Phone 200x or Wave 1 Terminals.

68.4.2 ACD Call force

The IP Phone 2007 supports the ACD call force feature in the same manner as the IP Phone 2004.

68.4.3 SRG Support

The Survivable Remote Gateway (SRG) solution is based on the Business Communications Manager (BCM) platform and technologies. It allows distribution of trunking across the WAN so remote users can get dial tone from their local central office or from any other IP Telephony gateway hosted by Succession 1000. Local telephone numbers can be published, supporting a local presence within the community the remote office supports. This capability can also reduce unnecessary toll charges and provides required local trunking for Emergency 911 calls. Additionally, the Survivable Remote Gateway provides a full suite of IPbased data and routing capabilities including Network Address Translation (NAT), DHCP, Web caching, and firewall. IP Phone 2007 supports SRG feature in the same way as Phase 2 terminals.

68.4.4 Unistim Security

The IP Phone 2007 and CICM communicate using a stimulus protocol called Unistim. By interacting with the IP Phone 2007, an end user can use the services that are hosted by the CICM. The signalling protocol / communication between the terminal clients and the CICM were in the form of clear text and therefore susceptible to various signalling attacks. The purpose of the Unistim Security is to provide secure signalling communication (encryption / decryption / authentication) between the IP Phone 2007 and the CICM. The RTP (voice) path is not affected (i.e. remains non-secured).

68.5 Software Requirements or Dependencies

The IP Phone 2007 supports standard TFTP or Nortel UFTP (Unistim FTP) for firmware download. In case of UFTP, the CICM must be able to recognize, store and upload 2007 firmware

68.5.1 Firmware Download

The IP Phone 2007 has upgradeable firmware. The firmware may be upgrade by the following methods.

- The CICM can query the FW version and direct the phone to conduct a firmware download from a TFTP server or download the firmware using UFTP.
- A USEC secured CICM can direct the phone to conduct a firmware download under the protection of Secure UNIStim.
- The phone may be directed to a TFTP server either manually, by full DHCP or a .cfg file to download new firmware.

Firmware may be downloaded through the console port.

68.6 Glossary

ACD Automatic Call Distribution

CICM	Centrex IP Client Manager
CCFL	Cornell Coalition For Life
IP	Internet Protocol
KEM	Key Expansion Module
PRD	Product Requirements Document
SRG	Survivable Remote Gateway
TFTP	Trivial File Transfer Protocol
UFTP	Unistim File Transfer Protocol
Unistim	Unified Network IP Stimulus Protocol

69: Functional description (FN): A00009364

69.1 Feature name and Feature ID

A00009364 - CICM End-of-Call QoS Reporting

69.2 Description

In Voice over IP networks, Quality of Service (QoS) can be adversely affected by the components in the network. Unlike TDM networks where the voice quality is consistent for all calls, VoIP networks can experience different voice quality on all calls.

Per call QoS statistics can be used for the following:

- Network engineering
- Trend analysis
- Trouble-shooting network problems
- Service Level Agreement (SLA) validation

The CICM reports QoS statistics as shown in Figure 1, and can be described as follows:

- The CICM reports the QoS statistics at the end of the call. Each ephemeral associated with a call reports QoS statistics separately. When the GWC instructs the CICM to subtract the ephemeral termination QoS statistics are sent to:
  - — The gateway controller (GWC) over H.248
  - — The extended QoS server (a predefined ip address and port number) over UDP in an ANSI based XML format.
- The GWC reformats the QoS statistics reported by the gateway into a binary format and sends the QoS report to the QoS Collector Application (QCA).
- The QCA manages QoS streams from multiple GWCs, reformats the data to an IPDR format and stores the data to disk.

QoS statistics are accumulated on supported clients/terminals whilst a call is active. If a call is placed on hold the QoS statistics are frozen (no more statistics are accumulated) until the call is resumed.

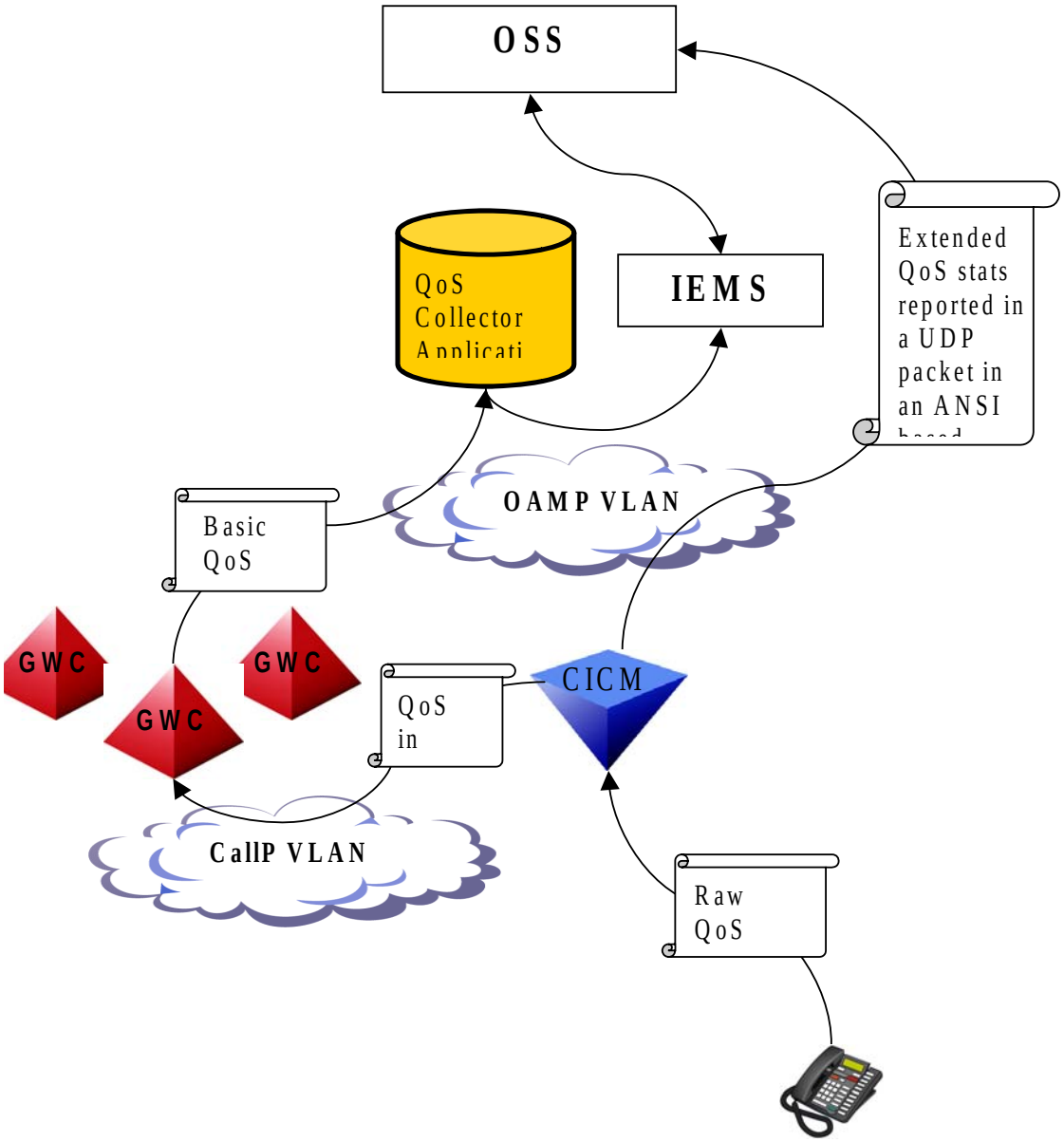


Figure 1 CICM QoS reporting

See Table 1 for a list of supported QoS parameters[1][2].

Note: [1]: Phase 1 terminals support version 1 QoS reporting only. Phase 2 terminals support version 2 “extended” QoS reporting. A complete list of QoS statistics is shown in Table 1. See section 2.5 for further details on supported client/terminal types and firmware requirements.

Note: [2]: Statistics which cannot be obtained from a client/terminal are reported upwards (to the GWC and extended QoS server) with a value of ‘0’.

Table 1 QoS parameters reported

Terminal / Client **QoS reporting version**					**CICM** **QoS Report type**	
1	**2**	**Parameter Name**	**Extended report abbreviation**	**Description**	**Basic** **(QCA)**	**Extended** **(extended QoS server)**
X	**X**	**Jitter Average**	JA	Average variation in packet arrival times due to transmission (routing, queuing delay, etc…) through the network. Represented in 1/65536 of seconds, of the incoming RTP packets inter-arrival time.	X	X
X	**X**	**Jitter High Water Mark**	JHW	Max variation in packet arrival times due to transmission (routing, queuing delay, etc…) through the network. Represented in 1/65536 of seconds, of the incoming RTP packets inter-arrival time		X
X	**X**	**Far End Originated Loss**	FEOL	Far end orginated loss	X	X

X	**X**	**Round Trip Average**	RTA	Average RTCP packets round trip time. Represented in 1/65536 of seconds, of the incoming RTCP packets round trip time		X
X	**X**	**Round Trip High Water Mark**	RTHW	Max RTCP packets round trip time. Represented in 1/65536 of seconds, of the incoming RTCP packets round trip time.		X
	X	**Local Silence Suppression**	SS	Indicates if silence suppression was used.		X
	X	**Local Rx and Tx Codec Type**	rC/tC	Codec Type		X
	X	**Local Rx and Tx Packetization Rate**	rPR/tPR	Frame duration in milliseconds.		X
	X	**End System Delay**	ESDA	most recently specified/calculated end system delay in milliseconds. This includes the sample accumulation and encoding delay, as well as the average jitter buffer delay, decoding and playout delay.		X
	X	**Average One Way Delay**	OWDA	average one-way delay in milliseconds.	X	X
	X	**Maximum One Way Delay**	OWDM	maximum one-way delay in milliseconds.		X

	X	**Average Noise Level**	NLA	ratio of the silent period background noise level to overflow signal power, expressed in decibels; 127	X
	X	**Average Signal Power**	SPA	ratio of the signal level to overflow signal level, expressed in decibels; measured only for packets containing speech energy.	X
	X	**Echo Return Loss**	ERL	sum of the measured echo return loss (ERL) and the echo return loss enhancement (ERLE) expressed in dB; the ratio of a transmitted voice signal that is reflected back to the talker.	X
	X	**Listening R factor**	LRF	direct measure of the call quality or transmission quality, and incorporate the effects of CODEC type, packet loss, discard, burstiness, delay etc.; this metric describes the segment of the call that is carried over this RTP session.	X

	X	**Conversational R factor**	CRF	segment of the call that is carried over a network segment, external to the RTP segment, for example a cellular network; relates to the outward voice path from the Voice over IP termination for which this metrics block applies.	X
	X	**Listening Quality MOS**	LM	estimated mean opinion score for listening quality. The valid scale is 10 to 50 representing MOS 1.0 to 5.0, respectively.	X
	X	**Conversational Quality MOS**	CM	estimated mean opinion score for conversational quality. The valid scale is 10 to 50 representing MOS 1.0 to 5.0, respectively.	X
	X	**Burst R factor**	BRF	R factor during a burst period; a burst is defined as a longest sequence of packets bounded by lost or discarded packets	X
	X	**Average Burst Density**	BDA	average percentage of MIU's lost or discarded during burst periods. This value is an 8:8 fixed-point value (i.e. scaled by 256).	X

	X	**Burst count**	BC	number of bursts that have occurred on the call	X
	X	**Average Burst Length in MS**	BLA	average length of all burst periods in milliseconds that have occurred on the call	X
	X	**Gap R factor**	GRF	R factor during a gap period; a gap is defined as the period of time between two bursts.	X
	X	**Average Gap Density**	GDA	average MIU'S lost or discarded within gap periods. This value is an 8:8 fixed-point value (i.e. scaled by 256).	X
	X	**Average Gap Length in MS**	GLA	average length in milliseconds of all gaps that have occurred on the call.	X
	X	**Average Loss Rate**	LRA	total average percentage of MIUs lost and/or discarded. This value is an 8:8 fixed-point value (i.e. scaled by 256).	X
	X	**Average Network Loss Rate**	NLRA	total average percentage of MIUs lost in the network. This value is an 8:8 fixed-point value (i.e. scaled by 256).	X

	X	**Average Discard Rate**	DRA	total average percentage of MIU's discarded. This value is an 8:8 fixed-point value (i.e. scaled by 256).	X
	X	**MIU Duration**	MD	duration of each MIU, in milliseconds	X
	X	**MIU per packet**	MPP	total number of MIU's in each RTP packet	X
	X	**MIU Loss percentage**	MLP	percentage of MIUs handled by the call channel that were lost in the network. This value is an 8:8 fixed-point value (i.e. scaled by 256).	X
	X	**MIU Discard percentage**	MDiP	percentage of MIUs handled by the call channel that were discarded by the endpoint. This value is an 8:8 fixed-point value (i.e. scaled by 256).	X
	X	**MIU Out of order percentage**	MOOOP	percentage of MIUs handled by the call channel that is discarded by the endpoint. This value is an 8:8 fixed-point value (i.e. scaled by 256).	X

	X	**MIU Duplicate percentage**	MDP	percentage of MIUs handled by the call channel that is discarded by the endpoint. This value is an 8:8 fixed-point value (i.e. scaled by 256).		X
	X	**Number of RTP packets rx/tx**	rP/tP	Number of RTP packets received and transmitted	X	X
	X	**Number of RTP packets out of order**	rPOOO	Number of RTP packets received out of order		X
		Octets rx/tx	rO/tO	Octets sent and received. NOTE: This parameter is not currently supported by any terminal types. This value will be set to '0' in all reports.	X	X

69.2.1 Extended QoS statistics

The complete list of QoS statistics[1] displayed in Table 1 can be obtained by configuring the ip address and port number of an extended QoS server on the element manager (see section 3.2.1 for further details on datafill). Extended QoS statistics for each call half will then be reported to the extended call server. Basic QoS statistics will still be reported to the QCA.

The extended report is sent to the configured destination by UDP (using the CICMs admin ip address, port number 34366) in an ANSI based XML format. An example extended QoS XML report is displayed below:

Note: Depending on the client/terminal type hosting the call. Please see section 2.5 for further information.

```
<?xml version="1.0" ?>
<qos>
<ST>2005-18-03T16:19:06Z</ST>
<ET>2005-18-03T16:19:08Z</ET>
<host>CICM-180-B</host>
<LEN>CICM 180 0 00 01</LEN>
<Ip>47.123.124.125</Ip>
<JA>4294967295</JA>
```

```
<JHW>4294967295</JHW>
<FEOL>256</FEOL>
<RTA>4294967295</RTA>
<RTHW>4294967295</RTHW>
<SS>1</SS>
<rC>256</rC>
<tC>256</tC>
<rPR>65535</rPR>
<tPR>65535</tPR>
<PE>256</PE>
<ESDA>65535</ESDA>
<OWDA>65535</OWDA>
<OWDM>65535</OWDM>
<NLA>65535</NLA>
<SPA>65535</SPA>
<ERL>65535</ERL>
<LRF>256</LRF>
<CRF>256</CRF>
<LM>65535</LM>
<CM>65535</CM>
<BRF>256</BRF>
<BDA>65535</BDA>
<BC>65535</BC>
<BLA>4294967295</BLA>
<GRF>256</GRF>
<GDA>65535</GDA>
<GLA>4294967295</GLA>
<LRA>65535</LRA>
<NLRA>65535</NLRA>
<DRA>65535</DRA>
<MD>65535</MD>
<MPP>65535</MPP>
<MLP>65535</MLP>
<MDiP>65535</MDiP>
<MOOOP>65535</MOOOP>
<MDP>65535</MDP>
<rP>4294967295</rP>
<tP>4294967295</tP>
<rPOOO>4294967295</rPOOO>
<rO>4294967295</rO>
<tO>4294967295</tO>
</qos>
```

The header information for the extended QoS XML report is described in Table 2.

Table 2 Extended QoS report header information

Extended QoS XML header tag	Description	Format	Example
ST	Start time (Universal time – UTC)	yyyy-dd-mm**T**hh:mm:ss**Z**	**2005-18-03T16:19:06Z**
ET	End time (Universal time – UTC)		
Host	Machine host name	CICM-xxx-x	CICM-180-A
LEN	LEN	CICM xxx x xx xx	CICM 180 0 00 01
Ip	Ip address of the client	xxx.xxx.xxx.xxx	47.121.122.123

69.2.2 Datafill

QoS reporting is enabled/disabled from the GWC element manager (see Figure 2).

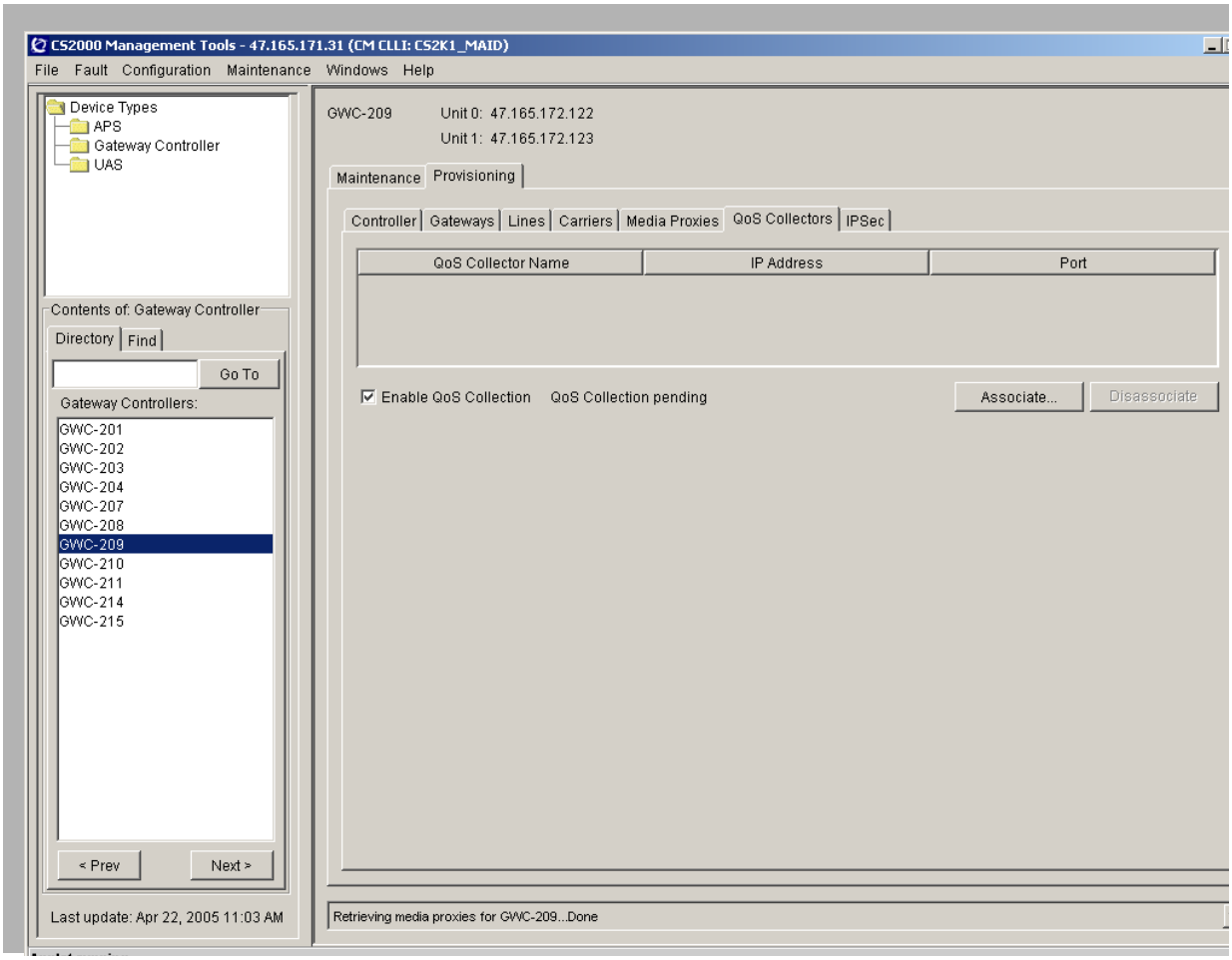


Figure 2 GWC element manager – Enabling/Disabling QoS

Extended QoS reporting is enabled/disabled from the CICM element manager (see Figure 3). Extended QoS statistics will only be sent if a destination ip address and port-number have been data-filled on the CICM element manager global settings page.

Modifications to the extended QoS ip address and port number are picked up dynamically (within 2 minutes) and do not require a reboot.

To disable extended QoS reporting both the extended ip address and port number must be deleted.

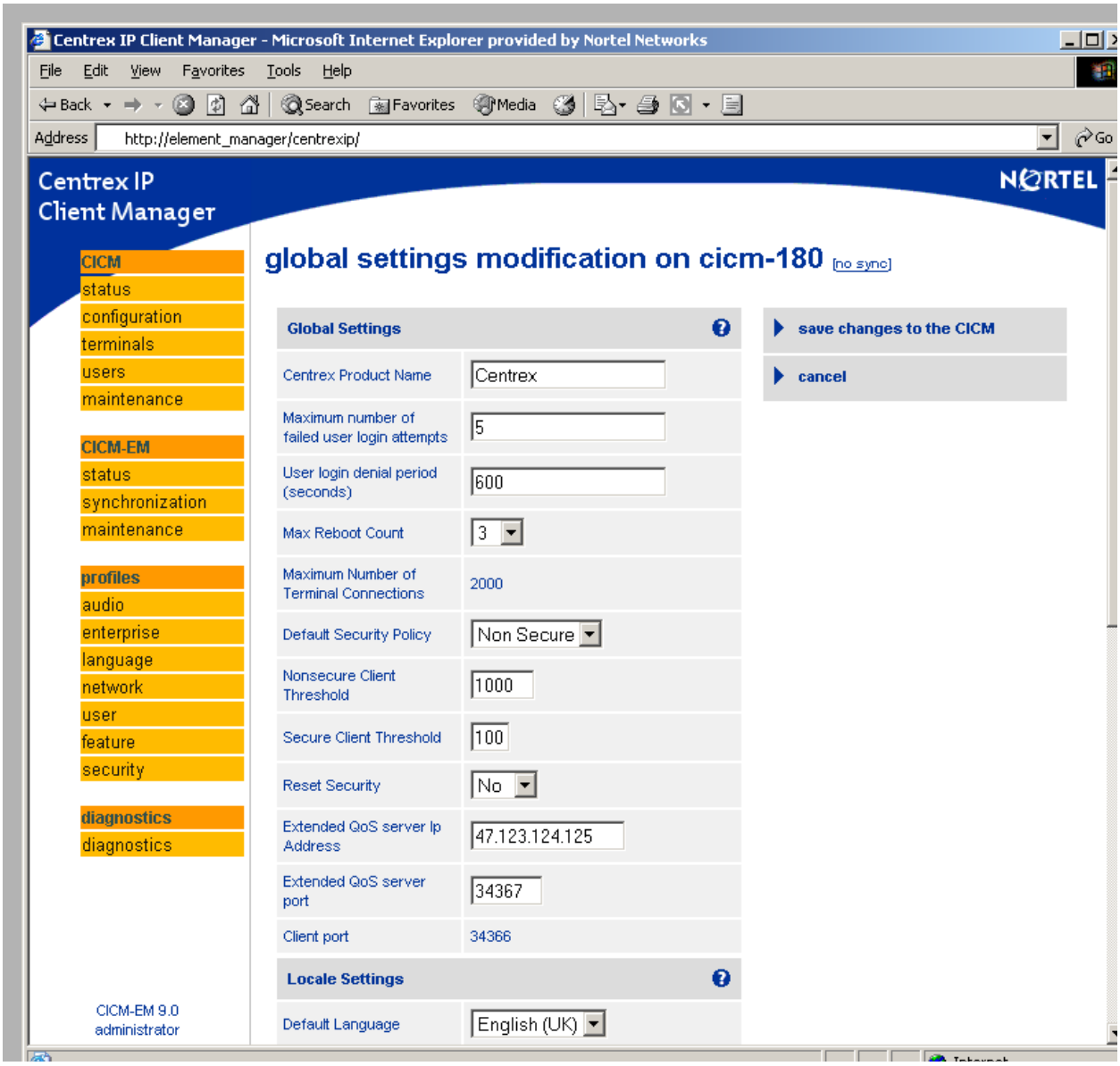


Figure 3 CICM element manager - Enabling/Disabling extended QoS reporting

69.3 Hardware Requirements or Dependencies

QoS Collector Application QCA

69.4 Software Requirements or Dependencies

Not Applicable

69.5 Limitations and restrictions

Terminal type	Version 1 QoS report supported		Version 2 “Extended” QoS report supported (Phase 2 terminals only)	
	Y/N	Minimum firmware version	Y/N	Minimum firmware version
i2001	Y	3.90	Y	3.90
i2002	Y	1.74	Y	3.90
i2004	Y	1.74	Y	3.90
i2007	N	N/A	N	N/A
i2033	N	N/A	N	N/A
I1001	N	N/A	N	N/A
I1002	N	N/A	N	N/A
I1006	N	N/A	N	N/A
I1007	N	N/A	N	N/A
I2210	N	N/A	N	N/A
I2211	N	N/A	N	N/A
I2212	N	N/A	N	N/A

Table 3 Supported terminal types and firmware requirements

Client type	Version 1 QoS report supported		Version 2 “Extended” QoS report supported	
	Y/N	Minimum version	Y/N	Minimum version
M6350	N	N/A	N	N/A
I2050	N	N/A	N	N/A

Table 4 Supported softclient types and version requirements

- Version 2 “Extended” QoS reports are only supported on Phase 2 terminals. Phase 1 terminals support Version 1 QoS reporting only. Please see Table 1 for a complete list of available statistics.
- Statistics which cannot be obtained from a client/terminal are reported upwards (to the GWC and extended QoS server) with a value of ‘0’.
- If the codec is renegotiated QoS statistics will only be reported from the point that the new codec starts.

69.6 Interactions

Not Applicable.

69.7 Logs

Alarm	SubtractConnectionAckFailed
Component Id	CICM
Category	Communications
Description	Subtract ConnectionAck Failed
Specific Problem	SubtractConnectionAck::can't determine destination for message
Severity	NONE
Log Type	CustomerLog
Report Number	363
Event Type	INFO

70: Functional description (FN): A00009365

70.1 Feature name and Feature ID

A00009365 - Mid-call Session Description Protocol (SDP) renegotiation

70.2 Description

70.2.1 Pre-answer and mid-call SDP renegotiation

This activity introduces support for pre-answer and mid-call IP address and codec renegotiation in CICM 9.0, and eliminates the requirement for a Media Portal for CICM lines in a flat network.

During call setup, CICM negotiates the codecs, packetisation times and destination IP information via the exchange of Session Description Protocol (SDP) messages with the far-end. Currently, CICM is unable to process SDP renegotiation attempts from the peer gateway. This causes problems when interworking with gateways which rely on SDP renegotiation to change codecs or destination IP address pre-answer or mid-call.

Prior to CICM 9.0, the lack of support for SDP renegotiation on the CICM causes problems when interworking with Multimedia Call Server (MCS), where an SDP renegotiation attempt can be triggered when MCS features are activated. This activity introduces support for pre-answer and mid-call IP address and codec renegotiation required when interworking with the MCS.

Figure 1 CICM interworking with MCS

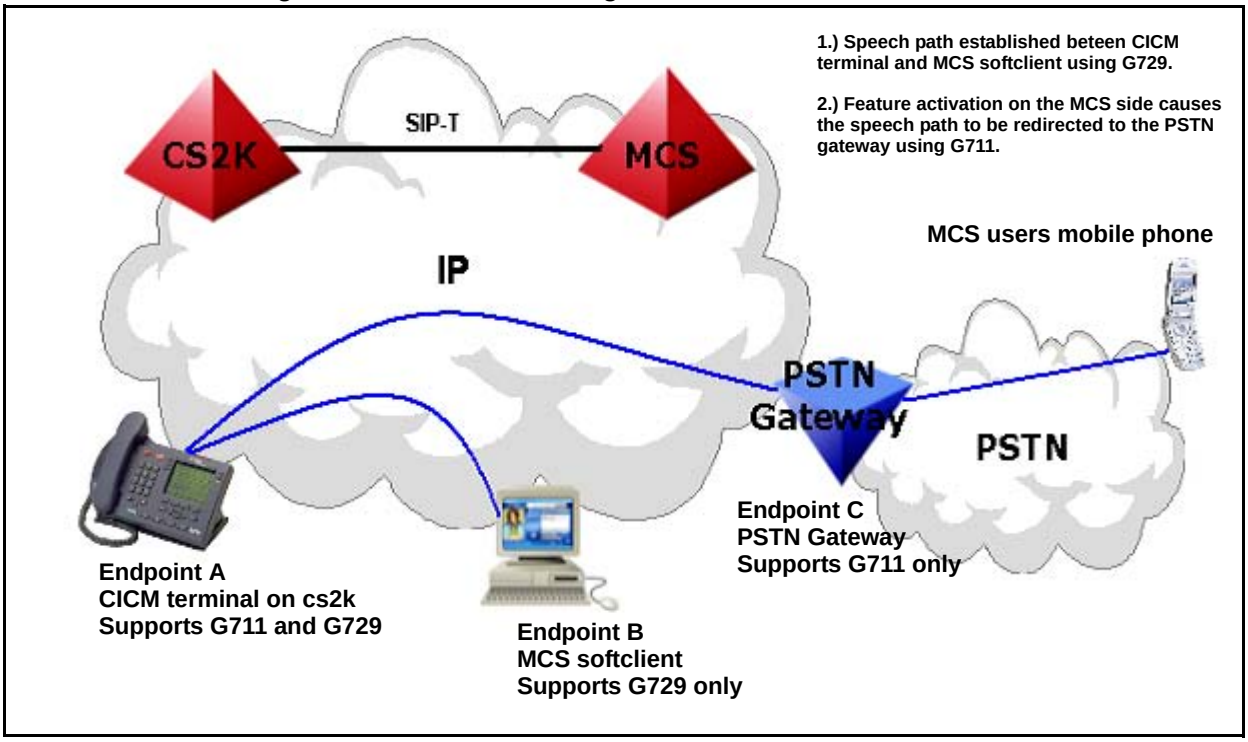


Figure 1 illustrates an example of how feature activation on the MCS can trigger changes in the destination IP address and codecs. This example shows a single CICM client hosted on the cs2k, and a softclient and PSTN gateway hosted on the MCS. The cs2k and MCS are connected by a SIP-T link.

Pre-answer IP address and codec renegotiation:

- CICM terminal calls MCS softclient. Speech path is negotiated to use G729, and terminate at the MCS softclient.
- MCS user does not answer, MCS softclient re-directs the call to the MCS user mobile via the PSTN gateway. Speech path is renegotiated to use G711, and terminate at the PSTN gateway.

Post-answer IP address and codec renegotiation:

- CICM terminal calls MCS softclient (or vice-versa). Speech path is negotiated to use G729, and terminate at the MCS softclient. MCS user answers the call.
- MCS user has to leave, and redirects the call to their mobile. Speech path is renegotiated to use G711, and terminate at the PSTN gateway.

70.3 Hardware Requirements or Dependencies

This activity does not introduce any new hardware requirements or dependancies.

70.4 Software Requirements or Dependencies

This activity does not introduce any new software requirements or dependancies.

70.5 Limitations and restrictions

This activity introduces support for IP address renegotiation at the CICM gateway level only. It does not imply that IP address renegotiation is supported by succession in general. Currently, the GWC Media Portal insertion software does not have the capability of processing mid-call destination IP address changes. For this reason, the MCS must be configured to always insert a Media Portal when interworking with the cs2k. This has the effect of shielding the cs2k from the destination IP address change, as the cs2k directs its audio stream to the MCS portal for the duration of the call.

70.6 Glossary

Term	Description
CICM	CentrexIP Client Manager
SDP	Session Description Protocol
MCS	Multimedia Communications Server
GWC	Gateway Controler

71: Functional description (FN): A00009375 & A00009376

71.1 Feature name and Feature ID

A00009375 & A00009376: CICM Third-party Corrective Content Patching & CICM Selective Binary Component Patching

71.2 Description

71.2.1 Overview

In pre-SN09 loads, all corrective content is delivered via the Maintenance Release (MR) process. In SN09, the MR process will be complimented with new functionality to allow the application of patches containing application, operating system or third party corrective content to the CICM or CICM-EM.

Patches will be built and released by Nortel CICM GNPS, and will be applied onto the CICM or CICM-EM, via the maintenance pages on the CICM-EM.

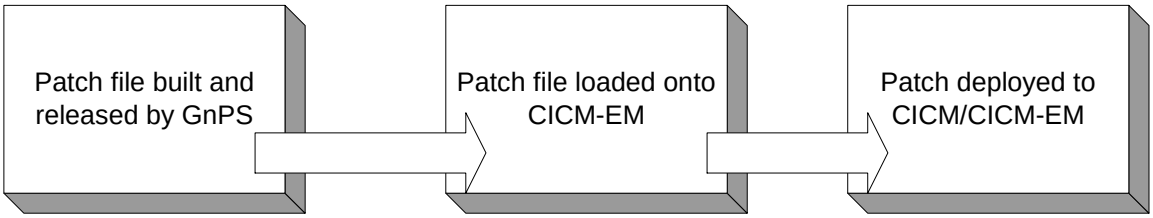


Figure 1 Patch Delivery Overview

71.2.2 Detail

The patching process will compliment the existing MR process by delivering corrective content quickly and efficiently in between the normal MR deliveries. From an end-user perspective the main differences will be as follows.

Maintenance Releases

- Will be delivered at regular intervals
- May contain a large number of corrective content fixes
- May contain a combination of application, operating system or third party corrective content.
- Will replace ALL application binaries (CICM/CICMEM software) on the system to which it is applied.
- The installation of an MR always requires at least one system restart.

Patches

- Will be delivered on an ‘as needed’ basis
- Will contain a single fix for a specific issue
- May contain application, operating system or third party corrective content. But typically not a combination.
- Will only replace application binaries / make other system image changes needed to deliver the corrective content.
- The installation of a patch will not always require a system restart.

71.2.3 Patch Delivery and Application

Nortel GNPS will deploy a patch to a customer in the form of a single patch file and a 128-bit MD5 checksum. The patch file and the checksum will be distributed separately in order to ensure the integrity of the patch file. The checksum of a file will be displayed upon the CICM EM web page once a patch has been selected, the craftsperson may wish to confirm that the number shown is the same as that expected.

This md5 checksum system described in the last paragraph will also be in place for Maintenance Releases.

71.2.3.1 Patch Delivery

The patch file will be delivered to the customer either via electronic transfer or on physical media. The MD5 checksum will be delivered to the customer via e-mail or through publication on an externally accessible Nortel website.

Nortel has corporate wide guidelines on the categorisation and description of Corrective Content (CC). Regional Patch Solutions (RPS) is our interface to the criteria and practice.

RPS offers the PatchFeed tool for submission of CC and this will be used by GnPS to deliver patches to the Nortel website, customer drop-boxes etc. once the patch has been built.

The patch that PatchFeed takes is encapsulated in metadata before being sent on. This metadata is in addition to the metadata added to the CAB files themselves and serves to identify the patch; it’s category, status and applicability conditions to RPS systems.

RPS defined categories for CC are:

- GEN--General content (mass deployment)
- EMG--Emergency content (accelerated mass deployment)
- ACT--Feature rich content (mass or specific Customer deployment)
- LTD--Limited content (specific Customer deployment)

- DBG--Debug content (specific Customer deployment)
- OBS--Obsolete content
- OBE--Obsolete Emergency content

Patches will fall under the GEN, EMG, LTD or DBG category, dependent upon the function of the patch in question.

The RPS statuses are:

- V--VO content (limited deployment)
- R--Released (mass deployment – depending on category)

Patches may be released with either of these statuses.

71.2.3.2 Patch Application

Upon receiving the patch file, the customer will transfer the file into the patching directory on the Master Element Manager (D:\CentrexIP\support\patches) via secure file transfer. Once there the patch can be applied to any suitable node that is under the management of the EM.

All patch management and installation will be carried out under the Element Manager Maintenance pages.

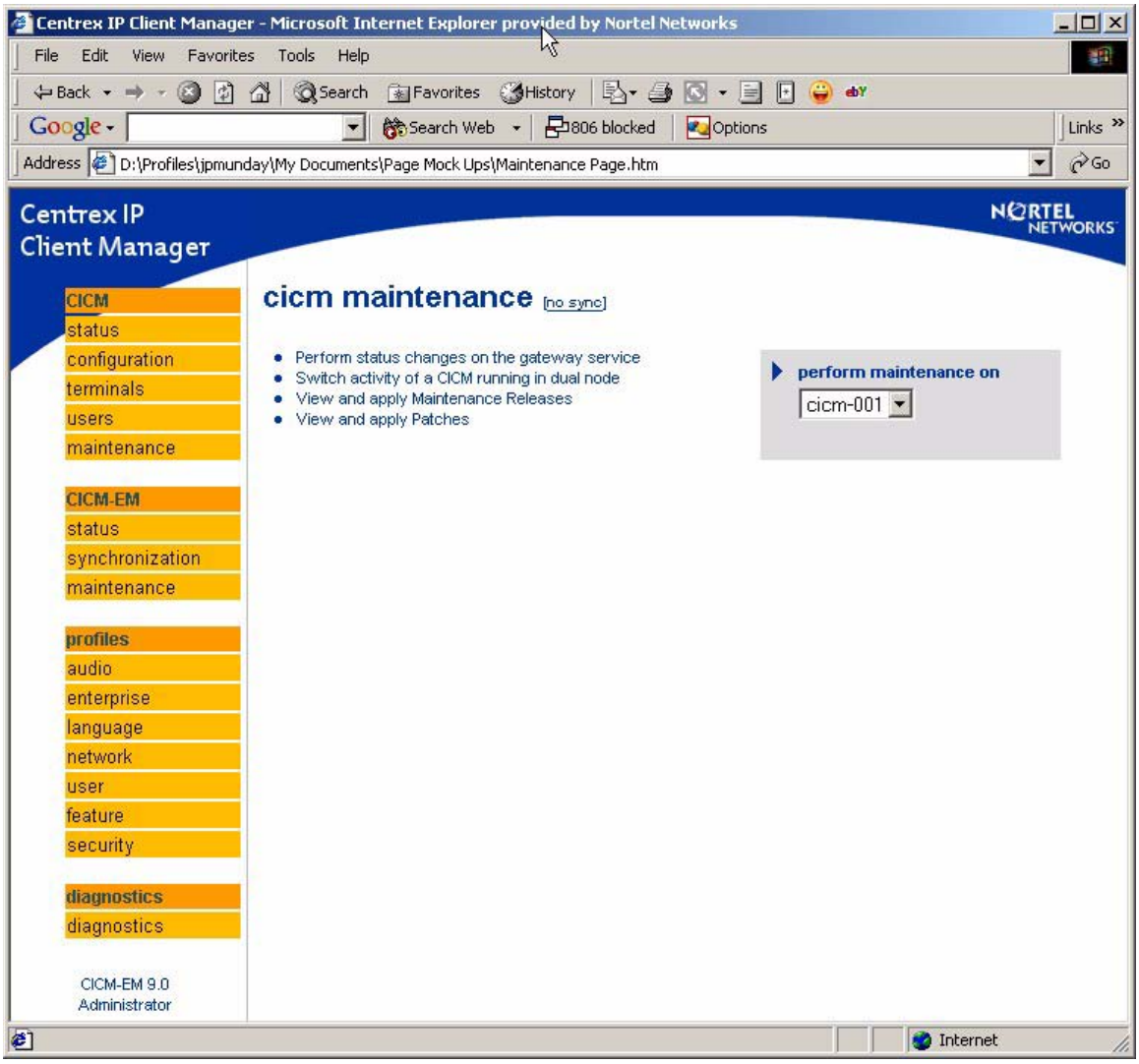


Figure 2 EM Maintenance Page

The diagram below shows the new web page layouts before and after the implementation of the SN09 patching features.

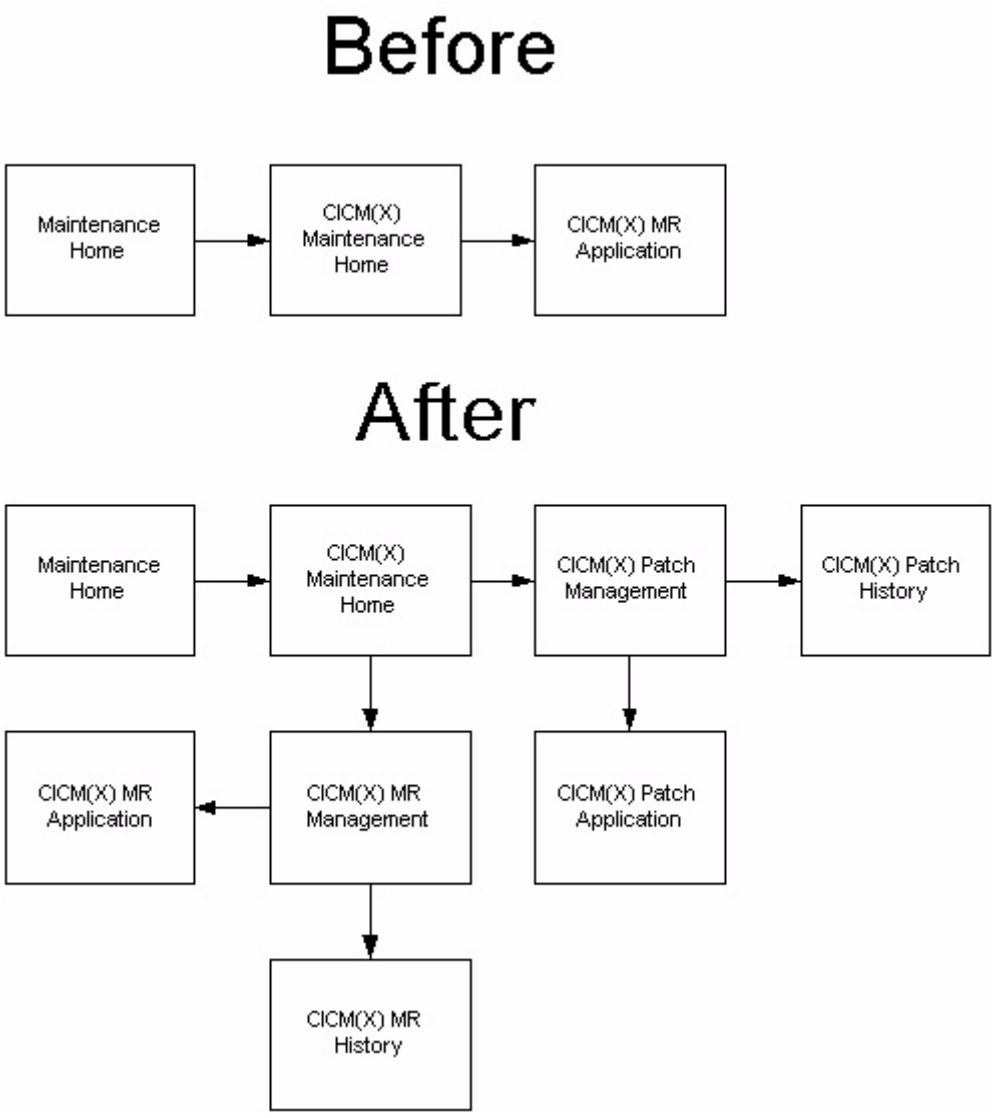


Figure 3 New Webpage access diagram

Once a user has selected the CICM node that they wish to carry out maintenance on they will be taken to the corresponding maintenance status page. The examples that follow show the maintenance and patching pages for a CICM, however the procedure and pages for applying a patch to a CICM-EM will be similar.

As with previous releases, the Maintenance Status page will display maintenance information for this CICM. In addition a new link will be available to allow access the patch management pages for a particular node on this CICM.

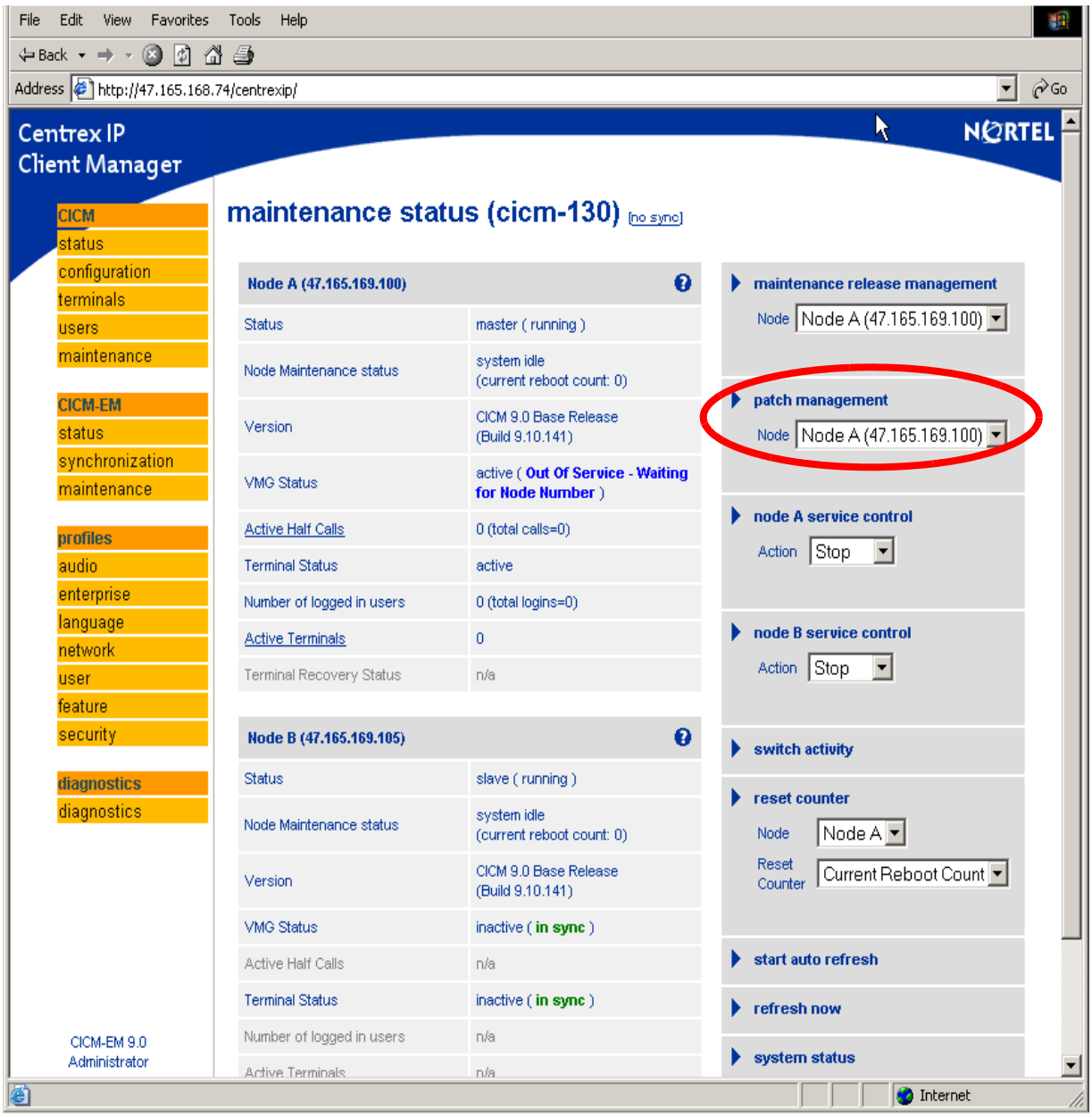


Figure 4 Maintenance Status Page

Selecting this link will take the user to the Patch Management page shown below…

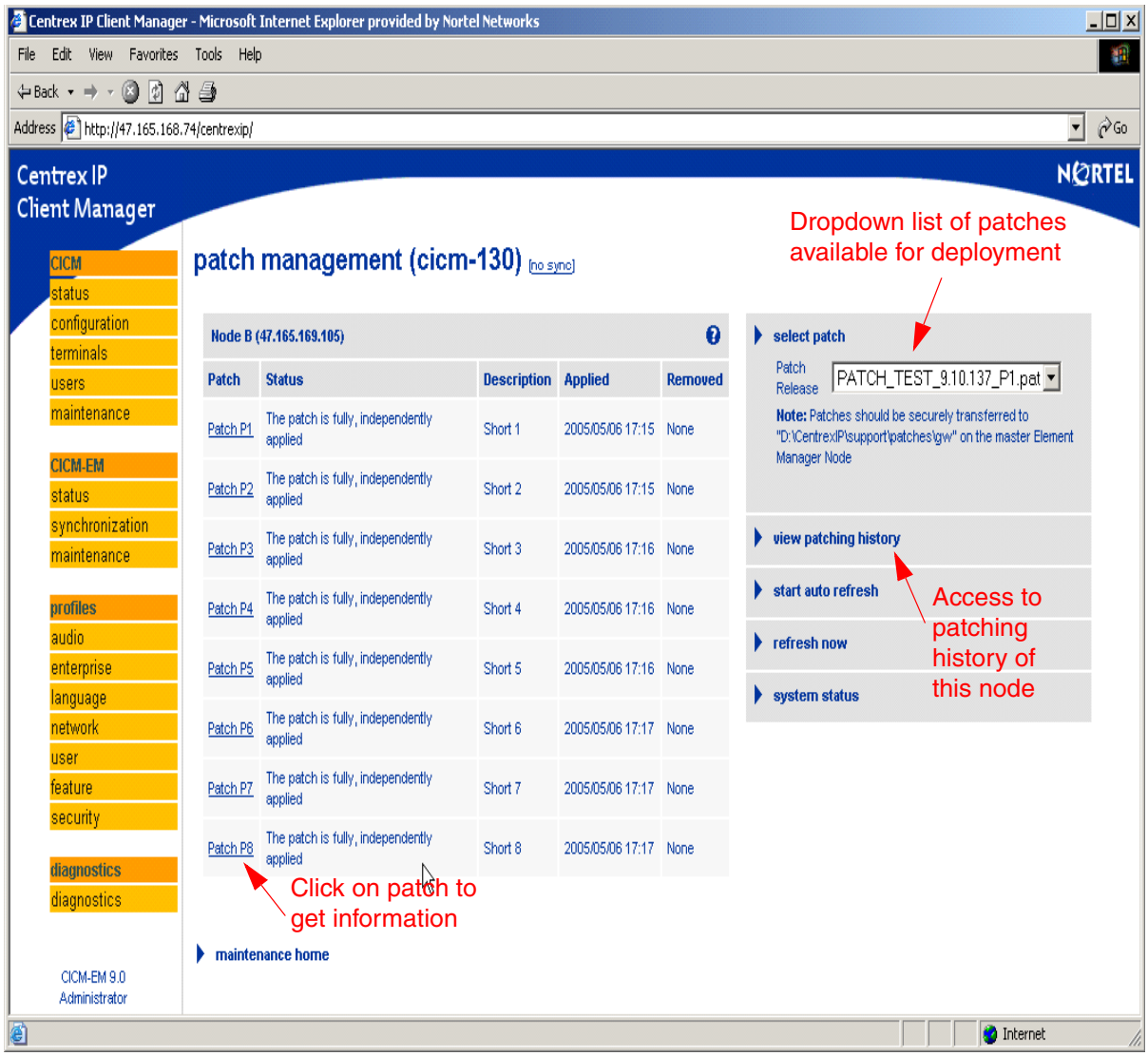


Figure 5 Patch Management Page

The patch management page shows a table of all patches that have been applied to this node **since the last Maintenance Release,** along with their application date and time, removal date and time (if applicable), a brief description and their status. This list is alphabetically ordered by Patch ID. Note that this Microsoft Windows convention of ordering will mean that patches 1, 2 and 10 will be ordered 1, 10 and 2. This ordering is independent of the order in which the patches were applied. To determine the application order the reader is referred to the paragraphs further down concerning the patch history page.

All patches will have a status of either ‘Applied’ – indicating that the corrective content of this patch is currently present on the system, ‘Removed’ – indicating that the corrective content of this patch has been removed by another patch or ‘Subsumed’ – indicating that the corrective content of the patch has been wholly subsumed by a later applied patch.

All patches copied into the patching directory on the Master Element Manager (D:\CentrexIP\support\patches) will be present in the ‘Select Patch’ dropdown menu.

When the user selects the patch to be applied from the dropdown list, they are taken to the patch application page shown below.

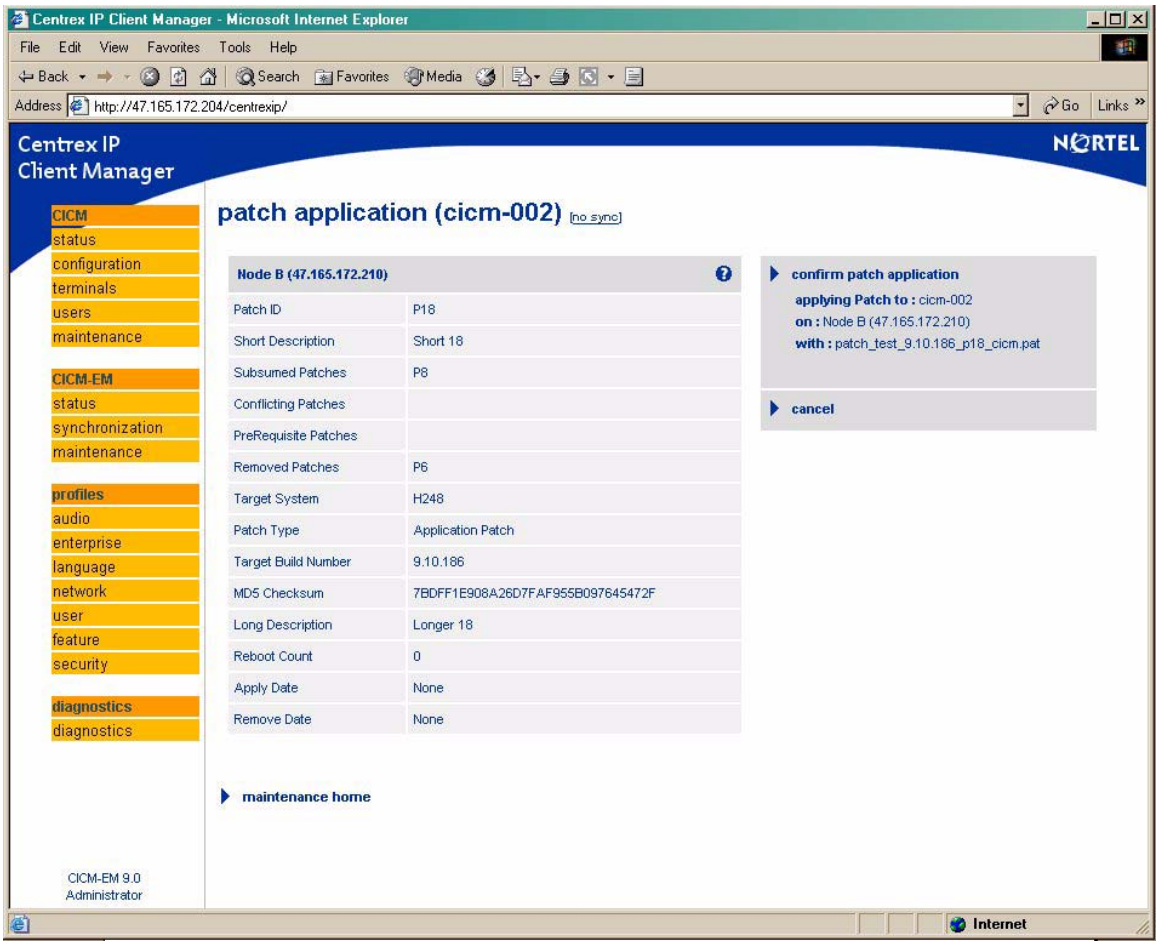


Figure 6 Patch Application Page

The Patch Application page will display all the details of the selected patch. Any conditions that would prevent this patch from being installed will be displayed in the right hand tab where the ‘confirm patch application’ link would normally appear.

If all Conflicts and Dependencies have been satisfied then the ‘Confirm Patch Application’ link will be enabled in order to allow patch application. Otherwise the link will be disabled along with details of why the patch cannot be applied, as shown.

The patch application page will display the following information.

Patch ID	The unique identifier for this patch
Target System	Indicates which type of node this patch can be applied to. This can be ‘H248 CICM’ or ‘CICM EM’. If this patch is not valid for this node type the ‘confirm patch application’ link will be disabled and replaced with a message indicating the conflict.
Target Build Number	Indicates the target release that this patch can be applied to. If this patch is not valid for this node type the ‘confirm patch application’ link will be disabled and replaced with a message indicating the conflict.
MD5 Checksum	The MD5 checksum of this patch file. The user should check that this checksum matches the checksum provided by Nortel for the patch file before applying the patch.
Description	A brief description of this patch
Conflicts	A list of patches with which this patch will conflict. Conflicts preventing installation will be shown in the right hand frame. *For more information see the section on Patch Version Control later.*
Dependencies	A list of patches upon which this patch is dependent. Dependencies preventing installation will be shown in the right hand frame. *For more information see the section on Patch Version Control later.*
Subsumes	A list of patches which are subsumed by this patch. Contained elements preventing installation will be shown in the right hand frame. *For more information see the section on Patch Version Control later.*
Removes	A list of patches which will be removed by this patch. Removed elements preventing installation will be shown in the right hand frame. *For more information see the section on Patch Version Control later.*
Reboot Count	The number of times the target system will reboot during the course of the patch application. See section “Selective Service Start-up and Shutdown” on page 610.
Short Description	The ‘patch title’ giving basic information on what this patch does.
Longer Description	More detailed information released by GNPS providing technical information on the patch.

Once the target system and all conflict and dependency checking as been satisfied, it is the responsibility of the user to ensure that the checksum

displayed for the patch file is identical to the checksum provided by Nortel before applying the patch.

Once this is done, the patch can be applied by clicking on the ‘Confirm Patch Application’ link. The user will then be taken to the Maintenance Status page where the status on the patch installation will be displayed. Patches can only be applied to the Slave node of a CICM or CICM-EM pair. However, application to the Master is permitted if the Slave is unavailable. The user will be shown a warning message in this scenario.

Assuming that the patch application is successful, the patch will appear on the Patch Maintenance page with a status of ‘Applied’. The user can now run sanity on the system or test the functionality of the patch.

If the patch installation fails for some reason, the patch will remain unapplied and will not be added to the list of applied patches on the Patch Management page. An entry will not be added into the patching history page. If the patch application failed during consistency checking the system service will not have been nor will be affected. If the application failed whilst the patch was actually being applied maintenance action may then be required to return the node to full service. In the event of a patch application installation failure in this latter case, customers are strongly recommended to contact the next level of support.

If the user wishes to view more detailed information on a previously applied patch, they can click on the Patch ID on the Patch Maintenance page. This will display the patch information page shown below.

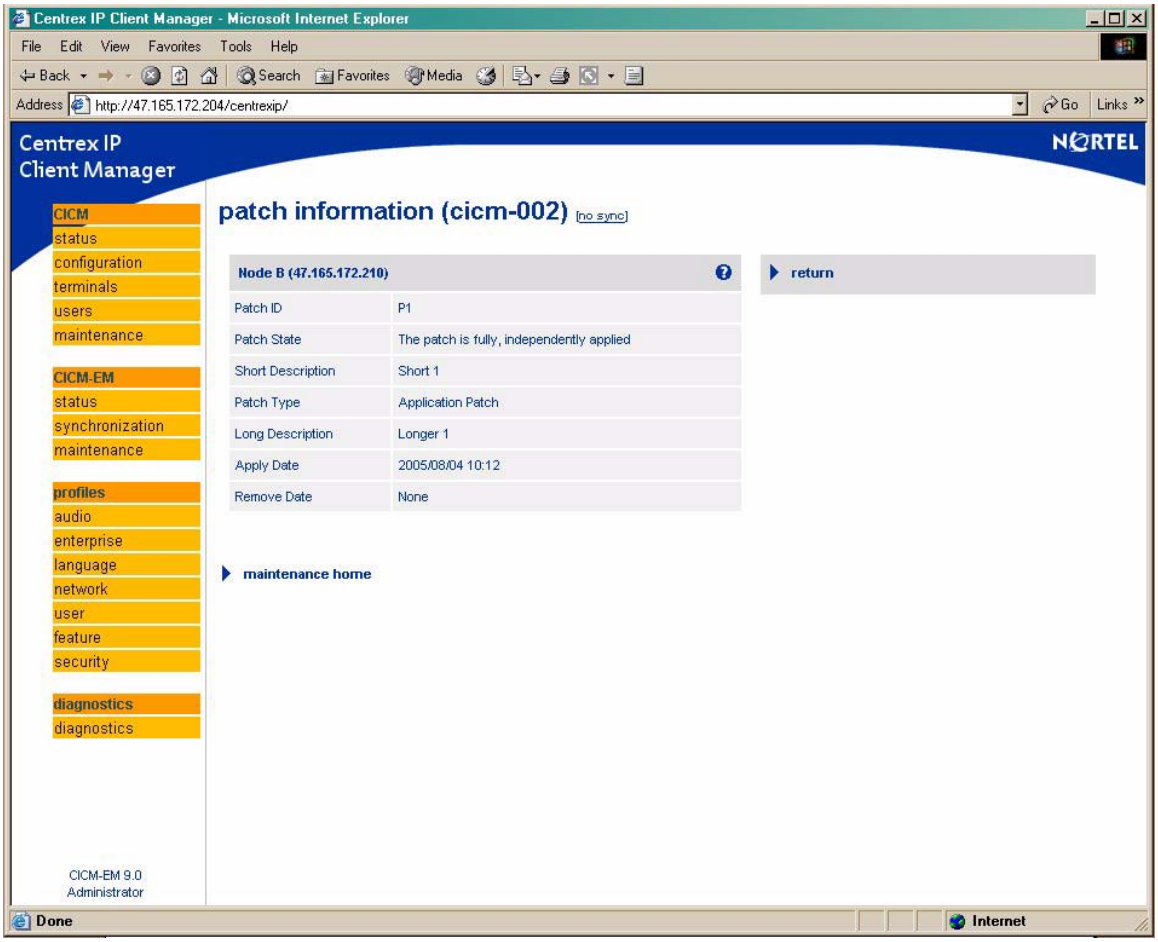


Figure 7 Patch Information Page

In addition, if a user wishes to view the patching history of a particular node, they can access the Patching History page via the ‘View Patching History’ link on the Patch Maintenance Page.

The Patching History page contains a list of all successful patching activity since the last Maintenance Release was applied. Details of patch applications, subsumations and removals will form this list.

A sample Patching History page is shown below.

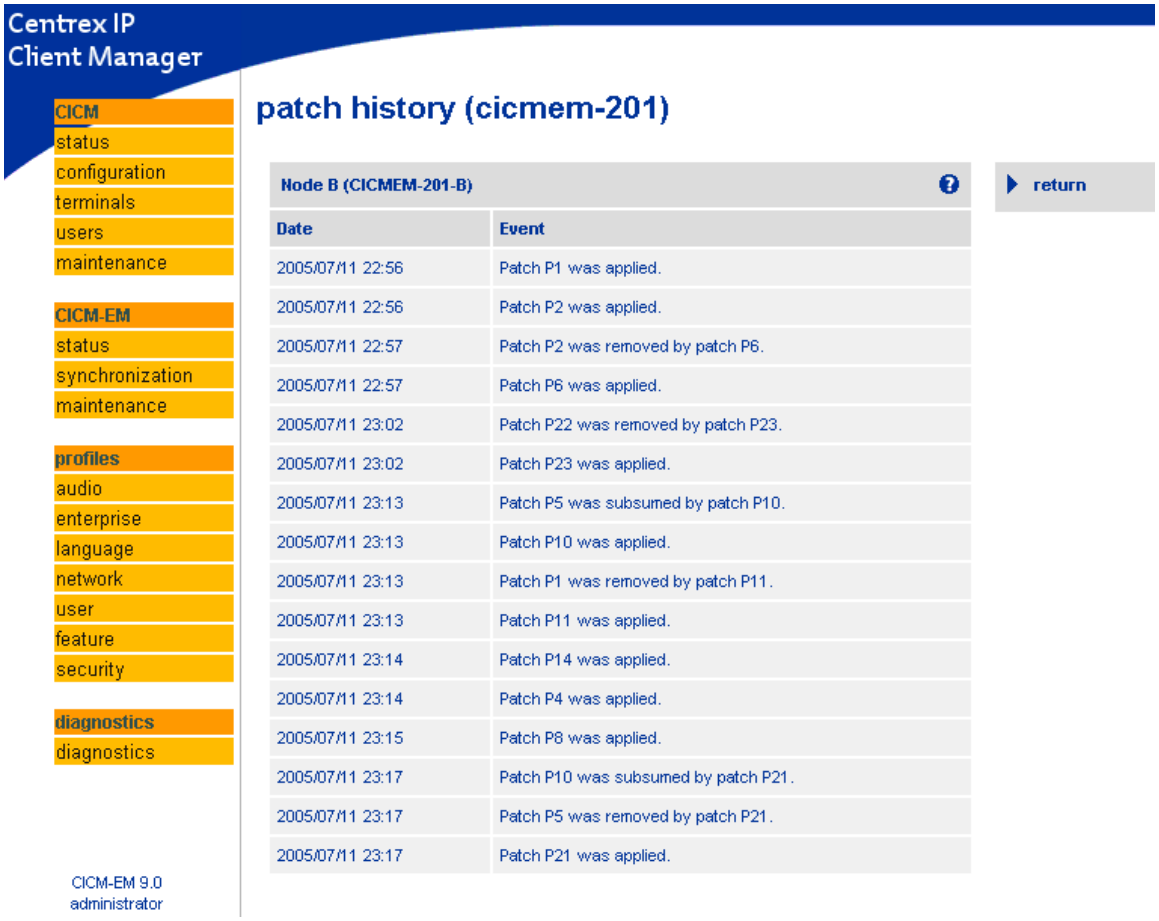


Figure 8 Patching History Page

When a Patch is not applied to the CICM or CICM-EM but it is in the removal list of a patch that was applied then the Patch History Page will still show the patch as removed (even though it may have never actually been applied). In this case the applied date field for the patch that was never applied will be “None”.

The possible states of patches are…

- The patch has been removed by another patch. A patch can not be re-applied to the system once it has been set to removed.
- The patch is fully, independently applied. The patch is independently applied and not subsumed by another. The ‘independence’ of a patch refers solely to subsumation i.e. whether it is contained in another patch or not. It does not have any bearing on the dependencies of the patch.
- The patch has been applied as a subsumation. This patch has been subsumed by another.

71.2.4 Maintenance Release Delivery and Application

Although the function of Maintenance Releases remains largely unchanged with the introduction of this feature, the addition of the Patching functionality will lead to changes in the deployment and application methods for installing an MR.

From SN09 Nortel GNPS will deploy Maintenance Releases to a customer in the form of a single MR file and a 128-bit MD5 checksum. The MR file and the checksum will be distributed separately in order to ensure the integrity of the Maintenance Release file.

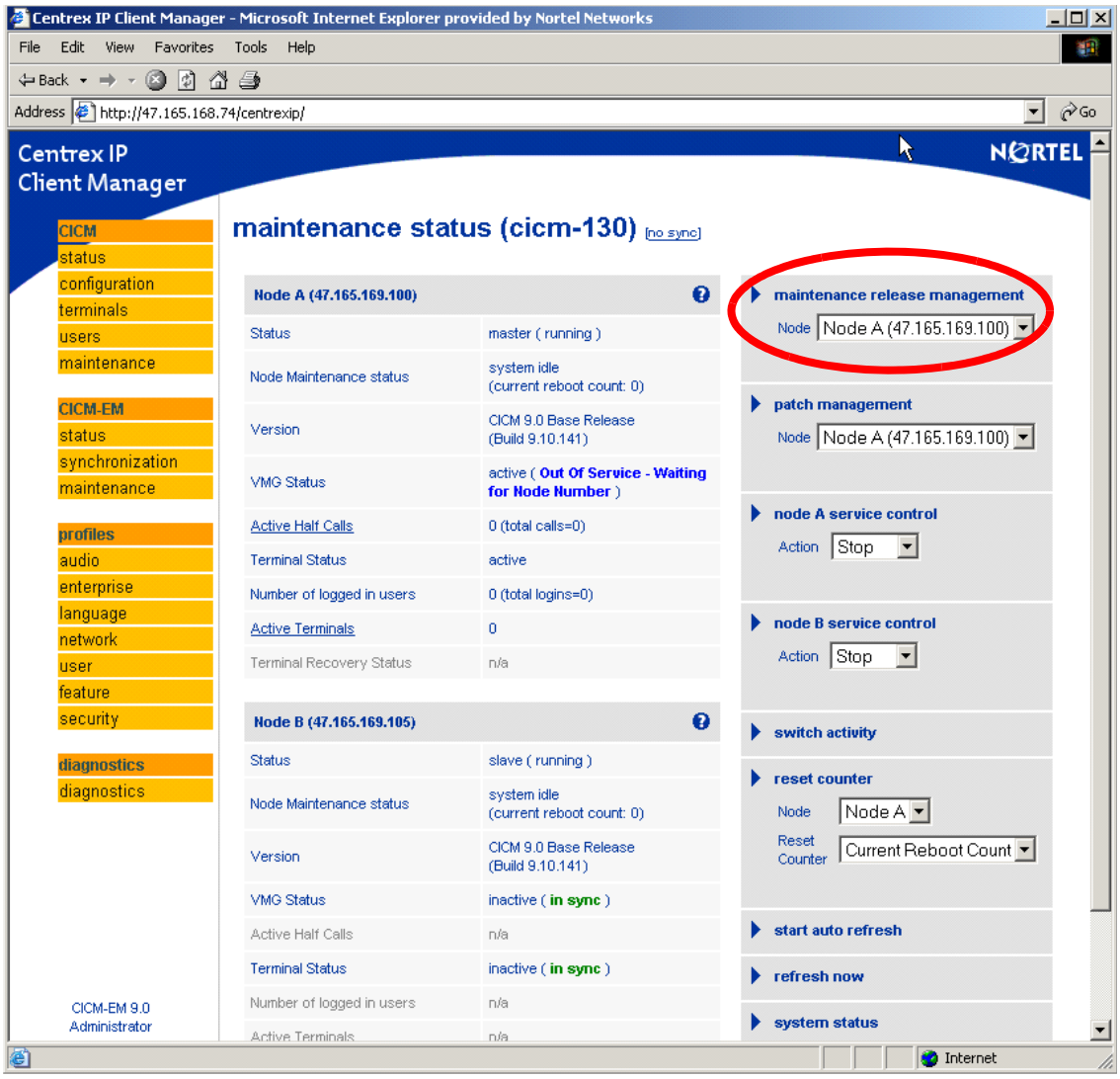


Figure 9 Maintenance Status Page

As with patches, the MR file will be delivered to the customer either via electronic transfer or on optical media. The MD5 checksum will be delivered to the customer either via e-mail or through it's publication on an externally accessible Nortel website.

Upon receiving the patch file, the customer will transfer the MR file into the Maintenance Release directory on the Master Element Manager (D:\CentrexIP\support\upgrades) via secure file transfer. Once there, the patch can be applied to any suitable node that is under the management of the CICM-EM.

From SN09, users will no longer be able to directly apply an MR from the main Maintenance Status page. Instead users will need to navigate to a new sub-Maintenance Release Management page from the main Maintenance Status page (see Figure 3).

The Maintenance Release Management page will display a table of all MRs that have been applied to this node along with their application time, date and status as shown below.

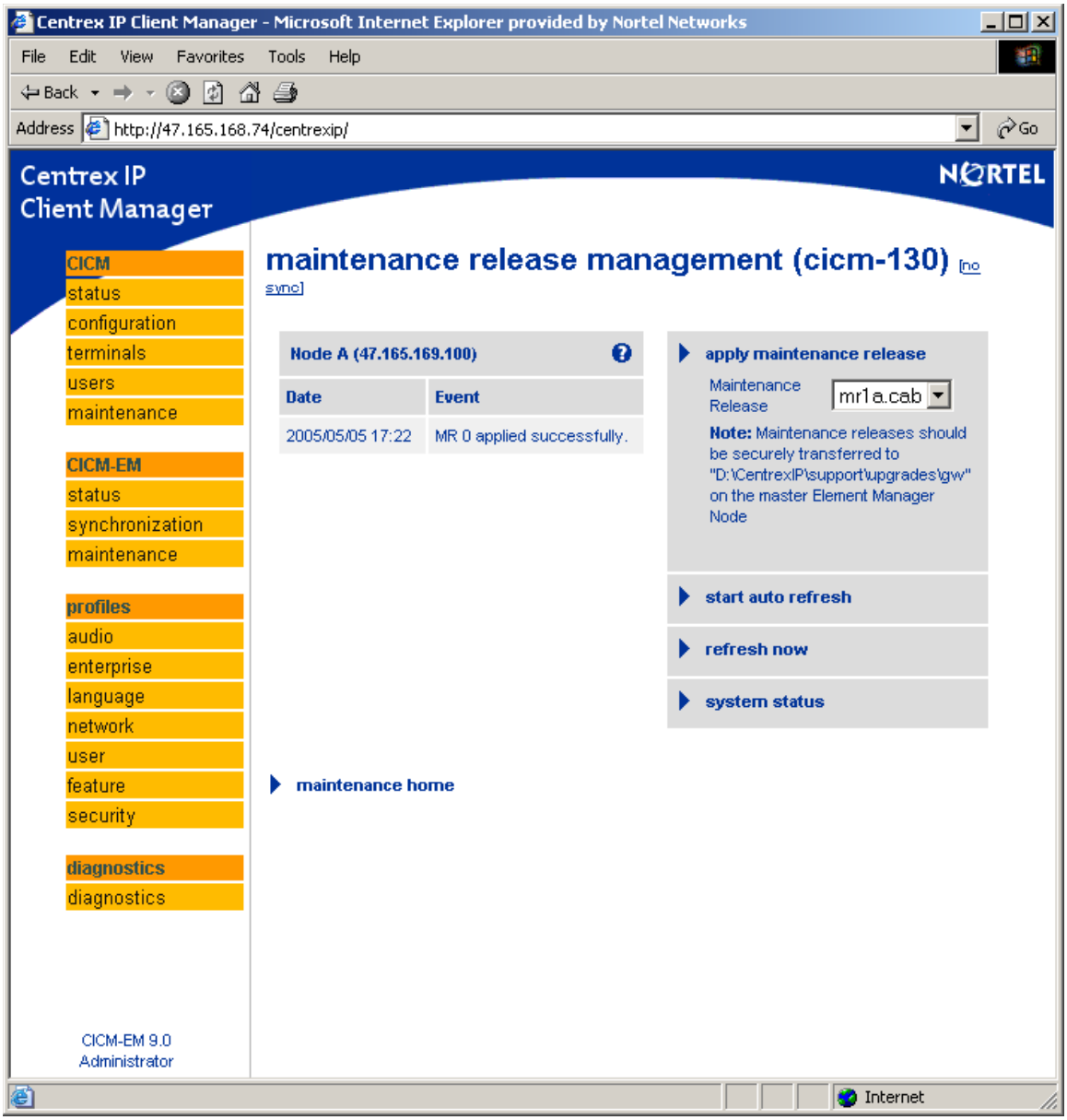


Figure 10 Maintenance Release Management Page

All MRs will have a status of ‘Applied’, since there is no way to remove an MR.

In addition, if a user wishes to view the patching history of a particular node, they can access the Patching History page via the ‘View Patching History’ link.

All Maintenance Releases copied into the MR directory on the Master Element Manager (D:\CentrexIP\support\upgrades) will be present in the ‘Select Patch’

dropdown menu. Once a user has selected the Maintenance Release to be applied from the dropdown list, they will be taken to the Maintenance Release Application page shown below.

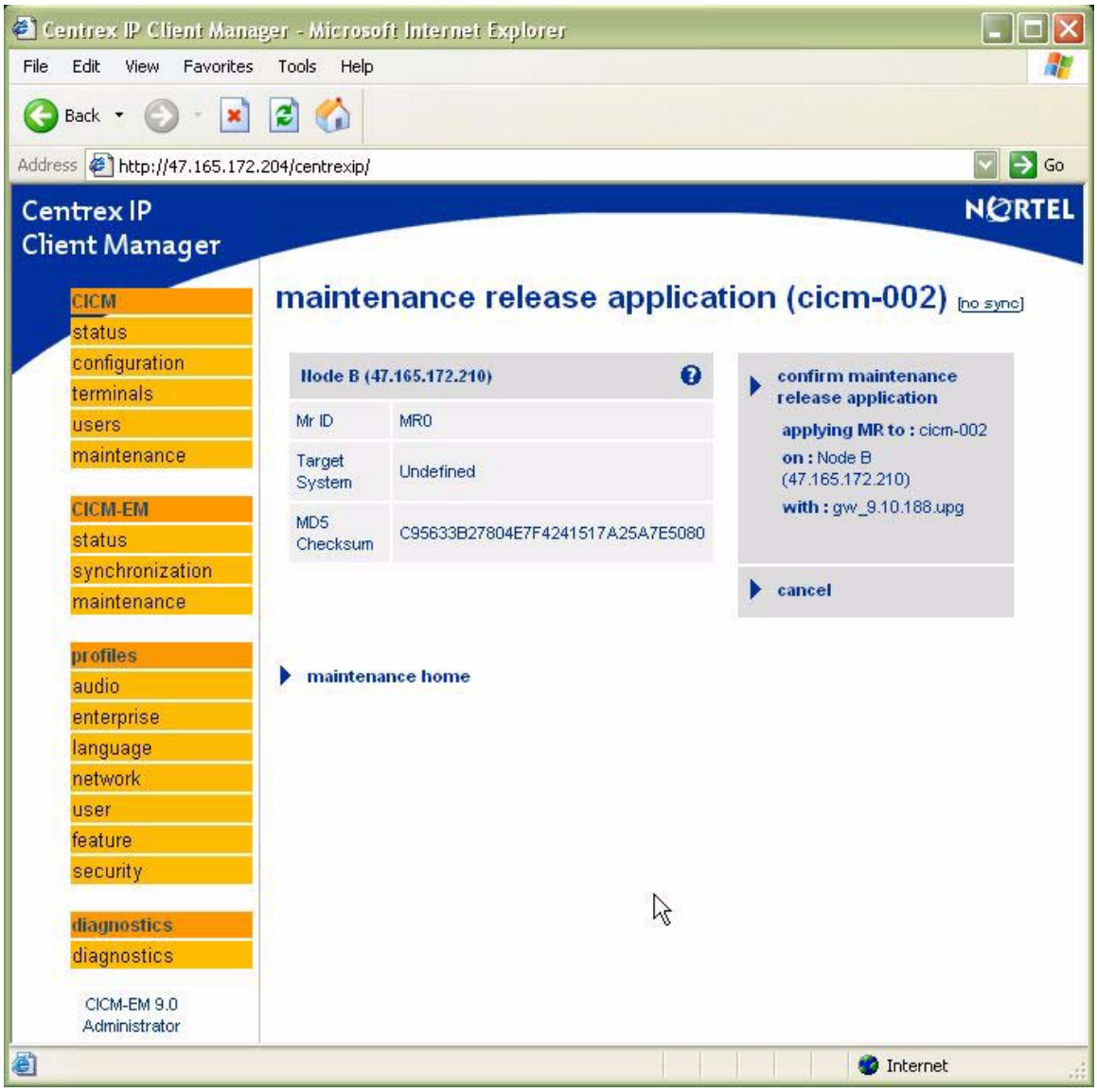


Figure 11 Maintenance Release Application Page

The Maintenance Release Application page will display all the details of the selected MR. If the selected node is of the correct system type and the MR has not already been installed, then the ‘Confirm MR Application’ link will be enabled in order to allow the application of the Maintenance Release. Otherwise the link will be disabled along with details of why the MR cannot be applied.

The Maintenance Release Application page will display the following information…

MR ID	The unique identifier for this MR
Checksum	The MD5 checksum of this patch file. The user should check that this checksum matches the checksum provided by Nortel for the Maintenance Release before applying the MR.
Target System	Indicates which type of node this patch can be applied to. This can be 'H248 CICM' or 'CICM EM'. If this patch is not valid for this node type it will be highlighted in Red.

It is the responsibility of the user to ensure that the checksum displayed for the patch file is identical to the checksum released for the patch by Nortel before applying the patch.

Once this is done, the Maintenance Release can be applied by clicking on the 'Confirm Patch Application' link. The user will then be taken to the Maintenance Status page where the status of the MR installation will be displayed. Assuming that the MR application is successful, it will appear on the Maintenance Release Management page with a status of 'Applied'.

If the MR installation fails for some reason, the MR will remain unapplied and will not be added to the list of applied MRs displayed on the Maintenance Release Maintenance page. As for patches, details concerning the failure will be generated in the debug log files.

In the event of a Maintenance Release installation failure, customers should contact the next level of Support.

71.2.5 Patch Version Control

The CICM and CICM-EM will follow an *independent* patching strategy. This means that as long each patch's rules for version control are satisfied…

- Customers can apply patches in any order they desire.
- Customers are not compelled to install *every* patch released by Nortel[1]

In order to allow this flexible independent patching strategy, whilst maintaining the overall sanity of the load content on the CICM and CICM-EM at all times, a patching version control system has been implemented.

This effectively defines what can and can not be applied to any particular CICM or CICM-EM. Overall load integrity and sanity is maintained by simply preventing incompatible content from being installed.

[1] Although customers should always follow the recommendation of Nortel CICM GNPS with regards to whether individual patches should be applied to in-service systems.

Patching Version Control is carried out by comparing records of what is currently installed on the system with information contained within each patch detailing its content and incompatibilities. If it is determined that the application of a particular patch would break one or more version control rules, then the 'Confirm Patch Application' link on the Patch Application page will be disabled, preventing the patch from being installed. In this instance, an the reason preventing the patch application will be given to the user so that corrective action can be taken.

Each patch will contain four lists defining its content, dependencies and conflicts as shown below.

Dependency List	This defines a list of patches that must be present on this node for this patch to be applied. If any of the patches contained within this list are not currently applied, then this patch cannot be applied.
Conflict List	This defines a list of patches which are incompatible with this patch. If any of the patches contained within this list are present on this node, then this patch cannot be applied. In addition, once applied, no patch contained within the conflict list of this patch can be applied without the removal of this patch first.
Subsumation list	This defines a list of all patches that are wholly subsumed (or contained) within in this patch. A patch can only subsume previously released patches. A patch which subsumes another patch contains fully the functionality of the previously released patch. Applying this patch will therefore also apply all the other patches contained within this list (if they are not already applied).
Removal list	This defines patches that will be removed by the application of this patch. Once applied, no patch contained within the removal list of this patch can be re-applied. Even if the patch has not been applied, the target system will not allow its application in the future.

When a patch is selected for application, the following simplified checks are carried out…

- The patch being installed must be of the correct type (CICM / CICM-EM) for the node it is about to be applied to.
- The build number of the target system must be that the patch is intended for.
- Each patch listed in the patch dependency list of the patch being installed must be presently installed on the system.
- None of the patches listed in the conflict list of the patch being installed may be presently installed on the system.
- None of the patches listed in the removal list of the patch being installed are present in the dependency lists of any of the currently applied patches.

- None of the patches listed in the content list of the patch being installed are present in the conflict or removal lists of any of the currently applied patches.

Only if ALL of the criteria above are met is the ‘Confirm Patch Application’ link enabled and the patch can be installed.

Once patch installation has been started ALL patches present in the Content list of the patch will be installed. Note that it is not possible to selectively install only some of the content of a patch.

Once a patch has been installed, the following changes are made to the patch content table on the node which the patch was applied to.

- All patches listed in the Content list of the patch applied are added to the list of applied patches with a status of 'Applied'.
- Any patches listed in the Removal list of the patch applied, that are present in the Applied Patch Table, will be changed to a status of 'Removed by <Patch ID>'.

In additional, the Dependency, Conflict, Content and Removal lists of the installed patch are stored on the node on which the patch was installed to assist with the version control checking of future patches.

71.2.6 Selective Service Start-up and Shutdown

An advantage the new patching functionality provides over the Maintenance Release functionality is that the application of a patch will not necessarily require a restart of the node that it is applied to, and may even be able to maintain service during its application.

Depending on the corrective content being delivered, the patch application software has the ability to apply a patch with either…

- A Full Node Outage (and loss of redundancy)
- A Partial Node Outage
- No Node Outage

The level of Service Outage required will always be defined by the patch. Patches that require a Full Service Outage will have the ‘Reboot Count’ field set to a non-zero number to indicate that as part of the patch installation the node will be rebooted and therefore be unavailable for a period.

Patches that have the ‘Reboot Count’ field set to nought will either require a Partial Service Outage or No Service Outage.

In the case of a patch that will need a partial service outage during installation, the exact level of the service outage that will be encountered, along with

exactly what service impact the customer can expect will be defined in the release notes of the patch by Nortel GNPS.

It is the responsibility of the craftsperson applying the patch to read and fully understand what impact the installation of a specific patch will have on an in-service system. And it is recommended that the supported patch installation procedure is always used when applying patched to in-service sites (see section 2.1.8 on Patching Procedure)

71.2.7 Patching Procedure

The following is the basic procedure for applying a patch to a pair of CICM nodes.

1 Take a system backup of the nodes being patched using the EM backup tool

2 SWACT call processing to Node A

3 Apply the patch to node B – should the patch installation fail, please stop and contact the next level of Support.

4 SWACT call processing to Node B

5 If possible verify the patch functionality and system sanity. If a problem is found, stop and contact the next level of Support.

6 Apply the patch to Node A – should the patch installation fail, please stop and contact the next level of Support.

7 SWACT call processing to Node A

8 If possible verify the patch functionality and system sanity. If a problem is found, stop and contact the next level of Support.

9 Patch installation is complete.

The following is the basic procedure for apply a patch to a pair of CICM-EM nodes.

1 Take a system backup of the nodes being patched using the EM backup tool

2 SWACT the CICM-EM if necessary so that Node A is the Master

3 Apply the patch to node B – should the patch installation fail, please stop and contact the next level of Support.

4 SWACT the CICM-EM so that Node A is the Master

5 If possible verify the patch functionality and system sanity. If a problem is found, stop and contact the next level of Support.

6 Apply the patch to Node A – should the patch installation fail, please stop and contact the next level of Support.

7 SWACT the CICM-EM so that Node A is the Master

8 If possible verify the patch functionality and system sanity. If a problem is found, stop and contact the next level of Support.

9 Patch installation is complete.

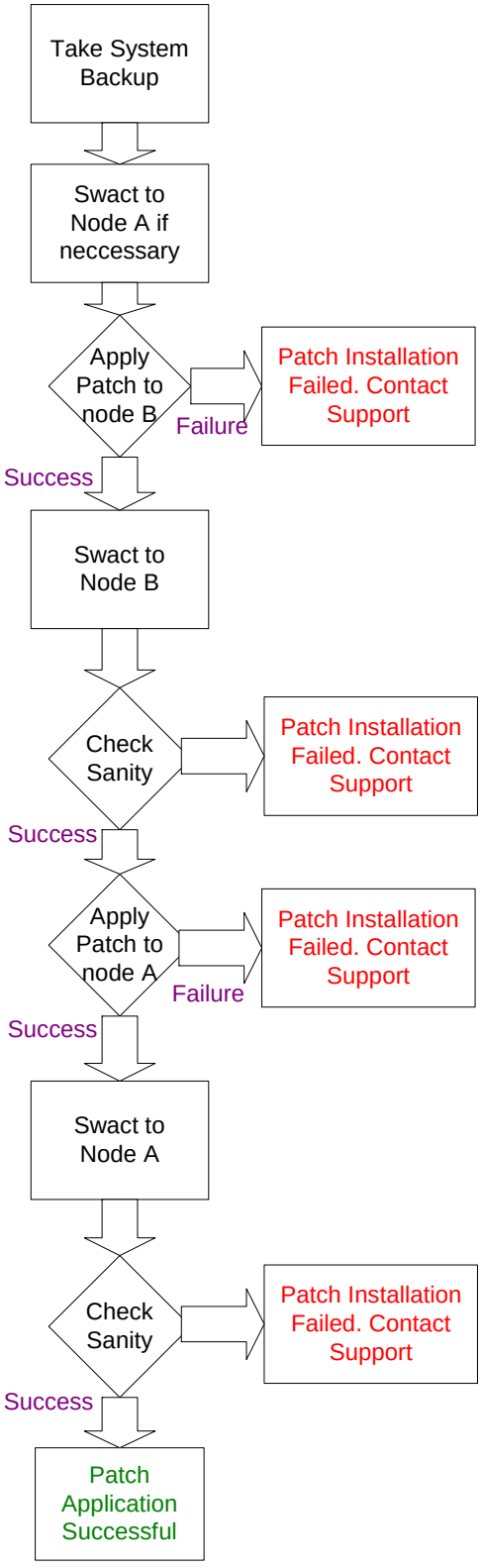


Figure 12 Patch Procedure

71.2.8 Maintenance Release Interaction with Patching

The web interface for Maintenance Release applications has been modified slightly. However from a functional point of view Maintenance Releases will be released and applied in exactly the same manner to the way they were before this feature was implemented.

The only minor exception is that from SN09 Maintenance Releases will be released with a checksum that should be checked to ensure integrity before application.

Maintenance Releases replace all application binaries on a system and apply all OS and Third Party Content up to a recognized and supported level (which is defined by the MR version).

An MR has no dependencies on the patch state of the target system before it is applied, since it is about to overwrite all content. Therefore an MR has no dependency or conflict lists and carries out no version checking against the current patch state before application. However, verification of the target type (CICM/CICM-EM) and upgrade path between build numbers is carried out.

Since a Maintenance Release overwrites all previous software versions, the record of all previous patches applied to this system will become irrelevant. For this reason, one impact of the application of a Maintenance Release is that it will erase the list of all currently applied patches. The content of this system is now defined by the MR version.

Normally the functionality of all the currently released patches will have been incorporated into a Maintenance Release. So although the record of applied patches has disappeared, the content of those patches will still be present on the system after the MR has been installed. A complete record of the content of a Maintenance Release, including all patches that it subsumes will be listed in its Release Notes of the Maintenance Release.

The current patch level of any system should be considered to be the MR version *plus* the patches listed in the applied patch list.

71.3 Hardware requirements

The SN09 Patching features introduce no new hardware dependencies or requirements.

The SN09 load is supported on:

- Motorola 5370 CPU cards
- Motorola 5385 CPU cards

71.4 Software Requirements or Dependencies

The Third Party Corrective Content Patching and Selective Binary Component Patching features are introduced in the SN09 CICM release. This load level must therefore be installed on any CICM-EM being used to apply a patch and on any CICM / CICM-EM that is being patched.

71.5 Limitations and restrictions

These features will only deploy Patches and Maintenance Releases built and released by Nortel CICM GNPS. Deployment of no other Patch or Maintenance Release files will be supported.

71.6 Interactions

This feature will modify the delivery of Maintenance Releases both by the inclusion of a Checksum for integrity checking and by the implementation of changes to the MR application web pages on the EM.

72: Functional description (FN): A00009378

72.1 Feature name and Feature ID

A00009378: LI Support of SIP Lines

72.2 Description

This feature provides the Call Data and Call Content interception functionality required to support Lawful Interception (LI) of calls originated by / terminated on SIP (Session Initiation Protocol) clients.

This document assumes that the reader is familiar with the United States Network Broadcast Delivery (USNBD) functionality as described in [1] and [2]. Therefore, only the functional areas that are modified or unique to SIP Line surveillances are covered by the subsequent sections.

72.2.1 Configuration and Administration Procedures

The list of procedures that can be performed by USNBD administrators and USNBD users are the following. The procedures with SIP Line specific behavior are highlighted in *italics*.

- Executing pre-provisioning requirements for USNBD
- *Configuring bearer channel tandeming (BCT) on an MS 200 series (AMS)*
- Activating software optionality control (SOC) option NBD00003
- Activating BCT
- Activating USNBD office-wide parameters
- Adding an agency
- Adding USNBD users
- *Creating call content resources (CCR*)
- Creating a call data channel (CDC)
- *Adding a surveillance*
- Listing a surveillance
- Associating a CDC with a surveillance
- Associating a CCR with a surveillance
- Activating a surveillance
- Deactivating a surveillance
- Taking down a surveillance
- Deleting a CCR

- Deleting a CDC
- Deleting USNBD agencies
- Deleting USNBD users
- Deactivating BCT
- Deactivating SOC option NBD00003
- Accessing LI-Specific operational measurements

72.2.1.1 Configuring BCT on AMS

A single SIP Line surveillance can result in multiple active surveillance sessions, since a SIP line agent supports multiple call appearances. This needs to be accounted for when enabling Lawful Intercept parameter on an Application Media Server (AMS). In other words, there should be sufficient AMSs / ports configured to support BCT on all targets that can be under Call Content surveillances

The required number of CCRs can be calculated using the formula in figure 1.

The total number of ports can be calculated by simply multiplying the required number of CCRs by the number of ports per CCR.

Figure 1 CCR Calculation

CCRs Required = (**A1** * **B1**) + (**A2** * **B2** * **m**)) * **C**

Where:

A1 Total number of non SIP Line surveillance expected on the switch

A2 Total number of SIP Line surveillances expected

B1 Percentage of A1 that requires call content delivery

B2 Percentage of A2 that requires call content delivery

C Average number of call content resources (CCR) for each surveillance. The maximum is 5.

m Maximum number of SIP Line call appearances (per line) that can be monitored simultaneously for call content. This is limited by the number of CCRs that can be assigned against each surveillance.

72.2.1.2 Creating CCRs

The SIP lines are not supported as CCR Call Content Channels (CCCs). In other words, the CR must use a line with a 10 digit DN, which is a "single party line" meeting the existing requirements with respect to the line class code and assigned options.

72.2.1.3 Adding a Surveillance

The SIP Line surveillances are provisioned against the line DN. When the surveillance is activated, multiple calls originating and terminating on the target are monitored.

If the call content is to be monitored, the number of calls that can be monitored for call content is limited by the number of CCRs that is assigned to the surveillance. A maximum of 5 CCRs can be assigned to each surveillance.

If both call data and call content monitoring are enabled for a given surveillance, the CDC messages are generated, even in the scenario where call content is not monitored due to CR unavailability.

72.2.2 Call Content Monitoring

72.2.2.1 Multi-Media Monitoring

SIP Lines support multi-media capabilities, which include video and Information Services.

This feature only supports monitoring of speech, 3.1 KHz audio, 64 Kb/s restricted and unrestricted data, and 64Kb/s unrestricted data rate adapted from 56Kb/s.

In other words, video and Information Services content is not monitored as FCC currently does not mandate monitoring of data for information services.

72.2.2.2 Private Network Interception (PNI)

Private Network Interception (PNI) provide the ability to intercept the call content of private network calls. The PNI also provides Internet Transparency (ITRANS) by allowing the USNBD user to specify if call content monitoring for private network should be enabled, when the media gateways of both call agents are behind the same intra-domain Network Address Translator (NAT).

The PNI can be enabled on individual surveillances. This capability is provided for surveillances associated with SIP Lines. All calls originated by or terminated on a SIP Line target is examined to determine the call content should be monitored. If the call content is not monitored as a result of PNI not being enabled, a "CCUnavailabe" CDC message is generated.

72.2.2.3 REFER Support

The call content monitoring associated with SIP REFER method is best described using the example scenarios listed in the subsequent sections. The monitored party (target) is identified with an asterisk.

All scenarios are based on party 'A' REFERing (party B) to C after A and B has established a call. Each scenario below examines the need to define multiple CCRs for a given surveillance depending on which agents are under being monitored.

72.2.2.3.1 Call Transfer to Target

Scenario:

1. A Calls B and establishes A<->B session
2. A REFER to C*, causing B<->C* session to be established. A drops out and is no longer part of the call.

In this scenario, two calls are monitored;

- A<->C*
- B<->C*

Only a single call (involving C*) needs to be monitored at a given time. Therefore, only one CCR needs to be associated with the C* surveillance.

72.2.2.3.2 Call Transfer by Associate to non-Target

Scenario:

1. A Calls B* and establishes A<->B* session
2. A REFER to C, causing B*<->C session to be established. A drops out and is no longer part of the call.

In this scenario, two calls are monitored;

- A<->B* (initial call)
- B*<->C

Only a single call (involving B*) needs to be monitored at a given time. Therefore, only one CCR needs to be associated with the B* surveillance.

72.2.2.3.3 Call Transfer by Associate to Target

Scenario:

1. A Calls B* and establishes A<->B* session

2. A REFER to C*, causing B*<->C* session to be established. A drops out and is no longer part of the call.

In this scenario, three calls are monitored;

- A<->B* (initial call)
- A<->C* (interim call)
- B*<->C*

Only a single call per subject needs to be monitored at a given time. Therefore, only one CCR needs to be associated with each B* and C* surveillances.

72.2.2.3.4 Call Transfer by Target to non-Target (1 Original Target)

Scenario:

1. A* Calls B and establishes A*<->B session
2. A* REFER to C, causing B<->C session to be established. A* drops out and is no longer part of the call.

In this scenario, two calls are monitored;

- A*<->B (initial call)
- A*<->C (interim call)

Two calls involving A* need to be monitored at a given time. Therefore, 2 CCRs need to be associated with A* surveillance. Otherwise, the A*<->C call content is not monitored.

72.2.2.3.5 Call Transfer by Target to Target (1 Original Target)

Scenario:

1. A* Calls B and establishes A*<->B session
2. A* REFER to C*, causing B<->C* session to be established. A* drops out and is no longer part of the call.

In this scenario, three calls are monitored;

- A*<->B (initial call)
- A*<->C* (interim call)
- B<->C*

Two calls involving A* need to be monitored at a given time. Therefore, 2 CCRs need to be associated with A* surveillance. Otherwise, the A*<->C* call content is not monitored.

72.2.2.3.6 Call Transfer by Target to non-Target (2 Original Targets)

Scenario:

1. A* Calls B* and establishes A*<->B* session
2. A* REFER to C, causing B*<->C session to be established. A* drops out and is no longer part of the call.

In this scenario, three calls are monitored;

- A*<->B* (initial call)
- A*<->C (interim call)
- B*<->C

Two calls involving A* need to be monitored at a given time. Therefore, 2 CCRs need to be associated with A* surveillance. Otherwise, the A*<->C call content is not monitored.

72.2.2.3.7 Call Transfer by Target to Target (2 Original Targets)

Scenario:

1. A* Calls B* and establishes A*<->B* session
2. A* REFER to C*, causing B*<->C* session to be established. A* drops out and is no longer part of the call.

In this scenario, three calls are monitored;

- A*<->B* (initial call)
- A*<->C* (interim call)
- B*<->C*

Two calls involving A* need to be monitored at a given time. Therefore, 2 CCRs need to be associated with A* surveillance. Otherwise, the A*<->C call content is not monitored.

72.2.2.4 Support for SIP 4XX Responses

To be completed after base prototype is completed.

72.2.3 Call Data Monitoring

72.2.3.1 REFER Support

The call data monitoring associated with SIP REFER method is best described using the examples listed in the subsequent sections. The monitored party

(target) is identified with an asterisk. The legend below explains other symbols and notations being used.

Table 6: Legend

Symbol	Explanation	Example
A, B, C	DNs of the agents involved in the call	CalledPartyIdentity - A / Pa
Nx	Sequence Number	CallIdentity - SequenceNo : N1
Pa, Pb, Pc	Ports of the agents involved in the call	CalledPartyIdentity - C / Pc

Note: For simplicity, the examples do not include the CCOpen and CCClose Call Data messages, even though they are being generated for the scenarios presented below.

72.2.3.1.1 Call Transfer to Target

Scenario:

1. A Calls B and establishes A<->B session
2. A REFER to C*, causing B<->C* session to be established. A drops out and is no longer part of the call.

In this scenario, two calls are monitored;

- A<->C*
- B<->C*

CDC Messages Generated as a result of REFER:

Table 7: CDC MEssages - Scenario 1

Message	Parameter Attribute Values	Notes
TerminationAttempt	CallIdentity - SequenceNo : N1	A to C* call
	CallingPartyIdentidy - A / Pa	
	CalledPartyIdentity - C / Pc	
Connect	CallIdentity - SequenceNo : N1	
	ConnectPartyIdentities - A / Pa, C / Pc	
Answer	CallIdentity - SequenceNo : N1	
	AsweringPartyIdentity - C / Pc	
Disconnect	CallIdentity - SequenceNo : N1	
Release	CallIdentity - SequenceNo : N1	
TerminationAttempt	CallIdentity - SequenceNo : N2	B to C* call
	CallingPartyIdentidy - B / Pb	
	CalledPartyIdentity - C / Pc	
Connect	CallIdentity - SequenceNo : N2	
	ConnectPartyIdentities - B / Pc, C / Pc	
Answer	CallIdentity - SequenceNo : N2	
	AsweringPartyIdentity - C / Pc	

72.2.3.1.2 Call Transfer by Associate to non-Target

Scenario:

1. A Calls B* and establishes A<->B* session
2. A REFER to C, causing B*<->C session to be established. A drops out and is no longer part of the call.

In this scenario, two calls are monitored;

- A<->B* (initial call)
- B*<->C

CDC Messages Generated as a result of REFER:

Table 8: CDC MEssages - Scenario 2

Message	Parameter Attribute Values	Notes
Disconnect	CallIdentity - SequenceNo : N1	A to B* call
Origination	CallIdentity - SequenceNo : N2	B* to C call
	CallingPartyIdentidy - B / Pb	
	CalledPartyIdentity - C / Pc	
	Input - UserInput: <dialed digits>	
Connect	CallIdentity - SequenceNo : N2	
	ConnectPartyIdentities - B / Pb, C / Pc	
Answer	CallIdentity - SequenceNo : N2	
	AsweringPartyIdentity - C / Pc	

72.2.3.1.3 Call Transfer by Associate to Target

Scenario:

1. A Calls B* and establishes A<->B* session
2. A REFER to C*, causing B*<->C* session to be established. A drops out and is no longer part of the call.

In this scenario, three calls are monitored;

- A<->B* (initial call)
- A<->C* (interim call)
- B*<->C*

CDC Messages Generated as a result of REFER:

Table 9: CDC MEssages - Scenario 3

Message	Parameter Attribute Values	Notes
TerminationAttempt	CallIdentity - SequenceNo : N2	A to C* call
	CallingPartyIdentidy - A / Pa	
	CalledPartyIdentity - C / Pc	
Connect	CallIdentity - SequenceNo : N2	
	ConnectPartyIdentities - A / Pa, C / Pc	
Answer	CallIdentity - SequenceNo : N2	
	AsweringPartyIdentity - C / Pc	
Disconnect	CallIdentity - SequenceNo : N1	HOLD A to B* call
Disconnect	CallIdentity - SequenceNo : N2	A to C* call Released
Release	CallIdentity - SequenceNo : N2	
Origination	CallIdentity - SequenceNo : N3	B* to C* call
	CallingPartyIdentidy - B / Pb	
	CalledPartyIdentity - C / Pc	
	Input - UserInput: <dialed digits >	
Connect	CallIdentity - SequenceNo : N3	
	ConnectPartyIdentities - B / Pb, C / Pc	
TerminationAttempt	CallIdentity - SequenceNo : N3	
	CallingPartyIdentidy - B / Pb	
	CalledPartyIdentity - C / Pc	
Connect	CallIdentity - SequenceNo : N3	
	ConnectPartyIdentities - B / Pc, C / Pc	
Answer	CallIdentity - SequenceNo : N3	
	AsweringPartyIdentity - C / Pc	
Release	CallIdentity - SequenceNo : N1	A to B* call released

72.2.3.1.4 Call Transfer by Target to non-Target (1 Original Target)

Scenario:

1. A* Calls B and establishes A*<->B session
2. A* REFER to C, causing B<->C session to be established. A* drops out and is no longer part of the call.

In this scenario, two calls are monitored;

- A*<->B (initial call)
- A*<->C (interim call)

CDC message details to be completed after base prototype is completed.

72.2.3.1.5 Call Transfer by Target to Target (1 Original Target)

Scenario:

1. A* Calls B and establishes A*<->B session
2. A* REFER to C, causing B<->C* session to be established. A* drops out and is no longer part of the call.

In this scenario, two calls are monitored;

- A*<->B (initial call)
- A*<->C (interim call)

CDC message details to be completed after base prototype is completed.

72.2.3.1.6 Call Transfer by Target to non-Target (2 Original Targets)

Scenario:

1. A* Calls B* and establishes A*<->B* session
2. A* REFER to C, causing B*<->C session to be established. A* drops out and is no longer part of the call.

In this scenario, three calls are monitored;

- A*<->B* (initial call)
- A*<->C (interim call)
- B*<->C

CDC message details to be completed after base prototype is completed.

72.2.3.1.7 Call Transfer by Target to Target (2 Original Targets)

1. A* Calls B* and establishes A*<->B* session
2. A* REFER to C*, causing B*<->C * session to be established. A* drops out and is no longer part of the call.

In this scenario, three calls are monitored;

- A*<->B* (initial call)
- A*<->C (interim call)
- B*<->C

CDC message details to be completed after base prototype is completed.

72.2.3.2 Support for SIP 4XX Responses

To be completed after base prototype is completed.

72.3 Hardware Requirements or Dependencies

SIP Line LI works with the base hardware used by USNBD. In other words, no SIP Line specific hardware is needed for monitoring SIP Line calls.

72.4 Software Requirements or Dependencies

This feature depends on the functionality provided by the following SIP Line features.

- A00007547 - SIP Lines Core Call Processing Support
- A00008234 - GWC Development for Support of CS2K SIP Lines
- A00008556 - SIP Core OAMP support
- A00009239 - SIP Lines Client Services Support

72.5 Limitations and restrictions

- A maximum of 5 basic calls per SIP Line surveillance can be simultaneously monitored for call content
- The maximum number of surveillances that can be provisioned is 1024. This can be reduced based on the number of provisioned CCRs, if the call content is to be monitored.
- The maximum number of surveillances that can be active is 1024.
- Video and Information Services media monitoring is not supported.
- SIP line DNs are not supported as dedicated CCR Call Content Channels.

72.6 Interactions

This feature provides the LI capability where SIP Lines interworks with non-SIP agents. This includes the following scenarios.

- Only the SIP Line is under surveillance
- Only the non-SIP Line agent is under surveillance
- Both SIP and non-SIP Line agents are under surveillance

The LI follow capability and replacement party monitoring (MRP) are supported in the following contexts

- Only the SIP-LInes are involved in the call
- The SIP-Line agents interwork with the non-SIP Line agents

Table 10, "SN09 SIP Line Feature Interactions," on page 629 lists the LI support of SIP Line features for each of the following monitoring categories.

- Subject: A status of Y indicates that monitoring of subject's call leg is supported if the feature is present on the call leg. A status of N indicates that USNBD does not monitor the call leg if the feature is present on the subject's call leg.
- MRP: A status of Y indicates that monitoring of Monitored Replacement Party's (MRP) call leg is supported if the feature is present on the call leg. A status of N indicates that, USNBD does not monitor the call leg if the feature is present in the MRP's call leg.
- Redirect: A status of Y indicates that the feature supports redirection and an MRP is provided. A status of N indicates that an MRP is not provided, if the call is redirected.

The status of Subject / MRP / Redirect can be augmented with one of the following notes to clarify any special handling.

a. Valid only for CENTREX

b. Monitoring will end if the feature is activated on the call leg

c. The LEA is provided with the required information, but the Release message includes the "non-monitored feature" Reason parameter.

d. Monitoring ends if bridging by other MADN members occurs.

Table 10: SN09 SIP Line Feature Interactions

Feature	Description	Subject	MRP	Redirect
3WC	Three-Way call	Y	Y	Y (a.)
ACRJ	Anonymous Caller Rejection	Y		
CCW	Cancel Call Waiting	Y	Y	
CFB	Call Forward Busy	Y		Y
CFD	Call Forwarding Don't Answer	Y		Y
CFDA	Call Forward Don't Answer	Y		Y
CFU	Call Forwarding Universal	Y		Y
CHD	Hold Call	N (b.)	N (b.)	
CLI	Calling Line Identification	Y	Y	
CNF	Conference	Y	N (b.)	
COT	Customer Originated Trace	Y (c.)		
CWT	Call Waiting	Y	Y	
CXR	Call Transfer (REFER)	Y	Y	Y
DND	Do Not Disturb	Y		
HOLD	Hold (connection)	Y	?	?
KSMOH	Keyset Music on Hold	Y	Y	
LNR	Last Number Redial	Y		
MMC	Meet-Me Conference	Y	?	?
MPB	MultiParty Bridging	Y	Y	Y
PRECONF	Preset Conference	Y	N (b.)	
RSUS	Requested Suspension	Y		
SCA	MADN Single Call Arrangement	Y	Y (d.)	
SCF	Selective Call Forwarding	Y		Y
SCRJ	Selective Call Rejection	Y	Y	

Table 10: SN09 SIP Line Feature Interactions

Feature	Description	Subject	MRP	Redirect
SDY	AT & T Line study	Y	Y	
SIMRING	Simultaneous Ringing	N?	N?	
SMDR	Station Message Detailed Recording	Y	Y	
SUPPRESS	Suppress Line Id	Y		
SUS	Suspend Service	Y		

72.7 Glossary

Term	Description
BCT	Bearer Channel Tandeming
CCC	Call Content Channel
CCR	Call Content Resource
CDC	Call Data Channel
LEA	Law Enforcement Agency
LI	Lawful Intercept
MRP	Monitored Replacement Party
SIP	Session Initiation Protocol
USNBD	United States Network Broadcast Delivery

72.8 References

[1] NN10190-113 Lawful Intercept

[2] USNBDFSD - USNBD Feature Specification Document (PLS FMDOC)

73: Functional description (FN): A00009417

73.1 Feature name and Feature ID

Cold Cache Recovery. Feature Number A00009417

73.2 Description

This feature adds the ability for a standby Session Manager to be fully synchronized with the provisioning manager when the Session Manager is set to active.

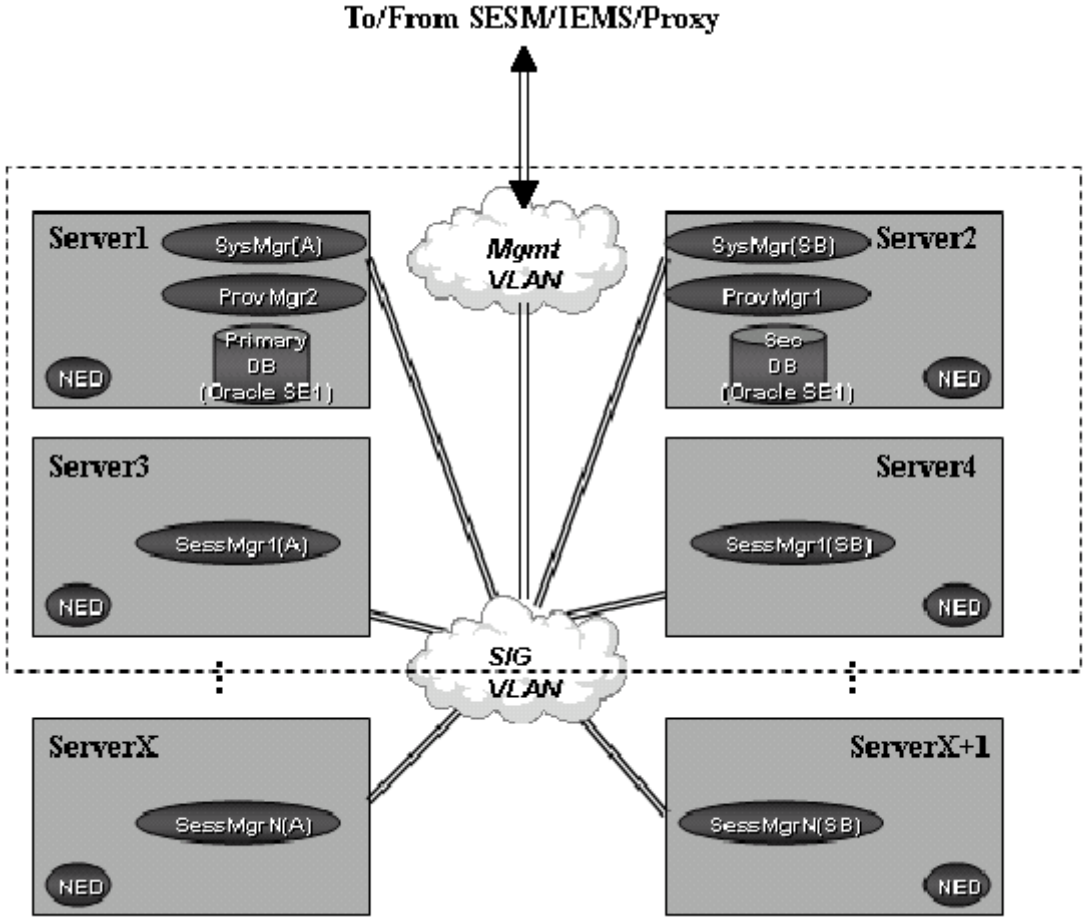
This feature is divided into two separate tasks. First, the Session Manager's In Memory Database (IMDB) tables must be synchronized with the data maintained by the provisioning manager. Synchronization between the Session Manager and the Provisioning Server is presently implemented by the Data Synchronization software. Unfortunately, MCP Data Synchronization relies upon the SIP NOTIFY message, and standby Session Managers are not able to receive and process NOTIFY messages since their Service Address (i.e. SIP listening address) is not enabled until the Session Manager goes active. This feature will convert the synchronization of data from the NOTIFY method to the Event Framework which does not require the Service Address to be enabled.

Secondly, the Session Manager presently employes a "lazy cache" method to populate the Subscriber tables. This lazy cache method involves not requesting Subscriber data until it is IMDB required by IPTel for session processing (call, IM, collaboration, etc.) processing. Features such as CallP Checkpointing require that the Subscriber data be known at the time the Session Manager goes from standby to active. This feature will now load and maintain the Subscriber IMDB tables while the Session Manager is in standby mode.

73.3 Hardware Requirements or Dependencies

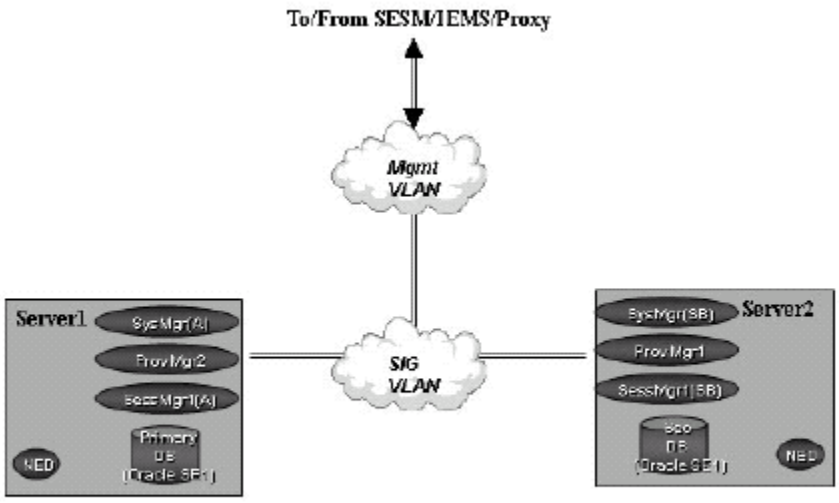
The diagram below represents the MSM configuration for 35000 subscribers. In this diagram, Server 3 and 4 represent an active/standby pair for Session manager instance 1 (SessMgr1). Server 3 is the active instance signified by the (A) and Server 4 represents the standby instance signified by (SB).

Figure 1: 35000 Subscriber System



The following diagram represents the configuration for 15000 subscribers. In this diagram, SessMgr1(SB) represents the standby instance for SessMgr1(A), the active instance.

Figure 2: 15000 Subscriber System



The diagrams above do not represent the only configuration possible.

73.4 Software Requirements or Dependencies

This feature is part of the MCP 9.0 release.

73.5 Limitations and restrictions

The time required for a Session Manager to start will be increased due to the fact that all Subscribers will be loaded at initialization time.

73.6 Interactions

This feature will speed up call processing in that IPTel will no longer be required to query the database for a new subscriber. All subscribers will be loaded into the Subscriber IMDB table prior to any session activity.

This feature will make extensive use of the Event Framework mechanism. The Event Framework uses a TCP socket monitored by a UDP ping (Perfect Channel). The Event Framework allows one MCP Network Element (NE) to send an event to another MCP NE.

73.7 Glossary

Term	Description
IMDB	In Memory Database
SIP	Session Initiation Protocol
IPTel	The MCP procession entity for SIP sessions
NOTIFY	A SIP message used to notify a SIP server of some activity

74: Functional description (FN): A00009418

74.1 Feature name and Feature ID

MCS as a 3G Application Server, activity A00009418

74.2 Introduction: 3GPP Network Overview

The 3GPP Application Server (AS) is one of the nodes of the IP Multimedia Core Network Subsystem (IMS) of the Core Network (CN) infrastructure in a 3GPP PLMN.

The intent of the IMS, is to enable the convergence of, and access to, voice, video, messaging, data and web-based technologies for the wireless user, and to combine the growth of the Internet with the growth in mobile communications.

The role of the AS in the IMS is to offer value added IP Multimedia (IM) services by hosting and executing network and user level services.

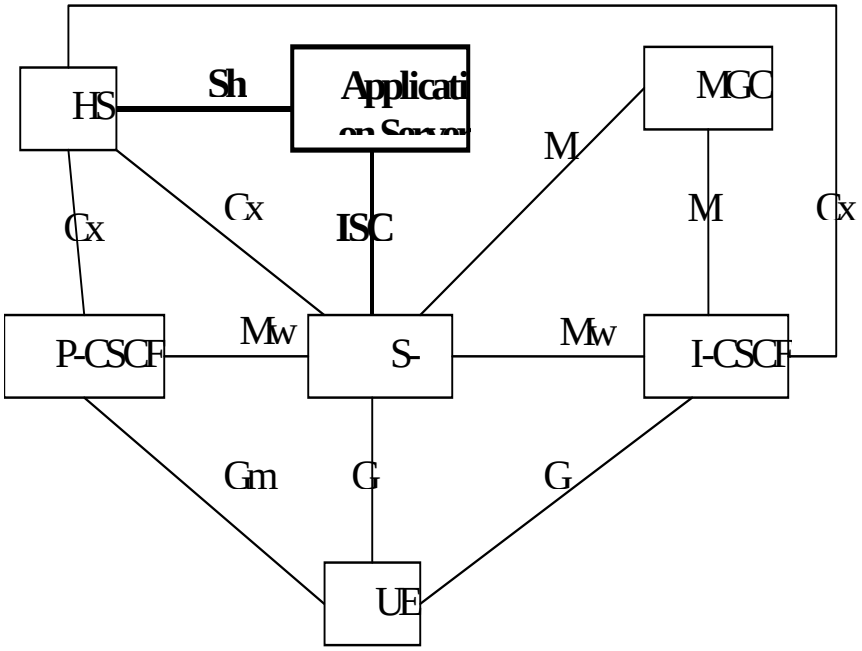


Figure 1 IMS Elements and their interworking interfaces

In a 3GPP network, the AS only becomes involved in a dialogue when the S-CSCF inserts it. Furthermore, an AS does not interact directly with the UE, instead it always interacts directly with the S-CSCF. The interface used for this interaction is the ISC interface.

The 3GPP specifications define the ISC interface as being compliant with IETF SIP (RFC 3261), but with additional support for 3GPP extensions (TS 23.228).

The S-CSCF inserts an AS into a dialogue mainly due to user provisioning data. When the S-CSCF insert the AS, it does so in a manner which indicates to the AS that it should execute either originating or terminating subscriber services, but never both simultaneously. This AS 3GPP requirement is referred to as “running in a half call model”.

The AS implications of running in a half call model are:

- only originating (or terminating) services are executed as requested by the S-CSCF
- completion of service execution results in the AS forwarding the dialogue back to the requesting S-CSCF

Subscriber registrations also occur on the AS without direct interaction with the UE. These are known as 3rd party registrations, and they originate from the S-CSCF. In other words, the UE originates registration requests to the S-CSCF and as a result, the S-CSCF originates a separate registration request to the AS on behalf of the UE. Furthermore, the S-CSCF places itself as the UE’s contact address in this separate request.

The S-CSCF also takes over the responsibility of performing subscriber authorizations. Therefore, the AS does not need to (and it must not) perform this task.

In a 3GPP network, the subscriber data is maintained in a single database: the HSS. The AS and the various CSCF nodes make use of this database when they require access to subscriber data. The interface used by the AS to interact with the HSS is the Sh interface.

The 3GPP specifications define the Sh interface as an IETF vendor specific Diameter application (TS 29.239).

For in-depth information about the 3GPP AS, CSCF nodes, and the various IMS interfaces and procedures, please consult TS 23.218, TS 23.228, and TS 24.229

74.3 Feature Description

The purpose of this feature is to modify the release 9.0 MCS Standalone Session Manager network element to function as a 3GPP AS with restrictions/ limitations. The resulting product will be referred to as MCS R6 AS.

The capabilities of the MCS R6 AS will be:

- Support for the Nortel 3GPP PC Client
- Support for the ISC interface to interact with the Nortel 3.0 S-CSCF
  - — Support for P-Charging-Vector ICID parameter
  - — Support for the orig-dialog-id tag in the route header
  - — Support for the nt_info tag in the route header
  - — Support for the P-Called-Party-ID header for call forwarding
  - — Support for the Request-Dispositon no-fork tag
- Support for terminating ½ call model subscriber services
  - — Call Screening and Routing
  - — AdHoc Conference
  - — MeetMe conference
  - — Hold (remote & local)
  - — Direct and Consultative Transfers
  - — Redirects
  - — Calling Line ID (note that only the terminating side of this service is supported)
  - — Instant Messaging
- 3rd Party registrations via the REGISTER method
- Support for a new IPDR record unit to collect the ICID
- Support for acting as a proxy between the S-CSCF and the MAS
- Support for AC PRI GW originations with restrictions
- Support for AC PRI GW terminations with restrictions
- 80K BHCA per node (weighted-use services model)

The restrictions and limitations of the MCS R6 AS are:

- Any subscriber service not explicitly mentioned in the previous list is not supported (ie. Presence is not supported, Callpark is not supported, etc…).
- RFC 2833 is the only supported method for DTMF
- No support for originating ½ call model subscriber services

- No support for originating or terminating full call model services (a non-compliant mode for a 3GPP AS)
- The MCS R6 AS will not support the Sh interface. Therefore, the AS will not be able to query an HSS for subscriber data.
- The MCS R6 AS will only be supported in the same hardware configuration as the 9.0 Standalone MCS.
- The MCS R6 AS will continue to use the same OAM system as the Release 9.0 Standalone MCS.
- The MCS R6 AS will need to be deployed in the same MCS network element topology as the 9.0 Standalone MCS, with the exception that Media Portal, IPCM and Gatekeeper are not supported (see the 9.0 MCS OAM System Architecture Document).
- Voicemail service is not supported on this release due to a sequential routing restriction existing on the S-CSCF.
- Sequential and Simultaneous routing is not supported on this release due to a sequential routing restriction existing on the S-CSCF.
- If multiple registrations exist for a user, only the most recent registration will be “rung” when such a user is on the receiving end of a call.
- The MCS R6 AS will only interface with the MAS (using RFC 3261) and the S-CSCF (using 3GPP ISC). Interacting with any other node is not supported. In other words: CS1K, CS2K, WCM, MediaPortal, IPCM, H.323 gatekeeper, etc… are not supported in this release.
- PSTN originations (through the AC PRI GW) are supported with the following restrictions (note: the following restrictions apply solely to PSTN originations, unless otherwise noted!!):
  - — R6 AS to accept calls coming from AC PRI GW, in the same way the Standalone MCS SessionMgr does today.
  - — If orig and term subscribers received in INVITE from GW match MCS subscribers, both orig and term services will run before the S-CSCF is involved in the call
  - — R6 AS services will execute twice per call: the first time will be when the AS receives the call from the GW, and the second time when the S-CSCF inserts the AS into the call.
  - — To the R6 AS, the call from the GW is one call, and the call from the S-CSCF is a separate and different call.
  - — R6 AS to add a route header (with orig parm) to INVITE it sends to S-CSCF. The information in that route header will be the information which was received (during registration of the final destination subscriber) in the contact header of the REGISTER message.

- R6 AS to add P-Charging-Vector to INVITE it sends to S-CSCF. The header will contain a newly generated ICID, and a R6 AS wide value in the IOI parameter.
- If no contact info is available for final destination subscriber, the behaviour will be identical to that of the standalone MCS ApplicationServer.
- No UPDATE message support due to the lack of support for this message in the AudioCodes PRI GW.
- User's who re-route calls (through CPL) to specific routes with IP Addresses will cause the R6 AS to contact those routes without involving the S-CSCF.
- Calls forwarded back to a PSTN number will route back to the PSTN without ever involving the S-CSCF
- Privacy on PSTN originations will be honored at the AS. The R6 AS considers the S-CSCF as a "privacy trusted" node, therefore the AS will not anonymize headers. However, the S-CSCF does not support any privacy setting other than "privacy: none", therefore the network cannot claim to support privacy.
- R6 AS can only route calls to registered MCS subscribers. If the subscriber is not an MCS subscriber, the call will be rejected with a 404 response. If the terminating subscriber is not registered, the call will be rejected with a 480 response. However, if an MCS subscriber is not registered, but has forwarded all calls to a routable destination, the call will complete to the new destination.
- If subscriber receiving call is forwarded to another subscriber (and so on), all involved subscriber's services will execute before S-CSCF is involved in the call.
- If subscriber is not forwarded and is registered, the INVITE will go to the registered contact address. Since in this network, the S-CSCF performs 3rdParty registrations, this registered contact address for all subscribers is expected to be the address of a S-CSCF. However, if for some reason, the registered contact address is not the address of a S-CSCF, the AS will still route the call to such addresses.

- PSTN terminations (through the AC PRI GW) are supported with the following restrictions (note: the following restrictions apply solely to PSTN terminations, unless otherwise noted!!):
  - R6 AS will route calls to a AC PRI GW as long as destination does not match a subscriber nor a MAS pooled resource alias, but it does match a telephony translation entry which contains a GW route.
  - When running subscriber term services and if the subscriber is requesting to be forwarded to the PSTN, the AS will route the call back to the S-CSCF with the forwarded to PSTN number as the destination.

It will be up to the S-CSCF at this point to find an AS which can route to that PSTN destination, and to send an INVITE to that AS with the proper nt_info parm.

— AS will use sip extension header(s) to transport information between appservers, if the S-CSCF happens to be a node in the middle, it shall proxy the headers unmodified. If this condition is not met, calls will most certainly fail.

— AS to filter 3GPP headers from GW if necessary.

— AS to filter route header from GW if necessary.

— On 200 OK sent towards the S-CSCF, the AS will insert (on behalf of the GW) an R6 AS wide value in the term IOI parameter of the p-charging-vector.

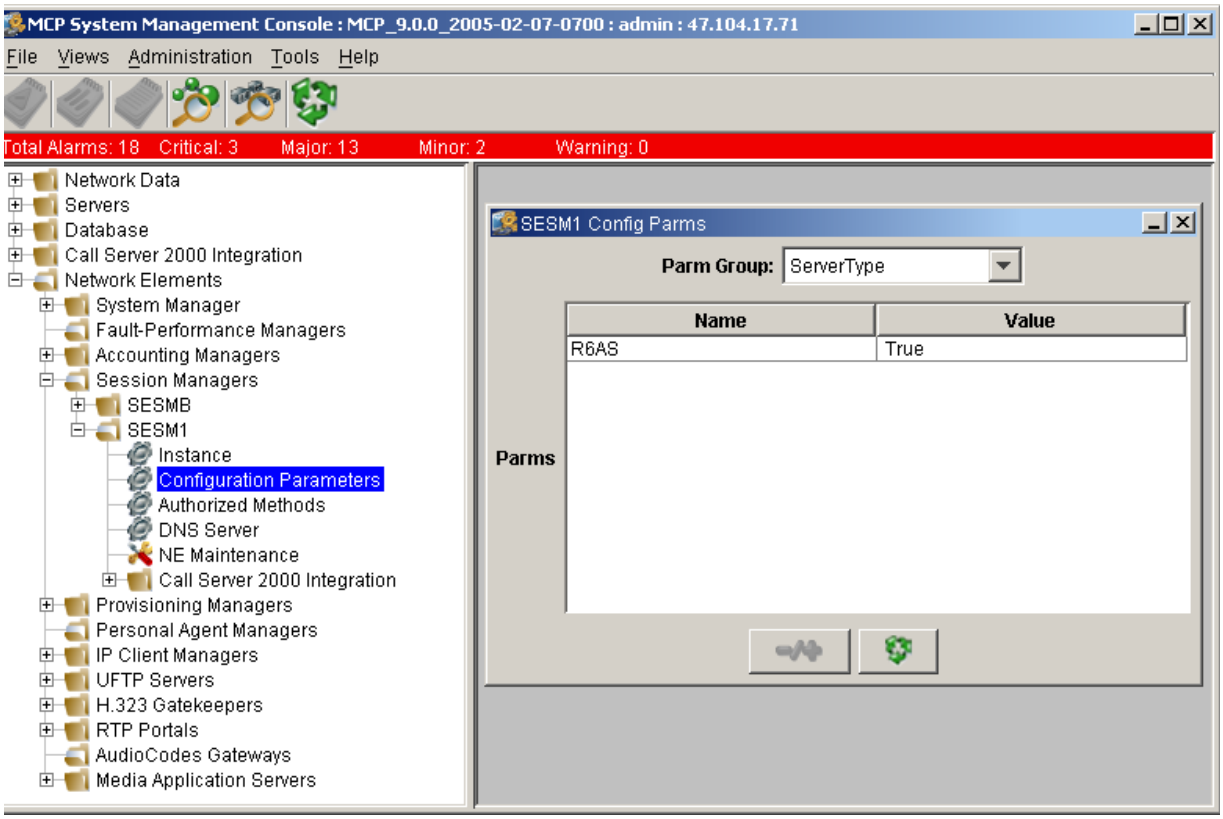
Additionally, there are a large number of client based services and AS services which are not affected by any software changes incurred by this feature. However, these services will not be tested, and are therefore not officially supported. Nevertheless, these services are expected to still function properly.

- Presence
- Automatic Software Update
- Codec selection
- Profile manager
- Quality of Service (QoS)
- Mute
- Decline
- Call subjects
- Do not disturb
- Ignore
- Outlook integration
- Call logs
- Directory (global address book),
- Import Outlook* contacts
- Personal Directory
- Clipboard
- File exchange
- Shared Whiteboard

- Sharing
- Call Waiting
- IM Broadcast
- Web push (Client)
- Whiteboard
- Decline

74.4 Proposal for R6 AS Provisioning

A new SessionManager configuration item will be added in the System Manager to configure a SessionManager as a R6 AS or standalone Session Manager.



A change to the setting of this parameter will require a restart, otherwise the AS will not see the change. If the change occurs while the AS is in service, an alarm (family: R6AS) will be generated. This alarm will not be clearable: it will only go away when the AS is restarted.

74.5 AS Orig/Term Call Half Determination

In order to meet the ½ call model 3gpp requirement, the AS is introducing a new, proprietary parameter into the route header, as follows:

An MCS R6 AS shall require that INVITES it receives from CSCFs contain, in the route header, the parameter nt_info, with its value set to one of: orig or term (e.g. "Route:<sip:appserver,lr,nt_info=orig").

An AS receiving the nt_info parm with a value of “orig” (e.g. "Route:<sip:appserver,lr,nt_info=orig"), will only execute services for the originating user specified in the "From" header of the INVITE. This is not supported in this release. If this shall occur, the AS will reject the request.

An AS receiving the nt_info parm with a value of “term” (e.g. "Route:<sip:appserver,lr,nt_info=term"), will only execute services for the terminating user specified in the Request URI.

If the AS receives the nt_info parameter set to any other value other than those discussed here, the AS shall reject the request.

If the MCS R6 AS receives a request without a route header or with a header, but without an nt_info parameter, the AS shall execute services in a full call model. In other words, the R6 AS will behave as a standalone MCS AS. This is not supported in this release. The behaviour of the AS in this situation is undefined.

Furthermore, in the case where nt_info=term (or nt_info=orig when it is supported in a future release) is present in the Route header, the R6 AppServer shall, upon completing the execution of the terminating (or originating) subscriber services, send an INVITE when applicable, with the destination in the request URI, to the node listed in the route header received in the INVITE.

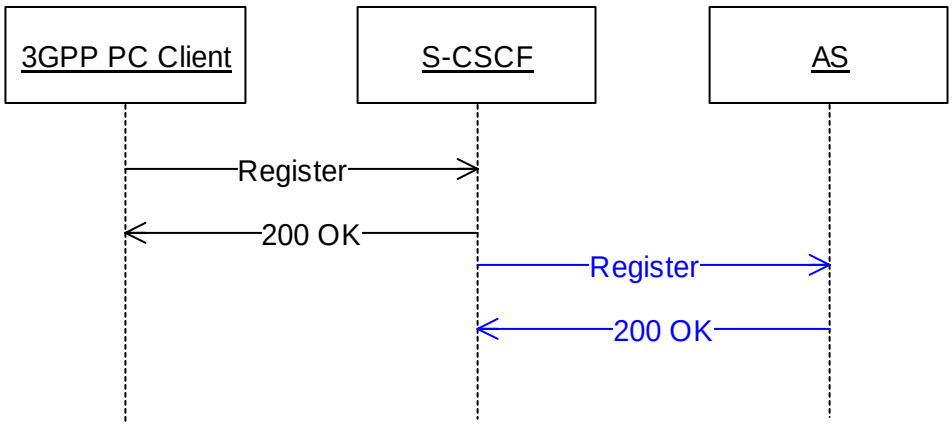
74.6 R6 AS Call Flows

74.6.1 Registration

In a 3GPP network, the 3GPP PC Client performs the registration of it’s public address with the S-CSCF and not with the Application Server. The S-CSCF stores the UE registration information in the HSS. Furthermore, all elements requiring access to UE registration information obtain it from the HSS, and a fully 3GPP compliant AS is no exception. A 3GPP AS uses its Sh interface to communicate with the HSS and obtain UE registration information.

However, in this release, the MCS R6 AS does not support the Sh interface and therefore it cannot use the HSS to retrieve registration information. Therefore, UE registration information must also be stored in the MCS R6 AS database. This is achieved by configuring the S-CSCF to perform 3rd Party Registrations (registrations on behalf of the UE) with the MCS R6 AS.

A 3rd Party Registrations message flow is depicted in the message diagram below.



Note: The message sequence that occurs between the client and the CSCF elements other than the S-CSCF have not been included in this flow. Only the message sequence between the S-CSCF and the MCS Application server has been detailed accurately. For the message sequences between the other 3GPP network entities please refer to the S-CSCF ISC document.

In 3rd Party registrations it is important to recognize the following:

- From the UE's perspective, its registration procedures have culminated once the S-CSCF sends the UE a 200 OK response to the REGISTER message.
- The S-CSCF sends the UE a 200 OK response for the REGISTER message before the S-CSCF has commenced any 3rd party registration attempt with the AS.
- A successful/failed 3rd Party Registration procedure between the S-CSCF and AS has no impact on the **outcome of the registration procedure** between the UE and the S-CSCF.

The S-CSCF shall include the following key items in its 3rd Party Registrations REGISTER message:

- The To header shall contain the public identity of the user on whose behalf the registration is being performed.
- The From header shall contain the contact address of a trusted S-CSCF node
- The Contact header shall contain the contact address of the S-CSCF serving the UE. The AS has no way of verifying the validity of this address, therefore, if the wrong S-CSCF is specified here, calls will not terminate to the UE.

- The Expires header shall contain an expiration timer value equal to the value it sent to the UE in the 200 OK response. The MCS R6 AS will permit for this value to be outside of its provisioned min/max range.

Note that the expiry timer min/max are no longer enforced at the AS, this is expected to be performed now at the S-CSCF/HSS. Also, the 3rd Party Registration does not get challenged by the MCS R6 AS due to the trusted relationship between it and the S-CSCF performing the registration.

Multiple registrations will not be blocked at the MCS R6 AS. However, terminating to a client which has multiple registered destinations will result in the AS only contacting the client's most recent registered destination. This behaviour is due to the S-CSCF's lack of support for simultaneous ringing.

In the following sample messages, the S-CSCF is located at 1.2.3.4 and the AS is at: 5.6.7.8

Register message from the S-CSCF to the AS

```
REGISTER sip:ds7sanity1.com;maddr=5.6.7.8 SIP/2.0
to: <sip:u100@ds7sanity1.com>
from: <sip:scscf@1.2.3.4:5070>;tag=244f-6c3c-6c08-ff5df9d3
call-id: 65e1-6c3c-6c08-ff5df9d3@9.8.7.6
cseq: 2 REGISTER
via: SIP/2.0/UDP 1.2.3.4:5070;branch=z9hG4bKfacb43e51d2524bbb4704a8eaaa2ae1d
max-forwards: 18
x-nt-guid: 004639860307a5a04d400b65c04db8d505b14e
x-nt-location: 567
accept-encoding: nt-im-2.0
allow: ACK,MESSAGE,NOTIFY,INVITE,BYE,CANCEL,REFER,OPTIONS,INFO
contact:
  <sip:scscf@1.2.3.4:5070;maddr=1.2.3.4;lr>;expires=86200;description="Login"
expires: 86200
require: path
supported: com.nortelnetworks.firewall
supported: p-3rdpartycontrol
supported: nosec
user-agent:  Nortel 3GPP PCC 3.0.266
p-charging-vector: icid-value=112_111230691041 7@1.2.3.4;orig-ioi=scscf3.com
content-length: 0
```

Response message from the AS to the S-CSCF

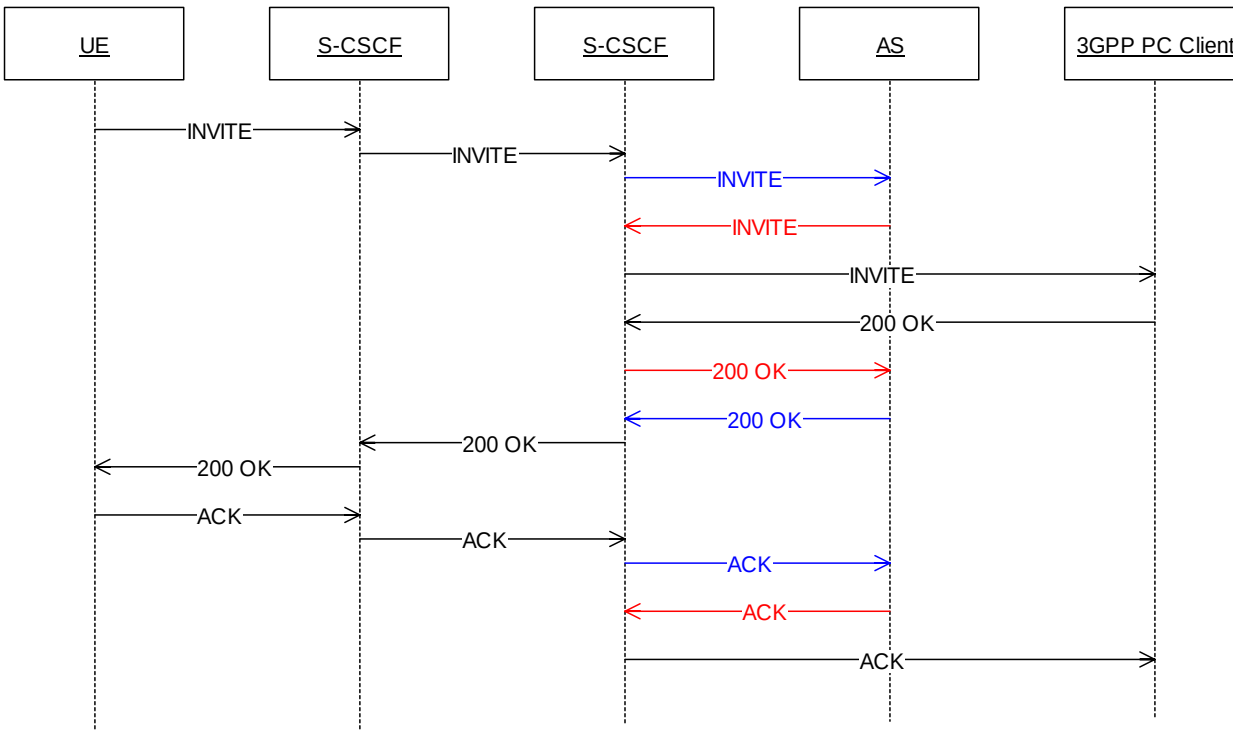
```
SIP/2.0 200 Registration Successful
to: <sip:u100@ds7sanity1.com>;tag=423504219
from: <sip:scscf@1.2.3.4:5070>;tag=244f-6c3c-6c08-ff5df9d3
call-id: 65e1-6c3c-6c08-ff5df9d3@9.8.7.6
cseq: 2 REGISTER
via: SIP/2.0/UDP 1.2.3.4:5070;branch=z9hG4bKfacb43e51d2524bbb4704a8eaaa2ae1d
contact: <sip:scscf@1.2.3.4:5070;lr;maddr=1.2.3.4>;expires=86200
supported: com.nortelnetworks.firewall,p-
  3rdpartycontrol,nosec,com.nortelnetworks.im.encryption
```

```
content-length: 0
```

74.7 Basic call

In a non-R6 Application Server, a call attempt between two clients results in the originating client sending an INVITE directly into the AS. This INVITE is then processed by the AS and, as part of this procedure, the AS runs the subscriber originating and terminating services as necessary. Finally, the AS routes the call directly to the registered contact address of the terminating subscriber.

However, from the point of view of the AS, a call between two clients flows differently in a 3GPP network. In a 3GPP network, the clients do not send their INVITE directly to the AS, the AS receives INVITE requests from a S-CSCF instead. Also, in a 3GPP network, such requests contain an indication of which subscriber services to execute: originating subscriber services or terminating subscriber services, but never both. Finally, once the AS has finished running the requested type of services (orig or term), an R6 AS routes the call back to the S-CSCF which initiated the dialogue, and the reqURI contains the registered contact address of the terminating subscriber.



Call scenario: An IMS subscriber calls an MCS subscriber.

High level breakdown:

1. The first S-CSCF receives the invite from the IMS client and determines (through an HSS) that this subscriber does not have originating services on an AS.
2. The S-CSCF determines (through an HSS) that the term subscriber is currently at another S-CSCF, and sends the INVITE to it.
3. The second S-CSCF receives the INVITE and determines (through an HSS) that the terminating subscriber has services on the AS, and sends an INVITE, with nt_info=term in the route header, to the AS.
4. The AS receives the INVITE and finds the nt_info parm. The value ("term") of the parm causes the AS to not run any services for the originating subscriber. However, the AS does execute the terminating subscriber services.
5. The AS finishes running the term services, and retrieves the contact address of the term party from the registration tables. This is the address of the S-CSCF. The AS places the contact address into the request URI, but sends the INVITE to the S-CSCF from which it originally received the INVITE.
6. The S-CSCF receives the INVITE and routes the call to the client.
7. The client answers the call and the 200 OK propagates through all the nodes until it reaches the originating client, which sends an ACK (again, through all the nodes) back to the terminating client.

AS incoming INVITE:

```
INVITE sip:u103@ds7sanity1.com SIP/2.0
to: <sip:u103@ds7sanity1.com>
call-id: 65e4-6c3c-6c08-ff70bfd8@9.8.7.6from:
  <sip:u100@ds7sanity1.com>;tag=2452-6c3c-6c08-ff70bfd8
cseq: 1 INVITE
via: SIP/2.0/UDP
  1.2.3.4:5070;branch=z9hG4bK198b309500abe31ee709831ae6a1a1f3
via: SIP/2.0/UDP
  1.2.3.4:5063;branch=z9hG4bKa520d7514f58fd9a607cfdb87f3eefe4
via: SIP/2.0/UDP 9.8.7.6:5061;branch=z9hG4bK424dae46-0
max-forwards: 18
x-nt-location: 567
accept: application/sdp
accept-language: en_us
allow: REFER
contact: <sip:u100@9.8.7.6:5061>
expires: 180
record-route: <sip:scscf@1.2.3.4:5070;lr>
```

```
record-route: <sip:1.2.3.4:5063;lr>
route: <sip:5.6.7.8;nt_info=term>
route: <sip:scscf@1.2.3.4:5070;orig;lr>;orig-dialog-id="65e4-
  6c3c-6c08-ff70bfd8@9.8.7.62452-6c3c-6c08-ff70bfd8"
supported: com.nortelnetworks.firewall
supported: p-3rdpartycontrol
supported: nosec
user-agent:  Nortel 3GPP PCC 3.0.266
privacy: none
p-charging-vector: icid-value=131_111230691041 7@1.2.3.4;orig-
  ioi=scscf3.com;term-ioi=scscf3.com
content-length: 491
content-type: application/sdp
d: no-fork

v=0
o=u100 4285579224 4285579224 IN IP4 9.8.7.6
s=nortelnetworks
p=+972 684 1000
c=IN IP4 9.8.7.6
t=0 0
m=audio 50002 RTP/AVP 0 8 18 111
c=IN IP4 9.8.7.6
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
m=video 50004 RTP/AVP 34 96
c=IN IP4 9.8.7.6
a=rtpmap:34 H263/90000
a=fmtp:34 CIF=3 QCIF=3 SQCIF=3 MAXBR=192 D1 D2 E F
a=rtpmap:96 X-NNVC/10
a=fmtp:96 p=152f
a=framerate:10.0
a=recvonly
```

AS outgoing INVITE:

```
INVITE sip:scscf@1.2.3.4:5070;maddr=1.2.3.4;lr SIP/2.0
to: "u103 basic" <sip:u103@ds7sanity1.com>
from: "u100 basic" <sip:u100@ds7sanity1.com>;tag=2452-6c3c-6c08-
  ff70bfd8
call-id: 02ff70c71c19bb44817e5e5562903c8d49de982@5.6.7.8
cseq: 1 INVITE
max-forwards: 17
x-nt-corr-id: 02ff70c52d3ed3f517e5e5708eb75a9084b414@5.6.7.8
x-nt-location: 567
```

```
accept: application/sdp
accept-language: en_us
allow: REFER
contact:
  <sip:u100@5.6.7.8:5060;nt_end_pt=YM0+~Kudj0~T4ta00utd1T0BP~QEq
  61~LXaxTc7devoMa~WbErty5oaGK6CC6So66~LKT_ci1~NrEa4X6QMX-
  6c.8Z2O_SNytG~FUk47rm08v116.QP~Nv2-
  i1~HtPX5mU5ti;nt_server_host=5.6.7.8>
expires: 180
route: <sip:scscf@1.2.3.4:5070;orig;lr>;orig-dialog-id="65e4-
  6c3c-6c08-ff70bfd8@9.8.7.62452-6c3c-6c08-ff70bfd8"
supported: com.nortelnetworks.firewall,p-
  3rdpartycontrol,nosec,com.nortelnetworks.im.encryption
user-agent:  Nortel 3GPP PCC 3.0.266
privacy: none
p-charging-vector: icid-value=131_111230691041 7@1.2.3.4;orig-
  ioi=scscf3.com;term-ioi=scscf3.com
content-length: 491
content-type: application/sdp
d: no-fork

v=0
o=u100 4285579224 4285579224 IN IP4 9.8.7.6
s=nortelnetworks
p=+972 684 1000
c=IN IP4 9.8.7.6
t=0 0
m=audio 50002 RTP/AVP 0 8 18 111
c=IN IP4 9.8.7.6
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
m=video 50004 RTP/AVP 34 96
c=IN IP4 9.8.7.6
a=rtpmap:34 H263/90000
a=fmtp:34 CIF=3 QCIF=3 SQCIF=3 MAXBR=192 D1 D2 E F
a=rtpmap:96 X-NNVC/10
a=fmtp:96 p=152f
a=framerate:10.0
a=recvonly
```

AS incoming 180 Ringing:

```
SIP/2.0 180 Ringing
to: "u103 basic" <sip:u103@ds7sanity1.com>;tag=6249-6cf8-6cd4-
  ff70ca18
```

```
from: "u100 basic" <sip:u100@ds7sanity1.com>;tag=2452-6c3c-6c08-
  ff70bfd8
call-id: 02ff70c71c19bb44817e5e5562903c8d49de982@5.6.7.8
cseq: 1 INVITE
via: SIP/2.0/UDP 5.6.7.8:5060;branch=z9hG4bK-11f58ab-62725e66-
  1cee1079
allow: REFER
record-route: <sip:1.2.3.4:5066;lr>
record-route: <sip:scscf@1.2.3.4:5070;lr>
user-agent:  Nortel 3GPP PCC 3.0.266
privacy: none
content-length: 0
```

AS outgoing 180 Ringing:

```
SIP/2.0 180 Ringing
to: <sip:u103@ds7sanity1.com>;tag=6249-6cf8-6cd4-ff70ca18
from: <sip:u100@ds7sanity1.com>;tag=2452-6c3c-6c08-ff70bfd8
call-id: 65e4-6c3c-6c08-ff70bfd8@9.8.7.6
cseq: 1 INVITE
via: SIP/2.0/UDP
  1.2.3.4:5070;branch=z9hG4bK198b309500abe31ee709831ae6a1a1f3
via: SIP/2.0/UDP
  1.2.3.4:5063;branch=z9hG4bKa520d7514f58fd9a607cfdb87f3eefe4
via: SIP/2.0/UDP 9.8.7.6:5061;branch=z9hG4bK424dae46-0
x-nt-party-id: u103/
allow: REFER
call-info: <http://zpves19n.us.nortel.com:80/pa/direct/
  pictureServlet?user=u103@ds7sanity1.com>;Purpose=icon
contact: <sip:u103@ds7sanity1.com:5060;maddr=5.6.7.8>
record-route: <sip:1.2.3.4:5066;lr>
record-route: <sip:scscf@1.2.3.4:5070;lr>
user-agent:  Nortel 3GPP PCC 3.0.266
privacy: none
content-length: 0
```

AS incoming 200 OK:

```
SIP/2.0 200 OK
to: "u103 basic" <sip:u103@ds7sanity1.com>;tag=6249-6cf8-6cd4-
  ff70ca18
from: "u100 basic" <sip:u100@ds7sanity1.com>;tag=2452-6c3c-6c08-
  ff70bfd8
call-id: 02ff70c71c19bb44817e5e5562903c8d49de982@5.6.7.8
cseq: 1 INVITE
```

```
via: SIP/2.0/UDP 5.6.7.8:5060;branch=z9hG4bK-11f58ab-62725e66-
 1cee1079
allow: REFER
contact: <sip:u103@9.8.7.6:5062>
record-route: <sip:1.2.3.4:5066;lr>
record-route: <sip:scscf@1.2.3.4:5070;lr>
user-agent:  Nortel 3GPP PCC 3.0.266
content-length: 349
content-type: application/sdp

v=0
o=u103 4285579224 4285579224 IN IP4 9.8.7.6
s=nortelnetworks
p=+972 684 1000
c=IN IP4 9.8.7.6
t=0 0
m=audio 50002 RTP/AVP 0 111
c=IN IP4 9.8.7.6
a=rtpmap:0 PCMU/8000
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
m=video 0 RTP/AVP 34
c=IN IP4 9.8.7.6
a=rtpmap:34 H263/90000
a=fmtp:34 CIF=3 MAXBR=192 D1 D2 E F
```

AS outgoing 200 OK:

```
SIP/2.0 200 OK
to: <sip:u103@ds7sanity1.com>;tag=6249-6cf8-6cd4-ff70ca18
from: <sip:u100@ds7sanity1.com>;tag=2452-6c3c-6c08-ff70bfd8
call-id: 65e4-6c3c-6c08-ff70bfd8@9.8.7.6
cseq: 1 INVITE
via: SIP/2.0/UDP
 1.2.3.4:5070;branch=z9hG4bK198b309500abe31ee709831ae6a1a1f3
via: SIP/2.0/UDP
 1.2.3.4:5063;branch=z9hG4bKa520d7514f58fd9a607cfdb87f3eefe4
via: SIP/2.0/UDP 9.8.7.6:5061;branch=z9hG4bK424dae46-0
x-nt-party-id: u103/
allow: REFER
contact:
 <sip:u103@5.6.7.8:5060;nt_end_pt=YM0+~KudjJ~T4ta00utd1T0BP~QEq
 6o~LXt~K!iW~P2U2O_S8T1mOfbbT-
 C1.aiQQ5QQfkmc8o!9fQf.9~DWi7l0dj!7zta04G~P68fiJ~NPnb5m-
 1CA;nt_server_host=5.6.7.8>
record-route: <sip:scscf@1.2.3.4:5070;lr>
record-route: <sip:1.2.3.4:5063;lr>
user-agent:  Nortel 3GPP PCC 3.0.266
```

```
content-length: 349
content-type: application/sdp

v=0
o=u103 4285579224 4285579224 IN IP4 9.8.7.6
s=nortelnetworks
p=+972 684 1000
c=IN IP4 9.8.7.6
t=0 0
m=audio 50002 RTP/AVP 0 111
c=IN IP4 9.8.7.6
a=rtpmap:0 PCMU/8000
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
m=video 0 RTP/AVP 34
c=IN IP4 9.8.7.6
a=rtpmap:34 H263/90000
a=fmtp:34 CIF=3 MAXBR=192 D1 D2 E F
```

AS incoming ACK:

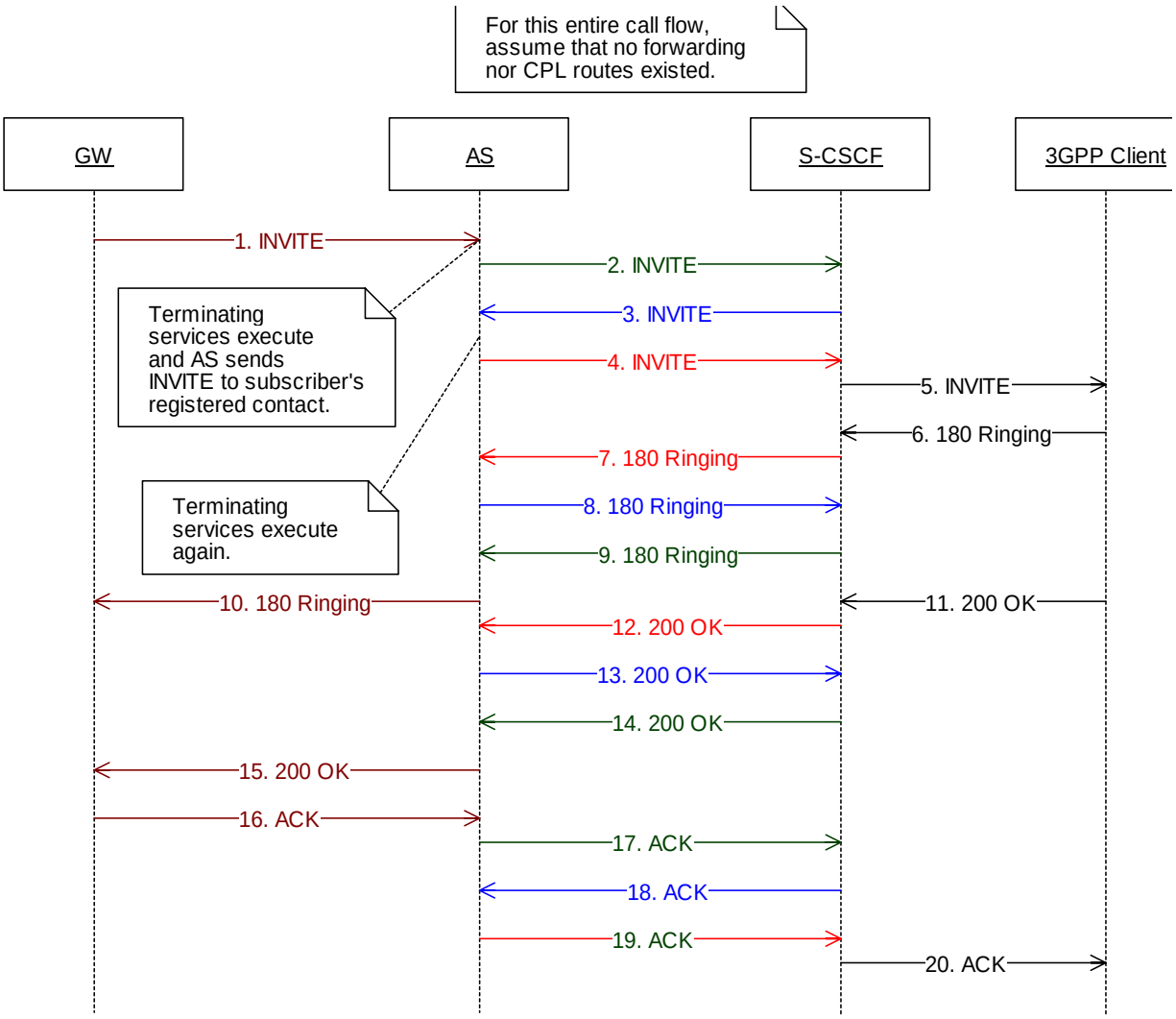
```
ACK sip:u103@5.6.7.8:5060 SIP/2.0
to: <sip:u103@ds7sanity1.com>;tag=6249-6cf8-6cd4-ff70ca18
from: <sip:u100@ds7sanity1.com>;tag=2452-6c3c-6c08-ff70bfd8
call-id: 65e4-6c3c-6c08-ff70bfd8@9.8.7.6
cseq: 1 ACK
via: SIP/2.0/UDP
  1.2.3.4:5070;branch=z9hG4bK198b309500abe31ee709831ae6a1a1f3
via: SIP/2.0/UDP
  1.2.3.4:5063;branch=z9hG4bK4dde191345250c57f3085bc197b869b3
via: SIP/2.0/UDP 9.8.7.6:5061;branch=z9hG4bK424dae46-0
via: SIP/2.0/UDP 9.8.7.6:5061;branch=z9hG4bK424dae46-0
max-forwards: 18
contact:
  <sip:u100@9.8.7.6:5061;nt_end_pt=YM0+~Kudj0~T4ta00utd1T0BP~QEq
  61~LXaxTc7devoMa~WbErty5oaGK6CC6So66~LKT_ci1~NrEa4X6QMX-
  6c.8Z2O_SNytG~FUk47rm08v116.QP~Nv2-
  i1~HtPX5mU5ti;nt_server_host=9.8.7.6:5061>
user-agent:  Nortel 3GPP PCC 3.0.266
content-length: 0
```

AS outgoing ACK:

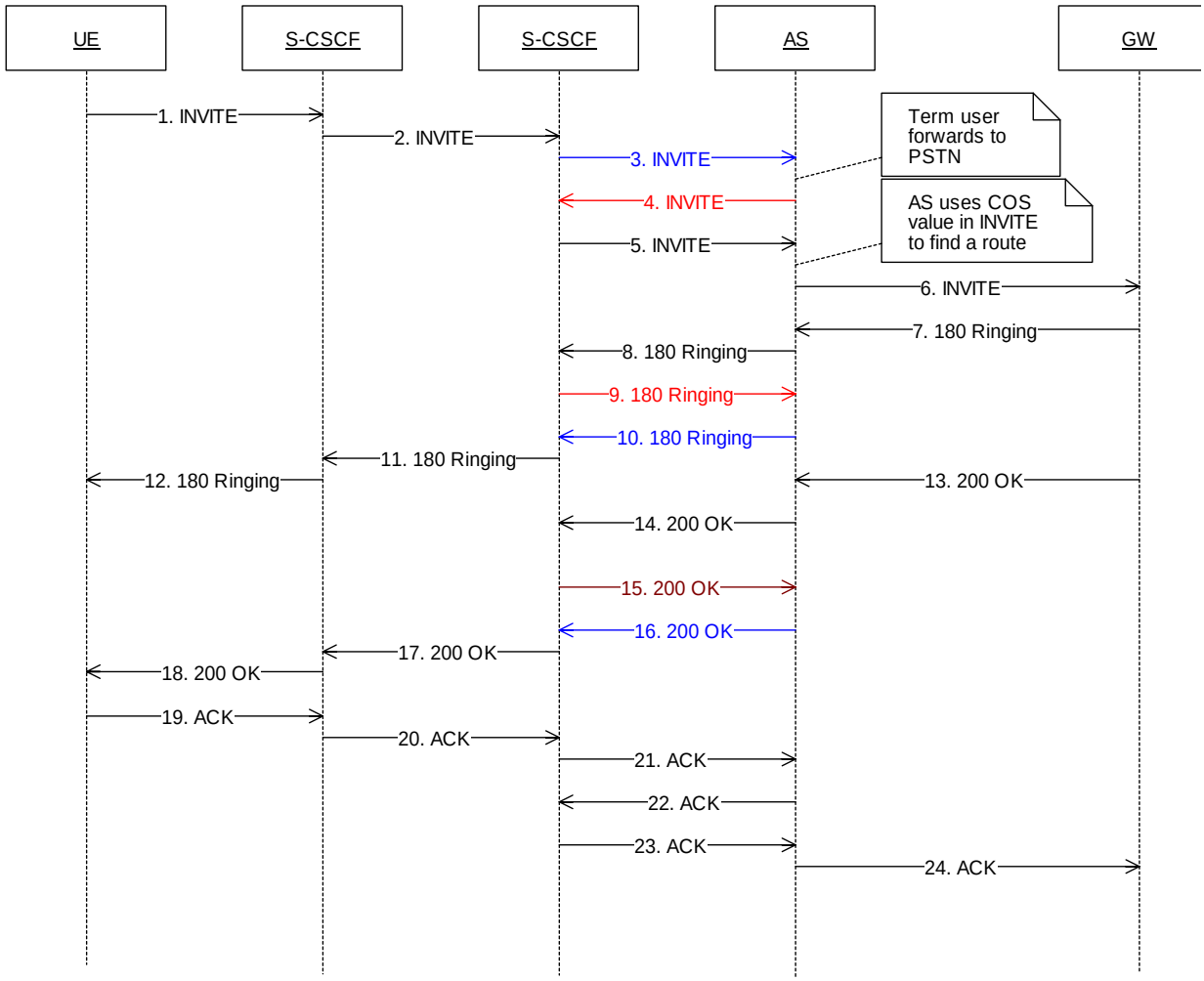
```
ACK sip:u103@9.8.7.6:5062 SIP/2.0
to: "u103 basic" <sip:u103@ds7sanity1.com>;tag=6249-6cf8-6cd4-
  ff70ca18
from: "u100 basic" <sip:u100@ds7sanity1.com>;tag=2452-6c3c-6c08-
  ff70bfd8
call-id: 02ff70c71c19bb44817e5e5562903c8d49de982@5.6.7.8
```

```
cseq: 1 ACK
max-forwards: 17
route: <sip:scscf@1.2.3.4:5070;lr>,<sip:1.2.3.4:5066;lr>
user-agent:  Nortel 3GPP PCC 3.0.266
content-length: 0
```

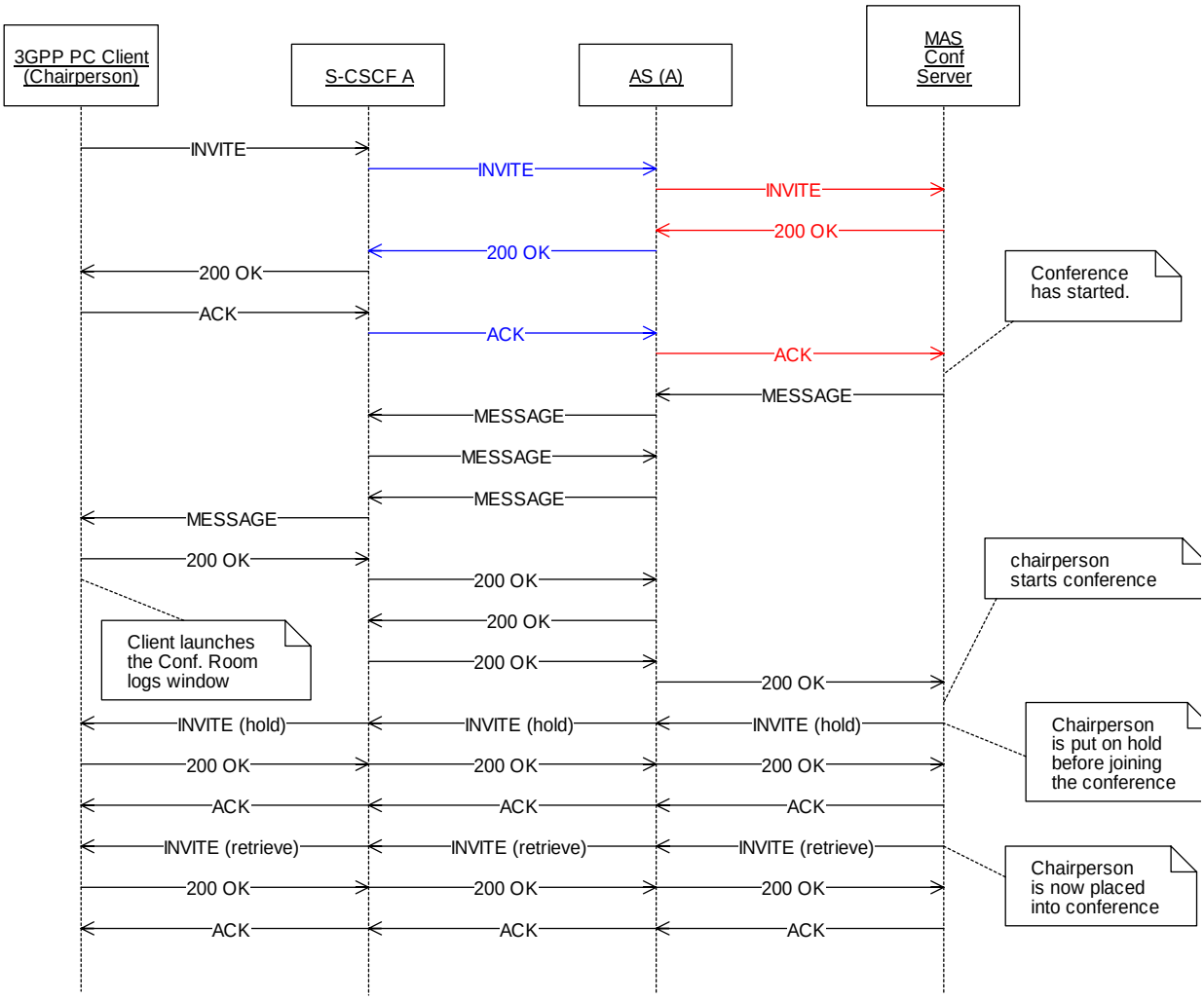
74.8 PSTN Originations

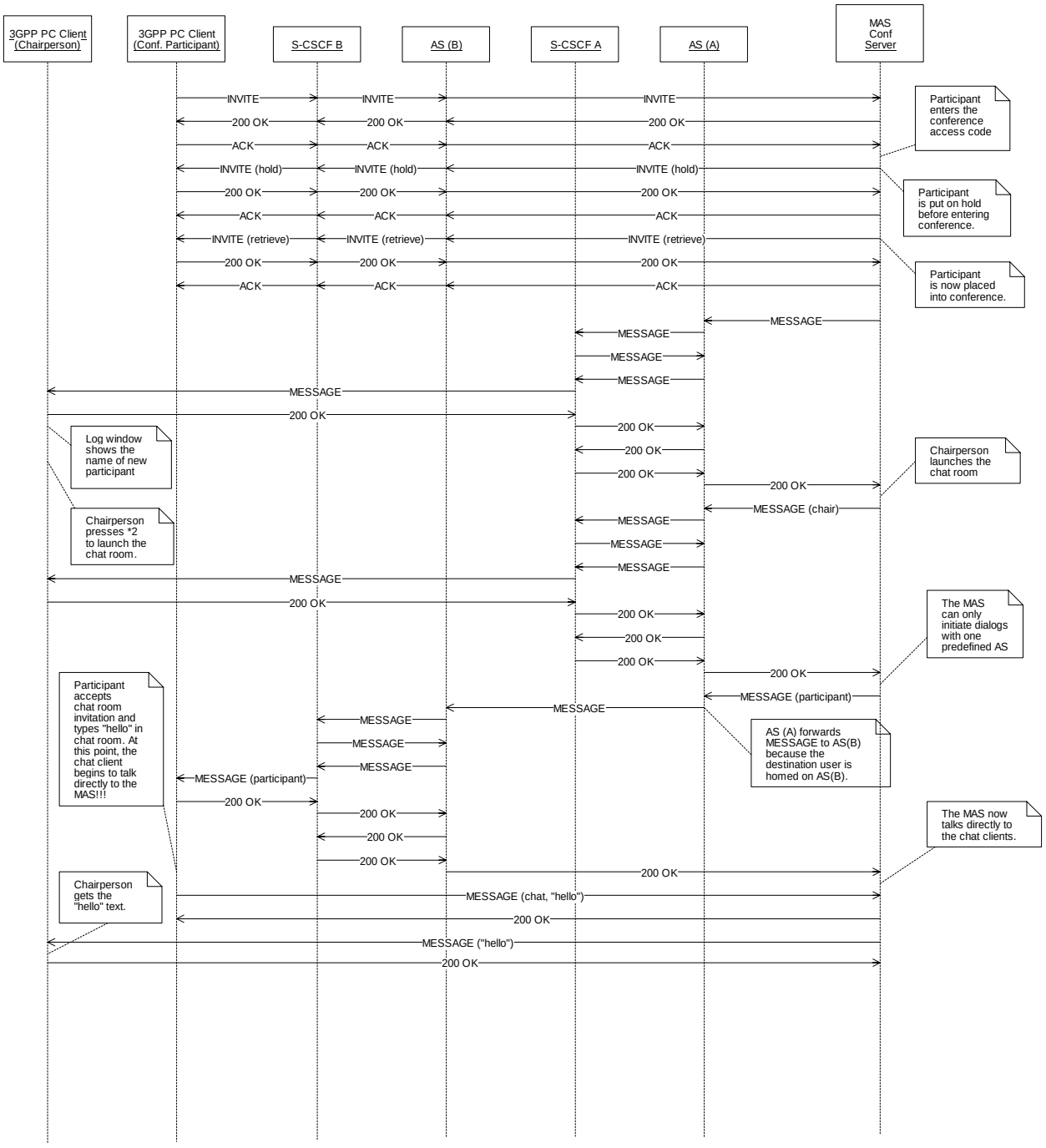


74.9 PSTN Terminations



74.10 MeetMe Conference



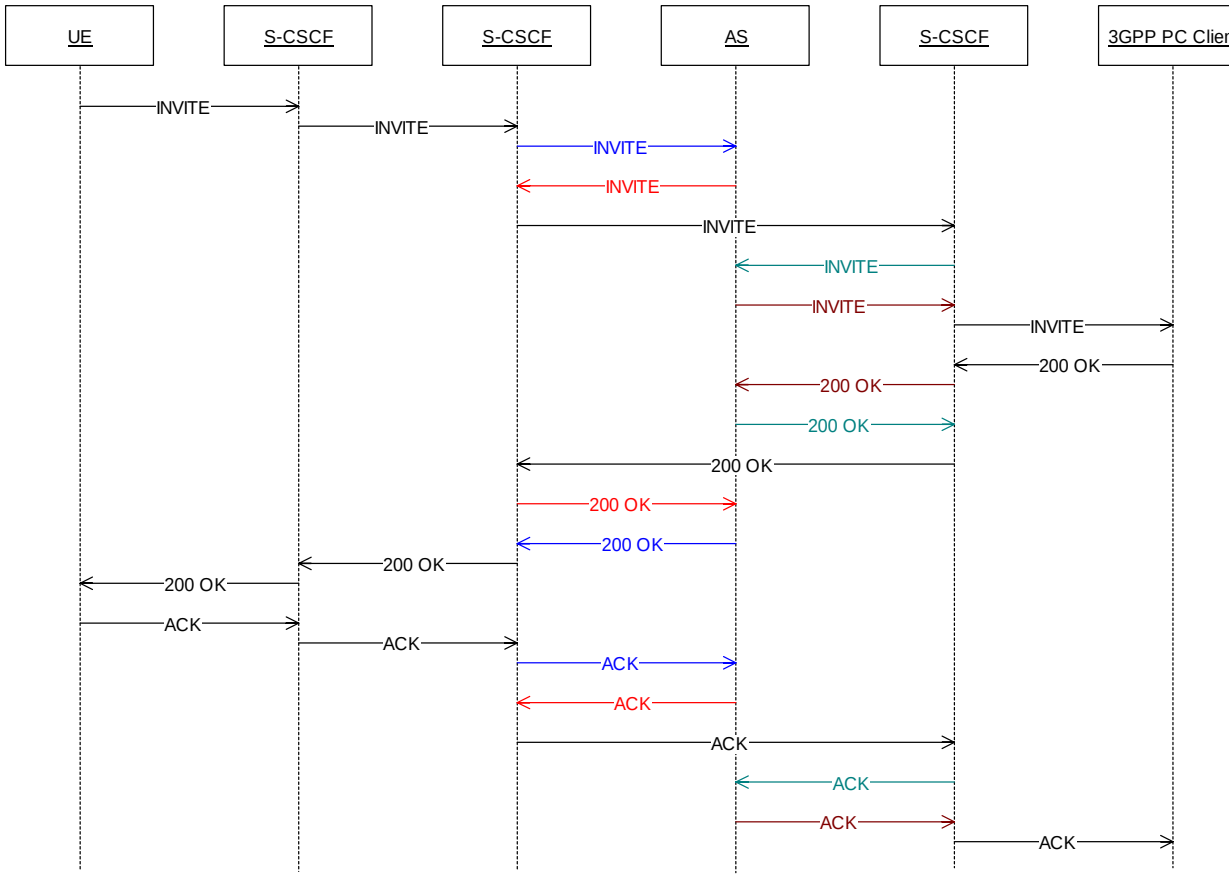


Call Scenario: An MCS subscriber calls the alias associated with the MeetMe service (eg. the user dials 4456200).

High level breakdown:

1. The S-CSCF receives the INVITE from the client and the S-CSCF has translations in place to realize that this is a call that needs to go to the MAS Conference Server.
2. The S-CSCF is not able to interact directly with the MAS (see S-CSCF documentation on the reasons why…), therefore it routes the call to the AS, and sends nt_info=term in the route header.
3. The “term” value in the nt_info route header parm causes the AS to skip originating subscriber based services. A lookup is attempted on the destination and a match is found in the pooled resource translations. Note: if a match is not found the AS will advance into telephony translations.
4. The AS sends an INVITE to the MAS Conference Server retrieved from pooled entity translations.
5. The MAS Conference server receives the INVITE, and it determines that the codecs in the SDP are supported and responds with a 200 OK. Note: will the MAS ignore the 3GPP headers?
6. The AS places the required 3GPP headers into the 200 OK and sends it to the S-CSCF, and the 200 OK propagates back to the originator.
7. The originator ACKS the 200 OK.

74.11 Call Forwarding



Call scenario: An IMS subscriber makes a call to an MCS subscriver (assume the IMS subscriber supports G.711 or G.729).

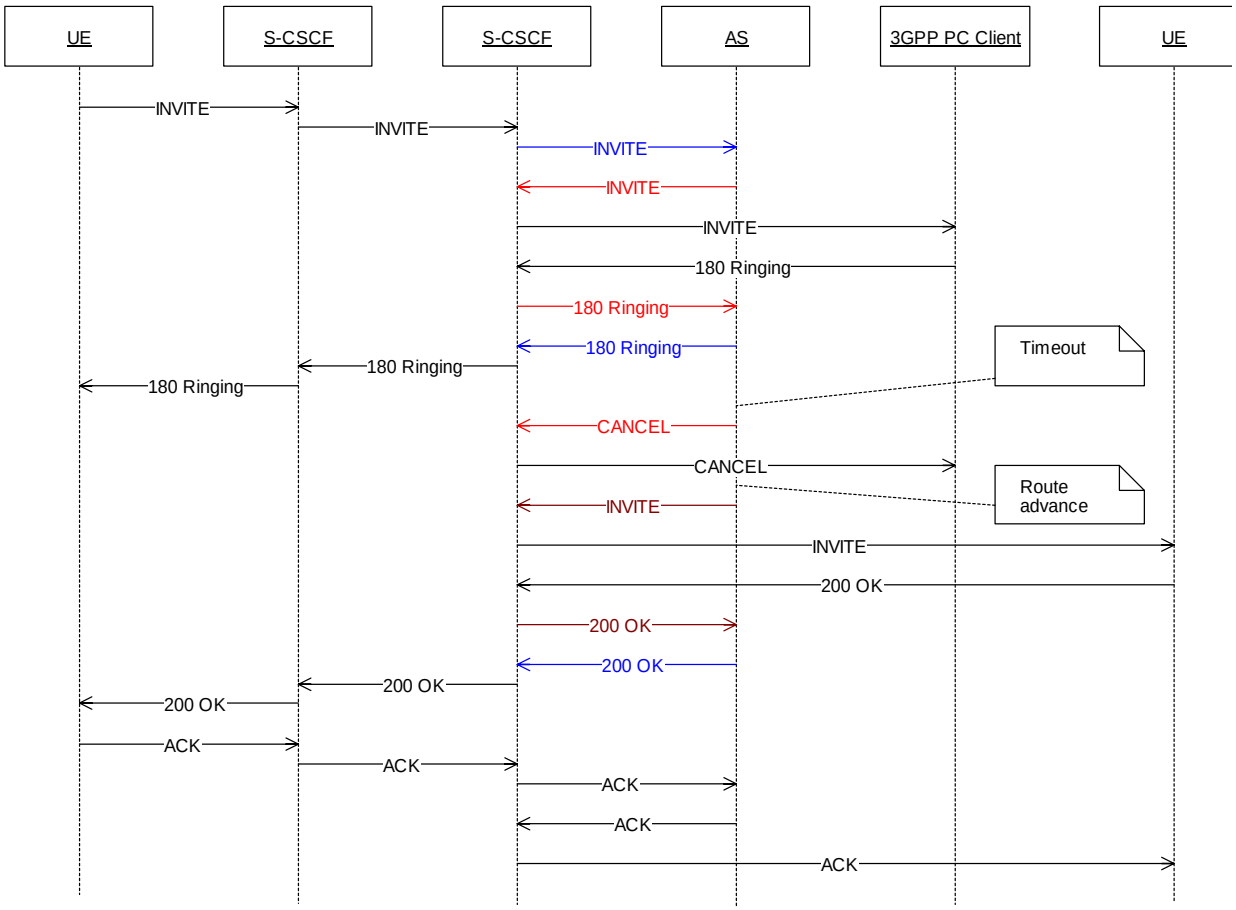
High level bereakdown:

1. The first S-CSCF receives the invite from the IMS client and determines (through an HSS) that this subscriber does not have originating services on an AS.
2. The S-CSCF determines (through an HSS) that the term subscriber is currently at another S-CSCF, and sends the INVITE to it.
3. The second S-CSCF receives the INVITE and determines (through an HSS) that the terminating subscriber has services on the AS, and sends an INVITE, with nt_info=term in the route header, to the AS.

4. The AS receives the INVITE and finds the nt_info parm. The value (“term”) of the parm causes the AS to not run any services for the originating subscriber. However, the AS does execute the terminating subscriber services.
5. While running through the term subscriber services, it determines that the subscriber has call forwarded his calls to another MCS subscriber (party C). The AS then sends an INVITE, with party C in the “to” header, to the S-CSCF which originally sent the INVITE being processed (the second S-CSCF). The Request URI is set to C’s contact address from registration. The P-Called-Party-Id header will contain the contents of the “to” header in the original INVITE (party B).
6. The S-CSCF receives the INVITE, queries the HSS and finds party C’s S-CSCF.
7. An INVITE is then sent from party B’s S-CSCF to party C’s S-CSCF.
8. Party C’s S-CSCF receives the INVITE and determines (through the HSS) that the AS should provide services for party C.
9. An INVITE is sent to the AS, and the call continues the same way it does in a basic call (see section 2.3.3.2).

74.12 Sequential Ringing

This is no longer supported due to the forking limitation found on the s-cscf. This content is left here for documentation purposes.



Call scenario: An IMS user calls an MCS subscriber who has the following rule in his personal agent CPL: ring self for 3 rings and, if no answer, route advance to ring UE3 for 3 rings.

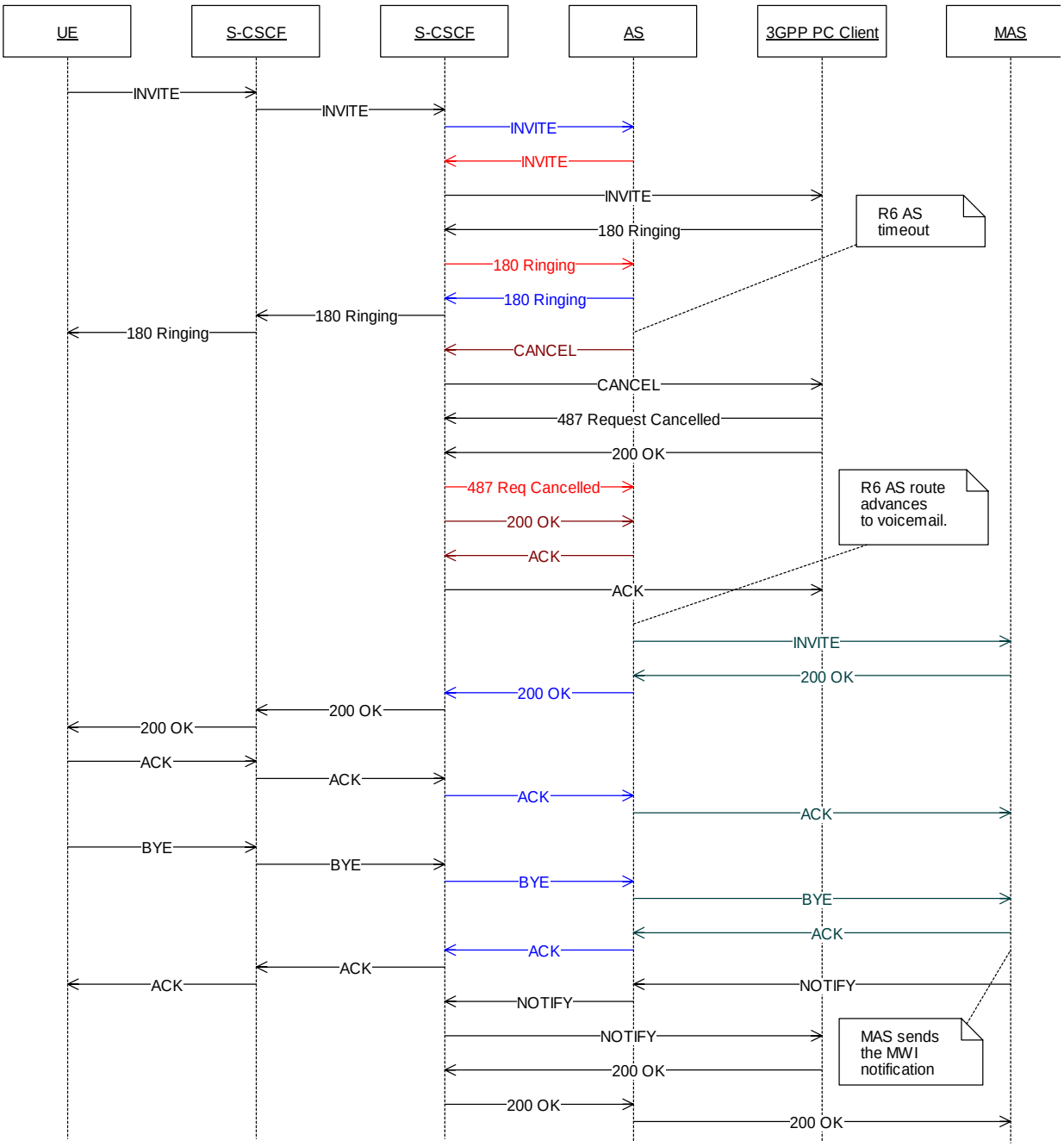
High level breakdown:

1. The first S-CSCF receives the invite from the IMS client and determines (through an HSS) that this subscriber does not have originating services on an AS.
2. The S-CSCF determines (through an HSS) that the term subscriber is currently at another S-CSCF, and sends the INVITE to it.
3. The second S-CSCF receives the INVITE and determines (through an HSS) that the terminating subscriber has services on the AS, and sends an INVITE, with nt_info=term in the route header, to the AS.

4. The AS receives the INVITE and finds the nt_info parm. The value (“term”) of the parm causes the AS to not run any services for the originating subscriber. However, the AS does execute the terminating subscriber services.
5. Upon executing the term subscriber services, the AS determines that the subscriber has sequential routes provisioned.
6. The AS sends an INVITE back to the S-CSCF which sent it the INVITE, but the INVITE has its request URI set to the contact address of the term subscriber.
7. Once the number of rings for the first route expire, the AS sends a CANCEL to the S-CSCF and route advances the same way it does in the Release 9.0 AS. The only noticeable difference is that the INVITE for the second termination is sent to the S-CSCF (the one who sent the INVITE to the AS), instead of directly to the client.

74.13 Unified Communications (Voicemail deposit)

This is no longer supported due to the forking limitation found on the s-cscf. This content is left here for documentation purposes.



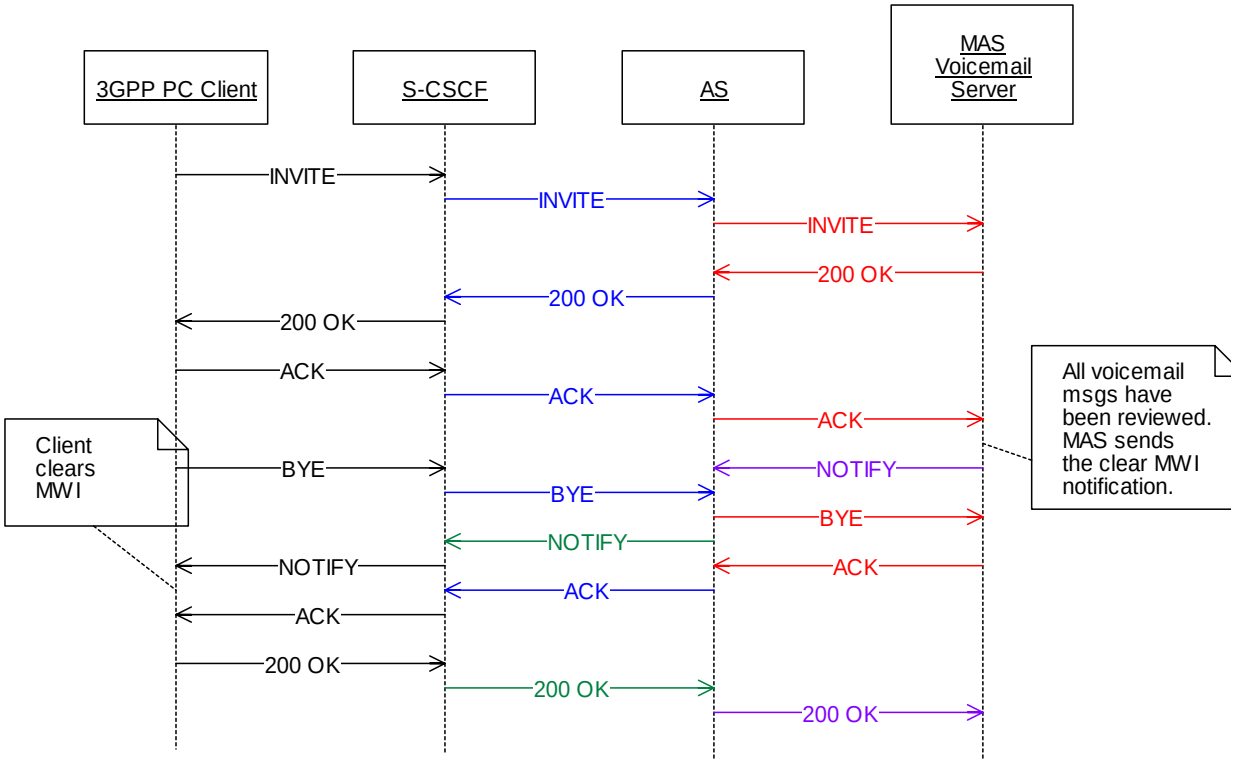
Call scenario: An IMS user calls an MCS subscriber who has the voicemail service and who does not answer the phone.

High level breakdown:

1. The first S-CSCF receives the invite from the IMS client and determines (through an HSS) that this subscriber does not have originating services on an AS.
2. The S-CSCF determines (through an HSS) that the term subscriber is currently at another S-CSCF, and sends the INVITE to it.
3. The second S-CSCF receives the INVITE and determines (through an HSS) that the terminating subscriber has services on the AS, and sends an INVITE, with nt_info=term in the route header, to the AS.
4. The AS receives the INVITE and finds the nt_info parm. The value ("term") of the parm causes the AS to not run any services for the originating subscriber. However, the AS does execute the terminating subscriber services.
5. An INVITE is sent to the S-CSCF with the client's contact address in the request URI.
6. The client fails to answer, and the AS sends a CANCEL.
7. The AS "route advances" to the MAS voicemail Server, and sends an INVITE to it.
8. The MAS Voicemail Server receives the INVITE and determines that the codecs in the SDP are supported, and replies with a 200 OK. From this point onward, the behaviour is the same as the one described (once the call is answerd) in section 2.3.3.2.
9. Once a new message is deposited into the subscriber's mailbox, the MAS will send a MWI NOTIFY message towards the subscriber. This will activate the MWI feature on the client.

74.14 Unified Communications (Voicemail retrieval)

Since VM deposit is not supported (see previous section), this is also not supported (there will never be any VM to retrieve!) This content is left here for documentation purposes.



Call scenario: An MCS subscriber calls his voicemail (eg. the user dials 445-6100) to listen to his messages.

High level breakdown: The call is identical to the call flow described for meetme conference in section 2.3.3.3. The only difference is in the NOTIFY message, sent by the MAS towards the client. This NOTIFY turns off the MWI on the client, and is only sent when all new voicemail messages have been reviewed.

Note: Add the incoming NOTIFY msg and the outgoing 200 OK (from AS point of view). Also, verify the contents of the messages already below.

AS outgoing NOTIFY:

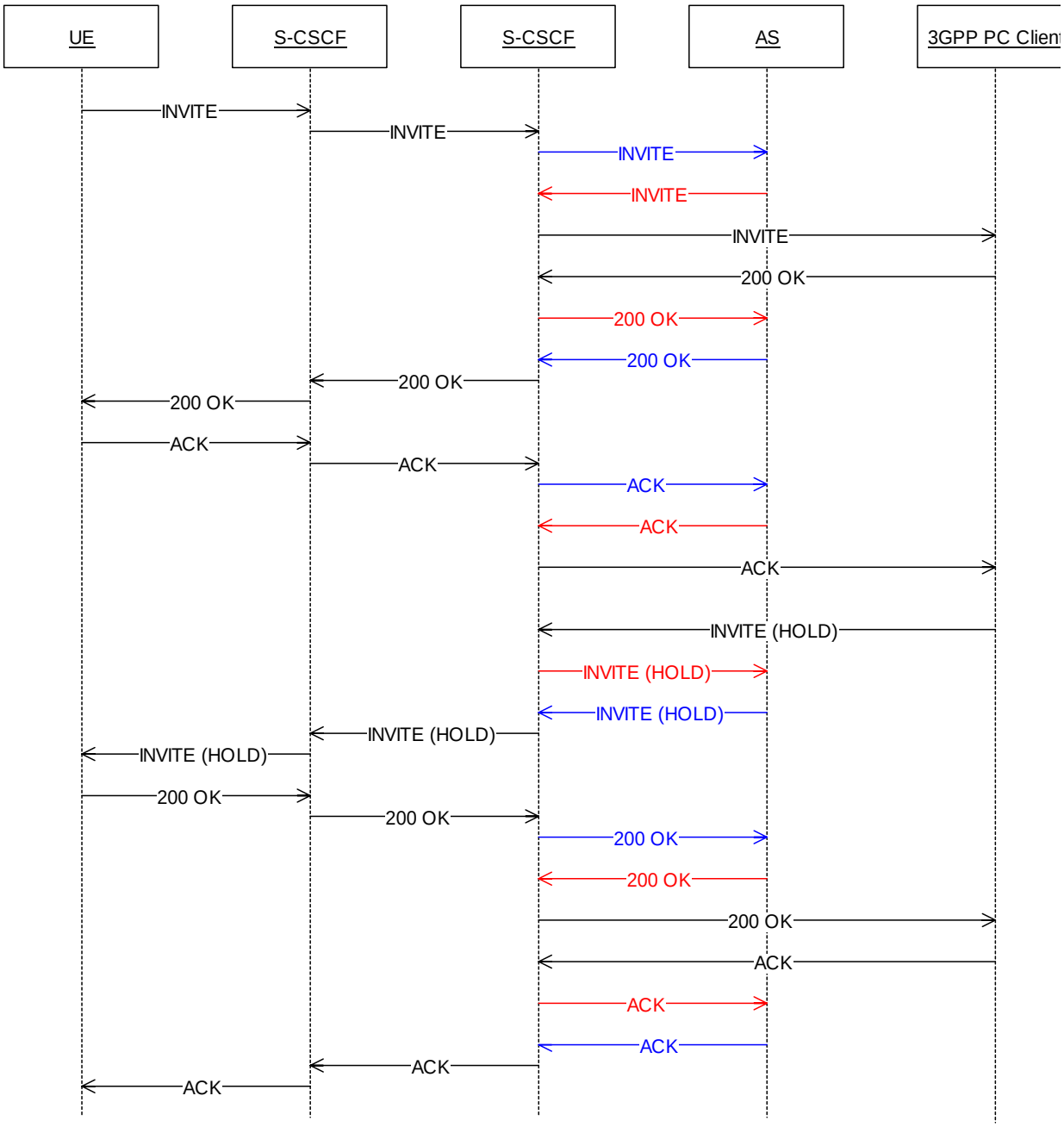
```
NOTIFY sip:jcanas@47.102.116.66 SIP/2.0
t: <sip:jcanas@rich.techtrial.com>
f: <sip:jcanas@rich.techtrial.com>;tag=15830211
i: 1019940e58a
CSeq: 5583380 NOTIFY
v: SIP/2.0/UDP
  47.103.142.13:5060;branch=z9hG4bKac2b3d0bc32bd32d287d3bc036a5fec7
```

```
Max-Forwards: 20
EVENT: message-summary
k: com.nortelnetworks.firewall,p-
  3rdpartycontrol,nosec,com.nortelnetworks.im.encryption
l: 22
c: application/simple-message-summary

Messages-Waiting: no
```

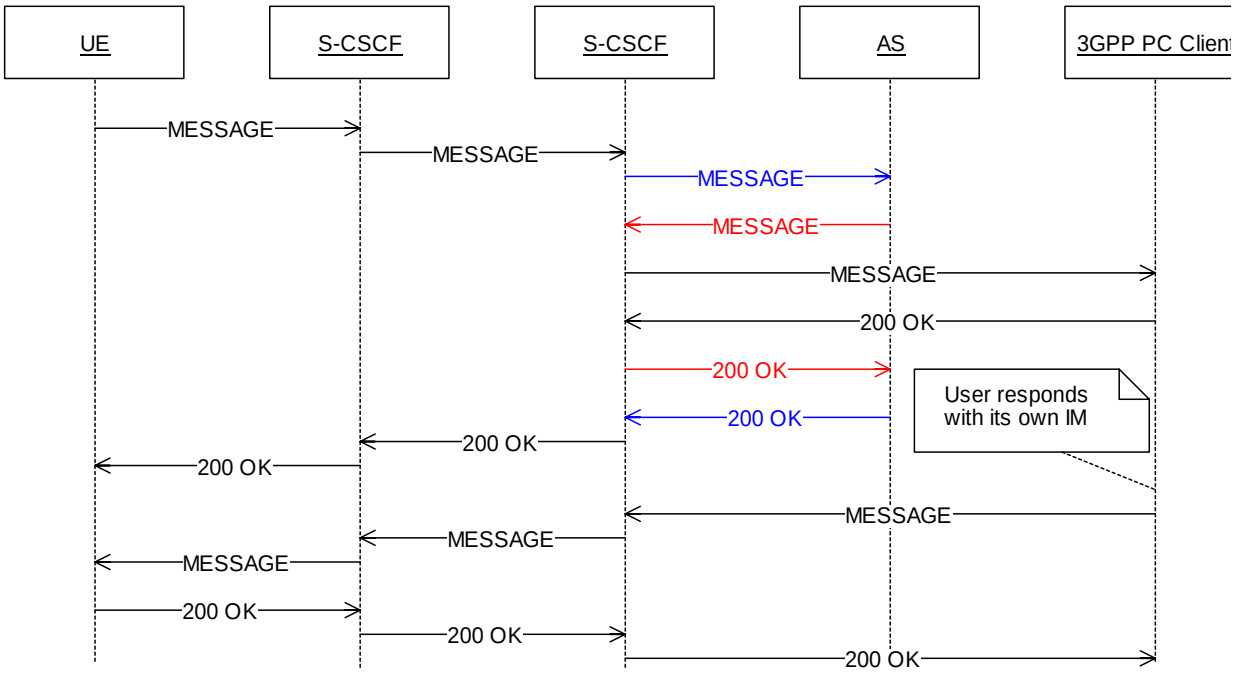
AS incoming 200 OK:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
  47.103.142.13:5060;branch=z9hG4bKac2b3d0bc32bd32d287d3bc036a5fec7
From: <sip:jcanas@rich.techtrial.com>;tag=15830211
To: <sip:jcanas@rich.techtrial.com>;tag=16a-d18-d2c-f410feb3
Call-ID: 1019940e58a
CSeq: 5583380 NOTIFY
User-Agent: Nortel PCC 4.0.276
Content-Length: 0
```

74.15 Hold


UE
S-CSCF
S-CSCF
AS
3GPP PC Client
INVITE
INVITE
INVITE
INVITE
INVITE
200 OK
200 OK
200 OK
200 OK
200 OK
ACK
ACK
ACK
ACK
ACK
INVITE (HOLD)
INVITE (HOLD)
INVITE (HOLD)
INVITE (HOLD)
200 OK
200 OK
200 OK
200 OK
200 OK
ACK
ACK
ACK
ACK

74.16 Instant Messaging



Call scenario: An MCS user receives an IM from an IMS user, and responds with his own instant message.

High level breakdown:

1. The first originators S-CSCF receives the MESSAGE and determines (through the HSS) that the destination party is currently located at another S-CSCF.
2. The MESSAGE is sent to the second S-CSCF. This S-CSCF determines (through the HSS), that the terminating subscriber has services in the AS.
3. The S-CSCF sends the MESSAGE to the AS, with nt_info=term in the route header.
4. The AS runs only through the term subscriber services, and sends a MESSAGE back to the S-CSCF request URI set to client contact address)
5. The S-CSCF sends the MESSAGE to the MCS client.
6. The MCS client displays the received instant message.
7. The MCS subscriber then types his own instant message and sends the MESSAGE back to the second S-CSCF (it was the one in the contact header?)

8. This S-CSCF determines (through the HSS) that no originating services are supported at the AS for this client, and it does not contact the AS.
9. The S-CSCF determines (through the HSS) that the terminating user is at another S-CSCF and forwards the MESSAGE to the other S-CSCF.
10. The first S-CSCF determines through the HSS that the destination subscriber is not an MCS user and therefore just sends the MESSAGE to the client.

74.17 Hardware Requirements or Dependencies

The R6 MCS Application server will only be supported in the same configuration as the 9.0 Standalone MCS. At this time, this translates to an eight N240 server configuration. However, because the R6 AS does not support interactions with IPCM and Gatekeeper, the number of N240 servers is reduced to 6.

Also, in this release, the R6 AS does not support interactions with a Media Portal. The target network for this release is not expected to require this node because there are no NATs or firewalls in the network.

74.18 Software Requirements or Dependencies

The R6 AS and its supporting MCS nodes shall use the same loads as their equivalent nodes in the 9.0 MCS Standalone configuration.

The only difference between the two deployments shall be the value assigned to a System Manager configuration parameter which converts the MCS SessionManager into the R6 AS.

74.19 Limitations and restrictions

Refer to the Feature Description section.

74.20 Interactions

None.

74.21 Glossary

Term	Description
New term	definition

75: Functional description (FN): A00009443

75.1 Feature name and Feature ID

T.38 Annex D for NGSS , activity A00009443.

75.2 Description

75.2.1 Overview

The main part of this activity provides support for H.248 T.38 Annex D interworking with SIP. This functionality is only available if both the remote MTA and SIP server support T.38 Annex D. A new provisioning flag **T.38 Annex D Supported** is added to the remote server option list to indicate that the remote server supports T.38 Annex D.

The call scenarios covered by this feature are described by ITU-T T.38 Annex D, specifically section D.2.2.4 - Voice and facsimile connection.

This activity intends to provide T.38 Annex D interworking support for SIP with H.248 PVG on the local side. For this feature to work, the Gateway controller must have T.38 enabled in the network codec profile provisioning, the H.248 GW PVG must support T.38, and the **T.38 Annex D Supported** flag must be enabled in the NGSS provisioning remote server option page. If so, then upon fax detection, a switch over is performed from G.729 (or G.711) to T.38 codec.

The switch-over is performed using an existing mechanism based on sending a re-Invite message with the new codec in the SDP. If the offer is accepted, the call switches to T.38 mode once the re-Invite sequence completes.

In case that a switch attempt is rejected by either end, an attempt will be made to preserve the call by switching to G.711 codec.

This feature is done in parallel with SN09 activity A00009294 which is responsible for the connection broker changes in the GWC.

The second part of this feature provides ability to prevent automatic upspeed from G729 to G711 by 248 PVG on fax detection as is the default PVG behavior. A new field **Re-Invite for Voice Band Data** is added to enable this functionality. If this field is enabled, the PVG will not auto upspeed to G711 but send a Re-Invite upon fax detection, to switch either to G711 codec or to

T.38 if **T.38 Annex D Supported** is provisioned. Note that if the original media for the call was set up using G711 codec, the new field has no effect, and the call behavior is dependent only on whether the **T.38 Annex D Supported** is enabled or not, as described above. If both **Re-Invite for Voice Band Data** and

75.2.2 Scenarios covered by this activity :

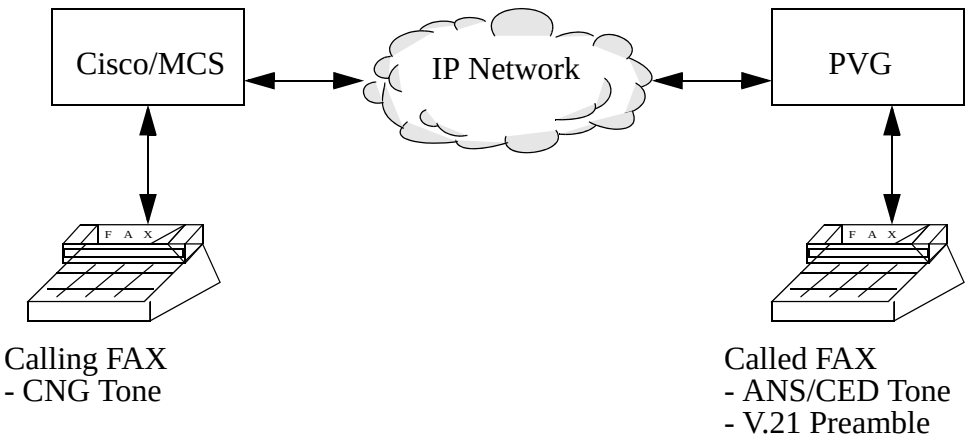
There are 2 basic T.38 scenarios covered by this feature, as illustrated in the following figures. Figure 1 shows a scenario in which PVG detects the T.38 tones and initiates the switch. Figure 2 shows a scenario in which T.38 tones are detected by the Cisco/MCS which initiates the switch to T.38.

Note that for the T.38 call scenarios covered by this feature it does not matter which side originated the original voice call, but which gateway sends the T.38 tones (emitting gateway) and which gateway (receiving gateway) detects the tones and initiates the switch. For this feature, it is always the receiving gateway that initiates the switch.

The call scenarios that use the field **Re-Invite for Voice Band Data** are very similar to the T.38 call scenarios discussed here. If the **Re-Invite for Voice Band Data** is provisioned, but **T.38 Annex D Supported** is not, then the call switches to G.711 codec upon fax detection exactly in the same fashion as described below for T.38. If both fields are provisioned, PVG end will attempt to switch first to T.38, and if the attempt is rejected by the far end which does not support T.38, PVG will send another Re-Invite to switch to G.711.

75.2.2.1 T.38 fax calls originating from SIP/NGSS and terminating at PVG.

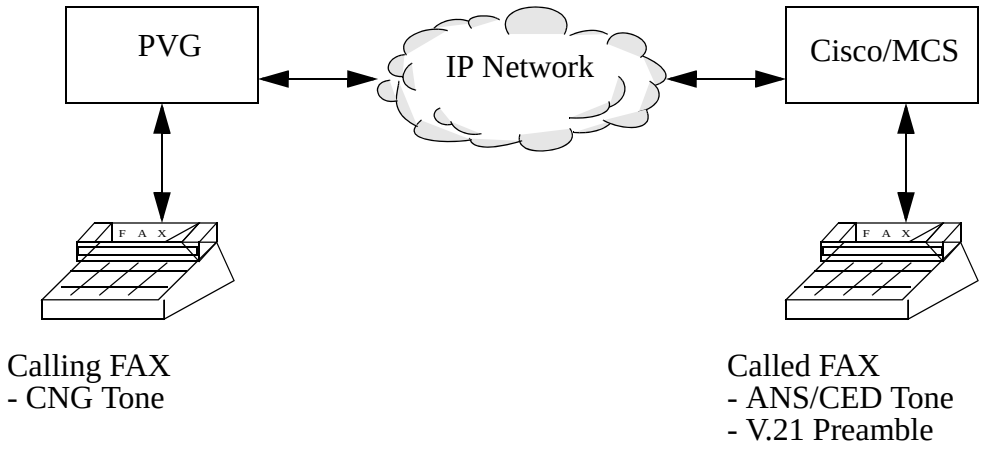
Figure 1



- A SIP Invite is sent to the CS2K by the CISCO/MCS requesting a voice connection.
- A voice connection is then established.
- Upon detection of fax tone the receiving gateway , PVG, it sends a V.21 notification to CS2K.
- CS2K then sends a SIP Re-Invite request to the emitting gateway (with the same Call-ID as the already existing voice connection) for a T.38 facsimile connection.
- Upon completion of the facsimile call establishment, the T.38 fax call proceeds with a T.38 V.21 flags indicator packet.

75.2.2.2 T.38 fax calls originating from PVG and terminating at SIP/ NGSS.

Figure 2



- For calls originating from the PVG end, a SIP Invite is sent to the CISCO/ MCS requesting for a voice connection.
- A voice connection is established.
- A V.21 notification is received by the CISCO/MCS.
- It sends a re-invite to the originating side PVG, and the switch-over to T.38 occurs.

75.2.3 New functionality provided by this feature

75.2.3.1 Provisioning

Two new provisioning fields are added by this feature.

A new boolean provisioning flag **T.38 Annex D Supported** is added to the NGSS option list on the remote server provisioning web page to indicate that the remote server supports T.38 Annex D. This flag has to be set to 'Y' to enable this functionality. It should be set to 'Y' only if the remote SIP server supports T.38 Annex D.

A new boolean provisioning flag **Re-Invite for Voice Band Data** is added to the NGSS option list on the remote server provisioning web page to prevent automatic upspeed from G729 to G711 by 248 PVG on fax detection as is the default PVG behavior. This flag has to be set to 'Y' to enable this functionality. It has no effect on non-PVG gateways.

75.2.3.2 Proprietary header for the SIP INFO message

A SIP info message is used to tandem the T.38 scan request to the other CS2K. It contains a new proprietary Nortel SIP header to indicate to the other CS2K that it should scan for T.38 tones.

The new header is defined as follows:

x-nt-action-req = "action" HCOLON action-value *(";" action-value)
action-value = "t38annexd" / "vbdannexd"

The following is an example of the SIP INFO message using this header:

INFO sip:9192461814@MGCA;user=phone SIP/2.0
Via:SIP/2.0/UDP MGCA;maddr=47.174.75.160
To:<sip:9192461814@MGCA;user=phone>
From:<sip:2461817@MGCA;user=phone>
Call-ID:0111.5119-22-19-49-11.68@MGCA
CSeq:1 INFO
X-nt-action-req: t38annexd
Content-Length:0

If a SIP info message containing the above header with action value of '38annexd' is received by an NGSS in any CS2K, it should have the same meaning as if the **T.38 Annex D Supported** was provisioned on the NGSS. The CS2K should start scanning for T.38 fax tones and initiate the switch to the T.38 codec if detected. In a similar fashion, a SIP info message containing

the above header with action value of ‘vbdannexd’ received by an NGSS in any CS2K should have the same meaning as if the **Re-Invite for Voice Band Data** was provisioned on the NGSS.

75.2.3.3 Call preservation in case of codec switch rejection.

In case that the remote SIP server rejects a re-Invite message initiating the switch to T.38 by sending a 488 Not Acceptable Here response, the CS2K will attempt to preserve the call by sending another re-Invite with G.711 codec offer. If this offer is accepted, the call will be preserved.

In case that the PVG rejects the attempt to switch to T.38 codec initiated by the remote server re-Invite, the CS2K will respond with 488 Not Acceptable Here message. It is up to the remote SIP server to initiate a switch back by sending another offer in the re-Invite.

75.2.4 Supported Call Flows

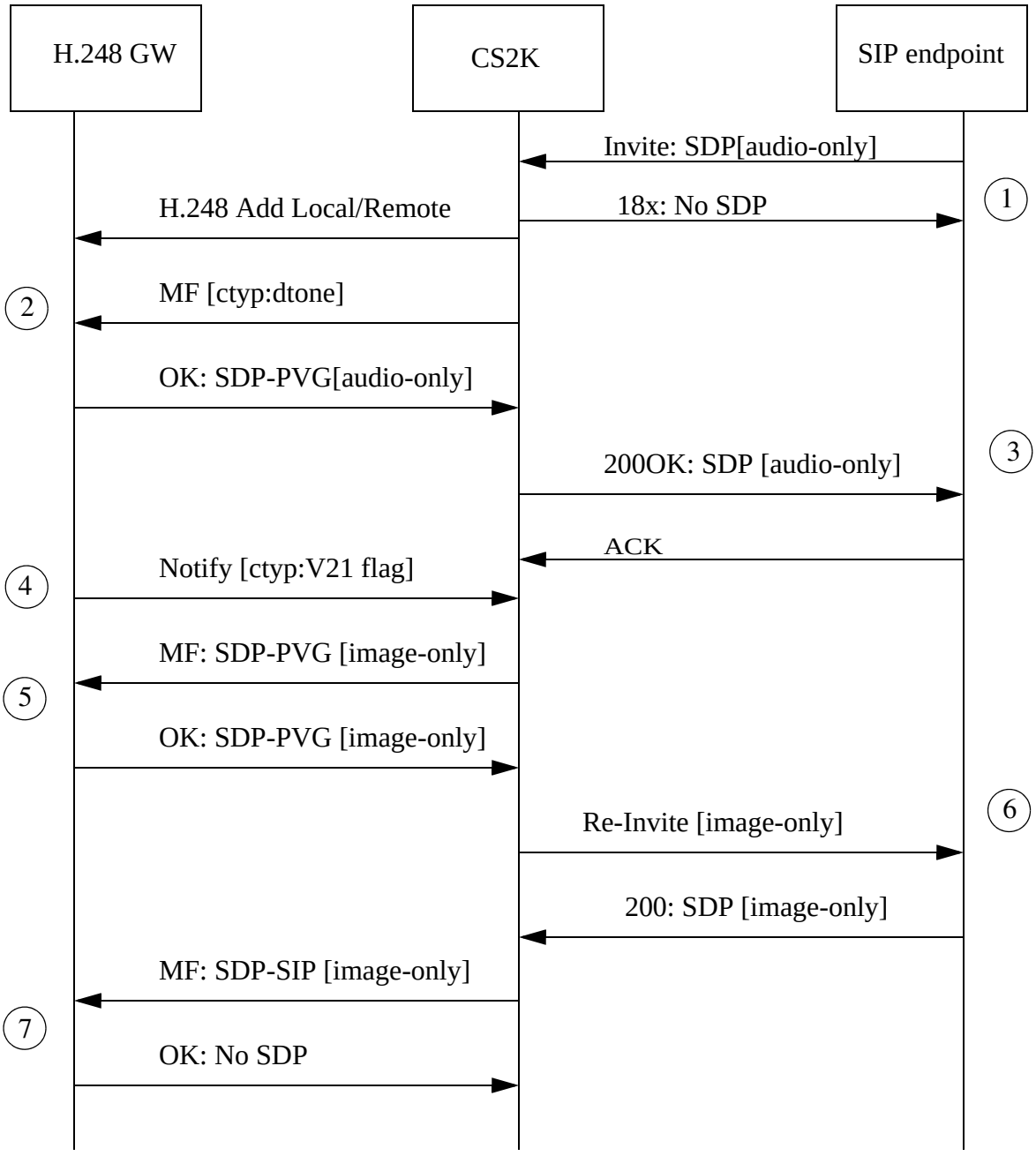
Description of T.38 Annex D functionality is provided via call flows provided in the following figures . The description of the first call flow is given in detail and may be applied to other subsequent call flows.

75.2.4.1 Basic Call Scenario: SIP to PVG interworking.

When the call is originated from the CISCO/MTS SIP endpoint:

In this scenario, the voice call is call originates from CISCO/MTS in the form of SIP INVITE sent to CS2K. Since the **T.38 Annex D Supported** is enabled in the NGSS for the remote server, during the voice call setup the PVG is asked to scan for fax tones. A voice call is established successfully, and then PVG detects a V.21 flag. V.21 Fax notify is sent from PVG which triggers an attempt to change the codec from G.711 or G.729 to T.38 communicated to the remote end via a re-Invite sequence.

Figure 3 T.38 Calls originating from CISCO/MTS and terminating at PVG on CS2K



Note 1: After receiving an INVITE from the SIP endpoint, a voice call is established. If in the Gateway controller configuration, T.38 is enabled in the network codec profile provisioning the ephemeral is added, and the PVG is asked to choose from m = audio $$$ m = image $ udptl t38.

Note 2: If the **T.38 Annex D Supported** flag is enabled on the remote server , the H248 GWC requests the PVG to scan for all events on the ctyp/ dtone package.

Note 3: The PVG replies with the intersection of the PVG capability and the offer from SIP Invite, which is sent to the remote SIP end point. At this point voice call is established.

Note 4: The PVG then reports any detected ctyp/dtone event to the GWC.

Note 5: Upon detection of a CNG or a V.21 flag the GWC will send a modify to the PVG with the local descriptor m=image $ udptl t38.

Note 6: CS2K sends this image only SDP to the remote SIP end point in Re-INVITE message.

Note 7: Upon receipt of SDP(T.38) from remote SIP end point, CS2K sends a modify indicating the offer has been accepted. At this point T.38 fax call is established.

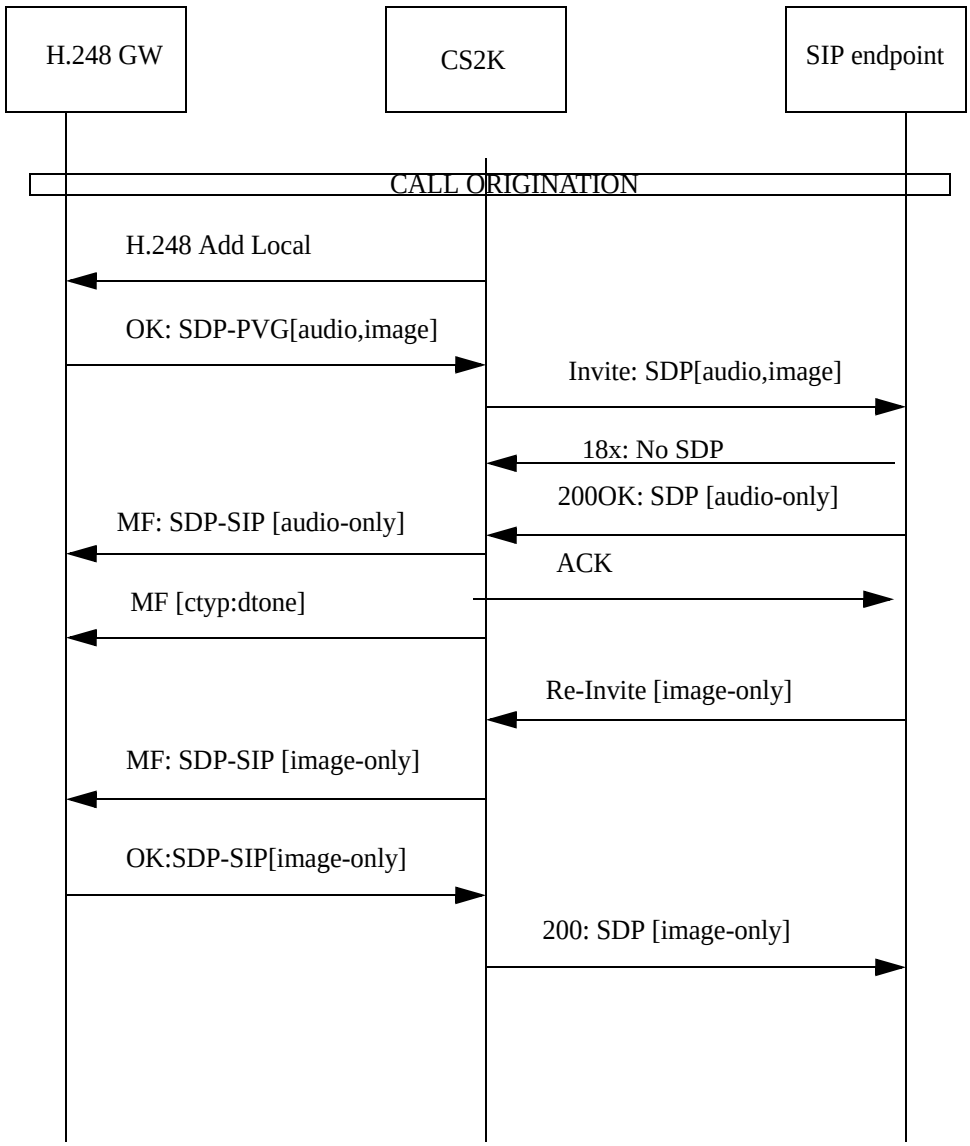
Note 8: The content of SDP uses following abbreviation:

- SDP(audio) for processing of audio media stream.
- SDP(t38) for processing of t38 media stream.
- SDP(audio, t38) for simultaneous processing of audio and t38 media streams.
- SDP(audio, t38-cap) for processing of audio media stream and for t38 capability indication.

75.2.4.2 Basic Call Scenario: PVG to SIP interworking.

When a call originates from PVG, a SIP INVITE is sent from CS2K to the SIP Endpoint which replies with its SDP. Since the **T.38 Annex D Supported** is enabled in the NGSS for the remote server, during the voice call setup the PVG is asked to scan for fax tones. After the voice call is established successfully the remote receiving gateway detects V.21 flag and starts the re-Invite sequence leading to change from G.711 or G.729 codec to T.38. Once the sequence completes, the T.38 fax call is established.

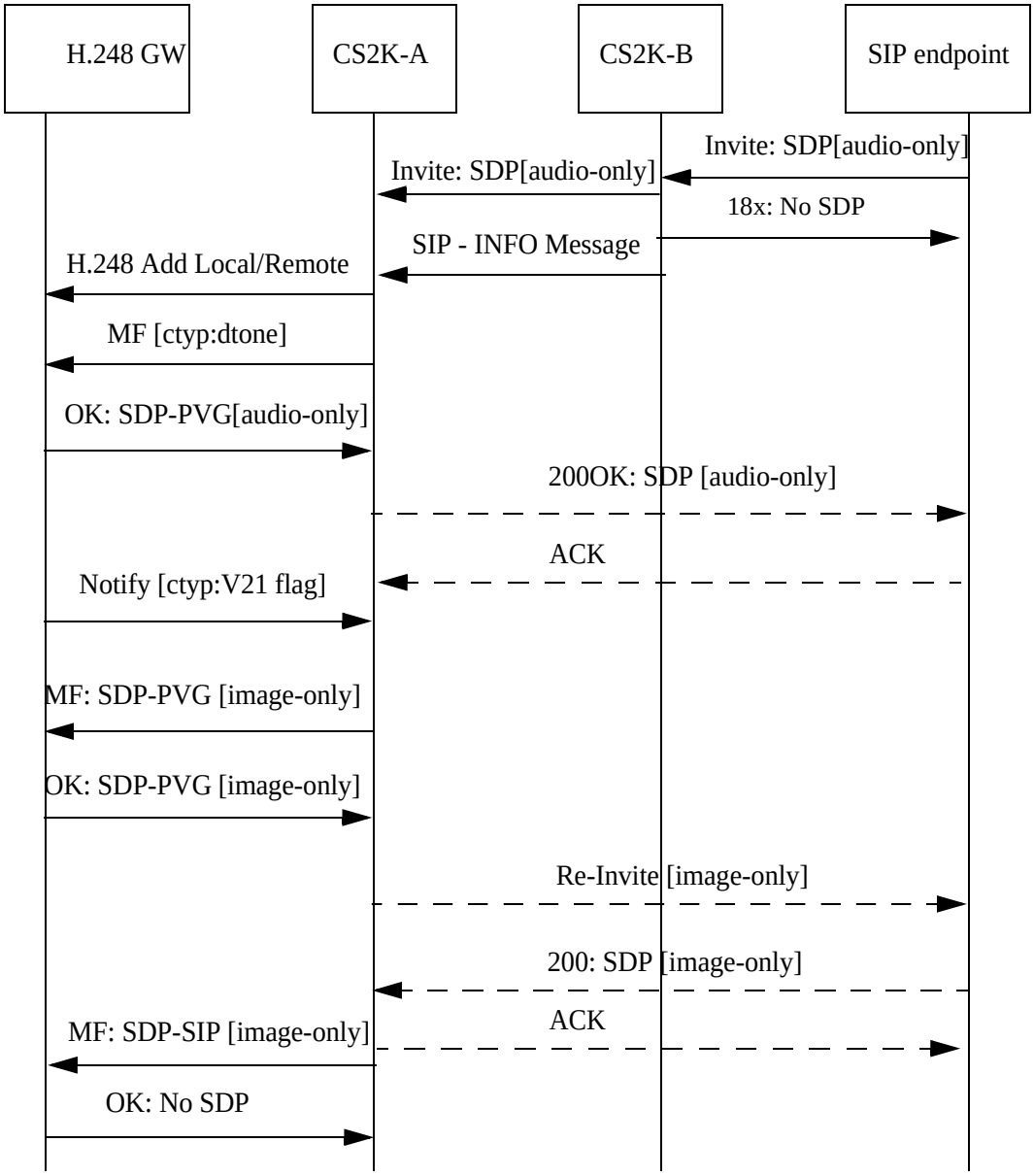
Figure 4 T.38 Calls originating from PVG on CS2K and terminating at CISCO/ MTS



75.2.4.3 Tandeming Support

In this scenario **T.38 Annex D Supported** is enabled in the CS2K-B NGSS, but the call is tandemed to CS2K-A which is not aware that the remote SIP server supports T.38. A SIP INFO message with a proprietary header is used to inform CS2K-A that T.38 support is required causing the CS2K-A to instruct the H.248 PVG to scan for fax tones during the voice call establishment. A voice call is established successfully, and then PVG detects a V.21 flag. V.21 Fax notify is sent from PVG which triggers an attempt to change the codec from G.711 or G.729 to T.38 communicated to the remote end via a re-Invite sequence.

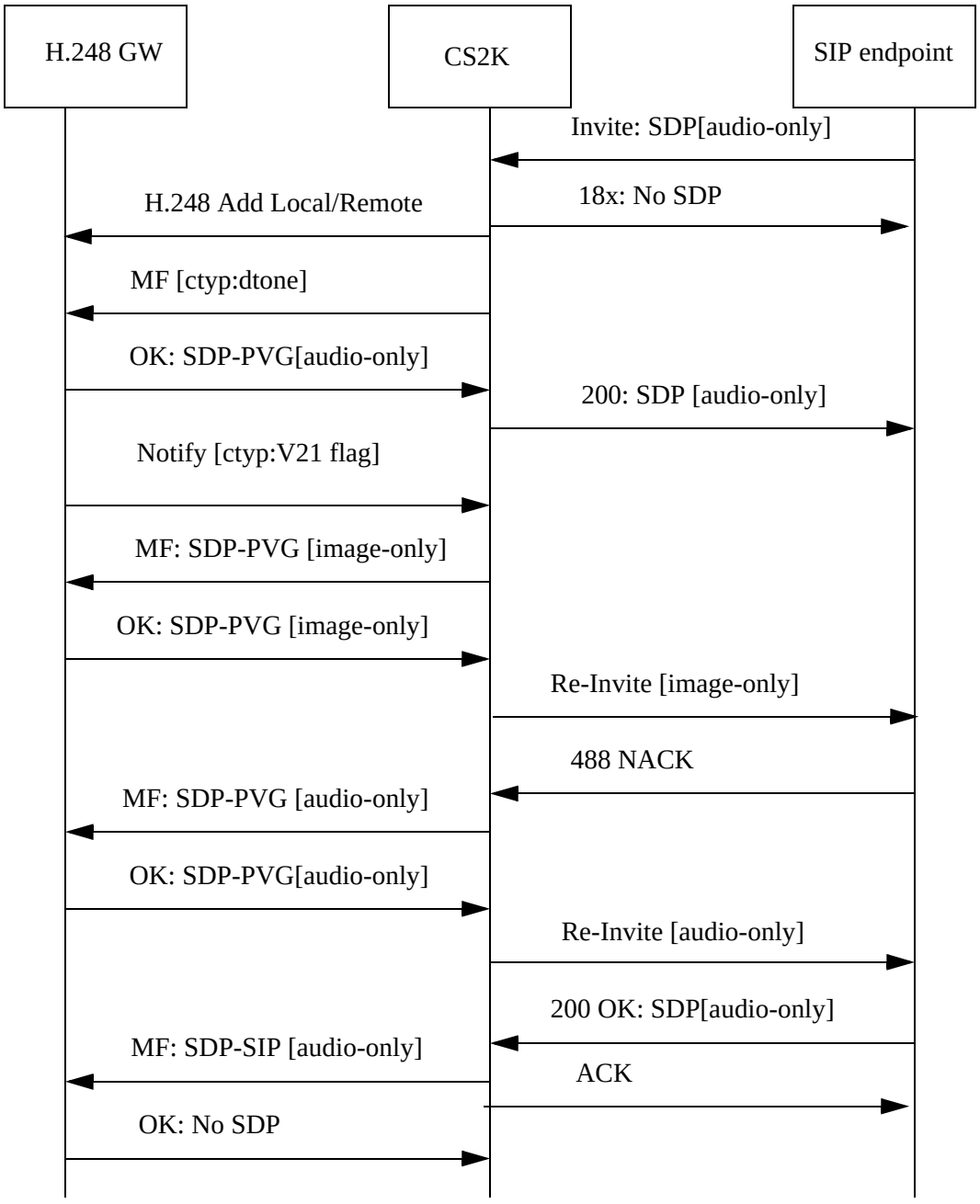
Figure 5 T.38 Fax calls spanning over more than one CS2K



75.2.4.4 Unsuccessful switch attempt, far end rejection.

This scenario describes an unsuccessful T.38 Fax call attempt, where the SIP Re-INVITE for the switch-over from voice to T.38 mode is rejected by a SIP 488 Not Acceptable Here response. In this case an attempt is made to preserve the call by switching back the codec to voice. This is done via another SIP Re-INVITE sequence with voice only codec to switch the call back to voice, as shown in Figure 6.

Figure 6 SIP endpoint rejects the Offer

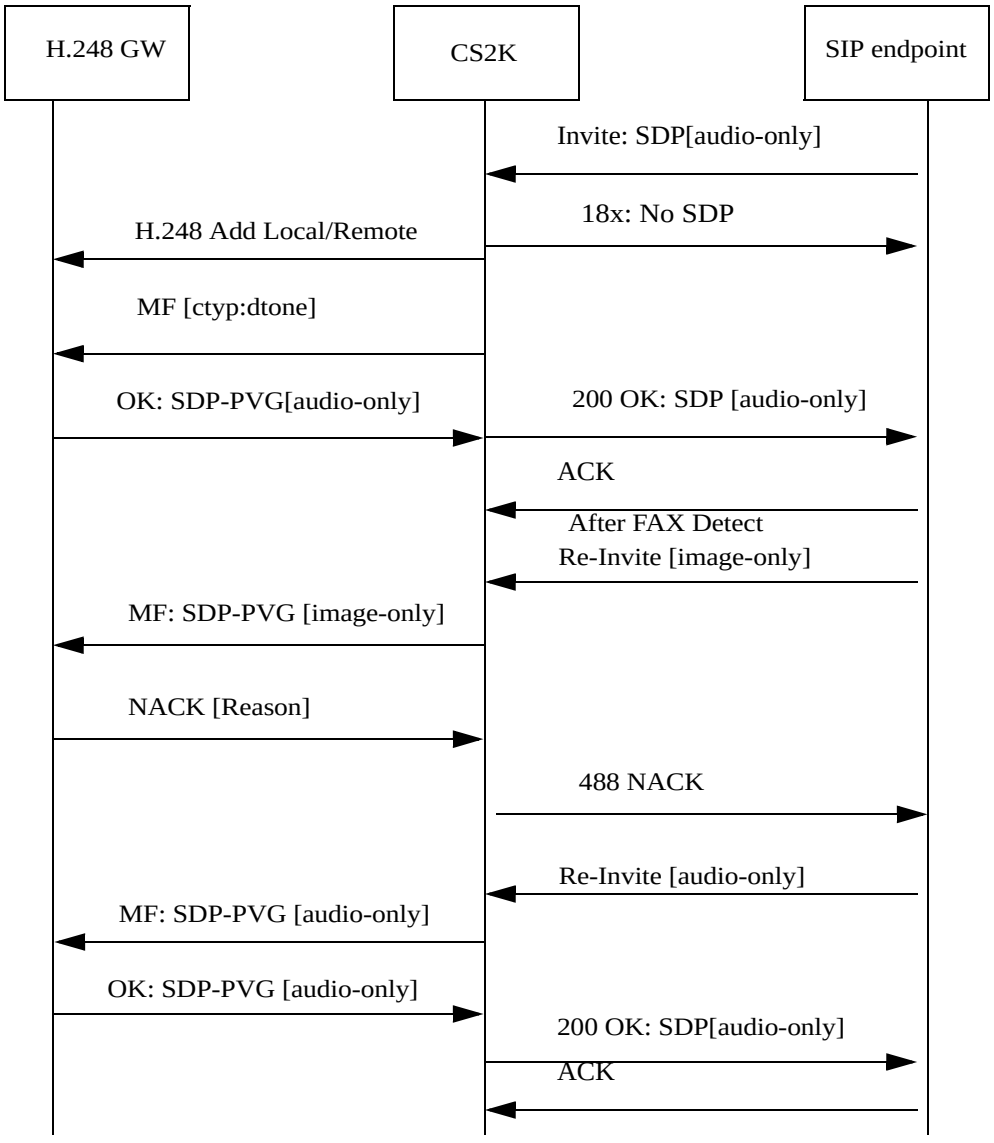


75.2.4.5 Unsuccessful switch attempt, local rejection

When the SIP Re-INVITE Fax offer for a switch to T.38 comes from the remote SIP side and the PVG NACKS it, the PVG sends the reason for the

rejection to the SIP side which in turn sends a SIP Re-INVITE to change the SDPs to audio-only mode.

Figure 7 PVG Rejects Offer



75.3 Hardware Requirements or Dependencies

No New hardware is required.

75.4 Software Requirements or Dependencies

CM/GWC/NGSS: SN09 load

H.248 GW: supporting H.248.1, H.248.2 ctyp package, T.38 mode.

T.38 should be provisioned on the H.248 GWC

T.38 Annex D Supported option should be provisioned on the NGSS Remote SIP Server provisioning page.

75.5 Limitations and restrictions

- This feature verifies T.38 Annex D interworking for H.248 PVG GW on one call leg and 3rd party SIP User Agent Server supporting T.38 Annex D functionality on the other call leg. It should not be enabled for remote SIP servers that don't support T.38 Annex D.
- **Re-Invite for Voice Band Data** field should be only used to prevent auto upspeed on fax detection from G.729 to G.711 by an H.248 PVG that is provisioned to support G.729.

75.6 Interactions

Not Identified.

75.7 Glossary

Term	Description
CED	Called terminal identification answer tone of Fax device (2100 +/- 15 Hz, continuous tone, duration 2.6-4.0 sec.) see T.30 chapter 4.1
CM	Call Manager, Computing Modules
CNG	Calling tone of Fax device (1100 +/- 38 Hz, 0.5 sec. on, 3.0 sec. off, duration 60-120 sec.) see T.30 chapter 4.2.
CS2K	Call Server 2000
G3FE	Group 3 Facsimile Equipment G3FE refers to any entity which presents a communication interface conforming to ITU- T Recommendation T. 30, T. 4, and optionally T. 6. A G3FE may be a traditional G3 facsimile machine, an application with a T. 30 protocol engine or any other possibility mention in the network model for IP Facsimile mentioned in Recommendation T. 38.

Term	Description
GW	Gateway (Signalling Gateway and Media Gateway)
GWC	Gateway Controller
MCS	Multimedia Communication Server
PSTN	Public Switched Telephone Network.
PVG	Passport Packet Voice Gateway
RFC	Request For Comments (IETF)
RTP	Real-time Transport Protocol (IETF 1889, 3550)
SDP	Session Description Protocol (IETF RFC 3266)
SIP	Session Initiation Protocol (IETF RFC 3261)
UDP	User Datagram Protocol (IETF RFC 768)
UDPTL	Facsimile UDP Transport Layer protocol (ITU T.38)
V.21 Preamble	Series of flag sequences 01111110 for 1 sec +/- 15%.

76: Functional description (FN): A00009446

76.1 Feature name and Feature ID

Feature ID: A00009446
Feature name: M2UA/SCTP Protocol for PVG SS7 backhaul support

76.2 Description

This feature implements the M2UA protocol thus providing the USP with the ability to backhaul MTP3 message, allowing the termination of MTP2 or SAAL on a remote node.

The USP always acts as the client with respect to SCTP associations and use SCTP port 2904. The USP implements the ASP portion of the M2UA while the PVG supports the SG portion.

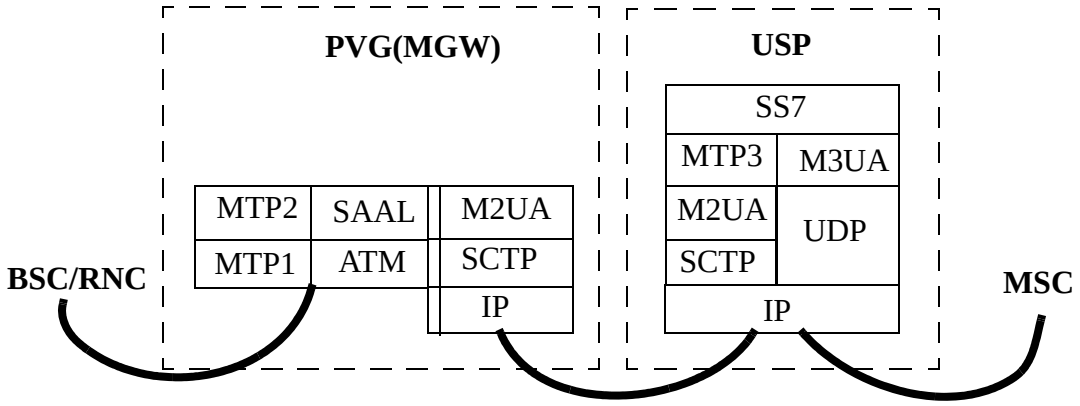
For the requirement, please refer to [2].

76.3 Support M2UA in USP

76.3.1 Functional overview

Broadband SS7 (MTP3b/SAAL/ATM) is the signaling transport used on the UMTS Iu interface, Iu-RANAP from the UTRAN is backhauled to the MSC over IP. The MGW provides the interworking function between bbSS7 and SIGTRAN over IP. The SG/USP accepts the SIGTRAN interface from the MGW and converts it to the proprietary interface required by the MSC.

In addition to the requirement for bbSS7 backhaul, narrowband SS7 (MTP3/MTP2/MTP1) backhaul over IP is also applicable. Narrowband SS7 is used for control signaling on the GSM A interface and ISUP signaling on the PSTN interfaces. Narrowband SS7 is carried over IP in much the same way as bbSS7. MTP2 is terminated on the MGW and transported over M2UA/SCTP/IP to MSC. The enables the MTP2 physical interface to be geographically separated from the MTP3 layer running on the USP.



76.3.2 Function provided by the M2UA Adaptation Layer

76.3.2.1 Mapping

Interface Identifier (IID) is used to tie the SCTP association/stream with the SS7 physical link in the SGP (PVG/MGW). When an ASP (USP) sends an ASP Active message for a particular IID, the SGP will try to provide the Signalling Link Terminal service to an SS7 link tied by the IID.

76.3.2.2 Support for the management of SCTP associations

The M2UA layer may be instructed by local management (LM) to establish an SCTP association to a peer M2UA node. This can be achieved using the MSCTP_ESTABLISH primitive to request, indicate and confirm the etablishment of an SCTP association with a peer M2UA node.

The M2UA layer MAY also need to inform local management of the status of the underlying SCTP associations using the M-SCTP_STATUS request and the indication primitive.

76.3.2.3 SCTP Stream Management

M2UA requires a stream for each ss7 link provisioned. The M2UA layer residing on a card can handle maximum 32 ss7 links. Each association (determined by far-endpoint ip address, local and remote port) can have up to 8 traffic streams and one more stream for management - stream '0' is reserved for ASP Management (ASPM) messages.

The SS7IPLink running M2UA can handle approx 1792 messages/sec at 80% capacity or 2300 messages/sec in overload regardless of message size. The bandwidth of 1792 messages/sec per card is shared among the M2UA links provisioned on that card.

76.3.3 M2UA Message Structure

76.3.3.1 Common Message Header

Table 1: Common Message Header for M2UA

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Version	Spare	Message Class	Message Type
Message Length			

Table 2: Message Class List

Value	Description
0	Management (MGMT) Message
3	ASP State Maintenance (ASPSM) Messages
4	ASP Traffic Maintenance (ASPTM) Messages
6	MTP2 User Adaptation (MAUP) Messages

Table 3: Message Type List

Message Class	Value	Description	Notes
0	0	Error (ERR)	
	1	Notify (NTFY)	
3	1	ASP Up (UP)	
	2	ASP Down (DOWN)	
	3	Heartbeat (BEAT)	never send BEAT
	4	ASP Up Ack (UP ACK)	
	5	ASP Down Ack (DOWN ACK)	
	6	Heartbeat Ack (BEAT ACK)	
4	1	ASP Active (ACTIVE)	
	2	ASP Inactive (INACTIVE)	
	3	ASP Active Ack (ACTIVE ACK)	
	4	ASP Inactive Ack (INACTIVE ACK)	

Message Class	Value	Description	Notes
6	1	Data	
	2	Establish Request	
	3	Establish Confirm	
	4	Release Request	
	5	Release Confirm	
	6	Release Indication	
	7	State Request	
	8	State Confirm	
	9	State Indication	
	10	Data Retrieval Request	
	11	Data Retrieval Confirm	
	12	Data Retrieval Indication	
	13	Data Retrieval Complete Indication	
	14	Congestion Indication	
	15	Data Acknowledge	

76.3.3.2 M2UA Message Header

For MAUP messages, there is a M2UA specific message header immediately follow the common message header. The format like the below.

Table 4 MAUP Specific Message Header

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x01)		Length (=8)	
Interface Identifier			

76.3.3.3 Parameters

M2UA messages consist of a Common Header followed by zero or more variable-length parameters, as defined by the message type. The variable-length parameters contained in a message are defined in a Tag-Length-Value format.

The common parameter tags (can be used by all User Adaptation layers) is supported as below.

Table 5: Common Parameters Tags

Value	Description	Notes
1	Interface Identifier (Integer)	
3	Interface Identifier (Text)	Not supported
4	Info String	Not supported
7	Diagnostic Information	Not supported
8	Interface Identifier (Integer Range)	Not supported
9	Heartbeat Data	
11	Traffic Mode Type	
12	Error Code	
13	Status Type/Information	
17	ASP Identifier	
19	Correlation Id	Not supported

Besides the common parameters, there are M2UA specific parameters.

Table 6: M2UA Specific Parameters Tags

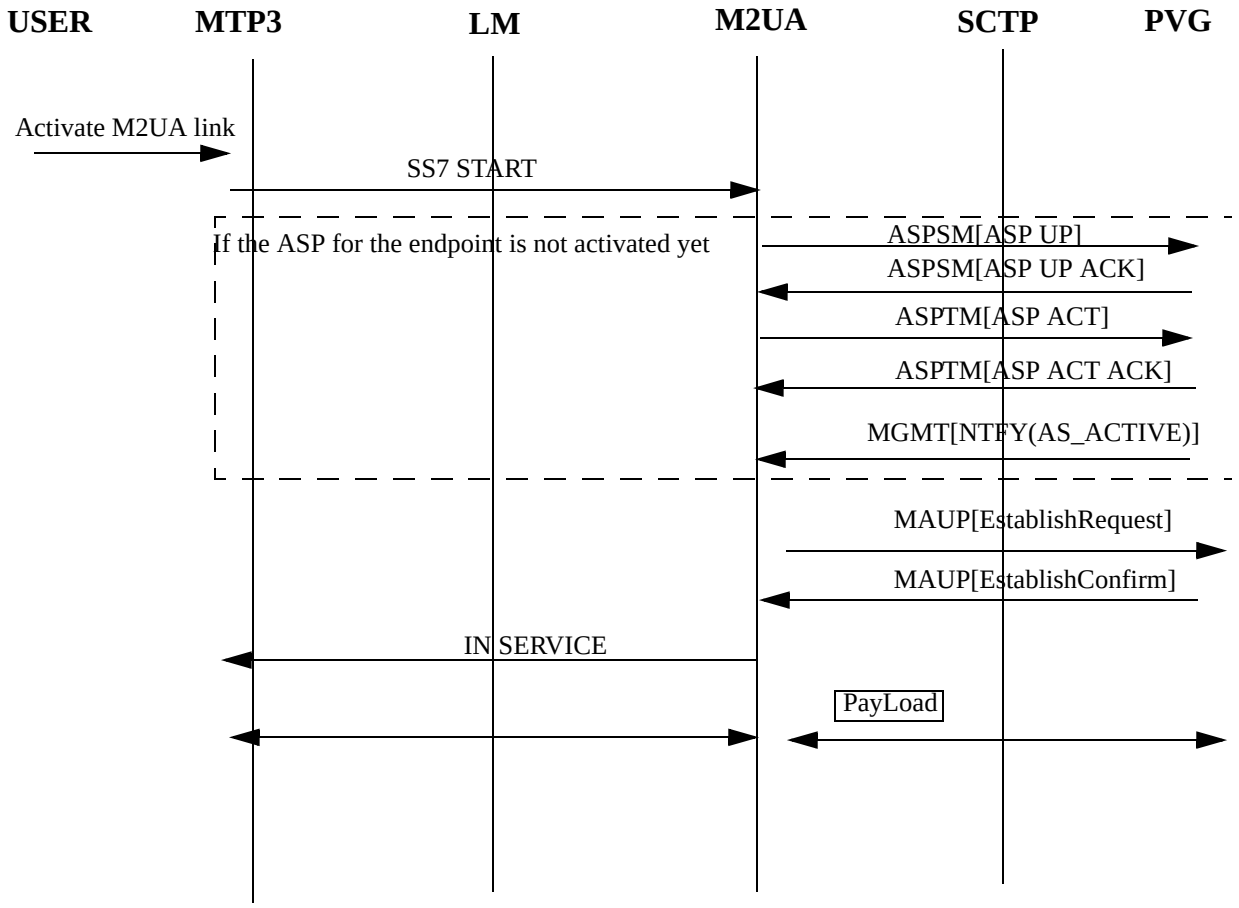
Value	Description	Notes
768	Protocol Data 1	
769	Protocol Data 2 (TTC)	Not supported
770	State Request	
771	State Event	
772	Congestion Status	
773	Discard Status	Not supported
774	Action	
775	Sequence Number	
776	Retrieval Result	
777	Link Key	Not supported

Value	Description	Notes
778	Local-LK-Identifier	Not supported

76.3.4 RFC M2UA procedures supported by USP

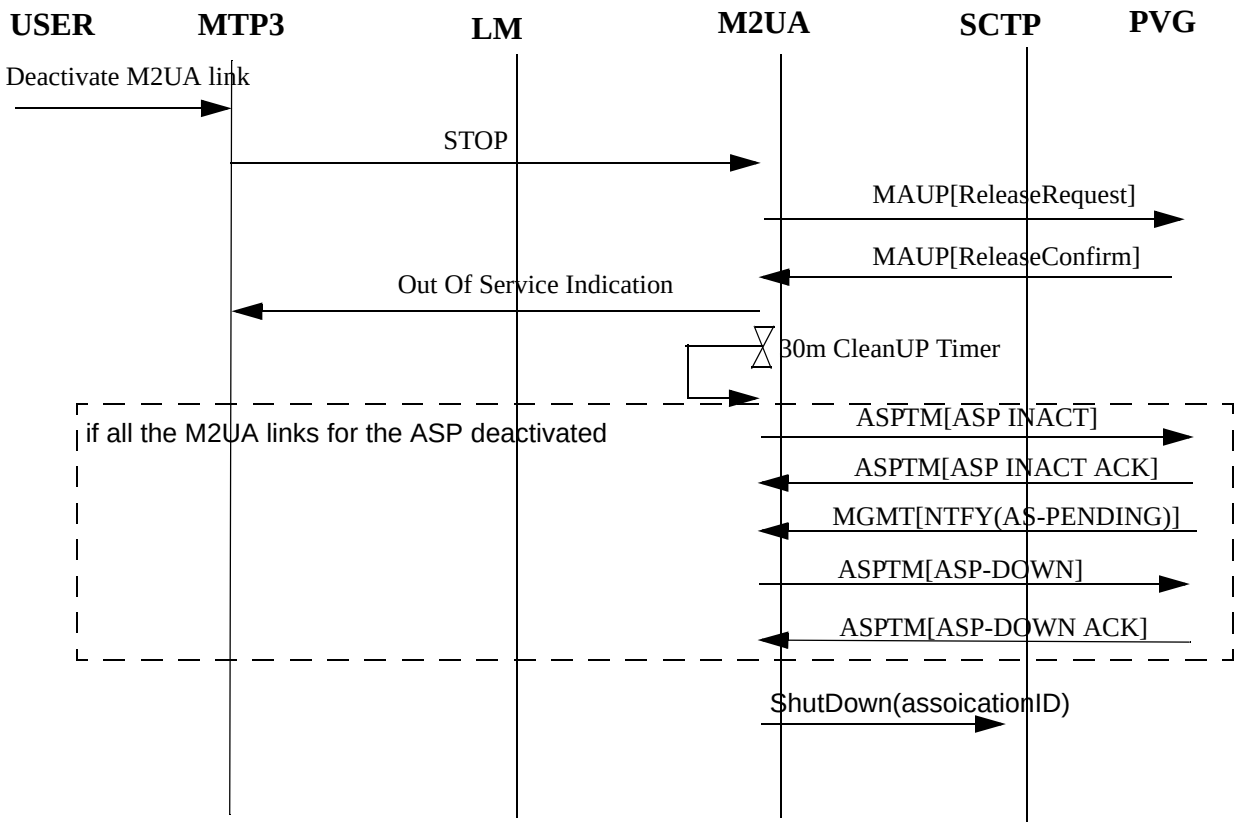
76.3.4.1 Activate M2UA link

Figure 7: Activation of M2UA link and ss7 link alignment



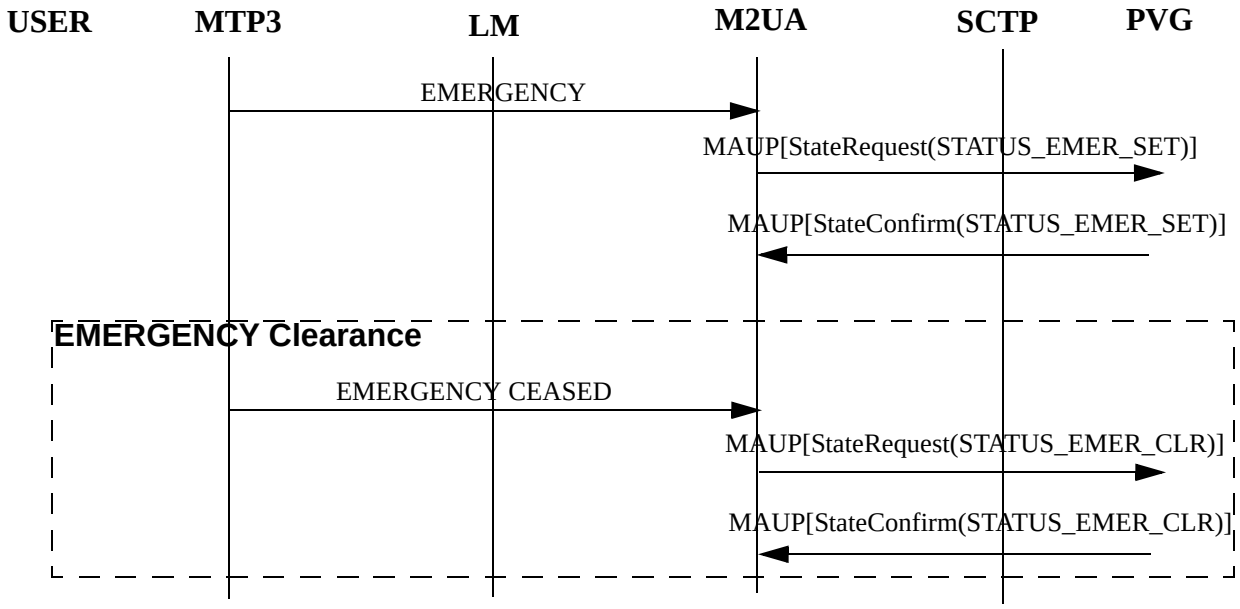
76.3.4.2 Deactivate M2UA link

Figure 8: Deactivation of M2UA link



76.3.4.3 Emergency and Emergency Clearance

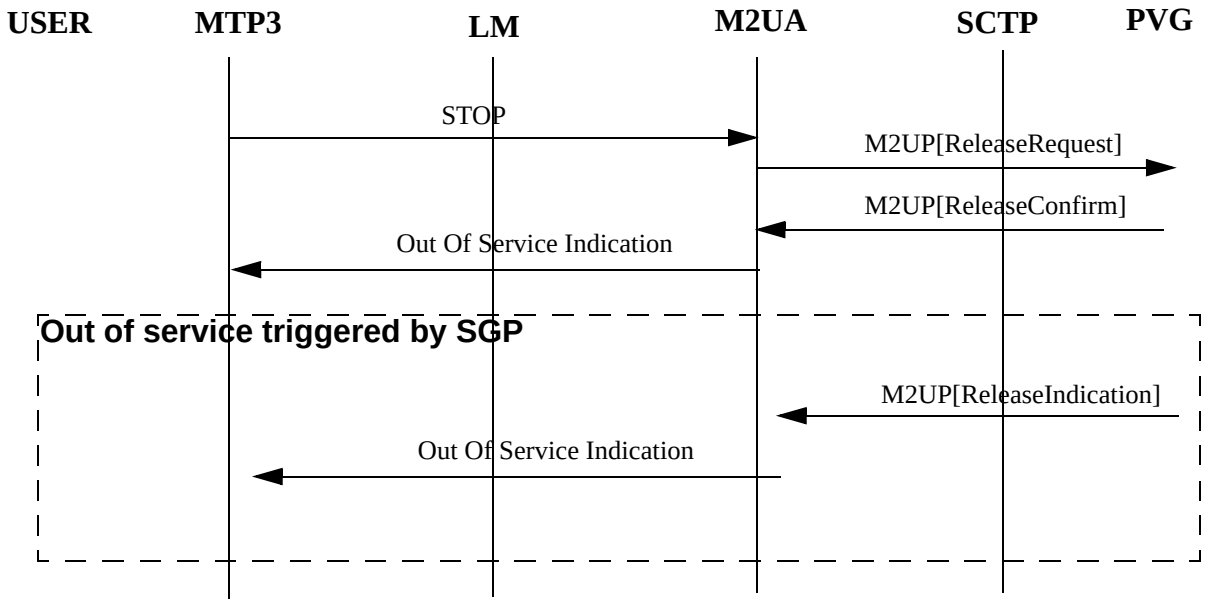
Figure 9: Emergency and Emergency Clearance



76.3.4.4 SS7 Link Deactivate

Refer to RFC3331 5.3.2

Figure 10: SS7 Link Deactivate

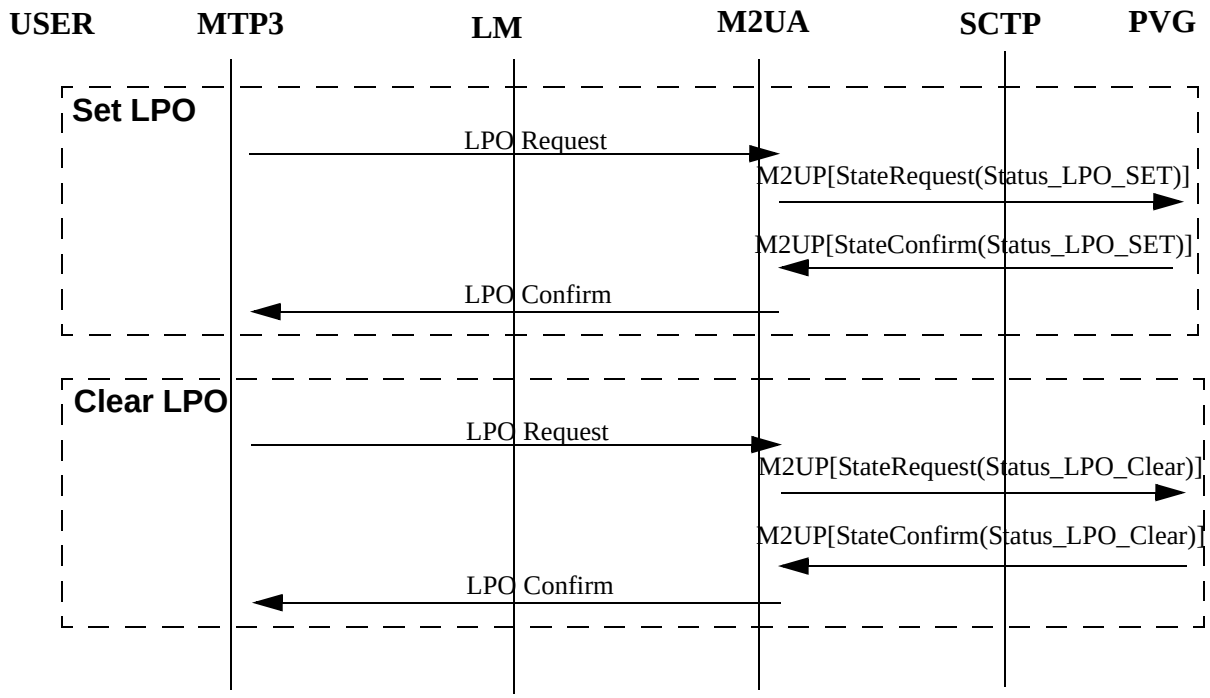


STOP is sent by L3 SLM (Signalling Link Management), if it thinks the l2 link is really needed to be stopped in some cases including some failure ones.

76.3.4.5 Set and Clear Local Processor Outrage

Refer to RFC3331 5.3.3

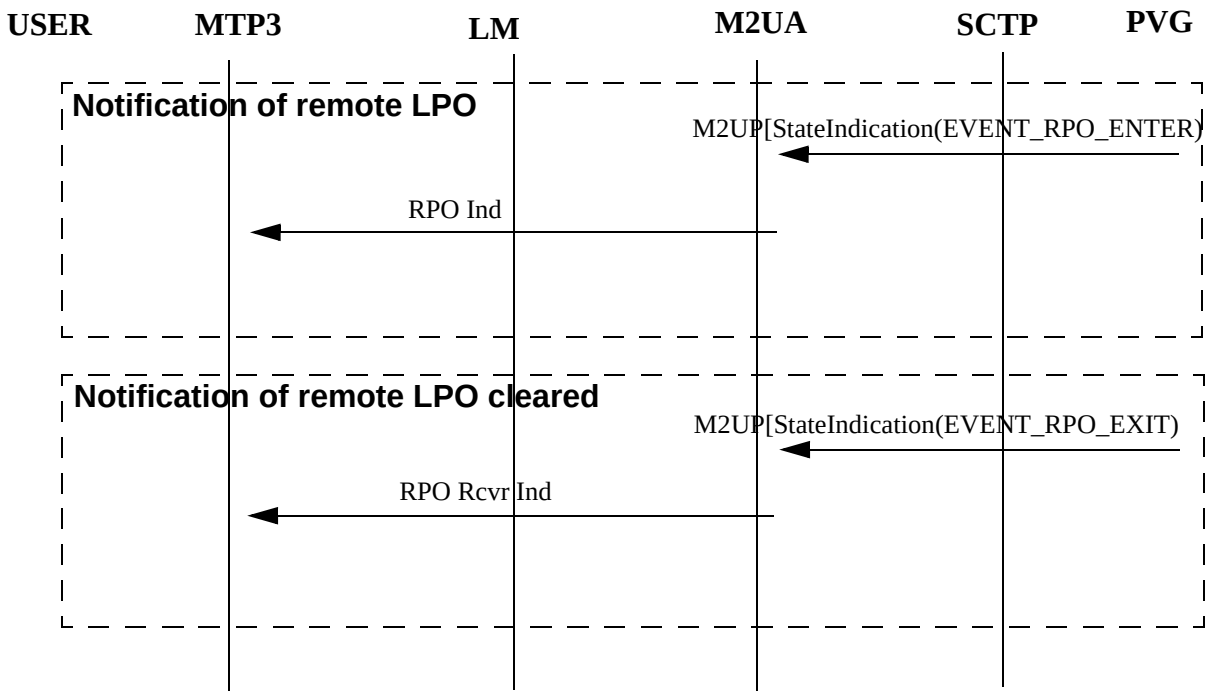
Figure 11: Set and Clear Local Processor Outrage



76.3.4.6 Remote processor outrage

Refer to RFC3331 5.3.4

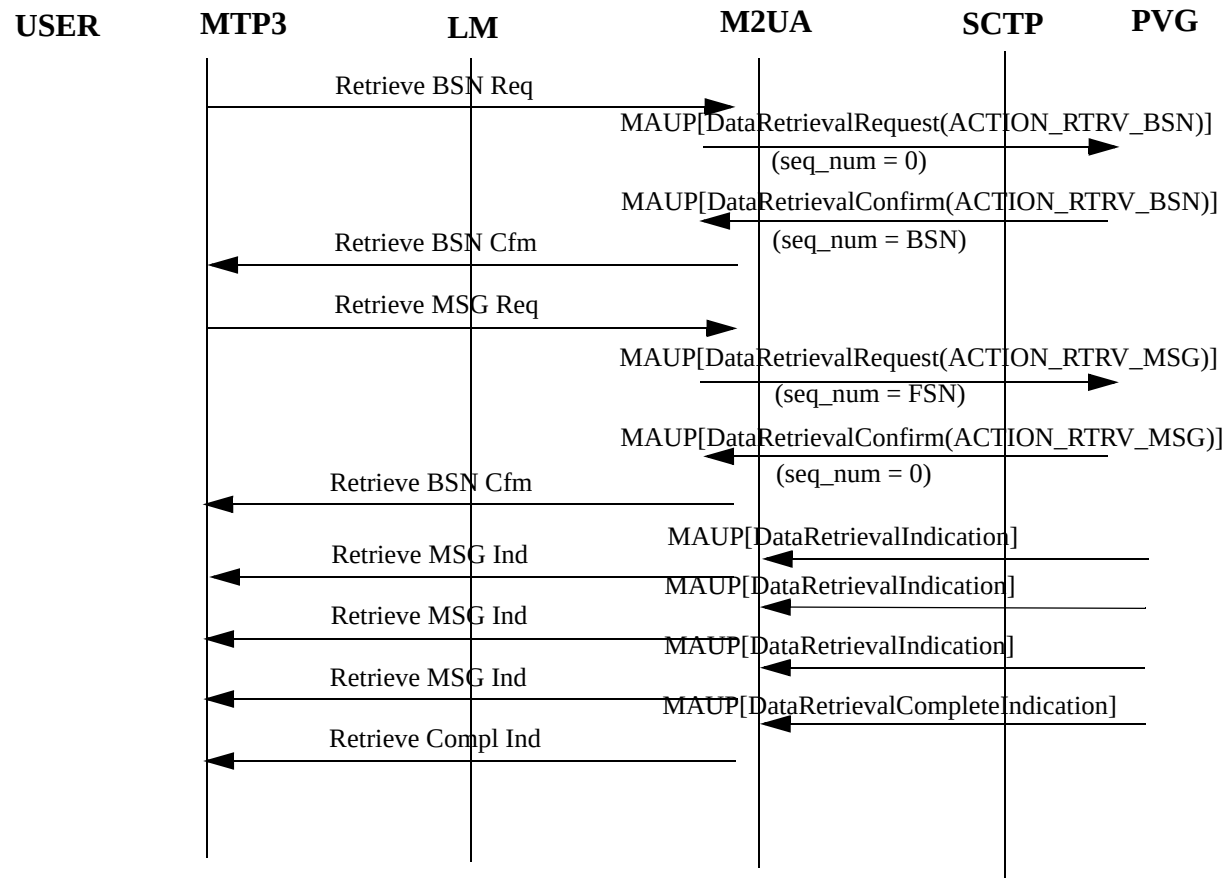
Figure 12: Remote Processor Outrage



76.3.4.7 SS7 Link Changeover

Refer to RFC3331 5.3.6.

Figure 13: SS7 Link Changeover

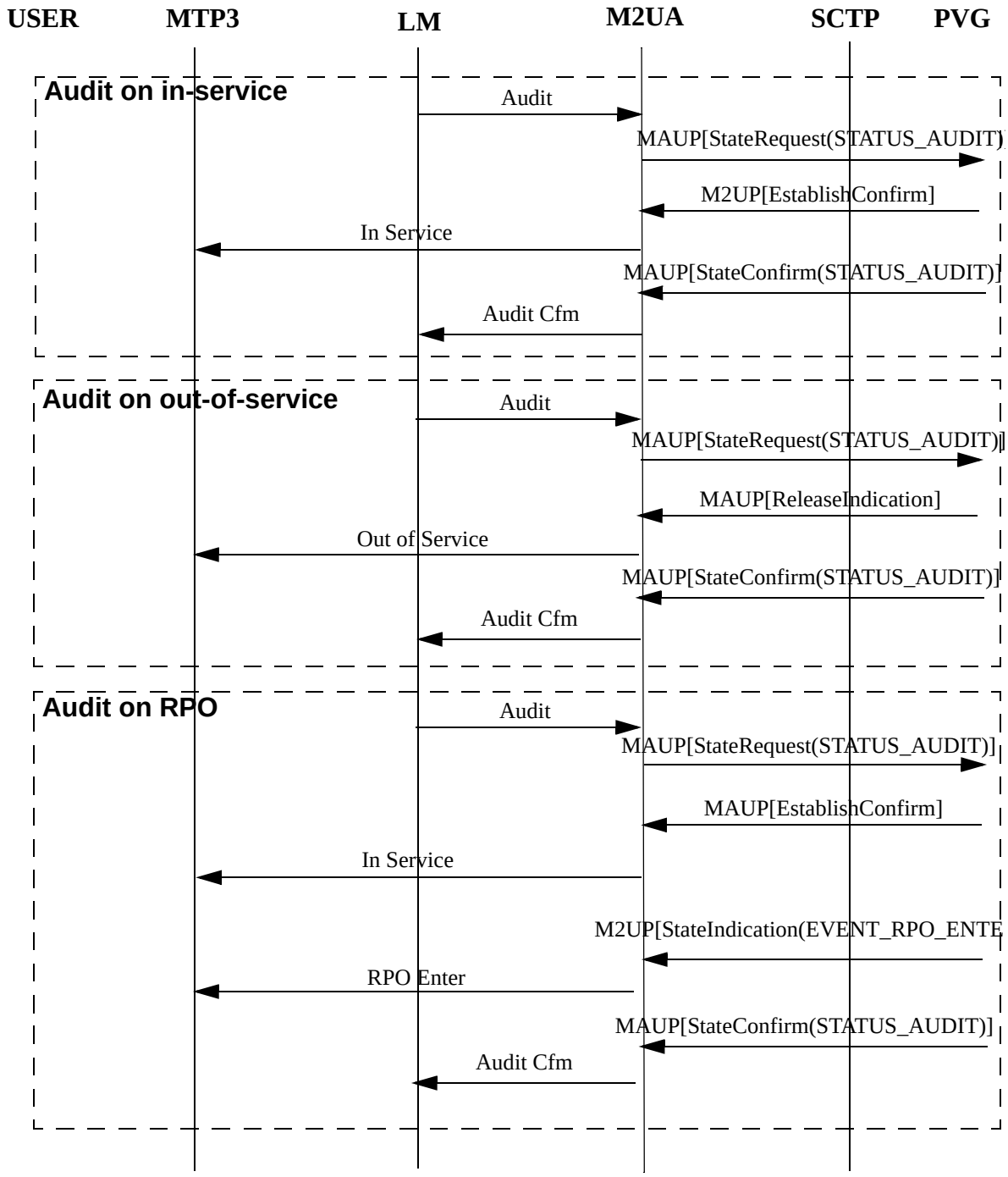


76.3.4.8 Auditing of SS7 link state

Refer to RFC3331 5.3.8

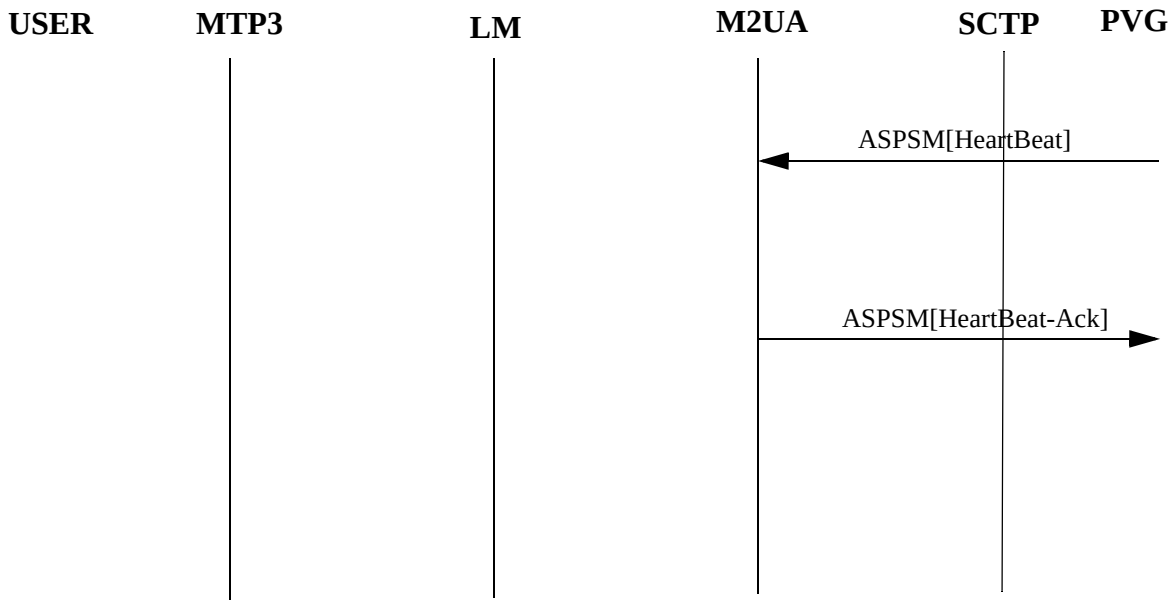
Audit on in-service, out-of-service and RPO are supported.

Figure 14: Auditing of SS7 link State



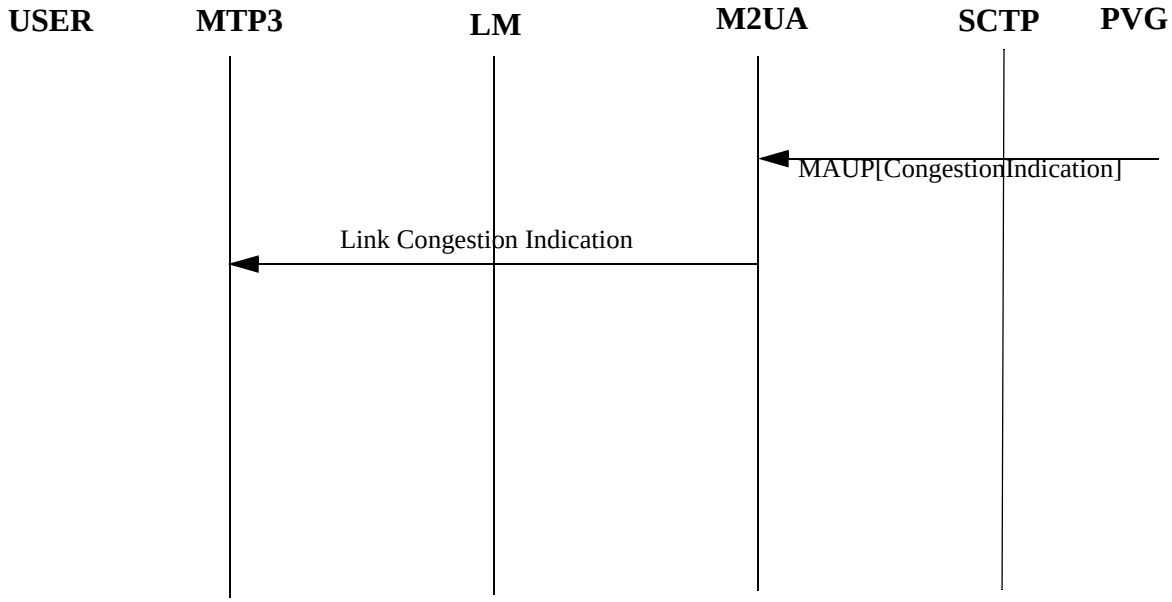
76.3.4.9 Heartbeat (and Ack)

Figure 15: BEAT and BEAT-ACK



76.3.4.10 Notification of SS7 link Congestion

Figure 16: Congestion Indication



76.3.5 Messages Contents

76.3.5.1 MAUP - Data (PDU of MTP3)

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x300)		Length (=8)	
Protocol Data			
Tag (0x13)		Length (=8)	
Correlation ID (optional)			

The purpose of Correlation ID is to permit the newly active ASP to synchronize its processing of the traffic in each ordered stream with other ASPs in the broadcast group. It’s optional and not supported by the feature.

TTC protocol data is not supported.

76.3.5.2 MAUP - Establish (Request, Confirm)

No specific parameters except for the Common Message Header.

76.3.5.3 MAUP - Release (Request, Confirm, Indication)

No specific parameters except for the Common Message Header.

76.3.5.4 MAUP - State (Request, Confirm)

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x302)		Length (=8)	
State			

State is Mandatory IE, the valid values for it are shown below.

Value	Define	Note
0x0	STATUS_LPO_SET	
0x1	STATUS_LPO_CLEAR	
0x2	STATUS_EMER_SET	
0x3	STATUS_EMER_CLEAR	
0x4	STATUS_FLUSH_BUFFERS	
0x5	STATUS_CONTINUE	
0x6	STATUS_CLEAR_RTB	

0x7	STATUS_AUDIT	
0x8	STATUS_CONG_CLEAR	
0x9	STATUS_CONG_ACCEPT	
0xa	STATUS_CONG_DISCARD	

76.3.5.5 MAUP - State Indication

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x302)		Length (=8)	
Event			

Event is Mandatory IE, the valid values for it are shown below.

Value	Define	Note
0x1	EVENT_RPO_ENTER	
0x2	EVENT_RPO_EXIT	
0x3	EVENT_LPO_ENTER	
0x4	EVENT_LPO_EXIT	

76.3.5.6 MAUP - Retrieval Request

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x306)		Length (=8)	
Action (Mandatory)			
Tag (0x307)		Length (=8)	
Sequence Number (Optional)			

The valid values for Action are shown below.

Value	Define	Note
0x1	ACTION_RTRV_BSN	
0x2	ACTION_RTRV_MSGS	

76.3.5.7 MAUP - Retrieval Confirm

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x306)		Length (=8)	
Action (Mandatory)			
Tag (0x308)		Length (=8)	
Result (Mandatory)			
Tag (0x307)		Length (=8)	
Sequence Number (Optional)			

The valid values for Result are shown below.

Value	Define	Note
0x1	RESULT_SUCCESS	
0x2	RESULT_FAILURE	

76.3.5.8 MAUP - Retrieve Indication

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x300)		Length (=8)	
Protocol Data			

The Retrieval Indication message is sent by the Signalling Gateway with a PDU from the transmit or retransmit queue. The Retrieval Indication message does not contain the Action or Sequence Number fields, just a MTP3 Protocol Data Unit (PDU) from the transmit or retransmit queue.

76.3.5.9 MAUP - Retrieve Complete Indication

The MTP2 Retrieval Complete Indication message is exactly the same as the MTP2 Retrieval Indication message except that it also indicates that retrieval is complete. In addition, it MAY contain a PDU (which MUST be the last PDU) from the transmit or retransmit queue.

76.3.5.10 MAUP - Congestion Indication

The Congestion Indication message can be sent from a Signalling Gateway Process to an ASP to indicate the congestion status and discard status of a SS7 link.

0	1	2	3

0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x304)		Length (=8)	
Congestion Status (Mandatory)			
Tag (0x308)		Length (=8)	
Discard Status (Optional)			

For the Congestion Status, there are the following values can be selected.

Value	Define	Note
0x0	LEVEL_NONE	
0x1	LEVEL_1	Not supported
0x2	LEVEL_2	Not supported
0x3	LEVEL_3	

76.3.5.11 ASPM - ASP UP

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x11)		Length (=8)	
ASP Idenfifier (optional)			
Tag (0x4)		Length (=8)	
Info String (optional)			

The optional ASP Identifier parameter would contain a unique value that is locally significant among the ASPs that support an AS. The SGP should save the ASP Identifier to be used, if necessary, with the Notify message.

76.3.5.12 ASPM - ASP UP Ack

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x4)		Length (=8)	
Info String (optional)			

76.3.5.13 ASPM - ASP Down

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x4)		Length (=8)	
Info String (optional)			

76.3.5.14 ASPM - ASP Down Ack

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x4)		Length (=8)	
Info String (optional)			

76.3.5.15 ASPM - ASP Active (Ack)

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0xb)		Length (=8)	
Traffic Mode Type (Optional)			
Tag (0x1, 0x8)		Length (=8)	
Interface Identifier(s) (Optional)			
Interface Identifier Start1			
Interface Identifier End1			
.....			
Interface Identifier StartN			
Interface Identifier EndN			
Tag (0x4)		Length (=8)	
Info String (Optional)			

76.3.5.16 ASPM - ASP Inactive (Ack)

The same format as ASP Active.

76.3.5.17 MGMT - ERR

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0xc)		Length (=8)	
Error Code (Mandatory)			
Tag (0x1,0x8)		Length (=8)	
Interface Identifier(s) (optional)			
Tag (0x7)		Length (=8)	
Diagnostic Information (optional)			

The Error (ERR) message is used to notify a peer of an error event associated with an incoming message. An Error message MUST not be generated in response to other Error messages.

The valid values for Error Code are shown below.

Value	Define	Note
0x1	Invalid Version	
0x2	Invalid Interface Identifier	
0x3	Unsupported Message Class	
0x4	Unsupported Message Type	
0x5	Unsupported Traffic Handling Mode	
0x6	Unexpected Message	
0x7	Protocol Error	
0x8	Unsupported Interface Identifier Type	
0x9	Invalid Stream Identifier	
0xa	Not Used in M2UA	
0xb	Not Used in M2UA	
0xc	Not Used in M2UA	
0xd	Refused - Management Blocking	
0xe	ASP Identifier Required	
0xf	Invalid ASP Identifier	
0x10	ASP Active for Interface Identifier(s)	

0x11	Invalid Parameter Value	
0x12	Parameter Field Error	
0x13	Unexpected Parameter	
0x14	Not Used in M2UA	
0x15	Not Used in M2UA	
0x16	Missing Parameter	

76.3.5.18 MGMT - NTFY

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0xd)		Length (=8)	
Status Type (Mandatory)		Status info (Mandatory)	
Tag (0x11)		Length (=8)	
ASP Identifier (Optional)			
Tag (0x1,0x8)		Length (=8)	
Interface Identifier(s) (optional)			
Tag (0x4)		Length (=8)	
Info String (optional)			

The Error (ERR) message is used to notify a peer of an error event associated with an incoming message. An Error message MUST not be generated in response to other Error messages.

The valid values for Error Code are shown below.

Value	Define	Note
0x1	Invalid Version	
0x2	Invalid Interface Identifier	
0x3	Unsupported Message Class	
0x4	Unsupported Message Type	
0x5	Unsupported Traffic Handling Mode	
0x6	Unexpected Message	
0x7	Protocol Error	
0x8	Unsupported Interface Identifier Type	

0x9	Invalid Stream Identifier	
0xa	Not Used in M2UA	
0xb	Not Used in M2UA	
0xc	Not Used in M2UA	
0xd	Refused - Management Blocking	
0xe	ASP Identifier Required	
0xf	Invalid ASP Identifier	
0x10	ASP Active for Interface Identifier(s)	
0x11	Invalid Parameter Value	
0x12	Parameter Field Error	
0x13	Unexpected Parameter	
0x14	Not Used in M2UA	
0x15	Not Used in M2UA	
0x16	Missing Parameter	

76.4 LOG

Log group M2UA_GROUP is defined for the M2UA.

Log Name	Type	Description
M2UA_SWEER	LOG_SWEER	generated when software error are detected in M2UA
M2UA_INFO	LOG_INFO	generated when an important event happened in M2UA that needs to be shown to the user

76.5 OM

N/A

76.6 Provisioning

76.6.1 Provisioning - CLI interface

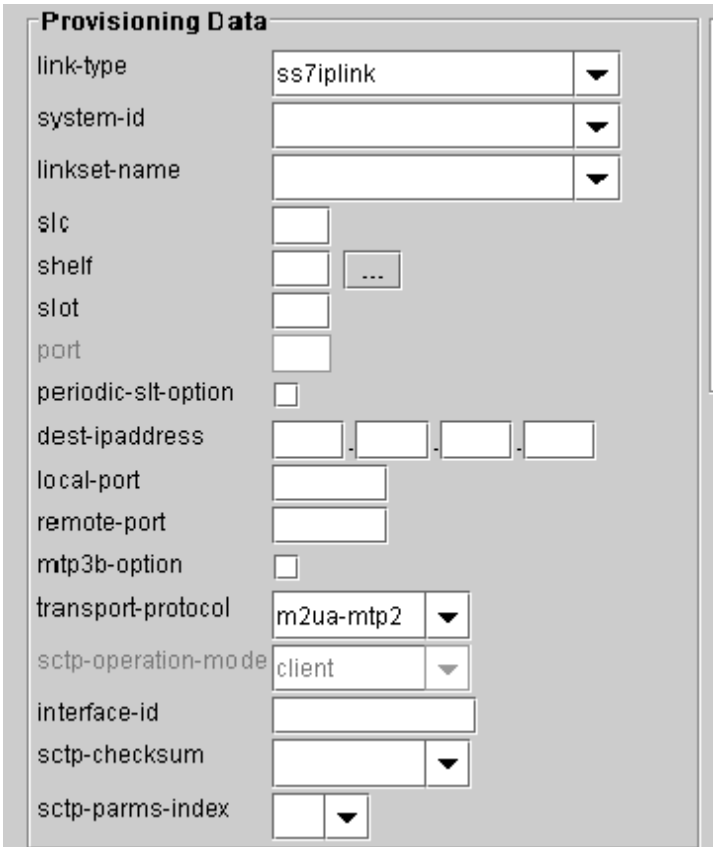
CMD: mtp link add <linkset-name> <slc> ss7iplink <shelf> <slot> <periodic-slt-option> <dest-ipaddr> <local-port> <remote-port> { m2ua client <sctp-checksum> <sctp-parm-index> | m2ua <interface-id> <sctp-checksum> <sctp-parm-index> }

CMD: mtp link mod <linkset-name> <slc> ss7iplink interface-id <interface-id>

CMD: mtp link mod <linkset-name> <slc> ss7iplink transport-protocol { m2ua client <sctp-checksum> | m2ua <interface-id> <sctp-checksum> }

CMD: mtp link show <linkset-name> <slc>

76.6.2 GUI



Some fileds are needed to be noticed when protocol M2UA is selected.

Field Name	Value	Description
transport-protocol	m2ua-mtp2/ m2ua-saal	select different value depending on the far-end l2 type in the PVG/MGC
local-port	2904	2904 is dedicated for M2UA
remote-port	2904	2904 is dedicated for M2UA

76.7 Hardware Requirements or Dependencies

N/A

76.8 Software Requirements or Dependencies

N/A

76.9 Limitations and restrictions

1. USP can only be configured as SCTP Client

2. The M2UA layer supports a n+k redundancy model(active-standby, load sharing, broadcast) where n is the minimum number of redundant ASPs required to handle traffic and k ASPs are available to take over for a failed or unavailable ASP. A simplex 1+0 model is also supported as a subset, with no ASP redundancy is supported by the feature. (ASP identifier <-> number of ASP, link(set) <-> ASP), (send it PVG team)

3. Registration procedure is not supported by the feature.

76.10 Interactions

N/A

76.11 Glossary

Term	Description
AS	A logical entity serving a specific application instance
ASP	A process instance of an Application Server
ASPSM	ASP State Maintenance
ASPTM	ASP Traffic Maintenance
M3UA	Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) -User Adaptation Layer
SCTP	Stream Control Transmission Protocol
SCTP	Stream Control Transmission Protocol
SG	Signaling Gateway

76.12 Reference

1. RFC3331 Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Adaptation Layer

77: Functional description (FN): A00009463

77.1 Feature name and Feature ID

Core and Billing Manager (CBM) to support the Centralized user Authentication, Authorization, and Administration, with Integrated Element Management System (IEMS) - A00009463.

77.2 Description

This feature provides the CBM capability to support Centralized Authentication, Authorization, Administration (AAA) with the Integrated Element Management System (IEMS). This feature activates PAM, RADIUS, PAM-MKHOMEDIR, NSS-SAML and SAML modules to enable integration of CBM with the IEMS and SAML, in order to allow the use of Centralized AAA.

This feature is the equivalent of the SN08 A00007489 which provided similar capability on the SDM product, with the exception of the following points:

- There is neither the support nor the introduction of any new user group on the CBM as part of this feature (not included in SN09 features).
- There is no new security or audit log generated by this feature.
- In addition to the SSH, there are other applications (e.g. login, su, etc.) that are supported on the CBM. The ProFTP and SFT (for CM->CBM Secure FTP) are however not supported.

Note: The details of the above-mentioned equivalent SDM feature is found in PLS fmdoc library under A00007489.aa14 design documents.

With respect to AAA functionality, there are two possible configurations supported by the CBM, which are described in this document, and captured in the following figures:

Figure 1 CBM with central security server configuration & components

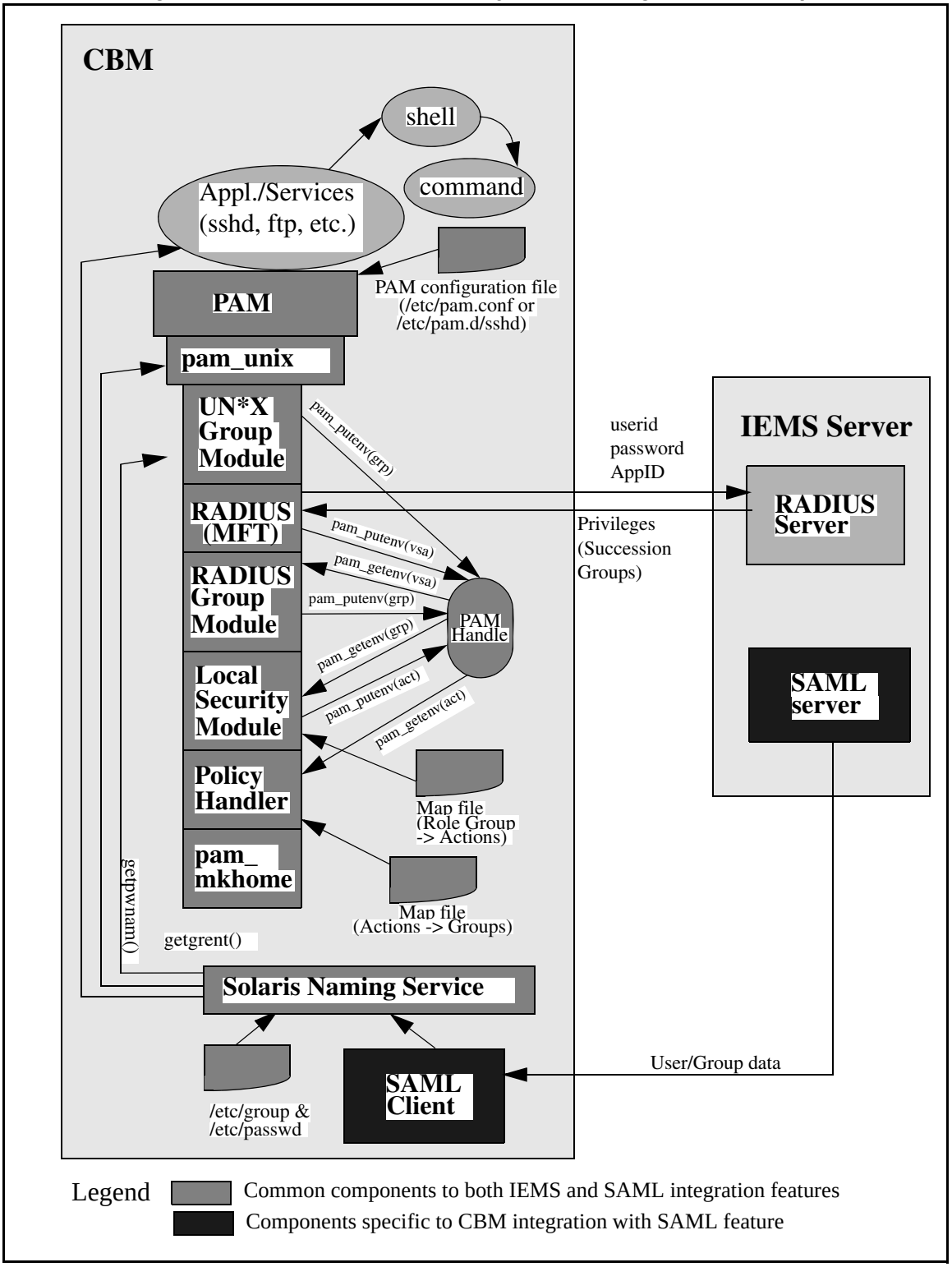
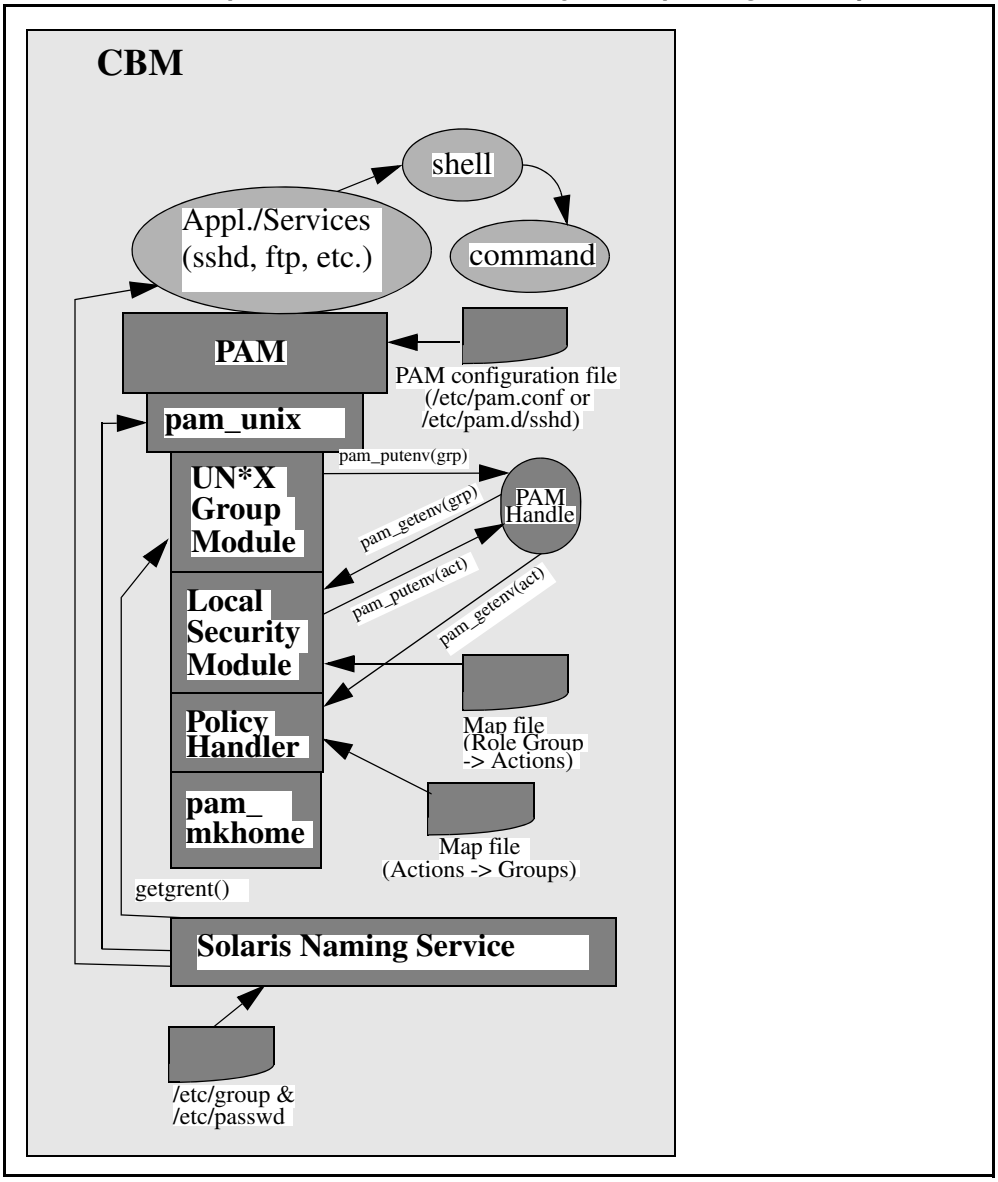
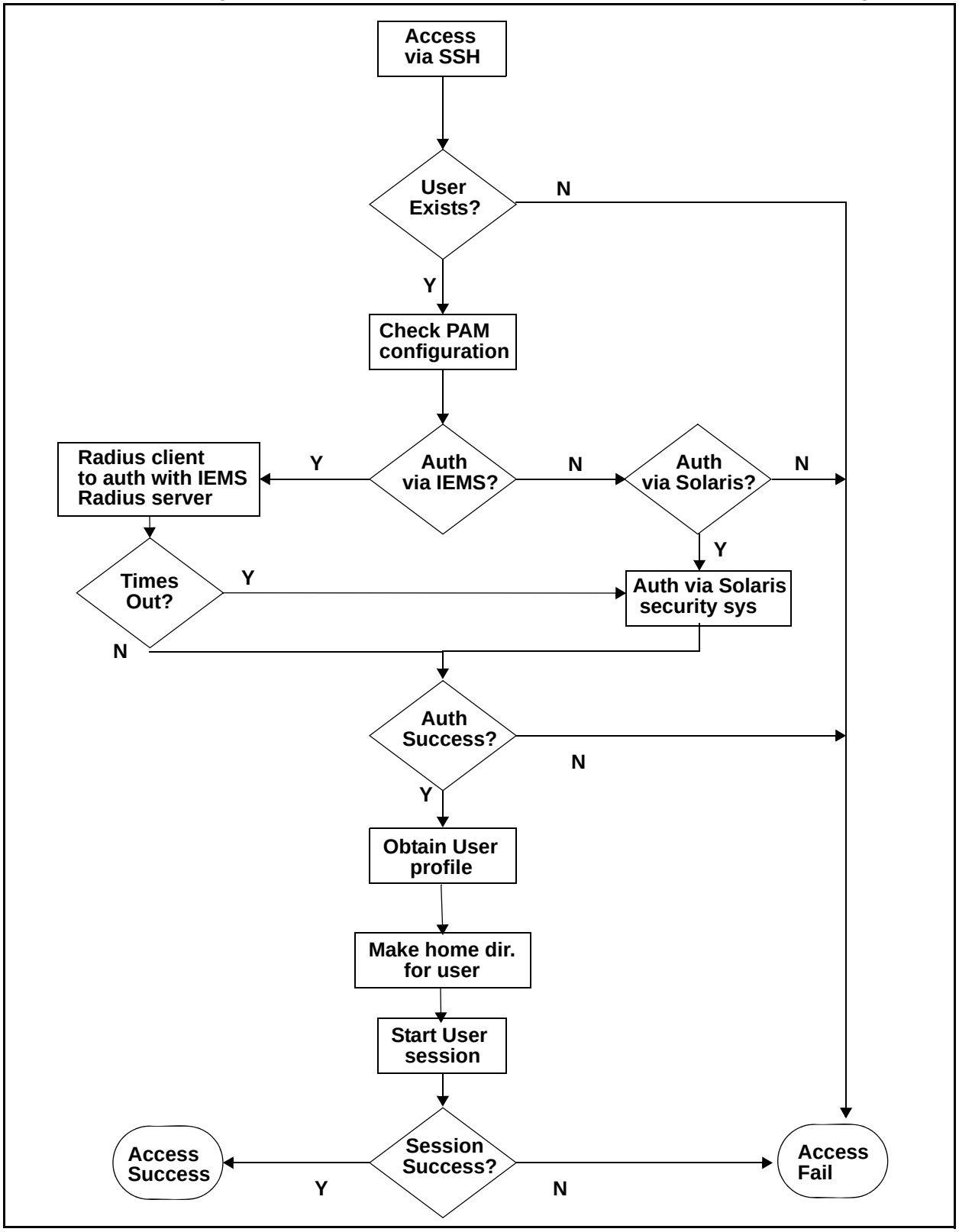


Figure 2 CBM Standalone (i.e. without central security server) config. & components



The following is a flow chart for user authentication and authorization through SSH.

Figure 3 Flow chart for user authentication and authorization through SSH



77.3 Hardware Requirements or Dependencies

No new hardware dependency is introduced in this feature for the Standalone CBM deployment (i.e. without centralized security server). For the CBM deployment with IEMS centralized security server, the IEMS and its hardware dependencies are required by this feature.

77.4 Software Requirements or Dependencies

The PAM, RADIUS and SAML software are required on the CBM. Also, for the CBM deployment with IEMS centralized security server, IEMS and its software dependencies are needed by this feature.

77.5 Limitations and restrictions

TBD

77.6 Interactions

Changes to Network Connectivity Applications

The following table shows the impact of this feature to network connectivity applications.

Table 1 Network Connectivity Applications

Application	Current Release	SN09	Configurable - i.e. Turn On/Off (Y/N)	Support IEMS central security server (Y/N)
SSH (with password)	Enable	Enable	N	Y
SFTP (with password)	Enable	Enable	N	Y
SSH (with key)	Enable	Enable	N	N
SFTP (with key)	Enable	Enable	N	N
Telnet	Enable	Enable	N	Y
FTP	Enable	Enable	N	Y
Console access	Enable	Enable	N	Y
su	Enable	Enable	N	Y
ProFTP	Disable	Disable	N	N
SFT (FTP Proxy)	Enable	Enable	N	N

Note: It is recommended that Telnet and FTP applications should not be used since SSH and SFTP are more secure tools.

When an application/service is not integrated to work with a central security server, the service can only permit access to users who have accounts locally on the CBM.

77.7 Glossary

Term	Description
AAA	Authentication, Authorization, Accounting
CBM	Core and Billing Manager
CUA	Centralized User Administration
IEMS	Integrated Element Manager System
PAM	Pluggable Authentication Module
SAML	Security Assertion Markup Language
SDM	SuperNode Data Manager
VSA	Vendor Specific Attributes

78: Functional description (FN): A00009470

78.1 Feature name and Feature ID

SuperNode Data Manager (SDM) to support Security Assertion Markup Language (SAML) NSSwitch client - A00009470.

78.2 Description

This feature will add SAML NSSwitch client function on SDM to integrate with centralized IEMS's (SS 1.1) SAML server.

This SN09 feature is to enhance the existing SDM security functionality which were developed in SN08. It will improve SDM centralized AAA function through IEMS by removing the need to update user accounts on SDMs whenever an SDM user is added/deleted/modified on IEMS.

> ***Note:*** Please refer to SN08 IEMS Integration feature document in PLS FMDOC (a00007489) for detail information on SN08 functionality.

In SN08, SDM only provides access to the user attributes (identification) information in local /etc files. It does not support other naming/identification information sources for the user attributes. As a result, when an SDM user account is created on IEMS, the user account also needs to be added on each SDM via an SDM script (enableIEMSUser). When an SDM user account is deleted on IEMS, the user account also needs to be removed on each SDM via an SDM script (disableIEMSUser).

This SN09 feature will address this limitation by providing SAML (Security Assertion Markup Language) client on SDM for user information retrieval. This will allow IEMS centralized security server to be one of the naming/identification information sources for the user attributes. There will be no need to maintain the local /etc files with enableIEMSUser and disableIEMSUser scripts whenever an SDM user is /added/modified/deleted on an IEMS server.

78.3 Hardware Requirements or Dependencies

No new hardware dependency is introduced in this feature for Standalone SDM deployment without centralized security server.

For SDM deployment with IEMS centralized security server, IEMS and its hardware dependencies are needed by this feature.

78.4 Software Requirements or Dependencies

For SDM deployment with IEMS centralized security server, IEMS and its software dependencies are needed by this feature.

This feature has included the following dependency software for SAML client:

- curl
- log4cpp
- Xerces-c
- xml_security_c
- OpenSAML

Please refer to 1.11 “License” in DID section for detail on third party software and their copyright notices.

78.5 Limitations and restrictions

- Authentication: This feature doesn’t change the existing authentication method for IEMS users. The users on the IEMS server will remain being authenticated by SDM through PAM, which in turn uses RADIUS protocol to authenticate IEMS users.
- SDMMTC User level can only be used to change user/group attributes when an SDM is configured to use local security server. When IEMS central security server is configured for the SDM, IEMS Security Administration GUI must be used to update the user/group information.
- Password update: This feature doesn’t provide IEMS users to change password from an SDM. The IEMS Security Administration GUI is still the tool for this purpose.
- Account and password status: An IEMS user will not get expiration warning when she/he logs into SDM. However, since the authentication is done through RADIUS, an IEMS user with an expired account and/or password will not be allowed to log into SDM because the RADIUS server will fail the login attempt.

78.6 Interactions

No new interaction is introduced by this feature,

78.7 Glossary

Term	Description
AAA	Authentication, Authorization, Accounting
CBM	Core and Billing Manager
IEMS	Integrated Element Manager System
LAM	Loadable Authentication Module
LDAP	Light-weight Directory Access Protocol
MFT	Management Framework Technology

Term	Description
NE	Network Element
OSS	Operations Support System
PAM	Pluggable Authentication Module
SAML	Security Assertion Markup Language
SDM	SuperNode Data Manager
SSL	Secure Sockets Layer
SSO	Single Sign-On
VSA	Vendor Specific Attributes

79: Functional description (FN): A00009508

79.1 Feature name and Feature ID

A00009508: Automatic Message Accounting Session Initiation Protocol (SIP) Line Identification

79.2 Description

Feature A00009508 introduces the new AMA billing Module 260 which captures originating and terminating agent component and protocol information for packet network agents. Module 260 contains two fields: Table 620 captures the connection side and component type. Table 622 captures the protocol type used. Module 620 is outlined below with current table values:

Module Code 260 - IP/Packet Party Identification (Vendor Specific)

Module Code	88	2	0
Component Type	620	4	1
IP Service Protocol	622	4	3
		Total	5

Table 620, Component Role (NDGR)
Chars Meaning
1: Connection Side (default = 0)
1 = Originating
2 = Terminating
2-3: Component Type
01 = Customer Premise Equipment
02 = Network Edge Component
03 = Gateway System
99 = Unspecified
4: SIGN (hex-C)

Table 622 - IP Service Protocol (Vendor Specific)
Chars Meaning
1: Reserved (default = 0)
2-3: Protocol Type
00 = unspecified
01 = SIP
02 = SIP-T
03 = SIP-I
04 = H.323 v1
05 = H323.v2
06 = H.248/MEGACO
07 = MGCP
4: SIGN (hex-C)

Feature A00009508 provides the framework to capture all variants; however, only the capturing of SIP lines client information is provided by this feature. This feature complements the OAM&P core development done under A00008556 by providing identification of SIP lines for billable calls. The following are sample records illustrating SIP line party information capture:

```
*HEX ID:AA  STRUCTURE CODE:40625C  CALL CODE:110C  SENSOR TYPE:036C
SENSOR ID:0619351C  REC OFFICE TYPE:036C  REC OFFICE ID:0619351C
DATE:50314C  TIMING IND:00000C  STUDY IND:0200000C  CLD PTY OFF-HK:1C
SERVICE OBSERVED:0C  OPER ACTION:0C  SERVICE FEATURE:000C  ORIG NPA:613C
ORIG NUMBER:6215671C  OVERSEAS IND:0C  TERM NPA:00519C
TERM NUMBER:8885672C  CONNECT TIME:1103004C  ELAPSED TIME:000000000C
IC/INC PREFIX:02221C  CC DATE:50314C  CC TIME:1102217C
ELAPSED CC:000000387C  IC/INC EVENT STATUS:007C  TRUNK GROUP NUMBER:30638C
ROUTING INDICATOR:0C  DIALING INDICATOR:1C  ANI INDICATOR:1C
MODULE CODE:306C  OLIP:031C  MODULE CODE:260C  COMPONENT ROLE:101C
IP SERVICE PROTOCOL:001C  MODULE CODE:000C

*HEX ID:AA  STRUCTURE CODE:40625C  CALL CODE:119C  SENSOR TYPE:036C
SENSOR ID:0619351C  REC OFFICE TYPE:036C  REC OFFICE ID:0619351C
DATE:50314C  TIMING IND:00000C  STUDY IND:0200000C  CLD PTY OFF-HK:1C
SERVICE OBSERVED:0C  OPER ACTION:0C  SERVICE FEATURE:000C  ORIG NPA:613C
ORIG NUMBER:6215671C  OVERSEAS IND:0C  TERM NPA:00519C
TERM NUMBER:8885672C  CONNECT TIME:1103009C  ELAPSED TIME:000000000C
IC/INC PREFIX:02221C  CC DATE:50314C  CC TIME:1102218C
ELAPSED CC:000000390C  IC/INC EVENT STATUS:001C  TRUNK GROUP NUMBER:30638C
ROUTING INDICATOR:0C  DIALING INDICATOR:FF  ANI INDICATOR:1C
MODULE CODE:306C  OLIP:031C  MODULE CODE:260C  COMPONENT ROLE:201C
IP SERVICE PROTOCOL:001C  MODULE CODE:260C  COMPONENT ROLE:201C
IP SERVICE PROTOCOL:001C  MODULE CODE:000C
```

For the above examples, the Call Code 110 originating Equal Access AMA record contains a Module 260 which shows that a SIP client at the customer's premise originated the call. Component Role value of 101 can be broken into (1) originating and (01) customer premise equipment. IP Service Protocol shows SIP (01) being used. The Call Code 119 terminating Equal Access AMA record contains a Module 260 that shows the call terminated to a SIP client. Component Role value 201 can be broken into (2) terminating and (01) customer premise equipment.

Feature A00009508 uses a new tuple in table AMAOPTS to activate and deactivate Module 260 inclusion. The new OPTION is called RECORD_MC260, and the SCHEDULE will be either ON or OFF. The default setting is OFF. The new option activates recording of packet client involvement for both originating and terminating agents. This option does not force billing; it collects the additional information for existing billable scenarios.

The following CI session shows how feature functionality is activated. Deactivation is achieved by setting schedule back to OFF.

```
>table amaopts
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: AMAOPTS
>pos RECORD_MC260
        RECORD_MC260                    OFF
>lis
           OPTION                   SCHEDULE
-----------------------------------------------------------
        RECORD_MC260                    OFF
>cha
```

```
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
AMASEL: OFF
>on
TUPLE TO BE CHANGED:
        RECORD_MC260                    ON
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE CHANGED
JOURNAL FILE INACTIVE
```

On the SDM/CBM Side:

This feature A00009508 introduces the new AMA Module Code 260 with two new fileds COMPONENT ROLE and IP SERVICE PROTOCOL to the BAF database on SDM/CBM.

The new Module 260 with the two new fileds and its definitions are added to baf.db file (BAF database) to be supported by AMADUMP tool on SDM/ CBM.

Definition of the two new fields added in baf.db are:

```
COMPONENT_ROLE 16 4 bcd 0 COMPONENT_ROLE
COMPONENT ROLE

IP_SERVICE_PROTOCOL 16 4 bcd  1 IP_SERVICE_PROTOCOL
IP SERVICE PROTOCOL
```

And the following is the complete module code defined in baf.db:

```
[Subrecord]
260
MODULE_CODE_ID
COMPONENT_ROLE
IP_SERVICE_PROTOCOL
[^]
```

This functionality could be verified using AMADUMP tool by executing the following steps:

Login to SDM or CBM as root user or maint user

Execute the listfile command for AMA stream to get the filename(s)

billmtc; filesys; listfile ama

Execute amadump command to display the billing file with module code 260

billmtc; tools; amadump ama

AMADUMP>> dump details sum fname <file- name>

Where <file-name> is from the output of listfile command.

The following is the AMADUMP output of a billing file with Module Code 260 on SDM/CBM:

```
Record data:
------------
                          RDW 00610000
                        HEX_ID aa
                   STRUCTURE_CODE 40625C
                      CALL_CODE 110C
                    SENSOR_TYPE 036C
                     SENSOR_ID 0000000C
                RECORD_OFFICE_TYPE 036C
                 RECORD_OFFICE_ID 0000000C
                        DATE 50418C
                 TIMING_INDICATOR 00000C
                  STUDY_INDICATOR 0001000C
                       ANSWER 0C
                 SERVICE_OBSERVED 0C
                  OPERATOR_ACTION 0C
                  SERVICE_FEATURE 000C
                  ORIGINATING_NPA 919C
                ORIGINATING_NUMBER 8472452C
                OVERSEAS_INDICATOR 0C
                  TERMINATING_NPA 00800C
                TERMINATING_NUMBER 9917782C
                    CONNECT_TIME 0902091C
                    ELAPSED_TIME 000098182C
                   IC_INC_PREFIX 00001C
              CARRIER_CONNECT_DATE 50418C
              CARRIER_CONNECT_TIME 0902091C
                 ELAPSED_FROM_CC 000000000C
               IC_INC_EVENT_STATUS 010C
                TRUNK_GROUP_NUMBER 00584C
                 ROUTING_INDICATOR 0C
                 DIALING_INDICATOR 8C
                    ANI_INDICATOR 1C

Subrecord data:
---------------
                  MODULE_CODE_ID 042C
        CALL_RECORD_SEQUENCE_NUMBER 0003851C

Subrecord data:
---------------
                  MODULE_CODE_ID 260C
                  COMPONENT_ROLE 199C
               IP_SERVICE_PROTOCOL 000C
Subrecord data:
---------------
                  MODULE_CODE_ID 000C
```

79.3 Hardware Requirements or Dependencies

There are no hardware dependencies for this feature.

79.4 Software Requirements or Dependencies

Since feature A00009508 changes AMA, display and downstream utilities need to be adjusted to handle the new information now present. This feature addresses all core required changes and SDM required changes to support this new module code; however, all downstream processing programs need to be updated as well.

79.5 Limitations and restrictions

There are no restrictions.

79.6 Interactions

Feature A00008556 introduces the DPL LGRP type and DPL line option. DPL is used to denote SIP lines' components in the core. This designation is also used by this feature in determining if an agent is a SIP line.

79.7 Glossary

Term	Description
AMA	Automatic Message Accounting
DPL	Dynamic Packet Line
EA	Equal Access
LGRP	Logical Group: Used to group Succession agents
SDM	Supernode Data Manager
SIP	Session Initiation Protocol
RECORD_MC260	New AMAOPTs OPTION which controls A00009508 functionality.
AMADUMP	AMADUMP is a tool, which displays the billing records from AMADNS or DIRP billing files stored on SDM.

80: Functional description (FN): A00009513

80.1 Feature name and Feature ID

A00009513 PMA for SIP Lines

80.2 Description

The PMA for SIP Lines feature extends support for the existing Packet Media Anchor (PMA) for Dynamic Packet Trunks (DPTs) to SIP Lines. SIP Lines use the PMA to access CS2k based features that require the collection of additional digits. These features include:

North America

- Call Forward Programming
- Call Screening Override
- AIN collect info
- Speed Dial Programming
- Subscriber Activated Call Blocking
- Direct Inward System Access
- Call Forward Remote Activation

International

- IBN Call Forward Programming
- Call Screening Override
- Speed Dial Programming
- Subscriber Activated Call Blocking
- Last Number Redial
- Anonymous Call Rejection
- IBN CFU/CFB/CFD intragroup / intergroup screening
- IBN Do Not Disturb

The PMA will be removed from the bearer path of SIP lines once it is no longer required by the feature which inserted it.

80.3 Hardware Requirements or Dependencies

This feature adds no new hardware dependencies to the system. The feature does have all the dependencies of the features it builds on. Please reference the feature documentation for A00007120 PMA dependencies and reference A00008234 for SIP Lines dependencies.

80.4 Software Requirements or Dependencies

This feature adds no new software dependencies to the system. The feature does have all the dependencies of the features it builds on. Please reference the feature documentation for A00007120 PMA dependencies and reference A00008234 for SIP Lines dependencies.

80.5 Limitations and restrictions

This feature adds no new limitations or restrictions to the system. The feature does have all the limitations and restrictions of the features it builds on. Please reference the feature documentation for A00007120 PMA dependencies and reference A00008234 for SIP Lines dependencies.

80.6 Interactions

The PMA for SIP Lines feature uses the existing Media Anchor (MA) pools to access the MA resources on the CS2k system. Since a connection through the MA can only be used by one SIP Line or DPT at a time the PktMA resource pool must be sized to support both functions in the system.

80.7 Glossary

Term	Description
DPT	Dynamic Packet Trunk
MA	Media Anchor
PktMA	Packet Media Anchor
PMA	Packet Media Anchor

81: Functional Description (FN): A00009514

81.1 Feature name and Feature ID

CS2K-MCS Interop for SN09

Feature ID: A00009514

81.2 Description

SIP on Succession Communication Server was first introduced in SN03 to enable Communication Server - Communication Server and Communication Server -MCS5200 communication. At the time of implementation, the IETF SIP/SIP-T standards were still at pre-RFC stage. Nortel being the pioneer has moved forward with its implementation and has gained vast experience in SIP-T interop in the past few years. In the meantime the IETF specifications have evolved and matured. Communication Server initial implementation was based on the GWC/VRDN architecture which has imposed few limitations on the overall application. In SN07, with the introduction of the Session Server, the SIP-T/SIP implementation on the Succession Communication Server has been revamped and evolved to an IETF compliant open interface. The Session Server is a high capacity carrier grade new platform consisting of hardware based on SAM-XTS and software consisting of base and share layers. The application introduced on this platform in SN07 was the SIP Gateway allowing interop between the Communication Server and 3rd party Call Servers and Application Servers. The Session Server enhances the capability of the Succession Communication Server which is critical in Nortel's strategic market positioning in VoIP solutions.

This feature provides support for SN09 NGSS interworking with MCS release 09 (a.k.a. MCS 4.1) and will also provide support for the backward compatibilty with MCS 3.0. SN09 NGSS interworking with MCS 4.0 will not be supported. This feature will address upgrade scenarios, new content integration, and regression testing. One of the new pieces of functionality is the support for private/public name delivery for Converged Desktop users, which includes the support for SIP phone-context tag fields.

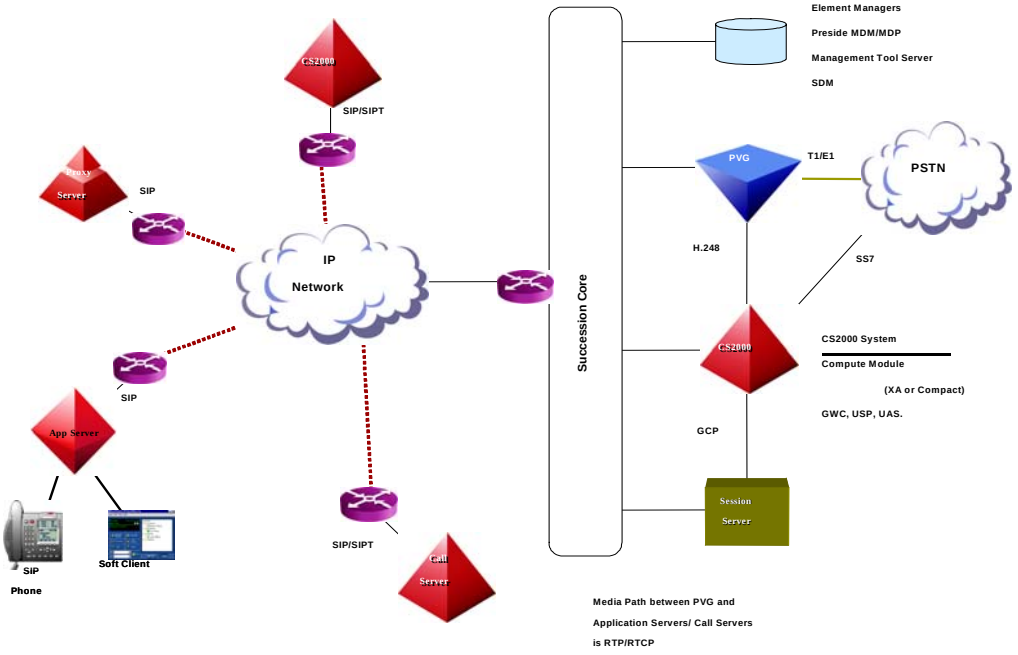


Figure-1 CS2K Network Configuration

81.2.1 Upgrade

The following table shows support for the interworking configuration of the CS2K and MCS releases.

Table 1: CS2K and MCS Releases Support

MCS	MCS 3.0	MCS 4.0	MCS 4.1
(I)SN07	Supported	Not Supported	Not Supported
(I)SN08	Supported	Supported	Supported
(I)SN09	**Supported ***	**Not Supported**	**Supported**

* Still under consideration

After any upgrade either on the CS2K side or on the MCS side the upgraded configuration must comply to the supported configuration. The following shows the CS2K configuration with the MCS.

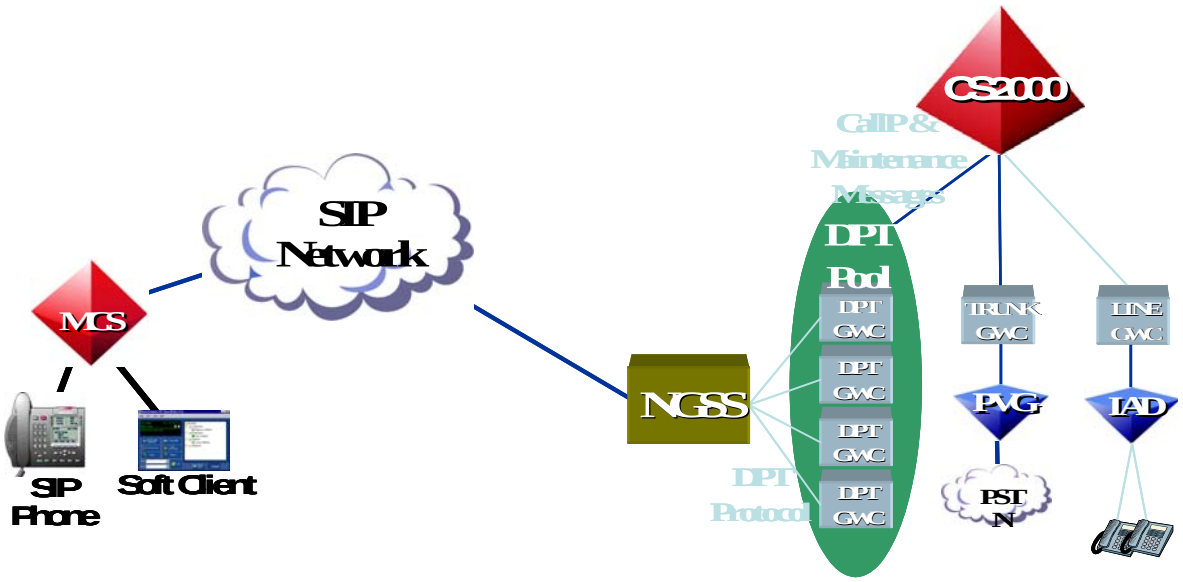


Figure-2 NGSS - MCS Interworking Configuration

The following walks through the different configuration scenarios and procedure which should be followed to upgrade the NGSS to the SN09 release.

81.2.1.1 SN07 or SN08 CS2K with VRDN Interworking with MCS 3.0

In this configuration the VRDN must be first migrated to the NGSS architecture prior to the CS2K upgrade. After the VRDN to NGSS migration CS2K components including NGSS should then upgraded to the SN09 software release. Depending on the customer requirement the MCS can either be left at MCS 3.0 or could be upgraded to MCS 4.1. MCS should not be, however, upgraded to MCS 4.0.

81.2.1.2 SN07 or SN08 CS2K with NGSS Interworking with MCS 3.0

In this configuration the CS2K components including NGSS could be directly upgraded to SN09 software release. Depending on the customer requirement the MCS can either be left at MCS 3.0 or could be upgraded to MCS 4.1. MCS should not be, however, upgraded to MCS 4.0.

81.2.1.3 SN07 CS2K with either VRDN or NGSS Interworking with MCS 4.0 or MCS 4.1 - This configuration is not supported

81.2.1.4 SN08 CS2K with VRDN Interworking with MCS 4.0

In this configuration the MCS must be first upgraded from MCS 4.0 to MCS 4.1 and the VRDN must be migrated to the NGSS architecture prior to the CS2K upgrade. When the MCS upgrade and the migration from the VRDN to NGSS has been completed then the CS2K components including NGSS could be upgraded to SN09 software release.

81.2.1.5 SN08 CS2K with NGSS Interworking with MCS 4.0

In this configuration the MCS must be first upgraded from MCS 4.0 to MCS 4.1 prior to the CS2K upgrade. When the MCS upgrade has been completed then the CS2K components including NGSS could be upgraded to SN09 software release.

81.2.1.6 SN08 CS2K with VRDN Interworking with MCS 4.1

In this configuration the VRDN must be first migrated to the NGSS architecture prior to the CS2K upgrade. When the migration from the VRDN to NGSS has been completed then the CS2K components including NGSS could be upgraded to SN09 software release.

81.2.1.7 SN08 CS2K with NGSS Interworking with MCS 4.1

In this configuration the CS2K components including NGSS could be directly upgraded to SN09 software release.

81.2.1.8 SN09 CS2K with VRDN - This configuartion is not supported because VRDN is not supported on SN09

81.2.1.9 SN09 CS2K with NGSS Interworking with MCS 3.0

Depending on the customer requirement the MCS can either be left at MCS 3.0 or could be upgraded to MCS 4.1. MCS should not be, however, upgraded to MCS 4.0.

81.2.2 GUI Support

This section describes how to access and data fill the Nature of Address/ Numbering Plan Indicator to Phone Context (NOA/NPI/PC) and Out of Band DTMF Payload portions of the Succession Communication Server 2000 Session Server Manager Graphic User Interface (GUI).

81.2.2.1 NOA/NPI/PC section access

Once logged in and accessed the Succession Communication Server 2000 Session Server Manager link, select Provisioning -> Application -> SIP Gateway to display the NOA/NPI/PC section menu option.

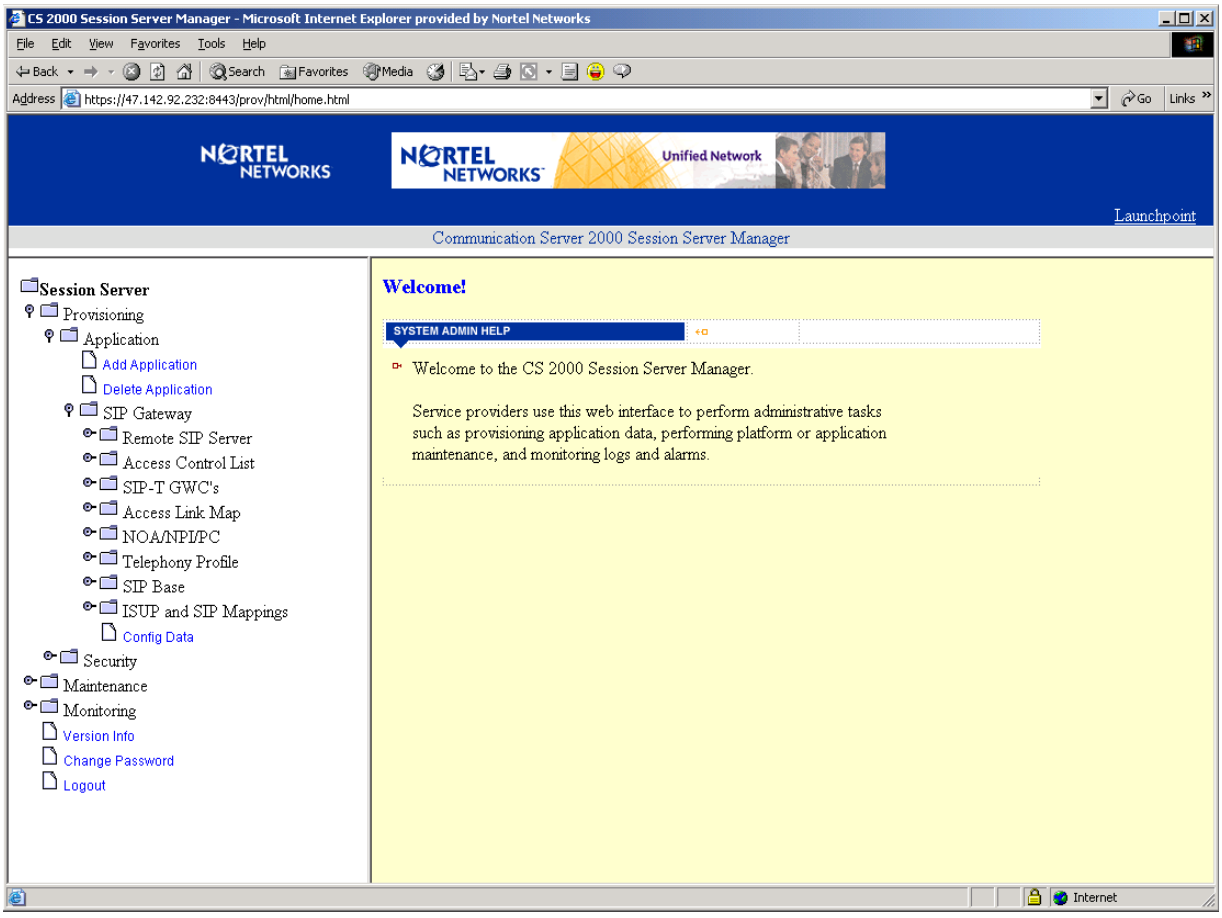


Figure 1 NOA/NPI/PC section access

81.2.2.2 Add/Listing NOA's

Select NOA/NPI/PC menu option to display the Add NOA, List NOA and NOA/NPI/PC Mapping menu options. Select List NOA menu option to view the default list of NOA's.

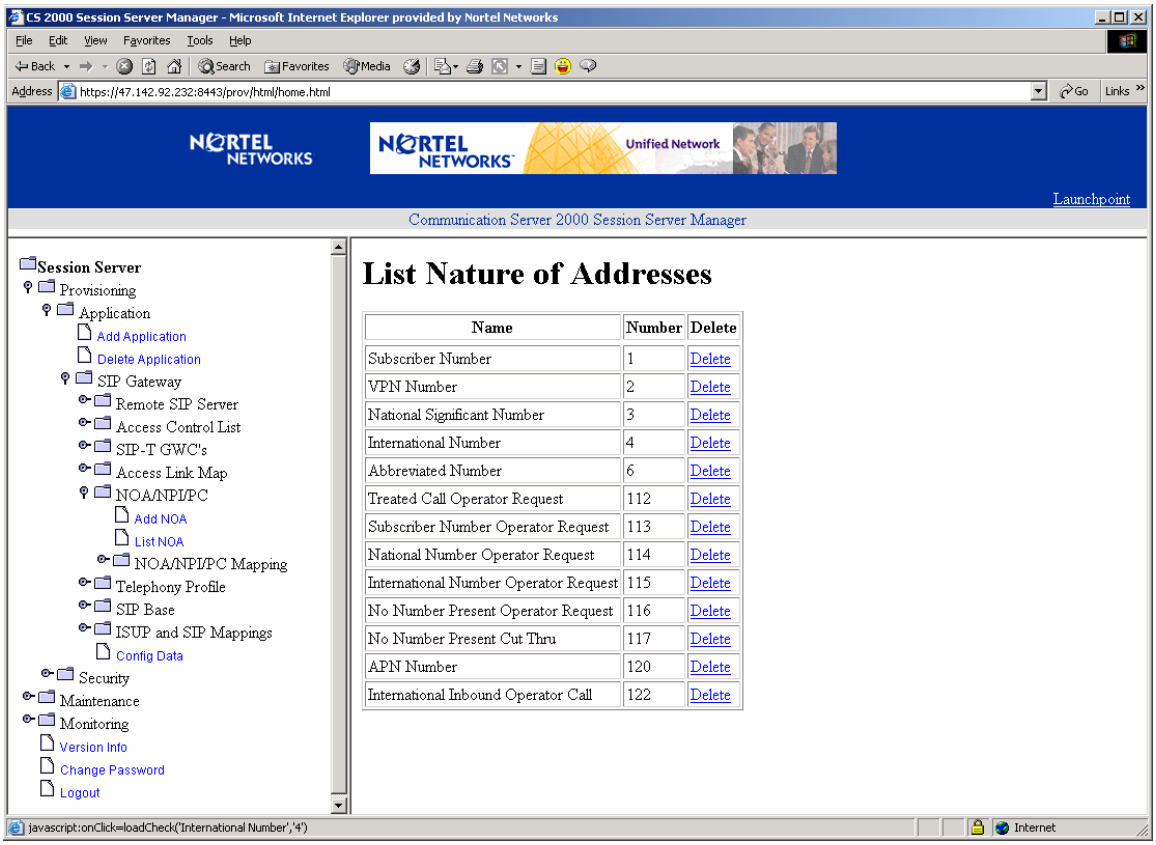


Figure 2 List Nature of Addresses

Select Add NOA menu option to add new NOA. Type in a NOA Name and NOA Number in the designated input areas and then click the Add button to complete the adding of the new NOA. If the addition of the NOA is successful, the new NOA entry will be displayed in the list of NOA's.

NOTE: Valid NOA numbers range from 1 to 150 inclusive.

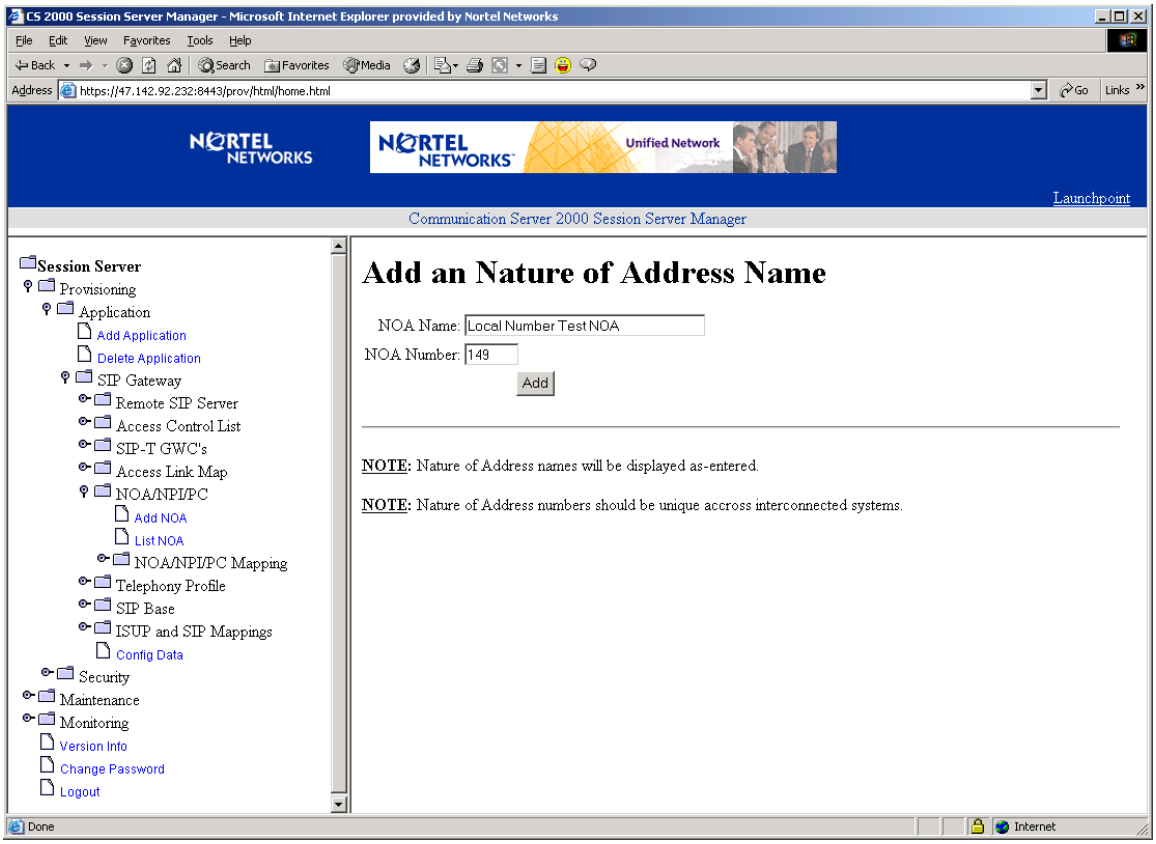


Figure 3 Add a Nature of Address Name

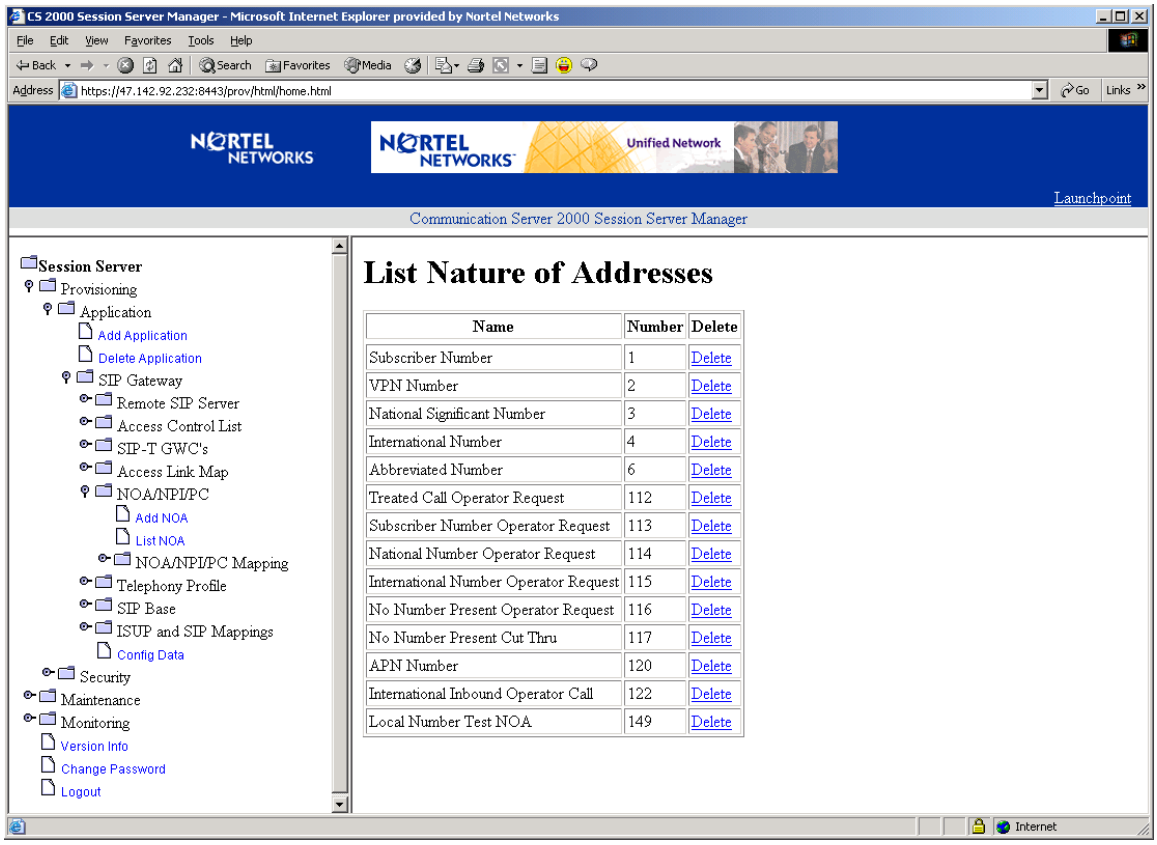


Figure 4 View of List NOA with New Entry

To delete a NOA entry, click Delete for the NOA entry to be removed and select OK in the validation pop-up window.

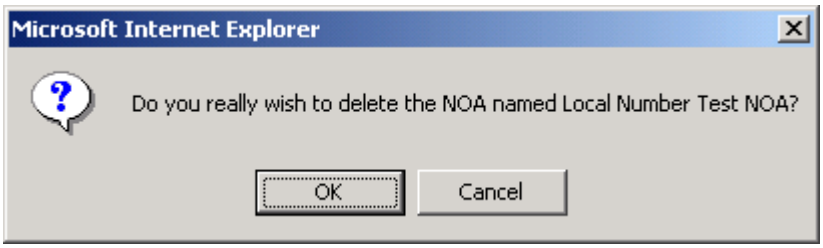


Figure 5 Delete NOA Validation Pop-up Window

The selected NOA entry is removed from the list of NOA's.

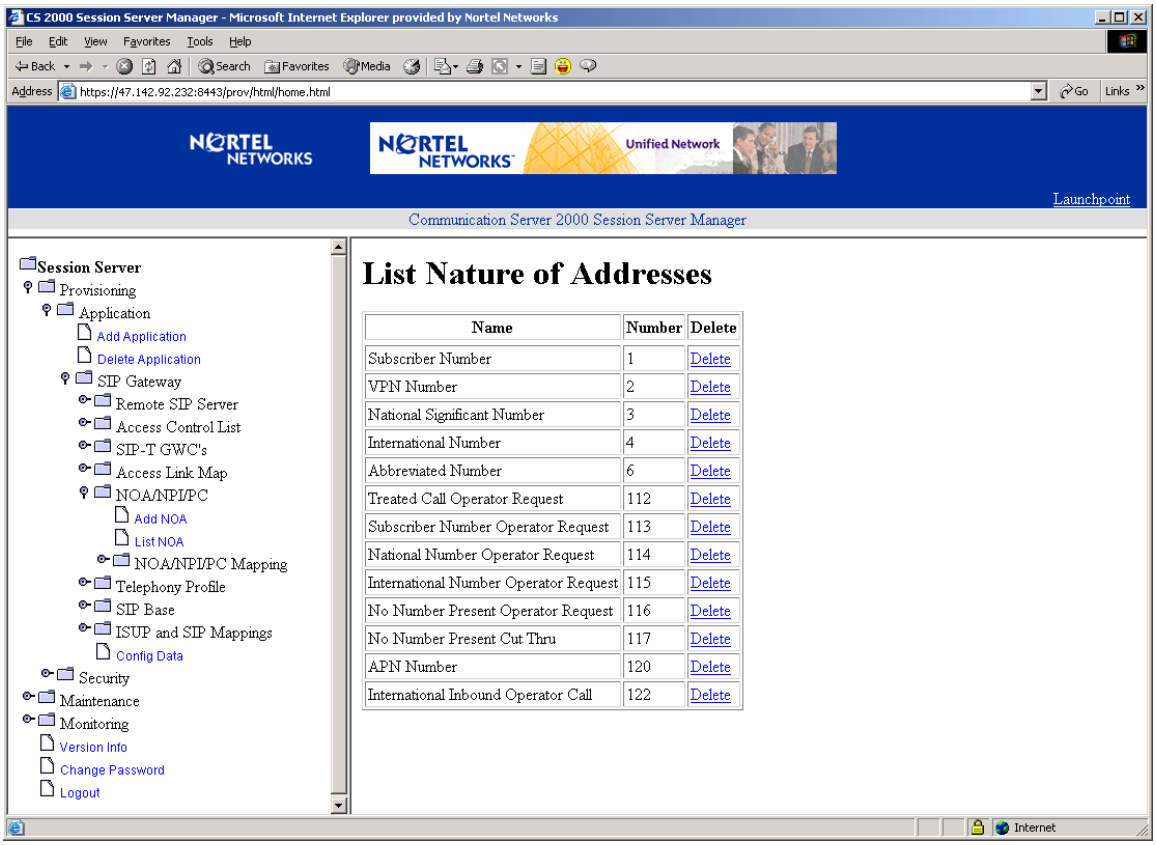


Figure 6 View of List NOA after Deletion of Entry

81.2.2.3 Addition, Deletion and Listing of Phone Context Mappings

Select the NOA/NPI/PC Mapping menu option to display Add Mapping, Delete Mapping and List Mappings menu options.

Select Add Mapping menu option to add a new NOA/NPI to Phone-Context mapping. Type in the New Mapping Name and select a Base Mapping Name from the pull down menu from the designed input areas and then click the Add button to complete the adding of the new mapping.

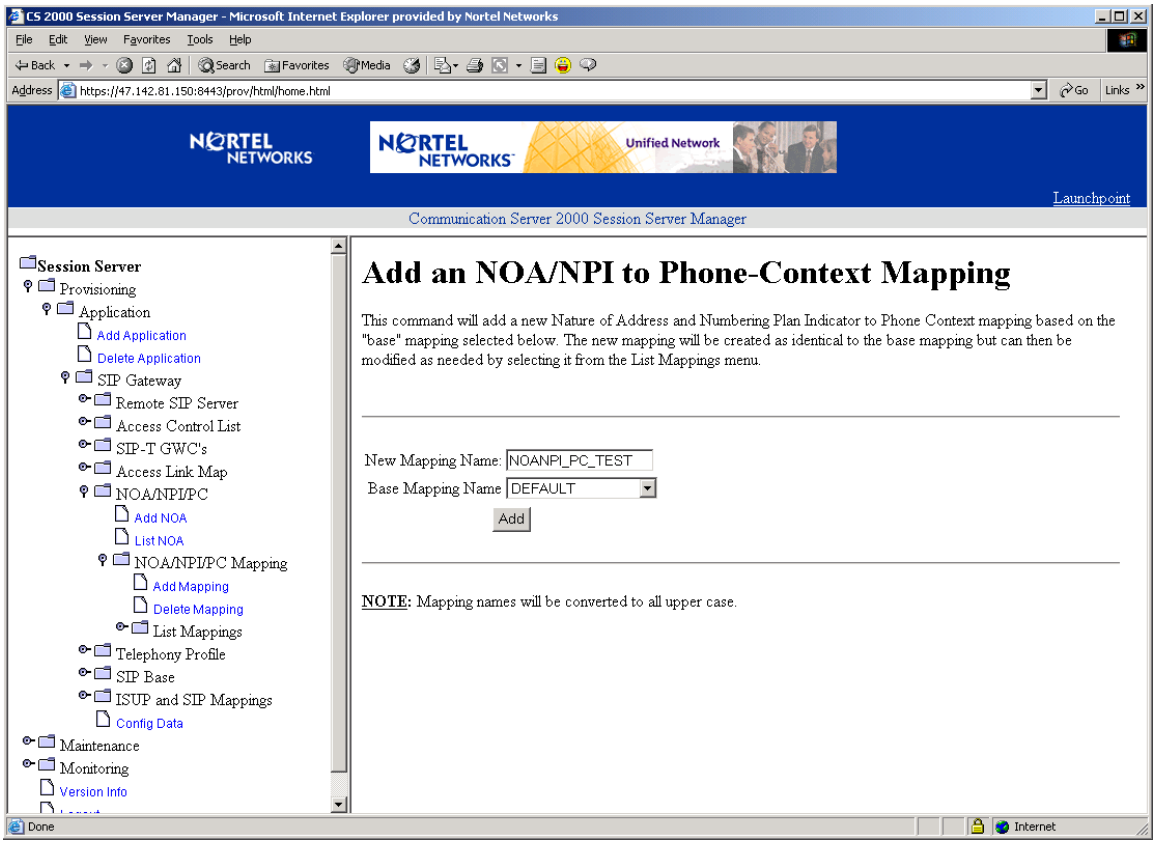


Figure 7 Add a NOA/NPI to Phone-Context Mapping

Click the Add button to add tuples to this new mapping.

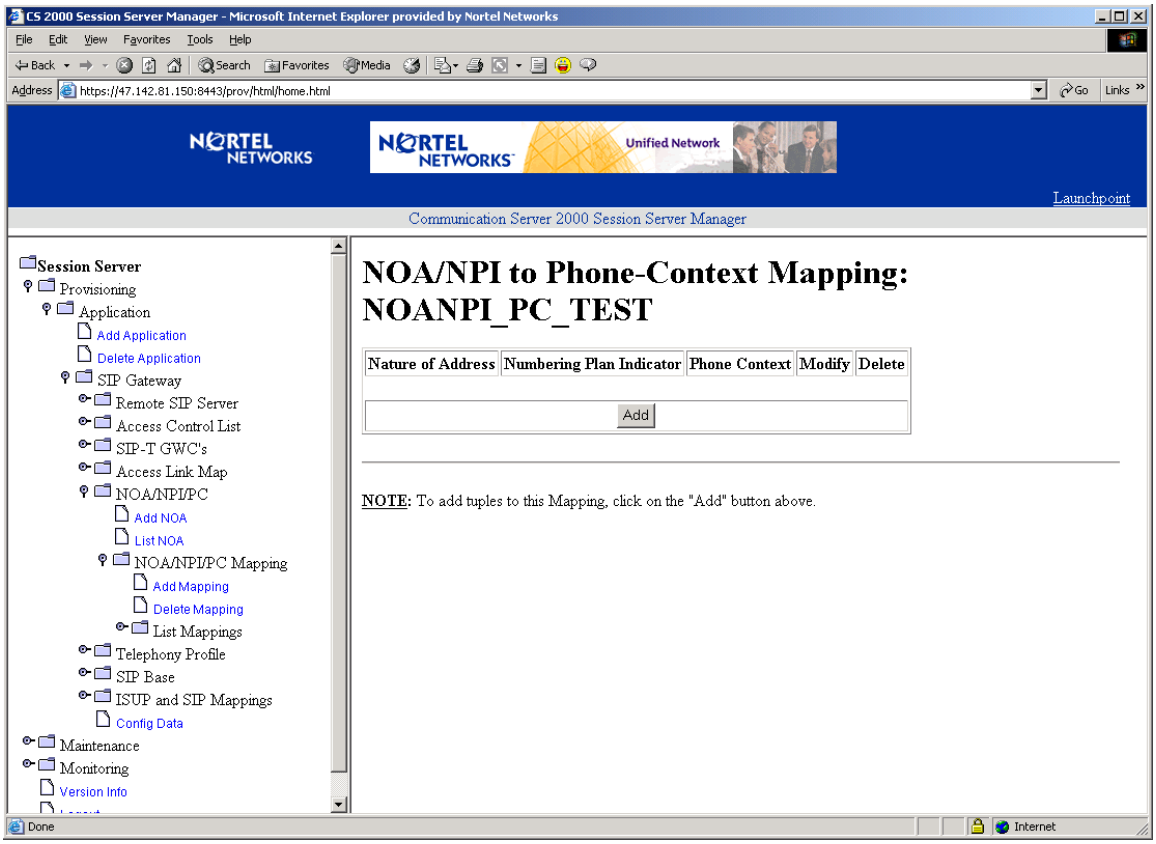


Figure 8 New Mapping NOANPI_PC_TEST View

Select Nature of Address and Numbering Plan Indicator from the pull down menus and type in the Phone Context name for this new tuple entry at the designated input areas. Click the Add button to add the new tuple.

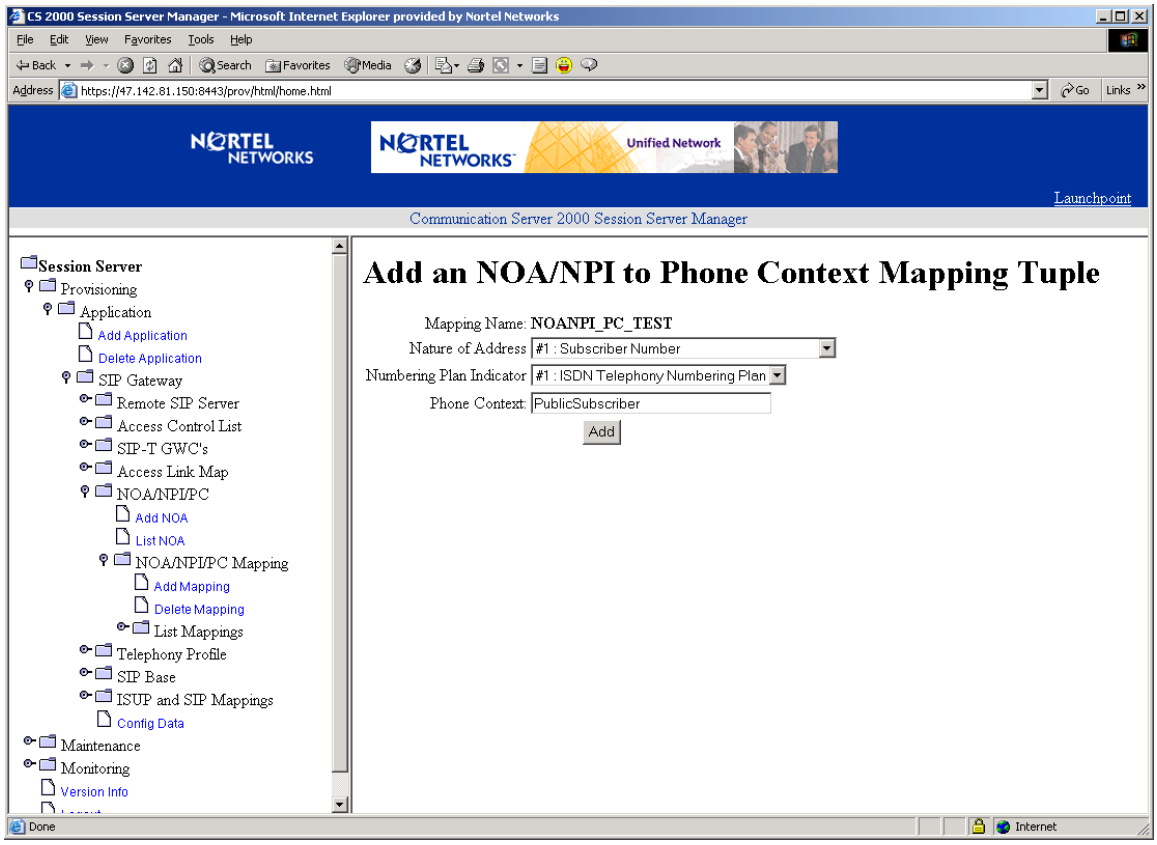


Figure 9 Add New Tuple to Mapping

If invalid selection is entered, a validation pop-up window will appear. Click OK to continue entering tuples for the mapping.

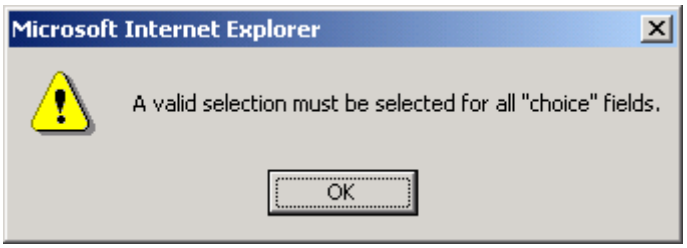


Figure 10 Invalid Selection Validation Pop-up Window

After each successful tuple addition for the mapping, the current list of tuples will be displayed.

To modify a tuple from the mapping, select Modify for the tuple.

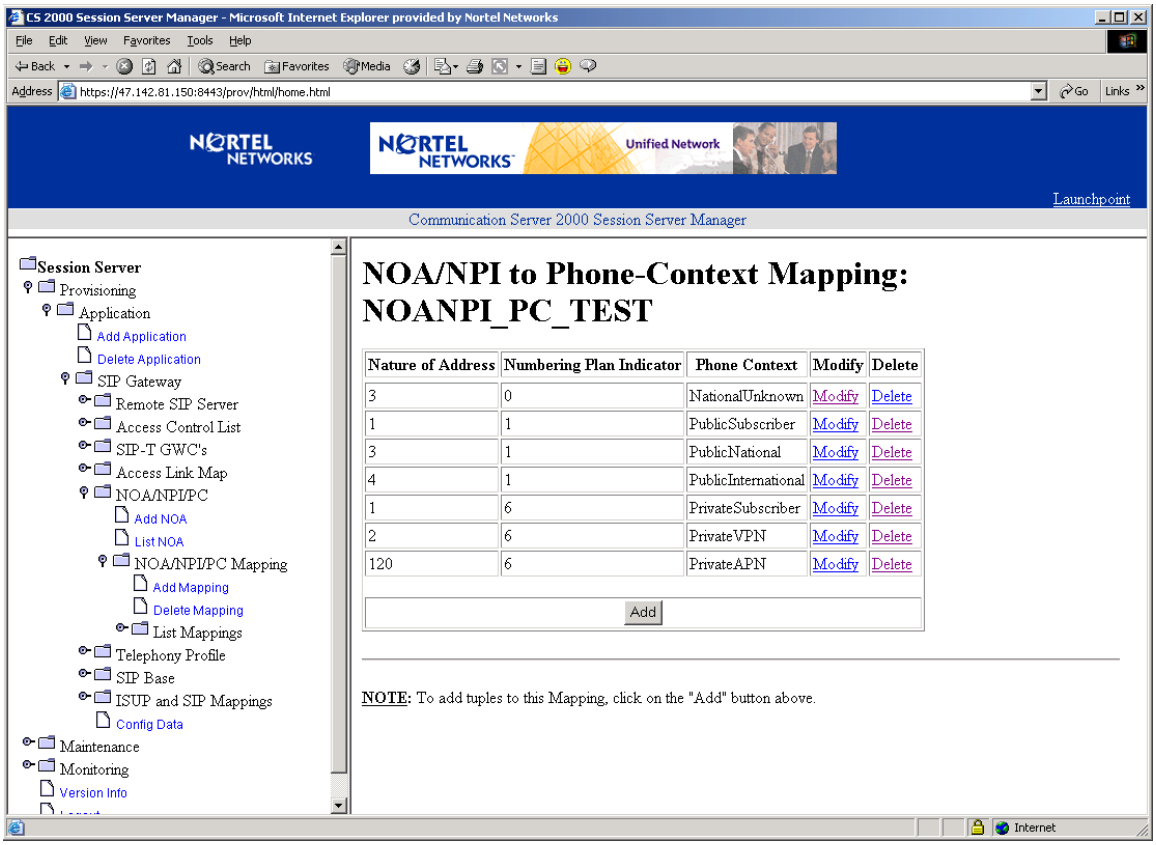


Figure 11 Tuple Listing for NOANPI_PC_TEST

The only tuple entity that can be modified is the Phone Context field.

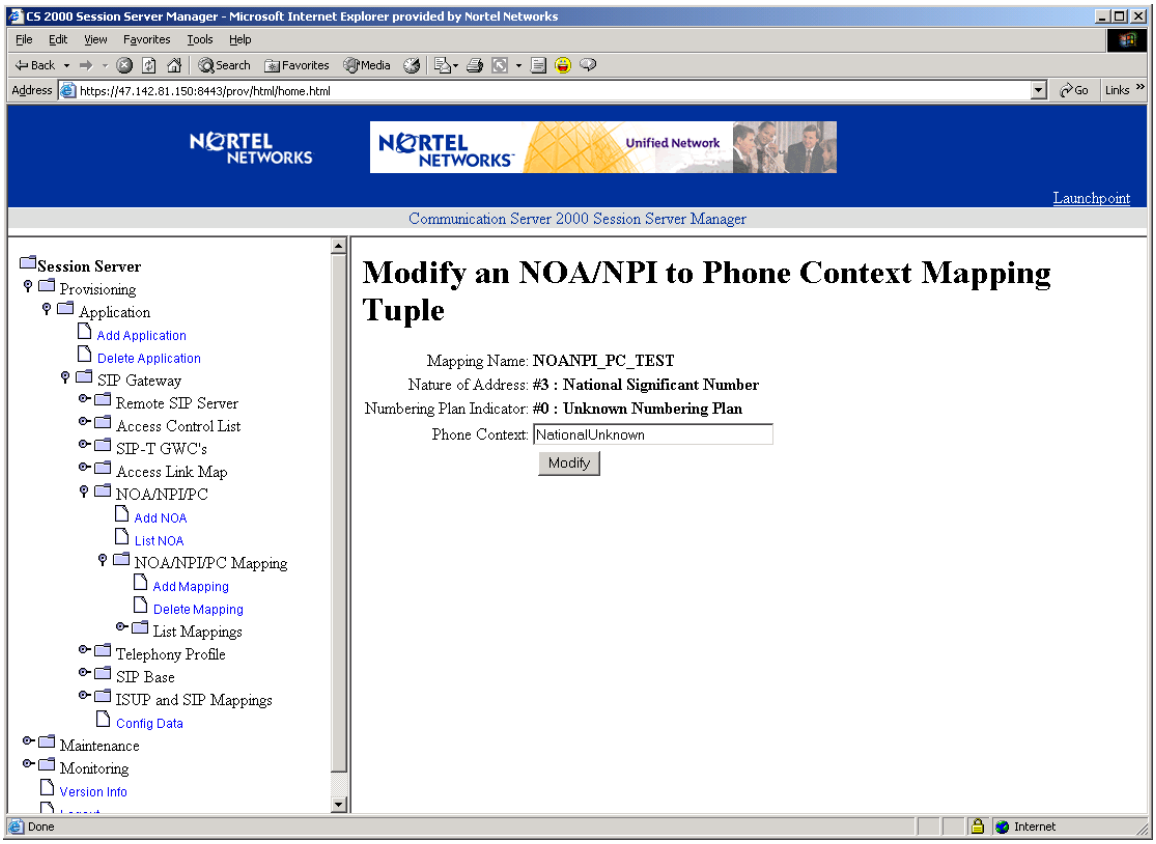


Figure 12 Modify a NOA/NPI to PC Mapping Tuple

Change the Phone Context field to the desired context then click the Modify button.

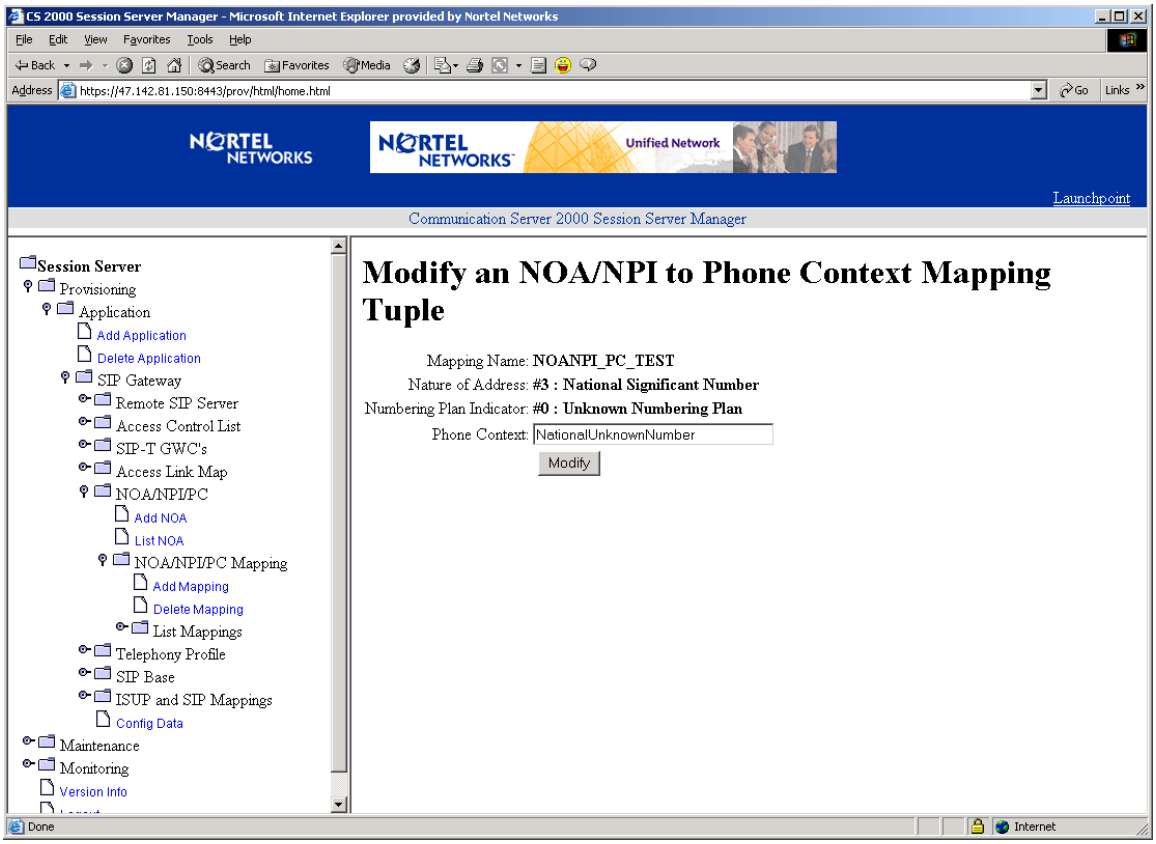


Figure 13 Modify Phone Context NationalUnknown

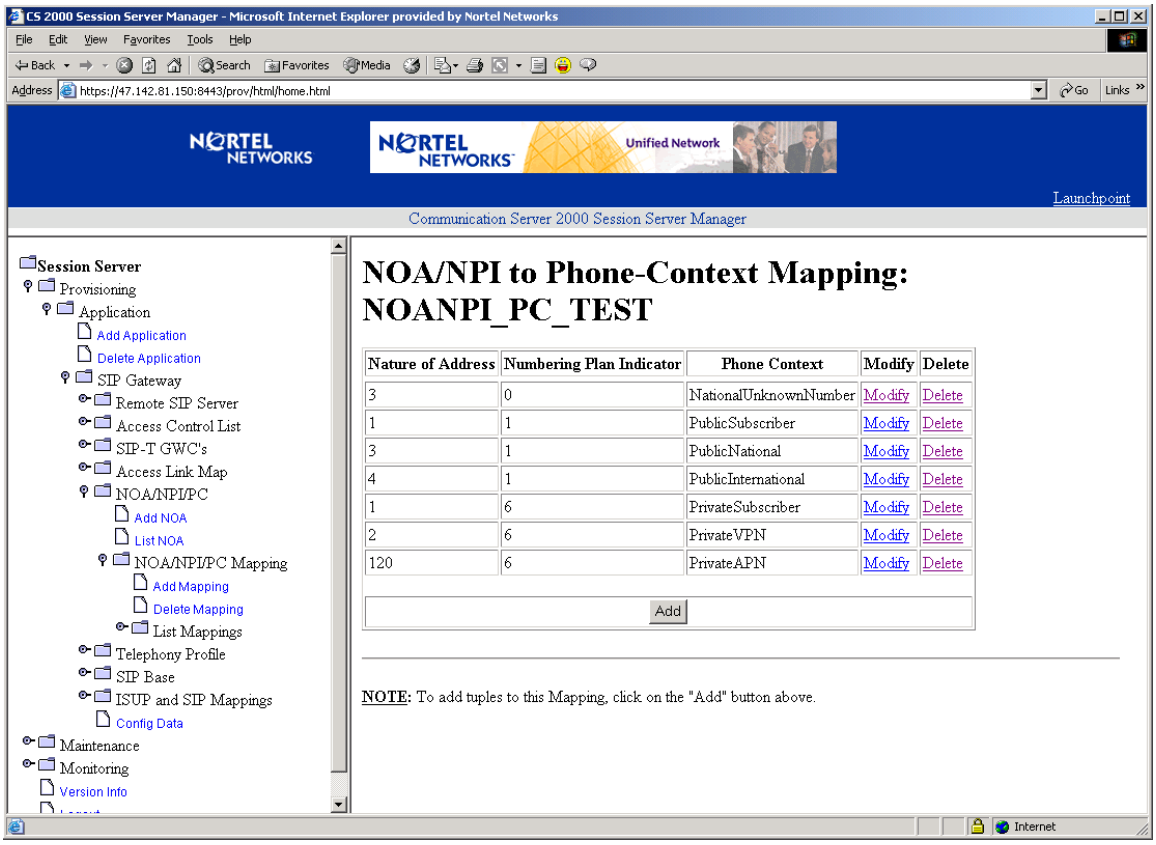


Figure 14 New Mapping Listing with Modified NationalUnknownNumber Tuple

To delete a tuple entry, click Delete for the tuple entry to be removed and select OK in the validation pop-up window.

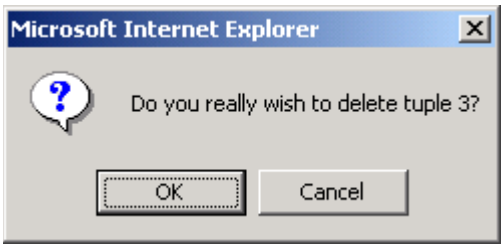


Figure 15 Delete Tuple Validation Pop-up Window

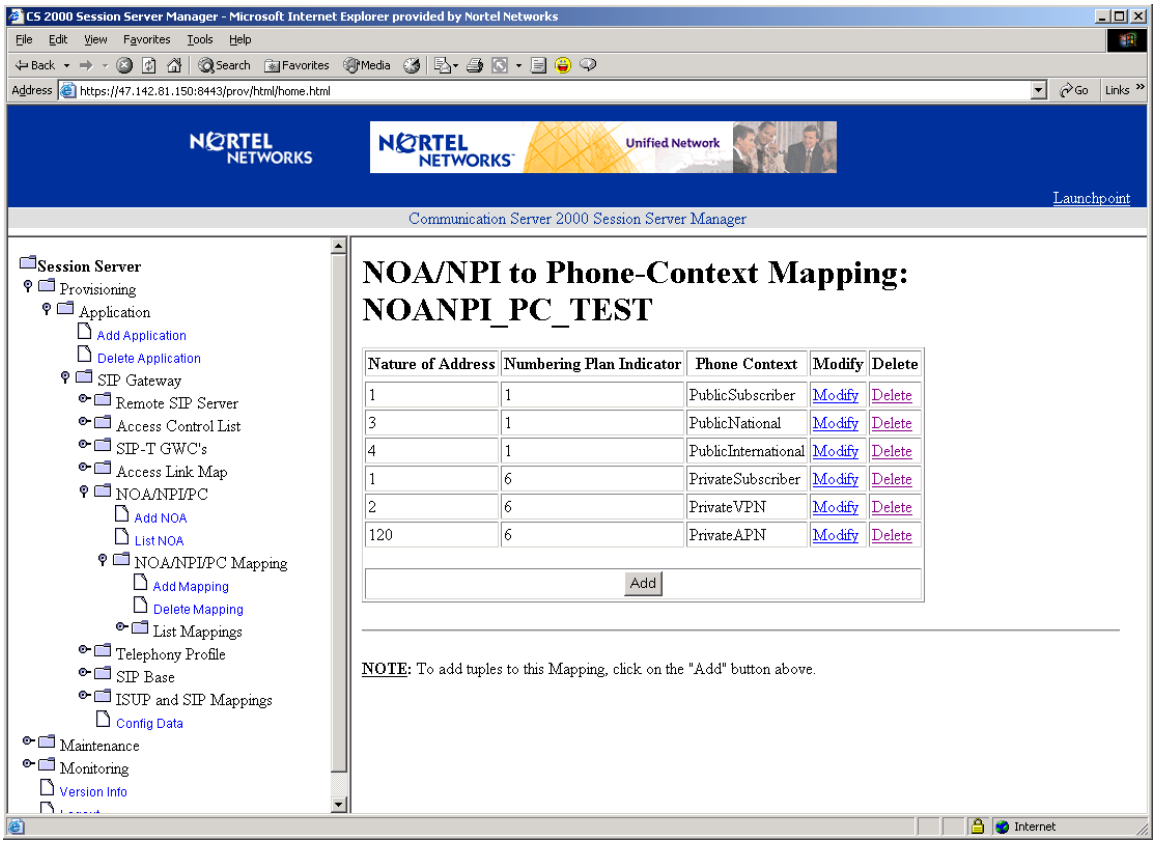


Figure 16 New Mapping Listing with NationalUnknownNumber Tuple Deleted

To view the list of phone-context mappings, select the List Mappings menu option.

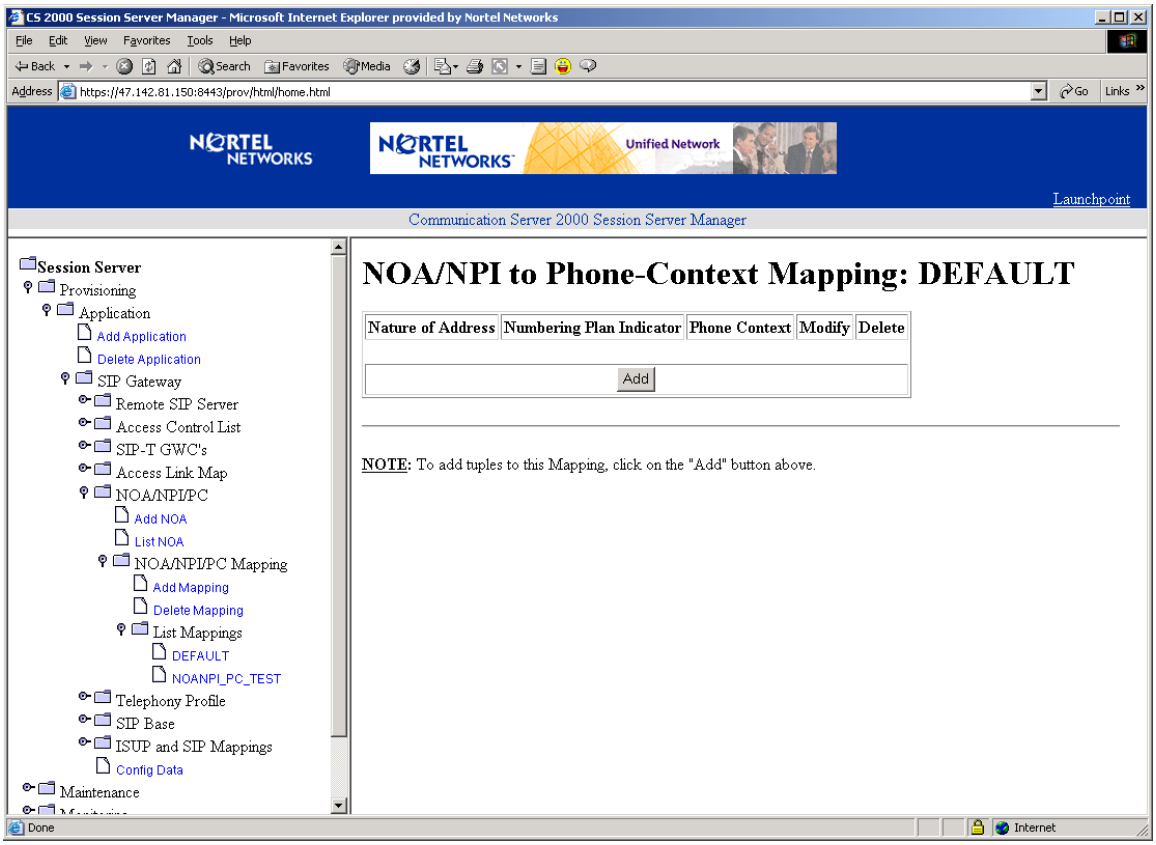


Figure 17 View of Phone-Context Mapping for DEFAULT

To view the tuples of a particular mapping, click on the mapping name under the List Mappings heading from the menu option section.

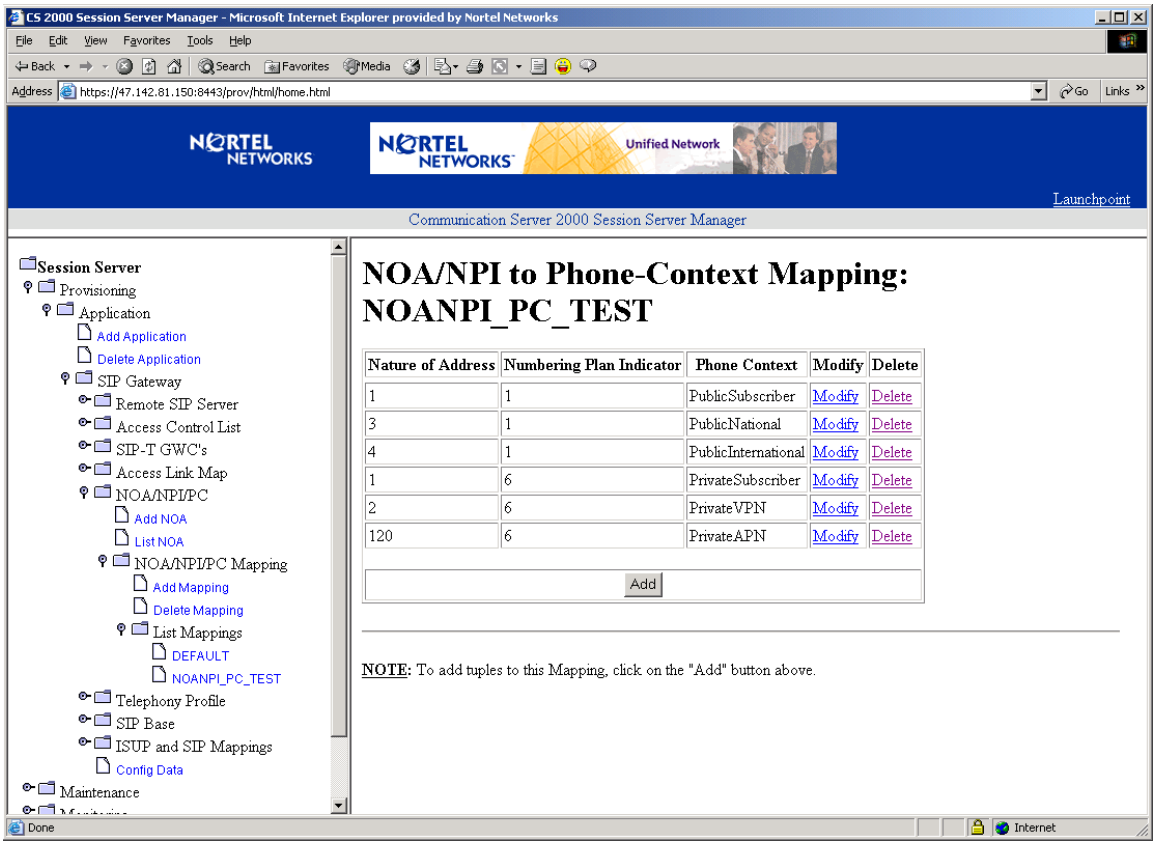


Figure 18 View of Phone-Context Mapping for NOANPI_PC_TEST

To access the section to delete a NOA/NPI to PC mapping, select the Delete Mapping menu option.

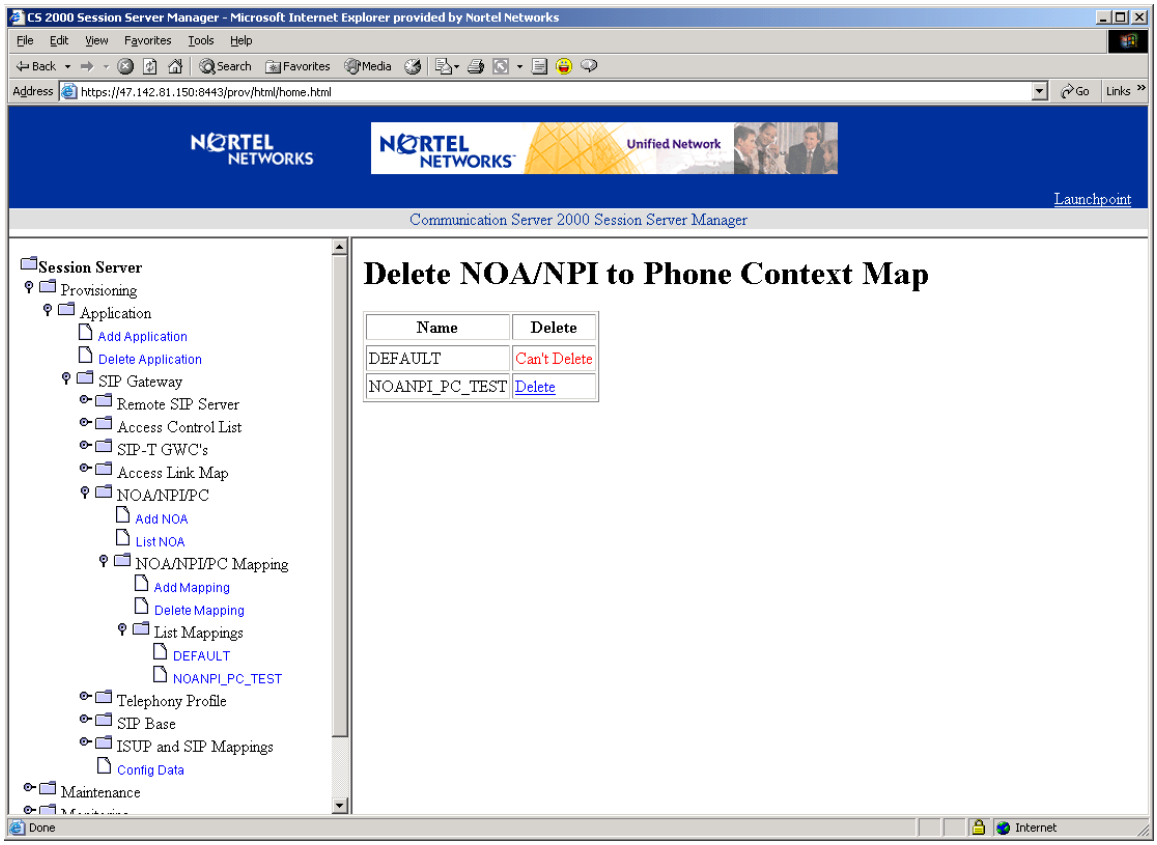


Figure 19 Delete NOA/NPI to Phone Context Map

To delete a phone context map, click Delete for the map entry to be removed and select OK in the validation pop-up window.

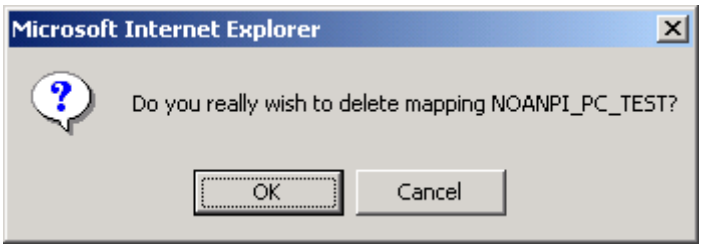


Figure 20 Delete Mapping Validation Pop-up Window

The phone context map has been removed.

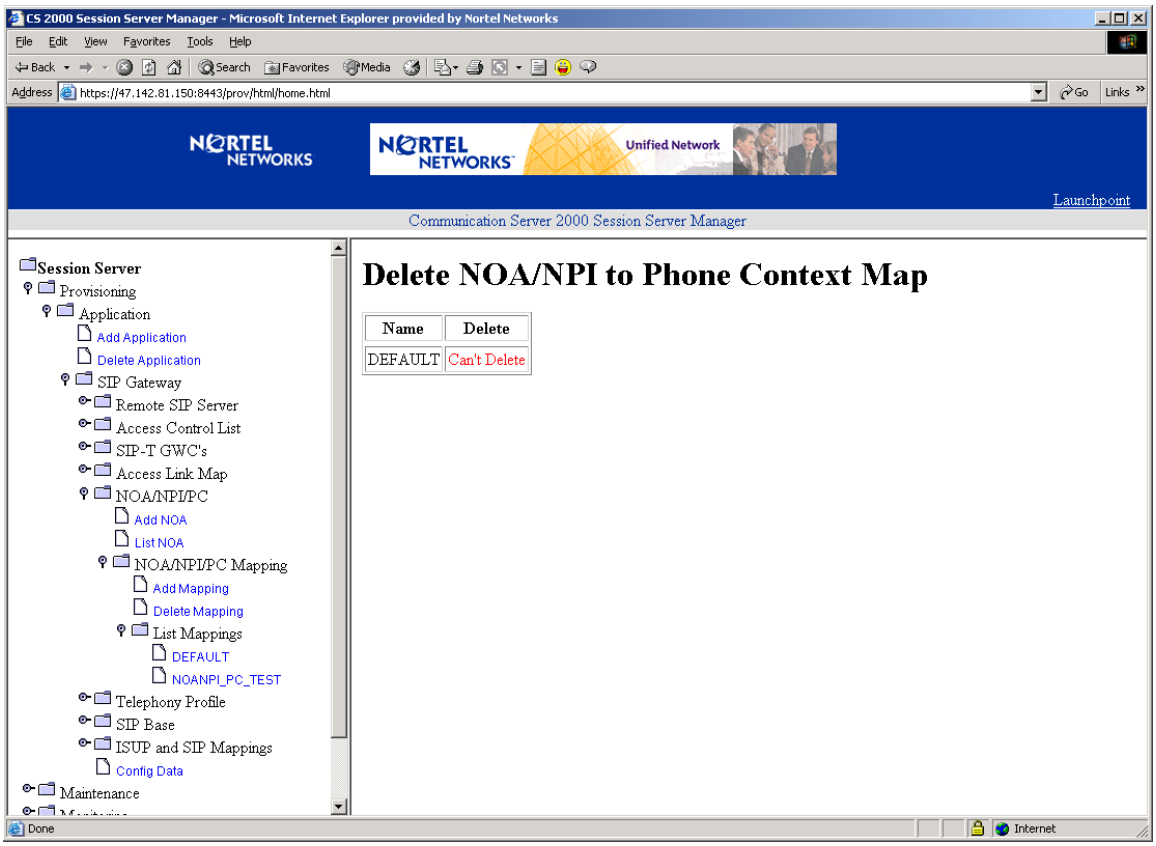


Figure 21 Delete NOA/NPI to Phone Context Map without NOANPI_PC_TEST Map

To refresh the map entries in the menu options column, select List Mappings menu option to hide mappings.

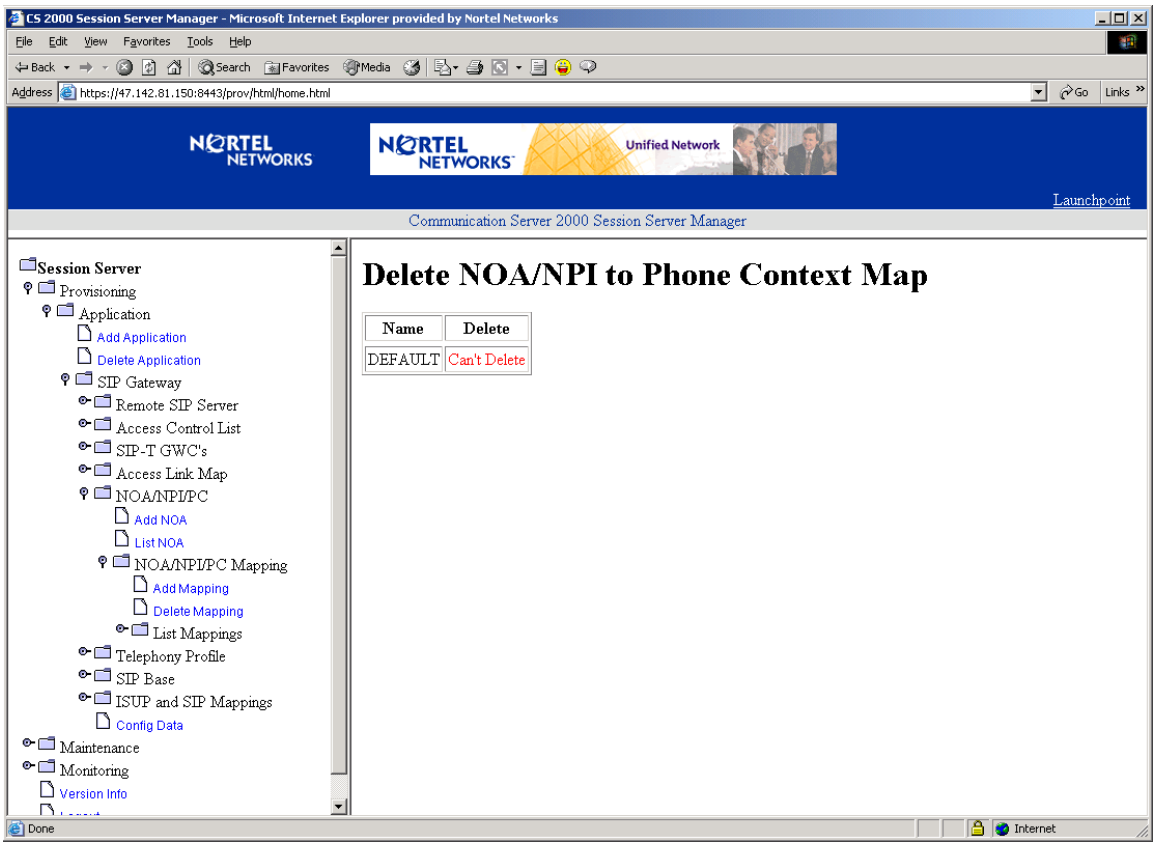


Figure 22 Hide List Mappings

To redisplay the new mappings, select List Mappings again.

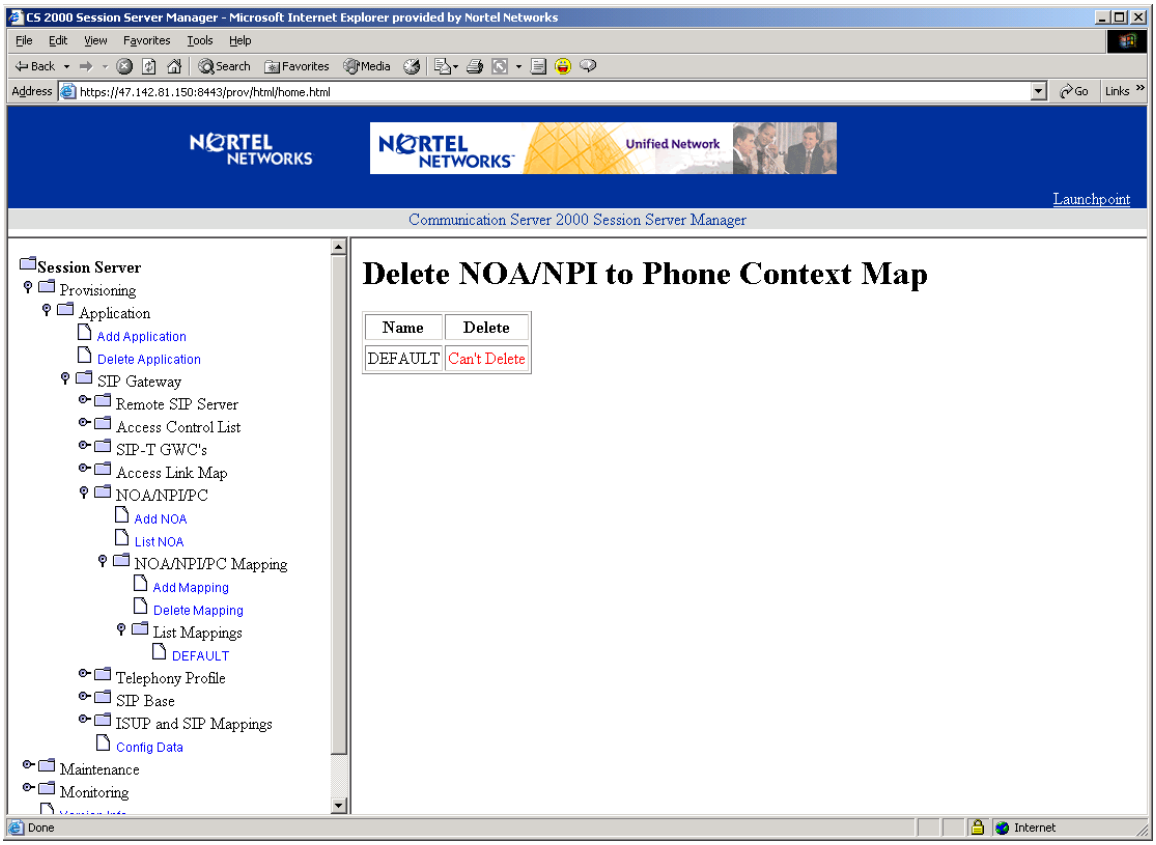


Figure 23 Display List Mappings

81.2.2.4 OOB DTMF Payload section access

Once logged in and accessed the Succession Communication Server 2000 Session Server Manager link, select Provisioning -> Application -> SIP Gateway to display the Remote SIP Server section menu option.

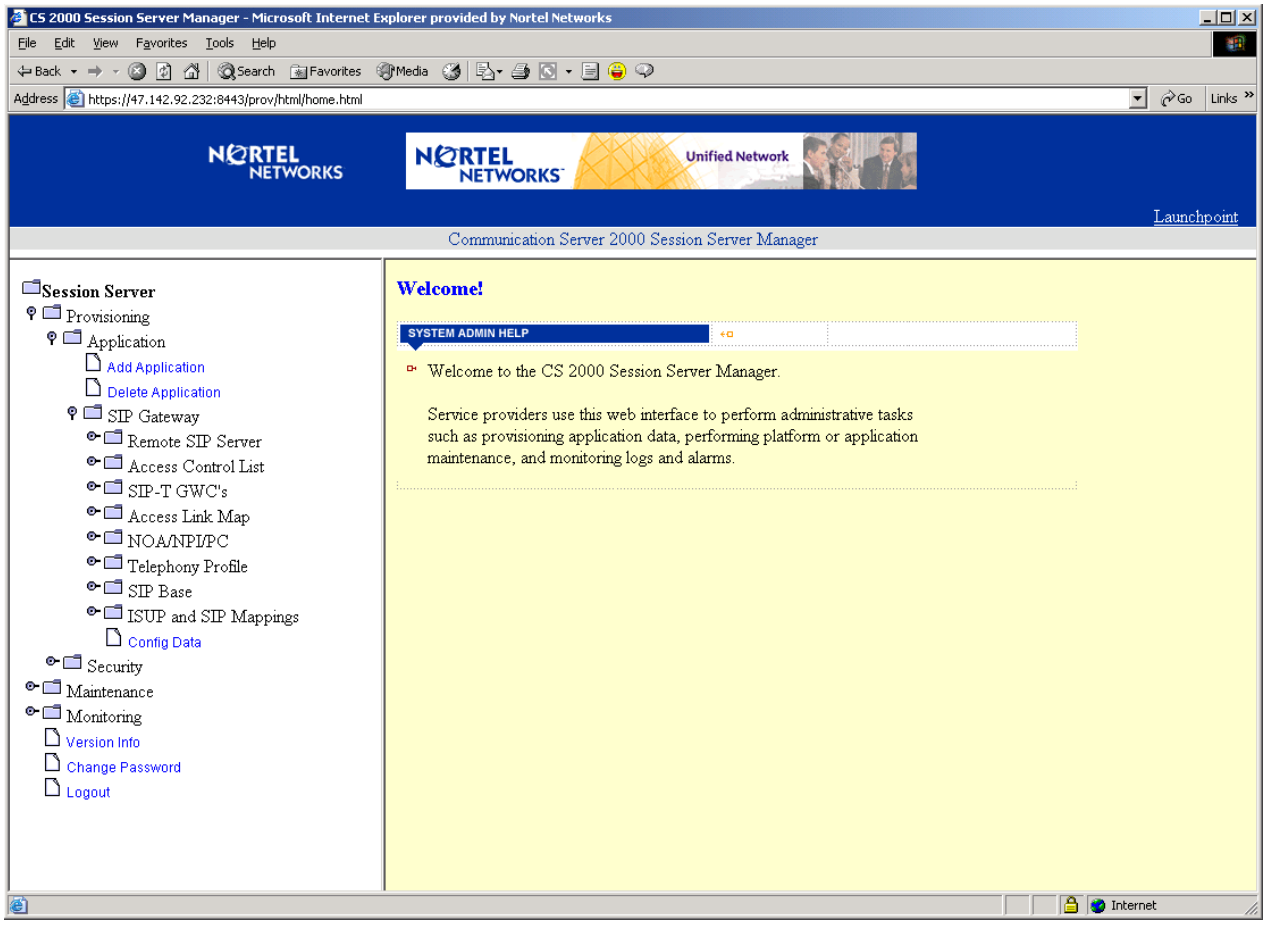


Figure 24 Remote SIP Server section access

Select Remote SIP Server menu option to display the Add Server and List Servers menu options.

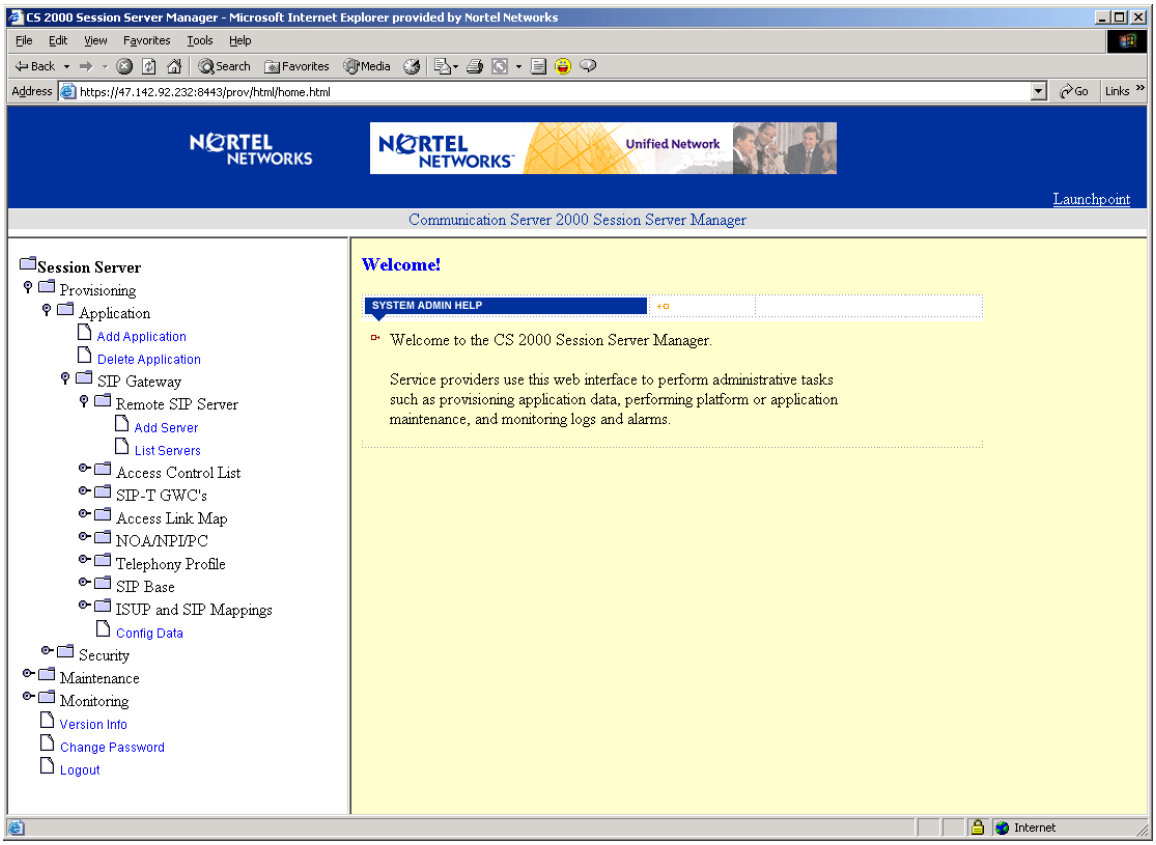


Figure 25 Remote SIP Server

Select List Servers menu option to view the current list of SIP servers.

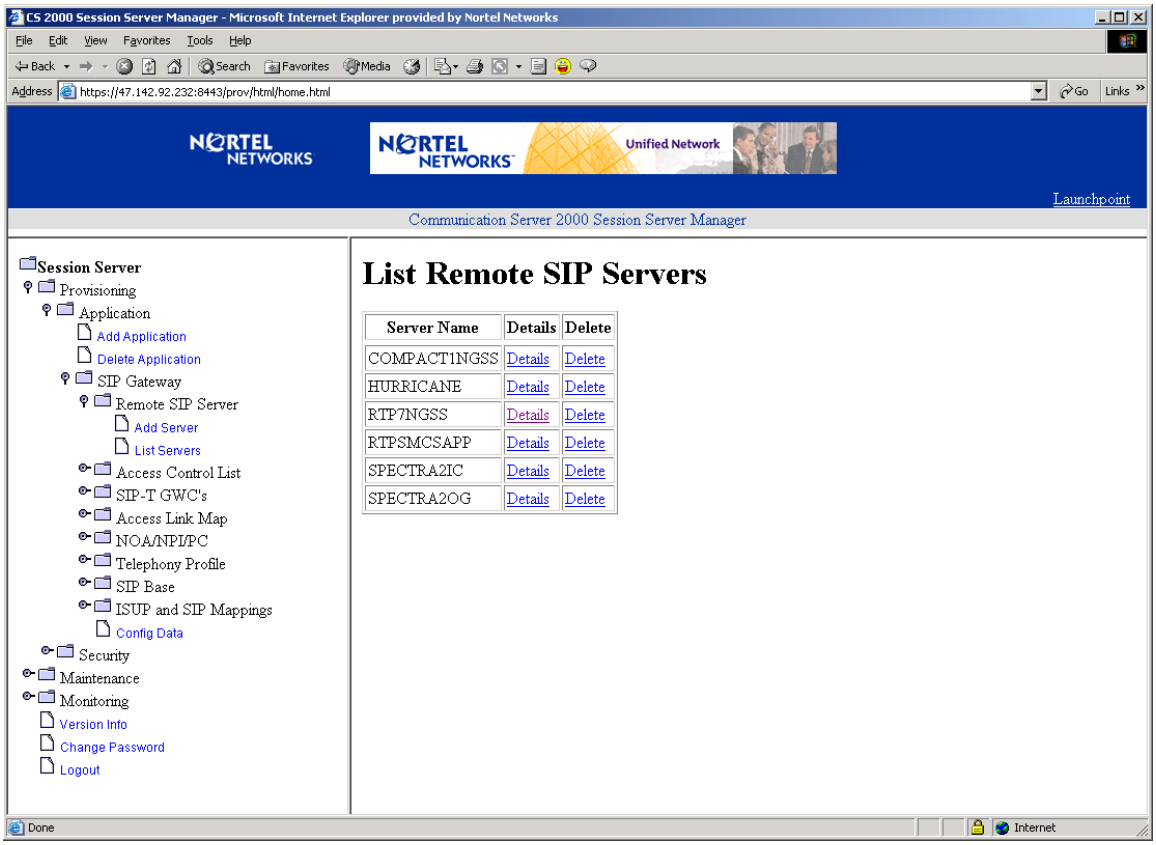


Figure 26 List Remote SIP Servers

To view the details of a particular SIP server, click Details of the Server Name to be viewed.

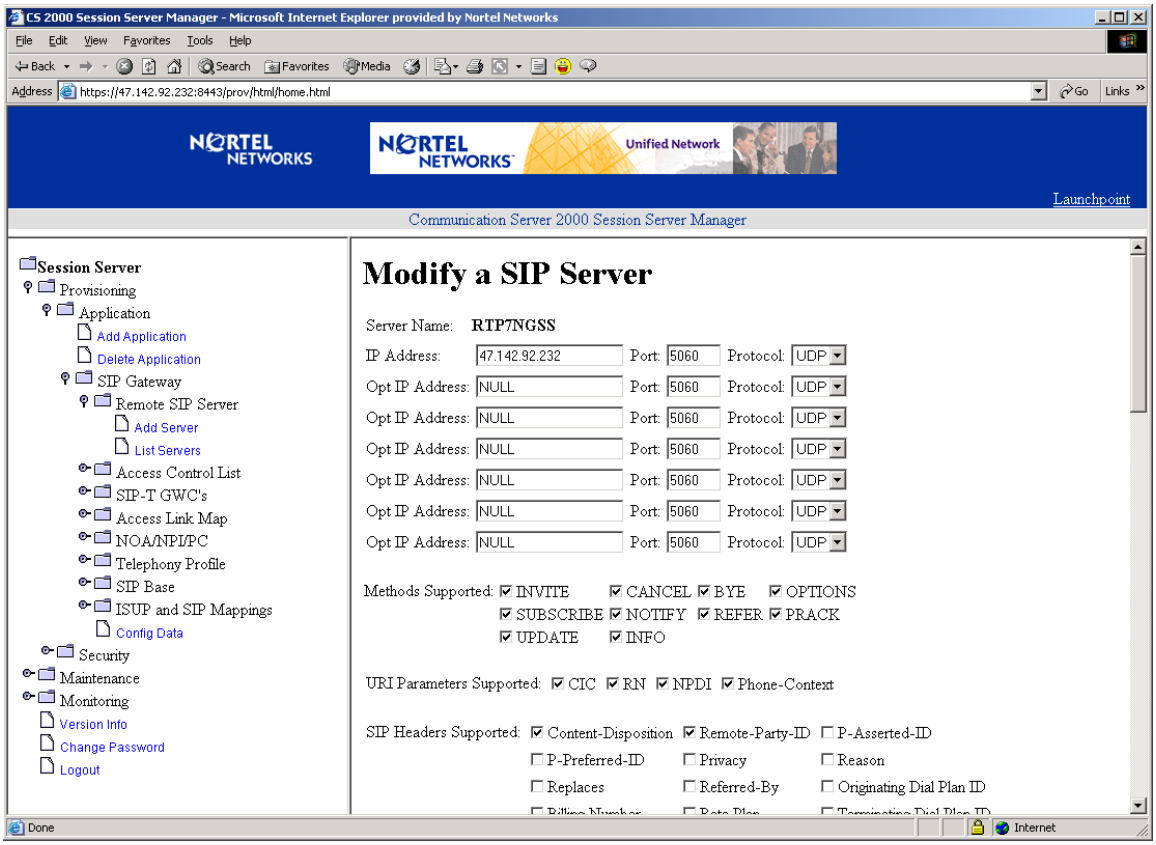


Figure 27 Modify a SIP Server

Scroll down to the Out of Band DTMF Payload option. Select application/ vnd.nortelnetworks.digits from the pull down menu for the designated input area.

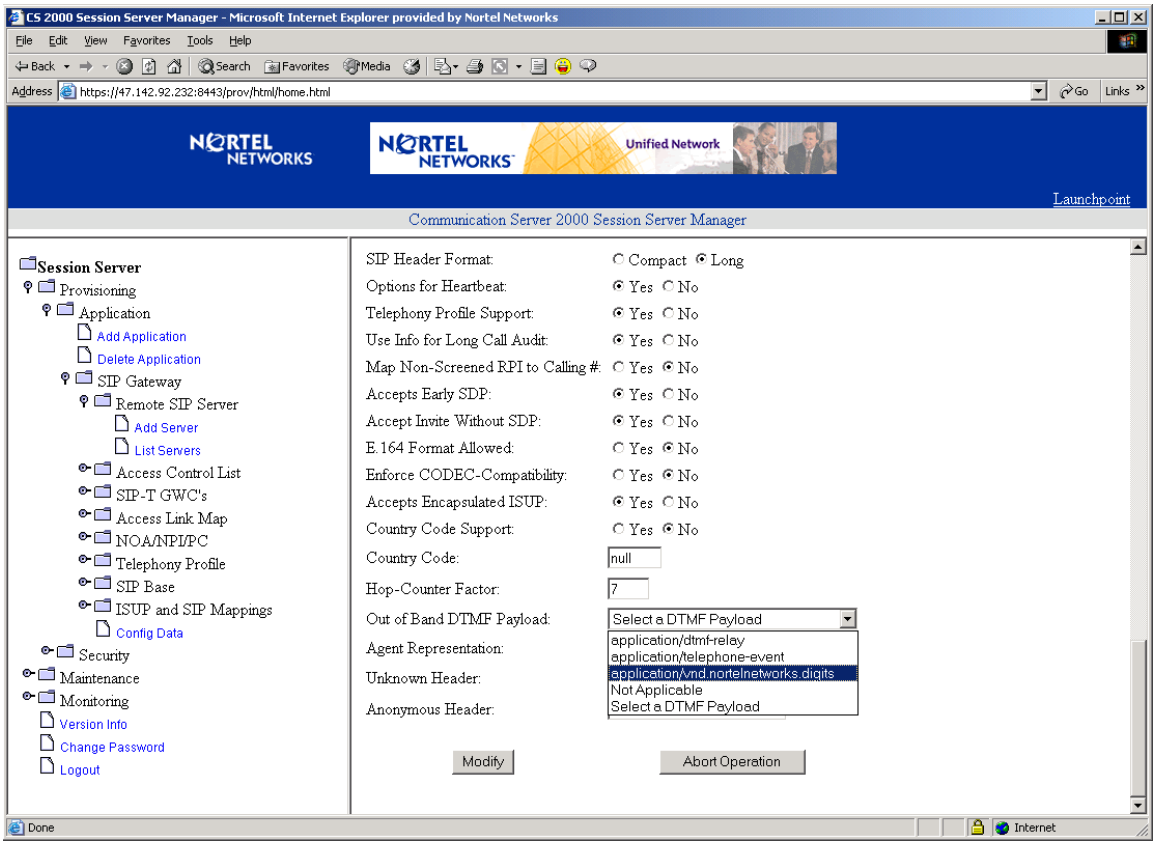


Figure 28 Out of Band DTMF Payload

To discontinue the change, click on the Abort Operation button and select OK in the abort the modification pop-up window.

Figure 29 Abort Modification Validation Pop-up Window

To accept change, click the Modify button and click OK in the modify validation pop-up window.

Figure 30 Modify SIP Server Validation Pop-up Window

To view the SIP server change, select Details of the SIP server that was changed.

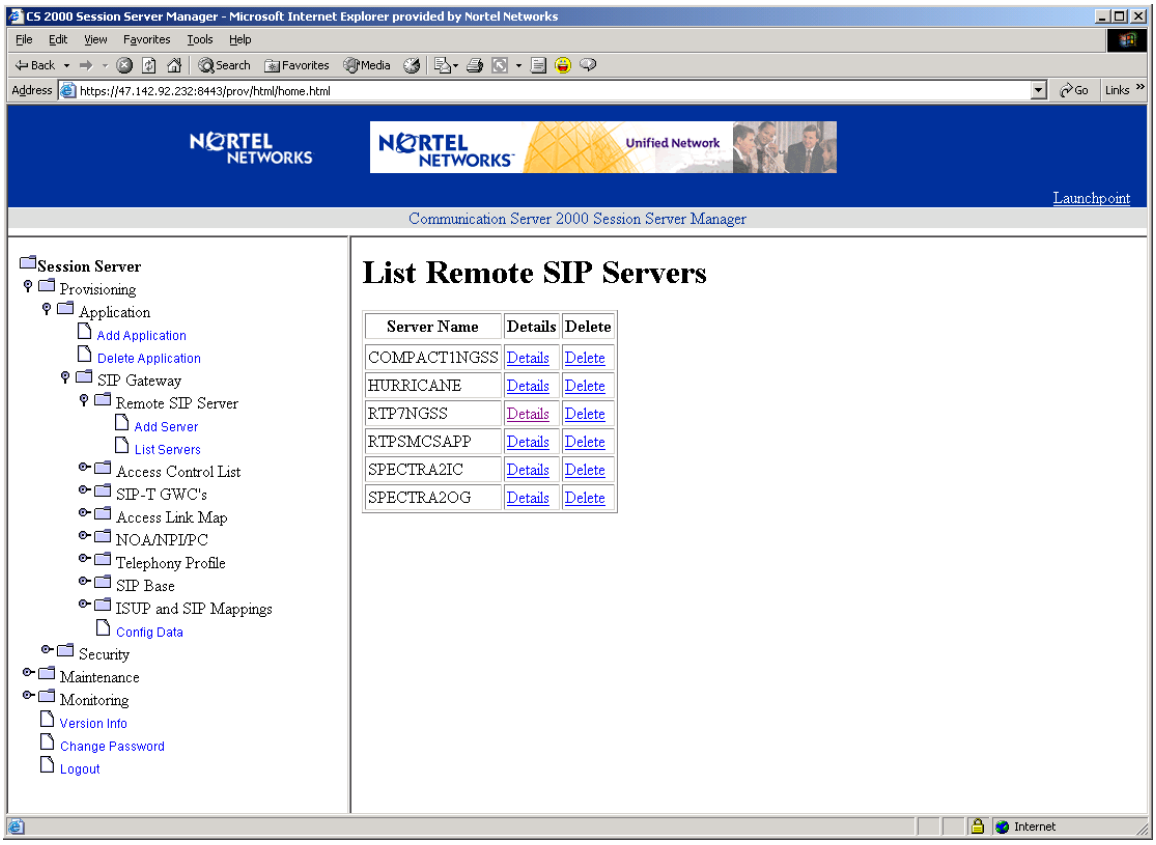


Figure 31 RTP7NGSS after Server Modification

81.2.3 Support for SIP INFO Method

Using SIP protocol, applications can establish and terminate multimedia sessions. Telephony applications that require mid session signalling, such as voice mail and meet-me conference, can accomplish that task by using one of the following ways:

RFC2833 - This standard is for defining the mechanism to encode DTMF tones within the Gate Ways (GW) and has already been implemented by most GWs.

Use of SIP INFO Message: This method is used to collect and transport DTMF digits. This activity will implements the use of SIP INFO method in Next Gen Session Server (NGSS).

A trunk option has been defined in NGSS GUI to send Out-Of-Band (OOB) DTMF tones. This option is set only if the remote server does not support RFC2833.

81.2.3.1 Outgoing CS2K Calls

When a user presses a digit on the keypad, PVG GW informs Tandem GWC about the digit. Tandem GWC sends INFORM message to the SIP GWC with digit payload. SIP GWC sends a GCP message to the Session Server (NGSS) with the tone information. NGSS checks the trunk options and if the option is **vnd.nortelnetworks.digits** OOB signalling will be used. In this case the INFO message with the DTMF payload will be sent to the remote server.

Following is a sample of the INFO message sent to the remote server:

```
INFO sip:123456@47.104.11.31:5060 SIP/2.0
v: SIP/2.0/UDP 47.104.11.207:5060
t: <sip:123456;phone-
context=myContext@enterprise.com;user=phone>;tag=345496207
f: UserA <sip:userA@enterprise.com>;tag=1652960069
m: <userA@47.104.11.205:5060;transport=udp>
i: 351f114f_f46db6dfe9@zngcs01
CSeq: 79007 INFO
c: application/vnd.nortelnetworks.digits
l: 35
p=Digit-Collection
y=Digits
d=1
```

Note that for outgoing CS2K calls, CS2K will send the INFO with digits to MCS only in a 323-SIP_MCS inter-working when the originating 323 does not support RFC2833.

81.2.3.2 Incoming CS2K Calls

For incoming CS2K calls, once NGSS receives an INFO message, the trunk option is checked and if **vnd.nortelnetworks.digits** is present, the new INFO template is used to parse the message and extract the digits.

81.2.4 Support for Public and Private Name/Number Display

In MCS09/SN09, enhancements are being made to extended the concepts of Public and Private Name and Number display within Centrex customer groups across the MCS CD (Converged Desktop) services. Enhancements to MCS are made under the feature A00009905, “Private Public Name and Number Display”. Enhancements are made to display the Private Name / Number information to the called party within the same Centrex group and the Public Name/Number to the called party outside the Centrex group. CS2K changes, specifically to the NGSS, are made under this feature to support these enhancements.

Directory Numbers within a Centrex customer group can be provisioned with a Public Display Name and a Private Display Name. Centrex features allow the Private Name and Number (which might be a 5 digit number) to be

displayed on calls between parties within the same Centrex customer group. They also allow the Public Name and Number (which can be a 10 digit PSTN number) to be displayed when the parties are not in the same Centrex customer group, such as when one of the parties is a PSTN caller.

Using MBG over IT trunks allows Centrex customer groups and their related services to be extended to Directory Numbers hosted off of different DMS switches. In the following figure, if party A and party B are in the same Centrex group, the Private Name and Number can be displayed.

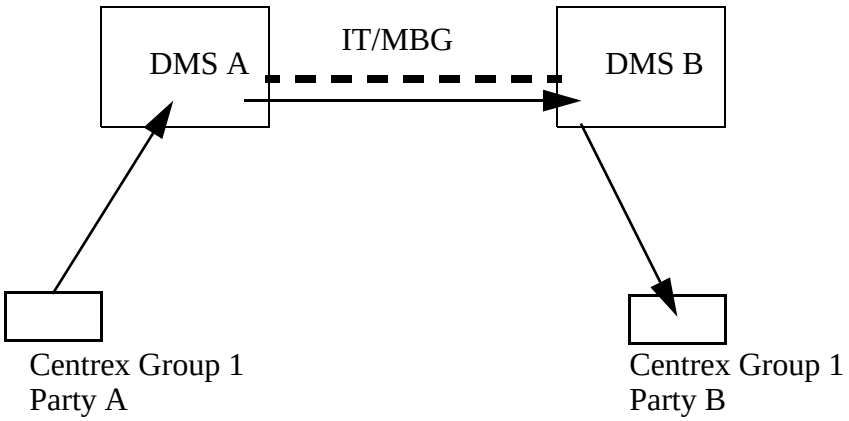


Figure 32 Extension of Centrex Groups using MBG

As in the following diagram, if one of the parties is a PSTN caller, the Public Name and Number can be displayed.

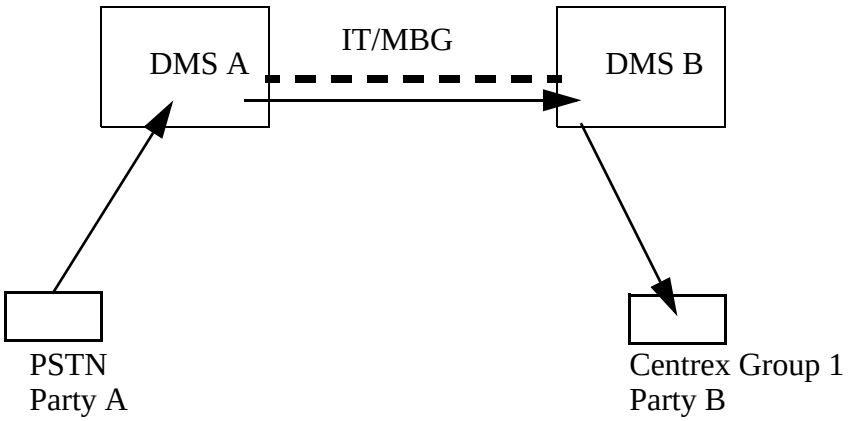


Figure 33 Call from outside the Centrex Group

The equivalent of a Centrex business group on the MCS system is a domain or sub-domain. A Private call is made within the domain or sub-domain. A Public call is one made outside the domain boundaries.

MCS CD functionality allows users to have an MCS Multimedia PC Client that can be used with a headset for VoIP telephony calls, as well as a PAD (Personal Audio Device) that can be an office telephone. The MCS PC Client has a display window that displays call status and can be used to control interactions between the Desktop telephone and the PC Client, such as controlling which phone to ring.

A basic diagram of a Converged Desktop system configuration is shown below..

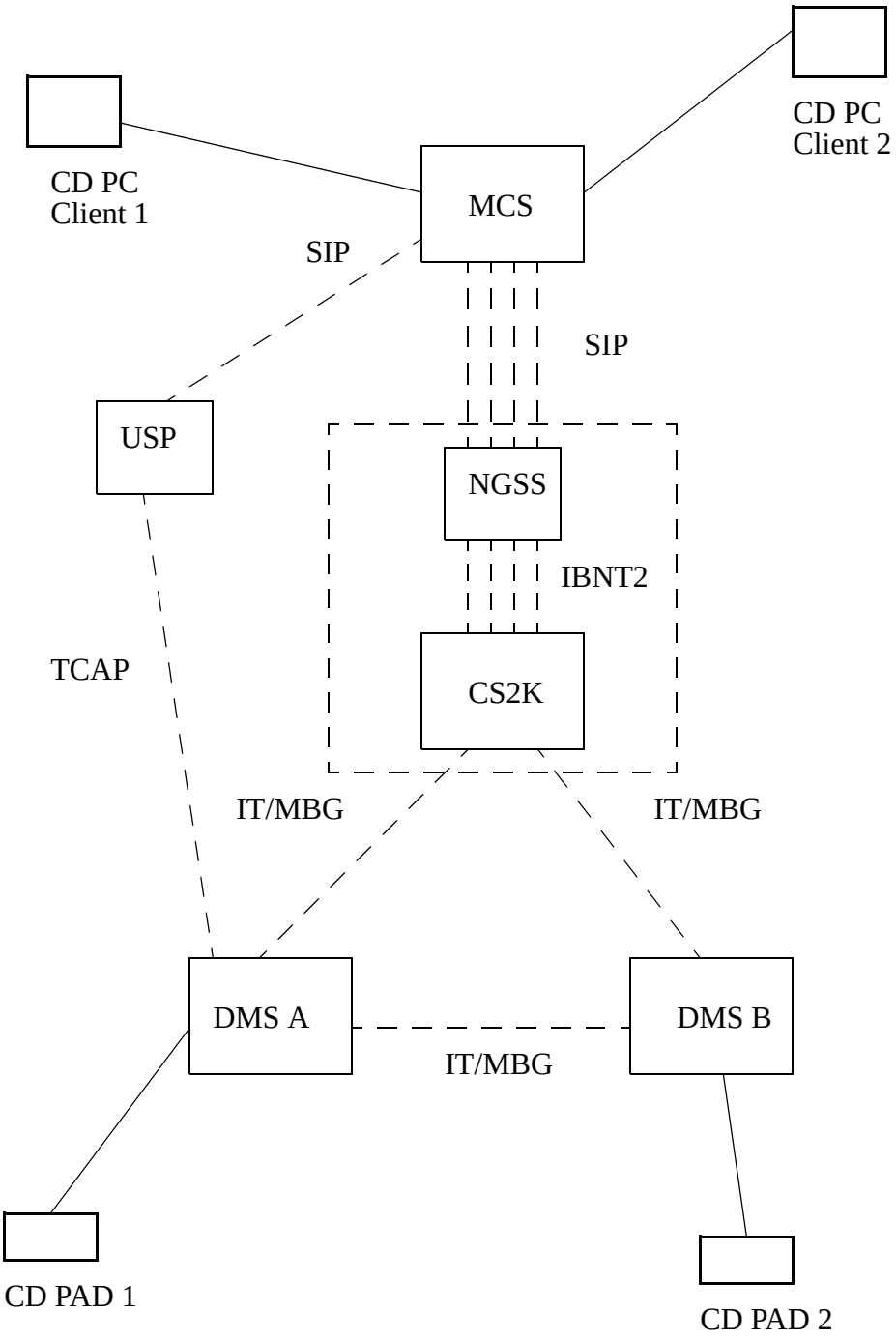


Figure 34 Converged Desktop Network Diagram

IT/MBG trunks are provisioned between DMS 100s and the CS2K to be shared among customer groups. MBG allows members of the same Centrex customer group to be known across different DMSs. IBNT2 SIP trunks are provisioned between the CS2K and the MCS, one dedicated per customer group.

The NGSS acts as the interface between the MCS and CS2K DPT trunking. The NGSS communicates using GCP protocol on the DPT trunks through a SIPT Gateway Controller. It communicates with the MCS using SIP. The IT/MBG trunks are ISUP trunks.

The USP provides an SS7 TCAP interface for the DMSs, and a SIP interface for the MCS.

CD User 1 has a CD PC Client and a CD PAD, as does CD User 2.

In the CD environment, there exists a number of complex call flows. Within these call flows, the Name and Number Displays on the CD PADS and on the CD PC Clients need to be consistent in terms of whether the Private or Public displays are used. If the two CD PADs are within the same Centrex business group, the Private Name and Number displays should be maintained.

An example of a complex call flow is given in the figure below.

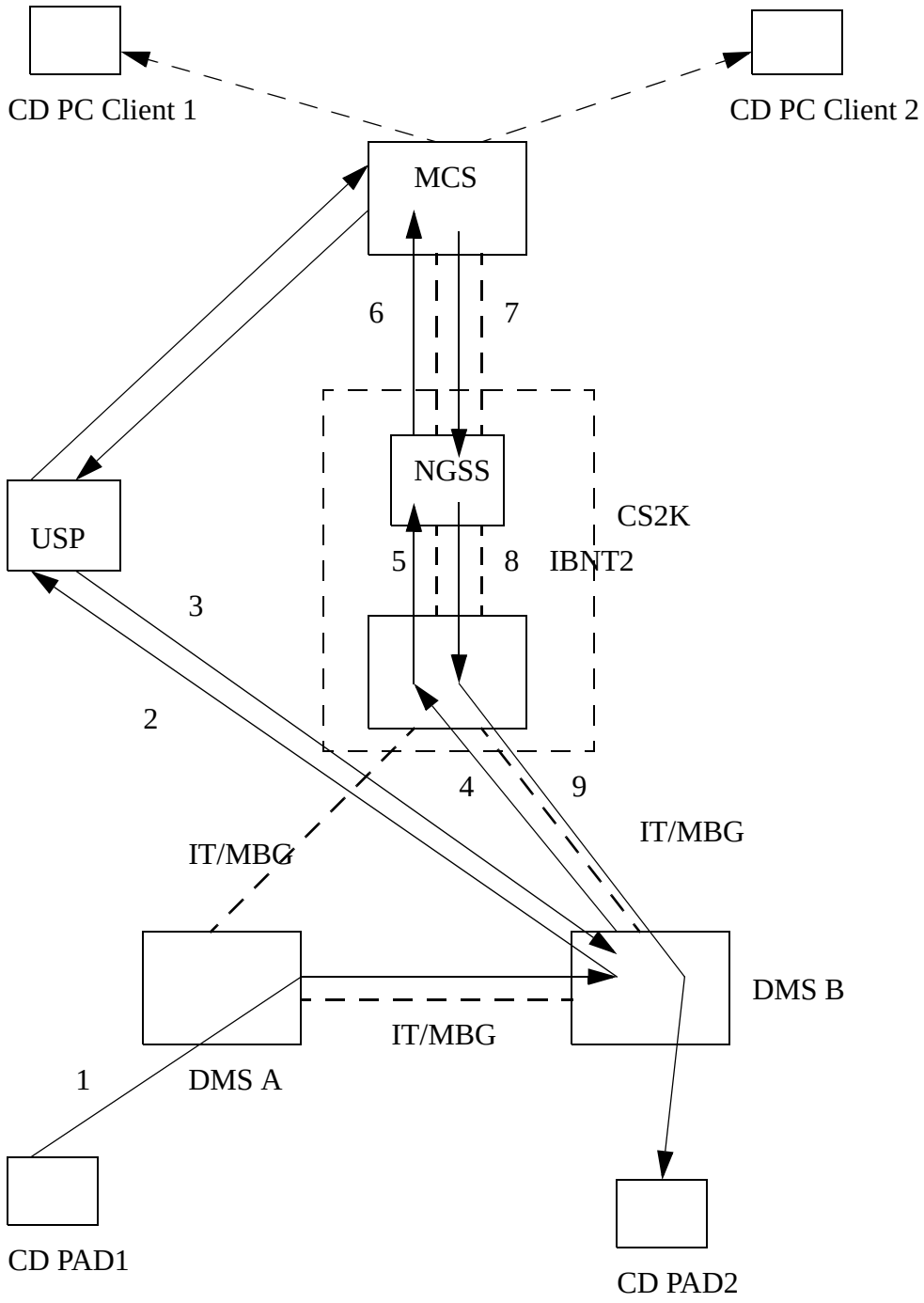


Figure 35 Converged Desktop System Call Flow

In this call, CD PAD1 and CD PAD2 are in the same Centrex group. The steps in the call flow are as follows:

In step 1, CD PAD1 calls CD PAD2. Since CD PAD2 is a converged desktop user, its Directory Number has a TAT trigger associated with it.

This causes step 2, where a TCAP query is generated to the USP, which in communicating with the MCS returns in step 3 the SDN (Converged Desktop Service Directory Number) associated with the Centrex business group of the called party. This is the SDN that the MCS has associated with the sub-domain of the called party. This tells the DMS to route the call to the SDN.

In step 4 the call is routed to the SDN for the business group over an IT/MBG trunk to the CS2K. The identity of the business group is maintained across the ISUP IT trunk by the MBG parameter. At the CS2K in step 5, the call is routed over a dedicated IBNT2 trunk for the business group. In this step, the ISUP call setup information is carried to the NGSS through the GCP protocol. The NGSS converts the call setup information to a SIP INVITE message to be sent to the MCS in step 6. The SIP INVITE message contains an X-Nortel-Profile header that associates the call with the specific business group.

The MCS performs the logic to update the status of the CD PC Client displays. In this call scenario, it is determined that CD User 2 has indicated through configuration that he wants the call to be routed to his telephone, CD PAD2.

In step 7, the MCS routes the call to the NGSS over the route associated with the business group. In step 8, the NGSS routes the call over the IBNT2 DPT trunk associated with the business group to the CS2K. In step 9, the CS2K routes the call over an IT/MBG trunk to DMS B, which, which after making another TAT trigger query to the USP terminates the call the call to CD PAD2.

Since in this scenario both CD users are in the same Centrex business group, the CD PAD2 display will use the Private Name and Numbers. The CD PC Clients displays will also be Private.

A similar call scenerio is shown below, but in this case the calling party is not in the Centrex business group.

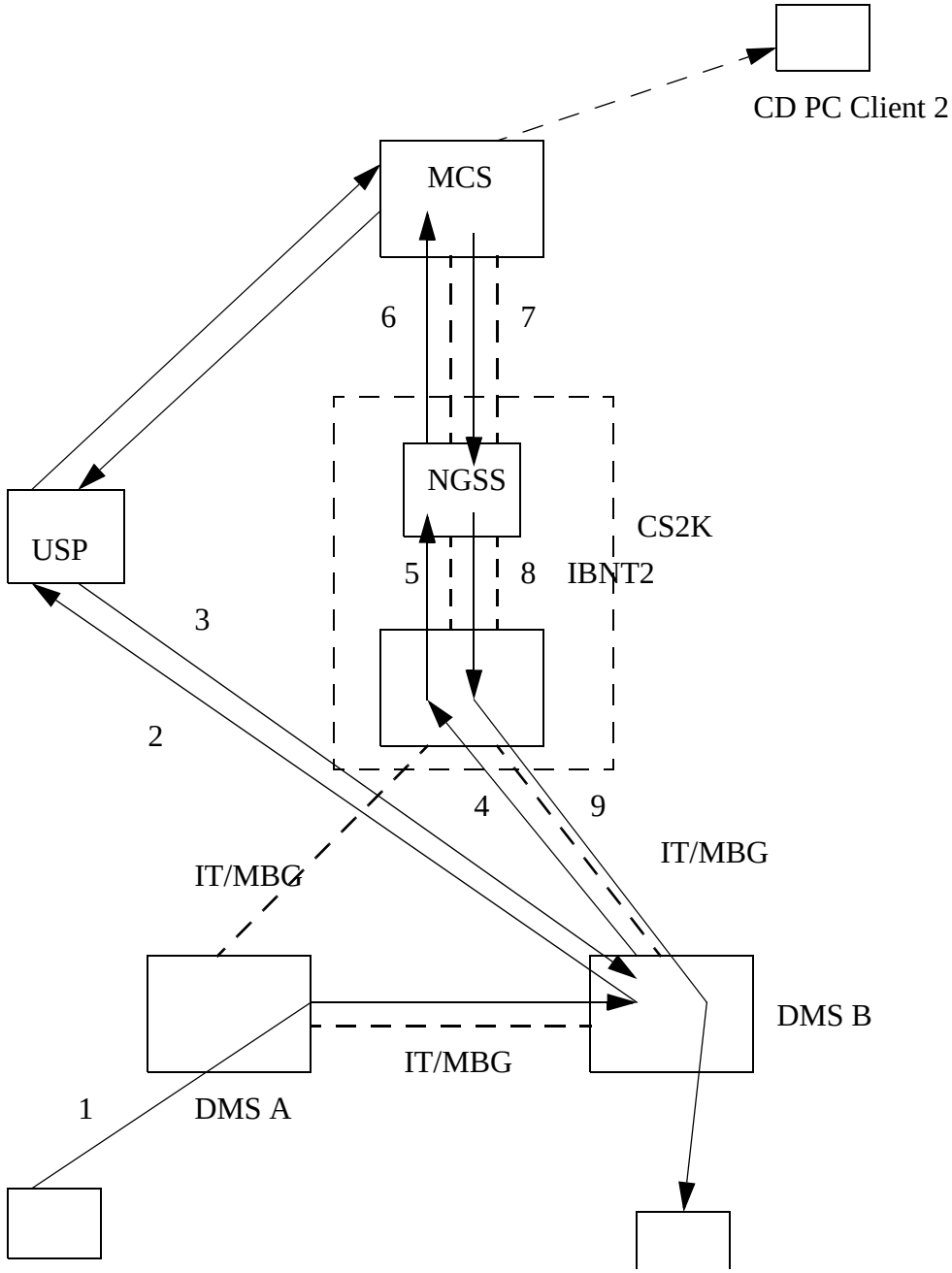


Figure 36 Call from PSTN User to Converged Desktop User

In this call scenario, a PSTN user calls a CD Centrex user; the CD PAD2 display will use the Public Name and Numbers. This display could be something like “PSTN”. The CD PC Client display will also indicate that the caller is outside the Centrex group.

A number of call scenarios exist between parties with at least one CD User involved. A summary of some of the expected display behavior in some of these call scenarios is given in the table below.

Table 2:

Calling Pary	Called Party	Calling PAD	Calling PC Client	Called PAD	Called PC Client
Centrex CD Phone	Centrex phone	dialed digits	No pop up window	Private	N/A
CD - from PC Client	Centrex phone	dialed digits	No pop up window	Private	N/A
CD- from Centrex phone	CD Centrex phone	dialed digits	SIP User ID	Private	SIP User ID
CD - from PC Client	CD Centrex phone	dialed digits	SIP User ID	Private	SIP User ID
Centrex	CD Centrex phone	dialed digits	N/A	Private	Private
CD - not in CD mode	Centrex phone	N/A	dialed digits	Private	SIP User ID
Centrex	CD - not in CD mode	dialed digits	N/A	Private	Private
PSTN	CD Centrex phone	dialged digits	N/A	Public	Public
CD - from Centrex phone	PSTN	dialed digits	N/A	Public	N/A
CD - from PC Client	PSTN	dialed digits	N/A	Public	N/A
CD - not in CD mode	PSTN	dialed digits	N/A	Public	N/A
CD Centrex	CD Centrex	dialed digits	SIP User ID	Private	SIP User ID
Centrex	CD Centrex	dialed digits	N/A	Private	Private
PSTN	CD Centrex	dialed digits	N/A	Public	Public

To support Private/Public Name and Number displays in calls that cross between the DMS Centrex group arena into the MCS SIP domain arena, a combination of translations, including utilization of MBG over IT trunks and provisioning of decicated IBNT2 trunks per Centrex group is used. Additionally, software changes are made on the MCS and the NGSS to map

ISUP NPI/NOA combinations to phone context information in SIP messages between the NGSS and the MCS.

81.2.5 Offer Answer SDP

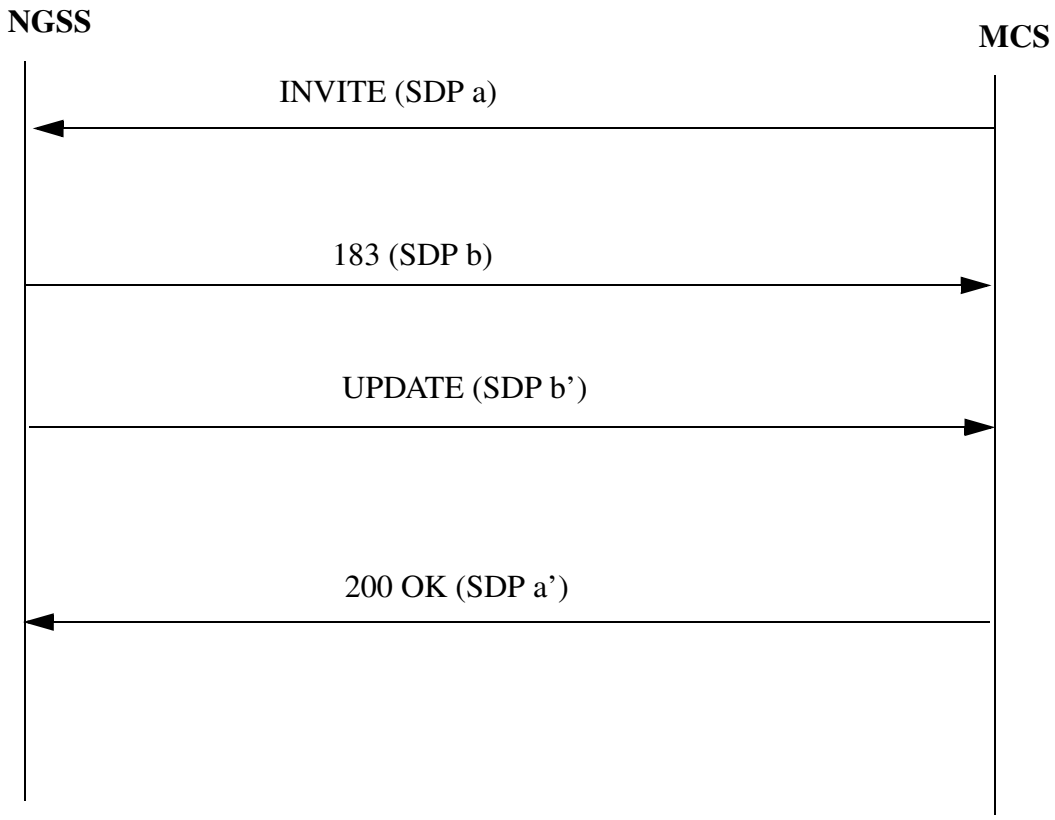
UPDATE method defined by RFC 3311 allows SIP entities to modify session attributes after initial offer answer has been exchanged. The session attributes can be modified before or after answer. Generally UPDATE is used to modify session attributes before answer as most SIP implementations use SIP re INVITE mechanism to modify session attributes after answer.

Currently NGSS sends UPDATE to modify session attributes before answer if the remote server configuration indicates that remote server supports UPDATE method. This is not the right means of deciding when to send UPDATE method. This activity improves on the design of when to send the UPDATE method as follows:

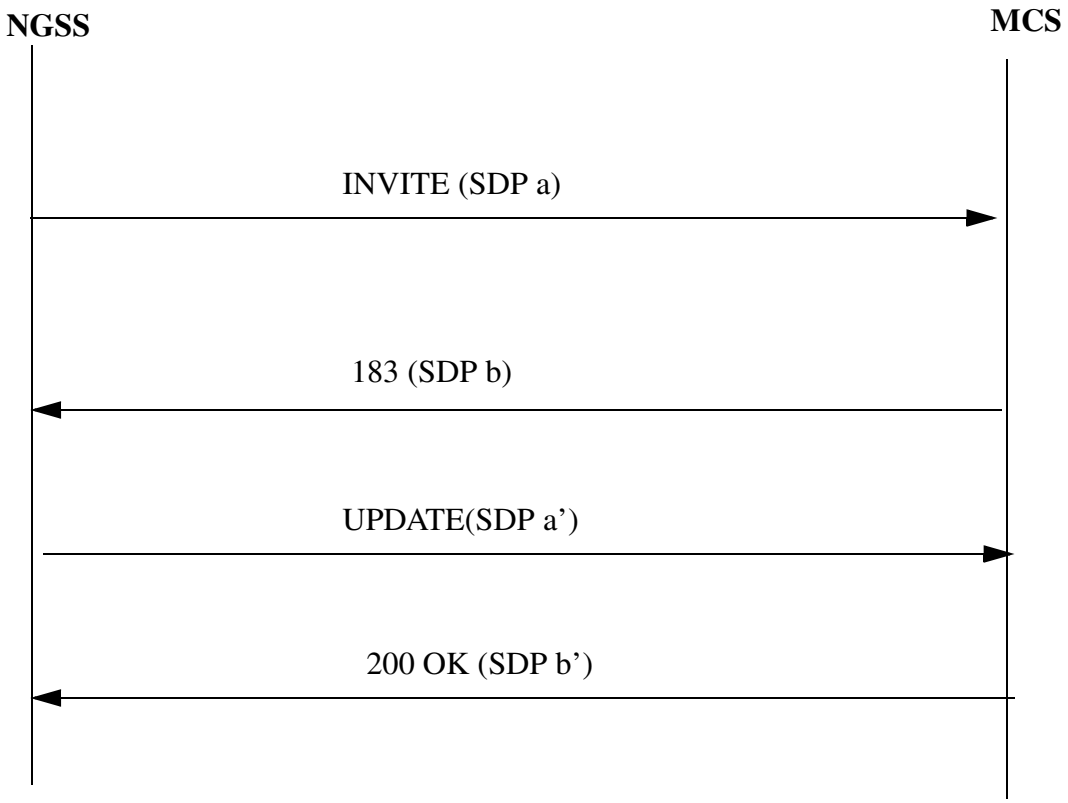
•The remote SIP node will basically indicate through means of Allow header when in a call UPDATE is allowed.
•NGSS will send UPDATE method when the remote server has indicated through messaging that UPDATE is allowed.
•NGSS will indicate that UPDATE method is allowed only after OFFER Answer SDP exchange has been completed.
•Due to backward compatibility with NGSSes prior to the SN09 release, that do not support UPDATE through messaging, UPDATE will still be supported through the GUI.

MCS uses the Allow header to indicate when UPDATE is allowed. NGSS will scan for Allow header for messages from the MCS and indicate in a call data block when UPDATE is allowed.

The call flow below indicates the interaction between the MCS and the CS2K on the usage of the UPDATE method.



a) UPDATE method accepted for processing by NGSS



b) UPDATE method sent out by the NGSS and accepted for processing by MCS

81.2.6 MCS Endpoints and Services

The following are the MCS endpoints and services that this feature will support.

81.2.6.1 MCS Endpoints

- MCS PC Client
- MCS i2002/i2004
- MCS PC Client Set
- RTP Media Portal
- AudioCodes Mediant 2000 SIP PRI Gateway
- Media Application Server
- Sipura IAD (Intergated Access Device)
- Ambit IAD (Intergated Access Device)
- Mediatrix PRI Gateway
- Rel 3.0 PC Client/Client Set

81.2.6.2 MCS Services

- Basic Call/incoming/G711
- Basic Call/outgoing/G711
- Basic Call/incoming/G729A
- Basic Call/outgoing/G729A
- Calling Number Delivery
- Calling Number Delivery Block
- Called Number Delivery
- Called Number Delivery Block
- Calling Name Delivery
- Calling Name Delivery Block
- Redirecting Name Delivery
- Redirection Name Delivery
- Original Called Number Delivery (OCdNo)
- CPL forking (Sim Ring)
- CPL Sequential Ringing
- Call Redirect
- Call Redirect Reason

- Call Reject With Reason
- Call Rejection on Unauthorized Request
- Call park against token
- Call park against user
- Call park auto retrieval
- Call retrieve against token
- Call retrieve against user
- Call Forwarding (CF)
- Call Forwarding Busy (CFB)
- Call Forwarding No Answer (CFNA)
- Call Forwarding Access Code (CFAC)
- Click to Call (C2C)
- Branding
- Hold/Retrieve (with Music On Hold)
- Hold/Retrieve (without Music On Hold)
- Ad-hoc Conferencing and Consultative Call Transfer
- Blind Call Transfer
- Meet-me Conference
- Call Park
- MCS Call Route Advancing
- Long Call Duration (MCS to CS2K)
- E911 (on CS2K)
- Message Waiting Indication (MWI)
- Call Pickup (CPU)
- Converged Desktop

81.2.7 CS2K Endpoints and Services

The following are the CS2K endpoints and services that this feature will support.

81.2.7.1 CS2K Endpoints

- IW-SPM (Interworking Spectrum Peripheral Module) with Legacy Lines
- Motorola CG4500 MTA (NCS)
- Arris TTM202/402 TTM (NCS)

- Mediatrix 1104/1124 (MGCP)
- Askey 4/12/30 port (MGCP)
- Ambit 1/16/32 port & MG1K (MGCP)
- Nuera gateway
- H.323 gateway
- CICM (Centrex IP Client Manager) gateway
- PVG (Passport Voice Gateway)

81.2.7.2 CS2K Services

- Basic Call/incoming/G711
- Basic Call/outgoing/G711
- Basic Call/incoming/G729A
- Basic Call/outgoing/G729A
- 3-Way Call (3WC)
- Message Waiting Indicator - Audible (MWT, STD sub-option only)
- Incoming MCS call to CS2K E911
- Call Forward
- Call Forward with Announcement
- (CFB) Call Forward Busy
- (CFD) Call Forward No Answer
- Call Forward of Call Waiting Calls
- (SCF) Selective Call Forward
- (CFU) Call Forwarding Universal
- Music On Hold (Call Hold)
- (CPK) Call Park
- (CPU) Call Pickup
- (CXR) Call Transfer
- (CWT) Call Waiting
- (CCW) Cancel Call Waiting
- 3 Party Conference
- Meet Me Conference
- (CNAMD) Calling Name Delivery
- (CNAB) Calling Name Delivery Blocking

- (CND) Calling Number Delivery
- (CNDB) Calling Number Delivery Blocking
- Called Number Delivery
- Called Number Delivery Block
- Redirecting Name Delivery
- Redirection Name Delivery
- Original Called Number Delivery (OCdNo)
- (MLH) Multi Line Hunt
- (NRAG) Network ring again
- (ARRDN) Automatic Recall Dialable Directory Number
- (AR) Automatic recall
- Long Duration (CS2K - MCS)
- AIN 0.1
- Delivery of Dialable Number (DDN)
- Warm Line
- CTX Automatic Dial
- IBS Last Number Redial
- IBS Call Forward D/A All Calls
- IBS Ring Again (Exec Ringback)
- IBS CTX Call Trace
- IBS Call Forward D/A Universal
- IBS Group Pick-up
- IBS Call Forward Busy Universal
- IBS Multiple Appearance Directory Number
- IBS CTX Public Name Display-Cms Set Only
- IBS Speed Call Short List
- IBS NCS Speed Call Short List
- IBS Message Waiting Line
- IBS Call Transfer with Recall
- IBS CTX Busy Lamp Field Key
- IBS Std Madn Sca Appearance
- IBS CTX Call Display 1501+ Lines ???

- IBS CTX Call Display 1-29 Lines ???
- Secondary Number on Ebs
- IBS Auto Route Sel-Per Line
- IBS CTX Call Display 501-1500 Lines ???
- NCS Call Display Over 1000 Activations ???
- IBS CTX Call Display 101-500 Lines ???
- NCS Visual M/W Ind On S/L Sets
- IBS Std Speed Call Long List
- IBS Acd Agent Incalls Key
- IBS Std Madn Mca Appearance
- NCS Call Display 1-500 Activations ???
- IBS CTX Perimeter Acd Mis Serv Bur Agent
- IBS CTX Enhance Ans Position
- IBS CTX Auto Call Back and Auto Recall
- NCS Madn 1-500 Activations ???
- CTX Ident-A-Call
- IBS Acd Queue Listed Number
- IBS CTX Network Acd (per Agent)
- CTX Distinctive Ringing Per Line Option
- Distinctive Ringing Enhanced Additional
- NCS Sp Call Long 1-500 Activations ???
- IBS CTX 1-100 Lines Visual Call Waiting
- IBS CTX Perimeter Acd Mis Serv Bur Que
- IBS UCD Listed Number 5 Yr
- IBS Custom Announcement In Co
- IBS UCD Listed Number
- Music External Source (Customer Premise)

81.3 Hardware Requirements or Dependencies

81.4 Software Requirements or Dependencies

81.5 Limitations and restrictions

SN09 CS2K Interworking with MCS 4.0 is not supported.

VRDN architecture will not be supported on SN09 CS2K.

81.6 Interactions

81.7 Glossary

Term	Description
New term	Definition

82: Functional Description(FN): A00009515

82.1 Feature name and Feature ID

A00009515: Out-of-Band Interop with MCS

82.2 Description

This activity will implement the support for Out of Band (OOB) SIP REFER signaling on the Session Server (formally known as NGSS).

REFER is a SIP method, which requests that the recipient REFER to a source provided in the request. It provides a mechanism allowing a party sending the REFER to be notified of the outcome of the referenced request. This can be used to enable many applications, including Click-to-Call.

A REFER placed outside the scope of the dialog created with an INVITE is called and an Out of Band REFER.

Out of Band SIP REFER support will address the following limitations with the current implementation of the MCS application Click-to-Call (C2C)

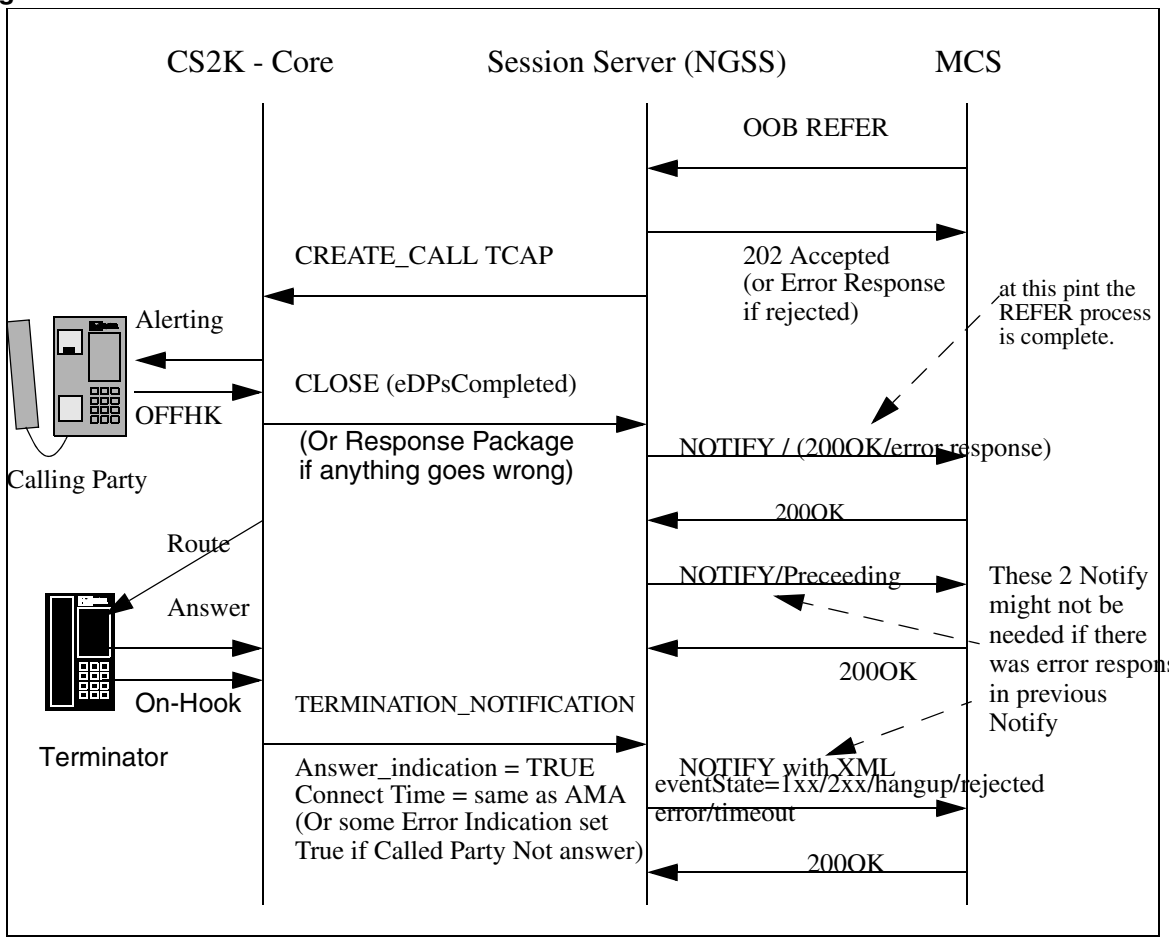
- The originator of the C2C ends up in the Termination Call MOdel (TCM) of the CS2K.
- Originating Call Manager (OCM) services and its feature interactions are bypassed (e.g. auth codes, acct codes, Denied Originations, PIC and other translation related services)
- Unnecessary TCM interactions on the originator of the C2C (like forwarding services.
- OCM updated incorrectly results in Incoming Call Memory (ICM) not being updated correctly, thus some features don’t function as designed.
- Since there are 2 distinct trunk-to-line calls with their media tied to MCS, this can cause issues around ring back and possibly tones, busy signal, even treatments not being heard by the originator. (The originator of the MCS call is already answered so the ringback request from the terminator is not propagated to the real originator).

- Billing is not captured correctly, since the call comes to the caller as an incoming terminating call rather than outgoing originating call.

82.2.1 Click-toCall flow using the new OOB REFER functionality

Following is a flow that illustrated the operation of C2C using the OOB REFER implementation as shown in Figure 1.

Figure 1 Click To Call Call Flow



1. Client invokes C2C on the MCS

2. MCS sends a OOB REFER msg to the Session Server. The REFER contains the following information which will be used in CreateCall NCAS message parameters:

- Mandatory Parameter - CallingPartyId (ReferBy): The DN of party A which is the logical originator who will be referred to Party B. CallingPartyId must be 10 digits
- Mandatory Parameter-CalledPartyId (ReferTo)
- Optional Parameter - ChargeNumber (ReferBy)

3. Session Server receives the OOB REFER request. It parses it and verifies that the REFER is NOT associated with any existing call context and thus it is an OOB REFER. Remote Server validation (provisioning data) is also performed at this point.

4. If the OOB REFER is accepted (i.e. passed the validation and authentication), the Session Server will send a 202 Response to the MCS. The Session Server responding to a REFER method will return a 400 (Bad Request) if the request contained zero or more than one Refer-To header field values.

5. NGSS then maps the REFER request to a create-call TCAP message with a Send_Notification attachment and sends it to the CS2K core via a NCAS link. For detailed description of NCAS link please see the documentation for the NA09 Activity A00007544.

The TCAP create-call is processed in the core as implemented for AIN under NA013 Activity A59011901.

6. A Create Call request is accepted by an analog user going off hook. It is rejected by the user not responding to the notification before a Create Call Timer (TCC) expires.Or if Create Call message has fatal protocol error; Create Call has invalid information in the parameters; Calling Party busy; SOC option is idle, etc., Session Server would receive some response back with cause reason. In this case, a NOTIFY message with appropriate payload content is sent to MCS OOB REFER process is over. Here is example NOTIFY with 503 service unavailable in the payload. Refer to the following table for the mapping between response of Create Call to SIP messages.

Table 1: Create Call response message to SIP response mapping

	Create-Call Response	**Mapping to SIP**
Termination_Notification	Answer_Indication	200OK
Termination_Notification	Busy_Indication: Destination Out of Order	502 Bad GAteway
Termination_Notification	Busy_Indication: User Busy	486 Busy Here
Termination_Notification	Busy_Indication: No Route to Destination	503 Service Unavailable
Termination_Notification	Busy_Indication: No Circuit Available	503 Service Unavailable

	Create-Call Response	Mapping to SIP
Response Package	Protocol Error: Missing Mandatory Parm	400 Bad Request
Response Package	Report Failure: CallingInterfaceBusy	486 Busy Here
Response Package	Report Failure: InappropriateUserInterface	484 Address Incomplete (if Calling Party is invalid) 503 Service Unavailable (if bearer compatibility)
Response Package	Report Failure: ResourceUnavailable	503 Service Unavailable
Response Package	Application Error: Missing Conditional Parm	503 Service Unavailable
Response Package	Application Error: Unexpected Communication	503 Service Unavailable
Response Package	Report Failure: RateTooHigh	503 Service Unavailable

7. When the core detects the user going off hook, it sends a CLOSE message to the Session Server with the cause value of eDPsCompleted and proceeds to route the call to the CalledPartyId.

8. Session Server decodes the CLOSE TCAP message. A NOTIFY/ 200OK msg is sent to the MCS indicating that the OOB REFER process is now complete. Subscription/context are closed at this point. Example of the NOTIFY msg being sent to the MCS and the 200OK response is as follows:

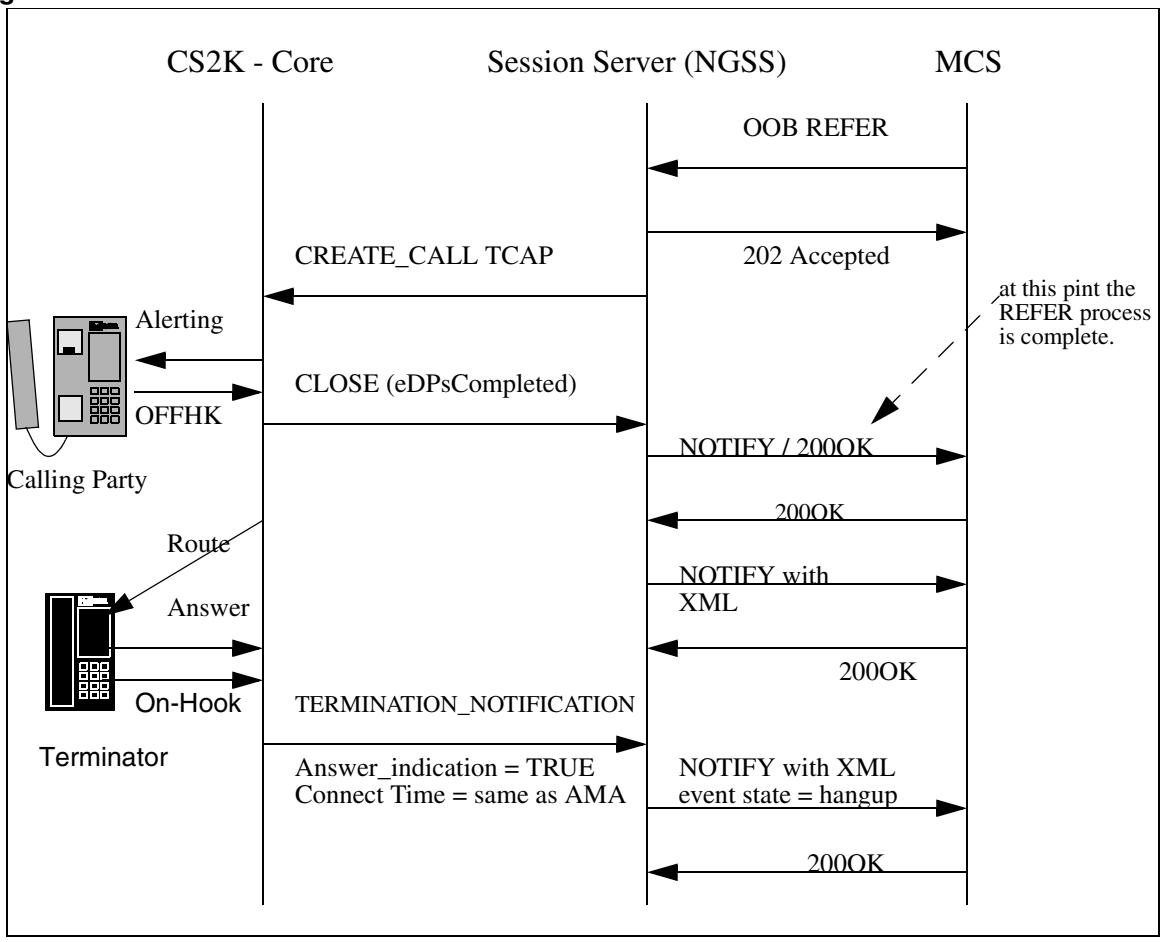
9. Once the 200OK is received by the Session Server another NOTIFY msg, this time with an XML event package, will be sent to the MCS to indicate that the call is proceeding. The Call-ID in this NOTIFY msg will be the same as in all the prior messages.

10. When the call returns to the NULL PIC, the core will send a Termination Notification msg to the Session Server with an appropriate termination indicator. If the call was answered by the Called Party the termination indicator would have Answer_Indication set to TRUE (Called Party has answered the call) and the connect time equal to the elapsed time of the call (same as the AMA record).

11. Once the Termination Notification message is received, Session Server will send the final NOTIFY to the MCS indicating that the call has been completed. In the event that the Answer_Indication is set to TRUE that notify msg will contain an events package indicating the event state of hangup.

82.2.1.1 Successful OOB Refer Message Flow

Figure 2 Successful OOB REFER Scenario



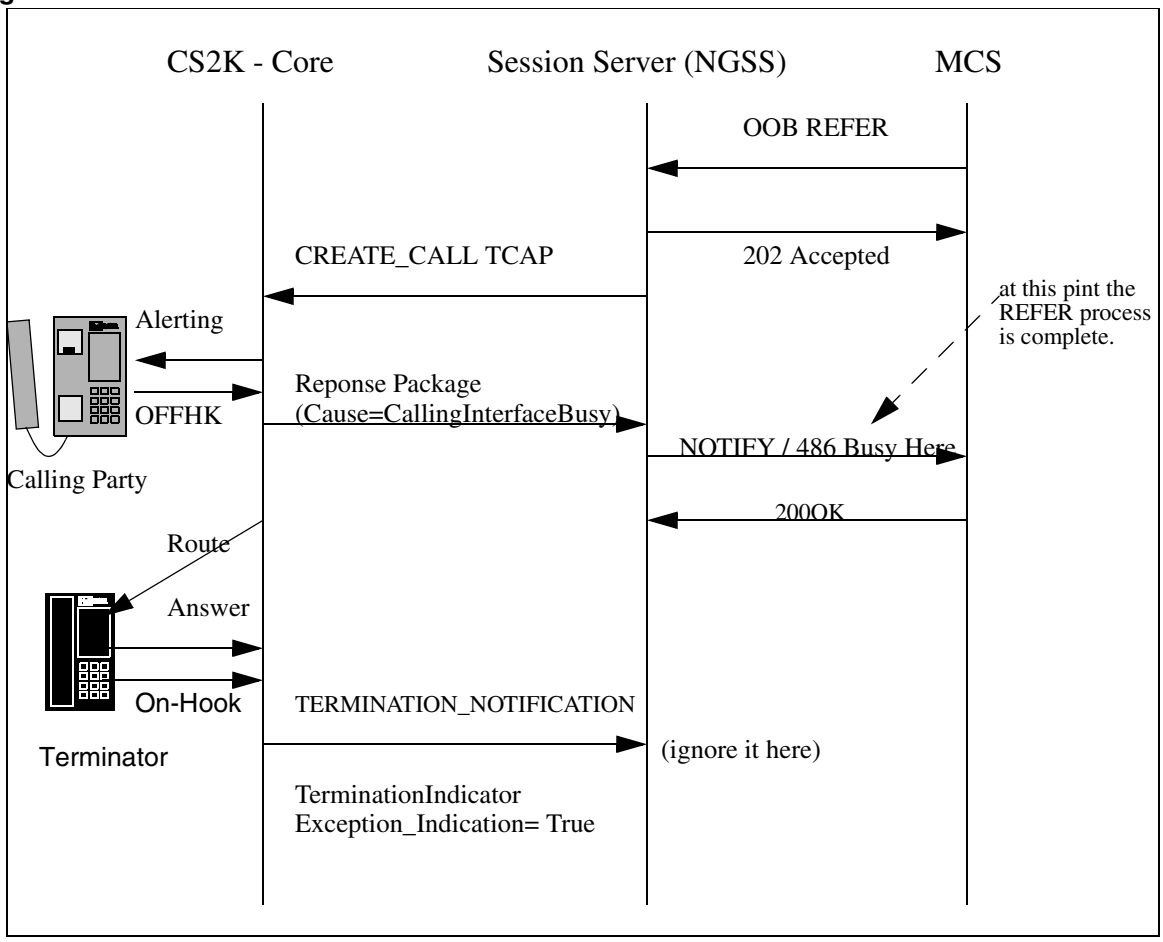

```
REFER sip:2149971908@47.104.26.49;user=phone SIP/2.0
t: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
f: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
i: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 53471 REFER
v: SIP/2.0/UDP 47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
Max-Forwards: 19
x-nt-corr-id: fd2f534f3c96dab16e70a70d1a2210b69f9f3@47.104.26.14
Allow: REFER,UPDATE
r: <sip:2149971914@cdcarrier.com;nt_service=c2c;privacy=id>
b: sip:2149971908@cdcarrier.com;
CorrelationID="fd2f534f3c96dab16e70a70d1a2210b69f9f3@47.104.26.14"
k: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
User-Agent: Nortel WCM 3.0.4.368
l: 0

SIP/2.0 202 Accepted
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
From: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
```

```
CSeq: 53471 REFER
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:rega1908@cdcarrier.com SIP/2.0
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
From: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 9999 NOTIFY
Max-Forwards: 70
Event: refer
Subscription-State: terminated;reason=noresource
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Type: message/sipfrag;version=2.0
Content-Length: 16

SIP/2.0 200 OK

SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
From: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 9999 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:convergeddesktop@cdcarrier.com SIP/2.0
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
From: <sip:convergeddesktop@cdcarrier.com>
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10000 NOTIFY
Max-Forwards: 70
EVENT: dialog
Content-Type: application/dialog-info+xml
Content-Length: 408

<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="4"
state="partial" entity="2149971914@cdcarrier.com">
     <dialog id="1" direction="initiator">
          <state event="1xx-notag">proceeding</state>
          <local-uri>sip:2149971908@cdcarrier.com;nt_service=c2c</local-uri>
          <remote-uri>sip:2149971914@cdcarrier.com</remote-uri>
     </dialog>
</dialog-info>

SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
From: <sip:convergeddesktop@cdcarrier.com>
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10000 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:convergeddesktop@cdcarrier.com SIP/2.0
t: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
```

```
f: <sip:convergeddesktop@cdcarrier.com>
i: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10001 NOTIFY
v: SIP/2.0/UDP 47.104.26.14:5060;branch=z9hG4bK0dce5e29aa278e1706738dc4eb313c1c
Max-Forwards: 20
EVENT: Dialog
k: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
l: 408
c: application/dialog-info+xml
<?xml version="1.0"?>

<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="4"
state="partial" entity="2149971914@cdcarrier.com">
     <dialog id="1" direction="initiator">
          <state event="hangup">terminated</state>
          <local-uri>sip:2149971908@cdcarrier.com;nt_service=c2c</local-uri>
          <remote-uri>sip:2149971914@cdcarrier.com</remote-uri>
     </dialog>
</dialog-info>

SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
From: <sip:convergeddesktop@cdcarrier.com>
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10000 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0
```

82.2.1.2 Calling Party User Busy Message Flow

Figure 3 Unsuccessful OOB REFER Scenario

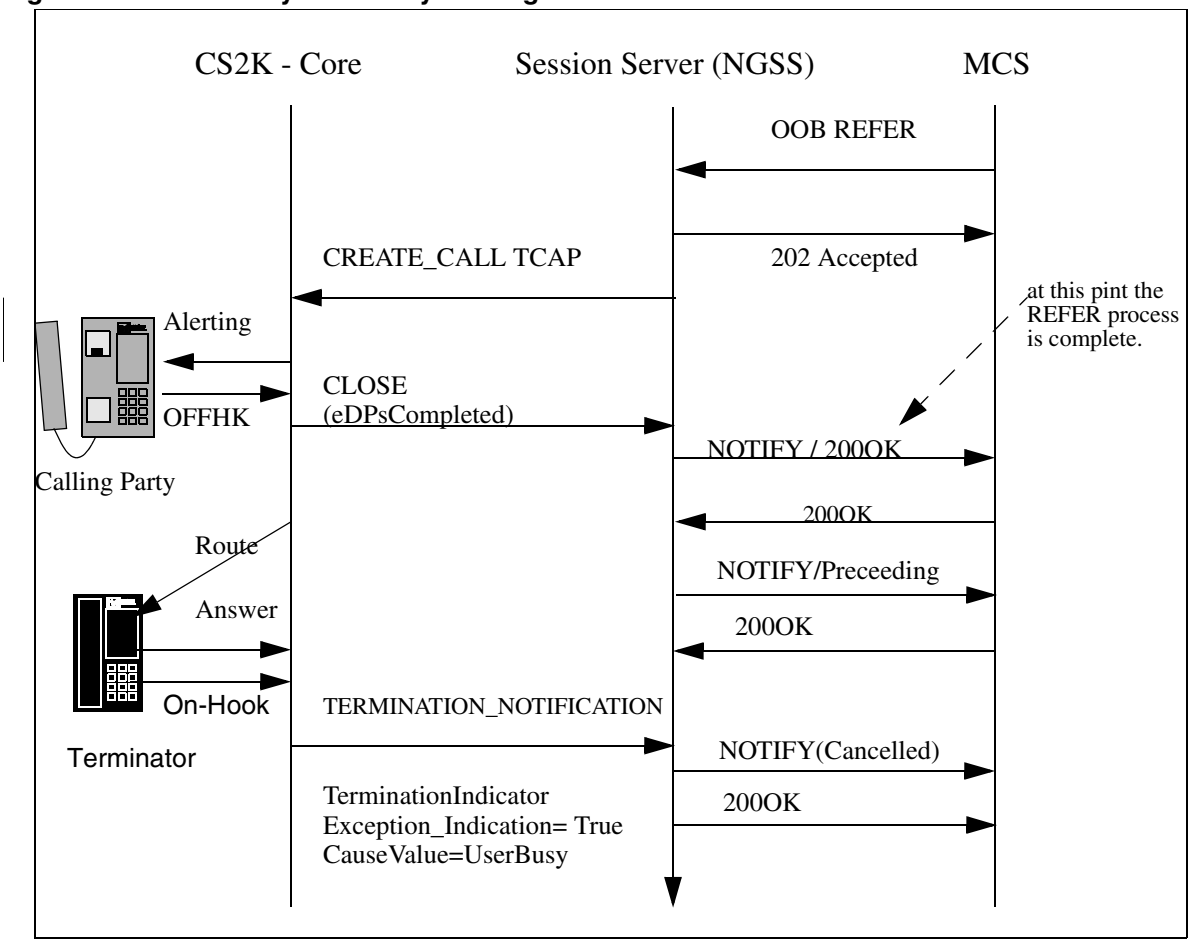



```
REFER sip:2149971908@47.104.26.49;user=phone SIP/2.0
t: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
f: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
i: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 53471 REFER
v: SIP/2.0/UDP 47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
Max-Forwards: 19
x-nt-corr-id: fd2f534f3c96dab16e70a70d1a2210b69f9f3@47.104.26.14
Allow: REFER,UPDATE
r: <sip:2149971914@cdcarrier.com;nt_service=c2c;privacy=id>
b: sip:2149971908@cdcarrier.com;
CorrelationID="fd2f534f3c96dab16e70a70d1a2210b69f9f3@47.104.26.14"
k: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
User-Agent: Nortel WCM 3.0.4.368
l: 0

SIP/2.0 202 Accepted
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
From: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
```

```
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 53471 REFER
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:rega1908@cdcarrier.com SIP/2.0
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
From: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 9999 NOTIFY
Max-Forwards: 70
Event: refer
Subscription-State: terminated;reason=noresource
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Type: message/sipfrag;version=2.0
Content-Length: 16

SIP/2.0 486 Busy Here



SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
From: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 9999 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0
```

82.2.1.3 Called Party User Busy Message Flow

Figure 4 Called Party User Busy Message Flow



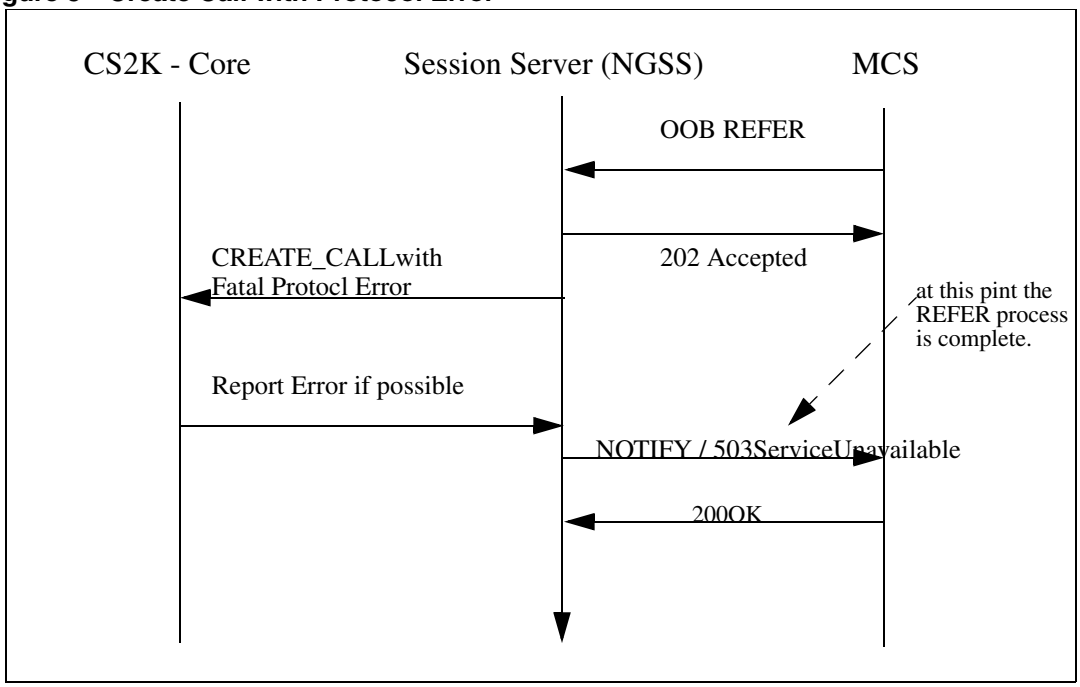

```
REFER sip:2149971908@47.104.26.49;user=phone SIP/2.0
t: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
f: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
i: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 53471 REFER
v: SIP/2.0/UDP 47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
Max-Forwards: 19
x-nt-corr-id: fd2f534f3c96dab16e70a70d1a2210b69f9f3@47.104.26.14
Allow: REFER,UPDATE
r: <sip:2149971914@cdcarrier.com;nt_service=c2c;privacy=id>
b: sip:2149971908@cdcarrier.com;
CorrelationID="fd2f534f3c96dab16e70a70d1a2210b69f9f3@47.104.26.14"
k: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
User-Agent: Nortel WCM 3.0.4.368
l: 0

SIP/2.0 202 Accepted
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
From: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
```

```
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 53471 REFER
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:rega1908@cdcarrier.com SIP/2.0
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
From: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 9999 NOTIFY
Max-Forwards: 70
Event: refer
Subscription-State: terminated;reason=noresource
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Type: message/sipfrag;version=2.0
Content-Length: 16

SIP/2.0 200 OK

SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
From: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 9999 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:convergeddesktop@cdcarrier.com SIP/2.0
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
From: <sip:convergeddesktop@cdcarrier.com>
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10000 NOTIFY
Max-Forwards: 70
EVENT: dialog
Content-Type: application/dialog-info+xml
Content-Length: 408

<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="4"
state="partial" entity="2149971914@cdcarrier.com">
     <dialog id="1" direction="initiator">
          <state event="1xx-notag">proceeding</state>
          <local-uri>sip:2149971908@cdcarrier.com;nt_service=c2c</local-uri>
          <remote-uri>sip:2149971914@cdcarrier.com</remote-uri>
     </dialog>
</dialog-info>

SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
From: <sip:convergeddesktop@cdcarrier.com>
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10000 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:convergeddesktop@cdcarrier.com SIP/2.0
```

```
t: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
f: <sip:convergeddesktop@cdcarrier.com>
i: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10001 NOTIFY
v: SIP/2.0/UDP 47.104.26.14:5060;branch=z9hG4bK0dce5e29aa278e1706738dc4eb313c1c
Max-Forwards: 20
EVENT: Dialog
k: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
l: 408
c: application/dialog-info+xml
<?xml version="1.0"?>

<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="4"
state="partial" entity="2149971914@cdcarrier.com">
     <dialog id="1" direction="initiator">
          <state event="Rejected">terminated</state>
          <local-uri>sip:2149971908@cdcarrier.com;nt_service=c2c</local-uri>
          <remote-uri>sip:2149971914@cdcarrier.com</remote-uri>
     </dialog>
</dialog-info>

SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
From: <sip:convergeddesktop@cdcarrier.com>
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10000 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0
```

82.2.1.4 Create Call with Protocol Error

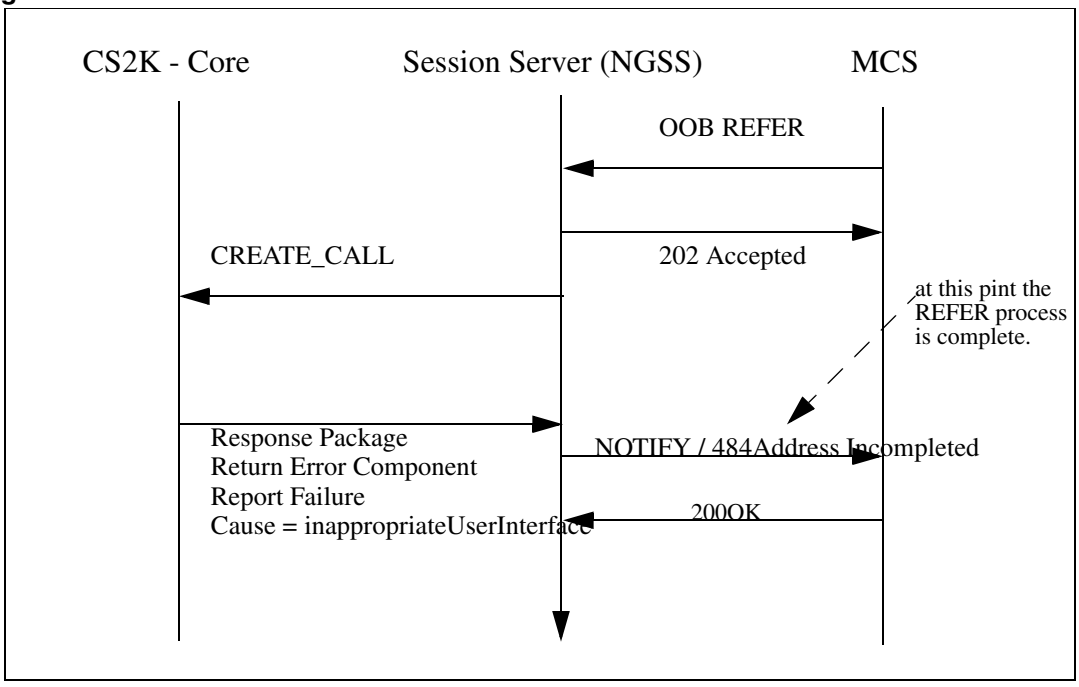
Figure 5 Create Call with Protocol Error



If a Create Call message contains a Protocol error, then it will be reported to the SCP if appropiate. NGSS will send final Notification to MCS with 503 Service Unavailable.

82.2.1.5 Create Call with Invalid Calling Party ID

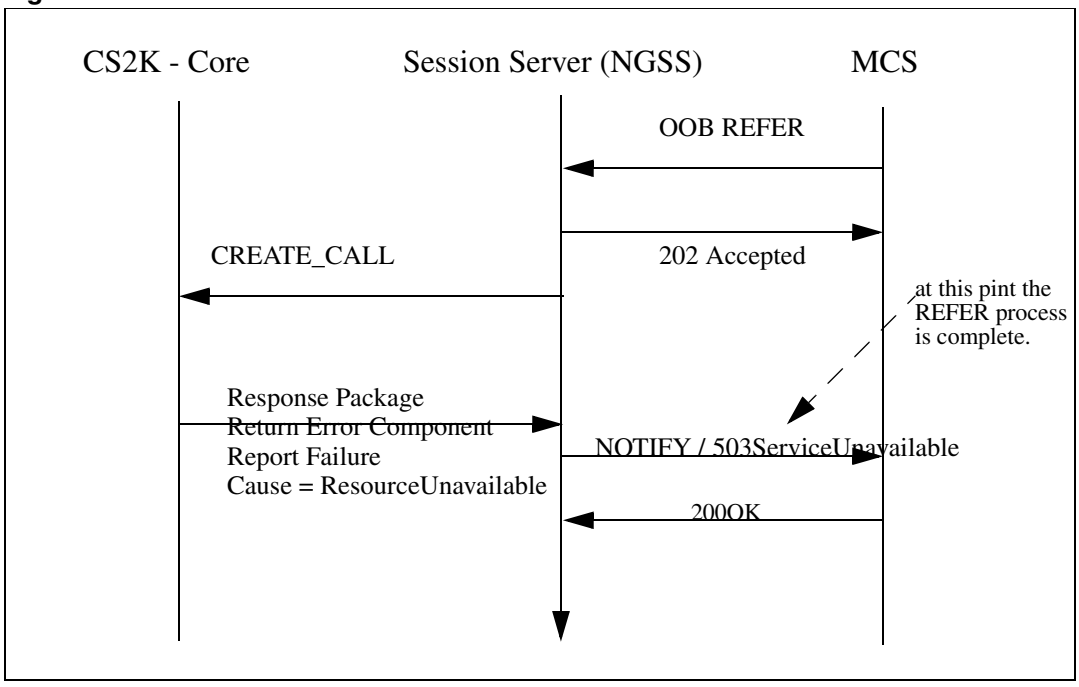
Figure 6 Create Call with Protocol Error



If a Create Call message contains a Protocol error, then it will be reported to the SCP if appropiate. NGSS will send final Notification to MCS with 484 Address Incompleted if it is Calling Party Invalid, or Notify with 503 Service Unavailable if it is invalid Bearer capability.

82.2.1.6 Create Call with Network Resource Unavailable

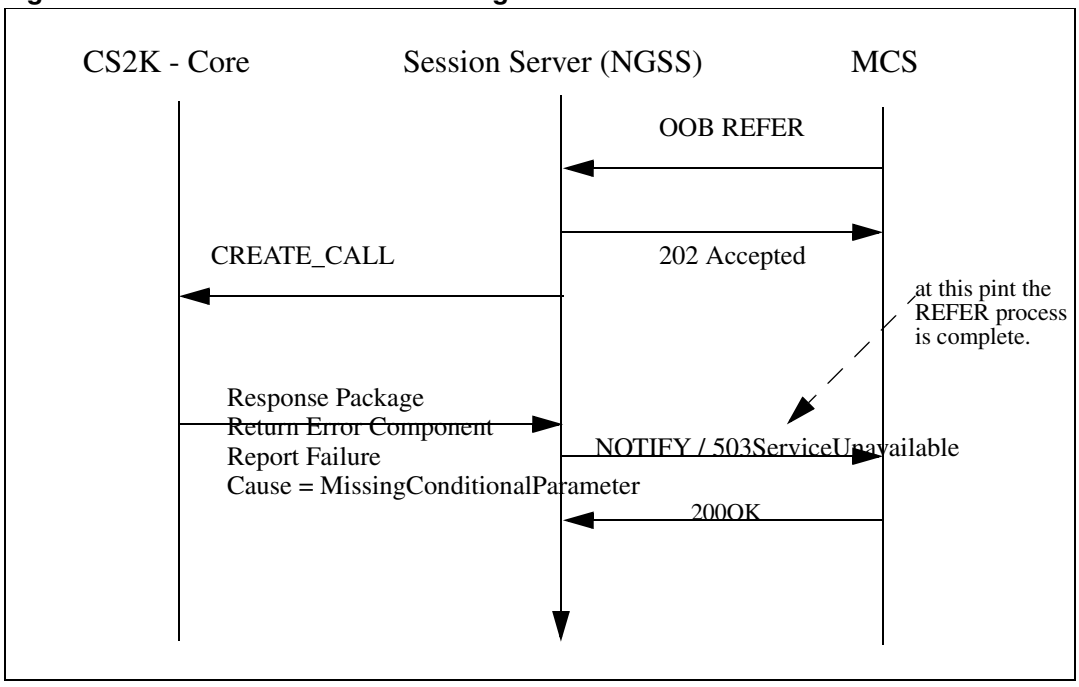
Figure 7 Create Call with Network Resource Unavailable



If Response Package returns failure as Resource Unavailable, NGSS would send final Notify message with 503 Service Unavailable to MCS.

82.2.1.7 Create Call with Fatal Missing Conditional Parameter

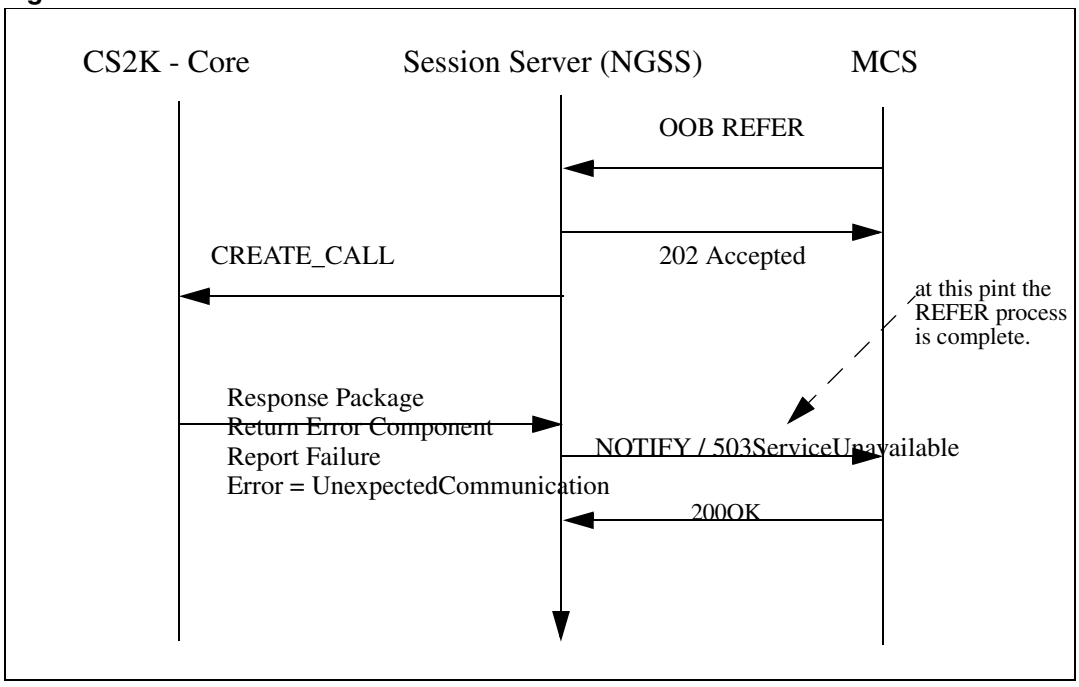
Figure 8 Create Call with Fatal Missing Conditional Parameter



If a Create Call message is determined to be missing an Optional parameter which is required then it is reported to the NGSS as a fatal Application Error with error as MissingConditionalParameter. NGSS then would send final Notify message with 503 Service Unavailable to MCS.

82.2.1.8 Create Call when SOC AIN00271 is IDLE

Figure 9 Create Call when SOC is IDLE



If a Create Call message is received when the SOC Option AIN00271 is IDLE then an Application Error with Error Cause set to Unexpected Communication is sent to NGSS. NGSS then would send final Notify message with 503 Service Unavailable to MCS.

82.3 Hardware Requirements or Dependencies

This feature doesn't introduce any new hardware requirements or dependencies

82.4 Software Requirements or Dependencies

Create Call must be enabled by SOC code AIN00271.

82.5 Limitations and restrictions

Following are the restrictions and limitations that apply to this feature;

- SIP Lines are not supported.

- NGSS standalone configuration, where the NGSS functions as converter from OOB REFER and TCP and the core is not running succession software and thus is not supported.
- List of agents not supported by this feature can be found in section 2.6.6 “Agent Support for Create Call”
- OFF Hook Delay Trigger (part of Info_Collected TDP) is not supported. See section 2.6.5. Interaction with AIN Triggers.
- TCAP messages from the CS2K to the Session Server can be lost during various maintenance actions (restarts, swacts.) which in turn could cause the Call Log on the MCS not to be updated correctly.

82.6 Interactions/Interworking

82.6.1 Feature Interactions with the Originator (CallingParty)

82.6.1.1 Originating Restriction Features

When the originator has one of the following call originating restrictions, the **Create Call request is rejected** by sending the NGSS a Failure message with failureCause=inappropriateCallingInterface:

DOR (denied Origination)

SUS/RSUS (suspended/requested suspension)

In addition to the above originating restriction features, the following originators also result in failing the Create Call request (a Failure message with failureCause=inappropriateCallingInterface is sent to the SCP):

Hotline Features AUL (automatic line), and MAN (Manual Line)

A line with the ESL (Emergency Service Line) option

one of the following MADN groups:

MADN SCA (Single Call Arrangement)

MADN MCA (Multiple Call Arrangement)

MADN EXB (Extension Bridge)

MADN CACH

ACD

UCD

MeetMe Conference

Non Resident DN

A line with BC (Bearer Capability) option with values other than SPEECH or 3_1KHZ.

When the originator has one of these features active, it is considered interface busy thus no alerting is provided to the originator:

all variants of Call Waiting, including TCW (Talking Call Waiting)

all variants of Hold

82.6.1.2 Terminating Features on the Originator

When alerting the originator, terminating features **are not activated** since the alerting is a treatment that applied to the originator indicating the Create Call request, not a call that is terminating on the originator. These terminating features include:

- All variants of Call Forwarding
- SCMP (Series CoMPletion)
- Termination Restrictions like DIN (Denied Incoming), DTM (Denied Terminating), DND (Do Not Disturb), MBK (Make Busy Key), MSB (Make Set Busy), MSBI (Make Set Busy Intragroup), PLP (PLug uP), SUS/RSUS (suspended/requested suspension) and RMB (Random Make Busy).
- EBCR (Enhance Busy Call Return)
- Intercept Feature like FLEXI (Flexible Intercept)
- Messaging Features like CSMI (Call Screening/Monitoring Intercept), EMW (Executive Message Waiting), FTS (FAX-Thru Service), ISA (In-Session Activation), SCM (Selective Call Messaging), SDS (Special Delivery Service), SODS (Special Offering Decoupling of SDS), MWT (station Message WaiTing) and UVM (universal Voice Messaging).
- Call Message Feature for RES
- Call Pickup

- Hunting Features (a member of a hunt group as the originator is alerted for the Create Call request if not busy, however, if it is busy, no hunting is done and the case is handled as the originator being busy.)
- Hunt Group Overflow Routing like LOD (Line Overflow to DN) and LOR (Line Overflow to Route)
- DLCM (Dual Line Call Management)
- SimRing (Res Simultaneous Ringing)
- ACRJ (Anonymous Caller ReJection)
- SCA (Selective Call Acceptance)
- SCRJ (Selective Call ReJection)
- SCF (Selective Call Forwarding)

82.6.1.3 Account Codes

Attempt to activate Account Codes (First or Last flavours) features prior to Called Party answers are denied. That is, if a Create Call is requested to originate from a line that requires Account Code, the Account Code is bypassed and the call is routed to the Called Party without the input of the Account Code.

The Account Code Voluntary feature shall be permitted to activate after flashing during an active call established through the Create Call functionality.

Note: Warning! It is assumed that the SCP/Adjunct is a "Trusted Node" and has authenticated the user request for Create Call functionality. The SCP/Adjunct provides Account Code data collection capabilities if the Service Provider deems them necessary.

82.6.1.4 Authorization Codes

Attempt to activate Authorization Codes (First or Last flavours) features prior to Called Party answers are denied. That is, if a
Create Call is requested to originate from a line that requires Authorization Code, the Authorization Code is bypassed and the call is routed to the Called Party without the input of the Authorization Code.

The Authorization Code Voluntary feature shall be permitted to activate after flashing during an active call established through the Create Call functionality.

Note: Warning! It is assumed that the SCP/Adjunct is a "Trusted Node" and has authenticated the user request for Create Call functionality. The SCP/Adjunct provides Account Code data collection capabilities if the Service Provider deems them necessary.

82.6.1.5 Authorization Code Immediate Dialing (ACID)

The ACID feature removes the seven second pause between the input of authorization codes and second dial tone. When an IBN subscriber dials a correct authorization code, including the correct security digits, the ACID feature assumes that no more authorization code digits are to be dialed. It then proceeds immediately to the next stage of call processing without waiting for an octothorpe (#) or interdigit time-out.

The interactions with this feature is the same as Create Call interactions with Authorization Codes.

82.6.1.6 Station Specific Authorization Codes (SSAC)

SSAC has the same interactions as authorization codes.

82.6.1.7 CRL (Code Restrictions)

Any DN that is blocked for the customer group through CRL is not blocked when a call is routed to that DN by the Create Call functionality.

82.6.1.8 SOR (Station Origination Restrictions)

The SOR feature determines whether the call should be restricted. SOR restrictions fall into one of the following four categories:

— calls permitted based on NCOS

— only intragroup calls or calls on an exception list are allowed

— only intragroup calls are allowed

— only calls on the exception list are allowed

— no calls are allowed

82.6.1.9 Toll Restriction Features

At the alerting originator phase, the originator is not checked against Toll Restrictions, that is, even if the originator has Toll Restrictions, the SSP will still alert the originator. When the originator accepts the call, the SSP then attempts to route the call to the called party -- this is when the Toll Restrictions are checked and applied to the call.

Toll Restrictions include:

- CTD (carrier toll denial)
- Equal Access Enhanced Carrier Toll Denial
- FCTDNTER (InterLATA Full Carrier Toll Denial)
- TDN (Toll Denial)
- TDV (Toll Diversion)

82.6.1.10 Features Treated as Interface Busy

When the originator has one of these features active, it is considered interface busy thus no alerting is provided to the originator:

- all variants of Call Waiting, including TCW (Talking Call Waiting)
- all variants of Hold

82.6.1.11 Call Waiting During Alerting Originator

When a call is terminating on an interface which is being notified as an originator of a previously received Create Call message, the SSP shall treat the call as terminating party busy. All call waiting features including SCWID (Spontaneous Call Waiting Identification, DSCWID (SCWID with Disposition) are not activated.

82.6.1.12 No Barge-in on Create Call

The SSP do not Barge-in on a call while attempting to service a Create Call request. In other words, when the originator is being alerted for a Create Call request, Barge-In features like executive busy override (EBO) and directed call pickup with barge in (DCBI) cannot be activated.

82.6.1.13 Feature Activation after Originator Accepts Create Call

Once the originator accepts the Create Call request by going offhook, the originator is able to activate any features that can be activated through normal call setup.

82.6.1.14 Distinctive Ringing Features

When optional parameter ControllingLegTreatment is included in the Create Call message, the value specified in this parameter overrides the switch based Distinctive Ringing features.

82.6.1.15 Feature Activation after the Calling Party accepts Create Call

Once the originator accepts the Create Call request by going offhook, the originator is able to activate any features that can be activated through normal call setup.

82.6.2 Feature Interaction during routing to Called Party

82.6.2.1 Terminating Features

Terminating features on the Called Party are activated and function the same way as the call has been initiated by the originator through going offhook and dialing the digits.

82.6.2.2 Calling Number/Name Display/Blocking

The presentation status in the Calling Party ID in the Create Call message overrides calling number/name display/blocking features.

82.6.2.3 Distinctive Ringing Features

When optional parameter PassiveLegTreatment is included in the Create Call message, the value specified in this parameter overrides the switch based Distinctive Ringing features.

82.6.2.4 UCD (Uniform Call Distribution) Call Queuing

If the Called Party ID maps to a station in a UCD group, the call created through the Create Call functionality is terminated to that station.

82.6.2.5 Direct Inward System Access (DISA)

when the Called Party ID maps to a DISA DN, it behaves the same way as if the user had dialed the DN.

82.6.2.6 Preset Conference

A call can be routed to a Preset conference DN through a Create Call request.

82.6.2.7 MeetMe Conference

A call can be routed to a MeetMe conference DN through a Create Call request.

82.6.2.8 Expensive Route Warning Tone

When routing to the Called Party, the Expensive Route Warning Tone is not heard.

82.6.2.9 Flash

When routing to the Called Party, before the call terminates on the Called Party, flash is not allowed. Flash after terminating on the Called Party is allowed.

82.6.2.10 Flexible Calling (FC)

When routing to the Called Party, before the call terminates on the Called Party, FC is not allowed. FC after terminating on the Called Party is allowed.

82.6.2.11 PVN (Private Virtual Network)

While routing to the Called Party, attempting to start the PVN feature results in FNAL treatment to be applied to the call.

82.6.2.12 MCDN (Message Center Directory Number)

While routing to the Called Party, attempting to start the MCDN feature results in FNAL treatment to be applied to the call.

82.6.2.13 E800

If the Called Party ID in the Create Call message is an E800 number, the SSP shall activate the E800 service and query the E800 database.

82.6.2.14 AIN TFS

If the Called Party ID in the Create Call message is an AIN TFS number, the SSP shall query the SCP.

82.6.2.15 Emergency 911

If the Called Party ID in the Create Call message contains digits '911', which correspond to the emergency service, the SSP shall route the call using the E911 service.

82.6.3 Interactions with AIN Triggers

- **When Alerting the Calling Party** - When alerting the originator for a Create Call request, all AIN triggers encountered (e.g., terminating triggers like TAT, T_No_Answer and T_Called_Party_Busy triggers) are ignored and queries to the SCP are not sent.
- **Calling Party goes OFFHK** - When the originator accepts the Create Call request by going offhook, any AIN triggers encountered at the Orig_Attempt TDP and Info_Collected TDP are ignored and queries to the SCP are not sent. **Off Hook Delay Trigger** is part of the Info_Collected TDP and thus will be IGNORED.
- **Routing to Destination** - After the originator accepts the call, the CS2K attempts to route the call to the called party of the Create Call message. During the routing phase, any triggers that may occur result in queries to be sent to the SCP.

82.6.4 Agent Support for Create Call

The Calling Number in a Create Call message must be a local line agent. This is by definition of the Create Call Message. Only agents supported by AIN may be the Calling Number. The following additional restrictions are placed upon which line agents are supported as Create Call Originators:

- ISDN PRI agents are not supported (PRI is considered to be a trunk)
- ISDN BRI agents are not supported
- Coin lines are not supported
- Attendant Consoles are not supported
- Virtual Agents are not supported.
- ADSI terminals are supported as an analog agent
- Party lines are not supported.
- Hunt group members are supported, but no hunting is done.

82.6.4.1 TOD (Time Of Day routing)

The route taken by Create Call can be affected by Time of Day(TOD) Routing.

82.6.4.2 Simplified Message Desk Interface (SMDI)

The Called Party in the Create Call message can be a line served by SMDI.

82.6.4.3 Series Completion (SCMP)

A call created through the Create Call functionality can terminate to an SCMP group and does not affect the SCMP terminating algorithm.

82.6.4.4 Hunt Groups

If the Called Party ID in the Create Call message corresponds to one of the following Hunt Groups, then the call is terminated on first available member of the Hunt Group:

- BNN (Bridged Night Number)
- DLH (Distributed Line Hunt)
- DNH (Directory Number Hunt)
- KSH (Key-Set Short Hunt Group)
- MLH (Multiline Hunt)
- MPH (Multiple Position Hunt)
- NSDN (Night Service Directory Number)

82.6.4.5 Feature Groups

A call established through the Create Call functionality can route either as FGB, FGC or FGD.

A call established through the Create Call functionality can not be routed as FGA.

82.6.4.6 MADN (Multiple Appearance Directory Nymber)

When the Called Party ID included in the Create Call message maps to one of the following MADN group, the call terminates on the MADN group:

- MADN SCA (Single Call Arrangement)
- MADN MCA (Multiple Call Arrangement)
- MADN EXB (Extension Bridge)
- MADN CACH

82.6.4.7 SimRing

When CalledPartyID parameter in the Create Call message is a pilot DN, then SIMRING is activated and the Call proceeds normally.

82.6.4.8 PLP (PLug uP)

When the Called Party has the PLP feature activated, a call created through the Create Call functionality is not allowed to terminate on the Called Party.

82.6.4.9 SUS/RSUS (suspended/requested suspension)

When the Called Party has the SUS/RSUS feature activated, a call created through the Create Call functionality is not allowed to terminate on the Called Party.

82.6.4.10 RSDT (restricted dial tone) with state in-effect

When the Called Party has the RSDT feature activated, a call created through the Create Call functionality is not allowed to terminate on the Called Party.

82.6.4.11 CLASS Outgoing Call Memory

When a call is originated via the Create Call request, the SSP does not update the outgoing Memory Slot (OMS), regardless whether or not the call is diverted through triggering while routing to the Called Party.

82.6.4.12 LNR (Last Number Redial)

Attempt to invoke LNR on a call established through the Create Call functionality shall result in calling the number the originator dialed before the Create Call request.

82.6.4.13 AR (Automatic Recall)

Attempt to invoke AR on a call established through the Create Call functionality shall result in calling the number the originator dialed before the Create Call request.

82.6.4.14 ACB (Automatic Call Back)

When an attempt to establish a call through a Create Call request fails due to the Called Party's interface busy status, invoking ACB from the originator of the Create Call message shall result in calling the number the originator dialed before the Create Call request.

82.6.4.15 Ring Again Features

- **Call Back Queuing (CBQ)**: CBQ cannot be invoked when the call encounters a busy facility while routing the Called Party of a Create Call message.

  Note: CBQ (also known as on-hook queuing) provides a ring back to the on-hook calling line when a facility that the call is queued against becomes available. CBQ can be activated by the caller after receiving no circuit treatment, expensive route warning tone, or during the off-hook queue tone or announcement.

- **Nodal ring again (RAG)**: Attempt to invoke RAG on a call established through the Create Call functionality shall result in calling the number the originator dialed before the Create Call request.
- **Network ring again (NRAG)**: NRAG is applicable when the ring again feature is networked across different switching nodes. From a user point of view, NRAG and RAG operate the same way for Create Call.

82.6.4.16 Dynamic Control Routing (DCR)

Dynamic Control Routing may encounter while routing to the Called Party.

82.6.4.17 ACD (Automatic call distribution) Termination

Automatic call distribution (ACD) permits calls to be evenly distributed to a number of designated ACD agent positions. When all positions are busy, new calls are queued and a ringing tone or announcement can be returned to the caller.

A call can be routed to an ACD DN through the Create Call request and ACD functionality is not impacted.

Parameter Calling Party Id in the Create Call message is not used to update the display of EBS sets with the ACD option.

82.6.4.18 SMDR (Station Message Detail Recording)

All calls that would normally generate SMDR records will continue to do so when the call is created through the Create Call functionality.

82.7 Glossary

Term	Description
AIN	Advanced Intelligent Network
DN	Directory Number
SOC	Software Optionality Control
TCC	Create Call Timer
TID	Terminal ID
CPID‘	Call Processing ID
GAME	Generic AIN Messaging Environment
TCAP	Transaction Capabilities Application Part
SS	Session Server (AKA NGSS)
SIP	Session Initiated Protocol
NCAS	Non-Call-Associated-Signaling

C2C	Click to Call
C2D	Click to Dial
SCP	Service Control Point or Signaling Control Protocol
SSP	Service Switching Point

83: Functional Description(FN): A00009520

83.1 Feature name and Feature ID

Feature ID: A00009520

Title: Trunk blocking tools for MG4K and GWC on SN09

83.2 Description

When a MG4K-ATM or GWC goes into overload, some trunks on that node need to be busied to offload traffic. In the current system, it provides the capability to busy whole trunk group or all members on a specific MG4K-ATM/GWC node. However, there is no way to busy specific trunks on an individual MG4K-ATM/GWC.

This feature enhances the existing post command under MAPCI TTP level to provide the following functions:

- Busy a specific trunk group on an individual MG4K-ATM gateway;
- Busy a specific trunk group on an individual GWC.

A new post type ‘I’ is introduced under MAPCI TTP level by this feature. When post command with type ‘I’ is entered in the command, it posts the trunks in the existing post set. If there is no existing post set, it returns error. The following is the error example:

The following is an example on how to post the trunk members of TRUNK_EXAMPLE on GWC 32.

```
                IOD          PM    CCS    Lns    Trks   Ext    APPL
                OCC  B       PMLOAD 3   RS  SYSB    42C..  2Crit   .
                *C*              *C*    *C*    *C*    *C*    *C*
TTP
 0 QUIT        POST      DELQ         BSYQ       DIG
 2 Post_       TTP 27-0102
 3 SEIZE       CKT TYPE    PM NO.       COM LANG    STA S R  DOT TE  RESULT
 4
 5 BSY
 6 RTS
 7 TST
 8
 9 CktInfo
10 CktLoc
11 Hold        NO CKT, SET IS EMPTY
12 NEXT        TTP:
13 RLS
14 Ckt_
15 TrnslVf_
16 StkSdr_
17 Pads
18 Level_
  TESTER
Time  15:32  > POST D GWC 32; POST I G TRUNK_EXAMPLE
```

1. *POST D GWC 32; // create a post set which contains all the trunks on GWC32;*
2. *POST I G TRUNK_EXAMPLE; // Post only the trunks whose CLLI are TRUNK_EXAMPLE in the post set.*

Only post type ‘D’ and ‘G’ are allowed to follow the type ‘I’. Only DEQ name ‘GWC’ and ‘SPM’ are allowed to follow the post type ‘D’ if it is after the type ‘I’. This feature is based on the existing BSY functions for trunks on GWC and SPM.

The trunks that supported by this feature are ISUP, PTS and PRI on GWC and MG4K-ATM.

83.3 Hardware Requirements or Dependencies

N/A

83.4 Software Requirements or Dependencies

N/A

83.5 Limitations and restrictions

- Only trunks on GWC and MG4K-ATM are supported by this feature.

83.6 Interactions

- A set of trunks must be posted prior to to ‘POST I’ command.

83.7 Glossary

Term	Description
CLLI	Common Language Location Identifier
DEQ	Digital EQuipment
TTP	Trunk Test Position
PTS	Per Trunk Signalling
PRI	Primary Rate Interface
ISUP	ISDN User Part
MG4K	SMG4000
ATM	Asynchronous Transfer Mode
GWC	Gateway Controller

84: Functional Description(FN): A00009530

84.1 Feature name and Feature ID

A00009530 - “H248 & xUA NAT traversal for CPE Gateways”

84.2 Description

Introduction

Small trunk gateways, such as the Audiocodes Mediant 2000 (M2k), are being deployed as Customer Premises Equipment (CPE). This is being done in order to connect TDM PBXs to packet telephony networks, as we expect that there will be many such older TDM PBXs in service for a number of years to come.

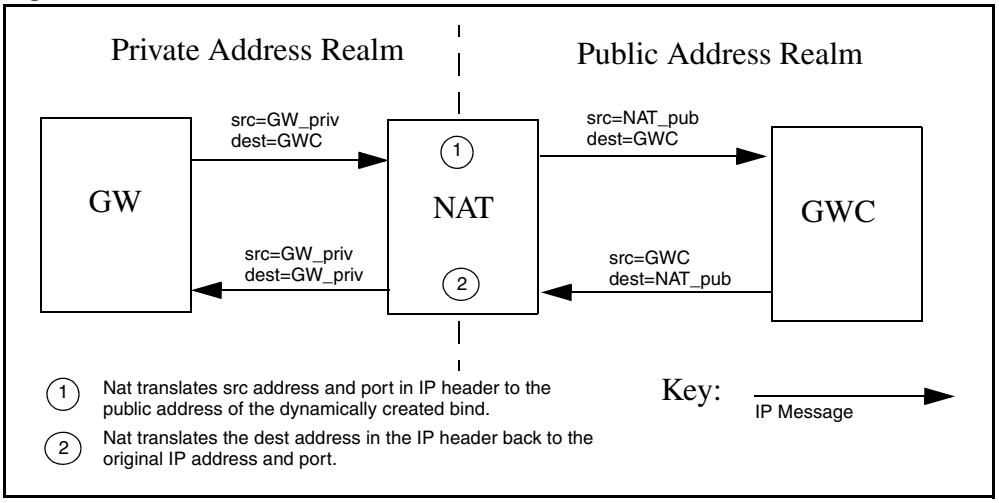
Various protocols are used to control these gateways. Within the scope of this feature, H.248 is used for control of the bearer path. Call control signalling can be via protocols such as ISDN PRI, or DPNSS. These signalling protocols are backhauled from the gateway to the CS2k over an SCTP connection. Currently, neither the H.248, nor the SCTP protocol can work over a NAT without special datafill in place. This feature will enable these protocols to work automatically when the gateway is located behind a NAT. Note that the CS2k and GWCs must remain within the core network.

84.2.1 Operation

NAT systems are in common use throughout IP networks today. They allow use of private addresses within a network by translation of IP addresses within the IP header. CPE gateways may well be connected via a NAT, so this needs to be a supported configuration for the CS2k.

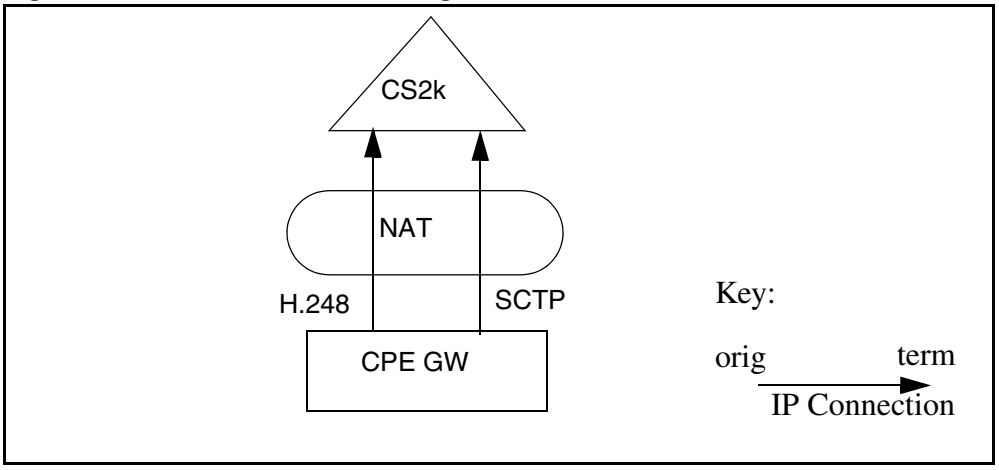
Figure 1 illustrates a simple case of NAT operation. The NAT creates a dynamic bind in response to the initial message from the gateway. This allows messages to pass in both directions between gateway and GWC. The NAT bind will be removed if there is no traffic over it for a specified period of time. In order to avoid this happening to an established connection, we need to ensure a minimum traffic level over the link. SCTP has an inbuilt heartbeat mechanism which will perform this function. For H.248, the gateway should use the Inactivity Timeout package to do this.

Figure 1 CPE GW Connected via a NAT



Without special NAT configuration, incoming IP connections are not possible to a host behind a NAT. So, in order for a connection to traverse a NAT, it must originate from within the NAT zone. For us, this means that the connections must be initiated by the gateway rather than the CS2k. The figure below shows both H.248 and SCTP connections being originated from a CPE gateway.

Figure 2 Functional Behavior Diagram



In a normal, non-NAT, setup, H.248 connections are already initiated from the gateway, but SCTP connections are done from GWC to GW. This is changed by this feature for gateways behind a NAT.

When the CS2k receives an incoming connection from the gateway, the connection will appear to be from the NAT's public IP address, rather than the gateway. As we cannot be sure of this address when provisioning the gateway, we need to rely on the GWC to determine the IP address and port by extracting them from the IP headers. This process is known as IP auto discovery, and has already been implemented for small line gateways using the MGCP protocol.

This was done by feature 59034470 - “CS2000 Support for IP Discovery”. When an IP address of 0.0.0.0 or a port of 0 is provisioned for a gateway, the GWC will attempt to automatically discover the true values. This feature extends support for this functionality to the H.248 and SCTP protocols.

84.2.2 H.248 Support

In order for H.248 to traverse a NAT, the following must be set up:

- The MID of messages sent by the gateway must match the provisioned name of the gateway on the CS2k. The FQDN of the gateway is suggested for use here.
- The gateway should NOT include the “AD” (ServiceChangeAddress) parameter in the H.248 ServiceChange message the it sends to the GWC.
- The GW must be provisioned with an IP address of 0.0.0.0 unless the public IP address that the NAT will use is known.
- The GW must be provisioned with a H.248 protocol port of 0 unless the public port that the NAT will use is known.
- The NAT/VPN that the GW resides behind must be specified when the GW is provisioned, via the 'adjacent Network Zone' field in the 'associate Gateway' dialog.
- The gateway must support the H.248 Inactivity Timeout package, and use it to maintain a minimum traffic level over the NAT. This traffic level must be sufficient to prevent the NAT bind timing out.

84.2.3 SCTP Support

In order for SCTP to traverse a NAT, the following must be set up:

- The gateway must attempt to initiate the SCTP connection to the GWC.
- The INIT message used to initiate the SCTP association must contain a Host Name Address parameter. The contents of the parameter must match the provisioned name of the gateway on the CS2k.
- The GW must be provisioned with an IP address of 0.0.0.0.
- The NAT/VPN that the GW resides behind must be specified when the GW is provisioned, via the 'adjacent Network Zone' field in the 'associate Gateway' dialog.
- The gateway must send SCTP heartbeat messages in order to maintain a minimum traffic level over the NAT. This traffic level must be sufficient to prevent the NAT bind timing out.

84.3 CS2M Provisioning Support For NAT Traversal

The CS2M platform is modified to allow the provisioning of adjacent Network Zones against the Audiocodes GW. This is done by enabling existing functionality currently supported for small line and H.323 type GWs.

For completeness the following figures show the newly enabled functionality for the Audiocodes GW.

Figure 3 shows the Associate Media Gateway dialog for the Audiocodes GW. The Internet Transparency selector box is enabled allowing an adjacent Network Zone to be optionally associated with the GW.

Figure 4 shows the GW list panel from the CS2M provisioning GUI. Here an Audiocodes GW has been previously added with an adjacent ITRANS Network Zone. The “Adj ITRANS MB” field is showing the Network Zone associated with the GW.

Figure 5 shows the input XML for the assocMG OSSGate interface. Here the itransMiddleboxName tag value pair has been specified to request an ITRANS Network Zone be associated with the new AUDIOCODES GW.

Figure 6 shows the Change GW - Change Adjacent ITRANS Network Zone dialog.

Figure 7 shows the changeAssocMB OSSGate XML interface as used to change the Network Zone associated with a GW.

Figure 3 Associate Media Gateway Dialog Showing IP-VPN / LBL Selection Box

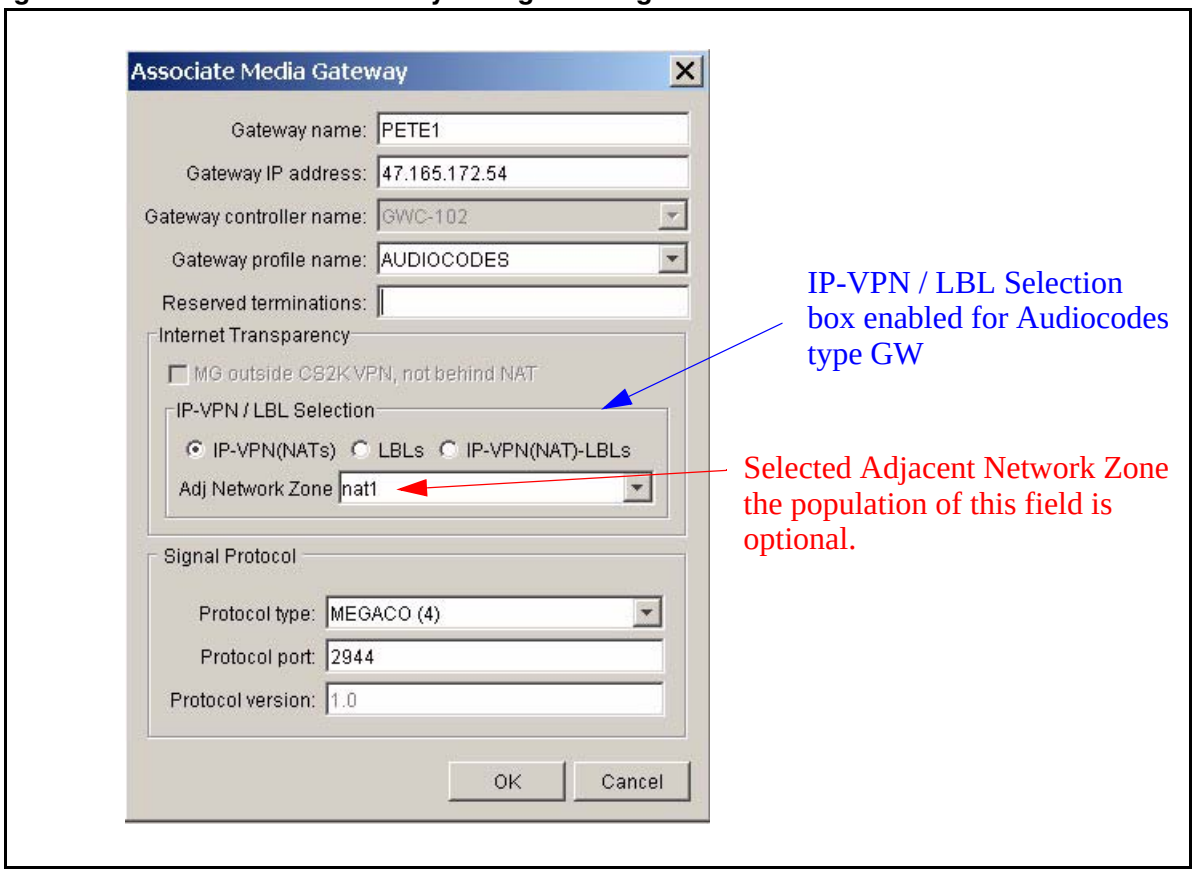


Figure 4 Adjacent Network Zone For Audiocodes GW Shown In GW List

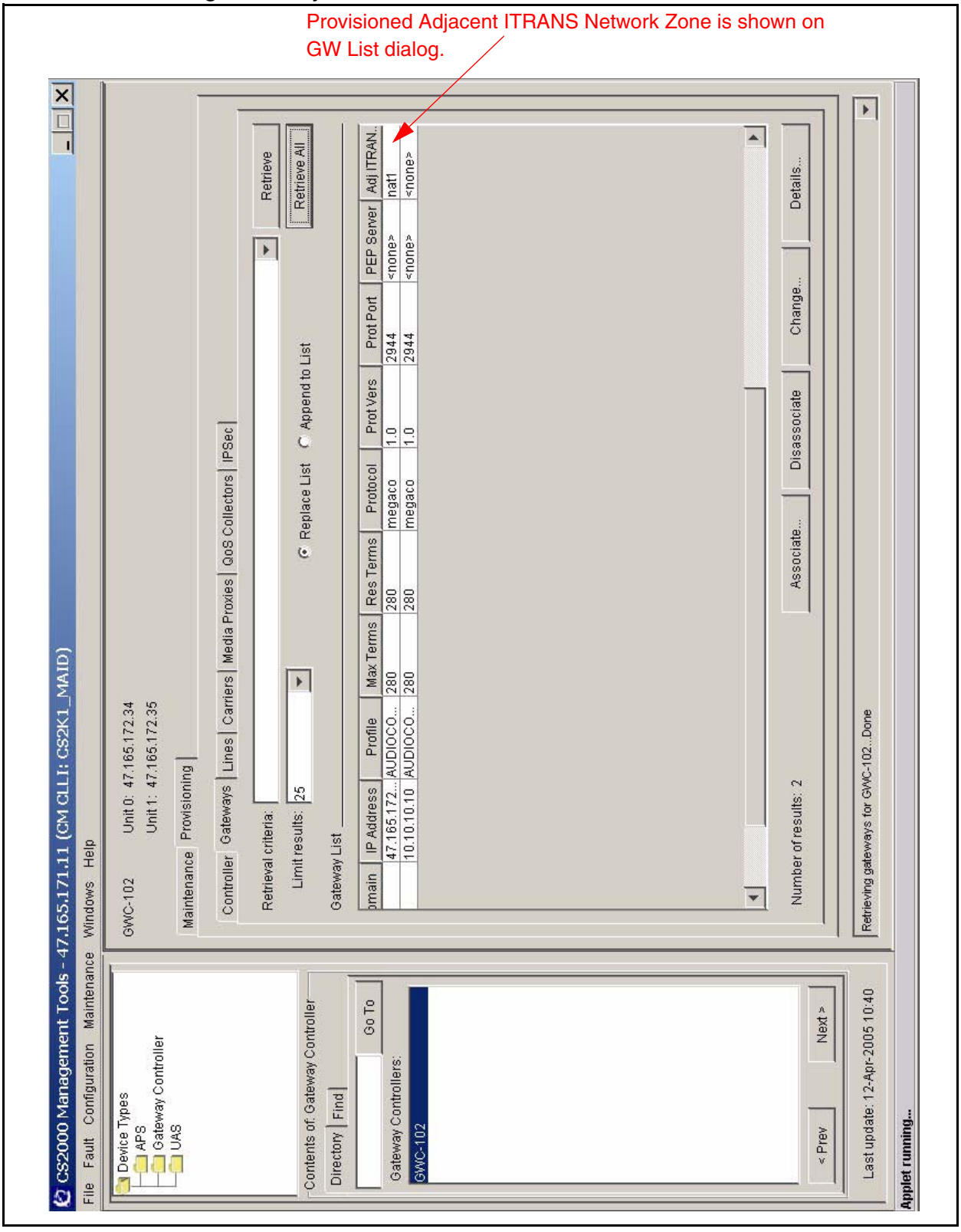


Figure 5 OSSGate assocMG Request Specifying adjacent ITRANS Network Zone

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <assocMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>PETE1</mgUIName>
          <mgProfileName>AUDIOCODES</mgProfileName>
          <mgIpAddr>2.2.2.2</mgIpAddr>
          <mgProtocolType>4</mgProtocolType>
          <mgProtocolVersion>1.0</mgProtocolVersion>
          <mgProtocolPort>2944</mgProtocolPort>
          <gwcUIName>GWC-102</gwcUIName>
          <itransMiddleboxName>nat1</itransMiddleboxName>
        </Parameters>
      </assocMG>
    </Methods>
  </Command>
</CommandList>
```

adjacent ITRANS Network Zone to be associated with this Audiocodes GW. This field is optional

Figure 6 Change Gateway - Change Adj ITRANS Zone

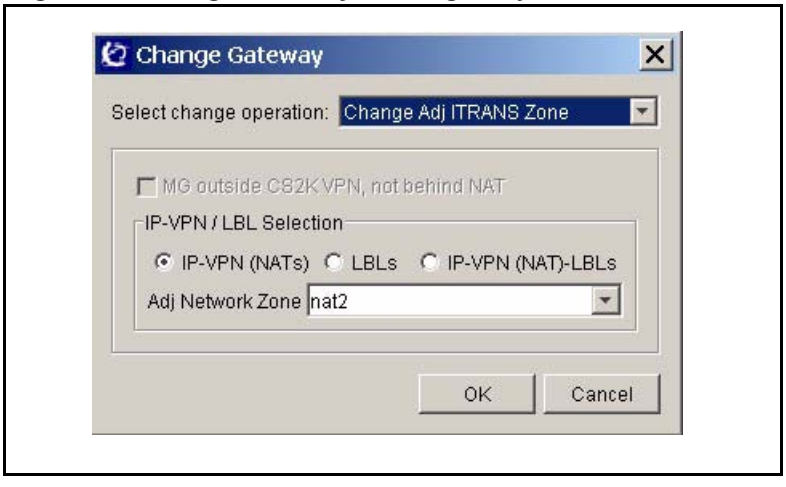


Figure 7 OSSGate changeAssocMB Request For Audiocodes GW

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <changeAssocMB usn="1" version="1.0">
        <Parameters>
          <MGname>PETE1</MGname>
          <itransMiddleboxName>nat2</itransMiddleboxName>
        </Parameters>
      </changeAssocMB>
    </Methods>
  </Command>
</CommandList>
```

84.4 Hardware Requirements or Dependencies

Not applicable.

84.5 Software Requirements or Dependencies

The software load on the gateway must be capable of fulfilling the gateway requirements in the “H.248 Support” and “SCTP Support sections above. The 4.6 version of software for the Audiocodes Mediant 2000 gateway will satisfy these requirements.

84.6 Limitations and restrictions

Currently support for this feature is limited to the Audiocodes gateway profile. Support for other gateway profiles will require an integration activity.

84.7 Interactions

Not applicable.

84.8 Glossary

Term	Description
SCTP	Stream Control Transmission Protocol
NAT	Network Address Translation

85: Functional Description(FN): A00009532

85.1 Feature name and Feature ID

Support host to host tunnels for all northbound OSS connections, A00009532

85.2 Description

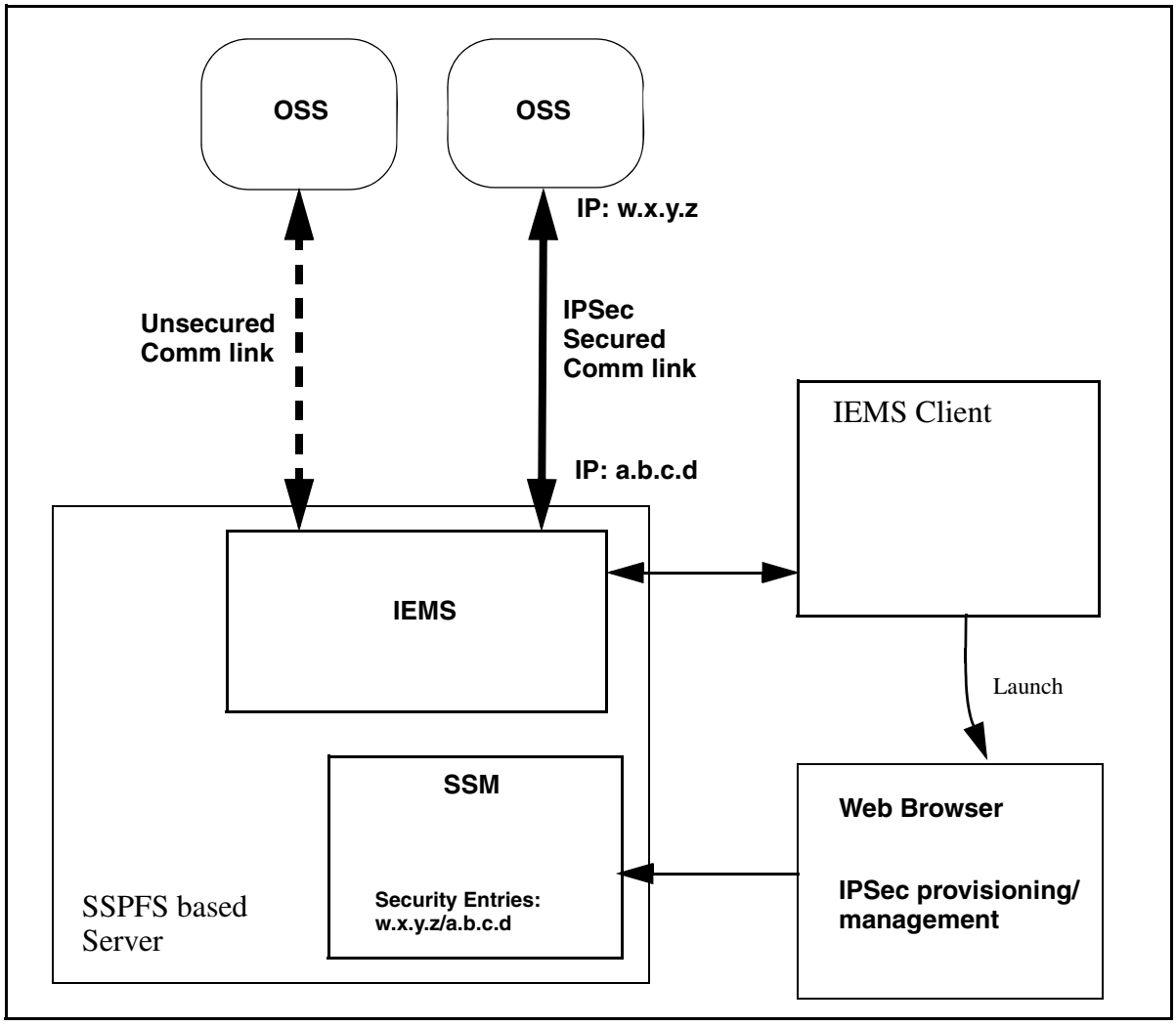
This activity is to test, verify and document host to host IPSec between SSPFS servers (namely IEMS, but not exlusively) and northbound OSSs. Securing this communications link will provide additional protection and encapsulation of OSS to IEMS traffic. The IPSec implementation will be in all other ways compliant with encryption key management and encryption protocol requirements in the Verizon agreement.

This activity will use the existing IPSec provisioning and management framework provided by SSPFS's Server Security Manager (SSM). SSM is currently used by the MG9K EM to secure communications channels with MG9K Network Elements.

All testing encompassing this feature will be based on the Solaris 9 software platform for SSPFS servers as well as OSS simulation. A Sun Netra 240 will be used for the SSPFS servers and a Sun Ultra 10 will be used for simulating the OSS.

The figure below gives a functional layout of the components involved with this feature. The main component of interest is the IEMS application running on a SSPFS based server. It provides input to the northbound OSS links. IEMS has a native GUI for craftsperson interaction. Another important component within SSPFS is the Server Security Manager (SSM). This component is used to provision and manage all IPSec related parameters for the SSPFS server and by extension all applications running on the server, such as IEMS. SSM is accessed using a standard web browser. The last component is the OSS which receives messaging output from IEMS. In this feature, for testing purposes, the OSS will be simulated.

Figure 1 Functional Layout



85.3 Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced in the feature for the IEMS server.

85.4 Software Requirements or Dependencies

The latest SN09 IEMS software will be required for IPSec.

85.5 Limitations and restrictions

IEMS will not have direct control over the provisioning and management of IPSec security. This functionality is the domain of the Server Security Manager (SSM).

No new security parameters are being introduced in the Server Security Manager (SSM). This feature will utilize the existing functionality of SSM. That means Internet Key Exchange with preshared keys is the only supported mechanism for relaying encryption key information.

85.6 Interactions

Using IPSec to secure the northbound OSS interface will be invisible to the functionality and not have any impact to managing the traffic except for the additional step of provisioning the IPSec security parameters.

85.7 Glossary

Term	Description
IEMS	Integrated Element Manager System
SSM	Server Security Manager

86: Functional Description(FN): A00009550

86.1 Feature name and Feature ID

CBM-NPM Patching Convergence A00009550

86.2 Description

Prior to SN09, two software tools exist to administer software updates associated with SSPFS-based software; Core Billing Manager (CBM) Software Installation Manager (SIM) and Network Patch Manager (NPM).

Prior to SN09, SIM is used to maintain software updates associated with the CBM software in TDM, Wireless, and Succession configurations. In those configurations, SIM is also used to administer SSPFS-based patches on the CBM Solaris-based machines.

The intention of this feature is to integrate the CBM SIM functionality into NPM, and to support a single patch manager for the whole network to administer software updates for TDM/Wireless and Succession configurations. The NPM user interface is utilized as a central location for administering all software updates. For SSPFS based patches, the NPM is used in TDM/Wireless and Succession configurations for patch maintenance and administration. Also, for Core Element (CEM) based applications delivered with CBM, NPM is used for patch maintenance and administration.

Figure 2 SN09 TDM/Wireless Behavior

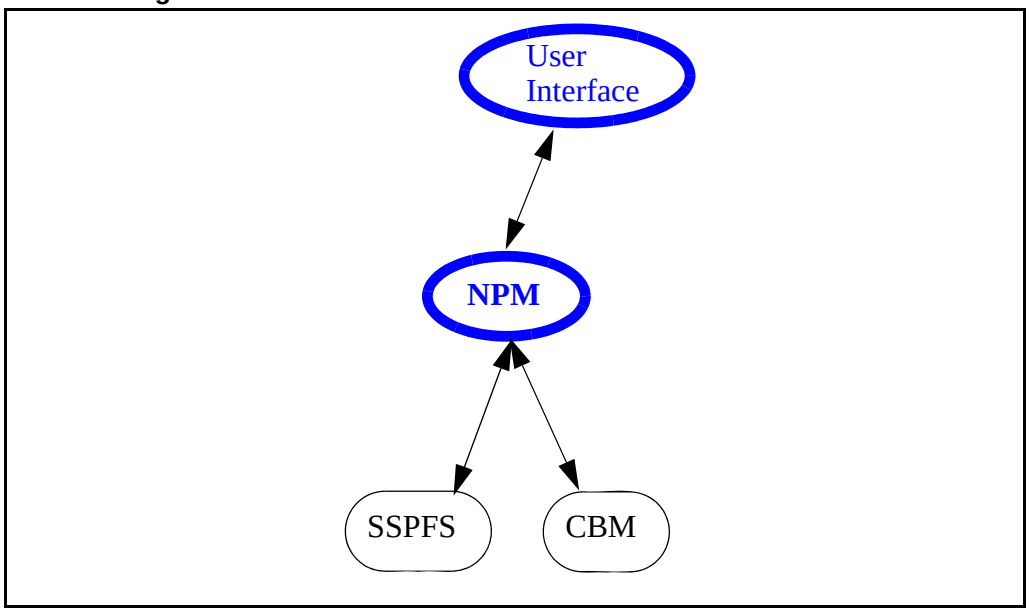
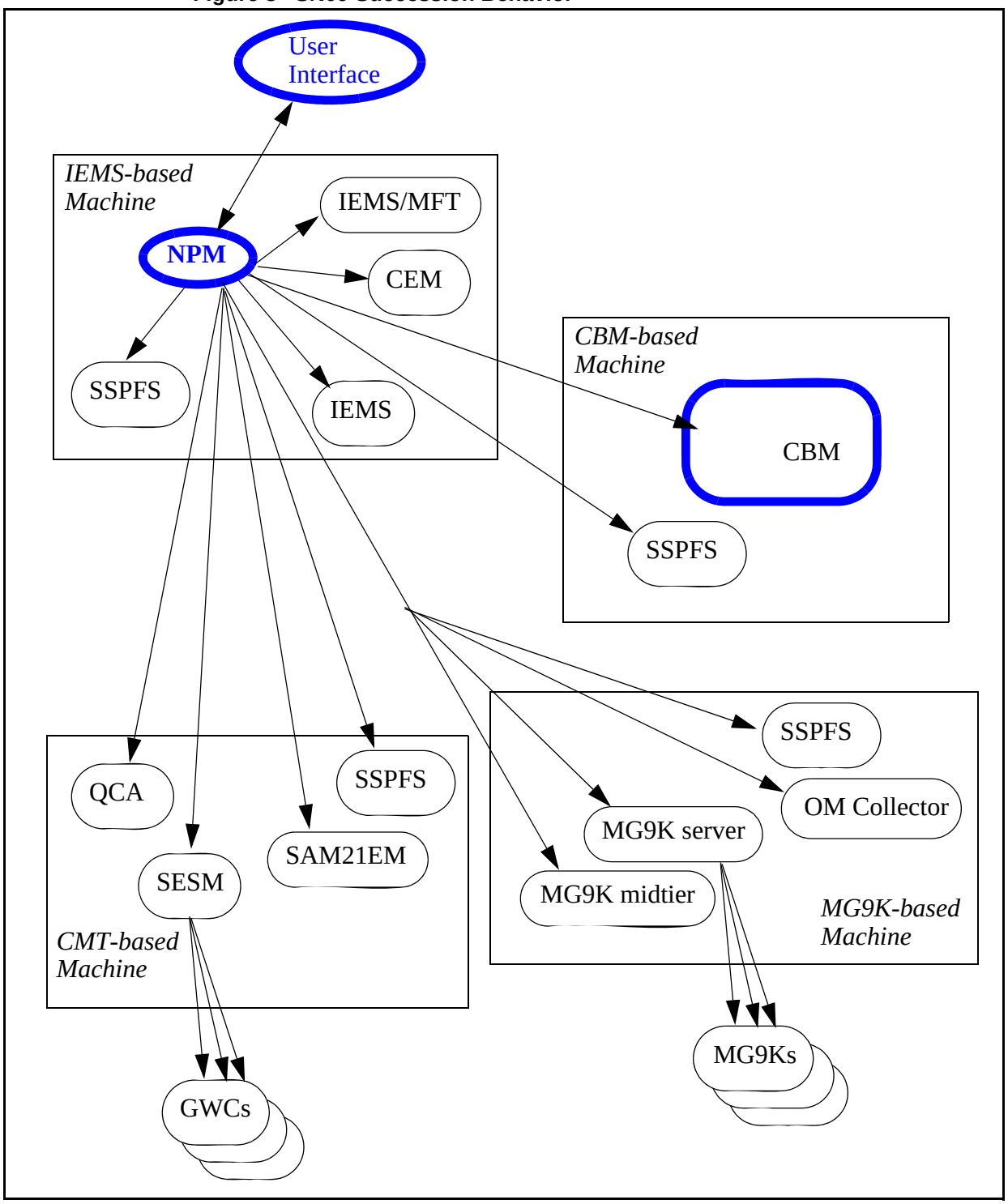


Figure 3 SN09 Succession Behavior



86.2.1 Cumulative Patching

CBM patches are cumulative. For CBM related applications, each patch

delivers the entire package content and subsequent patches contain the fixes that prior patches introduced. For CEM related packages, each patch delivers the file of the package that has changed and subsequent patches contain all previously changed files. Both approaches allows a customer to apply only the latest patch if desired since it will contain all of the fix content included in previous patches. CBM patches are delivered by RPS. There is only one Released patch at any given point in time for a particular package, unless it is the first patch for the package which can be at Verified or Released status. After a patch is Released for a package, all previous patches are set to Superseded in RPS and will no longer be delivered.

NPM is the patch management system to apply and remove CBM patches and perform maintenance patching activities on the CBM applications. All patching functionality available in NPM is available for CBM patching.

With this methodology of patching, if 3 patches have been released for a given package, and all 3 have been downloaded to a customer site, the customer can choose to physically apply patch 1, patch 2, and patch 3, or the customer can choose to apply patch 3 only. If only patch 3 is applied, this essentially results in having patch 1, patch 2, and patch 3 applied. If only patch 3 is applied, patch 1 and patch 2 cannot be removed individually. NPM will store a relationship attribute that indicates patch 3 is temporary (T) and patches 1 and 2 are bound (B). If only patch 3 is applied, when patch 3 is removed, patch 2 and patch 1 are also removed.

86.2.2 Multiple Devices

CBM registers with NPM as multiple patchable devices. A unique load name is associated with each device. The load name is used for patch calculation purposes. Patches are applied to and removed from a device. Devices are restarted to enable or disable patches. In a high availability (HA) or clustered environment, 2 instances of the device will appear; one instance for the active side and one instance for the inactive side. In a HA environment, customers have the option to apply patches on both sides individually, or request both sides be patched in one transaction.

An example CBM deviceid is CBM_BILLING.

86.2.3 Patching Maintenance

When the patchable CBM applications are installed, the NPM automatically becomes aware of them. CBM devices appear in reports and the device list of the NPM GUI or CLUI. The following functions that exist for other targets are now available for CBM devices.

- apply
- remove
- audit

- restart
- set/report creation
- plans/automation
- alarms

86.2.3.1 CBM Patch Application and Removal

Like existing OAM Java-based applications such as SESM, SAM21EM, or IEMS components, the CBM requires 2 steps for application and 2 steps for removal of patches.

application

- apply command from the NPM GUI or CLUI (sets patch to applied/ disabled and stages patch for actual patch application)
- restart command from the NPM GUI or CLUI on CBM device (sets patch to applied/enabled after restarting the device)

removal

- remove command from the NPM GUI or CLUI (sets patch to removed/ enabled and prepares patch for actual patch removal)
- restart command from the NPM GUI or CLUI on CBM devices to disable the patch (sets patch to removed/disabled after restarting the device)

When CBM is running in a clustered configuration, the 2 step application and removal of patches is necessary on the active side of the SSPFS-based machine, and only for those devices which have running applications on the inactive side. A restart from the NPM GUI or CLUI of a CBM device is required to enable or disable patches only for those devices which have running applications. When a patch is applied to or removed from CBM device which has no running applications, the patch is automatically enabled or disabled.

The apply and restart operations from the NPM GUI and CLUI can be automatically scheduled via NPM plans (autoapply and autorestart).

NPM will not automatically reboot a machine for a patch that has a reboot required.

86.2.4 Patchid

The patchid format for CBM patches can have up to 32 alpha-numeric characters. An example CBM patchid is NTBASE220203-01. The patchid of the second version of that patch is NTBASE220203-02.

86.2.5 Patch File Format Modifications

The patch file format is modified with this feature. The following additions and changes have been made.

- A new **H** record is introduced to track patches that cannot be applied when the given patch is applied. This would happen in the case of a patch that had previously depended on a patch which became obsolete. Once a dependency is obsolete, any new patches cannot depend on that. This new record is stored in the ADM section of the patch file. Zero to many of these records can exist.

  H ANTI_PREREQ <patchid> where patchid is the name of the patch that cannot be applied when the given patch is being applied.

86.2.5.1 Patch Delivery to Customers

RPS is used to deliver CBM patches to customers. NPM has a Patch File Receipt System (PFRS) setup that allows the customer to configure where to have patches delivered for NPM to retrieve, and where to deliver an inform report for RPS to use for patch calculation purposes. RPS will deliver CBM patches based on a calculation of the load name associated with a patch and the load name associated with the device on site. Information on PFRS setup can be found in the online NPM GUI or CLUI help.

RPS delivers only the latest version of a patch for a given software package. Once a new version of a patch is released, all previous versions are Superseded and are no longer delivered. The customer needs to only apply the latest version of a patch since it includes in it all previous software changes.

86.2.5.2 Online Help

NPM provides the user online help via the GUI or CLUI. A CLUI help document is also available in the NpmCluiHelp.PDF document on the NPM server machine at /opt/nortel/NTnpm/documents.

86.3 Hardware Requirements or Dependencies

A windows based PC machine is required to use the NPM GUI.

86.4 Software Requirements or Dependencies

The SN09 CBM load is required to interact with NPM.

86.5 Limitations and restrictions

86.5.1 Patch Dependencies and Maintenance Releases

In SN09, patch dependencies are permitted between patches applicable to different devices. A CBM patch can have a dependency on an SSPFS patch. If an SSPFS maintenance release (MR) is created and contains a dependent SSPFS patch, the CBM software that requires the now built in SSPFS patch will also have to build a new MR on top of the SSPFS MR. If this is not done,

some other type of software delivery strategy will need to be implemented for the CBM load that contains the patch with a dependency.

86.5.2 Patch Dependencies and Obsolete Patches

A CBM patch can have a dependency on a patch in the SSPFS device. If a patch dependency is created between a CBM patch and an SSPFS patch, and the SSPFS patch becomes obsolete, all CBM patches that depend on the obsolete SSPFS patch must be removed from customer sites. Once an SSPFS replacement patch is downloaded and applied, a new CBM patch is created that depends on the replacement patch, and then delivered to customers. If obsoleting an SSPFS patch is determined to be too disruptive, a new SSPFS patch should be written on top of the bad SSPFS patch and delivered to the customer.

86.6 Interactions

None

86.7 Glossary

Term	Description
NPM	Network Patch Manager
CEM	Core Element Manager
RPS	Regional Patch Selector
CBM	Core Billing Manager
HA	High Availability
GUI	Graphical User Interface
CLUI	Command Line User Interface

87: Functional Description (FN) A00009576

87.1 Feature name and Feature ID

SN09FF H.323 RASLess Provisioning - A00009576

87.2 Description

This feature delivers the ability for a craftperson to explicitly provision the CS2K with the optional "RAS-less" functionality on a H.323 gateway/ gatekeeper basis. The RAS-less capability is configured during gateway association via the CS2K Management Tools server.

H.225 defines RAS (Registration, Admission and Status) messages and procedures for controlling access to the network. These messages allow H.323 endpoints to discover and register with a H.323 gatekeeper, to provide information about their capabilities and to request the allocation of appropriate amounts of bandwidth. For some applications, H225/H245 signaling should be used between the CS2K and another entity (e.g. softswitch, gatekeeper, or gateway) for setting up calls, but with no RAS messages. This mode of operation is deemed "RAS-less".

The optional RAS-less capability can be provisioned via the GUI or OSSGate XML interface of the CS2K Management Tools server during gateway association. Only H.323 gateways/gatekeepers can be configured with the RAS-less option.

87.2.1 CS2K Management Tools GUI changes

The associate gateway operation has been updated with the ability to configure the optional RAS-less capability. The RASLess option is displayed as part of the GWC Provisioning Panel of the CMT (CS2K Management Tools) GUI. The "Details" button of the Gateway tab has been updated to display the RASLess option configuration setting.

Once the associate media gateway operation is invoked, the corresponding associate media gateway dialog is launched. To configure the RAS-less functionality, a craftperson must choose a H.323 gateway profile from the "Gateway profile name" pull down menu of the associate media gateway dialog box.

If a H.323 gateway profile is chosen, specific H.323 configuration data options are presented. A new optional gateway data application panel has been added to the associate gateway dialog box. The optional "RAS-less" data is presented as part of the new optional gateway data choices. A craftperson can enable the RAS-less capability by setting the option to "true". The default value is "false".

Once all the required data is entered, the “OK” button of the associate media gateway dialog box will be enabled. By clicking on the “OK” button, the GWC EM will process the operation and generate the required SNMP messages. The SNMP messages are sent to the respective GWC. The craftperson will receive a successful or failure response from the GWC EM upon completion of the operation.

The “Details” button of the Gateway tab of the GUI will display the new optional data if supported by the specific gateway profile. A craftperson can click on the Details button to launch a gateway’s Details dialog box. The optional gateway data will be displayed for the respective gateway. The RASLess option is listed in the dialog box if the selected gateway is H.323. If there isn’t any gateway application data defined for the selected gateway, a dialog box will be launched indicating the respective gateway profile does not have any optional data defined.

The Details button is also used to display the associated “root middleboxes” of a respective gateway. Currently, H.323 gateways do not support root middleboxes.

Note: *All current H.323 gateway profiles support the new optional RASLess configuration except for the H323_PROXY gateway profile.*

87.2.2 OSSGate XML interface changes

The assocMG and queryMG operations of the OSSGate interface have been modified to support the optional RAS-less configuration data. The optional RAS-less data is only applicable to H.323 gateways/gatekeepers.

XML Associate MG changes

The optional RAS-less data has been added to the assocMG operation and can be configured against a H.323 gateway/gatekeeper.

To configure a “RASLess” H.323 gateway/gatekeeper, a valid assocMG XML command must include the optional RAS-less data.

assocMG - specifies the provisioning method. It has two attributes: USN (Unique Sequence Number) and version. The USN is used by an OSS to map requests with responses. The USN value specified in the request is returned in the response. The version attribute specifies the version of the method being used.

Parameters - specifies that the following elements are parameters for the method. Included in the parameters are:

• **mgUIName** - delimits MG name value.

• **mgProfileName** - delimits the MG profile name value to be applied to the MG.

• **mgIpAddr** - delimits the MG IP address value.

The new parameter is:

• *gwAppDataList - delimits the new optional data which includes **RASLess.***

XML Query MG changes

The optional RAS-less data has been added to the queryMG operation ***response*** and will only be returned when a H.323 gateway/gatekeeper is queried. The queryMG XML command has not been modified.

queryMG - specifies the provisioning method. It has two attributes: USN and version. The USN is used by an OSS to map requests with responses. The USN value specified in the request is returned in the response. The version attribute specifies the version of the method being used.

Parameters - specifies that the following elements are parameters for the method.

mgUIName - delimits MG name value. When this parameter element is specified the attributes of the MG specified are returned.

If a H.323 gateway/gatekeeper is queried, the RAS-less configuration will be returned via the optional device data parameter.

The optcn component of the A00009576 book contains GUI and XML examples detailing the new RASLess option for H.323 gateways/ gatekeepers. The OSS User's Guide details the OSSGate interface.

87.3 Hardware Requirements or Dependencies

There are no hardware requirements or dependencies for the CS2K H.323 RAS-less optional capability.

87.4 Software Requirements or Dependencies

This feature is being delivered as part of the Succession release SN09FF.

87.5 Limitations and Restrictions

• The optional RAS-less feature can only be provisioned against H.323 gateways/gatekeepers on the CS2K.
• The gateway profile "H323_PROXY" does not support the RAS-less functionality.
• The optional RAS-less feature is not supported with a NAT configuration of N:1. The N:1 NAT configuration is when multiple gateways behind a NAT

share the same “NAT’d” IP address and the gateways are uniquely identified by the port value.
• The provisioned protocol port value of the H.323 gateway/gatekeeper on the H.323 GWC (via the CMT GUI or XML interface) must be set to the CS (call signaling) port value of the gateway for RAS-less mode. (i.e. If the H.323 gateway is not behind a NAT and the call signaling port value is set to 1720 on the gateway, the gateway’s provisioned protocol port value on the GWC must be set to 1720).
• A RAS-less H.323 gateway that is behind a NAT with a 1:1 configuration (one private IP mapped to one public IP to the H.323 GWC), must have the provisioned protocol port value on the GWC set to a non-zero port value. The non-zero port value on the GWC must be mapped via the NAT to the gateway’s call signaling port value.

87.6 Interactions

This activity enables a craftperson to explicitly provision the RAS-less functionality against a H.323 gateway/gatekeeper on the CS2K. The associate gateway operation processed on the CS2K Management Tools server is updated with the ability accept the optional data via the GUI or XML interface.

87.7 Glossary

Acronym	Definition
CLLI	Common Language Location Identifier
CM	Computing Module
CMT	Call Server 2000 Management Tools
CORBA	Common Object Request Broker Architecture
CPE	Customer Premises Equipment
CS2K	Call Server 2000
DMS	Digital Multiplex System
ETSI	European Telecommunications Standards Institute
GW	Gateway
GWC	Gateway Controller
GWC EM	Gateway Controller Element Manager
H.323	Industry protocol for GW/GK<->GW/GK communication (not an acronym).

IDL	Interface Definition Language
IP	Internet Protocol
ITA	Internet Transparency Agent
LAN	Local Area Network
MIB	Management Information Block
MTC	Maintenance
NA	North American
NAT	Network Address Translator
NN	Node Number
NPM	Network Patch Manager
NTNA	Northern Telecom North American (proprietary PRI variant)
OAM&P	Operations, Administration, Maintenance and Provisioning
OSS	Operation Support System
OSSDI	OSS Data Interface
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
RAS	Registration, Admission and Status
SDP	Session Description Protocol
SESM	Succession Element and Sub-Element Manager [system]
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSPFS	Succession Solaris Platform Foundation Software
SS7	Signaling System 7
TCP	Transmission Control Protocol
TID	Terminal Identifier
TMM	Trunk Maintenance Manager
TN	Terminal Number

USN	Unique Sequence Number
XML	Extensible Markup Language

88: Functional Description(FN): A00009610

88.1 Feature name and Feature ID

A00009610: IEMS Calix Integration

88.2 Introduction

IEMS serves as an integrated platform for managing various devices. One among those devices is Calix C7 Ultra Broadband Digital Loop Carrier. This document lists the changes that are required in IEMS in order to manage a Calix device.

The Calix C7 implements three network management interfaces: TL1, GUI and SNMP. IEMS will use the SNMP interface for inventory and fault management. For configuration the TL1 and GUI would be used in the form of launches.

88.2.1 2. Acronyms Used

IEMS – Integrated Element Management System

GUI – Graphical User Interface

SNMP – Standard Network Management Protocol

TL1 – Transaction Language 1

88.3 IEMS Changes

88.3.1 3.1 C7 Provisioning

The C7 Network can be provisioned in IEMS as a Network Element. The C7 Network can be added from the existing Tools-->Add-->EMS / NE menu. The IP Address field represents the IP of the Calix Proxy Agent. 'Type' should be selected as NE. In the 'Device Type' a new entry, named 'C7 Network', will be added. Two new text fields will be added for the GUI Launch IP Address and TL1 IP Address. The SNMP details can be filled up on the next screen. This would be the same as the existing Fault Interface screen.

In order to discover the C7 network the calixDeviceTable in the calixProxyAgentMib is queried. This table will be queried for the following conditions

1 When a C7 Network is provisioned in IEMS

2 When the IEMS server restarts

3 When there is a communication regained after a communication loss to the C7 device

4 User issues a manual Re-Synchronize Inventory from the IEMS client

5 Trap or an alarm for an unmanaged shelf is received in IEMS

The following table lists some of the managed object properties for these objects

Property Name	*C7 Network*	*C7 Node*	*C7 Shelf*
Name	<HostName of provisioned network>-C7	<C7NetworkName>_node<nodenumber>	<C7NodeName>_shelf<shelfNumber>
DisplayName	As provided by the user	<C7NetworkDisplayName>_<sysName using the networkIP and shelf port>	<C7NetworkDisplayName>_N1-1
Type	NE-C7	C7Node	C7Shelf

The C7Node and C7Shelf are modelled as CalixObject in IEMS. A separate table named CalixObject will be created in IEMS. We will be storing the following details pertaining to the C7Node and C7 Shelf.

Column Name	*Description*
NetworkName	Name of the C7Network to which this node belongs
DeviceName	This is the value as obtained from the calixDeviceName column of the calixProxyAgentMib. For a node this will be in the format N1,N2 etc and for a shelf this will be N1-1,N2-1 etc.
NodeNumber	This represents the node number
ShelfNumber	This represents the shelf number
Name	This is the name of node or shelf

The parent-child relationship is maintained between the C7 Network-Node-Shelf objects. While adding the C7 objects the C7Network is set as the parent for C7Node and the C7Node is set as the parent for C7Shelf.

88.4 Topology

The C7 Network would be listed under the Network Elements node of the topology tree. As there can be multiple C7 networks, each network is represented as a separate tree node. The topology tree for the Calix device is as below

Network Elements
C7 Network
- Net1
- N1

- N2

where ,
Net1 – is the displayName of the C7 Network as given while provisioning the network.
N1, N2 – represent the nodes of the provisioned network

The C7 Network, Net1, N1 and N2 all bring up a map when clicked.

On selecting the C7 Network tree node all the provisioned networks are listed in the right hand panel. These networks would also appear on selecting the Network Elements tree node.

On selecting the Net1 tree node all the nodes for that network are shown in the right hand panel.
On selecting the N1 and N2 tree node the corresponding shelves under that node are shown in the right hand panel.

89: Functional Description(FN): A00009611

89.1 Feature name and Feature ID

A00009611 IEMs Keymile Integration

89.2 Introduction

The UMUX Multi-service Access platform comprises a range of modular multi-service network elements (UMUX 1500/1200/900) and can be configured/managed by Keymile's UMUX Network Element Manager (UNEM).

IEMS serves as an integrated platform for managing various devices. The Keymile devices UNEM/ UMUX NEs Multi-service Access platform will also be managed by IEMS. This document lists the changes that are required in IEMS in order to manage a UMUX device.

The UMUX implements two network management interfaces: GUI and SNMP. IEMS will use the SNMP interface for inventory and fault management. GUI would be used in the form of launches.

89.3 Acronyms used

IEMS – Integrated Element Management System
GUI – Graphical User Interface
SNMP – Simple Network Management Protocol

89.4 IEMS Changes

89.4.1 UNEM Provisioning

The UNEM can be provisioned in IEMS as an Element Manager. The UNEM can be added from the existing Tools-->Add-->EMS / NE menu. The IPAddress field represents the IP of the UNEM . 'Type' should be selected as EMS. In the 'Device Type' a new entry, named 'UNEM Mgr', will be added. The SNMP details can be filled up on the next screen. This would be the same as the existing Fault Interface screen for other snmp devices.

89.4.2 Topology

The UNEM would be listed under the Element Managers node of the topology tree. As there can be multiple UNEM networks, each network is represented as a separate tree node. The topology tree for the UNEM device is as below

89.4.2.1 Element Mangers

- EMS-UNEM-Mgr (displayName of the UNEM)

- EMS-UNEM-Mgr (displayName of the UNEM)

89.4.2.2 Network elements

The UMUX Network Elements (UMUX 900/UMUX1200 & UMUX1500) will be auto discovered and added to the inventory. These network Elements will be represented in the tree as below

Network Elements
|-UMUX-1200
|-UMUX-1200-(displayName of the UNEM)
|-UMUX-1200-(displayName of the UNEM)
|-UMUX-900
|-UMUX-900-(displayName of the UNEM)
|-UMUX-900-(displayName of the UNEM)
|-UMUX-1500
|-UMUX-1500-(displayName of the UNEM)
|-UMUX-1500-(displayName of the UNEM)

The UMUX -1200 map will contain all the nodes of NE type (UMUX-1200) of a given UNEM Mgr which will be indicated using the displayName of the UNEM Mgr.

The UMUX -900 map will contain all the nodes of NE type (UMUX-900) of a given UNEM Mgr which will be indicated using the displayName of the UNEM Mgr.

The UMUX -1500 map will contain all the nodes of NE type (UMUX-1500) of a given UNEM Mgr which will be indicated using the displayName of the UNEM Mgr.

The neTable with the below mentioned information will be used to populate the Inventory table for the UMUX devices.

neFamily,neIndex,neName,neUNEMAdress,neType,

neFamily + neIndex -- will be the unique name of the UMUX devices

neName -- will be mapped to the displayName

neType – will represent the type of the device (family)

89.4.2.3 Inventory Synchronization

The Inventory Synchronization can happen on the below mentioned conditions:

- While IEMS is restarted
- When ever a trap loss is detected, IEMS will automatically invoke reSync of Inventory.

- Manually invoking the ReSync Inventory

89.4.3 Topology Trap handling

The below mentioned topology traps will be handled:

- neAddedTrap -- IEMS checks for the type of the device and if the type is either
- (neType-11, neType-8, neType-7) the same will be added to the inventory table. All other traps will be considered as traps from unknown devices and the traps will anyway be forwarded to the north bound as INFO events.
- neDeletedTrap – IEMS checks for the corresponding entry in the inventory table and deletes the device. For all the traps originating from the unknown device and the trap will be forwarded as an INFo event to north bound.
- neNameChangeTrap – IEMS checks for the corresponding entry in the inventory table and changes the neName (displayName) of the device. For all the traps originating from the unknown device and the trap will be forwarded as an INFo event to north bound.
- neOpStatModifiedTrap – IEMS will just forward the trap to the NorthBound as INFO events and will not store them in the Alarms table.
- nePollStatModifiedTrap - IEMS will just forward the trap to the NorthBound as INFO events and will not store them in the Alarms table.
- CardAddedTrap – IEMS will forward the trap to the NorthBound as INFO events and will not store them in the Alarms Table.
- CardDeletedTrap – IEMS will forward the trap to the NorthBound as INFO events and will not store them in the Alarms Table.

All the system traps (alarmNEFamily – 4 & alarmNE – 9999) will be mapped to the UNEM

90: Functional Description(FN): A00009612

90.1 Feature name and Feature ID

A00009612 Restricted Shell Access

90.2 Description

"Restricted Access Shell" in SN09 provides a new default shell for interactive users. This shell (called rash), unlike sh or ksh or bash will limit the available suite of commands. Additionally a user will not be able to alter their path and will therefore be restricted to only those commands authorized. Additional commands can be registered to be available to rash via servman.

Two of the commands used by IEMS that fall into this restricted access morass are telnet and ssh. As a result, the proxied "Command Line" context menu item used from the IEMS map will no longer work. The invocation of the telnet or ssh command will elicit a "command not found" message when invoked from rash.

In a proxied command line scenario the IEMS client uses SSH (Mindterm) to establish and login to a shell session on the IEMS server. From there the ssh or telnet command is issued and another SSH or telnet session is established with the southbound NE or EMS. The shell session on the IEMS server will use the restricted access shell provided by A00009310 and hence will be prohibited from invoking either the telnet or ssh commands.

This component will rectify this and insure that the proxied command line in SN09 will retain functionality equivalent to that found in SN08. A script (IEMSProxyCommandLine) will be created for the telnet and ssh commands on the IEMS server that will,

1 Perform a check to insure that the logged in user is authorized to access the target device. The check will use the same logic and code provided by IEMS. The users membership in the 30 Succession groups and any policy rules defined in the IEMS server will dictate authorization.

2 Create an audit log for successful authorization or a security log for unsuccessful authorization.

3 invoke the real ssh and telnet command to establish a remote session with the target device.

The script will support all options and parameters of both ssh and telnet and will not alter either the performance or appearance.

Additionally a login to the IEMS server will place the user into a restricted access shell with a home directory as defined in users profile in the security

server. A script run from pam during login will create the user's home directory and copy skeleton profiles to it.

90.3 Hardware Requirements or Dependencies

Not applicable

90.4 Software Requirements or Dependencies

This is required due to implementation of A00009310.

90.5 Limitations and restrictions

None

90.6 Interactions

90.6.1 IEMSProxyCommandLine script

The IEMSProxyCommandLine script will support all options and parameters of both ssh and telnet and will not alter either the performance or appearance. It does introduce any new options or arguments.

90.6.2 Home Directory and Skeleton Profiles

The home directory of the user will be created. Additionally, two sub-directories of "data" and ".ssh" will be created. The former is read-write and available at the discretion of the user. The latter is used to store public encryption keys used by ssh. Skeleton profiles, shipped with SSPFS and found in /etc/skel.rash, will be copied into the home directory.

90.6.3 Logs

An Audit Log Entry would be found for a successful authorized access.

Feb 22 11:39:37 comp5iems IEMS: IEMS class_security.ver01 STAT=SUCCESS SRC.USR=gumby EVNT.TYPE =/usr/bin/ssh to 47.142.106.26, device type EMS-CS2K-Mgr

A Security Log Entry would be found for an unsuccessful, unauthorized access. Note that for authorization to succeed both the userid and the target host ipaddress must be known to the IEMS server. If either is unknown then the authorization will fail.

Feb 22 11:39:37 comp5iems IEMS: IEMS class_security.ver01 STAT=FAILURE SRC.USR=gumby EVNT.TYPE =/usr/bin/ssh to 2.3.4.5, device type GWC

90.7 Glossary

91: Functional Description(FN): A00009614

91.1 Feature name and Feature ID

A00009614: Tamper-proof Key Storage and Event Generation

91.2 Description

This document will cover work for IEMS and SSPFS. This document does not address key material owned and controlled by the Security Server.

Key material is defined to be anything that is used to authenticate a user or machine to another machine. This includes X.509 certificates, cryptographic keys, userids, passwords, and SNMP community strings.

This feature will create cron job that will run once a day to:

- Generate a minor alarm for the expiration or warning expiration of certificates.
- Generate an alarm for the expiration of system or local accounts and passwords. A system account is defined to be any account used for program to program or machine to machine authentication.
- Generate an alarm warning that an account or password is about to expire.

Scripts that manage key material will also generate a security log for any attempt to add, delete, or modify key material--whether valid or under attack.

Alarm and log details can be found in the Fault Management (FM) section that follows.

91.3 Hardware Requirements or Dependencies

Not applicable

91.4 Software Requirements or Dependencies

This feature uses:

- the cron facility of unix to run a program periodically.
- the perl interpreter

91.5 Limitations and restrictions

This feature will not cover central user accounts managed by IEMS or certificates automatically generated by IEMS Security Server during installation.

91.6 Interactions

91.7 Glossary

Term	Description

92: Functional Description(FN): A00009616

92.1 Feature name and Feature ID

A00009616: IEMS Backward Compatibility and Upgrade

92.2 Introduction

IEMS serves as an integrated platform for managing various devices. This module is for providing Backward Compatibility in IEMS so that all the SN09 device versions and the previous device versions (n –2) are supported in IEMS. This document lists the devices and the changes required for the devices. The document also covers client interoperability and Upgrades.

92.3 Backward Compatibility

92.3.1 Device Version Changes:

In SN08 when an EM/Platform/application is added a drop down to choose the version is provided in most cases. The SN08 drop down box contains the following versions namely 6.2, 7.0 and 8.0. The SN09 version of IEMS will not support the 6.2 version of devices. So the SN09 drop down box will not contain the 6.2 version and it will contain 07, 08 and 09 versions.

SAM21-Mgr is an exception here. The user can provision the version as NONE for SAM21-Mgr. IEMS will auto-populate the version for SAM21-Mgr for the first time when it gets discovered. IEMS will query the versioned interface and populate the device version in the IEMS database of its own.

92.3.2 IEMS Version Changes:

In SN09, all the GUI titles/About boxes will show 09 as the current IEMS Version. The version of the package as output by the pkginfo command will show 09 as the current IEMS Version e.g., VERSION: IEMS_8_03_0 ==> IEMS_090_0503.

The output of pkginfo command:

```
iems-sf2:/> pkginfo -l IEMS
 PKGINST:IEMS
      NAME:Nortel Networks Integrated EMS
        CATEGORY:application
       ARCH:sparc
VERSION:IEMS_090_0503
```

```
BASEDIR:/opt/nortel/iems/current
VENDOR:Nortel Networks
 PSTAMP:cmsol2-build20050221080539
           INSTDATE:Jan 23 2005 08:14
 STATUS:completely installed
      FILES:3908 installed pathnames
             197 directories
               69 executables
         192995 blocks used (approx)
```

92.3.3 CBM Security Integration

SSO is being introduced on CBM in SN09. CBM will point back to IEMS server for authentication. Hence the launch of SSPFS with CBM needs to be performed via SSO in IEMS SN09.

To address the above requirement the following changes needs to be performed in IEMS.

1. Radius configuration of the CS2K Core Manager needs to happen during provisioning.
2. The launch of command line needs to be SSO enabled. Launch needs to be consistent with SDM.
3. Upgrade of CBM from version 07 to 09 should give options to include any new attributes.
4. Upgrade of CBM from version 08 to 09 should give options to include any new attributes.
5. SN09 IEMS should be backward compatible with older CBM versions.

92.3.4 MDM Integration in SSPFS

The following changes needs to be performed in IEMS for MDM moving to SSPFS platform.

1. When provisioning an MDM in IEMS an option needs to be provided for the user to select if the platform is SSPFS or not.
2. If user chooses SSPFS:
   - IEMS will not auto discover the platform in IEMS topology as we do in SN08. Platform Alarms will correlate to the MDM EM.
   - User should be able to associate an SSPFS platform if it has already been added.

— User will have to manually add the SSPFS platform.

3. If user selects no-SSPFS, existing behavior as in SN08.

92.4 Supported OS and browsers

The SN09 version of IEMS Client will be supported in the following Operating Systems and web browsers.

92.4.1 PC Platform

	Win 2000, SP4	Win XP, SP2
IE 6 SP1	YES	YES
Netscape 6.2+	YES	YES

92.4.2 Sun Platform

	Solaris 8 (2.8, 5.8)	Solaris 9 (2.9, 5.9)
Mozilla (1.4 +)	YES	YES
Netscape 6.2+	YES	YES

92.4.3 Collection Job Changes

In SN08, when defining a collection job by default the discovered devices are added into the job. The list of discovered device IPs is listed in the "Exclude Device List". If a user want to exclude some device, he needs to uncheck (x) the device, which listed in the "Exclude Device List".

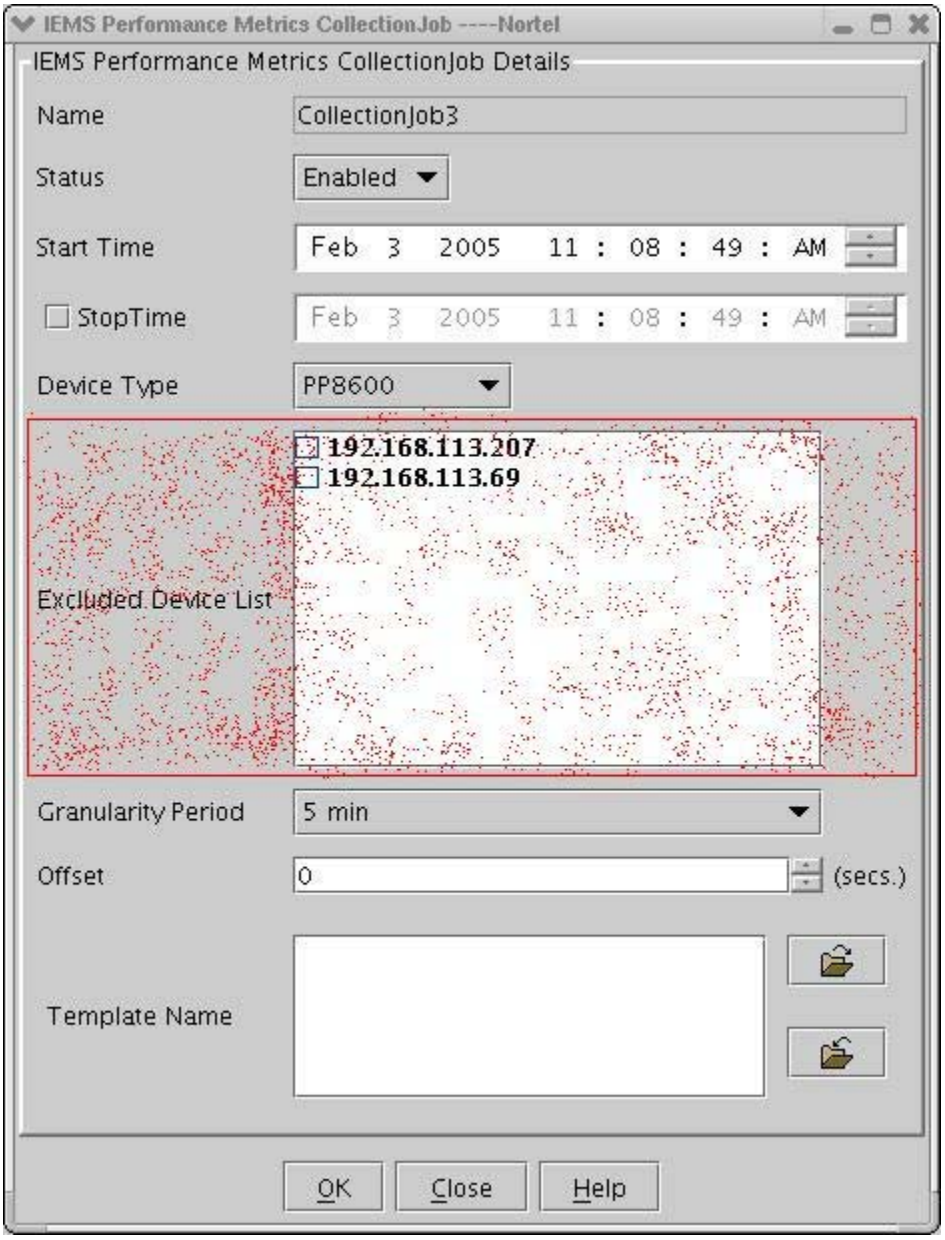


Figure 1 SN08: Collection Job Configuration Screen

But in SN09, when defining a collection job by default the discovered devices will not be added into the job. When defining a collection job user needs to add the devices (by enabling the check box) into the Collection Job i.e., the "Exclude Device List" is changed to "Include Device List".

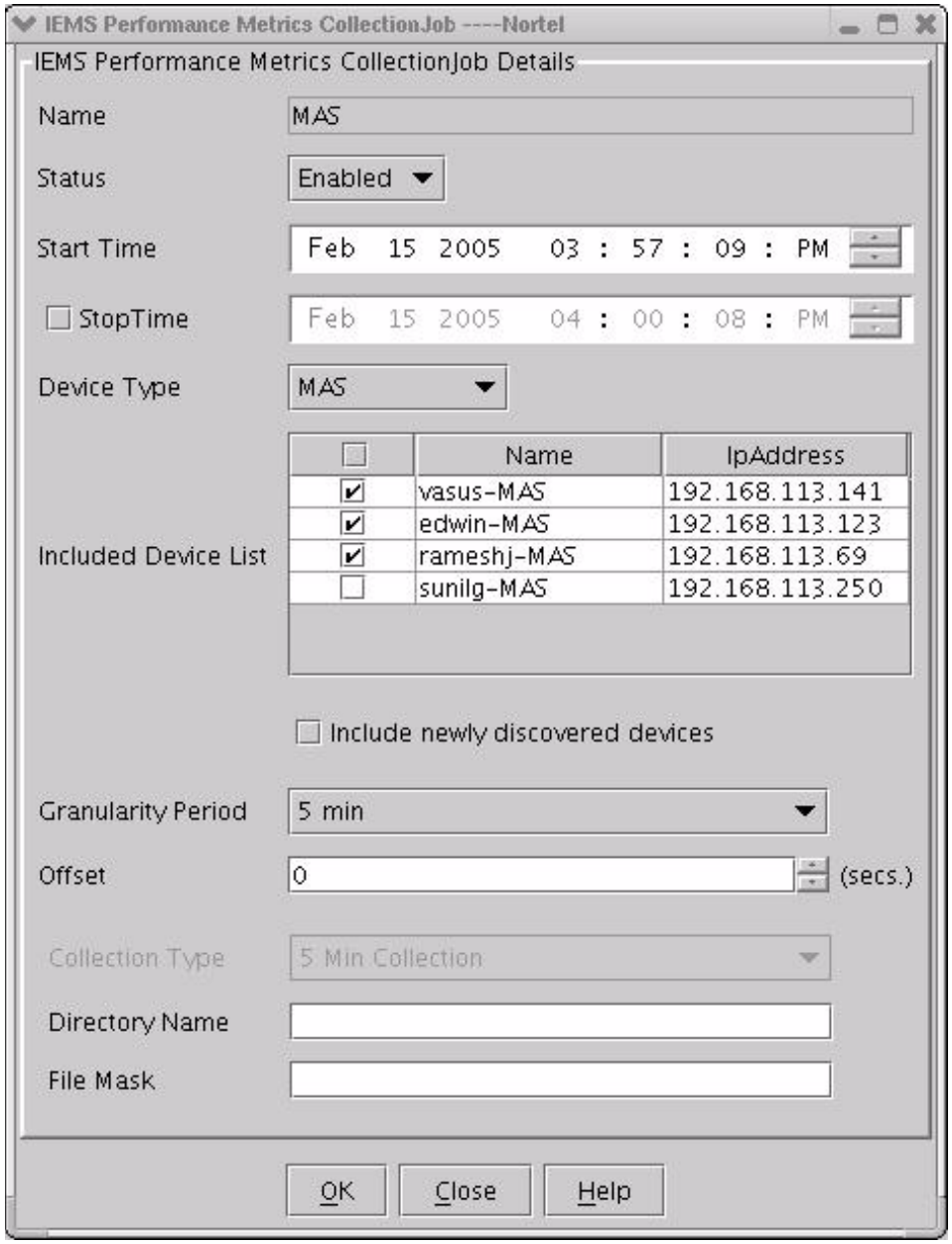


Figure 2 SN09: Collection Job Configuration Screen

The device list will be displayed in a table structure. The table has 3 columns with following headers,

- (Just a check box)
- Name
- IP Address

The first column header and all the first column cells will contain a check box. All the check boxes will be unchecked by default. If a user check /uncheck the first column header then, it will automatically check /uncheck all the devices in the table. The discovered devices name and IP Address will be displayed in the second and third column of the table respectively. The data collection will be performed only selected (checked) devices.

The checkbox “Include newly discovered devices” will be unchecked by default.
If this checkbox is checked, the data collection will be performed for the newly discovered devices.

For the already existing jobs in SN07/SN08 when migrated to SN09, the excluded device list will be displayed as unchecked in the new collection job GUI. This will be taken care during data migration from SN07/SN08 to SN09.

92.5 Upgrades

92.5.1 Upgrade Path

This section covers the functional description for IEMS (IEMS/MFT/CEM) upgrade in the following scenarios:

- SN07 to SN09 Upgrade
- SN08 to SN09 Upgrade
- SN09 to SN09 Upgrade
- SN09 to SN07 Rollback
- SN09 to SN08 Rollback
- SN09 to SN09 Rollback

92.5.2 Limitations & Restrictions:

- Downgrade of IEMS is not within the scope. i.e. Once the upgrade/ migration is completed fully and the SN09 version of IEMS is running, the downgrade of SN09 data to be compatible with SN08 / SN07 is not supported.
- Rollback will involve only Backup & Restore and hence it will resume activity at the last “save” point. Separate Rollback is not done for IEMS.
- IEMS server will not be running while upgrade procedure is invoked. HA upgrades will occur on inactive unit.
- IEMS does not support a “no outage” upgrade. The outage window is mainly determined by the failover time needed for SSPFS HA systems. In case of Simplex it will be the time required for completing the IEMS upgrade procedure and starting IEMS.

- IEMS upgrades do not support migration. This includes:
- Migration from a standalone IEMS to a co-resident IEMS (IEMS + CMT)
- Migration from a co-resident IEMS to a standalone IEMS
- If the Upgrade/Data migration fails, the only recovery technique is to restore via a file system backup.
- IEMS does not support a hardware migration.

In SN09 release, Integrated EMS will reside on the following platforms:

- Standalone (Integrated EMS on SSPFS)
  - On single N240 (simplex) 4G - NTRX51LC
  - On dual N240 (HA) 4G - NTRX51LC
- Co-Residency (CS2M & Integrated EMS on SSPFS)
  - On single N240 (simplex) 4G - NTRX51LC
  - On dual N240 (HA) 4G - NTRX51LC
  - On single T1400 (simplex) 4GB Only – NTRX51KW - Requires a T1400 upgrade procedure - for existing T1400customers only. No new T1400 installs are planned.

92.5.3 Hardware upgrade paths

The Integrated EMS will require the following upgrade plans

- T1400 in OAME cabinet standalone -> T1400 co-resident in OAME cabinet
- N240 simplex with CS2M in COAM cabinet -> N240 simplex co-resident in COAM cabinet
- N240 simplex in COAM cabinet -> N240 co-resident HA in COAM Fame
- OAME cabinet to COAM cabinet

92.5.4 Upgrade Procedure:

92.5.5 IEMS Upgrade pre-check:

A standalone script file (IEMSUpgradePreCheck.sh) will be present under <IEMS home>/bin directory.

The purpose of the pre-check script is so that the user can run this prior to upgrading f*rom* SN09 to a higher version. The script takes the *to* version as the input and lists all the devices that are not supported. The user should run this script before the upgrade and this should be documented in the steps. This script could potentially be used to interface into the upgrade manager.

Usage of the script file:

```
iems-sf2:/export/home/maint> sh
IEMSUpgradePreCheck.sh

Usage : sh IEMSUpgradePreCheck.sh <Version>

<Version> - 7 (or) 8 (or) etc..
```

Note: Do not give Version as SN07 (or) SN08 (or) etc..

Output of the script file:

iems-sf2:/export/home/maint> sh IEMSUpgradePreCheck.sh 9

```
IEMS Upgrade Pre-Check Test :

****************************

The IEMS upgrade pre-check test passed. The IEMS
upgrade may proceed.
```

```
iems-sf2:/export/home/maint> sh
IEMSUpgradePreCheck.sh 11

IEMS Upgrade Pre-Check Test :

****************************

The IEMS upgrade pre-check test Failed. The IEMS
upgrade should not proceed.

Device version check failed. The following devices
must be upgraded prior to

proceeding with the IEMS Upgrade to SN011:-

=========================================

| S.No. | Device Name       |   Version  |

=========================================

| 1     | umanand-MAS         |     8.0    |

| 2     | umanand-STORM    |     8.0    |

| 3     | USP-1328              |     8.0    |

| 4     | karanmercy-PP8600     |     8.0    |
```

In IEMS SN09, all the SN09 device versions and the previous device versions (n –2) are only supported. If any device of lower version (ex: 6.2) is found during data migration the IEMS upgrade will be aborted.

Note:

- If upgrade fails, the user needs to perform an entire restore of the backed up SSPFS image.
- If there is an MR release, the newly introduced device versions will also be taken care by this script file. For example in SN09 release the following versions will be supported.
  - 08
  - 07.1 (MR device version)
  - 07

A brief description of the different scripts involved.

92.5.5.1 Comboload Script:

This is basically the shrink-wrap script that controls the sequencing of the calls to the other scripts. It makes calls on the MFT scripts, CEM scripts, and data export scripts. It also is responsible for swapping the pam, nscd and nsswitch conf files, backing up and restoring some of the MFT conf files.It also provides warnings to users for missing SSL certs, and incorrect oracle file system sizes. The IEMS team owns this script.

92.5.5.2 MFT Script:

This script provides interfaces used by the comboload script to uninstall, install and start the MFT software. This script also takes care of the data migration. This script is not directly called by the user and is hidden in a zip file. It is unzipped and used by the comboload script. The MFT team owns this script.

92.5.5.3 CEM Script:

This script provides interfaces used by the comboload script to uninstall and install the CEM load. This script is not to be directly used by the user. The CEM team owns this script.

Data migration includes user data (security) as well as provisioning, faults, performance data. While this feature will test the combined install and upgrade, each of the subcomponents (MFT, CEM) are responsible to test their individual upgrade process and data migration and will provide input to the overall process to simplify/eliminate any manual steps involved.

Upgrade will be aborted if any devices outside the supported range are found. The Upgrade pre-check script (IEMSUpgradePreCheck.sh) will check for the non-supported devices as a first step during upgrade. Upgrades will continue only if the pre-check test gets passed.

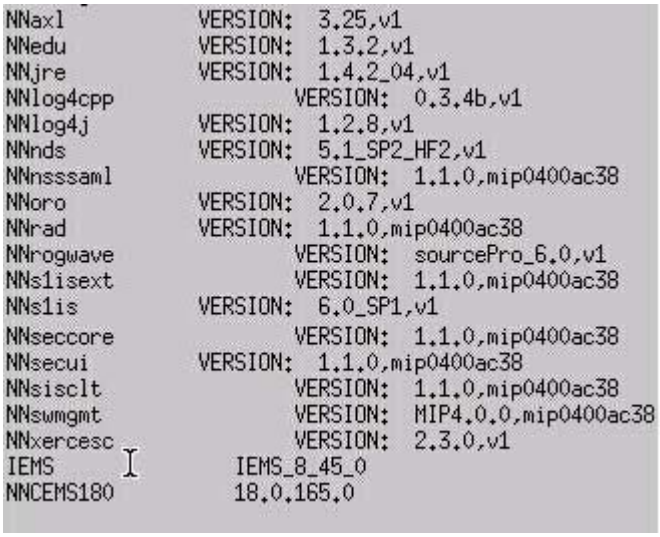
If Upgrade fails due to the presence of any non-supported devices, the user needs to follow the restore procedure to proceed.

92.5.6 SN07 – SN09 Upgrade:

For SN07 to SN08 upgrade,refer to *Upgrading a Carrier Voice over IP Network*, NN10440-450.

The comboload script file (appl_mgr.ksh) will be used to Install/Upgrade - SN09 Version of IEMS, before the IEMS SN09 server gets started the migration procedure will gets invoked.

Executing the comboload script file will display a message similar to the following screen shot.



The Upgrade process may take up to thirty minutes approximately. A message appears similar to the following screenshot:

```
Performing pkgrm on IEMS...
Successfully removed package IEMS

Installing the new security server components...
Done installing the new security server components.

==================================
Checking version of IEMS package...

Installing IEMS Package...
Done Installing IEMS Package.

Installing the CEM ...

==================================
Upgrade of the IEMS software package completed successfully
Configuring ... this may take a few minutes
Restoring backed up conf files
Configuration complete.
```

The IEMS data migration occurs in the order detailed below:

- Database Schema Migration - schema related changes
- Data Migration - device related changes needs to be handled here
- Configuration Migration - conf related changes

In case of failure in the upgrade / migration at any instance, the data and configuration changes done for the upgrade are reverted completely. The data and configuration can now be used again with the SN07 software.

92.5.7 Database Schema Migration

Database Schema Migration takes care of migration for any database schema changes that have been done for the SN09 version. Schema changes include changes such as:

- Any database tables added newly for SN09.
- Any new columns added to the existing database tables.
- Any change in the data type for the existing column in a table. Ex: Some of the columns of database tables existing in SN07 have been extended in SN09 to accommodate the additional data. Extension in column length is performed as required in SN09.

92.5.8 Data Migration

In addition to the schema changes, the format in which data is stored in the database may also have changed in the SN09 version of IEMS. In order to migrate the SN07 data to the format required in SN09, the data migration is done for the following functionalities.

1. Package name changes.
2. Rebranding.
3. Alert Filters & Event Filters conf update.

92.5.9 Configuration Migration

Changes made in Configuration files by the user at runtime while using the SN07 load will be backed up before removing the SN07 Software. And during the migration process the configuration files that were backed up earlier will be restored to preserve user changes in the new SN09 version of IEMS. Configuration files that will be backed up and restored are:

- oidtemplates – All XML files present in the oidtemplates directory will be backed up while uninstalling SN07 and restored at SN09 migration
- logging_parameters.conf
- event.filters
- alert. filters

92.5.10 Rollback

If the upgrade to the newly installed version of software fails before the point of no return (before executing the clean up scripts), all the changes done for migrating the data are reverted to the original state.

If failure occurs during Upgrade the following steps needs to be followed for a complete rollback:

- Downgrade SSPFS platform.
- Import Integrated EMS data (Integrated EMS, CEM).
- Restart MS20x0 application (for co-resident).

92.5.11 SN08 - SN09 Upgrade

The comboload script file (appl_mgr.ksh) will be used to Install/Upgrade - SN09 Version of IEMS, before the IEMS SN09 server gets started the migration procedure will gets invoked.

Executing the comboload script file will display a message similar to the following screen shot.

```
NNaxl          VERSION:  3.25,v1
NNedu          VERSION:  1.3.2,v1
NNjre          VERSION:  1.4.2_04,v1
NNlog4cpp              VERSION:  0.3.4b,v1
NNlog4j        VERSION:  1.2.8,v1
NNnds          VERSION:  5.1_SP2_HF2,v1
NNnsssaml              VERSION:  1.1.0,mip0400ac38
NNoro          VERSION:  2.0.7,v1
NNrad          VERSION:  1.1.0,mip0400ac38
NNrogwave              VERSION:  sourcePro_6.0,v1
NNs1isext              VERSION:  1.1.0,mip0400ac38
NNs1is         VERSION:  6.0_SP1,v1
NNseccore              VERSION:  1.1.0,mip0400ac38
NNsecui        VERSION:  1.1.0,mip0400ac38
NNsisclt               VERSION:  1.1.0,mip0400ac38
NNswmgmt               VERSION:  MIP4.0.0,mip0400ac38
NNxercesc              VERSION:  2.3.0,v1
IEMS           IEMS_8_45_0
NNCEMS180      18.0.165.0
```

The Upgrade process may take up to thirty minutes approximately. A message appears similar to the following screenshot:

```
Performing pkgrm on IEMS...
Successfully removed package IEMS

Installing the new security server components...
Done installing the new security server components.

==================================
Checking version of IEMS package...

Installing IEMS Package...
Done Installing IEMS Package.

Installing the CEM ...

==================================
Upgrade of the IEMS software package completed successfully
Configuring ... this may take a few minutes
Restoring backed up conf files
Configuration complete.
```

The IEMS data migration occurs in the order detailed below:

- Database Schema Migration - schema related changes
- Data Migration - device related changes needs to be handled here
- Configuration Migration - conf related changes

In case of failure in the upgrade / migration at any instance, the data and configuration changes done for the upgrade are reverted completely. The data and configuration can now be used again with the SN08 software.

92.5.12 Database Schema Migration

Database Schema Migration takes care of migration for any database schema changes that have been done for the SN09 version. Schema changes include changes such as:

- Any database tables added newly for SN09.
- Any new columns added to the existing database tables.
- Any change in the data type for the existing column in a table. Ex: Some of the columns of database tables existing in SN08 have been extended in SN09 to accommodate the additional data. Extension in column length is performed as required in SN09.

92.5.13 Data Migration

In addition to the schema changes, the format in which data is stored in the database may also have changed in the SN09 version of IEMS. In order to migrate the SN08 data to the format required in SN09, the data migration is done for the following functionalities.

- Package name changes.
- Rebranding.
- Alert Filters & Event Filters conf update.

92.5.14 Configuration Migration

Changes made in Configuration files by the user at runtime while using the SN08 load will be backed up before removing the SN08 Software. And during the migration process the configuration files that were backed up earlier will be restored to preserve user changes in the new SN09 version of IEMS. Configuration files that will be backed up and restored are:

- oidtemplates – All XML files present in the oidtemplates directory will be backed up while uninstalling SN08 and restored at SN09 migration
- logging_parameters.conf
- event.filters
- alert. filters

92.5.15 Rollback

If the upgrade to the newly installed version of software fails before the point of no return (before executing the clean up scripts), all the changes done for migrating the data are reverted to the original state.

If failure occurs during Upgrade the following steps needs to be followed for a complete rollback:

- Downgrade SSPFS platform.
- Import Integrated EMS data (Integrated EMS, CEM).
- Restart MS20x0 application(for co-resident).

92.6 References

92.7 Glossary

IEMS - Integrated Element Management System
EM - Element Managers
HA - High Availability
SM - System Manager
FPM - Fault Performance Manager.
SSH- Secure Shell

93: Functional Description(FN): A00009651

93.1 Feature name and Feature ID

A00009651: Meet Me Web Collaboration Multilingual

93.2 Description

93.2.1 Background

Meet Me Web Collaboration was introduced as a Fast Feature in the MCS 3.0 release and only supported English on the collaboration web pages presented to users. This activity incorporates the FTR 424 Fast Feature into the 9.0 release and enhances it by adding multilingual support for the collaboration web pages.

93.2.2 Overview

Web Collaboration allows people in different locations to view a PC generated presentation over the IP based network. The initial release of Web Collaboration did not include support for multiple languages. It is expected to provide the same languages supported within other portions of MCS.

In prior releases, MCS users have had the ability to select language preferences both as personal preferences for their PA, and by dialing Meet Me alias numbers that are associated with a specific language. This feature extends the language choice indicated by the Meet Me alias dialed, to the Web Collaboration GUI (tool tips and dialog boxes, and user help). As a result, the audio prompts of the conference and the display on the collaboration web pages will be in the same language. It is not intended to translate the presenter’s presentation.

Below is the list of languages supported in MCS 09. Meet Me Web Collaboration supports the same set of languages as the other MCS network components

1. English
2. Parisan French
3. Latin America Spanish
4. German
5. Japanese
6. Traditional Chinese
7. Simplified Chinese
8. Korean

93.3 Feature Description

93.3.1 Operator Configuration and Provisioning

This section presents Meet Me Web Collaboration configuration and provisioning information needed by operators and installers of the MCS solution.

93.3.1.1 Installation

Each Web Collaboration server must be configured with the required collaboration software. The major applications which will be installed are listed below.

- Microsoft Server 2000: Operating System (custom OS image is included on the hardware when ordered).
- Web Collaboration Application: Server side Web Collaboration software
- Provider Supplied:
  - Microsoft Office 2003: Office productivity Application suite required for collaborative document presentation (Word, PowerPoint and Excel)
  - MSDE 2000: Database required for run time collaboration data storage
  - IIS: Web Server
  - MS Internet Explorer 6.0
  - SSL 128 Certificates for HTTPS

93.3.2 Administrator Configuration and Provisioning

This section presents configuration and provisioning information needed by the system administrators for daily service and end-user support.

No new configuration or provisioning tasks are added.

93.3.3 Feature Provisioning

There are no new Meet Me Web Collaboration configuration options available to the end-user. However, all the existing Meet Me options a user has in their Personal Agent also apply to Meet Me Web Collaboration sessions. The user's language selection for their Meet Me Conference and Collaboration session is determined by the ALIAS dialed. The available Alias's are listed for a user in there PA under their Meet Me Preferences (language specific Meet Me aliases are not a new feature).

93.3.4 Feature Behavior

93.3.4.1 Overview

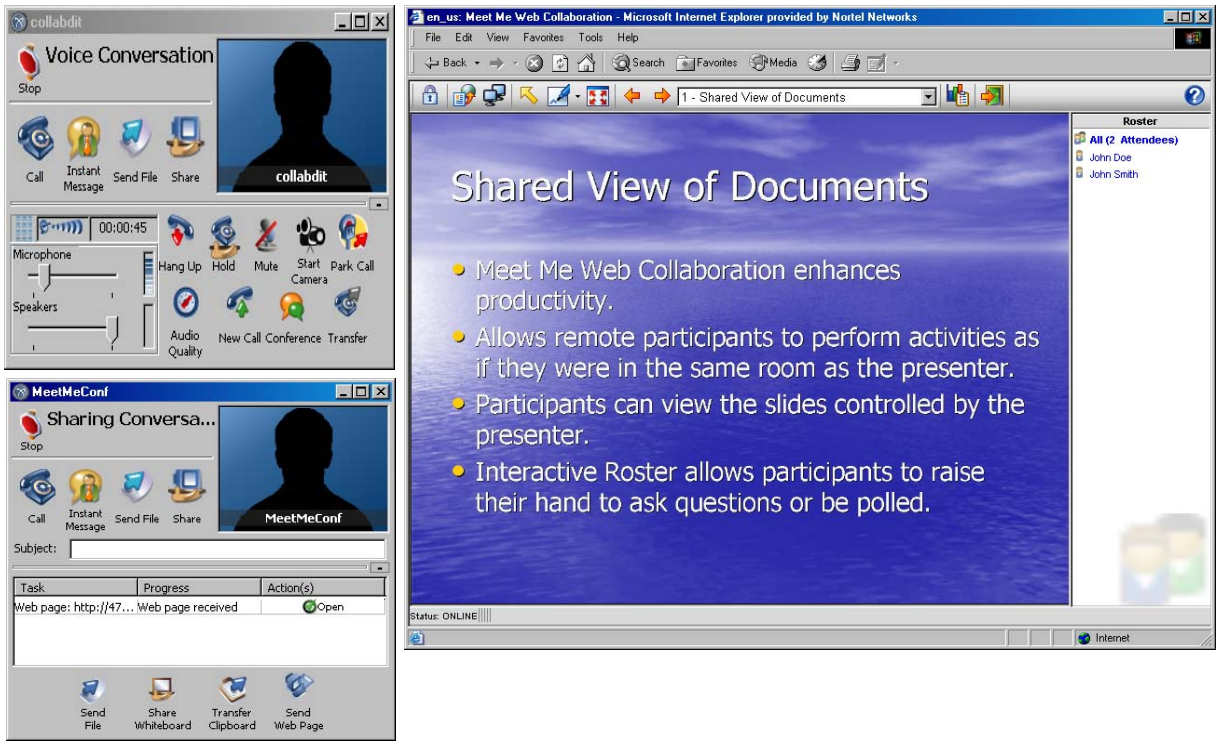
Language selection and use in the collaboration session is based upon Meet me Conference **alias a user dials**. The available aliases are listed for a user in their

PA under their Meet Me Preferences (language specific Meet Me aliases are not a new feature). Prior to the Multilingual Support for Web Collaboration, only the audio prompts reflected the language indicated by a dialed alias. N**ow the Collaboration session will also reflect the language indicated by the dialed alias**.

In addition to multilingual support, a few other enhancements are introduced. as outlined in this section.

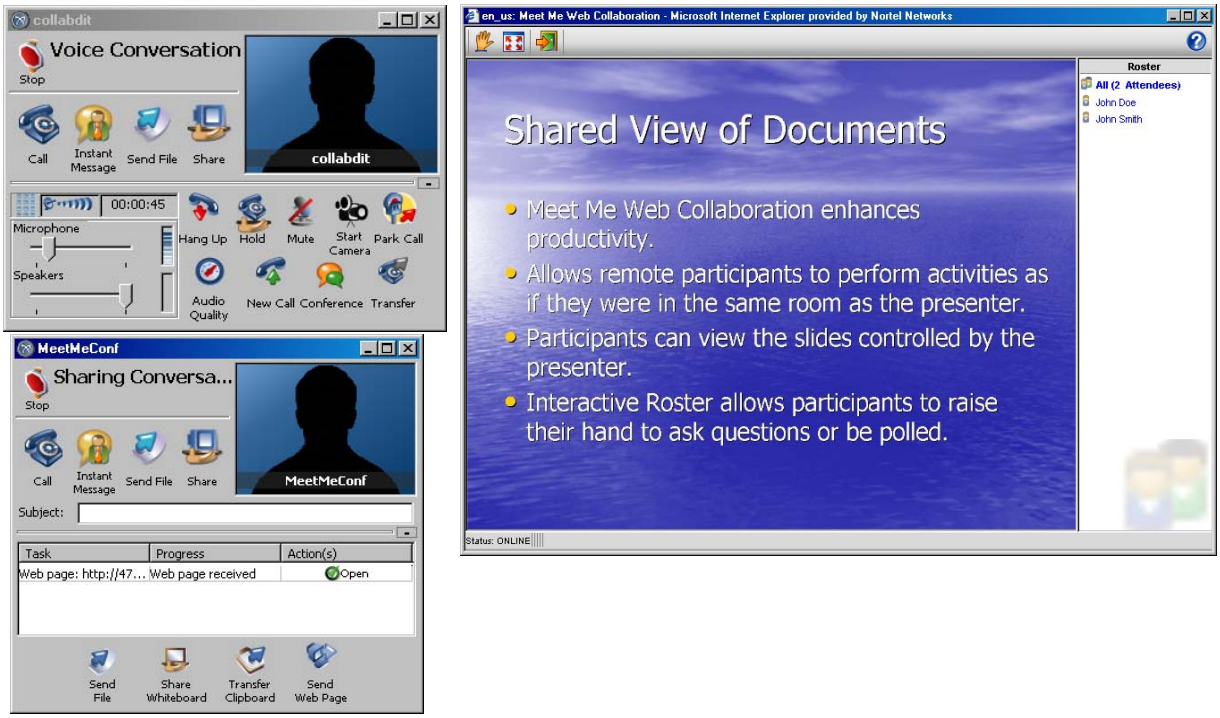
There have been some minor graphical updates to the displays as shown in the following figures.

Figure 1: Presenter's Client Call Control Window and View of Published Material



The participants now have a roster showing other participants. The main difference between the presenter and participant windows is the options available on the tool bars.

Figure 2: Participant's Client Call Control Window and View of Published Material



The publish interface has been changed and enhanced. There is a new window for publishing and the presenter (chairperson) may now login early and prepublish 1-30 documents. A presenter can then quickly jump between documents with out waiting for the uploading and conversion process of publishing. (All the documents are deleted when the Collaboration session is ended.).

To publish a document:

1 From the Presenter toolbar, click the Publish Documents icon . The "Publish Documents window is displayed.

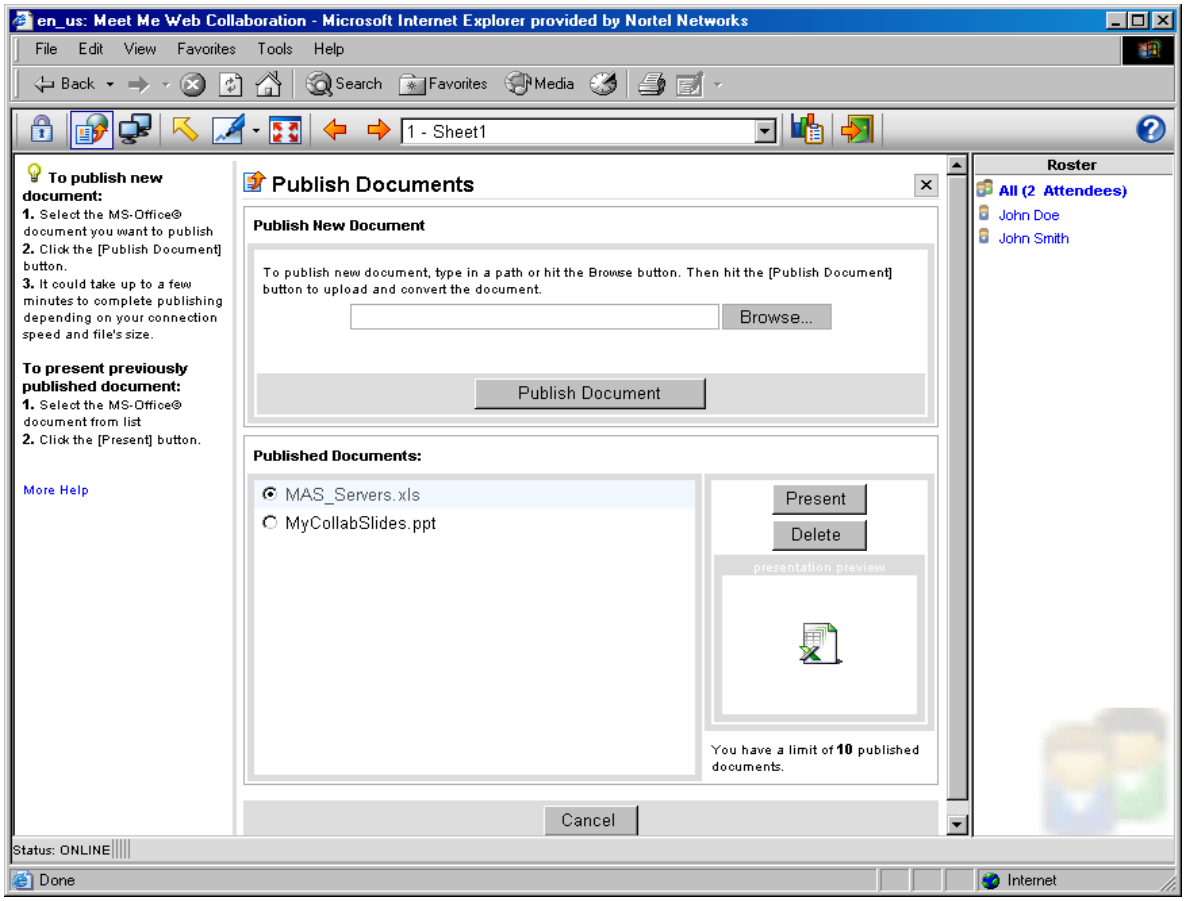
2 Click Browse, navigate to the directory containing the document to publish, and select the document.

3 Click Open.
The user is returned to the "Publish Documents" window and the full path to the document is displayed.

4 Click Publish Document.
The document is displayed in the main window. Note that uploading a document can take several minutes, depending on the speed of the network connection and the size of the document.

When the presenter is finished with one document, they may click the Publish Documents icon to return to the Publish New Document window to publish or present other documents.

Figure 3: Presenter Publishes Content



The presenter uses the above window to publish and manage published documents during a collaboration session. Office documents are published by using the Browse… button, selecting a file and then pressing the Publish Document button. Once this is done, the “Published Documents:” panel shows all the documents ready to present. A radio button allows selection of a particular document. The buttons Present and Delete perform the corresponding action on the selected document. All documents are deleted when the collaboration session ends.

The collaboration tool bars have been internationalized. The English labels under each button have been removed and replaced with hover help text which displays in the users language. The tool bar buttons also have a new graphic look and are defined below.

The Web Collaboration presenter's window has a tool bar with controls for the presentation. The following functionality is available to the presenter on the Presenter's Tool bar:

	Publish	Allows the presenter to specify the file to be published. After selecting the desired file the document is converted to a web publishable HTML format.
	Share	Allows the presenter to graphically share the view of any running program on their computer with participants.
	Point	Provides the presenter with an active mouse controlled pointer for the published document.
	Marker	Provides mouse annotation tool for the published document. All participants can see the resulting mark-ups.
	Full Screen	Toggles Full-Screen mode. When the presenter uses this button, the presenter's and all participants' collaboration screens switch to full screen mode. If the present toggle Full Screen Mode off, only his screen is normalized.
	Previous	Navigation to the previously displayed document page.
	Next	Navigation to the next document page.
	Content Selector	The Content Selector displays slide numbers and titles in a selectable drop down list providing the ability to quickly jump between slides.
	Poll	Launches a polling mechanism which allows the presenter to enter a question and multiple choice answers and get instant tabulated results.
	Exit	Ends the collaboration Session
	Help	Online user help.
	Lock	Locks the web portion of the collaboration session so that no new users may join. Does not impact the audio portion of the conference.

The Web Collaboration participant's window contains a toolbar with the following functionality:

	Raise Hand	Allows the participants to toggle “raising their hand.” The presenter’s roster shows a raised hand icon next to the participant’s name.
	Full Screen	Allows a participant to enter/exit the full screen collaboration mode (only for their own screen). Note: The presenter can force all participants to full screen, but then the participants may individually normalize their screens as desired.
	Exit	Removes participant from the collaboration session. The Meet Me Audio conference connection is unaffected.
	Help	Online user help.

93.4 Dependencies

93.4.1 Hardware Dependencies

IBM X335 or X336 eServers and the IBM Blade Center and Blade Center-T hardware may be used for the Web Collaboration Servers. Previous to this feature only the X335 eServer was supported.

93.4.2 Software Dependencies

93.4.2.1 Nortel Networks Software Dependencies

Not Applicable

93.4.2.2 Non-Nortel Networks Software Dependencies

Clients

Joining Conferences

The personal computers of people joining the collaboration session must meet the following minimum requirements to view published pages:

- 56kbps or higher connection speed is recommended
- Microsoft Windows 98/NT/ME/2000/XP/Server2003 with Internet

Explorer 5.5 or higher (preferred), Netscape 7.1 or higher.

- Cookies, Pop-Ups and Scripting Enabled in web browsers.

Application & Desktop Sharing

For application and desktop sharing, the sharing system must meet the following additional requirements:

- Microsoft Windows 98/NT/ME/2000/XP/Server2003 System with Internet Explorer 5.5 or higher
- Ability to run ActiveX sharing controls or pre-install sharing components
- 128kbps or higher connection speed is recommended
- The Microsoft or Sun JVM maybe used. A Java Virtual Machine 1.5 or higher is required to view or control shared screens (Windows NT systems should use Microsoft or Sun JVM 1.4.2_03). The latest service pack and patches should be applied to all Windows operating systems.

Servers

Table 2: External Software Dependencies

Component	External Dependency	Description
Media Application Server	Microsoft Windows Server 2000	Operating System
Collaboration Server	Microsoft Windows Server 2000	Operating System
Collaboration Server	Microsoft Office 2003 (All components except Access and Outlook)	Office productivity Application suite
Collaboration Server	Microsoft MSDE 2000	Database
Collaboration Server	Microsoft IIS	Web Server
Collaboration Server	Microsoft Internet Expoler 6.0	Web Browser

93.4.3 Network Component Dependencies

93.4.3.1 Nortel Networks Components

Interactions remain as described in FTR 424 Meet Me Web Collaboration.

93.4.3.2 Non-Nortel Networks Components

Not Applicable

94: Functional Description(FN): A00009655

94.1 Feature name and Feature ID

A00009655: BladeCenter-T RTP Media Portal

94.2 Background

The RTP Media Portal has been a part of the Multimedia Communications Portfolio (MCP) since its inception. The RTP Media Portal was a pooled resource that provides a variety of media-plane functions to MCP solutions including:

- Firewall and NAPT (FW/NAPT) Traversal for obscured endpoints.
- Media-Plane Firewall to protect sensitive components in the service network.
- Media Anchor/Pivot capabilities that enable media-stream manipulation without the involvement of a participating endpoint.
- Replication of media streams for CALEA.

The introductory version of the RTP Media Portal was delivered as a distributed set of subcomponents that ran on the carrier-grade Motorola CPX8216T hardware chassis. The Motorola CPX8216T chassis is a compact PCI (cPCI) architecture that provided the environmental requirements for the processing blades on which the distributed RTP Media Portal subcomponents executed. The Motorola CPX8216T chassis was partitioned into two separate PCI control domains that enabled two RTP Media Portals to reside in a single chassis. Each of these PCI control domains support the hardware components that constitute a RTP Media Portal:

- A CPV5370 Intel processor board (the Host card) with 1 GB memory, a SCSI input/output (IO) daughter board, and rear Transition Module.
- One (or more) Motorola MCPN765 Power PC processor board (the Media Blade), with 64 MB RAM and associated Rear Transition Module.
- The Hot Swap Controller and Bridge (HSC) modules.
- SCSI CD-ROM drive.
- SCSI hard drive.
- Floppy drive.

From one perspective the introductory version of the RTP Media Portal had a software architecture that closely matched the hardware architecture. However, it was also designed to be portable so that it would be platform-agnostic and poised to benefit from the advances provided by Moore’s Law.

Since its first introduction, the RTP Media Portal has fared well and proven itself to be a stable component of the MCP solution. Unfortunately, the maturation of the Voice-Over-IP (VoIP) market has begun to stress some of the first generation RTP Media Portal's limitations:

- Need for higher density (more media flows per unit of rack space).
- Need for more media bandwidth than can be provided by the dual 10/100 Mbps Ethernet links on the MCPN765 Media Blade.
- Need for improved supportability (PPC Linux).
- Need for improved reliability strategy.

The demands of the market, the benefits being reaped by other MCP components that were migrating onto the IBM BladeCenter-T platform, and the synergies that could be realized by being able to deliver all MCS components on the same platform, came together in the program to evolve the RTP Media Portal and migrate it to the IBM BladeCenter-T platform. Migration to the IBM BladeCenter-T platform provides many benefits:

- Component simplification.
- Increased capacity.
- Decreased footprint.
- Decreased cost-per-port.
- Commonality with other components (e.g. MAS, and MCS Linux Port).

94.3 Overview

The evolution to the second generation Media Portal involves the following activities:

- Migration to the IBM BladeCenter-T platform.
- Rearchitecture of the RTP Media Portal software.
- Introduction an N+1 (N-active and 1-standby) fault tolerance strategy.

94.3.1 Migration to the IBM BladeCenter-T Platform

The IBM BladeCenter-T (Type 8720 – DC Power) unit is based on proven off-the-shelf IBM Enterprise X-Architecture technologies.

The BladeCenter-T unit is a rack-mounted, high-density, high-performance blade- server system developed for NEBS telecommunications network applications and other applications requiring additional physical robustness.

The BladeCenter-T unit uses Blade Servers, switches, and other components that are common to the IBM BladeCenter product line. This common component strategy makes it ideal for applications in telecommunications

networks that need high levels of computing power and access to common off-the-shelf middleware packages that are used in IT data centers.

The BladeCenter-T unit supports up to eight Blade Servers, making it ideally suited for networking environments that require a large number of high-performance servers in a small amount of space.

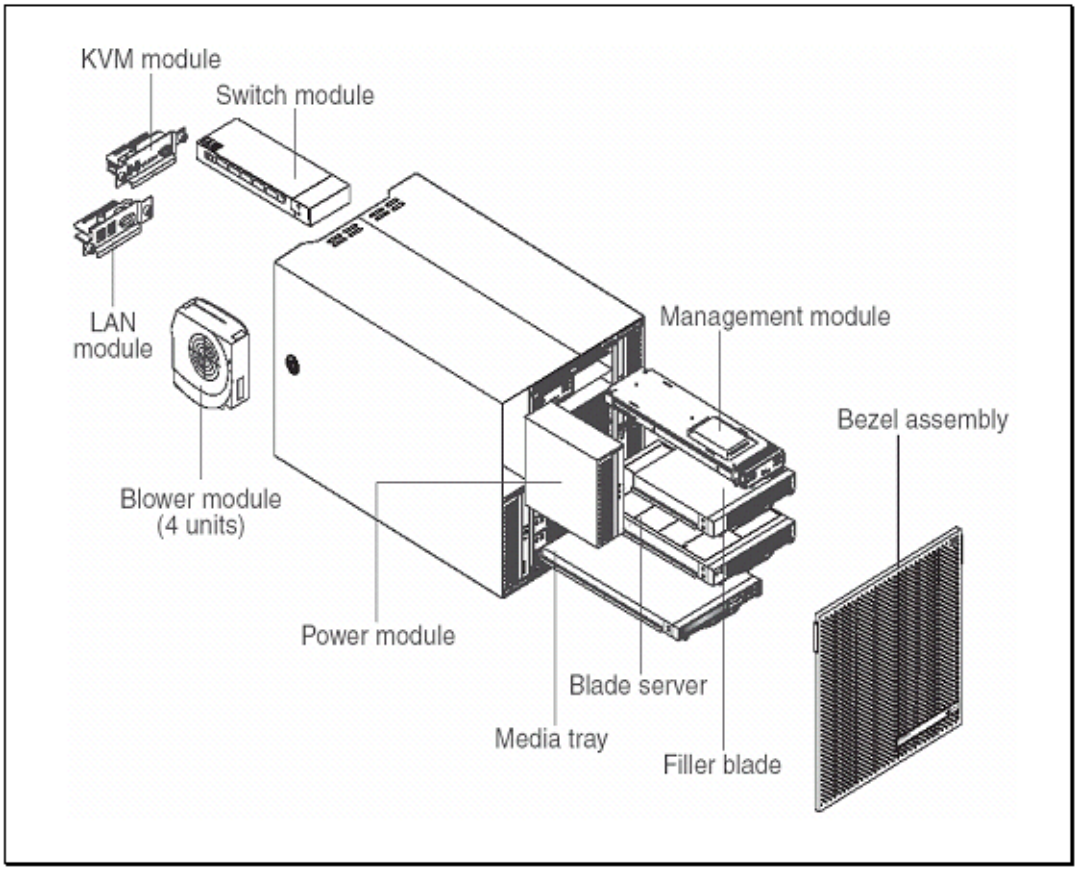
The BladeCenter-T unit provides common resources that are shared by the Blade Servers, such as power, cooling, system management, network connections, backplane, and IO (CD-ROM drive and connectors for USB, keyboard, video, mouse, and network interfaces). Refer to Figure 1 on the following page.

Performance, ease of use, reliability (NEBS/ETSI compliance), and expansion capabilities were key considerations in the design of the BladeCenter-T unit. These design features make it possible for you to customize the system hardware to meet your needs today, while providing flexible expansion capabilities for the future.

This feature activity ports the MCP RTP Media Portal component on to these Blade Servers - expanding the commonality of the IBM BladeCenter-T in MCP technology. In another move towards technology consolidation this feature also up-versions the Operating System upon which the RTP Media Portal runs to Red Hat Linux Advanced Server 3 (AS3). This is the Operating System utilized by other MCP components and its adoption by the RTP Media Portal contributes to further simplification of the overall solution.

You can obtain up-to-date information about the BladeCenter-T Type 8720 product at http://www.ibm.com/eserver/xseries/.

Figure 1: IBM BladeCenter-T Chassis (8720 – DC Version) Exploded View



94.3.2 Rearchitecture of the TRP Media Portal Software

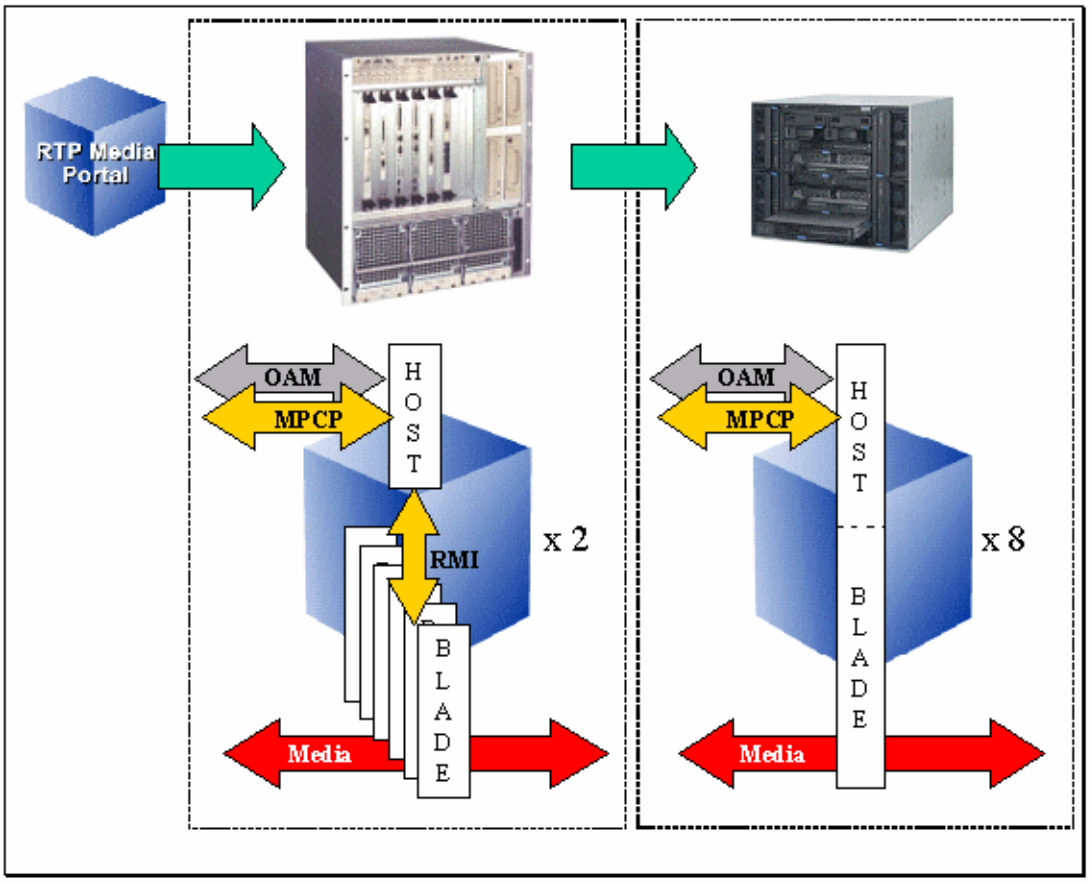
The migration from a distributed hardware architecture to a new hardware architecture that consolidates all service functionality onto a single hardware component necessitated a re-architecture of the internal software that comprises the RTP Media Portal and the services it provides.

The RTP Media Portal software was originally architected to operate in a distributed system (with a single Host communicating over the network to one or more Media Blades). This architecture has been enhanced so that the software will properly configure itself to conform with the operating environment of the target platform: it will either initialize as a distributed collection of networked sub-components (i.e. a Host communicating to one or more Media Blades), or as a consolidated amalgamation of Host and Media Blade functions into a single entity. Refer to the following figure.

The consolidation of Host and Media Blade functionality into a single entity also results in simplification through the elimination of the internal

complexities involved with coordinating service delivery amongst many distributed elements.

Figure 2: RTP Media Portal Platform Migration: Overview of Software Architectures



94.3.3 Introduction of N+1 Fault Tolerance Strategy

The original RTP Media Portal reliability strategy was to treat the RTP Media Portal as a pooled resource. Each RTP Media Portal was configured to advertise its availability to provide service to a set of Call Servers. The Call Servers would place each available RTP Media Portal into a media resource pool that would be used to serve-up available media resources during call processing.

In this manner traffic was distributed over many RTP Media Portals which lessened the impact of a failure. While lessening the impact of most failure conditions, this strategy did not preserve media sessions that existed on a piece of failed hardware. As a result, there are failure scenarios for the original RTP Media Portal that could result in loss of active calls (in the case of a Media Blade failure this could mean the loss of 400 calls, in the case of a single

chassis domain failure 2400 calls could be lost, and in the case of a full chassis failure there could be up to 4800 calls lost).

Simplification of the software architecture afforded an opportunity to take a quantum leap forward in terms of the fault tolerance attributes of the RTP Media Portal when it executes on the IBM BladeCenter-T platform. The consolidation of both Host and Media Blade functions into a single entity greatly reduced the complexity of providing the N+1 fault tolerance capabilities delivered by this feature.

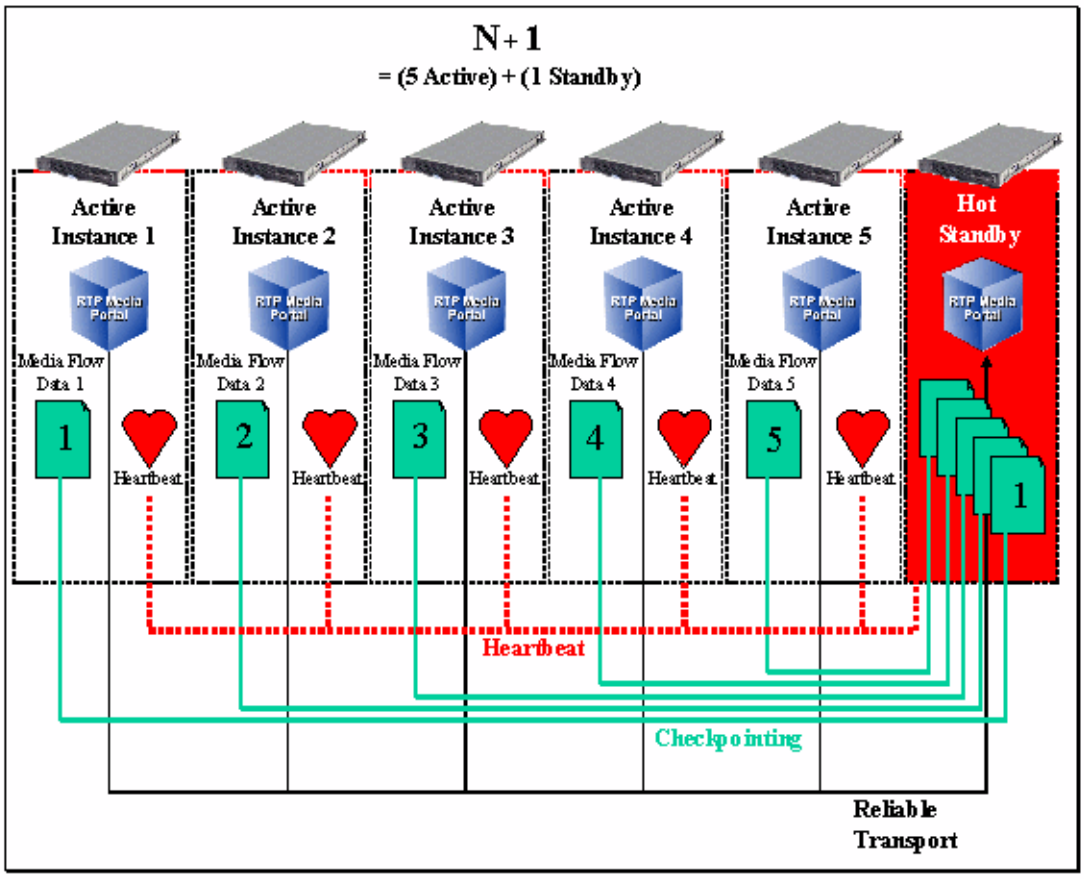
The N+1 fault tolerant RTP Media Portal is achieved through the creation of fault tolerant service clusters that define a set of RTP Media Portal instances (the “N” logical service instances) and that identifies the target servers that host the instances (“N” servers to run the active service instances and an additional server that runs a standby service instance). In this way a fault tolerant RTP Media Portal is provided that is able to have active media sessions survive the catastrophic failure of a single instance of the service by having a “standby” instance that is ready-and-able to takeover all media sessions that were hosted on the failed instance. Refer to Figure 3 on the next page.

The N+1 fault tolerant capabilities of the RTP Media Portal are built upon a reliable messaging framework that ensures connectivity between cluster members. The operating context of the cluster members is established through an election protocol that runs over the reliable messaging framework to dynamically determine which servers will be running active instances of the RTP Media Portal – and which server will be running the standby instance. This operating context is maintained through use of a heartbeat mechanism that continuously validates the state of members in the cluster. Once the cluster is formed, all state data for each active media stream (on each active instance of the RTP Media Portal in the cluster) is checkpointed to the standby RTP Media Portal instance. In this way, the standby instance remains synchronized with all active instances and is thereby ready to takeover processing of the sessions for any of those instances should a failure occur.

The N+1 takeover process is transparent to the endpoints that are originating and terminating the media streams relayed through the failed instance. This is because the standby instance begins receiving and relaying those same media streams as soon as the failure is detected and takeover is affected.

Initially, N+1 fault tolerance capabilities are restricted to the confines of a single IBM BladeCenter-T chassis. This enables configuration of fault tolerant clusters as small as 1+1 (“1-active-instance” + “1-standby-instance”) and up to as large as 7+1 (“7-active-instances” + “1-standby-instance”).

Figure 3: RTP Media Portal N+1 Fault Tolerant Service Cluster (example 5 active +1 standby configuration)

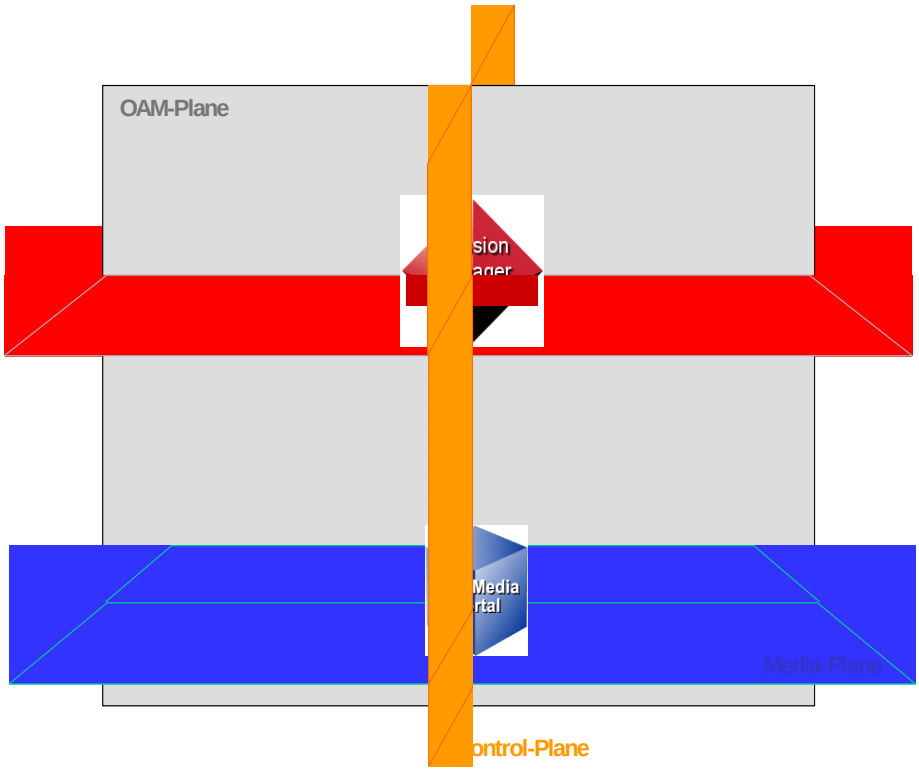


94.4 Functional Description

94.5 Overview

The RTP Media Portal has always existed in the Control-plane, the Management-plane, and the Media Plane. Refer to the following figure.

Figure 4 Legacy RTP Media Portal Presence in Service-planes

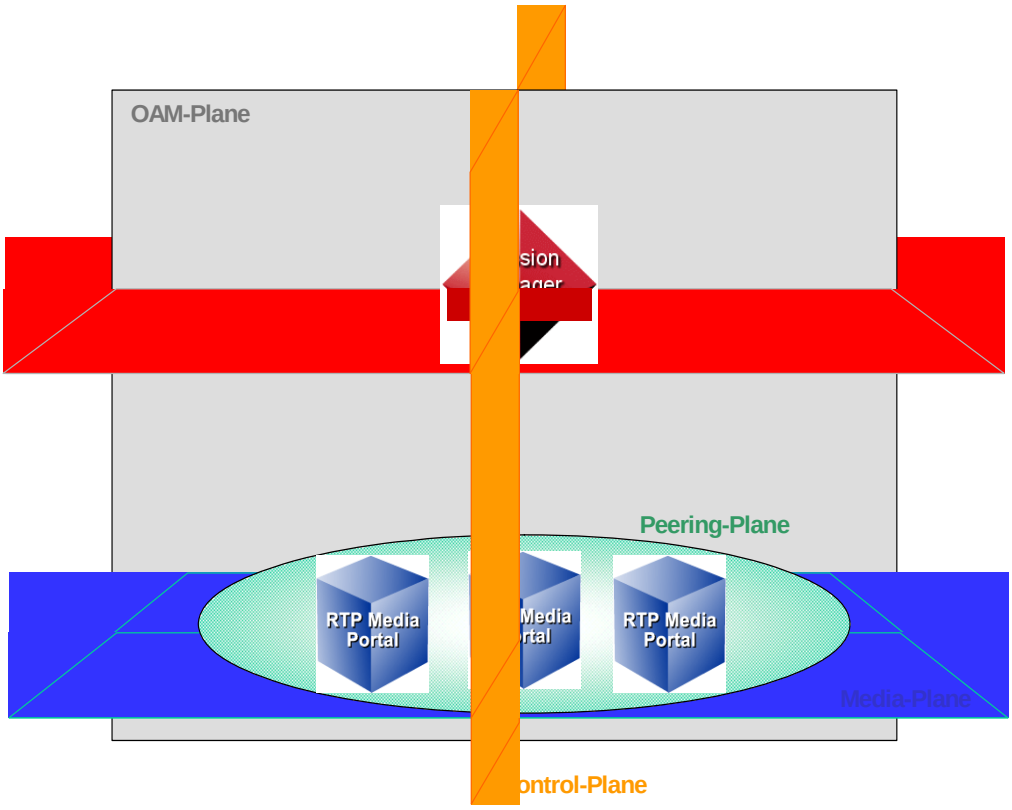


The BladeCenter-T RTP Media Portal continues to have presence in the Control, Management, and Media service-planes thus appearing (from a macro-level) to be the same as established legacy deployments to the outside world. Refer to the figure that follows. While appearing the same to the outside world, the BladeCenter-T RTP Media Portal does introduce some change as to how it is present in each of the service-planes at a sub-atomic level (not visible to the outside world):

- The BladeCenter-T RTP Media Portal has abstracted the RTP Media Portal Service from the platform. So, in fact the BladeCenter-T RTP Media Portal consists of an RTP Media Portal Service (which resides in the Control-plane and the Media-Plane), and a separate BladeCenter-T Platform (which resides in the Management-plane). This architectural change enables the BladeCenter-T RTP Media Portal to have separate and distinct points of presence in the Control-plane (the Controlipaddr), the Management-plane (the Blade Server's physical IP address), and the Media-plane (Net1MediaIP and Net2MediaIP). Previously, the RTP Media Portal was a tight coupling of hardware and software configuration that constituted a single point (the Host IP address – which was also the Server's physical IP address) through which the RTP Media Portal participated in the service-planes.

- The introduction of N+1 Fault Tolerance with the BladeCenter-T RTP Media Portal has created a new service-plane (orthogonal to all others) to support Intra-Cluster Service Communications as part of the N+1 Fault Tolerance Framework. This new service-plane is called the Peering-plane.

Figure 5 BladeCenter-T RTP Media PortalPresence in Service-planes



By retaining presence in the service-planes, and making changes that are not visible to the outside world, the BladeCenter-T RTP Media Portal maintains compatability with legacy configurations:

- The BladeCenter-T RTP Media Portal appears identical from the perspective of the MCS Management Server as viewed in the Management-plane. This is accomplished transparently as the BladeCenter-T RTP Media Portal utilizes the pre-existing RTP Portal Network Element as its point of attachment to the Management-plane:
  - the BladeCenter-T RTP Media Portal is deployed using the RTP Portal Network Element,
  - the BladeCenter-T RTP Media Portal conveys telemetry (Logs, Alarms, and Operational Measurements) through the RTP Portal Network element,

- and the BladeCenter-T RTP Media Portal is managed (Start, Stop, Kill) through the RTP Portal Network Element.

- The BladeCenter-T RTP Media Portal appears identical from the perspective of the controlling Call Server as viewed in the Control-plane because it supports the same version of the Media Portal Control Protocol (MPCP) that is supported by legacy systems.
- The BladeCenter-T RTP Media Portal also provides the same media-layer functions as provided in legacy systems and so appears identical in terms of Media-plane capabilities.

Note: There is a new RTCP CNAME screening capability introduced into the Media-plane as part of this feature activity. This new capability was implemented as part of the Media Packet Engine – and so is common to both legacy and BladeCenter-T RTP Media Portals. Thus compatability, and equivalence is maintained across platforms.

94.6 BladeCenter-T RTP Media Portal Service Instantiation

94.6.1 Overview

The following activities must be performed in order to deploy the RTP Media Portal to actively provide service in the network:

1. Installation and Commissioning of the base hardware (IBM BladeCenter-T) and software (Red Hat Advanced Server 3) platforms. This ensures proper cabling, network connectivity, and IP address assignments. Refer to “The BladeCenter-T RTP Media Portal Installation and Commissioning Guide”[1] for detailed information on the installation and commissioning procedure.
2. Configuration of the Service. (Refer to the "Configuration” section of this feature.)
3. Deploy the Service software to distribute the service logic to each of the Blade Servers participating in the Service Cluster.
4. (Finally) The Service Instance must be started (the START command must be issued from the Management Console) in order for instatiation to occur and service to be provided.

The Deploy and Start activities are described in more detail in the following sections.

Note: Deploy and Start are very similar for Stand-Alone and Service Cluster configurations, but each will be described separately for completeness.

94.6.2 Stand-Alone RTP Media Portal Instance

94.6.2.1 Stand-Alone Instantiation

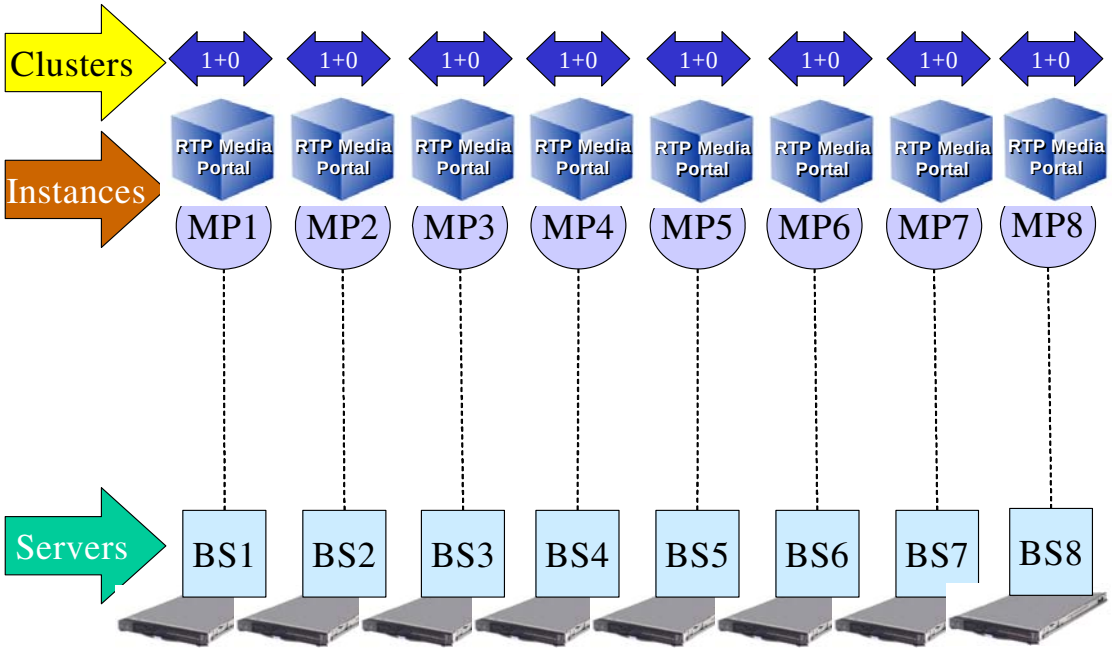
This section describes the deployment of Service software and the start-up of the RTP Media Portal service for a Stand-Alone RTP Media Portal Service Instance. The deployment phase places the Service software on the target Blade Server, and the start phase causes the instantiation of run-time structures so that the Stand-Alone RTP Media Portal Service Instance can become active and begin providing service.

The Stand-Alone RTP Media Portal Service is a single non-redundant instance of the service that runs independently of all other instances. Even though the Stand-Alone RTP Media Portal Instance is operationally different from the RTP Media Portal Service Cluster in a number of ways, it is configured as if it were a “1+0” Cluster – that is one (1) active service instance and zero (0) standby instances.

One characteristic that distinguishes a Stand-Alone RTP Media Portal Instance from an RTP Media Portal Service Cluster is that the stand-Alone Instance is only configured with one element of Service Instance Data (in Network Data => Clusters). When instantiated this effectively creates as one-to-one association of the Stand-Alone RTP Media Portal Service Instance with the target Blade Server.

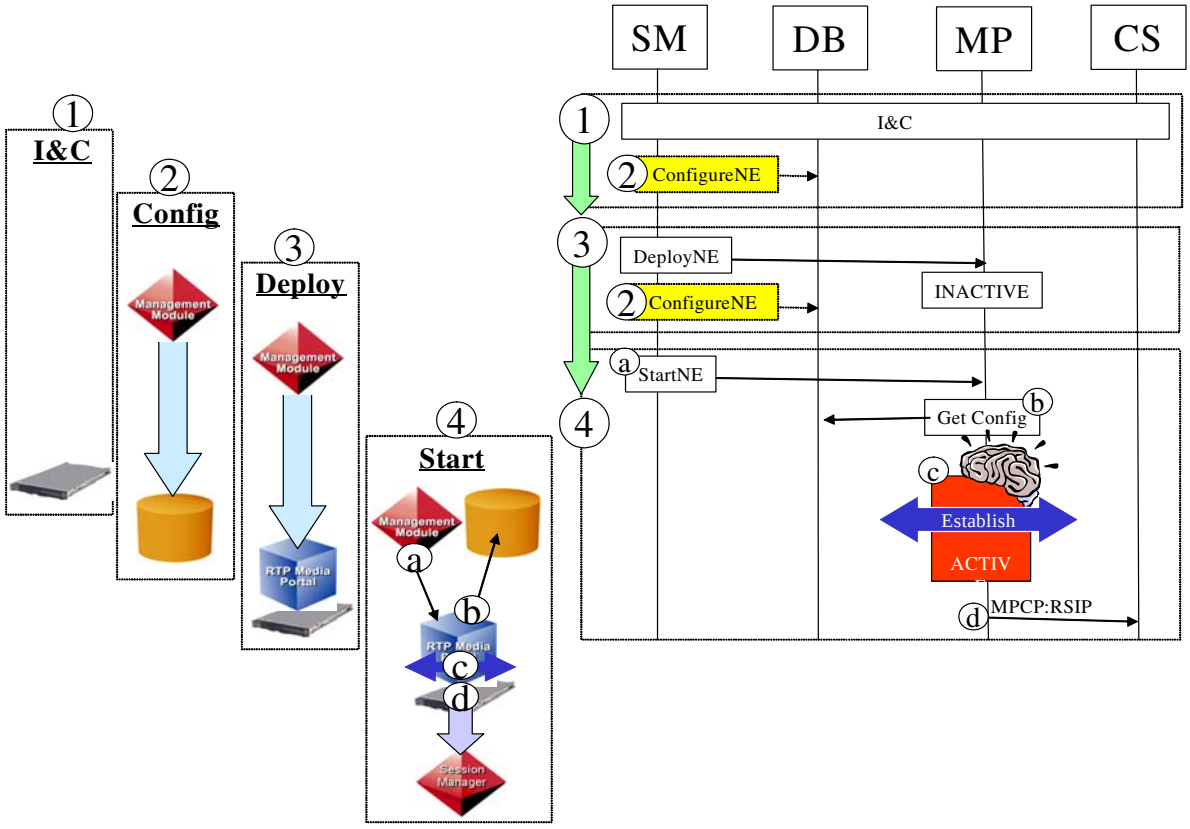
A single BladeCenter-T chassis can host up to eight (8) Stand-Alone RTP Media Portal Instances (refer to the following figure).

Figure 6 Stand-Alone RTP Media Portal Service Instances (Logical View)

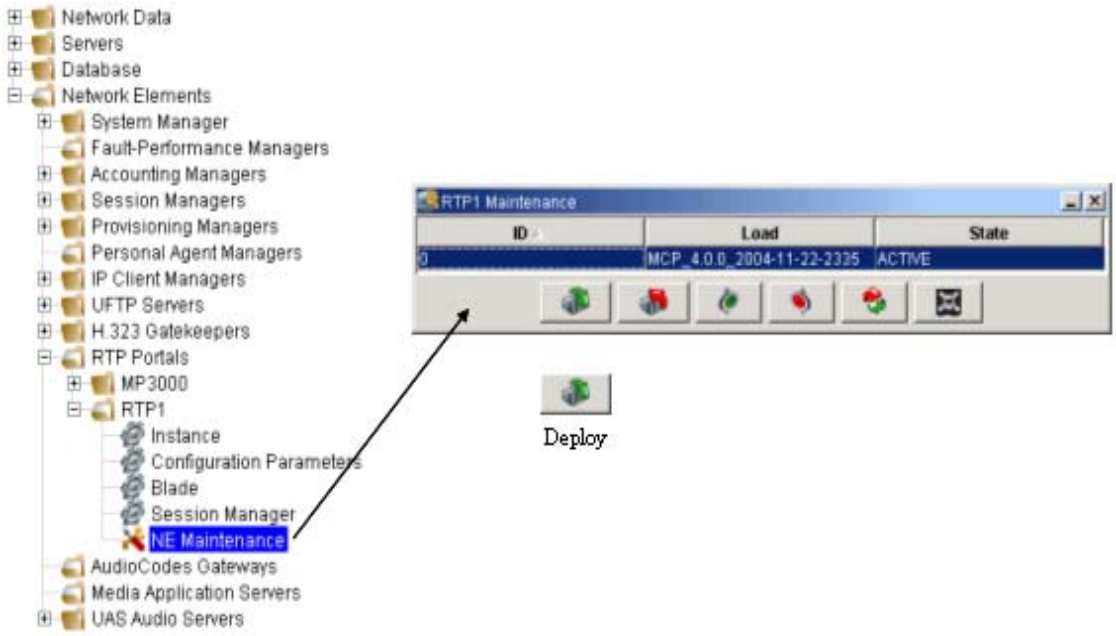


The following figure is provided as reference for the activities to be discussed that are performed in in the course of introducing a new Stand-Alone RTP Media Portal Service Instance into a site.

Figure 7 RTP Media Portal Service Deploy

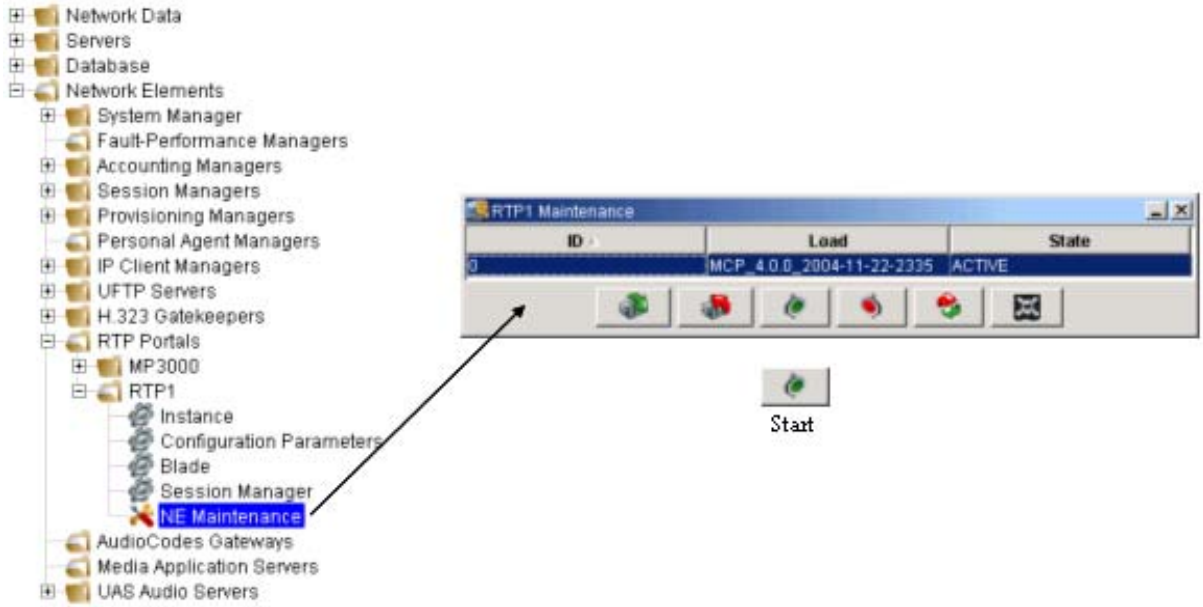


1. Installation and Commissioning of the base hardware and software platforms. Refer to “The BladeCenter-T RTP Media Portal Installation and Commissioning Guide”[1] for detailed information on the installation and commissioning procedure.
2. Configuration of the Service. The RTP Media Portal Service configuration can be changed at any time but (for the most part) is only picked up by the service on start-up. Refer to section “Service Configuration.”
3. Navigate the Management Console to the RTP Portal Network Element representing the Blade Server participating in this “1+0” Service Cluster (this will be the only RTP Portal NE that has been configured to participate in this Cluster – making it a Stand-Alone). Open the NE Maintenance window and click the Deploy button to dispatch all Service software to the Blade Server:



4. Once successfully deployed the Service Instance must be started so that instantiation of the run-time structures occurs and the service can be offered:

   a. Once again, navigate the Management Console to the RTP Portal Network Element representing the Blade Server participating in this "1+0" Service Cluster. Open the NE Maintenance window and click the Start button to start-up a RTP Media Portal Service Instance on this Blade Server:



b. As the RTP Media Portal Service Instance on the target Blade Server begins to come into service it retrieves its configuration data from the MCS Database Server. The RTP Media Portal Service Instance determines that it is configured to participate in a Cluster and then locates the specific Cluster configuration in the Network Data. Instantiation then proceeds using the Cluster Network Data to configure the service.

c. Some of the first processes started by the RTP Media Portal Service Instance are those that support the N+1 Fault Tolerant Framework (i.e. they allocate the configured multicast address and port, start the reliable messaging framework to open the intra-cluster communications channel, etc.). As the N+1 Fault Tolerant Framework Processes come up they establish the Cluster in run-time. Since this is the first RTP Media Portal Service Instance in the Cluster it is determined to be an active instance.

d. Once a RTP Media Portal Service Instance is set to active state, it issues MPCP RSIP messages to all of its configured Call Controllers (as configured in the Cluster Network Data) in order to advertise its ability to provide service. After this point the RTP Media Portal Service Instance will be called upon to service calls.

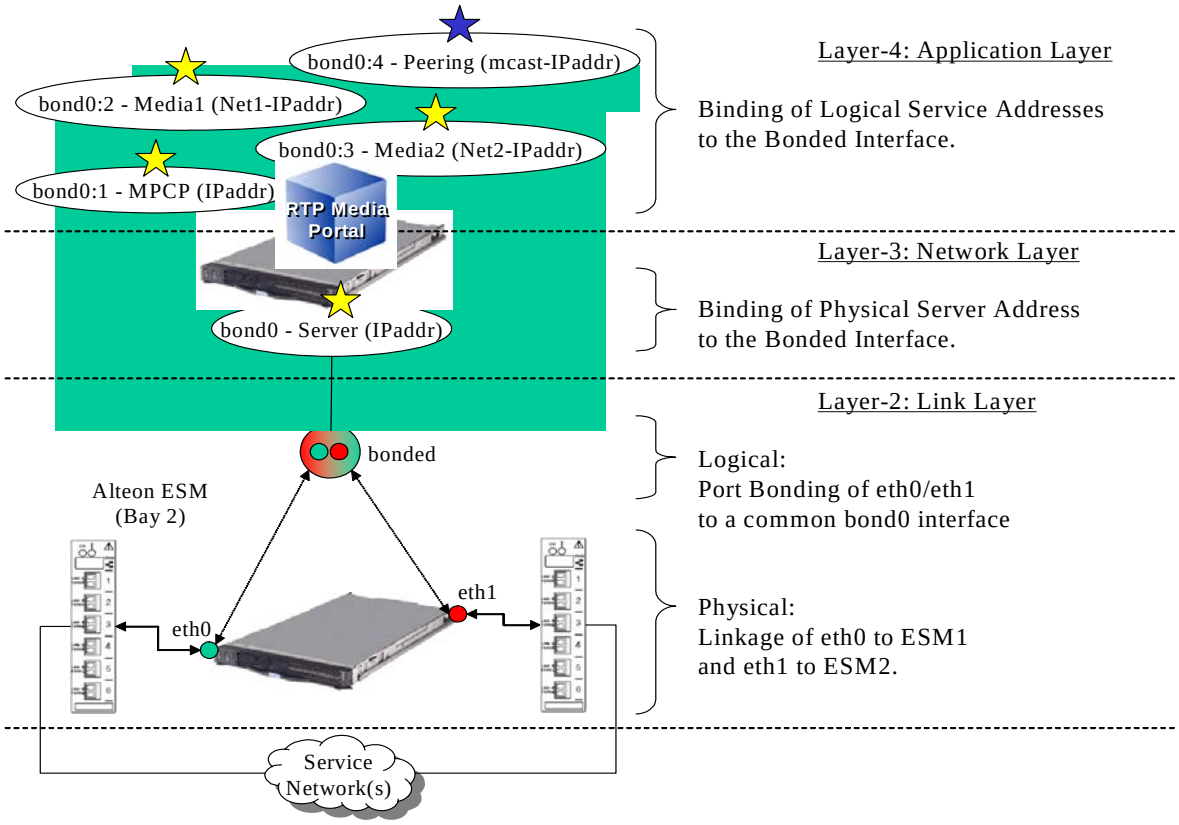
94.6.2.2 Stand-Alone Run-Time

Once instantiated the Stand-Alone RTP Media Portal Service Instance consists of the following run-time characteristics: (refer to the following figure.)

- A single physical Server IP address (bond0) that is connected to the Service Network(s) through redundant (Active/Standby Network Interface Teaming) Layer-2 connections. This physical Server IP address establishes the RTP Media Portal Service Instance's presence in the Management-plane through which the service can be managed.
- A single logical MPCP Control IP address (bond0:1) that is associated with bond0 – and so benefits from the configured Active/Standby Network Interface Teaming. This logical MPCP Control IP address represents this RTP Media Portal Service Instance in the Control-plane establishing a point from which the service can advertise its availability – and from which to process service requests.
- One, or two, logical Media IP addresses (bond0:2 and bond0:3) that are also associated with bond0 (and its redundant Layer-2 network connectivity). The Media IP addresses provide points of presence in the Media-plane to which endpoints can direct their media streams for handling by the RTP Media Portal Service Instance.
- A single logical multicast IP address (bond0:4) associated with bond0 and its inherent benefits. The multicast IP address (and port) uniquely identify a Cluster to its members. This multicast IP address represents the Cluster in the Peering-plane and is used by all Cluster members as the

communications channel through which they participate in the Cluster. In the case of a “1+0” Cluster there is only one member active on this channel and so that lone member is effectively operating in a Stand-Alone configuration.

Figure 8 RTP Media Portal Service Instance: Stand-Alone Run-Time

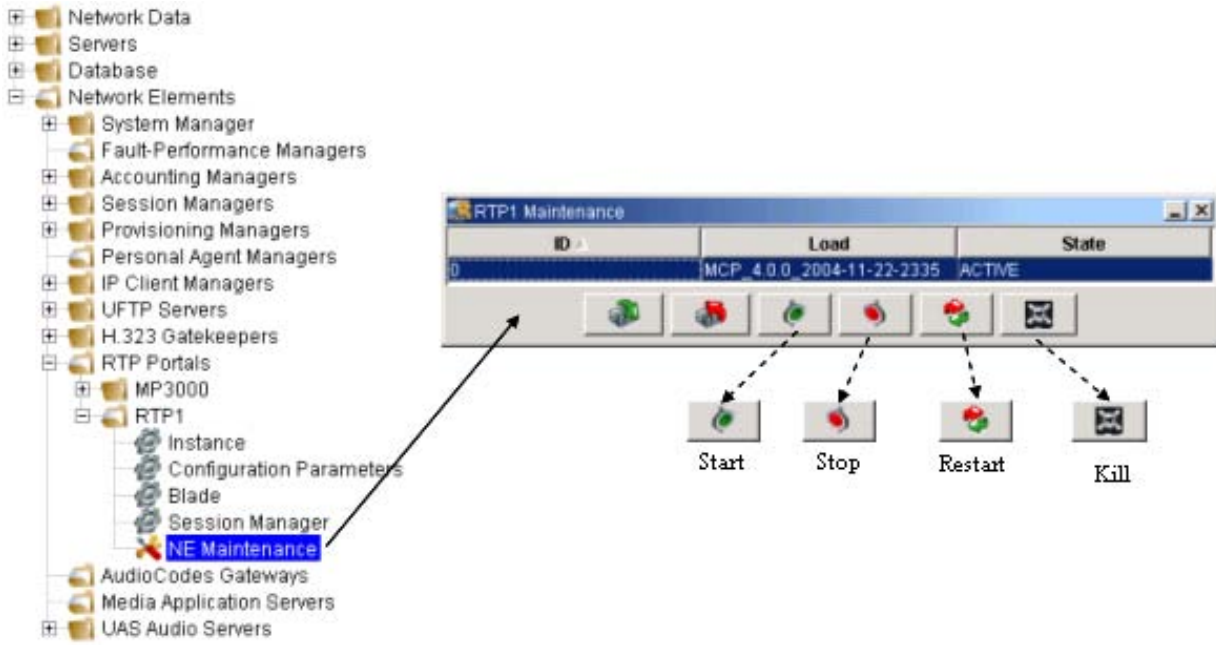


94.6.2.3 Stand-Alone RTP Media Port Management

The Stand-Alone BladeCenter-T RTP Media Portal is managed (telemetry monitoring and state changed) in exactly the same manner used to manage the stand-alone RTP Media Portal components that existed in all previous releases – that is the MCP System Management Console.

Logs, Alarms, and Operational Measurements are viewed in their respective areas of the Management Console.

Likewise, State Management (Start, Stop, Kill commands) continues to be performed through the RTP Portal NE’s Instance window:



94.6.3 RTP Media Portal Service Cluster

94.6.3.1 Service Cluster Instantiation

This section describes the deployment of Service software and the start-up of the RTP Media Portal service for an RTP Media Portal Service Cluster. The deployment phase places the Service software on the target Blade Servers, and the start phase causes the instantiation of run-time structures so that the RTP Media Portal Service Cluster forms and begins to actively provide service.

The RTP Media Portal Service Cluster is an N+1 redundant collection of RTP Media Portal Service Instances. Each instance of the RTP Media Portal Service that runs in the Cluster coordinates its activities with the other member instances. Service coordination takes place over the intra-Cluster communications channel (the Reliable Messaging Framework) that is used to form (using the Election Protocol) and maintain the Cluster (using the Checkpointing functions).

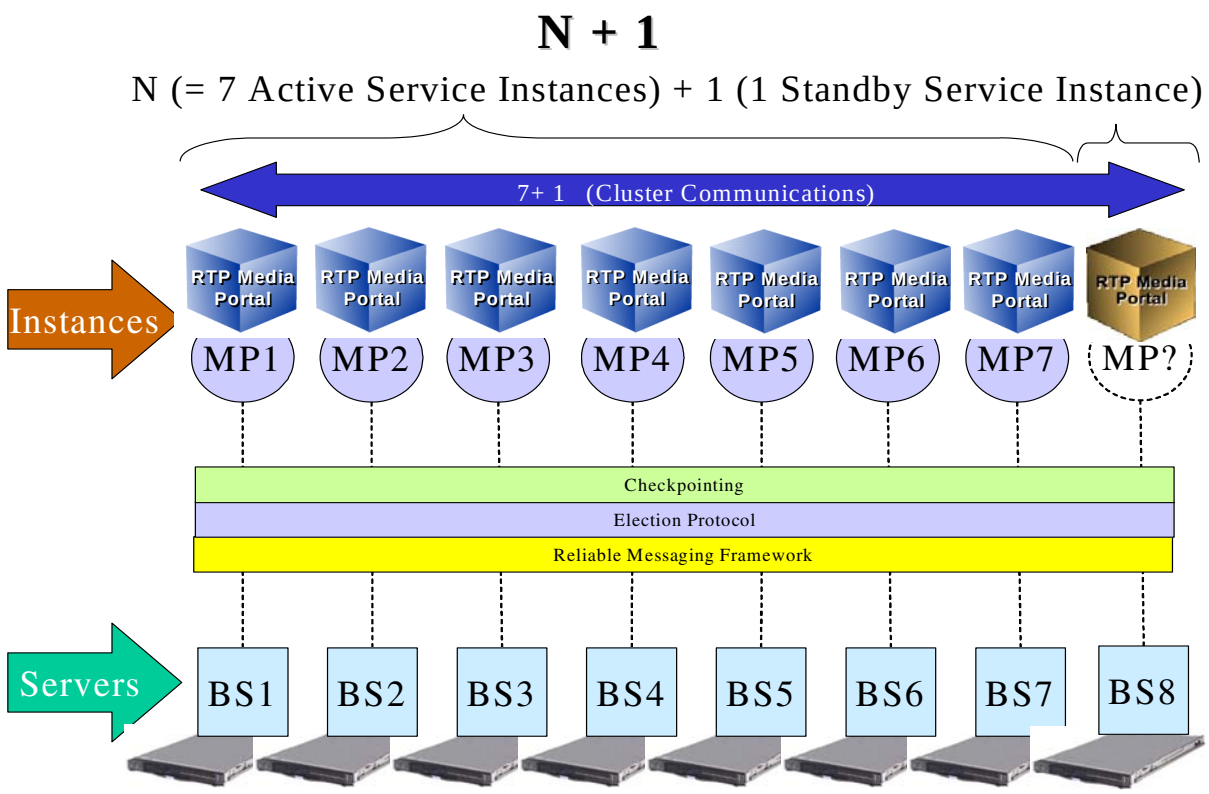
When forming an N+1 Cluster (“N” active instances and “1” standby instance), the lastinstance to join the Cluster becomes the standby instance. This ensures that that a Cluster reaches optimal operational capacity as quickly as possible before electing a standby instance.

The characteristic that distinguishes the configuration of an RTP Media Portal Service Cluster from a Stand-Alone RTP Media Portal Instance is that the Service Cluster is configured with multiple of Service Instance Data elements (in Network Data => Clusters). Once instantiated, any of the RTP Media Portal

Service Instances in the Cluster can be running on any of the Blade Servers participating in the Cluster – ther is NOT a one-to-one relationship..

A single BladeCenter-T chassis can host an RTP Media Portal Service Cluster of up to “7+1”: seven (7) active RTP Media Portal Service Instances and one (1) standby RTP Media Portal Service Instance (refer to the following figure).

Figure 9 RTP Media Portal Service Cluster (Logical View)



The following figures are provided as a reference when performing the next set of numbered steps.

Figure 10 RTP Media Portal Service Cluster Deploy (1 of 2)

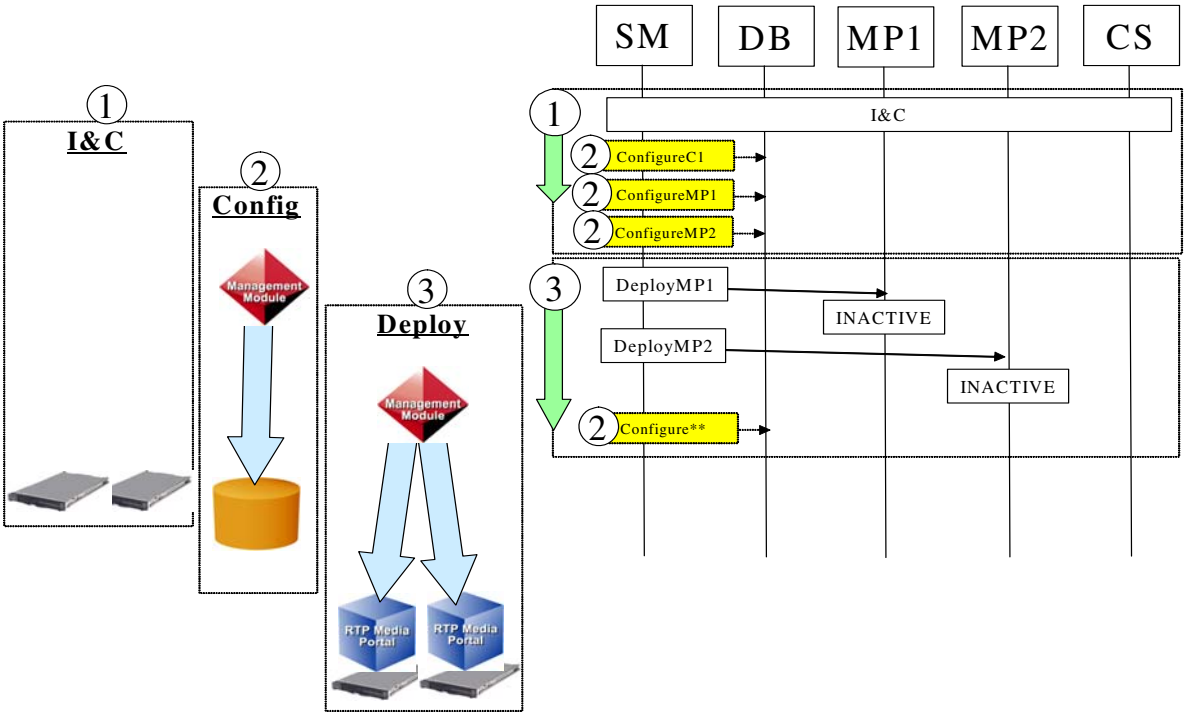
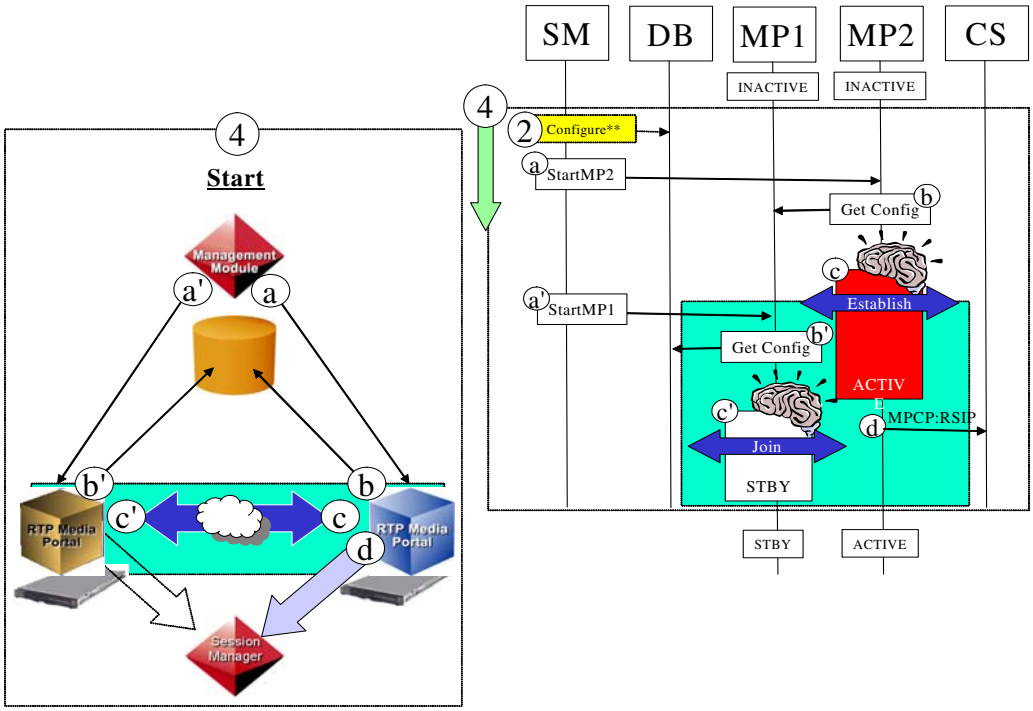
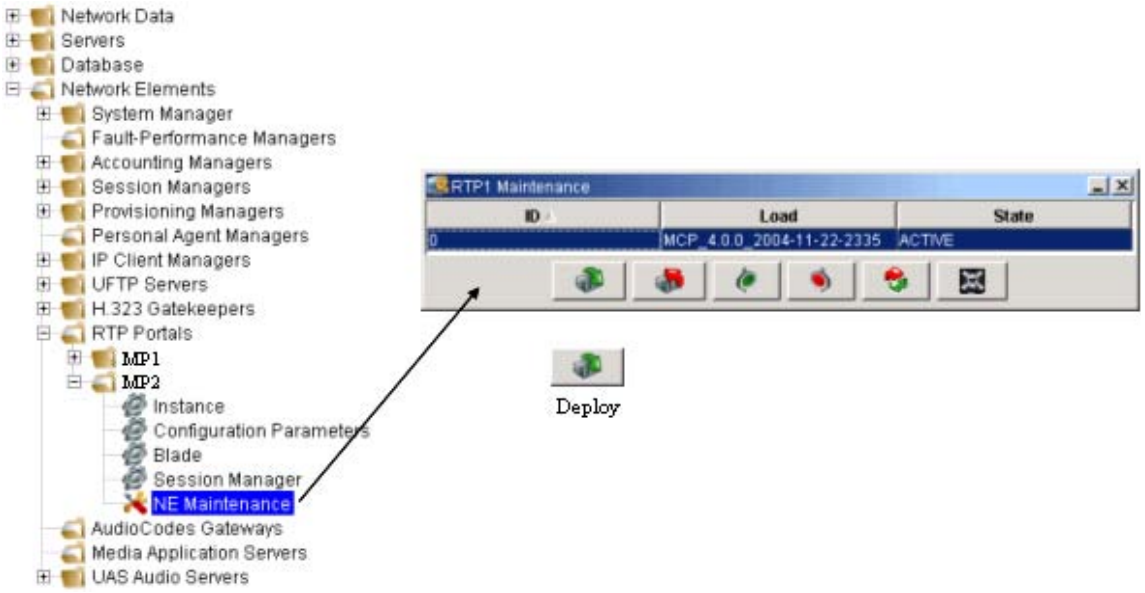


Figure 11 RTP Media Portal Service Cluster Deploy (1 of 2)

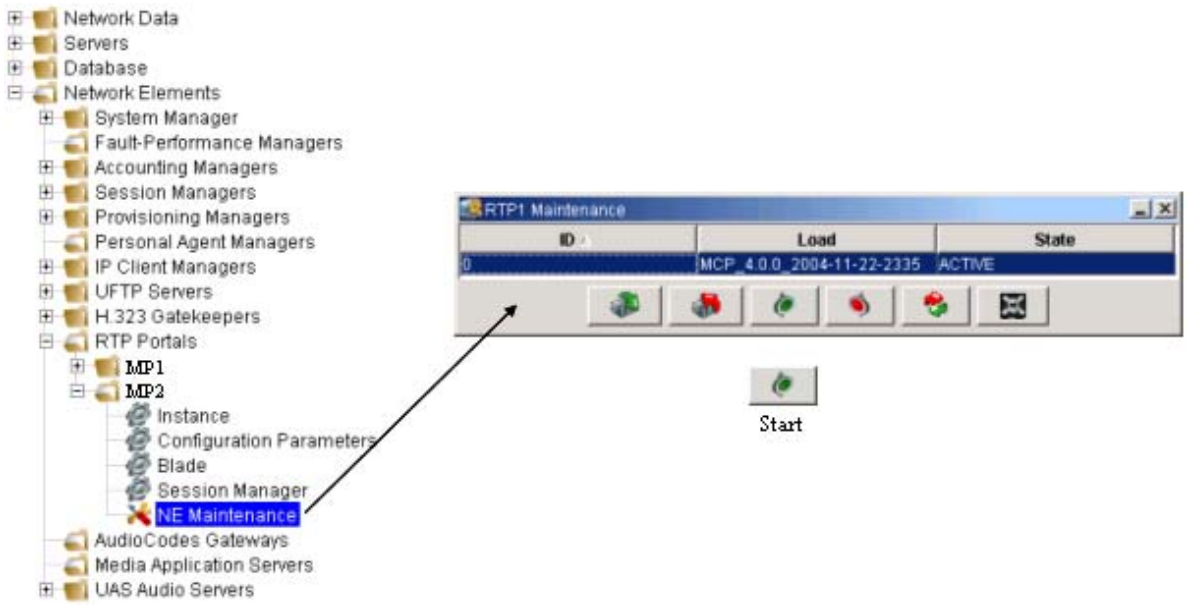


The following activities are performed in the course of introducing a new RTP Media Portal Service Cluster into a site:

1. Installation and Commissioning of the base hardware and software platforms for each of the Blade Servers intended to participate in the Cluster. Refer to “The BladeCenter-T RTP Media Portal Installation and Commissioning Guide”?[1] for detailed information on the installation and commissioning procedure.
2. Configuration of the Service. The RTP Media Portal Service configuration can be changed at any time but (for the most part) is only picked up by the service on start-up. Refer to the “Service Configuration” section of this feature.
3. Navigate the Management Console to the RTP Portal Network Elements representing each of the Blade Servers that will participate in this (“1+1”) Service Cluster. For each of these RTP Portal NEs: open the NE Maintenance window and click the Deploy button to dispatch all Service software to the associated Blade Server:



4. Once successfully deployed the member Service Instances must be started so that instantiation of the run-time structures occurs, the Cluster forms, and the service can be offered. Start-up of the individual Service Instances can occur any time after the service software is deployed to the BladeServers participating in the Cluster. This process is repeated for each of the RTP Portal NEs representing a member of the Cluster:
    a. Once again, navigate the Management Console to the RTP Portal Network Element representing a Blade Server participating in this “1+1” Service Cluster. Open the NE Maintenance window and click the Start button to start-up a RTP Media Portal Service Instance on this Blade Server:



(a' – Issuing Start command to the RTP Portal NE representing the next Cluster participant occurs in a similar fashion)

b. As the RTP Media Portal Service Instance on the target Blade Server begins to come into service it retrieves its configuration data from the MCS Database Server. The RTP Media Portal Service Instance determines that it is configured to participate in a Cluster and then locates the specific Cluster configuration in the Network Data. Instantiation then proceeds using the Cluster Network Data to configure the service.

   (b' – The next RTP Media Portal Service Instance starts-up in a similar fashion)

c. Some of the first processes started by the RTP Media Portal Service Instance are those that support the N+1 Fault Tolerant Framework (i.e. they allocate the configured multicast address and port, start the reliable messaging framework to open the intra-cluster communications channel, etc.). As the N+1 Fault Tolerant Framework Processes come up they establish the Cluster in run-time. Since this is the first RTP Media Portal Service Instance in the "1+1" Cluster it is determined by the N+1 Fault Tolerant Framework to be an active instance.

   (c' – As the second RTP Media Portal Instance starts-up and joins the Cluster, the N+1 Fault Tolerant Framework determines that, since this is configured as a "1+1" Cluster, this instance must be the Standby. The second RTP Media Portal Instance operates in Standby mode –

checkpointing all service data from the active Service Instance and monitoring its status – waiting for the opportunity to assume activity in the event that the active Service Instance encounters a fault)

d. Once a RTP Media Portal Service Instance is set to active state, it issues MPCP RSIP messages to all of its configured Call Controllers (as configured in the Cluster Network Data) in order to advertise its ability to provide service. After this point the Cluster has come into service (not yet at full capacity, but able to provide service) and this RTP Media Portal Service Instance will be called upon to service calls. In the course of processing its service requests, all active RTP Media Portal Service Instances communicate inside the Cluster to checkpoint service data and convey status so that the Cluster remains synchronized and able to survive the failure of one of its members.

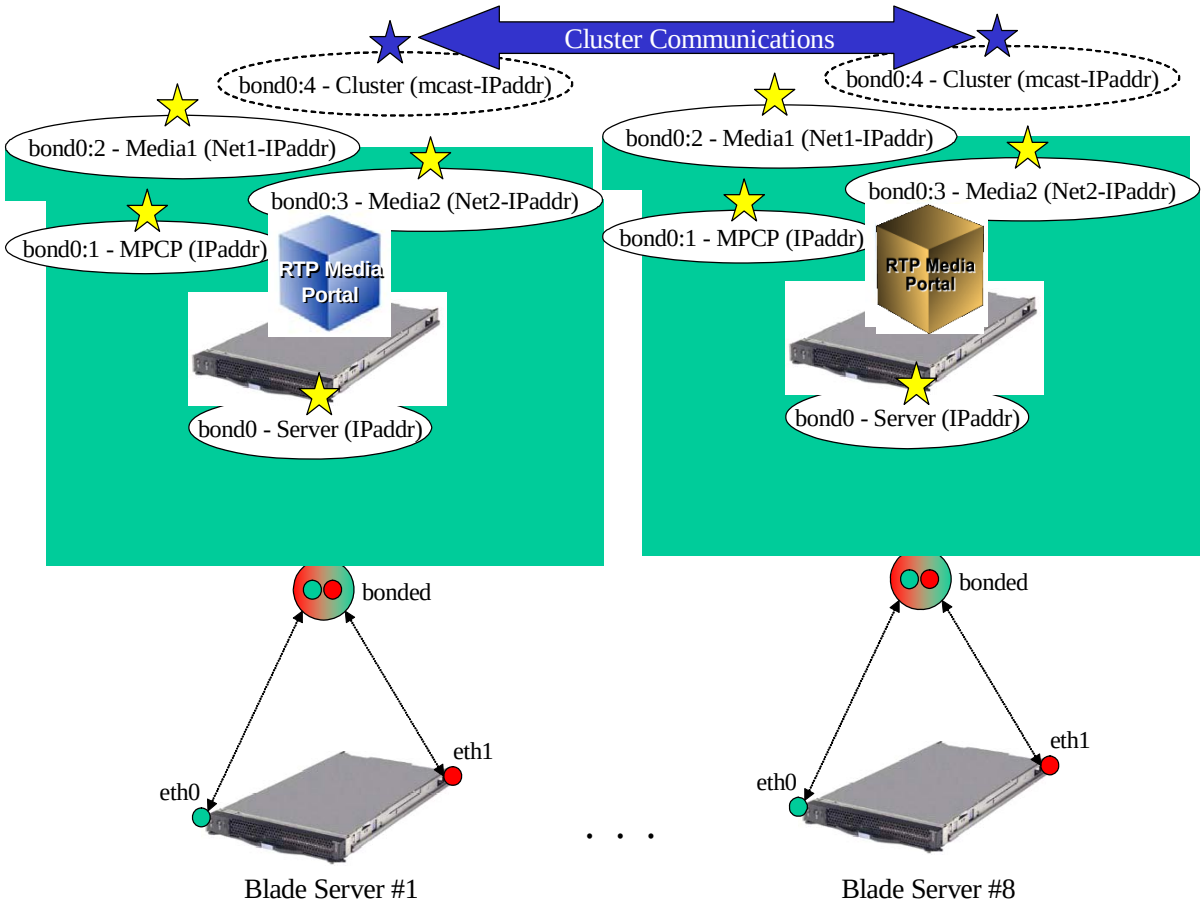
94.6.3.2 Service Cluster Run-Time

Once instantiated, an RTP Media Portal Service Cluster exists as a collection of individual RTP Media Portal Service Instances that communicate with each other (within the Cluster) to checkpoint service data and convey status information. As such the run-time characteristics of the RTP Media Portal Service Cluster is comprised of the run-time characteristics of the member Service Instances. These characteristics are very similar to the Stand-Alone RTP Media Portal Service Instance with the exception of the activity in the Peering-plane: (refer to the figure that follows).

- Each member Service Instance has a single physical Server IP address (bond0) that is connected to the Service Network(s) through redundant (Active/Standby Network Interface Teaming) Layer-2 connections. This physical Server IP address establishes this member RTP Media Portal Service Instance's presence in the Management-plane through which the service can be managed.
- Each member Service Instance has a single logical MPCP Control IP address (bond0:1) that is associated with bond0 – and so benefits from the configured Active/Standby Network Interface Teaming. This logical MPCP Control IP address represents this member RTP Media Portal Service Instance in the Control-plane establishing a point from which the service can advertise its availability – and from which to process service requests.
- Each member Service Instance has one, or two, logical Media IP addresses (bond0:2 and bond0:3) that are also associated with bond0 (and its redundant Layer-2 network connectivity). The Media IP addresses provide points of presence in the Media-plane to which endpoints can direct their media streams for handling by this member RTP Media Portal Service Instance.
- Each member Service Instance in a Service Cluster shares a logical multicast IP address (bond0:4) associated with bond0 and its inherent

benefits. The multicast IP address (and port) uniquely identifies a Cluster to its members. This multicast IP address represents the Cluster in the Peering-plane and is used by all Cluster members as the communications channel through which they participate in the Cluster. In the case of a “1+1” Cluster there is one active RTP Media Portal Service Instance on this channel and and one standby RTP Media Portal Service Instance on this channel. Generally, active Service Instances provide service and convey their service data over the Cluster communications channel to the standby Instance. The standby RTP Media Portal Service Instance checkpoints the service data received from all active Service Instances so that it can effect a transparent take-over of activity for any of the active Service Instances (should the need arise). The standby RTP Media Portal Service Instance also monitors the health of the active Service Instances so that it can take-over activity if a fault is detected on any one of the active Service Instances.

Figure 12 RTP Media Portal Service Cluster Run-Time



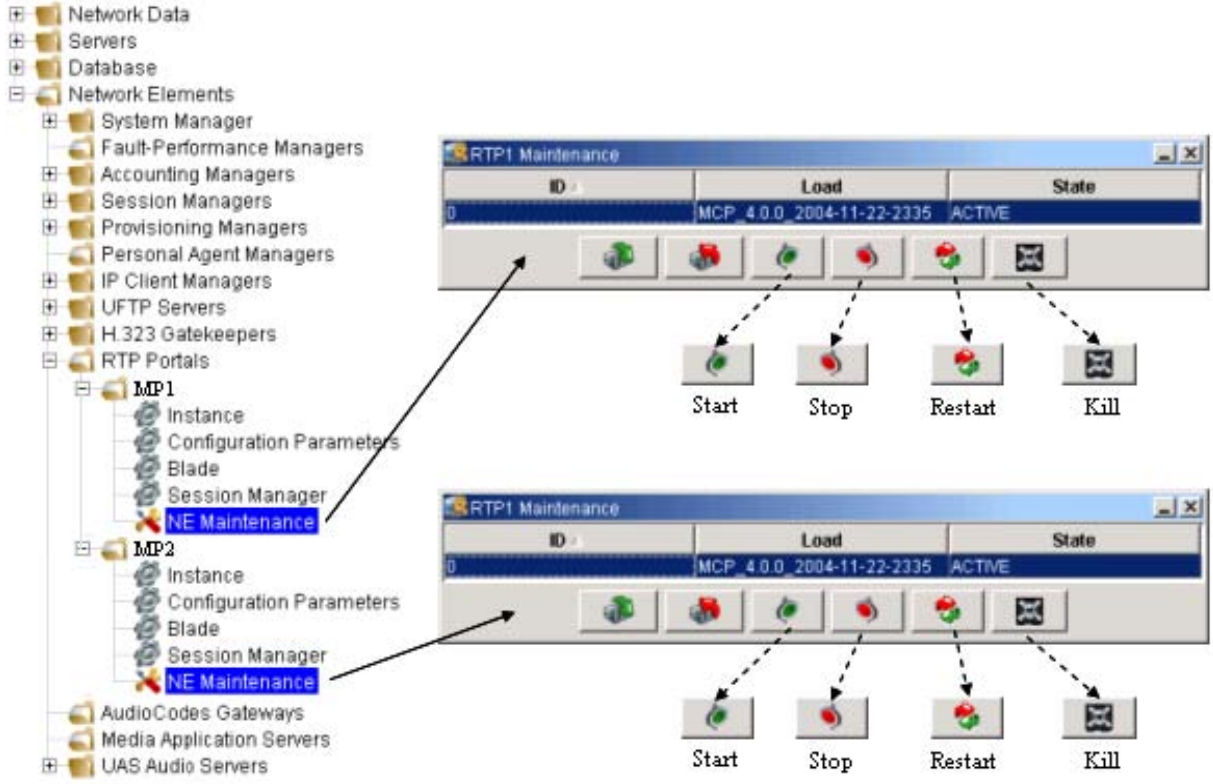
94.6.3.3 RTP Media Portal Service Cluster Management

Unfortunately, there is no capability provided to manage at the Cluster-level. As a result the BladeCenter-T RTP Media Portal Service Cluster is managed (telemetry monitoring and state changed) through administrative coordination of the management of each individual RTP portal NE.

This effectively reduces the management of the RTP Media Portal Service Cluster to the coordinated management of the collection of member RTP Portal NEs through the MCP System Management Console.

Logs, Alarms, and Operational Measurements are available for each member RTP Portal NE and are viewable in their respective areas of the Management Console.

Likewise, State Management (Start, Stop, Kill commands) must be performed in a coordinated fashion on the member RTP Portal NEs in order to achieve the desired operational result. Each member RTP Portal NE is managed using the RTP Portal NE's Instance window:



94.7 Hardware Dependencies

This feature requires IBM BladeCenter-T hardware:

- Chassis.
- DC Power Modules.
- Media Tray.
- Management Modules.
- Blower Modules.
- KVM Module.
- LAN Module.
- IO Modules.
- Blade Servers.

94.8 Software Dependencies

This feature requires Red Hat Linux Advanced Server 3 Linux Operating System.

94.8.1 Network Component Dependencies

This feature requires the collaboration of the following components:

- Management Server (and Management Console): to enable configuration and management through the MCP OAM Framework.
- Database Server: to enable persistence of configuration data and to integrate into the MCP OAM Framework.

94.8.1.1 Nortel Networks Components

Management Server (and Management Console)

The Management Server and the Management Console provide a graphical interface from which to configure and manage the BladeCenter-T RTP Media Portal. In addition to pre-existing functions, the Management Console provides access to the following new structures:

- The new Clusters are created in the Network Data.
- The new Cluster field introduced into the RTP Portal NE Instance Data.

Database Server

The Database Server provides persistent storage and centralized distribution for the newly introduced configuration information related to the BladeCenter-T RTP media Portal:

- Clusters Table (new table)
- RTP Portal Network Entity Table (new Cluster field)

94.8.1.2 Non Nortel Networks Components

Not Applicable.

94.9 Accounting

Pre-existing MCS functionality captured the following information in the accounting stream to identify which RTP Media Portal resources were selected to facilitate a call:

- mediaPortalHost: the RTP Media Portal Host IP address used to facilitate the media path of the call
- origMPConnAddr: The RTP Media Portal Media Blade IP address that replaced the Originator's media connection IP address in the SDP.
- origMPPort: RTP Media Portal Media Blade Port that replaces the Originator's media connection Port in the SDP.
- termMPConnAddr: RTP Media Portal Media Blade connection IP address that replaces the Terminator's media connection IP address in the SDP.
- termMPPort: RTP Media Portal Media Blade Port that replaces the Terminator's media connection Port in the SDP.

This information is still conveyed in the accounting stream but, as a result of this feature, some of the relationships previously implied by this information may no longer exist. Specifically, in previous releases this data not only identified service information – it also uniquely identified a piece of hardware. With the introduction of the RTP Media Portal Service Cluster the service information has been abstracted from the hardware information (a set of Service Instances can be executing on any of the hardware platforms participating in the Cluster at any given point in time) and so there is no longer a precise correlation between service information and hardware information.

94.10 Glossary

Term	Definition
APD	Address and Port Discovery
BPT	Bulk Provisioning Tool
CPU	Central Processing Unit
ERL	Emergency Response Location
FD	Functional Description
FSD	Functional Specification Document
FW	Firewall
IP	Internet Protocol

Term	Definition
MCP	Multimedia Communications Platform
MGCP	Media Gateway Control Protocol
MP	Media Portal
MPCP	Media Proxy Control Protocol (for control of RTP Media Portal)
MPG	Media Portal Group
NAT	Network Address Translation
NAPT	Network Address and/or Port Translation
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network (the legacy circuit-switched telephone network)
RSIP	Restart In Progress (an MPCP message)
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
UDP	User Datagram Protocol

95: Functional Description(FN): A00009711

95.1 Feature name and Feature ID

A00009711 Multimedia Communication Server E911 Caller Hold

95.2 Description

The MCS 3.0 Enhanced 911 feature provided the ability for an MCS originated emergency call to be routed to a local PSAP based on the location of the client device as chosen by the user. It also provided an ANI to the PSAP which could be used to query an ALI database to determine the physical location of the caller. The ANI also provided a callback number to the PSAP in order to allow the PSAP operator to call back the originator of an E911 call.

This feature provides the following enhancements to the MCS E911 service:

1. Denial of originator initiated mid-call features on an E911 call.

2. Terminator call control on an E911 call.

The first enhancement provides the capability to deny the originator of a 911 call the ability to invoke a feature that essentially puts the call on hold. This includes the following features:

- Hold
- Transfer
- Call Park
- Conferencing
- Making a 2nd call from the device (where applicable)
- Receiving incoming requests outside the emergency session

The second enhancement disallows an MCS originator of an E911 call from disconnecting the call. The only party that can disconnect the E911 call is the PSAP.

95.3 Session Manager Behavior

To offer terminator call control and mid-call request denial during an emergency call, the behavior of the Session Manager Emergency service has been modified to perform the actions described in the following sections.

95.3.1 Addition of Resource-Priority Header

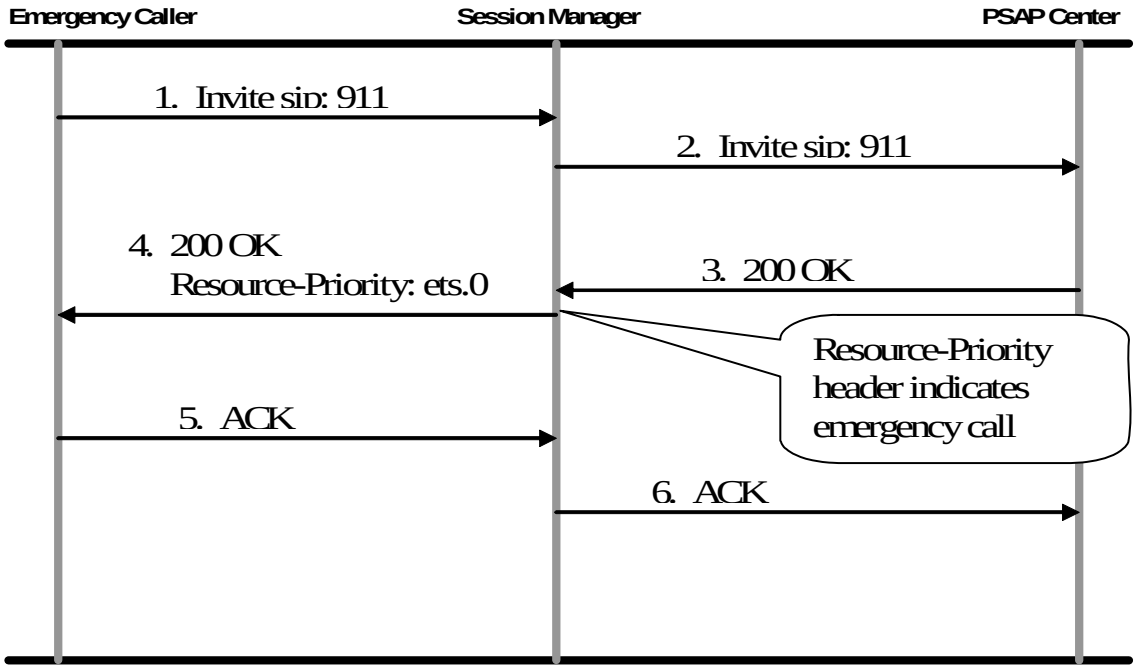
As described in Internet-draft [1], the Resource-priority header may be used to interrupt lower-priority requests at a user terminal, such as an IP phone. Thus, upon discovering that the caller is making an emergency call, the session manager may add a Resource-Priority header to the answer signal (200 OK) during initial call setup signaling. The purpose of the Resource-Priority header in the answer signal is to instruct the caller's device that the call is an emergency call and to set itself in emergency mode. By emergency mode we expect the device to reject any action taken by the user that would interfere with the voice path between the caller and the PSAP operator.

The MCS Session Manager will send a Resource-Priority header in the following format.

```
Resource-Priority: ets.0
```

The namespace ets and priority 0 is used to indicate the call is an emergency call with highest priority, thus instructing the device to handle the current session in emergency mode and to grant high priority to voice services.

Figure 1 Emergency Call Setup



Actions that are expected to be blocked by the emergency caller's device are:

- Terminating the call
- Logging out, Exiting
- Putting the call on hold
- Transfer
- Conferencing
- Receiving/Initiating new calls
- Receiving/Initiating instant messages
- Receiving/Initiating Collaboration
- Codec changes
- Muting the phone

The criteria used by the Session Manager to determine whether a Resource-Priority header is added during the answer setup message is based on a property provisioned at the domain or sub-domain: E-911 Originator Hold.

The Resource-Priority SIP header applies to IADs, gateways, CS2K, and softclients.

95.3.2 Configurable ANI Registration Time

The emergency application on the session manager will be modified to allow a configurable ANI registration time for enterprise Emergency Response Location (ERL). The value is assigned on the provisioning client (refer to Section 95.6.2.1).

95.3.3 Profile Override

The emergency application on the session manager will be modified to allow a direct association between an ERL and a CS2K profile, thereby overriding the profile of the originating subscriber. The profile override is assigned on the provisioning client (refer to Section 95.6.2.2).

95.3.4 Checkpoint Impact

The session manager implements a checkpoint mechanism to achieve fault tolerance[1]. During an enterprise emergency call an ANI is selected from a pool and temporarily associated with the originator. This temporary association is accomplished using the SIP REGISTER method where the expires time is the ANI registration time. Therefore, for enterprise PSAP callbacks to work after failover, the ANI registration times are checkpointed.

Provisioned data, such as the Emergency Response Locations, are synchronized across all session managers using an alternate data-sync (NOTIFY) mechanism.

[1]A00009045 - Call Processing Checkpointing

95.3.5 Mid-Call request denial

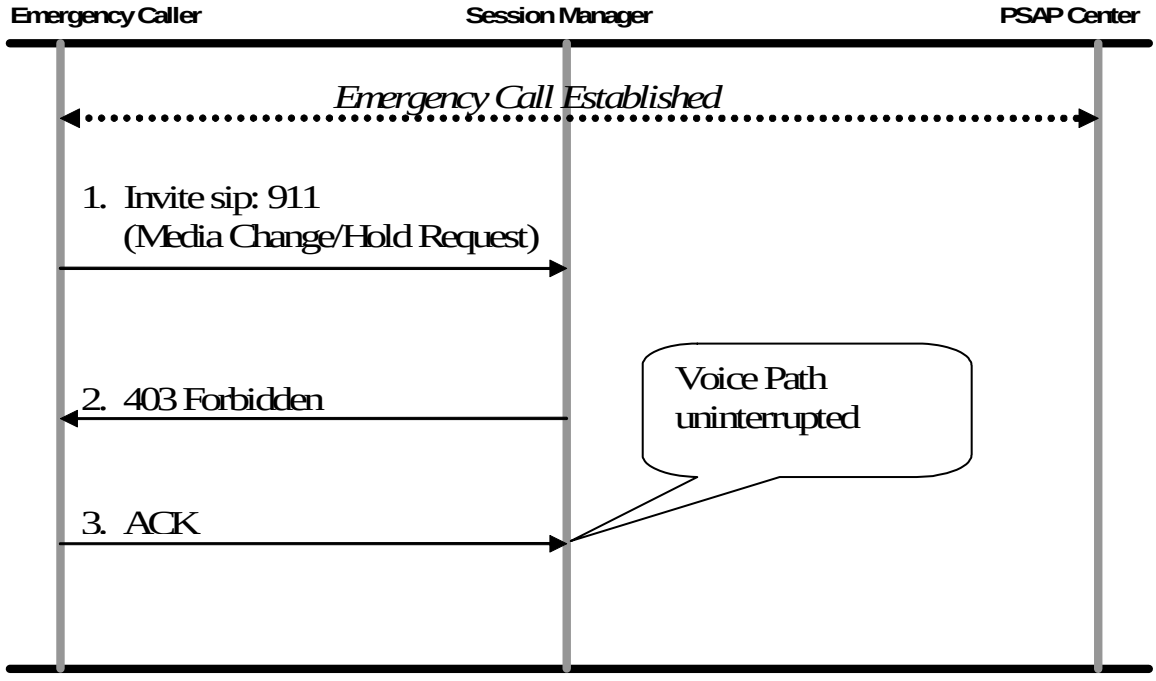
Once an emergency call is established, the session manager will reject all incoming mid-call requests that may affect voice path between the emergency caller and the PSAP operator. Mid-call requests denial applies to all emergency calls independent of the value of the 'Emergency Caller Hold' property. Specific Mid-Call request denial actions taken by the Session Manager are described below.

95.3.5.1 Media changes including Hold requests

Any type of media changes such as putting the call on hold, changing audio settings and adding video will be rejected during an emergency call by the session manager. Media changes initiated with a Re-Invite message will be rejected by the Session manager with a 403 Forbidden error response. The error response is expected to be interpreted as a denial for media change and not as a termination of the media path. While the request for media change and denial is processed, the media path established during call setup must not be interrupted by the caller's device. It is expected that third party devices initiating a mid-call request, do not interrupt media until successful response (200 OK) for media change is received from the Session Manager.

Since most mid-call services (Transfer, Conference, Call Park) start out with a successful hold request, blocking the hold at the session manager will indirectly prevent these mid-call services from being requested.

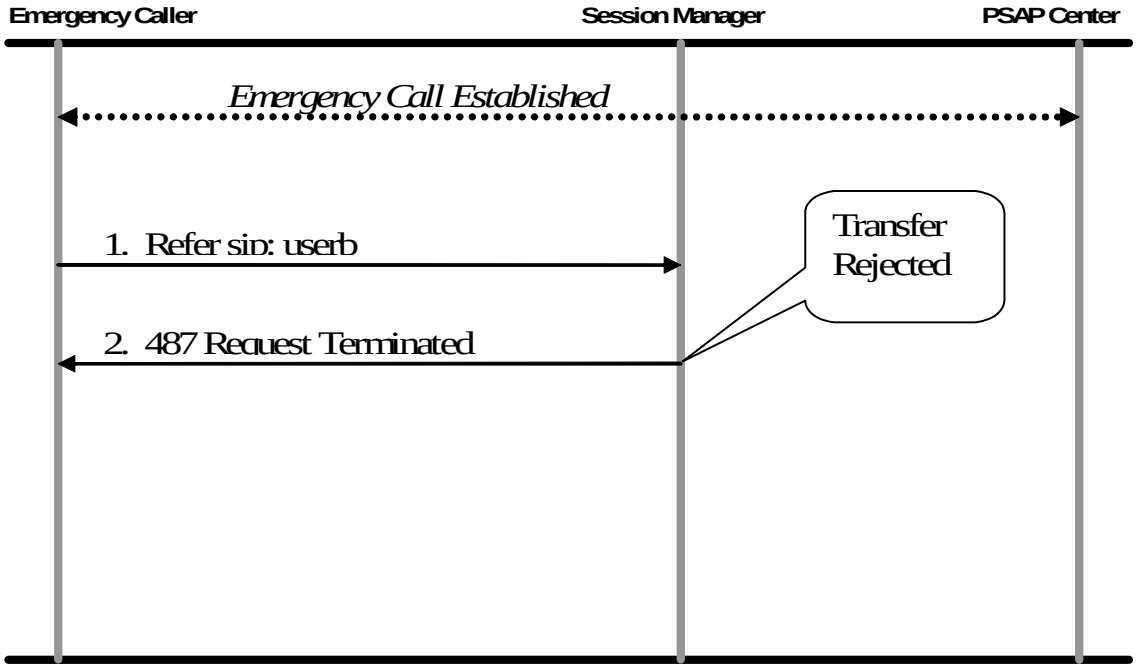
Figure 2 Mid-Call - Media Change Request Denial



95.3.5.2 Transfer

Transferring a call is typically initiated by putting the existing call on hold followed by a REFER message. The session manager will send a 403 in response to the hold request and expect the emergency caller's device to give up on the transfer. However in the event that the device of the emergency caller sends a REFER, the session manager will deny the transfer by failing the transfer request. This is done by sending a “487 Request Terminated” in response to the REFER. The expected client behavior in receiving the 487 would be to revert back to the previous audio stream.

Figure 3 Mid-Call Transfer Request Denial



95.3.5.3 Consultative Transfer and Ad Hoc Conference

Consultative transfers are basically calls where the originator establishes a three-way call by transferring the terminator to a conference server. Typically the caller puts the existing call on hold, then initiates a new call to the conference server and then transfers the existing call on hold to the conference server.

In this scenario, the session manager will block the call hold by sending a 403 response when the emergency caller attempts to put the PSAP operator on hold (similar to Figure 2). It is expected that the emergency caller's device will quit the consultative transfer after receiving the 403 and do not attempt to establish a new call with the conference server.

In the event that the emergency caller's device is non-compliant to the 403 response to the hold and establishes a new call with the conference server, the voice path between the original emergency parties will be broken.

95.3.5.4 New Call

Typically when making a new call while on an active call, the active call is first put on hold and the new call is established. While an emergency call is active the ability to place a new call must be blocked by the emergency caller's device by disabling any New Call controls. However, devices that allow the media hold request signal to be sent to the Session Manager will receive a 403 response (similar to Figure 2). It is expected that the emergency caller's device will quit the consultative transfer after receiving the 403 and do not attempt to establish a new call with the new destination.

In the event that the emergency caller's device is non-compliant to the 403 response to the hold and establishes a new call with the new destination, the voice path between the original emergency parties will be broken.

95.3.6 Emergency Caller Termination

Since RFC 3261 states that clients should stop sending and receiving media just after constructing the BYE (RFC3261-Sec. 15.1.1), the media path between the emergency caller and the PSAP center would be lost if the caller's device allows the user to end the call. Thus enforcing caller hold for emergency call is a feature that must be enforced by third-party clients.

Devices that receive a Resource-Priority header are expected to prevent the user from disconnecting the call by any means. A call may be terminated by putting the handset on-hook, pressing a Hang Up/Release button or closing an Active Call Dialog window of a soft-phone.

However, in the case where the device allows the user to disconnect despite the presence of the Resource-Priority header the session manager will allow the call to disconnect by forwarding the disconnect signaling to PSAP terminator gateway. It is strongly advised that third party devices interacting with MCS are compliant with the Resource-Priority header to avoid undesired emergency call interruptions.

95.3.7 Abnormal Disconnect

Emergency calls that abnormally disconnect should be detected and handled so that emergency resources can deallocate promptly. This feature will introduce a mechanism to detect abnormal disconnects at the session manager for emergency calls.

During an emergency call, an audit (polling) mechanism will transmit a SIP INFO message to the originator at a periodic fixed interval of thirty seconds. In the event that the client does not respond to the INFO request or responds

with an unacceptable response, the audit will fail indicating an abnormal disconnect.

The following INFO responses (from client) are considered unacceptable and will cause an audit failure:

- 404 Not Found
- 408 Request Timeout
- 410 Gone
- 480 Temporarily Unavailable
- 481 Call Leg Transaction Does Not Exist[1]
- 604 Does Not Exist Anywhere

Upon audit failure, the session manager will procede to tear down the call. Accounting records are created each time the audit runs indicating the outcome of the audit.

95.4 SMC Call Control Behavior

When the PC Client is used to originate an E911 call the behavior of the client will change during that call to prevent the originator from disconnecting or initiating new mid-call features. Since the client does not have knowledge of the emergency dial plans, the client will be modified to trigger this feature when the SIP Resource-Priority header is present in the 200 OK.

95.4.1 Call Setup

When a subscriber makes an emergency call, the clients existing behavior is unchanged. That is, the originator may abandon the call while ringing (during call setup), provided the operator has not answered (Figure 4). As part of call setup, the session-manager can signal the client to enable this ‘originator hold’ feature via the Resource-Priority SIP header (Section 95.3.1).

[1]Except when sent from an MCS Session Manager

Figure 4 E911 call window during call setup

95.4.2 Call Established

By default, this feature is disabled in provisioning. In this trivial case, this feature is not activated and the call windows existing behavior applies. The following figure illustrates the non-modal active call window which is common for all calls established on the client.

Figure 5 E911 call window without Originator Hold

95.4.2.1 Originator Hold

When this feature is enabled (provisioned on the originators domain), all buttons on the pop-up window for the emergency call will be disabled and the window cannot be terminated by pressing the “Close” button in the top right corner (Figure 6). The following PCC buttons will be disabled and illustrate a greyscale icon:

- Stop
- Instant Message
- Share
- Hold
- Start Camera
- New Call
- Transfer
- Call
- Send File
- Hang Up
- Mute
- Audio Quality
- Conference

Figure 6 E911 call window with Originator Hold enabled

While the client is in an emergency session, the active call window will become modal (blocking frame with active focus over all other PCC windows). The clients main window (or any other) cannot be accessed until the active call dialog is released. This prevents the originator to shut down by “Login -> Exit” menu.

The emergency call can be disconnected if the process crashes or is killed from the task manager. Within thirty seconds, the session manager will detect the abnormal disconnect and cleanup all resources. After the emergency session

has completed, the client returns to the state it was in prior to the emergency call.

95.4.2.2 DND Behavior

During the E911 call, this feature will transition the client into a mandatory Do-Not-Disturb (DND) mode. This results in rejecting all new inbound requests. Requests subject to being rejected include: new calls, instant messages, collaborations, etc. After the operator disconnects the call, the client will disable this DND behavior.

95.4.2.3 Active Collaboration Behavior

Active collaboration sessions (those created before an emergency call) will be cancelled if the client establishes a call to the emergency operator. Remote participants of the collaboration will observe the cancelled collaboration as if the used had clicked the “Stop” button of the collaboration session window.

95.4.2.4 Client Set Behavior

During the E911 call, the i200x device will behave as described in Section 95.5 “i200x Call Control Behavior”.

95.4.3 SMC Backward Compatability

The complete E911 Originator Hold feature will not be sourced in the 3.x clients. However, 3.x clients can benefit from the ‘mid-call request denial’ (Section 95.3.5) portion of the feature, as this is a network feature. Additionally, limited compatability testing will be performed to ensure the 3.x clients function correctly with the MCS 9.0 Session Manager. For instance, the mid-call reject scenarios should always revert the call back to the PSAP operator.

95.5 i200x Call Control Behavior

When the i200x client is used to originate an E911 call, the behavior of the set will change during that call to prevent the originator from disconnecting the call or initiating mid-call features.

95.5.1 Emergency Call Established

By default provisioning this originator hold feature is disabled. In this case, the clients behavior is not modified. However, if the feature is enabled and an emergency call is established, the device behavior will be modified in the following areas:

1. Do-not-disturb (DND) behavior will be enabled for the life of the call
2. All soft-keys are removed from the LCD display.
3. Subset of keys will not function.
4. Device mode behavior is modified

95.5.1.1 DND Behavior

During the emergency call this feature will temporarily enable DND on the device that is involved in the call. This results in rejecting all new inbound requests. Requests subject to being rejected include: new calls, instant messages, collaborations, etc. After the operator disconnects the call, the device will disable this DND behavior.

95.5.1.2 Soft Key Behavior

During the emergency call this feature will remove all soft-labels from the LCD display, and disable all softkeys. This new behavior prevents the originator from initiating new mid-call features.

95.5.1.3 New Key Behavior

During an emergency call this feature will consume key press events that would normally allow the call to be disconnected. For instance, pressing the 'Release' key or the 'onhook' button (on which the handset usually rests) would typically disconnect the call. The i2004 illustrated in Figure 7 highlights the keys that are impacted. The following keys will be disabled during an E911 call:

- Hold
- Line Keys
- Mute
- Inbox
- Service
- Release
- Soft Keys
- Address Book
- Outbox
- Transfer

Figure 7 i2004 during E911 call with originator hold enabled

95.5.1.4 Device Mode Behavior during Emergency Call

During the emergency call, new behavior will be assigned to the ‘Release’ button and hook-switch button as illustrated in Table 2. Bidirectional transitions between handset mode and speakerphone (or headset) mode are allowed. After the emergency session has completed, the i200x returns to the state it was in prior to the emergency call.

Table 2: i200x Emergency Terminator Call Control Behavior

Emergency call is made using:	Action taken: Handset On-hook (assuming handset was offhook)	Action taken: Release Key Pressed
Handset Mode	The device transitions to speakerphone mode. The call is not disconnected.	No action taken. The call continues in handset mode. The call is not disconnected.
Speakerphone Mode	No action taken. The call continues in speakerphone mode. The call is not disconnected.	No action taken. The call continues in speakerphone mode. The call is not disconnected.
Headset Mode	No action taken. The call continues in headset mode. The call is not disconnected (current behavior).	The device transitions to speakerphone mode. The call is not disconnected.

95.5.1.5 Multi-Line Behavior

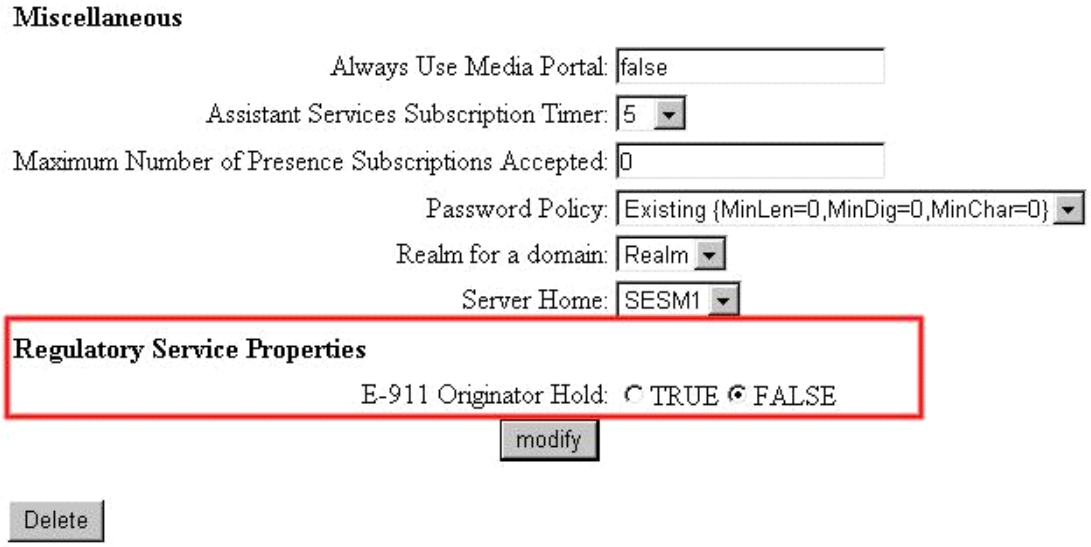
The i200x devices allow for multiple subscribers (6 maximum) to be concurrently logged in to the device. When this feature is enabled, the line that establishes a call to an emergency operator will become active and the remaining lines will be ignored. For instance, inbound calls for any subscriber logged in on the device will not be presented when an emergency call is active.

95.6 Provisioning Client Behavior

95.6.1 Domain Configuration

The E911 Originator Hold feature will be provisioned as a boolean (sub) domain parameter. Provisioning the service option against the domain allows the feature to be enabled on inbound 911 calls from non-registered routes, for instance a PRI gateway. The default value of this parameter will be false indicating that the feature is disabled. The figure below illustrates this domain parameter.

Figure 8 E911 Originator Hold domain parameter

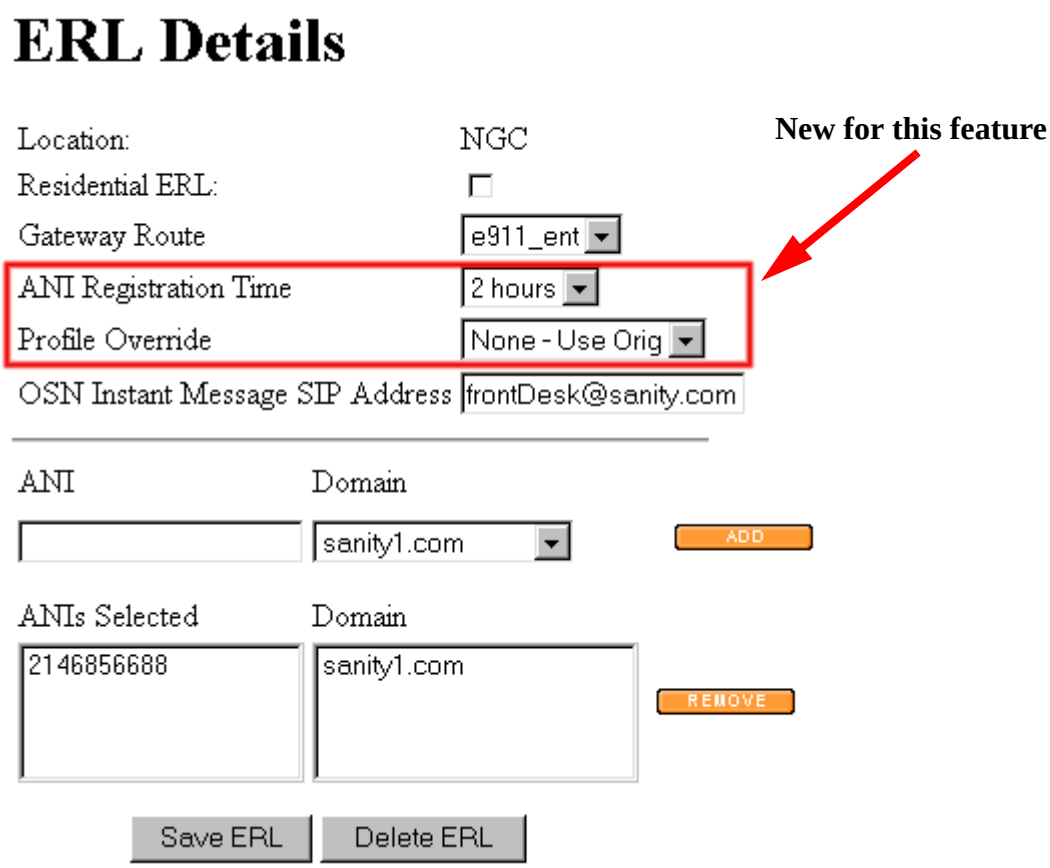


The parameter configuration at the sub-domain will have higher precedence over the configuration at the root domain.

95.6.2 ERL Configuration

The Emergency Response Location provisioning will be modified by this feature to include a customizable ANI Registration time and a Profile Override.

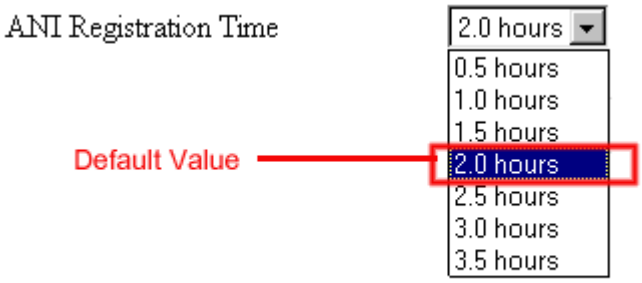
Figure 9 ERL Provisioning



95.6.2.1 ANI Registration Time

This parameter allows the domain administrator to configure the amount of time a enterprise callback number is bound to the originating E911 subscriber. Previously, this value was fixed at 2 hours. The dropdown will allow the administrator to select a value from a list as shown in Figure 10 .

Figure 10 Ani Registration Time

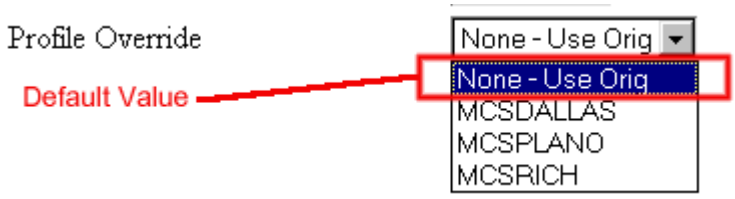


The ANI registration time applies only to enterprise ERLs.

95.6.2.2 Profile Override

This parameter allows the administrator to associate a CS2K profile to an ERL location. This simplifies routing on the MCS session manager[1] by not using telephony translations to override the profile. The dropdown will display all CS2K profiles available in the root domain and all sub-domains, as well as the default value of 'None - Use Orig' as shown in Figure 11 .

Figure 11 Profile Overide



The profile override parameter applies only when routing to CS2K gateway routes that require a different profile. For example, routing to a CS2K that has connectivity to multiple PSAP jurisdictions.

The default value of 'None- Use Orig' should be used to continue using the profile of the originating subscribers (sub)domain. That is, no static association between the ERL location and the profile.

95.6.3 Open Provisioning Interface

The open provisioning interface allows third-party applications to invoke methods on the remote MCS provisioning server. This feature will add two new attibutes to the ErlInfo provisioning entity:

- ANI_REG_TIME
- PROFILE_OVERRIDE

Additionally, a new OPI exposed method will be added under "Domain Profile Operations" to allow a client to retrieve a list of profiles under a given root domain. An OPI client would invoke this method prior to adding or modifing the ERL(s).

String[]::getAllDomainProfiles(String::domainName)

95.7 Hardware Requirements or Dependencies

Not Applicable.

[1]Q00902906 : E911 calls can complete to wrong E911 PSAP

95.8 Software Requirements or Dependencies

Not Applicable.

95.9 Limitations and restrictions

1. The behaviors introduced by this feature are limited to the MCS clients, and may not work with third party SIP clients or legacy clients not compliant with the Resource-Priority header.
2. MCS clients compliant are SMC 4.0, SMC 9.0 and IPCM 9.0.
3. Unable to establish a three way call with an emergency number.
4. During an emergency call the operator will not hear a tone when the originator attempts to disconnect the call.
5. Protocols implementing a single stage release (e.g. H323 protocol) will not be able prevent the originator from disconnecting the call.
6. Emergency calls from foreign domains, including other MCS systems, are not supported.
7. Emergency calls initiated using Click-To-Call will not complete when the Session Manager is in overload.
8. Blind transfer to an emergency number are not allowed.
9. All limitations and restrictions documented in [3] (“MCS3.0 E911 Enhanced 911”) also apply to this feature.

95.10 Compliance Statement

This feature introduces a partial implementation of the Resource-Priority SIP header as documented in draft-ietf-sip-resource-priority-05 [2].

The documented intention of the Resource-Priority header is to request a level of priority when allocating resources (by including the Resource-Priority header in a SIP Request message). The MCS intention of the Resource-Priority header is to add a Resource-Priority header in the 200 OK response message to indicate the User Agent Client that the call is an emergency call and that a certain level of priority has been granted.

The MCS session manager does not implement request behavior relating the Resource-Priority SIP header as described in [2].

95.11 Interactions

95.11.1 Call Park

Call Park is service supported only with MCS core clients. Thus the Call Park service is disabled in emergency calls by disabling Call Park controls from MCS clients during emergency calls.

95.11.2 Assistant / Assisted User

95.11.2.1 Assistant calls 911

In the event the assistant calls an emergency number and establishes a call to the PSAP operator, the clients will exhibit modified behavior to minimize interruptions to the emergency call.

The assistant console will continue to be updated with presence information of the assisted users. However, the context menu will disallow any new call or session from being initiated from the assistant console during that call.

When an assisted user parks a call while an assistant is on a 911 call, the assistant will *not* be presented with this parked call. After the emergency call is completed, the assistant would need to logout and login again to receive the notification of the parked calls. The assisted user can retrieve the parked call at any time. The purpose is to prevent any distractions while the client is engaged in an emergency call.

95.11.2.2 Assisted User calls 911

The emergency call from an assisted user behaves in the same manner as previously describer in the client sections (Section 95.4 for SMC or Section 95.5 for i200x Device).

95.11.3 Click-to-Call

Click-To-Call calls are made either by: directly by logging in to the Personal Agent (PA) from the Click-To-Call page or indirectly by initiating a call form a SMC in converged mode.

Click-To-Call calls work by having the PA establish a call with the originator and then transferring the originator to the terminator. Added complexity is introduced depending on whether the originating user is hosted by a CS2K device.

Emergency calls attempted via Click-To-Call will be established. However limited caller hold feature support is provided. Detailed scenario behavior is presented in the following sections.

Warning: It is not recommended to place emergency calls using Click-To-Call for the following reasons:

- The selected emergency location is determined by the location provisioned in the user screen of the Provisioning Client and not the location selected during login / registration.
- The emergency numbers dial plan and translations may not be synchronized between the PAD's switch and MCS.
- The E911 caller hold feature is not enforced on all Click-To-Call scenarios.

95.11.3.1 PA Click-To-Call; Orig: Sip User, Term: emergency number

This scenario works as long as the subscriber originating the call is located at Provisioning Client User location. The Sip User's client will receive the Resource-Priority header and should be able to disable all mid-call and terminating controls.

95.11.3.2 PA Click-To-Call; Orig: emergency number (hosted by CS2K), Term: Sip User

In this scenario the Emergency center is called first and then transferred to the Sip User. The Emergency center operator will answer the call and hear ringback until the Sip User Answers the call. If the terminator does not answer the call, the operator will hear ringback until the answer timer expires.

However, if the Click-To-Call call is established, the caller hold feature would not be enforced by the terminator's device. Mid-call requests will be rejected by the session manager.

95.11.3.3 PA Click-To-Call; Orig: emergency number (not hosted by CS2K), Term: Sip User

In this scenario the Emergency center is called first and then transferred to the Sip User. The Emergency center operator will answer the call and hear ringback until the Sip User Answers the call. If the terminator does not answer the call, the operator will hear ringback until the answer timer expires.

However, if the Click-To-Call call is established, the caller hold feature would not be enforced by the terminator's device. Mid-call requests will not be rejected by the session manager.

95.11.4 Converged Desktop Calls

95.11.4.1 Emergency Call originated from PAD

In this scenario the subscriber is dialing the emergency number directly from the Preferred Audio Device (PAD). The device hosting the PAD may be engineered to route emergency calls directly or through the MCS Session Manager.

When the call is routed directly by the PAD's hosting switch the emergency call will follow the PAD's switch emergency call policy.

When the call is routed via the MCS, the MCS session Manager will send the Resource-Priority header back to the switch hosting the PAD in the 200 OK. The PAD's switch must implement the Resource-Priority Header in order to prevent caller disconnect. Mid-call requests will be rejected by MCS Session Manager with a 403 error response.

95.11.4.2 PA Click-To-Call; Orig: 911 (hosted by CS2K) , Term: Converged Desktop User

In this scenario the Emergency center is called first and then transferred to the Sip User. The emergency center operator will answer the call and hear ringback until the Sip User Answers the call. If the terminator does not answer the call, the operator will hear ringback until the answer timer expires.

If the Click-To-Call call is established, the CD user will be allowed to terminate the call. Mid-call requests will be rejected by the session manager.

95.11.4.3 PA Click-To-Call; Orig: 911 (not hosted by CS2K) , Term: Converged Desktop User

In this scenario the Emergency center is called first and then transferred to the Sip User. The emergency center operator will answer the call and hear ringback until the Sip User Answers the call. If the terminator does not answer the call, the operator will hear ringback until the answer timer expires.

If the Click-To-Call call is established, the CD user will be allowed to terminate the call. Mid-call requests will not be rejected by the session manager.

95.11.4.4 PA Click-To-Call; Orig: Converged Desktop User with PAD hosted by CS2K, Term: 911

In this scenario the subscriber PAD device is called first and then transferred to the emergency center.

After the Click-To-Call call is established, the CD user will be allowed to terminate the call, but mid-call requests will be rejected by the session manager.

95.11.4.5 PA Click-To-Call; Orig: Converged Desktop User (not hosted by CS2K), Term: 911

In this scenario the subscriber PAD device is called first and then transferred to the emergency center.

It is assumed that the switch hosting the PAD is engineered to route the emergency call directly, thus following the PAD's switch emergency call policy.

95.11.4.6 Emergency Call originated from SMC Converged Client

Same behavior as Personal Agent Click-To-Call. See Section 95.11.4.4 and Section 95.11.4.5.

95.11.5 Call Pickup

Emergency Enterprise callbacks to a subscriber belonging to a Call Pickup group will not be routed to the call pickup terminal. Call Pickup terminal routing is driven by CPL routes which are disabled during emergency enterprise callbacks.

95.12 Glossary

Term	Description
MCS	Multimedia Communication Server
SMC	Personal Communication Client
PAD	Preferred Audio Device
PA	Personal Agent

95.13 References

1. SIP: Session Initiation Protocol (http://www.ietf.org/rfc/rfc3261.txt?number=3261)
2. Communications Resource Priority for the Session Initiation Protocol (http://www.ietf.org/internet-drafts/draft-ietf-sip-resource-priority-05.txt)
3. MCS3.0 FTR307 Enhanced 911 Feature Description

96: Functional Description(FN): A00009726

96.1 Feature name and Feature ID

A00009726, Addition of CALIX_C7 Gateway certificate

96.2 Purpose

In SN09, the gateway certificate/profile “CALIX_C7” is created in order to provision the Calix C7 H.248 large line gateways in SESM. The Calix C7 gateway will support up to 1023 endpoints (POTS lines) per VMG.

This MG is being introduced under ICAF A00009726. The SESM provisioning code was submitted as part of activity A00011746. That feature was introduced to set the LGRP type in the certificate.

96.3 Customer Facing Document Changes

After the code changes, when associating a media gateway using SESM GUI, in the “Gateway Profile Name” pull down list, the following new profile name in addition to the existing profiles will show up as a selection choice.

CALIX_C7

The characteristics of the above gateway are listed in the following table.

GW Profile Name	GW Category	Signal Protocol	Protocol Version	Protocol Port	Service Type	Port/EP Capacity	GWC Profile No.
CALIX_C7	Large	MEGACO(4)	1.0	2944	Line	1023	74

When creating an OSSGATE input XML file for associating a “CALIX_C7” gateway, please reference the above table for values of the tags <mgProfileName>, <mgProtocolType>, <mgProtocolVersion>, and <mgProtocolPort>.

96.4 Related Documentation

GWProfile LGRP_Type (A00011746).doc

The above feature was done in support of assigning a specific LGRP type to a gateway based on the content of the certificate as part of MG association.

97: Functional Description (FN): A00009777

97.1 Feature name and Feature ID

A00009777 - IEMS Mediant 2000 Integration

97.2 Description

IEMS serves as an integrated platform for managing various devices. This document lists the changes that are required in IEMS in order to manage the new device MG 3200 (Network Element).

IEMS will handle the Fault and Performance Management for this new device through SNMP interface.

97.2.1 Acronyms used

NE - Network Element

OID – Object Identifier

MS2000 - Media Server 2000

MG 3200 - Media Gateway 3200

EMS - Element Management System

MIB – Management Information Base

IEMS - Integrated Element Management Systems

SNMP - Standard Network Management Protocol

HTTPS - Secure Hypertext Transfer Protocol

97.2.2 MG 3200 Provisioning

The MG 3200 Network Element can be added using Tools--> Add--> EMS / NE menu. In the initial screen, the "IP Address" field represents the IP of the MG 3200 device to be added, "Type" represents whether it is a EMS or NE (in our case it is "NE"), "Device Type" represents the name of the device to be added (in our case it is "MG 3200"), "Device Version" represents the version of device (in our case it is "9.0") to be added and the "Web Username and Web Password" are the username and password that are needed for the configuration tool.

The subsequent screens gets all the necessary SNMP interface details that are needed for fault and performance. IEMS supports only SNMP "v1" and "v2c" versions of MG 3200 not of "v3" version.

97.2.3 Automatic INI File Backup

MG 3200 has the IPSec configurations stored in a INI file named BOARD.ini, this file will change based on IPSec Configuration changes. IEMS will be taking a backup of this file at regular intervals (configurable) and store it for future use.

IEMS will have the following abilities with respect to the MG 3200 INI Backup functionality,

IEMS will be using HTTPS to communicate and retrieve the INI Files from the MG 3200 device. The design of the HTTPS communication will be by creating an URLConnection with the specified HTTPS URL and establishing a connection. The Authentication will be
taken care by using the appropriate Headers in the URLConnection (basic and digest authentication).

The Right Click Menu on the MG 3200 will have a new menu item to Configure INI Backup . This will popup the INI Configuration dialog similar to that of a MS 2000 device. This screen will have the provision to configure the INI Backup to occur daily or a weekly basis and at a particular time.

A successful configuration will initiate and schedule the next back up time using the timer scheduler. In the design part IEMS will mostly be using the MS 2000 code for scheduling and the GUI pop up. IEMS will write new code to handle the HTTPS communication, Certificate Handling and Authentication for MG 3200 INI Backup. The following will give a clear picture and what can be done and not done:

- IEMS will be using the following URL to retrieve the INI File - https://<mg3200 ip>/FS/BOARD.ini
- The web username and web password given while datafilling the MG3200 device in to IEMS will be used for Authentication.
- Thus retrieve INI files will be stored in the /data/loads/audiocodes/<mg3200 ip>/<current time>.Board.ini If the file is encoded in the device, the IEMS backup will retrieve and store it in the same way. Please refer Appendix 3 for INI encoding details.
- IEMS will trigger the INI Backup based on earlier configurations during a warmstart of the IEMS.
- IEMS will not push this file to the SDM as it is the case in MS2000

- Configuration of INI back up can be done to all the MG3200 devices configured on the IEMS and not for a single MG3200. And you can schedule it and cannot execute it immediately.

97.2.4 IPSec and IKE Configuration

This feature adds IPSec and IKE configuration capabilities to the MG 3200 node configuration tool. This will allow the craftsperson to enable IPSec for secure messaging between the IEMS and MG 3200 as well as configure the IPSec and IKE parameters necessary for the MG 3200 to securely send and receive messages.

A menu "IPSec and IKE Config Tool" will be available on the right click of the MG 3200 Map Symbol. On clicking this menu, IEMS opens a panel over which the IPSec Configuration frame is embedded.

Refer to the document IPSecFN_CN.pdf for "Add IKE and IPSec parameters to the MG 3200 for IEMS MG 3200 secure messaging."

98: Functional Description (FN): A00009822

98.1 Feature name and Feature ID

A00009822 - General Security Log When the User Logs Out

98.2 Description

The Client Session Monitor tracks and records the authentication's, client starts and client stops of the users within the system. For SN09, those applications which begin reporting client start and stops are MG9kEM and CS2M.

The Client Session Monitor allows the end security user to view reports that display which client application sessions are currently active and for what user. It will also provide the reporting ability to view historical data regarding client application usage by user, date or device. The historical data includes start and end times of client sessions, source ip, destination ip, application name and reason for the session end.

The Client Session Monitor also provides interfaces for the clients to retrieve the last time a given user successfully authenticated against the system. This feature modifies the common launch page to display this last successful authentication time - as well as the sspfs LoginAuthentication GUIs.

The Client Session Monitor Reporting Utility is launchable via the IEMS client as well as direct URL or a cli interface provided on the server.

98.3 Hardware Requirements or Dependencies

This feature is available only on IEMS Central SS systems.

98.4 Software Requirements or Dependencies

SN09 IEMS Central SS software
Oracle

98.5 Limitations and restrictions

Only successful user initiated authentications which are authenticated via the IEMS SS are recorded. Any authentication which is performed locally will not be recorded in the Client Session Monitor.

In the case where a client session appears to still be active via the report - but the security user knows the session to no longer be active - the security user can mark that session as completed. Marking a session as completed will not cause any actions outside the realm of this report. It will simply update the

session activity in the database - it will not force a user off - end their session - etc. If a user is still active and their session is marked completed, when the user truly ends the session - the row will be updated with that action's end time.

98.6 Interactions

None

98.7 Glossary

Term	Description
CS2M	Call Server 2000 Manager
IEMS	Integrated Element Manager Server
IEMS Central SS	IEMS Central Security Server
MG9kEM	Media Gateway 9000 Element Manager

99: Functional Description (FN): A00009823

99.1 Feature name and Feature ID

A00009823 - Security Logging for SSPFS

99.2 Description

This feature adds security logging to the SSPFS CLI scripts. Security logs are to be generated whenever any security affecting parameter is changed from the CLI.

In the event that a hacker or user were to change a security parameter using the CLI, a discrete entry will be written to the security log. Each security log will contain a description of the action, an action identifier, the identity of the user, source address of the user, and the date and time that the action occurred.

99.2.1 Security Log location

The Security Log file is stored at:

/var/log/securitylog

99.2.2 Affected CLI Scripts

99.2.2.1 Login Retries Limit

SSPFS CLI will log whenever an MSAP access threshold is changed. CLI 2-14-6; Login Retries Limit in login_timeout.ksh.

99.2.2.1.1 Security Log output

Feb 22 16:36:31 wnc0y0nr PROG=login_timeout.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=login_timeout.ksh MESSAGE="Setting Retries Limit = 3"

99.2.2.2 Login Session (User Inactivity) Timeout

SSPFS CLI will log whenever an MSAP time interval that controls keyboard lockout is changed. CLI 2-14-1; Login Session (User Inactivity) Timeout configuration in login_timeout.ksh.

99.2.2.2.1 Security Log output

Feb 22 16:33:05 wnc0y0nr PROG=login_timeout.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=login_timeout.ksh MESSAGE="Setting Login Session Timeout = 1440"

99.2.2.3 User Termination Timeout

SSPFS CLI will log whenever an MSAP time interval that controls keyboard lockout is changed. CLI 2-14-2; User Termination Timeout configuration in login_timeout.ksh.

99.2.2.3.1 Security Log output

Feb 22 16:33:28 wnc0y0nr PROG=login_timeout.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=login_timeout.ksh MESSAGE="Setting Login Session Termination Timeout = 1440"

99.2.2.4 User Reauthentication Disable Timeout

SSPFS CLI will log whenever an MSAP time interval that controls keyboard lockout is changed. CLI 2-14-3; User Reauthentication Disable Timeout configuration in login_timeout.ksh.

99.2.2.4.1 Security Log output

Feb 22 16:33:44 wnc0y0nr PROG=login_timeout.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=login_timeout.ksh MESSAGE="Setting Login Session Reauthentication Disable Timeout = 30"

99.2.2.5 Login Session Master Server

SSPFS CLI will log whenever an MSAP time interval that controls keyboard lockout is changed. CLI 2-14-4; Login Session Master Server configuration in login_timeout.ksh.

99.2.2.5.1 Security Log output

Feb 22 16:34:14 wnc0y0nr PROG=login_timeout.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=login_timeout.ksh MESSAGE="Setting Login Session Master Server = test"

99.2.2.6 Socks Security Service

SSPFS CLI will log whenever changes to MSAP security profiles and attributes occurs. CLI 2-13-1-1; Socks Security Service configuration in configureSocksPorts.sh.

99.2.2.6.1 Security Log output

Feb 22 16:41:08 wnc0y0nr PROG=configureSocksPorts.sh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=configureSocksPorts.sh MESSAGE="Setting Socks Server port = 10080"

Feb 22 16:41:12 wnc0y0nr PROG=configureSocksPorts.sh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=configureSocksPorts.sh MESSAGE="Setting Socks Client port = 10090"

99.2.2.7 IEMS Server IP Address

SSPFS CLI will log whenever changes to MSAP security profiles and attributes occurs. CLI 2-13-1-1; IEMS Server IP address configuration in chg_iems_ip.ksh.

99.2.2.7.1 Security Log output

Feb 22 16:42:09 wnc0y0nr PROG=chg_iems_ip.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=chg_iems_ip.ksh MESSAGE="Setting IEMS Server IP Address = 4.4.4.4, Domain Name = wnc0y0nr"

99.2.2.8 Default PAM

SSPFS cli will log whenever changes to the MSAP security configuration (e.g., routing to a security server) occurs. CLI 2-13-3-1-1; Default PAM configuration in pam_switch.ksh.

99.2.2.8.1 Security Log output

Feb 22 16:45:12 wnc0y0nr PROG=pam_switch.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=pam_switch.ksh MESSAGE="Setting Default PAM Configuration"

99.2.2.9 Radius PAM

SSPFS cli will log whenever changes to the MSAP security configuration (e.g., routing to a security server) occurs. CLI 2-13-3-1-2; Radius PAM configuration in pam_switch.ksh.

99.2.2.9.1 Security Log output

Feb 22 16:46:25 wnc0y0nr PROG=pam_switch.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=pam_switch.ksh MESSAGE="Setting PAM Radius Parms: Radius Client Timeout = 12, SAML Connection Timeout = 20, SAML Request Timeout = 10"

99.3 Hardware Requirements or Dependencies

Not applicable.

99.4 Software Requirements or Dependencies

Not applicable.

99.5 Limitations and restrictions

Not applicable.

99.6 Interactions

Not applicable.

100: Functional Description (FN): A00009828

100.1 Feature name and Feature ID

A00009828 - Granular Service Packaging

100.2 Background

Curretly services like Instant Messaging, Client Collaboration features like webpush, filetransfer, whiteboard, transfer clipboard, Etherset support for 1220x phone etc. are part of the basic services and are not service package controlled. There was no way to limit the availability of these services to the end users on a per domain/user basis. The objective of this feature is to make these services part of the service package framework, so that these can be controlled on a per domain/user basis.

100.3 Overview

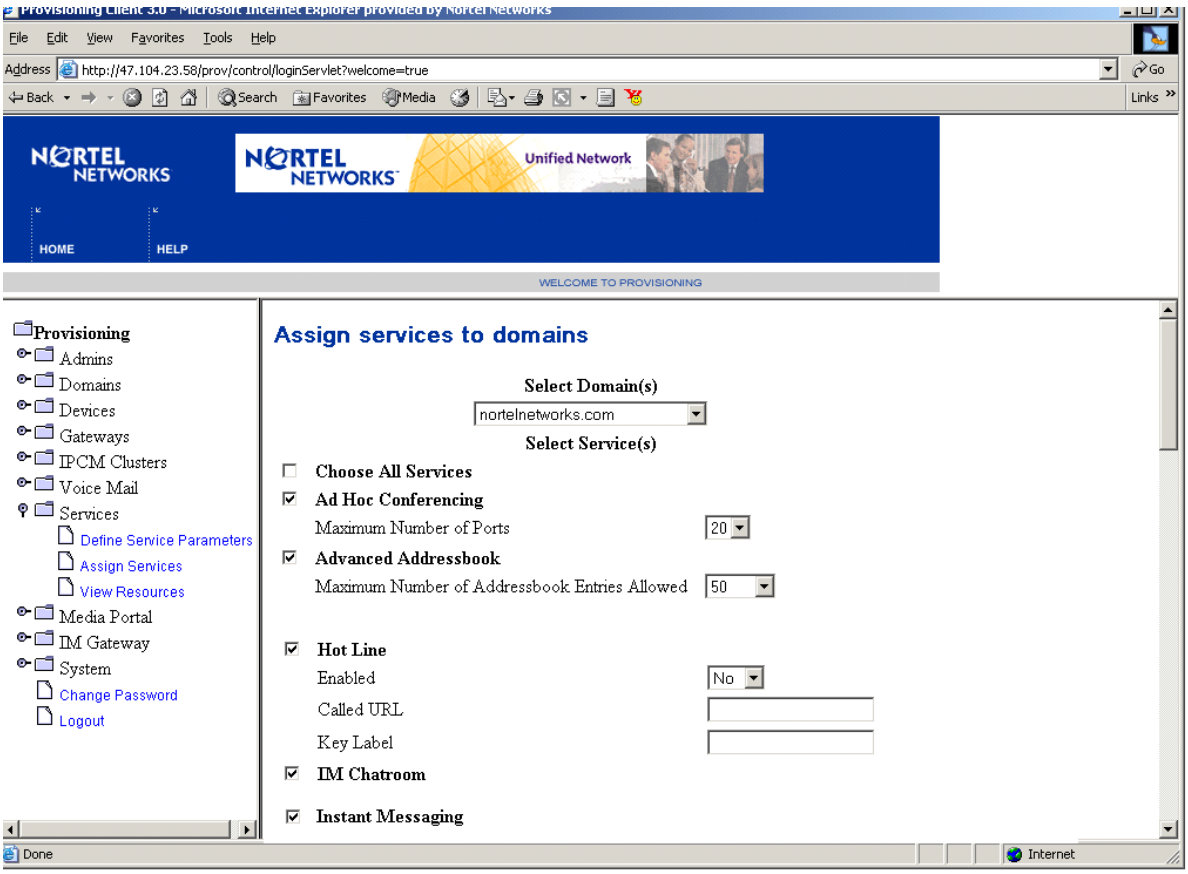
These new services enable an MCS customer to limit the availability of these services to the end users and will provide an option to create service packages at a more granular level.

100.4 Feature Description

100.4.1 Administrator Configuration and Provisioning

100.4.1.1 Instant Messaging Service

Figure 1 Assign Services to Domain(s)



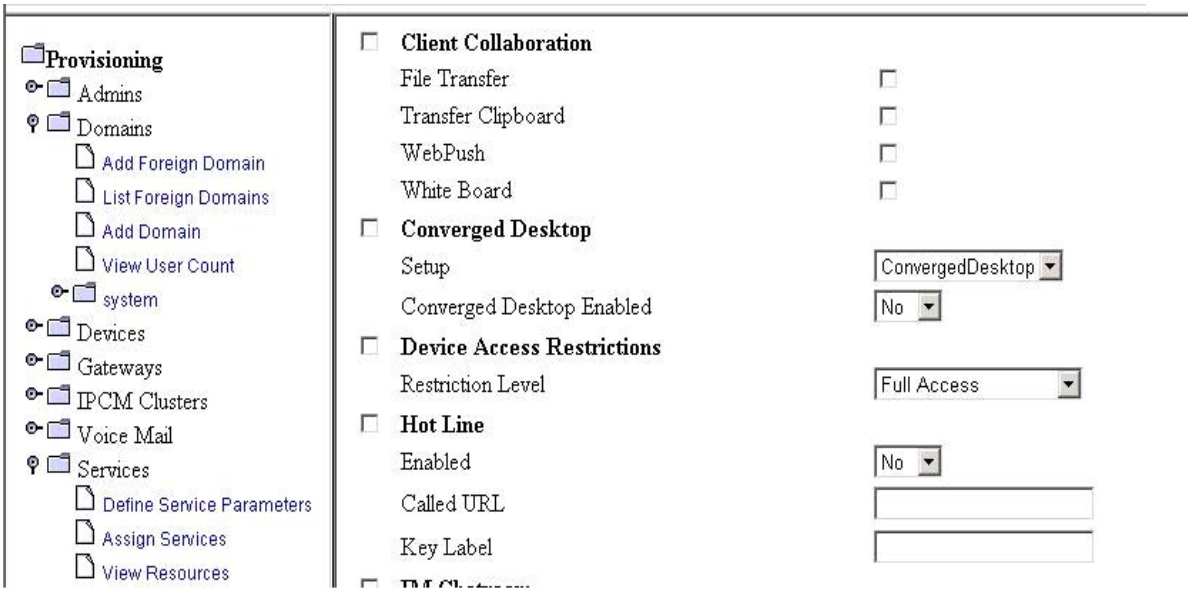
As part of this feature a new service called “Instant Messaging” is defined.

The above web page shows how this service can be assigned to domain(s) in order to include it in the service packages created within that domain.

The “IM Chatroom” service is dependent on the “Instant Message” service. Therefore, the “IM Chatroom” service cannot be assigned to a service package without the “Instant Messaging” service. This dependency is enforced by the Provisioning Client and the Provisioning Module’s service framework.

100.4.1.2 Client Collaboration Service

Figure 2 Assign Services to domain(s)

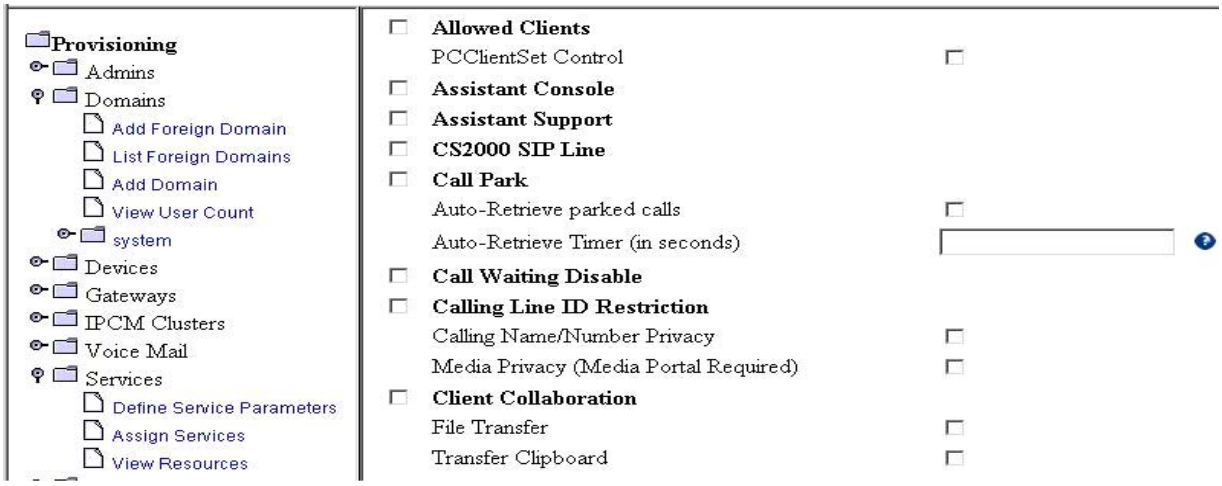


As part of this feature a new service called “Client Collaboration” is defined.

“File Transfer”, “Whiteboard”, “Transfer Clipboard” and “Web Push” are each considered a collaboration that is exposed for use by the subscriber using the Multimedia PC Client as provisioning parameters of the “Client Collaboration” Service.

100.4.1.3 Allowed Clients Service

Figure 3 Assign Services to domain(s)



As part of this feature a new service called “Allowed Clients” is defined. This service will have all the different clients as parms. A new parm called “PC ClientSet Control ” is defined under this service. Interaction of the PC Client with the Nortel i200x phone is controlled by this service parm.

100.4.2 Feature Provisioning

None.

100.4.3 Instant Messaging Service

A new service called “Instant Messaging (IM)” will be defined as part of this feature. A user who has this service in their service package will be able to send/ receive instant messages to/ from other users in the system via the PC Client, PC Client Set, or device as controlled by the IPCM.

Removing this service from the user’s service package will take away this ability from the user. In addition the PC Client will no longer display the icon for this service. Chat services will also be disabled since instant messaging service is necessary to participate in chat services. IM Broadcast service will also be disabled. The IM Routing option will not be available for the user if the IM service is not present in this service package.

The service package contains indication of whether to enable instant messaging for the user. When the “Instant Messaging” service is included in the service package, instant messaging will function on the PC Client, PC Client Set, and IPCM device as it did previous to this feature.

When the “Instant Message” service is absent from the user’s service package, the following changes in functionality will be observed as described in the following subsections.

100.4.3.1 Instant Messaging Service - Multimedia PC Client

This section describes Multimedia PC Client functionality that is removed when the “Instant Messaging” service is absent from the user’s service package.

100.4.3.1.1 Main GUI

The Instant Message and Chat icons will not be present on the icon panel of the main GUI.

Figure 4 Instant Message and Chat Icons on Main GUI

100.4.3.1.2 Quick Start Menu

The Instant Message and Chat icons will not be present on the the Quick Start panel.

Figure 5 Instant Message and Chat Icons on Quick Start Pane

100.4.3.1.3 Session Frame

The Session Frame no longer shows an icon for opening the Instant Message panel. The user will not be able to access the panel, nor will the panel be opened if the PC Client receives an instant message.

Figure 6 Session Frame without Instant Message Icon

100.4.3.1.4 In Session Frame

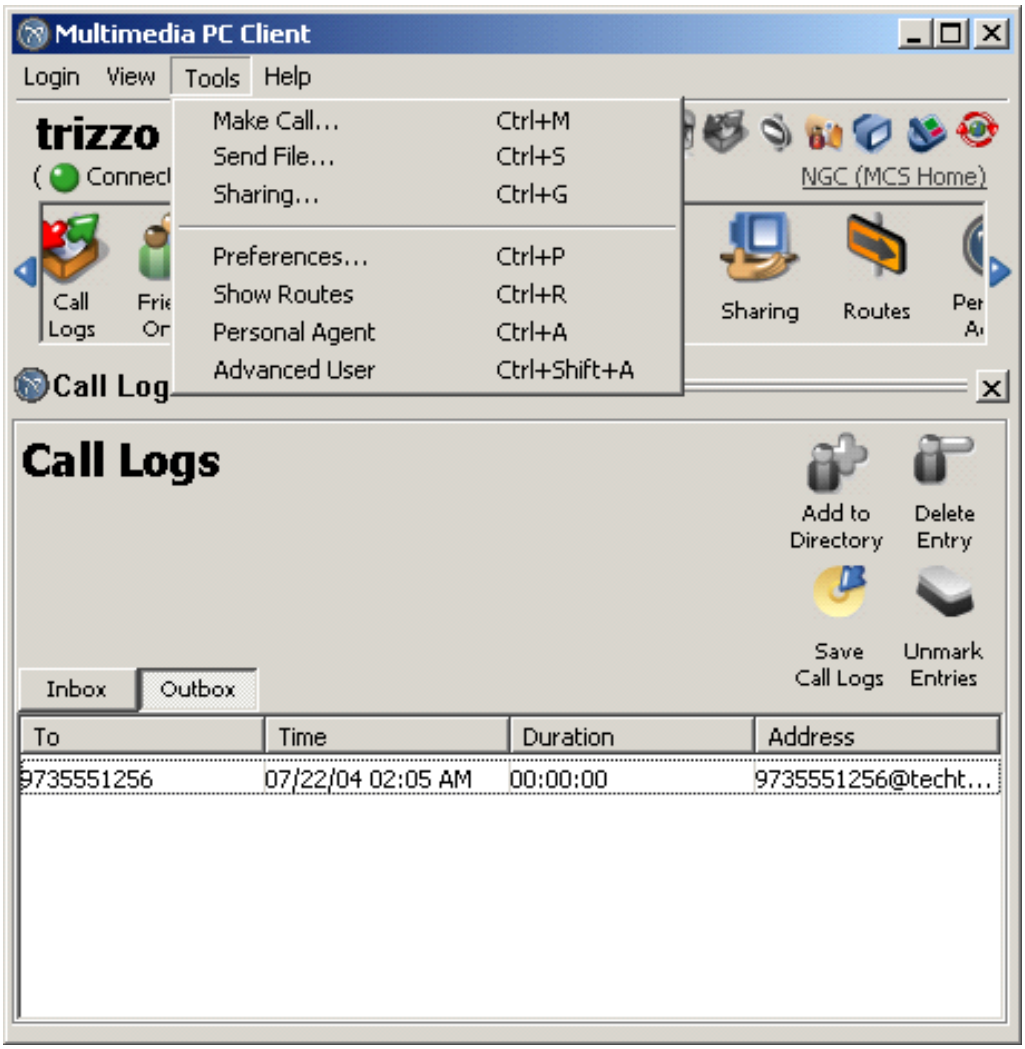
The In Session Frame will no longer show the “Reply with IM” option if the user does not have Instant Messaging Service.

Figure 7 Session Frame without Reply with IM option

100.4.3.1.5 Menus

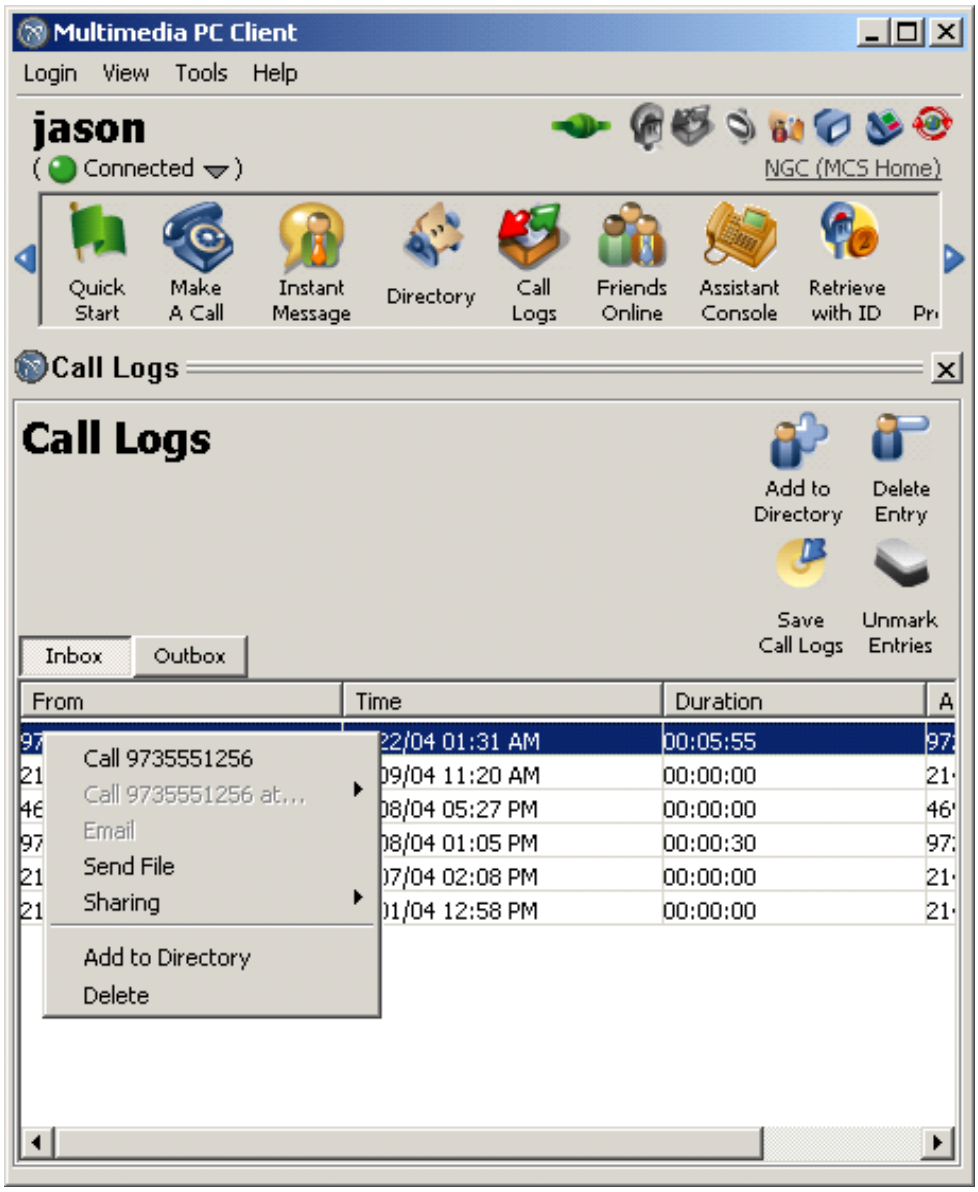
The “Instant Message” and “Start Chat” options will not be present on the Tools menu of the main GUI.

Figure 8 Tools Menu without Instant Message and Chat Items



The right-click popup menus on the Call Logs, Address Book, and Friends panels will not contain the “Send Instant Message” or “Start Broadcast” options.

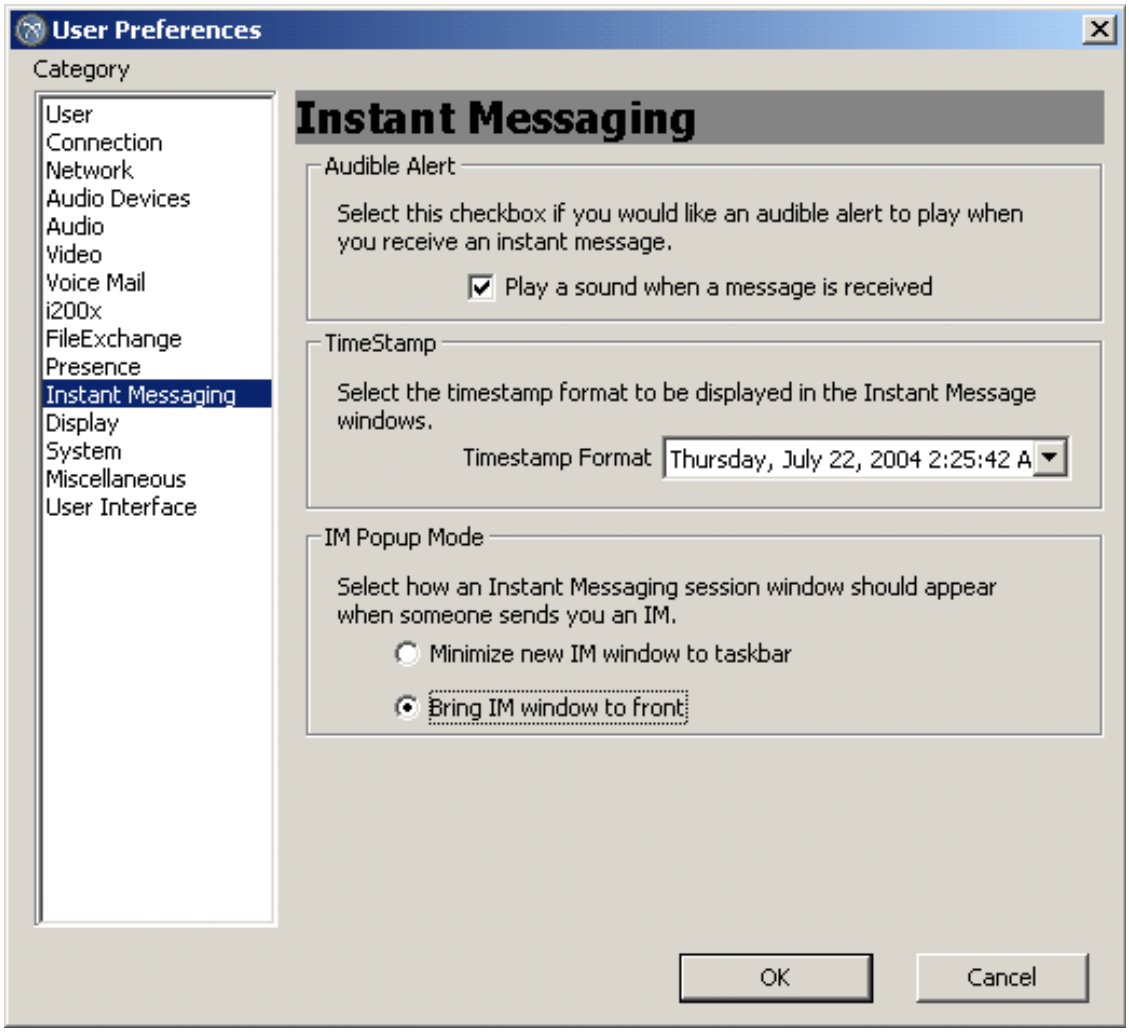
Figure 9 Call Logs Right-Click Menu without Instant Message and Broadcast Items



100.4.3.1.6 1.1.3.1.1.6Preferences

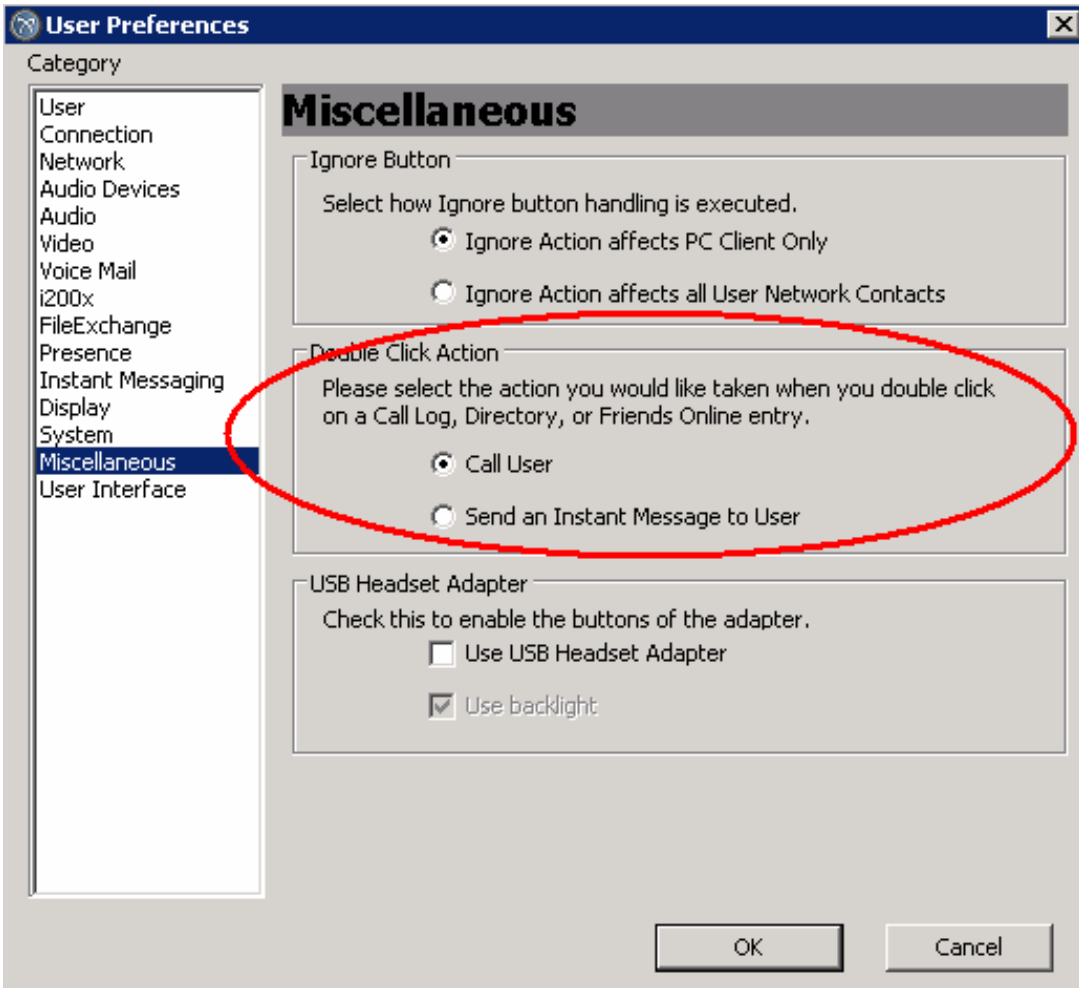
The “Instant Messaging” tab will not be included on the Preferences Panel.

Figure 10 IM tab will not be present when Instant Messaging is disabled



In addition to the Instant Messaging tab, there is a reference to Instant Messaging in the Miscellaneous tab – you can set whether a double-click in the Directory initiates a call or an IM. The entire “Double-Click Action” section of the Miscellaneous tab will not be included, and the double-click action will always be to initiate a call.

Figure 11 Double-click action will not be shown and will always initiate a call



100.4.3.1.7 Messaging

With Instant Messaging disabled, the PC Client will not be able to receive instant messages. If the client does receive an instant message, it will respond to the SIP MESSAGE message with a SIP 415: Unsupported Media Type response.

The same response will be sent if the user receives an invitation to a chat room. The message that is displayed to the user in the GUI will be

“Contact does not have support for instant messages.” for IMs and

“Contact does not have support for chat.” for chatroom invitations.

100.4.3.2 Instant Messaging Service - Multimedia PC Client Set

This section describes Multimedia PC Client Set (200x device that is controlled by the Multimedia PC Client) functionality that is removed when the “Instant Messaging” service is absent from the user’s service package.

100.4.3.2.1 Service Menu

When the “Instant Messaging” service is not included in the user’s service package, the PC Client restricts the device display of the Instant Messaging service menu option as depicted in the following figure.

Note: The option “Send IM” is removed from the Services menu.

Figure 12 Services Menu without “Instant Messaging” Service

100.4.3.2.2 Friends and Address Book

When the “Instant Messaging” service is not included in the user’s service package, the PC Client controlling the 200x device restricts the ability for the user to send an IM from the Friends and Address book as depicted in the two figures that follow.

Note: The option “Send IM” is removed as it was previously available via soft key 3.

Figure 13 Friends Menu without “Instant Messaging” Service

When a user has the “Instant Messaging” service, the Address Book allows the user the abilty to “Send IM (via soft key 2) when viewing the details for a given contact. When the user does not have the “Instant Messaging” service, “Send IM” functionality is removed from the Address Book.

Figure 14 Address Book without “Instant Messaging” Service

100.4.3.3 Instant Messaging Service – IPCM Device

This section describes device functionality that is removed from the user’s devices (200x devices controlled by the IPCM) when the “Instant Messaging” service is absent from the user’s service package.

100.4.3.3.1 Service Menu

When the “Instant Messaging” service is not included in the user’s service package, the IPCM restricts display of the Instant Messaging service menu option as depicted in the following figure: Services Menu without “Instant Messaging” Service.

Note: The option “Send IM” is removed from the Services menu.

Figure 15 Services Menu without “Instant Messaging” Service

100.4.3.3.2 Friends and Address Book

When the “Instant Messaging” service is not included in the user’s service package, the IPCM restricts the ability for the user to send an IM from the Friends and Address book as depicted in the following figure.

Note: The option “Send IM” is removed as it was previously available via soft key 3.

Figure 16 Friends Menu without “Instant Messaging” Service

When a user has the “Instant Messaging” service, the Address Book allows the user the abilty to “Send IM (via soft key 2) when viewing the details for a given contact. When the user does not have the “Instant Messaging” service, “Send IM” functionality is removed from the Address Book.

Figure 17 Address Book without “Instant Messaging” Service

100.4.3.3.3 Assistant Console

When the “Instant Messaging” service is not included in the user’s service package, the IPCM restricts the ability for the user to send an IM from an Assistant Console Quick Actions menu for an “Assistant Console” service subscriber. For more information on the “Assistant Console” service, please see “FTR308 Boss-Secretarial Services” Fuctional Description.

Note: Note: The option “IM” is removed as it was previously available via soft key 3.

Figure 18 Assistant Console Quick Actions without “Instant Messaging” Service

100.4.3.3.4 Messaging

With Instant Messaging disabled, the IPCM device will not be able to receive instant messages. If the IPCM receives an instant message for a user that does not have the “Instant Messaging” service, it will respond to the SIP MESSAGE message with a SIP 415: Unsupported Media Type response.

The message that is displayed to the user in the GUI will be

“Contact does not have support for instant messages.”

100.4.3.4 Client Collaboration Service

A new service called “Client Collaboration” is defined as part of this feature. “File Transfer”, “Whiteboard”, “Transfer Clipboard” and “Web Push” are each considered a collaboration that is exposed for use by the subscriber using the Multimedia PC Client as provisioned parameters of the “Client Collaboration” Service.

If the user’s service package does not contain the “Client Collaboration” service or the respective collaboration parameters are not enabled, then the respective collaboration functionality on the Multimedia PC Client is disabled

as described in the following subsections. The service “Client Collaboration” is used to define if the user can receive any collaboration form other users. If the service is present, then the user will be able to receive all kinds of collaboration requests from other users. The individual service parms are used to define if the user can initiate any collaboration requests. If the parms are not present then the user will not be able to initiate any collaboration request.

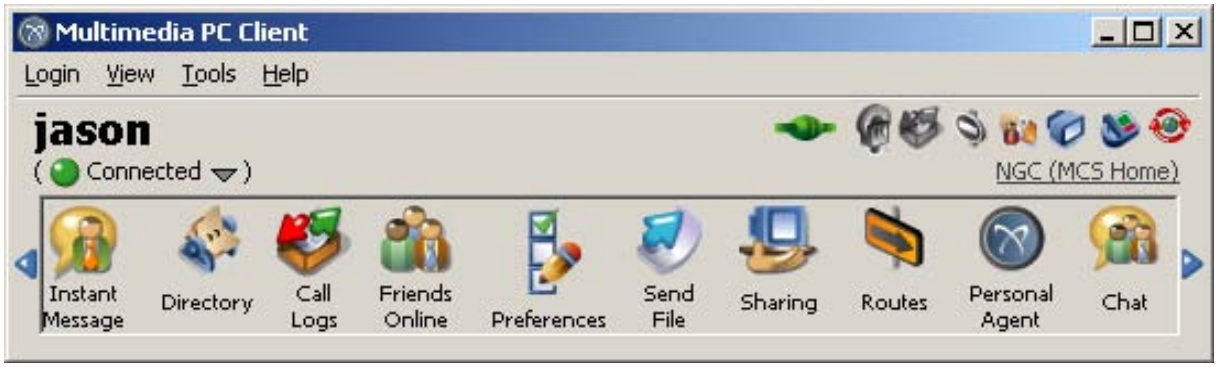
100.4.3.4.1 File Transfer

This section describes how the File Transfer functionality is restricted on the PC Client when the “File Transfer” collaboration is disabled in the service package.

100.4.3.4.2 Main GUI

The *Send File* icon will not be present on the icon panel of the main GUI.

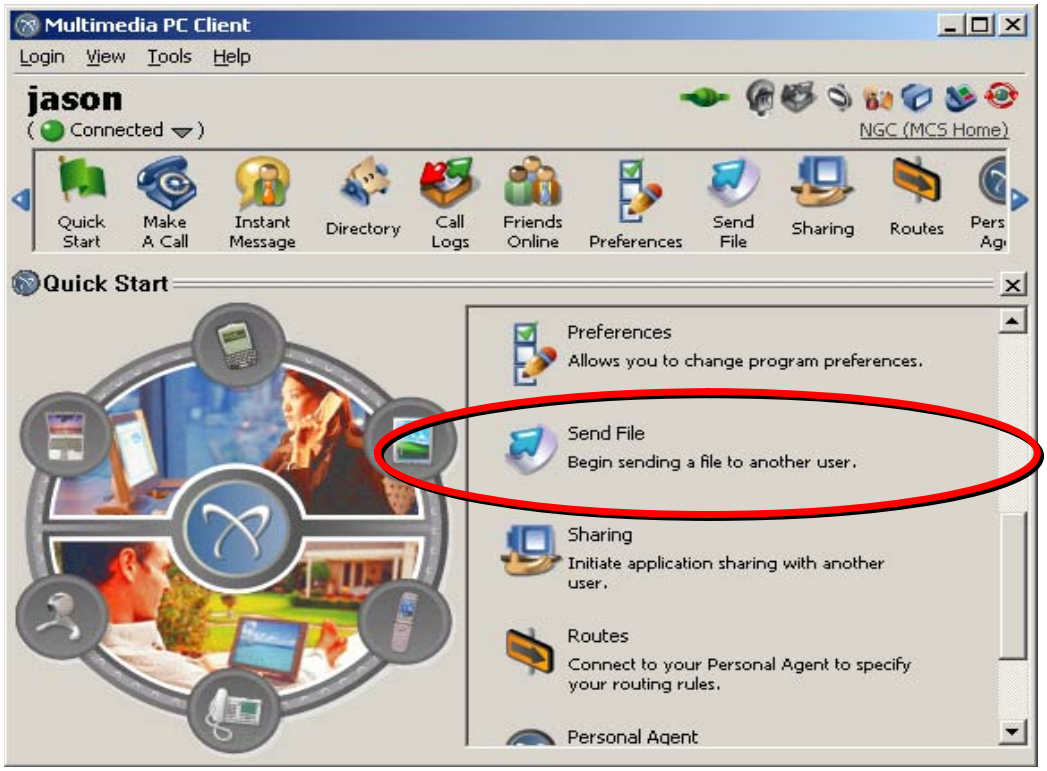
Figure 19 Send File Icon on the main GUI Icon Panel



100.4.3.4.3 Quick Start Menu

The Send File icon will not be present on the the Quick Start panel.

Figure 20 Send File Icon on Quick Start Panel



100.4.3.4.4 Session Frame

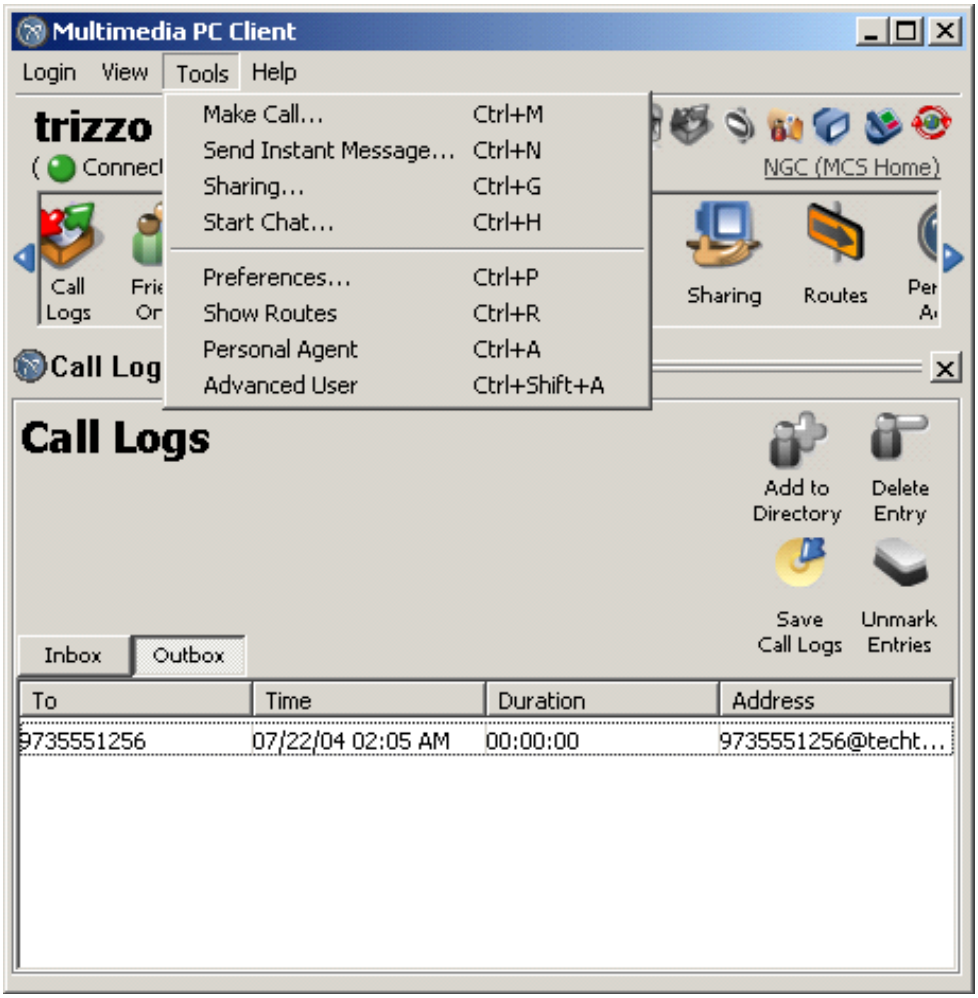
The Session Frame no longer shows the Send File icon. Additionally, the Share panel will not show its Send File icon either.

Figure 21 Collab Panel of the Session frame without the Send File Icon

100.4.3.4.5 Menus

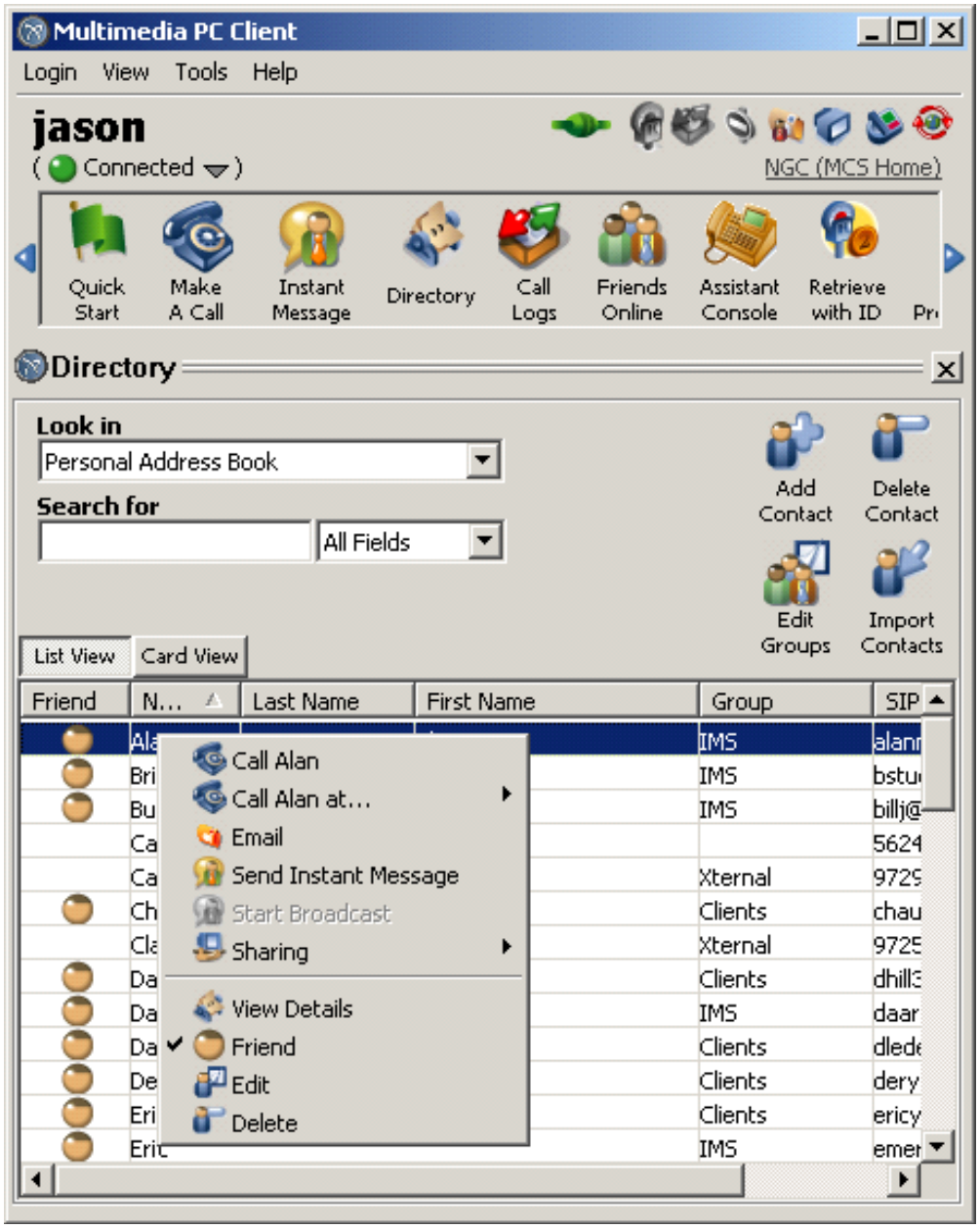
The “Send File” option will not be present on the Tools menu of the main GUI.

Figure 22 Tools Menu without the Send File Item



The right-click popup menus on the Call Logs, Address Book, and Friends panels will not contain the “Send File” option.

Figure 23 Right-Click Menu of the Directory Panel without the Send File Item



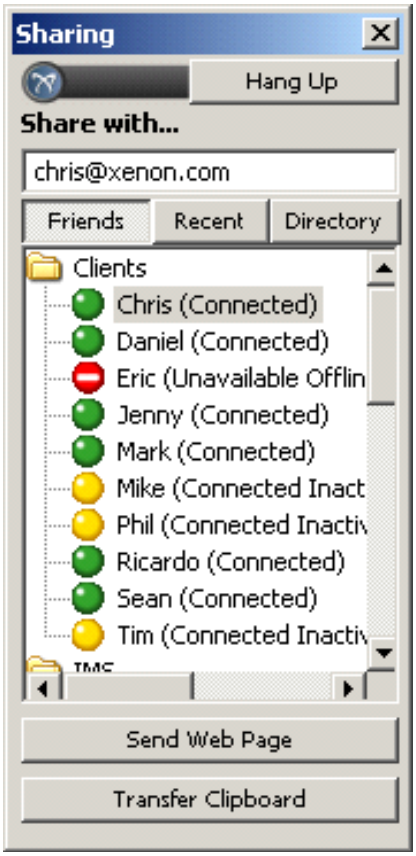
100.4.3.4.6 Whiteboard

This section describes how the Whiteboard functionality is restricted on the PC Client when the “Whiteboard” collaboration is disabled in the service package.

100.4.3.4.7 Share Dialog

The Share Whiteboard button will not be present on this dialog panel.

Figure 24 Share Dialog without the Share Whiteboard Button



100.4.3.4.8 Session Frame

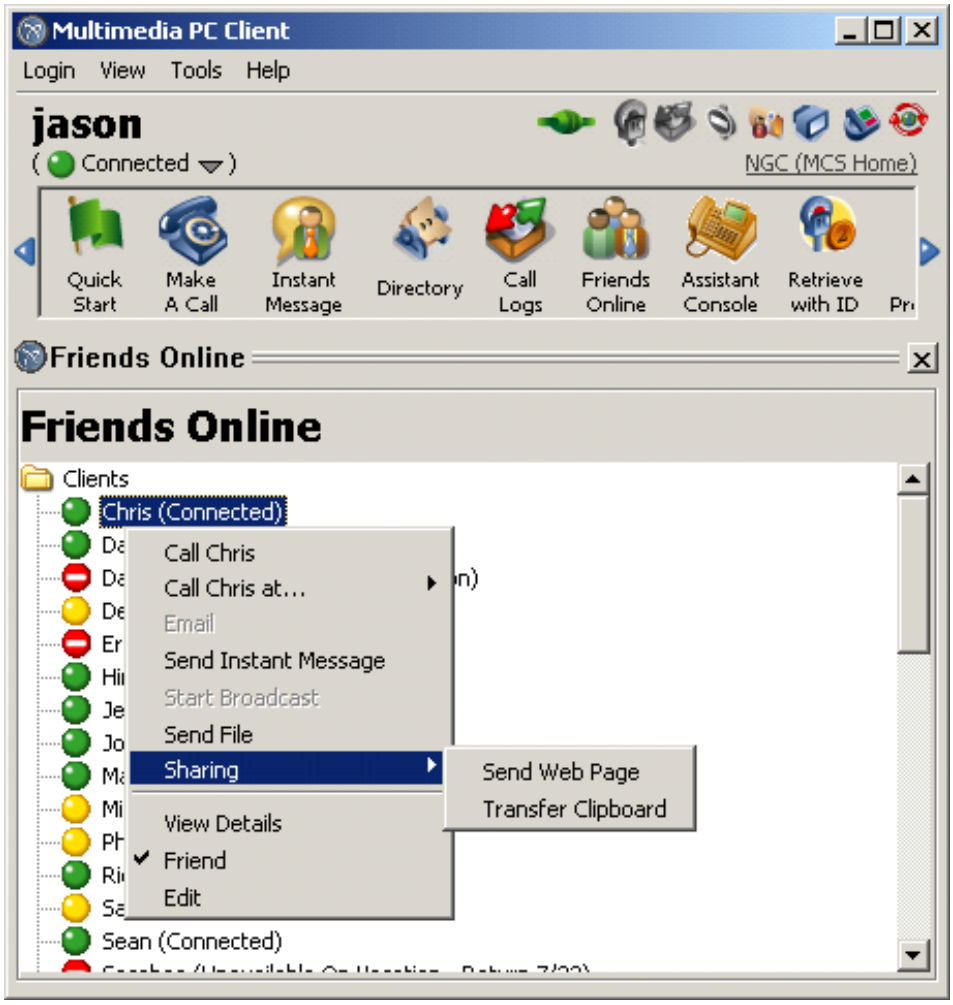
The Share panel on the Session Frame no longer shows the Share Whiteboard icon.

Figure 25 Collab Panel of the Session Frame without the Share Whiteboard Icon

100.4.3.4.9 Menus

The “Sharing” sub-menu of the right-click popup menus on the Call Logs, Address Book, and Friends panels will not contain the “Share Whiteboard”option.

Figure 26 Right-Click Menu of the Friends Panel without the Share Whiteboard Item



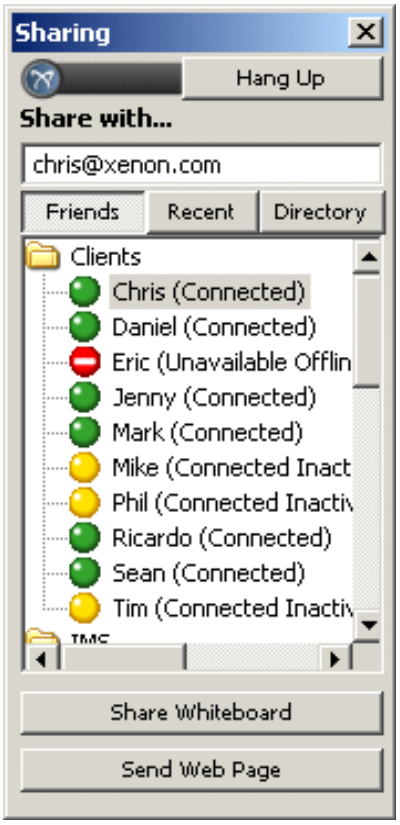
100.4.3.4.10 Transfer Clipboard

This section describes how the Transfer Clipboard functionality is restricted on the PC Client when the “Transfer Clipboard” collaboration is disabled in the service package.

100.4.3.4.11 Share Dialog

The Transfer Clipboard button will not be present on this dialog panel.

Figure 27 Share Dialog without the Share Whiteboard Button



100.4.3.4.12 Session Frame

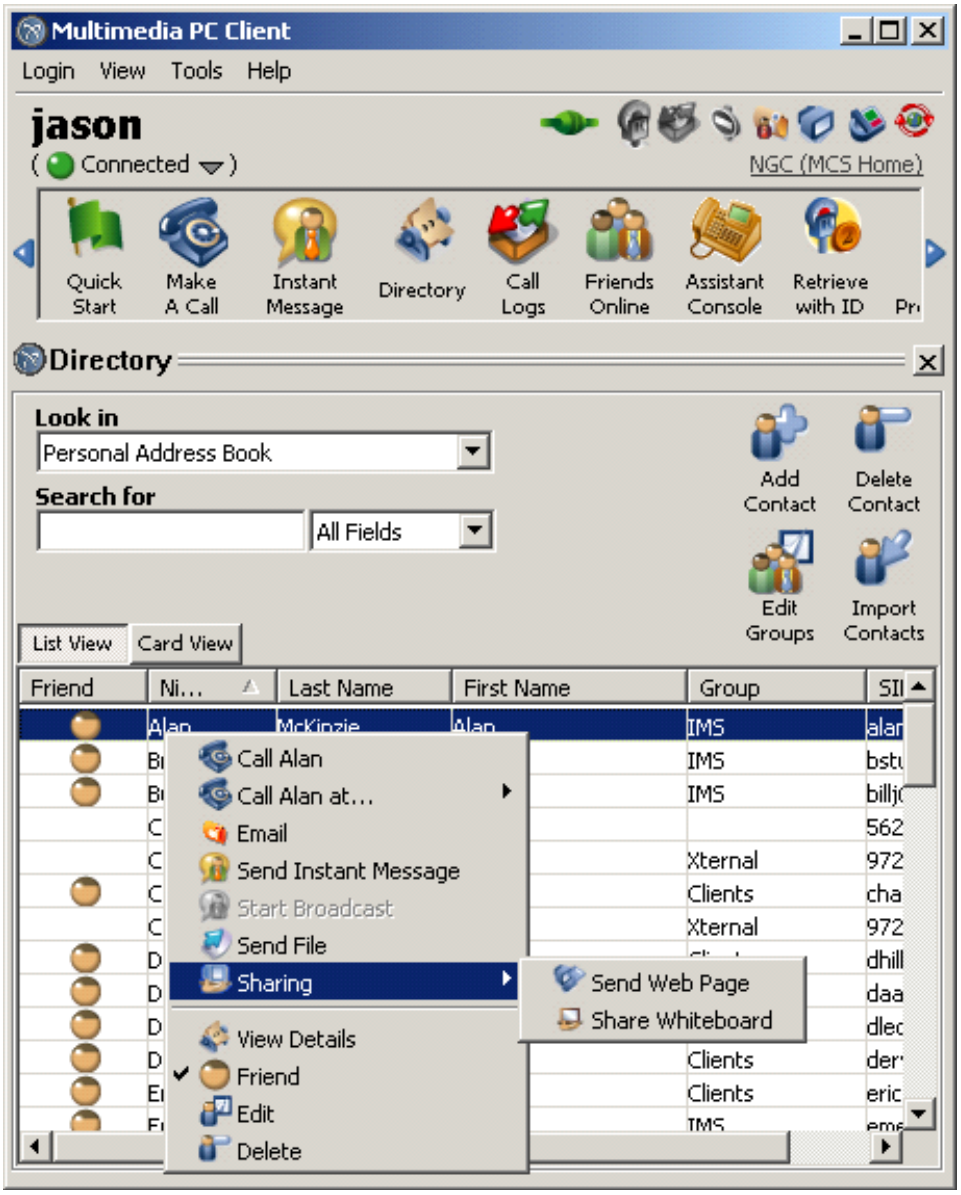
The Share panel on the Session Frame no longer shows the Transfer Clipboard icon.

Figure 28 Collab Panel of the Session Frame without the Transfer Clipboard Icon

100.4.3.4.13 Menus

The “Sharing” sub-menu of the right-click popup menus on the Call Logs, Address Book, and Friends panels will not contain the “Transfer Clipboard” option.

Figure 29 Right-Click Menu of the Directory Panel without the Share Whiteboard Item



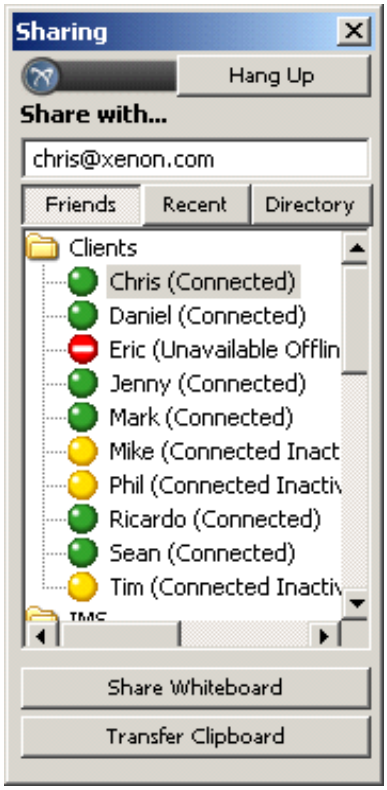
100.4.3.5 Web Push

This section describes how the Web Push functionality is restricted on the PC Client when the “Web Push” collaboration is disabled in the service package.

100.4.3.5.1 Share Dialog

The Send Web Page button will not be present on this dialog panel.

Figure 30 Share Dialog without the Send Web Page Button



100.4.3.5.2 Session Frame

The Share panel on the Session Frame no longer shows the Send Web Page icon.

Figure 31 Collab Panel of the Session Frame without the Send Web Page Icon

100.4.3.5.3 Menus

The “Sharing” sub-menu of the right-click popup menus on the Call Logs, Address Book, and Friends panels will not contain the “Send Web Page” option.

Figure 32 Right-Click Menu of the Friends Panel without the Send Web Page Item

100.4.3.6 Additional Behavior

In addition to the functionality described in the previous sections for the individual collaboration, the following behaviors are also present when disabling collaboration functionality.

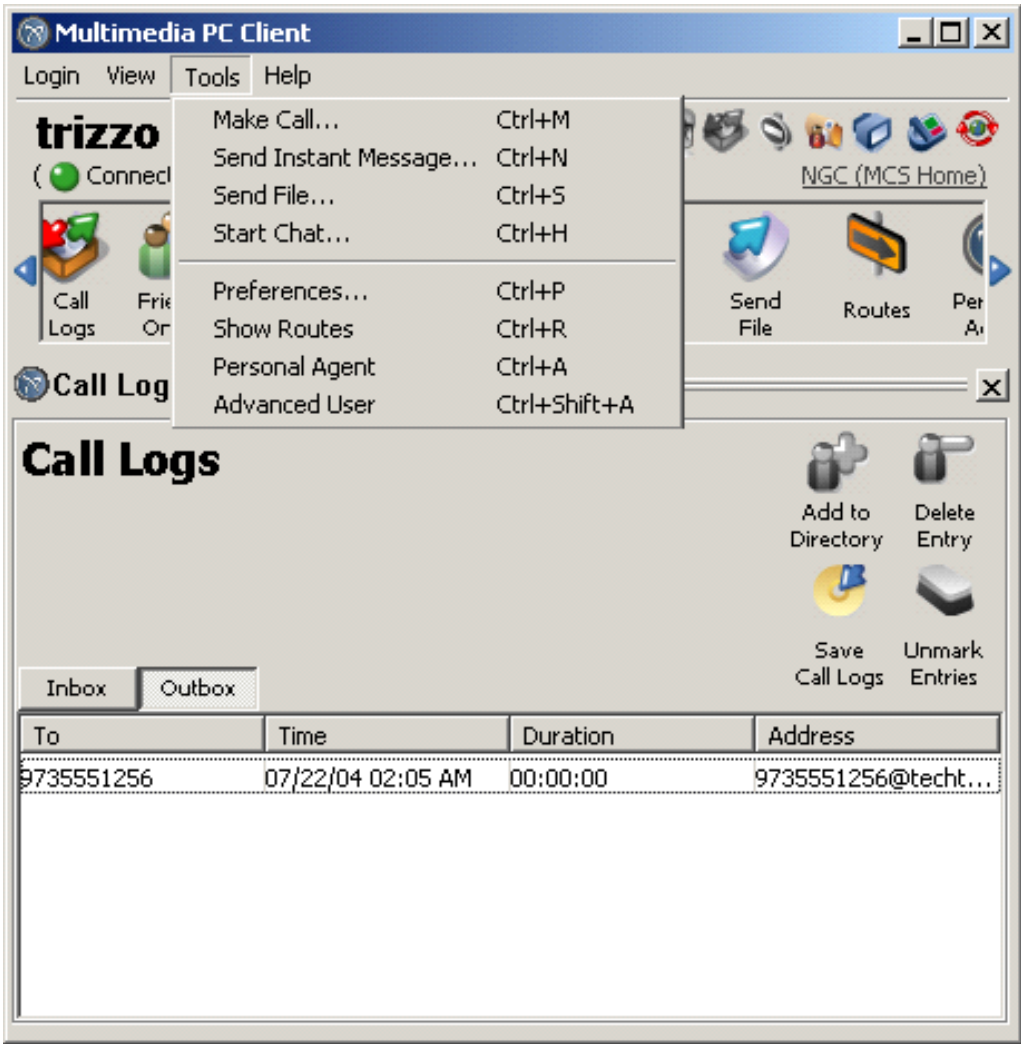
100.4.3.6.1 Collective Sharing Service

Since the Whiteboard, Transfer Clipboard, and Web Push collaboration functionality is grouped for the user on the PC Client as “Sharing” functions, when all three of these collaborations are disabled through the service framework, the “Sharing” functionality will also be disabled as identified in the following subsections.

100.4.3.6.2 Main GUI

The Share icon will not be present on the icon panel of the main GUI.

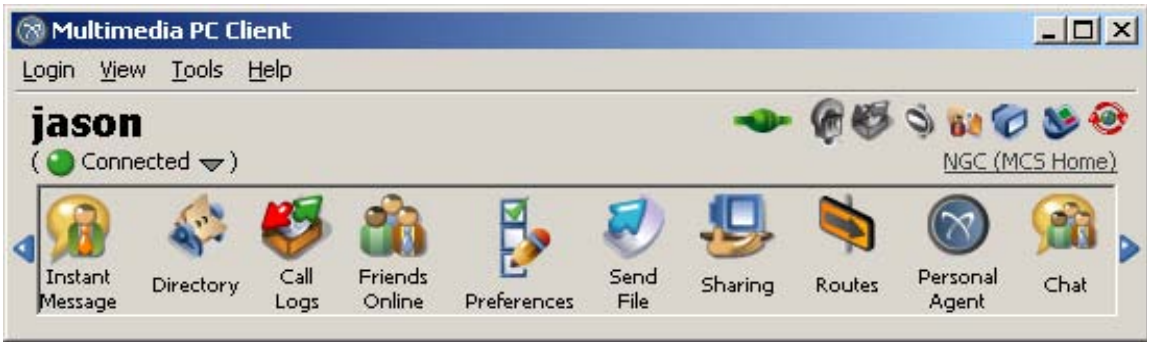
Figure 33 Tools Menu without the Sharing Item



100.4.3.6.3 Quick Start Menu

The Share icon will not be present on the the Quick Start panel.

Figure 34 Sharing Icon on the Main GUI Icon Panel



100.4.3.6.4 Session Frame

The Session Frame will continue to show the Share icon if the File Transfer collaboration is enabled. This icon serves to open and close the collaboration panel on the Session Frame, which is also used for File Transfer. If File Transfer is also disabled, the Share icon will not be present on the Session Frame.

Figure 35 Collab Panel of the Session Frame with only the Send File Icon

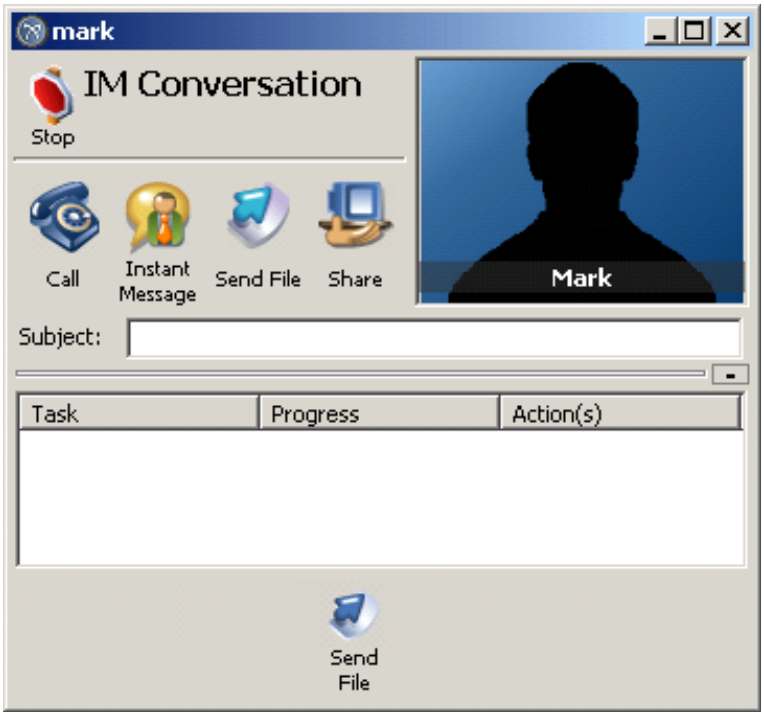
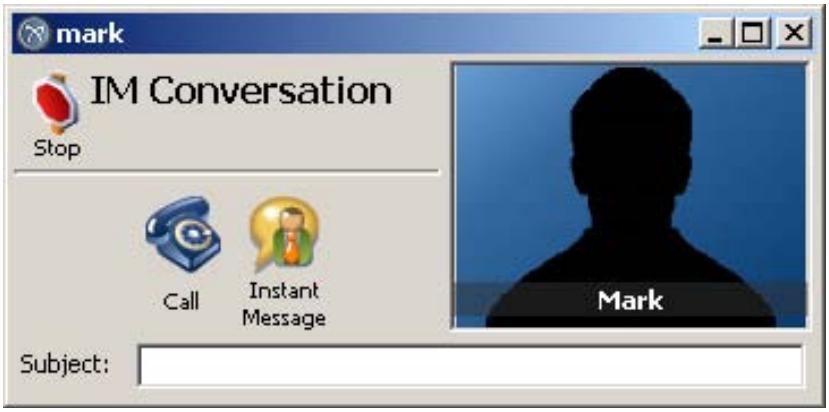


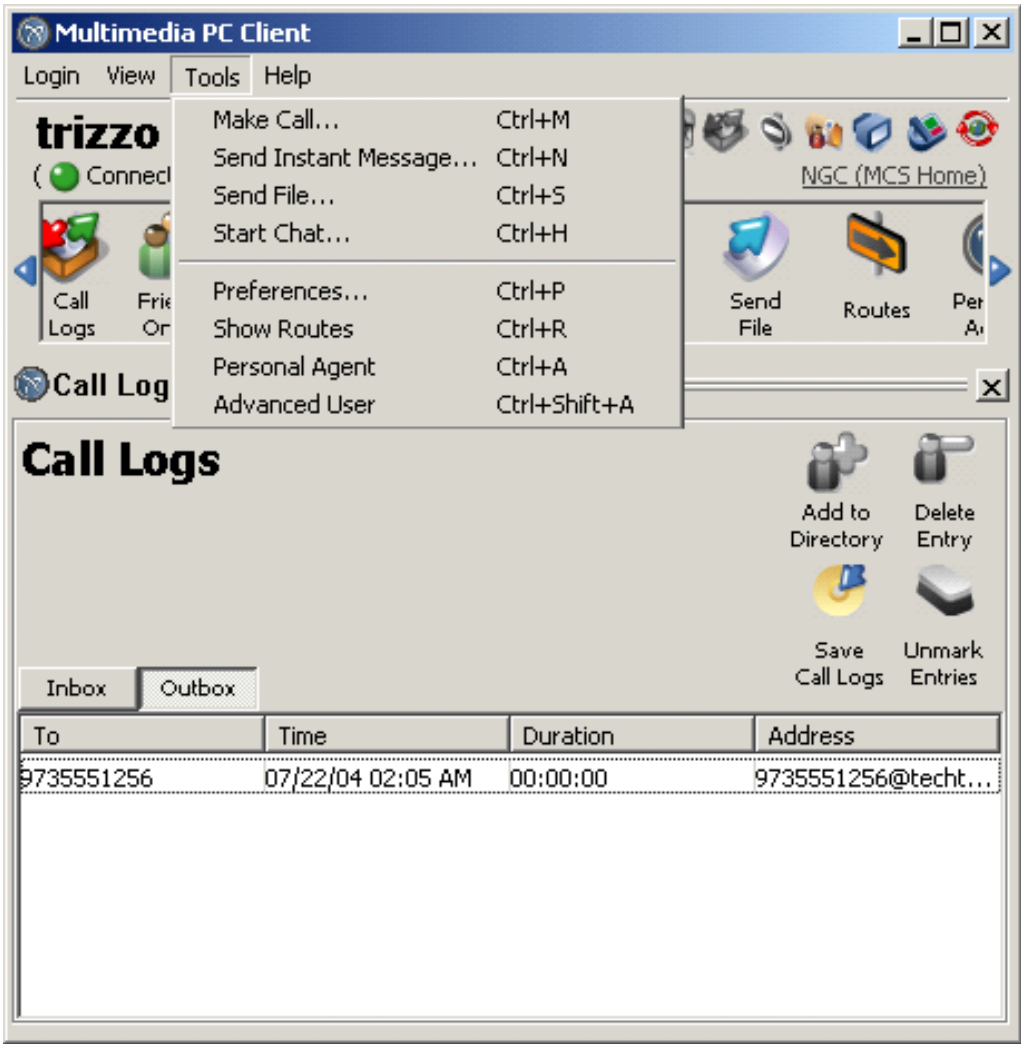
Figure 36 Session Frame without the Sharing and Send File Icons



100.4.3.6.5 Menus

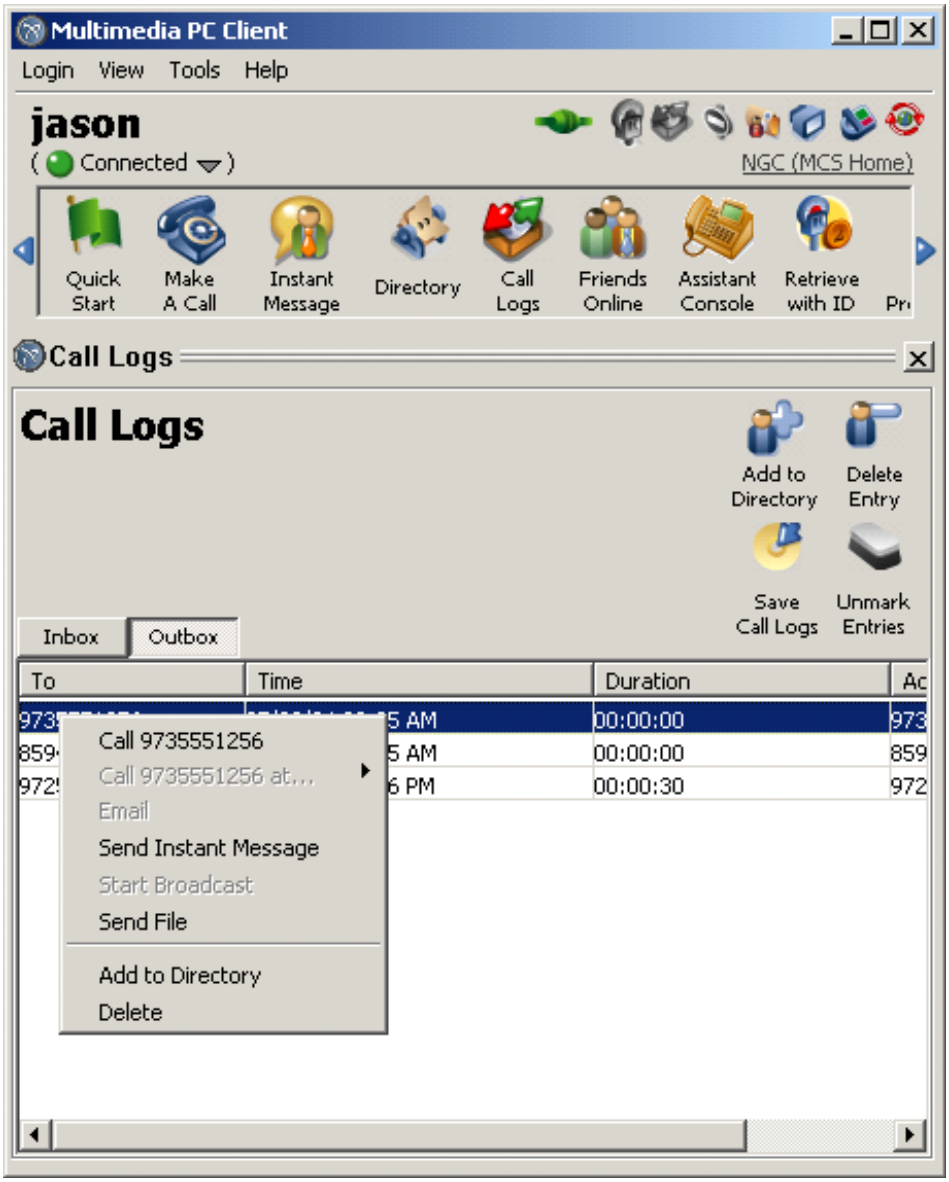
The “Share” option will not be present on the Tools menu of the main GUI.

Figure 37 Tools Menu without the Sharing Item



The right-click popup menus on the Call Logs, Address Book, and Friends panels will not contain the “Sharing” sub-menu.

Figure 38 Right-Click Menu of the Call Logs without the Sharing Sub-Menu



100.4.3.6.6 Messaging

When any collaboration is disabled, the PC Client will respond with a SIP 415: Unsupported Media Type response to any SIP MESSAGE message which invokes a disabled collaboration. MESSAGE messages invoking enabled services will receive SIP 200 OK responses as before.

> ***Note:*** The SIP message that is returned may vary depending on the type of collaboration INVITE that is received.

The message that is displayed to the user in the GUI will be

"Contact does not have support for [collab service]." where [collab service] may be file exchange, whiteboard, application sharing, etc.

100.4.3.7 PC Client Control of Etherset Service

A new service parm called "PC ClientSet Control " is defined as part of the new service "Allowed Clients" . Interaction with the Nortel i200x phone is exposed for use by the subscriber using the Multimedia PC Client as provisioned parameters of the "Allowed Clients" Service.

If the user's service package does not contain the "PC ClientSet Control " parm then the i200x interaction functionality on the Multimedia PC Client is disabled as described in the following subsections.

100.4.3.7.1 Main UI

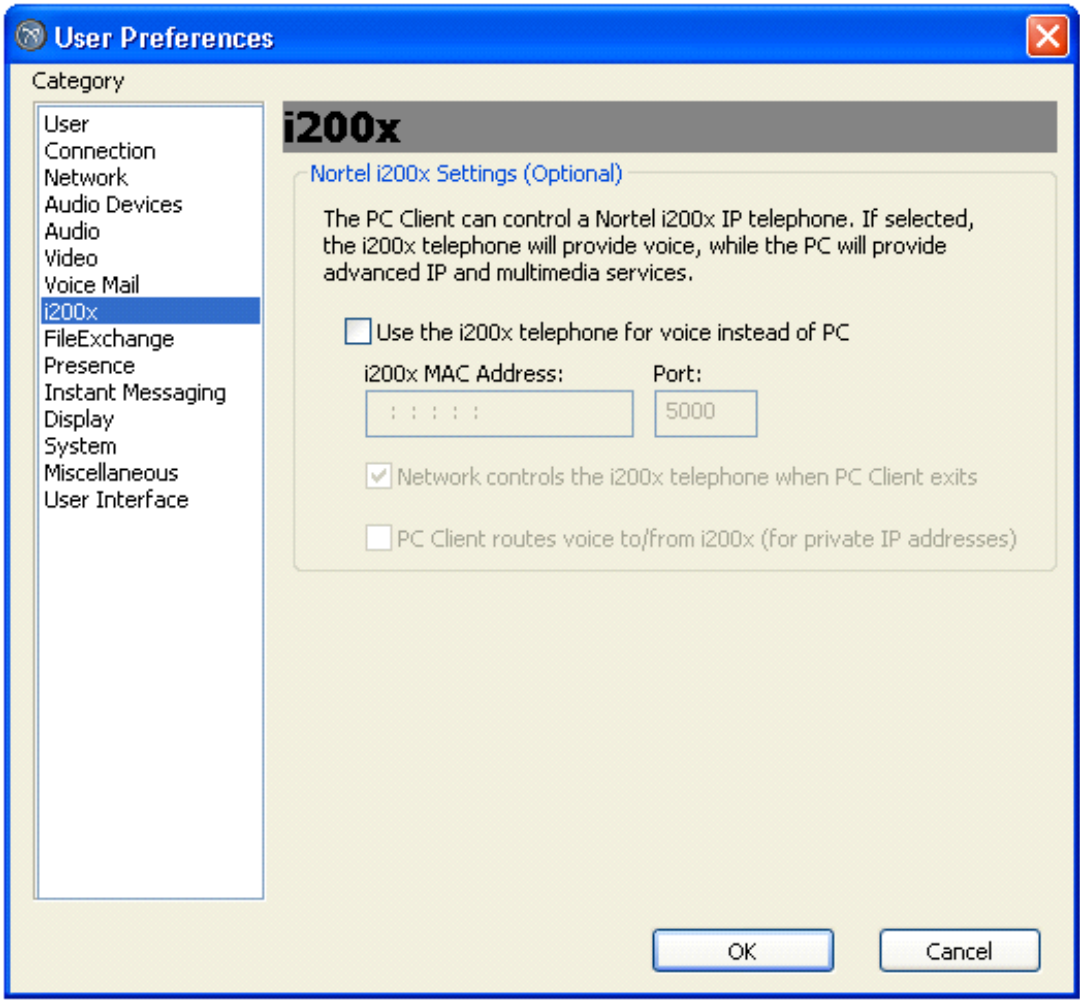
The changes on the main UI will consist in the removal of the i200x button.

Figure 39 i200x button is removed from main window

100.4.3.7.2 Preferences

The "i200x" tab will not be included on the Preferences Panel.

Figure 40 i200x page is removed



100.4.3.8 Special Cases

100.4.3.8.1 Services Disabled by Default

When the user is not logged in, any service whose availability depends on the service is assumed to be unavailable and therefore hidden in the UI and disabled at the network level. Therefore, when the user is logged out of the PC Client, the IM and Sharing services will not be visible or functional. Only when the user has logged in and retrieved the service package will the enabled services activate.

Note: Default behavior will be just like Assistant Console feature, which does not appear by default but pops up when the service package is downloaded with the Boss/Secretary service enabled.

100.4.3.8.2 Dynamic Change of Service Package

If a user is logged in and suddenly receives a new service package which disables one of the granular services, all activity related to the service will be stopped and all UI disabled and hidden except for the following:

- In the case of an IM session in progress, the send button will be disabled and no further IMs can be sent or received. The IM panel remains open until the user closes it, allowing the user to save the IM conservation. No new IM panels can be opened.

Figure 41 IM Send Button Disabled

- Any collaborations in progress (file transfers, whiteboard session, etc.) will be allowed to finish, but no new collaborations can begin.

Figure 42 Collaborations in Progress

If PCClientSet Control service parm is lost, the i200x phone will continue to be controlled by the soft client until the connection is lost or the client is restarted.

100.4.3.8.3 Additional Client Behavior

- It is possible to still display a disabled UI control that would normally be hidden when a service is not available. This is done by setting the control's "collapsetype" property in the XML skin to "none". For example, in the main window's main.xml skin, set the IM button (mainWindowInstantMessaging component) property collapsetype=none. When the main window is loaded and IM is not an available service, the IM button will be visible but disabled.
- Systray menu options "Start Sharing...", "Start Send File..." and "Send Instant Message..." will be disabled and hidden if corresponding services are not available in the service package.
- IM and Collab buttons must collapse not only in the regular In Session window but also the Converged Desktop In Session window.

100.4.3.9 Personal Agent Enhancements

100.4.3.9.1 Instant Messaging Service

This service affects the Routes functionality of the Advanced Screening service in the following way:

- If a user does have the Instant Messaging service then the user will be able to send/receive any instant messages. Therefore the routes wizard will display the option for handling instant messages in the ‘Step 1. Initiate action’ screen.

As part of this feature, the routes wizard will be modified to display the Instant Messaging option only when the user’s service package contains the ‘Instant Messaging’ service.

The two variations of the screens are displayed as below.

Figure 43 Instant Messaging Present

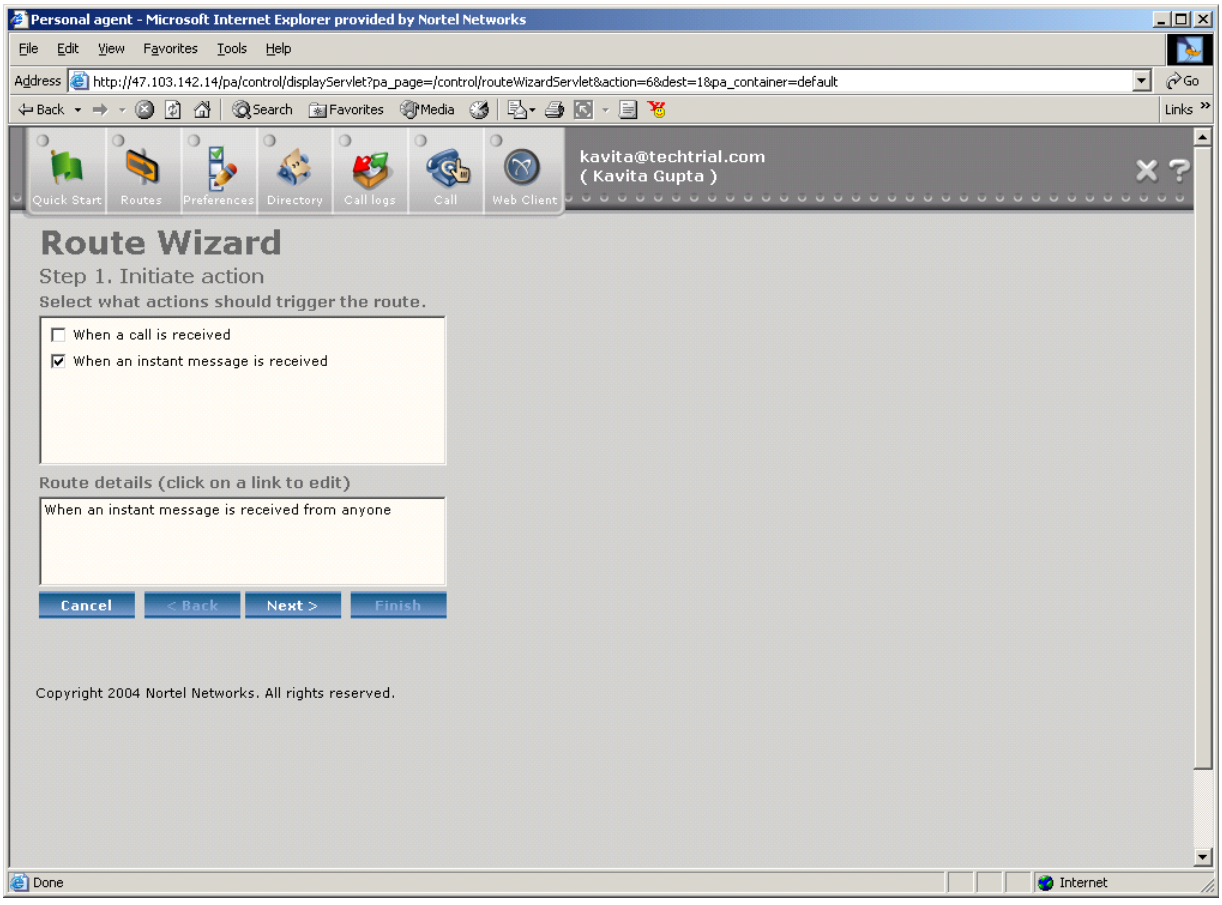
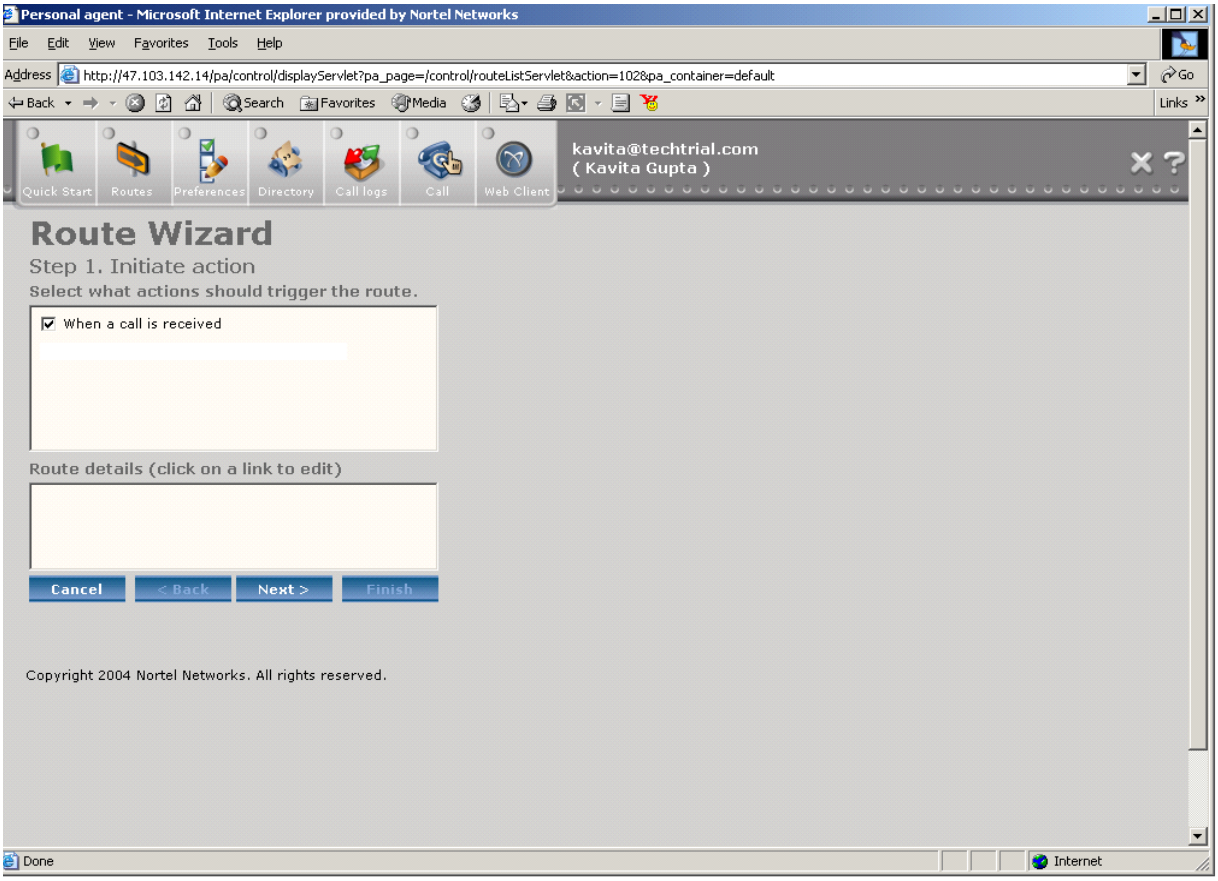


Figure 44 Instant Messaging Absent



100.5 Dependencies

Not Applicable

100.5.1 Hardware Dependencies

Not Applicable

100.5.2 Software Dependencies

Not Applicable

100.5.2.1 Nortel Networks Software Dependencies

This feature impacts the Personal Agent and Provisioning Client software as decribed in earlier sections.

100.5.2.1.1 Service Interactions

The following chart displays the effect of the feature (if any) on the other Service Package Services that are part of Release 4.1.

Table 1 Service Interactions

Service Name	Dependency/ Interaction
Ad Hoc Conferencing	None
Advanced Addressbook	None
Advanced Screening	See section “Personal Agent Enhancements”
Allowed Clients/PCClientSet Control	Mutually Exclusive relation with the CS2000 Sip Lines Service
Assistant Console	None
Assistant Support	None
Call Park	None
Call Waiting Disable	None
Calling Line ID Restriction	None
Client Collaboration	None
Converged Desktop	None
Device Access Restrictions	None
Hot Line	None
Instant Messaging	None
IM Chatroom	Dependent on Instant Messaging.See section “Instant Messaging Service”
Meet Me Conferencing	None
Mobility Client	None
Music On Hold	None
Net6 Support on 2004	None
Network Call Logs	None
Presence	See sections “Error! Reference source not found. Error! Reference source not found.” “Error! Reference source not found. Error! Reference source not found.”

Table 1 Service Interactions

Service Name	Dependency/ Interaction
QoS	None
SMS Interworking	None
Unified Communications	None
Video	None

100.5.2.2 Non Nortel Networks Software Dependencies
Not Applicable

100.5.3 1.1.2Network Component Dependencies
Not Applicable

100.5.3.1 1.1.2.1Nortel Networks Components
Not Applicable

100.5.3.2 1.1.2.2Non Nortel Networks Components
Not Applicable

100.6 Accounting

100.6.1 IPDR (Internet Protocol Detail Record)
Not Applicable.

100.7 Faults
Not Applicable.

100.7.1 Fault Management Strategy
Not Applicable.

100.7.2 Fault Management Tools and Utilities
Not Applicable.

100.7.3 Logs and Alarms

100.7.3.1 Change Log for User Service Package changes
Provisioning audit logs will be generated for user service package changes by the provisioning administrator's. The logs will have the following information.

a. The IP Address of the machine from which the operation was performed:

b. The admin name who is performing the operation

c. The command performed

d. Description

Here is the sample log for a user's service package change from package "silver" to "gold". In addition to the above information, the log will have the new service package name. The method name present in the log is "modifyExtendedUser", since that is the method used to perform the service package change.

PROV1_0 PROVC 606 INFO JAN05 12:17:06:207 MCP_4.0.0

RequestType:ProvClient, Username:admin, Command:Modify a single extended user (modifyExtendedUser) , IP Address:47.102.112.151, Comments: User name=[n1@nortel.com], User=[username:n1@nortel.com&firstname:n1&lastname:n1&servicepackage:gold]

Here is the sample log for the customization of a user's service package.In this case, the user's Presence and Unified Communications service preferences are being modified by the admin.

PROV1_0 PROVC 606 INFO JAN05 12:17:06:207 MCP_4.0.0

RequestType:ProvClient, Username:admin Command:Modify all preferences for a user (modifyAllUserPreferences), IP Address:47.102.112.151, Comments: User name=[n1@nortel.com], Service List=ListSize:2,ListContents[name:Presence,parms:(name:Report when inactive,value:N),(name:Report when on the phone,value:Y)&name:Unified Communications,parms:(name:Maximum Storage (in minutes),value:20),(name:Maximum Message Length (in seconds),value:180),(name:Maximum Number of Messages,value:50)]

100.8 Performance Management

Not Applicable.

100.8.1 Performance Management Strategy

Not Applicable.

100.8.2 Performance Management Tools and Utilities

Not Applicable.

100.8.3 Performance Measurements (PM), Operational Measurements (OM), and Stats

Not Applicable.

100.9 Upgrade

Since these services were part of the basic services that were supported by the clients in the previous releases (i.e. 3.0 ,2.0 ,1.1 etc), when the system is upgraded to 4.1/9.0, all the existing servicepackage's will be given the above set of services. This will enable the users to use these services when the system is upgraded to 9.0.

Also, since this functionality is implemented only on the clients, the customer has to update the clients used by the end-users to limit the availability of these new services to the end- users.

100.10 Restrictions and Limitations

- If a user's service package changes dynamically and a service that was enabled is suddenly disabled (such as IM), that service will be immediately disabled in the PCClient and will not be available for the user to use.
- The service Client Collaboration is used to define if the user can receive any collaboration requests. The individual service parms will define if the user can initiate any collab requests.
- PA behavior on Service Package changes. If a user who has the IM service is logged into the PA session and is creating routes and at the same time if his service package has been changed to remove the IM service, then the user will still be able to see the IM routing options but will not be able to save any routes or make any routes active which have the IM routing options in them. The user will not be able to see the IM options the next time he logs into the PA session. Same with the Send WebPage options. This is consistent with the current behavior in PA for other services.
- If a user has MeetMe service and no IM service, then he will not be getting MeetMe chair IM notifications.
- If a user has WebCollab and does not have the Client Collaboration service webpush parm, then web collaboration will not work.
- The enforcement for the availability of these services is done only at the client level
- UI components related to services which are not available will be hidden. Other visible UI components on the same dialog will not necessarily be re-centered to make up for excess space left by the hidden components.
- This feature does not have any impact or relation to the wireless communicator project.
- The wireless client will not be modified to enforce these new service restrictions.

100.11 References

[1] J. Rosenberg et al, SIP: Session Initiation Protocol, RFC 3261, IETF; June 2002

[2] B. Campbell, A. Niemi, S. Olson, J. Peterson, J. Rosenberg, B. Stucker, An Event State Publication Extension to the Session Initiation Protocol (SIP), draft-ietf-sip-publish-04, IETF; May, 2004.

[3] H. Sugano, S. Fujimoto, G. Klyne, A. Bateman, W. Carr, J. Peterson, Presence Information Data Format (PIDF), draft-ietf-impp-cpim-pidf-08, IETF; May 2003 (Expired).

[4] Brian Stucker, MCP 4.0 SIP Enhancements – State Publication Functional Description, June 4, 2004

101: Functional Description (FN): A00009829

101.1 Feature name and Feature ID

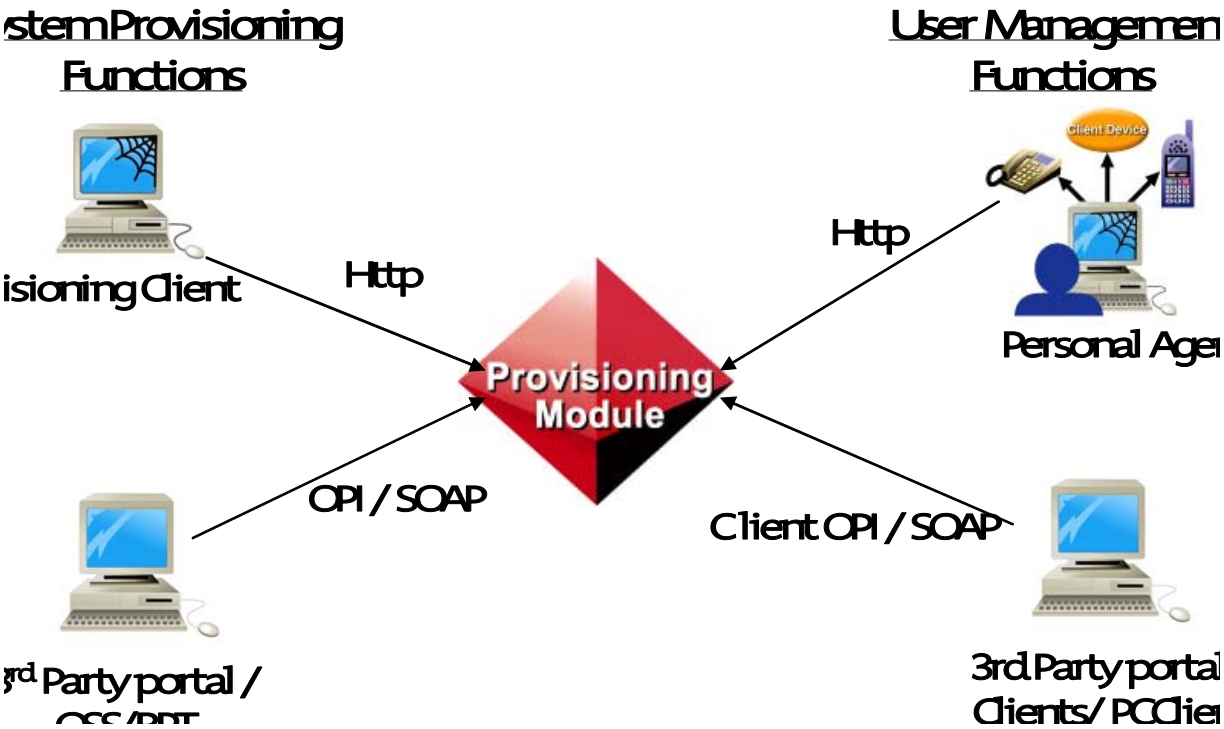
A00009829 - Subscriber Open Provisioning Interface Productization

101.2 Description

As of release MCS4.0, all the user management functions were performed via the provisioning interfaces like the Provisioning Client, Bulk Provisioning Tool(BPT) and/or the Open Provisioning Interface (OPI) and was limited to the provisioning administrators. The only interface available for the end users to manage their account was the Personal Agent (PA). Although, a small set of user related operations are available in the existing Client OPI interface, this is used only by the PCClient. However, this interface was never published for third party use like the provisioning OPI. This has given way to the Subscriber OPI (SOPI). The new interface will be an enhanced and extended version of the existing client OPI and will include all the options available in Personal Agent and PCClient for the end users to manage their accounts. Access to this functionality will be enforced by the service package framework via a new service that will be introduced. User credentials are used for authentication.

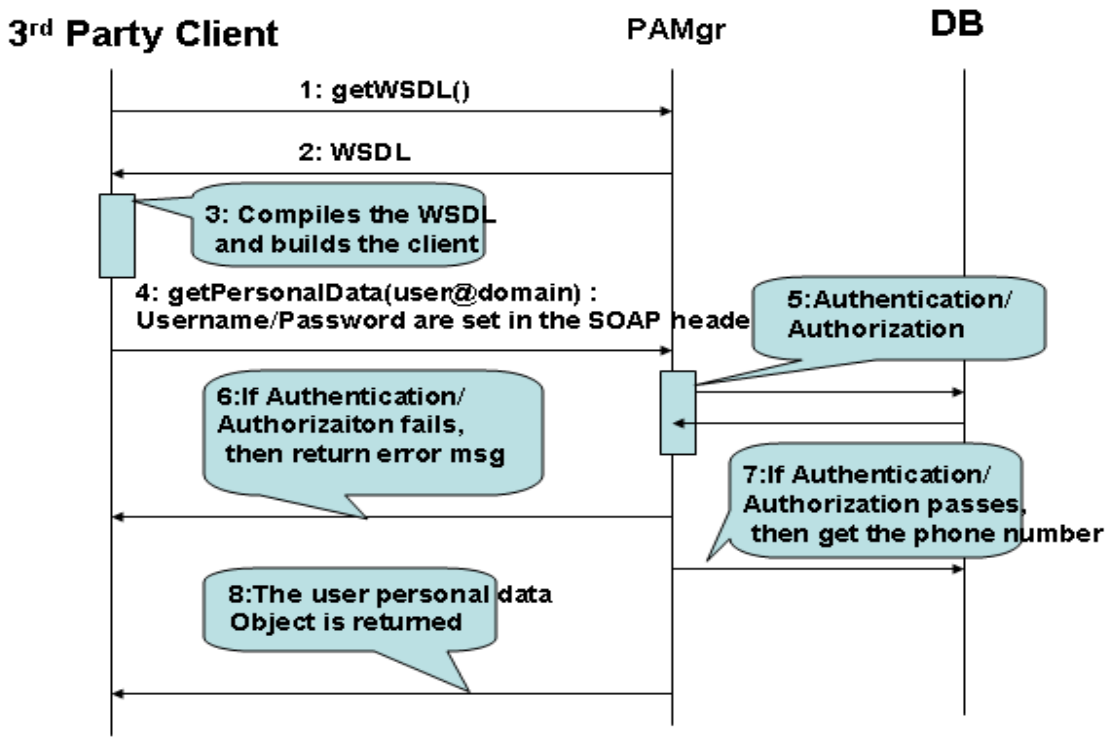
Some of the advantages of Subscriber OPI are as follows:

- Web-Service based API, providing an option for the customers to build their own clients and custom web portals for the end user to manage his account thereby giving the end users a different look and feel.
- This interface can be used to add MCS user management functions into an already existing customer client or web portal thereby removing the need for the end user to learn and use a new application to manage his account.
- The benefits of the current existing Provisioning OPI can all be applied to this interface.



101.2.1 Subscriber OPI Request Flow

The following diagram explains the message flow between a third party client built using Subscriber OPI and the MCS PAMgr. The first two operations are needed only when the third party client is built the first time and when there is a interface change between releases. The rest of the actions take place for every subscriber OPI request.



Steps :

1. Get the latest WSDL document from the PAMgr for the area for which the client is being built. In this case get the UserPersonalData web service WSDL.
2. Generate the client's stubs from the WSDL document. The client stubs have to be compiled before they can be used to access the interface. The detailed steps involved in building a client using the SOPI interface is out of the scope of this document
3. Build the SOAP request by setting the username/password and version number in the header. Get the service locator for the required service and call the method. In this case call the getPersonalData(user@domain).
4. The request comes to the PAMgr/UserPersonalData web service. The respective authentication handler performs the authentication by getting the username and password information from the SOAP message. After successful authentication, the request is forwarded to the respective web service where the authorization check is performed.
5. If authentication or authorization fails, then an error message is returned to the client. The failed attempt is logged.

6. If authentication and authorization passess, then the data is obtained from the DB.
7. The requested information is returned to the client. In this case the user personal data object is returned.

101.2.2 Authentication

The difference between OPI and Subscriber OPI is the authentication process. OPI is used by the provisioning administrator's and credentials of the respective administrator are needed for authentication. Whereas in Subscriber OPI, user credentials i.e. username and password of the user who is using the client built using the Subscriber OPI are needed for authentication.

101.2.3 Authorization

The access to this functionality will be controlled by the new "Subscriber OPI" service that will be introduced as part of this feature. If this service is present in the user's service packages, then the Subscriber OPI requests coming from this user will be allowed to go through. In addition to this service, additional restrictions will be in place to limit the availability of the sub-areas to the users. For ex. if the service "Advanced

In addition to the service enforcement, the subscriber OPI requests coming from users who are inactive i.e. if their status/statusreason is set to "INACTIVE

101.2.4 2.2.4User Operations and Methods

The Subscriber Open Provisioning Interface will have all the operations that are available for the user in PA and PCClient. The user operations are grouped as follows:

- User Personal Information
- User Time Block Groups
- Personalized Call Settings
- Address Book and Search
- Call Screening and Routes
- Service Preferences
- MeetMe Service Data
- Unified Communications Service Data
- Call Logs

The SOPI is a set of different web services, with each web service dealing with a different area of the user operations. Each of the above will be its own web service and will have its own WSDL. This means that if a client wants to access the address book methods then the corresponding addressbook WSDL

has to be used to generate the stubs. This provides maintainability, extensibility and granularity of functionality which can be used to license these services later.

101.2.4.1 User Personal Information

This interface has the methods which can be used to access and manage the user's personal information like email, office phone number, home phone number, etc. These methods will be available for all the user's and are not service package controlled. The UserPesonalData object will have the username, aliases, first name , last name, email, business phone number, home phone number, cell phone number, pager, fax, timezone and locale information. There will be a restriction on the server side which will prevent the modification of username and alias information. First and last names can be modified through this interface. Even though, first and last names can be modified, both of them cannot be null. One of them should be present as it will be used by the IPCM feature to generate the display name. There are certain fields of the user personal data which are synced through the LDAP server. The list of fields that are synced by the LDAP server is provisioned at the domain level. Currently, PA restricts the ability to modify these fields. To maintain the same behavior, there will be a method which will return the fields that are synched by the LDAP server for a user which will enable the clients to make these fields as read only. There will also be a check on the server side which will prevent the modification of these fields through SOPI.

Provisionable Entity: UserPersonalData

WebService Name: PersData

Required ServicePackage Service : None

Method Summary

void	**authenticateUser**(java.lang.String userName, java.lang.String password) This method is used to authenticate the user.
void	**changePassword**(java.lang.String userName, java.lang.String oldPassword, java.lang.String newPassword) This method is used to change the user password.
void	**getUserPersonalData**(java.lang.String userName) This method is used to get the user personal information.
void	**modifyUserPersonalData**(java.lang.String userName, com.nortelnetworks.ims.base.prov.opi.shared.user.UserPersonalData upd) This method is used to modify the user personal information.

User Personal Data	
PEMgr	**UserPersonalDataMgr**
PE	**UserPersonalData**
Method	**Description**
addUserPersonalData	To add the user personal information like email,office phone, home phone etc.
modifyUserPersonalData	To modify the user personal information like email,office phone, home phone etc.
removeUserPersonalData	To remove the user personal information like email,office phone, home phone etc.
getUserPersonalData	To get the user personal information like email,office phone, home phone etc.
Password	
authenticateUser	To authenticate the user
changePassword	To change the user password

101.2.4.2 2.2.4.2TimeZones

Provisionable Entity: TimeZone

WebService Name: TimeZone

Required ServicePackage Service : None

Method Summary	
TimeZone[]	**getAllTimeZones**() Returns all the TimeZones existing in the System

101.2.4.3 Locales

Provisionable Entity: LocaleData

WebService Name: Locale

Required ServicePackage Service : None

Method Summary	
LocaleData[]	**getSystemLocalesList**() Returns all the Locales existing in the System

101.2.4.4 Password Policy

Provisionable Entity: NONE

WebService Name: UserPwd

Required ServicePackage Service : None

Method Summary	
java.lang.String	**getPasswordPolicyDescription**(java.lang.String userName) This method is used to get the password policy description for the user's domain.

101.2.4.5 E911 Location List

Provisionable Entity: LocList

WebService Name: E911Loc

Required ServicePackage Service : None

Method Summary	
LocList	**getLocationList**(long timestamp, boolean forceDownload, java.lang.String domainName) This method is used to retrieve the location list for a particular domain to send to a client.

101.2.4.6 UserPicture

Provisionable Entity: UserPicture

WebService Name: Picture

Required ServicePackage Service : None

This interface has the user picture methods.

Method Summary	
void	**addUserPicture**(java.lang.String userName, UserPicture picture) This method is used to add a picture that is associated with the userName that is passed in
UserPicture	**getUserPicture**(java.lang.String userName) This method is used to retrieve the picture associated with the userName that is passed in
void	**modifyUserPicture**(java.lang.String userName, UserPicture picture) This method is used to modify the picture associated with the userName that is passed in
void	**removeUserPicture**(java.lang.String userName) This method is used to remove the picture associated with the userName that is passed in

101.2.4.7 2.2.4.7User TimeBlocks

This interface has the methods which can be used to access and manage the user's time block groups. These methods will be available for all the user's and are not service package controlled. These time blocks are used by the advanced screening and routing functionality and will only be useful if the user has the "Advanced Screening" service.

Provisionable Entity: TimeBlockGroup

WebService Name: TimeBlock

Required ServicePackage Service : None

Method Summary	
void	**addTimeBlockGroup**(java.lang.String userName, TimeBlockGroup timeBlockGrp) This method is used to create a new TimeBlockGroup with the information provided for the user with username given
void	**addTimeBlockGroups**(java.lang.String userName, TimeBlockGroup[] timeBlockGrps) This method is used to create a new TimeBlockGroup with the information provided for the user with username given

TimeBlockGroup	**getTimeBlockGroupByName**(java.lang.String userName, java.lang.String timeBlockGrpName) This method is used to get the TimeBlockGroup for a user specified by the name provided
TimeBlockGroup[]	**getTimeBlockGroupsByUser**(java.lang.String userName) This method is used to get the TimeBlockGroups for a user
void	**modifyTimeBlockGroup**(java.lang.String userName, java.lang.String timeBlockGrpName, TimeBlockGroup timeBlockGroup) This method is used to modify the timeblock group with the parameters given
void	**removeTimeBlockGroup**(java.lang.String userName, java.lang.String timeBlockGrpName) This method is used to delete a TimeBlockGroup idenfied by the name provided for the user whose name is given
void	**removeTimeBlockGroups**(java.lang.String userName) This method is used to delete all the timeblock groups associated to the user whose user name is given

101.2.4.8 Personalized Call Settings

This interface has the methods which can be used to access and manage the user's personalized call notes like subjects, reasons, and personalized presence notes. These methods will be available for all the user's and are not service package controlled.

Provisionable Entity: UserData

WebService Name: UserData

Required ServicePackage Service : None

Method Summary	
java.lang.String[]	**getNotesByUserName**(java.lang.String userName) This method is used to retrieve the list of notes associated to the user whose username is being passed in
java.lang.String[]	**getRejectReasonsByUserName**(java.lang.String userName) This method is used to retrieve the list of reasons associated to the user whose username is being passed in
java.lang.String[]	**getSubjectsByUserName**(java.lang.String userName) This method is used to retrieve the list of subjects associated to the user whose username is being passed in

UserData	**getUserData**(java.lang.String userName) This method is used to retrieve the UserData associated to the user whose username is passed in
void	**modifyUserData**(java.lang.String userName, UserData userData) This method is used to update the UserData associated to the user whose username is given with the UserData information being passed in
void	**modifyUserNotes**(java.lang.String userName, java.lang.String[] notes) This method is used to update the notes associated to the user whose username is given with the notes list information being passed in
void	**modifyUserReasons**(java.lang.String userName, java.lang.String[] reasons) This method is used to update the reasons associated to the user whose username is given with the reasons list information being passed in
void	**modifyUserSubjects**(java.lang.String userName, java.lang.String[] subjects) This method is used to update the subjects associated to the user whose username is given with the subjects list information being passed in
void	**removeAllCallSubjects**(java.lang.String userName) This method is used to remove all the subjects associated to the user whose username is passed in
void	**removeAllRejectReasons**(java.lang.String userName) This method is used to remove all the reasons associated to the user whose username is passed in
void	**removeAllUserNotes**(java.lang.String userName) This method is used to remove all the notes associated to the user whose username is passed in
void	**removeUserData**(java.lang.String userName) method is used to remove the UserData associated to the user whose username is passed in

101.2.4.9 Address Book

This interface has the methods which can be used to access and manage the address book and directory information of a user.

Provisionable Entity: AddressBookEntry

WebService Name: AddrBook

Required ServicePackage Service : None

Note: Although no service is required for the address book methods, the number of address book entries that the user can have and the ability to have buddies is controlled by the Maximum Number of Address Book entries and the Presence service respectively.

Method Summary

void	**addAddressBookEntries**(java.lang.String userName, AddressBookEntry[] addrBookEntries) This method is used to create a new addressbook entry for the user specified
void	**addAddressBookEntry**(java.lang.String userName, AddressBookEntry addrBookEntry) This method is used to create a new addressbook entry for the user specified
AddressBookEntry[]	**getAddressBook**(java.lang.String userName) This method is used to get the addressbook for the user whose name is passed in.
AddressBookEntry	**getAddressBookEntry**(java.lang.String userName, java.lang.String nickName) This method is used to get an addressbook entry for the user whose name is passed in and identified by the nic++kname provided.The addressbook retrieved contains information on the uses buddies, banned users and groups.
FullAddressBookEntry[]	**getAddressBookWithPhoto**(java.lang.String userName)
java.lang.String[]	**getBuddies**(java.lang.String userName) This method is used to get the buddies for the user with user name userName.
FullAddressBookEntry	**getFullAddressBookEntry**(java.lang.String userName, java.lang.String nickName)
AddressBookEntry[]	**getLightWeightAddressBook**(java.lang.String userName)
void	**makeBuddy**(java.lang.String userName, java.lang.String buddyName)
void	**modifyAddressBookEntries**(java.lang.String userName, java.lang.String[] nickName, AddressBookEntry[] addrBookEntry) This method is used to update an addressbook entry for the user specified and identified by the nickname provided

void	**modifyAddressBookEntry**(java.lang.String userName, java.lang.String nickName, AddressBookEntry addrBookEntry) This method is used to update an addressbook entry for the user specified and identified by the nickname provided
void	**removeAddressBook**(java.lang.String[] userNames) This method is used to delete addressbook for the user identified by the username(s) provided
void	**removeAddressBookEntries**(java.lang.String userName, java.lang.String[] nickName) This method is used to delete multiple addressbook entry identified by the nickname provided for the user whose username is specified
void	**removeAddressBookEntry**(java.lang.String userName, java.lang.String nickName) This method is used to delete an addressbook entry identified by the nickname provided for the user whose username is specified
void	**removeBuddy**(java.lang.String userName, java.lang.String buddyName) This method is used to remove an addressbook entry identified as a buddy in this user's addressbook from the buddy list and make his a normal entry

101.2.4.10 2.2.4.10 AddressBook Groups

Provisionable Entity: None

WebService Name: AbGroup

Required ServicePackage Service : None

Method Summary

void	**addAddressBookGroup**(java.lang.String userName, java.lang.String groupName) This method is used to add a group to the user whose user name is given, the group name can be anything from Family,Friends,Work etc.
void	**addAddressBookGroups**(java.lang.String userName, java.lang.String[] groupNames)
void	**addUsersToAddressBook**(java.lang.String userName, java.lang.String[] users) This method is used to add all the users given to this user's address book.

java.lang.String[]	**getAddressBookGroups**(java.lang.String userName) This method is used to get all the groups associated to a user in his address book which are used for adding entires to his address book
void	**modifyAddressBookGroups**(java.lang.String userName, java.lang.String[] groupName) This method is used to add more groups to the user whose user name is given, the method verifies if there is a group in this list already existing, if so does not add it, but if it does not, it is added to the groups list that the user has
void	**removeAddressBookGroup**(java.lang.String userName, java.lang.String groupName) This method is used to remove an addressbook group identified by the groupname given from this user's addressbook
void	**renameAddressBookGroup**(java.lang.String userName, java.lang.String groupName, java.lang.String updatedGroupName)

101.2.4.11 Global Address Book Search

The search Global Address Book functions are included in this interface.

Provisionable Entity: `FullAddressBookEntry`

WebService Name: GABSearch

Required ServicePackage Service : None

Method Summary	
FullAddressBookEntry[]	**searchGABByFirstName**(java.lang.String userName, java.lang.String firstName) This method can be used to obtain the user's in the global address book with the passed in search criteria.
FullAddressBookEntry[]	**searchGABByLastName**(java.lang.String userName, java.lang.String lastName) This method can be used to obtain the user's in the global address book with the passed in search criteria.
FullAddressBookEntry[]	**searchGABByName**(java.lang.String userName, java.lang.String name) This method can be used to obtain the user's in the global address book with the passed in search criteria.

FullAddressBookEntry[]	**searchGABByPhoneNumber**(java.lang.String userName, java.lang.String phoneNumber) This method can be used to obtain the user's in the global address book with the passed in search criteria.
FullAddressBookEntry[]	**searchGABByUserName**(java.lang.String userName, java.lang.String searchUserName) This method can be used to obtain the user's in the global address book with the passed in search criteria.

101.2.4.12 Call Screening and Routes

This interface has the methods which can be used to access and manage the user routes information which is used to generate the CPL of a user. These methods will be controlled by the "**Advanced Screening**" service. If the user does not have this service in his service package, then he will not be able to execute these methods

Provisionable Entity: Route

WebService Name: Routes

Required ServicePackage Service : AdvancedScreening and Routing for advanced routing options. Instant Messaging for the IM Routing options. Client Collaboration/WebPush service and/or parm for the "Send WebPage" option.

Method Summary

void	**activateRoutes**(java.lang.String userName, java.lang.String[] routeNames) This method is used to set the status of the routes specified in the input list as Active.
void	**addRoute**(java.lang.String userName, Route route) This method is used to create a new RouteList with the information provided for the user with username given
void	**addRoutes**(java.lang.String userName, Route[] routes) This method is used to create a new RouteList with the information provided for the user with username given
void	**deactivateRoutes**(java.lang.String userName, java.lang.String[] routeNames) This method is used to set the status of the routes specified in the input list as Inactive.
java.lang.String[]	**getAllRouteParmNames**() This method return the valid names to be used in the parms attribute of the route.

Route	**getRoute**(java.lang.String userName, java.lang.String routeName) This method is used to get the Route with the name of the route specified and for the user identified by the username provided.
java.lang.String[]	**getRouteNames**(java.lang.String userName) This method is used to get the names of the routes for the user with the given userName
Route[]	**getRoutes**(java.lang.String userName) This method is used to get all the routes for the user with the given user name.
void	**modifyRoute**(java.lang.String userName, java.lang.String routeName, Route newRoute) This method is used to modify a Route for the user with name given with the route information provided
void	**removeAllRoutes**(java.lang.String userName) This method is used to delete all routes identified by the username of the user to whom these routes belong.
void	**removeRoute**(java.lang.String userName, java.lang.String routeName) This method is used to delete a Route identified by the route name and the username.
void	**reorderRoutes**(java.lang.String userName, java.lang.String[] routeNames) This method reorders the routes specified in the input.
void	**setActiveRoutes**(java.lang.String userName, java.lang.String[] routeNames) This method sets only the routes specified in the input to active status and resets the status of all the remaining routes (if any) to inactive.

101.2.4.13 Service Preferences

This interface has the methods which can be used to access and manage the service package information of a user. These methods will be controlled by the different services present in the user's service package. For ex. If the user does not have "Presence" in his package, then he will not be able to set the user preferences for that service. The banlist methods are controlled by the "Presence" service.

Provisionable Entity: ServicePackage, Service and DetailedService

WebService Name: UserPref

Required ServicePackage Service : None. But, the user can only access the preferences for the services present in his service package.

Method Summary	
DetailedService[]	**getAllDetailedUserPreferences**(java.lang.String userName) This method is used to obtain the user preferences for all the services that he has.
Service[]	**getAllUserPreferences**(java.lang.String userName) This method is used to obtain the user preferences for all the services that he has.
ServicePackage	**getUserServicePackage**(java.lang.String userName) This method is used to obtain the ServicePackage object to which the user belongs to.
void	**modifyAllUserPreferences**(java.lang.String userName, com.nortelnetworks.ims.base.prov.opi.shared.Service[] services) This method is used to add/modify user preferences .This method should only be used when adding/modifying the user preferences for all the services that he has.
void	**modifyUserPreferences**(java.lang.String userName, com.nortelnetworks.ims.base.prov.opi.shared.Service service) This method is used to add/modify user preferences for a specific service.
void	**removeAllUserPreferences**(java.lang.String userName) Thismethod is used to remove all the user preferences

101.2.4.14 MeetMe Service Data

This interface has the methods which can be used to access the meetme service data of a user. These methods will be controlled by the "**Meet Me Conferencing**" service. If the user does not have this service in his service package, then he will not be able to execute these methods. In addition to that if the MeetMe service(MAS) is not properly configured for the user's domain, then these methods will not be executed and an error message will be returned.

Provisionable Entity: MeetMeConfData

WebService Name: MeetMe

Required ServicePackage Service : Meet Me Conferencing.

If the MeetMe service(MAS) is not properly configured for the user's domain, then these methods will not be executed and an error message is returned.

Method Summary	
MeetMeConfData	**addMeetMeConfUser**(java.lang.String userName, MeetMeConfData meetmeConfData) This method is used to add a new MeetMe conf user.
MeetMeConfData	**getMeetMeConfData**(java.lang.String userName) This method is used to retrieve MeetMe Conf data for a particular user.
MeetMeConfData	**modifyMeetMeConfUser**(java.lang.String userName, MeetMeConfData meetmeConfData) This method is used to update an existing MeetMe conf user.
void	**removeMeetMeConfUser**(java.lang.String userName) This method is used to delete an existing MeetMe conf user from the system.

101.2.4.15 Unified Communications Service Data

This interface has the methods which can be used to access the unified communications service data of a user. These methods will be controlled by the "**Unified Communications**" service. If the user does not have this service in his service package, then he will not be able to execute these methods. In addition to that if the Unified Communications(MAS) service is not properly configured for the user's domain, then these methods will not be executed and an error message will be returned.

Provisionable Entity: UCUserData

WebService Name: UC

Required ServicePackage Service : Unified Communications

If the Unified Communications service(MAS) is not properly configured for the user's domain, then these methods will not be executed and an error message is returned.

Method Summary	
void	**addSecondaryUCAutoID**(java.lang.String userName, UCAutoIDData autoIDData) This method is used to add the auto id data for an UC user in the associated Media Application Server (MAS) database.
UCUserData	**addUCUser**(java.lang.String userName, UCUserData ucUserdata) This method is used to add the user preferences relevant to UC service in the associated Media Application Server (MAS) database.

java.lang.String	**getActiveGreeting**(java.lang.String userName) This method is used to get the active greeting for an UC user.
long	**getPasswordExpiryTime**(java.lang.String userName) This method is used to retrieve the time the user's password will expire.
UCAutoIDData	**getPrimaryUCAutoID**(java.lang.String userName) This method is used to get the auto id data for which the address is same as the sip user id of the UC user in the associated Media Application Server (MAS) database.
UCAutoIDData[]	**getSecondaryUCAutoIDs**(java.lang.String userName) This method is used to get the secondary auto id data for an UC user in the associated Media Application Server (MAS) database.
long	**getTemporaryGreetingExpiryTime**(java.lang.String userNam e) This method is used to retrieve the time the temporary greeting will expire.
UCGreetingData[]	**getUCGreetings**(java.lang.String userName) This method is used to get the greetings data for an UC user in the associated Media Application Server (MAS) database.
UCUserData	**getUCUser**(java.lang.String userName) This method is used to retrieve the preferences for an UC user from the associated Media Application Server (MAS) database.
java.lang.String[]	**getValidAccountStatus**() This method returns all the valid strings representing account status .
java.lang.String[]	**getValidAutoReadValues**() This method returns all the valid values for the auto read field (UCUserData)
java.lang.String[]	**getValidEmailAttachmentTypes**() This method returns all the valid email attachment types.
java.lang.String[]	**getValidGreetingKeys**() This method returns all the valid greeting keys that are used to construct the greeting data.
java.lang.String[]	**getValidGreetingNames**() This method returns all the valid greeting names.
java.lang.String[]	**getValidPrimaryAutoLoginValues**() This method returns all the valid values for the auto login field (UCAutoIDData)
java.lang.String[]	**getValidSecondaryAutoLoginValues**() This method returns all the valid values for the auto login field (UCAutoIDData)
void	**modifySecondaryUCAutoID**(java.lang.String userName, UCAutoIDData autoIDData) This method is used to modify the secondary auto id data for an UC user in the associated Media Application Server (MAS) database.

UCUserData	**modifyUCUser**(java.lang.String userName, UCUserData data) This method is used to update the preferences relevant to UC service in the associated Media Application Server (MAS) database.
void	**removeSecondaryUCAutoID**(java.lang.String userName, java.lang.String autoIDAddress) This method is used to remove the secondary auto id data for an UC user in the associated Media Application Server (MAS) database.
void	**removeUCUser**(java.lang.String userName) This method is used to delete the preferences for an UC user from the associated Media Application Server (MAS) database.
void	**setActiveGreeting**(java.lang.String userName, java.lang.String greetingName) This method is used to mark a greeting as active for an UC user in the associated Media Application Server (MAS) database.
void	**setPrimaryUCAutoID**(java.lang.String userName, UCAutoIDData autoIDData) This method is used to add the primary sip user id as the auto id address for an UC user in the associated Media Application Server (MAS) database.
void	**setTemporaryGreeting**(java.lang.String userName, long timeExpires) This method is used to set the expiry time interval for a temporary greeting for an UC user in the associated Media Application Server (MAS) database.
void	**setUCGreeting**(java.lang.String userName, UCGreetingData greetingData) This method is used to update/add a greeting data for an UC user in the associated Media Application Server (MAS) database.

101.2.4.16 Call Logs

This interface has the methods which can be used to access the call log information of a user. These methods will be controlled by the "**Network Call Logs**" service. If the user does not have this service in his service package, then he will not be able to execute these methods.

Provisionable Entity: CallLog

WebService Name: CallLog

Required ServicePackage Service : NetworkCall Logs

Method Summary

void	**deleteCallLogs**(java.lang.String username, java.lang.String[] callIds)
CallLog[]	**getCallLogs**(java.lang.String username)
CallLog[]	**getIncomingCallLogs**(java.lang.String username)
CallLog[]	**getOutgoingCallLogs**(java.lang.String username)

101.2.4.17 Banned Users

Provisionable Entity: None

WebService Name: BanUser

Required ServicePackage Service : None

Method Summary	
void	**addBannedUser**(java.lang.String userName, java.lang.String bannedUserName)
void	**addBannedUsers**(java.lang.String userName, java.lang.String[] bannedUserNames)
java.lang.String[]	**getBannedUsers**(java.lang.String userName) This method is used to get all the users banned from subscribing to this user's presence information from the ban list in the addressbook.
void	**modifyBannedUser**(java.lang.String userName, java.lang.String bannedUserName) This method is used to add a user to the ban list of a user's addressbook which would prevent the banned user from subscribing to this user's presence information
void	**removeAllBannedUsers**(java.lang.String userName) This method is used to remove all users banned from subscribing to this user's presence information from the ban list in the addressbook.
void	**removeBannedUser**(java.lang.String userName, java.lang.String bannedUserName)

101.2.4.18 AssistantUser Mgr

Provisionable Entity: None

WebService Name: AssUser

Required ServicePackage Service : Assistant Console

Method Summary	
java.lang.String[]	**getAssistedUsers**(java.lang.String userName)

101.2.4.19 ClickToCall

Provisionable Entity: None

WebService Name: CTCall

Required ServicePackage Service : None

Method Summary	
void	**clickToCall**(java.lang.String userName, java.lang.String password, java.lang.String ctcFromParty, java.lang.String ctcToParty)

101.2.4.20 I200x

Provisionable Entity: None

WebService Name: i200x

Required ServicePackage Service : None

Method Summary	
void	**logoutUserFromDevice**(java.lang.String userName, java.lang.String Macaddress)

101.2.4.21 SOPI Version

Provisionable Entity: None

WebService Name: SOPIVersion

Required ServicePackage Service : None

Method Summary	
java.lang.String	**getCurrentSOPIVersion**()
java.lang.String[]	**getSupportedSOPIVersions**()

101.2.5 Logging of Subscriber OPI requests

All failed authentication and authorization subscriber OPI requests will be logged.

101.2.6 Release Information

Since this is the first official release for this interface, all the existing user management functions available in PA and PCClient will be included in the MCS4.1 Subscriber OPI specification. Any new functionality or methods introduced by any other features in this release have to be included in this interface as part of the respective feature work. The subscriber OPI will be forward compatible with the PAmgr for one official release. This means that the MCS 4.1/09 subscriber OPI will be supported by the MCS 10 PAmgr, if 10 is our next official release.

101.2.7 Deploy Information

A new WAR called Subscriber OPI or SOPI will be created to place these new web services. This war will be packaged as part of the PA network element and will be deployed as part of the PAMgr. Since PROV mgr is a super set of all these web services, when PROV is deployed, PA is also deployed and is installed on a different virtual server. Please refer to FTR460 for more information on this.

101.3 Hardware Requirements or Dependencies

None

101.4 Software Requirements or Dependencies

None.

101.5 Limitations and restrictions

Password Change from Subscriber OPI. If a user changes his password from this interface, the change will be immediate and the subsequent requests should include the new password in the header. This is different from the behavior in PA wherein the new password takes effect when the user log's in the next time.

101.6 Interactions

- The existing ClientOPI interface will be supported in two forward releases starting from 4.1/09. For ex. if 10.0 and 11.0 are the next two releases after 4.1/09, the client OPI interface will be deprecated in this release and will be removed in 11.0. The client OPI has to be supported in 10.0 for backward compatibility issues with 4.1/09 PCClient. This would also mean that the PCClient which is currently using the client OPI interface will have to be changed in 10.0 to use the new SOPI interface.
- Refer to FTR460 for information regarding the SSL support for these web services.
- Watchers list methods are not supported by this interface.

101.7 Glossary

Term	Description
Subscriber OPI	Subscriber Open Provisioning Interface
WSDL	Web Services Description Language
WAR	Web Application Archive
CPL	Call Processing Language

102: Functional Description (FN): A00009830

102.1 Feature name and Feature ID

A00009830 - Complete Re-IP Support

102.2 Background

The requirement for this feature stems from two distinct needs in the MCP marketplace. First, since the install of the system is a lengthy and time consuming process there is a need to shorten the “order to delivery” time in order to make our supply chain more responsive to orders that it receives. To do this the concept of pre-staging of software is used. Pre-staging allows software to be completely installed on the system prior to receiving a customer order. Once an order is placed, the customer specific addressing is added and the system can then be shipped. This feature does not change the overall time to install and deliver a system, but it does reduce the time period from “order to delivery”.

Pre-Staging software is defined as the ability to assemble and load the product before customer specific information is received. This is differentiated from staging of software because it is done with generic customer information, where as staging is typically done once the order is received and the specific customer information can be used in the staging process.

The second need for this feature stems from the fact that customer networks are an ever changing entity. In order to provide the best support/customer service to our customer base, the ability to adapt to these network changes is important. This feature allows the changing of IP addresses to accommodate network topology changes without requiring a reload or redeploy of the MCP product.

102.3 Overview

This feature enables the ability to change various server identification parameters, such as country, time-zone, and IP address, while maintaining the implemented system OS hardening aspects. This feature does not require re-loading software from CD.

In addition this feature provides a central place in the management GUI to change the IP address for MCS software components that are deployed on a box that is Re-IPed. It will not be required to undeploy or re-deploy the MCS software when changing the box IP address.

This feature also provides a mechanism for all the provisioning data on the Provisioning Client to be changed automatically when a particular box is Re-IPed.

This feature is not a procedure to migrate MCP software to a different server nor is it a procedure to add or remove servers to the network. Any topology change to the network is not covered by this feature, other than Re-IP of servers.

102.4 Feature Description

The Re-IP feature can be divided into two distinct logical functions.

1. Re-IP of MCS servers.
2. Re-IP of MCS software components.

102.4.1 Re-IP of MCS Server

The MCS components run on servers with several different operating systems:

1. The core services run on the Sun Solaris and the Linux OS. This includes the System Manager, Accounting Manager, IP Client Manager, Database, Provisioning Manager and Session Manager. This feature will enable the Re-IP of these servers.
2. The RTP Media Portal runs on Red Hat Linux OS. This feature will enable the Re-IP of these servers.
3. The Media Servers and UAS PRI Gateway run on the Windows 2000 OS. These servers are not managed by the System Manager and are not Re-IPed under this feature.
4. Re-IP of third party servers is not a part of this feature.

Servers supported by this feature will be Re-IPed using an OS specific script which is required to run on each of the servers being Re-IPed. All MCS software components running on the server should be stopped before starting the Re-IP process.

All data to be changed will be required at the beginning of the script and can be provided interactively or via a file. A confirmation message will be displayed at the end for the user to accept or reject the changes and the user has the option to back out at this time and no changes will be done.

If the user chooses to proceed, the script will run and the machine will be Re-IPed. After the script has completed, the server will require a reboot.

102.4.1.1 Re-IP Sun Solaris System

This feature enables the ability to change the Sun Solaris country and timezone parameters and all IP addresses. It will maintain the implemented system OS hardening aspects. This feature does not require re-loading software from CD.

102.4.1.2 Re-IP Linux System

This feature enables the ability to change the country and timezone parameters and all IP addresses on Linux servers for core components and RTP Media Portal. It will maintain the implemented system OS hardening aspects. This feature does not require re-loading software from CD.

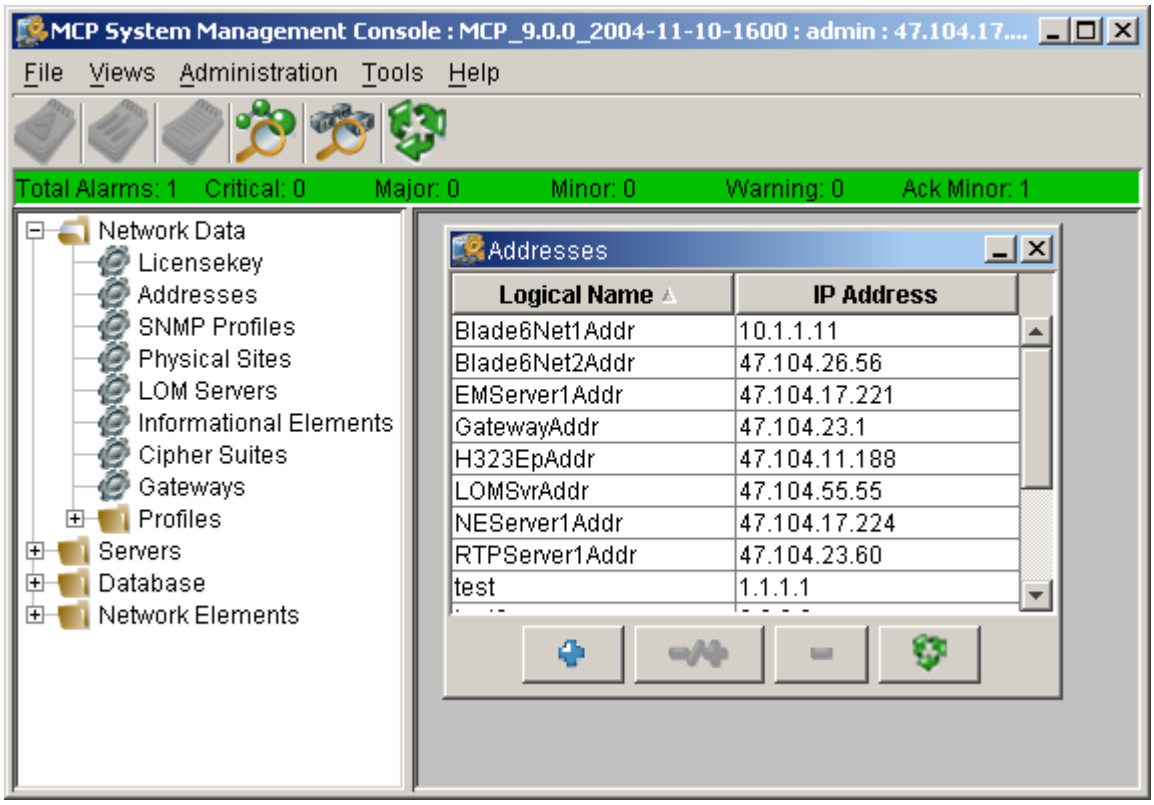
102.4.2 Re-IP of MCS Software Components

The MCP software components can be divided into three broad categories based on their interactions with the System Manager:

1. Managed: The System Manager manages the core components of the MCS solution, such as the Accounting Manager, IP Client Manager, Database, Provisioning Manager and Session Manager.
2. Monitored: Some components may not be deployed by the System Manager but may just be monitored. These components may or may not be running on a server where Re-IP is supported.
3. Informational: Some components are neither managed nor monitored by the System Manager. The System Manager is just aware of the IP address of these components.

This feature provides an Address Table (refer to Figure 1) which is a central location in the System Manager for all IP addresses in the network. Any software component that falls outside the scope of Managed, Monitored, or Informational will not be listed in the Address Table and is not covered by this feature. A System Administrator with sufficient privileges can add, edit, or delete entries in the Address Table via a script or the System Manager GUI.

Figure 1: Address Table



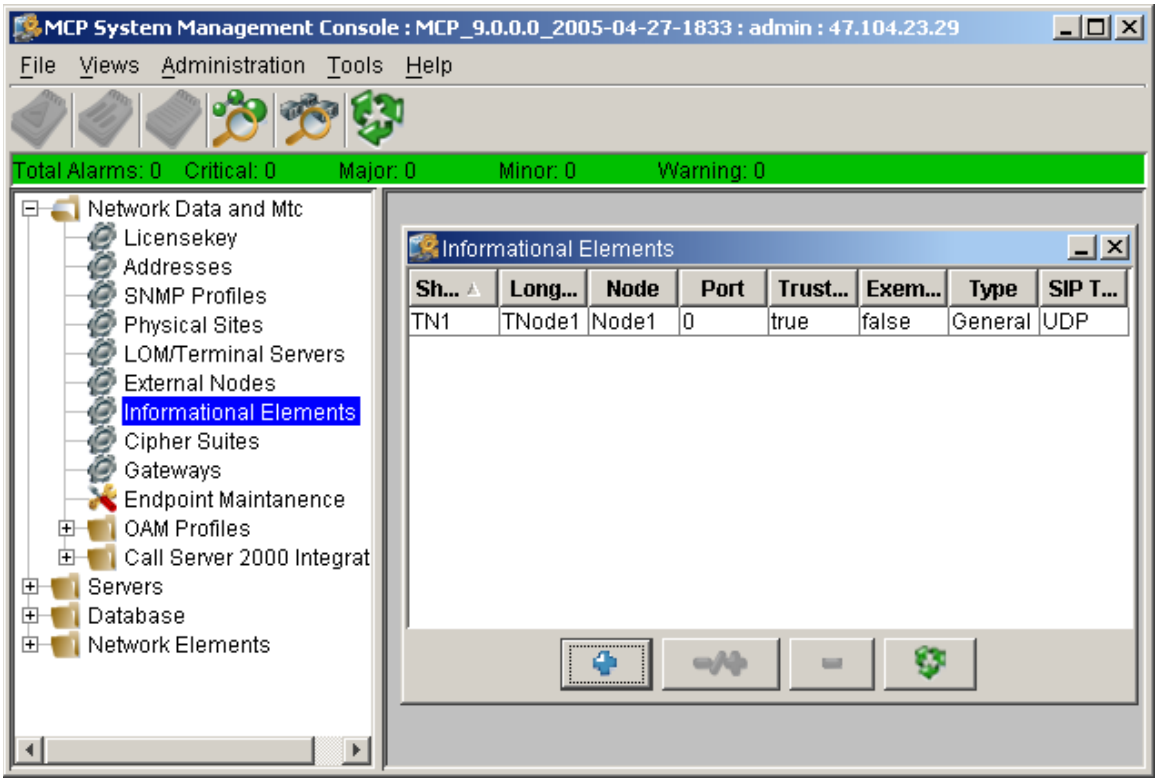
When adding, editing, or deleting an IP address, a confirmation message is displayed before the settings are applied to the system. The address change is then applied to all MCS components managed by the System Manager.

The existing Third Party Trusted Devices configuration service is being changed to provide type information.The new service is called Informational Element service (refer to Figure 2). The provisioning system will use this configuration service for Gateway, Terminal Server, Pooled Entity and LDAP provisioning. The following OMI methods are added for adding, updating, deleting and getting the list of informational elements:

- public RuntimeResult addInfoElement(InfoElementData ieData) throws RemoteException, RequestException;
- public RuntimeResult deleteInfoElement(InfoElementNaturalKey ieKey) throws RemoteException, RequestException;
- public RuntimeResult updateInfoElement(InfoElementData ieData, InfoElementNaturalKey ieKey) throws RemoteException, RequestException;
- public InfoElementData[] getInfoElementList() throws RemoteException, RequestException;

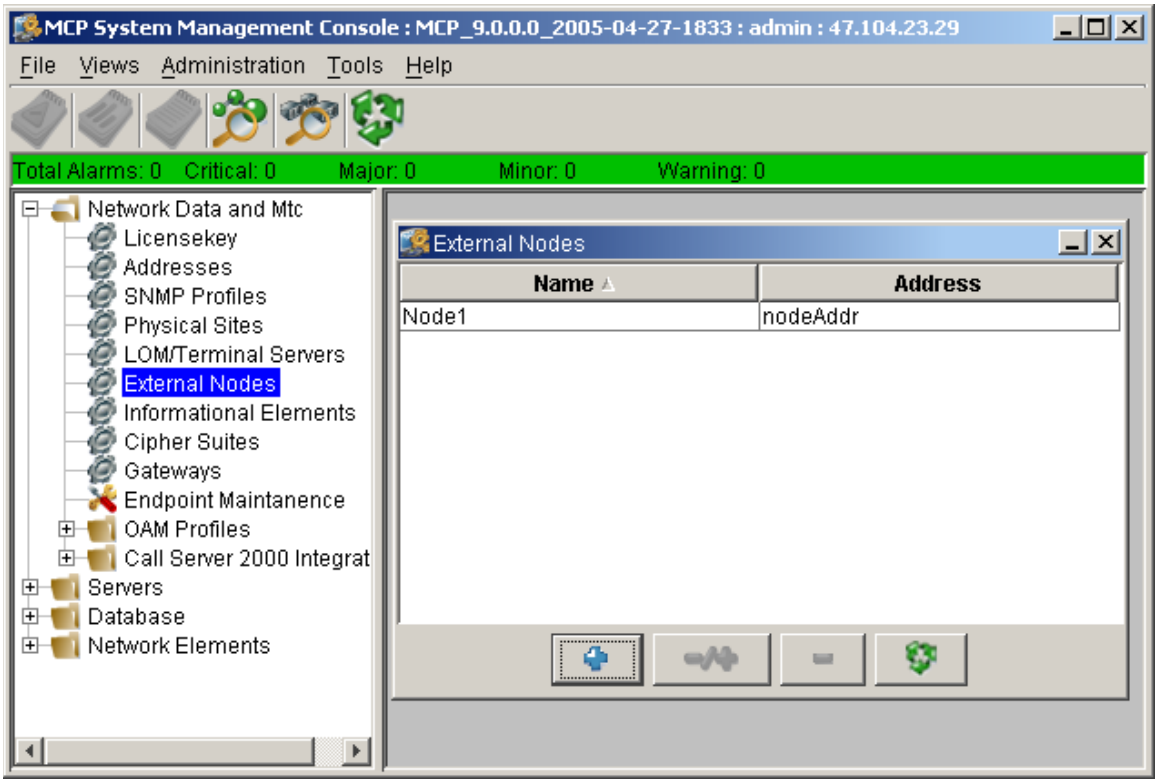
- public String[] getInfoElementTypes() throws RemoteException, RequestException;

Figure 2: Informational Element Service



A new configuration service called External Nodes (refer to Figure 3) is added so that multiple Informational Elements can be added with same IPAddress and different ports.

Figure 3: External Nodes



102.4.2.1 Pre-Staged System Re-IP

When Re-IPing a pre-staged system, first Re-IP all the servers as described in section Re-IP of MCS Server3.1.1. Once the servers are inservice, there are two ways of Re-IPing the MCS components.

1. Run a script on the server that will be running the System Manager and provide the IP addresses for all components. After the changes have been applied, start the System Manager. All managed components can then be started.
2. Run a script on the server that will be running the System Manager and provide only the IP addresses of the System Manager server and the Database server. Apply changes and start the System Manager. Once the System Manager is up, change the individual IP addresses from the System Manager GUI and apply the changes. Then start the remaining MCS components.

102.4.2.2 In Service System Re-IP

In general the following steps will be required to Re-IP a server running a managed MCS component:

1. Using the System Manger GUI, stop all MCS components running on the server to be Re-IPed.
2. Run the Re-IP script on the server and restart the server.
3. Using the System Manager GUI, change the address of the server from the old IP address to the new IP address.
4. Restart all MCS components on the server.

There are exceptions to the above where the System Manager and the database server are involved. These exceptions are listed below.

102.4.2.2.1 Re-IP System Manager Server

The steps necessary to Re-IP the server running the System Manager are as follows:

1. Using the System Manger GUI, stop all MCS components other than the System Manager running on the server.
2. From the command line on the server, stop the System Manager.
3. Run the Re-IP script on the server and restart.
4. Restart the System Manager. Then using the System Manager GUI, restart any other MCS components assigned to the server.

102.4.2.2.2 Re-IP Database Server

The steps necessary to Re-IP the server running the database are as follows:

1. Using the System Manager GUI change the IP address of the server running the database.
2. On the database server, stop the database process.
3. Run the Re-IP script on the database server and restart.
4. Restart the database.

In the case where database replication is enabled, the primary and secondary database must be reconfigured to allow replication from the new IP address. A script is provided to be run on the Oracle servers after the servers have been Re-IPed. This script will make the necessary configuration changes to Oracle in order to continue database replication.

102.4.2.2.3 Re-IP MCS components which are deployed in fault tolerance mode

If a particular component is deployed in a fault tolerant mode, the component deployed on the server being Re-IPed should be made offline, so that the other component instance becomes active.

Once the peer instance has become active, the procedure is the same as described in section In Service System Re-IP 3.1.2.2.

102.4.3 MOPs

Detailed MOPs are provided as part of the feature for each of the following cases:

- **Pre-Staged System Re-IP:**
  - — SUN Servers N240 AC/DC / V100 / T140X running Session Manager, System Manager, Accounting Manager, Provisioning Manager, IP Client Manager, H.323 and Database.
  - — IBM BladeCenter / IBM x306 running RTP Media Portal on Linux.
- **In-Service System Re-IP:**
  - — SUN Servers N240 AC/DC / V100 / T140X running Session Manager, System Manager, Accounting Manager, Provisioning Manager, IP Client Manager, H.323 and Database.
  - — IBM BladeCenter / IBM x306 running RTP Media Portal on Linux.

The in-service system Re-IP will differ in steps from the Pre-Staged Re-IP. MOPs will be written to cover all the following scenarios.

1. Changing customer addresses on entire system.
2. Changing the customer addresses on one or more resources (i.e. gateways, RTP Media Portal)
3. Changing the customer addresses on one or more Session Managers.
4. Changing the customer addresses on one or more Database Servers.
5. Changing the customer addresses of one or more Provisioning Managers.
6. Changing the customer addresses of one or more IP Client Managers.
7. Changing the customer addresses of one or more System Manager / Accounting Managers.
8. Changing the customer addresses of one or more H.323 Servers.

- **OPI/BPT Script Updates:**

  This MOP will describe in detail which OPI methods have been obsoleted and how existing scripts should be updated to utilize the new methods. No existing functionality will be lost.

102.5 Provisioning System Changes

The data on the Provisioning client that uses any IP address will be changed to use the logical names for the addresses or the NE's (if it is NE specific).

The areas identified for change are discussed in the following sections. DB upgrade scripts are written to handle each of these changes for a 3.x to 4.1 and 4.0 to 4.1 system upgrade.

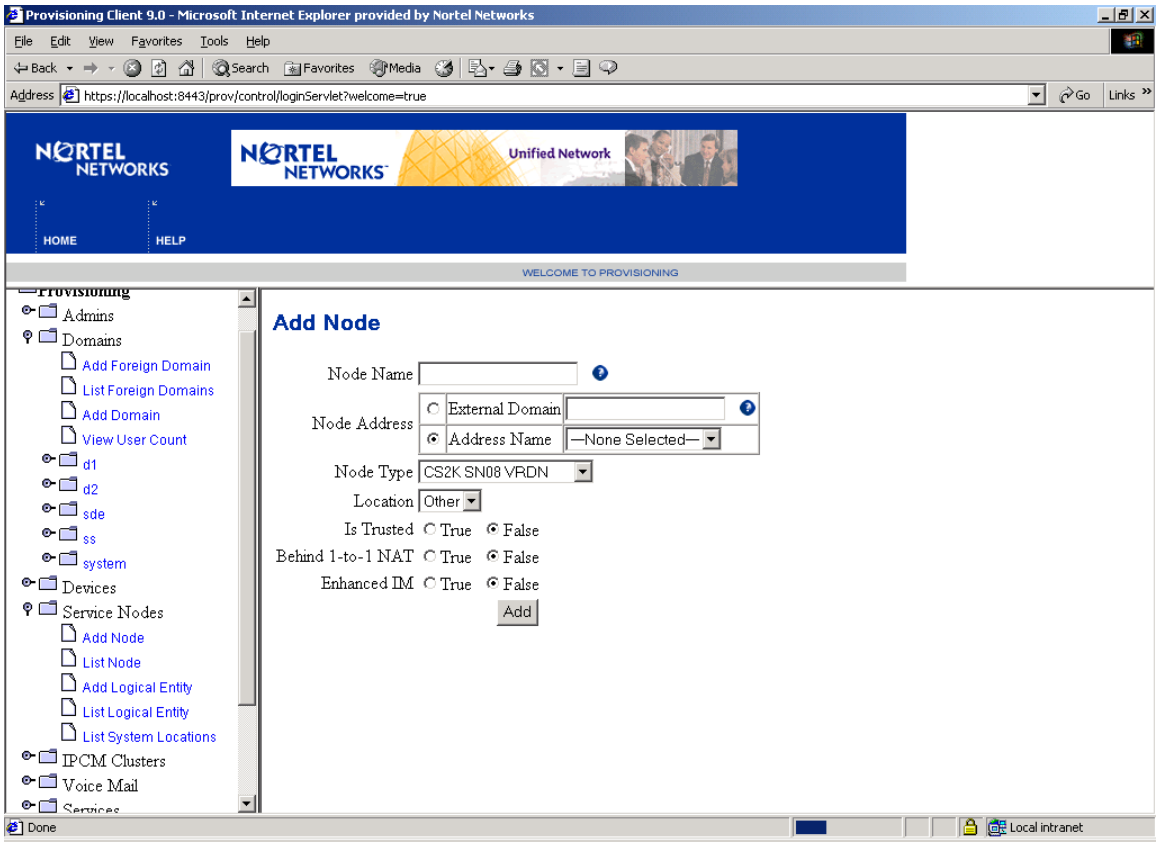
102.5.1 Service Node Provisioning

This feature creates a new menu item under the System level called Service Nodes. A Service Node is defined as any network element which provides a service. Examples include protocol gateways, conference servers, voicemail servers, etc. Attributes such as location, trust status, etc. are associated with each service node. A logical node consists of one or more service nodes. Each service node it contains may have additional system or user defined parameters (e.g. trkgrp) associated with it that affect the service offered by the service node.

A new Right “Node Provisioning” (NODE) is being added. Only admins with this right would be able to manipulate Nodes.

The following shows what the new provisioning page for adding a service node to the system looks like.

Figure 4: Add Service Node



The Add Node page allows the administrator to add a GW, a MAS server, or any third party box as well as provide the necessary attributes such as location and node type that pertain to that box.

The node name is an identifier for the node and has a maximum length of 30 characters. Only alpha numeric and _ chars are allowed.

The External Domain / Address Name fields are mutually exclusive and only one can be enetered.

Under normal circumstances, only the Address Name field should be used. This is a drop down of names of the following elements on the System Manager:
a MAS Server, an Audio Code Gateway, an H323 Gatekeeper, or an Informational Element of type General or Gateway or Pooled Media Resource.

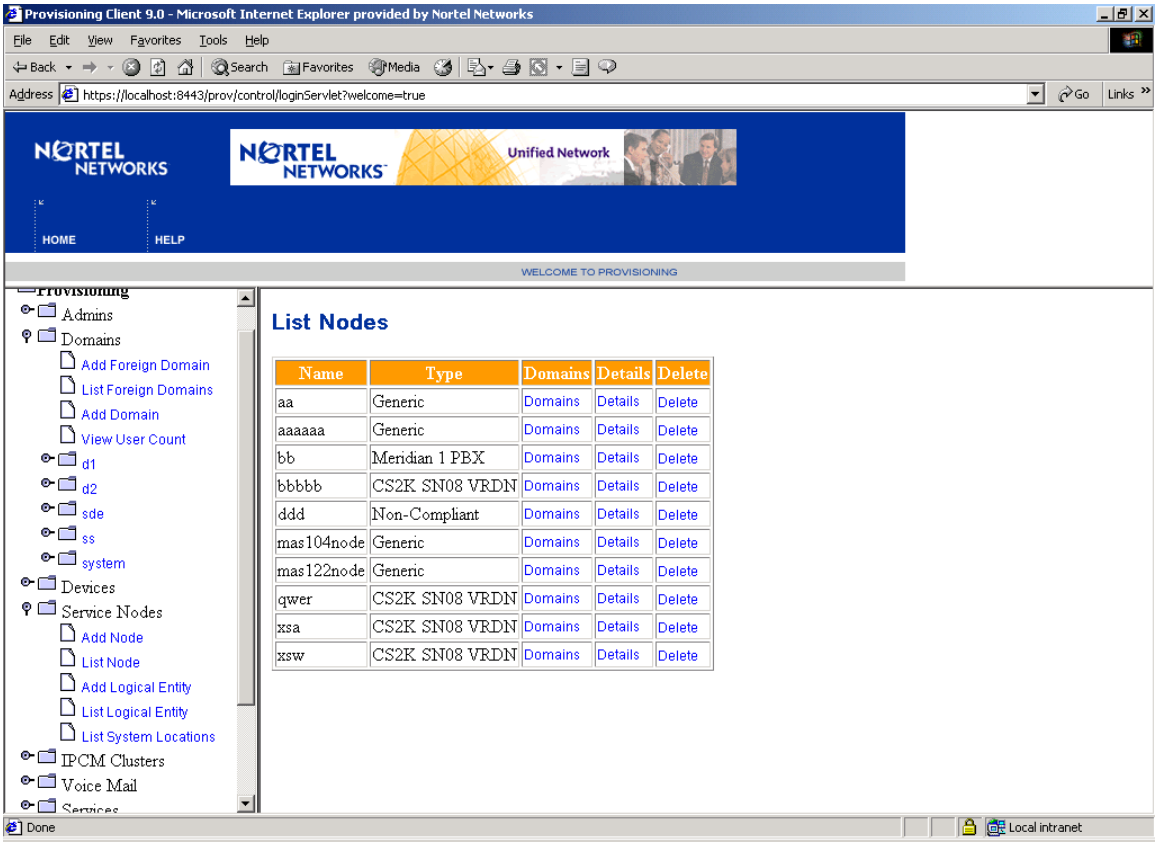
The External Domain field is available in case there is an address that does not have an IP. At this point this is used during upgrades where if the host field on the gateway or the route on the pooled entity cannot be parsed properly, we put the entire route in this field. That ways the calls will still work. A log is generated for all these types and the customer is suggested to fix their provisioning data. No data available in this field is validated and the data is not reipable.

If the customer chooses to add an IP here, and use it instead of the right way of adding it on the SM and then use from pull down, then this data would not be re-ipable.

Node Type: This is the old Gateway Type. The Description for Non-Compliant Gateway and Generic Gateway ahave been changed to Non-Compliant and Generic, so they can be used for other servers.

The following figure shows the ‘List Node’ screen.

Figure 5: List Node



Once the administrator has added the physical nodes, the node can be assigned to root domains. Only after the nodes are assigned, the domains can use those to create gateway routes or ERLs or Assign to Routable Services.

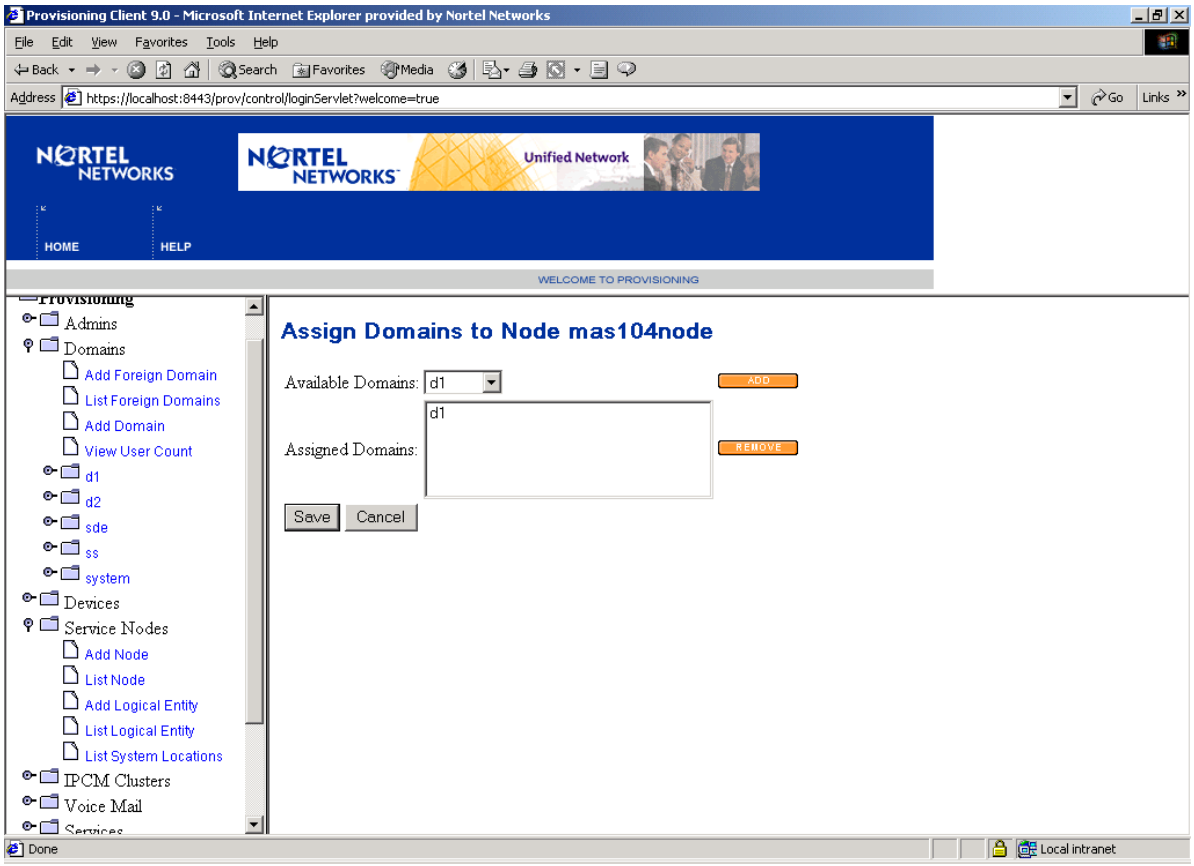


Figure 6: Assign domains to Node

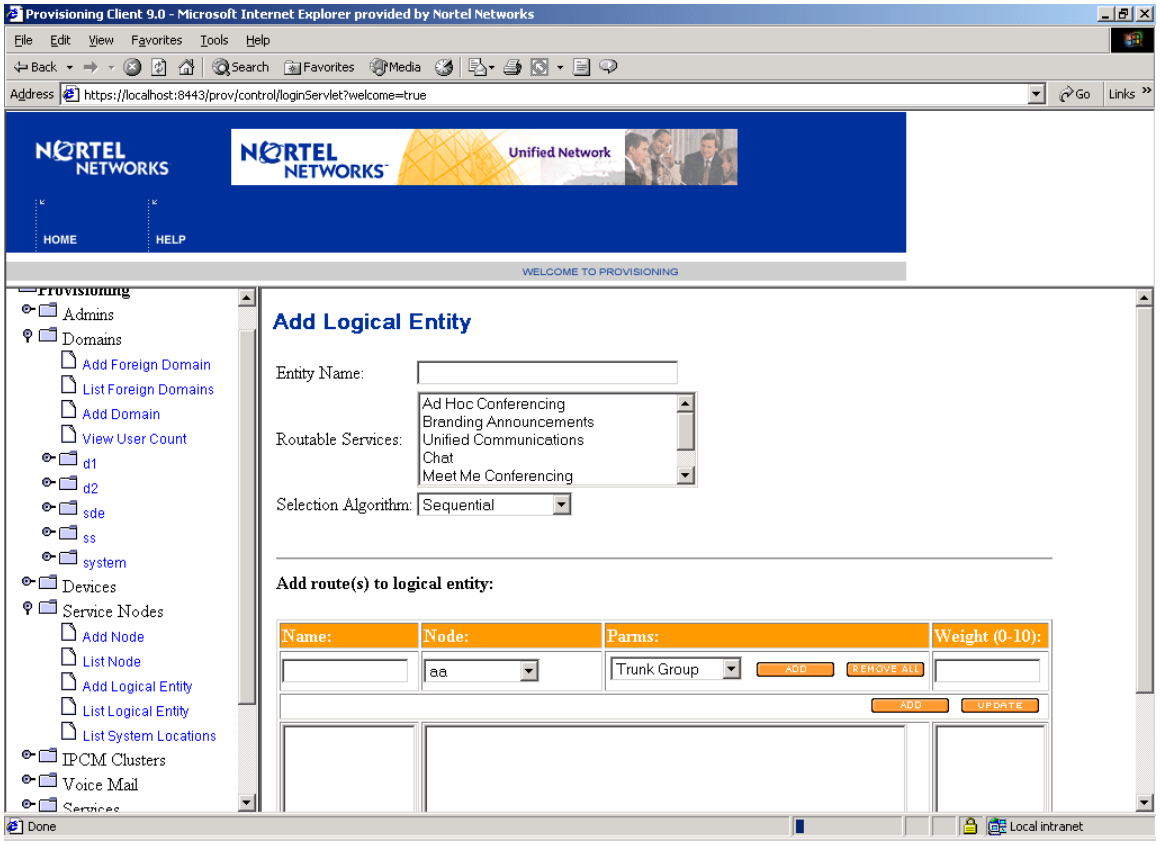
The administrator can also use the nodes to add logical nodes. Logical nodes are comprised of one or more physical nodes and allow for the following:

- **Route parameters**: The admin is given the ability to associate parameters with a given physical node. For example, the admin may have provisioned one physical GW but wants to be able to route to different trunk groups owned by the GW. To do this the admin would create a Logical Node for each trunk group by picking the physical node and then associating a ‘norteltrkgrp’ parameter with it.
- **Pooled Entities**: The admin is also given the ability to define more than one physical node as part of the logical node definition. This provides for the Pooled Entity functionality previously provisioned at the domain level. By placing the PE functionality within the definition of a Logical Node, we have removed the need for the admin to make a distinction between a single node and a PE for the purpose of provisioning in all other areas such as telephony routes, ERLs, etc.

Once the administrator has added the logical entity, the logical entity can be assigned to root domains. Only after the nodes are assigned, the domains can use those to create gateway routes or ERLs or Assign to Routable Services.

A logical entity can contain any of the nodes that are defined in the system. It does not matter if the node is not assigned to a domain. Only the node/ logical entity that are assigned to a domain are available at a particular domain for use. The assignment of nodes to domains gives us the flexibility where a gateway does not need any additional parameters and hence does not need an additional logical entity to be created.

Figure 7: Add Logical Node



The Entity Name is an identifier for the logical entity and is a 30 character max alphanumeric and _ field.

The Routable Services are optional for a Logical entity that is a collection of gateways only.

A new routing algorithm “Sequential” is added which can be used for pooled gateways.

The routes have a name which is a 30 character max alphanumeric and _ field.

The node is the list of nodes provisioned under the dd Node link.

Additional parameters can be added to the route by selecting the elements from the drop down.

A weight of 0 implies that the route is not considered for routing.

Once added, Logical Nodes can be listed as follows:

Figure 8: List Logical Node

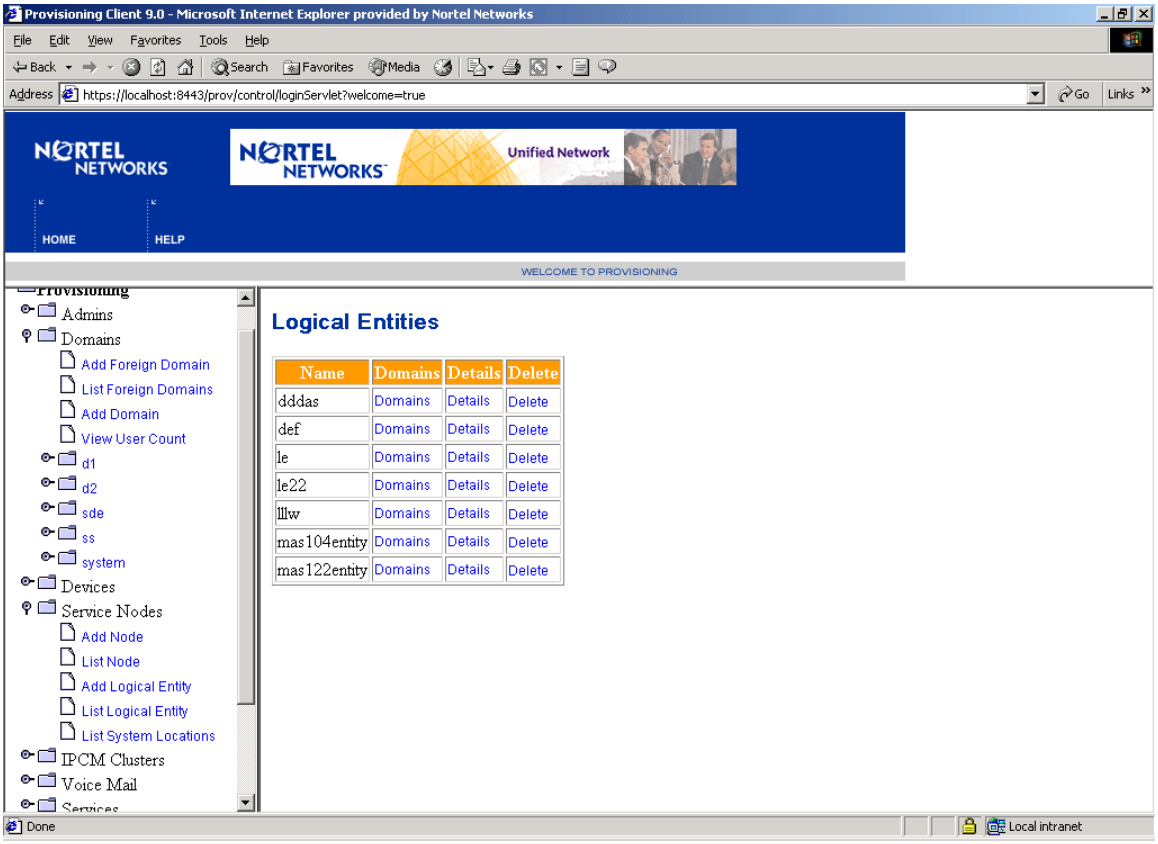
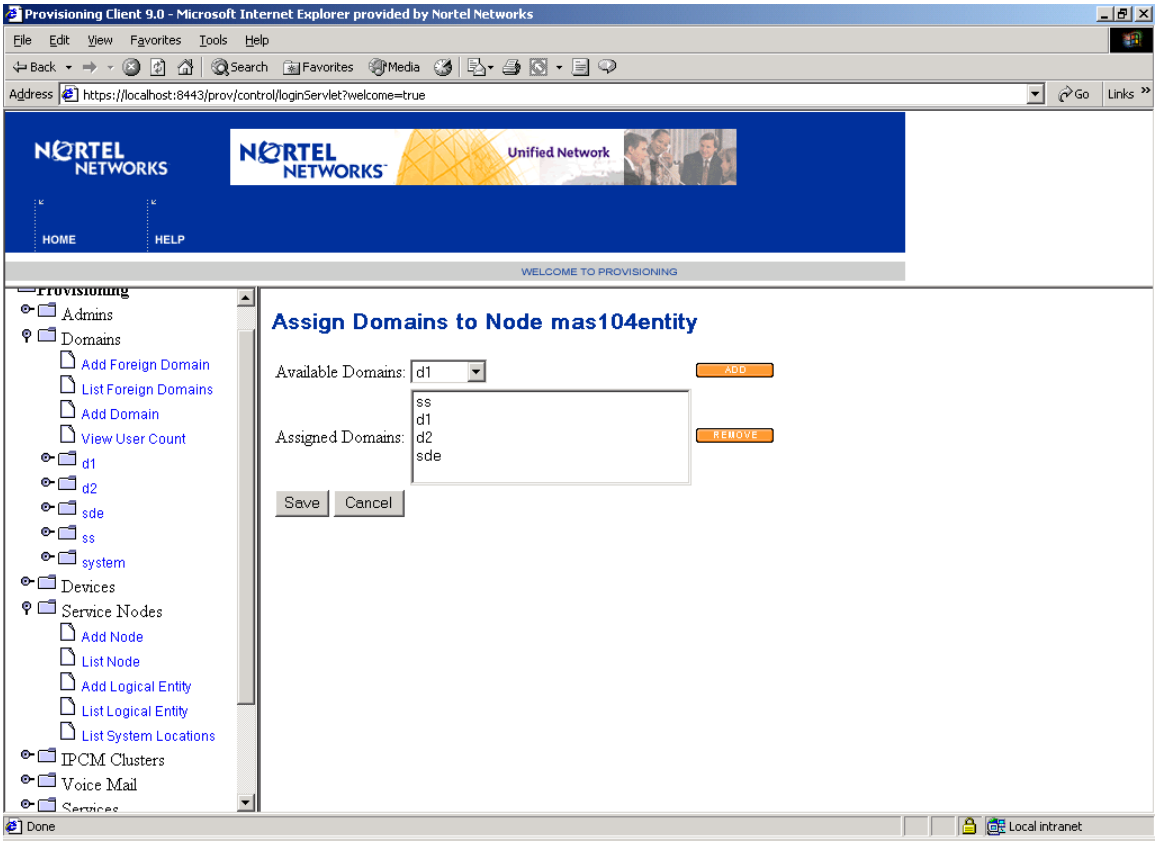


Figure 9: Assign Domains to Logical Entities



The nodes and logical entities can then be assigned to sub domains at the root domain level by the domain administrator. The sub domain assignement is used only for gateway routes and ERLs that point to the Service Nodes. The Routable Services at the sub domain level still get the entire list that is assigned to the root domain. This is in accordance with how the gateway routes / erls and routable services had access to gateways and pooled entities prior to this feature.

Figure 10: List Nodes for domain

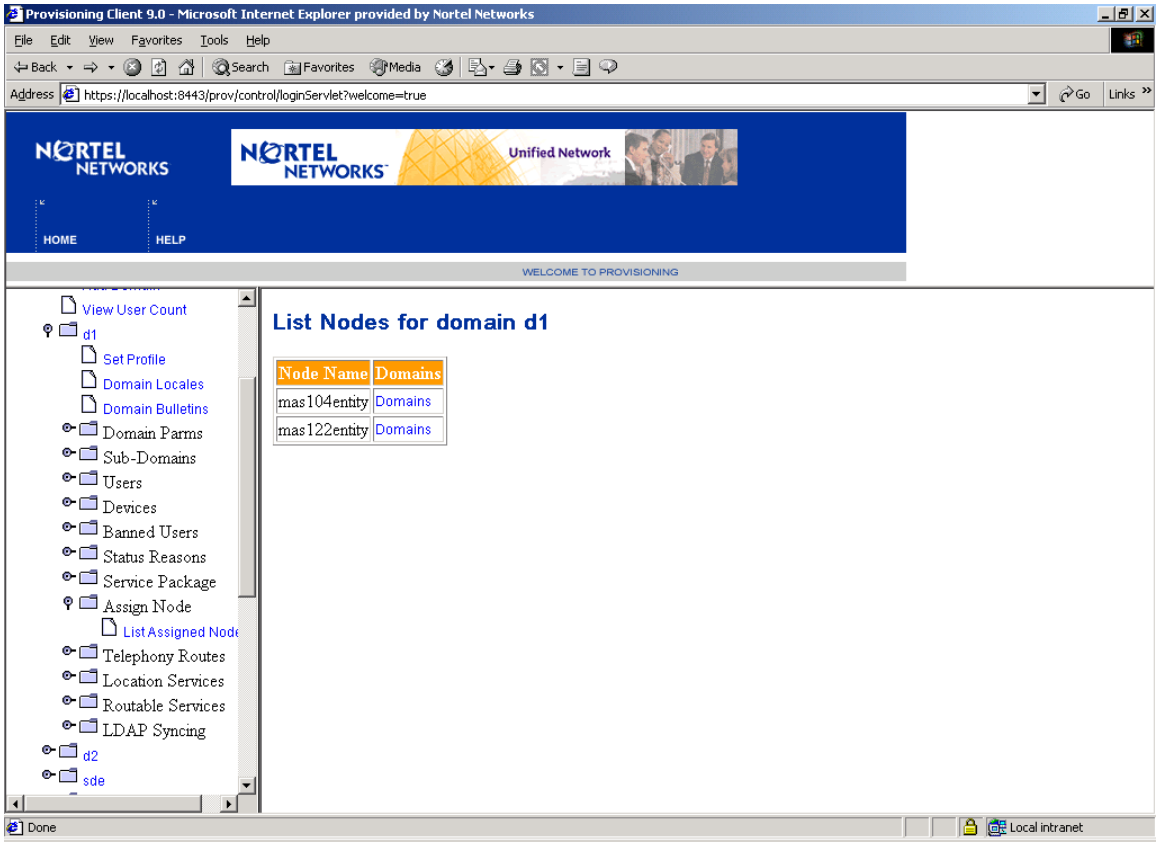
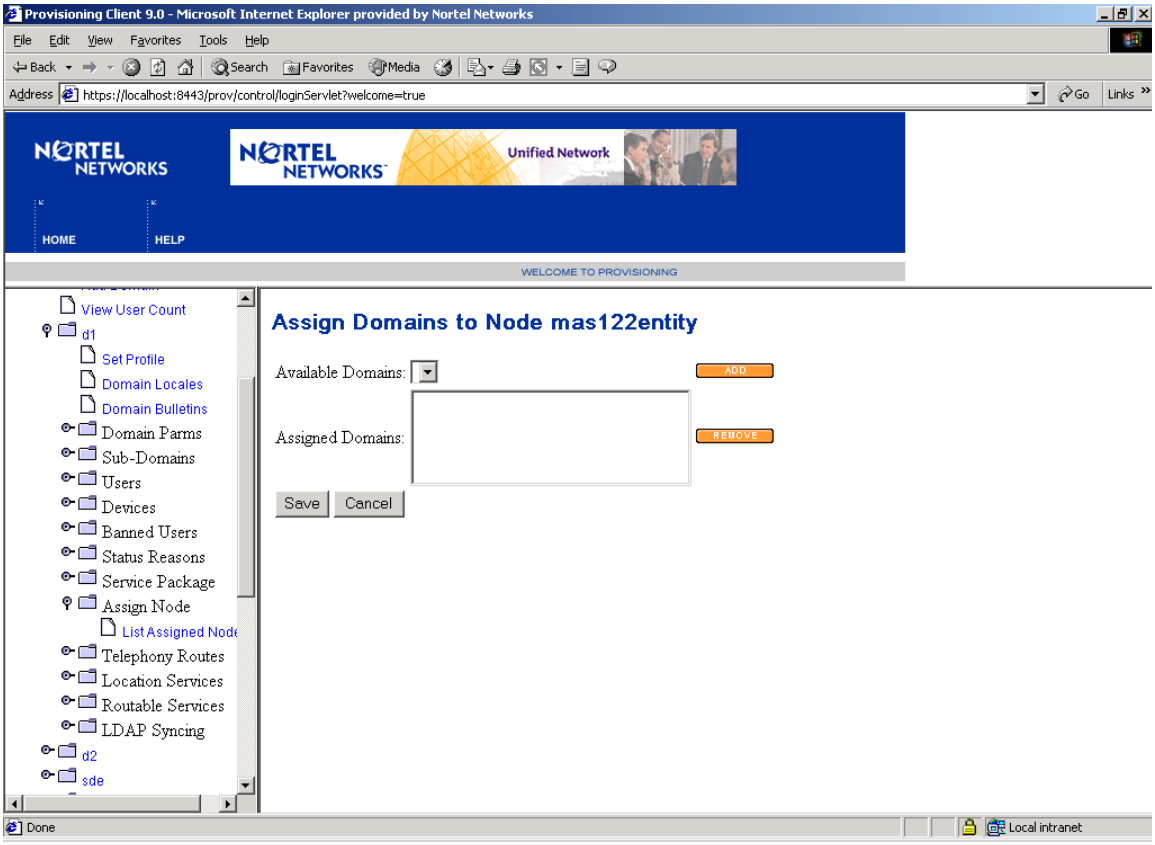


Figure 11: Assign node to sub domains



The following methods are being added to support the functionality using OPI.

- public String[] getAllNodeTypeNames() throws ProvisionException;
- public void addNode(Node node) throws ProvisionException;
- public void addNodes(Node[] nodes) throws ProvisionException;
- public void modifyNode(String nodeName, Node node) throws ProvisionException;
- public void removeNode(String nodeName) throws ProvisionException;
- public Node getNode(String nodeName) throws ProvisionException;
- public Node[] getAllNodes() throws ProvisionException;
- public int getNodeCount() throws ProvisionException;
- public void addLogicalEntity(LogicalEntity node) throws ProvisionException;
- public void addLogicalEntitys(LogicalEntity[] nodes) throws ProvisionException;

- public void modifyLogicalEntity(String logicalEntityName, LogicalEntity node) throws ProvisionException;
- public void removeLogicalEntity(String logicalEntityName) throws ProvisionException;
- public LogicalEntity getLogicalEntity(String logicalEntityName) throws ProvisionException;
- public LogicalEntity[] getAllLogicalEntitys() throws ProvisionException;
- public int getLogicalEntityCount() throws ProvisionException;
- public void assignDomainsToNode(String nodeName, String[] domains) throws ProvisionException;
- public String[] getNodeDomains(String nodeName) throws ProvisionException;
- public String[] getNodeSubDomains(String domainName, String nodeName) throws ProvisionException;
- public String[] getAllNodeNamesForDomain(String domainName) throws ProvisionException;
- public void assignNodeToSubDomains(String parentDomainName, String nodeName, String[] subdomains) throws ProvisionException;
- public String[] getDomainNodes(String domainName) throws ProvisionException;
- public String[] getAllRoutableServices() throws ProvisionException;
- public String[] getAllRoutableServiceGroups() throws ProvisionException;
- public String[] getAllNodesByRoutableService(String domain, String service) throws ProvisionException;
- public String[] getAllNodesByRoutableServiceGroup(String domain, String serviceGroup) throws ProvisionException;
- public String getAssignedNodeByDomainByServiceGroup(String domain, String serviceGroup) throws ProvisionException;
- public String getAssignedNodeByLocationByServiceGroup(String domain, String location, String serviceGroup) throws ProvisionException;
- public void assignNodeToDomain(String domain, String nodeName, String serviceGroup) throws ProvisionException;
- public void assignNodeToLocation(String domain, String location, String nodeName, String serviceGroup) throws ProvisionException;
- public void assignNodeToLocations(String domain, String[] location, String nodeName, String serviceGroup) throws ProvisionException;

- public String[] getAllLocationsForNodeByServiceGroup(String domain, String nodeName, String serviceGroup) throws ProvisionException;
- public String[] getAllAvailableLocationsByServiceGroup(String domain, String serviceGroup) throws ProvisionException;

102.5.1.1 Steps to provision Service Nodes

To add a gateway:

Step 1:

To add an Audio Codes Gateway: Add an AudioCodeServer on SM.

To add an H323 GK:Add an H323 GK on SM.

To add any other kind of Gateway: Add an Info Element of type Gateway on SM

a. Add Address on SM
b. Add an External Node on SM
c. Add an Info Element of type Gateway. Add the port if any specific port.

Step 2:

Add a Node on Prov

Service Nodes -> Add Node

Choose the name of the Audio Code Server or the H323GK or InFo Element that you added.

Assign the node to the domain that you want to use it for. The link is on the List Nodes page against the Node name.

If you do not need any parms etc, you are good to go.

Add a Logical Entity on Prov

Service Nodes -> Add Logical Entity

Give a name. Routing Algorithm Sequential.

Add routes: This is equivalent to the Gateway routes in the old world.

Give a name to the route.

Select the node you added as the destination.

From the drop down, select trunggroup and add the tg info.

Select facility domain if you want to provide one.

nn.com;maddr=IP:port;norteltrkgrp=xyz

In this nn.com is your facility domain, and xyz is the trunk group parameter.

To add a MAS:

Step 1:

To add a MAS: Add a MAS on SM.

To add any other kind of Pooled Media Resource: Add an Info Element of type Pooled Media Resource on SM

a) Add Address on SM

b) Add an External Node on SM

c) Add an Info Element of type Pooled Media Resource. Add the port if any specific port.

Step 2:

Add a Node on Prov

Service Nodes -> Add Node

Choose the name of the MAS or InFo Element that you added.

Assign the node to the domain that you want to use it for. The link is on the List Nodes page against the Node name.

Add a Logical Entity on Prov

Service Nodes -> Add Logical Entity

Give a name. Routing Algorithm Weighted Average.

Add routes: This is equivalent to the Pooled Entity Routes in the old world.

Give a name to the route.

Select the node you added as the destination.

Assign Logical Entities to Domains and then the rest is as it used to be.

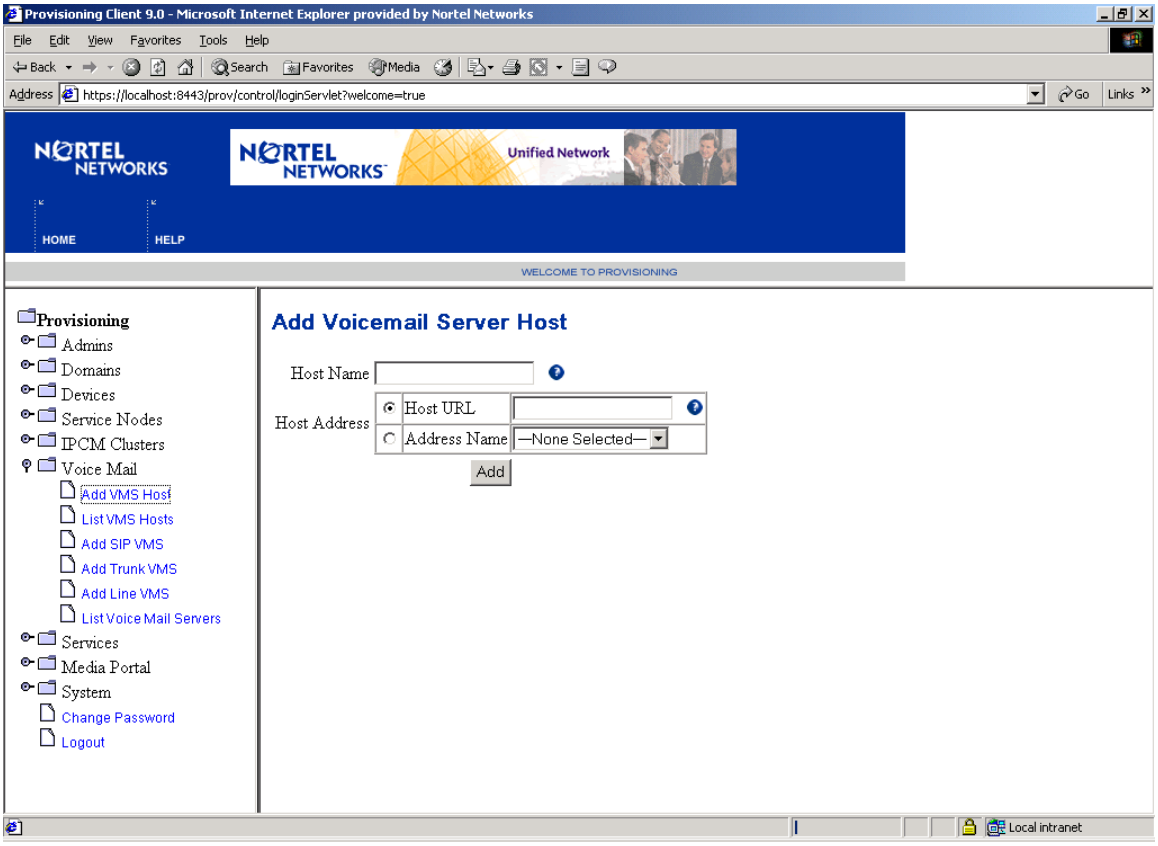
102.5.2 Voicemail Server Provisioning

102.5.2.1 Voicemail Server Host

A new menu is added to provision the host for Voicemail Servers. This is needed because the existing voicemail servers may have a URI provisioned which translates to a voicemail server instead of actual server info. There is no way for the upgrade to figure out the node.

Hence the existing URI can be used or a node can be provisioned to add a voicemail server host.

Figure 12: Add Voicemail Server Host



The host name is an identifier for the node and has a maximum length of 30 characters. Only alpha numeric and _ chars are allowed.

The Host URL / Address Name fields are mutually exclusive and only one can be enetered.

The Host URL field is available so that the existing VM server configuration still works. No data available in this field is validated and the data is not reipable.

If the customer chooses to add an IP here, and use it instead of the right way of selecting a node, then this data would not be re-ipable.

The Address Name is the list of nodes/ logical entities provisioned on the system.

The List VM Hosts page displays the list of hosts.

Figure 13: List VM Server Hosts

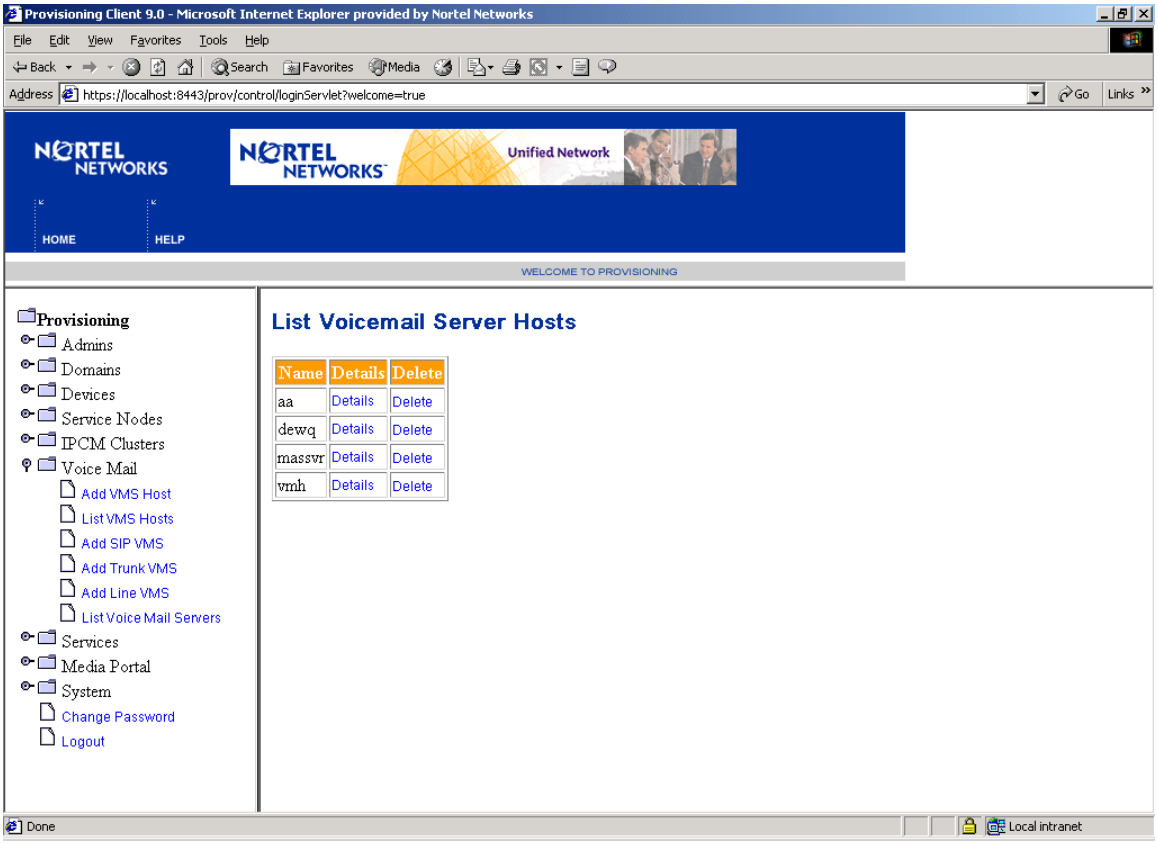


Figure 14: SIP Voicemail Server

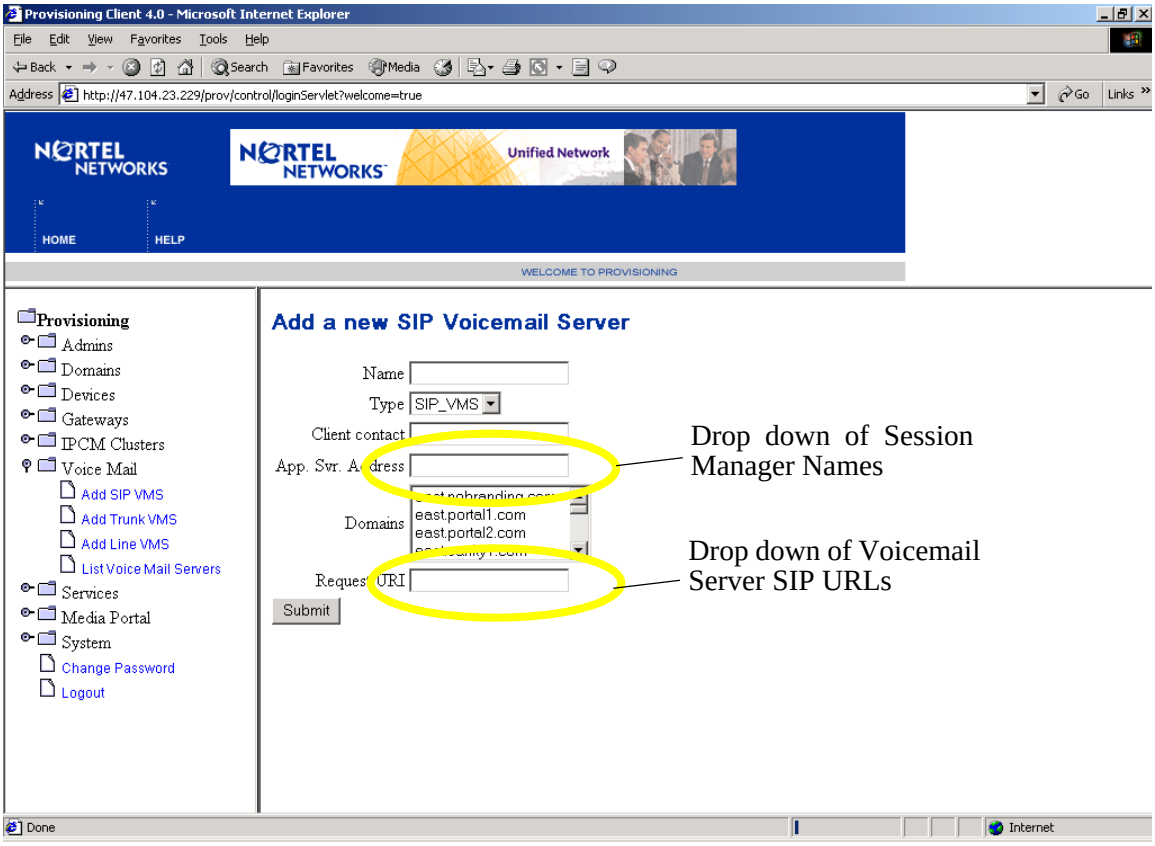


Figure 15: Trunk Voicemail Server

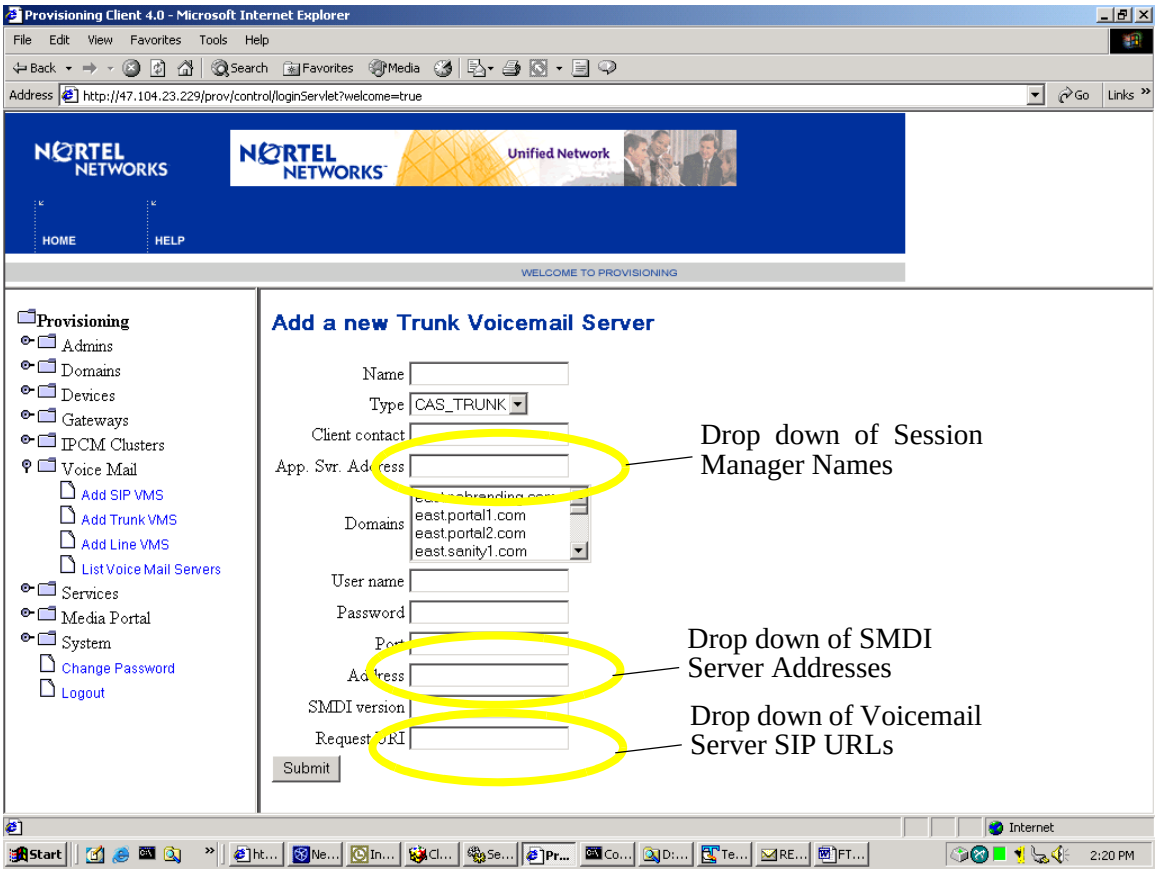


Figure 16: Line Voicemail Server

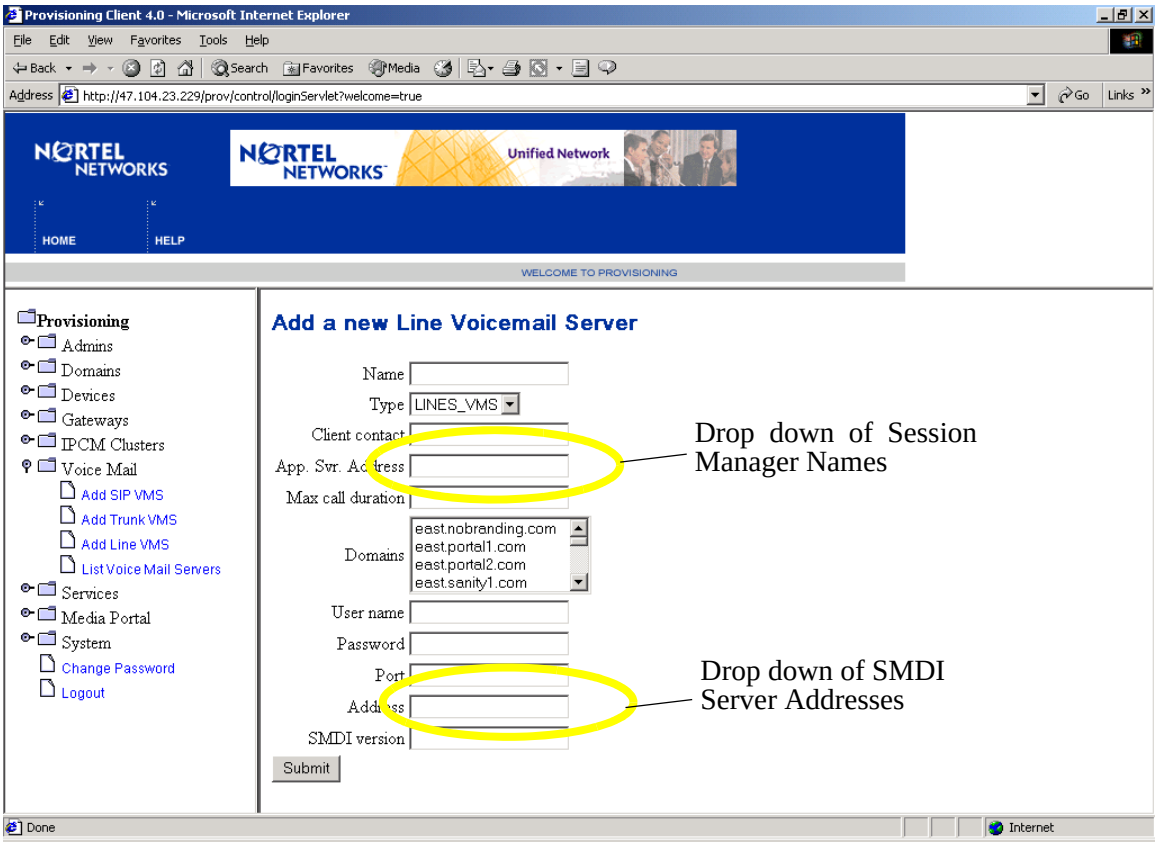
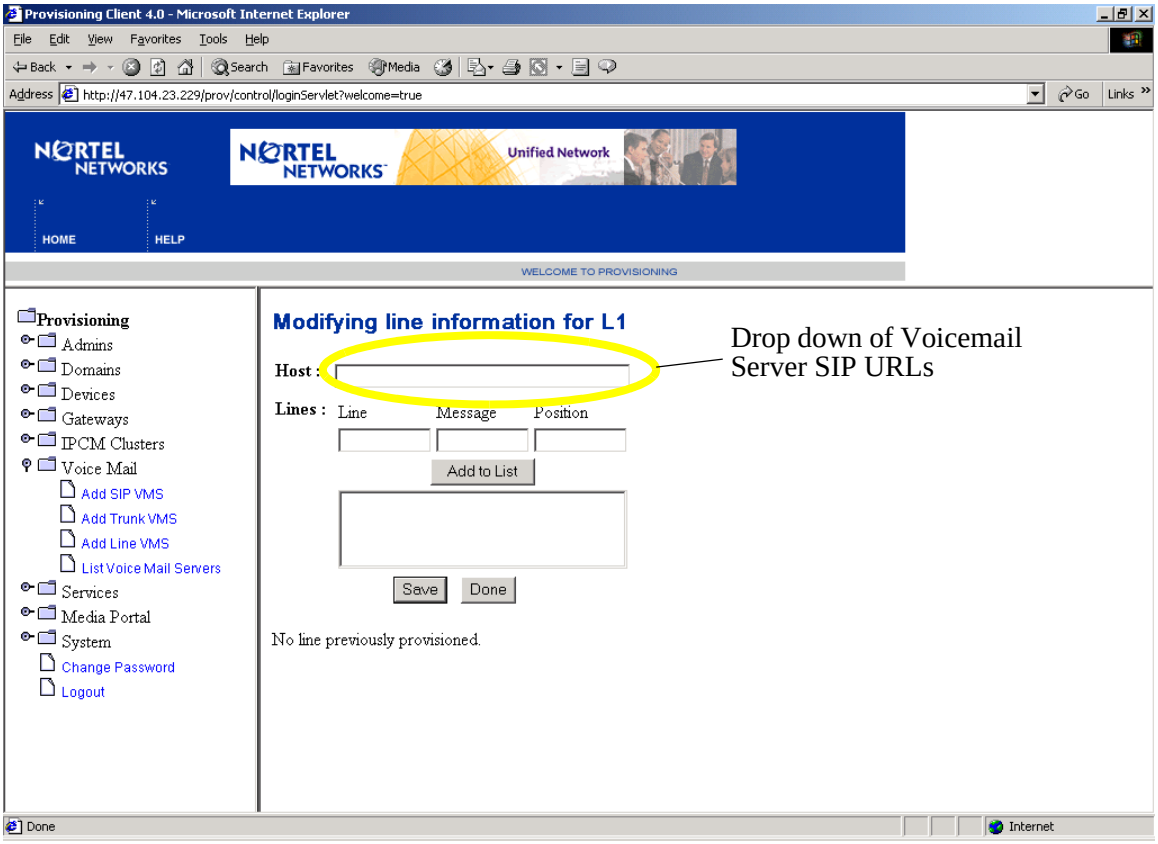


Figure 17: Line Provisioning



102.5.2.2 App Server IP Address

SIP, LINE and TRUNK Voicemail Server Provisioning require the operator to enter the Application Server IP address.

This will be changed on the Provisioning Client to let the operator select a Session Manager from a list containing logical names for all the Session Managers configured on the system.

The OPI interface does not get affected as the existing methods and data objects would work and hence the change is backward comptabile. The OPI client would now have to send the Session Manager name instead of the IP Address in the Voicemail data object. The field is highlighted below in the example for SIPVoicemailServer. The same is true for Line and Trunk Voicemail Servers also.

Usage: addSIPVoicemailServer using ([The name of the voicemail server,the type of voicemail server,The client contact for the voicemail, right now the string voicemail is used,**The address of the appserver which will be used by**

the voicemail server in an n+m scenario,The maximum amount of time that the call will be tried before rolling off to voicemail,[The domains that the voicemail server would serve, .. ,The domains that the voicemail server would serve],[The host of the SIP voicemail server, .. ,The host of the SIP voicemail server]])

The following OPI methods would now contain the Session Manager name as opposed to the IP Address.

- public void addSIPVoicemailServer(SIPVoicemailServer sipVms) throws ProvisionException;
- public void modifySIPVoicemailServer(String serverName, SIPVoicemailServer sipVms) throws ProvisionException;
- public SIPVoicemailServer[] getAllSIPVoicemailServers() throws ProvisionException;
- public SIPVoicemailServer[] getAllSIPVoicemailServersByDomain(String domainName) throws ProvisionException;
- public void addTrunkVoicemailServer(TrunkVoicemailServer trunkVms) throws ProvisionException;
- public void modifyTrunkVoicemailServer(String serverName, TrunkVoicemailServer trunkVms) throws ProvisionException;
- public TrunkVoicemailServer[] getAllTrunkVoicemailServers(String trunkType) throws ProvisionException;
- public TrunkVoicemailServer[] getTrunkVoicemailServerByDomain(String domainName, String trunkServerName) throws ProvisionException;
- public void addLineVoicemailServer(LineVoicemailServer trunkVms) throws ProvisionException;
- public void modifyLineVoicemailServer(String serverName, LineVoicemailServer lineVms) throws ProvisionException;
- public LineVoicemailServer[] getAllLineVoicemailServers() throws ProvisionException;
- public LineVoicemailServer[] getLineVoicemailServerByDomain(String domain) throws ProvisionException;
- public VoicemailServer[] getAllVoicemailServers()throws ProvisionException;
- public VoicemailServer[] getAllVoicemailServersByDomain(String domainName)throws ProvisionException;

Changes will be made on the Session Manager to use the name to resolve the IP address.

102.5.2.3 SMDI Server IP Address and Port

LINE and TRUNK Voicemail Server Provisioning require the operator to enter the SMDI Server IP address and port.

This will be changed to let the operator select a SMDI Server from a list containing logical names for all the iTouch Terminal Server addresses configured on the system.

The OPI interface does not get affected as the existing methods and data objects would work and hence the change is backward comptabile. The OPI client would now have to send the SMDI Server name instead of the IP Address in the VmTerminalServer data object. The Port field is no longer used and is deprecated in this release.

The following OPI methods would now contain the SMDI Server name as opposed to the IP Address.

- public void addTrunkVoicemailServer(TrunkVoicemailServer trunkVms) throws ProvisionException;
- public void modifyTrunkVoicemailServer(String serverName, TrunkVoicemailServer trunkVms) throws ProvisionException;
- public TrunkVoicemailServer[] getAllTrunkVoicemailServers(String trunkType) throws ProvisionException;
- public TrunkVoicemailServer[] getTrunkVoicemailServerByDomain(String domainName, String trunkServerName) throws ProvisionException;
- public void addLineVoicemailServer(LineVoicemailServer trunkVms) throws ProvisionException;
- public void modifyLineVoicemailServer(String serverName, LineVoicemailServer lineVms) throws ProvisionException;
- public LineVoicemailServer[] getAllLineVoicemailServers() throws ProvisionException;
- public LineVoicemailServer[] getLineVoicemailServerByDomain(String domain) throws ProvisionException;
- public VoicemailServer[] getAllVoicemailServers()throws ProvisionException;
- public VoicemailServer[] getAllVoicemailServersByDomain(String domainName)throws ProvisionException;

Changes will be made on the Session Manager to use the name to resolve the IP address.

102.5.2.4 Request URI and Host

SIP, LINE and TRUNK Voicemail Server Provisioning require the operator to enter the host in the Request URI and Host fields.

This will be changed to let the operator select a pre-provisioned Voicemail Server Host.

The OPI interface does not get affected as the existing methods and data objects would work and hence the change is backward comptabile. The OPI client would now have to send the VM Host name instead of the entire SIPURI in the host field.

The following OPI methods would now contain the VM Host name as opposed to the entire SIP URI.

- public void addSIPVoicemailServer(SIPVoicemailServer sipVms) throws ProvisionException;
- public void modifySIPVoicemailServer(String serverName, SIPVoicemailServer sipVms) throws ProvisionException;
- public SIPVoicemailServer[] getAllSIPVoicemailServers() throws ProvisionException;
- public SIPVoicemailServer[] getAllSIPVoicemailServersByDomain(String domainName) throws ProvisionException;
- public void addTrunkVoicemailServer(TrunkVoicemailServer trunkVms) throws ProvisionException;
- public void modifyTrunkVoicemailServer(String serverName, TrunkVoicemailServer trunkVms) throws ProvisionException;
- public TrunkVoicemailServer[] getAllTrunkVoicemailServers(String trunkType) throws ProvisionException;
- public TrunkVoicemailServer[] getTrunkVoicemailServerByDomain(String domainName, String trunkServerName) throws ProvisionException;
- public void addLineVoicemailServer(LineVoicemailServer trunkVms) throws ProvisionException;
- public void modifyLineVoicemailServer(String serverName, LineVoicemailServer lineVms) throws ProvisionException;
- public LineVoicemailServer[] getAllLineVoicemailServers() throws ProvisionException;

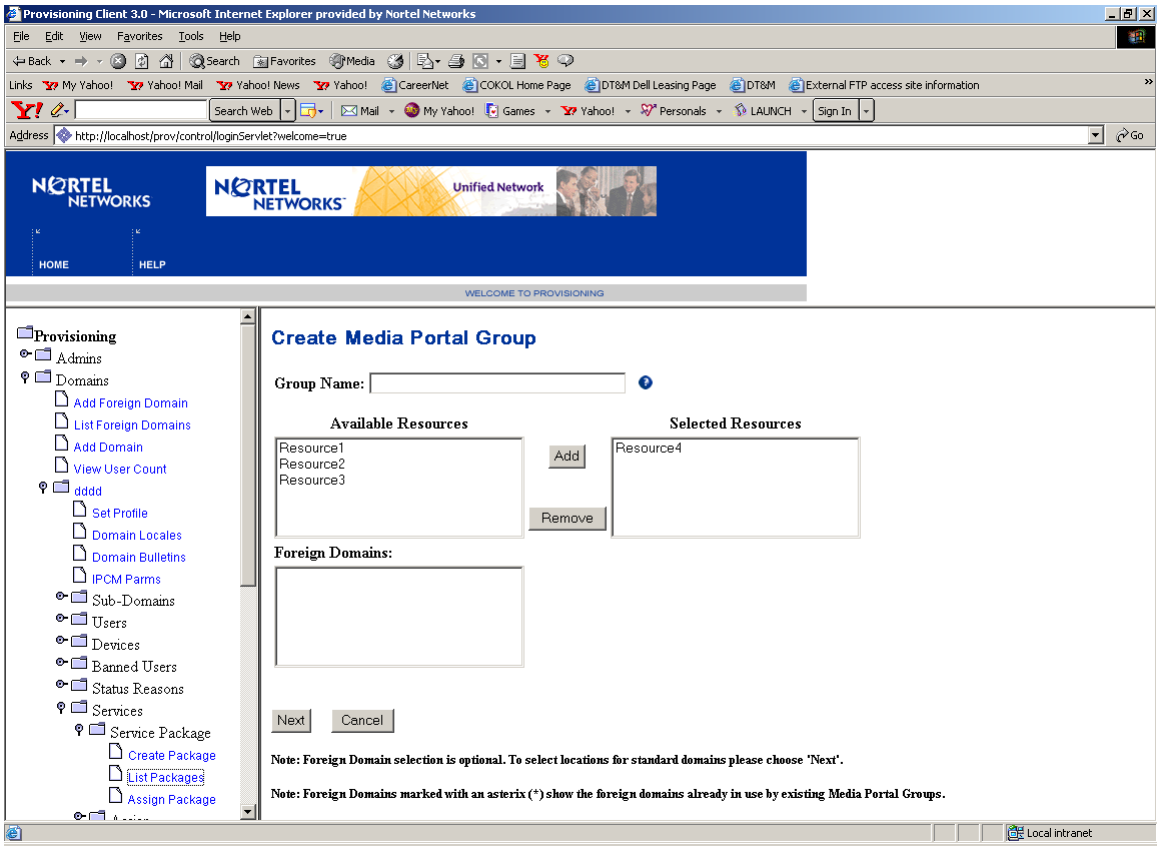
- public LineVoicemailServer[] getLineVoicemailServerByDomain(String domain) throws ProvisionException;
- public VoicemailServer[] getAllVoicemailServers()throws ProvisionException;
- public VoicemailServer[] getAllVoicemailServersByDomain(String domainName)throws ProvisionException;

The domains as assigned to voicemail servers the same way as they were done before. If a Service Node is selected for creating the voicemail server host/ the domains that it is assigned to has no impact on the list of domains that the VM server can be assigned to.

102.5.3 Media Portal Group

The Media Portal Group provisioning uses direct IP addresses for a list of available and assigned resources. This will change to display the media portal logical names in the two lists on the Provisioning Client.

Figure 18: Media Portal Groups provisioning



The OPI interface does not get affected as the existing methods and data objects would work and hence the change is backward comptabile. The OPI client would now have to send the RTP Portal names instead of the IP Address in the MediaPortalGroup data object.

The following OPI methods would now contain the MediaPortal name as opposed to the IP Address.

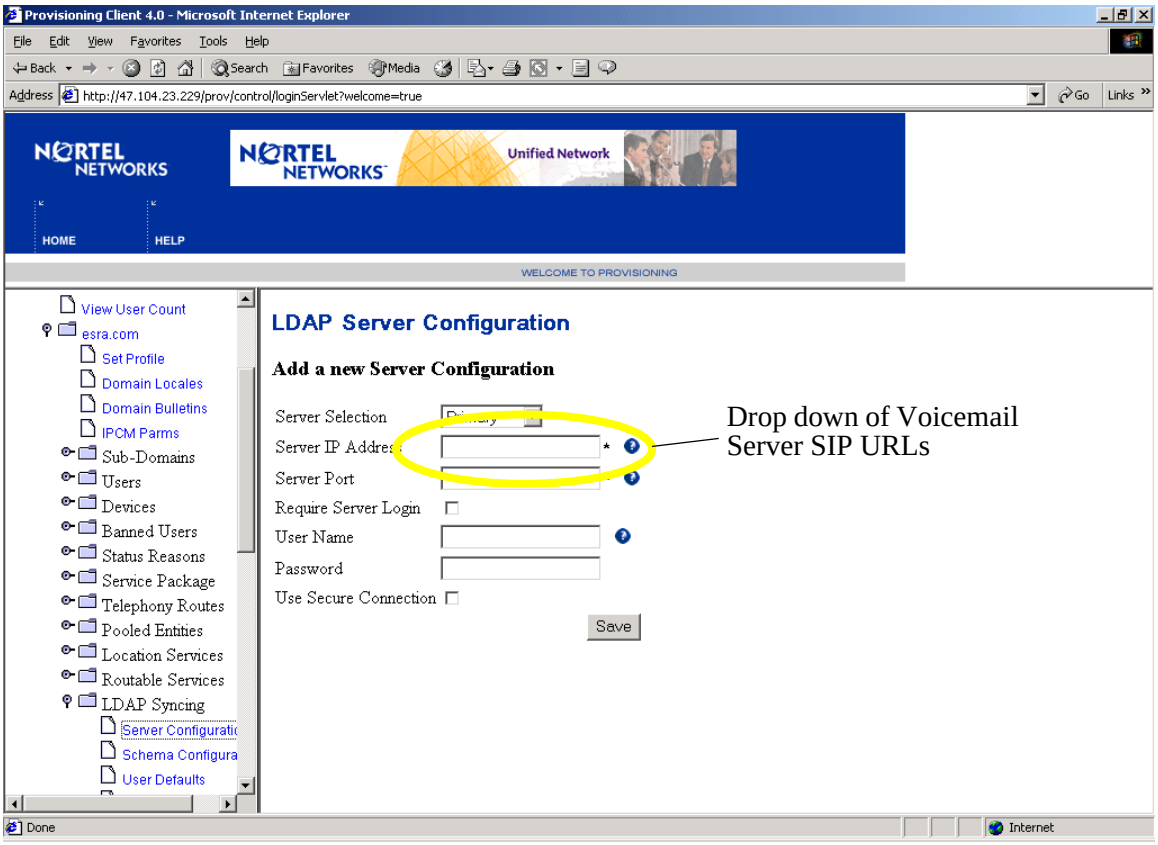
- public void addMediaPortalGroup (MediaPortalGroup mpgroup) throws ProvisionException;
- public void addMediaPortalGroups (MediaPortalGroup[] mpgroups) throws ProvisionException;
- public void modifyMediaPortalGroup(String groupName,MediaPortalGroup mpgroup) throws ProvisionException;
- public MediaPortalGroup getMediaPortalGroupByName(String groupName)throws ProvisionException;
- public MediaPortalGroup[] getAllMediaPortalGroups()throws ProvisionException;
- public String[] getAllMediaPortalResourceIPs() throws ProvisionException;

Change will be required on the Session Manager to handle this change.

102.5.4 LDAP Server Configuration

The LDAP Server provisioning require the operator to enter the SMDI Server IP address and port. This will change to display the LDAP Server logical names on the Provisioning Client.

Figure 19: LDAP Server Provisioning



The OPI interface does not get affected as the existing methods and data objects would work and hence the change is backward comptabile. The OPI client would now have to send the LDAP Server names instead of the IP Address in the LDAPInfo data object for the Primary and Secondary servers.

The following OPI methods would now contain the LDAP Server name as opposed to the IP Address.

- public void addLdapInfo(String domainName, LDAPInfo ldapInfo)throws ProvisionException;
- public LDAPInfo[] getLdapInfo(String domainName) throws ProvisionException;

102.5.5 Gateway Provisioning

This whole menu item has been removed from the system in favor of the new Service Nodes provisioning (see above). The Gateway Provisioning Right is removed.

OPI methods removed:

- public void addGateway(Gateway gateway) throws ProvisionException;
- public void addGateways(Gateway[] gateways) throws ProvisionException;
- public void modifyGateway(String gatewayHost, String gatewayType, Gateway gateway) throws ProvisionException;
- public void removeGateway(String gatewayHost, String gatewayType) throws ProvisionException;
- public void addGatewayRoute(String domainName,GatewayRoute gatewayRoute) throws ProvisionException;
- public void addGatewayRoutes(String domainName,GatewayRoute[] gatewayRoutes) throws ProvisionException;
- public void modifyGatewayRoute(String domainName,String routeName, String updatedDomainName,
- GatewayRoute gatewayRoute) throws ProvisionException;
- public void removeGatewayRoute(String domainName,String routeName) throws ProvisionException;
- public void addTrunkGroup(String domainName,TrunkGroup trunkGroup) throws ProvisionException;
- public void addTrunkGroups(String domainName,TrunkGroup[] trunkGroups) throws ProvisionException;
- public void modifyTrunkGroup(String domainName,TrunkGroup trunkGroup, TrunkGroup updatedTrunkGroup)
- throws ProvisionException;
- public void removeTrunkGroup(String domainName,TrunkGroup trunkGroup)throws ProvisionException;
- public TrunkGroup[] getTrunkGroups()throws ProvisionException;
- public Gateway[] getGateways()throws ProvisionException;
- public Gateway[] getGatewayByType(String gatewayType)throws ProvisionException;
- public GatewayRoute[] getGatewayRoutes()throws ProvisionException;
- public GatewayRoute[] getGatewayRoutesByDomain(String domainName)throws ProvisionException;
- public GatewayRoute[] getGatewayRoutesByName(String routeName) throws ProvisionException;
- public String[] getAllGatewayTypeNames() throws ProvisionException;

102.5.6 Pooled Entity Routes Provisioning

Pooled Entity provisioning has been removed altogether and has been replaced by Service Nodes at the system level (see above). No functionality has been lost by this transition.

Routable Services use the Pooled Entity Provisioning Rights. This was also used for Pooled Entity Provisioning. This right will now only be used by Routable Services.

OPI methods Removed:

- public void addPooledEntity(String domainName, PooledEntity pooledEntity) throws ProvisionException;
- public PooledEntity[] getAllPooledEntities(String domainName) throws ProvisionException;
- public PooledEntity getPooledEntity(String domainName, String pooledEntityName) throws ProvisionException;
- public void modifyPooledEntity(String domainName, String pooledEntityName, PooledEntity pooledEntity) throws ProvisionException;
- public void deletePooledEntity(String domainName, String pooledEntityName) throws ProvisionException;
- public String[] getAllPooledEntityServices() throws ProvisionException;
- public String[] getAllPooledEntitiesByService(String domain, String service) throws ProvisionException;
- public String[] getAllPooledEntitiesByServiceGroup(String domain, String serviceGroup) throws ProvisionException;
- public String getAssignedPoolByDomain(String domain, String serviceGroup) throws ProvisionException;
- public String getAssignedPoolByLocation(String domain, String location, String serviceGroup) throws ProvisionException;
- public void assignPoolToDomain(String domain, String poolName, String serviceGroup) throws ProvisionException;
- public void assignPoolToLocation(String domain, String location, String poolName, String serviceGroup) throws ProvisionException;
- public void assignPoolToLocations(String domain, String[] location, String poolName, String serviceGroup) throws ProvisionException;
- public String[] getAllLocationsForPool(String domain, String pool, String serviceGroup) throws ProvisionException;
- public String[] getAllAvailableLocations(String domain, String serviceGroup) throws ProvisionException;

- public String[] getAllPooledEntityServiceGroups() throws ProvisionException;

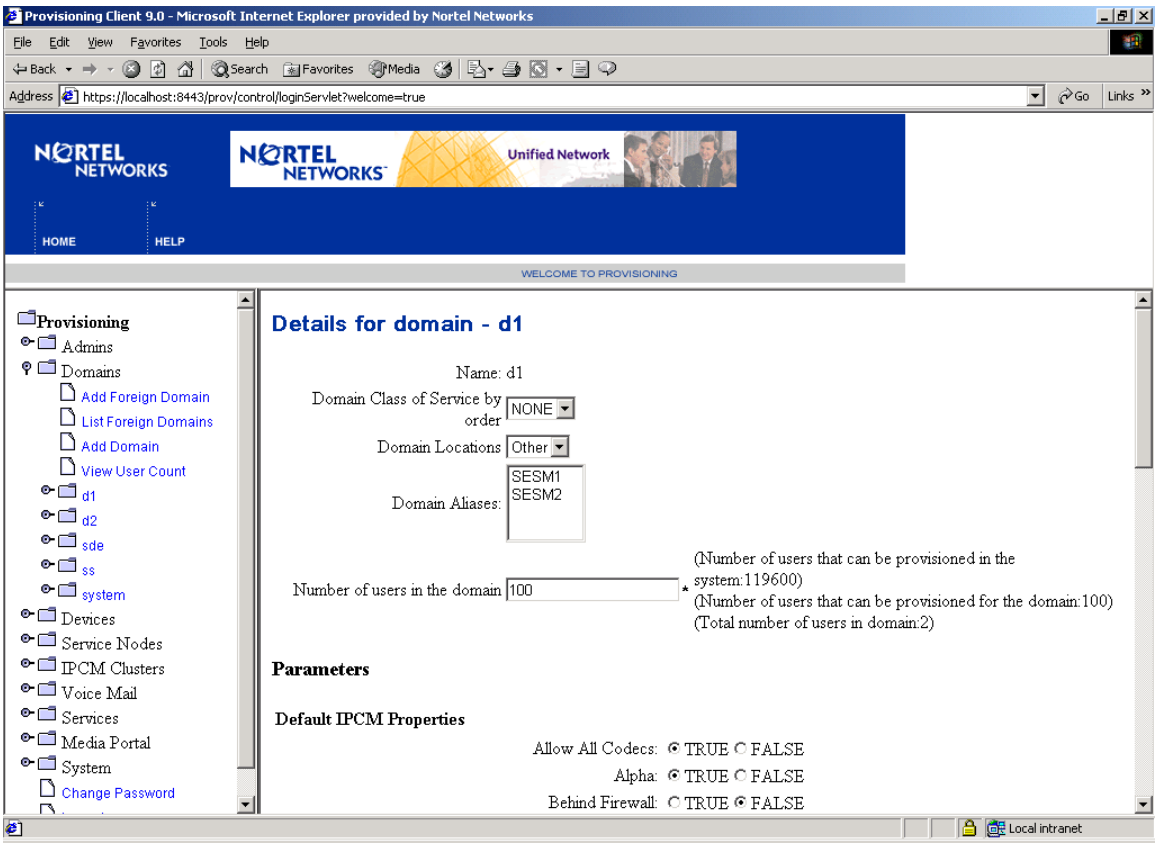
102.5.7 Domain Alias

The domain alias is changed to be the names of addresses that it represents.

The Domain Alias can either be a Session manager or an Info Element of type General.

The Add Domain page now lists these names instead of letting the customer enter free form IP addresses.

Figure 20: Add Domain



The following OPI methods now have the short name of the SM elements instead of IP addresses in the alias field.

- public void addRootDomain(Domain domain) throws ProvisionException;

- public void addSubDomain(String parentDomainName, Domain domain) throws ProvisionException;
- public void modifyDomain(String domainName,Domain domain) throws ProvisionException;
- public Domain[] getAllDomains() throws ProvisionException;
- public Domain[] getChildrenDomains(String parentName) throws ProvisionException;
- public Domain getParentDomain(String subDomainName) throws ProvisionException;
- public Domain getRootDomain(String domainName) throws ProvisionException;
- public Domain[] getDomains(int start, int stop) throws ProvisionException;

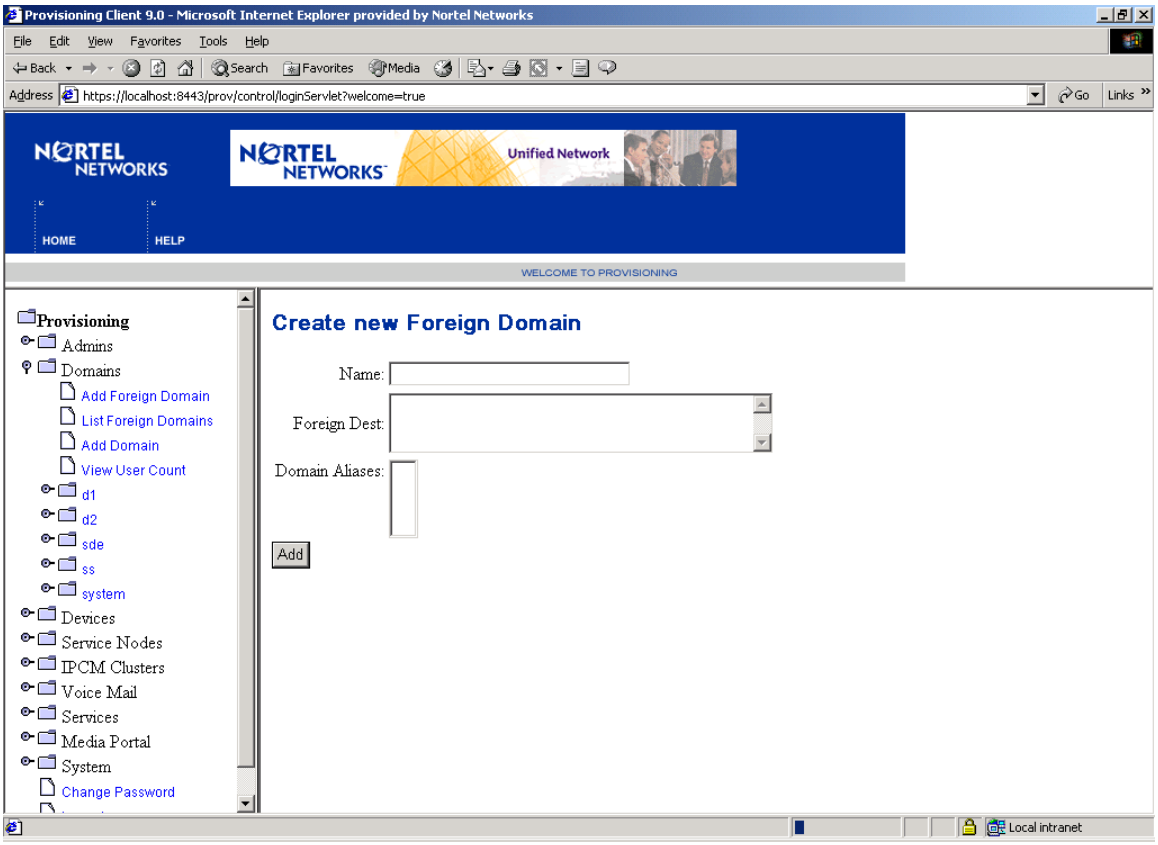
102.5.8 Foreign Domain Alias

The foreign domain alias is changed to be the names of addresses that it represents.

The Domain Alias can be an Info Element of type General.

The Add Foreign Domain page now lists these names instead of letting the customer enter free form IP addresses.

Figure 21: Add Foreign Domain



The following OPI methods now have the short name of the SM elements instead of IP addresses in the alias field.

- public void addForeignDomain(ForeignDomain forDomain) throws ProvisionException;
- public void modifyForeignDomain(String name,ForeignDomain forDomain) throws ProvisionException;
- public ForeignDomain getForeignDomain(String forDomains) throws ProvisionException;

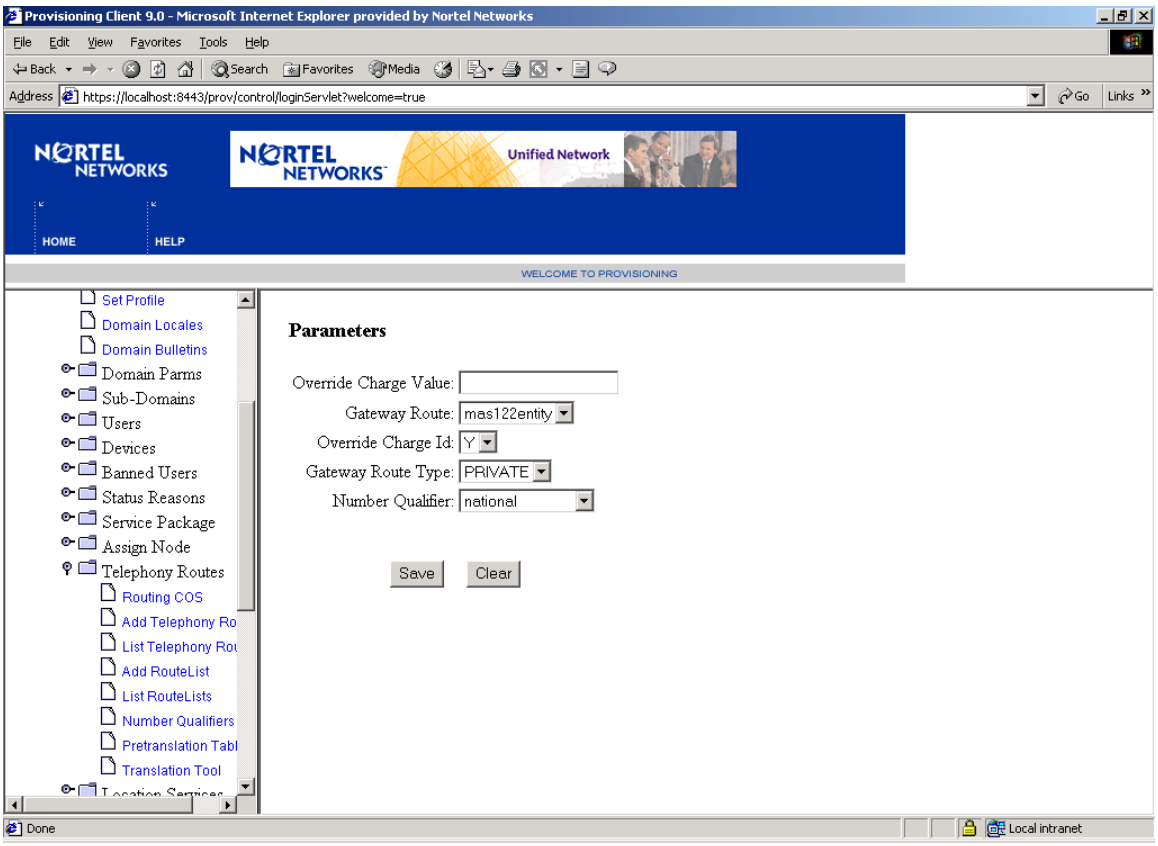
The foreign Dest field is left as is. Since these are addresses of external systems, there is no need for ReIP support on these.

102.5.9 Telephony Routes

102.5.9.1 Gateway Telephony Routes

The Gateway Telephony routes will now select a node/ logical entity assigned to the domain/ sub domain instead of the gateway routes as in previous releases.

Figure 22: Gateway Telephony Routes



The OPI interface does not get affected as the existing methods and data objects would work and hence the change is backward comptabile.

The following OPI methods would now contain the node/ logical entity names instead of the gateway route names.

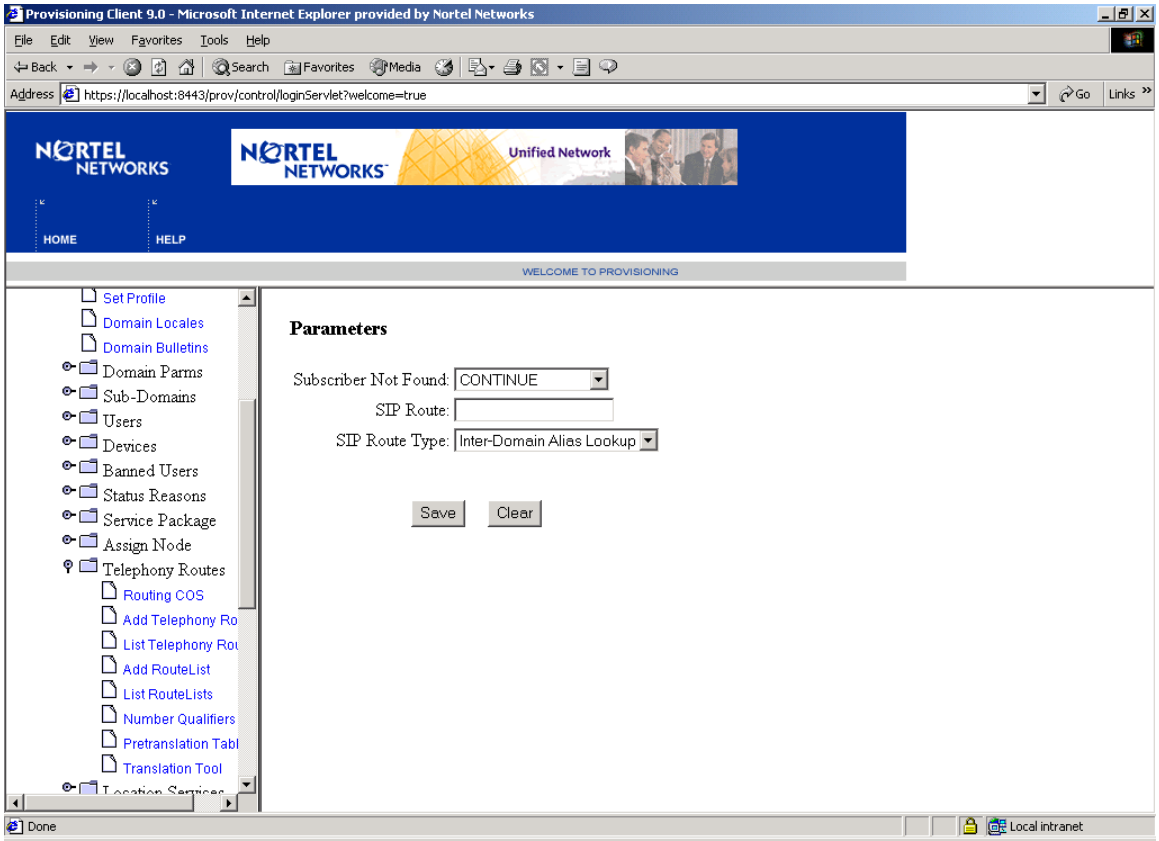
- public void addTelephonyRoute (String domainName, TelephonyRoute teleRoute) throws ProvisionException;
- public void addTelephonyRoutes (String domainName, TelephonyRoute[] teleRoutes) throws ProvisionException;
- public TelephonyRoute[] getTelephonyRoutesByDomain (String domainName) throws ProvisionException;

- public TelephonyRoute[] getTelephonyRoute (String domainName, String routeName) throws ProvisionException;
- public void modifyTelephonyRoute (String domainName,String routeName,TelephonyRoute teleRoute) throws ProvisionException;

102.5.9.2 SIP Telephony Routes

Telephony Routing is changed by this feature to remove the need to create a fake Gateway in order to route to another domain. Instead a new option is added to the Sip Route Config page that allows the admin to select whether the entry is a Sip Route in its traditional sense (checking for a subscriber alias in another domain) or an actual route to another domain (where full translations are applied).

Figure 23: SIP Telephony Routes



The OPI interface does not get affected as the existing methods and data objects would work and hence the change is backward comptabile.

The following OPI methods would now contain the node/ logical entity names instead of the gateway route names.

- public void addTelephonyRoute (String domainName, TelephonyRoute teleRoute) throws ProvisionException;
- public void addTelephonyRoutes (String domainName, TelephonyRoute[] teleRoutes) throws ProvisionException;
- public TelephonyRoute[] getTelephonyRoutesByDomain (String domainName) throws ProvisionException;
- public TelephonyRoute[] getTelephonyRoute (String domainName, String routeName) throws ProvisionException;
- public void modifyTelephonyRoute (String domainName,String routeName,TelephonyRoute teleRoute) throws ProvisionException;

The TelephonyRoute object can also take a new Name Value: SIP Route Type (0 or 1). The absence of this assumes 0 which is the old way of doing SIP translations.

The two types are:

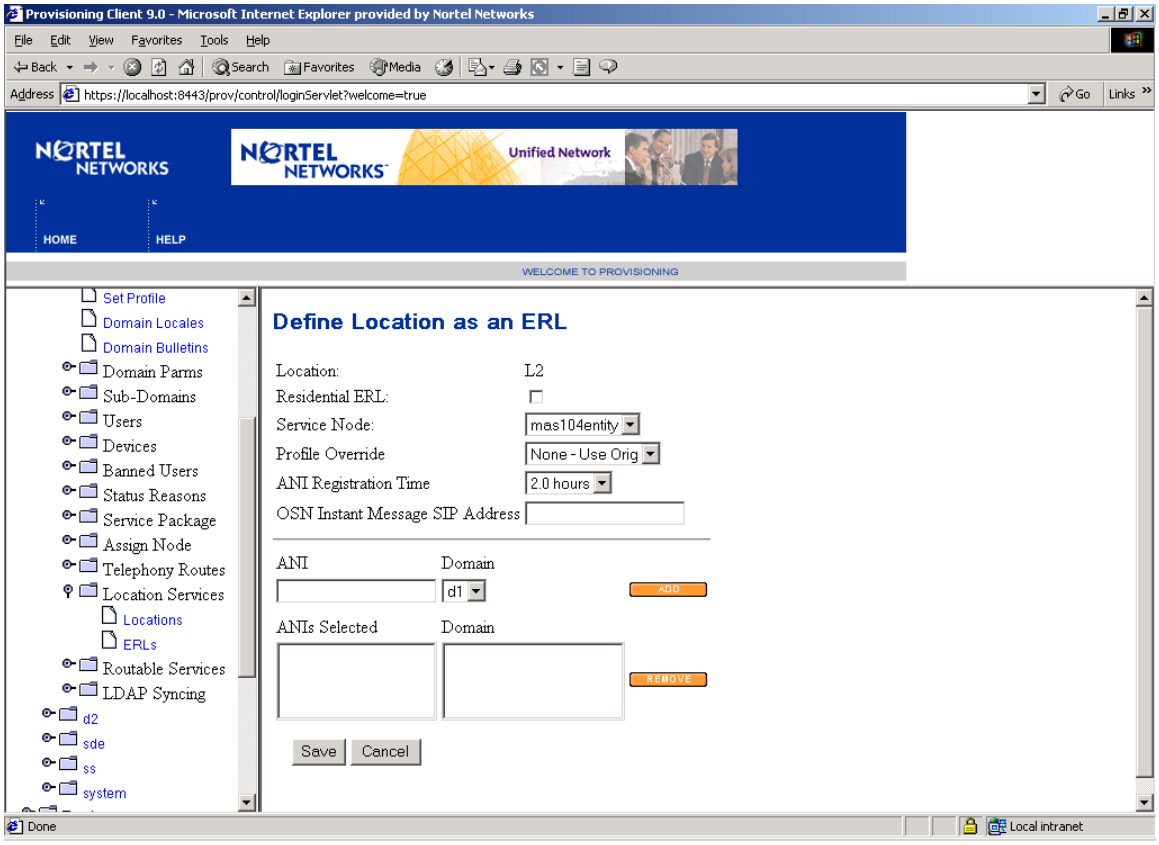
“Inter-Domain Alias Lookup” which maps to 0 and is the old way of SIP translations.

“Inter-Domain Routing” which maps to 1 and eliminates the need for the fake gateways.

102.5.10 ERL Provisioning

ERL provisioning required a gateway to be selected. This is changed to now select a node/ logical entity when creating an ERL.

Figure 24: ERL Provisioning



The OPI interface does not get affected as the existing methods and data objects would work and hence the change is backward comptabile.

The following OPI methods would now contain the node/ logical entity names instead of the gateway route names.

- public void addErl(String domain_name, String location_name, ErlInfo erlInfo) throws ProvisionException;
- public void modifyErl(String domain_name, String location_name, ErlInfo erlInfo) throws ProvisionException;
- public ErlInfo getErl(String domain_name, String location_name) throws ProvisionException;

102.5.11 Net6 IP Address

When creating a Service Package, Net6 service requires the operator to enter the IP address of the Net 6 box. Since this is a 3rd party box and would not be Re-IPed, this is not converted as part of the Re-IP feature.

102.6 Dependencies

NA

102.7 Faults

102.7.1 Logs and Alarms

A new alarm and log are added as part of this feature.

102.7.1.1 IPAddress change Log

Explanation

This log is generated when IPAddress is changed from Management Console. The details of the log are as follows:

Short Name: ADDR

Long Name: ADDRESS

Description: <<Logical Name>> IPAddress changed from <<OldIPAddress>> to <<NewIPAddress>>

102.7.1.2 Alarm

A new alarm is added as part of this feature. This alarm is raised when the service address of SM is changed from Management Console. The details of the alarm are as follows:

```
AlarmName: SM Service Address change

FaultNumber: 801

ShortFamilyName: SVCA

LongFamilyName: SMSVCADR

Severity: CRITICAL

ProbableCause: information modification detected

Description: System Manager service address changed

Corrective Action: Redeploy System Manager
```

102.8 Restrictions and Limitations

1. Solaris and RTP Media Portal only. 2K, MAS (Windows platform not supported).
2. Individual Server Re-IP required on each server. No central site.
3. No GUI for changing the server Re-IP.
4. This feature does not include any notification to the clients (PCC, Web or i200x phones) about the IP address change. Therefore after the change the clients will have to re-connect to their respective servers.

It is expected that this kind of activity will be done in a maintenance window and it is the Service Providers responsibility to inform the users of the outage if any.

102.9 References

102.9.1 Other References

[1] Sun Docs - http://docs.sun.com/

102.10 Definitions & Abbreviations

CD	Compact Disk
GUI	Graphical User Interface
IP	Internet Protocol
IPCM	IP Client Manager
MAS	Media Application Server
MCP	Multimedia Communication Platform
OAM&P	Operational, Administration, Management & Provisioning
SIP	Session Initiation Protocol
SMDI	Simplified Message Desk Interface

103: Functional Description (FN): A00009831

103.1 Feature name and Feature ID

A00009831 - Patching

103.2 Description

103.2.1 Background

The delivery of emergency maintenance releases (EMRs) for the MCS product currently require tier 1 support groups to redistribute an entirely new load to the customer site. Since MCS 9.0 load sizes generally exceed 120MB, electronic distribution of the EMR can be delayed in situations where a high speed connection to the site is unavailable.

This feature provides the limited ability to create and deliver an EMR that represents a delta of the changes between the general release and the maintenance release. It is estimated that a typical “delta” EMR will be less than 3MB, and it can be transferred to a customer site over 56K dial-up in 10 minutes or less.

For the remainder of this document, the concept of an Emergency Maintenance Release "delta" is simply referred to as a “patch”.

103.2.2 Overview

This feature introduces a patch application utility that analyzes a delivered patch and applies it to the appropriate load for redeployment in the normal manner.

The following MCS patch capabilities are provided:

- Back-end (proprietary) tools are created to build a patch for a general load release. These are Nortel tools, and they are not delivered to the customer.
- A System Manager (SM) command line script is created to apply a delivered patch. The patch application script is a supplement to the other SM installation and deployment tools.

- A SM command line script is created to remove an applied patch. The patch removal script is a supplement to the other SM installation and deployment tools.

103.2.2.1 Cumulative Patch Content

Patches provided by this feature have cumulative content. This means that the content from all previously released patches are included in any newly released patch. For example, consider the following series of releases:

Initial Release (Maintenance Release 0): MCP_9.0.0.0

Patch 1: MCP_9.0.0.1

Updates the content of release MCP_9.0.0.0.

Patch 2: MCP_9.0.0.2

Includes and updates the content of patch MCP_9.0.0.1.

Maintenance Release: MCP_9.0.1.0

Updates the content of the initial release, and it includes the content of patches MCP_9.0.0.1 and MCP_9.0.0.2. The patch count is reset to zero.

Patch 1: MCP_9.0.1.1

Updates the content of maintenance release MCP_9.0.1.0.

...

Cumulative patch content is an important concept to remember when a new patch is applied or when an applied patch is removed. Applying a patch applies all content accumulated by all patches since the last maintenance release. Removing a patch removes all content accumulated by all patches since the last maintenance release.

103.2.3 Patch Generator

A patch generation tool is created by this feature. The patch generation tool is responsible for identifying the differences introduced by an emergency maintenance release and for bundling them into a compressed archive. The archive is made available to GNPS and Channel Management teams for delivery to the customer.

The patch generation tool is Nortel proprietary, and it does not represent a customer deliverable.

103.2.3.1 Capabilities

The generation tool is capable of creating a cumulative patch for any release of software against any base load. The content of a patch is not dependent on the physical name of the patch file, so GNPS and Channel Management are free to assign any naming convention that is relevant to the software delivery mechanism.

For this feature, the generation tool can only create patches for the Java-based components of the MCS product. Refer to “Limitations and Restrictions” on page 1034 for further information about patch generation capabilities.

103.2.3.2 Patch Content

A patch contains two types of data:

1. **Load Content**
   This represents Java byte code content of the MCS software. Only load content that has been added or modified is included in the patch.
2. **Meta Data**
   This represents any data that describes information about the patch context or contents. Meta data enables accurate unbundling and application of the patch.

Patch meta data includes (but is not limited to) the following critical pieces of data:

- **Patch Load Name**
  This meta data element identifies the release name of the patch.
- **Patch Base Load**
  The patch base load refers to the load updated by the patch.
- **Added File List**
  The added file list data element provides a listing of all files added by the patch (with checksum information).
- **Modified File List**
  A listing of all files modified by the patch (with checksum information) is provided by the modified file list element.
- **Legal README**
  This meta data defines legal information applicable to the patch. The content of this text is defined by GNPS, and its definition is outside the scope of this feature.
- **Patch README**
  This meta data defines installation information applicable to the patch. This might include identification about the network elements affected by the patch, special application procedures, or appropriate warnings. The content of this text is defined by GNPS, and its definition is outside the scope of this feature.

103.2.3.3 Patch Size

The goal of the generation tool is to create a compact patch file, but the nature of a maintenance release may necessitate that a patch file exceed the recommended 3MB maximum size. To better adapt to customer requirements, this feature does not restrict the size of a patch, and such considerations are left to the GNPS and Channel Management teams.

103.2.4 Patch Application

To apply a patch, this feature introduces a '`mcspatch.pl`' script that can be executed from the operating system command line of the SM.

103.2.4.1 Script Actions

The following actions are performed by the `mcspatch.pl` script:

1. Open the patch archive file and read the meta-data.
2. Present the user with the legal README text.
3. Provide the user with the opportunity to read the included installation README information.
4. Make sure the patch base load is installed. If not, patch application is aborted. The name of the base load is taken from the meta data.
5. Provide a brief summary and confirm the user's intent to install the patch. The summary includes:
   - patch creation date
   - base load name
   - patch load name
   - number of files added
   - number of files modified
6. Apply the patch to the base load. Existing patches are preserved in case the user requests removal ("back-out").
7. Present the user with the installation information.

Encountered errors abort application with an error-specific message and return code. Once applied, the patched load can be redeployed at the discretion of the administrator.

103.2.4.2 Command Line Syntax

The `mcspatch.pl` command line has the following GNU-style command syntax:

```
Usage: mcspatch [-qv] [--no-prompt] [--readme-legal]
             [--readme-patch] [--load-dir=dir] [--log=file]
             <patch-file>

Applies the patch identified by the <patch-file> argument.

Arguments:

   <patch-file>
      The patch to apply.

Options:
   --load-dir=dir
      Specifically defines the directory where the base load
      resides.  This option supports non-standard
installations
      where the name of the base load directory does not match
      the name of the base load itself.

   --log=file
      Indicates the log file used to record patch application
      output.  By default, the log file is
      /var/mcp/install/logs/mcspatch.<time> where <time> is
      replaced by HH-MM-SS.

   --no-prompt
      Apply the patch without prompting for confirmation.
      This option assumes acceptance of legal terms and no
      interest in reading the patch information before the
      patch is applied.

   -q
     Minimize standard output.  Complete information is still
      preserved in the log file.

   --readme-legal
      Displays the legal information and exits.  No patch is
      applied.

   --readme-patch
      Displays the patch information and exits.  No patch is
      applied.

   -v
      Maximize standard output.

   --version
      Displays version information and exits.  No other action
      is taken.
```

103.2.4.3 Example

The following is a simple patch application example:

```
 $ mcspatch.pl MCP_9.0.0.1.jar
```

103.2.4.4 Deployment

Once applied, the patched load is not automatically realized by components of the MCS system. For the patch to become active, the patched load must be re-deployed to all MCS components that require it. Load deployment is not covered by this document.

Since patch application is not incremental, only one patch can be applied at any given time. When a new patch is applied, the existing patch (if one exists) is replaced.

103.2.5 Patch Removal

To remove a patch, this feature introduces a '`mcsunpatch.pl`' script that can be executed from the operating system command line of the SM.

103.2.5.1 Script Actions

The following actions are performed by the `mcsunpatch.pl` script:

1. Determine if the specified load is patched. If not, abort execution.
2. Read the patch meta-data.
3. Provide a brief summary and confirm the user's intent to remove the patch. The summary includes:
   - patch creation date
   - base load name
   - patch load name
   - number of files added
   - number of files modified
4. Remove the patch from the base load.

103.2.5.2 Command Line Syntax

The `mcsunpatch.pl` command line has the following GNU-style command syntax:

```
Usage: mcsunpatch [-qv] [--no-prompt] [--load-dir=dir]
             [--log=file] <patch-name>

Removes the patch identified by the <patch-name> argument.

Arguments:

   <patch-name>
      The name of the patch to remove.

Options:
   --load-dir=dir
      Specifically defines the directory where the base load
      resides.  This option supports non-standard
installations
      where the name of the base load directory does not match
      the name of the base load itself.

   --log=file
      Indicates the log file used to record patch application
      output.  By default, the log file is
      /var/mcp/install/logs/mcsunpatch.<time> where <time> is
      replaced by HH-MM-SS.

   --no-prompt
      Remove the patch without prompting for confirmation.

   -q
      Minimize standard output  Complete information is still
      preserved in the log file.

   -v
      Maximize standard output.

   --version
      Displays version information and exits.  No other action
      is taken.
```

103.2.5.3 Example

The following is a simple patch removal example:

```
 $ mcsunpatch.pl MCP_9.0.0.1.jar
```

103.2.5.4 Deployment

Once a patch is removed, the base load returns to an unpatched state. This change is not automatically realized by components of the MCS system. To revert, the base load must be re-deployed to all MCS components that require it. Load deployment is not covered by this document.

103.2.6 Backing-out a Patch

No scripts are provided to specifically “back-out” a patch. Instead, patch back-out can be accomplished via one of two mechanisms:

1. Remove the existing patch and return the base load to an unpatched state.
2. Reapply a previously applied patch (the current patch will be overwritten).

Once backed-out, the load must be re-deployed to all MCS components that require it. Load deployment is not covered by this document.

103.3 Hardware Requirements or Dependencies

This feature does not require any hardware that is outside the scope of existing hardware platform requirements.

103.4 Software Requirements or Dependencies

This feature does not require any software that is outside the scope of existing installation and commissioning platform requirements.

103.5 Limitations and Restrictions

103.5.1 Patchable Components

This feature provides patch generation capabilities for most MCS Network Elements (NEs) running Java byte codes that can be deployed from the management console (or operating system command line) of the SM. Specifically:

- System Managers
- Fault-Performance Managers
- Accounting Managers
- Session Managers
- Provisioning Managers (except for Java Servlet Pages)
- IP Client Managers
- H.323 Gatekeepers
- RTP Portal / BladeCenter / Media Portal (Java component only)

Any component not specifically identified as “patchable” should be considered “non-patchable”.

103.5.2 Non-Patchable Components

The feature does not provide patch generation capabilities for the following MCS components:

- System Manager Console
- Media Application Server (MAS)
- Nortel Media Gateway 3200 (AudioCodes PRI Gateway)
- Provisioning Manager Java Servlet Pages
- Non-Java RTP Portal components
- Java Native Interface components
- All components provided by Installation & Commissioning.
- All operating system components.

Any component not specifically identified as “patchable” should be considered “non-patchable”.

103.5.3 Patch Applicator

The patch applicator script provided by this feature is designed to complement the installation and deployment scripts associated with the MCS SM. The patch application script is not intended for use as a standalone component. The application script provided by this feature is capable of running on any operating system where a MCS SM can be installed and deployed.

EMR application via the patching capabilities introduced by this feature is not necessarily consistent with other EMR application mechanisms.
The EMR application for all deployable MCS NEs is unified by this feature.

103.5.4 Custom Feature Delivery

This feature provides a mechanism for deploying an EMR to the customer site. It is not designed as a mechanism for interim release feature delivery (sometimes referred to as, "fast feature development"), and such use is not supported.

103.5.5 Data Schema Changes

This feature does not provide a mechanism to patch data schema or upgrade the customer database.

103.5.6 Maintenance Releases

The patching functionality provided by this feature is not a substitute for periodic maintenance releases. Furthermore, maintenance releases contain all patch content since the last maintenance release.

103.5.7 Patch Delivery

While this feature does not assume a specific patch delivery mechanism, continuation of the existing mechanisms is planned for MCS09. These mechanisms include:

- CDs
- ESDs (Electronic Software Delivery)

103.6 Interactions

N/A

103.7 Glossary

Term	Description
EMR	Emergency Maintenance Release (i.e. a “patch”)
GNPS	Global Nortel Product Support
MCS	Multimedia Communications System
NE	Network Element
RPS	Regional Patch Selector
SM	System Manager

104: Functional Description(FN): A00009838

104.1 Feature name and Feature ID

Removal of DCE from default install and install wizards - A00009838

104.2 Description

DCE and DCE dependant applications on the SDM are being "MDed" in the SDM22/SN09 release. The DCE software will continued to be delivered with the CS2E00090 and CS2E00100 loads. The DCE Applications will be removed from the load as of the SDM24/SN11 release.

DCE will be removed from the list of commissioning tasks.

DCE software will be part of the SDM load and DCE user interfaces (‘sdmmtc->dce’ level) will still remain available to support existing DCE users. A note mentioning the DCE Manufacturing Discontinued will be displayed on the DCE user interface ().

```
    SDM     CON    512    NET    APPL   SYS     HW    CLLI: SNM1
     .       .     . .     .       .     .       .    Host: wcary2p3
                   . .                                Fault Tolerant
DCE
 0 Quit       DCE State: .
 2           Components: rpc sec_cl cds_cl dts_cl
 3            Cell name: sdm.dce.net                    Profile: lan-profile
 4 Logs      Created by: cell_admin                     Min DTS servers: 1
 5           Alarming DCE server failures - Master: Y   Replica: N
 6
 7           ****************************************************
 8           *                  Note !!!!                       *
 9           *                                                  *
10           *   DCE will be MDed on SDM in the SDM24/SN11      *
11           *                    release.                      *
12           ****************************************************
13
14
15
16
17 Help
18 Refresh
  root
Time  07:56  >
```

Figure 1 DCE User Interface with the new note

104.3 Hardware Requirements or Dependencies

No new hardware dependencies introduced by this feature.

104.4 Software Requirements or Dependencies

None

104.5 Limitations and restrictions

None.

104.6 Interactions

None.

104.7 Glossary

Term	Description
SDM	SuperNode Data Manager
DCE	Distributed Computing Environment

105: Functional Description(FN): A00009839

105.1 Feature name and Feature ID

Ability to apply patches during ESUP upgrade - A00009839

105.2 Description

To equip ESUP with patching capabilities. There are three requirements for this feature. They are as follows:

- ESUP should be able to read and apply ".patch" files.
- ESUP should support patching along with regular upgrades.
- ESUP should also have an option of "patch only" upgrade, wherein user should be able to apply only patches (and not any other files).

Format for patch files has changed from SDM20. Prior to SDM20, the patch files used to be in IBM "bff" format with ".tape" as extension. From SDM20, after creating the patches they are tarred and zipped (gzip). The resulting patch files has an extension of ".patch".

105.3 Hardware Requirements or Dependencies

No new hardware dependencies has been introduced by this feature.

105.4 Software Requirements or Dependencies

With this feature ESUP will use the NTSimTool package to convert ".patch" files to ".tape" files.

105.5 Limitations and restrictions

None

105.6 Interactions

This feature brings some changes in user interactions. Please see the configuration section of this document.

105.7 Glossary

Term	Description
SDM	SuperNode Data Manager
ESUP	Enhanced SDM UPgrade

106: Functional Description(FN): A00009840

106.1 Feature name and Feature ID

CBM IPSec Northbound Interface : A00009840

106.2 Description

This activity provides an easy-to-use IPSec configuration interface on the CBM for configuring IPSec/IKE parameters. This would be bundled as part of CLI tool of SSPFS for all SSPFS profiles.

This interface can be accessed only by the root user. No other users will be allowed to use this IPSec/IKE configuration interface.

This interface would accept user input values for various parameters related to the IPSec and IKE configurations. This interface will only support IPSec with IKE in preshared mode. No manual keying or certificate-based authentication will be supported by this CLI.

Following are the capabilities provided by the IPSec/IKE configuration interface

- Supports the option to save or edit changes
- Supports capability to abort configuration interface at any point of time
- All the configuration information would be automatically synchronized over to the mate system.
- This interface would generate configuration information for configuring IPSec on the downstream (for Solaris box). This information would be made available on the CBM in the /etc/inet/remotesystem/solaris directory as static file. The downstream would require to be manually modified to reflect this configuration information.[1] A sample downstream configuration file which would be generated by this interface is documented in the Appendix section of this document.

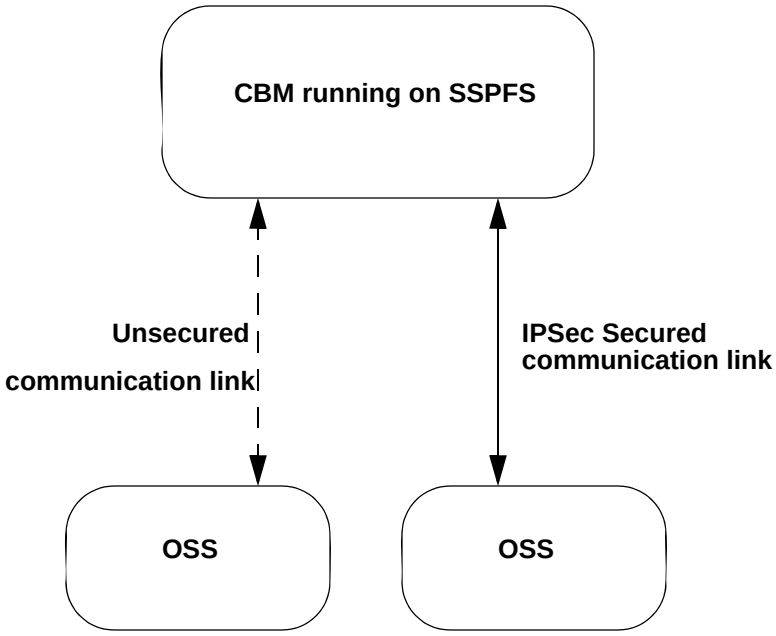
Details about the different parameters, valid options which would be accepted by each of these parameters and the configuration interfaces (snapshots) with examples have been documented in the CN section of this activity.

Figure 1 indicates a broad picture on the secure and unsecured communication between the CBM and the OSS. If IPSec communication is enabled between the OSS and the CBM, then the communication channel would be secure.

[1]**Warning :** This static file contains confidential information (related to the preshared key) and should be removed from the machine once its no longer needed.

Note: IPSec is used to provide additional security between OSS and CBM and is not meant to replace the use of standard secure protocols such as SSH, SFTP or HTTPS.

Figure 1 : Functional Layout



106.3 Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced by this feature

106.4 Software Requirements or Dependencies

SN09 or later SSPFS load (with NTIpSec package) for the CBM.

The OSS should support IPSec for secure communication.

106.5 Limitations and restrictions

This activity only supports IPSec in Transport Mode.

IPSec Tunnel mode configuration would not be supported as part of this activity.

106.5.1 Security

For secure communication, all security parameters provisioned on the OSS must match with security parameters provisioned on the CBM.

106.5.2 IP Addresses

Only IPv4 (32 bit) addresses will be supported

106.5.3 Keys

Only Preshared keys would be used for IKE communication.

106.5.4 Test Strategy

- The OSS which would be tested in this activity would be a solaris 9 machine.

106.5.5 HA system key negotiation

IPSec or IKE SA's will not be replicated on HA CBM's. There would be loss of communication for inbound connections (from OSS to CBM) post CBM fail-over, until the existing IPSec SA's expire and IPSec SA's get re-negotiated.

This issue could become prevelant again if the OSS is an HA platform and it fails over.

106.6 IPSec Precedence Order

When there are numerous IPSec policy entries in the IPSec configuration file, the system could resort to reordering of the policy entries or attach precedence to some rules defined in the IPSec configuration files. This can happen in the following conditions.

If the new policy entry has been defined with action bypass ("action" attribute can take in values drop, ipsec and bypass), then this entry would be attached the highest precedence. If there are more than one bypass entries, the system would match all the bypass entries before matching any other entries.

If there are IPSec configuration entries with matching entries for the input and output datagrams, then the first such kind of a match would be taken.

In case of matching entries for input and output datagrams, the policy entries would be reordered (adding the new entry before the old entry) if the new policy entry has a higher level of protection strength than the old entry.

The strength of the policy entries would be defined as

AH and ESP > ESP > AH

Entries with both the AH and ESP present in the policy entry would be ordered before entries with AH-only and ESP-only entries.

For other entries, the order specified by the user would not be modified, newer entries are added at the end of all the old entries.

A new entry is considered duplicate of the old entry if an old entry matches the same traffic pattern as the new entry.

106.7 Interactions

None

106.8 Glossary

Term	Description
AH	Authentication Header
CBM	Core and Billing Manager
CLI	Command Line Interface (config tool on SSPFS)
ESP	Encapsulated Security Payload
IP	Internet Protocol
IPSec	Internet Protocol Security
IKE	Internet Key Exchange
IPv4	Internet Protocol Version 4
OSS	Operations Support System
SA	Security Association
SSPFS	Succession Server Platform Foundation Software
SSH	Secure Shell
SFTP	Secure File Transfer Protocol

106.9 Appendix A for A00009840

This interface would generate configuration information for configuring IPSec on the downstream (for Solaris box). This information would be made available on the CBM in the /etc/inet/remotesystem/solaris directory as static file. The downstream would require to be manually modified to reflect this configuration information. Following section provides snippets of downstream configuration files.

106.9.1 Sample IPSec downstream configuration file (downstream.ipsec)

The following new rule should be added into the ipsecinit.conf file on the downstream in the similar format. This file is available in the directory /etc/inet and this instruction is applicable only for a solaris (sspfs) box

{ laddr 47.135.214.62 raddr 47.135.214.130 dir both } ipsec { encr_auth_algs sha1 encr_algs 3des auth_algs sha1 }

106.9.2 Sample IKE downstream configuration file (downstream.ike)

The following rule below needs to be added into IKE config file on the downstream in the similar format. This file is available in the directory /etc/inet/ike and the file to be updated with the below changes is config. This instruction is applicable only for a solaris (sspfs) box.

{

label Newrule

remote_addr 47.135.214.130

local_addr 47.135.214.62

p2_pfs 2

p2_lifetime_secs 400

p1_xform { oakley_group 2 auth_method preshared encr_alg 3des auth_alg sha1 p1_lifetime_secs 400 }

}

The following key information should be updated on the file ike.preshared in the directory /etc/inet/secret on the downstream. This instruction is applicable only for a solaris (sspfs) box. This key information should be matching with the above added IKE rule

{

localidtype IP

localid 47.135.214.62

remoteidtype IP

remoteid 47.135.214.130

key 12333895734895abc23489237489723

}

107: Functional Description(FN): A00009865

107.1 Feature name and Feature ID

A00009865: Add MCP820 supporting on SAM21 EM SN09 release

107.2 Description

107.2.1 Feature Functionality

In the SN09 release, there will be a new kind SC card (i.e. MCP820) introduced into SAM21 shelf. MCP820 card is a Motorola card with 512M memory. Since the load image files for each type card are different, each build of SC load RPM in SN09 release will include two image files, one for each.

This feature includes the upgrade job on the SAM21 EM side. Currently, EM only supports one kind of SC and selecting one image file during the provision. and memory requirements definition for the applications.

107.2.1.1 MCP 820 card function list

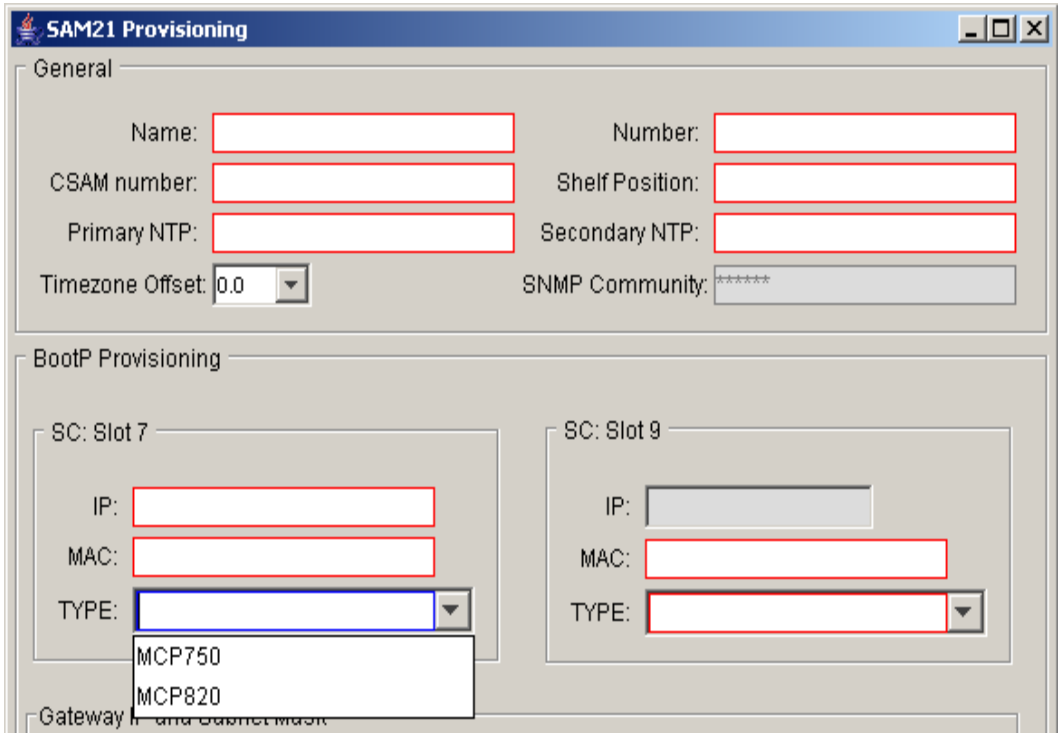
Table 1 MCP820 memory/funtion list

Card Type	Memory Size	Function
MCP820	512M	SC

107.2.1.2 Provision/Re-provision a shelf

In SN09 release, there are two drop list added for each SC card type selection in the provision window.When provisioning or re-provisioning a shelf, the User needs to choose the right type for each slot and can not leave it blank. The look of shelf provision window is shown in Picture 1:

Picture 1: the new look of shelf provision window



107.2.1.3 The change of SC bootp entry in the /etc/bootptab file

There are two bootp entries for two SC cards in the /etc/bootptab file. SC will find the entry when it boots from the network. In SN08 and before version, the value of “bf” item, boot file name, will keep the same as the SC load version for these two entries. In SN09 release, the value will be different if the SC card type is not the samd. For a MCP750 card, the value of “bf” will keep same as SC load version; for a MCP820 (or other type SC card introduced in the future) card, the value will be “SCLoadVersion.CardType”. The sample shows below:

47.142.114.238 stands for a MCP750 card, and 47.142.114.239 stands for a MCP820 card.

47.142.114.238:\

bf=12.0.0.0410071440:\

gw=47.142.114.1:\

hd=/swd/sam21:\

ht=ether:\

ha=0001AF0177CB:\

```
        ip=47.142.114.238:\
        sa=47.142.114.248:\
        sm=255.255.255.0:\
        vm=rfc1048:\
        T42=0x2f8ca06f:\
        T134=2f8e72d92558:
47.142.114.239:\
        bf=12.0.0.0410071440.MCP820:\
        gw=47.142.114.1:\
        hd=/swd/sam21:\
        ht=ether:\
        ha=0001AF02D722:\
        ip=47.142.114.239:\
        sa=47.142.114.248:\
        sm=255.255.255.0:\
        vm=rfc1048:\
        T42=0x2f8ca06f:\
        T134=2f8e72d92558:
```

107.3 Hardware Requirements or Dependencies

This feature will support a new shelf controller card model, MCP 820.

107.4 Software Requirements or Dependencies

No new customer software or firmware dependencies are introduced in this feature.

107.5 Limitations and restrictions

No limitations or restrictions that is visible to any user are planned as part of this feature.

107.6 Interactions

N/A

107.7 Glossary

Term	Description
SC	shelf controller

108: Functional Description(FN): A00009890

108.1 Feature name and Feature ID

ACTID A00009890

Provisioning for Media Proxy insertion for SIP lines

108.2 Description

In SN09 SIP lines will be supported on the CS2k via a new component, the Session Server (aka ‘Phoenix’), which is based on re-use of various MCS components. It is necessary to allow SIP Lines to reside in private VPNs, as is already provided for fixed VOIP line gateways and CICM terminals. This is achieved by appropriate Media Proxy insertion by the CS2K. This feature provides the provisioning necessary to support Media Proxy insertion for SIP lines.

During a call, the VPN ID of a SIP line will be determined by the Session Server (via a mapping of ‘Location ID’ to ‘Routability Group’), while the VPN ID of a fixed VOIP/CICM line is determined by the GWC, via SESM provisioned IP-VPN(NAT) Network Zones and ‘Distributed VPNs’. Hence in order to allow correct comparison if the VPN IDs at the two ends of a call and Media Proxy insertion if required, the VPN IDs in GWC and Session Server must be consistent. This feature ensures that both the GWC and the Session Server have the same VPN ID information to allow the correct insertion of Media Proxies, by flow-through provisioning of IP-VPN(NAT) network zones and Distributed VPNs from SESM to the Session Server.

Data synchronisation is managed by the CS2K Audit, for cases in which the SESM and Session Server data are inconsistent and for commissioning support.

Example flow-through case: To create a IP-VPN(NAT) Zone.

- Use the SESM GUI to add a new IP-VPN(NAT) Zone named “maidenhead.com”.
- If a Session Server(MCS-EM) is configured into the SESM an add Routability Group request is sent to the Session Server via the OPI interface.
- On a successful response from the Session Server, the SESM will allow the IP-VPN(NAT) Zone to be created and displayed to the user.

Related activities are:

- ACTID xxxxx MP insertion for SIP lines OPI changes on Session Server(MCS-EM)
- SN09 feature A00008522, SESM Support for SIP Lines, which implements the SIP Proxy on SESM
- SN09 feature A00007217, OAM-Itrans Media Proxy Selection

Hardware Requirements or Dependencies

Not applicable

108.3 Software Requirements or Dependencies

Session Server OPI version 9.0 software (OPI version allows Routability Group ID's)

108.4 Limitations and restrictions

Multiple CS2M Configuration managers should not connect to a single Session Server(MCS-EM). The result of this would mean that a shared IP-VPN(NAT) Zone would not be allowed to be provisioned into the 2nd to nth CS2M Configuration managers and hence omit the 2nd...nth CS2Ks from having gateways/endpoints provisioned within the shared IP-VPN(NAT). This is not a supported configuration for SN09 release.

108.5 Interactions

For customer deployments where a Session Server is introduced into the CS2k for SIP Lines functionality, this feature will enforce data synchronisation between the SESM and Session Server. Where data synchronisation fails, an alarm will be generated to inform the customer.

The existing funtionality of creating a IP-VPN(NAT) Zone and creating a Distributed IP-VPN (NAT) Zone will only succeed if the Session Server accepts the flow-through provisioning data from the SESM.

e.g. If the flow-through provisioning of the IP-VPN (NAT) Zone information to the Session Server fails this will cause the creation of the IP-VPN (NAT) Zone to fail on the SESM.

The existing funtionality of the CS2K data audit, will also attempt to synchronise the data between the SESM and the Session Server.

108.6 Glossary

Term	Description
NAT	Network Address Translation
IP-VPN	Internet Protocol - Virtual Private Network

109: Functional Description(FN): A00009893

109.1 Feature name and Feature ID

Session Server Call Processing Overload

109.2 Description

This feature provides enhancements to the Session Server SIP Gateway Application overload functionality that was introduced by the SN08 feature A00007270, Session Server Call Processing Overload.

A00007270 used an overload detection scheme that was based solely on the depth of two call processing messaging queues - the Generic Control Protocol (GCP) queue used for CS2K-originated calls and the Session Initiation Protocol (SIP) queue used for remote SIP server- originated calls. If either queue was determined to be above its threshold at the end of a sampling period, the application was put into an overload state.

Once the application was in overload, all new incoming calls received from a remote SIP server were rejected. This call rejection continued until the results of a subsequent sample period indicated the queue sizes had decreased below the overload threshold.

A few areas of note regarding SN08 application overload detection:

- The amount of work being done by the CPU (the CPU occupancy) was not a factor in determining whether the application was in overload.
- When the application was in overload, all new remote SIP server calls were rejected. There was no throttling mechanism that would have allowed some new SIP calls to continue to be processed while the application attempted to come out of overload.
- Since only new remote calls were rejected, a server that handled a higher proportion of local originations (i.e., calls from a CS2K) got little or possibly no overload relief using the SN08 overload handling mechanism.

An overview of the new functionality provided by this feature for SN09:

- For **Overload Detection**, CPU occupancy is now a factor in the algorithm for determining overload.
- For **Flow Control**, instead of blocking all new SIP originations during overload, new calls - both CS2K-originated and remote SIP server-originated - will be throttled to allow a certain percentage of both call types to complete.

- **Babbling Node Detection** - Provides the ability to detect and limit the impact of a remote SIP server that is sending an excessive number of bad messages to the Session Server.
- **Overload Monitoring and Fault Management** - New OMs, logs and alarms are created for the purpose of providing information regarding CPU occupancy, queue sizes and percentage of calls that are being rejected.

109.2.1 Overload Detection

For SN09, in addition to getting periodic samples of each of the call processing queue sizes, the CPU occupancy is also checked at the same time. At the end of each sampling period, the SIP Gateway Application is considered to be in overload if at least **one** of the following conditions exists:

- CPU occupancy exceeds its overload threshold
- GCP queue length exceeds its overload threshold
- SIP queue length exceeds its overload threshold

If the application is found to be in overload, a major alarm is generated along with a SIPC310 log (SN08 functionality).

The application can also be in a pending overload state, meaning it is either approaching overload or possibly receeding from an earlier overload condition. Again, the application is considered to be in an overload pending state if at least one of the following condistions exist:

- CPU occupancy exceeds its pending threshold
- GCP queue length exceeds its pending threshold
- SIP queue length exceeds its pending threshold

There are no changes to call processing while in the pending state, unless the application is in the early stages of recovering from overload. In the latter case, some calls may still be getting rejected. This is discussed in more detail in the Flow Control section.

As in SN08, when the application is in pending overload, a minor alarm is generated, along with a SIPC310 log.

109.2.2 Flow control

Once the application has entered the overload state, new call originations are throttled as a means of easing the load on the CPU. The level of throttling is determined by the Flow Control Rate (FCR). FCR is analogous to the percentage of new calls allowed to complete while the application is in this condition. This percentage is applied to both local (CS2K-originated) and remote (SIP-originated) calls. In other words, if the FCR is 90, 90% of new local calls and 90% of new remote calls are allowed, or every 10th call of each type is rejected. Calls in progress are not affected in any way.

When the system goes into overload an initial FCR value is calculated, causing a certain percentage of calls to be rejected. For each subsequent sample period the FCR can fluctuate between 0 (all calls blocked) and 100 (no calls blocked), based on the current overload state.

If conditions improve and a sampling period indicates the application is no longer in overload, the FCR is not immediately returned to 100%. Instead, a gradual increase each period is done to ensure the system does not bounce back into overload.

For call rejection, a Local Release with Cause Value of 42 is sent for GCP originations and a 503 Service Unavailable is sent for SIP originations.

In SN08, when the SIP Gateway application was in overload it responded to a SIP OPTIONS request with a 503 Service Unavailable response. The purpose of this was to indicate to the remote server that the Session Server was no longer accepting any new calls. If the far end reacted appropriately to this reponse, it would stop sending new calls to the overloaded Session Server.

With the changes in this feature that now allows for a certain percentage of calls to complete during overload, the 503 response will no longer be sent in response to an OPTIONS request when the application is in overload.

109.2.3 Babbling Node Detection and Isolation

This component provides the ability to detect and limit the impact of a remote SIP server IP address that is flooding the Session Server with an excessive number of bad syntax messages. Once an IP address is labeled as a babbling node, lower level software intercepts all messages from the node before they reach the application, thereby freeing the application from the time it would have to spend processing each message.

Babbling node detection involves keeping a count of the number of SIP messages with bad syntax received from an IP address. Every 5 seconds, this counter is scanned for each IP address. If the number of new bad messages received from an IP since the last check exceeds the threshold value, the address is removed from service in such a way that no further messages from this IP are processed by the application.

Note that in order to determine the source (the remote SIP server) of a bad syntax message, the Session Server must at a minimum be able to parse the SIP via header. If the via header is too corrupted for parsing, the message will not be counted as a bad syntax message.

Babbling node isolation is implemented by using the Linux iptables functionality. When a node is determined to be babbling it is marked in iptables in such a way that all messages from the IP will be discarded. No responses are sent to the remote node. In the session server, the connection

status of the remote SIP server is marked inactive and all access links mapped to the server are removed from service. Corresponding trunks in the CS2K are put into a SYS state. This effectively disables all incoming and outgoing calls from the server.

After the IP has been disabled for 5 minutes, it's status in the iptables is changed so that its messages are no longer dropped and the associated access links/trunks are brought back into service. The same criteria are again used to detect and isolate the IP if it continues to send an excessive amount of SIP messages with syntax errors.

109.2.4 Overload Monitoring and Fault Management

As a means of providing the ability to monitor overload-related events and statistics, new Operational Measurements, logs and alarms are created by this activity.

A new OM group, SIPGW_OVERLOAD, contains information related to the level of usage for each of the monitored resources (CPU, GCP queue, SIP queue). The following types of registers are in the group:

- CPU occupancy calculation from the latest sampling period
- GCP queue size from the latest sampling period
- Radvision queue size from the latest sampling period
- High water marks for each resource over a 30 minute period. Reset to 0 every 30 minutes.

Below is a sample output of the new OM group SIPGW_OVERLOAD:

```
Active Register Counts
START Thu Feb 10 10:30:00 2005   STOP Thu Feb 10 10:31:44 2005

OMGROUP: SIPGW_OVERLOAD
*****************************************************************

TUPLE KEY: 0            TUPLE KEY NAME:

Register Name                          Value
-------------------------------       ----------
CPU_OCCUPANCY                              45
CPU_OCCUPANCY_HWM                          67
GCP_QUEUE_SIZE                             15
GCP_QUEUE_SIZE_HWM                         29
SIP_QUEUE_SIZE                             25
SIP_QUEUE_SIZE_HWM                         30
*****************************************************************
```

In addition to the OMs, three new STGW700 logs are added to cover various scenarios:

- Changes in the Flow Control Rate. Note that this log can be generated when the application is not in overload, such as when it is still recovering from an earlier overload state.
- When an IP address is either removed from or re-added to the Access Control List as a result of babbling node isolation.
- When a critical, major or minor CPU occupancy level has been reached.

Per existing functionality, a minor alarm is raised when the application is in a pending overload state and a major alarm when in overload. These remain unchanged.

Note the minor and major CPU alarms can be activated even if the application is not in overload.

Here are examples of the new logs:

```
Mar 16 12:46:20 pnc1y0jp sipgwyappln: STGW700 NONE INFO SIPOVLD FCR Change OLD
FCR: 90 NEW FCR: 80

Mar 16 22:58:02 pnc1y0jp sipgwyappln: STGW700 NONE INFO SIPOVLD Babbling node
timeout, RTPFMGC 47.142.123.48 IP enabled

Mar 16 22:58:37 pnc1y0jp sipgwyappln: STGW700 NONE INFO SIPOVLD Babbling node
detected, RTPFMGC 172.16.80.24 IP disabled

Mar 16 22:59:33 pnc1y0jp sipgwyappln: STGW700 NONE INFO SIPOVLD All babbling node
IPs re-enabled due to initialization

Mar 16 12:46:10 pnc1y0jp alarmd: STGW700 CRIT TBL  SIPOVLD NCGL=pnc1y0jp;SIPC CPU
occupancy critical alarm

Mar 16 12:17:42 pnc1y0jp alarmd: STGW700 NONE TBL  SIPOVLD NCGL=pnc1y0jp;SIPC CPU
occupancy major alarm cleared
```

109.3 Hardware Requirements or Dependencies

No new hardware requirements or dependencies.

109.4 Software Requirements or Dependencies

No new software requirements of dependencies.

109.5 Limitations and restrictions

In addition to the normal, 5 minute timeout, disabled babbling nodes are re-enabled in the following situations:

- When Remote SIP Server configuration data is changed in the Session Server.
- When the Session Server is suspended. Upon unsuspension the IP will be enabled.

- When the Session Server switches activity to the other unit.

In order to count the number of bad syntax messages received from a remote SIP server for babbling node detection, the Session Server must be able to parse the SIP via header in the offending message to determine the sender of the message. Without the source IP address, the bad message cannot be counted against a server.

109.6 Interactions

In SN09, the 503 response will no longer be sent in response to an OPTIONS request when the application is in overload.

When Access Control List (ACL) functionality is activated, babbling node message discarding using iptables takes precedence over the ACL iptables setting. In other words, if the ACL iptables setting allows messages from an IP to be received, but the node was found to be babbling, all messages from the IP will be discarded until the babbling node timeout. At that point, the ACL setting determines what to do with messages from the IP.

109.7 Glossary

Term	Description
ACL	**Access Control List** - the list of allowable IP addresses from which the Session Server can receive messages.
FCR	**Flow Control Rate** - the percentage of new call originations allowed while in overload or during the recovery period when the application is coming out of overload.
GCP	**Generic Control Protocol** - call control protocol used between the gateway controller and the session Server.
SIP	**Session Initiation Protocol** - an application-layer protocol for creating, modifying and terminating sessions with one or more participants.

110: Functional Description(FN): A00009905

110.1 Feature name and Feature ID

A00009905 – Private and Public Name and Number Display

110.2 Description

MCS09/SN09 Private and Public Name and Number Display feature is introduced for the MCS platform that allows the MCS to deliver the **Calling** Private or Public Name/Number based on a set of rules***. The Calling Private/ Public Name and Number Display has been common a feature for TDM Centrex Networks where groups can exchange Private Name and Numbers within a group, but provide Public appearance when calling party is outside the Centrex group.***

110.3 Introduction

This feature will introduce the TDM Centrex concepts of Private/Public Name and Number display when SIP domains are involved and when parties from SIP domains are involved with TDM parties that are an extension of the same group. For example, a Centrex group where some of the members reside on the TDM network and some of the members reside in the SIP network. This will allow the calling parties in the SIP Network to deliver Private Name and Number to the TDM group members and provide Public Calling Name and Number to PSTN users. Similarly, the TDM Centrex group can deliver the Private Calling Name and Number to the SIP network users.

The MCS behavior today is that the private name of the MCS subscriber is delivered regardless of where the terminator is located. The private number is delivered to the terminator only when Private Gateway Telephony routes are used.

This feature will also provide a way to restrict direct SIP inter-domain calls. This restriction could be added when users from one domain cannot use "Name Dialing" to reach another user. For example, a user in domain A.com is calling a user in B.com by either using an MCS alias or SIP user ID.

New parameters will be added to the MCS Provisioning System to provision the Public Name and Number.

110.3.1 Feature Activation

Provisioning the public name or number in the domain hierarchy tree activates this feature. Without provisioning a public name against a domain the private name is delivered based on the call scenario. If a public number is not provisioned either against a domain the private number or SIP user ID is delivered based on the call scenario.

110.3.2 MCS Private Call

Within a TDM network a “Private call” is considered a call within a Centrex group where the subscriber’s “Private” name and number are delivered to the called party. This number could be an extension like a 4 or 5 digit number. The equivalent of Centrex group on the MCS system is a domain or sub-domain. Subscribers within an MCS domain or sub-domain can setup translations to deliver the private name and number to their TDM Centrex group, but provide the public appearance to other domains and TDM terminations. Within MCS a call is considered private if the following rules apply and this feature is activated:

1. The originator and terminator of the call are in the same domain hierarchy tree. This is the case where the originator is a known MCS subscriber. The MCS subscriber could be a CD2 or a non-CD2 user.
2. Incoming call party from the Gateway and the terminator are in the same domain hierarchy tree. This is the case where the originator of the Gateway is not known, but the Gateway is using the same domain hierarchy tree as the terminator of the call.

The rules would apply to basic calls, calls that are forwarded or transferred within the MCS or to TDM users.

110.3.3 MCS Public Call

Within the MCS system a “Public call” is a call that is made outside the domain hierarchy boundaries. This could be another domain or Gateway that is reached using public translations. For example, to call a PSTN subscriber a public Gateway route is used for termination and in this case the MCS subscriber’s public name and number will be delivered. The following rules for a Public Call would apply when this feature is activated at the MCS domain level:

1. The originator and terminator are in different hierarchy tree. This includes domains supported by the MCS system and foreign domains located on other systems.
2. Incoming calling party from a Gateway is in a different domain than the terminating domain root tree.

The rules would apply to basic calls, calls that are forward or transferred within the MCS or to TDM users.

110.3.4 MCS Private Calling Name and Number

The “Private” calling name and number assigned to a subscriber are provisioned by the MCS Provisioning Server Administrator. The subscriber’s name is a mandatory field that is provisioned when adding a new subscriber. The first and last names of the subscriber are used to create the private name. A subscriber can only be assigned a single “Private” name.

The “Private” calling number is an optional field that is assigned to the subscriber and is referred to as the “Private Charge ID” for provisioning purpose. This field is used for calling line number display and in some cases for billing purposes. Only a single “Private” calling number can be assigned to a subscriber.

110.3.5 MCS Public Calling Name and Number

On the MCS a “Public” calling name and numbers are NOT assigned to a subscriber, but to domain/sub-domain and are available to subscribers within that domain/sub-domain. Based on the call scenario, the MCS will select the domain’s public name and number on behalf of the calling party. If a domain tree hierarchy is present a sub-domain can use a parent’s public name and number if the following rule applies:

- If a public name is **NOT** provisioned for the sub-domain, the application server checks if there is a public name provisioned for the parent domain. If one exists, public name is delivered for inter-domain and PSTN calls.
- If a public number is **NOT** provisioned for the sub-domain, the application server checks if there is a public number provisioned for the parent domain. If one exists, public number is delivered for inter-domain and PSTN calls.

There is an exception to the rules above when Gateway or SIP Telephony routes are involved. A Gateway or SIP Telephony route can override the call type based on the type of route. A Gateway/SIP Telephony route can be provisioned as a “Private” or “Public” route.

If the public name for an originating domain or sub-domain is provisioned and applied the following changes will be made:

1. Replace the calling party’s display name with the public name.
2. Remove the picture ID of the calling party
3. The connected name display of the originator is removed.

If the public number for and originating domain or sub-domain is provisioned and applied the following changes will be made:

4. The calling party’s number is replaced with the domain public number.
5. The originating client’s SIP User Agent is removed.

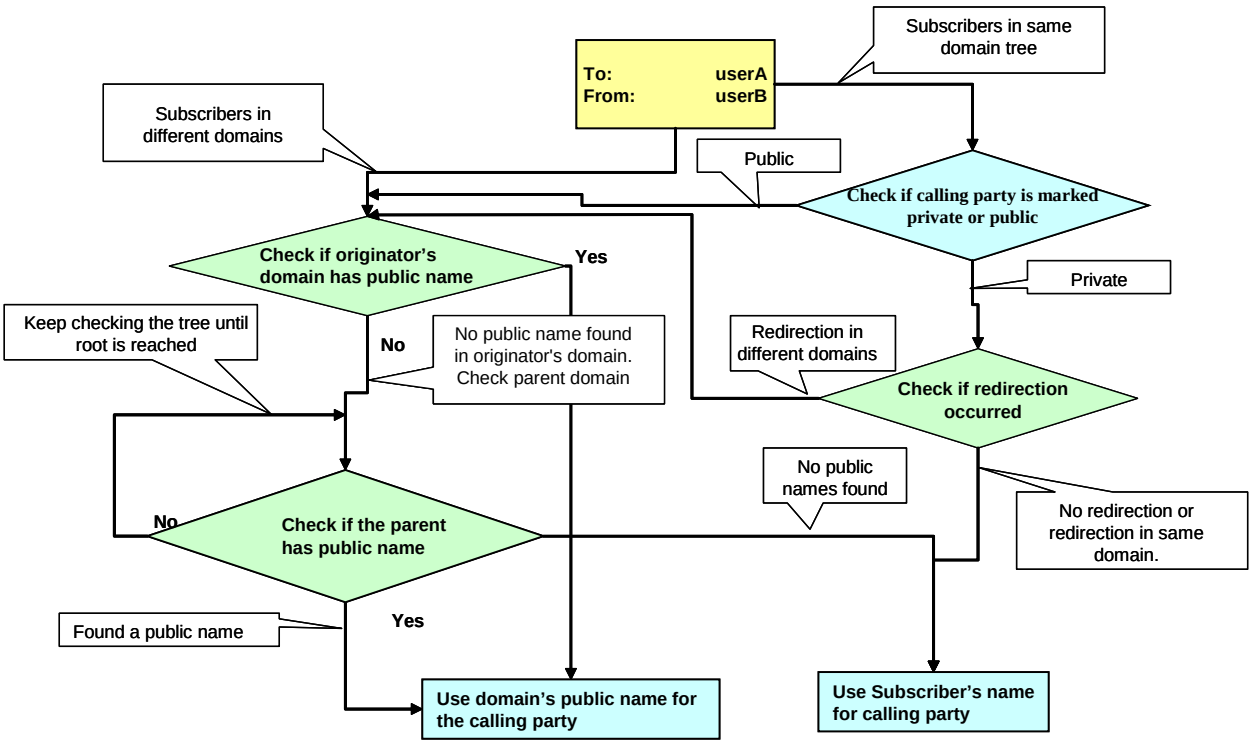
6. The SIP Contact header is replaced with the domain public number

Note: Note: MCS public calling name and number are is applied to intermediate parties when redirection occurs and it only applied to the calling party. One example is when user (A) in domain A calls another user (B) in the same domain and B redirects the call to C in a different domain. In this case Public Name/Number is applied to the calling party (A) only and to the redirecting party (B).

110.3.6 Determining Public/Private name and number

The following diagram provides a high level flow of determining the calling Public/Private name when using SIP User IDs or SIP Aliases to call a user in the same or different domain.

Figure 1 Name lookup for direct SIP inter-domain calls



The following diagram provides a similar flow of when calls are made from a domain to a Gateway.

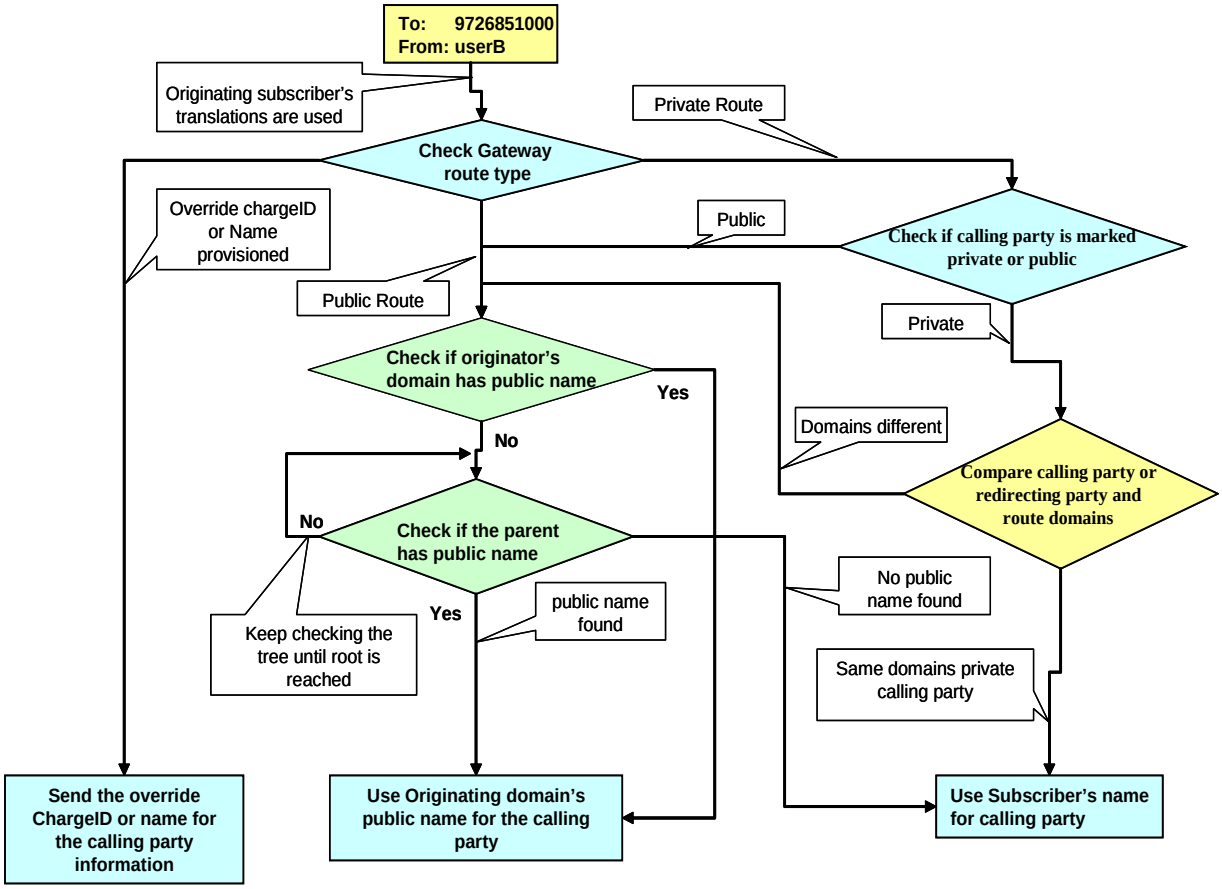


Figure 2 Name lookup Gateway routed calls

Note the both flows only show how the public/private name is found, but the same rules apply to the public/private number as well.

110.3.7 Scenario matrix

110.3.7.1 Direct SIP calls

The following sample call matrix provides the display of name and number or SIP User ID between Non-Converged Desktop calls when this feature is activated. In the Direct SIP calls domain "A" calls between itself and another domain "B". Calling Party for the Gateway scenarios in the columns below show what the call type is tagged as when the MCS receives the call from the Gateway.

#	Calling Party	Called Party	Calling Client Display	Called Client Display
Direct SIP calls				
1	Domain A	Domain A	Private	Private
2	Sub-domain in A	Different Sub-domain in A	Private	Private
3	Domain A	Domain B	Public	Public
4	Sub-domain in A	Sub-domain in B	Public	Public
Outgoing Gateway calls				
6	Domain A	Domain A's Gateway route (Private)	Dialed digits	Private
7	Domain A	Domain A's Gateway route (Public)	Dialed digits	Public
8	Domain A	Domain B's Gateway route (Private)	Dialed digits	Private
9	Domain A	Domain B's Gateway route (Public)	Dialed digits	Public
Tandem Gateway calls				
11	Private	Outgoing Gateway route (Private)	Dialed digits	Private
12	Private	Outgoing Gateway route (Public)	Dialed digits	Public
13	Public	Outgoing Gateway route (Private)	Dialed digits	Public
14	Public	Outgoing Gateway route (Public)	Dialed digits	Public

Figure 3 Calling party display for SIP calls[1]

110.4 Gateway calls

The following matrix provides the Converged Client and Converged Phone displays when using Converged Desktop service with this feature:

[1]The assumption in the table is that both domains have public name and number provisioned.

#	Calling Party	Called Party	Calling PAD Display	Calling Client Display	Called PAD Display	Called Client Display
Complex CD calls						
1	Centrex CD phone	Centrex phone	Dialed digits	No pop up	Private	N/A
2	CD - from PCClient (C2C)	Centrex phone	Calling Party's Private Number.	No pop up	Private	N/A
3	CD - from Centrex phone	CD Centrex phone	Dialed digits	SIP User ID	Private	SIP User ID
4	CD - from PCClient (C2C)	CD Centrex phone	Calling Party's Private Number.	SIP User ID	Private	SIP User ID
5	Centrex	CD Centrex phone	Dialed digits	N/A	Private	Private
6	CD - not in CD mode	Centrex phone	N/A	Dialed Digits	Private	Public Number
7	Centrex	CD - not in CD mode	Dialed digits	N/A	Private	Private
8	PSTN	CD Centrex phone	Dialed digits	N/A	Public	Public
9	CD - from Centrex Phone	PSTN	Dialed digits	N/A	Public	N/A
10	CD - from PCClient (C2C)	PSTN	Calling Party's Private Number.	N/A	Public	N/A
11	CD - not in CD mode	PSTN	Dialed digits	N/A	Public	N/A
Simplex CD calls						
12	CD-Centrex	CD-Centrex	Dialed digits	SIP User ID	Private	SIP User ID
13	Centrex	CD-Centrex	Dialed digits	N/A	Private	Public Number
14	PSTN	CD-Centrex	Dialed digits	N/A	Public	Public

Figure 4 CD client/PAD Display

Notes :

1. CD calls from the PC client assume that click to call is used.
2. Calling PAD Display assumes that the connected name and number are not available.

Note: domain mapping differs on the Gateways supported by MCS. CS2k sends a Nortel proprietary header to map domains to the incoming requests. AudioCodes gateways use direct domain mapping to the MCS domains.

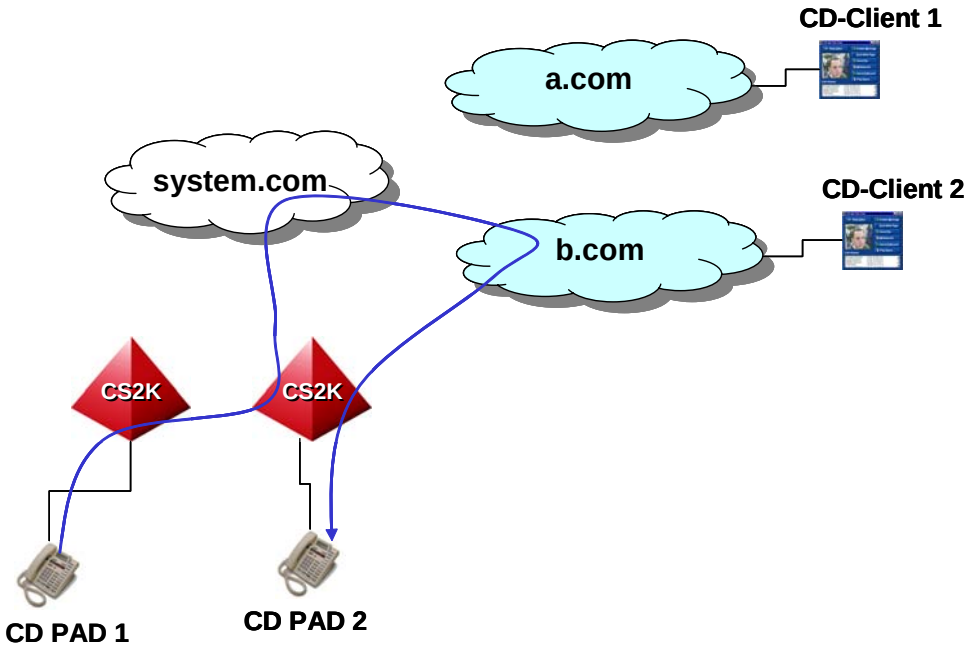
110.4.0.1 Calls that involve multiple domain hops

In some scenarios incoming calls from a Gateway could hop multiple domains before reaching the final destinations. In these scenarios public name and number of the calling party could change based on domain's public name and number provisioning. The following rule applies for changing calling party's name and number for incoming Gateway calls that could route to other domains or Gateways:

1. *Incoming requests from the Gateway look up the public name and number of the calling party only if the calling party is known at the MCS. Converged Desktop 2 is one of scenarios where calling party is known at that MCS.*

2. *If the incoming request traverses a SIP inter-domain or a Gateway route the route can override the calling name and number.*

Since Converged Desktop is the only feature known where PSTN subscribers are also known at the MCS the following example provides a call behavior. The following figure applies rule #1 above in an example of a CD2 subscriber in one domain (a.com) calling another CD2 subscriber in a different domain (b.com). The incoming request from the terminating switch is received in a common domain (system.com) and then forwarded using SIP inter-domain translations to terminating domain (b.com). Since the originator is in a different domain (a.com) than the terminating subscriber, and domain a.com has a public name/number provisioned – domain a.com's public name/number is delivered to CD2 PAD/Client.



If the originator of the call is not known, and the incoming request passes from one domain to another the calling party information is not changed unless the inter-domain routes force a change through provisioning.

110.4.1 MCS Connected name and Picture ID

MCS connected name and picture ID is a feature which provides the originating user the "Display name" and picture ID of the terminating party when the terminating party is ringing or has answered the call. This feature is also available when sending IM and using collaboration. The public name and number provisioning at the terminating domain will change how the connect name and picture ID are displayed to the originating client if the originating client is in a different root domain. If the terminating party has public name provisioned in its domain tree the originating domain will not receive the

connected and picture ID or the terminator. In addition the picture ID will not be available to the originating client if the originator puts the terminator in its personal address book.

110.4.2 Public Name and Number and IM and Collaboration

If public number is provisioned for an originating domain the originating client can send an Instant Message (IM), push a Web Push or start MCS Collaborations. The terminating client is unable to reply to and IM, send Web Push or reply to Collaboration attempt because the identity of the originator is replaced with the public number. The terminating client can send an IM, Web Push to request for Collaboration if the terminating user knows the originator's user ID (e.g. user@domainA.com).

If only public name is provisioned within a domain tree then IM, Web Push and MCS Collaborations between the originator and terminator will continue to work. But the display name and picture ID are removed from the call.

110.4.3 Interactions with Converged Desktop (CD)

In a Converged Desktop configuration Voice could be provided by Centrex group lines from a TDM switch, but multi-media and advance routing capabilities to the user are provided by the MCS system. In some of the Converged Desktop scenarios calls can route through the MCS before terminating to a Centrex line. To preserve the Public/Private name and number in the call this feature will add additional field to provision the CD Preferred Audio Device (PAD) for incoming private calls. The existing field used to provision the PAD number will default for accessing the PAD when incoming Public calls are received.

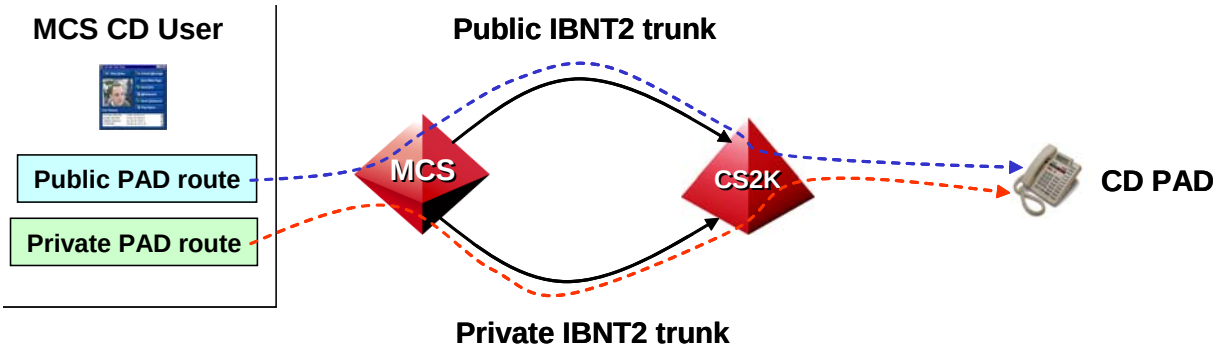


Figure 5 Converged Desktop PAD's public and private routes

The rules for selecting the public or private PAD number provisioned at the MCS are as follows:

Table 1 Rules for using the Private or Public number

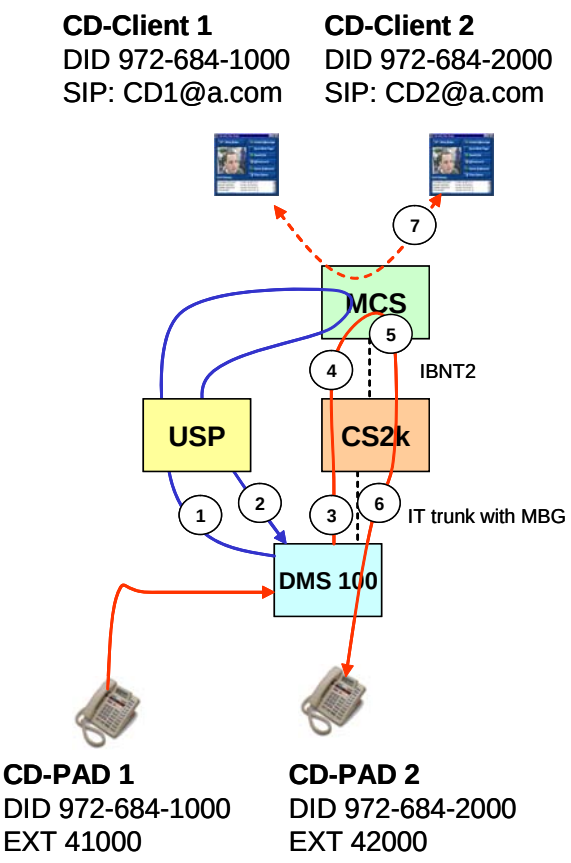
Private PAD Number is used when
1. Originator and terminator are in the same root domain. Originator could be another PC Client or a CD2 user. 2. Originator and terminator are in different domains, but the public name or number for the originator is NOT provisioned. 3. Public PAD number is not provisioned.
Public PAD number used when
1. Originator and terminator are in different domains and the originator has a public name or number provisioned. 2. Incoming subscriber is not known at the MCS. 3. Private PAD number is not provisioned.

The next diagram shows a complex CD call where call traverses the MCS before terminating to a CD PAD. The sample is based on Centrex groups located on a DMS switch instead of the CS2k and MBG protocol is used between the CS2k and DMS to route Private name and number. After Terminating Attempt Trigger response is complete the CS2K routes the call MCS over IBNT2 trunk using the CD Service Provisioned on the MCS. The CS2K marks this call as private because MBG was involved between the CS2k and DMS switch. In Step 5 since the incoming call was marked private the MCS selects the “Private” PAD number assigned to the terminator to perform translations and route lookup. The “Private” PAD number should be provisioned so that a private Gateway route is used to terminate back to the CS2k (step 5) for incoming private calls. The same private route will be used if a PC Client that is in the sub-domain calls this CD user. Similarly, a public PAD number should be provisioned to route incoming public calls.

Normally, when a Converged Client makes a call from the PC Client the first leg of the call will always take the Private GW route because the originator’s CD client and the originator’s PAD are provisioned to use the same domain. After the originator answers its PAD and the terminating call will be determined where if the terminator is located in the same domain as the originator.

If a private PAD number is not provisioned the public route will always be used.

Restriction/Limitation: the MCS CD clients will display the calling/called numbers provided by the CS2k. No reverse translations are performed at the MCS for number display.



1. TAT Trigger
   Calling Number: 972-684-1000
   Called Number: 972-684-2000

2. Forward Response
   Forwarded Number: 972684000(CD Service DN)

3. Calling Display Name: CDPad1
   Calling Display Number: 9726841000
   Called Number: 972684000(CD Service DN)
   OCN: 9726842000
   MGB Centrex group ID: 1

4. Calling Display Name: CDPad1
   Calling Display Number: 9726841000
   Called Number: 972684000(CD Service DN)
   OCN: 9726842000
   NT-ServiceProfile: Group1

5. Calling Display Name: CDPad1
   Calling Display Number: 9726841000
   Called Number: 9726842000
   OCN: 9726842000
   NT-ServiceProfile: Group1

6. Calling Display Name: CDPad1
   Calling Display Number: 9726841000
   Called Number: 9726842000
   OCN: 9726842000
   MGB Centrex group ID: 1
   (another TAT query occurs here, but not shown)

7. Calling Display Name: CDPad1
   Calling Display Number: 972684100@a.com
   Called Display Name: CDPad2
   Called Number: 972684200@a.com

Figure 6 Converged Desktop Complex call

110.4.4 Interactions with Call Forward

Call forward scenarios include calls that are received from a PC Client or incoming from a Gateway that get routed to other domains or Gateways. The following figure shows the various scenarios and behavior of the private/ public name and number display.

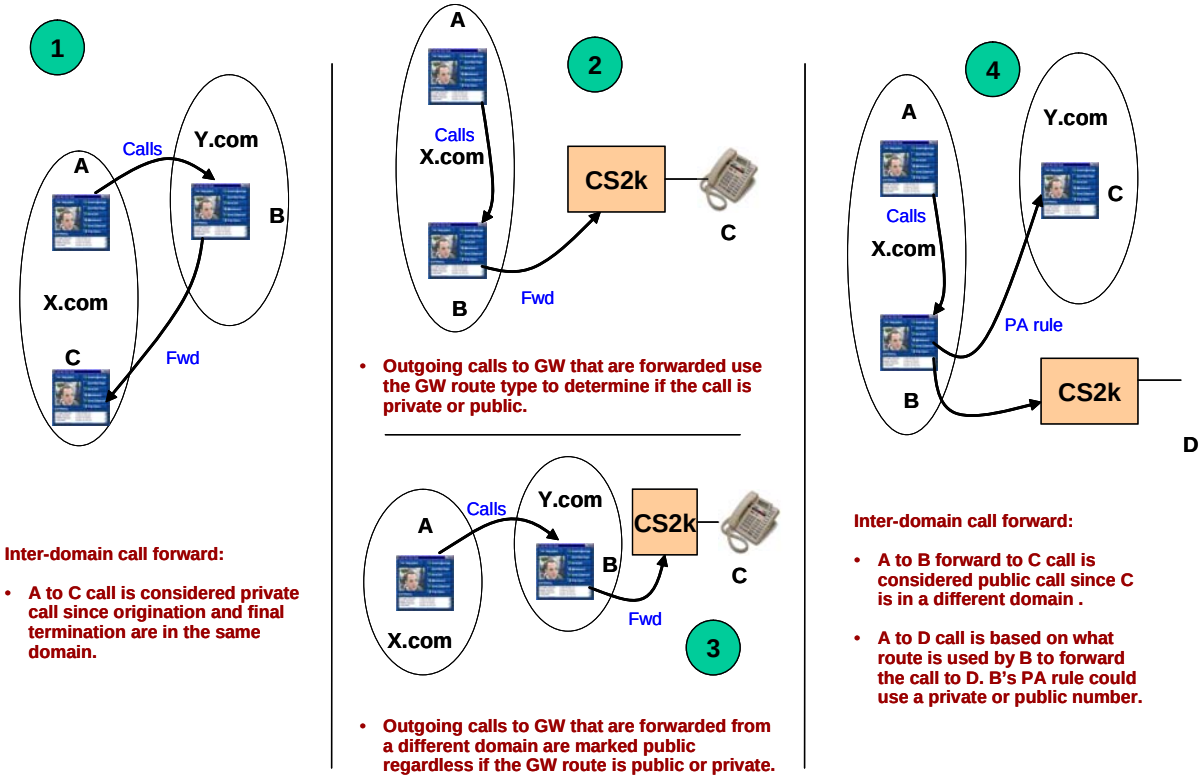


Figure 7 Call forward scenarios

Basically if the originator and terminator are in the same root domain then the call is considered private. The same rules will apply when A is transferred between domains and Gateways.

Public Name and Number is also applied to intermediate parties that involved in the redirection. For example, in scenario number 3 if domain Y.com has public name/number provisioned, and the Gateway route to C is marked "Public". When party B forwards the call to party C using the Gateway the redirecting headers are updated with party B's public name and number.

110.4.5 Interactions with Call Transfer

Call Transfer using SIP is implemented a little different than the traditional PSTN networks. In SIP networks when two parties are connected (A connected to B) and one party (B) transfers the call to another party (C), the party transferring the call (B) sends the request to the connected (A) and then the connected party sets up a new call to the target (C). The transferring party (B) is notified when the transfer is complete and releases the original connected call (call between A and B). The difference between SIP and traditional PSTN network transfer is that in PSTN networks the transfer

request is not sent to the originator of the call, but the PSTN switch handles the request.

The difference requires that the party transferring the call be hidden if the transferring party has public name and number provisioned. It also requires that the new target be hidden and presented with originator's public name/ number. The following figure shows how the call transfer with PPND works:

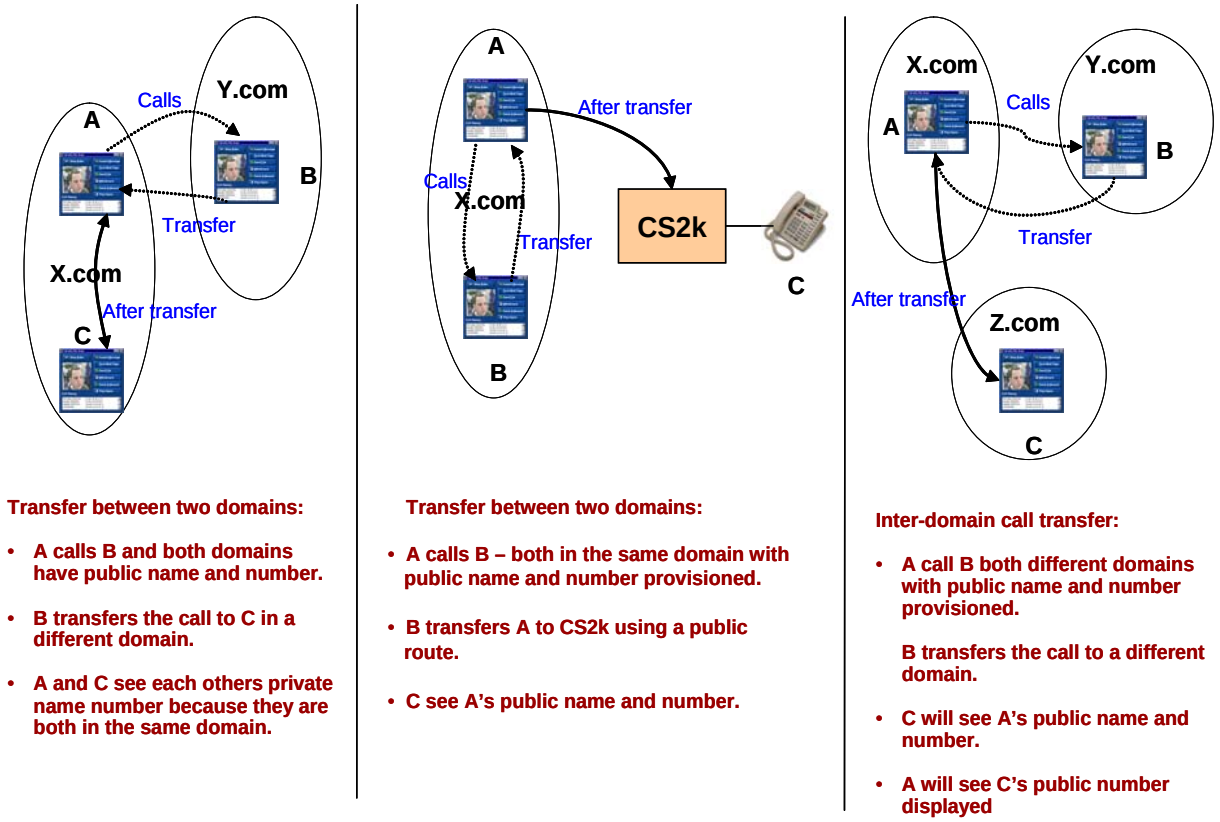


Figure 8 Call transfer scenarios

The call transfer service is also the underlining service used by the MCS Call Park and Boss Admin service. If calls are parked and retrieved in a different domain, the originating party will see the public number of the party that retrieved the call. *Note: Call Park and Boss Admin service can only be used in a single domain and cannot span multiple domains – i.e. cannot park a call in one root domain and retrieve it in another root domain.*

The public name and number rules are summarized here when a call transfer occurs:

1. The originator (A is the figure above) sees the connected public number of the terminator (C in figure above) if it is provisioned. If only the public *name* is provisioned at the domain level then the private user ID or number is displayed on the originator (A).
2. The target (C in the figure above) sees the public name/number of the originator if the two are in different domains.

110.4.6 Interactions with Foreign domains

Foreign domain incoming or outgoing calls are considered PUBLIC and it is up to the foreign domain to control what name or number is sent in the request to the next proxy.

Call forward and call transfer that occur in the foreign domain could provide the public name and number, but it all depends on how the foreign domain proxy handles the call forward and transfer requests. Some systems can handle the call redirections, and other systems might send the request back to the originating system to handle the call redirections. If the requests are sent back to the originating system for call redirection then the originating system can re-apply its public name and number rules. If the foreign system handles the call redirection then the foreign domain's public name and number rules will apply to any redirection.

If the foreign domain system is an MCS system and the terminating subscriber in the foreign domain transfers the call. The transfer request is sent back to the originator on the different system. The originator re-applies the public name and number rules before calling the target. For example, A and B are in foreign domains on different systems and B transfers the call to C who happens to be in the same system/domain as A. A will apply public name number rules when connecting to party C and deliver A's private name and number. If C happens to be in a foreign domain on different system, A's public name and number will be delivered to C.

110.4.7 E911 Interactions

The public/private name display service does not run if the E911 call in involved.

110.4.8 Interactions with Privacy

This feature will look for privacy tags for name and number. If privacy is enabled for calling name and number then public/private name and numbers will not be populated. For calls with partial privacy where number might be allowed, but not name only the public/private number rules used by this feature will be applied.

110.4.9 Interactions with Meet-me

If the public name/number are provisioned for a domain, a call to a meet-me bridge in a different domain will result in call being public.

110.4.10 Network Call logs

Network call logs available for both incoming and outgoing calls for an MCS subscriber. If the domain name/number is provisioned for the originating domain the terminating user in a different domain will have the originator's public name/number in the call logs. The originator's outbox call logs will have dialed digits if the terminating domain has public name provisioned and is different than the originating domain.

110.5 SIP Telephony route

The MCS RE-IP feature changed the way SIP routes can now be defined with the MCS. There are now two ways a SIP telephony route can be defined:

1. **Alias Lookup** – this type of sip route performs an alias lookup of the incoming digits in the domain provisioned in the sip route. If the subscriber is found with the alias the call terminates. Otherwise, based on the route option (continue, stop, etc) the call continue on to Gateway translations or gets rejected.
2. **Inter-domain** – this type of sip route forwards the request to the new domain specified in the sip route. The domain specified in the sip performs that required translations based on the incoming request. The sip route can modify the number before forwarding the request to the other domain for translations. This route is similar to how Gateways can be setup to route call to another domains on the same MCS system – sometimes referred to as "fake" gateway routes.

110.6 Inter-domain blocked calls

Inter-domain routing restriction is a new capability added by this feature to block **"direct SIP calls**" between two different SIP domains hosted by the MCS system. "Direct sip calls" refer to a subscriber dialing a number or a sip user ID from one domain to another domain by specifying the other domain in the request. For example, a user in domain A.com dials a user in B.com by using userB@B.com. The domains have to be **root domains** and not sub-domains hosted by the ***same*** MCS system. Today in some of the carrier deployments if a user dials a user in another domain using digits, the call routes over to the CS2K before returning back to the MCS for termination. This allows the carrier to reuse some of services currently not available on MCS (.e.g. PICS for carrier selection, SMDR billing, etc). If domain "A" blocks direct SIP calls to domain "B" then the following MCS services are blocked as well:

- Instant Messages
- Presence – sending presence of a user to the banned domain. This can be confusing, but presence banning is opposite of making calls. For example, if A.com adds provisioning to ban all service to B.com. All calls to B.com from A.com are banned and users from B.com cannot watch users in

A.com. Users in A.com can still watch users in B.com unless B.com adds a banned list for A.com.

- Collaborations
- Web Co-Browsing
- Send File
- Direct call forwarding and call transfers to restricted domains

A domain that restricts direct SIP calls to another domain is applied to making calls using Telephony routes as well. These telephony routes can be SIP routes to other domains that either perform an Alias lookup or perform inter-domain routing in the other domain. Inter-domain calls terminating to a Converged Desktop are not restricted. Refer to the next section for more information on this restriction.

Blocked calls are rejected by a SIP 403 forbidden response.

There are two ways to provision blocking in the “Banned” user list menu. Either the complete root level domain is banned (.e.g. *@domain.com) or a single user ID is blocked (e.g. 2146841038@domain.com).

110.6.1 Inter-domain blocked call restrictions

This feature would allow an administrator to block “direct” inter-domain calls using user’s aliases or SIP User ID. This restriction will apply to CD subscribers that use the PC Client to dial another subscriber in a different domain using an Alias or SIP User ID. If the restriction between domains is set then call will not complete and is rejected by a SIP 403.

Inter-domain restriction will NOT apply if the terminator is a CD2 user and in a different domain than the originator of the call. This is to prevent calls from getting denied when a CD2 users in one domain using a PAD calls another CD2 users on a different domain. In this scenario call could loop through the MCS and get denied because the originator is in a different domain than the terminator even though both users a using PSTN phones.

The following table provides the various scenarios when calls are blocked with inter-domain restriction:

	Originator type (A.com)	Terminating type (B.com)	Termination blocked
1.	SIP	SIP	Yes
2.	SIP (e.g. 444@B.com)	Gateway Route	Yes
3.	SIP	Foreign domain	Yes
4.	SIP	SIP PA forwarded back to A.com	Yes

5.	Gateway route	Gateway route	Yes
6.	Gateway route	SIP	Yes
7.	Gateway route	Foreign domain	Yes
8.	Gateway route	SIP PA forwarded back to A.com	Yes
9.	SIP	CD2 User	***No***
10.	CD2 User	CD2 User	***No***
11.	CD2 User	SIP	Yes
12.	CD2 User	Gateway Route	Yes
13.	CD2 User	Foreign domain	Yes
14.	SIP	CD2 User PA forwarded to SIP user in B.com	**No**
15.	SIP	CD2 User PA forwarded to Gateway route A.com	Yes
16.	SIP	CD2 User PA forwarded to a Foreign domain in B.com	Yes
17.	SIP	CD2 User PA forwarded to a SIP user in domain A.com	Yes
18.	Gateway route	CD2 User PA forwarded to SIP user in B.com	**No**
19.	Gateway route	CD2 User PA forwarded to Gateway route B.com	**No**
20.	Gateway route	CD2 User PA forwarded to a Foreign domain in B.com	Yes
21.	Gateway route	CD2 User PA forwarded to a SIP user in domain A.com	Yes

The table assumes that A.com is blocking calls to B.com and B.com is blocking calls to A.com.

Inter-domain restrictions WILL apply to CD2 users other features if the incoming call is from a domain that is blocked from calling CD2 user's domain:

1. If Branding is assigned to the CD2.
2. If Music on Hold is assigned.

Domain restrictions should only be provisioned between root level domains and NOT for sub-domains. For example, if *@a.com is provisioned as a banned user in b.com then any requests from b.com to a.com are blocked. If a.com has a sub-domain sub.a.com and this is provisioned at b.com then blocking will NOT work. Inter-domain restriction only works at the root level domains.

110.6.2 Network configurations

For private name and number to work between the MCS and CS2k it is required that the CS2k trunk type to the MCS be set as IBNT2. The following diagram shows a mapping of Private/Public calls between a Sub-domain on the MCS and a Centrex group on the CS2K.

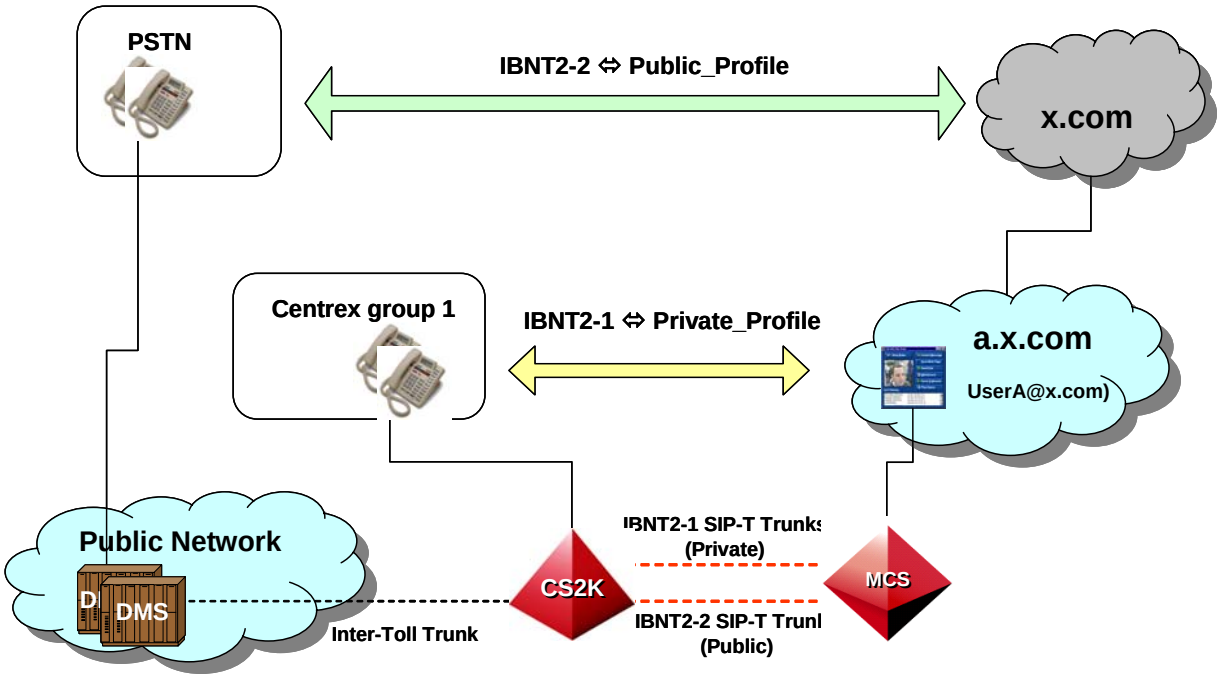


Figure 9 Centrx group profile mapping to MCS domain

A “Profile” header is used between the MCS and CS2K to determine what translations need to be handled on each node. On the MCS a “Profile” maps to a domain or sub-domain. On the CS2k the “Profile” header maps to a set of IBNT2 trunk types. In the diagram above a “Private” Profile is defined between the CS2k Centrex group and MCS sub-domain “a.x.com”. Any private calls that originate from the CS2k could map to the MCS sub-domain that is an extension of the Centrex group. The sub-domain’s translations are run because of the “Profile” header mapping and terminate to the users within the sub-domain. For outgoing calls to the Centrex group from the MCS the sub-domain’s translation can be setup to route add the “Private” profile, private name and number.

Users in the sub-domain “a.x.com” can be setup to route “Public” calls to the Public TDM network using a different set of translations that delivers the public name and number. In the diagram above the “Public” translations for the sub-domain are defined in the parent domain. During MCS translations if a number range does not match in the sub-domain the parent domain is searched

for match. In this case the parent domain has a Profile that maps to an IBNT2 trunk on the CS2k for handling public calls to the TDM network. The parent domain can be setup to route the call to TDM using the “Public” name and number of the sub-domain when a user from “a.x.com” makes a call.

The following diagram shows an example on how a Centrex group could be extended between the MCS and other TDM switches. If IBNT2 trunks are provisioned for private calls the private call indication can be passed to other TDM switches using the concept of Multi-Location Business Groups (MBG) over Inter-Toll trunks (IT).

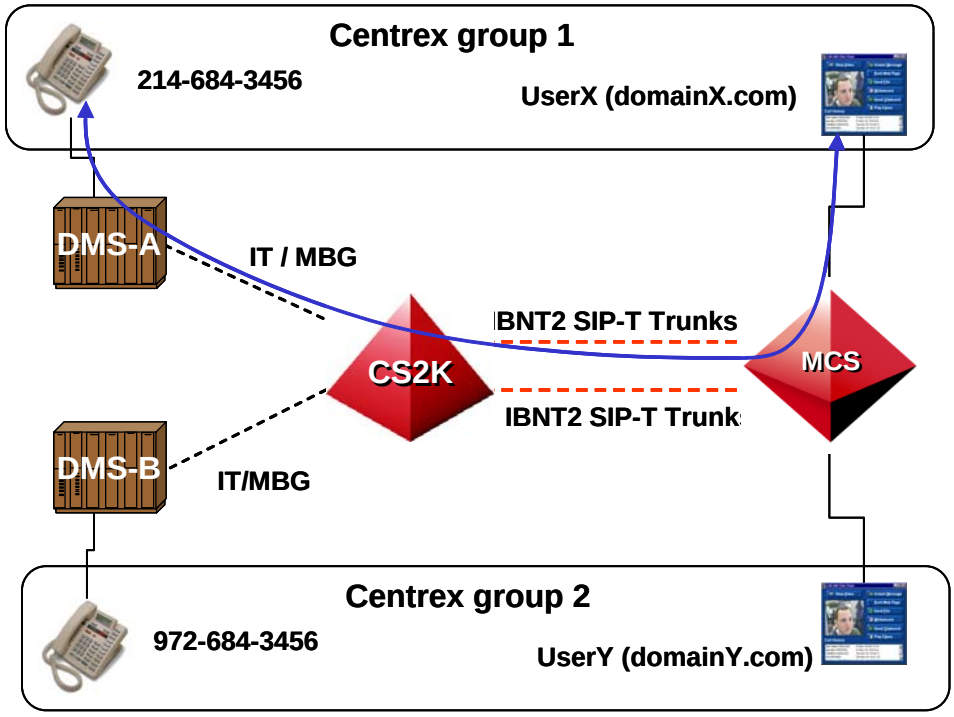


Figure 10 Centrex group and MCS domain example

The Centrex group transparency for “Private” name and number between Centrex group users on a DMS and MCS is provided by MBG. The CS2K in the middle maps the private name/number from the IBNT2 trunk to the Inter-Toll trunks using the MBG parameters.

110.7 Configuration changes/additions

110.7.1 Provisioning Client / Database additions

New parameters will be added to the database that can only be provisioned by the operator with system admin level privilege. These parameters are:

- Public name and number fields for domain and sub-domains.
- Sip telephony routes to define public and private routes.

Upgrade scripts will have to be written to take into account these new fields when upgrading the database from an existing release to a new release that supports this feature.

110.7.2 Configuring Public Name and Number

Two new fields called Public Name and Public Number will be added in the domain parameters section of the domain and also in the sub-domain.

- By default both of these fields will be empty when a new domain is created.
- A sub-domain (if created) can have its own unique Public Name and Public Number fields.
- For both domain and sub-domain the system administrator needs to data-fill the two sub-domain fields with a valid name and a valid number.
- For both domain and sub-domain, the system will not perform any checks to determine if the public number data-filled is route able or not.

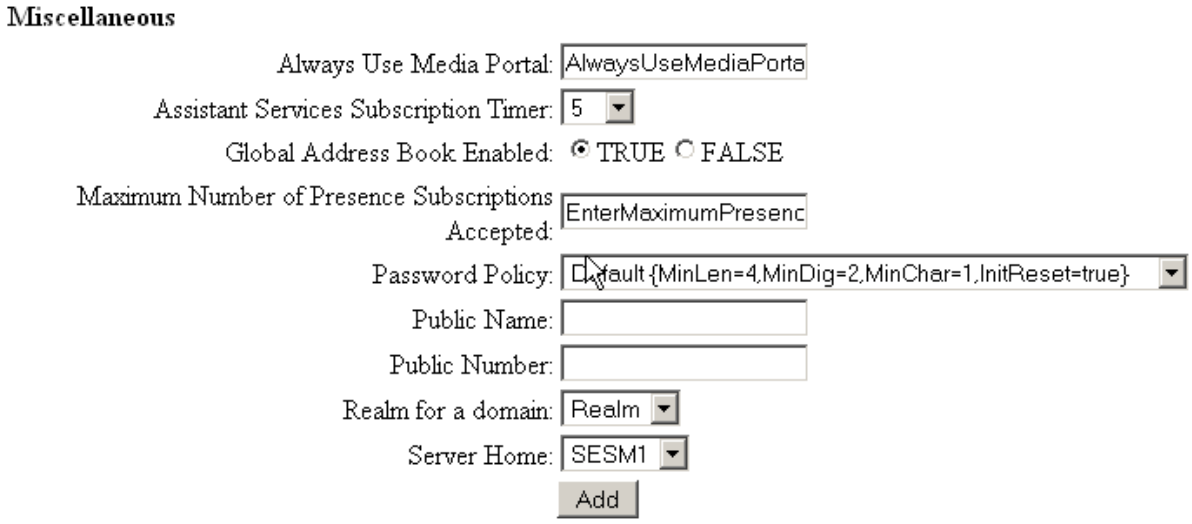


Figure 11 Domain parameter

Note: provisioning these fields basically triggers this feature to deliver public or private name/number. Without provisioning a public name against a domain the private name is delivered based on the call scenario. If a public number is not provisioned either against a domain the private number or SIP user ID is delivered based on the call scenario.

110.7.3 Configuring Restricted Domains

Existing Banned User menu (for a domain) will be utilized to restrict *name dialing* between two domains that have been defined in the MCS system.

- A user put in banned list will not be able to make any calls, IMs, or Collaboration outside his/her domain.
- Admin operator can put a restriction at a domain level to disallow all users making any calls, IMs, or Collaboration, outside their domain.

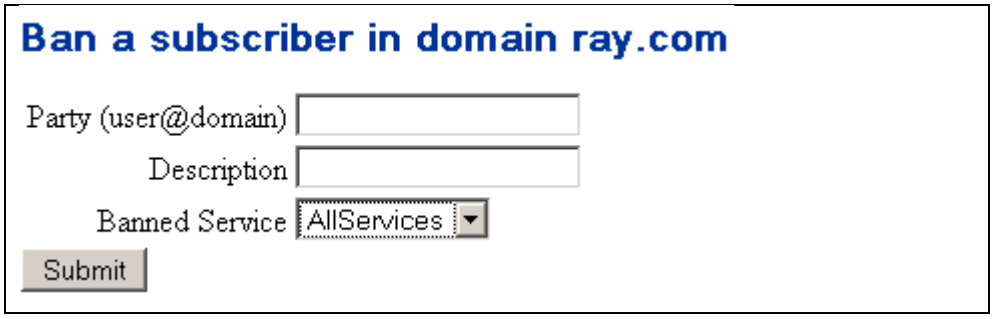


Figure 12 Restricted domains menu

There are two ways to provision blocking in the “Banned” user list menu. Either the complete root level domain is banned (.e.g. *@domain.com) or a single user ID is blocked (e.g. 2146841038@domain.com).

110.7.4 Configuring Gateway routes

A new provisioning field is available with Gateway routes. A new field called Override Public Name will be added for both SIP and gateway route to override the domain’s public name.

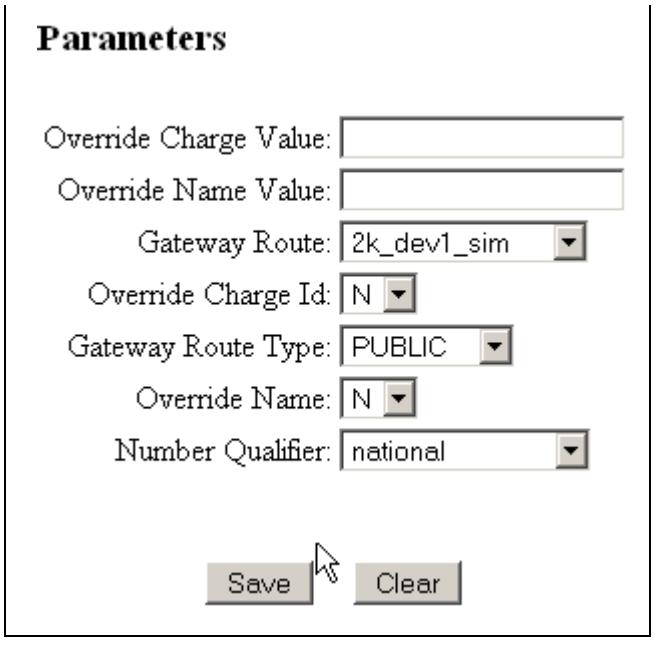


Figure 13 SIP/Gateway Telephony route parameters

110.7.5 Configuring SIP Telephony Routes

SIP Routes have a new option “Inter-Domain Routing” that allows the use of Telephony routing to lookup subscriber and other Telephony routes in other domains. If “Inter-Domain Alias Lookup” route type is selected then the telephony route lookups the subscriber alias in the other domain.

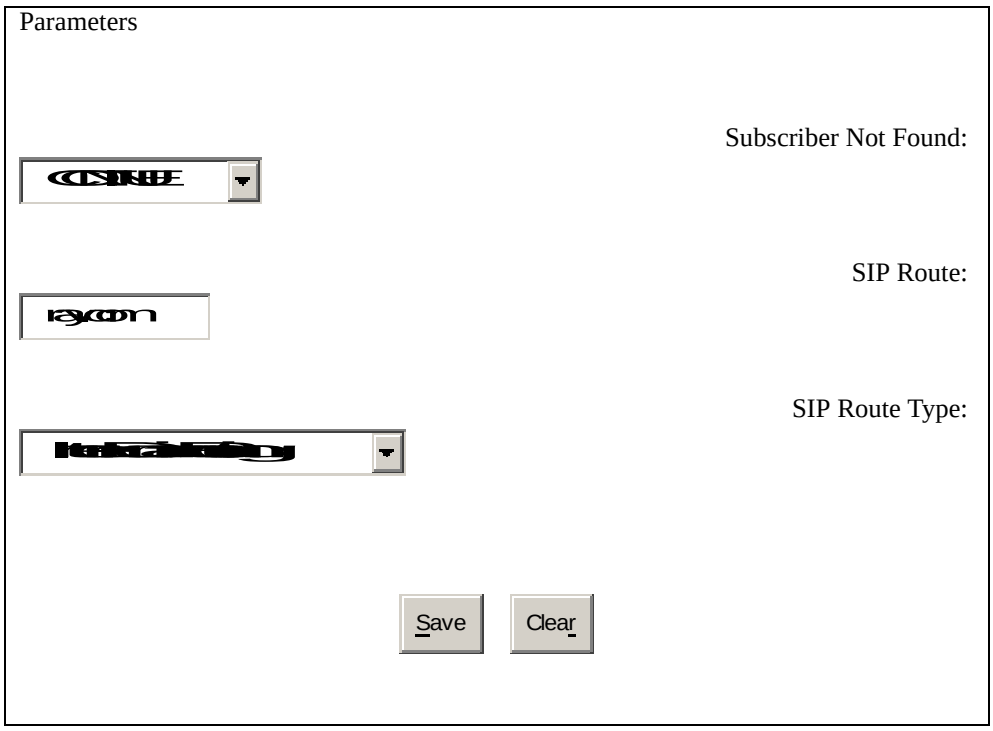
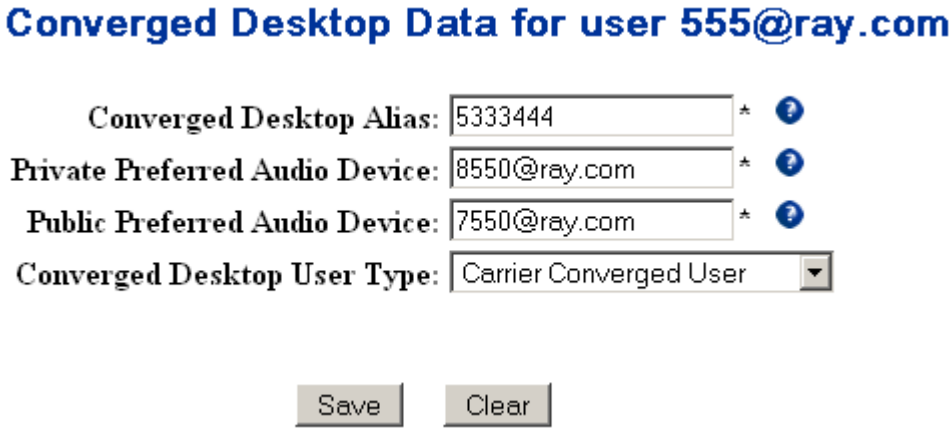


Figure 14 SIP/Gateway Telephony route parameters

110.8 Converged Desktop PAD provisioning

An additional field is added by this feature to provision digits that would allow “Public” call to be reached to Converged Desktop users PAD.

Figure 15 Private and Public PAD provisoning



110.9 Software Requirements or Dependencies

This feature is part of the MCS09 release and dependant on some of the function introduced by feature – A00009419 Out Of Band Refer for Converged Desktop 2. ***Out of Band Refer is only available to native lines on the CS2k and this Refer is NOT propagated to other CS2k or DMS switches.***

To determine the Public/Private nature of the call the PSTN Gateways like CS2k, and PRI Gateways need to provide Phone-Context indication. The use of Phone-Context is described in the MCS inter-working specifications and in IEFT RFC2806.

110.10 Limitations and restrictions

The following restrictions and limitations are applied by this feature:

- The MCS CD clients will display the calling/called numbers provided by the CS2k. No reverse translations are performed at the MCS for number display.
- IBNT2 Trunk Type is required between the CS2k and MCS to support Private Name/Number display.
- Inter-domain blocking does not apply to Converged Desktop users.
- Public/private name and number display is not applied on the MCS Presence service.

110.11 Interactions

This feature inter-acts with the following MCS server features and these are described in the previous sections for this document:

1. Converged Desktop
2. Call Forward
3. Call Transfer
4. Privacy Server
5. Network Call logs
6. E911
7. Meet-me

110.12 Glossary

Term	Description
CD	Converged Desktop
CS2K	Call Server 2000
MBG	Multi-Location Business Groups
MCS	Multimedia Communications System
PAD	Preferred Audio Device
PRI	Primary Rate Interface
TDM	Time Division Multiplexing

111: Functional Description(FN): A00009950

A00009950 (CICM) & A00010293 (GWC) - Media Portal Removal for Inactive CICM Clients

111.1 Description

Calls terminating to CICM lines are allowed to complete even if the user associated with the DN is not logged into a CICM client at the time of the call. This behavior is required to allow feature interactions such as call forwarding and voice mail to function correctly when the terminating CICM user is not logged in. Additionally, the user in question can log into a CICM client whilst being called and receive alerting and answer the call.

Prior to this SN09 feature, this behavior has been achieved by inserting a Media Portal for calls terminating to a logged out CICM user. This provides the originating endpoint with a real network location to send its pre-answer audio stream to, and automatically discovers the media address of a terminal that logs in and starts transmitting its audio stream. This allows a two-way speech path to be achieved if the user logs in and answers the call.

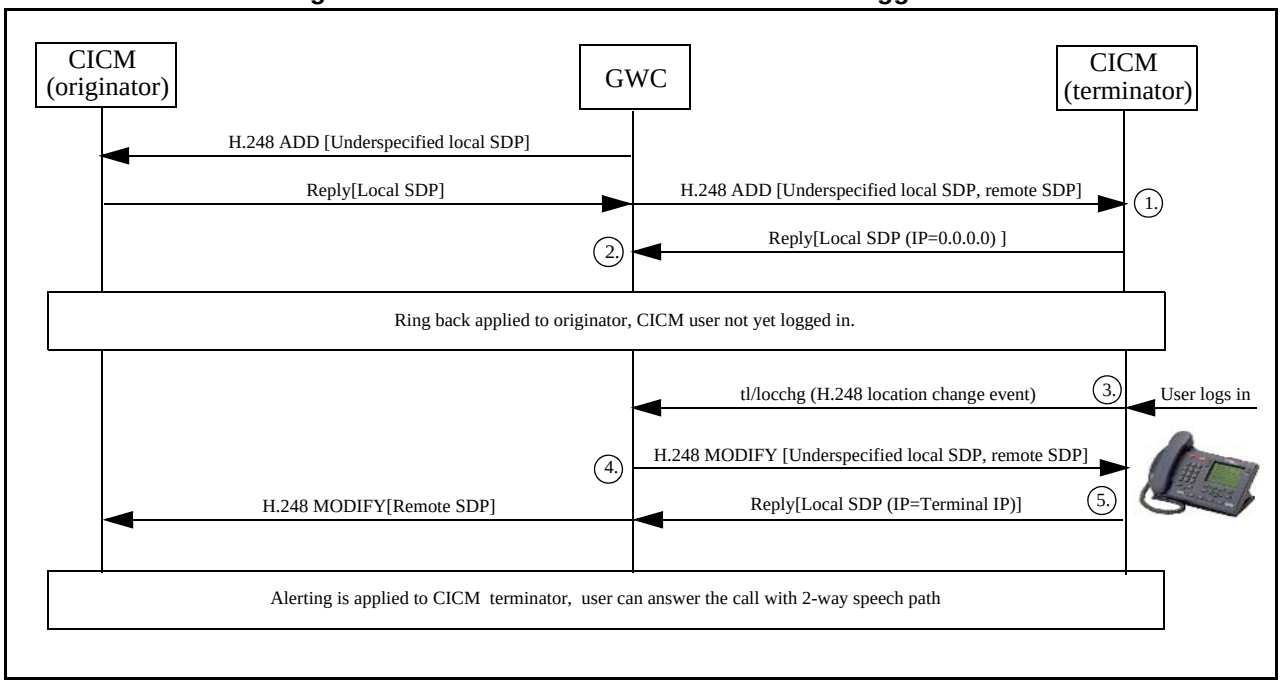
The previous architecture leads to the requirement that Media Portals must be deployed in all CICM networks, even if the NAT traversal capabilities usually associated with Media Portals are not required (ie in a flat network solution). This CICM 9.0 activity will removes this requirement and allows such feature interactions to function correctly without the use of a Media Portal. This is a cost reducing effort for customers who have networks that do not require NAT traversal.

111.1.1 GWC-CICM message flow

For a call terminating to a CICM client in a flat network, the CICM sends the originating endpoint (via the cs2k) a Session Description Protocol (SDP) message, which contains the media address of the CICM client to which the originator will direct is audio stream. This happens at call setup time (pre-answer), so if the terminating CICM user is not logged in then the media address of the CICM client is not known, therefore the Media Portal is required to provided a sink for the pre-answer audio stream.

This feature removes the requirement for the Media Portal by delaying the terminating CICM users Session Description Protocol (SDP) until the CICM user logs in, at which point the media address of the CICM client is known.

Figure 1 - CICM to CICM call - terminator is logged out



1.) Terminating CICM receives a H.248 ADD with the underspecified local and remote SDPs. The CICM user is not logged in, therefore the IP address of the terminating client is not available, so the CICM responds with a local SDP with a dummy IP address.

2.) The GWC does not pass the SDP onto the originating CICM, but simply ignores it.

3.) Terminating user logs in. The CICM raises the H.248 location change event to the GWC.

4.) The GWC responds with a H.248 MODIFY with underspecified local and remote SDP.

5.) Terminating CICM responds with the updated local SDP, containing the IP address of the terminating CICM client.

111.2 Hardware Requirements or Dependencies

This activity does not introduce any new hardware requirements or dependencies.

111.3 Software Requirements or Dependencies

This activity does not introduce any new software requirements or dependencies.

111.4 Glossary

Term	Description
CICM	Centrex IP Client Manager
DN	Directory Number
GWC	Gateway Controller
SDP	Session Description Protocol

112: Functional Description(FN): A00009951

A00009951: Introduction of 221X Wireless handset

112.1 Overview

This feature introduces CICM support for the IP Phones 2210, 2211 and 2212. These are 802.11b compliant VoIP wireless handsets, the IP Phone 2210 is the cost effective low end model and IP Phone 2211 is the high end model with more advanced features. The IP Phone 2212 is visually similar to 2210, but with backlit keypad and display, push to talk, and a more robust design.

2210 is a lightweight, durable handset which is more suitable for a typical office environment whereas IP Phone 2211 is bulky and is engineered for a robust kind of environment. The IP Phone 2212 is essentially a combination of the other two phones in the form factor of the 2210, and therefore is ideally suited for either the office or a more robust environment.

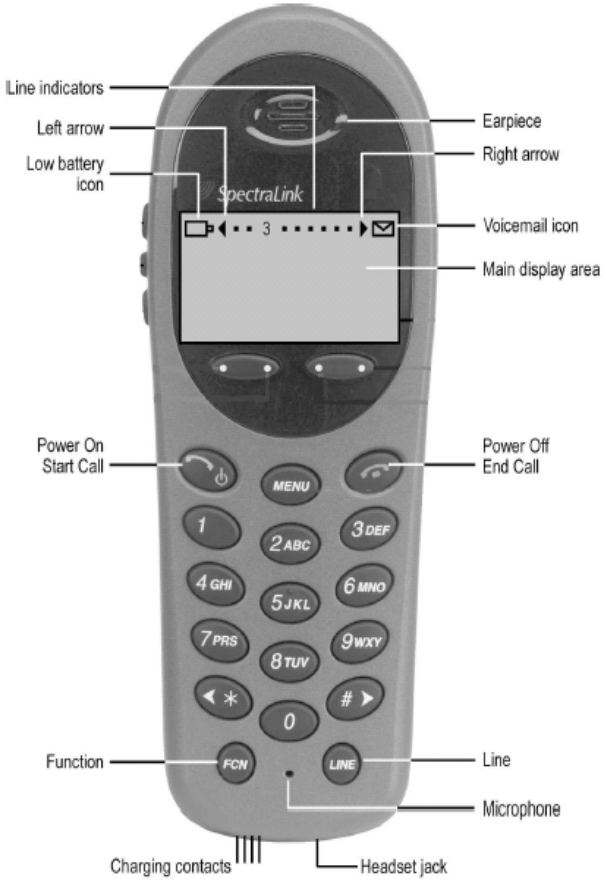


Figure 1 IP Phone 2210 handset

Figure 2 IP Phone 2211 handset

The IP Phone 2210/2211/2212 emulates an IP Phone 2004.

The features of these handsets are:

- The IP Phone 2210 is a cost effective low end model and the IP Phone 2211 and 2212 are the high end models with advanced features. All of them are 802.11b compliant.
- They support the UNIStim signaling protocol.
- The IP Phone 2211 handset has a “Push to Talk “feature.

- The IP Phone 2212 handset has the compact form factor of the 2210, but the Push To Talk and robustness functionality of the IP Phone 2211

112.2 Comparison of IP Phone 221X over IP Phone 2004

The IP Phone 221x emulates an IP Phone 2004. The IP Phone 221x has fewer buttons and a smaller display. Following are the features supported by IP Phone 221x and differences when compared with IP Phone 2004:

112.2.1 Standby/Active On-Hook state

The idle state of the handset is Standby state. The handset is still in communication with the CICM in this mode. In this mode, the handset does not communicate button pushes to the CICM and hence no features can be activated. The phone's display is also inactive

The Handset needs to be brought into active state to perform any actions. The handset can enter active On-Hook state by pressing the key sequence ON+FCN+3 or by pressing the Power On (green) key. In this mode the user can access the CICM functionalities. The phone's display is active and displays a message "EXT----- "and the phone's display is active and the phone rings loudly (i.e. NOT in-ear ringing).

The user exits the active On-Hook state and returns to standby state by pressing the END key. The phone returns to the standby state if no key is pressed for a period of 10 seconds which is the timeout for the active On-Hook state.

When the phone is in active On-Hook state, the user has access to various menus (MENU, FCN, or LINE).The phone remains in an active state when any menu is selected or a soft key is pressed, phone performs in-ear ringing and does not return to standby state. Menu can be exited by pressing the END key. Pressing the END key again returns the phone to standby mode.

The Predial feature is present in IP Phone 221x.

112.2.2 Hands Free State

The Set does not have any hands free capability and hence any feature requiring the hands-free is not supported. For example when there is an incoming call to the IP Phone 2004 which is in idle state but off-hook, the set will buzz the hands free speaker. This feature is not supported on IP Phone 221x.

112.2.3 Available Keys

The IP Phone 221X does not support all the buttons present on IP Phone 2004 and the operations on those keys are not supported.

The keys which are not available on IP Phone 221x are:

- Globe Key
- Expand to PC key
- Navigation (Left, Right, Up, Down) Keys
- Stop Key
- Copy Key
- Headset Key
- Hands free Key

112.2.4 Navigational keys

IP Phone 221x does not have navigational keys. Navigation of menus is provided by two soft keys (refer to figure 3). These soft keys scroll through the menu options in the same way as the up down keys of IP Phone 2004. IP Phone 221x does not have the Navigational up down arrows. See Figure 3.

Figure 3 Navigation using soft key

IP Phone 221x supports directional keys. They provide the directional keys only inside the terminal specified menus, viz "*"and "#" keys act as Left/Right keys (refer to figure 4) and the "volume keys" positioned on the left side of the handset behave as UP/DOWN (refer to figure 5).

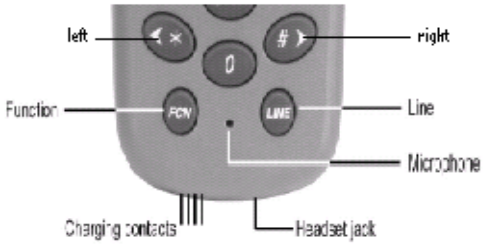


Figure 4 - Left/Right Keys

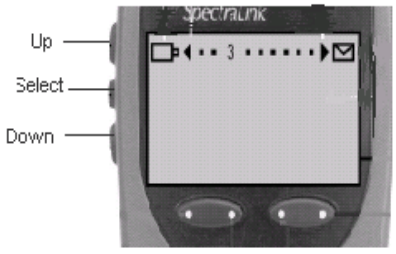


Figure 5- Up/DownKeys

112.2.5 Display

The set display is divided into 3 main areas:

- The top area is a status row which displays the status icons of each line appearance, a message waiting indicator which is an envelope icon, a battery level indicator, and left and right arrows.
- Below that is a text area that is 4 lines by 19 characters when compared to 24 characters of IP Phone 2004. Lines in 4 x 19 text area which are longer than 19 characters are truncated by special algorithm that removes spaces and punctuation first, then vowels, etc., right to left.
- Below that is a row of soft labels. A soft label is a maximum of 4 characters long. The soft labels are compressed with the same algorithm as used in the text area. The soft labels support soft key layers and cadences so that the flashing icon associated with some features, e.g. conference, are supported.

In Figure 5 the top area shows the status icon and a message waiting indicator. This area of display is also used to display the feature key selected. The number 3 in the above figure represents that the key 3 is selected.

The contrast levels of the terminal via CICM cannot be adjusted. The menu option for contrast level adjustment is blocked.

The time and date display fields are not available as the 221x terminals don't support them. Refer to figure 6. The menu option for setting the time and date format is blocked.

The menu options which are available on i221x terminals are shown in figure 8.

The 221x terminals do not support extended ASCII characters. 221x terminals use an asterisk sign (" * ") to represent a default selected item instead of tick mark when compared to 200x terminals. Refer to figure 7.

The handsets support all languages.

Figure 7

112.2.6 Soft Labels:

The soft labels on IP Phone 221x are 4 characters in width when compared to 7 characters on IP Phone 2004. Although the number of characters is 4, the menu button has a list of complete words available for the features.

112.2.7 Soft Keys:

The terminals have four soft keys (two rocker switches) directly below the display**.** The soft keys are not available when the handset is in the standby state. The character strings displayed on screen is the result of compression mechanism which removes vowels and spaces. A range of specific strings are created to make the screen legible, changes are only made to the menu options and not to the user defined feature keys.

112.2.8 Feature Keys

IP Phone 2004 has 14 feature keys when compared to IP Phone 221x which has only 6 feature keys.

These feature keys can be accessed by pressing the LINE key. A user can have 14 features data filled against the line; however he will be able to activate the first six features only if he logs into the CICM using an IP Phone 221x.

The figure below shows the menu which is available on a 221x terminal.

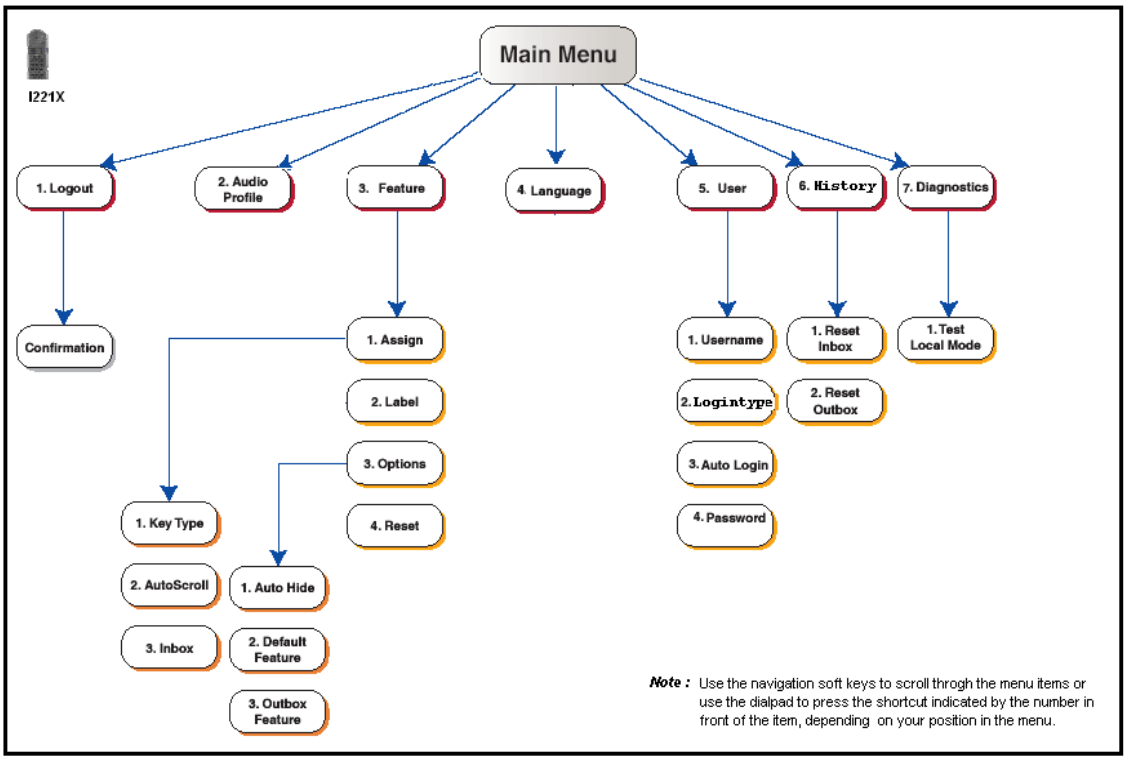


Figure 8

112.2.9 Tones

The 221x terminal doesn't currently support the stream based tones due to a firmware limitation. Therefore, until an updated firmware is available, the tones are not able to be tailored to specific markets and the current set of tones do not accurately match those of the North American Market. This is expected to be a short term workaround but please check on the delivery timeframe prior to committing to any deployment.

112.2.10 Message waiting and Missed Call indicator

An Envelope icon is displayed to indicate the Missed calls but along with the envelope icon the user is presented with the display of text messages to indicate if there is any missed call also to indicate if there is any message waiting. Please refer to figure 9 and figure 10.

Figure 9

Figure 10

112.2.11 Handset User Interface

The handset is a close adaptation of IP Phone 2004 user interface. The following keys of IP Phone 2004 are mapped into the IP Phone 221x handsets.

- Soft keys: These are directly mapped to handset soft keys with display in compressed format. Also menu list is mapped under the MENU key with display in an uncompressed format
- Feature / DN keys: Mapped to the menu list under the LINE key. To access feature keys located to left and right of the main display, press the LINE key and then select the required key from the list.
- Hold, Goodbye, Directory, Inbox, Mute and Outbox: These are mapped to the menu list under the FUNCTION key. To access these keys press FUNCTION key and select the relevant key from the list. On pressing the Mute key the message Mute is displayed as shown in figure 11.

The below figure shows the mapping of keys of IP Phone 2004 to IP Phone 221x wireless handsets:

Fig 12 IP Phone 2004

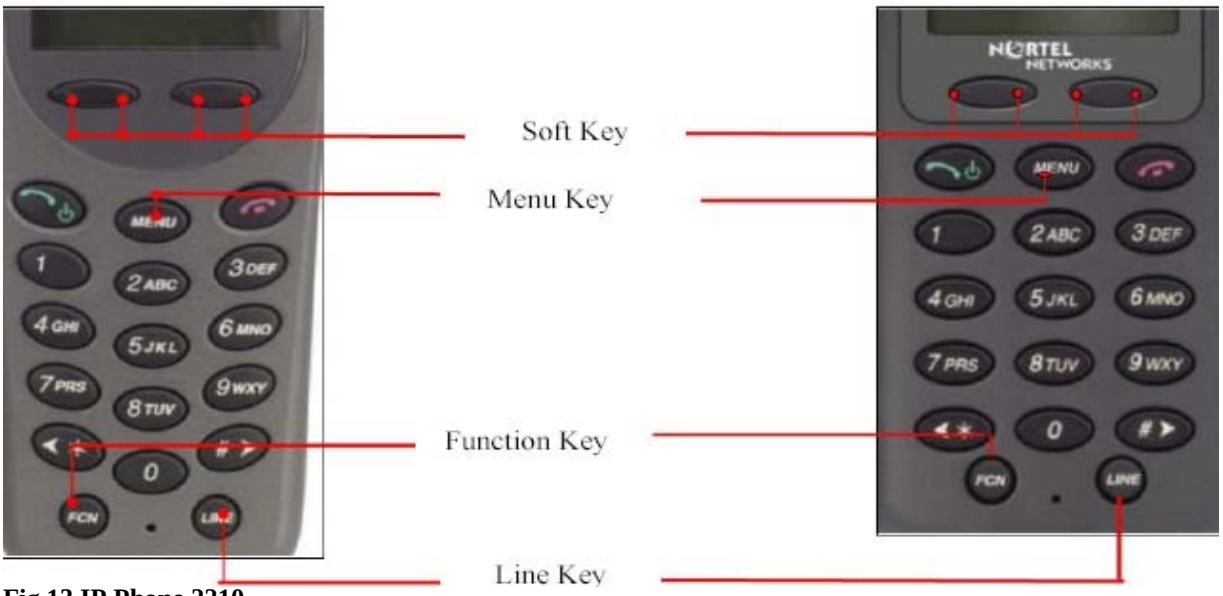


Fig 13 IP Phone 2210

Fig 13 IP Phone 2211

112.2.12 Disconnecting

When a call to IP Phone 221x is terminated by the far end and the 2210/11 user does not press the END key the phone continues to stay in the active state even though the call has been terminated i.e. it can receive another call. In the active state, the IP Phone 221x exchanges messages with the 2245 server (refer section 2.6) every 30 msec. This consumes RF bandwidth and reduces battery life.

112.2.13 QoS

End to end QoS, i.e. DiffServ, is not supported.

Layer 2 QoS, i.e. 802.1 p/q is not supported.

Quality of Service is provided by the 2245 (refer section 2.6) using the Spectra Link Voice Priority (SVP) protocol.

112.2.14 Codecs

Both G.711 and G.729 A/B codecs are supported. The RTP packets which transit between the IP Phone 221x and the 2245 server always contain 30 msecs of voice. The 2245 server repackages the voice data to the correct packet size. The jitter buffer is always configured to 70 msecs.

112.2.15 RTCP

RTCP is not supported. Incoming RTCP packets are discarded. On a query for RTCP parameters dummy values are returned.

112.2.16 SLR/RLR

The IP Phone 221x does not support the UNIStim messages used to adjust the SLR and RLR of the set. This means the default volume feature cannot be supported.

112.3 Administration - Element Manager

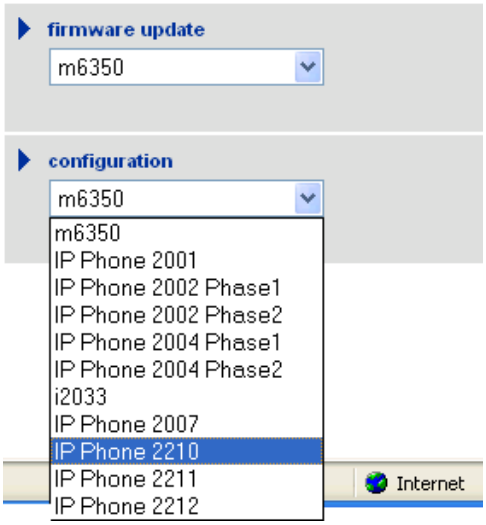


Figure 15

The administration and configuration of the IP Phone 221x uses the same pages which are available for other terminal types.

Figure 16 provides the information of the terminal configuration like feature key attributes, Voice Parameters like default audio profile and default voice codec and RTP Port number for IP Phone 2210. The Default Volume settings have been deleted as this terminal doesn’t support this feature and TFTP port address information is included.

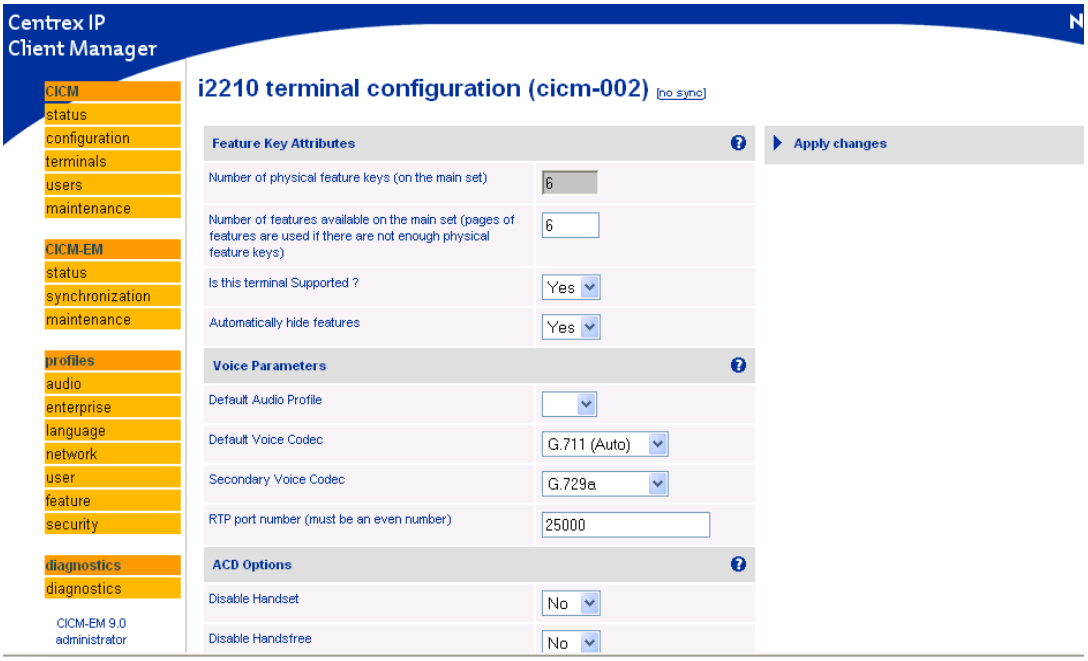


Fig 16 - IP Phone 2210 terminal configuration

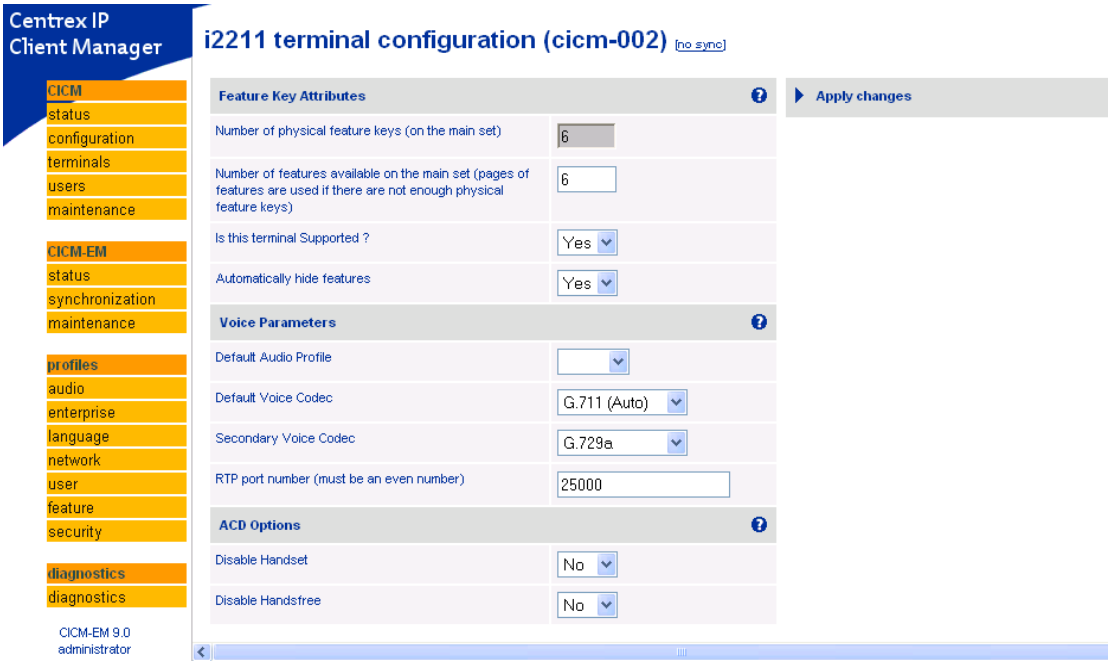


Fig 17 - IP Phone 2211 terminal configuration

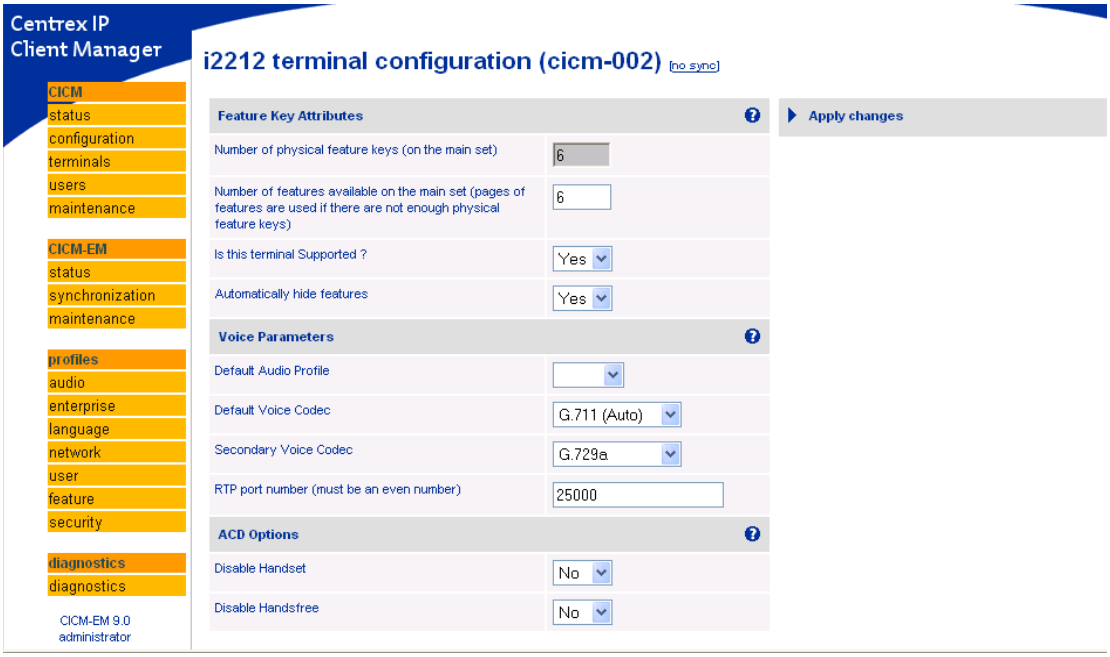


Fig 18 - IP Phone 2212 terminal configuration

112.4 Interactions

112.4.1 Joint session

The IP Phone 221x can join a session with the m6350 Softclient. In this scenario, it will always adopt the master position in their master/slave relationship. In this case, the IP Phone 221x will function in the same manner as the IP Phone 2004.

IP Phone 221x doesn’t support a joint session with another IP Phone 200x or 221x terminal.

112.4.2 SRG Support

The Survivable Remote Gateway (SRG) solution is based on the Business Communications Manager (BCM) platform and technologies. It allows distribution of trunking across the WAN so remote users can get dial tone from their local central office or from any other IP Telephony gateway hosted by CS2K. Local telephone numbers can be published, supporting a local presence within the community the remote office supports. This capability can also reduce unnecessary toll charges and provides required local trunking for Emergency 911 calls. Additionally, the Survivable Remote Gateway provides a full suite of IP based data and routing capabilities including Network Address Translation (NAT), DHCP, Web caching and firewall. The IP Phone 221x supports SRG same as IP Phone 2004.

112.4.3 Unistim Security

The IP Phone 221x does not support UNIStim security.

112.5 Software Requirements or Dependencies

The terminals IP Phone 221x do not support UFTP upgrades as a result only TFTP server is used.

112.5.1 Firmware Download

The IP Phone 221x Terminals have upgradeable firmware. The firmware may be upgraded using TFTP only as UFTP is not supported by the terminal.

The TFTP server address is set as part of terminal configuration either from DHCP server or manually entered.

The TFTP server (RFC 1350) holds the software images for IP Phone 221x and 2245 server. Whenever a wireless handset boots it checks for the firmware version and if it's different download the new version. In a similar way whenever a 2245 reboots or is manually reset it checks for the version against the software available in the TFTP server and if it's different the new firmware is downloaded.

- The time taken for a handset to check the version of software against the one available in TFTP server is less than 2 seconds.
- If the TFTP server is offline or unreachable the 221x tries for about 10 seconds before giving up and using its existing version of firmware.
- The 221x firmware downloading process takes about takes about 30 seconds.
- The TFTP server must be capable of supporting multiple TFTP sessions.
- Software updates for the Nortel 2245 Telephony Manager and Nortel 221x Wireless Handsets should be installed into the root directory of the TFTP server.

The firmware download for the 221x terminals via the CICM is not supported. 221x terminals are blocked to download the firmware through the CICM.

The Element manager is adapted for the 221x terminals to indicate that the firmware downloads via CICM is not allowed. They would be required to download the firmware from the TFTP server mentioned in the Terminal configuration page.

Fig 19 IP Phone 221x terminal firmware configuration

112.6 Hardware Requirements

IP Phone 221x, 2245 server 2246 Applications Gateway, 2230 Access point, 2270 WSS and SN09 CICM required.

2245 Server Overview:

Fig 20 2245 Server

The 2245 acts as a proxy for the wireless handsets and provides several services for the handsets. It should be connected to the same subnet as the wireless handsets. The handsets always communicate voice and signaling directly with the 2245 using the proprietary SVP protocol.

SVP is required for QoS because the current IEEE 802.11b wireless LAN standard provides no mechanism for differentiating audio packets from data packets

Note: **Note**. IP multicast addresses are used by the 2211 push-to-talk (PTT) feature. This requires that multicasting be enabled on the subnet used for the 2211 telephones and the 2245.

112.7 Functional Description

The 2245 provides the following services to the handsets:

- It acts as a proxy for every handset, that is all UNIStim signaling and RTP media to /from the wireless handset pass through the 2245 server. Except for the initial DHCP and TFTP sessions the handsets only communicate with the 2245 server.

Each 2245 server is configured with an IP address which all of the handsets communicate with. In addition, each 2245 is configured with a pool of addresses. When a handset registers with a 2245, it is assigned one of the addresses from the pool. All communication between this 2245 and wireless sets is always done via its pool address. In this sense the 2245 acts as a NAT.

Note: Note: The 2245 has a single physical Ethernet interface and MAC address so all of the IP addresses are mapped to a single MAC address.

SVP is required for QoS because the current IEEE 802.11b wireless LAN standard provides no mechanism for differentiating audio packets from data packets.

- The RTP packets between the handset and the 2245 server always contain 30 msec worth of voice no matter what has been configured on the call server. The 2245 server repackages the RTP packets to conform to the size which has been configured in the call server. This provides more efficient use of the available RF bandwidth at the expense of slightly increased jitter and latency.
- The 2245 server is configured with a maximum allowable number of simultaneous media streams on a single access point. The 2245 server keeps track of the number of media streams on each AP and blocks calls to / from a set which would exceed the configured capacity.
- There is also a keep alive packet exchange which runs between the handset and the 2245 every 30 seconds. If the handsets detects the 2245 server is unreachable it will reset and attempt to re-establish a connection with the Master 2245 server.

If the call originates from a wireless which is on a bandwidth restricted AP the caller hears a warning tone and the call is blocked.

If a set is mobile and moves into an AP which is already at capacity the handset will remain associated with an AP that has sufficient bandwidth. This could result in degraded signal and voice quality and ultimately a call could be dropped.

Call Server. A CS2K server with SN09 load running on it.

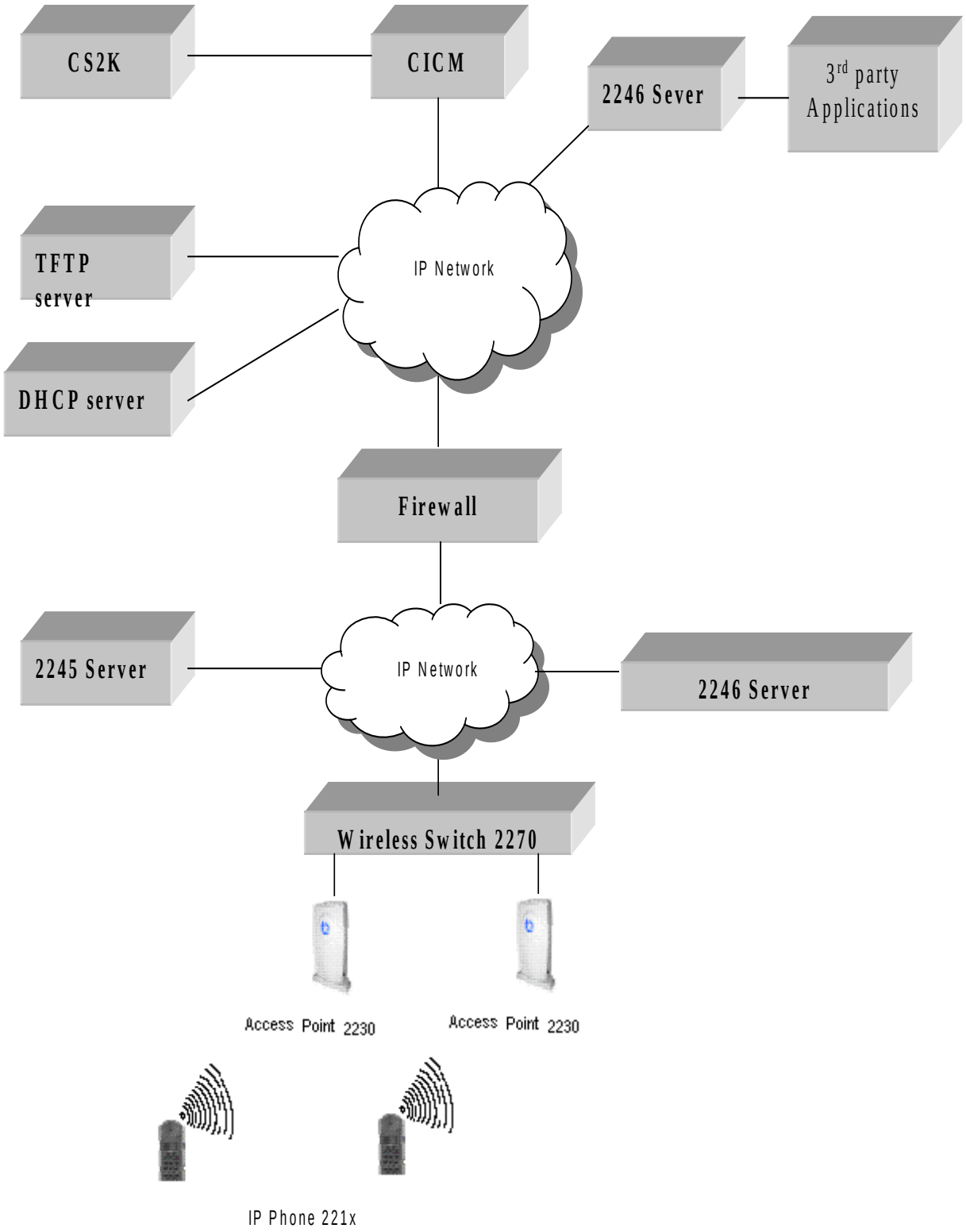
2246 Applications Gateway. This device provides an access gateway so that 3rd party applications can have access to the wireless handsets.

2230 Access Point. An 802.11b access point. For best QoS performance the Access Point should be SVP compliant such as the Nortel 2230 Access Point.

2270 Wireless Security switches: 2270 act as aggregation points for a number of access points or ports and are the gateways from the Wireless LAN into the wired LAN. 2270 allows the phone to roam from subnet to subnet but retains their IP address.

A Wireless handset system is shown in Figure 21:

Figure 21 Wireless Handset system



112.8 Glossary

AP	Access Point
CICM	Centrex IP Client Manager
DHCP	Dynamic Host Control Protocol
PTT	Push To Talk
RTP	Real Time Protocol.
RTCP	Real-time Transport Control Protocol
RLR	Receive Loudness Rating
SLR	Send Loudness Rating
SVP	Spectralink Voice Priority protocol
TFTP	Trivial File Transfer Protocol
UFTP	UNIStim File Transfer Protocol
UNIStim	Unified Network IP Stimulus Protocol

112.9 References

For information on the SVP protocol refer to

http://www.spectralink.com/products/pdfs/SVP_white_paper.pdf.

For more information on i221x please refer the feature specification document

221xFSv1.2.pdf

http://nbvws300.ca.nortel.com/~daveward/IPTerminals/SpectraLinkWireless/FeatSpec/221xFSv1.2.pdf

113: Functional description (FN): A00010024

Nortel Carrier Grade Linux kernel emergency pool, A00010024

113.1 Description

The basic concept of the proposed design is to maintain a kernel emergency memory pool that will be released at the instant where normally the Linux OOM killer would run and thus delaying unpredictable behavior.With the proper notification mechanism and the right threading model it will be feasible to have an application responding to critical condition and take the proper action.

The Memory pressure on the MPE depends largely on the non-deterministic network conditions the box is exposed to. Under extreme pressure the MPE software exhaust the entire memory on the system and die as of a result of OOM killer. It should then be clear that MPE need a more deterministic way to react to such a condition. Given the huge number of different scenarios where the memory can be exhausted, it's impossible to fine tune the OOM algorithm to be 100% deterministic. In other words, MPE needs predictable early warning

113.2 Limitations and restrictions

It's up to the application to properly engineer the threading/scheduling model in order to respond in time to the critical out-of-memory notification as the only guarantee of that feature is to delayed a possible OOM situation.

113.3 Interactions

The proposed design involved some modification to SWMON and the Linux kernel. SWMON has already the capabilities to monitor memory usage and generate alarm (Minor Major Critical) to an application that register through HAPI. The actual monitoring capabilities are too slow to catch fast memory consumption and need to be enhanced by using asynchronous notification from the kernel..

113.4 Glossary

Term	Description
OOM	Out Of Memory
OOM killer	Kernel thread that kill user process when the system run out of memory.

Term	Description
Kswapd	Kernel thread that reclaim memory to the system

114: Functional description (FN): A00010168

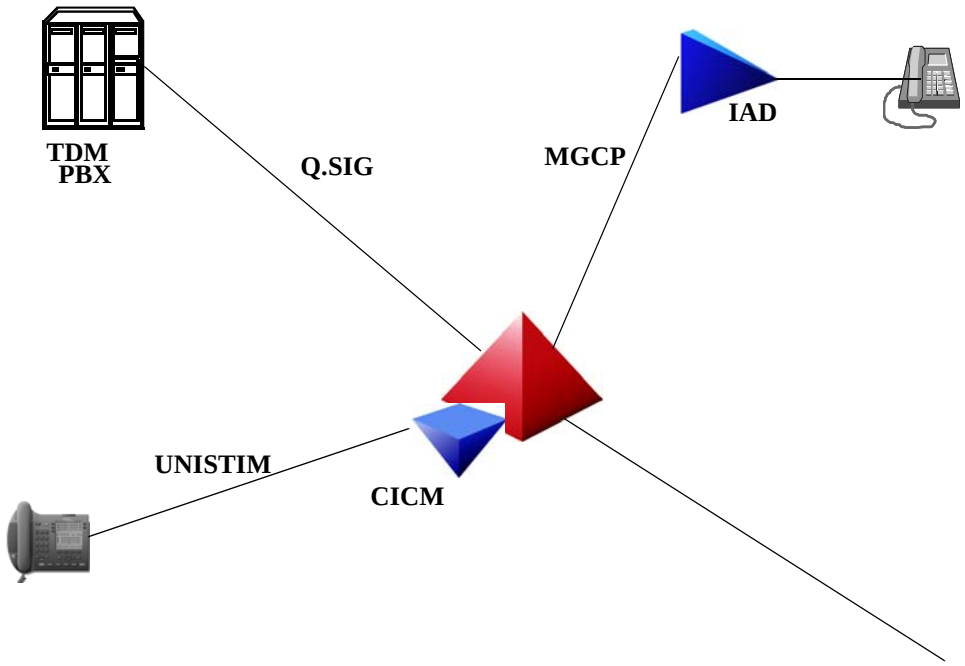
114.1 Feature name and Feature ID

H.323 support for COnnected Line Presentation/COnnected Line Restriction (COLP/COLR).

114.2 Description

This feature is to support COLP/COLR on International H.323 Gateways.
In the context of H.323, QSIG (Q-reference point SIGnalling) is a private (i.e. corporate) network signaling protocol for communication between ISDN Private BranchExchanges (PBX). In respect to H.323 GWs Q.SIG will be used between H.323 and the core. COLP/COLR are existing QSIG functionalities. No new COLP/COLR capabilities are introduced by this feature.
Please refer to ìFigure 1 COLP/COLR Supplementary Servicesî on page 30.

Figure 1: Agent Interworkings over which COLP/COLR Mapping will be supported



2.2.1 COnnected Line Identification Presentation

COnnected Line Identification Presentation (COLP) supplementary service (SS) provides the calling party with the possibility to receive the connected users number.

COLP has the following functionalities:

Provides the calling user with the connected number (CNN).

The CNN IE is provided in the CONNECT message.

The service is provided on a per trunk-group basis, datafilled in table LTDATA.

When the COLP SS is activated, the Connected Party Subaddress Information Element (CNS IE), if provided by the connected user is included in the CONNECT message if COLR is not activated.

For a Private call provisioning is not required for the presentation of the CNN or the CNS IEsí. Whenever a CNN IE and CNS IE are received they are transparently passed on.

Supposing no information is provided by the connected user, the network provides the Default Number associated with the connected user. The DFLTCNN option in table LTDATA stores the Default Connected Number for the terminating side. If this is not datafilled then no digits are sent across to the originating side.

If the Presentation number is datafilled, then COLP enables the originator to receive the connected presentation number.
If NOSCRN option is datafilled, then the COLP enables the originator to receive the unscreened connected number.

For a call originated by a QSIG trunk which does not have COLP datafilled in table LTDATA, the COLP SS is not supported. To invoke the COLP SS, the originating QSIG trunk must be defined with the COLP option in table LTDATA. Please refer to ìTable 1 Sample Datafill for COLP in Table LTDATAon page 31.

Table 1 Sample Datafill for COLP in Table LTDATA

LTDKEY LTDRSLT
ISDN 4 SERV SERV N N ALWAYS ALWAYS **COLP**

Default Connected Number :
In case, the COLP SS is activated for the originator QSIG trunk and no information (CNN IE) is provided by the connected user or the information provided is invalid, the network provides the DeFauLT CoNnected Number (DFLTCNN) associated with the connected userís QSIG access in the destination local network. The default connected number is obtained from the DFLTCNN option in table LTDATA associated with the terminating QSIG trunk. The maximum number of connected number digits is 15.

Refer to the following table.

Table 2 Sample Datafill for Default Connected Number in Table LTDATA

LTDKEY LTDRSLT
ISDN 4 SERV SERV N N ALWAYS ALWAYS **DFLTCNN 6966970**

2.2.3 COnnected Line Identification Restriction

COnnected Line Identification Restriction (COLR) supplementary service (SS) enables the connected party to prevent presentation of its number to the calling party.

COLR has the following functionalities:

- The COLR SS is offered at the terminating end.
- It prevents the presentation of the connected number (CNN).
- The service is provided on a per trunk-group basis. For COLR temporary, the default value (allowed/restricted) can be overwritten on a per call basis.
- It prevents the presentation of the Connected Party Subaddress (CNS).
- The COLR SS is offered by a permanent mode (PERM), or by a temporary mode (TEMP):

PERM mode: The COLR SS is invoked automatically by the network on all calls. If the calling party has subscribed to COLP SS, and the COLR SS datafilled as PERM RESTRICT is invoked and the valid CNN IE is sent from the terminating side, then the calling party receives the Connected Number IE with the indication of ìpresentation restrictedî and the digits not included.

TEMP mode: The COLR SS is invoked on a per call basis. This means that one of the following scenarios occurs, according to the default value set in the network:

a. If the Presentation Indicator (PI) value is supplied into the Connected Number Information Element (CNN IE), then the PI remains as received from the connected user.

b. If the PI value is not supplied into the Connected Number IE, the presentation indicator is set according to the COLR TEMP sub option that could be Allow or Restrict.

Refer to the following table.

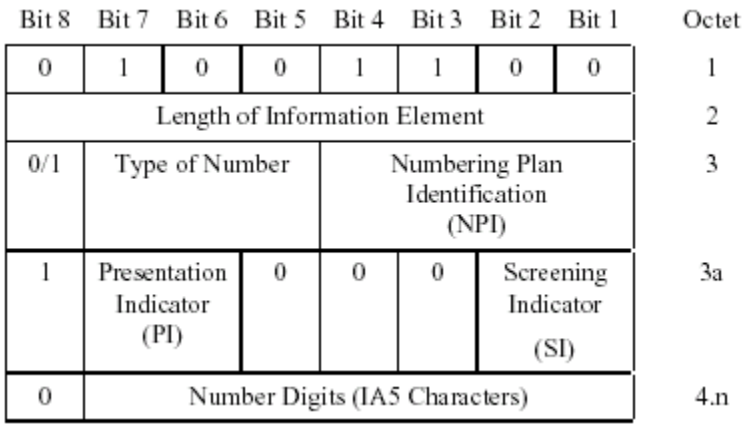
Table 6 Sample Datafill for COLR: Table LTDATA

LTDKEY LTDRSLT
ISDN 3 SERV SERV N N ALWAYS ALWAYS **COLR TEMP ALLOW**
ISDN 3 SERV SERV N N ALWAYS ALWAYS **COLR PERM RESTRICT**
ISDN 3 SERV SERV N N ALWAYS ALWAYS **COLR TEMP RESTRICT**

2.2.4 Values supported for SI, PI, TON, NPI in CNN IE

The connected number information is contained in the optional connected number information element (CNN IE) of the Q.931 connect message. The CNN IE is coded as shown in fig. 6. Please observe that octet 3 can have 0 or 1 value depending upon the usage. The maximum length of this information element is 24 octets. Please refer to ìFigure 5 Connected Number Information Element (CNN IE)î on page 41.

Figure 5 Connected Number Information Element (CNN IE)



The different option values of Screening Indicator (SI), Presentation Indicator (PI), Type Of Number (TON), Numbering Plan Indicator (NPI) as supported on the DMS100, are explained below.

Refer to the following figure.

Figure 6 Option Values

Screening Indicator (SI)

2	1	
0	0	user-provided, Not Screened
0	1	user-provided, Verified, and Passed
1	0	user-provided, Verified and Failed
1	1	Network Provided

Presentation Indicator (PI)

7	6	
0	0	Allow
0	1	Restrict
1	0	Not available

Type Of Number (TON)

7	6	5	
0	0	0	Unknown
0	0	1	International Number
0	1	0	National Number
1	0	0	Subscriber number

Numbering Plan Identification (NPI)

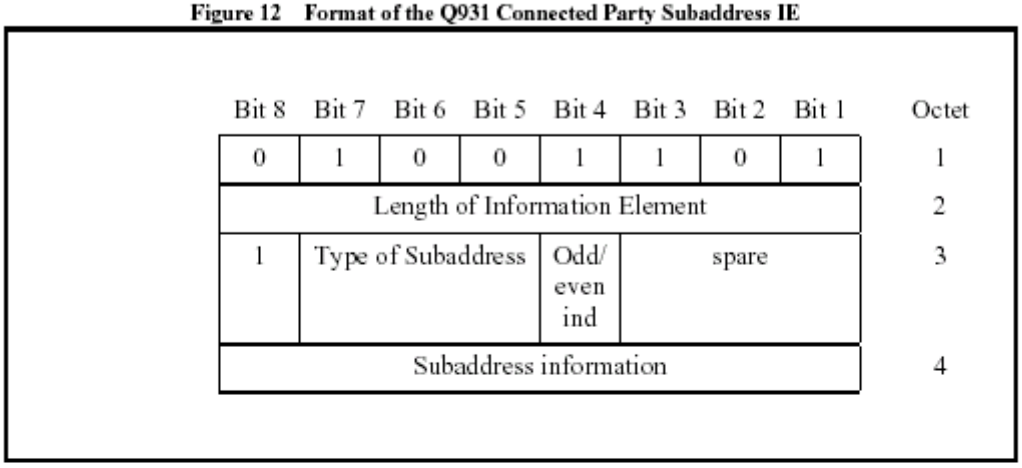
4	3	2	1	
0	0	0	0	Unknown
0	0	0	1	ISDN Telephony Numbering Plan (E164)
1	0	0	1	Private Numbering Plan

An incoming CNN IE at the terminating side is considered as valid only if the NPI field has "Unknown" or "ISDN Telephony Numbering Plan (E164)" values. Otherwise the information is discarded. The CNN fields from CONNECT message are updated at the CM level to reflect the CNN information that is delivered to the originating interface.

2.2.6 Connected Party Subaddress (CNS)

The purpose of the Connected party subaddress information element is to identify a subaddress associated with the terminator of a call. Please refer to "Figure 12 Format of the Q931 Connected Party Subaddress IE" on page 54.

Figure 12 Format of the Q931 Connected Party Subaddress IE



Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
0	1	0	0	1	1	0	1	1
Length of Information Element								2
1	Type of Subaddress			Odd/ even ind	spare			3
Subaddress information								4

For the Connected Party Subaddress the following is done,

- The CNS is mapped to the APP-PSS1 parameter. (For QFT only)
- The CNS is mapped to the ATP parameter in case of ISUP.
- If COLP SS is activated, add the Connected Party Subaddress Information Element to the CONNECT message.
- If COLR SS is activated, the Connected Party Subaddress Information Element is not added to the CONNECT message.
- If the calling user has not subscribed to COLP, then the CNN IE and the CNS info are not sent in the CONNECT message.
- On interworking of QSIG to QSIG, the CNS IE shall be mapped independently of the COLP SS.

The Presentation of the CNS IE depends on the following:

Public call:

- When COLP SS is not subscribed, the CNN IE and CNS IE are not sent to the calling user.

- When COLP SS is subscribed and PI = allowed, the CNN IE and CNS E (if available) are sent to the calling user.

- When COLP SS is subscribed and PI = restrictd, an 'empty/restricted' CNN IE is sent to the calling user. The CNS IE is not sent in this case.

Private Call:

- The CNN IE and CNS IE are mapped transparently.

- Exception for Originating and END PINX:

- When COLP SS is subscribed and PI = restricted, and empty/restricted' CNN IE is sent to the calling user. The CNS IE is not sent in th

2.2.8 Interworkings

Networked services support for interworking QSIG for H.323-based originating/ terminating at a 3rd party based PBX (e.g., Siemens HiPath) should include the following:

. i.COnnected Line Identification Presentation (COLP) supplementary service (SS).
ii.COnnected Line Identification Restriction (COLR) supplementary service (SS).

Networked services support for interworking QSIG for H.323-based originating/ terminating at a Nortel PBX (e.g., BCM50, BCM 200/400) should include the following:

i.COnnected Line Identification Presentation (COLP) supplementary service (SS).
ii.COnnected Line Identification Restriction (COLR) supplementary service (SS)

114.3 Limitations and restrictions

There is no attempt within this feature to map MCDN versions of COLP/ COLR to H.323 or to Q.SIG. This feature merely maps Q.SIG versions of COLP/COLR to H.323 versions of COLP/COLR (and vice versa). The following provide specific examples of messaging in MCDN environments

This feature is implemented exclusively for the support of International H.323 COLP/COLR. Refer to A59027747 QSIG Support for COLP/COLR for additonal restrictions on COLP/COLR.

114.4 Glossary

Table 1:

TERM	DESCRIPTION
CNN	Connected Number
CNN IE	Connected Number Information Element
CNS	Connected Number Subaddress
CNS IE	Connected Number Subaddress Infomation Element
COLP	COnnected Line identification Presentation
COLR	COnnected Line identification Restricton
QSIG	Q Interface Signaling
SS	Supplementary Service

114.5

References

1. AF7494, PLS DOC, COLP/COLR
2. AR2191, PLS DOC, ND ISDN SVCs:WT: Basic Call Services
3. AJ5284, PLS DOC, Presentation CLI Support
4. AU3248, PLS DOC, COLP/COLR Phase I
5. COLPRDOC in FMDOC, PRI COLP/COLR Phase II
6. A59012493 in FMDOC, PRI COLP/COLR Phase III
7. ETS 300-173 Specs
8. ECMA 148 Specs
9. ITU Q.699 Interworking Between ISDN access and non-ISDN access over ISUP SS #7
10. AE0975, CLIP/CLIR, Supplementary Services
11. A59027747 QSIG support for COLP/COLR.

115: Functional description (FN): A00010303

115.1 Feature name and Feature

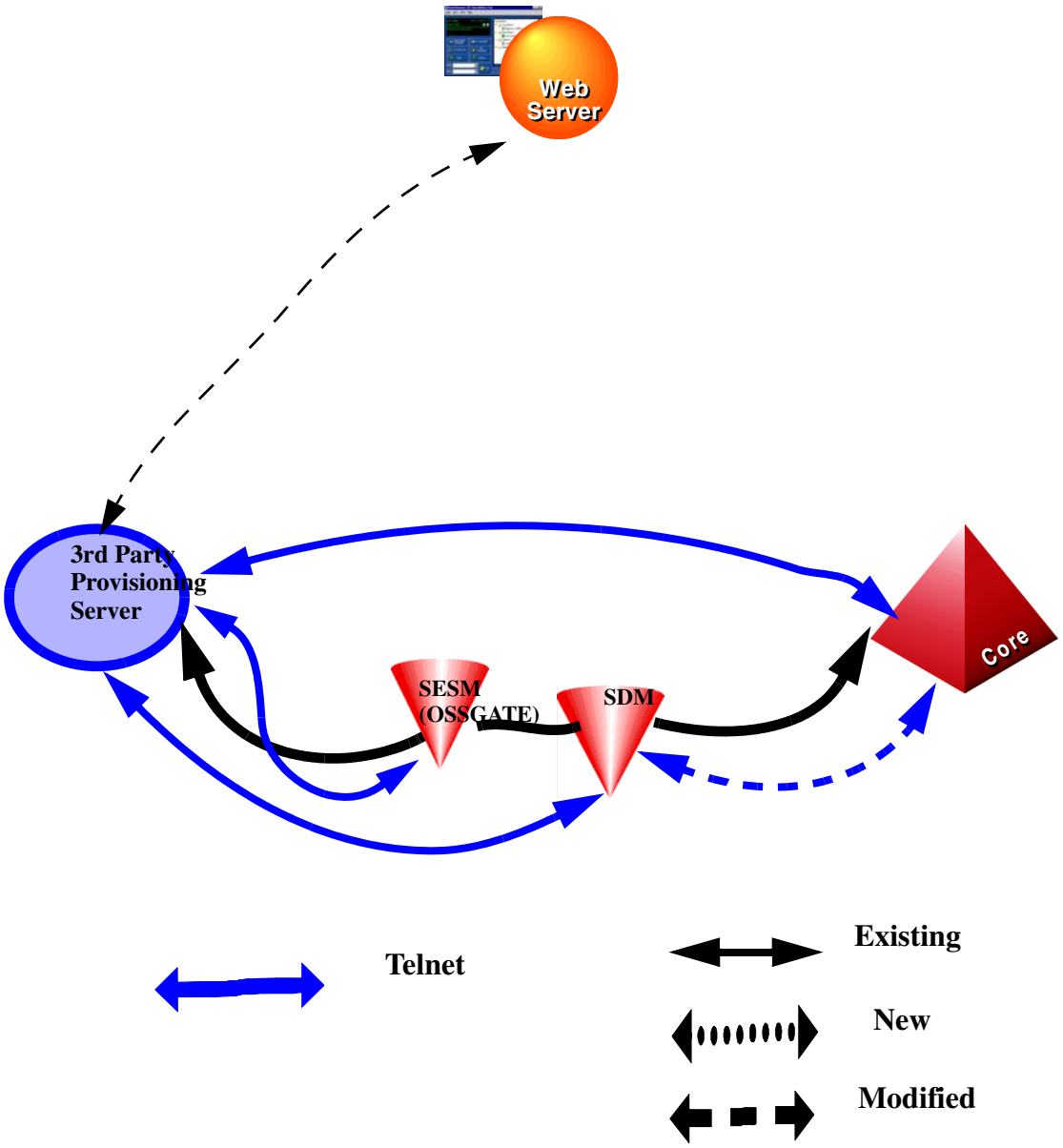
A00010303- Map Level Service Control Application Programming Interface

115.2 Description

This activity addresses the development associated with enabling in DMS and CS2000, the update and/or query capabilities for the switch based services. With the addition of this set of capabilities, subscribers will have the ability to both query the status and/or programmed information as well as activate/ deactivate and update their corresponding service. Based on the service provider's interface for the end user, it takes out the complexity faced by the user to activate, deactivate, add, delete, change or edit specific data. The command performance will be in the range of 1 to 3 seconds.

Functional Behavior:

For CS2K, the commands issued by the end user will be sent via a 3rd party provisioning server to the OSSGATE via telnet. This is then sent to the SDM(Supernode Data Manager or CS2K Manager) which is the interface to the core for processing. The output will then be sent back and displayed to the end user via the web server. For TDM lines, there is a direct telnet connection between the 3rd party provisioning server and the SDM. This architecture can be used both for DMS and CS2K.


Web Server
3rd Party Provisioning Server
SESM (OSSGATE)
SDM
Core
Telnet
Existing
New
Modified

115.3 The Query command

Depending on the feature, the Query command can be used to query different fields such as the status, the list (if present), the delay interval and so on. When issued at the CI prompt, the query command will take the input parameters and call the query procedure for that feature. Depending on whether the feature is present or not, the corresponding return code is output.

115.3.1 QueryRequest

For a query request, the following are the input parameters:

- The DN of the subscriber associated with the given request would be a 10 digit DN.
- The corresponding feature/service would be simple enumerated type similar to the one defined in SERVORD and representing all supported services.
- The list of service attributes being queried would be simple set or enumerated type representing all possible attributes.

115.3.2 QueryResponse

The response will include the following:

Values corresponding to the service attributes queried.

- Only attributes for a single service per query will be supported in SN09.
- For list queries, the privacy indicator should be checked prior to displaying the corresponding DN.

115.3.3 List of supported Query Attributes

Table 1 List of supported Query Attributes

Enumeration	Return Value	Description
status	active or inactive	Query the status of the corresponding service
list	list of DNs 10 digits in length with/ without priv. ind.	Query all entries in the corresponding service's screening list.
listSize	positive integer less than 255	Query the number of entries in the corresponding service's screening list.
forwardDN	DN upto 30 digits in length	Query the forwarding DN of the corresponding call diversion service.

Enumeration	Return Value	Description
delayInterval	Positive integer between 1 and 10	Query the delay Interval of the corresponding service.This represents the number of rings.
scList	List of DNs variable in length up to 30 digits	Query all entries in the corresponding Speed Call list
all	Some aggregate of the above	Query all attributes of the corresponding service.

115.3.4 Service to Query attribute matrix

Each service belongs to a group from group1 to group9. These groups are based on the attributes of each service. The matrices below show the attributes present for each service.

Table 2 Service to Query Attribute matrix

Service	Status	Delay Interval	List	List Size	Forward DN	Speed Call List
MWI	X					
VMWI	X					
AMWI	X					
ACRJ	X					
ACB	X					
AR	X					
CSMI	X					
CWT	X					
LDSA	X					
SUPPPRESS	X					
MSB	X					
DRCW	X		X	X		
SCRJ	X		X	X		
SIMRING	X		X	X		
CFU	X				X	
CFDA	X				X	
CFB	X				X	

Service	Status	Delay Interval	List	List Size	Forward DN	Speed Call List
SCA	X		X	X		
SCF	X		X	X	X	
CFDVT		X				
CNDB						
CNAB						
COT						
CCW						
SCS						X
SCL						X
SCU						X

115.3.5 Error codes for the Query command

Table 3 Error codes for the Query Command

Return Code	Description
Failure - Invalid_Dn	DN entered is not valid.
Failure - Unavailable_Resources	The service is not subscribed on the DN.
	The feature SOC is idle.
	SLE SOC is idle.
Failure - SOC_Idle	The svcntrl SOC is idle.

115.3.6 Query Examples

Syntax to query the status of SCRJ for 6136631001

>svcntrl query 6136631001 scrj status

Status - Service_Active

Syntax to query the SCRJ list for 6136631001

>svcntrl query 6136631001 scrj list

List_Dn -

6136634567; 6136638901; 6136671001

6136671023; 6136789021; 6136779001

6136772021;

Syntax to query SCRJ for 6136631001

>svcntrl query 6136631001 scrj all

Status - Service_Active

List_Size - 7

List_Dn -

6136634567; 6136638901; 6136671001

6136671023; 6136789021; 6136779001

6136772021;

If the DN is not provisioned with the service, then the following error message displayed:

>Syntax to query status of CSMI on 6136671021

>svcntrl query 6136671021 CSMI status

Failure - Unavailable_Resources

115.4 The Update command

Depending on the feature, the Update command can be used to update different attributes such as the status, the delay interval, the forward DN and so on. When issued at the CI prompt, the Update command will take the input parameters and call the Update procedure for that feature. Depending on whether the feature is updated or not, the corresponding return code is output.

115.4.1 Update Request

For an Update request, the following are the input parameters

- The DN of the subscriber associated with the given request will be a 10 digit DN.
- The corresponding service will be represented as a simple enumerated type similar to the one defined in SERVORD and representing all supported services.

- The action to be taken will be represented as a simple enumerated type representing all supported actions.

115.4.2 Update Response

Will include the following:

Return codes indicating non availability of the API (ie is the CI SOC idle)

- The return code will be in the form of readable text.

Return codes indicating the confirmation or denial of the Update request.

- Simple enumerated type representing all supported Update return codes.
- The return code will be displayed as readable text.

  For example, confirmation from an Update request to activate CSMI would be represented as “Success - Service_Activated”.

115.4.3 List of supported Update Actions

The following table gives the list of actions that is supported for each service.

Table 4 List of supported Update Actions

Enumeration	Description
activate	Activate corresponding service.
deactivate	Deactivate corresponding service.
delayInterval	Set delay interval for corresponding service.This is the number of rings.
adddn	Add specified DN to corresponding service’s screening list.
deletedn	Delete specified DN from corresponding service’s screening list.
deleteAlldn	Delete all DNs from corresponding service’s screening list.
deleteAllPrivdn	Delete all private DNs from corresponding service’s screening list.
setfwdDN	Set forwarding DN for corresponding call diversion service.
clearFwdDN	Clear forwarding DN for corresponding call diversion service.
toggle	Toggle status of the corresponding services.
invoke	Invoke the corresponding service.
changeList	Change a specified speed call cell entry.

115.4.4 Service to Update Action matrix

Each service belongs to a group from group1 to group9. These groups are based on the attributes of each service. The matrices below show the attributes present for each service.

Table 5 Service to Update Action matrix

Service	Activate	Deactivate	DelayInterval	Addn	Deletedn	DeleteAlldn	Delete All Privatedn	Set Fwd Dn	Clear Fwd DN	Toggle	Invoke	Change List
MWI	X	X										
VMWI	X	X										
AMWI	X	X										
ACRJ	X	X										
ACB	X	X										
AR	X	X										
CSMI	X	X										
CWT	X	X										
LDSA	X	X										
MSB	X	X										
SUPPRESS	X	X										
DRCW	X	X		X	X	X	X					
SCRJ	X	X		X	X	X	X					
SIMRING	X	X		X	X	X						
CFU	X	X						X	X			
CFDA	X	X						X	X			
CFB	X	X						X	X			
SCA	X	X		X	X	X	X					
SCF	X	X		X	X	X	X	X	X			
CFDVT			X									
CNDB										X		

Service	Activate	Deactivate	DelayInterval	Addn	Deletedn	DeleteAlldn	Delete All Privatedn	Set FwdDn	Clear FwdDN	Toggle	Invoke	Change List
CNAB										X		
COT											X	
CCW											X	
SCS												X
SCL												X
SCU												X

Update Examples
Syntax to activate Call Forward BusyLine on 4164731051

>svcntrl update 4164731051 cfb activate

Success - Service_Activated

Syntax to clear the forward DN on 4164731051

>svcntrl update 4164731051 cfb clearFwdDn

Success - ForwardingDn_Cleared

>svcntrl update 4164731051 cfb setFwdDn dn 4164631001

Success - ForwardingDn_Set

Error conditions:

If we try to activate an already activated service

>svcntrl update 4164731051 cfb activate

Failure - Service_Already_Active

If the user tries deleting a list which is empty, the response would be

>svcntrl update 4164731051 simring deleteallDN

Failure - List_Is_Empty

If the SOC for SPRING (call forward ringing) is not turned on, the response would be

>svcntrl update 4164731051 cfdvt delayInterval 4

Failure - Unavailable_Resources

Ex6: If the parameters entered are insufficient

>svcntrl update

The response would be:

Failure - Missing_Parameter

115.4.5 List of supported Update responses

Table 6 List of supported Update responses

Response	Meaning
Success - Service_Activated	Successful activation of the service.
Success - Service_Deactivated_or_Cancelled	Successful deactivation of the service.
Success - AnonymousEntry_Added	Successful addition of a private no. to the list of a DN.
Success - PublicEntry_Added	Successful addition of a DN to the list of another DN.
Success - AnonymousEntry_Removed	Successful deletion of a private number from a DNs list.
Success - PublicEntry_Removed	Successful deletion of a DN from a DNs list.
Success - All_Anonymous_Entries_Removed	Successful deletion of all private DNs from the list.
Success - All_Entries_Removed	Successful deletion of all DNs from the list.
Success - ForwardingDn_Set	Successful setting of a FwdDN to another DN.
Success - ForwardingDn_Cleared	Successful clearing of a FwdDN from another DN.
Success - DelayInterval_Updated	Successful updation of delay interval of a DN.
Failure - Service_Already_Active	Not updated because the service is already active on the DN.
Failure - Service_Not_Activated	Gives this response because the service might be inactive and the user is trying to deactivate or in the case of ACB/AR if the feature queue is not present.
Failure -Invalid_Forwarding_Dn	FwdDN not set because the FwdDN did not pass validation.

Response	Meaning
Failure - List_Is_Empty	When trying to delete a DN from the list of another DN and if the list is empty.
Failure -List_Is_Full	When trying to add a DN to the list of another DN and if the list is full and cannot accommodate more DNs.
Failure - Public_Dn_Already_On_List	If the DN you are trying to add to the list of another DN is already present.
Failure - Anonymous_Dn_Already_On_List	If the private DN you are trying to add to the list of another DN is already present.
Failure - Dn_Not_On_List	If the DN you are trying to delete is not on the list.
Failure - No_Match	When trying to update the delay interval, if the ring control is not programmable ring type.
Failure - Unsuccessful_Update	This message comes when the update is not successful and for different features and actions, are different.
	For ACB/AR, activation of the feature is not supported.
	For CFB, if Fixed or Programmable version is not provisioned.
	For CFBL & CFDA, with control N type.
	FOR CFDA if IECFD is provisioned or if CFD Normal is provisioned.
	For Speed Call, if SCU is provisioned.
	For services that use SLE, if SLE datafills are missing in Table CUSTSTN.

115.4.6 Error codes for the update command

Table 7 Error codes for the Update Command

Return Code	Description
Failure - Invalid_Dn	DN entered is not valid.
Failure - MSRID_Does_Not_Match_User_Profile	For all types of MWT an Msr Id has to be input.This will be validated against Table MSRTAB.If there is a mismatch, then it returns this code.

Return Code	Description
Failure - Unavailable_Resources	The service is not subscribed on the DN.
	The feature SOC is idle.
	For ACB and AR, checks the validity of the feature and if the feature is not allowed gives this response.
	For ACRJ, COT if universal access is not permitted.
	For CFB, if IECFB is provisioned.
	For CFD, if IECFD is provisioned.
	For CFU, if CFU/CFI/CFF is not provisioned.
	For CNAB & CNDB, if the call is not up.
	FOR MWI, if EMW or CALLOG is assigned to the line.
	The SLE SOC is idle.
	Deactivate MWT when MWT is not active
Failure - SOC_Idle	The SVCNTRLl SOC is idle.

115.5 Error responses for Invalid Entries

Table 8 Error responses for invalid entries

Return Value	Description
Failure - Invalid_Action	When any other value other than update or query is entered after svcntrl.
Failure - Invalid_DNformat	When the DN entered has alpha numeric values or if the DN is not of 10 digit form.
Failure - Unrecognized_Service	When the service entered is invalid.
Failure - Invalid_Attribute	When the attribute entered for that service is invalid.
Failure - Invalid_Attribute_Parameter	When the parameters for the attributes are specified incorrectly. For e.g., if the value of delay interval to be updated is greater than 10.
Failure - Missing_Parameter	When an incomplete command is issued, i.e. if the service, attribute, or any of the parameters are missing.

Ex 1: When the action given is not update/query

>svcntrl updation 6136631001 acrj activate

The response would be:

Failure - Invalid_Action

Ex2: If the DN is invalid

>svcntrl query abc6790123 drcw list

The response would be:

Failure - Invalid_DNformat

Ex3: If the DN entered is not 10 digit

>svcntrl query 6631001 cfb ForwardDN

The response would be:

Failure - Invalid_DNformat

Ex4: If the service is not valid

>svcntrl update 6136671021 cssi activate

The response would be:

Failure - Unrecognized_Service

Ex5: If the attribute is not valid for that service

>svcntrl update 4164671021 cndb FwdDn

The response would be:

Failure - Invalid_Attribute

EX7: If the attribute parameters are invalid

>svcntrl update 4164671001 cfdvt delayInterval 65

The response would be:

Failure - Invalid_Attribute_Parameter

Ex6: If the parameters entered are insufficient

>svcntrl update

The response would be:

Failure - Missing_Parameter

>svcntrl query scs

Failure - Missing_Parameter

115.6 Hardware Requirements or Dependencies

In order to enable this capability for affected subscribers, the following must be present in the provider's network

- Some Provider Network Server designed to support service queries/ updates via some Web or PC Client based interface.
- SESM/OSSGATE - An application that is used for the provisioning and maintenance of lines, trunks etc. The OSSGATE passes on the command information to the SDM.
- SDM /CS2K Core Manager - The SDM is an interface to the core. It takes in the commands given by the SESM and passes them onto the core and also takes the responses from the core and gives it to the SESM.

115.7 Software Requirements or Dependencies

The new SOC XXX will control the CI interface to Service Management. This XXX SOC will be independent of the AIN TCAP Service Management SOC control. The following table gives the possible supported state of both the SOCs:

Table 9 Supported SOC States

AIN SOC	Service Management SOC	Implication
ON	ON	Both interfaces will be active at the same time.
IDLE	IDLE	Both interfaces will be inactive at the same time.
ON	IDLE	AIN interface to be active and SVCNTRL to be inactive.
IDLE	ON	AIN interfaces to be inactive and SVCNTRL to be active.
ON for some	ON	Some combination of AIN interfaces active and SVCNTRL active.
ON for some	IDLE	Some combination of AIN interfaces active and SVCNTRL inactive.

115.8 Limitations and restrictions

This capability will be applicable only to North American loads. If some invalid characters are entered after a valid command, then the command will not be rejected. The command will be processed with the valid input. Refer to A00004036 FN for the limitations and restrictions of each service.

115.8.1 List of supported services/features

The following table gives the list of supported services/features the market that they are valid for.

Table 10 Supported Services/Features

Service	Servord Acronym
Message Waiting Indicator [a]	MWI
Visual Message Waiting Indicator <Superscript1>a.	VMWI
Audio Message Waiting Indicator <Superscript1>a.	AMWI
Anonymous Call Rejection	ACRJ
Automatic Callback	ACB
Automatic Recall	AR
Call Screening<Superscript1>a.	CSMI
Outside Calling Area Alerting<Superscript1>a.	LDSA
Calling ID delivery & Suppression	SUPPRESS
Call Waiting(requires CWTACT)	CWT
Make Set Busy	MSB
Distinctive Ringing Call Waiting [b]	DRCW
Selective Call Rejection<Superscript1>b.	SCRJ
Simultaneous Ringing	SIMRING
Call Forward Dont Answer [c]	CFDA
Call Forwarding Variable	CFU
Call Forward Busy Line[d]	CFB
Selective Call Acceptance <Superscript1>a.	SCA
Selective Call Forwarding<Superscript1>a.	SCF

Service	Servord Acronym
Call Forwarding Ringing Control<Superscript1>b.	CFDVT
Calling Number Delivery Blocking	CNDB
Calling Name Delivery Blocking	CNAB
Customer Originated Trace	COT
Cancel Call Waiting	CCW
Speed Calling Short	SCS
Speed Calling Long	SCL
Speed Calling User	SCU

a. North American Market Only
b. North American Dialplan Only

c. This service will include both CFDA and CFD.
d. This service will include both CFBL and CFB.

115.8.2 List of supported DN specifiers

Table 11 Supported DN Specifiers

Enumeration	Description
user	DN being added or deleted provided explicitly by the subscriber.
speed call	Add/Delete the DN in the subscriber's corresponding speed call entry
icm	Add/Delete the DN in the subscriber's Incoming Call Memory.

115.9 Applicable customer facing sections

Fault Management

Logs ___N/A

Alarms ___N/A

Configuration

Data Schema ___N/A

User Interface ___N/A

Element Management ___X

Security ___N/A

Service Order ___N/A

Office Parameters ___N/A

Accounting (includes AMA billing) _____X

Performance (includes operational measurements) _____X

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with "N/A" if these sections do not apply to this functionality.

Realtime ___N/A

Engineering Information ___X

115.10 Glossary

Table 12 Glossary

Term	Description
SDM	Supernode Data Manager or CS2K Manager
SESM	Succession Element Sub element Manager

115.11 References

A00004036 - Off Board Service Control

116: Functional description (FN): A00010329

116.1 Feature name and Feature ID

A00010329 - Remove ASPEN protocol support on PVG

116.2 Introduction

In 1999, when MG7K/MG15K was first introduced, ASPEN was used as the only Signalling and Call Control protocol between Gateway Controller (GWC) and the MG7K/15K Gateway. Several years later in 2003 (SN06), standards based H.248 was introduced. Over time, H.248 has been the protocol of choice for most customers.

From SN09/PCR7.1 onwards, ASPEN will no longer be supported in a Succession solution. This feature removes the ASPEN protocol support on PVG from SN09/PCR7.1.x onwards on Switched AAL2 and Switched IP, NT0482AB VSP2 7K, NTHW87AB VSP2 15K, NTHW84AA, VSP3, and NTHW77AA VSP3-o.

During HSM, customers cannot upgrade to SN09/PCR7.1 with ASPEN provisioned. Appropriate error message is displayed informing customer to upgrade to H.248 prior to upgrading to SN09/PCR 7.1.x. The craft person is required to upgrade to H.248, prior to migrating to SN09/PCR7.1.

116.3 Terminology

The list of various terminology used in the document are:

- PVG Packet Voice Gateway
- GWC Gateway Controller
- CAS Component Administration System
- PCR Passport Carrier Release
- H.248 A Media Gateway Control Protocol
- Nsta NarrowbandServicesTrunkOverATM
- MG Media Gateway
- Vgcp VoiceGatewayControlProtocol
- HSM Hitless Software Migration

117: Functional description (FN): A00010452

117.1 Feature name and Feature ID

A00010452 LANComm Multi-home Enhancements

117.2 Description

This feature will add enhancements to existing functionality to allow the Ethernet Interface Unit (EIU) to integrate better into existing customer network topologies. By extending the Internet Protocol (IP) address assignment range and relaxing the current rule that govern what IP addresses can be assigned to EIUs equipped as interfaces, this feature will provide the ability to home the core onto any IP network regardless of it's IP class. In addition, this feature allows the SUBNET value for any interface to be independent of all other entries data filled on the core.

In addition to increased flexibility in the assignment of IP interfaces, enhanced checking will be added to table control for table IPNETWRK that will vlidate each entry to make sure that as entered, the interface will perform as expected. Some of these enhancements include:

SUBNET value range checking based on the IP class

Prevention of overlapping IP subnets with different SUBNET values

Special handling of interfaces with the IRM_INTERFACE parameter

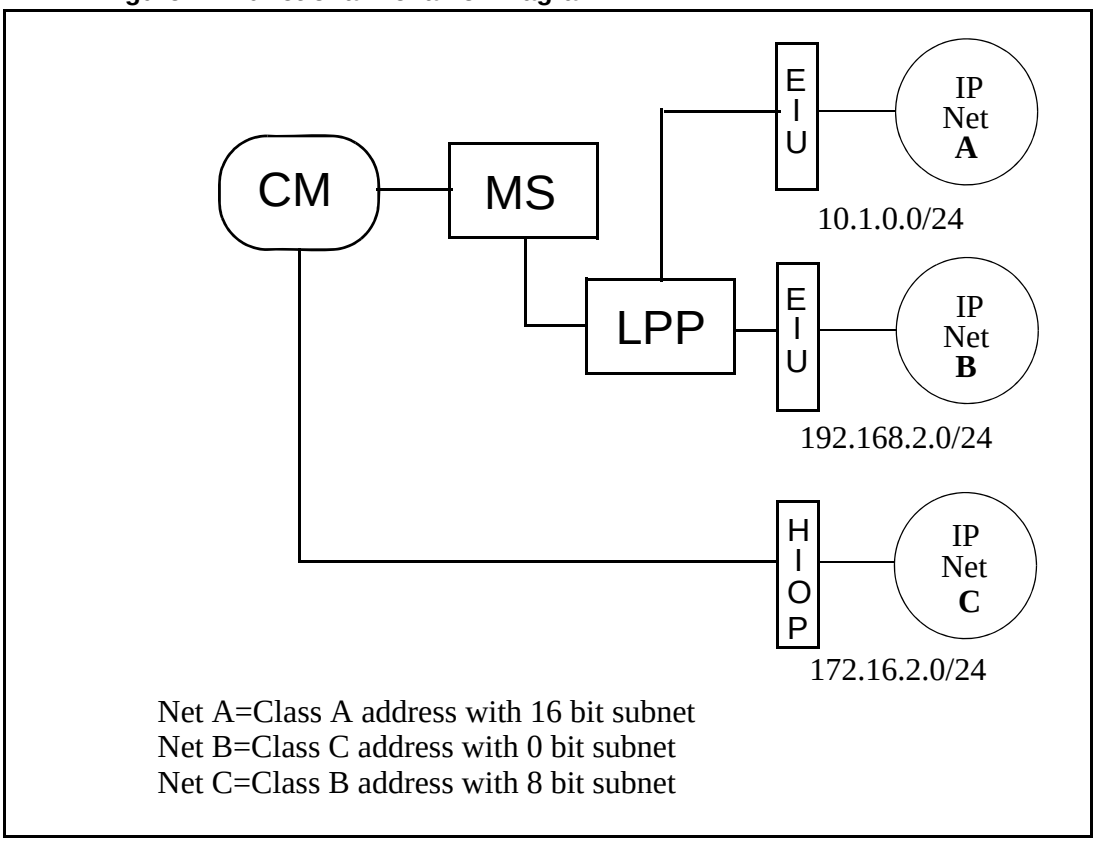
Entry with IRM_INTERFACE can not have DFLT_INTERFACE Y

Current network topologies used for Succession solutions have the EIUs homed onto the customer OAM&P network. The HIOP is normally homed onto the call processing network. These two networks traditionally are in different address spaces and network class. Feature A00002510 introduced the ability to assign an HIOP as an interface in table IPNETWRK. This was done to allow the HIOP to use the Transmission Control Protocol (TCP) transport layer in the LANCOMM TCP/IP stack.

In order to support such an arrangement, the LANCOMM stack needs to be able to support multiple network classes for EIUs and HIOPs equipped as interfaces to the XA-Core. This will require changes to the internal data structures that are used to perform such things as source and destination IP address validation for incoming and destination IP address validation for outgoing packets. This feature will make the necessary changes to support

homing the XA-Core onto different networks regardless of their class. Figure 1 shows a typical multi-homed arrangement that can be support by this feature.

Figure 1 Functional Behavior Diagram



117.3 Hardware Requirements or Dependencies

None.

117.4 Software Requirements or Dependencies

None.

117.5 Limitations and restrictions

This feature will not alter the way in which an Ethernet Interface Unit (EIU) equipped as a router (EIUs data filled in table IPROUTER) currently function. The restrictions that currently exist for EIUs equipped as routers are that all IP addresses for all EIUs equipped as routers must reside in the same IP class and network.

117.6 Interactions

None.

117.7 Glossary

Term	Description

118: Functional description (FN): A00010490

118.1 Feature name and Feature ID

A00010490CS2M - Adding Support MCPN905-270 card in SAM21 EM (Corrective)

118.2 Purpose

In this CAF, two new variants of the Motorola MCPN905 hardware for the Universal Signaling Point (USP) and Call Agent (CCA) are being introduced. The new hardware for USP is the MCPN905 866MHZ 512MB card, and the new hardware for CCA is the MCPN905 1GHZ 2GB. This feature is an add-on to the A00007564 feature which introduced the MCPN905 1GHz 512MB card for the GWC Software. Since all the maintenance actions supporting the 905 card are already added in the feature A00007564, this CAF will only add the CCA enable on MCPN905 1GHZ 2GB to the SAM21 EM.

After this feature, there are total three types of MCPN905 card supported:

- 905 for GWC = 905-240
- 905 for USPc = 905-220
- 905 for CCA = 905-270

118.3 Problem symptoms

This feature is a function enhancement feature.

1. Enable support for the MCPN905-270 card in SAM21 EM.

2. Add the CCA service provision on MCPN905-270 card.

3. Verify that CCA is fully supported by MCPN905-270 and USPc is fully supported by MCPN905-220.

118.4 Description of fix

This feature introduces the MCPN905-270 card support to SAM21 EM. The card supporting and related maintenance actions for this card are added in the feature A00007564. This feature enables the customer to provision CCA to this card, and to do the maintenance test to verify whether this card can work well with the SAM21 shelf and that USPc and CCA can be provisioned successfully.

118.5 Customer facing documentation changes

N/A

118.6 Enabling the MCPN905-270 for CCA

Complete the following steps.

1. Insert into the SAM21 shelf a MCPN905-270 card with 2GB of memory.

2. Verify that the Shelf View displays the card on the corresponding slot and that it marks the card “No Service”.

3. Right click the card and bring up the card view.

4. Switch to the equip tab, verify the card name is “MCPN905” and the memory is “2048M”.

5. From the Shelf View of the SAM21 EM client, right click the card’s slot and then select “Assign Service”.

6. A pop-up dialog entitled “Service Assignment” appears that includes a “Call Agent” option.

7. Select “Call Agent” and provision the card.

8. Verify that the first two MAC addresses are displayed on the provision dialog.

9. Verify that the Shelf View changes the display for that card from “No Service” to “Call Agent”.

10. Verify the bootptab information for this GWC card is stored in SSPFS (/ etc/ bootptab).

11. You have completed this procedure.

119: Functional Description (FN) A00010567

119.1 Feature name and Feature ID

Corrective CAF: A00010567: CS2M - G729 CODEC for AAL2

119.2 Purpose

In the current CS2kmt implementation, the network codec combinations for AAL2 network only include
G.711 a-law
G.711 u-law
G.711 a-law, G.711 u-law
G.711 u-law, G.711 a-law
G.726-32, G.711 a-law, G.711 u-law
G.726-32, G.711 u-law, G.711 a-law

This CAF will add six new combinations for AAL2 as customers request, which are
G.729, G.711 a-law
G.729, G.711 u-law
G.729, G.711 a-law, G.711 u-law
G.729, G.711 u-law, G.711 a-law
G.726-32, G.711 u-law
G.726-32, G.711 a-law

Note that from SN09 version the terminologies G.711 u-law, G.711 a-law are translated to PCMU, PCMA, respectively.

119.3 Problem symptoms

Previously only six codec combinations for AAL2 are allowed. If users input a combination like “G.729, G.711 a-law” and click OK button, a warning dialogue will be popped up with following message “Codec selection is invalid. Please modify it and try again. For more information about valid codec selections, please refer to the help document.

If users check the help document, they will find the following information.

AAL2	G.726-32	PCMA	PCMU
	G.726-32	PCMU	PCMA
	PCMA	PCMU	
	PCMU	PCMA	
	PCMA		
	PCMU		

The codec combination users selected is shown in field “Codec Selection”.

The help document will be

AAL2	G.726-32	PCMA	PCMU
	G.726-32	PCMU	PCMA
	PCMA	PCMU	
	PCMU	PCMA	

120: Functional description (FN): A00010617

120.1 Feature name and Feature ID

A00010617: Addition of NUERA_BTX4K and MGCP_IAD_40 Gateway certificates lines (Corrective)

120.2 Purpose

In SN09, the gateway certificate/profile “NUERA_BTX4K” is created in order to provision 4032 endpoints on TGCP large trunks gateways in SESM and support DS3 endpoint naming formats (e.g., “ds/ds3-<u1>/ds1-<u2>/[1-24]”). The certificate/profile is needed to support the Nuera BTX-4K gateway which allows 6 DS3s to be provisioned (4032 DS0s – 6x28x24). Up to now, the largest supported TGCP gateway was the Nuera BTX-21 which allowed at most 21 DS1s to be provisioned.

Additionally, the gateway certificate/profile “MGCP_IAD_40” is created in order to provision “Carrier Access Adit 600” MGCP small line gateways in SESM. The “Carrier Access Adit 600” gateway will support up to 40 endpoints (POTS lines).

120.3 Configuration

After the code changes, when associating a media gateway using SESM GUI, in the “Gateway Profile Name” pull down list, the following new profile names in addition to the existing profiles will show up as a selection choice.

- NUERA_BTX4K
- MGCP_IAD_40

The characteristics of the above gateways are listed in the following table.

GW Profile Name	GW Cate-gory	Signal Protocol	Protocol Version	Protocol Port	Service Type	Port/EP Capacity	GWC Profile No.
NUERA_BTX4K	Large	tgcp(6)	1.0	2427	Trunk	4032	60
MGCP_IAD_40	Small	MGCP(5)	1.0	2427	Line	40	49

When filling in the “Protocol Type”, “Protocol Version” and “Protocol Port” fields in the “Associate Gateway” dialog using SESM GUI, please enter in what’s specified in the above table.

When creating an OSSGATE input XML file for associating a “NUERA_BTX4K” or “MGCP_IAD_40” gateway, please reference the above table for values of the tags <mgProfileName>, <mgProtocolType>, <mgProtocolVersion>, and <mgProtocolPort>.

After the introduction of the NUERA_BTX4K certificate/profile, when adding a carrier using SESM GUI, in the “Add Carrier” dialog box, the following carrier name format can be specified in the “Carrier name:” field:

- ds/ds3-<u1>/ds1-<u2>

120.4 Related Documentation

N/A

121: Functional Description (FN) A00010742

121.1 Feature name and Feature ID

GWC EM Enhancements to Support SIREN - A00010742

121.2 Description

In Succession, the provisioning of a Gateway Controller Card (GWC) is performed by the GWCEM/SESM and the SAM21 software components.

The SAM21 component is responsible for provisioning sufficient card data to identify the card (e.g., the IP addresses and the software load file location), and to initiate the booting of the GWC application.

The GWCEM/SESM component is responsible for provisioning all other data required for the GWC to operate as a switch (e.g., gateway data, endpoint data, alarm processing, trap processing, IPSEC data, middle boxes, timing parameters, sizing limitations, capabilities, etc.). Also included is an array of activities which include, for example, the ability to audit, monitor, patch, alarm, initiate card imaging, core provisioning and synchronization, and general health and maintenance of the GWC devices and their application processing.

For Siren, the SAM21 component is being replaced by various Siren subsystems (e.g., Config, AMF, and MTCE). In addition, the GWC application itself is being moved onto new Siren blades, and may be modified to use new interfaces within the Siren platform.

The GWCEM/SESM software will still reside on the Sun N240 SSPFS platform. The items implemented by this feature are the design changes required for the GWCEM and the SESM software to function correctly with the removal of the SAM21 component, and to address any changes required in the GWCEM to GWC interfaces made as a result of the GWC incorporation into the new Siren architecture.

This feature implements the changes required to allow the GWCEM/SESM to provide the same provisioning functionality with the newly based GWC on the Siren ATCA platform.

121.2.1 User Interface Changes

There are two user interface changes made by this activity in the GWC EM GUI.

1. In Siren configuration, the ability to bring up the SAM21 card view of the GWC card is removed, and the warm and cold swact buttons are replaced with a single ‘swact’ button. There is no change for Carrier VoIP installations.
2. In both Siren and Succesion configurations, the ‘Add GWC’ dialog box will now prompt only for GWC name and not the IP address. The IP addresses will be determined internally by the hardware management software.

There is also one change made to the OSSGate XML schema. For the add GWC (addGWCtoCS) operation, the GWC IP address will now be looked up using the GWC name (gwcUIName). Therefore, the active IP address (gwcActvIp) is no longer required by the EM software and is being made optional. Note that this parameter may still be specified, but it will be ignored.

121.3 Hardware Requirements or Dependencies

For customers continuing with the Succession product line, there are no new hardware requirements.

For customers choosing the Siren product line, there are no new hardware requirements specifically for this activity, but changes are made to the current GWC EM software to work with the new Siren product line.

121.4 Software Requirements or Dependencies

For customers continuing with the Succession product line, there are no new software requirements or dependencies.

For customers choosing the Siren product line, there are no new software requirements specifically for this activity, but changes are made to the current GWC EM software to work with the new Siren product line.

121.5 Limitations and restrictions

This feature does not address Succession to Siren migration for SESM/GWC EM.

121.6 Interactions

Not Applicable

121.7 Glossary

Term	Description
GWC	Gateway Controller
EM	Element Manager

122: Functional Description (FN) A00010880

122.1 Feature name and Feature ID

A00010880 - ABI SMU Support

122.2 Description

This activity adds support for the SMU (Subscriber Module Urban) and its subtending RCU (Remote Concentrator Urban) to the list of legacy PMs supported by the ABI program. The ABI program allows legacy host XPMs to be connected to the packet network without use of an ENET and an I/W Bridge. Instead the XPM is connected to an ABI card in the MG9K via its legacy DS-512 interface. The MG9K in turn provides connectivity to the packet network. This feature will support only the IP version MG9K.

The main customer viable changes for this activity will be the ability yo provision the EXTDS512 optional field as part of the tuple in table LTCINV for the SMU Peripheral Type. The optional field is used to identify the IP Address of the ABI Card and the Gateway Controller that the peripheral is 'hosted' off (the GWC must be datafilled in table SERVRINV prior to entering this information). A full description of the table control changes is available in the Data Schema section of this document (part of the Configuration chapter).

No RMM functionality will be supported off an ABI SMU. To support line test on the RCUs, the test configuration will be via an RMM off an ABI LTC/LGC or off an ABI SMA2.

This feature also allows the ABI SMU to be support in MG9K ESA.

122.3 Hardware Requirements or Dependencies

There are no hardware requirements for this project.

122.4 Software Requirements or Dependencies

The CM changes will be in SN10. Some core software will be submitted in tthe SN09 timeframe to make patchback to SN09 easier. The GWC changes will be in GC100. The SMU load is currently frozen. The last load was built in the XPM13 time frame out of the XPM13BC context. The XPM portion for the SMU loads will be patched back to XPM13.

122.5 Limitations and restrictions

- LDT PSAP (Line Digit Trunk Public Safety Answering Point) will not be supported off an ABI SMU.
- RMMs will not be supported off an ABI SMU.

- ABI SMU is supported in MG9K ESA but ISDN functionality will not be supported while in ESA. Currently, ISDN is not supported on any ABI XPM while in ESA.
- The SMU supports PPhones by using the D-channels provides by the ISP (ISDN Signalling Processor) and DCH (D-Channel Handler) cards. Because ISDN is not supported in MG9K ESA, the SMU will not support PPhones in MG9K ESA.
- Only the IP version of the MG9K is suported. The ATM version is not supported.

122.6 Interactions

This new code will need to interact with the existing ABI framework for link maintenance, packet connection setup, and MG9K ESA.

122.7 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema ___X__

User Interface ___X__

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

122.8 Glossary

Term	Description
ABI	Access Bridging Interface
LDT PSAP	Line Digit Trunk Public Safety Answering Point
RCU	Remote Concentrator Urban
RMM	Remote Maintenance Module
SMU	Subscriber Module Urban

123: Functional Description (FN) A00011167

123.1 Feature name and Feature ID

A00011167 - MG9KEM - Central Userid and Password Support

123.2 Description

This activity enables central IEMS/ Radius authentication of the MG9K userid and password for EM SFTP access to the MG9K. The userid and password will be configured on a per MG9K Element Manager (EM) basis in addition to an NE basis. If Radius is not available when the EM communicates with the MG9K, the NE-level userid and password will be used for authentication instead of the EM-level userid and password. If the Radius is available, there will not be an attempt to authenticate using the NE-level userid and password.

The same userid and password must be configured on the EM and Radius. At the EM, the EM-level userid and password will be configured using a new GUI that is accessed at the subnet level. A warning message will inform the user that the EM-level userid and password will be used instead of the NE-level userid and password. The EM-level userid and password will be stored in the EM Oracle database.

123.3 Hardware Requirements or Dependencies

None.

123.4 Software Requirements or Dependencies

This feature will be delivered in the SN09 software release.

123.5 Limitations and restrictions

For the Radius server authentication to work correctly, when the central userid and password is changed at the Radius server, the EM level userid and password must be changed to match the Radius central userid and password. Note that if an NE-level userid and password happens to match the Radius userid and password, the authentication will work if the Radius server is not available.

123.6 Interactions

None

123.7 Glossary

NA

124: Functional Description (FN) A00011281

124.1 Feature name and Feature ID

A00011281 - MS2000 IPSec Configuration via IEMS

124.2 Description

This feature adds IPSec and IKE configuration capabilities to the MS2000 node configuration tool introduced in SN08. This will allow the craftsperson to enable IPSec for secure messaging between the IEMS and MS2000 as well as configure the IPSec and IKE parameters necessary for the MS2000 to securely send and receive messages to and from the GWC.

See the configuration section for full details on the new functionality.

124.3 Hardware Requirements or Dependencies

No specific requirements beyond what is necessary to support the SN09 software.

124.4 Software Requirements or Dependencies

SN09 IEMS and SSPFS.

SN08 or later MS2000 (?)

124.5 Limitations and restrictions

The MS2000 node does not support in-service updates to IPSec configuration data. Any changes to the IPSec data requires a reset of the MS2000 node.

124.6 Interactions

This feature extends the MS2000 configuration tool introduced in SN08 on the IEMS. It adds an additional tab to the tool that allows for the configuration of IPSec.

124.7 Glossary

Term	Description
IEMS	Integrated Element Management System

125: Functional Description (FN) A00011533

125.1 Feature name and Feature ID

A00011533: Support of SIP DID Trunks on Session Server Trunking

125.2 Description

This feature provides IETF compliant SIP and SIP-T interface for interworking between switches and/or any other third party SIP servers.

Session Server Trunking (SSt) will replace VRDN to provide SIP functionality/interface. This feature can be sub-divided into following components:-

- Preserve existing SIP-T functionality provided by VRDN
- Support MTX DID trunk type on the SST
- Provide enhanced ANSI ISUP parameter mapping to SIP to support SIP interface to remote switch and/or third party SIP servers.
- Support Session Timer (RFC 4028)

Both SIP and SIP-T are supported by SST. Provisioning via web GUI allows to configure a remote server to support either SIP or SIP-T. Note that simultaneous SIP and SIP-T interface to a remote server is not supported.

There are no design changes anticipated for supporting MTX DID trunks over SIP-T interface. Its an integration test activity.

All development work will be done in SN09+ stream and patched back to SN09.

SIP interface requires mapping of ISUP parameters in MTX DID trunks into SIP headers and parameters. Currently SSt supports IT and IBNT2 trunks. This feature builds on top of existing functionality in SST to support MTX DID specific parameters and features.

The following table lists the ISUP parameters and their mappings into SIP and vice-versa. The SIP parameters in **bold** are either impacted or introduced by this feature.

Table 1: ISUP to SIP to ISUP mappings

ISUP Param	ISUP to SIP		SIP to ISUP		Comments
	ISUP	SIP	SIP	ISUP	
Nature of Connection	Satellite Indicator	**sat-hops=**	**sat-hops=**	Satellite Indicator	New Param in Request URI **Nortel Prop.**
	Cont Check Indicator			0 No_check	No mapping - Default Only TDM side is supported
	Echo Supress Indicator			1 Half_Echo_Sup	No mapping - Default Assumed to be done by both ends

Table 1: ISUP to SIP to ISUP mappings

ISUP Param	ISUP to SIP		SIP to ISUP		Comments
	ISUP	SIP	SIP	ISUP	
Forward Call Indicator	ISUP_Call Type				No mapping - GUI Provision
	E_to_E_Method			0 No_E_to_E_Method	No mapping - Default
	ISUP_Interworking				No mapping - GUI Provision
	E_to_E_Info_Check			0No_E_to_E_Info	No mapping - Default
	ISDN_UP_Ind				No mapping - GUI Provision
	ISDN_UP_Pref_Ind				No mapping - GUI Provision
	ISDN_Access_Ind				No mapping - GUI Provision
	Trans_Called_Num_Ind	npdi=yes rn=CPN	npdi=yes rn=CPN	Trans_Called_Num_Ind	URI params RFC 3398
	Routing_Attempt_Ind			0 No_Routing_Attempt	No mapping - Default
Calling Party Category	cpc	**cpc=**	**cpc=**	cpc	User Info in both PAID header and From header **Nortel Prop.**

Table 1: ISUP to SIP to ISUP mappings

ISUP Param	ISUP to SIP		SIP to ISUP		Comments
	ISUP	SIP	SIP	ISUP	
User Service Information	Xmission Medium			0	No mapping - Default
	Info Xfer Cap			#10 Audio 3_1_Khz	No mapping - Default
	Coding Standard			0 STD_CCITT	No mapping - Default
	Info Xfer Rate				No mapping - Derived
	Xfer mode			0 Circuit	No mapping - Default
	Layer 1 Info			#02 or #03 A-law or U-law	No mapping - Derived
	User Rate			0 - Nil	No mapping - Default
	Synchroni-zation			0 Sync	No mapping - Default
	Negotiation			0 NOT_INBAND	No mapping - Default
	Message Priority			1	No mapping - Default

Table 1: ISUP to SIP to ISUP mappings

ISUP Param	ISUP to SIP		SIP to ISUP		Comments
	ISUP	SIP	SIP	ISUP	
Called Party number	Even_Odd_ Ind			Even/Odd	Derived from digits
	Nature_of_ Address				Derived from digits and GUI provisioning
	Numbering _plan				Derived from digits and GUI provisioning
	Address_inf ormation	Request URI	Request URI	Address_inf ormation	RFC 3261
Calling Party Number	Even_Odd_ Ind			Even/Odd	Derived from digits
	Nature_of_ Address				Derived from digits and GUI provisioning
	Addr_Pres_ Restricted_I nd	Privacy Header	Privacy Header		History Info Draft
	Numbering _plan				Derived from digits and GUI provisioning
	Address_inf ormation	PAID	PAID	digits	RFC 3325
HopCounter	counter value	Max-For-wards	Max-For-wards	counter value	Mutliplied by Max-Forwards factor RFC 3261

Table 1: ISUP to SIP to ISUP mappings

ISUP Param	ISUP to SIP		SIP to ISUP		Comments
	ISUP	SIP	SIP	ISUP	
Charge Number	NOA	**noa=**	**noa=**	NOA	New param in a new SIP header **Nortel Prop.**
	Odd Ind			odd/even	Derived from digits
	Numering Plan				Derived from digits
	Address	**charge:<addr-spec>**	**charge:<addr-spec>**	address	New SIP header **Nortel Prop.**
OLI	OLI	**oli=**	**oli=**	oli	User Info in both P-Asserted-ID header and From header **Nortel Prop.**
CIP	cic	**cip=**	**cip=**	cic	User info in Request URI **Nortel Prop.**
	Network_Id	**netid=**	**netid=**	Network_Id	User info in Request URI **Nortel Prop.**
	Network_Plan			4-digits	No Mapping - Default **Nortel Prop.**

Table 1: ISUP to SIP to ISUP mappings

ISUP Param	ISUP to SIP		SIP to ISUP		Comments
	ISUP	SIP	SIP	ISUP	
TNS	Network_Id	**netid=**	**netid=**	Network_Id	User info in Request URI **Nortel Prop.**
	Network_Plan			4-digits	No Mapping - Default
	cic	**cic=**	**cic=**	cic	User info in Request URI **Nortel Prop.**
	circuit code	**sc=**	**sc=**	circuit code	User info in Request URI **Nortel Prop.**
JIP	jip	**jip=**	**jip=**	jip	User Info in both P-Asserted-ID header and From header **Nortel Prop.**
Original Called Number Redirecting Number	NOA_ind				Not Mapped - Derived
	Addr_Pres_Restricted_Ind	**Privacy:**	**Privacy:**		Privacy header in History Info Draft
	Address	**URI in History Info**	**URI in History Info**	Address	History Info Draft
Redirecting Information	Counter	**Index=**	**Index=**	counter	Param in History Info Draft
	Reason	**Reason: Q.732, text=**	**Reason: Q.732, text=**	Reason	Reason Header in History Info Draft
Generic Address	address	Request URI	Request URI	address	

Table 1: ISUP to SIP to ISUP mappings

ISUP Param	ISUP to SIP		SIP to ISUP		Comments
	ISUP	SIP	SIP	ISUP	
Generic Name	Type			#1 calling	Not Mapped - Default
	Availability			0 available	Not Mapped - Default
	Presentation	PAID	PAID	Presentation	RFC 3325
	Name	PAID	PAID	Name	RFC 3325
Generic Digits	Type	**type=**	**type=**	Type	New Generic Digits header with type param **Nortel Prop.**
	Encoding Scheme				Derived from digits
	Digits	**Gen-Digit:**	**Gen-Digit:**	Digits	New Generic Digits header **Nortel Prop.**

Table 1: ISUP to SIP to ISUP mappings

ISUP Param	ISUP to SIP		SIP to ISUP		Comments
	ISUP	SIP	SIP	ISUP	
BackWard Call Indictors	Charge_ind			#02 charge	No mapping Default
	Called_party_status	180/182/183	180/182/183	Called_party_status	RFC 3261
	Called_party_category			#01 Ordinary	
	E_to_E_Method			0 No_E_to_E_Method_Avail	No mapping - Default
	Interworking_ind				No mapping - GUI Provision
	E_to_E_info			0 No_E_to_E_Info_Avail	No mapping - Default
	Isup_ind				No mapping - GUI Provision
	Reverse_holding_ind			0 Not Required	No mapping - Default
	ISDN_access_ind				No mapping - GUI Provision
	echo_control_dev_ind			0 No_Incoming	No mapping - Default
	sccp_method			0 No_sccp	No mapping - Default
Optional BCI					Not Mapped
Cause Indicator	cause			cause	No mapping - GUI Provision

Table 1: ISUP to SIP to ISUP mappings

ISUP Param	ISUP to SIP		SIP to ISUP		Comments
	ISUP	SIP	SIP	ISUP	
UUI	Info	**UUI Payload**	**UUI Payload**	Info	New payload type. **Nortel Prop.**
Geodetic Location	Geodetic location	**application/location**	**application/cpim-pidf+xml**	Geodetic location	New payload type. **Nortel Prop.**
Precedence	Level	**Precedence:**	**Precedence:**	Level	New header Precedence value **Nortel Prop.**
	LFB	**lfb=**	**lfb=**	LFB	Param in new header Precedence **Nortel Prop.**
	NetID	**netid=**	**netid=**	NetID	Param in new header Precedence **Nortel Prop.**
	MLPP_SD	**mlpp=**	**mlpp=**	MLPP_SD	Param in new header Precedence **Nortel Prop.**
Carrier Selection	carrier selection	**csel=**	**csel=**	carrier selection	User info of Request URI. **Nortel Prop**.

125.2.1 Satellite Indicator

A new parameter, satellite, will be created and added to the Request URI. The parameter will be defined as follows.

satellite = satellite-tag "=" number-of-satellite

satellite-tag = "sat-hops"

number-of-satellite = 0|1|2|3

Example:

```
INVITE sip:6137222000@47.174.73.240:5060;sat-hops=2 SIP/2.0
From: <sip:6137222010@47.174.73.240:5060>;tag=f-13c4-419b7608-137445-144454f6
To: <sip:6137222000@47.174.73.240:5060>
Call-ID: 41840594f049ae2f13c4419b760813744521850ff89430478-0125-7168
CSeq: 1 INVITE
User-agent: CS2000/NGSS/9.0
X-Nortel-Profile: DEFAULT
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY, PRACK
Via: SIP/2.0/UDP SP2KDON:5060;maddr=47.174.73.240;branch=z9hG4bK-419b7608-137445
P-Asserted-Identity: <sip:6137222010@47.142.211.17;user=phone>
```

125.2.2 Calling Party Category

A new parameter, cpc, will be created in the SIP URI and added to the PA-Id header and From header user information. CPC User info present in PA-ID header overrides user info CPC if present in From header. The parameter will be defined as follows.

cpc = cpc-tag "=" cpc-value

cpc-tag = "cpc"

cpc-value = string

string = { “unknown”|
“op-french” |
“op-english” |
“op-german” |
“ op-russian” |
“op-spanish” |
“cpc-[6, 7, 8]” |
“op-national” |
“ordinary” |
“priority” |
“data” |
“test” |
“non-voice” |
“payphone”|
“voice-information” |
“executive-intrusion" |
“cpc-[18, ..., 21]” |

"mobile" |
"cpc-[23, 24, 25]" |
"mexico-payphone" |
"cpc-[27, ..., 160]" |
"attendant" |
"ac-prec-2" |
"ac-prec-3" |
"ac-prec-4" |
"ac-prec-5" |
"cpc-[166, ..., 223]" |
"emergency" |
"cpc-225" |
"nsep" |
"cpc-[227, ..., 249]" |
"prec-2" |
"prec-3" |
"prec-4" |
"prec-5" |
"cpc-[254, 255]"

}

Example:

```
INVITE sip:6137222000@47.174.73.240:5060 SIP/2.0
From: <sip:6137222010;cpc=payphone@47.174.73.240:5060>;tag=f-13c4-419b7608-137445-
144454f6
To: <sip:6137222000@47.174.73.240:5060>
Call-ID: 41840594f049ae2f13c4419b760813744521850ff89430478-0125-7168
CSeq: 1 INVITE
User-agent: CS2000/NGSS/9.0
X-Nortel-Profile: DEFAULT
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY, PRACK
Via: SIP/2.0/UDP SP2KDON:5060;maddr=47.174.73.240;branch=z9hG4bK-419b7608-137445
P-Asserted-Identity: <sip:6137222010;cpc=payphone@47.142.211.17;user=phone>
```

125.2.3 Charge Number

Charge Number is an optional parameter in IAM message. This parameter will be mapped into a new SIP header.

```
charge = "charge" HCOLON "<" addr-spec ">" ";" noa
noa = "noa" EQUAL  1*DIGIT [1*DIGIT] [1*DIGIT]
```

Table 2: Charge Number NOA Digit Values

Charge NOA DIGIT(s)	GR-317 Definition/Interpretation
0	Unknown/Spare
1	ANI of calling party, Subscriber Number
2	ANI not available not provided
3	ANI of calling party, National Number
5	ANI of called party, Subscriber Number
6	ANI of called party Not Included
7	ANI of called party, National Number
120	Charge Number Operator Collected

An example IAM message:

```
OPTIONAL PART:        CHARGE NUMBER:
                         NATURE_OF_ADDR_IND : CLGP_ANI_SUBSCRIBER_NUMBER
                         ODD_IND :            ODD
                         NUMBERING_PLAN :      ISDN_TELEPHONY_NUM_PLAN
                         ADDRESS : 1234567
```

The resulting SIP message:

```
INVITE sip:6137222000@47.174.73.240:5060;SIP/2.0
From: <sip:6137222010@47.174.73.240:5060>;tag=f-13c4-419b7608-137445-144454f6
To: <sip:6137222000@47.174.73.240:5060>
Call-ID: 41840594f049ae2f13c4419b760813744521850ff89430478-0125-7168
CSeq: 1 INVITE
User-agent: CS2000/NGSS/9.0
X-Nortel-Profile: DEFAULT
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY, PRACK
Via: SIP/2.0/UDP SP2KDON:5060;maddr=47.174.73.240;branch=z9hG4bK-419b7608-137445
P-Asserted-Identity: <sip:6137222010@47.142.211.17;user=phone>
Contact: <sip:47.174.73.240:5060>
Charge:<sip:1234567>;noa=1
```

125.2.4 Originating Line Information (OLI)

OLI may be present in the ISUP IAM message. OLI information is used to identify special calls(hotel/prison etc) and can be used to identify location services available in 911 scenarios.

OLI will be carried in a new parameter added to the PAID header and From header user information. OLI User Info arriving in PAID header overrides OLI user info arriving in From header.

```
oli = "oli" EQUAL 1*DIGIT [1*DIGIT][1*DIGIT]
```

Table 3: OLI Digit Values

OLI DIGIT(s)	GR-317 Definition/Interpretation
0	Normal ANI/No Special Treatment
1	Normal ONI(multiparty)
2	ANI Failure
3	Service Analyzed ANI
4	Service Analyzed ONI
5	Service Analyzed ANI Failure
6	Hotel(without room ID)
7	Coinless Payphone
8	Interlata Restricted
10	Test Call
20	AIOD Listed DN Sent
23	Coin or Non Coin
24	800 Call
25	800 Payphone Call
27	Coin Phone
29	Prison Phone
61	Cellular Services Type 1

Table 3: OLI Digit Values

OLI DIGIT(s)	GR-317 Definition/Interpretation
62	Cellular Services Type 2
63	Cellular Services Type 3
68	Hotel Interlata Restricted
70	Private Pay Phone
78	Coinless Interlata Restricted

Example SIP message(oli is cellular services type 1):

```
INVITE sip:6137222000@47.174.73.240:5060 SIP/2.0
From: <sip:6137222010;cpc=payphone; oli=61@47.174.73.240:5060>;tag=f-13c4-419b7608-
137445-144454f6
To: <sip:6137222000@47.174.73.240:5060>
Call-ID: 41840594f049ae2f13c4419b760813744521850ff89430478-0125-7168
CSeq: 1 INVITE
User-agent: CS2000/NGSS/9.0
X-Nortel-Profile: DEFAULT
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY, PRACK
Via: SIP/2.0/UDP SP2KDON:5060;maddr=47.174.73.240;branch=z9hG4bK-419b7608-137445
P-Asserted-Identity: <sip:6137222010;cpc=payphone; oli=61@47.142.211.17;user=phone>
```

125.2.5 Redirection Parameters

Redirection information is carried in the new header introduced by this feature. History-Info is the header proposed by an IETF draft and is most likely to be converted into a RFC. Current implementation which uses Remote-Party-ID and Diversion headers are still available. Customers have a choice on which method to use per remote server via provisioning choices on the GUI.

Below is an example message to illustrate how the ISUP IAM redirecting params are mapped into a SIP message.

The scenario described here is:

- A calls B
- B is busy and has CFB to C.
- C does not answer and has Call Forward No Answer to D
- The C to D call leg is over SIP.

A = 6137222010; B = 6137222009; C = 6137222015; D = 6137222000

The relevant parts of the IAM look like this:

```
CALLING PARTY :
    EVEN_ODD_IND:                      EVEN_NUM_NIBBLES
    NATURE_OF_ADD :                    NATIONAL_SIG_NUMBER
    ADDR_PRES_RESTRICTED_IND           PRESENTATION_ALLOWED
    NUMBERING_PLAN :                   ISDN_TELEPHONY_NUM_PLAN
    SCREENING_IND  :                   NOT USED
    ADDRESS_INFORMATION = 6137222010
REDIRECTION INDICATOR :
    REDIR_IND :                         REDIR_CALL_FORWARDED
    CFD_INDICATOR :                     TRUE
    ORIG_REDIR_REASON :                 REDIR_USER_BUSY
    REDIR_COUNTER :                     2
    REDIR_REASON :                      REDIR_NO_REPLY
 ORIGINAL CALLED NUMBER :
     EVEN_ODD_IND:                      EVEN_NUM_NIBBLES
     NATURE_OF_ADD :                    UNIQUE_NATIONAL_SIG_NUMBER
     ADDR_PRES_RESTRICTED_IND :         PRESENTATION_RESTRICTED
     NUMBERING_PLAN :                   ISDN_TELEPHONY_NUM_PLAN
     SCREENING_IND  :                   USER_PROVIDED_NOT_SCREEN
     ADDRESS_INFORMATION = 6137222009
   REDIRECTING NUMBER
      EVEN_ODD_IND:                     EVEN_NUM_NIBBLES
      NATURE_OF_ADD :                   NATIONAL_SIG_NUMBER
      ADDR_PRES_RESTRICTED_IND :        PRESENTATION_ALLOWED
      NUMBERING_PLAN :                  ISDN_TELEPHONY_NUM_PLAN
      SCREENING_IND  :                  NOT USED
      ADDRESS_INFORMATION = 6137222015
```

The resulting SIP message:

```
INVITE sip:6137222000@47.174.73.240:5060 SIP/2.0
From: <sip:6137222010@47.174.73.240:5060>;tag=f-13c4-419b7608-137445-144454f6
To: <sip:6137222000@47.174.73.240:5060>
Call-ID: 41840594f049ae2f13c4419b760813744521850ff89430478-0125-7168
CSeq: 1 INVITE
User-agent: CS2000/NGSS/9.0
X-Nortel-Profile: DEFAULT
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY, PRACK
Via: SIP/2.0/UDP SP2KDON:5060;maddr=47.174.73.240;branch=z9hG4bK-419b7608-137445
P-Asserted-Identity: <sip:6137222010@47.142.211.17;user=phone>
History-Info: <sip:6137222009@NGSS1?Reason:Q.732; text="user busy”&Privacy:History-
Info>;index=1, <sip:6137222015@NGSS1?Reason:Q.732; text="no reply”>;index=2
Contact: <sip:47.174.73.240:5060>
Content-Type: application/SDP
Content-Length: 174

v=0
o=MGCP 0 0 IN IP4 47.174.73.241
```

```
s=MGCP Call
c=IN IP4 47.174.73.241
t=0 0
m=audio 5004 RTP/AVP 18 0 96
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

125.2.6 CIP/TNS Parameters

Carrier Identification Parameter(CIP) and Transit Network Selection(TNS) information are carried in new parameters introduced by this feature to the Request-URI Header. Below are examples of CIP transport and TNS transport.

The CIP and TNS are valid optional parameters in the ISUP IAM message

cip = 4*DIGIT

cic= 4*DIGIT

netid= 1*DIGIT

sc = 1*DIGIT [1*DIGIT]

Table 4: CIP/TNS Netid DIGIT Values

Netid DIGIT	Q.763 Interpretation
0	CCITT /ITU-T Standard
2	National Network

An example IAM message optional part transporting CIP:

```
OPTIONAL PART:      CARRIER IDENTIFICATION PARAMETER :
                    NETWORK_ID_PLAN :        FOUR_DIGIT_CIC
                    TYPE_OF_NETWORK_ID :     CCITT_STANDARDIZED
                    CARRIER_IDENTIFICATION_CODE : 4712
```

The resulting SIP message:

```
INVITE sip:6137222000;cip=4712;netid=0@47.174.73.240:5060 SIP/2.0
From: <sip:6137222010@47.174.73.240:5060>;tag=f-13c4-419b7608-137445-144454f6
```

```
To: <sip:6137222000@47.174.73.240:5060>
Call-ID: 41840594f049ae2f13c4419b760813744521850ff89430478-0125-7168
CSeq: 1 INVITE
User-agent: CS2000/NGSS/9.0
X-Nortel-Profile: DEFAULT
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY, PRACK
Via: SIP/2.0/UDP SP2KDON:5060;maddr=47.174.73.240;branch=z9hG4bK-419b7608-137445
P-Asserted-Identity: <sip:6137222010@47.142.211.17;user=phone>
Contact: <sip:47.174.73.240:5060>
Content-Type: application/SDP
Content-Length: 174

v=0
o=MGCP 0 0 IN IP4 47.174.73.241
s=MGCP Call
c=IN IP4 47.174.73.241
t=0 0
m=audio 5004 RTP/AVP 18 0 96
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

An example IAM message optional part transporting TNS:

```
             OPTIONAL PART:  TRANSIT NETWORK SELECTOR :
                             NETWORK_ID_PLAN :                    FOUR_DIGIT_CIC
                             TYPE_OF_NETWORK_ID :                 NATIONAL_NETWORK
                             CARRIER_IDENTIFICATION_CODE :        4713
                             CIRCUIT_CODE :
INTNTL_CALL_NO_OPERATOR_REQUESTED
```

The resulting SIP message:

```
INVITE sip:6137222000;cic=4713;netid=2;sc=1@47.174.73.240:5060  SIP/2.0
From: <sip:6137222010@47.174.73.240:5060>;tag=f-13c4-419b7608-137445-144454f6
To: <sip:6137222000@47.174.73.240:5060>
Call-ID: 41840594f049ae2f13c4419b760813744521850ff89430478-0125-7168
CSeq: 1 INVITE
User-agent: CS2000/NGSS/9.0
X-Nortel-Profile: DEFAULT
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY, PRACK
Via: SIP/2.0/UDP SP2KDON:5060;maddr=47.174.73.240;branch=z9hG4bK-419b7608-137445
P-Asserted-Identity: <sip:6137222010@47.142.211.17;user=phone>
Contact: <sip:47.174.73.240:5060>
Content-Type: application/SDP
```

```
Content-Length: 174

v=0
o=MGCP 0 0 IN IP4 47.174.73.241
s=MGCP Call
c=IN IP4 47.174.73.241
t=0 0
m=audio 5004 RTP/AVP 18 0 96
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

125.2.7 Jurisdiction Information Parameter

Jurisdiction Information Parameter is a six digits optional parameter in the IAM message representing the geographic location for the call origination.

A new parameter, jip, will be created and added to the PA-Id and thr From header user information. The parameter will be defined as follows. If present, JIP user info arriving in PAID header overrides JIP user info arriving in From header.

Jurisdiction Information Parameter= jip-tag "=" six-digit-string

jip-tag = "jip"

six-digit-string = 6[0|1|2|3|4|5|6|7|8|9]

Example SIP message:

```
INVITE sip:6137222000@47.174.73.240:5060 SIP/2.0
From: <sip:6137222010;cpc=payphone;oli=61;jip=919991@47.174.73.240:5060>;tag=f-13c4-
419b7608-137445-144454f6
To: <sip:6137222000@47.174.73.240:5060>
Call-ID: 41840594f049ae2f13c4419b760813744521850ff89430478-0125-7168
CSeq: 1 INVITE
User-agent: CS2000/NGSS/9.0
X-Nortel-Profile: DEFAULT
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY, PRACK
Via: SIP/2.0/UDP SP2KDON:5060;maddr=47.174.73.240;branch=z9hG4bK-419b7608-137445
P-Asserted-Identity: <sip:6137222010;cpc=payphone;oli=61;jip=919991@47.142.211.17;user=phone>
```

125.2.8 Generic Digits

Generic Digits is an optional parameter in IAM message. This parameter will be mapped into a new SIP header.

```
Gen-Digit = "Generic-Digits" HCOLON addr ";" type
type = "type" EQUAL  ("authcode" |
                      "priv-net-trav-classmark"|
                      "clli-admin" |
                      "ani-index" |
                      "member-range-info" |
                      "uss-redir-info" |
                      "term-swid"
                      "call-id" |
                      "wireless-emergency"|
                      "access-node-orig-info" |
                      "osid-plus-otg" |
                      "imt-info" |
                      "hotel-room" |
                      "hotel-guest-name"
                      "division-id" |
                      "trunk-id"|
                      "ooy" |
                      "transport-info" |
                      "super-gd" |
                      "fallback-context-block" |
                      "keyed-fallback-digits"
                      "e911tandem-prefix" |
                      "ind-con"|
                      "correlation-id" )
```

An example IAM message:

```
OPTIONAL PART:        Generic Digits:
                         GENERIC_DIGITS_TYPE : E911TANDEM_PREFIX
                         ENCODING_SCHEME :     BCD_ODD
                         DIGITS :              12345
```

The resulting SIP message:

```
INVITE sip:6137222000@47.174.73.240:5060;SIP/2.0
From: <sip:6137222010@47.174.73.240:5060>;tag=f-13c4-419b7608-137445-144454f6
To: <sip:6137222000@47.174.73.240:5060>
Call-ID: 41840594f049ae2f13c4419b760813744521850ff89430478-0125-7168
CSeq: 1 INVITE
User-agent: CS2000/NGSS/9.0
X-Nortel-Profile: DEFAULT
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY, PRACK
Via: SIP/2.0/UDP SP2KDON:5060;maddr=47.174.73.240;branch=z9hG4bK-419b7608-137445
P-Asserted-Identity: <sip:6137222010@47.142.211.17;user=phone>
Contact: <sip:47.174.73.240:5060>
Gen-Digit:12345;type=e911tandem-prefix
```

125.2.9 User to User Indicator/Information (UUI)

UUI can be received in IAM, ACM or ANM. Since User to User information can be large, it does not make sense to make it a SIP header or parameter. Instead UUI will be tunnelled as a payload using a newly defined MIME type

content-type: application/UUI

Example SIP message:

```
INVITE sip:6137222000@47.174.73.240:5060 SIP/2.0
From: <sip:6137222010@47.174.73.240:5060>;tag=f-13c4-419b7608-137445-144454f6
To: <sip:6137222000@47.174.73.240:5060>
Call-ID: 41840594f049ae2f13c4419b760813744521850ff89430478-0125-7168
CSeq: 1 INVITE
User-agent: CS2000/NGSS/9.0
X-Nortel-Profile: DEFAULT
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY, PRACK
Via: SIP/2.0/UDP SP2KDON:5060;maddr=47.174.73.240;branch=z9hG4bK-419b7608-137445
P-Asserted-Identity: <sip:6137222010@47.142.211.17;user=phone>
Contact: <sip:47.174.73.240:5060>
Content-Type: application/UUI
Content-Length: 40
<payload>
```

125.2.10 Geodetic Location

This is an optional parameter in IAM and is used in the network to carry cell/ sector ID for 911 calls. Draft draft-ietf-sip-loaction-conveyance-00.txt recommends that location information be carried as a payload in SIP message Geo Location will be tunnelled as a payload using a newly defined MIME type

content-type: application/cpim-pidf+xml

Example SIP message:

```
INVITE sip:6137222000@47.174.73.240:5060 SIP/2.0
From: <sip:6137222010@47.174.73.240:5060>;tag=f-13c4-419b7608-137445-144454f6
To: <sip:6137222000@47.174.73.240:5060>
Call-ID: 41840594f049ae2f13c4419b760813744521850ff89430478-0125-7168
CSeq: 1 INVITE
User-agent: CS2000/NGSS/9.0
X-Nortel-Profile: DEFAULT
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY, PRACK
Via: SIP/2.0/UDP SP2KDON:5060;maddr=47.174.73.240;branch=z9hG4bK-419b7608-137445
P-Asserted-Identity: <sip:6137222010@47.142.211.17;user=phone>
Contact: <sip:47.174.73.240:5060>
Content-Type: application/cpim-pidf+xml
Content-Length: 40
<payload>
```

125.2.11 Precedence

This is an optional parameter in IAM and is used in the network to carry precedence calls.

A new proprietary header called Precedence with Precedence level, LFB, and MLPP_SD will be created

precedence : Level ; LBF ; MLPP_SD ; NETWORK_ID

Level = “precedence” EQUAL (“FLASH_OVERRIDE” |
“FLASH “ |
“PRIORITY” |
“ROUTINE”)

LFB = “lfb” EQUAL (“ALLOWED” |
“RESERVED” |
“NOT_ALLOWED”)
MLPP_SD = (MLPP_SD_1, MLPP_SD_2, MLPP_SD_3)

MLPP_SD_1 = byte

MLPP_SD_2 = byte

MLPP_SD_3 = byte

NET_ID = (NET_ID_2, NET_ID_1, NET_ID_4, NET_ID_3)

NET_ID_1 = byte

NET_ID_2 = byte

NET_ID_3 = byte

NET_ID_4 = byte

125.2.12 Carrier Selection

Carrier Selection is an optional parameter in the IAM message.

A new parameter, csel, will be created and added to user info of the Request URI The parameter will be defined as follows.

csel-tag = "csel"

csel-string = [“noind”, “sub”, “subdialed”, ”subnoind”, ”dialed”]

Example SIP message:

```
INVITE sip:6137222000;csel=sub@47.174.73.240:5060 SIP/2.0
From: <sip:6137222010@47.174.73.240:5060>;tag=f-13c4-419b7608-137445-144454f6
To: <sip:6137222000@47.174.73.240:5060>
Call-ID: 41840594f049ae2f13c4419b760813744521850ff89430478-0125-7168
CSeq: 1 INVITE
User-agent: CS2000/NGSS/9.0
X-Nortel-Profile: DEFAULT
```

```
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY, PRACK
Via: SIP/2.0/UDP SP2KDON:5060;maddr=47.174.73.240;branch=z9hG4bK-419b7608-137445
P-Asserted-Identity: <sip:6137222010@47.142.211.17;user=phone>
```

125.2.13 Session Timer

The Session Timer extension (RFC4028) enables SIP servers and endpoints to know if an endpoint is no longer in a session (for example in case of a crash) and to limit the duration of a session. An endpoint that has the Session Timer extension activated will send periodic keep-alive messages to notify that it is active or to extend the duration of the session.

RFC 4028 Session Timers in the Session Initiation Protocol (SIP) defines two new headers - Session-Expires and Min-SE and a new response code of 422. The Session-Expires header conveys the lifetime of the session, the Min-SE header conveys the minimum value for the Session Timer, and the 422 response code indicates that the Session Timer duration is too small. The Session-Expires/session timer value allowed to provisioned on SST GUI is 5-30 minutes.

The Session Timer extension enables determining the duration time of a call. A Session-Expires header included in the 2xx response of an initial INVITE determines the session duration. Periodic refresh enables extending the duration of the call and allows both User Agents (UAs) and proxies to determine if the SIP session is still active. The refresh of a SIP session is done through a re-INVITE or UPDATE. UPDATE method is preferred if remote sip server supports UPDATE.

The Session-Expires header in the 2xx response also indicates which side will be the refresher, in other words, which side will be responsible for generating the refresh request. The refresher can be UAC or UAS. The refresher should be generated a refresh request (using re-INVITE or UPDATE) before the session expires, normally at half of the Session-Expires value. If no refresh request is sent or received before the session expires, or if the refresh request is rejected, both parties will send BYE.

To enable Session Timer on Remote Sip Server, following steps need to be followed:

- SIP Gateway, Config Data, supportedExtensionList, change from “100rel” to “100rel, timer”. This change requires callp restart to take effect. Steps required to update config parameters which can not be changed dynamically need to follow here.
- SIP Gateway, Remote SIP Server, Advanced SIP Options, Long Call Audit Mechanism, choose Session Timer, default is INFO

- SIP Gateway, Remote SIP Server, Advanced SIP Options, choose timer value between 5-30 minutes, default is 20 minutes

125.2.14 Provisioning

The new functionality introduced by this feature is by default turned off when a new remote SIP server is provisioned. To enable specific or all mappings, a craftpserson can select ‘Advanced SIP Options’ section and enable the capabilities.

Advance SIP options feature are divided into following categories:
- Methods Supported
- SIP Headers Supported
- URI Parameters Supported
- General Configuration

Methods Supported is not impacted by this feature this feature.

SIP Headers Supported
Craftsperson can use this section to enable/disable specific SIP headers a remote SIP server can support. The choices relevant to this features are:
- History Info
- Generic Digits
- Charge Number
- Geodetic Location
- Precedence

URI Parameters Supported
Craftsperson can use this section to enable/disable specific parameters in the URI. The choices relevant to this feature are:
- Satellite Indicator
- Calling Party Category (CPC)
- Originating Line Information (OLI)
- CIP
- JIP

General Configuration
Craftsperson can use this section to enable/disable other enhanced SIP options. The choices relevant to this feature are:
- UUI support
- Automatic Congestion Level
- Long Call Audit Mechanism
- Session Timer Value

In addition to Advance SIP options, craftperson has a choice to provision Advanced PSTN Transparency options for a remote SIP server. The only

choice added by this feature is ‘National Circuit Code’ which has default value of eight and can be modified by the craftsperson.

125.2.15 SIP/SIP-T Interworking Support for North America

The following table provides the SIP/SIP-T interworking support for North America.

Table 5: North American SIP/SIP-T interworking

	PMTX 13	PMTX 14 VRDN	PMTX 14 NGSS	CS2K NGSS	CS2K VRDN	PGMSC 13	PGMSC 14 VRDN	PGMSC 14 NGSS
PMTX13	SIP-T	SIP-T	SIP-T	No Support	No Support	SIP-T	SIP-T	SIP-T
PMTX14 VRDN	SIP-T	SIP-T	SIP-T	No Support	No Support	SIP-T	SIP-T	SIP-T
PMTX14 NGSS	SIP-T	SIP-T	SIP or SIP-T	No Support	No Support	SIP-T	SIP-T	SIP or SIP-T
CS2K NGSS	No Support	No Support	No Support	SIP or SIP-T	SIP-T	No Support	No Support	No Support
CS2K VRDN	No Support	No Support	No Support	SIP-T	SIP-T	No Support	No Support	No Support
PGMSC 13	SIP-T	SIP-T	SIP-T	No Support	No Support	SIP-T	SIP-T	SIP-T
PGMSC 14 VRDN	SIP-T	SIP-T	SIP-T	No Support	No Support	SIP-T	SIP-T	SIP-T
PGMSC 14 NGSS	SIP-T	SIP-T	SIP or SIP-T	No Support	No Support	SIP-T	SIP-T	SIP or SIP-T

- VRDN to SST interworking will support only SIP-T between two packet switches (Serving or Gateway).
- SST to SST interworking will support both SIP or SIP-T between two packet switches (Serving or Gateway).

- At this time no testing has been done to verify support of SIP/SIP-T between packet and CS2k irrespective of SST or VRDN. Test setup and testing is not in the scope of this feature and needs a test activity.

125.2.16SIP/SIP-T Interworking Support for International Market

The following table provides the SIP/SIP-T interworking support for International variants. In SN09U only CCITT Brazil MTX_BLUE variant is supported

Table 6: International (Brazil) SIP/SIP-T interworking

	PMTX 13	PMTX 14 VRDN	PMTX 14 NGSS	CS2K NGSS	CS2K VRDN	PGMSC 13	PGMSC 14 VRDN	PGMSC 14 NGSS
PMTX13	SIP-T	SIP-T	SIP-T	No Support	No Support	SIP-T	SIP-T	SIP-T
PMTX14 VRDN	SIP-T	SIP-T	SIP-T	No Support	No Support	SIP-T	SIP-T	SIP-T
PMTX14 NGSS	SIP-T	SIP-T	SIP-T	No Support	No Support	SIP-T	SIP-T	SIP-T
CS2K NGSS	No Support	No Support	No Support	SIP-T	SIP-T	No Support	No Support	No Support
CS2K VRDN	No Support	No Support	No Support	SIP-T	SIP-T	No Support	No Support	No Support
PGMSC 13	SIP-T	SIP-T	SIP-T	No Support	No Support	SIP-T	SIP-T	SIP-T
PGMSC 14 VRDN	SIP-T	SIP-T	SIP-T	No Support	No Support	SIP-T	SIP-T	SIP-T
PGMSC 14 NGSS	SIP-T	SIP-T	SIP-T	No Support	No Support	SIP-T	SIP-T	SIP-T

- For international markets, only SIP-T is supported between two packet switches (Serving or Gateway) irrespective of SST or VRDN.qqqq

- At this time no testing has been done to verify support of SIP/SIP-T between packet and CS2k irrespective of SST or VRDN. Test setup and testing is not in the scope of this feature and needs a test activity.

125.3 Hardware Requirements or Dependencies

None

125.4 Software Requirements or Dependencies

None

125.5 Limitations and restrictions

- Since most of the new SIP headers and parameters introduced by this feature are not part of any SIP RFC or draft (except History-Info), the enhanced SIP mapping provided by this feature will only work with between two Nortel CS2Ks/PMSCs.
- Simultaneous SIP and SIP-T interface to a remote server is not supported.
- This feature supports only ANSI ISUP. SIP interface for international variants (e.g Brazil ISUP) is not supported.
- This feature functionality will be delivered as a patch(s) in SN09.

125.6 Interactions

None

125.7 Glossary

Term	Description
NGSS	Next Generation Session Server
SIP	Session Initiation Protocol
RFC	Request For Comment
OLI	Originating Line Information
JIP	Juridiction Information Parameter
CIP	Circuit Identification Parameter
CIC	Circuit Identification Code
ACL	Automatic Congestion Level
PAID	P-Asserted ID
SST	Session Server Trunking

126: Functional Description (FN) A00011740

126.1 Feature name and Feature ID

A00011740: Packet Cable Multimedia for CS2K

126.2 Description

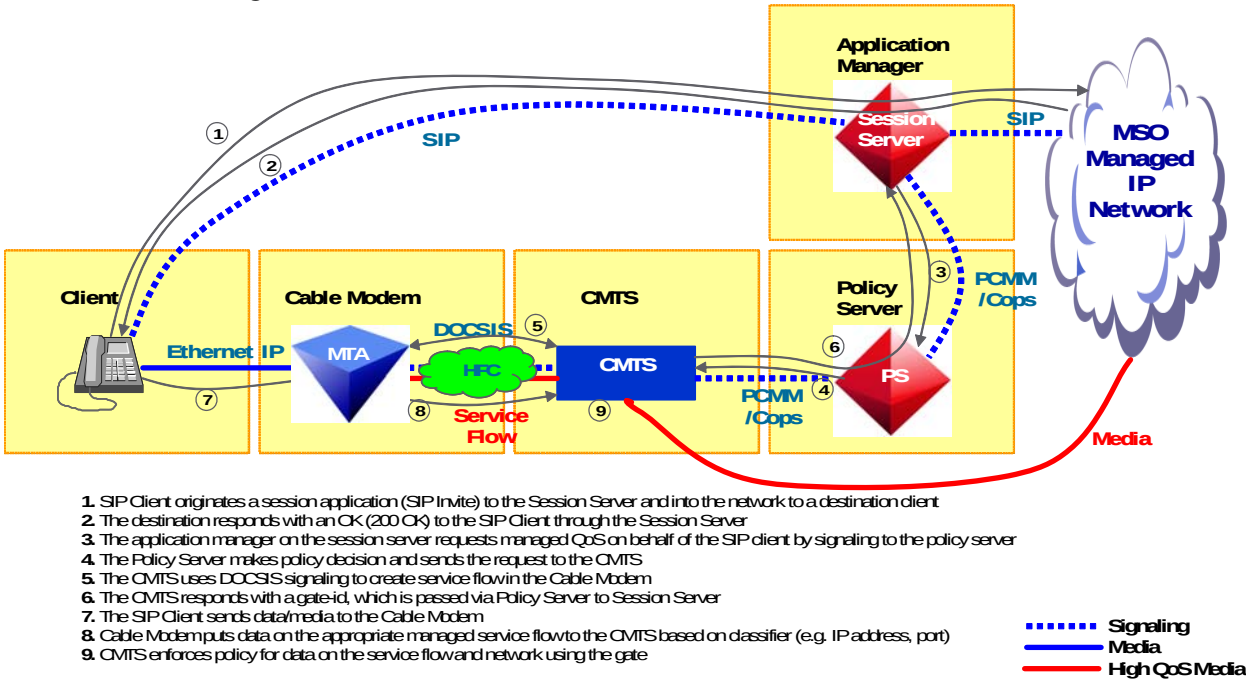
126.2.1 Functional Overview

PacketCable Multimedia is an architecture developed by CableLabs to enable MultiService Operating Companies to deliver Quality of Service enabled multimedia services over DOCSIS networks. PacketCable Multimedia extends the Dynamic Quality of Service architecture developed as part of PacketCable 1.X to allow Application Managers in the MSO network to request and obtain Quality of Service treatment for multimedia traffic flows on behalf of an end user.

This service enhances the CS2000 SIP Lines solution to take advantage of the PacketCable Multimedia mechanisms to provide QoS for voice and video sessions established over an MSO DOCSIS network. The PCMM signaling implementation is compliant with PacketCable specification PKT-SP-MM-I02-040930 (refer to section 126.8 on page 1219 for a detailed compliance matrix).

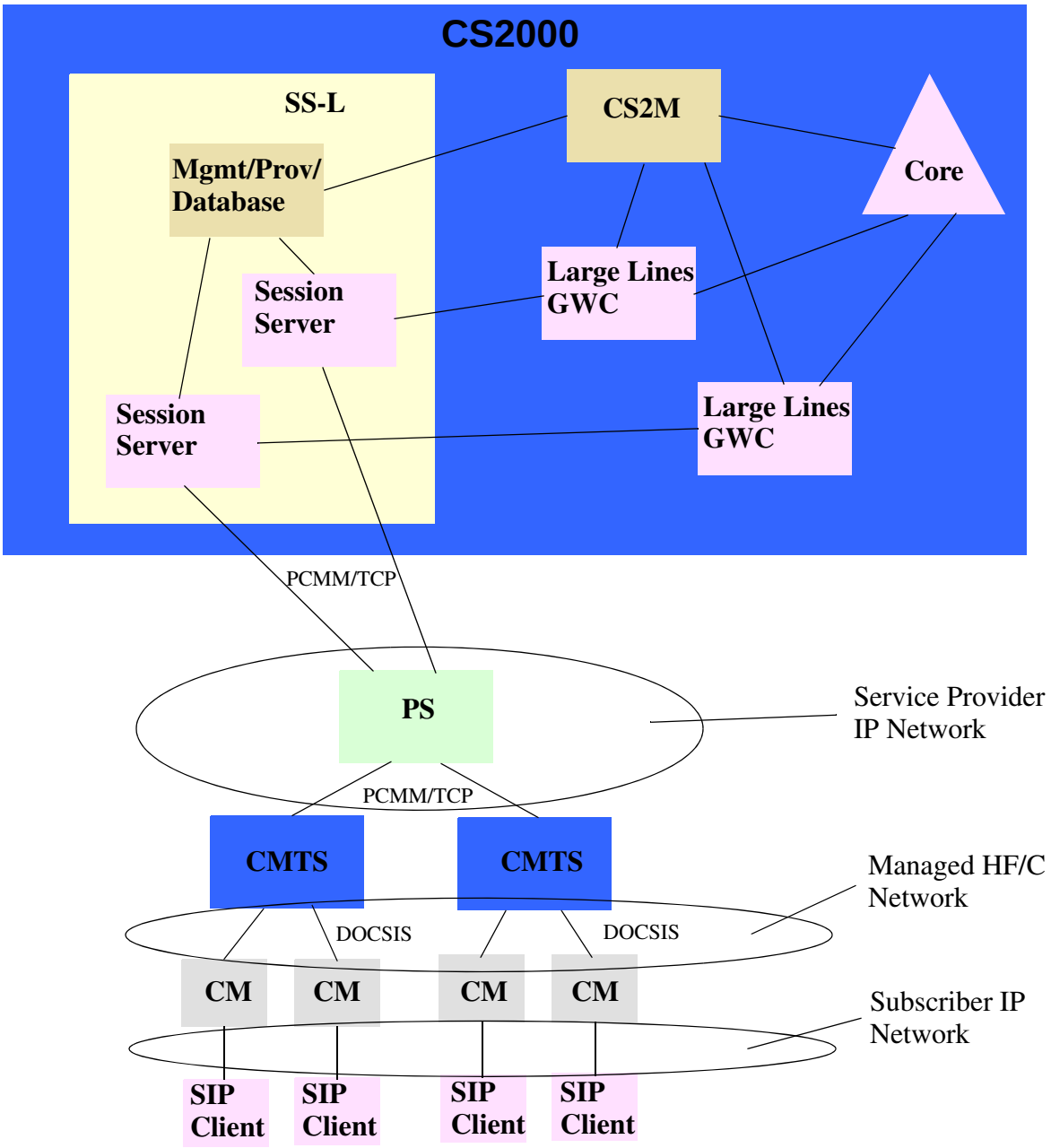
The following diagram illustrates a high level call flow for a PacketCable Multimedia (PCMM) SIP call in the CS2000.

Figure 1 PCMM SIP Call Flow



The following diagram illustrates a typical cable network topology for a SIP lines deployment. Both MCS and CS2K are shown.

Figure 2 PCMM Network Diagram



The diagram points out three networks: the service provider IP network, the HF/C (hybrid fiber/coax) network and the subscriber IP network. The network that is not explicitly shown is the call server IP network by which the CS2K and MCS network elements communicate.

The HF/C network is the focal point of PCMM since that is where we are managing QoS. For media stream network connectivity between a SIP client

and another endpoint, DIFFSERV is used for QoS outside of the HF/C network.

The subscriber IP network may be behind a NAT. SIP clients can be SIP phones or SIP soft-clients such as the Nortel's MCS Multimedia PC client.

The following sections describe how to setup PCMM, how to determine if PCMM is working correctly, and how to alter the PCMM configuration after it is up and running.

126.2.2 Setting up PCMM

In order to setup the PCMM service the following high level steps must be carried out in order. Detailed instructions for each step can be found by following the links.

1. Enable the PCMM Service Key (see section 126.2.5 on page 1180)
2. Add a policy server IP address (see section 126.2.6 on page 1181)
3. Add a policy server (see section 126.2.7 on page 1182)
4. Configure the policy server AMIDs for each session manager (see section 126.2.8 on page 1185)
5. Assign Diffserv value for subscriber (see section 126.2.9 on page 1188)
6. Assign PCMM capability to subscribers (see section 126.2.10 on page 1191)

126.2.3 Verifying that PCMM is working

Once you have gone through the steps outlined in section 126.2.2 on page 1180, you can do the following to verify that PCMM is working as expected.

1. Check for PCMM alarms (see section 126.2.11 on page 1197)
2. View PCMM operational measurements (see section 126.2.12 on page 1201)

126.2.4 Altering PCMM configuration

If you need to alter your PCMM configuration or provisioning, please see the following sections.

- Changing PCMM configuration (see section 126.2.13 on page 1207)
- Removing PCMM service from a subscriber (see section 126.2.14 on page 1208)
- Deleting a policy server (see section 126.2.15 on page 1209)

126.2.5 Enabling the PCMM Key

The PCMM service is key coded. To use the PCMM functionality, the PCMM key must be enabled, and part of your systems license key.

The PCMM key within the license can be generated as enabled, disabled, or not present. If the key is not present then the service is disabled.

Key codes within a license key can be added or upgraded, but keys can not be removed. Once a license is added to a system with PCMM enabled, The PCMM key can not be disabled.

The generation of the license key with the PCMM key code is done using the Nortel KRS (Key Registry System).

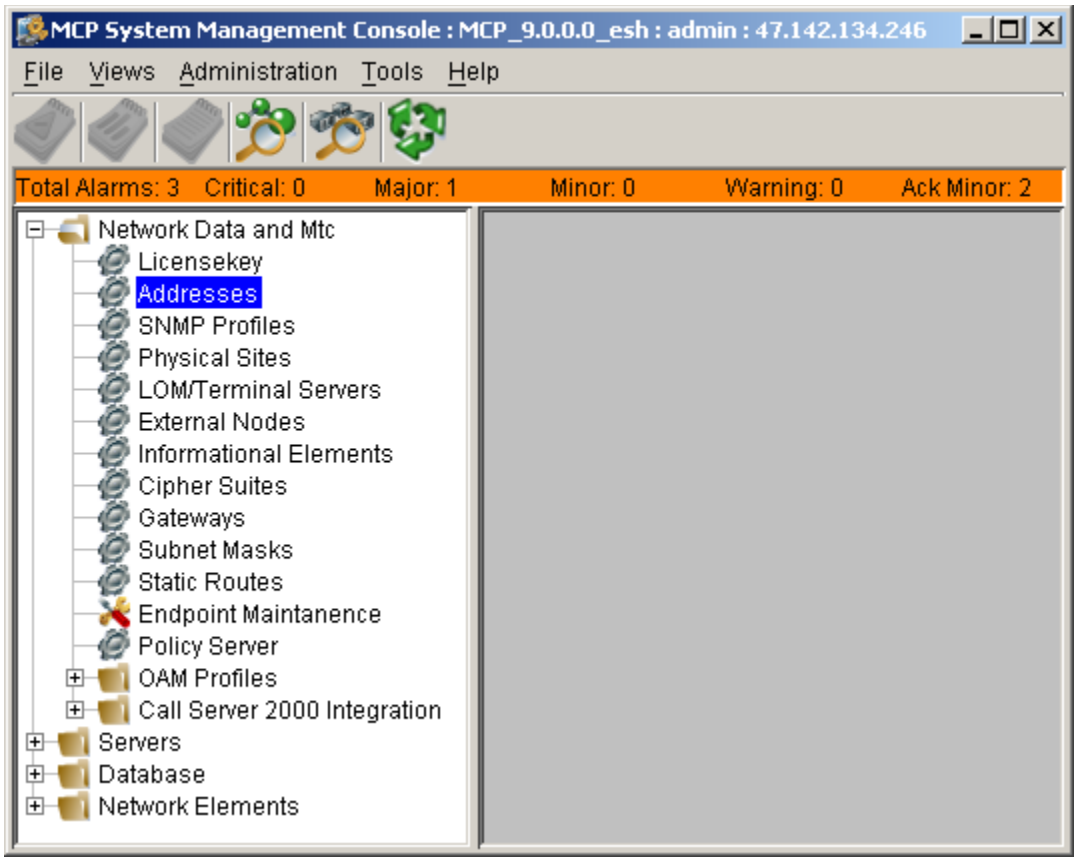
The addition of a system license key is covered as part of the installation and commissioning process.

126.2.6 Associating a Logical Name to a Policy Server IP address

To configure a policy server IP address and associate the address with a name that will be used in subsequent references to the address:

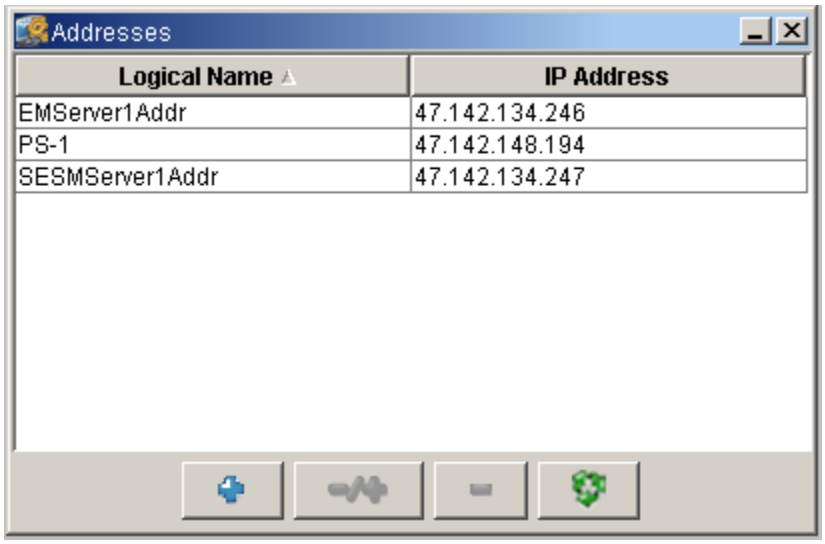
- From the MCP System Management Console expand the “Network Data and Mtc” item

Figure 3 MCP System Management Console for Addresses



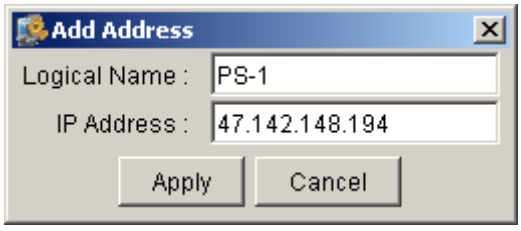
- Click the ‘Addresses’ icon, the ‘Addresses’ window will appear

Figure 4 Addresses Dialogue



- Select '+'and provide the PS address logical name and IP address in the form x.x.x.x

Figure 5 Add Address



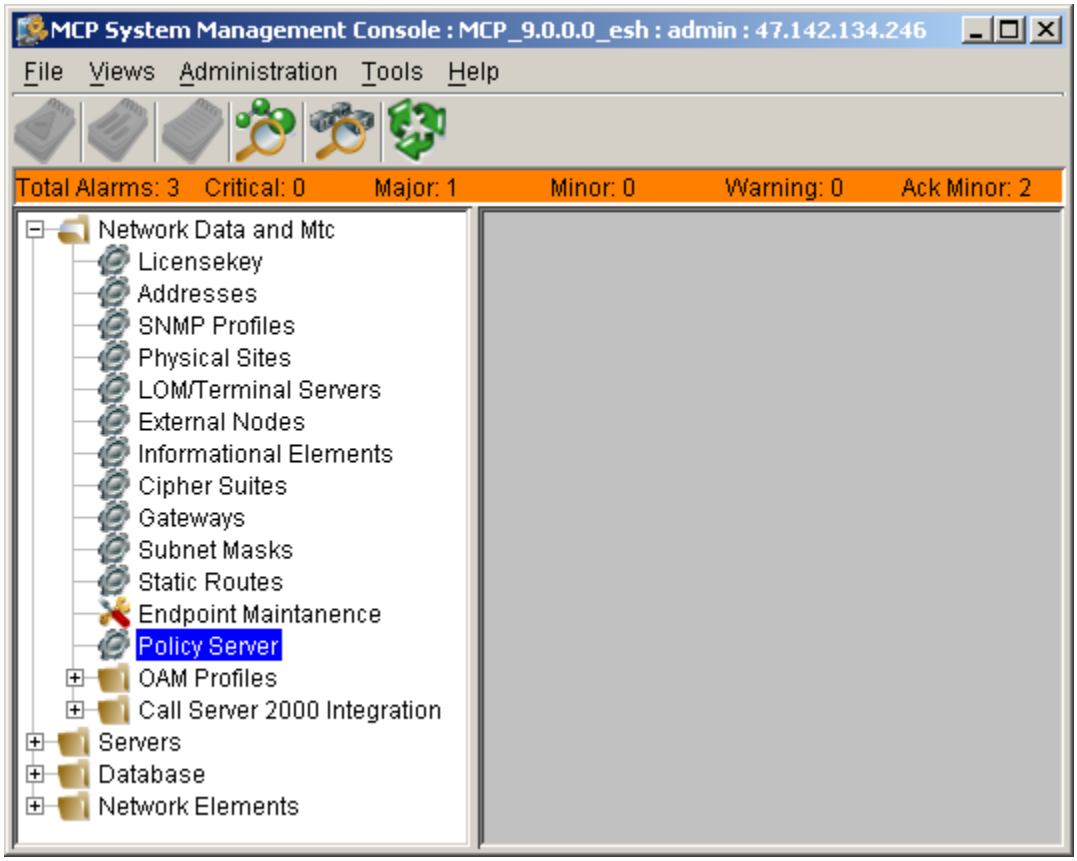
Now the logical name ("PS-1" in this example) will appear as a choice anywhere you need to enter an IP address.

126.2.7 Adding a Policy Server

To add a policy server:

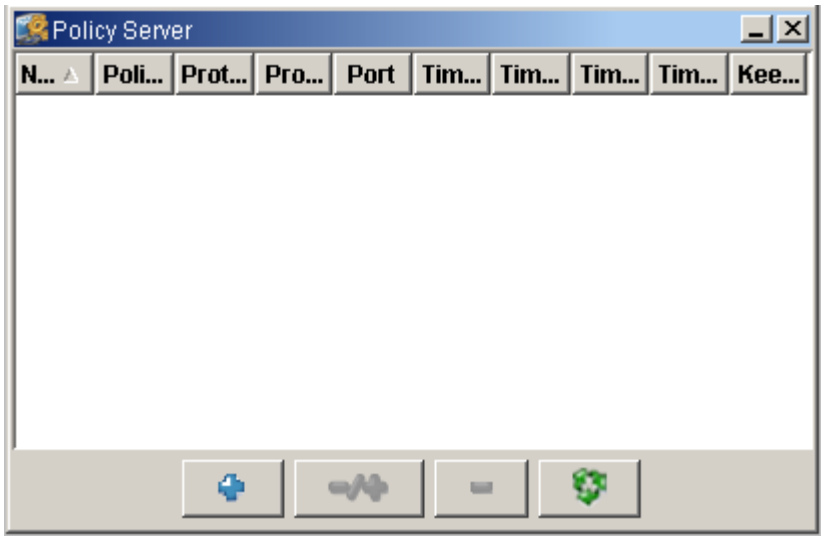
- On the MCP System Management Console GUI expand the "Network Data and Mtc" tree

Figure 6 System Management Console for Policy Server



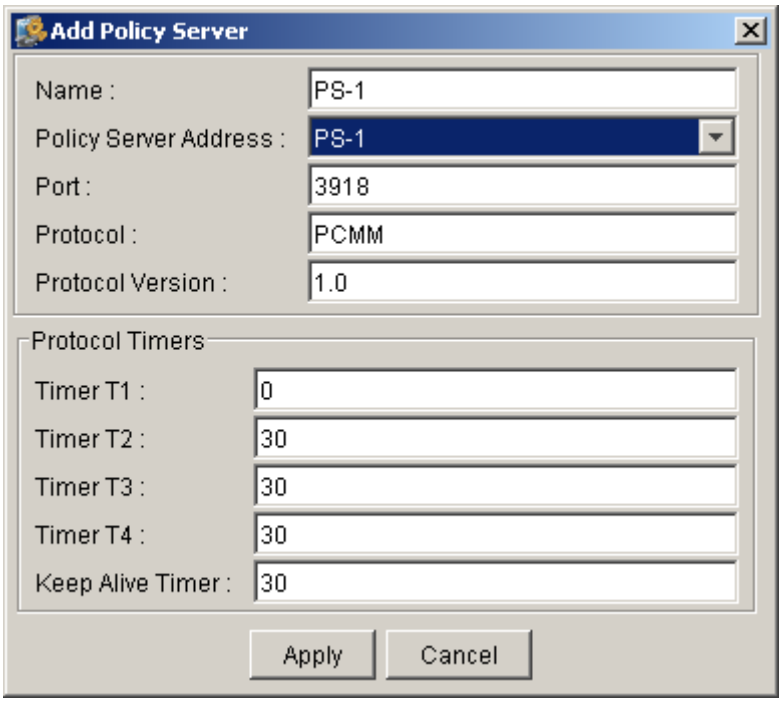
- Click “Policy Server” and a Policy Server window will appear showing the existing policy servers (if any)

Figure 7 Policy Server Dialogue



- Select the '+' icon and a new window appears. Enter the following fields:

Figure 8 Add Policy Server



a. **Name**: customer defined string up to 16 characters

b. **Policy Server Address**: select the logical address to assign from the pull down list which was configured under the 'Addresses' icon (see section 126.2.6 on page 1181). This is the address that the policy server will listen on for PCMM signaling.

c. **Port:** this is the port number the policy server will listen on for PCMM signaling. It must be and integer value from 1 to 65,535. The IANA well-known port for PCMM is 3918, so unless a different port is required by the policy server 3918 should be used.

d. **PCMM Protocol**: the PCMM signalling protocol used by the Policy Server. This should be set to the string "PCMM".

e. **Protocol Version -** the pulldown menu shows PCMM protocol versions supported by the CS2000. Choose the highest protocol version that you want the CS2000 to negotiate to for the policy server being configured. For example, if the policy server and the CS2000 both support versions 1.0 and 2.0, but you wish to continue using version 1.0, you can select 1.0 for this field.

f. **Timer T1:** timer maintained by the CMTS to determine the time in seconds that a gate can be in the 'authorized state'. A value of zero (the default) indicates that CMTS should use its own provisioned value.

The suggested range for this timer (if not zero) is between 5 and 180 seconds.

g. **Timer T2:** timer maintained by the CMTS to determine the time in seconds that excess reserved bandwidth must be held by CMTS. A value of zero disables this timer. The default value is 30 seconds. The suggested range for this timer (if not zero) is between 5 and 180 seconds.

h. **Timer T3:** timer maintained by the CMTS to determine the time in seconds that the service flow can be idle (no packets flowing) before being reported by CMTS. A value of zero disables service flow activity monitoring. **Nortel strongly recommends against disabling this timer as this can lead to hung resources in the CMTS**. The default value is 30 seconds. The allowed range for this timer is between 10 and 300 seconds.

i. **Timer T4:** timer maintained by the CMTS to determine the time in seconds that a gate can remain in the 'committed-recovery state' (due to T3 expiration). **Nortel strongly recommends against a T4 value less than 10 seconds**. The default value is 30 seconds. The allowed range for this timer is between 10 and 300 seconds.

j. **Keep Alive Timer:** this is the PCMM keep alive timer which is used to determine if the PS connection is healthy. The default value is 30 seconds. The allowed range for this timer is between 10 and 180 seconds. Keep-alive messaging cannot be disabled.

Once these fields are entered, click "Apply" and the PS will be configured.

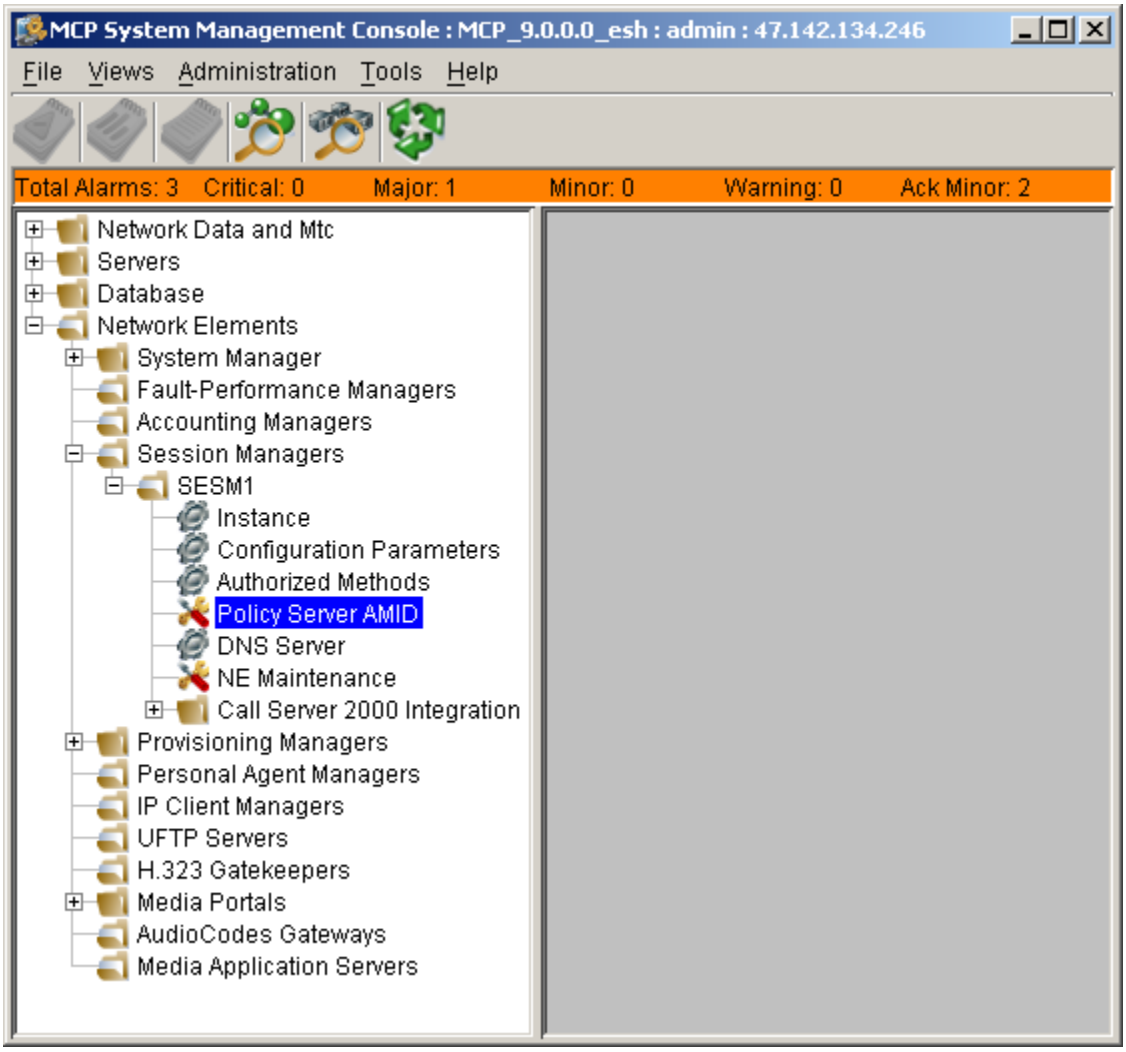
126.2.8 Configuring AMIDs for a Policy Server

For each PCMM signaling connection to a policy server, a set of application manager IDs must be configured. These AMIDs may be used by the policy server to keep track of application manager connections or may even be used to give the policy server an indication of the type of service being requested (audio or video).

In the MCS system, each active session manager has a connection to the policy server. Each active session manager must therefore have a set of AMIDs configured against the policy server. Here are the steps to set up AMIDs for a session manager. ***These steps must be repeated for each active session manager in the system.*** You need not configure AMIDs for redundant session managers.

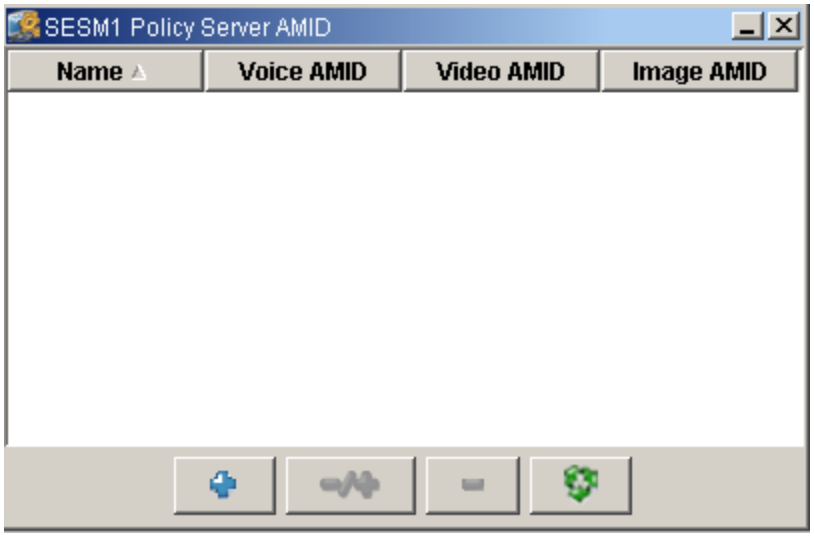
- From the MCP System Management Console, expand the Network Elements, Session Managers and then an instance of a session manager (SESM1 in this example).

Figure 9 System Management Console for AMIDs



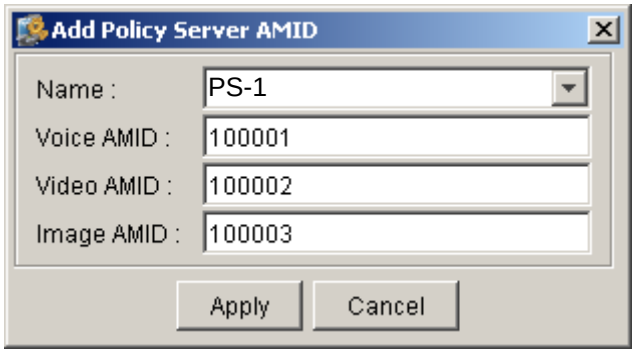
- When you click on “Policy Server AMID”, a window appears showing the configured policy servers. Select a policy server and a window will appear to allow AMID entry.

Figure 10 Policy Server AMIDs Dialogue



- Select a policy server and click on the "+" button and a window will appear to allow you to input AMID values. The MCS will ensure that the AMIDs for each Session Manager / policy server combination are unique. The voice/video/image service AMID values may be the same within each Session Manager/PS assignment.

Figure 11 Add Policy Server AMID



a. **Voice AMID:** value which represents the voice service type. Value between 0-4,294,967,295.

b. **Video AMID** - value which represents the video service type- value between 0-4,294,967,295.

c. **Image AMID** - value which represents the image (fax) service type- value between 0-4,294,967,295.

- Select 'Apply' and the Policy Server AMIDs are will be configured.
- Repeat these steps for each active session manager.

126.2.9 Setting up Diffserv for PCMM

The DiffServ parameters used for PCMM come from the existing QoS provisioning in the service package. The PCMM and QoS Services must be assigned to a domain, and both services created as part of a service package. The service is then assigned to all users you wish to have the PCMM service enabled. These associations are done using the Provisioning Client interface.

126.2.9.1 Assigning DSCP values to a Service Package

To assign the QoS service to the domain, from the Provisioning Client, select Services -> Assign Services.

Figure 12 Assigning Services

In the Assign Services window select the domain to add the QoS service package to and then click the Continue button.

Figure 13 Assigning Services to a Domain

To enable the QoS Service on the domain, from the Assign services to domain... window select QoS (a checked box to the left of the service name) from the list of available services, and once selected, click the Save button at the bottom of the screen.

To add QoS to an existing service package, under your Domain, open Service Package then List Packages.

Figure 14 Listing Service Packages

On the Service package list for domain … window to the right, select Details-Modify next to the Package you wish to add the service to.

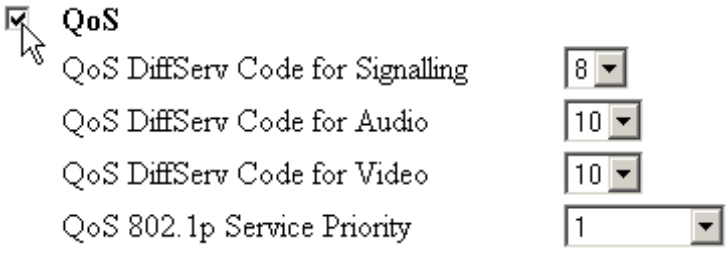
Figure 15 Package Name Details

In the window Package details for package everything belonging to domain...., select the check box to the left of the QoS Service, and Verify that the DiffServ values are correct for your domain. You can use the pull down menus to select the values for the users who subscribe to the service package.

The values in the fields represent the decimal representation of the high-order 6 bits of the DSCP/TOS field to be set in the IP header. To select the value for “expedited forwarding”, for example, choose a value of 46 (decimal). This corresponds to an IP header bit pattern of 1011 1000, where the low-order 2 bits are always set to zeros.

Note that PCMM signaling does not use the QoS DiffServ Code for Signalling.

Figure 16 Setting QoS DiffServ for a Package



If the pulldown boxes don’t have the DSCP value you want, you can define new DSCP values as follows:

Otherwise, click “Save and Enforce Now” to have the values updated, or “Save and Enforce Later” for that outcome.

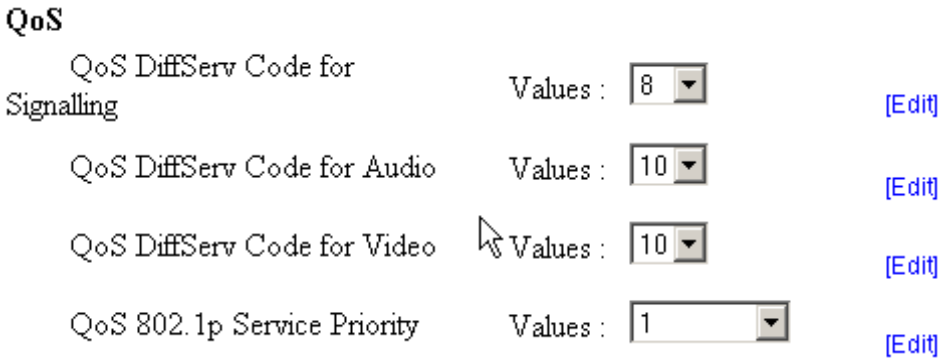
126.2.9.2 Defining New DSCP Values

To create new DSCP values for PCMM, from the Provisioning Client, open Services -> Define Service Parameters, then scroll down to the QoS Section.

Figure 17 Defining Service Parameters

In the List of available services window, scroll down to the QoS Section. If you wish to use a value that is not in the pre-defined list, then select the [edit] hyperlink to the right of the QoS fields,

Figure 18 QoS DiffServ Settings

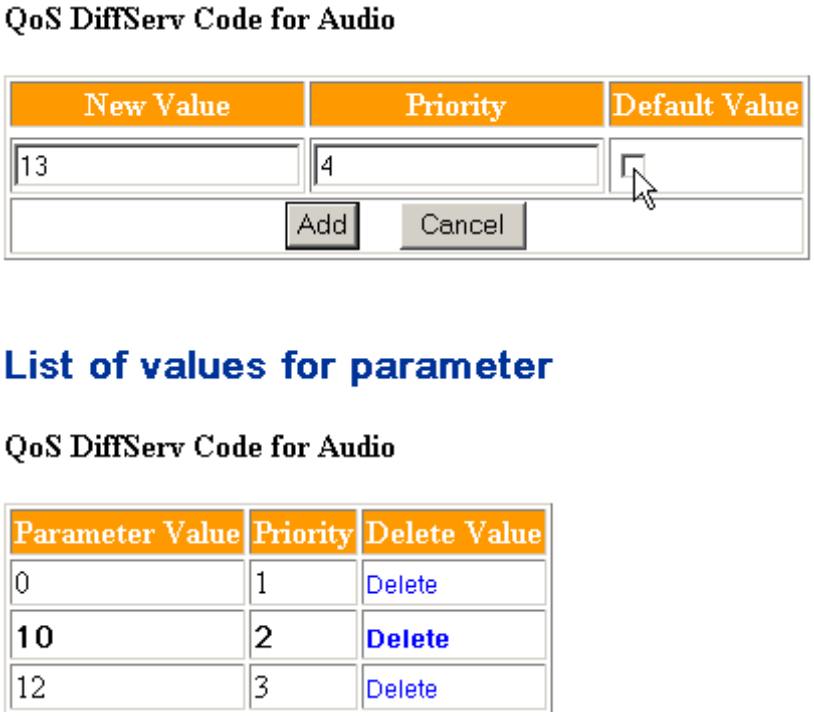


In the picture below the provisioner has chosen to edit the values for the Audio DiffServ value. After selecting edit, the window Add new parameter values for parameter will appear and allow you to add new values, assign priorities to the values, and select if it is the default value.

If you wish to make your new DSCP value the default for all new service packages, check the Default Value checkbox prior to clicking “Add” to add the new value. The default value will be displayed in the values list in bold font.

In the example below, we have chosen to add the value 13 with priority 4, and are about to select this as the default value for audio. If priority 4 already exists, the existing priority 4 value must be deleted before the new value can be added, by selecting the Delete, under the Delete value column.

Figure 19 QoS DiffServ Code for Audio



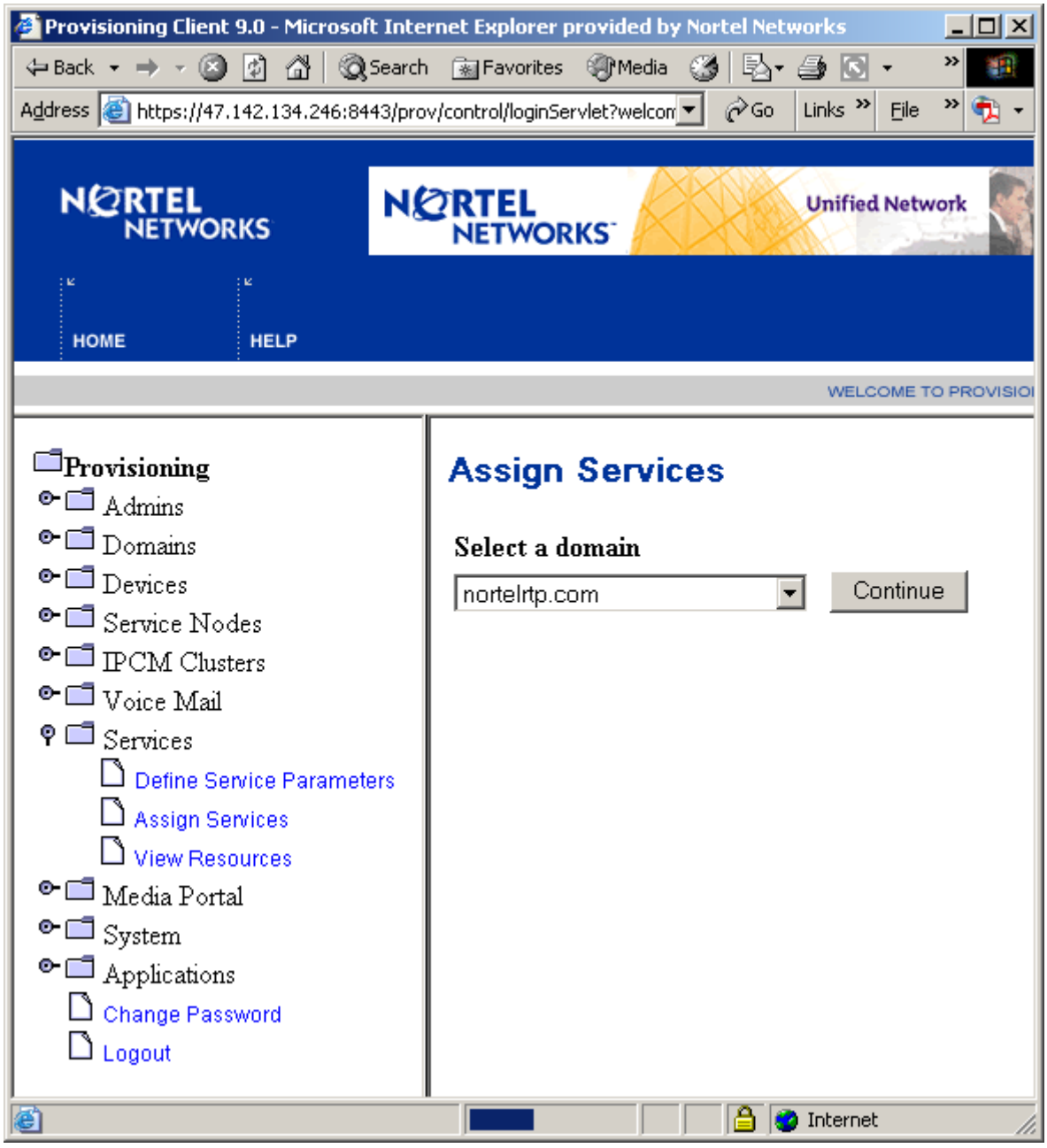
126.2.10 Assigning PCMM Capability to a Subscriber

The ability to provide managed quality of service on a per call / per subscriber level for cable SIP calls is implemented through the use of a new service called PacketCable Multimedia or PCMM. This new service is service package/ domain/sub-domain enabled/disabled through the Provisioning Manager on the MCS.

The steps required to assign the PacketCable Multimedia capability on the Provisioning Manager to a subscriber are:

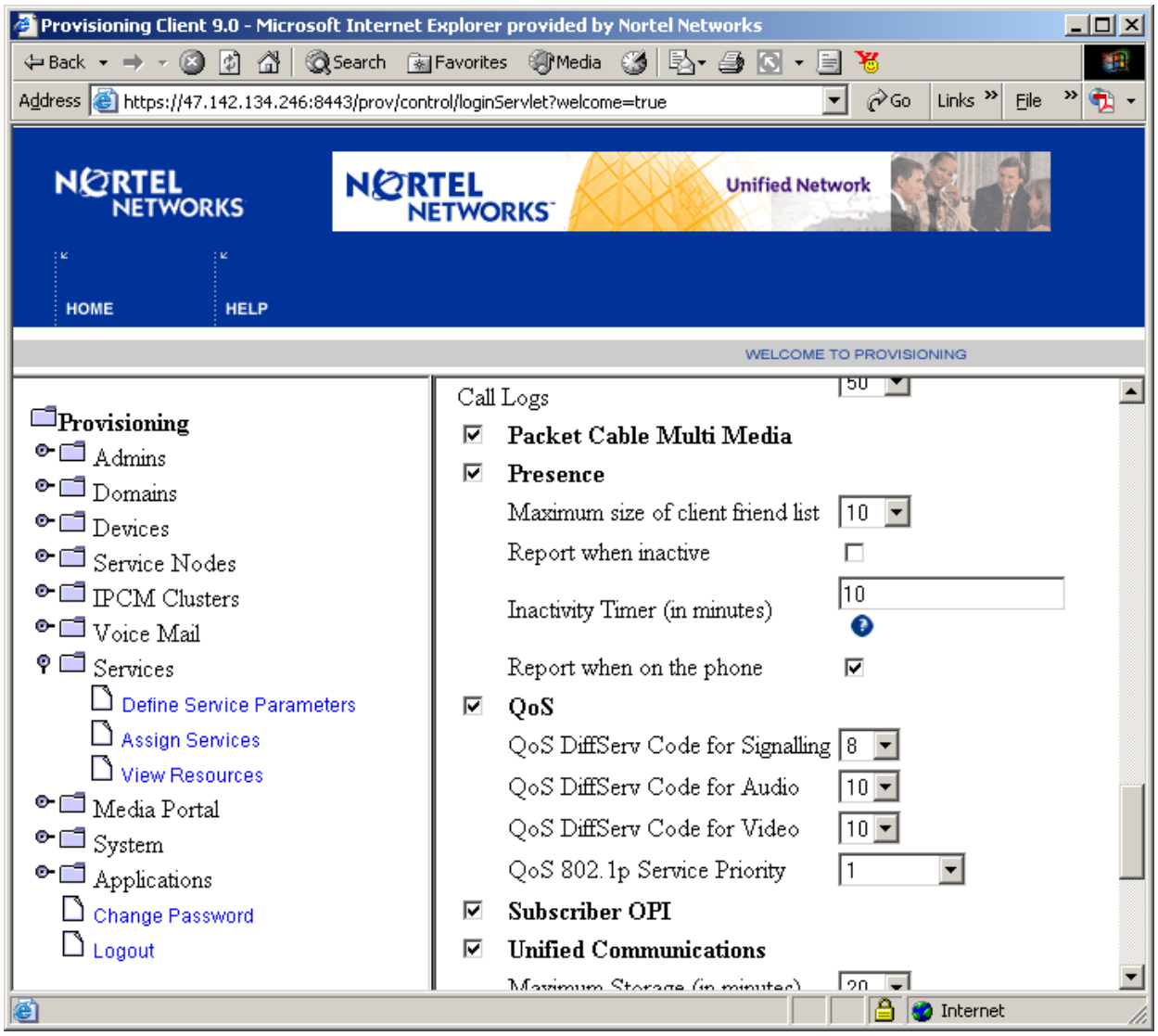
- Create a new domain or sub-domain as desired for PCMM subscribers.
- Open the MCS Provisioning Client, expand the “Services” item and click on “Assign Services”

Figure 20 Provisioning Client for Services



- Select the domain or sub-domain that you want to assign PCMM capability to from the pull-down box and click “Continue” and you will see the list of services will show up in the right-hand frame. Scroll down until you see the “PacketCable Multimedia” checkbox. Check the box and then click “Save” at the bottom of the frame.

Figure 21 Provisioning PacketCable Multimedia

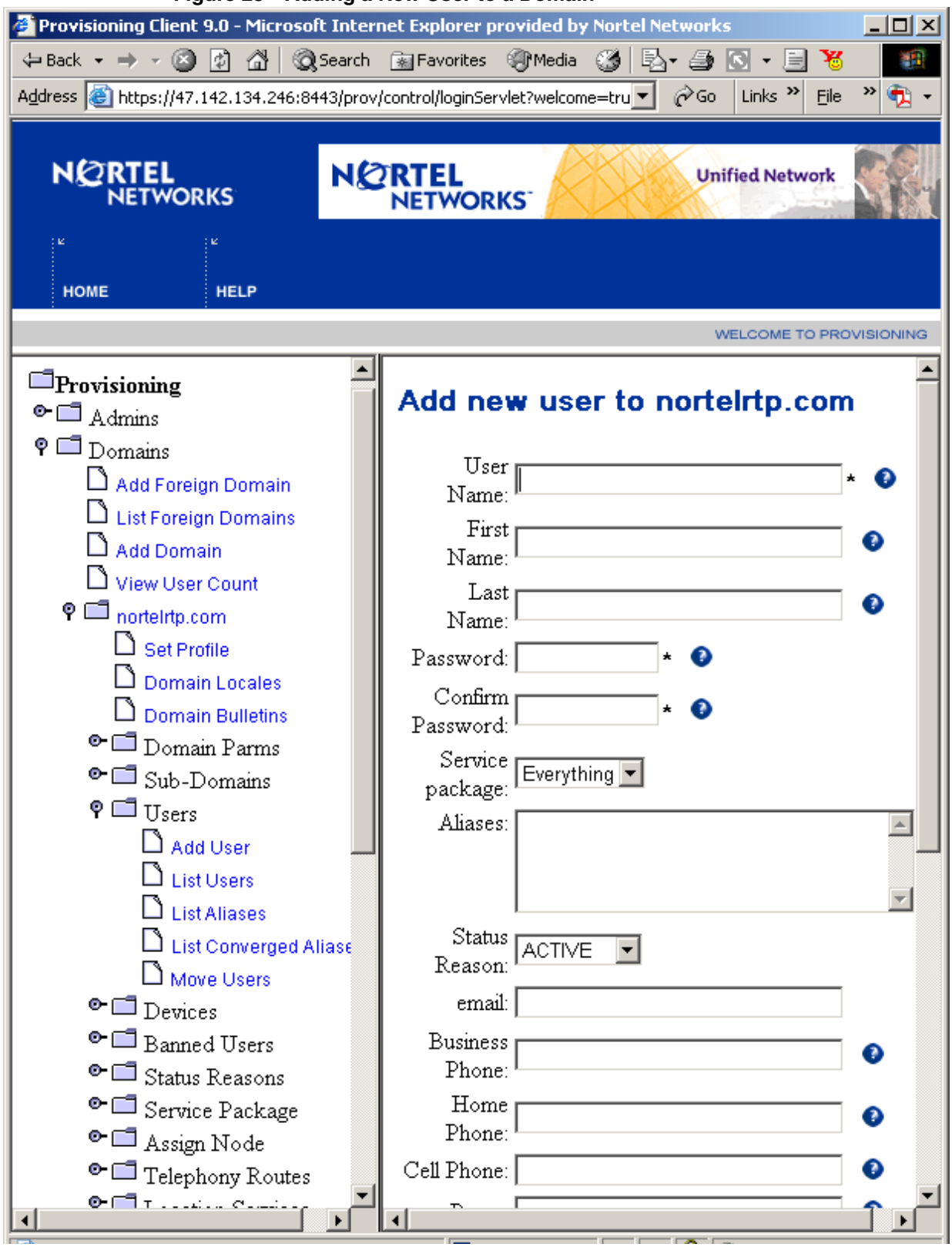


- Expand the desired domain/subdomain icon and create a service package with the PCMM service selected by clicking on “Create Package”.

Figure 22 Creating a new Package for a Domain

- Again under the specific domain/sub-domain, under the ‘Users’ icon select ‘Add User’ icon and fill in the required fields using the service package name created above.

Figure 23 Adding a New User to a Domain



The service is now assigned to a subscriber.

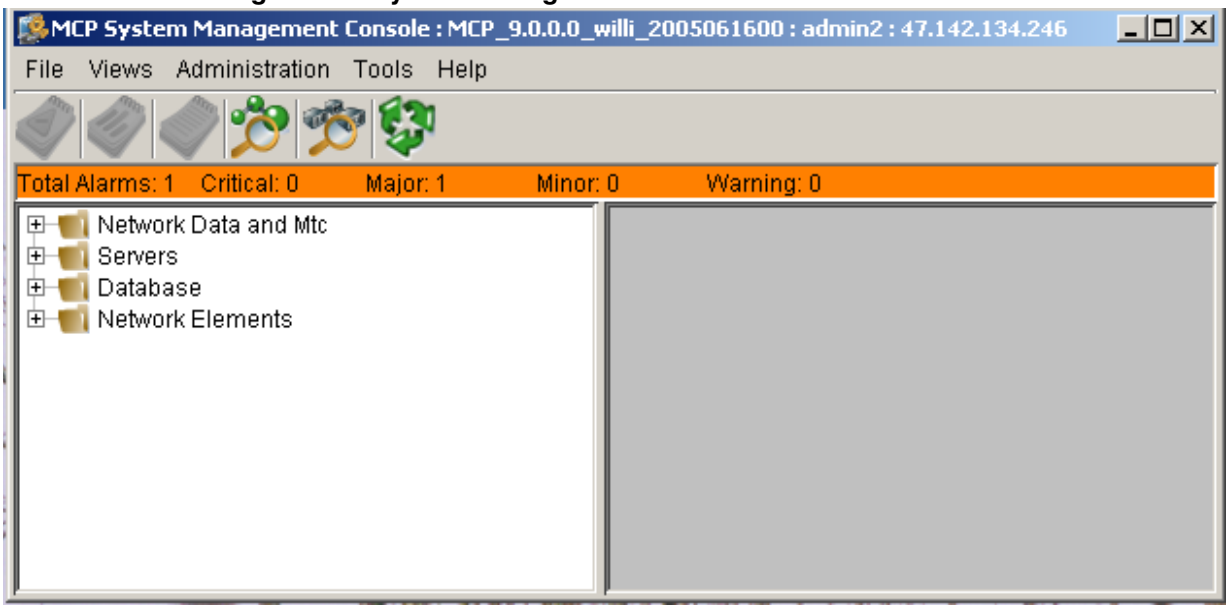
126.2.11 Checking for PCMM Alarms and Logs

As soon as the policy server is configured, the CS2000 will start trying to communicate with it. If this communication fails, a session manager alarm will be raised indicating that the PCMM signaling link cannot be setup. When the PCMM signaling link is down, calls will proceed, but without managed quality of service in the HF/C network.

To check for PCMM alarms, do the following:

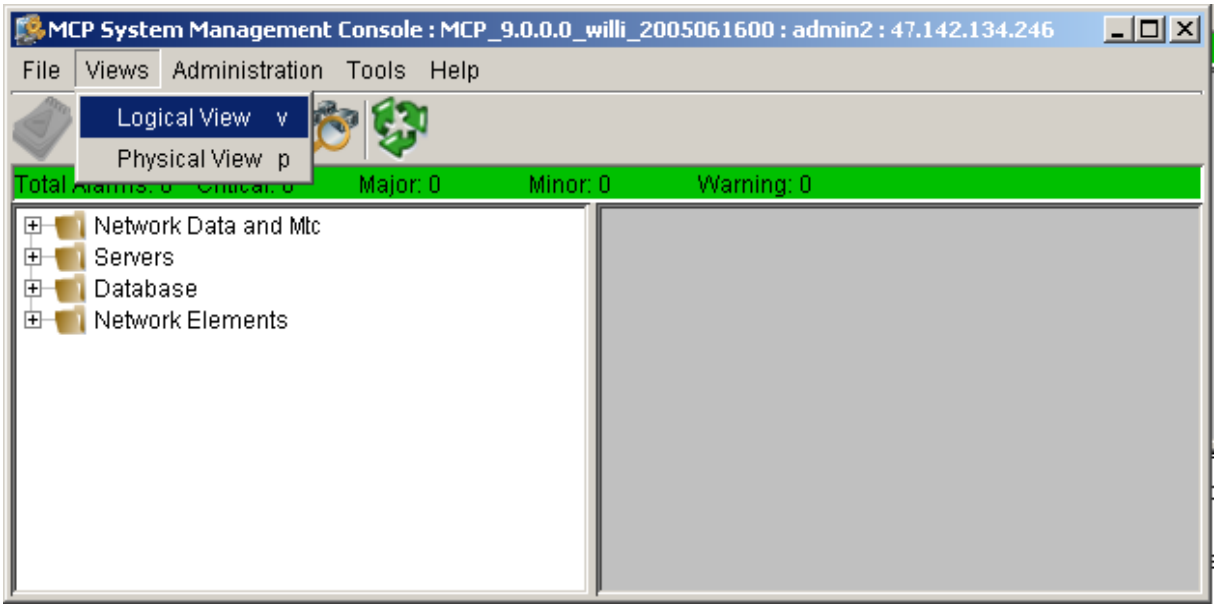
- Login to the System Management Console
- Once you successfully login you will see a screen like the following:

Figure 24 System Management Console



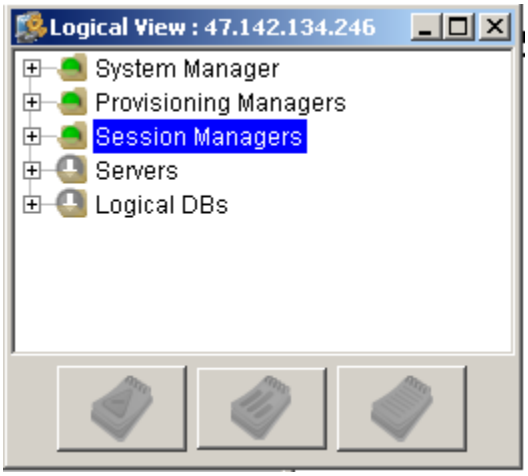
- Note the banner just beneath the tool-bar with a summary of the alarms for the SS-L. If there are any alarms, continue with the next steps to view the alarm details. If no alarms are present, then the PCMM signaling link is operational.
- Start a Logical View of your SS-L as follows:

Figure 25 Starting a Logical View of the MCP System



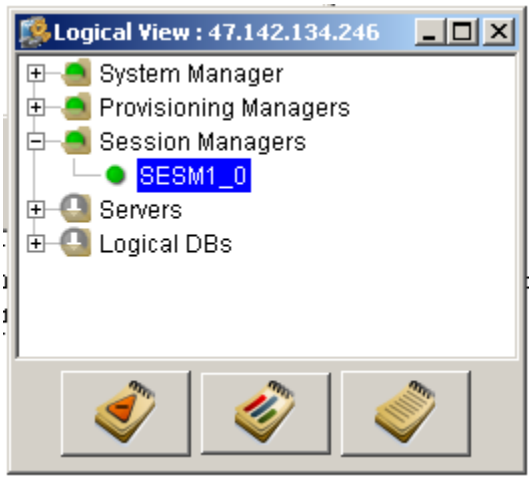
- This will cause a window like the following to appear:

Figure 26 MCP System Logical View



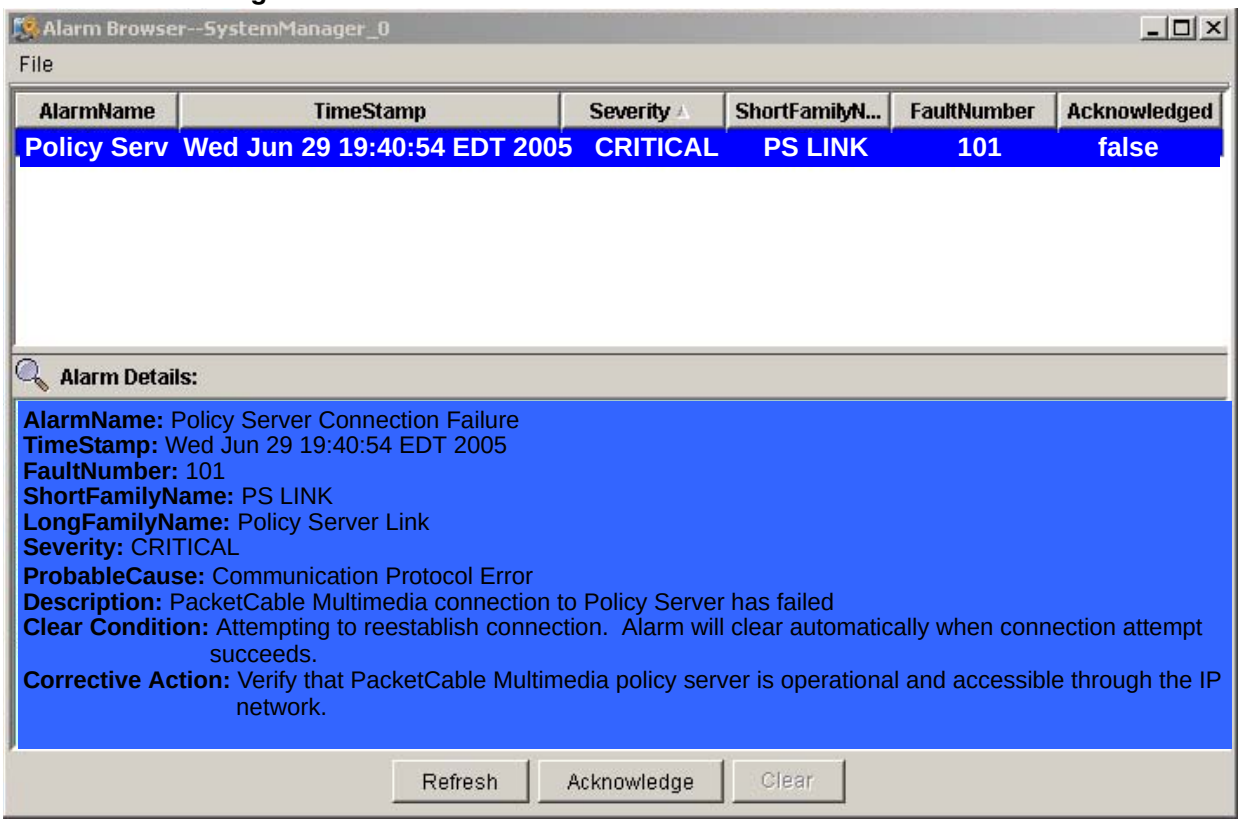
- Expand Session Managers by clicking the "+" to the left of it and highlight a session manager as follows:

Figure 27 Selecting a Session Manager



- Click the button on the lower left to view the alarm browser as follows:

Figure 28 Alarm Browser for PS Connection Failure



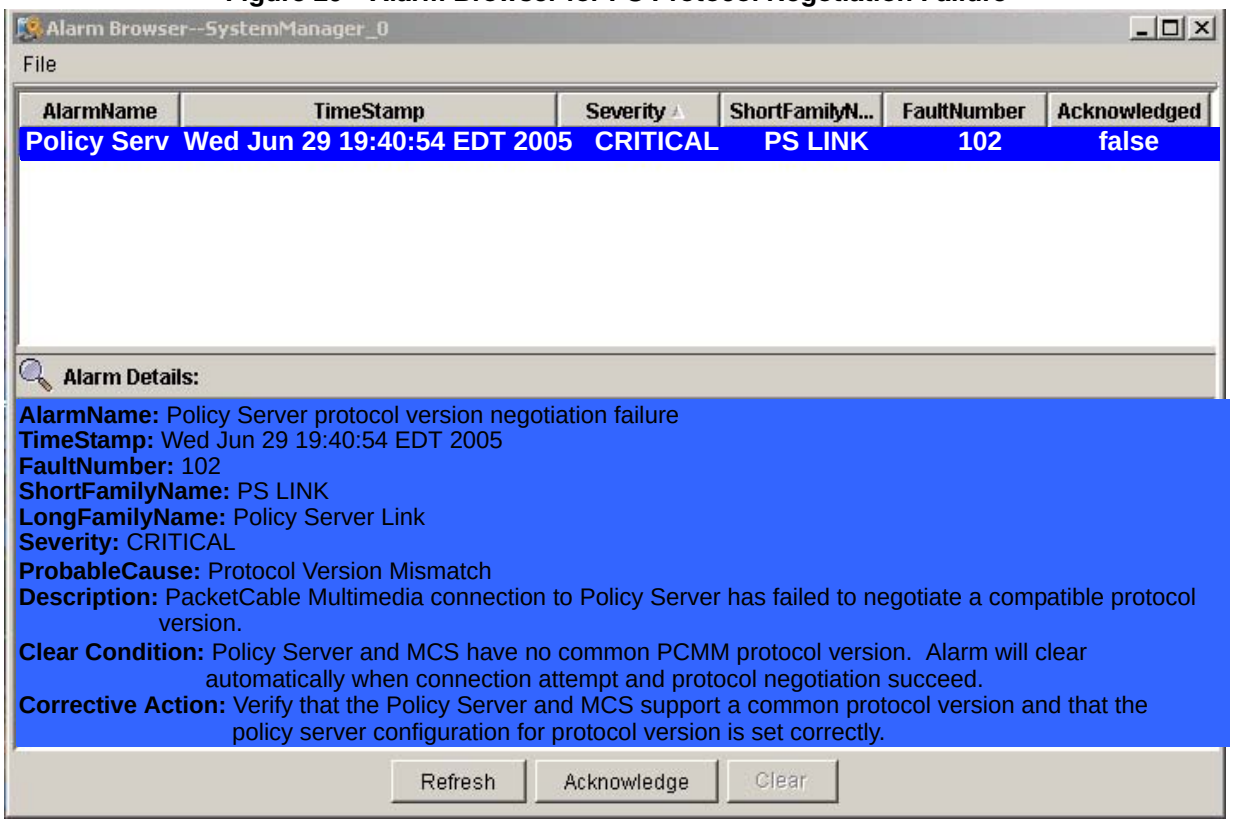
- The alarm view can be manually refreshed by clicking the “Refresh” button.
- Look for alarms with AlarmName “Policy Server Connection Failure” in the upper half of the window. These are PCMM signaling link alarms.

- If you see one, highlight it and the alarm details will be displayed in the lower half of the window.

If you have a PCMM signaling link alarm, all SIP calls from the session manager with the failed PCMM connection will receive best-effort QoS until the problem is resolved. Please refer to the Troubleshooting section of this document for next steps.

Here is an example of the PCMM protocol negotiation alarm that is raised when the PCMM connection fails to come up due to protocol negotiation failure.

Figure 29 Alarm Browser for PS Protocol Negotiation Failure



Following is a summary of all the PCMM alarms and the conditions upon which they are asserted and cleared.

Table 7: PCMM Alarm Conditions

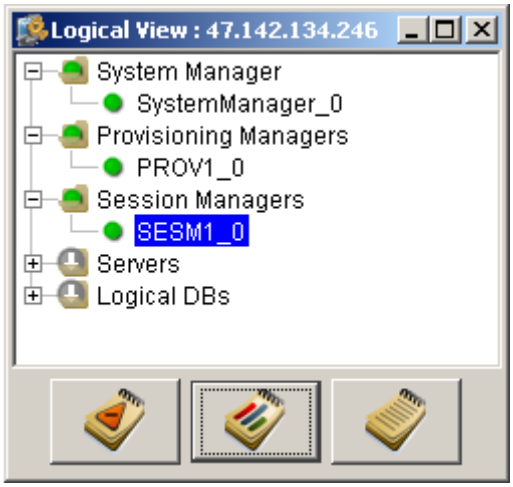
Alarm Name	Severity	Assert	Clear
Policy Server Connection Failure	Critical	Connection drop TCP-layer connection failure Initialization sequence failure other than protocol negotiation	Successful completion of initialization sequence. Deletion of PS from configuration database System or unit shutdown PCMM disabled
Policy Server Protocol Version Negotiation Failure	Critical	Protocol version negotiation failure	Successful completion of protocol negotiation.
PCMM Partial Configuration	Minor	First call to use a policy server for which the session manager AMIDs have not been configured.	Session manager AMIDs successfully configured.

126.2.12 Viewing Operational Measurements

There are a number of operational measurements associated with PCMM. To view PCMM OMs follow this procedure:

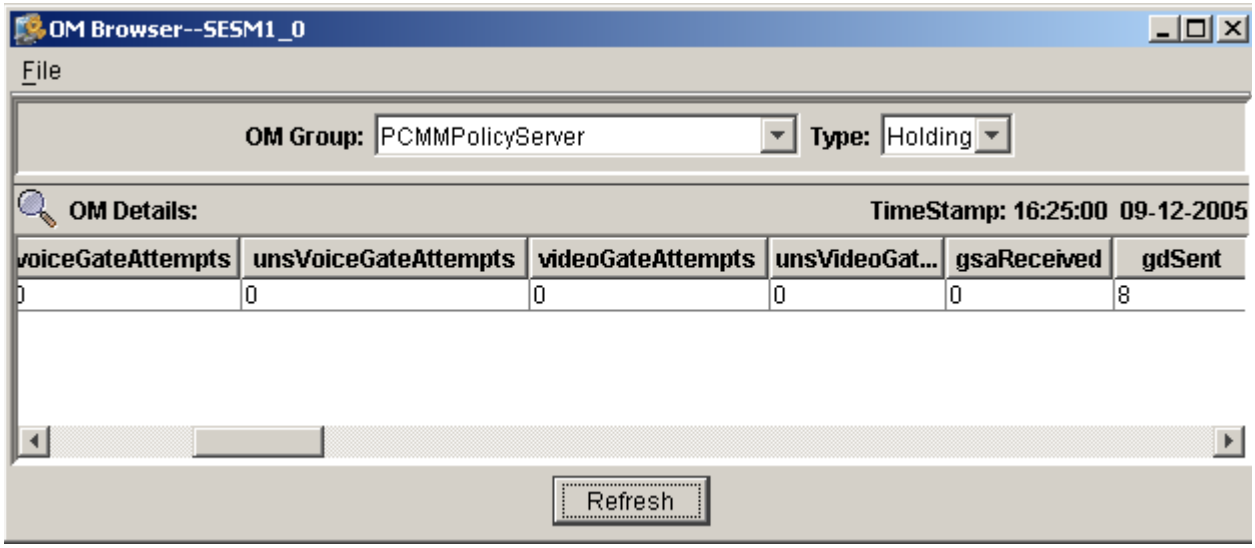
- Pull up the logical view of the MCS as follows:
- Highlight the session manager that you are interested in:

Figure 30 MCP System Logical View



- Click the center button at the bottom of the Logical View window to bring up the OM browser. You will see a window like the following:

Figure 31 Session Manager OM Browser Example



- From the OM Group pull-down menu, select “PCMMAggregate” to access the session manager-wide PCMM OMs. PCMM Aggregate OMs indicate usage of resources that are not specific to any particular policy server.
- Select “PCMMPolicyServer” to access the per-policy server PCMM OMs.

The following tables describe the PCMM operational measurements.

Table 8: PCMM Aggregate Operational Measurements

OM Name	Description
incomingMsgQHighWater	When incoming PCMM signaling messages arrive at the session server they are queued for processing. This OM indicates thehighest percentage used for the incoming PCMM message queue. This value represents the high water mark since the system was started. It is not reset each time the OMs are reported. If this queue gets above ~90%, it may indicate a problem with the PCMM. Please contact your next level of support for assistance.
transactionQHighWater	When the session server sends PCMM messages, the outgoing messages are queued for processing. This OM indicates the highest percentage used for the outgoing PCMM message queue. This value represents the high water mark since the system was started. It is not reset each time the OMs are reported. If this queue gets above ~90%, it may indicate a problem with the PCMM. Please contact your next level of support for assistance.
outstandingQHighWater	After the session server sends a PCMM message to the policy server for processing, the message is held in the outstanding transaction queue until a response is received (or until the transaction times out). This OM indicates the highest percentage used for the outstanding PCMM message queue. This value represents the high water mark since the system was started. It is not reset each time the OMs are reported. If this queue fills up, the oldest outstanding transactions will be removed to make room for newer transactions. This queue can fill up if the policy server is not responding or is responding slowly.
voiceGateAttempts	Total number of PCMM voice half calls processed across all policy servers connected to this session server.
unsVoiceGateAttempts	Total number of unsuccessful PCMM voice half calls processed. There are a number of reasons that a half call might fail to get managed QoS. These include: internal resource errors, no response to transaction, COPS connection down, Gate-Set-Err received from the policy server, etc. Calls that fail to get managed QoS receive best-effort QoS.
unsupCodecVoiceGateAttempts	Total number of PCMM voice half calls with an SDP containing at least one codec for which bandwidth could not be calculated. In order to reserve and commit bandwidth for a call, a mapping must be made between the codec and the flow-spec describing the network resources required. If this mapping fails, then the call might not get optimal bandwidth for managed QoS.

Table 8: PCMM Aggregate Operational Measurements

OM Name	Description
videoGateAttempts	Total number of PCMM video half calls processed across all policy servers connected to this session server.
unsVideoGateAttempts	Total number of unsuccessful PCMM video half calls processed. There are a number of reasons that a half call might fail to get managed QoS. These include: internal resource errors, no response to transaction, COPS connection down, Gate-Set-Err received from the policy server, etc. Calls that fail to get managed QoS receive best-effort QoS.
unsupCodecVideoGateAttempts	Total number of PCMM video half calls with an SDP containing at least one codec for which bandwidth could not be calculated. In order to reserve and commit bandwidth for a call, a mapping must be made between the codec and the flow-spec describing the network resources required. If this mapping fails, then the call might not get optimal bandwidth for managed QoS.
outstandingDiscStale	The number of transactions that were discarded because no response was received from the policy server or because the outstanding transaction queue was full and the oldest transaction waiting for a response was removed to make room for a new transaction.
unkMediaGateAttempts	The number of PCMM gate attempts that could not be processed because the media type was unknown (i.e. not voice, video, or image). Calls that fail to get managed QoS receive best-effort QoS.

Table 9: PCMM Policy Server Operational Measurements

OM Name	Description
numInitializations	Number of times the policy server COPS connection successfully completed the PCMM initialization sequence.
cnxPSDrop	Number of times the policy server gracefully closed the COPS TCP connection (i.e. in a way that caused a TCP FIN message to be sent from the policy server to the session server).
cnxDropProtTimeout	Number of times the connection was dropped by the session server due to lack of PCMM response from the policy server. This could be caused by failure of the session server to receive keep-alive messages or connection initialization sequence messages from the policy server (either because the policy server never sent them or the network prevented them from arriving).

Table 9: PCMM Policy Server Operational Measurements

OM Name	Description
tcpSendFail	Number of times that PCMM messages had to be discarded due to the outgoing TCP buffer being full. Normally this happens if the policy server is not keeping up with the rate of messages being sent from the MCS. TCP send failures can also occur if the network quality is poor, causing a lot of retransmissions.
transDiscLinkDown	Number of PCMM transactions that were discarded due to the PCMM signaling link being down. Since we cannot predict how long a PCMM signaling link might be down, transactions are discarded until the connection is restored. Half-calls whose PCMM transactions are discarded will get "best-effort" quality of service.
transDiscStale	Number of PCMM transactions that were discarded because no response was received from the policy server for more than seven seconds. Or, if the outstanding transaction queue is full, the number of oldest transactions that were discarded to make room for new outstanding transactions.
voiceGateAttempts	Total number of PCMM voice half calls processed for this policy server.
unsVoiceGateAttempts	Total number of unsuccessful PCMM voice half calls processed. This number includes unsuccessful voice calls for all possible reasons.
videoGateAttempts	Total number of PCMM video half calls processed for this policy server.
unsVideoGateAttempts	Total number of unsuccessful PCMM video half calls processed. This number includes unsuccessful video calls for all possible reasons.
gsaReceived	Total number of Gate-Set-Ack messages received from the policy server.
gdSent	Total number of Gate-Delete messages sent to the policy server.
upVoiceGSEReceived	Total number of Gate-Set-Err messages received from the policy server for upstream voice gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason.
upVoiceGSENoResources	Number of Gate-Set-Err messages for upstream voice gates with error code 1 - Insufficient Resources
upVoiceGSEUnkGateId	Number of Gate-Set-Err messages for upstream voice gates with error code 2 - Unknown GateID

Table 9: PCMM Policy Server Operational Measurements

OM Name	Description
upVoiceGSEOther	Number of Gate-Set-Err messages for upstream voice gates with error code 127 - Other, Unspecified Error
dnVoiceGSEReceived	Total number of Gate-Set-Err messages received from the policy server for downstream voice gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason.
dnVoiceGSENoResources	Number of Gate-Set-Err messages for downstream voice gates with error code 1 - Insufficient Resources
dnVoiceGSEUnkGateId	Number of Gate-Set-Err messages for downstream voice gates with error code 2 - Unknown GateID
dnVoiceGSEOther	Number of Gate-Set-Err messages for downstream voice gates with error code 127 - Other, Unspecified Error
gseInvSubscr	Number of Gate-Set-Err messages for voice and video, upstream and downstream gates with error code 13 - Invalid Subscriber ID
gseInvAMID	Number of Gate-Set-Err messages for voice and video, upstream and downstream gates with error code 14 - Unauthorized AMID
upVideoGSEReceived	Total number of Gate-Set-Err messages received from the policy server for upstream video gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason.
upVideoGSENoResources	Number of Gate-Set-Err messages for upstream video gates with error code 1 - Insufficient Resources
upVideoGSEUnkGateId	Number of Gate-Set-Err messages for upstream video gates with error code 2 - Unknown GateID
upVideoGSEOther	Number of Gate-Set-Err messages for upstream video gates with error code 127 - Other, Unspecified Error
dnVideoGSEReceived	Total number of Gate-Set-Err messages received from the policy server for downstream video gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason.
dnVideoGSENoResources	Number of Gate-Set-Err messages for downstream video gates with error code 1 - Insufficient Resources
dnVideoGSEUnkGateId	Number of Gate-Set-Err messages for downstream video gates with error code 2 - Unknown GateID
dnVideoGSEOther	Number of Gate-Set-Err messages for downstream video gates with error code 127 - Other, Unspecified Error

Table 9: PCMM Policy Server Operational Measurements

OM Name	Description
grsClose	Total number of Gate-Report-State messages received indicating that a gate was closed by the CMTS for all reasons.
grsCloseResReassign	Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 1 - reservation reassignment.
grsCloseMacLayer	Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 2 - lack of DOCSIS MAC-Layer responses
grsCloseT1	PCMM timer T1 specifies the number of seconds a PCMM gate can be authorized but not reserved. This OM indicates the number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 3 - timer T1 expiration
grsCloseT2	PCMM timer T2 specifies the number of seconds a PCMM gate must hold bandwidth reserved in excess of what was committed. Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 4 - timer T2 expiration
grsCloseResMaint	Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 6 - lack of reservation maintenance
grsCloseT4	Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 8 - timer T4 expiration.
grsNotif	Total number of Gate-Report-State messages received indicating a change of gate state (for any reason) that did not result in the gate being closed.
grsNotifT3	Number of Gate-Report-State messages received indicating that a gate was transitioned to the Committed-Recovery state by the CMTS due to the T3 timer expiring. If the T3 timer expires frequently, you may wish to increase the T3 timer value to a longer duration.

126.2.13 Changing Policy Server Attributes

Some policy server attributes can be changed with no service impact. Other attributes require a re initialization of the PCMM signaling link. The policy server name cannot be changed without deleting and re adding the policy server.

126.2.13.1 Changes requiring a PCMM connection reinitialization

Policy server attributes that define the address of the policy server or are communicated to the policy server only when the connection is started require

that the connection be re initialized. Changing these fields will cause the PCMM signaling connection between the MCS and the policy server to be dropped and immediately reestablished. Calls being setup during the short interval when the PCMM signaling link is down will proceed, but with best-effort quality of service. Changing any of the following fields will cause a PCMM connection reinitialization.

- Policy Server Address
- Policy Server Port
- Protocol Version
- Keep-Alive Timer

See section 126.2.7 on page 1182 for a description of policy server attributes.

When the "Apply" button is clicked after changing any of these fields, a warning dialog will be displayed indicating the consequences of changing these fields and asking you to confirm the operation. Clicking "Yes" will save the changes and reinitialize the connection. Clicking "No" will revert to the prior values.

126.2.13.2 Changes that take effect immediately

The remaining policy server fields can be changed without bouncing the policy server connection. They are:

- Timer T1
- Timer T2
- Timer T3
- Timer T4

See section 126.2.7 on page 1182 for a description of the PCMM protocol timers T1 through T4.

These values will be used for the next call that is started after the "Apply" button is clicked to save the changes.

126.2.14 Removing PCMM Capability from a Subscriber

There are two ways to remove PCMM capability from a subscriber:

- Change the service package that the subscriber is assigned to so that it no longer has the PacketCable Multimedia box checked.
- Change the subscriber to use an existing service package that does not have the PacketCable Multimedia capability assigned.

126.2.15 Deleting a Policy Server and its associated AMIDs

A policy server may be deleted using the MCS System Management Console. Before a policy server can be deleted, however, the AMIDs associated with the policy server on all active session managers must be deleted first. A window displaying an error message will appear if an attempt is made to delete a policy server when an AMID is still provisioned against that policy server on any active session manager.

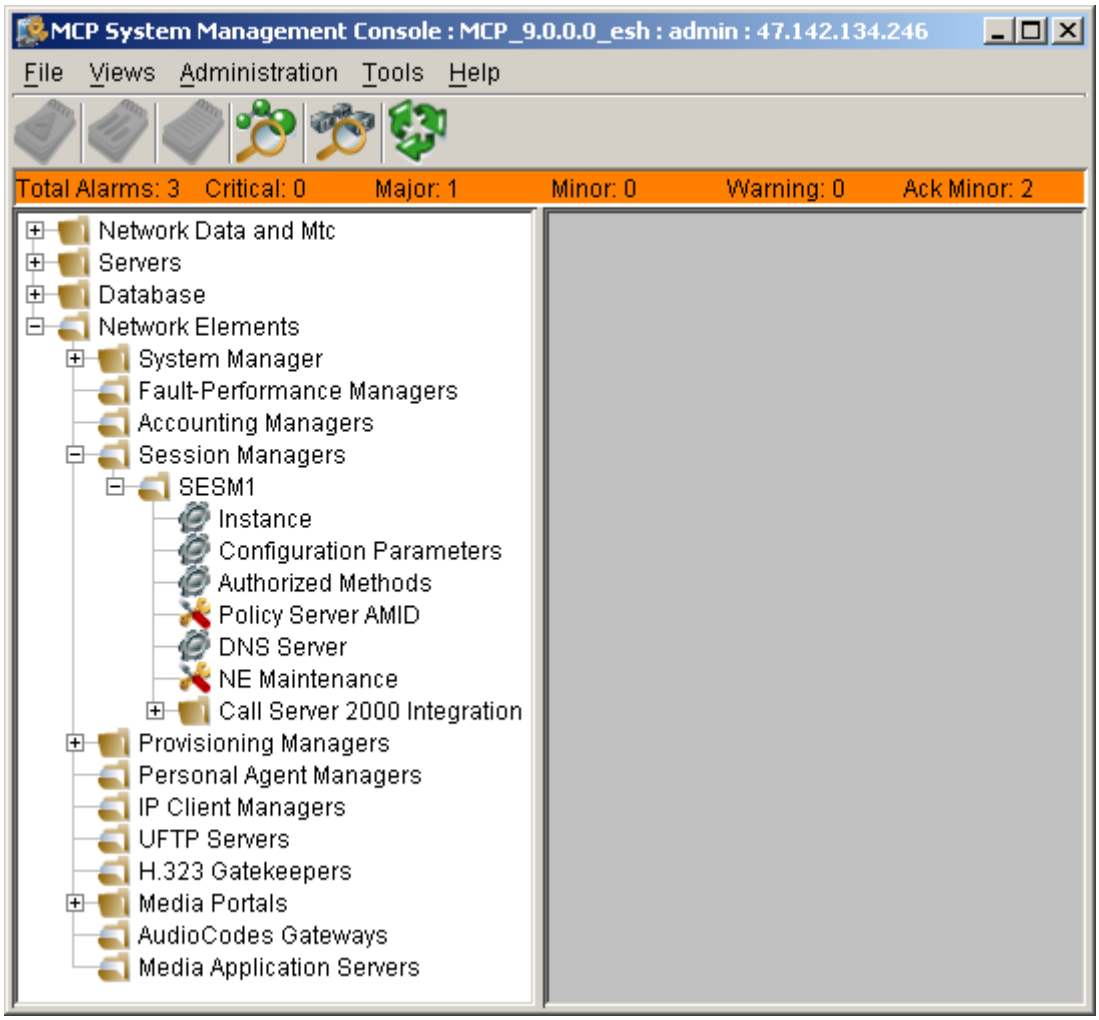
In order to delete the policy server:

- Expand the “Network Elements” and “Session Managers” items

Figure 32 System Management Console for Network Elements

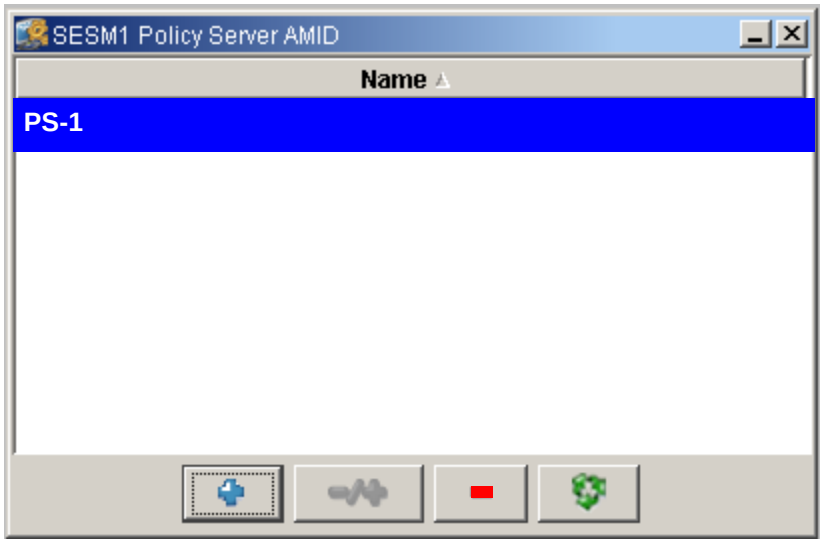
- Select and expand each active session manager

Figure 33 System Management Console for Session Managers



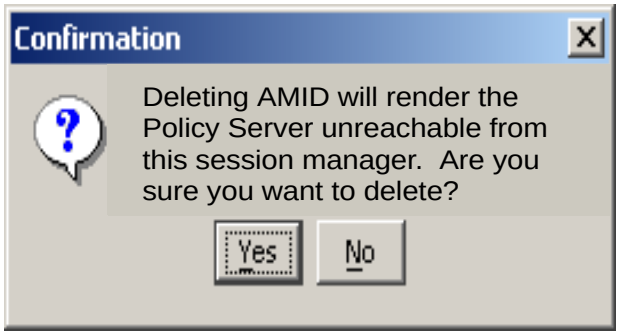
- Click Policy Server AMID and a window will appear showing the assigned policy servers.

Figure 34 Session Manager AMID Dialogue



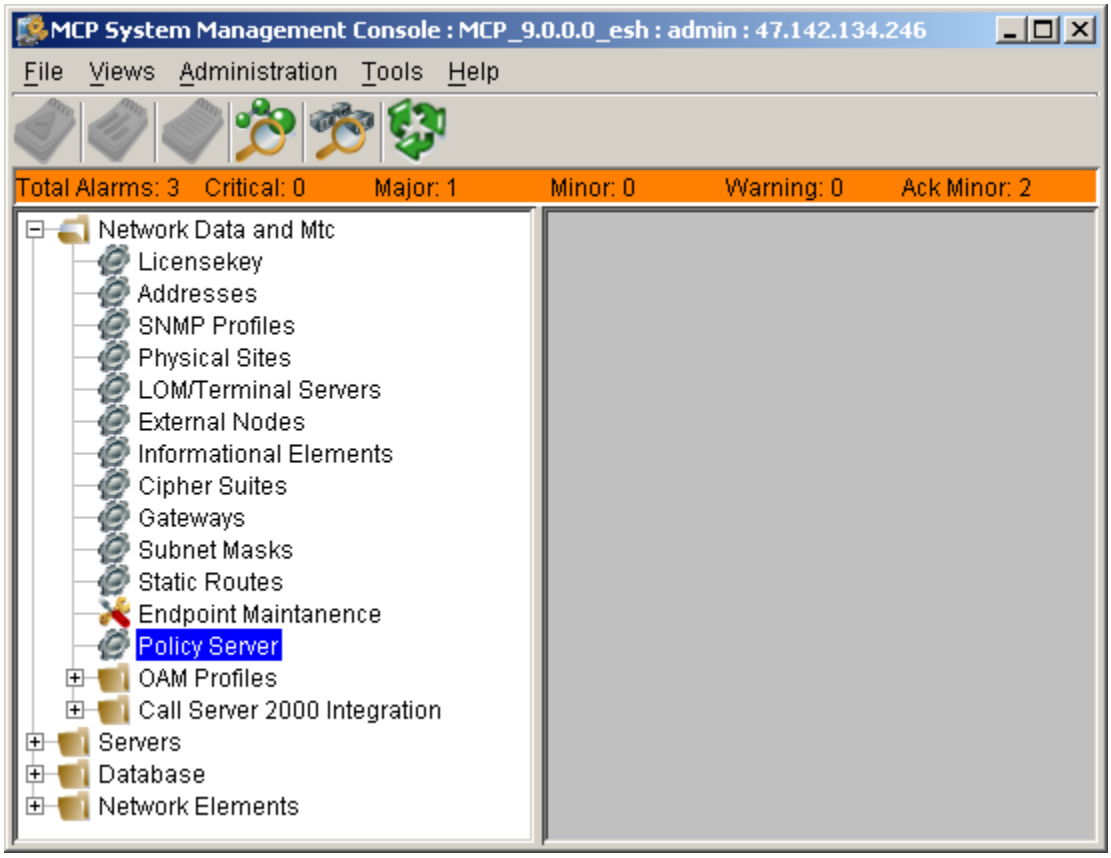
- Highlight the policy server to be deleted <<and the AMIDs will be displayed???>>
- Click the "-" minus button and click "Apply" to remove the AMIDs from that session manager
- A warning dialogue will appear indicating that removal of AMIDs will render the connection from this session manager to the policy server unusable. Once the AMID has been removed and prior to removal of the policy server, a minor alarm will appear for the session managers that no longer have AMIDs (see section 126.2.11 on page 1197). This alarm indicates that a partial configuration is present and will clear once the policy server is deleted.

Figure 35 AMID Delete Confirmation



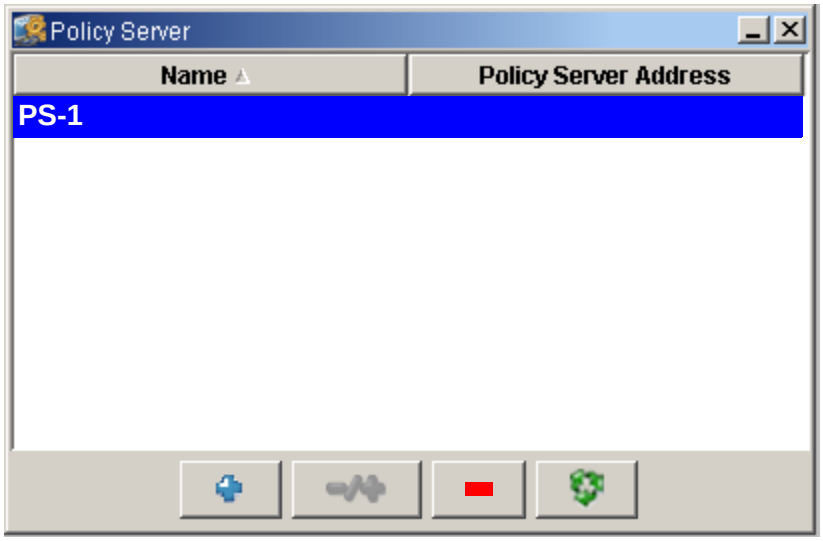
- Repeat above to remove the AMIDs from all active session managers.
- Now that all associated AMIDs have been removed, expand the "Network Data and Mtc" item

Figure 36 System Management for Policy Servers



- Select the Policy Server icon, a window will appear showing the configured policy servers.

Figure 37 Policy Server Dialogue



- Highlight the policy server to be deleted and click the "-" (minus) button and click "Apply" to delete the policy server.

WARNING: Deletion of a Policy Server will cause all new PCMM capable calls to receive best-effort quality of service within the cable network.

126.2.16 Understanding Session Manager Failover

The session manager can be configured for redundancy, thus enabling failover if something goes wrong. This section describes what happens to calls in the event of a failover. A warm failover is when the active unit fails and the standby unit is up and ready to become the active unit. A cold failover happens when there is no standby unit or when the standby unit is not ready to become active.

126.2.16.1 Warm

A stable subscriber session and its managed QoS will survive a warm failover. Subscribers on calls in the conversation phase at the time of the warm failover will not notice that a failover has occurred.

Calls that are held or for any reason have no media packets flowing at the time of the session manager failover may lose their managed QoS if the T3 and T4 timers subsequently expire. The held calls will not be torn down, but they may lose their managed QoS and continue using best-effort QoS.

Calls in the setup phase at the time of the warm failover are not guaranteed to succeed. If they do succeed, they may get only best-effort QoS.

126.2.16.2 Cold

All calls are torn down on cold failover.

126.2.17 Troubleshooting

The following table lists the more common failure modes and gives advice on resolving the problem. In general, always check for alarms first. If an alarm is present, look for logs generated around the same time the alarm was

generated. Also look at PCMM OMs to determine if there are any unexpected peg-counts.

Table 10: PCMM Troubleshooting

Condition	Possible Causes and Corrective Actions
Policy Server connection failure alarm	Incorrect policy server IP address or port. Verify that the policy server IP address and port configuration are correct. Network problem between session manager and policy server. Verify that you can ping the policy server from the session manager. Make sure any firewalls are configured to allow TCP packets between the session manager and policy server. Policy server not running or not configured correctly. Verify that your policy server is operating correctly.
Policy Server protocol version negotiation failure alarm	Protocol version misconfigured. Verify that your PCMM protocol version number is set to the highest protocol that you want to allow for the PCMM connection. For this initial release, the protocol version should be set to 1.0. Policy server is running incompatible software. Verify that the policy server supports the protocol version for which you have configured the CS2000 PCMM protocol version.
Poor voice or video quality	PCMM signaling connection is down. Verify that you don't have any Policy Server alarms. The audio or video codec being use for the call is not supported for PCMM. Calls not using G.711 or G.729 for voice, or H.263 or DIVX for video do not receive managed QoS. Other PCMM signaling problems are occurring. Check your PCMM operational measurements (OMs) to see if any unexpected peg counts are present. Please refer to the OM section of this document for a complete description of all PCMM OMs. Calls active at the time of a failover can lose their managed QoS if they are subsequently placed on hold (no media packets flowing) for longer than the combined length of the T3 and T4 timers. (The T3 and T4 timers are configured against the policy server in the MCP System Management Console.)

126.3 MCP Provisioning Client PCMM Help Information

In lieu of additional PCMM help information in the MCP Provisioing Client the following provides a description PCMM service.

Service Name : PCMM

Parameters : None

Desciption: When assigned to a user thru a service package, this parameter in conjunction with a configured Policy Server will provide the user the ability to receive managed quality of service for all voice and or video sessions. The service is provisioned on a service package level for domains or sub-domains-- see the MCS Provisioning Client Help information under “Defining and Assigning Services” and “Assigning Services and Creating Service Packages”.

126.4 Hardware Requirements or Dependencies

In order to implement the PCMM feature, the MSO needs to have cable network elements that are not supplied by Nortel. These cable network elements include cable modems, CMTSs, and a policy server.

There are no additional CS2000 hardware elements required for PCMM other than what was necessary for a basic SIP lines deployment.

Nortel has tested PCMM with all endpoints supported by the CS2000 SIP lines program, including the following SIP clients:

- Nortel Networks PC Client
- Cisco 7960 SIP phone

126.5 Software Requirements or Dependencies

The policy server and CMTSs in the cable network must support PacketCable Multimedia specification PKT-SP-MM-I02-040930. The cable modems must support DOCSIS 1.1.

The CS2000 components must be at SN09 including the MCS software for PCMM.

126.6 Limitations and restrictions

This initial release of the PCMM service has the following limitations:

- Single policy server per CS2000
- Emergency calls are not distinguished from normal calls with respect to PCMM
- No support for IPSec on the PCMM signaling connection

- No PCMM marking in billing records
- Support for audio codecs G.711 and G.729 only
- Support for video codecs H.263 and DIVX only
- Inability to disable DSCP overwrite
- DSCP must be the same for upstream and downstream flows
- PCMM signaling only for committed state

The following items indicate *optional* protocol elements that are not included in this release of the PCMM service:

- No support for optional Time Based Usage Limits
- No support for optional Volume Based Usage Limits
- PCMM signaling only for committed state
- Only Flow-Spec Traffic-Profile supported
- No support for optional Opaque-Data
- No support for optional state synchronization with policy server
- Single classifier based on media source and destination IP addresses and ports (no classification based on DSCP)

126.7 Interactions

The PCMM feature sets up managed quality of service for SIP line calls originating from or terminating to the cable network. PCMM operates on a half-call basis. This means that PCMM signaling and managed QoS happen only for the half of the call that is in the cable network. For example, an on-net to off-net call will only do PCMM signaling for the originating line half of the call. The trunk half of the call is not touched by PCMM.

The PCMM service works for all call types supported by the CS2000 SIP lines program.

126.7.1 Basic Call

The PCMM feature attempts to set up managed quality of service when the SDP information is known for both of the media endpoints (originating and terminating). If PCMM fails to set up managed QoS, the call proceeds with "best-effort" QoS. Calls will never fail due to PCMM, but it is possible under some error conditions that a call might not receive managed QoS.

126.7.2 Codec Support

The following codecs and packetization rates are supported:

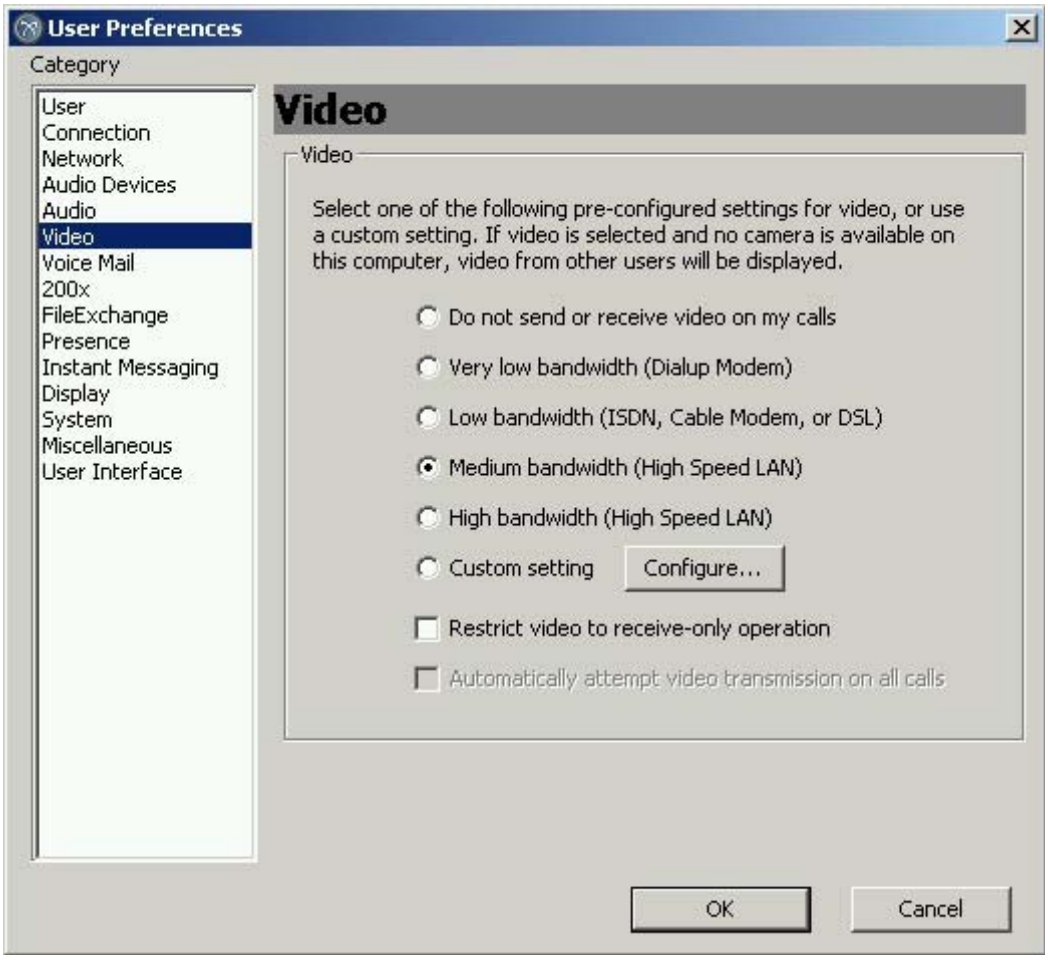
Table 11: PCMM Supported Codec/ptime Combinations

Codec	ptime
PCMU	10 20 30
PCMA	10 20 30
G.729A	10 20 30
H.263	
DIVX	

126.7.3 Supported Video Configuration using Multimedia PC Client

The Nortel Networks Multimedia PC Client provides extensive flexibility in the configuration of video parameters. Not all configurations cans be supported with the PacketCable Multimedia capability.

Figure 38 Multimedia PC Client Video Preferences



There are 4 preset configurations optimized for different bandwidth usage from “very low bandwidth” to “high bandwidth”. Each of these settings can be used with the PacketCable Multimedia capability.

The “custom setting” is not supported for use with the PacketCable Multimedia capability.

126.8 PacketCable Requirements Compliance

The following table lists the PacketCable requirements from PKT-SP-MM-I02-040930 that apply to an application manager and indicates Nortel CS2000 compliance.

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15004	The AMID MUST be a globally unique value assigned to the Application Manager by the service provider.	Yes	MUST	
MMREQ15005	The Application Manager MUST use the assigned AMID in all its interactions with Policy Servers.	Yes	MUST	
MMREQ15011	The Policy Server or Application Manager MUST define the Traffic Profile for a Gate using one of the following: (1) the FlowSpec, (2) DOCSIS Service Class Names, or (3) DOCSIS-Specific Parameters.	Yes	MUST	
MMREQ15014	There MUST be at least one set of Traffic Profile parameters specified when the Gate is first being installed.	Yes	MUST	
MMREQ15017	A controlled load service MUST contain only the TSpec token bucket parameters, and not the RSpec.	Yes	MUST	
MMREQ15018	A guaranteed service MUST contain both the TSpec and the RSpec.	Yes	MUST	
MMREQ15022	If the Application Manager wishes to use this third way of defining a Traffic Profile, it MUST include an object containing the DOCSIS Specific Parameters.	Yes	MUST	
MMREQ15041	To reserve resources, the Policy Server MUST issue a subsequent Gate-Set message with a Traffic Profile that includes the Reserved Envelope.	Yes	MUST	
MMREQ15051	The Reserved envelope MUST always be less than or equal to the Authorized envelope.	Yes	MUST	

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15053	However, all requests to modify Authorized, Reserved or Committed envelopes MUST conform to the general rule:	Yes	MUST	
MMREQ15061	In the Committed state, the Application Manager MAY delete the Gate by issuing a Gate-Delete message to the Policy Server, which in turn MUST relay the message onto the CMTS.	Yes	MUST	
MMREQ15073	The Application Manager MUST either refresh the policy by issuing a Gate-Set message, or remove the Gate by issuing a Gate-Delete message.	Yes	MUST	
MMREQ15093	In contrast, PacketCable Multimedia implementations MUST use the TransactionID object to match responses with requests and SHOULD send RPT messages as soon as they are ready.	Yes	MUST	
MMREQ15095	Protocol messages for Gate Control MUST be transported within the COPS protocol messages.	Yes	MUST	
MMREQ15096	The PDP and PEP MUST establish and use a TCP connection for communication, and utilize the mechanisms specified in [17] to secure the communication path.	Yes	MUST	
MMREQ15097	The Application Manager, Policy Server and CMTS MUST use the COPS Common Message format as defined below as the message format for all message exchanges.	Yes	MUST	
MMREQ15098	This field MUST be set to 1.	Yes	MUST	
MMREQ15099	, a solicited decision sent in response to a request) this flag MUST be set to 1.	Yes	MUST	
MMREQ15100	, an unsolicited decision) the flag MUST NOT be set (value = 0).	Yes	MUST	

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15101	In keeping with the DQoS model, the first Decision message sent in response to a Request message is a solicited response and its solicited message flag MUST be set.	Yes	MUST	
MMREQ15102	All other Decision messages are unsolicited and the solicited message flag MUST be cleared.	Yes	MUST	
MMREQ15103	All other flags MUST be set to zero.	Yes	MUST	
MMREQ15104	For PacketCable Multimedia use, the Client-Type MUST be set to PacketCable Multimedia client (0x800A).	Yes	MUST	
MMREQ15105	For Keep-Alive messages (Op-code = 9) the Client-Type MUST be set to zero, as the KA is used for connection verification rather than per-client session verification.	Yes	MUST	
MMREQ15106	Messages MUST be aligned on 4-byte boundaries, so the length MUST be a multiple of four.	Yes	MUST	
MMREQ15107	All the objects MUST conform to the same object format where each object consists of one or more 4-byte words with a four-octet header, using the following format.	Yes	MUST	
MMREQ15108	Length is a 2-byte unsigned integer value that MUST give the number of bytes (including the header) that compose the object.	Yes	MUST	
MMREQ15109	If the original length in octets is not a multiple of four, padding MUST be added to the end of the object so that it is aligned to the next 4-byte boundary.	Yes	MUST	
MMREQ15110	Each of these objects MUST conform to the format and rules relating to the individual object as defined in[10].	Yes	MUST	

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15111	These objects MUST be placed inside a Decision object, C-Num = 6, C-Type = 4 (Client Specific Decision Data) when carried from PDP to PEP in a Decision message.	Yes	MUST	
MMREQ15113	S-Num and S-Type MUST be one octet.	Yes	MUST	
MMREQ15114	The COPS Length field MUST be two octets.	Yes	MUST	
MMREQ15115	The TransactionID MUST also contain the command type that identifies the action to be taken or response.	Yes	MUST	
MMREQ15116	The TransactionID Object MUST conform to the following format.	Yes	MUST	
MMREQ15118	Gate Command Type is a 2-byte unsigned integer value which identifies the Gate Control message type and MUST be one of the following:	Yes	MUST	
MMREQ15119	The Application Manager MUST include this object in all messages it issues to the Policy Server.	Yes	MUST	
MMREQ15122	The AMID object MUST conform to the following format.	Yes	MUST	
MMREQ15123	The SubscriberID object MUST conform to the following format.	Yes	MUST	
MMREQ15126	The GateID object MUST conform to the following format.	Yes	MUST	
MMREQ15127	The GateSpec object MUST conform to the following format.	Yes	MUST	
MMREQ15128	Bit 0: direction bit, MUST be either zero for a downstream Gate, or one for an upstream Gate.	Yes	MUST	
MMREQ15129	Bit 1: DSCP/TOS enable bit, MUST be either zero to disable DSCP overwrite, or one to enable.	Yes	MUST	

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compli-ance	Cate-gory	Comment
MMREQ15130	Bits 2-7: reserved, MUST be zero.	Yes	MUST	
MMREQ15139	The Classifier object MUST conform to the following format.	Yes	MUST	
MMREQ15140	Source IP Address and Destination IP Address MUST be a pair of 4-octet IPv4 addresses, or zero for no match (i.e.,	Yes	MUST	
MMREQ15141	Source Port and Destination Port MUST be a pair of 2-byte unsigned integer values, or zero for no match	Yes	MUST	
MMREQ15142	Protocol ID MUST conform to section C.2.1.5.2 of [1], or zero for no match.	Yes	MUST	
MMREQ15143	DSCP/TOS Field is a 1-byte bit field which MUST conform to the following alternative structures:	Yes	MUST	
MMREQ15146	Thus, all traffic parameters associated with a given Gate MUST be included in every message that includes a Traf-fic Profile.	Yes	MUST	
MMREQ15147	Only the following values are legal: 001, 011 and 111; the Envelope Field MUST be set to one of these three legal values.	Yes	MUST	
MMREQ15148	Otherwise, the PDP MUST ensure that exactly one set of envelope parameters is included for each of the envelope types that are indicated in the envelope field.	Yes	MUST	
MMREQ15149	The FlowSpec object MUST conform to the following specification:	Yes	MUST	
MMREQ15153	The DOCSIS Service Class Name object MUST conform to the following specification:	Yes	MUST	
MMREQ15154	The Service Class Name is MUST be 2-16 bytes of null-terminated ASCII string.	Yes	MUST	

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15155	This name MUST be padded with null bytes to align on a 4-byte boundary.	Yes	MUST	
MMREQ15156	The Best Effort object MUST conform to the following specification:	Yes	MUST	
MMREQ15158	The Non-Real Time Polling object MUST conform to the following specification:	Yes	MUST	
MMREQ15161	The Real-Time Polling object MUST conform to the following specification:	Yes	MUST	
MMREQ15164	The Unsolicited Grant object MUST conform to the following specification:	Yes	MUST	
MMREQ15165	The Unsolicited Grant with Activity Detection object MUST conform to the following specification:	Yes	MUST	
MMREQ15167	The Downstream object MUST conform to the following specification:	Yes	MUST	
MMREQ15170	The Event Generation Info object MUST conform to the following specification:	Yes	MUST	Optional - not used
MMREQ15171	Primary-Record-Keeping-Server-IP-Address is a 4-byte field which MUST contain the IPv4 address of the primary RKS to whom event records are to be sent.	Yes	MUST	Optional - not used
MMREQ15172	Primary-Record-Keeping-Server-Port field is a 2-byte unsigned integer which MUST contain the port number on the primary RKS where event records are to be sent.	Yes	MUST	Optional - not used
MMREQ15173	Secondary-Record-Keeping-Server-IP-Address is a 4-byte field which MUST contain the IPv4 address of the secondary RKS to whom records are to be sent if the primary RKS is unavailable.	Yes	MUST	Optional - not used

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15174	Secondary-Record-Keeping-Server-Port is a 2-byte unsigned integer which MUST contain the port number on the secondary RKS where event records are to be sent.	Yes	MUST	Optional - not used
MMREQ15175	Billing-Correlation-ID is a 24-byte field which MUST contain the identifier assigned by the AM or PS for all records related to this session.	Yes	MUST	Optional - not used
MMREQ15176	It MUST NOT be used in any other messages.	Yes	MUST	Optional - not used
MMREQ15177	The Volume-Based Usage Limit object MUST conform to the following specification:	Yes	MUST	Optional - not used
MMREQ15178	The Time-Based Usage Limit object MUST conform to the following specification:	Yes	MUST	Optional - not used
MMREQ15180	It MUST NOT be used in any other messages issued by the PDP to the PEP.	Yes	MUST	Optional - not used
MMREQ15198	Messages that perform gate control between the Application Manager and Policy Server are defined and MUST be formatted as follows.	Yes	MUST	
MMREQ15199	Note that messages from the Application Manager to Policy Server MUST be formatted as COPS Decision messages, and messages from Policy Server to Application Manager MUST be formatted as COPS Report-State messages.	Yes	MUST	
MMREQ15202	For Gate Control command messages, the Context object (C-Num = 2, C-Type = 1) in the COPS Decision message MUST have the R-Type (Request Type Flag) value set to 0x08 (Configuration Request) and the M-Type set to zero.	Yes	MUST	

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15203	The Command-Code field in the mandatory Decision-Flags object (C-Num = 6, C-Type = 1) MUST be set to 1 (Install Configuration).	Yes	MUST	
MMREQ15211	Any Application Manager or Policy Server (PDP) with a need to contact a PEP MUST initiate a TCP connection to the PEP on that port.	Yes	MUST	
MMREQ15214	Upon successful receipt of the Client-Open message, the PDP MUST send a Client-Accept message if the protocol version specified in the Version Info object is supported.	Yes	MUST	
MMREQ15215	This message MUST include the Keep-Alive-Timer object, which tells the PEP the maximum interval between Keep-Alive messages.	Yes	MUST	
MMREQ15216	If the protocol version supplied by the PEP is not supported, the PDP MUST send a Client-Close messages with a COPS Error Object specifying error code 4 (Unable to process).	Yes	MUST	
MMREQ15217	After sending the Client-Close, the PDP MUST retain the TCP connection and security association with the PEP so that the PEP can reattempt the COPS initialization without reestablishing the TCP connection and security association.	Yes	MUST	
MMREQ15219	The PDP MUST then send a Client-Close message to the PEP to acknowledge that protocol negotiation has failed.	Yes	MUST	
MMREQ15221	Devices compliant with this specification MUST use a version of 1.0, i.e.	Yes	MUST	
MMREQ15227	Upon receipt of the COPS KA message, the PDP MUST echo a COPS KA message back to the PDP.	Yes	MUST	

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15230	All messages from the PDP to the PEP MUST be sent using Client-Specific objects within the Decision object of a COPS Decision message.	Yes	MUST	
MMREQ15233	The Decision messages and Report-State messages MUST contain the same Client-Handle as provided in the initial Request sent by the CMTS when the COPS connection was initiated.	Yes	MUST	
MMREQ15237	The PDP MUST keep track of when KAs are received.	Yes	MUST	
MMREQ15238	If the PDP has not received a KA from the PDP in the time interval specified in [10] or the PDP has not received an error indication from the TCP connection, then the PDP MUST tear down the TCP connection and attempt to re-establish the TCP connection.	Yes	MUST	
MMREQ15239	, Gate-Set, Gate-Info, and Gate-Delete) MUST include (in addition to other mandatory objects) both AMID and SubscriberID objects.	Yes	MUST	
MMREQ15249	At any one point in time, the Committed envelope MUST fit within the Reserved Envelope which MUST fit within the Authorized envelope.	Yes	MUST	
MMREQ15254	For traffic profiles in the form of a Service Class Name, the Service Class Name string MUST exactly match the preexisting Service Class Name on the CMTS.	Yes	MUST	
MMREQ15255	The Gate-Set message MUST contain exactly one GateSpec object, describing one upstream or downstream Gate.	Yes	MUST	
MMREQ15284	: The Application Manager MUST handle received reports.	Yes	MUST	

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15285	Thus, the Application Manager MUST enforce the Time-Based Usage Limit of the Gate.	Yes	MUST	Optional - not used
MMREQ15286	Upon receiving the Gate-Set-Ack for a Gate with a Time-Based Usage Limit, the AM MUST start an application timer.	Yes	MUST	Optional - not used
MMREQ15287	When the application timer is equal to the Time-Based Usage Limit, the Application Manager MUST respond by performing one of the following actions:	Yes	MUST	Optional - not used
MMREQ15299	The PDP in response MUST automatically delete any state associated with the PEP when the TCP connection is terminated.	Yes	MUST	
MMREQ15324	If present, this object MUST contain a valid BCID which can be used by the AM, PS, and CMTS to correlate billing information for the flow.	Yes	MUST	Optional - not used
MMREQ15330	The PS MUST include the BCID in the EM header for all subsequently generated Policy Event Messages associated with this request.	Yes	MUST	Optional - not used
MMREQ15332	Also, the PS MUST include the BCID in the Gate-Set message sent to the CMTS.	Yes	MUST	Optional - not used
MMREQ15373	The Application Manager - Policy Server COPS interface MUST be secured using the IPsec ESP protocol, as specified in Section 7.2.1.3.2 of [17].	No	MUST	Planned
MMREQ15374	The key management requirements for this interface MUST comply with Section 7.2.1.4.1 of [17].	No	MUST	Planned

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15375	For this interface, Application Manager MUST comply with all the Gate Controller requirements listed in Sections 7.2.1.3.2 and 7.2.1.4.1 of [17].	No	MUST	Planned
MMREQ15376	The first component of Application Manager's principal name MUST be:	No	MUST	Planned
MMREQ15377	The value of <Sub-System Name> for an Application Manager MUST be the following 2-character string: am.	No	MUST	Planned
MMREQ15381	Guaranteed service MUST contain both the TSpec and the RSpec.	Yes	MUST	
MMREQ15387	The RSpec parameters MUST be specified for a guaranteed service.	Yes	MUST	
MMREQ15389	If the Application Manager/Policy Server wishes to set those Service Flow parameters to something other than the defaults specified by this specification, the Application Manager/Policy Server MUST use either the Service Class Names or the DOCSIS-specific parameterization formats to define the traffic profile.	Yes	MUST	
MMREQ15484	A default value of 64 SHOULD be used if a specific priority value is not required.	Yes	SHOULD	
MMREQ15485	If all of the envelope types that are indicated in the envelope field share a common set of envelope parameters, then the PDP SHOULD ensure that exactly one set of envelope parameters are present in the traffic profile.	Yes	SHOULD	
MMREQ15486	A default Traffic Priority of 0 SHOULD be used if a specific Traffic Priority value is not required.	Yes	SHOULD	
MMREQ15487	A default Request/Transmission policy of 0 SHOULD be used if a specific Request/Transmission Policy value is not required.	Yes	SHOULD	

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15488	A default Maximum Sustained Traffic Rate of 0 SHOULD be used if a specific Maximum Sustained Traffic Rate is not required.	Yes	SHOULD	
MMREQ15489	A default Maximum Traffic Burst of 3044 bytes SHOULD be used if a specific Maximum Traffic Burst is not required.	Yes	SHOULD	
MMREQ15490	A default Minimum Reserved Traffic Rate of 0 SHOULD be used if a specific Minimum Reserved Traffic Rate is not required.	Yes	SHOULD	
MMREQ15491	A default Assumed Minimum Reserved Traffic Rate Packet Size of 0 SHOULD be used if a specific Assumed Minimum Reserved Traffic Rate Packet size is not required.	Yes	SHOULD	
MMREQ15492	A default Traffic Priority of 0 SHOULD be used if a specific Traffic Priority value is not required.	Yes	SHOULD	
MMREQ15493	A default Maximum Sustained Traffic Rate of 0 SHOULD be used if a specific Maximum Sustained Traffic Rate is not required.	Yes	SHOULD	
MMREQ15494	A default Maximum Traffic Burst of 3044 bytes SHOULD be used if a specific Maximum Traffic Burst is not required.	Yes	SHOULD	
MMREQ15495	A default Minimum Reserved Traffic Rate of 0 SHOULD be used if a specific Minimum Reserved Traffic Rate is not required.	Yes	SHOULD	
MMREQ15496	A default Assumed Minimum Reserved Traffic Rate Packet Size of 0 SHOULD be used if a specific Assumed Minimum Reserved Traffic Rate Packet size is not required.	Yes	SHOULD	

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15497	A default Nominal Polling Interval of 0 SHOULD be used if a specific Nominal Polling Interval is not required.	Yes	SHOULD	
MMREQ15498	A default Maximum Sustained Traffic Rate of 0 SHOULD be used if a specific Maximum Sustained Traffic Rate is not required.	Yes	SHOULD	
MMREQ15499	A default Maximum Traffic Burst of 3044 bytes SHOULD be used if a specific Maximum Traffic Burst is not required.	Yes	SHOULD	
MMREQ15500	A default Minimum Reserved Traffic Rate of 0 SHOULD be used if a specific Minimum Reserved Traffic Rate is not required.	Yes	SHOULD	
MMREQ15501	A default Assumed Minimum Reserved Traffic Rate Packet Size of 0 SHOULD be used if a specific Assumed Minimum Reserved Traffic Rate Packet size is not required.	Yes	SHOULD	
MMREQ15502	A default Tolerated Polling Jitter of 0 SHOULD be used if a specific Tolerated Polling Jitter is not required.	Yes	SHOULD	
MMREQ15503	A default Traffic Priority of 0 SHOULD be used if a specific Traffic Priority value is not required.	Yes	SHOULD	
MMREQ15504	A default Maximum Sustained Traffic Rate of 0 SHOULD be used if a specific Maximum Sustained Traffic Rate is not required.	Yes	SHOULD	
MMREQ15505	A default Maximum Traffic Burst of 3044 bytes SHOULD be used if a specific Maximum Traffic Burst is not required.	Yes	SHOULD	
MMREQ15506	A default Minimum Reserved Traffic Rate of 0 SHOULD be used if a specific Minimum Reserved Traffic Rate is not required.	Yes	SHOULD	

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compli-ance	Cate-gory	Comment
MMREQ15507	A default Assumed Minimum Reserved Traffic Rate Packet Size of 0 SHOULD be used if a specific Assumed Minimum Reserved Traffic Rate Packet size is not required.	Yes	SHOULD	
MMREQ15508	A default Maximum Downstream Latency of 0 SHOULD be used if a specific Maximum Downstream Latency is not required.	Yes	SHOULD	
MMREQ15509	When the PDP is going to shutdown, it SHOULD send a COPS Client-Close message to the PEP.	No	SHOULD	
MMREQ15510	In the COPS Client-Close message, the PDP SHOULD NOT send the PDP redirect address object PDPRedirAddr.	No	SHOULD	
MMREQ15514	This field MAY be unspecified in which case the DSCP/TOS field in the packet is not over-written by the CMTS.	Yes	MAY	
MMREQ15515	This field MAY be used in both the upstream and downstream directions.	Yes	MAY	
MMREQ15516	A Classifier MAY have wild-carded fields (indicated by zeroed fields), but care must be taken so that multiple IP flows do not unintentionally match the same Classifier, which can lead to unexpected results.	Yes	MAY	
MMREQ15517	The Policy Server and Application Manager MAY specify a second set to represent the reserved envelope, and a third set to represent the committed envelope.	Yes	MAY	Optional - not used
MMREQ15519	Alternatively, the PS/AM MAY issue separate Gate-Set messages to tell the CMTS to authorize and reserve and then to commit via a subsequent Gate-Set message.	Yes	MAY	

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15520	If the approximations do not give the Policy Server or Application Manager the control it desires, the PS/AM MAY use the other methods of defining the Traffic Profile, which includes the ability to define some DOCSIS-specific parameters.	Yes	MAY	
MMREQ15534	Application Managers that provide novel services MAY use the Configurable field to specify new session classes.	Yes	MAY	
MMREQ15537	The Application Manager or Policy Server MAY also query for this object as part of a failure recovery or other mechanism.	Yes	MAY	
MMREQ15538	The Opaque Data object contains information that a Policy Server or Application Manager MAY store on a CMTS that remains opaque to the CMTS.	Yes	MAY	
MMREQ15542	At this point, the PDP MAY periodically attempt to re-establish the connection.	Yes	MAY	
MMREQ15543	Messages that MAY be initiated by the Application Manager and Policy Server include Gate-Set, Gate-Info and Gate-Delete.	Yes	MAY	
MMREQ15546	The Gate-Set message MAY be sent by the PDP to the PEP to initialize or modify the operational parameters of a Gates.	Yes	MAY	
MMREQ15551	To modify the Traffic Profile associated with an existing Gate, an Application Manager MAY send a Gate-Set message with the GateID of the Gate to be modified and the new Traffic Profile.	Yes	MAY	

Table 12: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15552	To modify the Usage Limits associated with an existing Gate, an Application Manager MAY send a Gate-Set message with the GateID of the Gate to be modified.	Yes	MAY	
MMREQ15557	For applications that require a high-degree of time accuracy, the AM MAY query the CMTS for its Gate Time Info object after it moves a Gate into or out of a committed state.	Yes	MAY	Optional - not used
MMREQ15562	An Application Manager MAY provide an optional Event Generation Info object in a Gate-Set message.	Yes	MAY	Optional - not used
MMREQ15564	The Application Manager MAY specify a primary RKS IP address in the optional Event Generation Info object or the Application Manager MAY allow the Policy Server to use its default primary and secondary RKS IP Addresses.	Yes	MAY	Optional - not used
MMREQ15565	If the AM specifies a primary RKS IP Address, it MAY also specify a secondary RKS IP Address.	Yes	MAY	Optional - not used
MMREQ15566	In some situations, where the Application Manager and the Policy Server is acutely aware of DOCSIS, it MAY specify the Traffic Profile for the Gate using the DOCSIS Service Class Name or the DOCSIS-specific parameterization format.	Yes	MAY	
MMREQ15576	All envelopes used in a Traffic Profile MUST be the same type, i.e. either FlowSpec, DOCSIS Service Class Names, or DOCSIS-Specific Parameters.	Yes	MUST	

126.9 Glossary

Term	Definition
AM	Application Manager - logical network element defined in the PacketCable Multimedia architecture responsible for making bandwidth requests on behalf of a cable agnostic client.
Best effort	The default service flow. The characteristics for this service flow are defined in the cable modem config file. If a packet does not match any classifier then it is assigned to the best effort service flow.
CableLabs	A standards body that writes interface specifications and defines functional behavior for cable network elements.
Classifier	The set of parameters by which a media packet is judged to determine which service flow the packet belongs on.
Client	A SIP client
CM	Cable Modem - a cable network device that provides access to the cable network from an ethernet IP network.
CM	Call Manager - an MCS architecture component responsible for managing call-halves.
CMTS	Cable Modem Termination System - gateway between the cable HF/C network and the ethernet IP network. The CMTS receives the PCMM messages and communicates with the cable modem via DOCSIS to set up managed service flows.
COPS	Common Open Policy Service - a protocol defined in RFC 2748 that sets up a master/slave relationship between network elements for policy decisions. The PCMM protocol is an extension of COPS.
CS2M	CS2000 Management Tools - the CS2K GWC provisioning GUI
DOCSIS	Data Over Cable System Interface Specification - the protocol used between cable modems and their CMTS to set up service flows and classifiers.
DIFFSERV	Differentiated Services - an IP packet marking scheme that allows IP packets to be treated differently in the network
DSCP	DIFFSERV Code Point - the bit pattern used for DIFFSERV
GETS	Government Emergency Telephone Service - a telephony service that gives higher priority to some callers so that government services can function in the presence of extremely high call loads
HF/C	Hybrid-Fiber/Coax
IKE	Internet Key Exchange - used in PCMM to authenticate the PS from the AM
IPSec	IP Security - used in PCMM to secure the PCMM signaling between the AM and the PS (and between the PS and the CMTS)
KRS	Key Registration System
NAT	Network Address Translator - a device that translates between public network addresses and private network addresses.

Term	Definition
PacketCable	A subdivision of CableLabs that focuses on standards for VoIP over cable and multimedia over cable.
PC	Personal Computer (in this case)
PCMM	PacketCable Multimedia - an architecture and protocol for managing cable network bandwidth on behalf of cable agnostic clients.
PDP	Policy Decision Point - the COPS network element responsible for formulating network policy. The AM is a PDP. The PS is a PEP w.r.t. the AM and a PDP w.r.t. the CMTS.
PEP	Policy Enforcement Point - the COPS network element responsible for enforcing policies created by the PDP. The CMTS is a PEP. The PS is a PEP w.r.t. the AM and a PDP w.r.t. the CMTS.
Policy	A policy in the context of PCMM defines the access to and level of managed QoS available to a PCMM subscriber.
PS	Policy Server - network element defined in the PacketCable Multimedia architecture responsible for receiving PCMM signaling from and AM and forwarding it to the correct CMTS.
QoS	Quality of Service - the set of network characteristics that determine how a media packet is treated
SA	IPSec or IKE Secure Association
Service Flow	A managed QoS pipeline through the cable HF/C network defined by the quality of service given to the packets that transit the service flow.
SIP	Session Initiation Protocol - a VoIP signaling protocol
Socket	The IP address and port number used to communicate over an IP network to a particular service.
SS-L	Session Server Lines - a name for the MCS application server when used with CS2000
TOS	Type Of Service - a set of bits in the IP header that can be used to mark IP packets for different treatment in the network. Some of the TOS bits are used for DSCP.

127: Functional description (FN): A00011746

127.1 Feature name and Feature ID

A00011746: Addition of LGRP_TYPE field to GW profiles (Corrective)

127.2 Purpose

In SN08 the ability to define a GWs profile by creating an XML document (referred to as a certificate) was introduced. The SN08 certificate included all of the flexible fields that were available in SN08 for the most part. However, the ability of the core to define profiles was also made available in SN08. This core field was not included in a 1 to 1 relationship with the certificate, but rather was coupled with certificate field Endpoint_Type. Because of the difficulties of updating profiles when this core field is updated, a new field is introduced for SN09 into the CMT certificates that will define the Lgrp Type value that is sent to the core. Therefore, a direct relationship between core Lgrp types and a specific profile is made available by this enhancement.

127.3 Customer Facing Document Changes

A gateway certificate/profile captures a set of characteristics of a particular type of gateway. This set of characteristics can help us associate a gateway with the right type of gateway controller, manage the load balance of the gateway controller, and eventually achieve CallP purpose using the gateway.

This activity introduces a new optional field that is included in the profiles certificate. The LGRPType field is introduced and is used to drive “core” datafill for table LGRPINV. As suggested from the core table datafilled, LGRPINV, this field is only applicable for line gateways and is therefore optional in the XML document certificate. Even though this is an optional certificate field, this field is mandatory for all profiles that generate LGPRs.

In general, this field affects “core” behaviors applied to LGRPs. For a detailed discussion concerning core behavior driven by this field, refer to core NTP documentation.

127.3.1 SCHEMA UPDATES

Certificate.xsd

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                version="1.0"
                xml:lang="en" >
```

```
<xsd:include schemaLocation="../../xsd/certificateif/certificateTypes.xsd" />

<xsd:element name="certificate">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="MaxEndpoints"            type="maxEndpointsType"/>
      <xsd:element name="Category"                type="categoryType"/>
      <xsd:element name="EndpointType"            type="endpointTypeType"/>
      <xsd:element name="LgrpType"                type="lgrpType"
minOccurs="0"/>
      <xsd:element name="GenerateLGRP"            type="stringBoolean"/>
      <xsd:element name="MultiSiteNamesAllowed"   type="stringBoolean"
minOccurs="0"/>
      <xsd:element name="ResvTermMandatory"       type="stringBoolean"/>
      <xsd:element name="ChangeIPAvailable"       type="stringBoolean"/>
      <xsd:element name="DispPhyLocation"         type="stringBoolean"/>
      <xsd:element name="FQDNSupported"           type="fqdnSupportedType"
minOccurs="0" maxOccurs="1"/>
      <xsd:element name="InventoryType"           type="inventoryTypeType"/>
      <xsd:element name="InventoryRole"           type="inventoryRoleType"/>
      <xsd:element name="SupportedProtocol"       type="supportedProtocolType"/>
      <xsd:element name="GWCProfileNumber"        type="profileNumberType"/>
      <xsd:element name="EPIDGenDesc"             type="EPIDGenDescType"/>
      <xsd:element name="ServiceTypeList"         type="serviceTypeListType"
minOccurs="1" maxOccurs="7"/>
      <xsd:element name="CompatibleGWProfileList" type="profileNameType"
minOccurs="1" maxOccurs="5"/>
      <xsd:element name="BearerFabricList"        type="bearerFabricListType"
minOccurs="0" maxOccurs="5"/>
      <xsd:element name="GwAppData"               type="gwAppDataType"
minOccurs="0" maxOccurs="20"/>
      <xsd:element name="GatewayNameFormatList"   type="nameFormatsType"/>
      <xsd:element name="EndpointNameFormatList"  type="nameFormatsType"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

</xsd:schema>
```

CertificateTypes.xsd

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                 version="1.0"
                 xml:lang="en" >

<xsd:include schemaLocation="../../xsd/namesif/nameFormatsType.xsd" />

<xsd:simpleType name="profileNumberType">
```

```
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="1" />
    <xsd:maxInclusive value="599" />
  </xsd:restriction>
</xsd:simpleType>

.
.
.

<xsd:simpleType name="bearerFabricListType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="AAL1"/>
    <xsd:enumeration value="AAL2"/>
    <xsd:enumeration value="IP"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="lgrpType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="C"/>
    <xsd:enumeration value="S"/>
    <xsd:enumeration value="M"/>
    <xsd:enumeration value="SSDPL"/>
    <xsd:enumeration value="LL_3RDPTY"/>
    <xsd:enumeration value="CALIX_C7"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="fqdnSupportedType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="true"/>
    <xsd:enumeration value="false"/>
    <xsd:enumeration value="trueWithDefaultDomain"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:complexType name="gwAppDataType">
  <xsd:attribute name="name"    type="xsd:token"  use="required" />
  <xsd:attribute name="values"  type="xsd:string" use="optional" />
  <xsd:attribute name="pattern" type="xsd:string" use="optional" />
</xsd:complexType>
```

127.4 Related Documentation

N/A

128: Functional Description (FN) A00011827

128.1 Feature name and Feature ID

A00011827 - GWC Autonomous SWACT

128.2 Description

The objective of this feature is to provide an optional capability for Gateway Controllers (GWCs) to autonomously switch activity (SWACT) when communication has been lost with all associated media gateways. This functionality adds an additional layer of redundancy to the network in an attempt to reduce Call Processing outages during partial network failures.

128.2.1 Overview

The autonomous SWACT is an additional option provided to the customer for utilizing redundant network components. The autonomous SWACT functionality is on a GWC node basis and is only supported on GWCs supporting trunk and/or large line gateways. This option is provided as an attempt to automatically recover lost communication between the GWC and its associated media gateways. An autonomous SWACT of the GWC is by no means guaranteed to recover communication between the network components; however, it provides an additional mechanism for the customer to reduce outages and minimize the need for manual intervention.

An autonomous SWACT of a GWC is only performed after the provisioned timer expires, given that the timer is started after all associated media gateways, for that GWC, have been taken out of service by the GWC, and the messaging queues that notify the Core of the state transitions have been processed. The time period to wait before performing a SWACT is a provisionable value on a per GWC basis through the CMT GUI. The delay period helps to ensure the GWCs will not autonomously SWACT during brief network interruptions.

Prior to an autonomous SWACT, the GWC will verify that the inactive unit is in-service and capable of accepting activity. The GWC cannot guarantee connectivity to the gateways will be restored after the SWACT is performed. Depending on the location of the outage in the network, the SWACT may, or may not, restore connectivity.

After an autonomous SWACT, the newly active unit will not attempt another autonomous SWACT until communication has been restored to at least one gateway. Until communication can be verified between the GWC and at least one gateway, additional SWACTs will provide no appreciable benefit in recovering communication with the gateways.

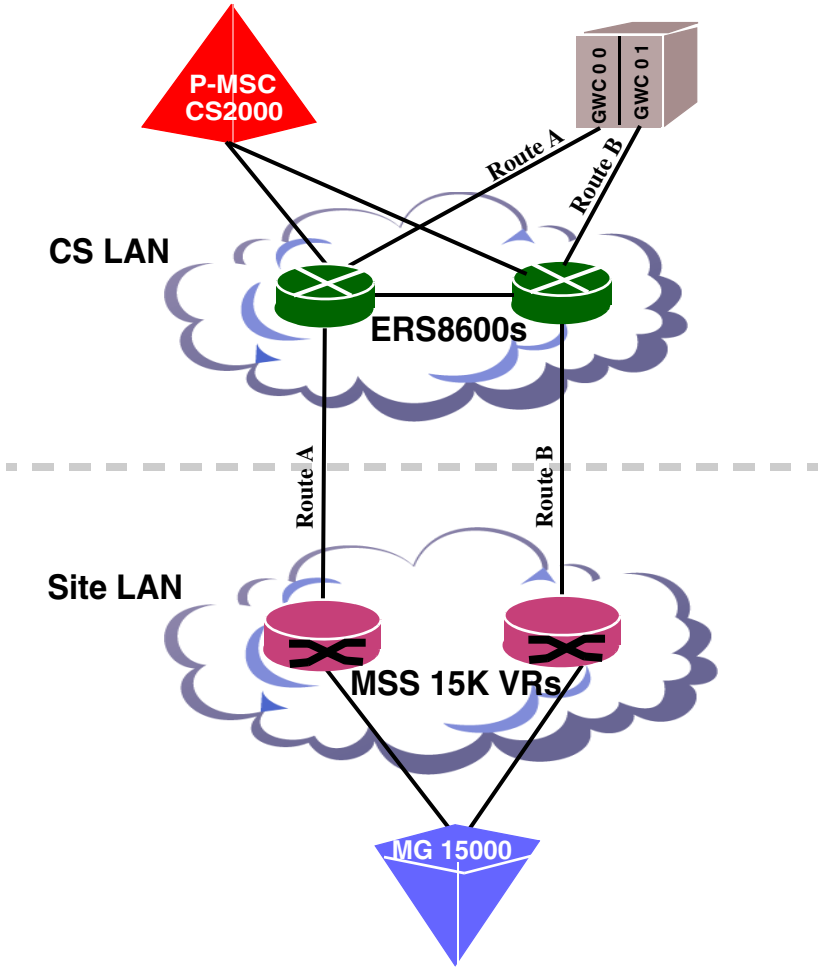
To assist the customer with identifying network failures, a critical alarm is raised in CMT when communication is lost with the GWC's associated gateways. A second critical alarm is raised when the autonomous SWACT has been initiated.

128.2.2 Network Topology

In certain network configurations, an autonomous SWACT may recover lost communication between the GWC and its associated media gateways.

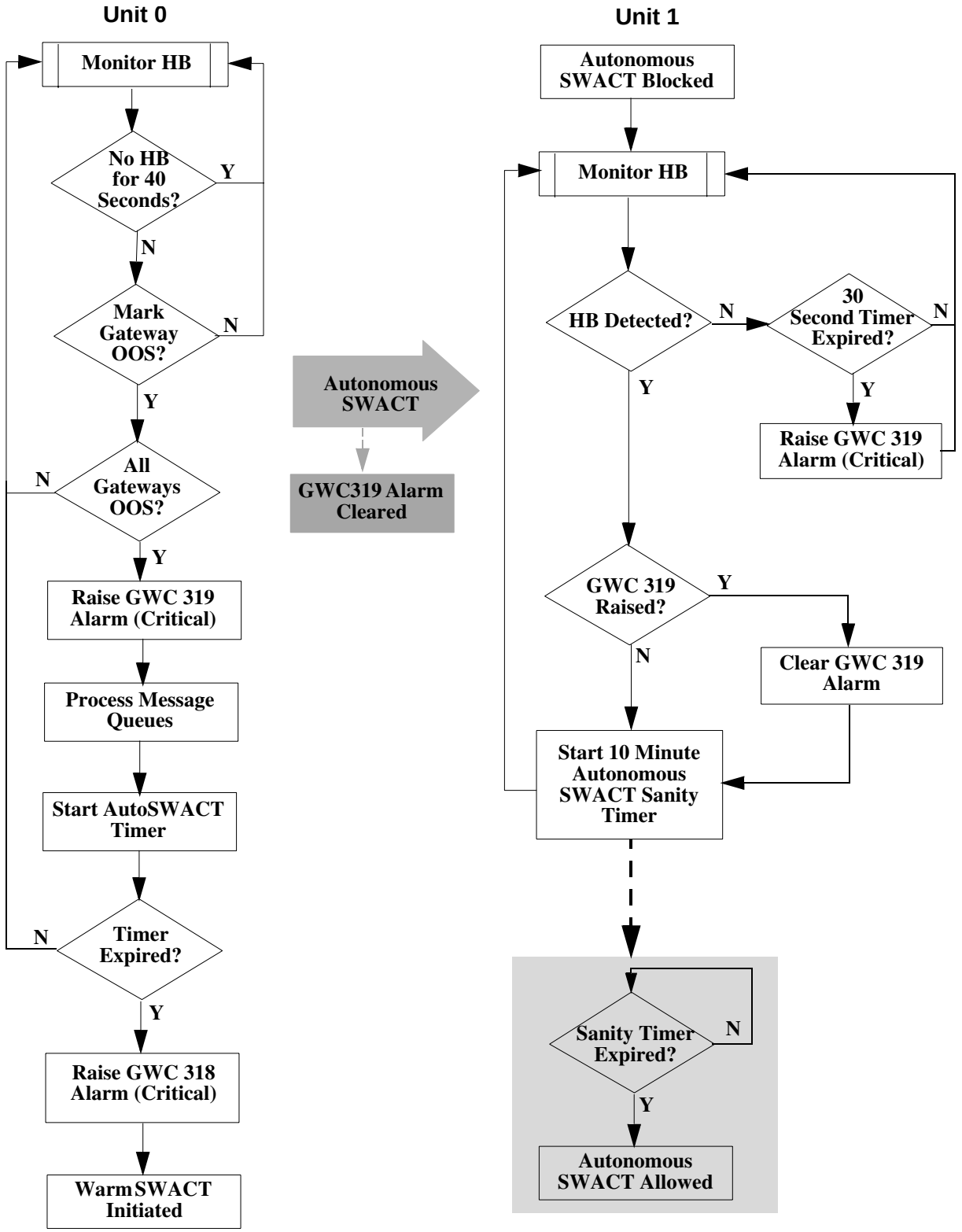
In the following network diagram, each GWC unit is associated with a different MSS 15000 Virtual Router (MSS 15000 VR). In the event the MSS 15000 VR associated with the active unit encounters a network fault, a SWACT to the mate GWC unit will utilize the redundant path restoring communication between the GWC and the media gateway.

Figure 1 Network Configuration

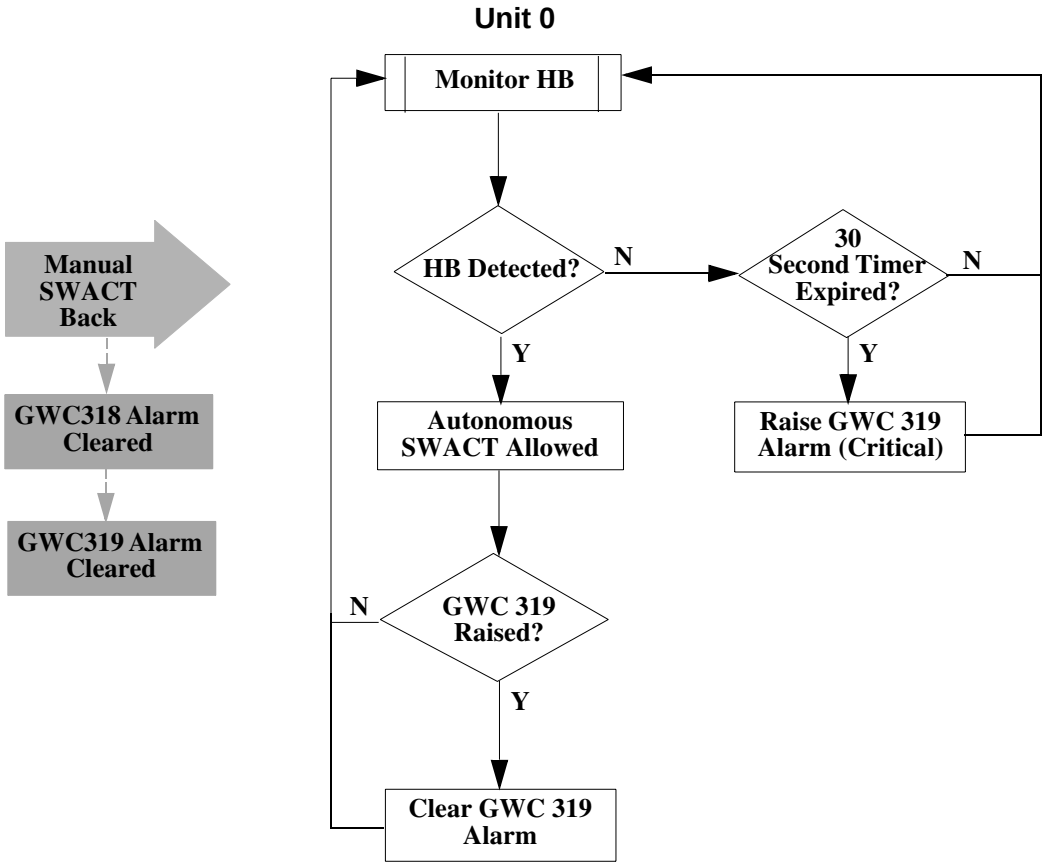


128.2.3 Flow Diagram

The following diagram details the flow of control for the GWC autonomous SWACT functionality. In the flow diagram that follows, HB refers to heartbeat.


Unit 0
Monitor HB
No HB for 40 Seconds?
Y
N
Mark Gateway OOS?
N
Y
All Gateways OOS?
N
Y
Raise GWC 319 Alarm (Critical)
Process Message Queues
Start AutoSWACT Timer
Timer Expired?
N
Y
Raise GWC 318 Alarm (Critical)
Warm SWACT Initiated
Autonomous SWACT
GWC319 Alarm Cleared
Unit 1
Autonomous SWACT Blocked
Monitor HB
HB Detected?
N
30 Second Timer Expired?
N
Y
Raise GWC 319 Alarm (Critical)
Y
GWC 319 Raised?
Y
N
Clear GWC 319 Alarm
Start 10 Minute Autonomous SWACT Sanity Timer
Sanity Timer Expired?
N
Y
Autonomous SWACT Allowed

The following diagram shows the logic flow following a manual Warm SWACT back to the original active unit following an autonomous SWACT.



128.3 Autonomous SWACT Controls

128.3.1 GWC Safeguards

Safeguards have been added in the GWC to prevent

- an autonomous SWACT from occurring prior to an outage condition being cleared, and,
- to prevent an autonomous SWACT from being performed too soon after the system has recovered.

After the autonomous SWACT has completed, the newly active unit prevents a second autonomous SWACT from occurring until the previous condition has been cleared.

Once the condition is cleared, a ten (10) minute sanity timer is started. During this ten minute period autonomous SWACT requests are queued. When the sanity timer expires, the request is processed as normal.

Should the condition clear, either while the request is queued, or while the time delay is being processed, the request will be canceled and no SWACT will occur.

128.3.2 Manual SWACT Interactions

At no time are manual SWACT requests from the GWC element manager blocked due to the autonomous SWACT functionality. Manual SWACTs are processed regardless of the state of the autonomous SWACT functionality. Any pending autonomous SWACT requests are canceled when a manual SWACT is processed.

128.4 Call Management

The autonomous SWACT application performs a Warm SWACT to switch activity to the mate unit. The Warm SWACT permits stable calls to remain active over the SWACT for certain gateway and call types. The handling of calls over the SWACT is described in the following sections.

128.4.1 H.248 Trunk Gateways

128.4.1.1 ISUP and PRI Trunk Calls

Calls on ISUP and PRI trunks remain active on the Call Server when heartbeat is lost with the gateway. When the gateway is determined to be unresponsive, the gateway is taken out-of-service and trunks with stable calls are transitioned from the Call Processing Busy (CPB) state to the Call Processing Deload (CPD) state. Once communication is restored, trunks in the CPD state are transitioned back to the CPB state.

128.4.1.2 PTS Trunk Calls

PTS trunk calls do not survive when the gateway is taken out-of-service. When the gateway is determined to be unresponsive, and subsequently taken out-of-service, all calls are immediately released.

128.4.2 TGCP Trunk Gateways

TGCP trunk calls do not survive when the gateway is taken out-of-service. All calls on TGCP gateways are immediately released when the gateway is determined to be unresponsive and taken out-of-service.

128.4.3 Line Gateways

128.4.3.1 Large Line Gateways

Large line gateways may provide Emergency Standalone (ESA) capabilities. For such gateways, intra-switched calls survive when the gateway is taken out-of-service; however, all other calls are released when the gateway is taken out-of-service.

128.4.3.2 Small Line Gateways

The autonomous SWACT functionality is not supported for GWCs supporting small line gateways.

128.5 Provisioning

The autonomous SWACT functionality is provisionable on a per GWC node basis. When a GWC is added the functionality is disabled, which is the default state. The CMT GUI is used to enable, or disable, the functionality. The GUI also provides the ability to set the timer value. The timer value identifies the time to wait before performing the autonomous SWACT after the loss of communication has been identified.

Please refer to the Configuration section of this document for provisioning details.

128.6 Logs and Alarms

New CMT alarms and logs are generated to indicate actions taken by the autonomous SWACT activity. This section provides a brief description of the alarms and logs. Please refer to the Fault Management section of this document for complete details.

128.6.1 Alarms

Two new critical CMT alarms are created to supplement existing major alarms which are raised when communication is lost to a gateway. The new alarms identify these conditions:

- Communication with the GWC's associated gateways is down
- Autonomous SWACT initiated

The first alarm is raised if communication to the GWC's associated gateways is lost. This alarm is cleared when communication is detected with at least one associated gateway. It is also cleared when the GWC is manually or automatically SWACT and is raised again on the newly active unit if communication is still lost with all the associated gateways.

The second alarm is raised when an autonomous SWACT is initiated from the unit detecting the communication outage. This alarm indicates that the system has taken action to correct the problem. The alarm is cleared

- manually from the CMT interface, or
- when activity is switched back to the original unit.

Additional information on clearing this alarm manually may be found in the Configuration (CN) section of this document.

These alarms are raised in addition to the existing major alarms raised against each gateway that loses communication with the GWC. Individual gateway

alarms are raised prior to the SWACT and cleared as communication is restored to the gateways.

128.6.2 Customer Logs

Customer logs are generated for the raising and clearing of alarms. Please refer to the Fault Management section for a list of the supported logs.

128.7 Hardware Requirements or Dependencies

The autonomous SWACT activity does not require special hardware. The autonomous SWACT functionality is supported on the MCPN750, MCPN905, and ATCA platforms.

128.8 Software Requirements or Dependencies

The autonomous SWACT functionality is available for packetized voice solutions that utilize IP solutions (IP over GigE and AAL5) and ATM solutions (Voice over AAL2) with these products:

- MSC Server 1000
- MSC Server 2000
- CS 2000 (North American and International software loads)
- CS 2000 - Compact (North American and International software loads)

128.9 Limitations and restrictions

1. The capability to enable GWC autonomous SWACT is available on CMT for all GWCs but the GWC autonomous SWACT action can only occur on GWCs hosting trunk and/or large line gateways. This action can not occur on GWCs hosting audio servers or small line gateways.
2. The GWC cannot verify the autonomous SWACT will restore lost communication to the associated gateways prior to attempting the SWACT.

128.10 Interactions

None.

128.11 Use Cases

128.11.1 Network Outage, GWC SWACT Recovers Gateways

1. The loss of communication with a gateway is detected.
2. The gateway is taken out-of-service.
3. It is confirmed that all associated media gateways have lost communication with this GWC.

4. The critical alarm (GWC 319) is raised indicating communication with all associated media gateways has been lost.
5. It is confirmed that all messaging queues have completed processing.
6. The SWACT is delayed for the duration of the timer value provisioned in the CMT.
7. A critical alarm (GWC 318) is sent to CMT indicating a autonomous SWACT is being initiated.
8. A Warm SWACT is performed, clearing the GWC 319 alarm.
9. The newly active unit monitors for communication with the associated media gateways.
10. Communication with at least one gateway is detected.
11. A ten (10) minute sanity timer is started to prevent further autonomous SWACTs until the timer expires.
12. After the sanity timer expires, autonomous SWACTs are again permitted.

Note: If communication with all associated media gateways is lost while the sanity timer is running, a SWACT event is queued an processed upon expiration of the sanity timer. Should communication be restored while the event is still queued, the event is cancelled and no SWACT is performed.

128.11.2 Network Outage, GWC SWACT Delayed Recovery

1. The loss of communication with a gateway is detected.
2. The gateway is taken out-of-service.
3. It is confirmed that all associated media gateways have lost communication with this GWC.
4. The critical alarm (GWC 319) is raised indicating communication with all associated media gateways has been lost.
5. It is confirmed that all messaging queues have completed processing.
6. The SWACT is delayed for the duration of the timer value provisioned in the CMT.
7. A critical alarm (GWC 318) is sent to CMT indicating a autonomous SWACT is being initiated.
8. A Warm SWACT is performed, clearing the GWC 319 alarm.

9. The newly active unit monitors for communication with the associated media gateways.
10. No communication is detected after thirty (30) seconds.
11. The critical alarm, GWC 319, is raised indicating communication with all associated media gateways has not been recovered.
12. The GWC continues to monitor for heartbeat from associated media gateways.
13. Communication with at least one media gateway is detected.
14. The GWC 319 alarm is cleared.
15. A ten (10) minute sanity timer is started to prevent further autonomous SWACTs until the timer expires.
16. After the sanity timer expires, autonomous SWACTs are again permitted.

Note: If communication with all associated media gateways is lost while the sanity timer is running, a SWACT event is queued an processed upon expiration of the sanity timer. Should communication be restored while the event is still queued, the event is cancelled and no SWACT is performed.

128.11.3 Manual Warm SWACT back to the original GWC unit when Communication has not been restored with an Autonomous SWACT

1. The loss of communication with a gateway is detected.
2. The gateway is taken out-of-service.
3. It is confirmed that all associated media gateways have lost communication with this GWC.
4. The critical alarm (GWC 319) is raised indicating communication with all associated media gateways has been lost.
5. It is confirmed that all messaging queues have completed processing.
6. The SWACT is delayed for the duration of the timer value provisioned in the CMT.
7. A critical alarm (GWC 318) is sent to CMT indicating a autonomous SWACT is being initiated.
8. A Warm SWACT is performed, clearing the GWC 319 alarm.

9. The newly active unit monitors for communication with the associated media gateways.
10. No communication is detected after thirty (30) seconds.
11. The critical alarm, GWC 319, is raised indicating communication with all associated media gateways has not been recovered.
12. A manual Warm SWACT is performed from the CMT
13. Both the GWC 318 and GWC 319 alarms are cleared
14. The newly active unit monitors for communication with the associated media gateways.
15. No communication is detected after thirty (30) seconds.
16. The critical alarm, GWC 319, is raised indicating communication with all associated media gateways has not been recovered.
17. The GWC continues to monitor for heartbeat from associated media gateways.
18. Communication with at least one media gateway is detected.
19. The GWC 319 alarm is cleared.

128.12 Glossary

Term	Description
ATCA	Advanced Telecom Computing Architecture
CS2000	Call Server 2000
CDMA	Code Division Multiple Access
CMT	CS2000 Management Tools
ERS8600	Ethernet Routing Switch 8600
ESA	Emergency Standalone
GWC	Gateway Controller
ISUP	ISDN User Part
MSC	Mobile Switching Center
P-MSC	Packet Mobile Switching Center
PRI	Primary Rate Interface
PTS	Per Trunk Signaling

Term	Description
SWACT	Switch of Activity
TGCP	Trunking Gateway Control Protocol
VR	Virtual Router

128: Functional Description (FN) A00012001

128.1 Feature name and Feature ID

A00012001 - IEMS Call Server 2000 SIP Integration

128.2 SN07/SN08 Background

In SN07&8, IEMS manages the Multimedia Communication Server Manager (MCS Manager). The MCS Manager when added can have as its managing type either an MCS/CSE MX NE or Media Proxy NE. When an MCS Manager is added to they IEMS, the MCS/CSE MX NE or Media Proxy NE is added as a map symbol under the Network Elements. The MCS System Manager is added as an element in the Element Managers map.

Along with the configuration of the MCS device was the ability to associate Fault Performance Managers, FPM's, to an MCS device which would be another input for faults and performance data for IEMS.

There were provisions for fault, performance, and configuration management of MCS and FPM devices.

The current existing MCS device functionality along with the RTP Media Proxy and FPM will continue to be supported in SN09.

To see more information concerning the addition of the MCS device in SN08, please see document SN08 A00007346 - Backward Compatibility Functional Specification at :http://livelink.us.nortel.com/livelink/livelink.exe?func=ll&objId=7485824&objAction=browse&sort=name

128.3 Main work Items

One of the first items is branding name changes for both the NGSS and MCS. The existing NGSS managed object to align with the Call Server 2000 Session Server. The Trunks version is relabelled to SSTrunks. The MCS SIP lines which is now deployed on a Linux platform will be relabelled SSLines.

The MCS configuration and management remains the same from SN08 to SN09. The Icon for the MCS on the Solaris platform for the NE will be modified to MC52 and the tree name will be changed from MCS/CSE to MCS5200. Also, a change is made in the configuration of the MCS Mgr as an EM with a type from Media *Proxy* to Media *Portal.*

Integrating the management of the fault and performance interfaces of the new SSLines platform, Langley hardware running Linux OS. The SSLines system will also have the ability to configure the Session Manager platforms

associated with the System Manager EM. There will also need to be configuration of the Provisioning Client servers. The configuration of the Session Managers will allow SSH launch to each Session Manager. The configuration of the Provisioning Client servers will allow the client to launch the MCS Provisioning Client.

Another work item consists of proxying all GUI/CLUI launches through the IEMS. The GUI/CLUI's that require proxying consist of:

1 MCS System Manager Console

2 Provisioning GUI

3 SSH to each platform associated with the SSLines deployment

The SSLines Element Manager and Network Element will provide and support all the existing functionality of the MCS/RTP Media Portal functionality pertaining to Fault Management, Performance collection, and device change management. There will however only be the option of being able to add the SSLines device as an SSLines Manager without the ability to configure the SSLines device as an RTP Media Portal. Also in SN09, the SSLines device will not be supporting FPM's.

To configure performance collection jobs, please refer to the SN08 document concerning MCS, http://livelink.us.nortel.com/livelink/livelink.exe?func=ll&objId=7485824&objAction=browse&sort=name

128.4 Existing functionality

As specified previously this activity is for rebranding and proxying the MCS GUI's through the IEMS. The functionality of handling faults and provisioning data remains unchanged.

The change, and deletion of an SSLines type device has remained the same except for the type being deleted or changed.

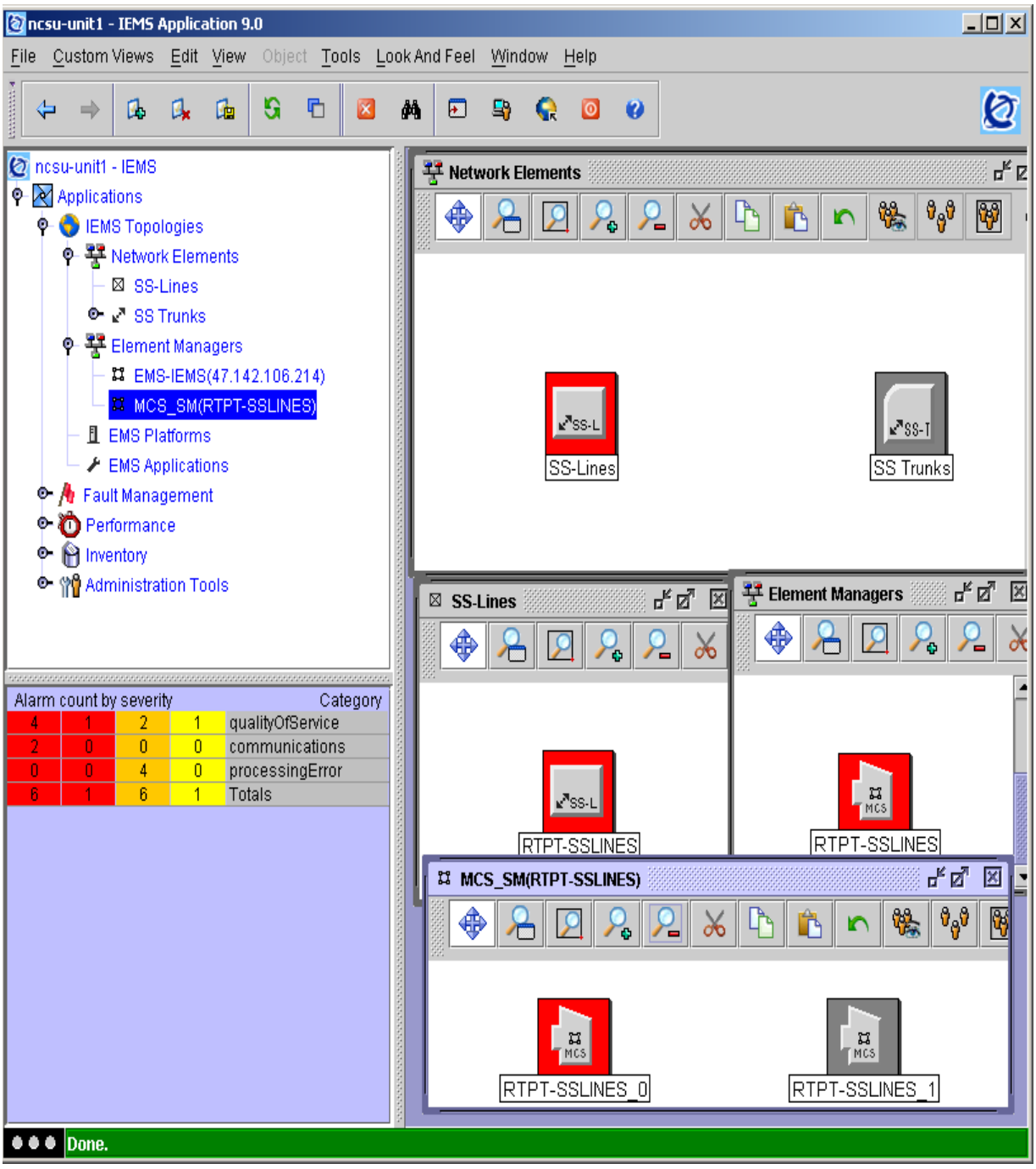
128.5 Changed Functionality

First and foremost is the branding change. When adding the SSLines device, an SSLines Mgr is added instead of an MCS Mgr or RTP Media Portal. The same information is entered concerning IP addresses, userid's, SNMP information, and performance data collection.

128.5.1 Topology

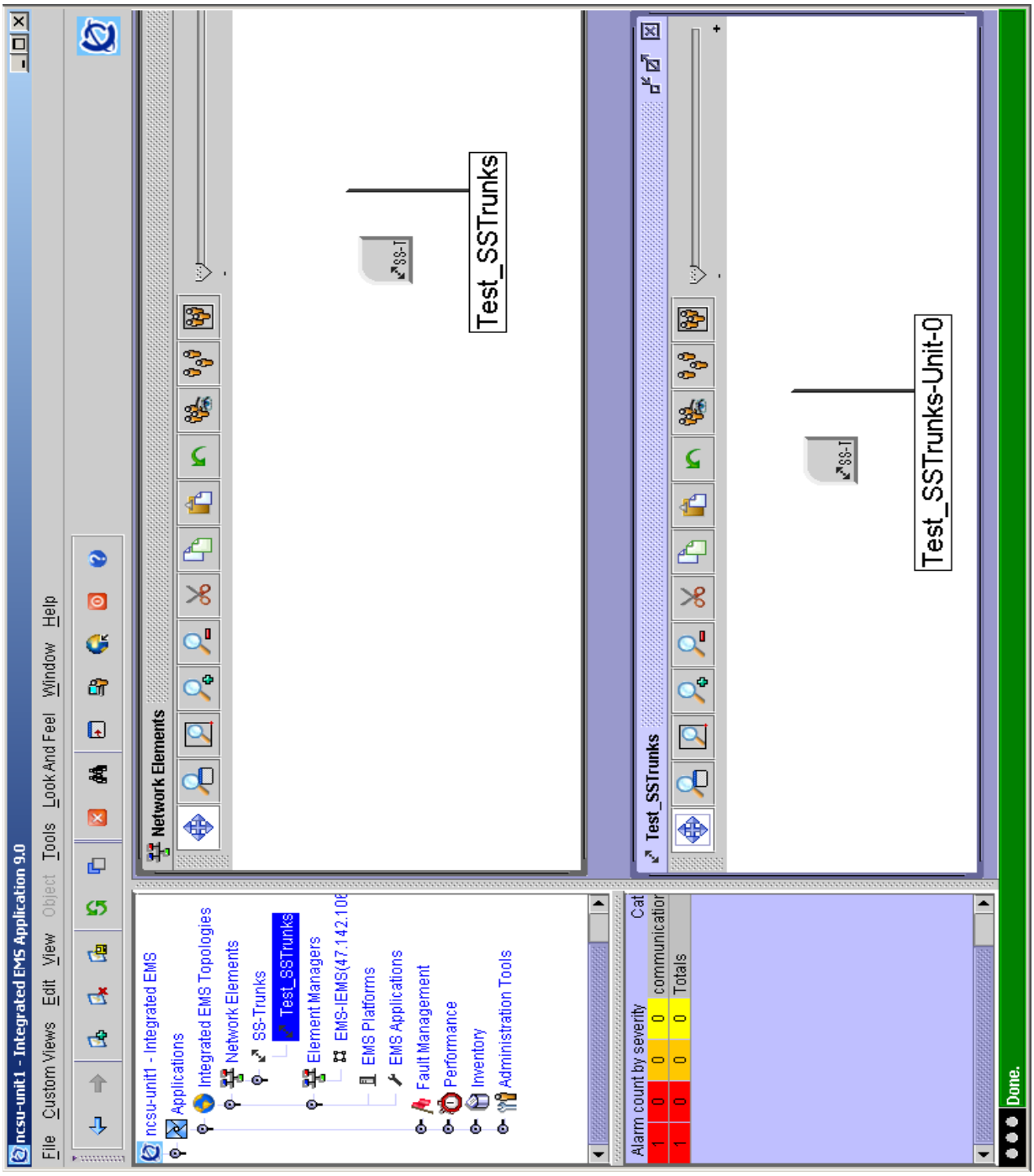
The topology of an SSLines as added into IEMS is displayed is in the same hierarchy as the existing SN08 MCS. The following screen shot shows the new branding and topology for the SN09 SSLines.

Figure 1 Topology of SSLines EM and NE



The SS Trunks topology will be similar to that of the Session Server and will be displayed as follows in SN09.

Figure 2 Topology of SS Trunks NE



128.5.2 Launch of applications

The launch of a command line has been modified in that it is now possible to launch a command line to any platform that is configured. When launch

command line is selected, a new frame will be displayed which will allow the user to select the platform to launch a command line to.

The launch of the command line for the System Manager and Session managers can be done from any of the maps in the GUI except from the Network Elements screen.

Figure 3 Launch of Command line From SSLines

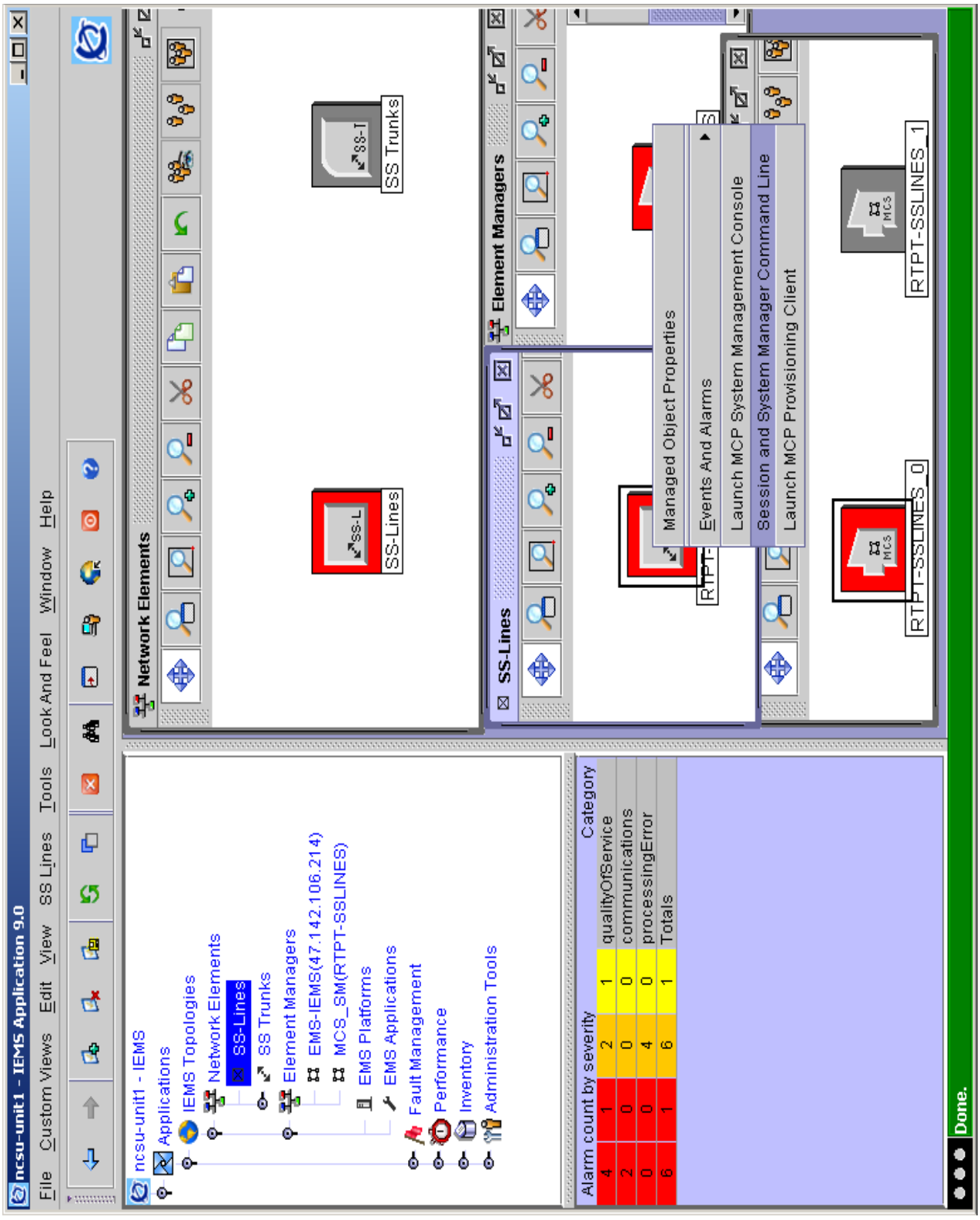
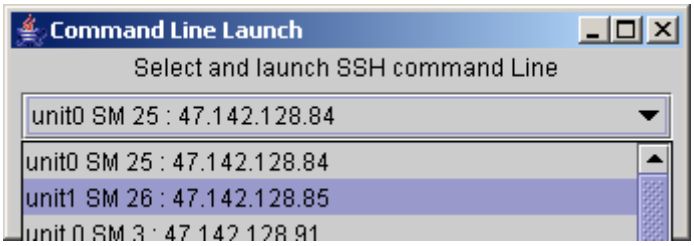


Figure 4 Launch of SSH command line to platform



The drop down box will allow the user to choose any of the platforms that SSH can be launched to. The SSH connections will be proxied via the IEMS server.There will be a new option aganst the EM to configure the platforms which will allow the user to configure these platforms.

128.6 New Functionality

128.6.1 GUI

For SN08, it was only possible to configure the platform(s) associated with the System Manager associated with an MCS or RTP Media Portal. In SN09, it is possible to configure all the platforms associated with an MCS/SSLines deployment including the IP addresses of

1 The Provisioning Clients (two IP addresses)

2 The Session Manager platform IP addresses (up to three pairs)

This configuration is done from the map reference of the SSLines EM.

From the EM or NE it is possible to launch the Provisioning client GUI.

Figure 5 Launch of Provisioning Client from EM Map

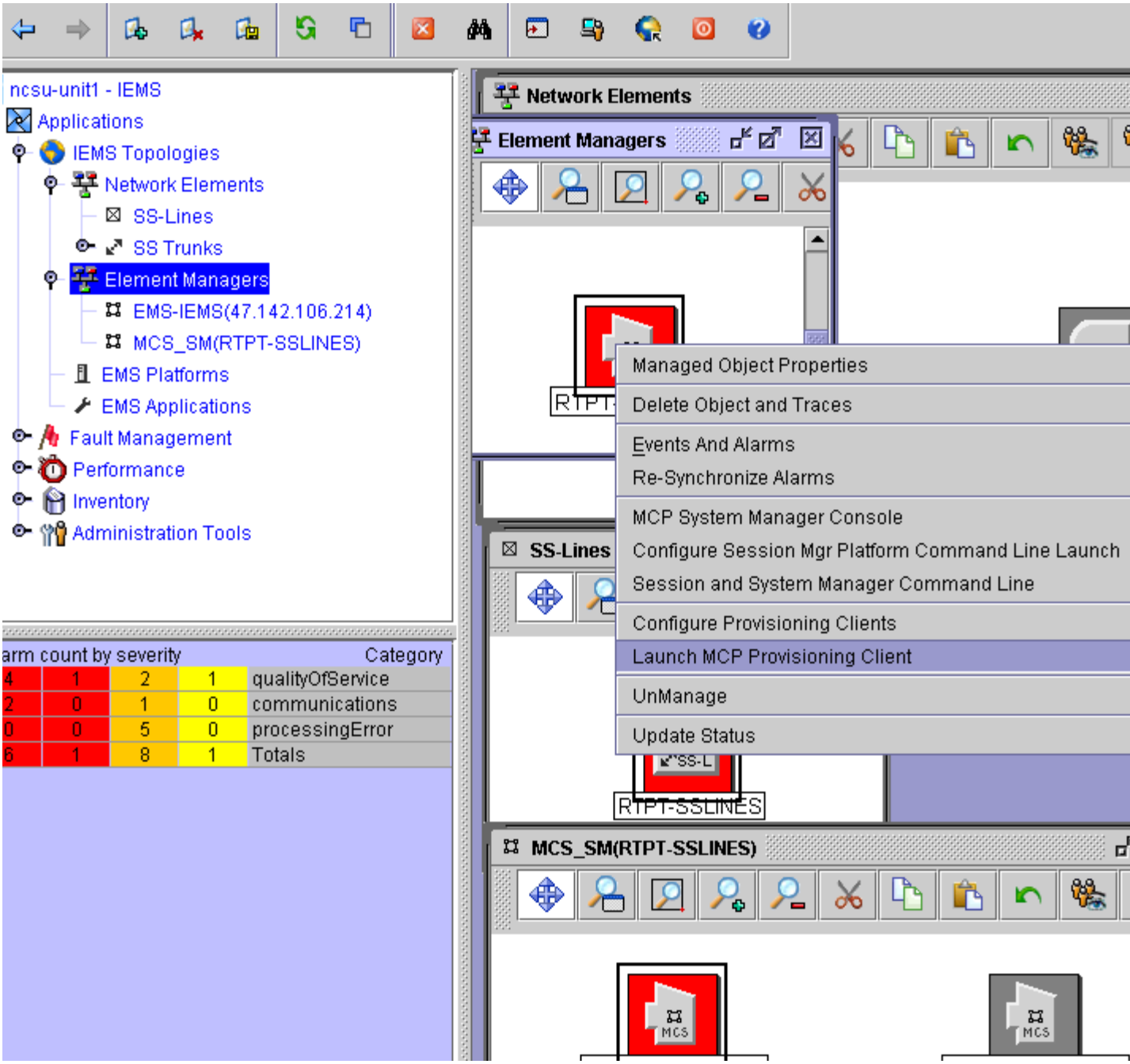


Figure 6 Launch from SSLines Element Manager Map

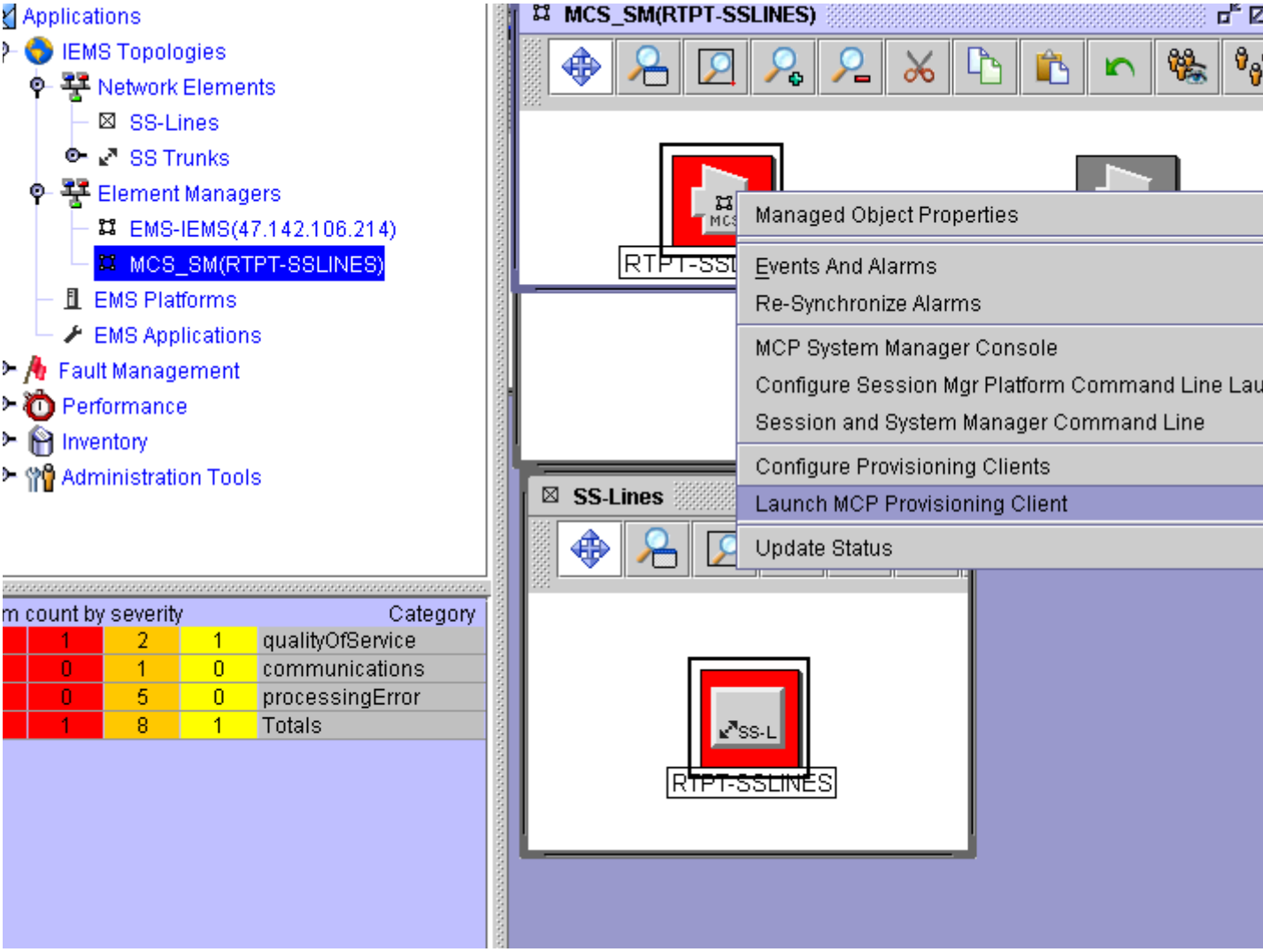
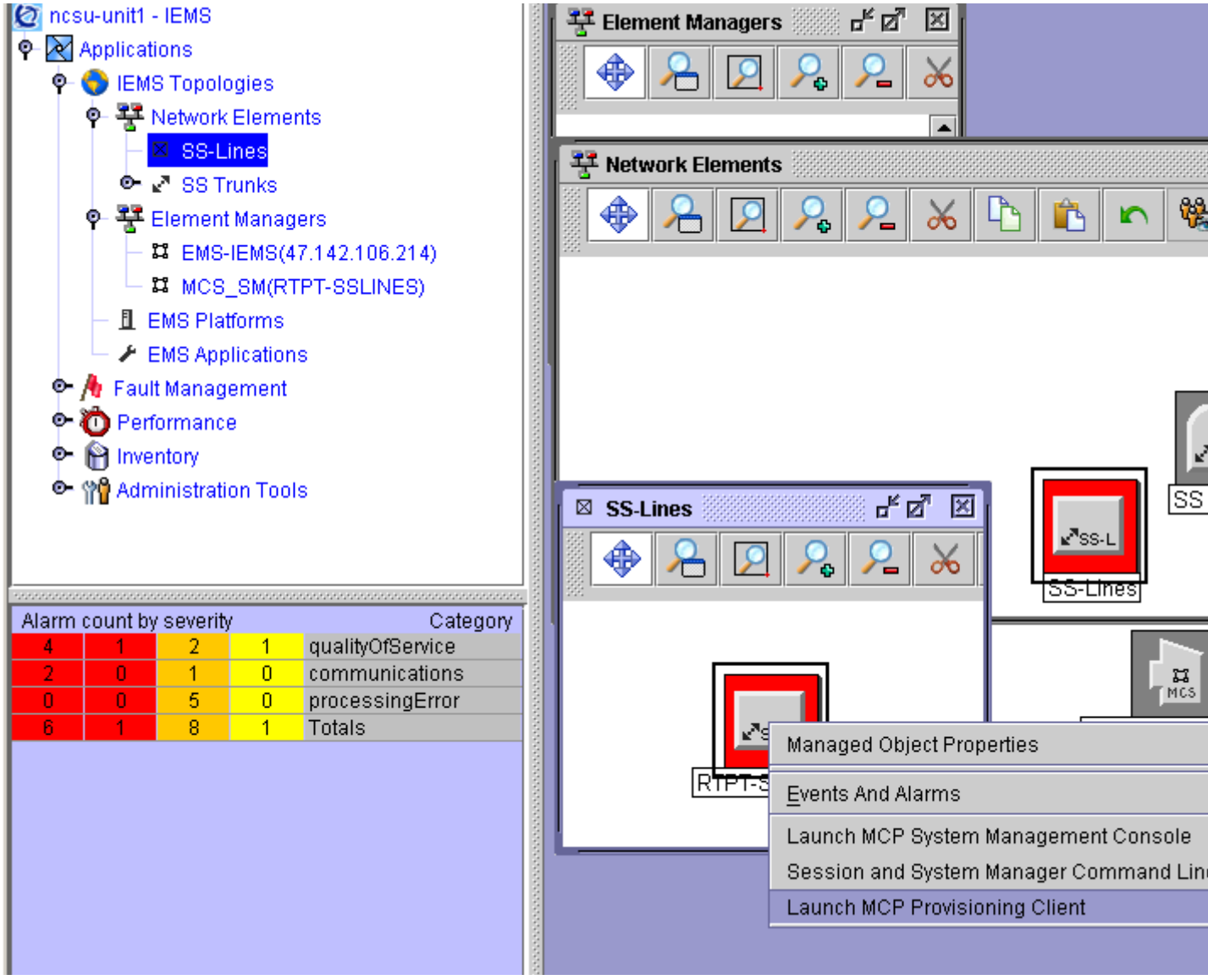
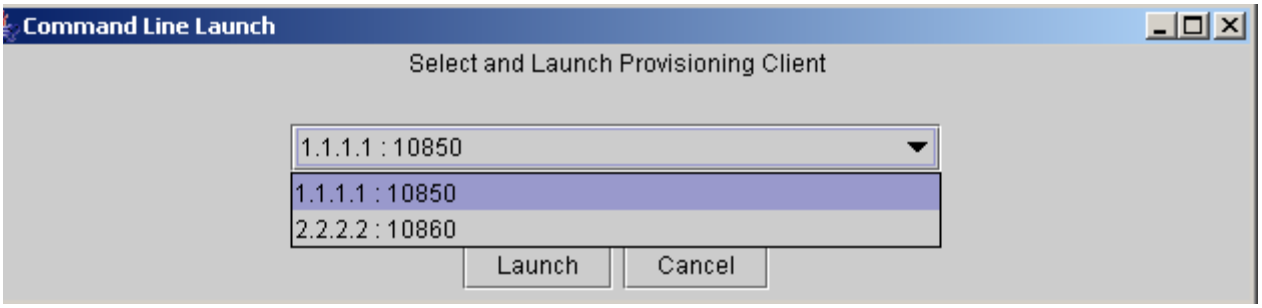


Figure 7 Launch of Provisioning Client from SSLines NE Map



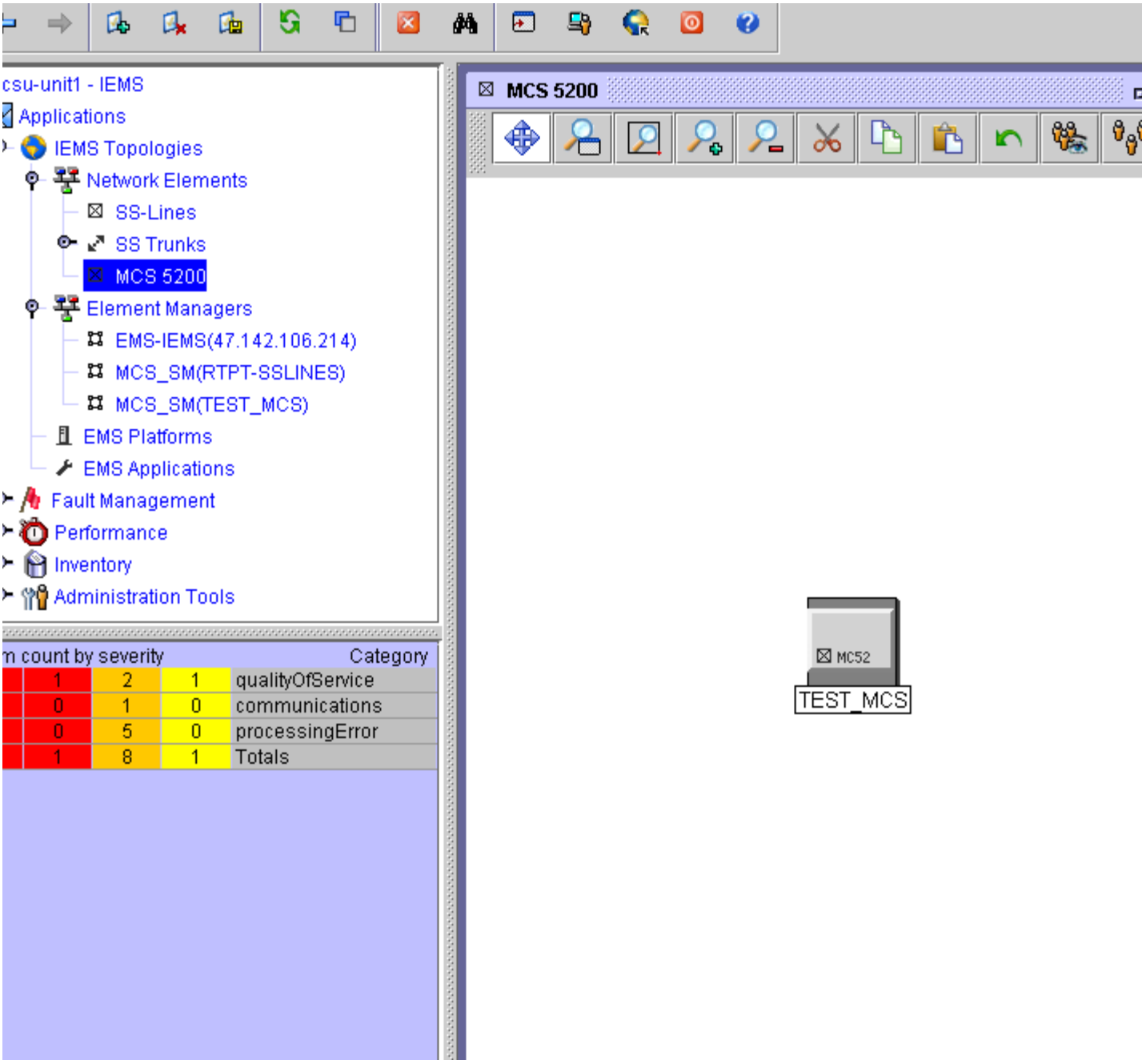
In all cases of lauching the Provisioning Client, there will be a combo dialog displayed which will have the user choose which platform to launch the Provisioning Client to as following.

Figure 8 Provisioning Client Launch



The Topology is changed somewhat for the MCS as an MCS/CSE device in the tree display to the following.

Figure 9 MCS MCS/CSE rebranded to MCS 5200



128.6.2 Proxy of MCS system manager and Provisioning client

As mentioned earlier, the MCS system manager console and provisioing cleint will be launched via the HTTP proxy. Both GUIs communicate with their servers via HTTPS. The apache proxy must be configured using the SSPFS CLI command. These details will be specified in the CN section.

No new ports will need to be opened on the firewall for this component.

128.7 Upgrade Considerations

128.7.1 Upgrade

For an upgrade the SSLines and SSTrunks configuration will be stored in the Oracle database as well as the faults and performance data and will be handled with the database upgrade.

128.7.2 Downgrade

For an upgrade the SSLines and SSTrunks configuration will be stored in the Oracle database as well as the faults and performance data and will be handled with the database downgrade.

128.8 Security

N/A

128.9 Hardware Requirements or Dependencies

This feature requires the SIP Lines componenets to reside on the Langley Linux platform.

128.10 Software Requirements or Dependencies

This will require an SN09 or later version of SSPFS.

128.11 Limitations and restrictions

Log streaming and bulk import and export will not be supported for the proxied system manager launch (see “128.6.2 Proxy of MCS system manager and Provisioning client”).

128.12 Interactions

N/A.

128.13 Glossary

Term	Description
IEMS	Integrated Element Management System

129: Functional Description (FN) A00012109

129.1 Feature name and Feature ID

A00012109 - Session Server Shared Library Replacement (SLR) Patching

129.2 Description

This activity enables Shared Library Replacement (SLR) patching for the SIP Trunking application on the NGSS.

The Unified Software Management (USM[1]) Patch manager application running on the Session Server will be used to download and apply/remove/query patches on the Session Server. USM is also responsible for pushing Inform Lists from the Session Server to an appropriately configured location.

Figure 1 provides a broad overview of the general patching process for Session Server.

Figure 2 provides a more detailed illustration of the steps involved in the Patch Creation process.

> ***Note:*** This feature is only responsible for the SLR patching functionality on the SessionServer. Other information provided here related to patch creation, downloading, and general patching, etc...on the Session Server is provided here for informational purposes only and is not a function of this specific feature.

[1]The USM functionary is part of the Siren program. USM provides a number of capability; however, the Session Server is only making use of the patch management functionality. Detailed information on USM patch management capabilities can be found in A00009264 - SIREN Installation and Patching.

Figure 1 Session Server Patching Process

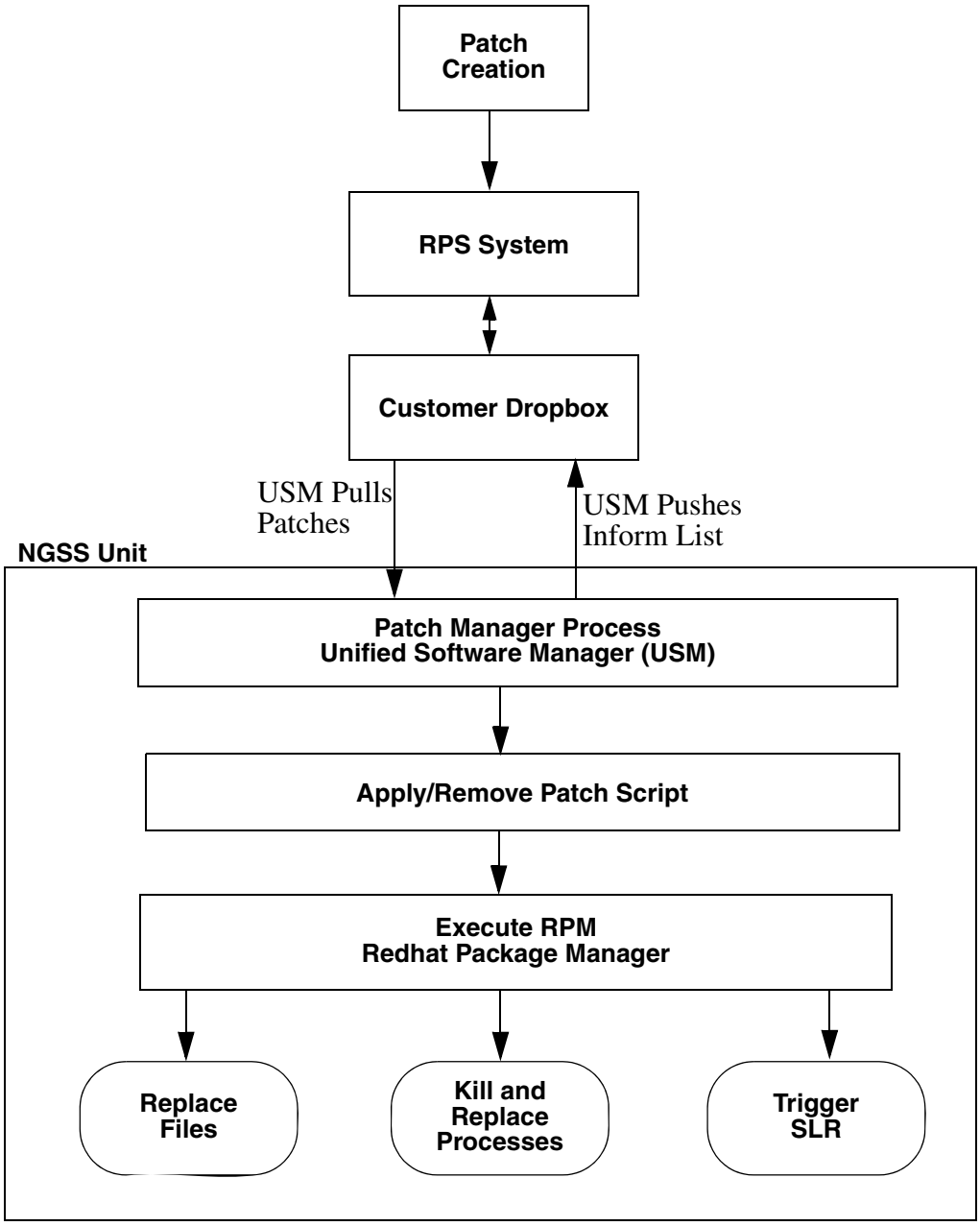
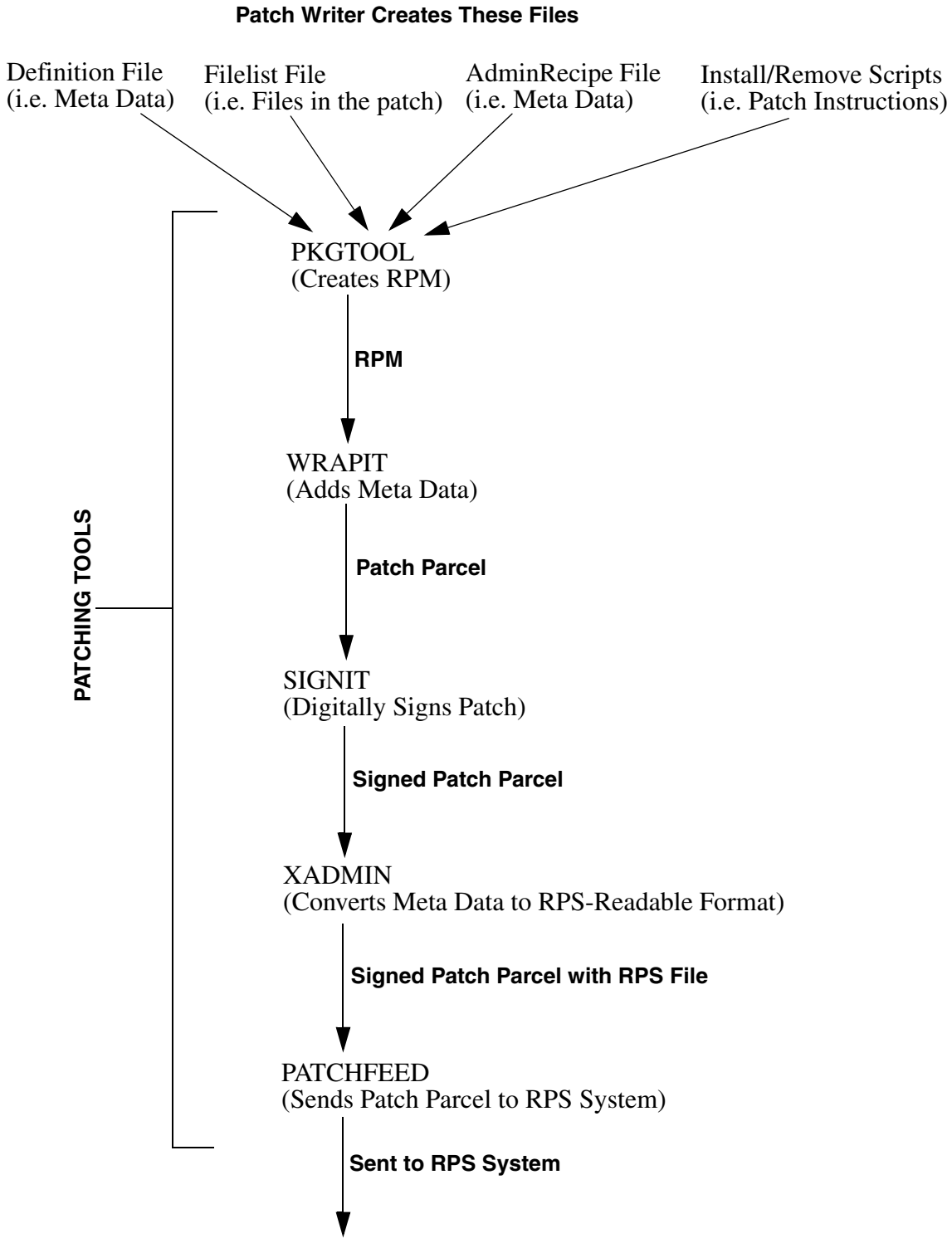


Figure 2 Session Server Patch Creation Process



During patch creation a few files are called by the patching too (***pkgtool***)l to perform the actual tasks required to apply the patch and to include necessary patch administration information as part of the patch. These files are discussed here briefly.

- Filelist.pkg

  The filelist file defines which elements should be included with your software package. For example, this is where the patch writer defines which files are to be replaced on the Session Server, and the directory path of those files in both the Clearcase view and within the Session Server.

- Definition.pkg

  The definition file defines information describing the package such as name, version, prerequisites, description. These items are defined via XML Tags. There are over 40 possible tags - although only those designated as pertinent to the particular application need to be filled in. The only tags currently being used out of the Definition.pkg at the time of this writing are the pkg_summary and pkg_description. Output from this file is used to populate fields in the RPM.

- AdminRecipeFile

  This file, similar to the definition.pkg file, consists of tags. These tags are used to populate the adminfile that results from a patch build. All of the documented tags can be used in this file and will result in adminfile entries. Again, only those deemed applicable need to be populated.

  The pkgtool builds RPM packages based on filelist.pkg and definition.pkg files. The wrapit tool metadata wraps the RPM packages produced by pkgtool. Wrapit will default the metadata fields unless there is an admindata recipe file that overrides the defaults.

- Install, Remove scripts

  Next come the install and remove scripts. These files define the action that will occur when the patch is applied or removed.

129.1 Hardware Requirements or Dependencies

Not applicable.

129.2 Software Requirements or Dependencies

Session Sever SLR patching is available in SN09 drop 2.

129.3 Limitations and restrictions

Please note the following:

- The SLR capability provided by this feature only addresses the Session Server Trunk (SST) application.
- This feature does not address SLR patching for NCGL

- This feature does not address SLR patching for SPC.
- Figure 1 on page 1270 lists the Session Server components that are SLR patchable (i.e., hitless).

Table 1 Session Server Software Component Patchability

Component	Patching Method	SLR/ Hitless	Comments
HTML files and scripts (e.g. database upgrade scripts)	Simple file replacement	Yes	None.
JSP files used in OAMP interface	File replacement, followed by stopping and restarting Tomcat servlet container	Yes	Web access for the OAMP interface is temporarily inaccessible during the patch application. Users will get an error when trying to access a web page during this window. Call processing is not affected.
Solid database	Kill and replace	Yes	In this case, the version of the Solid database is being changed on the Session Server. The previous version of the database is killed and the new version supplied in the patch is started. During this kill and replace window, web access to the provisioning pages is temporarily unavailable and users will receive an error message if they attempt to access those pages while the patch is being applied. Call processing is not affected since all provisioning data is cached in the application at startup and the database does not need to be accessed during call processing. Note the database watchdog process must be stopped before replacing the Solid database to prevent a swact.
Web Server	Kill and replace	Yes	In this case, the version of the onboard web server is being changed on the Session Server. Access to the OAMP interface through the web is temporarily unavailable during the patch. Call processing is not affected.
Miscellaneous auxiliary processes (e.g. database watchdog process, SCP NCAS server process, SCPLite process, app mtc)	Kill and replace	Yes	Any process that can be stopped, replaced, and restarted in a patch without affecting call processing or causing a swact falls in this category. Currently this category includes the process that monitors the health of the Solid database and the process used for Non-Call Associated Signalling (NCAS) between the DMS core and the Session Server.
SPC Application (Session Policy Controller)	Kill and replace on inactive unit, swact, and then kill and replace on newly inactive unit	No	Patching any part of the SPC application currently requires the entire executable to be replaced. This means that the executable must be stopped before it can be replaced and thus these patches cannot be done in a hitless manner.

Table 1 Session Server Software Component Patchability

Component	Patching Method	SLR/ Hitless	Comments
3rd Party RadVision software used in SIP application	Kill and replace on inactive unit, swact, and then kill and replace on newly inactive unit	No	If a new version of the RadVision stack must be patched in or if specific bug fixes are required in the Radvision code for the SIP application, the patch cannot be done in a hitless manner.
Adding new OM (Operational Measurements) registers or groups to the SIP application	Kill and replace on inactive unit, swact, and then kill and replace on newly inactive unit	No	Note that existing OM registers can be pegged in new places in the SIP application in a hitless patch, but new registers or groups cannot be added without requiring a swact. To lessen the impact of this restriction, this activity will add placeholders for new OM groups and new registers within existing OM groups so that these “spare” OM structures could be used in a hitless patch.
SIP application process (except for RadVision code and new OMs)	SIP shared library replacement (SLR)	Yes	The vast majority of patches fall in this category since it covers all call processing fixes for the SIP application, except for the RadVision code and new OMs. Global data structures within the SIP application cannot be changed with an Session Server SLR patch, but this activity will add placeholders for new data that could be used in a patch. If these placeholders are not sufficient for a particular patch, then a kill and replace with swact patch is required or the functionality could be delivered in an MR.

129.4 Interactions

None known at this time.

129.5 Operational Measurements

This activity adds spare OM registers and spare OM groups for use by the SIPGW application. Refer to the Performance section for details.

129.6 Glossary

Term	Description
NCGL	Nortel Carrier Grade Linux
RPM	Redhat Package Manager
SLR	Shared Library Replacement
SPC	Session Policy Control.
USM	Unified Software Management

130: Functional Description (FN) A00012183

130.1 Feature name and Feature ID

A00012183 - Public Key Manager

130.2 Description

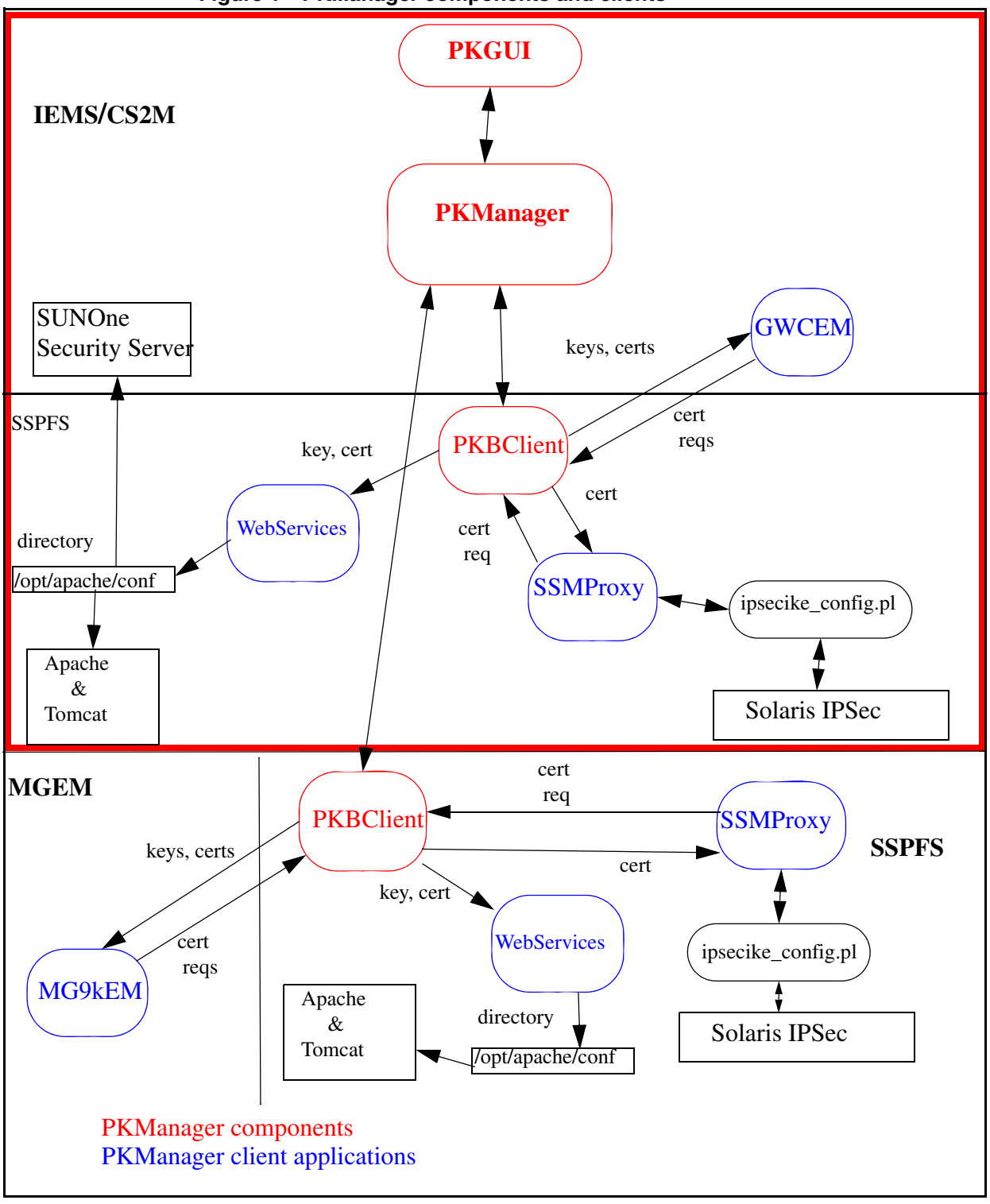
130.2.1 PKManager

The PKManager provides the user with the ability to automate the tracking and management of certificate replacement for the following supported devices:

- MG9KEM
- MG9K
- GWCEM
- GWC
- SSM
- WebServices

The following figure shows the PKManager relationships with its client components.

Figure 1 PKManager components and clients



Note: Certificates are always delivered directly to the active unit of an HA cluster and then mirrored using filesystem synchronization services.

The PKManager automates the management and replacement of device certificates for supported devices. In addition to this, a Web interface (PKGUI) is available to authorized users to perform a variety of manual actions. This GUI can be launched independently from a web browser or from within the IEMS client window. A new application managed object is added to IEMS to allow single sign-on launching and alarm integration for the PKManager with IEMS.

Note: This tool restricts access to users belonging to the authorization groups "***secadm***" and "***secro***". All operations in the GUI will check for group membership before allowing access to a given operation. The group "***secadm***" is used to permit all operations in this tool; while "***secro***" is used to permit viewing and browsing only. See CN doc for this feature for further operation mapping details.

The section following summarizes the operations available to the user through the PKGUI interface. **Further details on the PKGUI can be found in the configuration document for this feature**.

130.2.2 PKGUI User Operations

1 **Generate CSR for Export** - this request is used to initiate the process of importing certificates that are generated by a commercial or external certificate authority. This request will cause the PKBroker to generate a file that contains an openssl PKCS#10 certificate signing request.

2 **Import Certificate for Integrated Client** - this request is used to import a certificate generated by a commercial or external certificate authority. By doing so the certificate management and monitoring services of the PKManager for a device whose certificate management is integrated with that supported by the PKManager are obtained. The matching CSR must be present to successfully import the associated certificate.

3 **Import Certificate for Non-Integrated Client** - this request is used to obtain the expiration monitoring services of PKManager for a certificate that authenticates a device whose certificate management is not integrated with that supported by the PKManager.

4 **Create Non-Integrated Certificate for Export** - this request is used to have the PKBroker generate a file that contains a private key, a second file that contains a compatible X509 v3 certificate for a non-integrated device whose certificate management is not integrated with that supported by the PKManager. PKBCA signing and root certificate files are also provided

for export. The expiration monitoring services of PKManager are activated on the certificate.

5 **Create Integrated Certificate for Export** - this request is used to have the PKBroker generate a file that contains a private key, a second file that contains a compatible X509 v3 certificate for a device whose certificate management is integrated with that supported by the PKManager. PKBCA signing and root certificate files are also provided for export. The expiration monitoring services of PKManager are activated on the certificate. Integrated applications that require manual installation of initial certificates are handled through this request.

6 **Revoke Certificate** - this request is used to immediately revoke any certificate that is monitored by the PKManager. Integrated device certificates that are revoked result in creation and delivery of replacement certificates using the appropriate process (notify of replacement or notify request CSR).

7 **Revoke CA Certificate** - this request is used to initiate the CA certificate replacement procedures for a certificates generated by the PKManager. This is potentially a highly processing intensive procedure that can take several hours to complete depending on the device types and number of certificates that must be replaced.

8 **Inherit Certificate** - this request is used to import a WebServices certificate generated by a commercial or external certificate authority. By doing so the certificate management and monitoring services of the PKManager are obtained. This enables a purchased and the valid certificate to continue to be used.

9 **Browse certificates** - The PKGUI provides the user with the ability to list managed certificates and their states.

10 **Alarm Browser** - PKGUI provides access to view all outstanding alarms generated by the PKManager. PKManager logs and alarms can be found in the fault management section of this feature.

See the Configuration section of this feature for further user interface details.

130.2.2.1 MG9K-EM

MG9kEM is enhanced to support the use of public key certificates for securing the MG9k's OAM&P link and the VMG call control links. MG9kEM will be used to provision, distribute and manage the public key certificates for the MG9k gateways.

See the Configuration section of this feature for further user interface details.

130.2.2.2 GWC-EM

The intent of this development is to address the need to support large scale IP telephony deployments which require digital certificates for authentication.

Digital certificates are used mainly to support IPSEC which is used by NE's (for example GWCs, MG9000) to insure secure call control message communications. They are also used on a smaller scale for secure communication between element managers and network elements.

The GWCEM will retrieve the certificates and private key from IEMS and provision, distribute and manage them for the GWCs.

The GWCEM GUI is changed to allow customer to enable IKE authentication in communication between Gateway Controller and Media Gateway.

- Create/Change IKE authentication item.
- Apply IKE authentication to Connection Policy.
- View/Replace PKI certificate chain.

See the Configuration section of this feature for further user interface details.

130.3 Hardware Requirements or Dependencies

There are no hardware dependencies imposed by this feature.

130.4 Software Requirements or Dependencies

PKManager

The PKManager will initially be bundled and installed as part of IEMS installation on SSPFS. The application itself depends on certain common functions provided by SSPFS to provide consistency with other solution components. These include logging, security, and database services.

MG9KEM

The Mg9kEM PKI support is dependent on the PKBroker software running on SN09.x IEMS and PKBClient software running on SN09.x SSPFS.

The new Mg9kEM PKI capabilities are only supported for Mg9k gateways running SN09.x and newer software loads.

GWCEM

N/A

130.5 Limitations and restrictions

PKManager

MG9KEM

GWCEM

In order to provide backwards compatibility, for pre-SN09.1 GWC loads, only one authentication method can be selected. see CN doc

130.6 Interactions

PKManager

The PKManager interacts with its clients through the PKBClient interface introduced into all SSPFS installations. Each supported client application communicates with the PKManger through this interface.

MG9KEM

The IPsec and IKE provisioning is controlled at the SSM and not the Mg9kEM. Adding/deleting policies may result in communication loss between the EM and Mg9k.

Enabling security for the Mg9k is done from the LCI; not from the EM.

Mg9kEM PKI support does not change the existing IPSec preshared key procedures.

GWCEM

N/A

130.7 Glossary

Term	Description
PKManager (PKBroker)	Public Key Manager
PKBClient	Public Key Broker Client
PKGUI	Public Key GUI
IEMS	Integrated Element Management System
GWCEM	Gateway Controller Element Manager
MG9KEM	Media Gateway9000 Element Manager
CA	Certificate Authority
CA Certificate	Certificate issued to a certificate authority, used to sign digital signature certificates that the CA issues
CSR	Certificate Signing Request
IKE	Internet Key Exchange
PKI	Internet public key infrastructure

131: Functional Description (FN) A00012198

131.1 Feature name and Feature ID

A00012198 - GLC12 Coin Card Support from EM

131.2 Description

This GLC12 card is replacing the existing SAA12 card. So this card has to support all the capabilites of the SAA card inclusive of the coin telephone support.

This feature is supported in SN09.1 release. When the user opens the GLC12 card view, the GLC12 card details will be displayed and with twelve port graphics for the GLCports (The GLC12 card has twelve ports). When the user double clicks on the port icon, the GLC circuit view will be displayed. The GLC12 circuit view will display circuit details.

The user will be able to replace the SAA12 with GLC12 without deprovisioning the card. When the card is replaced, the EM will update its details.

131.3 Hardware Requirements or Dependencies

GLC12 card with 12 ports is required.

131.4 Software Requirements or Dependencies

The MG9000 with GLC12 card and support load is required.

131.5 Limitations and restrictions

Since this new GLC12card is patched back in GW till SN08, but not on EM, this card would be displayed as SAA12 in SN08 and SN09 EM.

131.6 Interactions

NONE

131.7 Glossary

SAA12: Service Adaptive Access Line Card w/12 circuits, Supports POTS, GND, Pphone, Coin

GLC12: Global Line Card w/12 circuits Supports POTS, GND, Pphone, Coin.

MG9000: Media Gateway 9000

MG9KEM: MG9K Element Management System

132: Functional Description (FN) A00012199

132.1 Feature name and Feature ID

A00012199 - MG9K EM CPR Robustness

132.2 Description

This feature is supported for MG9Ks with version SN091 and greater. This feature will be supported for all the types of NEs present in subnet (e.g. discovered and undiscovered). The following will be supported for this feature.

1 The craftsperson will be able to initiate an LCI session directly from the MG9K EM subnet screen for all the nodes. It is mandatory that browser path is defined in OS environment. LCI will be invoked on Netscape browser for Unix OS and default browser on a Windows PC. As EM GUI can be launched only from Solaris and Windows PC, this behavior is supported only in Solaris and Windows OS.

The craftsperson must be warned that modification made at LCI may result in node isolation and hence will be required to type (not click) “Agrees” before launching browser.

The craftperson will be given an option of connecting to LCI through inband or out of band.

2. The craftsperson will be able to launch a "clear persist and discover" operation from the MG9K EM for all the nodes.

The craftsperson will be warned that the “clear persist and discover” operation will disrupt services, and will result in an outage condition, and will be required to type (not click) “Agrees” prior to action being taken.

132.3 Hardware Requirements or Dependencies

There is no specific hardware required for this feature.

132.4 Software Requirements or Dependencies

This feature needs changes on the MG9K also and depends on the same.

132.5 Limitations and restrictions

1 The MG9K EM client should have browser path defined on the OS environment. For Unix OS “PATH” environment must have Netscape path defined. For Window OS, the default browser must be set to either Netscape or Internet Explorer.

2 If the browser is already open, LCI session will be launched on the same browser window.

3 When craft person selects the option of launching LCI through inband IP of MG9K, he/she must be aware that if inband address of MG9K is allocated from a private co-lan address space, a client located on the same co-lan or a client which had been connected to the co-lan via a VPN firewall will be able to launch the LCI session. Hence the networking routing is very important while launching the LCI through inband IP. Valid network routing can be checked using ping & traceroute commands. Either command line or “Configuration -> Tools” subnet EM menu can be used for these utilities.

4 LCI out of band access is only available if face plate ethernet is connected on the supercore and a valid out of band IP has been previously configured at LCI.

5 If the LCI browser session returns 404 not found, use the ping command to verify that the out of band address on MG9K responses. The out of band address is the address in the URL shown on the browser screen when out of band LCI is launched.

6 If ping and traceroute do not succeed, the swact of SCO on MG9K may restore connectivity.

132.6 Interactions

N/A

133: Glossary

Term	Description
CPR	Capacity Performance and Robustness
DCC	Data Controller Card
EM	Element Manager
GW	Gateway. It refers to MG9K here.
LCI	Local Craft Interface
MG9K	Media Gateway 9000
OS	Operating System

134: Functional Description (FN) A00012210

134.1 Feature name and Feature ID

A00012210: Geo OA&M Automatic Backup and Accelerated Restore

134.2 Description

This Automatic Backup and Accelerated restore feature, henceforth referred to as "remote backup", will remotely backup all data on the “target” unit. This provides a standby backup system ready to provide service should the primary system or cluster be unavailable for an extended period of time (e.g., catastrophic site loss). The remote backup can assume the identity of the target system with data and files accurate to the last sync. This feature is driven by the geographic survivability configuration where the remote backup will be at a different site from the target system. Previous backup relied on physical media which needs to be transported between the primary and backup systems. Also, the media based restore requires a multistep restore process.

This feature performs the backup via TCP/IP connection and stores an exact copy on the standby server which can be quickly and remotely activated. The data is transferred via an encrypted ssh tunnel over the CS LAN. This remote backup copies all files in each file system marked for backup. This is the same behavior as a full system backup.

If the file system layout has not changed, the backup will transfer file differences since the last backup, a practice commonly referred to as an incremental backup. This is a built in feature of the open source rsync tool. By transferring only differences there are major savings in time and bandwidth.

A remote backup configuration tool is provided to set the necessary parameters and schedule for automatic backup. These backups can be scheduled to automatically occur from once a day to four times per day. Users will be able to enter up to four times of their choice for the automatic backup to occur. For example, "02:00", "06:00", "15:00" and "21:00". This tool also provides a facility for manually initiating a backup and monitoring its progress. Each remote backup session will provide detailed logs of that session.

The standby server has an identical copy of files from the last backup, so it can become the primary system via changing the boot pointer and rebooting. When it boots it will have the IP address and all configuration as of the last backup.

When the primary site is again available, the remote backup feature can be reused to transfer current system configuration back to the primary site and system.

Following is a high level overview for OA&M recovery using the standby server:

1. Normal state: primary site is providing service and the standby site is automatically backing up data at the scheduled times.
2. Primary site goes down. Craft person can remotely login to the standby system and activate the standby backup system.
3. The standby system boots with the configuration and data from the primary site as of the last scheduled backup. Standby site provides service.
4. Sometime later the primary site is repaired. To transfer "current" data and setting from the standby to the primary site, a craft person at the primary site installs cluster unit0 as a remote backup system.
5. Craft person at the primary site performs a remote backup of the standby site.
6. Standby site can be remotely shutdown and primary site activated
7. Primary site should clone the other cluster unit to restore normal cluster operations.
8. Craft person at standby site will need to install the standby system for automatically backing up data. Once this is complete, everything is back to the normal state.

134.3 Hardware Requirements or Dependencies

The hardware of the standby server must match the primary server. This is especially important with regard to hard disk size. This feature is supported with Sun Netra 240 servers.

134.4 Software Requirements or Dependencies

(I)SN09 or higher release.

134.5 Limitations and restrictions

Scheduled backups to the standby server will not complete if a full system backup of the primary HA server pair is in progress.

134.6 Interactions

This feature is very similar to a full system backup. The interactions are similar to the existing full system backup. Due to the exclusive use of file system snap shots, a full system backup to local media and a remote backup to a standby system can not be running at the same time. If the remote backup function detects either of these in progress, it will cleanly exit and re-try at the

next scheduled backup. If a local full system backup is attempted while a remote backup is in progress it will indicate that another backup is in progress and will exit.

Remote system backup should not have any interactions with SBA file transfer via ftp or SBA backup to DVD.

134.7 Glossary

Term	Description
New term	Definition

135: Functional Description (FN) A00012215

135.1 Feature name and Feature ID

A00012215 - Global Line Card Field Programmable Gate Array

135.2 Description

Currently, GLC cards do not have any loads which need to be downloaded from the MG9k Element Manager. The FPGA is currently flashed directly onto the board. In SN09.1, new GLC hardware is introduced which has the capability for the FPGA to be downloaded. The GLC cards must provide the capability for software download of the FPGA. This capability prevents any class “A” retrofits of the GLC-32 or GLC-12 due to a configuration load issue in the FPGA on the card. The NY53BA card replaces the existing POTS-32 and GLC-32 cards.

This feature also covers the need to be able to reload a single circuit controller on the GLC card from the EM. Currently, when the line card is force locked all 8 of the circuit controllers on the GLC-32 cards are reloaded. Each circuit controller controls 4 line circuits. The reload is taking upwards of 4 minutes for a single card which is too long to reload a card. Therefore, we need to be able to reload a single circuit controller on the GLC instead of all 8 being reloaded at the same time.

135.3 Hardware Requirements or Dependencies

Hardware produces the GLC loads for the FPGA configuration load. It is assumed different GLC loads are produced for each different GLC PEC code. The MG9kEM depends upon hardware to produce the different GLC loads for each GLC PEC code.

The GLC can be plugged into any version of the gateway but until the ITP card is running a load that is able to download the GLC FGPAs, the download will not work since the ITP is used to perform the software download to the GLC FPGA. The ITP provides a temporary location to store the FPGA load until it is moved to the GLC card.

Hardware must provide a mechanism to read the FPGA load name in order to display the loadname to the customer. The load name would allow the customer to figure out if the FPGA for the particular vintage of GLC needed to be software downloaded with a new load.

Hardware also produces the coefficients for each GLC PEC code. This new GLC card depends upon hardware to produce a copy of coefficients for this new GLC PEC code.

135.4 Software Requirements or Dependencies

The new GLC download file is loaded onto the SDM/CBM along with the other gateway loads. The MG9kEM software must be at SN09.1 or patched with this feature content in order to provide the software download capability to the GLC card.

Replacing GLC FPGA loads is a function of the gateway loadbuild process. The MG9kEM assumes there is a process in place for replacing GLC loads at the customer site in the event a new GLC load is required outside the normal software release cycle.

135.5 Limitations and restrictions

GLC NTNY53AA and NTNY53AB cards can not be software downloaded.

The GLC downloading capability is available once the GLC card PEC code is NTNY53BA or greater.

Software downloading FPGAs on GLC cards require the GLC card to be locked and thus affects call processing.

The GLC cards are not downloaded as part of a release to release upgrade. The GLC cards can be downloaded after the entire network element, MG9k, has been upgraded if required. Or can be downloaded prior to a release to release upgrade if absolutely required. The preferred method of downloading is to download once the entire network element has already been upgraded.

Running diagnostics on the circuit controller affects 4 circuits at the same time. If the circuit controller needs to be restarted, call processing is affected.

No alarms are output in the event two GLC cards with the same PEC code have different configuration loads.

Unlike the MTA Card View where the customer sees two downloadable loads which can be used to restart the card. The GLC card view only shows a single FPGA configuration load. There is no backup load for the GLC FPGA. There is no restart load capabilities on the GLC card.

135.6 Interactions

Software upgrades - From the frame view, all of the GLC cards for a particular vintage can be downloaded. The GLC software download does not apply to every release to release upgrade. Hopefully, only in rare instances would a new GLC FPGA load be release. Therefore, the upgrade CLUI does not include GLC as a downloadable component. GLC cards must be locked prior to attempting a software download.

Diagnostics- If the circuit controller needs reloading during a circuit controller diagnostic test, 4 circuits are affected. Call processing is dropped during a circuit controller reload. If the circuit controller does not need reloading during the diagnostic, as determined by the gateway, no reload occurs and calls remain operational.

There are no patching interactions since the GLC card can not be patched. The GLC card can not be imaged as well.

135.7 Glossary

Term	Description
CLUI	Command Line User Interface
EM	Element Manager
FPGA	Field Programmable Gate Array
GLC	Global Line Card
SDM	Succession Data Manager

136: Functional Description (FN) A00012223, A00012217, A00012225

136.1 Feature name and Feature ID

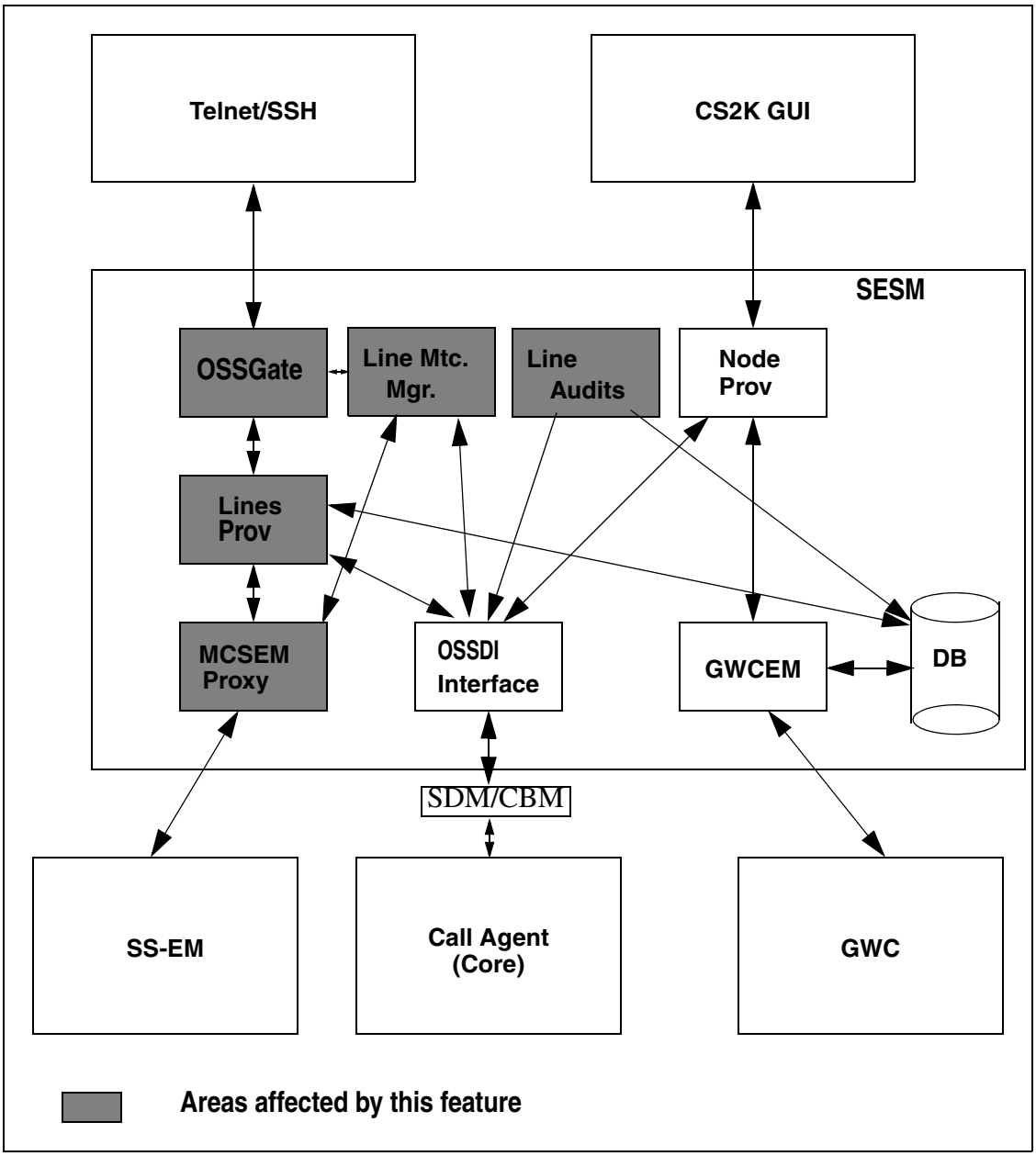
A00012223, A00012217, A00012225--SESM Support for SIP Lines, Part 2

136.2 Description

This activity, SESM Support for SIP Lines Part 2, consists of 3 features:

- A00012223 - SESM: SESM: Additional Provisioning for SIP Lines
  A richer set of SERVORD+ and query commands will be supported for SIP lines. Some of the newly supported commands and will trigger flowthrough of new data to the Session Server Element Manager (SS-EM). The support of HUNT and MADN commands will entail new flowthrough logic for group information to the SS-EM.
- A00012217 - SESM: SIP Lines - Data Sync Audit
  The Line Audit feature component will add auditing coverage of SIP line data on the SS-EM. The data to be audited on the SS-EM includes the Directory Number(DN), the termination name, the Virtual Media Gateway (VMG), and the HUNT/MADN group name information.
- A00012225 - SESM: SIP Lines - Maintenance Enhancements
  Maintenance Enhancements introduces a Services Maintenance Command Line User Interface (CLUI) to replace the LMM GUI and eventually the LTP (Lines Test Position) level of the MAPCI.
  For the introduction, this CLUI will allow the user to post Succession and non-Succession lines (TDM) and perform functions similar to that of the LTP level. This LMM CLUI defined in this document will be generic, intended for use with line or gateway types other than SIP.

Figure 1 Functional Behavior Diagram



136.2.1 Line Maintenance Manager CLUI

The LMM CLUI performs similar functions as the LMM GUI, providing a human/machine interface to view LMM configurations, generate “Query GW in Trouble” reports and line maintenance commands.

136.2.2 Configure

In the SESM, the /opt/nortel/NTsesm/admin/bin/configure tool must be used to configure SESM access to the Session Server Element Manager (SS-EM). This tool is currently used to provision the OPI link. The OMI link requires similar entries.

```
SESM-CS2KSS configuration


OPI - Provisioning Manager Interface configuration

Enter OPI transport protocol to EM server ( http/https - default: https)
 [1] - http
 [2] - https
 [x] - exit

select - 2

 Enter the IP address / Name of the primary CS2KSS prov server (default:
47.142.91.164) : 47.142.91.164
 Enter the primary CS2KSS prov server https port (default is 8443): 8443


 Enter the IP address / Name of the secondary  CS2KSS prov server (default:
47.142.91.164) : 47.142.91.164
 Enter the secondary CS2KSS EM server https port (default is 8443): 8443


 Enter the OPI administrator user name (default: admin): admin

 Enter the OPI administrator password:
 Re-enter the OPI administrator password:

OMI - Provisioning Manager Interface configuration

Enter OMI transport protocol to EM server ( http/https - default: https)
 [1] - http
 [2] - https
 [x] - exit

select - 2

 Enter the IP address / Name of the primary CS2KSS mtc server (default:
47.142.91.164) : 47.142.91.164
 Enter the primary CS2KSS mtc server https port (default is 12121): 12121



 Enter the IP address / Name of the secondary  CS2KSS mtc server (default:
47.142.91.164) : 47.142.91.164
 Enter the secondary CS2KSS mtc server https port (default is 12121): 12121


 Enter the OMI administrator user name (default: admin): admin

 Enter the OMI administrator password:
 Re-enter the OMI administrator password:


OPI - Provisioning Manager configuration
```

```
Transport protocol to EM server                   :   https://
Primary CS2KSS Provisioning Manager IP / Name     :   47.142.91.164
Primary CS2KSS Provisioning Manager port          :   8443
Secondary CS2KSS Provisioning Manager IP / Name   :   47.142.91.164
Secondary CS2KSS Provisioning Manager port        :   8443
The administrator user name                       :   admin


OMI - Maintenance Manager configuration

Transport protocol to Maintenance Manager         :   https://
Primary CS2KSS Maintenance Manager IP / Name      :   47.142.91.164
Primary CS2KSS Maintenance Manager port           :   12121
Secondary CS2KSS Maintenance Manager IP / Name    :   47.142.91.164
Secondary CS2KSS Maintenance Manager port         :   12121
The administrator user name                       :   admin

Is the information correct? (y or n) :
```

The configuration tool will prompt the user to enter the following for the OMI link information:

- Transport protocol to SS-EM server (https).
- IP address / host name of primary SS-EM server
- IP address / host name of secondary SS-EM server. Some configurations may not include a secondary SS EM server. If so, configure the same information provided for the primary server (by default this should be the case).
- HTTPS communication port to SS EM server (12121).
- SS-EM Provisioning Manager administrator user name
- SS-EM Provisioning Manager administrator password

The OPI version information is not required anymore since it is dynamically determined when the OPI and OMI links come into service.

The IP address and port will be used to generate the SS-EM Provisioning Manager URL which in turn will be added to sesm.properties file.

As part of the configuration, the IP address will be validated for format, range and reachability. Other user entered data will be validated for format, range, values etc.

The user name will be added to sesm.properties as clear text.

The password will be stored separately and accessible only to the root user.

All configuration information (url, username, etc.) except password can be displayed by using the SESM “/opt/nortel/NTsesm/admin/bin/configure” tool.

136.2.3 Audits

The Line Audit will now audit the endpoints of Session Server EM with GWCEM and compare group information in SS EM with core and also compare DN to LEN mapping stored in SS EM with core. See section “2.6.2 Line Audit” for information on changes to GUI, BPT, and audit output data (valid and problem log file)

136.2.4 Line Provisioning

Existing support for provisioning SIP lines at OSSGate via SERVORD+ commands will be extended to include a more robust and richer set of commands. See section “136.6.2 SERVORD+ via OSSGate” on page 1304 for detailed information.

136.3 Hardware Requirements or Dependencies

Not applicable.

136.4 Software Requirements or Dependencies

This actrivity requires that the following components are loaded with SN09 drop 2 or equalivalent loads.

CM, XAC or 3PC

GWC

MSM

136.5 Limitations and restrictions

136.5.1 SERVORD+ via OSSGate

See “136.6.2 SERVORD+ via OSSGate” on page 1304 for the various limitations and restrictions related to the support for the expanded set of SERVORD+ commands.

136.6 Interactions

136.6.1 LMM CLUI

To access the LMM CLUI telnet to OSSGate, enter ^B, “mode MTC”. Once in the MTC level, “LMM” is entered for access to the LMM CLUI.

```
>
? mode MTC

Mode is MTC.
```

The CMCLLI command is used to return the SDM IP and CMCLLI name:

```
>CMCLLI
      SDM IP = 47.142.134.124
      CM CLLI = RTP2
```

```
>LMM
      report <-v>
      report <-l> <report name>
      report <-gen> <GWC Options>

      post <-d, -l, -gw, -u, -r, -set, -display, -count>

      bsy <-d, -l, -gw, -set> [inb]
      rts <-d, -l, -gw, -set>
      tst <-d, -l, -gw, -u, -set>
      FRLS <-d, -l>

      qdn <dn>
      qlen <len>
      qsip <dn, len>

      help

      quit
```

The commands (i.e. report, bsy) can be entered in either upper or lower case. The options (i.e. -d, -l) must be entered in lower case. The parms can be entgered in either case but in the case of the GW name, should be in the proper case.

136.6.1.1 REPORT Commands

The REPORT commands are used with the GW in Trouble reports. Using the commands, the user has the ability to list, view and delete any of the reports. The GENERATE or GEN is used to run the process to create a report.

Command format:

```
report <-l>
report <-v> <REPORT NAME>
report <-gen> <GWC List | all>
```

Command usage:

To obtain a list of reports currently available

```
>report -l
The following reports are available:
Report-2005-08-10-22-06-14
```

To view a specific report

```
>report -v Report-2005-08-10-22-06-14
GW Name   Results for GWC-0
t1124ent.us.nortel.com   GW DISABLED

GW Name   Results for GWC-10
test4   GW DISABLED
```

To request a new GW in Trouble report for GWC 1

```
report -gen 1
```

To request a new GW in Trouble report for GWC 1, 2 and 3

```
report -gen 1, 2, 3
```

or

```
report -gen 1-3
```

or

```
report -gen 1, 2-3
```

To request a new GW in Trouble report for all valid (small and large line) GWCs

```
report -gen all
```

136.6.1.2 MTC Commands

This set of commands is used to perform operations on either one or a set of lines.

Command format:

```
post -d <DN> [verbose]
post -l <LEN> [verbose]
post -gw <GW/VMG> [verbose]
post -u <URI> [verbose]
post -r <Domain name> [verbose]
post -display [verbose]
post -count

bsy -d <DN> [inb]
bsy -l <LEN> [inb]
bsy -gw <GW or VMG> [inb]
bsy -set [inb]

rts -d <DN>
rts -l <LEN>
rts -gw <GW/VMG>
rts -set

tst -d <DN>
tst -l <LEN>
tst -gw <GW/VMG Name>
tst -u <URI>
tst -set

frls -d <DN>
frls -l <LEN>
```

136.6.1.2.1 REPORT Commands

The REPORT commands are used with the GW in Trouble reports. Using the commands, the user has the ability to list and view any of the reports. The -gen is used to run the process to create a report.

Command format:

```
report <-l>
report <-v> <REPORT NAME>
report <-gen> <GWC List | all>
```

Command usage:

To obtain a list of reports currently available

```
>report -l
The following reports are available:
Report-2005-11-14-12-12-01
```

To view a specific report

```
>report -v Report-2005-11-14-12-12-01
GWC-14  Number of GWs out of service = 1

R7A20204.rtp7.net status = GW DISABLED

GWC-13  Number of GWs out of service = 11


To request a new GW in Trouble report for GWC 1
report -gen 1
```

To request a new GW in Trouble report for GWC 1, 2, 3 and 4

```
report -gen 1, 2, 3, 4
```

or

```
report -gen 1-4
```

or

```
report -gen 1, 2-4
```

To request a new GW in Trouble report for all valid (small and large line) GWCs

```
report -gen all
```

136.6.1.2.2 POST

The POST command can be used to generate a set of lines and be used for maintenance (BSY, etc.) actions.

The POST command will list the contents of the post set to the screen using a “brief” format. The information listed will be dn, len, uri, clientIp, gwc, lcc, cm line state, scc line state and MCS line state (if a SIP Line).

The VERBOSE option includes included the above and adds the following, GW/VMG name, GW ipaddress, GW type, endpointName, domain/ subdomain.

To post by DN (SIP Line)

```
      >post -d 7550505
DN         = 6137550505
LEN        = SS 00 0 00 05
LCC        = IBN
GWC NAME   = GWC-5
GW NAME    = rtp7ssa
EPT NAME   = SS/000/0/0005
GW EPT ST  = ON-HOOK
CM EPT ST  = IDL
SIP URI    = user5@rtp7ssa.com
CLIENT IP =
SS EPT ST =
```

```
Number of endpoints returned = 1
```

To post by DN, non SIP Line

> post -d 6210010

```
DN         = 6136210010
LEN        = UAIP 00 1 00 00
LCC        = IBN
GWC NAME   = GWC-14
GW NAME    = rtp7-1104b.us.nortel.com
EPT NAME   = aaln/1
GW EPT ST  = ON-HOOK
CM EPT ST  = IDL

Number of endpoints returned = 1
```

To post by LEN:

```
      > post -l ss 0 0 0 5
DN         = 6137550505
LEN        = SS 00 0 00 05
LCC        = IBN
GWC NAME   = GWC-5
GW NAME    = rtp7ssa
EPT NAME   = SS/000/0/0005
GW EPT ST  = ON-HOOK
CM EPT ST  = INB
SIP URI    = user5@rtp7ssa.com
CLIENT IP =
SS EPT ST =
```

To post by GW:

Note: Since the minimum VMG sizze for SIP is 1023 endpoints, posting by vmg may take a long time (approx 5 mins per LGRP) and will produce a huge output.

```
      > post -gw rtp7-1104b.us.nortel.com
DN         = 6136210010
LEN        = UAIP 00 1 00 00
LCC        = IBN
GWC NAME   = GWC-14
GW NAME    = rtp7-1104b.us.nortel.com
EPT NAME   = aaln/1
GW EPT ST  = ON-HOOK
CM EPT ST  =

DN         = 6136210011
LEN        = UAIP 00 1 00 01
LCC        = IBN
```

```
GWC NAME  = GWC-14
GW NAME   = rtp7-1104b.us.nortel.com
EPT NAME  = aaln/2
GW EPT ST = ON-HOOK
CM EPT ST =

DN        = 6136210012
LEN       = UAIP 00 1 00 02
LCC       = RES
GWC NAME  = GWC-14
GW NAME   = rtp7-1104b.us.nortel.com
EPT NAME  = aaln/3
GW EPT ST = ON-HOOK
CM EPT ST =

DN        = 6136210013
LEN       = UAIP 00 1 00 03
LCC       = RES
GWC NAME  = GWC-14
GW NAME   = rtp7-1104b.us.nortel.com
EPT NAME  = aaln/4
GW EPT ST = ON-HOOK
CM EPT ST =
```

To post by URI:

```
      > post -u user5@rtp7ssa.com
DN        = 6137550505
LEN       = SS 00 0 00 05
LCC       = IBN
GWC NAME  = GWC-5
GW NAME   = rtp7ssa
EPT NAME  = SS/000/0/0005
GW EPT ST = ON-HOOK
CM EPT ST =
SIP URI   = user5@rtp7ssa.com
CLIENT IP =
SS EPT ST =
```

To post Registered users by domain. This command will return the users that have registered their clients with their provisioned domains.

Note: This command may take a long time and will produce a huge output.

```
      > post -r rtp7ssa.com
DN        = 6137550505
LEN       = SS 00 0 00 05
LCC       = IBN
GWC NAME  = GWC-5
GW NAME   = rtp7ssa
EPT NAME  = SS/000/0/0005
GW EPT ST =
CM EPT ST =
SIP URI   = user5@rtp7ssa.com
CLIENT IP =
SS EPT ST =

DN        = 6137550510
LEN       = SS 00 0 00 10
LCC       = IBN
GWC NAME  = GWC-5
GW NAME   = rtp7ssa
```

```
EPT NAME  = SS/000/0/0010
GW EPT ST =
CM EPT ST =
SIP URI   = user10@rtp7ssa.com
CLIENT IP =
SS EPT ST =


Number of endpoints returned = 2
```

To display the contents of the post se using the verbose option:

```
      >  post -display verbose
DN         = 6137550505
LEN        = SS 00 0 00 05
LCC        = IBN
GWC NAME   = GWC-5
GW NAME    = rtp7ssa
EPT NAME   = SS/000/0/0005
GW EPT ST  = ON-HOOK
CM EPT ST  = IDL
SIP URI    = user5@rtp7ssa.com
CLIENT IP  =
SS EPT ST  =
Node Num   = 213
Term Num   = 6
GWC IP     = 47.142.92.172
GW IP      = 47.142.91.154
GW TYPE    =
```

To display the number of entries in the post set:

```
      >post -count
      Post set size = 104
```

136.6.1.2.3 BSY

The BSY commands informs the CM to perform the requested action. A response message indicates the success or failure of the command. These messages are generated by the CM.

To Maintenance/Manual Busy a line by DN:

```
      > bsy -d 7550505
DN = 7550505
CM RETURN CODE = CM_OK
```

To Maintenance/Manual Busy a line by LEN:

```
      >  bsy -l ss 0 0 0 5
LEN = ss 0 0 0 5
CM RETURN CODE = CM_OK
```

To Maintenance/Manual Busy all lines on a GW:

```
      > bsy -gw rtp7-1104b.us.nortel.com
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
```

```
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

To Busy by the posted set:

```
      > bsy -set
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

The BSY INB operation performs two operations; first is a BSY then upon success, performs the INB operation. If the line is already in the BSY state then only the INB operation is performed.

If the line is IDL

```
      >  bsy -d 7550505 inb
DN = 7550505
CM RETURN CODE = CM_OK
DN = 7550505
CM RETURN CODE = CM_OK
```

If the line is BSY

```
> bsy -d 7550505 inb
DN = 7550505
CM RETURN CODE = CM_ALRDY_IN_REQ_STATE
DN = 7550505
CM RETURN CODE = CM_OK
```

136.6.1.2.4 RTS

To return-to-service a line by DN:

```
      > rts -d 7550505
DN =  7550505
CM RETURN CODE = CM_OK
```

To return-to-service a line by LEN:

```
      >  rts -l ss 0 0 0 5
LEN = ss 0 0 0 5
CM RETURN CODE = CM_OK
```

To return-to-service all lines on a GW:

```
      > rts -gw rtp7-1104b.us.nortel.com
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
```

```
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

To Busy by the posted set:

```
      > rts -set
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

136.6.1.2.5 TST

The TST performs a diag (where possible) depending upon the GW's ability to perform diagnostics on endpoints. Only GCP and MGCP GWs support the TST command.

To test by DN (SIP):

```
> tst -d 7550505

DN = 6137550505
LINE_STATE = PASSED
ENDPOINT_STATE = UNKNOWN
CLIENT = user5@47.142.166.65
TEST RESULT = PASSED
```

To test by DN (MGCP line):

```
> tst -d 6210010

DN = 6136210010
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
```

To test using the LEN (SIP)

```
      > tst -l ss 0 0 0 5

DN = 6137550505
LINE_STATE = PASSED
ENDPOINT_STATE = UNKNOWN
CLIENT = user5@47.142.166.65
TEST RESULT = PASSED
```

To test using the URI

```
      > tst -u user5@rtp7ssa.com

URI = user5@rtp7ssa.com
LINE_STATE = PASSED
ENDPOINT_STATE = UNKNOWN
CLIENT = user5@47.142.166.65
TEST RESULT = PASSED
```

To test by GW (or VMG).

Note: Testing by VMG may take a long time and produce a large amount of information.

MGCP based GW:

```
> tst -gw rtp7-1104b.us.nortel.com

DN = 6136210010
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
DN = 6136210011
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
DN = 6136210012
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
DN = 6136210013
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
```

SIP GW

```
> tst -gw rtp7ssa

DN = 6137550500
LINE_STATE = FAILED
ENDPOINT_STATE = UNKNOWN
ERROR = Test Executed

DN = 6137550501
LINE_STATE = FAILED
ENDPOINT_STATE = UNKNOWN
ERROR = Test Executed
```

136.6.1.3 QUERY Commands

The query commands are used to perform various existing queries. These queries are the same as those from Servord.

Command format:

```
qdn <DN>
qlen <LEN>
qsip <DN, LEN>
```

Command usage:

To Query a DN

```
QDN 7201000
--------------------------------------------------------------------------------
DN:     7201000
TYPE: SINGLE PARTY LINE
SNPA: 619   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     SS    00 2 00 00
END POINT: rtp2sesm1  SS/000/2/0000
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:            BNR     SUBGRP: 0  NCOS: 0
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: N
```

```
PM NODE NUMBER     :    142
PM TERMINAL NUMBER :    1
OPTIONS:
CWT DGT DPL Y 10
OFFICE OPTIONS:
SRA

END POINT DATA:
SIP_CLIENT_TYPE: ont
SIP_EP_NAME: SS/000/2/0000
SIP_VMG_NAME: rtp2sesm1
SIP_DN: 6197201000
SIP_LOCATION: rtp2
SIP_PACKAGE: basic
SIP_URI: user0@rtp2.com
--------------------------------------------------------------------------------
```

To query by LEN

```
> qlen SS 0 2 0 0
--------------------------------------------------------------------------------
LEN:     SS    00 2 00 00
END POINT: rtp2sesm1  SS/000/2/0000
TYPE: SINGLE PARTY LINE
SNPA: 619
DIRECTORY NUMBER:     7201000
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:            BNR     SUBGRP: 0  NCOS: 0
SIGNALLING TYPE:  DIGITONE
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: N
PM NODE NUMBER     :    142
PM TERMINAL NUMBER :    1
OPTIONS:
CWT DGT DPL Y 10
OFFICE OPTIONS:
SRA
END POINT DATA:
SIP_CLIENT_TYPE: ont
SIP_EP_NAME: SS/000/2/0000
SIP_VMG_NAME: rtp2sesm1
SIP_DN: 6197201000
SIP_LOCATION: rtp2
SIP_PACKAGE: basic
SIP_URI: user0@rtp2.com
--------------------------------------------------------------------------------
```

To query using the QSIP command. The parm can be either a DN or LEN.

```
> qsip 7550505
SS    00 0 00 05
SS/00/0/0005
--------------------------------------------------------------------------------
SIP USER DATA
=============
SIP URI: user5@rtp7ssa.com
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: Y
NUMBER OF CONTACTS: 1
CONTACTS: user5@47.142.166.65
SERVICE PACKAGE:
basic_package
SERVICES:
ALCLNT N IM SIPLN ADVSCR 3 3 N CLNTCO N N N N ADHOC 4 ADDRBK 50 PRES 10 Y
```

```
20 Y VIDEO N N NWLOG 50 50

SIP LINE DATA
=============
ENDPT ID: SS/000/0/0005
VMG: rtp7ssa
ZONE ID(s):
CLIENT TYPE: ONT
STATIC CLIENT: Y

SIP CALL DATA
=============
ACTIVE CALL APPEARANCES:
  NODENO   TERMNO
NUMBER OF ACTIVE SESSIONS IN CS2000 SESSION SERVER: 0
--------------------------------------------------------------------------------
>
```

136.6.1.4 MISC Commands

To quit from the LMM level - the user will remain in the MTC mode.

```
QUIT
```

136.6.1.5 Command Parsing

Multiple commands can be input input on the same line - they must be separated by a ";". Up to 4 lens, dns or uris can be specified with the POST, BSY, TST and RTS commands. Due to the potential volume of output, only one GW or VMG can be specified.

The commands are not case sensitive, but the parameters may be, ie. GW name will be case sensitive.

136.6.2 SERVORD+ via OSSGate

This feature extend existing capabilities of the Succession SERVORD+ system for SIP client provisioning. SIP client commands/data will distributed to the SS-EM from the SERVORD+ system within the SESM. The following commands will trigger data distribution to the SS-EM from SESM SERVORD+ when SS vmgs/endpoints (or associated LENs) are found within the command:

- NEW
- OUT
- CHF
- ADD
- EST
- DEL
- ADO (for MDN options)

- DEO (for MDN options)
- CDN
- CHF
- CLN/CTP
- QCUST
- QLEN/QTP (show endpoint for HASU SIP LENs)
- QDNWRK (show SIP_DATA queried from SS-EM)
- QLENWRK (show SIP_DATA queried from SS-EM)
- QSIP

For SIP Line clients, the NEW, OUT and CHF commands are currently supported. New development is required to support the remaining commands in this release.

Note: CHF requires the use of gateway/termination names (or the equivalent LEN) in order to trigger data flow through for SS lines. Use of DN instead of primary LEN or gateway/termination will result in the command being processed only by the CM.

Note: CDN commands which modify the DN assigned to the user will ***not*** automatically update the SIP_URI. The use of Directory Number in the SIP_URI value (e.g. 2145209999@nortel.com) is not recommended.

Note: EST/ADD/DEL commands support only single SIP LENs/ Endpoints in the command due to the limitation of a single SIP_DATA option being processed in the options area. Use of multiple SIP LENs/ Endpoints in these commands will result in command failure.

Query commands such as QCUST, QLENWRK and QDNWRK (which return formatted line/service information) will include the SIP_DATA options provisioned via the NEW/EST/ADD/CHF commands in their output. The SIP_DATA option information will be appended to the end of the existing QLENWRK/QDNWRK output, but prior to the dashed line (eg. "----------")query output terminator for each line in the output.

Existing data tags presented in query output with sample values:

END POINT DATA: *(This is the endpoint data header, no info/value associated with this tag)*

SIP_CLIENT_TYPE: sip line

SIP_EP_NAME: SCOT/000/0/0000

SIP_VMG_NAME: vmg1

SIP_DN: 6195209998

SIP_LOCATION: nortel networks.rtp.nc0

SIP_PACKAGE: sip lines

SIP_URI: slynch@mordor.com

New data tags presented in query output with sample values:

SIP_GROUP_DN: 6195209999

SIP_GROUP_TYPE: MLH

SIP_SUBDOMAIN: doom.mordor.com

See query examples in the next section for details on presentation and positioning within query output.

136.6.2.1 SERVORD+ Command Examples

See Configuration Section for SIP_DATA option format details and provisioning rules.

136.6.2.1.1 NEW command Examples:

NEW $ 6195209998 1FR LATA1 0 **SCOT 00 0 00 00** dgt SIP_DATA SIP_PACKAGE SIP Lines SIP_URI slynch@mordor.com SIP_SUBDOMAIN doom.mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD scott11 $ DPL Y 10 $

NEW $ 6195209998 1FR LATA1 0 **vmg1 SCOT/000/0/0000** dgt SIP_DATA SIP_PACKAGE SIP Lines SIP_URI slynch@mordor.com SIP_SUBDOMAIN doom.mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD scott11 $ DPL Y 10 $

136.6.2.1.2 CHF Command Examples

The change feature command is currently supported for SIP lines and SIP_DATA except SIP_URI. SIP_URI may be included in the CHF command, but it must match the existing value assigned to the user. Change of the SIP_SUBDOMAIN for the user will be supported.

CHF $ SCOT 00 0 00 00 SIP_DATA SIP_PACKAGE siplines SIP_PASSWD scott11 SIP_CLIENT_TYPE IBN SIP_LOCATION IBM.RTP $ $

CHF $ **vmg1 SCOT/000/0/0000** SIP_DATA SIP_PACKAGE siplines SIP_PASSWD scott11 SIP_CLIENT_TYPE IBN SIP_LOCATION IBM.RTP $ $

Moving a line/user between domains/subdomains can be accomplished using the CHF command. For example, if user slynch@mordor.com is currently provisioned in the root domain (mordor.com) and needs to be moved to subdomain doom.mordor.com, the following CHF command may be used:

CHF $ SCOT 00 0 00 00 SIP_DATA SIP_SUBDOMAIN doom.mordor.com $ $

By simply specifying a SIP_SUBDOMAIN sub-option, the user associated with LEN SCOT 00 0 00 00 will be moved from their currently assigned domain to the value specified by the SIP_SUBDOMAIN sub-option. A user may be moved between root domain and subdomains, between subdomains, or between root domains using this mechanism. However, it is important to note that user moves between domains can have serious consequences on user based data in the Session Server Element Manager. If packages, locations, or group information does not match in the target domain, then the users existing data will be *lost* following the move, replaced by default data in the target domain. **NO WARNING IS GIVEN WHEN THIS OCCURS.** ***Therefore, CHF based user moves should be used with caution as important domain specific data may be lost during the move. QLEN/QDN executed before and after the move should reveal any data mismatch/loss.***

136.6.2.1.3 OUT Command Examples

OUT $ 6195209998 SCOT 00 0 00 00 BLDN

OUT $ 6195209998 **vmg1 SCOT/000/0/0000** BLDN

136.6.2.1.4 QDN and QLEN Query Examples

The following examples of query output show the newly added SIP_DATA sub-options SIP_SUBDOMAIN, SIP_GROUP_TYPE, and SIP_GROUP_DN.

```
> QLEN SCOT  00 0 00 00
------------------------------------------------------------------------------
LEN:     SCOT  00 0 00 00
END POINT: vmg1  SCOT/000/0/0000
TYPE: SINGLE PARTY LINE
SNPA: 619
DIRECTORY NUMBER:     5209998
LINE CLASS CODE:      1FR
SIGNALLING TYPE:  DIGITONE
LINE TREATMENT GROUP:     0
LINE ATTRIBUTE INDEX:     0
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: Y
PM NODE NUMBER     :    87
PM TERMINAL NUMBER :    1
```

```
OPTIONS:
DGT DPL Y 10
OFFICE OPTIONS:
SRA
END POINT DATA:
SIP_CLIENT_TYPE: sip line
SIP_EP_NAME: SCOT/000/0/0000
SIP_VMG_NAME: vmg1
SIP_DN: 6195209998
SIP_LOCATION: nortel networks.rtp.nc0
SIP_PACKAGE: sip lines
SIP_URI: slynch@mordor.com
SIP_SUBDOMAIN: doom.mordor.com
--------------------------------------------------------------------------------

> qdn 5209998
--------------------------------------------------------------------------------
DN:     5209998
TYPE: SINGLE PARTY LINE
SNPA: 619   SIG: DT    LNATTIDX: 0
LINE EQUIPMENT NUMBER:     SCOT  00 0 00 00
END POINT: vmg1  SCOT/000/0/0000
LINE CLASS CODE:      1FR
LINE TREATMENT GROUP:     0
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: Y
PM NODE NUMBER     :    87
PM TERMINAL NUMBER :    1
OPTIONS:
DGT DPL Y 10
OFFICE OPTIONS:
SRA

END POINT DATA:
SIP_CLIENT_TYPE: sip line
SIP_EP_NAME: SCOT/000/0/0000
SIP_VMG_NAME: vmg1
SIP_DN: 6195209998
SIP_LOCATION: nortel networks.rtp.nc0
SIP_PACKAGE: sip lines
SIP_URI: slynch@mordor.com
SIP_SUBDOMAIN: doom.mordor.com
--------------------------------------------------------------------------------
>qlen TEST  01 1 09 22
--------------------------------------------------------------------------------
```

```
LEN:     TEST  01 1 09 22
END POINT: vmg1 TEST/001/1/0922
TYPE: MEMBER OF MLH HUNT GROUP
SNPA: 214
HUNT GROUP:  13        HUNT MEMBER:  1
DIRECTORY NUMBER:     5209999              (NON-UNIQUE)
LINE CLASS CODE:      1FR
IBN TYPE: STATION
CUSTGRP:         RES214     SUBGRP: 0  NCOS: 1
SIGNALLING TYPE:  DIGITONE
LINE TREATMENT GROUP:     0
LINE ATTRIBUTE INDEX:     520_1FR
XLAPLAN KEY :   214_P520_1              RATEAREA KEY :        RA214_2
CARDCODE:  RDTLSG    GND: N  PADGRP: PKLNL  BNV: NL MNO: N
PM NODE NUMBER     :    213
PM TERMINAL NUMBER :    923
OPTIONS:
DGT
RES OPTIONS: NONE
PILOT LEN: TEST  01 1 09 23
GROUP OPTIONS:
RCVD
END POINT DATA:
SIP_CLIENT_TYPE: sip line
SIP_EP_NAME: TEST/001/1/0922
SIP_VMG_NAME: vmg1
SIP_DN:
SIP_LOCATION: nortel networks.rtp.nc0
SIP_PACKAGE: sip lines
SIP_URI: slynch@mordor.com
SIP_SUBDOMAIN: doom.mordor.com
SIP_GROUP_TYPE: MLH
SIP_GROUP_DN: 2145209999
--------------------------------------------------------------------------------
>qlen TEST 01 1 09 23
--------------------------------------------------------------------------------
LEN:     TEST  01 1 09 23
END POINT: vmg1 TEST/001/1/0923
TYPE: MULTIPLE APPEARANCE DIRECTORY NUMBER
SNPA: 214
DIRECTORY NUMBER:     5209999              (NON-UNIQUE)
LINE CLASS CODE:      1FR
IBN TYPE:  MADN
MADN INFO - TYPE:SCA  PRIMARY:N  RING:NEVER
```

```
MADN GROUP INFO - DENIAL_TRMT:   TONE   BRIDGING:N
CUSTGRP:         RES214  SUBGRP:0  NCOS: 1
SIGNALLING TYPE:  DIGITONE
LINE TREATMENT GROUP:     0
LINE ATTRIBUTE INDEX:     520_1FR
XLAPLAN KEY :   214_P520_1              RATEAREA KEY :        RA214_2
CARDCODE:  RDTLSG    GND: N  PADGRP: PKLNL  BNV: NL MNO: N
PM NODE NUMBER     :    213
PM TERMINAL NUMBER :    924
OPTIONS:
DGT
RES OPTIONS: NONE
END POINT DATA:
SIP_CLIENT_TYPE: sip line
SIP_EP_NAME: TEST/001/1/0923
SIP_VMG_NAME: vmg1
SIP_DN:
SIP_LOCATION: nortel networks.rtp.nc0
SIP_PACKAGE: sip lines
SIP_URI: slynch@mordor.com
SIP_SUBDOMAIN: doom.mordor.com
SIP_GROUP_TYPE: MDN
SIP_GROUP_DN: 2145209999
--------------------------------------------------------------------------------
```

136.6.2.1.5 QLEN For HASU LEN

The QLEN command output currently shows endpoint and SIP_DATA information for LENs with assigned service, however no endpoint data is shown for HASU LENs. The output is updated in this release to add the associated endpoint information (if any) to the end of the query output for HASU LENs.

```
>qlen TEST 00 1 01 00
--------------------------------------------------------------------------------
TYPE: HARDWARE ASSIGNED SOFTWARE UNASSIGNED
CARDCODE:  RDTLSG    GND: N  PADGRP: PKLNL  BNV: NL MNO: N
PM NODE NUMBER     :    136
PM TERMINAL NUMBER :    101
END POINT: ssvmg.42 TEST/000/1/0100
--------------------------------------------------------------------------------
```

136.6.2.1.6 QCUST

Example command and output for a SIP line:

```
>qcust bnr $
1 SS12 00 6 00 07 IBN PKLNL RDTLSG N
```

```
2 7207167 BNR 0 0 613
9 CWT DGT DPL Y 10 $
23 SIP_URI me@mydomain.com SIP_LOCATION my house
99
```

New record type “23” is introduced which contains SIP_DATA information.

136.6.2.1.7 QDNWRK/QLENWRK

QDNWRK and QLENWRK are bulk queries which display all or ranges of working DNs or LENs. The Detailed output of these commands resembles lists of individual QDN and QLEN query output. A Summary output simply displays a count.

Examples:

```
QDNWRK R 7215554 7215554 NLCC $ D
COMMAND AS ENTERED
QDNWRK R         7215554         7215554 ALL NLCC $ ALL D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>REPORT ON WORKING DIRECTORY NUMBERS
FROM      6197215554 TO      6197215554
  LCC ALL                      OPTION ALL
--------------------------------------------------------------------------------
DN:     7215554
TYPE: SINGLE PARTY LINE
SNPA: 619   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     C411  01 0 02 01
END POINT: vmg1 C411/001/0/0201
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:            BNR     SUBGRP: 0  NCOS: 0
CARDCODE:  RDTLSG    GND: N  PADGRP: PKLNL  BNV: NL MNO: N
PM NODE NUMBER     :    147
PM TERMINAL NUMBER :    50
OPTIONS:
DGT
END POINT DATA:
SIP_CLIENT_TYPE: sip line
SIP_EP_NAME: C411/001/0/0201
SIP_VMG_NAME: vmg1
SIP_DN: 6197215554
SIP_LOCATION: nortel networks.rtp.nc0
SIP_PACKAGE: sip lines
SIP_URI: slynch@mordor.com
SIP_SUBDOMAIN: doom.mordor.com
--------------------------------------------------------------------------------
```

```
--------------------------------------------------------------------------------
TOTAL COUNT OF WORKING DN FROM      6197215554 TO      6197215554:          1
>

COMMAND AS ENTERED
QLENWRK R C411  01 0  C411  01 0  ALL  ALL NLCC $ D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
WARNING : Queries of all LENs or a large range of LENs
          may run for 30 minutes or more before producing any output
Please confirm ("YES", "Y", "NO", or "N"):
>y
REPORT ON WORKING LINE EQUIPMENT NUMBERS
FROM C411  01 0   TO C411  01 0      DRAWERS ALL
  LCC ALL                      OPTION ALL
--------------------------------------------------------------------------------
LEN:     C411  01 0 02 01
TYPE: SINGLE PARTY LINE
DN 6197215554  LCC  IBN    SIG DT  LNATTIDX N/A
IBN TYPE: STATION
CUSTGRP:            BNR     SUBGRP: 0  NCOS: 0
CARDCODE:  RDTLSG    GND: N  PADGRP: PKLNL  BNV: NL MNO: N
PM NODE NUMBER     :    147
PM TERMINAL NUMBER :    50
OPTIONS:
DGT
END POINT DATA:
SIP_CLIENT_TYPE: sip line
SIP_EP_NAME: C411/001/0/0201
SIP_VMG_NAME: vmg1
SIP_DN: 6197215554
SIP_LOCATION: nortel networks.rtp.nc0
SIP_PACKAGE: sip lines
SIP_URI: slynch@mordor.com
SIP_SUBDOMAIN: doom.mordor.com
--------------------------------------------------------------------------------
                  TOTAL:           1
```

136.6.2.1.8 ADO and DEO for MADN

For most forms of ADO/DEO, a SIP line would be unaffected, however adding a MDN option to an existing line may change that line's directory number (set to empty on the Session Server). Adding the MDN option may also trigger group creation on the Session Server if the line is the first Session Server line in the MDN group.

Examples:

```
NEW $ 7215555 IBN BNR 0 0 619 NILLATA 0 C411  01 0 02 00 SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user2@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user21 $ DPL Y 10 dgt $

ADO $ c411 1 0 2 0 MDN SCA Y Y 6197215555 TONE N $
```

C411 01 0 02 00 is now the Primary member of the MADN group 6197215555. A MDN group named “6197215555” is created on the Session Server element manager and user “user2@mordor.com” is added to the group. The DN of user “user2@mordor.com” is cleared (blanked) in the Session Server element manager.

A second line is added with a different DN, 6197215554:

```
NEW $ 7215554 IBN BNR 0 0 619 NILLATA 0 C411  01 0 02 1 SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user3@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user21 $ DPL Y 10 dgt $
```

Now the MDN option is added to this second line specifying a different DN (6197215555) and a treatment (BLDN) for the original DN (6197215554) :

```
ADO $ C411 01 0 02 01  MDN SCA N Y 6197215555 BLDN  $
```

The end result of this is that the DN for C411 01 0 02 01 changed from 6197215554 to 6197215555 on the core and the line is now a member of MADN group 6197215555 on the Session Server element manager. Now, delete the MDN option from this newly added member and specify it's new DN.

```
DEO $ C411 01 0 02 01 MDN 6197215554 $
```

Following the DEO of the MDN option, the DN for C411 01 0 02 01 is changed from 6197215555 to 6197215554 on the core and the line is no longer a member of MADN group 6197215555 in the Session Server element manager. User “user3@mordor.com” will have a DN assignment of 6197215554 on the Session Server element manager.

136.6.2.1.9 NEW, OUT and CDN for MADN

MADN groups may be created and populated using the NEW command.

Examples:

```
NEW $ 7215554 IBN BNR 0 0 619 NILLATA 0 C411 01 0 02 01 DGT MDN SCA Y Y TONE N SIP_DATA
SIP_PACKAGE SIP Lines SIP_URI user1@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION
Nortel Networks.RTP.NC0 SIP_PASSWD user11 SIP_SUBDOMAIN doom.mordor.com $ $

NEW $ 7215554 IBN BNR 0 0 619 NILLATA 0 C411 01 0 02 02 DGT MDN SCA N Y SIP_DATA SIP_PACKAGE
SIP Lines SIP_URI user2@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel
Networks.RTP.NC0 SIP_PASSWD user11 SIP_SUBDOMAIN doom.mordor.com $ $

CDN $ 6197215554 6197215555 BLDN

OUT $ 7215555 C411  01 0 02 02 BLDN

OUT $ 7215555 C411  01 0 02 01 BLDN
```

A group with type “MDN” and name “6197215554” is created during processing of the first NEW command and user “user1@mordor.com” is

added to that group. The second NEW command adds user "user2@mordor.com" to the same group. The CDN command results in the DN for the MDN group being changed in the core for all members and also the group name changing from "6197215554" to "6197215555" in the Session Server element manager.

On the SS-EM, the OUT command will removed the line/user from the MDN group, and if the user is the last member of the group, the group will also be removed.

136.6.2.1.10 EST, ADD, DEL,CHDN

Huntgroup flowthrough architecture only triggers flowthrough for hunt flavors which can assign service to a HASU line: MLH, DLH, and DNH. MPH can also be used to assign service to a HASU line, however MPH is not supported for SIP line. Other flavors such as CPU, CMG, SIMRING, and BNN are assigned to lines with existing service and therefore trigger no flowthrough and hence no group creation/deletion on the Session Server element manager.

Examples:

DLH:

```
EST $ DLH 6195209998 1FR LATA1 0 SCOT  00 0 00 00 $ dgt SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user1@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user11 SIP_SUBDOMAIN doom.mordor.com $ DPL Y 10 $

ADD $ DLH SCOT  00 0 00 00 SCOT 00 0 00 01 $ dgt SIP_DATA SIP_PACKAGE SIP Lines SIP_URI
user2@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD
user21 SIP_SUBDOMAIN doom.mordor.com $ DPL Y 10 $

DEL $ DLH SCOT 00 0 00 01 $

OUT $ 6195209998 SCOT  00 0 00 00 BLDN
```

With these commands, a group is created on the Session Server named "6195209998" (GROUP_DN in query output for these lines) with a type of "DLH" (GROUP_TYPE in query output for these lines). The Session Server group is created when the EST command is processed and user "user1@mordor.com" is added to the group. The ADD command triggers no group creation, but user "user2@mordor.com" is added to group "6195209998" on the Session Server Element Manager. The DEL command removes user "user2@mordor.com" from the group and from the Session Server element manager in general. Finally, the OUT command removes group "6195209998" from the Session Server element manager and also removes user "user1@mordor.com".

MLH:

```
EST $ MLH 6195209998 1FR LATA1 0 SCOT  00 0 00 00 $ dgt SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user1@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user11 SIP_SUBDOMAIN doom.mordor.com $ DPL Y 10 $
```

```
ADD $ MLH SCOT  00 0 00 00 SCOT 00 0 00 01 $ dgt SIP_DATA SIP_PACKAGE SIP Lines SIP_URI
user2@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD
user21 SIP_SUBDOMAIN doom.mordor.com $ DPL Y 10 $

CHDN $ SCOT 00 0 00 01 2145200999

DEL $ MLH SCOT 00 0 00 01 $
```

The CHDN command shown above results in the DN change of member SCOT 00 0 00 00 to 2145200999 in the core but no change to the currently blank DN assigned to user “user2@mordor.com” in the Session Server element manager. The user’s DN will remain blank in the Session Server as long as it is a member of a group regardless of DN changes which occur in the Core.

DNH:

```
EST $ DNH 2145200998 1FR LATA1 0 SCOT  00 0 00 00 $ DGT SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user1@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user11 SIP_SUBDOMAIN doom.mordor.com $ DPL Y 10 $ 5

ADD $ DNH 2145200998 2145200997 SCOT  00 0 00 01 $ DGT SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user2@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user21 SIP_SUBDOMAIN doom.mordor.com $ DPL Y 10 $ 5

DEL $ DNH 2145200997 SCOT  00 0 00 01 $ bldn
```

Note that the SERVORD+ format requires insertion of GW/EP or LEN in the DEL command for DNH groups. This is normally not required in Core SERVORD.

Only ONE SIP LEN/gw-ep is supported in any EST or ADD command since only one SIP_DATA option is allowed in the options area of the command. Use of more than one SIP LEN/gw-ep in the EST/ADD command will result in command failure.

136.6.2.1.11 CDN

SESM logic will support flow through of change DN requests for SIP Lines, however the CDN command will be blocked for MLH/DLH hunt pilots/ members but will be supported for MADN and DNH group pilot/link/ members (this is a legacy implementation restriction on CDN commands).

Example:

```
NEW $ 7215555 IBN BNR 0 0 619 NILLATA 0 C411  01 0 02 00 SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user2@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user21 $ DPL Y 10 dgt $

CDN $ 6197215555 6197215554 BLDN
```

CDN commands which modify the DN assigned to the user will ***not*** automatically update a SIP_URI containing directory number information. The use of Directory Number in the SIP_URI value (e.g. 2145209999@nortel.com) is not recommended.

136.6.2.1.12 CLN

A limited OSSGate/SERVORD+ infrastructure is provided to process flowthrough for CLN commands for SIP lines, however the processing is limited to changes between SIP lines only. For CLN of SIP lines, the from_value and to_value in the CLN command must both contain SIP LENS/ endpoints, otherwise the command will fail.

Examples:

```
CLN $ C411 01 0 02 00 C411 01 0 02 01
CLN $ C411 00 0 00 00 C411 01 0 02 01
```

136.6.3 Line Audit :

In this feature, the line audit will also audit the data in Session Server EM. The audit GUI look and feel does not change, except that few checks are added to warn the user of system load. Also the audit output file (both valid and problem files) will have extra information pertaining to the Session Server audit.

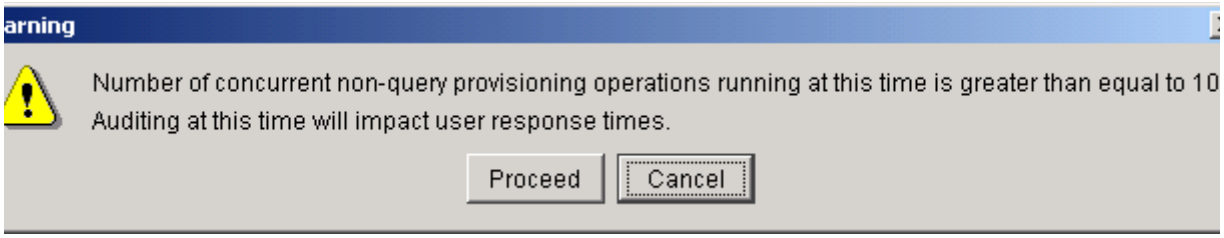
136.6.3.1 Warning Dialogues in Audit GUI

One of the requirements in this feature is to avoid running(atleast warn) line audit when the system is loaded, as the audit might impact more important provisioning activities. In this feature, the manual line audit will check for the system load and warn the user if its not an appropriate time to run audit.

When the user choose line audit from GUI and clicks RunAudit button, the GUI first checks with Audit server if its ready to run the audit. The server does three checks to determine if its ready or not. If any of the three checks is true, then the server will return ‘not ready’ with details to the GUI, which in turn will pop a dialogue box to warn user of system load and gives him a chance to decide if he wants to run the audit at a later time, since running audit has the potential to slow down the system impacting higher priority provisioning activities.

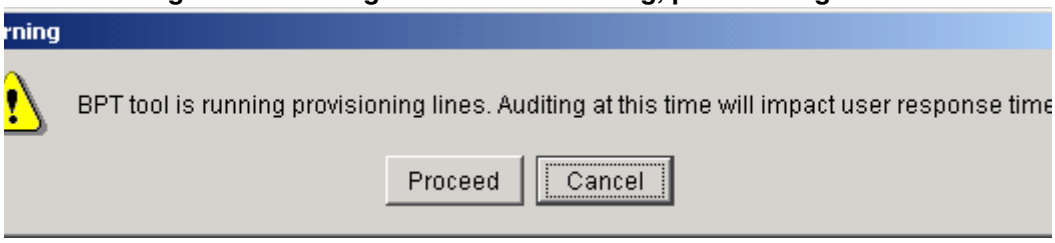
First check done by the server is to see if there are 10 or more concurrent non-read-only operations in progress. If yes, the audit server returns ‘not ready’ with details to the GUI. Shown below is example dialogue box.

Figure 2 Warning if 10 or more non-query type line provisioning in progress



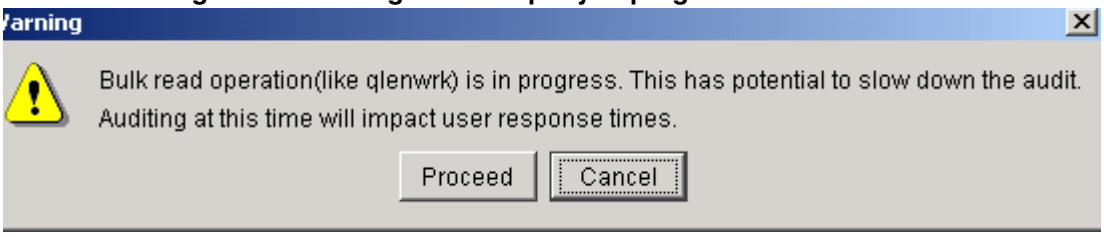
The second check is to see whether BPT tool is running a lines batch operation. If yes, the server returns ‘not ready’ with details to GUI. Shown below is example dialogue box in this condition.

Figure 3 Warning if BPT tool is running, provisioning lines



The third check is to see whether any bulk query operation(like qlenwrk,qdnwrk etc) is already in progress . If yes, the server will return ‘not ready’ to the GUI. Shown below is example dialogue box in this scenario.

Figure 4 Warning if a bulk query in progress before line audit starts



136.6.3.2 Warning in BPT on Audit Running

In addition to the line Audit GUI warnings(2.6.2.1), a check is introduced in BPT tool where it determines if Line Audit is currently running. If yes, BPT tool will warn the user that line audit is in progress and gives the user a chance to run the lines batch later, as the throughput of the Lines batch could be slower due to line audit running.

Screen shot from BPT tool when lines batch is started while line audit is in progress.

***** W A R N I N G *****

Line Audit is currently in progress.

This lines batch may run slower and may also invalidate audit results

Do you still want to proceed with lines batch? <y/n>:

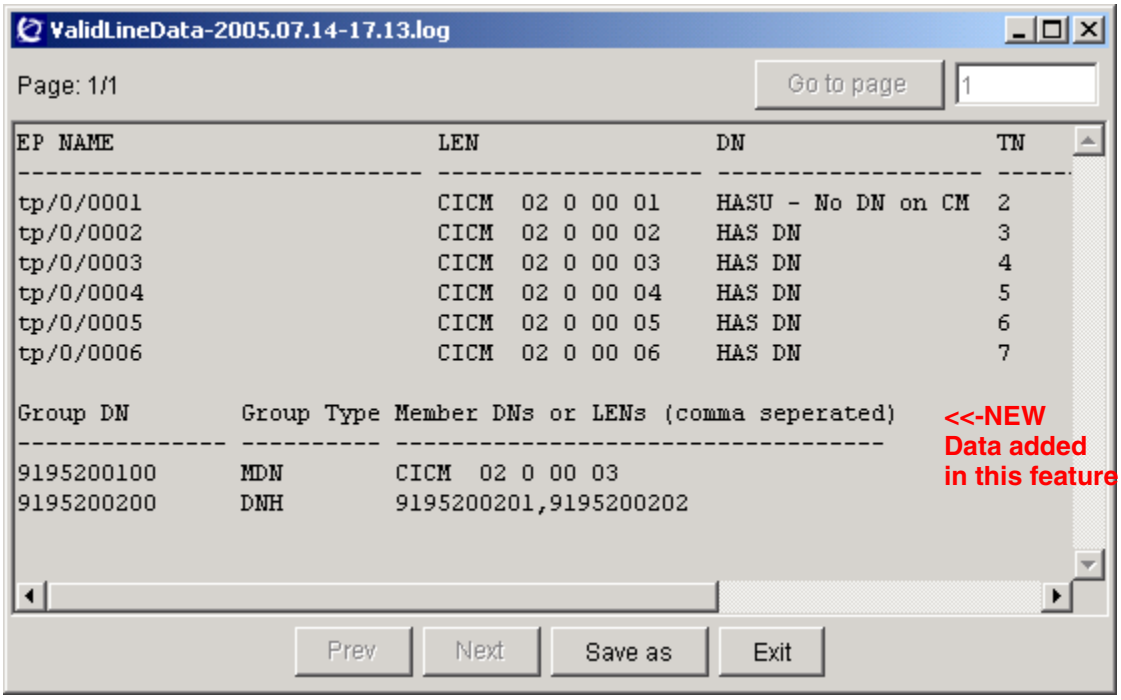
The above warning tells the user that line audit is in progress and perhaps the lines batch should be run after the audit is finished

136.6.3.3 Line Data Audit Valid Data output:

After the line data audit finishes, the ValidLineData.log file will have additional information obtained by auditing the Session Server EM.

The endpoints in GWCEM will be compared with SS EM, the group DN and its member DN information will be compared with the core and the DN to len mapping will also be compared with the core.

In the first screen shot is shown, valid data w.r.t the Session server will be at bottom. In the foll screen shot, the group DN and its type and the member DNs are printed on screen, which is new audit data added by this feature if SIP MGs are provisioned.



136.6.3.4 Line Data Audit Problem Data output:

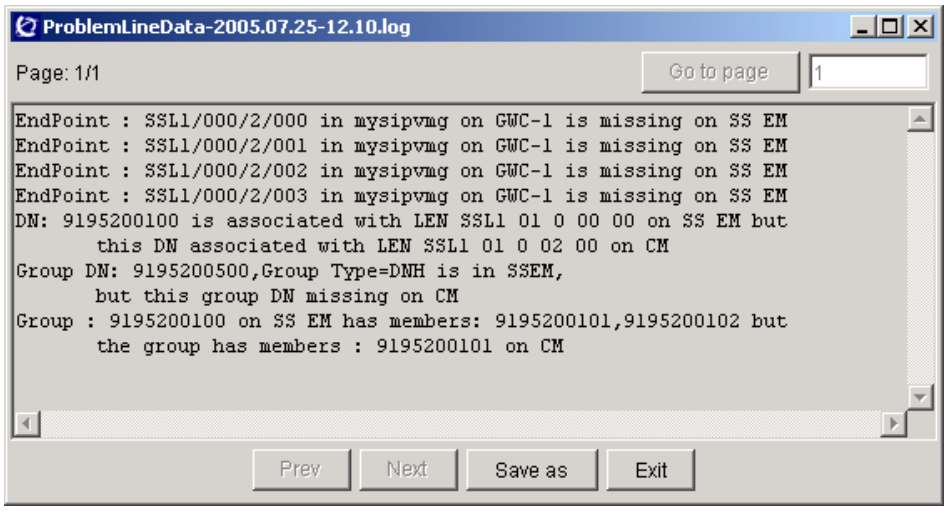
Shown below is screen shot of problem line data results. The problems could be in following areas

1. Endpoint exists in GWCEM, but not in Session server EM

2. DN associated with endpointId(len) in SS EM, while that same DN maps to different LEN on core

3. group DN in SS EM but that group information is missing in core

4. member DN/LENs in SS EM belonging to a group do not match the member list in that group on core.



Glossary

Term	Description
New term	Definition

138: Functional Description (FN) A00012242

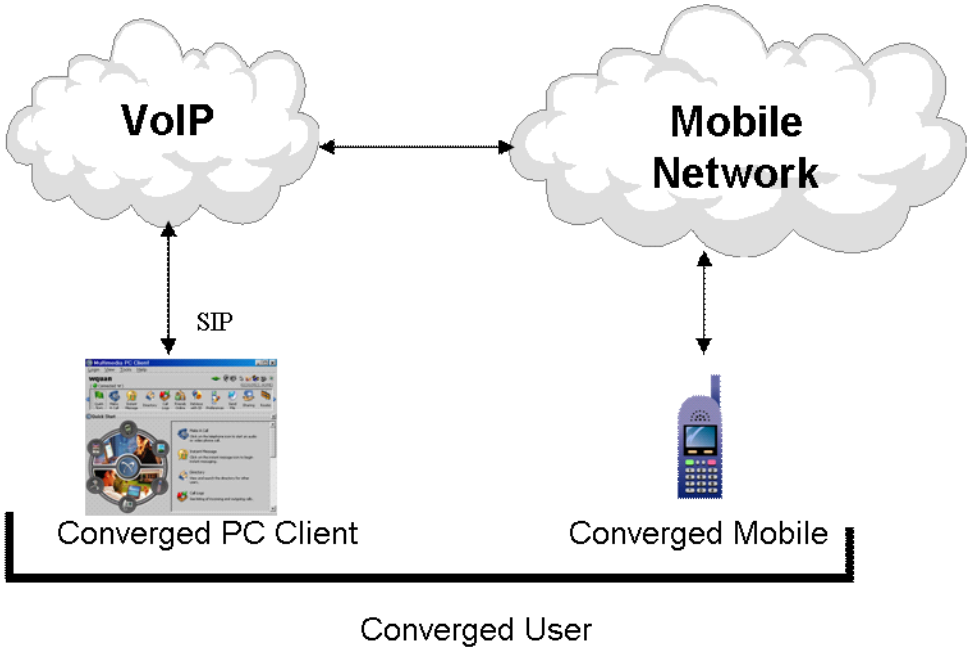
138.1 Feature name and Feature ID

A000122423: TME-CD with GSM Wireless Client, Ph-1: “Mobility for Converged Desktop - MCD”

138.2 Description

The Converged Desktop feature was introduced in previous versions of MCS and enabled subscribers to use their SIP PC Client for the multi-media portion of their communication, while using their existing telephony system for voice.

Figure 1 Mobile Converged Network



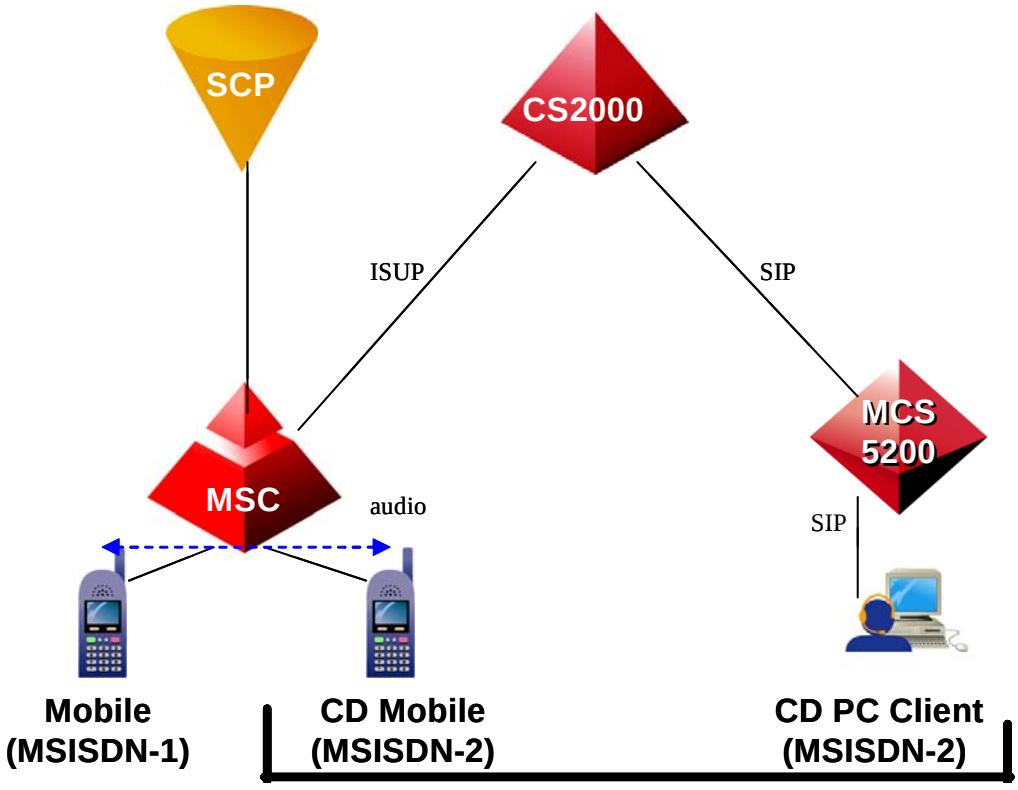
This feature provides a new Centrex service on the MCS application server that enables limited call control of wireless calls from the terminating Converged PC Client, while the audio streams to a preferred audio device in

an existing wireless network. In this phase, the services are limited to terminating services without video.

Generally, the feature sets offered by each network are independent such that mobile features are not integrated with the MCS network. Only within the context of this feature are the networks ‘converged’. Features provided on the mobile network are in no way limited by this feature. The operator should consider feature interactions, as they may intersect on the converged networks. Voicemail is an example of this interaction, as either / both networks can provide a network based voicemail service.

The network component view of the converged networks and the connectivity between the CD Mobile and the CD PC Client is shown in Figure 2.

Figure 2 Network Component Diagram



The mobile network is typically comprised of several MSC (and peripherals for the radio interface) so the illustration is simplified in this regard. The mobile converged phone is illustrated as ‘CD Mobile’ and is also referred to as the preferred audio device throughout this document. The established voice path (audio stream) is between the mobile terminals. The CD PC Client is used to manage calls terminating to CD Mobile.

The only Intelligent Network (IN) node illustrated on the mobile network is the SCP. This is clearly a simplification of the Intelligent Network, and the figure illustrates only the nodes relevant to this feature. The SCP serves as a central point of service logic, which includes the necessary digit manipulation and logic enabling the MCS to later supervise the call. Generally, the IN nodes are not assumed to be Nortel switching nodes.

The MSC is expected to possess SSP functionality to interact with the SCP. In general terms, the terminating mobile will subscribe to a trigger in the AIN terminating call model. Thereafter when a termination attempt is processed, the trigger will be hit, and call processing will suspend on the MSC to query the SCP for service processing. Service logic in the SCP will execute to prefix digits and respond to the query with an analyze_route message to the MSC. The MSC (SSP) will continue processing the call and terminate the call to the CS2000. The MSC (SSP) nodes of the network need not be Nortel switching nodes.

The Nortel CS2000 is a key network component employed to tandem calls between the MCS IP network and the mobile TDM network, and is a required component for this feature. The CS2000 serves as a gateway between the mobile network and the MCS IP network. When this feature is enabled, calls destined for CD Mobile will be routed through the CS2000 and down to the MCS5200 for supervision before being presented to the CD Mobile.

This converged network topology requires overflow route engineering on the CS2000 to ensure mobile calls are properly routed during an IP network outage. The CS2000 is able to detect the SIP trunk status by sending periodic heart-beat messages on the SIP trunk connecting it with the MCS5200. The SIP trunk status could be out-of-service if the MCS5200 becomes network isolated on the IP network or is simply offline for any reason. The CS2000 must be configured to route traffic to an alternate overflow route if the SIP trunk status is detected as out-of-service. The operator should engineer overflow routes on the CS2000 to accommodate the mobile traffic in such an outage on the MCS IP network. The operator should refer to CS2000 documentation for detailed discussions of provisioning this functionality.

This feature is only designed to interact with the clients shown in Figure 2. That is, the CS2000 and the MCS5200 may be hosting other lines and user agents, yet these call-types fall outside the scope of this feature.

Based on PC Client, this feature has been designed for Small to Medium Enterprises with limited access bandwidth, so that audio streams are never exchanged between the PC Client and the network. Once the terminating CD Mobile voice path is established, this feature allows the MCS 5200 to supervise all calls terminating to that CD Mobile via the MCD Client. Thus, the subscriber can use the MCD PC Client to modify the audio stream to the CD Mobile. This is made possible in the MCS IP network because the audio

session can be updated (third party call control) without modifying the audio connection on the mobile network. The functionality provided by the MPC Client will be especially useful in scenarios with several concurrent calls, since the GUI of the MCD PC Client can be more intuitive in managing multiple calls and initiating multi-call features such as conference or transfer.

Provisioning this Centrex service requires configuration on the Mobile Network and the MCS network. As part of the PSTN configuration, a required dial-plan must be established (section 138.3.2 Dial Plans), and a prefix numbering scheme is provisioned by the operator across the network. Mobile CD subscribers will be provisioned on the SCP as fixed extensions of the company they belong to in the Corporate Service, linked to the company's new "non-existent" PBX (MCS). Unless otherwise stated, mobile features enabled on the PSTN are not coordinated with those provided by this service and therefore mobile subscribers can continue to invoke features from the mobile without the MCS5200 knowledge or supervision. This document will later consider only one such feature- voicemail.

On the MCS system, the operator must provision the following prefixes to use this mobility converged service. These can be provisioned on the sub-domain or the subscriber. If both the sub-domain and subscriber have a prefix provisioned, the subscriber prefix will be used. Provisioning is discussed in more detail in section 138.2.12.1 Service Prefix Provisioning.

- Destination Call Leg Return Code (CRD): This is the sum of navigational digits that will be placed in front of the (non CD) destination mobile number for outgoing calls from the MCD client to the mobile network.
- Associated Call Leg Return Code (CRA): This is the sum of navigational digits that will be placed in front of the CD destination mobile number (PAD). This prefix can be used to identify this call leg on the GSM network as a non-chargeable call.

On the MCS network, the operator can assign services and create service packages that expose features to the 'Personal Agent' and enable the feature set at the client. Some services are not compatible with this feature. Logic in the provisioning server will prevent incompatible services from being packaged together in the same service package. Section 20.7.1 Service Compatibility covers these service interactions in more detail.

The services that are supported in the MCD PC Client generally fall into two categories: multimedia services and voice services. Generally, multimedia services are available only to MCS clients. For example, the 'whiteboard collaboration' feature of the PC Client requires both parties to use the MCS PC Client. Multimedia services have no interaction with the mobile network. Multimedia services are supported only between MCS Clients, and can be enabled (and disabled) via the existing service assignment and packaging mechanism by the administrator. The existing behavior of the client is to

render service related buttons only when that service is exposed to the subscriber. That is, the PC Client GUI has dynamic behavior based on the subscriber service package contents. This document assumes these services are enabled.

The following optional services are the only multimedia services supported in this feature. Services not listed will not be supported in this release.

- Collaboration: File Transfer
- Collaboration: Clipboard Transfer
- Collaboration: Web Push
- Collaboration: White Board
- SIP based Instant Messaging

The voice services in the MCD PC Client allow the subscriber to manage calls and invoke call related features. Some voice services will require service assignment and packaging. For example, conferencing requires the service ‘Ad Hoc Conferencing’ and the service package parameter for the ‘maximum number of conference ports’ is enforced in the MCS application server.

The MCD subscriber can perform the following services from the MCD PC Client. Services not listed will not be supported in this release.

- Originate new calls
- Receive incoming calls
- Hold and Retrieve calls
- Switch between several connected calls
- Direct transfer an existing call to another party
- Request a new conference
- Join all calls into a single conference

138.2.1 SIP Client Registration

All features of the MCD PC Client are enabled after successful login to a MCS Application Server. The authenticated login process essentially employs a SIP REGISER transaction to associate the users contact on the application server. Additionally, the client retrieves a service package which itemizes all services and capabilities available to the subscriber and the parameters associated with those services. This section details the registration behavior the subscriber can expect for various client configurations.

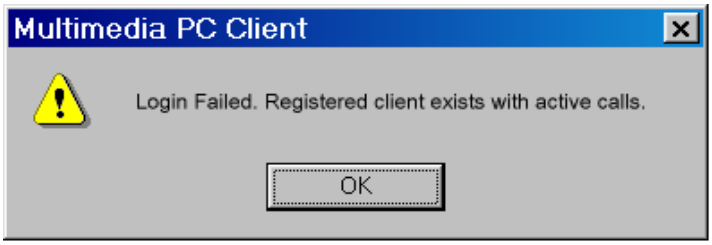
138.2.1.1 MCD Client Login

The mobile converged PC client logic is automatically activated in the Multimedia PC Client if the service package contains the Mobile Converged

Desktop service. Unlike the previous converged-desktop client, once activated the PC Client may not be manually un-converged via the ‘preference’ GUI. The PC Client in the mobile converged mode of operation will be referred to as MCD PC Client within this document.

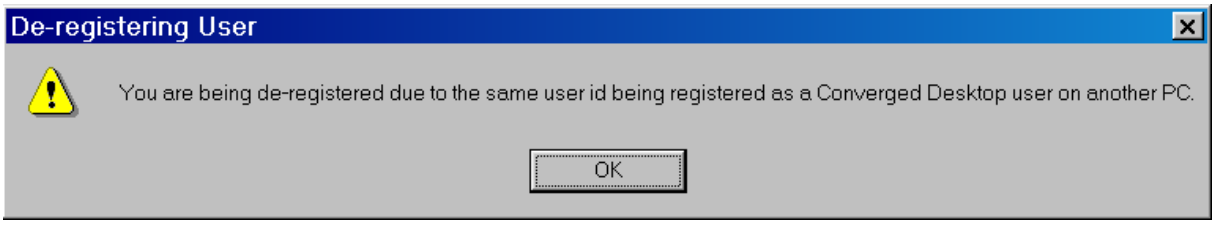
A subscriber should only login a single instance of the MCD PC Client. If the subscriber attempts to register a second instance of the MCD PC Client while calls are in progress, the second registration will be rejected by the MCS application server and the client will indicate to the user that active calls are still in progress

.



If there are no calls in progress when the second instance registers, the first instance will be de-registered. The deregistered client will display a notification to the user as shown in Figure 3.

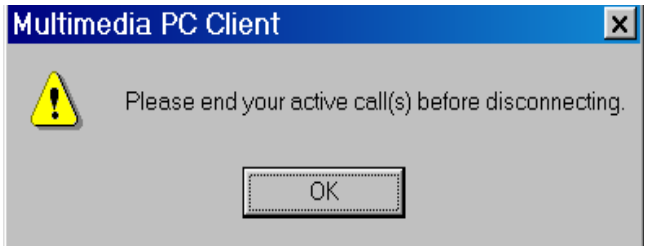
Figure 3 Deregistered on client



138.2.1.2 MCD Client Logout (or Exit)

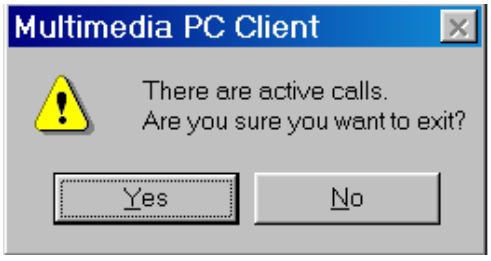
The subscriber may attempt to logout or exit the client at any time. The client logout process involves the typical SIP REGISTER (with a subscriber contact and expires of zero). During a ‘Logout’ attempt with active calls, the MCD PC Client will prompt the user to end active calls before disconnecting (Figure 4). The user can only click ‘OK’ and should manually release any active calls before to proceeding with the logout.

Figure 4 Logout attempt with active calls



During an ‘Exit’ attempt with active calls, the MCD PC Client will warn the user that calls are still in progress. The user can either click ‘Yes’ to release all active calls and shutdown the client or ‘No’ to cancel the attempt.

Figure 5 Exit attempt with active calls



In the event the MCD PC Client becomes network isolated with active calls, the mobile subscriber will lose the ability to manage the existing calls. The best way to cleanup the existing calls is to release the PAD leg on the CD Mobile. The application server will automatically release all calls for the MCD subscriber when the CD Mobile (PAD) leg is released. Additionally, the MCS application server executes periodic call audits to release calls that are apparently stranded. The situation where the MCD client is network isolated or unavailable is discussed in more detail in 138.2.11 Client Unavailable / Calls of Grace.

138.2.1.3 Standard Client Registration

Non converged clients perform a ‘standard’ client registration upon subscriber login. If a subscriber with the MCD service assigned in the service package utilizes a non-converged client (e.g. I200x device), then call terminations to them will be presented to the clients using the existing call forking mechanism at the Application Server and no mobile converged client control functionality (as described in this document) will be provided.

138.2.2 Supported Releases of the Multimedia PC Client

The MCD PC Client functionality is only supported in the 4.1 release of the PC Client.

138.2.3 Call Origination Behavior

This section assumes the MCD PC Client is registered and the corresponding CD Mobile is actively available on the mobile network for originating calls. The subscriber can originate calls either from the CD Mobile or the MCD PC Client. The following sections consider the behavior for both scenarios. Detailed call processing (signaling) details are deferred to a later section.

138.2.3.1 MCD PC Client Origination / Click-to-call

Even though the MCD PC Client is not used for voice, the subscriber can use the MCD PC Client to originate calls. This call scenario is also referred to as 'click-to-call' and behaves much like a direct transfer. In the click-to-call scenario, a call leg to CD Mobile is first established and immediately followed by the PAD being transferred to the destination mobile (MSISDN-2). All calls originated from the MCD PC Client employ the click-to-call mechanism.

The basic origination initiated on the MCD Client is performed by clicking 'New Call' and providing the address of the terminating mobile (MSISDN-2). The client will establish a secure HTTP connection (via SSL) to the Personal Agent to initiate the call to the MCS application server. Upon initiating the click-to-call, the MCD PC Client displays a call window similar to that shown in Figure 6. Call originations may be abandoned on the MCD Client.

Figure 6 Click-to-call Outgoing call window

Additionally, the click-to-call origination can be initiated directly from the Personal Agent web application. However in this case, the subscriber cannot cancel (abandon) the call attempt like on the MCD PC Client.

The mobile converged service suspends the MCD subscriber from making or receiving additional calls while a click to call outgoing call attempt is 'In Progress'. The MCS Session Manager will reject subsequent outgoing call attempts indicating that active calls are still in progress, and, likewise, the MCS Session Manager will also reject any incoming calls by responding with a 600 Busy Everywhere SIP response. Thus, once call is originated on the MCD PC Client, it will not be possible to originate another call from the client or terminate another call to the client until the initial call is either answered or terminated

138.2.3.2 CD Mobile

When the PAD originates a new call, the wireless network (MSC) will route the call without interaction with MCS application server. The MCD PC Client will not be supervised from the wireless network for originating call scenarios from the PAD.

138.2.4 Call Termination Behavior

This section assumes the MCD PC Client is registered and the corresponding CD Mobile is available on the mobile network for receiving calls. When a call attempt is made to the CD Mobile, the MCS application server will present the call to the registered MCD PC Client. The PC Client will to display a call dialog GUI indicating a call is being received at the same time the CD Mobile starts ringing. This section discusses the MCD PC Client behavior for various terminating scenarios. Detailed call processing (signaling) details are deferred to section 138.3.4 PAD Terminated Scenarios.

MCD PC Client behavior depends on the subscriber assigned services. Thus, the MCD PC Client GUI may display icons that enable various features such as Reply with Instant Messaging, Transfer, or Conference. Recall, it is possible to limit the features exposed on the client by provisioning a service package without collaboration features, conferencing, etc. The following sections illustrate the client GUI behavior in the standard theme with all supported services enabled.

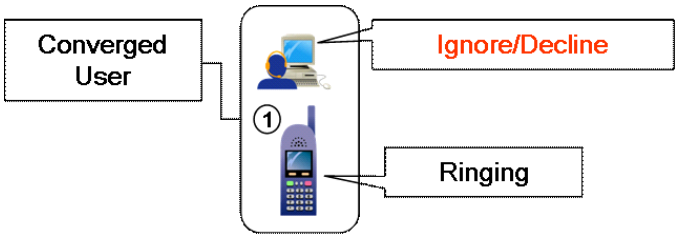
138.2.4.1 Call Window Before Answer

Before a call is answered on the CD Mobile, the MCD PC Client displays a call window similar to that shown in Figure 7. When the call is presented, a Picture-ID and the calling party number are provided. A custom Picture-ID is only available if the other end is an MCP user and has assigned such a picture in Preferences section of the Personal Agent. Otherwise a default Picture-ID[1] will be used. Additionally, the subscriber may have the option to initiate multimedia services such as SIP Instant Messaging[2]. Recall, these services may not be exposed to all subscribers.

[1]The default Picture-ID can be modified in a custom PC Client theme.
[2]SIP Instant Messaging is not integrated with mobile network SMS messaging in this release.

Figure 7 Initial Inbound Call to MCD PC Client

Note the ‘Answer’ button is inactive. Thus, the audio options available for this pending call simply allow the subscriber to immediately ignore or decline the call.



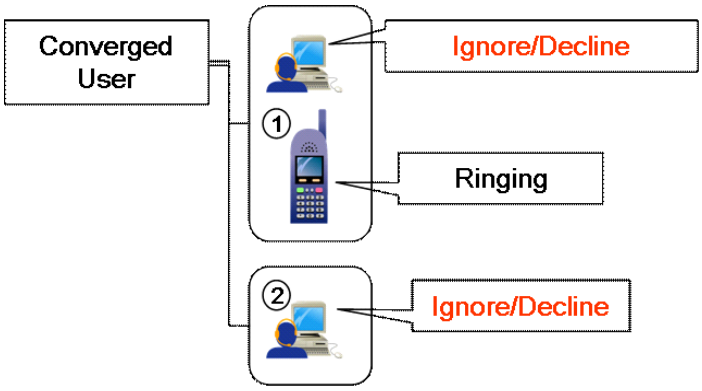
When the ‘Ignore’ button is pressed it would stop the client from ringing while the application server would continue executing any terminating services for the call. That is, terminating service logic is executed to route advance to another destination or voicemail. After all terminating services completed on the application server, it would release the call with cause and the mobile network could execute terminating services. Within the context of this feature, the Ignore button affects all user network contacts. This behavior, while typically customizable from the “Users Preference GUI –> Miscellaneous –> Ignore Buttons” menu, will not be customizable for the MCD PC Client.

The decline option results in releasing the call such that terminating services on the application server would cease for the call. The MCS application server would release the call with cause and the mobile network could execute terminating services.

The ‘Answer’ button remains disabled on the MCD PC Client until the CD Mobile has answered. That is, the initial call attempt to the CD Mobile can not be answered from the MCD PC Client. Subsequent calls can be answered from the MCD PC Client.

In the case of two or more simultaneous incoming calls prior to answering the CD Mobile, the ‘Answer’ buttons on all incoming call windows is disabled as shown in Figure 7. The first incoming call will be answered upon answering the CD Mobile, and the call window for that call will appear as shown in the following section. Additionally, the ‘Answer’ buttons on any remaining call windows will be enabled, and these remaining calls will be handled as subsequent incoming calls in the multiple call scenario described in section 138.2.5.1 Call Waiting.

Aside from the behavior of the ‘Answer’ button, multiple incoming pending calls will exhibit behavior similar to the initial call.



138.2.4.2 Call Window After Answer

An initial call can only be answered on the CD mobile. Thus, to accept this initial call the CD mobile answers the call. Once the call is answered on the mobile, the PAD leg is established. Subsequent calls may be answered from the PC client.

The MCD PC client call window updates after the CD mobile answers similar to the illustration in Figure 8. The MCS application server signals the client by means of a SIP message to update the GUI with new audio options

Figure 8 Initial call is answered on MCD PC client

The only supported audio options for answered calls are listed below.

Audio options available on answered call	
New Call	Used to place a new call. Clicking 'New Call' will implicitly (local) Hold any existing established calls.
Hold / Retrieve	The user can hold and retrieve the call from the MCD PC Client (local hold). However, the user cannot initiate a local hold if the call is already in remotely held. This scenario is referred to as dual-hold, and is not supported.
Conference	Initiates an audio conference. Established calls will be placed on local hold until conference is joined.
Transfer	Initiates a direct transfer of the established call to another destination.
Hang Up	Releases the established call. The CD Mobile call leg will remain established if other calls are on Hold by the MCD PC Client.

Assuming the originator is an MCS SIP subscriber, the following multimedia capabilities must be provisioned by the administrator to be utilized from the terminating MCD PC Client.

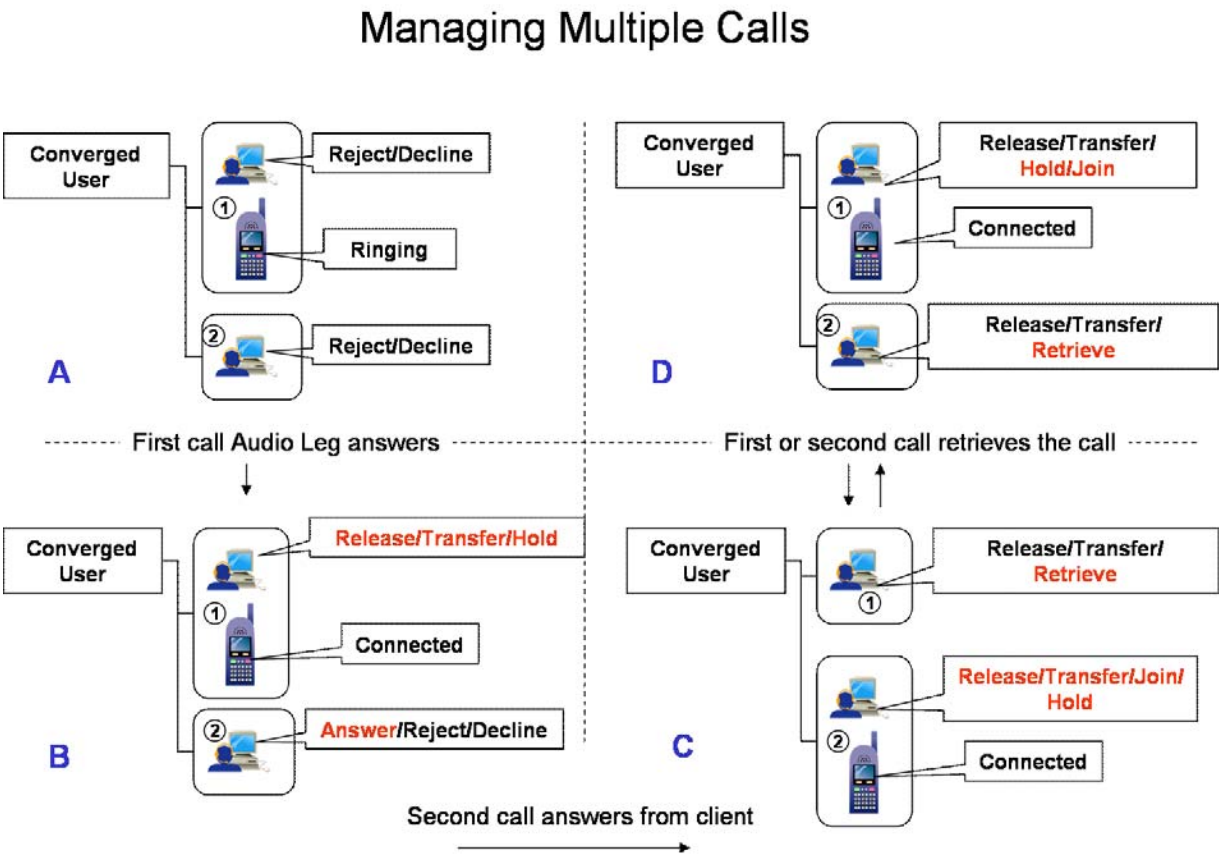
Multimedia capabilities available between MCS SIP clients	
Picture Calling Line Id	Shows a picture of the other party involved in the call
File Transfer	Allows the user to transfer files between MCS PC Client
White Board sharing	Allows the user to establish a White board collaboration session between MCS PC Client
Clip Board Transfer	Allows the user to send the 'clipboard' to another MCS PC Client
Web Co-browsing	Allows the user to push a web page to another MCS PC Client
Instant Messaging	Allows the user to establish SIP Instant Message session between MCS PC Clients
Presence state indications	The presence state of the MCD PC Client is monitored, while the state of the MCD Mobile (PAD) is not. On-the-phone presence is not supported.

138.2.5 MCD Multimedia PC Client with Multiple Calls

This feature introduces new behavior in the MCD PC Client to assist managing multiple established calls and call waiting scenarios. The MCD PC Client uses the PAD as the only audio device and therefore can only support one active voice conversation while the remaining established calls are placed on hold. Thus, the MCD PC Client now provides an interface to juggle several calls on behalf of the PAD.

An illustration summarizing multi-call PC Client behavior is shown in Figure 9. Each quadrant represents a scenario with two calls. The PAD is indicated by the mobile phone icon, and the features available to each call leg are shown in a box next to each.

Figure 9 Managing Multiple Calls



The quadrant labeled ‘A’ illustrates two incoming calls coming into the MCD PC Client, and the PAD has not yet answered. The PAD is ringing for the first inbound call attempt, and is therefore grouped together with the first call leg.

Just as the PAD answers, the transition to quadrant ‘B’ occurs. With the audio stream now established to the PAD, the MCD PC Client GUI is updated to reflect the functionality available to the converged user. The first call leg is associated to the PAD, and can now Hold, Release or Transfer the call from the MCD PC Client. The second call continues to ring, but the call can now be answered from the MCD PC Client. These new options are indicated in the figure with an orange color.

Assuming the second call leg is answered from the MCD PC Client, the transition to quadrant ‘C’ occurs. If the first call leg is not already on hold, upon answer the MCD PC Client will automatically place the first call leg on local hold. The MCS Session Manager will then exchange the audio stream to establish voice-path on the second call leg. Since the audio stream at the PAD is now established on the second call leg, the PAD is re-grouped to the second call leg in the figure. With multiple calls now active, the PC Client offers the

ability to establish a conference by introducing the ‘Join’ button on the established (PAD) call leg. If the user creates such a conference, all active call legs will reduce to a single call leg to the conference server (not shown). Additionally, the user may (direct) transfer this call from MCD PC Client to an alternate address.

The user can alternate between locally held calls from the MCD PC Client. The transition to quadrant ‘D’ indicates this behavior at the client. The MCS Session Manager will exchange the audio stream to the PAD to associate the single established call, while the remaining calls will be placed on local hold. At any time the converged user can ‘Join’ the calls into a single conference.

138.2.5.1 Call Waiting

Call waiting is the ability to present incoming calls while already engaged in a conversation. This section discusses how the subscriber can handle these subsequent calls. When a subsequent call is presented to the PC client, the available options are ‘Answer’, 'Ignore', 'Decline' or 'Reply with IM'. These options are similar to those presented on the initial call with the exception of the ability to answer the new call. The screenshot in Figure 10 illustrates these options.

Figure 10 Second inbound call to MCD PC Client

Audio options are similar to the pending call behavior as described in 138.2.4.1 Call Window Before Answer. There is no modification of the active CD Mobile (PAD) call leg.

If the subscriber chooses to answer the new call, the initial call is automatically placed on local hold by the MCD PC Client, and the audio will be established between the CD mobile and the new caller.

138.2.5.2 Joining Multiple Established Calls into Conference

When a subscriber already has an active call in progress and multiple calls on local hold, the converged PC client offers the ability to join these calls into conference. That is, the ‘Conference’ button will transition to a ‘Join’ button when multiple simultaneous calls are present. Note the ‘Join’ button in the active call GUI as shown in Figure 11.

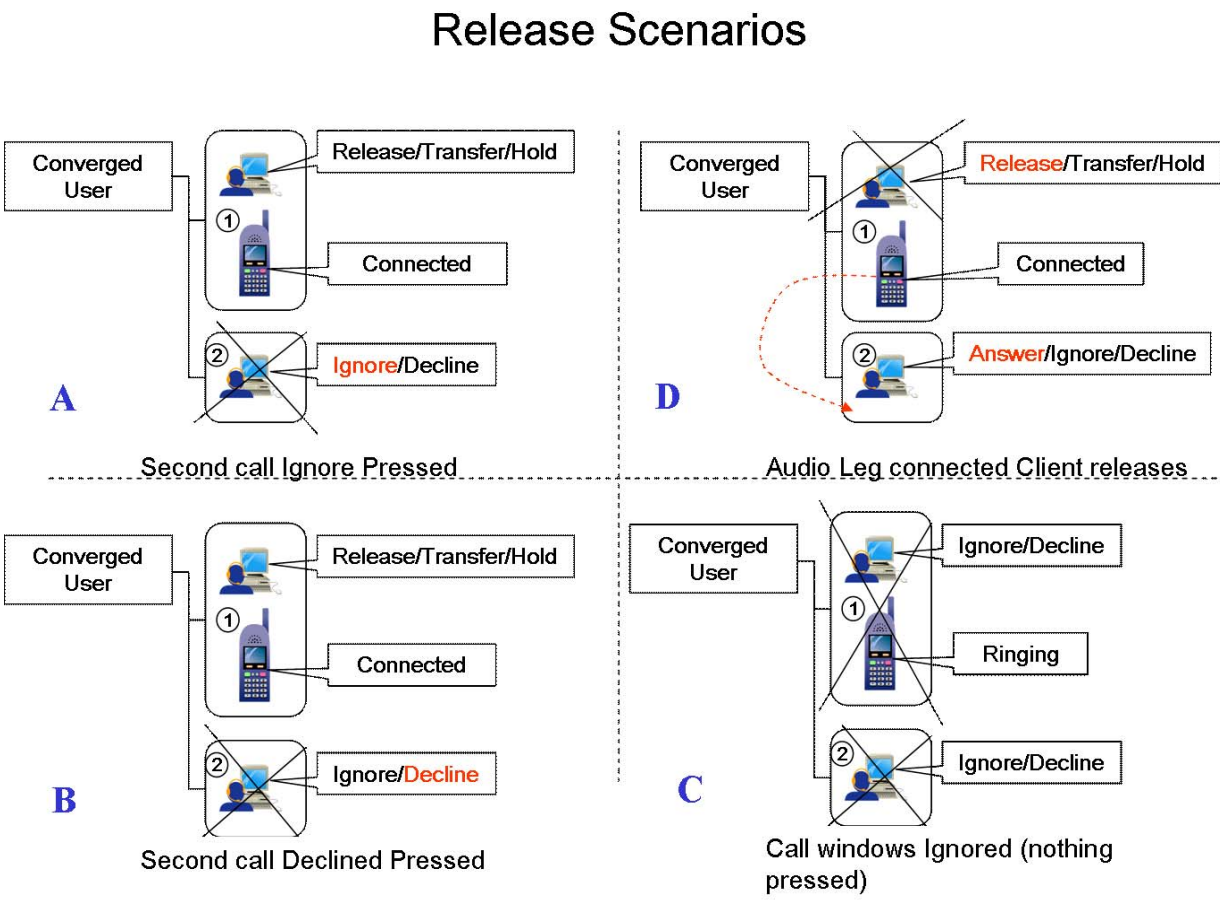
Figure 11 Active Call

If the subscriber joins the calls into an audio conference, all the call dialogs will reduce to a single call dialog to ‘Conference’. A maximum number of simultaneous calls are enforced on the MCS application server during call processing with the exception that the conference leg does not count against the maximum call limit while joining calls into a conference.

138.2.6 MCD Multimedia PC Client Release

This section considers the MPC Client behavior when calls are released. An illustration summarizing multi-call MPC Client release behavior is shown in Figure 12. Each quadrant represents a scenario with two calls. The PAD is indicated by the mobile phone icon, and the features available to each call leg are shown in a box next to each.

Figure 12 Release scenarios



The quadrant ‘A’ illustrates the scenario when a call is already established on the PAD and a subsequent call attempt is pending. The subscriber then chooses to ignore the second incoming call by clicking the ‘Ignore’ button. The Ignore function on the application server allows remaining terminating services to be executed, such as CPL. However, in the absence of CPL, the ignore will result in releasing the call attempt on the mobile network. The call released may not be forwarded to voicemail on the mobile network. For signaling details of this call processing scenario please refer to 20.3.4.2 Call Ignore from MCD PC Client.

Similarly, quadrant ‘B’ illustrates a subsequent pending call attempt. However, in this scenario the subscriber chooses to decline the call by clicking the ‘Decline’ button on the call window. The decline function on the application server does not allow remaining terminating services to run, and the call is immediately released. The call released may be forwarded to voicemail on the mobile network. For signaling details of this call processing scenario please refer to 20.3.4.2 Call Ignore from MCD PC Client.

The scenario shown in quadrant ‘C’ is a simple one, yet its significance can not be overlooked. The scenario involves two pending call attempts where the subscriber chooses to not press any buttons. Perhaps the subscriber is not physically at the PC Client at the time these call attempts are being made. Regardless, a couple of important topics to consider here are call timers and forwarding to voicemail. Typically a call attempt timer would expire (e.g. ISUP timer T9) and release the call with cause. The MCS application server will implement a timer to release these ignored call attempts with a cause. The mobile network may execute additional terminating services to handle the release with cause. For example, forward these unanswered calls to a voicemail system in the mobile network.

The release scenario in quadrant ‘D’ illustrates PC client behavior when the PAD leg is released while another pending call attempt is presented. When the user clicks the ‘Hang Up’ or ‘Stop’ button on the active call window the first call will be released, and the PAD would then be associated to the second call. However, the voice path would not be established until the ‘Answer’ button is pressed on the second pending call window

138.2.7 Direct Call Transfer

The MCD PC Client can perform a direct call transfer once the call is answered on the CD mobile. As part of the call transfer operation the PC client will automatically put the callers on local hold before transferring to the target party. The consult transfer functionality is not supported in this release.

138.2.8 Conference Calls

Only after an initial call is established can the MCD PC Client initiate a conference call and join multiple calls into a conference. Pending calls can not be joined into conference.

138.2.9 Hold / Retrieve

The MCD PC client control window provides the ability to initiate a hold for the call should that call be active, conversely a retrieve option (same button) is available should the call already be on hold.

The client will instigate the holding of the active call leg by means of a SIP INVITE to the Application Server with an SDP containing the following headers:

`c=`**`0.0.0.0`**`, specifying 0.0.0.0 as the IP address for the audio connection`

`m= audio 50010 RTP/AVP` **`0`** `8 18 110 111, specifying 0 as the port for the audio connection`

A held leg can then be subsequently retrieved by the client again sending a SIP INVITE but with a valid c= line. This will cause the Application Server to re-bridge the media via use of re-INVITEs.

If the MCD subscriber has 'music on hold' in their service package then this feature will apply as appropriate in call hold scenarios.

138.2.10 Call Logs

Call logs provide the subscriber with a record of all incoming and outgoing calls. The PC Client will locally manage these call logs, as opposed to Network Call Logs (NCL) feature which resides on the Personal Agent. Calls may be originated from the call logs and will behave as described in 138.2.3.1 MCD PC Client Origination / Click-to-call.

138.2.10.1 Inbox

Inbound call attempts are recorded in the Inbox. The ability to successfully re-dial a caller from this call log depends on the calling line id provided by the adjacent switch (CS2K). The prefix (CRD) introduced in this feature will automatically be prefixed to the outgoing address to assist in routing.

138.2.10.2 Outbox

Only outbound call attempts made from the MCD PC Client are recorded in this Outbox. Outbound call originations from the PAD will not be recorded in this log (or the NCL).

138.2.11 Client Unavailable / Calls of Grace

Previous sections have described the PC Client behavior when both the converged PC Client and the converged Mobile are actively available and how the feature is then utilized. This section will focus on the feature behavior when the client is unavailable or transitions between available and unavailable. In this context ‘unavailable’ would mean the client is non-accessible due to network isolation or simply unregistered. In addition, the concept of the ‘call of grace’ will be presented, along with how these calls are handled on the application server.

Let us begin with a couple of simple scenarios. One simple scenario occurs when the subscriber is not logged in on a PC Client and the CD Mobile is available. Then mobile calls will continue to be routed back to the mobile network, where mobile terminating services may execute. Another simple scenario is when the CD Mobile is unavailable (maybe out-of-area or turned off) and the PC Client is registered. The PC Client does not have audio capabilities, and the PAD leg will not be established. These are the trivial cases not only because they involve only an initial call, but also because part of the converged client was unavailable.

More complicated scenarios can be constructed when the client transitions between active and inactive. Recall, for this feature the mobile network is configured to route calls to the MCS5200 by triggering service logic in the SCP. Thus, terminating services will be executed at the application server before being processed in the mobile network. This introduces the possibility of latency during call setup. To address this, the application server implements

a mechanism of detecting the PC client network connectivity and minimizing call latency. That is, all calls will be presented to the converged PC client via a SIP INVITE. In order to provide a consistent interface between the application server and the PC Client, irrespective of whether this is a new call or a subsequent call in a multi-call scenario, the client will auto-answer all initial INVITE requests received. This does not mean that the client has indicated that call should be answered; it simply means that the client has initiated a control window for this session and is ready for further instruction from the Application Server. The auto-answer approach simplifies the notification of the client when an initial call has been answered at the MCD mobile, and makes the detection of an isolated client far faster. The detection of an isolated client is faster since the Application Server will shorten the number of re-transmissions of the INVITE to four attempts (equaling 4 seconds) as the client should be auto-generating a 100 Trying provisional response followed by a final 200 OK response if available. The 100 Trying is the first response received by the Application Server to the INVITE and, in effect, indicates the client active and triggers the Application to cease retransmission of the INVITE request. The following examples discuss this behavior.

For example, it is possible for the PC Client to login after a non-CD call has already been established on the CD Mobile. Further assume subsequent call attempts to the converged subscriber occur. When the application server executes this feature as part of its terminating services, it will now present these subsequent calls to the newly registered PC client and create a new PAD leg. Thus, when the client is unregistered all call attempts will be directly presented to the CD Mobile. However, once the client is registered the application server must assume the client is available and attempt to present the call to the client (expecting the auto answer 200 OK from the client). The application server will process this as an initial call described in section 138.2.4 Call Termination Behavior.

Similarly, it is possible for the PC Client to become isolated after calls were established on the CD mobile. Further assume a subsequent call attempt to the converged mobile occurs. Since the MCS application server is aware of the initial established call, the application server does not modify the voice path until after the user clicks ‘Answer’ on the PC Client. The application server assumes the client is accessible and will transmit an INVITE expecting an auto-answer from the client. However, in this case the timer expires after four seconds, and only then does the application server route the call back to the mobile network. Once the application server detects the client is isolated (with established calls), an internal flag is set to store this isolated status. This flag is later observed when subsequent call attempts occur. When subsequent calls attempts occur and the client has previously been detected as isolated, most of these subsequent calls will be directly routed back to the mobile network to avoid the extra four second latency.

For the scenario when the application server has already detected an isolated client, the application server can be engineered to present one of every N subsequent call attempts to the PC client. These calls-of-grace will be presented to the PC client to test the client network connectivity. If the client network connectivity is restored, the multi-call behavior will resume as described in section 138.2.5 MCD Multimedia PC Client with Multiple Calls. The term call-of-grace refers to the scenario when the MCS application server presents a call to the PC Client even when the status of the MCD PC Client is assumed to be isolated. In this context, that one call attempt of N is considered a call-of-grace. The call-of-grace may involve longer call setup latency when the client remains isolated. The value of N is configured through the System Management Console as shown in section 138.2.12.7.1 CallOFGraceInterval. It must be a positive number (default=5), where N=0 deactivates these call-of-grace attempts.

When the MCD PC Client is registered and used to terminate mobile calls, limitations may apply that enforce a maximum number of simultaneous calls supervised at the MCS application server. This limits the number of simultaneous calls that are placed on local hold, or joined into a single conference. The calls routed directly to the mobile network do not count against this maximum number of calls as they are being handled by the CD mobile directly. Incoming call attempts from the mobile network that exceed this threshold will be rejected on the MCS application server (SIP 486 Busy Here).

Call audits occur on the MCS application server to verify established calls are still valid and to provide a mechanism to detect and release network resources that appear stranded. If the call has a Mobile call leg associated to it, the call audit will be forwarded on to the CS2000. If the call does not have a mobile call leg associated and fails the call audit, the application server will release the call to free network resources.

138.2.12 System Configuration and Provisioning

138.2.12.1 Service Prefix Provisioning

As part of the proposed prefix numbering scheme, the operator has to provision the following numbers for each domain to be used by the wireless converged service.

Destination Prefix (CRD): This is the prefix that will be placed in front of the destination number for outgoing calls from the MCD client.

Audio Device Prefix (CRA): This is the prefix that will be placed in front of the destination number for click to call scenarios from the MCD client.

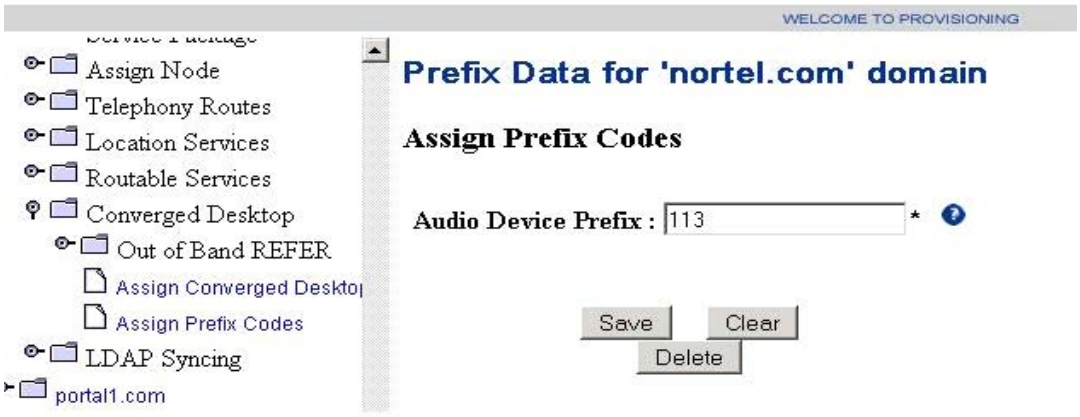
These numbers will be provisioned for each domain/sub-domain that will provide this service. The service on the MCS application server will

automatically insert these prefixes before translations are executed. Thus, it is important that the domain administrator has verified that translations do not exist that may conflict with this dial plan. If translations exist that match the CRA/CRD prefixed destination, calls may be misrouted.

138.2.12.1.1 Audio Device Prefix

A new option called “Assign Prefix Codes” will be added to the Converged Desktop Menu in the provisioning client to provision the audio device prefix.

Figure 13 Provisioning prefix codes



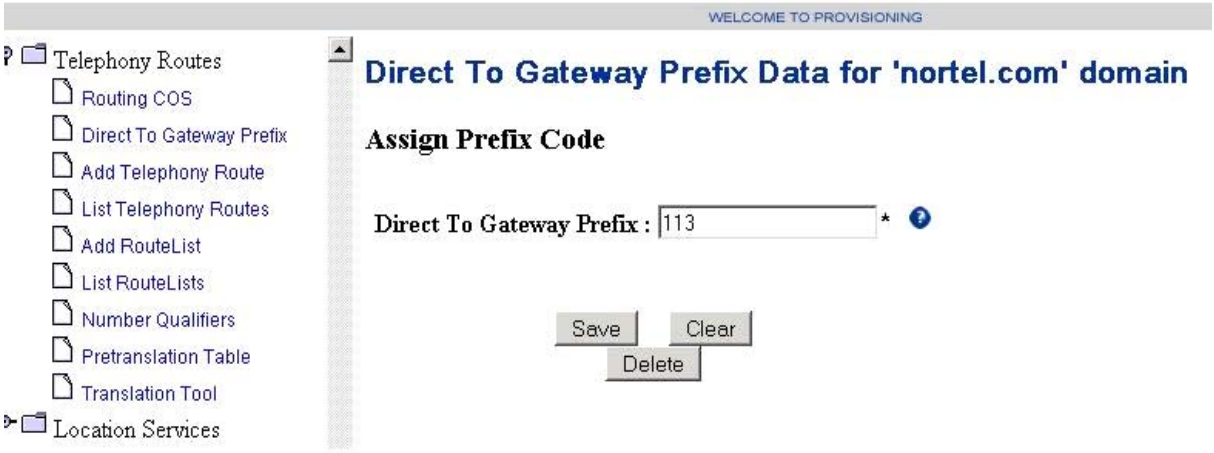
The following new methods will be added to the OPI interface to provision these prefixes. These methods will be added to the existing ConvergedDesktopServiceMgr interface.

```
/**
    * Adds the Prefix data for the mobile converged Service using the
Domain as the key
   * @param String domain, the domain to which the service data belong.
    * @param String domPrefixData, the new service data
   * @throws ProvisionException: This exception is thrown when an input
parameter is invalid,
    * a duplicate object exists in the data store, a dependency exists
in the data store or the data
    * store is not available.
    */
   public void assignDomainMCPrefixData(String domain, String
domPrefixData) throws ProvisionException;


   /**
```

```
    * Returns the domain prefix data for the mobile converged Service
using the Domain as the key

    * @param String domainID, the domain to which the service data
belong.

    * @param String domPrefixData, the new service data

   * @throws ProvisionException: This exception is thrown when an input
parameter is invalid,

    * a duplicate object exists in the data store, a dependency exists
in the data store or the data

    * store is not available.

    */

   public String getDomainMCPrefixData(String domain) throws
ProvisionException;

     /**

    * This method is used for removing prefix data associated with a
domain for the mobile converged service

    * @param String domain, domain from which the service data needs
to be removed.

   * @throws ProvisionException: This exception is thrown when an input
parameter is invalid,

    * a duplicate object exists in the data store, a dependency exists
in the data store or the data

    * store is not available.

    */

   public void removeDomainMCPrefixData(String domain) throws
ProvisionException;
```

138.2.12.1.2 Destination Prefix

A new option called “Direct To Gateway Prefix” will be added to the Telephony Routes menu in the provisioning client to provision the destination prefix or the direct to gateway prefix.



The following new methods will be added to the OPI interface to provision the direct to gateway or the destination prefix. These methods will be added to the existing TelephonyRouteMgr interface.

```
/**
    * This method is used to assign the DirectToGW service prefix data
to the domain
    * @param String domain, the domain name
    * @param String domPrefixData, the prefix data
    * @throws ProvisionException, if there was any problem retrieving
the
   *                        telephony Route information due to the data
   *                          store not being available or invalid data
    *                               being passed in
    **/
   public void assignDirectToGatewayPrefixData(String domain, String
domPrefixData) throws ProvisionException;
    /**
    * This method is used to get the DirectToGW service prefix data of
the domain
    * @param String domain, the domain name
    * @returns String domPrefixData, the prefix data
```

```
    * @throws ProvisionException, if there was any problem retrieving
the
   *                          telephony Route information due to the data
   *                            store not being available or invalid data
    *                                 being passed in
    **/
   public String getDirectToGWPrefixData(String domain) throws
ProvisionException;
    /**
   * This method is used to remove the DirectToGW service prefix data
of the domain
    * @param String domain, the domain name
    * @throws ProvisionException, if there was any problem retrieving
the
   *                          telephony Route information due to the data
   *                            store not being available or invalid data
    *                                 being passed in
    **/
```

138.2.12.2 Outbound Translations

This section provides an overview of the basic provisioning required on the MCS to route an outbound MCD PC Client originated call to the wireless network. Essentially two routes will need to be defined:

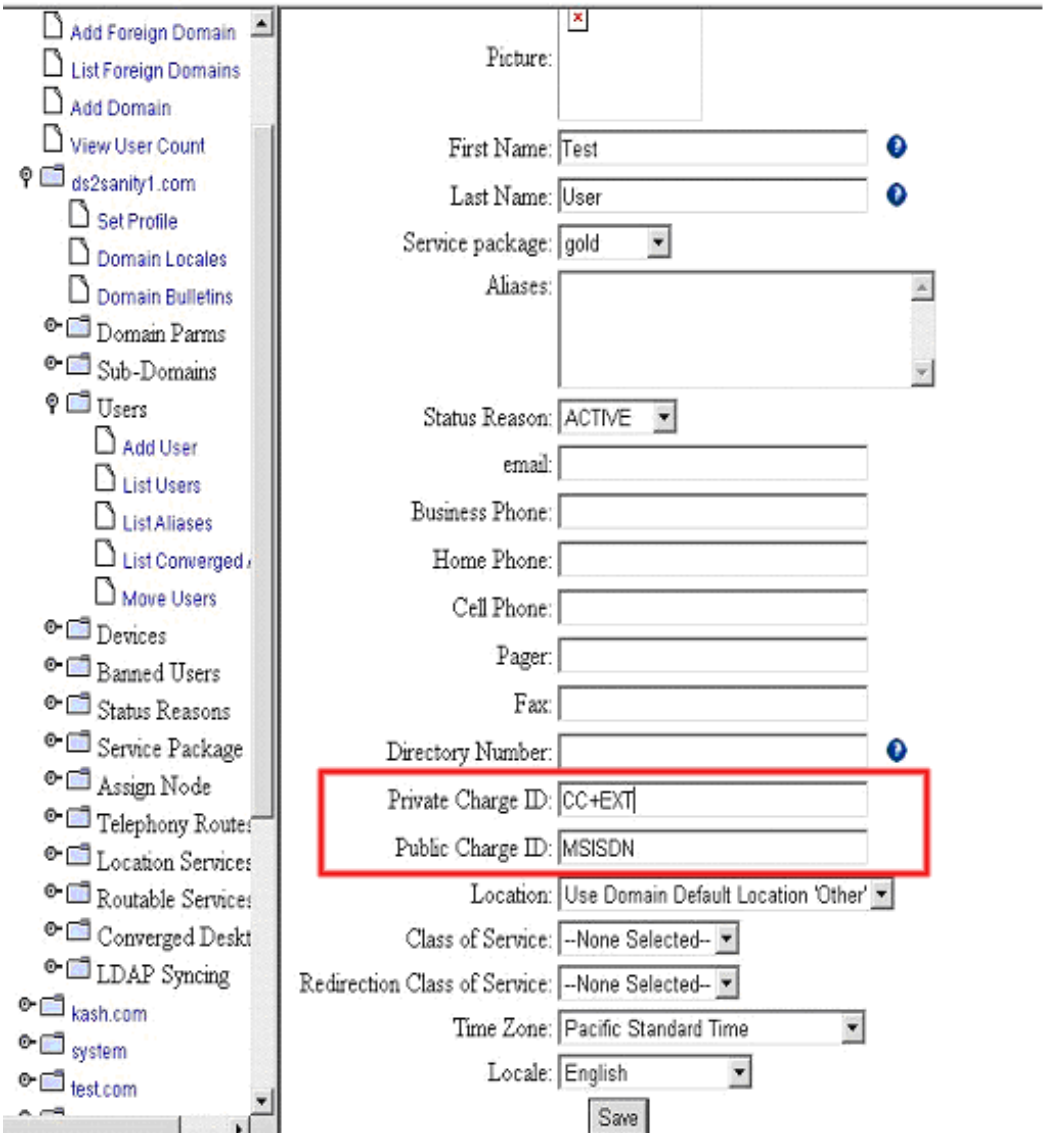
- Private route to the CS2000 – Used when signaling the destination mobile.
- Public route to the CS2000 – Used when signaling the CD Mobile (PAD).

The Mobile CD service will insert the prefixes automatically for the call. The routes are necessary for delivering the correct charge id (public/private) to the CS2000. The routes have to be based on the CRA/CRD values for each domain. A private route based on the CRD is required to send the private chargeid of the user i.e. CC+Ext as the calling party. A public route based on the CRA of the domain is required to send the public charge id of the user, i.e. MSISDN as the calling party.

The private and public charge ids for a user can be provisioned from the user details page in the provisioning client. From the above figure, the private charge id will be used when signaling the destination mobile and the public charge id will be used when signaling the CD mobile.

Provisioning screen shot of the user details page. The user's MSISDN should be provisioned as the public charge id and CC+Ext should be provisioned as the private charge id.

Figure 14 Provisioning subscriber charge IDs



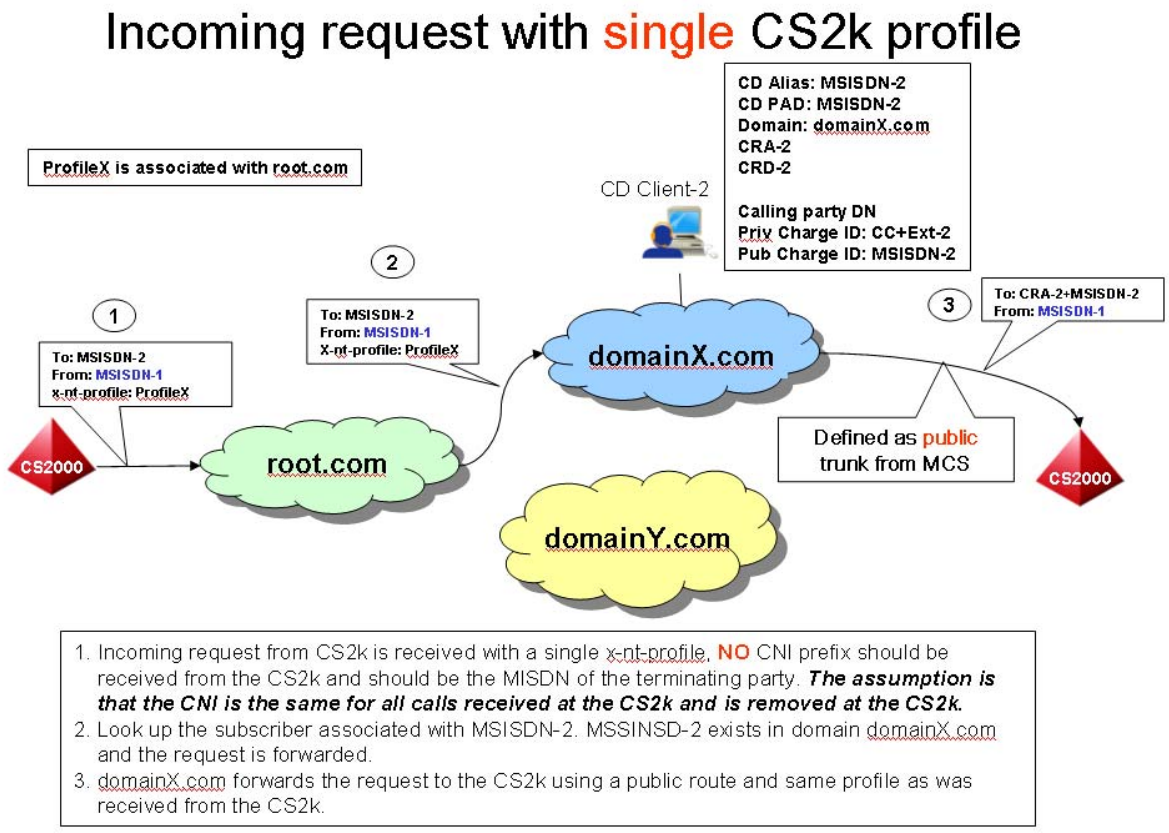
138.2.12.3 Inbound Translations

This section provides an overview of the basic provisioning required on the MCS to route an inbound call to a MCD subscriber.

138.2.12.3.1 Incoming Request with Single CS2K Profile

The following figure illustrates a call flow when there is only one CS2000 profile for all incoming requests. No translations are required in this case since the CNi is removed by the CS2K.

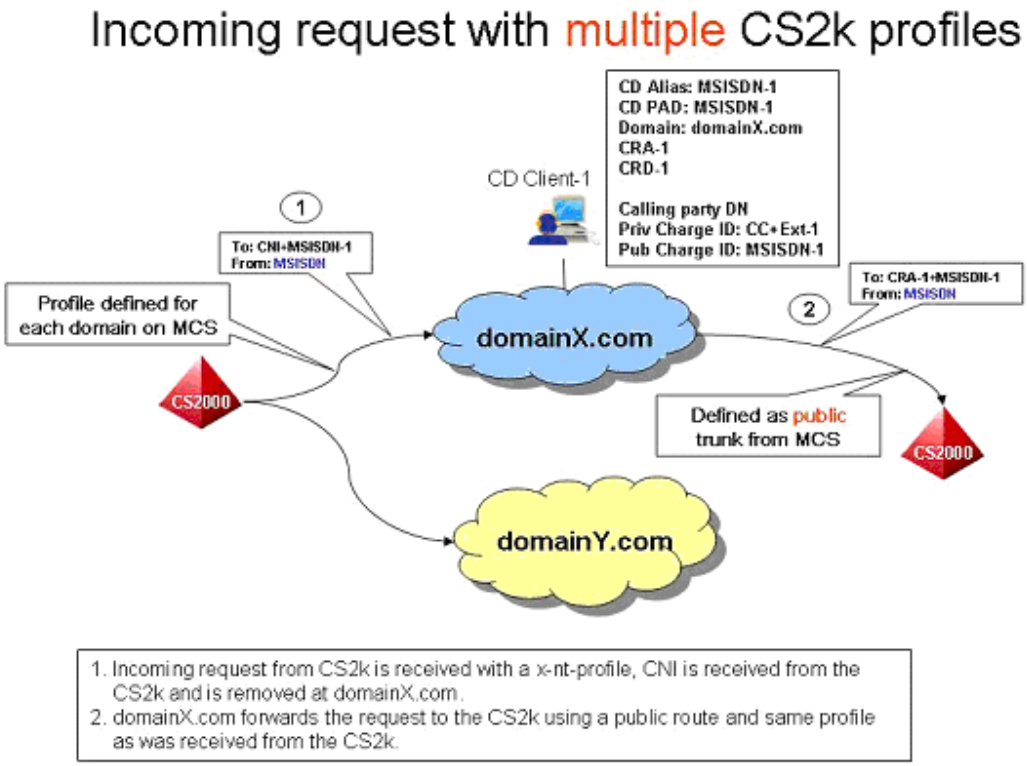
Figure 15 Incoming request with single CS2000 profile



138.2.12.3.2 Incoming Request with Multiple CS2K Profiles

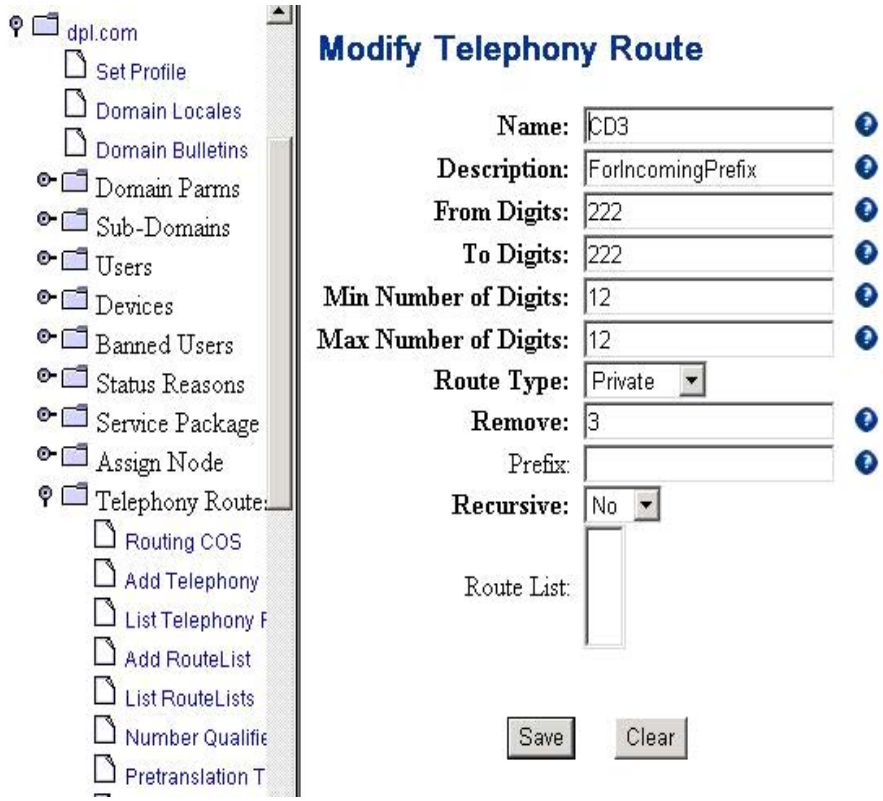
The following figure illustrates the call flow when the incoming requests have multiple CS2k profiles.

Figure 16 Incoming request with multiple CS2000 profiles



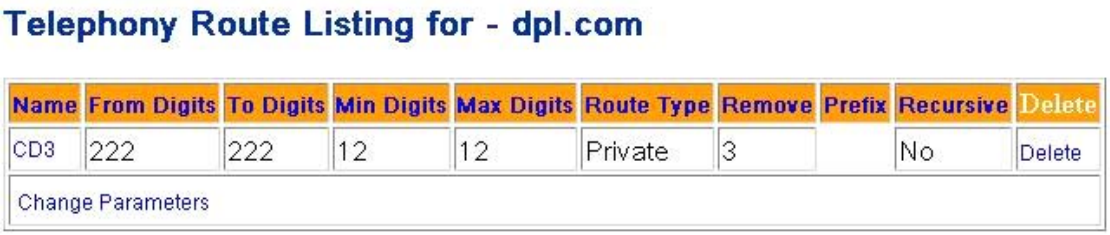
The administrator has to set up translations for each domain /sub-domain to strip the incoming prefix. For example, Figure 17 shows a route ‘CD3’ provisioned to remove the digits ‘222’.

Figure 17 Telephony route to strip CNi prefix



The following figure is the “List Telephony Routes” page from the provisioning client showing the route that was created to remove the incoming prefix (CNi).

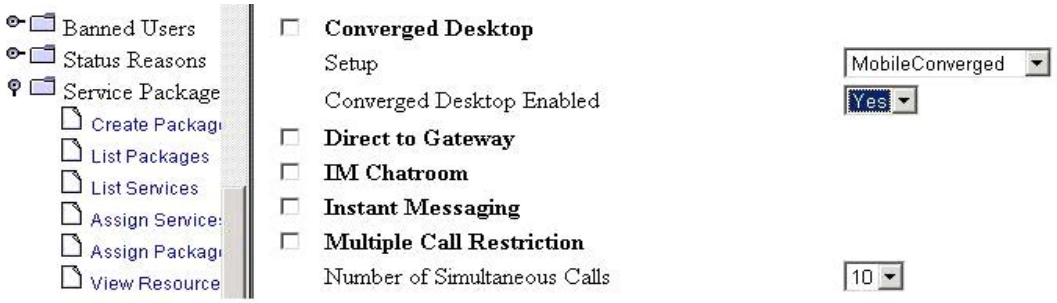
Figure 18 Listing of the telephony route



138.2.12.4 Service Package

A new option called “Mobile Converged” will be added to the Setup parameter of the Converged Desktop service. This option will be used to identify the users that will have this Mobile Converged service. In addition to that a new service called “Direct to Gateway” is introduced by this feature. This service defines if the calls have to be directed to a predefined gateway or not.

Figure 19 Provisioning the mobile converged desktop service



A new service called “Multiple Call Restriction” will be created. This service defines if the multiple call restriction should be enforced on the user or not. If enabled, the number of simultaneous calls that a user can have will be defined by the new parameter labeled “Maximum Number of Calls Allowed” that will be added to the “Multiple Calls Restriction” service. This will indicate the number of calls that the user can answer/hold. Min=1, Max=20, Default=10.

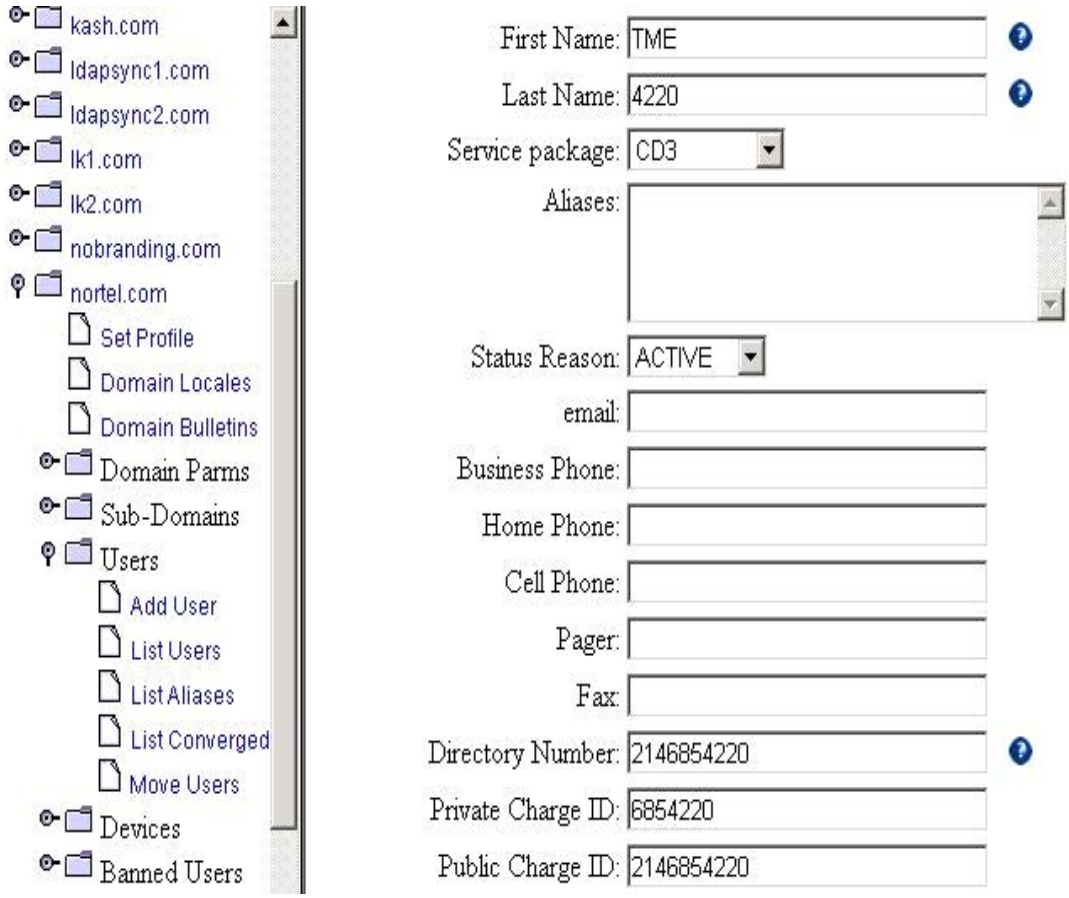
Figure 20 Provisioning Client screen shot for the new service parameter

Note: Refer to the Feature Interactions section for the list of supported and mutually exclusive services

138.2.12.5 Subscriber Provisioning

For users to be able to use this new service, the following information has to be provisioned. The user should be assigned to a service package that has the Converged Service which has the setup parameter of the service set to “Mobile Converged”.

The directory number (DN) field of the user is used to provision the user's MSISDN. The directory number of the user should be unique in the whole system. The directory number should be unique in the whole system. Provisioning rules will be in place which will make sure that the DN is unique in the whole system. Identifying a converged user without knowing the domain is necessary because converged calls that are routed from an existing switch to the MCP will always contain the same domain. This domain may or may not be the user's real domain. The following figure explains the page wherein the directory number can be provisioned for a user.



The audio device prefix (CRA) and the direct to gateway prefix (CRD) can optionally be provisioned at the user level to override the (sub) domain prefixes.

138.2.12.5.1 Audio Device Prefix

The audio device prefix can also be provisioned at the user level. This can be provisioned from the Converged Desktop Properties tab in the user details page. This will only be available to Mobile Converged users.

The following methods will be added to the existing ConvDesktopUserMgr OPI interface to be able provision this value from OPI.

```
/**
 * Adds the Prefix data for the mobile converged Service using the user as the key
 * @param String username, the user to which the service data belong.
 * @param String userPrefixData, the new service data
 * @throws ProvisionException: This exception is thrown when an input parameter is invalid,
 * a duplicate object exists in the data store, a dependency exists in the data store or the data
 * store is not available.
 */
public void assignUserMCPrefixData(String username, String userPrefixData) throws ProvisionException;


/**
 * Returns the user prefix data for the mobile converged Service using the username as the key
 * @param String username, the user to which the service data belong.
 * @param String userPrefixData, the user service data
 * @throws ProvisionException: This exception is thrown when an input parameter is invalid,
```

```
    * a duplicate object exists in the data store, a dependency exists
in the data store or the data
    * store is not available.
    */
```

public String getUserMCPrefixData(String username) throws ProvisionException;

```
     /**
    * This method is used for removing prefix data associated with a
user for the mobile converged service
    * @param String username, user from which the service data needs
to be removed.
   * @throws ProvisionException: This exception is thrown when an input
parameter is invalid,
    * a duplicate object exists in the data store, a dependency exists
in the data store or the data
    * store is not available.
    */
```

public void removeUserMCPrefixData(String username) throws ProvisionException;

138.2.12.5.2 Direct to Gateway Prefix

The direct to gateway prefix can also be provisioned at the user level. This can be provisioned from the new “Prefix Data” tab in the user details page. This will only be available to Mobile Converged users who have the “Direct to Gateway” service.

A new interface called “UserPrefixDataMgr” will be created to have the methods required to provision this value from OPI.

```
/**
    * Adds the Prefix data for the user using the username as the key
    * @param String username, the user to which the data belongs.
    * @param String userPrefixData, the new prefix data
   * @throws ProvisionException: This exception is thrown when an input
parameter is invalid,
    * a duplicate object exists in the data store, a dependency exists
in the data store or the data
    * store is not available.
    */
   public void assignUserDirectToGWPrefixData(String username, String
userPrefixData) throws ProvisionException;


   /**
    * Returns the prefix data for the user using the username as the key
   * @param String usernameD, the user to which the prefix data belongs
to.
    * @param String domPrefixData, the new service data
   * @throws ProvisionException: This exception is thrown when an input
parameter is invalid,
    * a duplicate object exists in the data store, a dependency exists
in the data store or the data
    * store is not available.
    */
   public String getUserDirectToGWPrefixData(String username) throws
ProvisionException;
     /**
   * This method is used for removing prefix data associated with a user
    * @param String username, the user for which the data needs to be
removed.
   * @throws ProvisionException: This exception is thrown when an input
parameter is invalid,
    * a duplicate object exists in the data store, a dependency exists
in the data store or the data
```

```
    * store is not available.
    */
   public void removeUserDirectToGWPrefixData(String username) throws
ProvisionException;
```

138.2.12.6 Open Provisioning Interface (OPI)

The following summarizes the OPI methods that will be exposed as part of this feature.

These commands will also be available from the BPT command line tool.

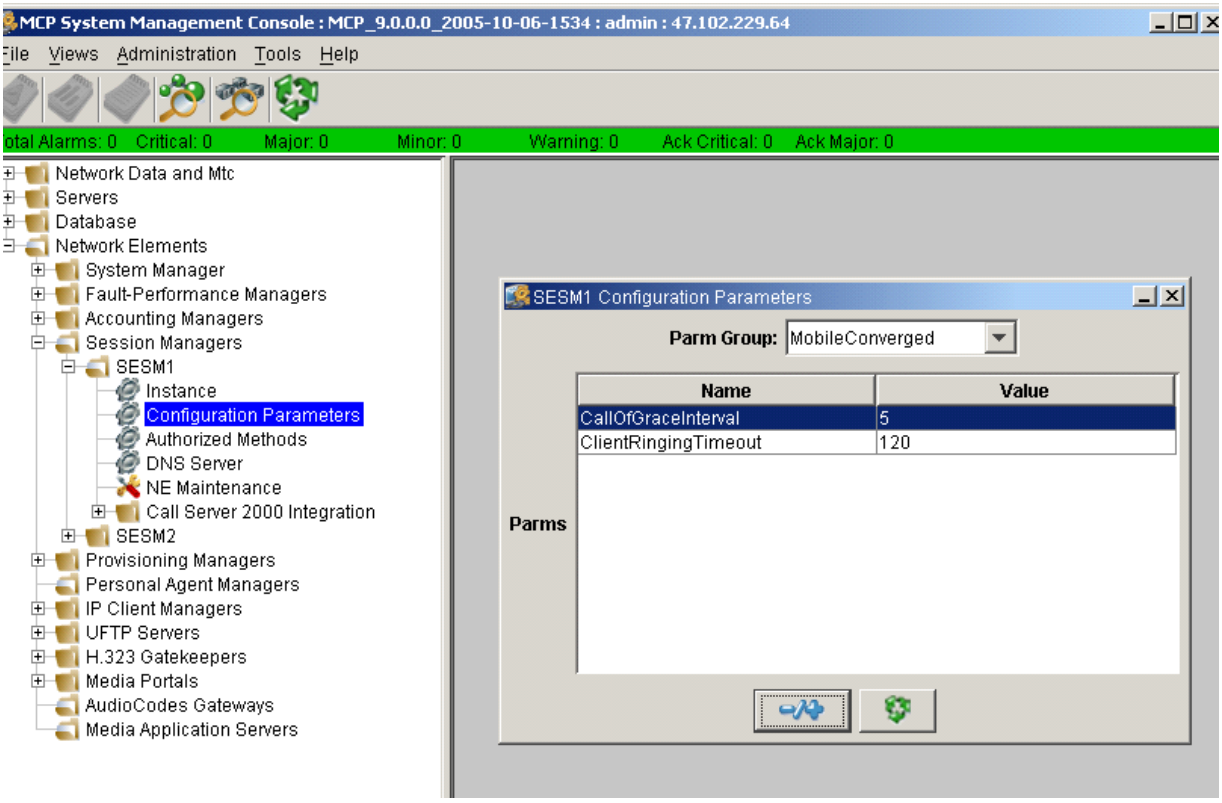
	Command	Parameter List
User Prefix	addMobileConvDesktopUserData	String username, MobileConvDesktopUserData userData
	getMobileConvDesktopUserData	String username
	removeMobileConvDesktopUserData	String username
Domain Prefix	addMobileConvDesktopDomainData	String domain, MobileConvDesktopDomainData domPrefixData
	getMobileConvDesktopDomainPrefixData	String domain
	removeMobileConvDesktopDomainPrefixData	String domain

138.2.12.7 System Configuration Parameters

Two new system parameters are available through the System Management Console GUI, the CallOfGraceInterval and ClientRingingTimeout. These parameters are both accessible through the System Management Console GUI and are provisioned for each Session Manager individually.

To access these parameters, click on the Configuration Parameters for a Session Manager and selecting the “Mobile Converged” Parm Group in the Configuration Parameters panel shown in the following figure.

Figure 21 Configuration Parameters Panel



138.2.12.7.1 CallOFGraceInterval

This parameter sets the call number interval the session manager will wait before attempting to present a subsequent call attempt to an MCD client after it has become “unavailable” as described in section “Client Unavailable / Calls of Grace” on page 1339.

138.2.12.7.2 RingingTimeout

This is a timer setting the number of seconds the session manager will allow an incoming call to a user currently registered on an MCD Client to remain ringing before bringing the call down. When this timer expires, a SIP BYE message is sent to the client to terminate the call leg to the MCD Client and a 480 Temporarily Unavailable sent to the originator to terminate the call and the call leg to the PAD is dropped.

138.3 Call Processing

This section details the call flow and supervision from the MCS network perspective.

138.3.1 Interfaces supported

The supported interface between the MCP and the existing switching system is Session Initiation Protocol (SIP).

138.3.2 Dial Plans

Two prefixes must be provisioned on the system for this feature. The CRD and CRA are defined again as follows:

- Destination Call Leg Return Code (CRD): This is an E.164 number that will prefix the (non CD) destination mobile number for outgoing calls from the MCD client to the mobile network.
- Associated Call Leg Return Code (CRA): This is an E.164 number that will prefix the CD mobile number (PAD). This prefix can be used to identify this call leg on the GSM network as a non-chargeable call.

The following sections discuss the usage of these prefixes for both terminating to a CD Mobile and originating from an MCD PC Client. Note that there is no section addressing conference calls since conference calls do not require establishing a new PSTN connection; thus, CDR and CDA prefixes are not required for joining the previously established calls into a conference.

138.3.2.1 Prefix usage for CD Mobile Terminations

The following table describes when the CRA is prefixed to a CD Mobile termination. The two scenarios considered are:

1. Call is received from another CD Mobile (row 1)
2. Call is received by non CD Mobile (row 2)

These rules also apply to ‘Advanced Routing’ (if provisioned) where the terminator has multiple destinations. For example, MSISDN-2 rings another CD mobile and then a non CD mobile. For both destinations the CRA needs to be added as described.

Figure 22 Prefix on CD Mobile Terminations

CD Mobile Terminations			
Originator	**Terminator**	**Called Number**	**Description**
CD Mobile (MSISDN-1) (CRA-1)	CD Mobile (MSISDN-2) (CRA-2)	CRA-2+MSISDN-2	CRA of the terminator is used in the called number here because the originator could be known, but not looked up at the MCS for CD Mobile to Mobile call.
Non - CD Mobile (MSISDN)	CD Mobile (MSISDN-2) (CRA-2)	CRA-2+MSISDN-2	CRA of the terminator is used here because the originator is unknown at the MCS.

138.3.2.2 Prefix usage for MCD PC Client Originations

The following table describes when the CRA and CRD are used when a client origination takes place to a

1. CD Mobile
2. Non CD Mobile
3. PSTN number

These rules also apply to ‘Advanced Routing’ (if provisioned) where the terminator has multiple destinations. For example, MSISDN-2 rings another CD mobile and then a non CD mobile. For both destinations the CRA/CRD needs to be added as described.

Figure 23 Prefix for Client Originations

MCD Client Origination / click-to-call				
Originator	**Terminator**	**CRA (Owner) First Leg (orig)**	**CRD (Owner) Second Leg (term)**	**Description**
CD Mobile (MSISDN-1) (CRA-1) (CRD-1)	CD Mobile (MSISDN-2) (CRA-2) (CRD-2)	CRA-1+MSISDN-1	CRD-1+MSISDN-2	CRA of the originator is used for the first and CRD of the originator is used in the terminating leg because it is a client origination.
CD Mobile (MSISDN-1) (CRA-1) (CRD-1)	CD Mobile (user ID) (MSISDN-2) (CRA-2) (CRD-2)	CRA-1+MSISDN-1	CRD-1+MSISDN-2	CRA of the originator is used for the first and CRD of the originator is used in the terminating leg because it is a client origination.
CD Mobile (MSISDN-1) (CRA-1) (CRD-1)	Non-CD Mobile (MSISDN)	CRA-1+MSISDN-1	CRD-1+MSISDN	CRA of the originator is used for the first and CRD of the originator is used in the terminating leg because it is a client origination.

138.3.2.3 Prefix Usage for Call Transfer

The following table describes when the CRA and CRD are used when a client transfers a call. The table below has a call setup between party A and B, then party B transfers the call to party C.

The rules need to also apply to ‘Advance Routing’ where the terminator has multiple destinations. For example, MSISDN-3 rings another CD mobile and

then a non CD mobile. For both destinations the CRD needs to be added as described. The same rules will apply if Party B forwards the request to Party C.

Figure 24 Prefix used for call transfer

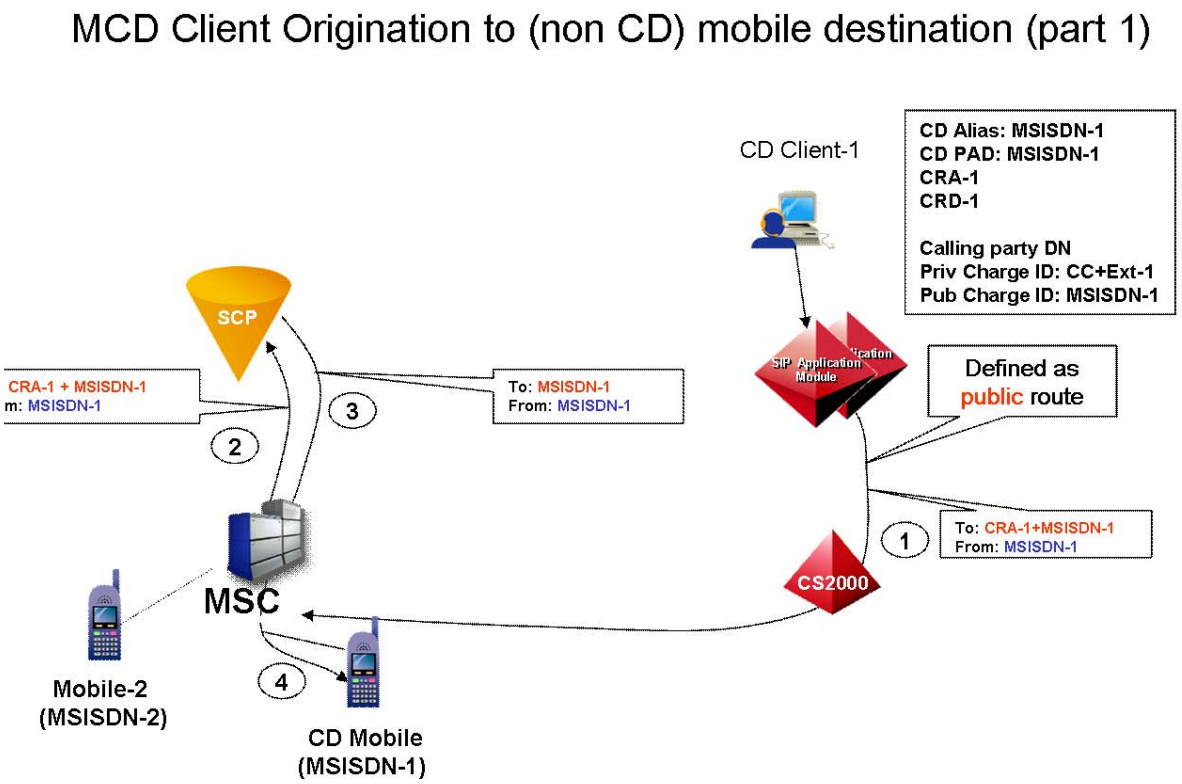
Call transfer					
Party A	**Party B (transferring party)**	**Party C (transfer party)**	**Calling Number sent to Party C**	**Called Number sent to Party C**	**Description**
CD Mobile (MSISDN-1) (CRA-1) (CRD-1)	CD Mobile (MSISDN-2) (CRA-2) (CRD-2)	CD Mobile (MSISDN-3) (CRA-3) (CRD-3)	(TBD)	CRD-2+MSISDN-3	CRD of the transferring party is used because party C is a known MCS user. This is similar to party B just originating a call to party C.
CD Mobile (MSISDN-1) (CRA-1) (CRD-1)	CD Mobile (user ID) (MSISDN-2) (CRA-2) (CRD-2)	Non-CD Mobile (MSISDN)	(TBD)	CRD-2+MSISDN	CRD of the transferring party is used because party C is a known MCS user. This is similar to party B just originating a call to party C.

138.3.3 MCD PC Client Originated Scenarios

The situation in which a converged user (MCD Client-1) makes a call to a mobile user (Mobile-2) from the MCD PC Client is discussed. Since the MCD PC Client does not provide the audio for the call, all originations from the PC client are click-to-call scenarios.

The Click-to-call scenario always involves two call legs. The first call is to the CD Mobile (MSISDN-1), and is illustrated in Figure 25.

Figure 25 Call origination from MCD PC Client (part 1)



Step 1: MCS Application Server attempts to establish the audio call with the MSISDN-1 by first prefixing with the originators CRA and routing to the CS2000. The CS2000 translates and sends ISUP IAM to the MSC of the mobile network.

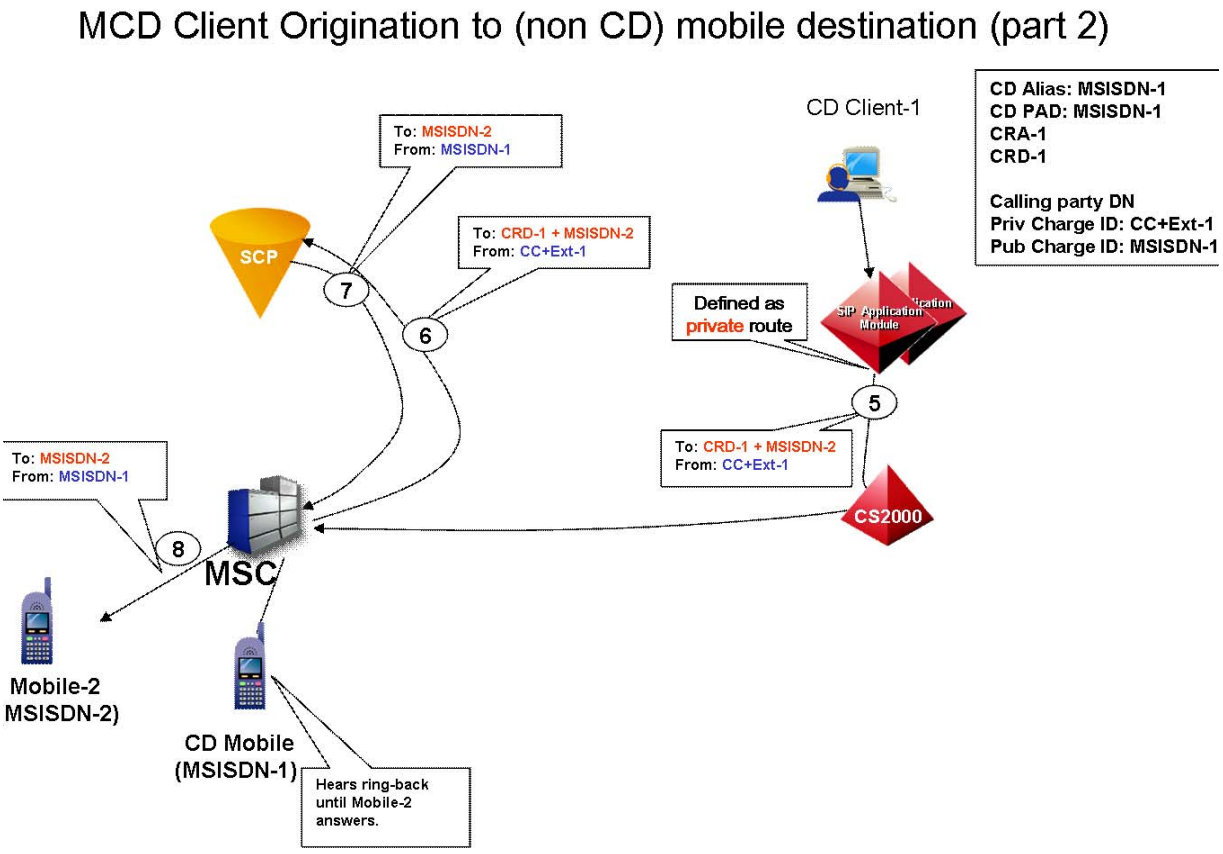
Step 2: The CRA+MSISDN-1 is presented to SCP for the originating leg.

Step 3: SCP removes CRA and sends the call to the CD Mobile (MSISDN-1). Note that the request is not sent back to MCS.

Step 4: The originator's mobile rings and originator answers the call.

The second half of the call attempts to establish the audio call with the non CD terminating Mobile-2. This scenario is illustrated below in Figure 26.

Figure 26 Call origination from MCD PC Client (part 2)



Step 5: The MCS application server sets up a call leg to the terminating mobile by prefixing the CRD of the originator to the terminators address (MSISDN-2). The ‘From’ is changed to the CC+Ext-1 of the originator.

Step 6: The MSC send the request to the SCP.

Step 7: SCP modifies the called and calling party to the actual MSISDN involved

Step 8: Request to MSC is sent to ring the terminating mobile.

The MCS Session Manager click-to-call call flow is slightly more complicated than described in the proceeding overview. The call flow from the perspective of the MCS Session Manager is shown in Figure 27. Most SIP signaling must go through the CS2000, thus the SESM executes internal REFER logic using Hold/Retrieve. Relevant aspects of the hold/retrieve are highlighted in the call flow.

Figure 27 MCD PC Client origination with ringback from far end

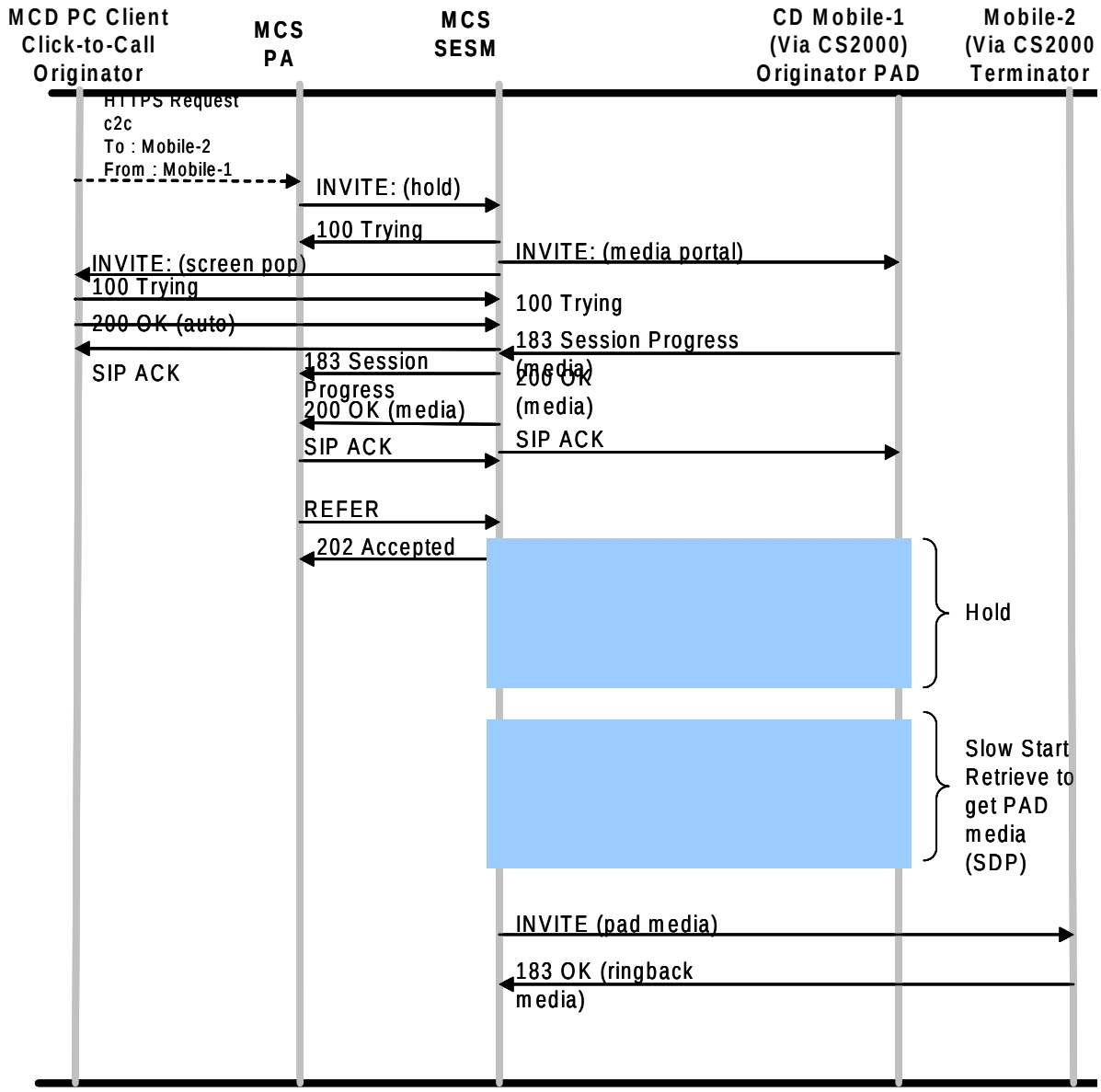
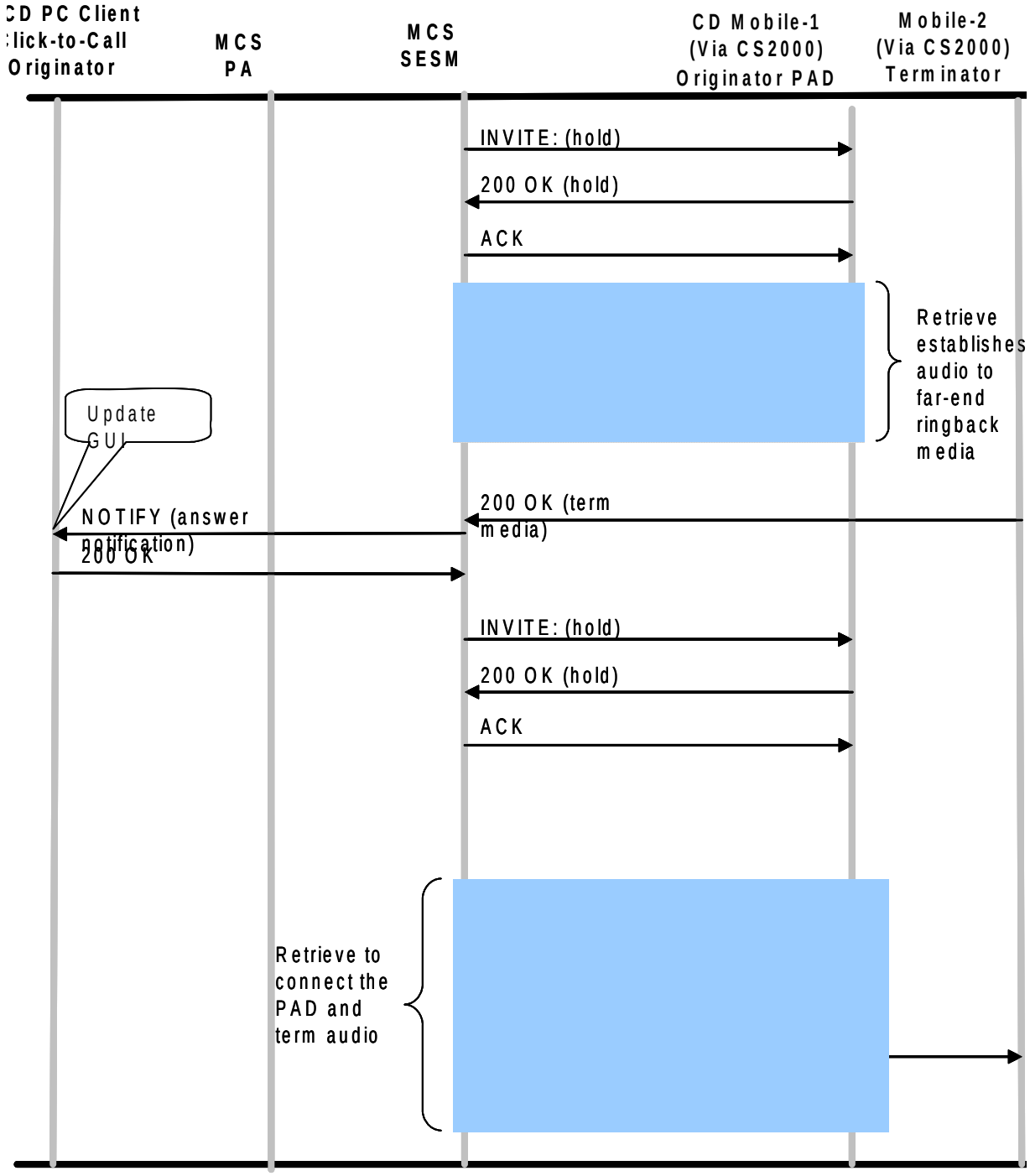


Figure 28 MCD PC Client origination with ringback from far end (cont.)



138.3.4 PAD Terminated Scenarios

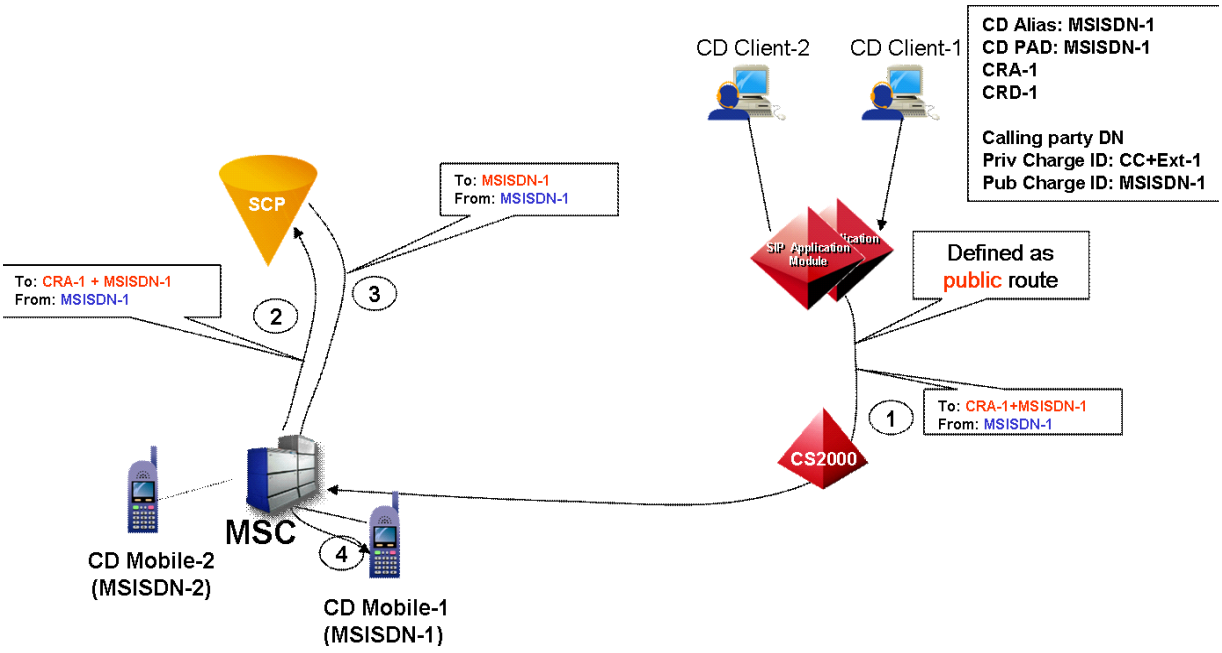
This section covers the termination scenario in which a converged subscriber (CD mobile-1) makes a call to a CD User (CD mobile-2). It also deals with

situations in which the inbound call is Ignored and Rejected from the MCD PC Client.

138.3.4.1 Call Answer on PAD

The basic termination to the converged users PAD is shown in Figure 28. In this scenario a converged wireless subscriber (CD Mobile-1) calls another converged wireless subscriber (CD Mobile-2).

Figure 29 CD call termination (part 1)



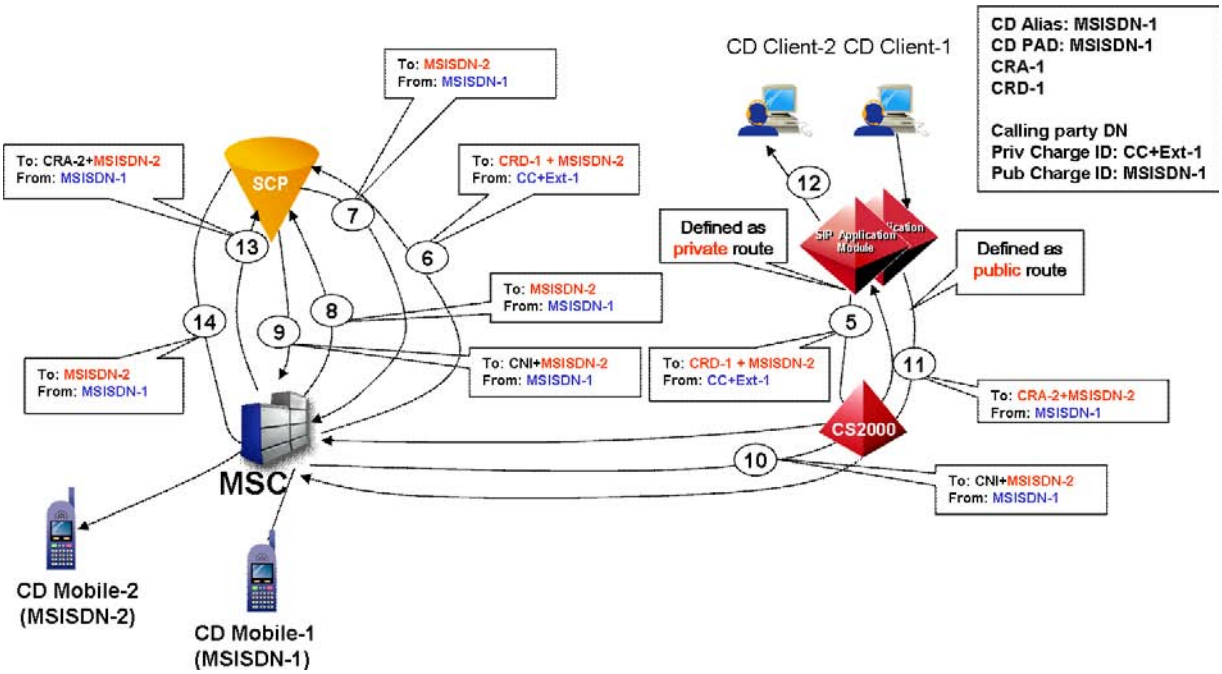
Step 1: First leg terminates to the CD mobile's own mobile device. Owner's CRA+MSISDN is the called and MSISIDN-1 is the calling party. CRA routing needs to use a public telephony route so public charge ID (MSISDN-1) is presented as the calling number.

Step 2: CRA+MSISDN-1 is presented to SCP for the originating leg

Step 3: SCP removes CRA and sends the call to the Mobile-1 which answers the call.

Step 4: The originator's mobile rings and the originator answers the call.

Figure 30 Call Termination (part 2)



Step 5: CRD of the originator is prefixed to the terminator's MSISDN and from party is changed to CC+Ext of the originator.

Step 6: The MSC sends the request to SCP.

Step 7: SCP modifies the called and calling party to the actual MSISDN involved.

Step 8: The MCS sends the request to the SCP again to add the CNI.

Step9: SCP prefixes the CNI to the terminating call

Step 10: Request received at the MCS with CNI (or without if CS2k removes it).

Step 11: MCS adds the CRA of the terminating party and routes the request to the MSC

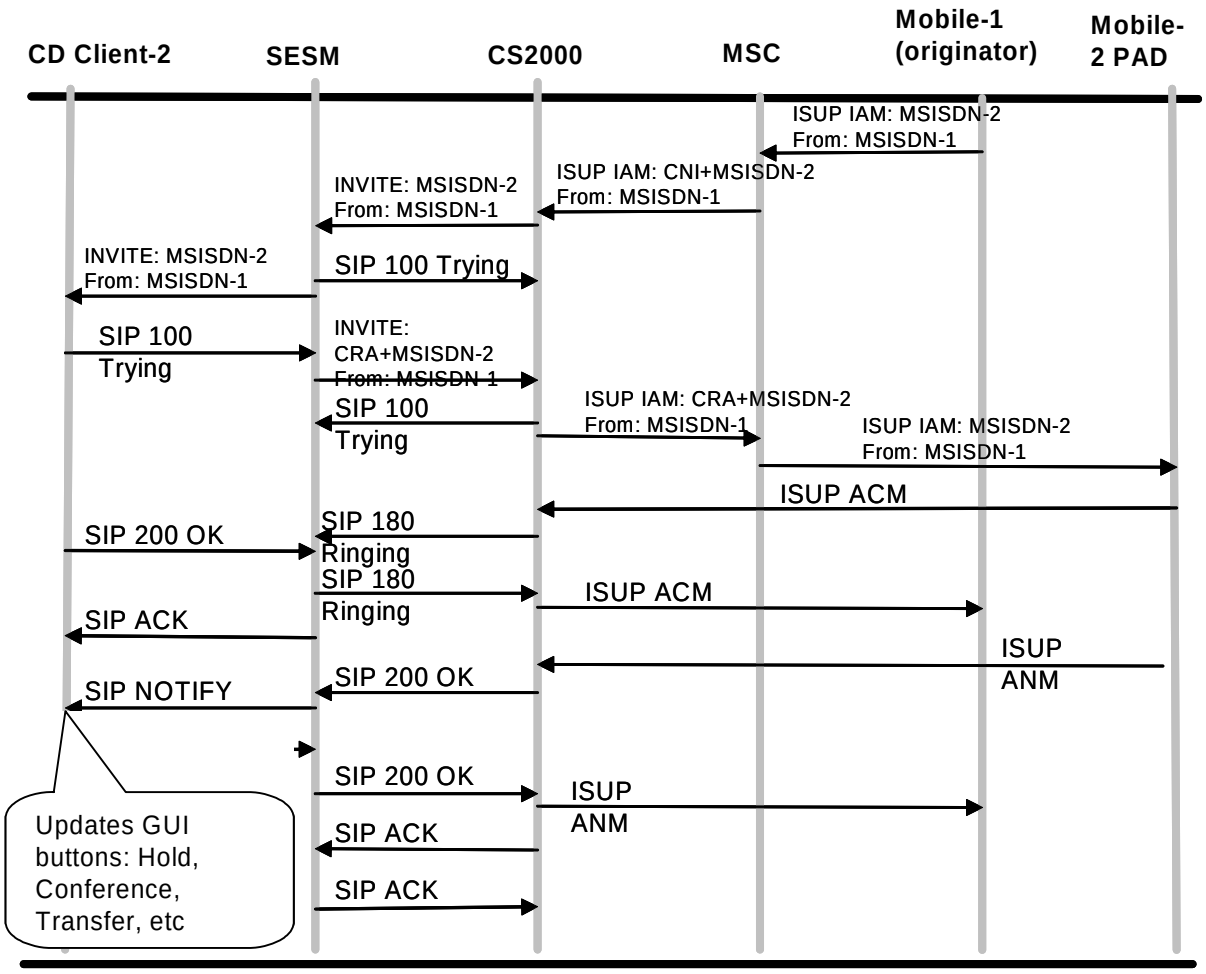
Step 12: CD Client-2 is presented with call.

Step 13: MSC sends the request to the SCP to remove the CRA.

Step 14: Request to MSC is sent to ring the terminating mobile.

The call flow from the perspective of the MCS Session Manager is shown below.

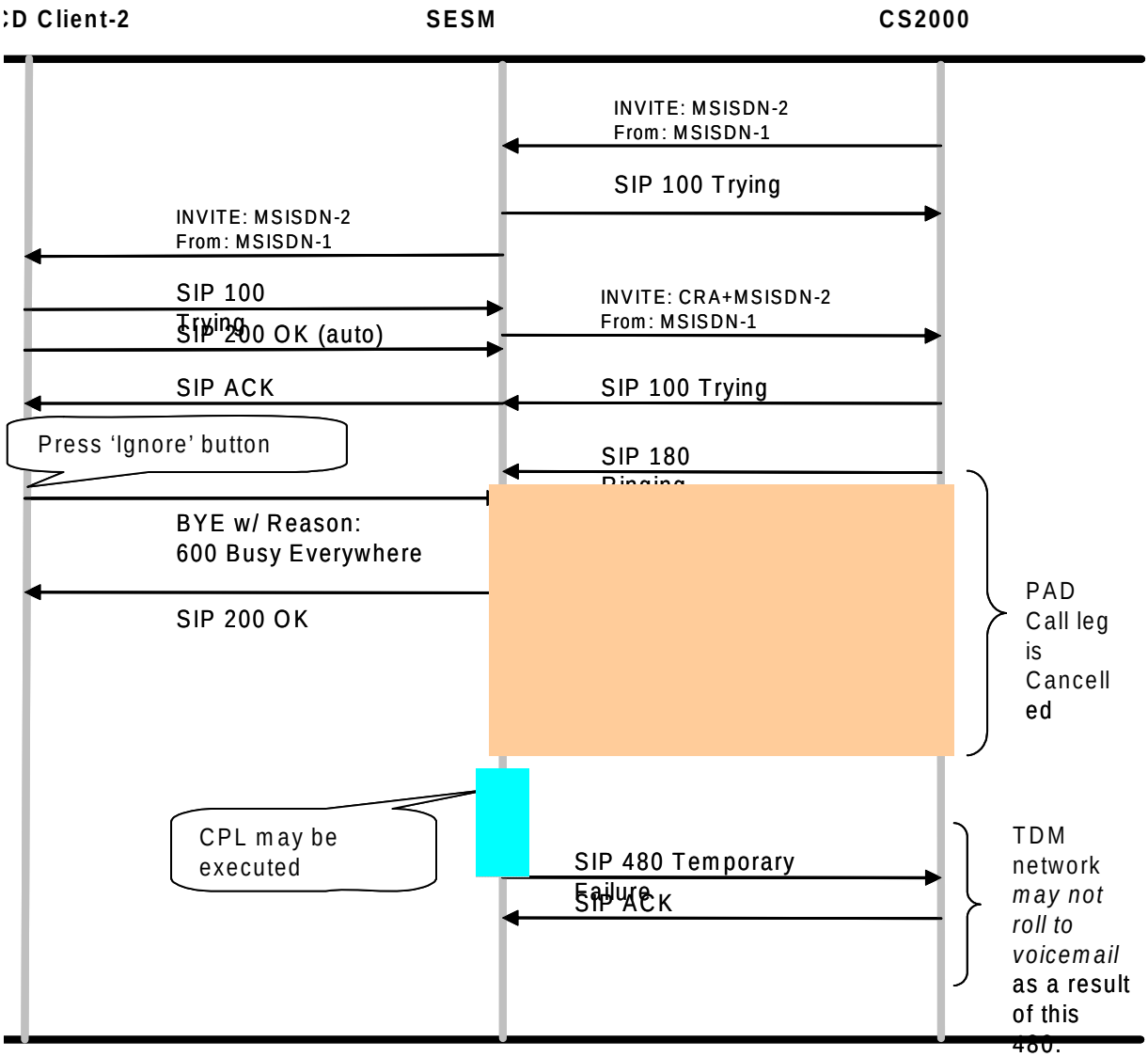
Figure 31 MCD PC Client termination



20.3.4.2 Call Ignore from MCD PC Client

Incoming calls to the MCD PC Client call be ignored. This will allow the SESM to execute any MCS CPL scripts (advanced routing) and/or roll to MCS voicemail. The call flow from the perspective of the MCS Session Manager is shown below.

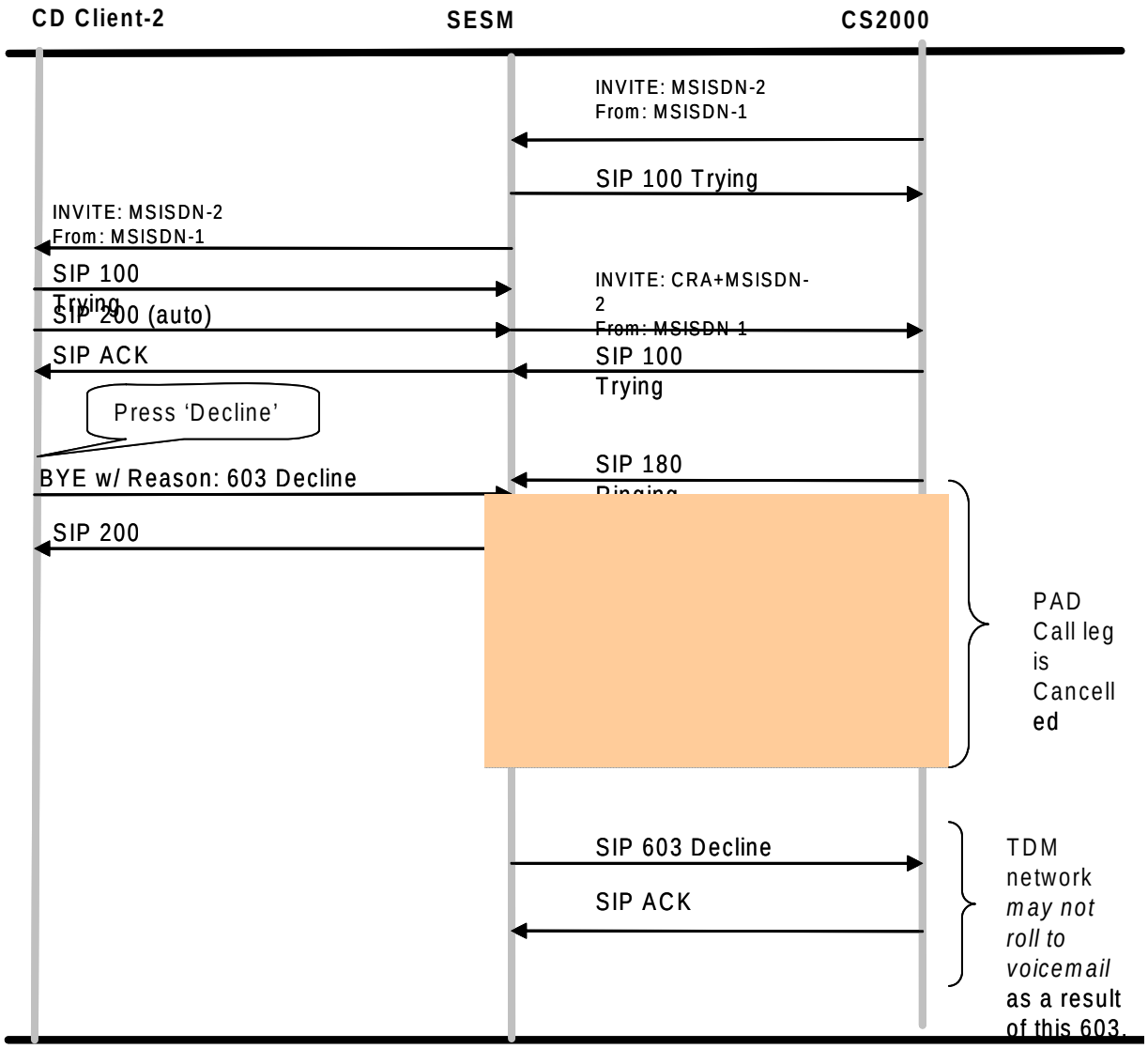
Figure 32 MCD PC Client Ignores inbound call (no CPL)



20.3.4.3 Call Decline (reject) from MCD PC Client

Incoming calls to the MCD PC Client call be rejected. The call flow from the perspective of the MCS Session Manager is shown below.

Figure 33 MCD PC Client Declines inbound call



20.3.5 Established Call Behavior

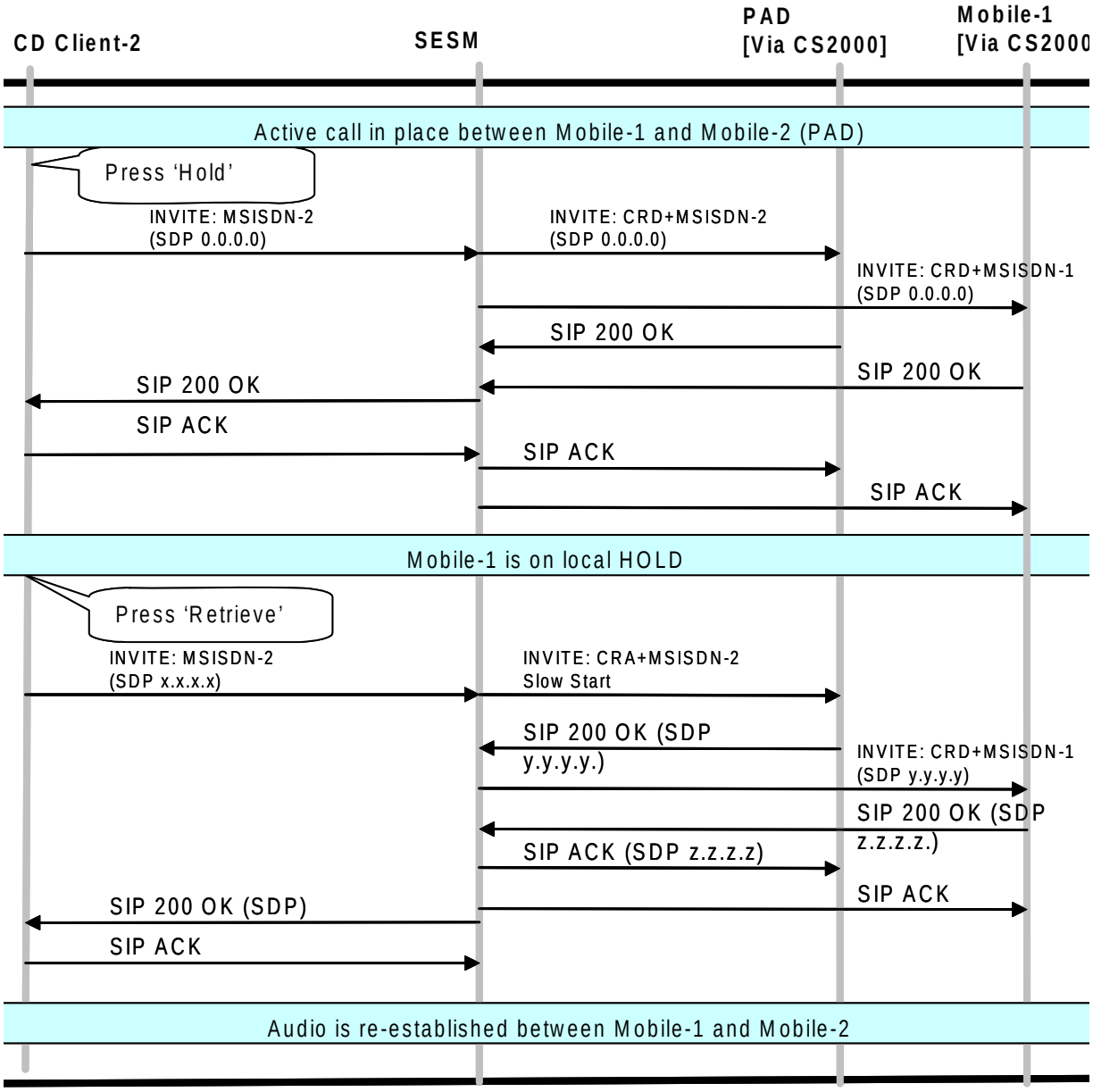
This section covers the situations in which a converged subscriber (mobile-1) already has an established call and additional mid-call features are being requested from the terminating MCD PC Client. Specifically, the scenarios presented are Hold / Retrieve, Conference, and Direct Transfer from the MCD PC Client.

20.3.5.1 Hold/Retrieve from MCD PC Client

The PC Client allows active calls to be placed on local hold by pressing the Hold button. This behavior is also invoked automatically if the client answers subsequent incoming calls. The call flow for the PC Client invoking local hold

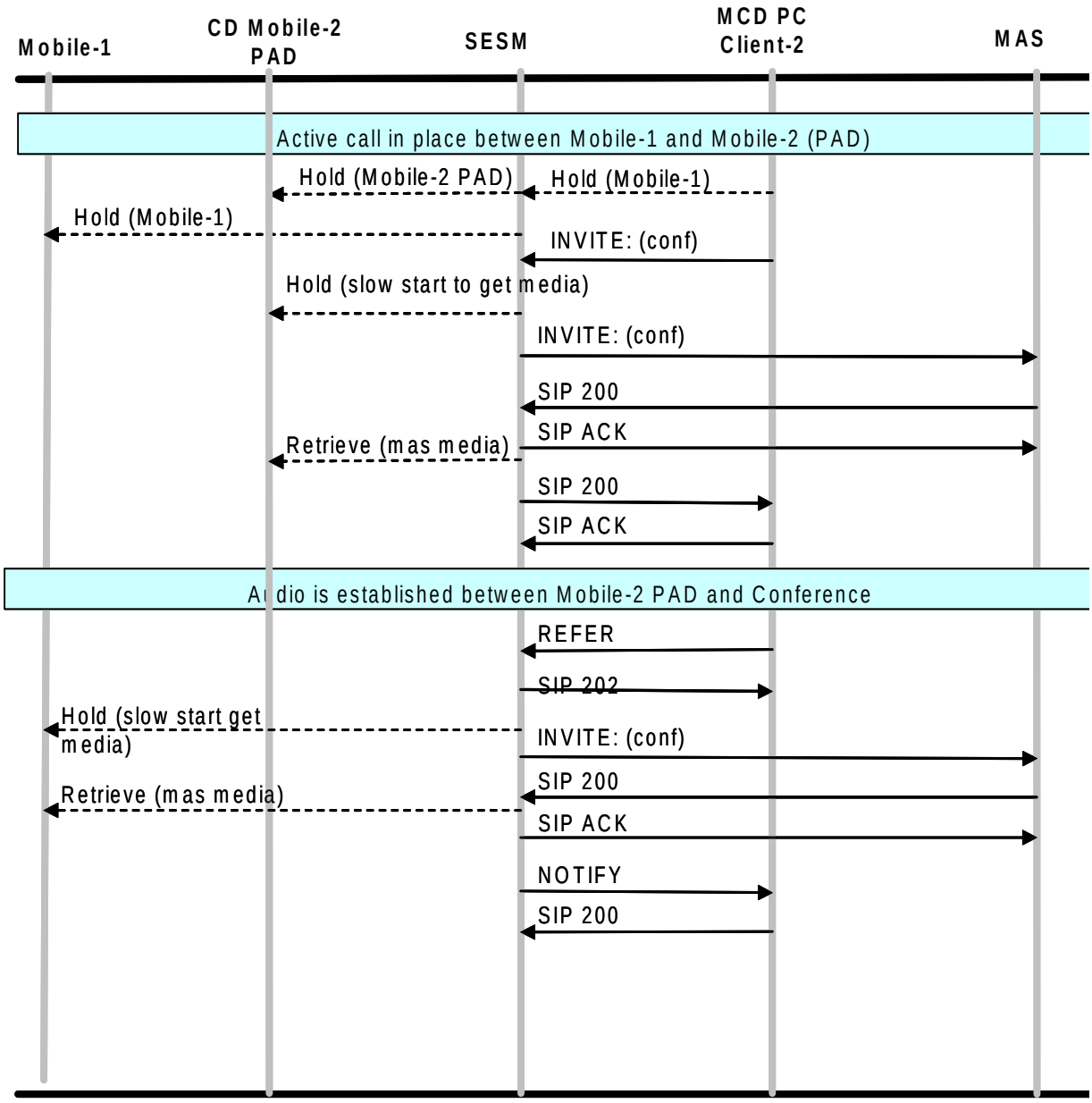
is as follows. (Note that call flows for hold and retrieve may be abbreviated in subsequent sections for simplicity.)

Figure 34 MCD PC Client Hold/Retrieve call



20.3.5.2 Conference from MCD PC Client

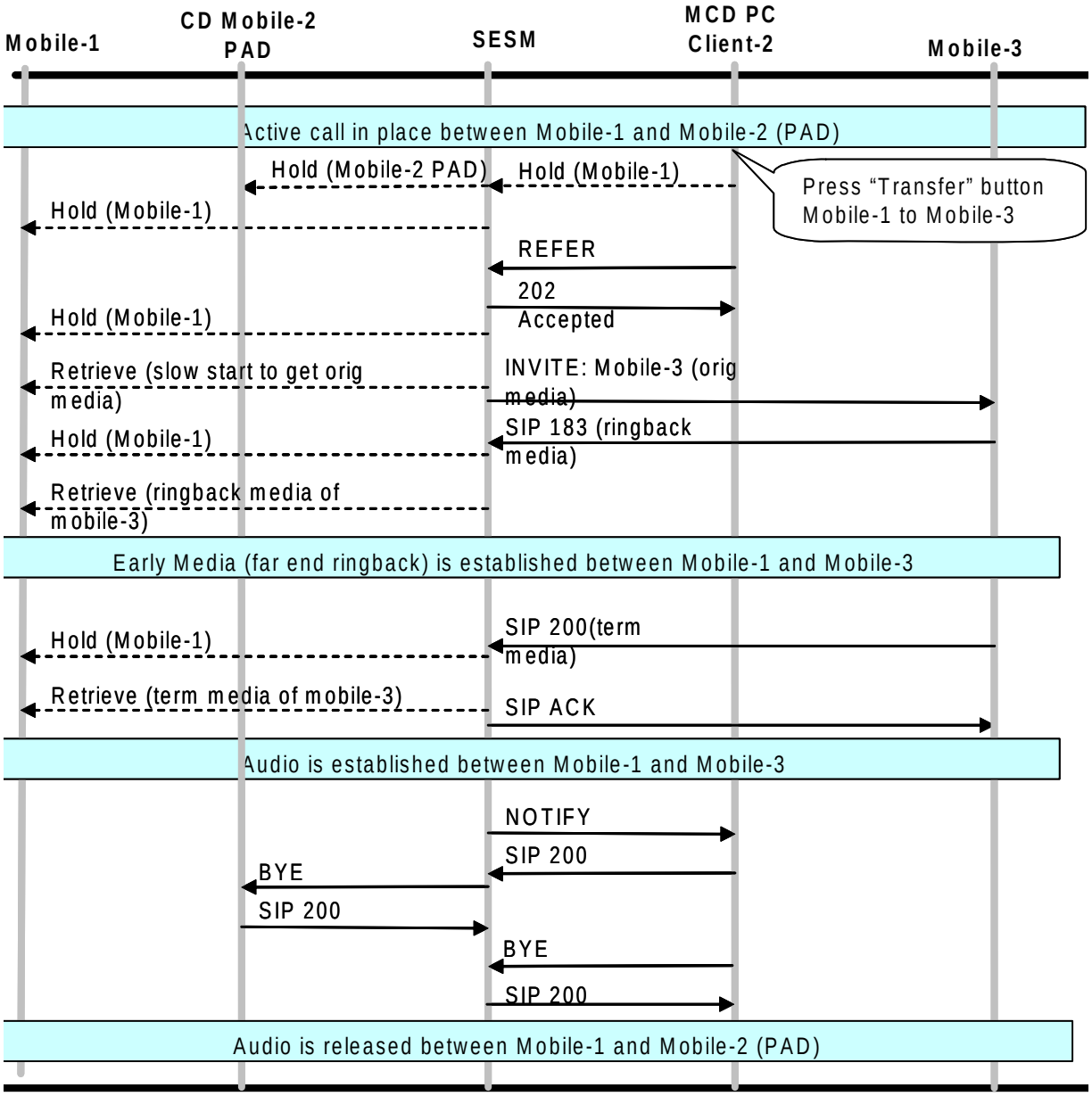
The call flow for the PC Client joining users into a conference is as follows.



20.3.5.3 Transfer from MCD PC Client

An established call exists between Mobile-1 and CD Mobile-2 (PAD). The MCD PC Client-2 invokes a direct transfer of this established call to Mobile-3. An abbreviated call flow for the direct transfer to is shown in Figure 35. Only Mobile-2 is a converged user. Most SIP signaling must go through the CS2000, thus the SESM executes internal REFER logic using Hold/Retrieve.

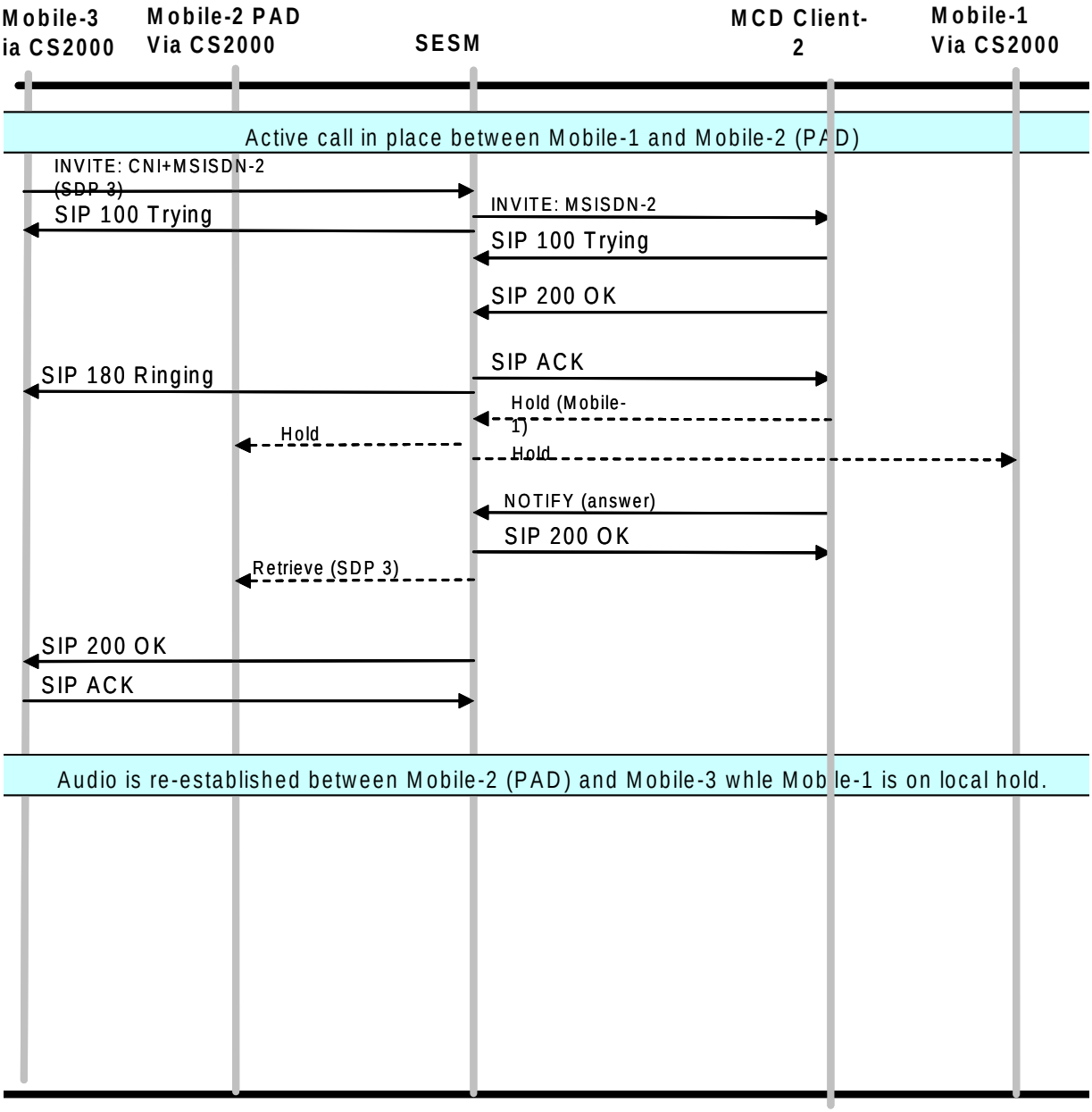
Figure 35 MCD PC Client Transfers call



20.3.5.4 New Inbound Call to PAD (multi-call)

The call flow for the PC Client new call is as follows.

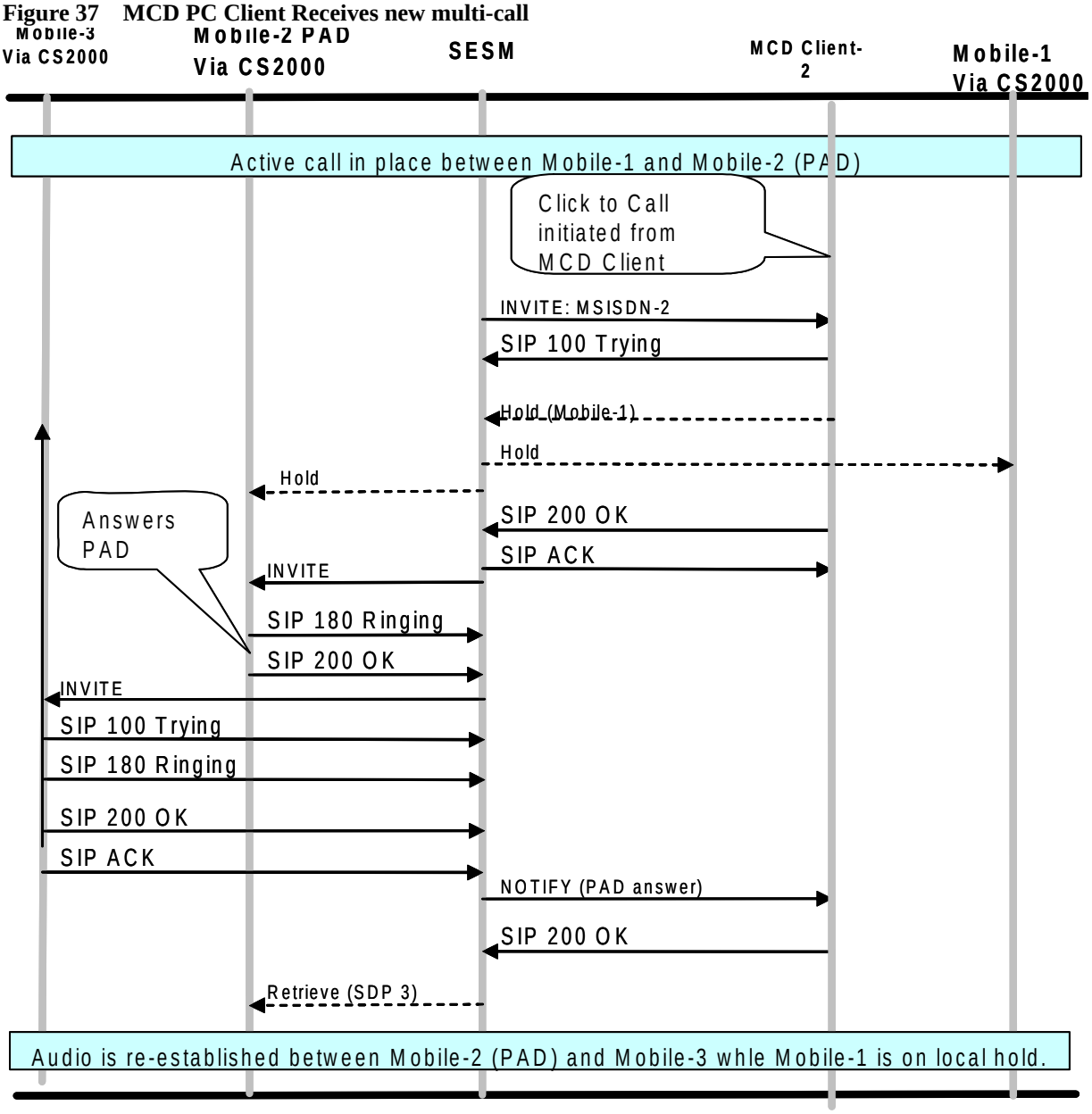
Figure 36 MCD PC Client Receives new multi-call



20.3.5.5 New Outbound Call to PAD (multi-call)

The call flow for the PC Client new call is as follows.

Figure 37 MCD PC Client Receives new multi-call



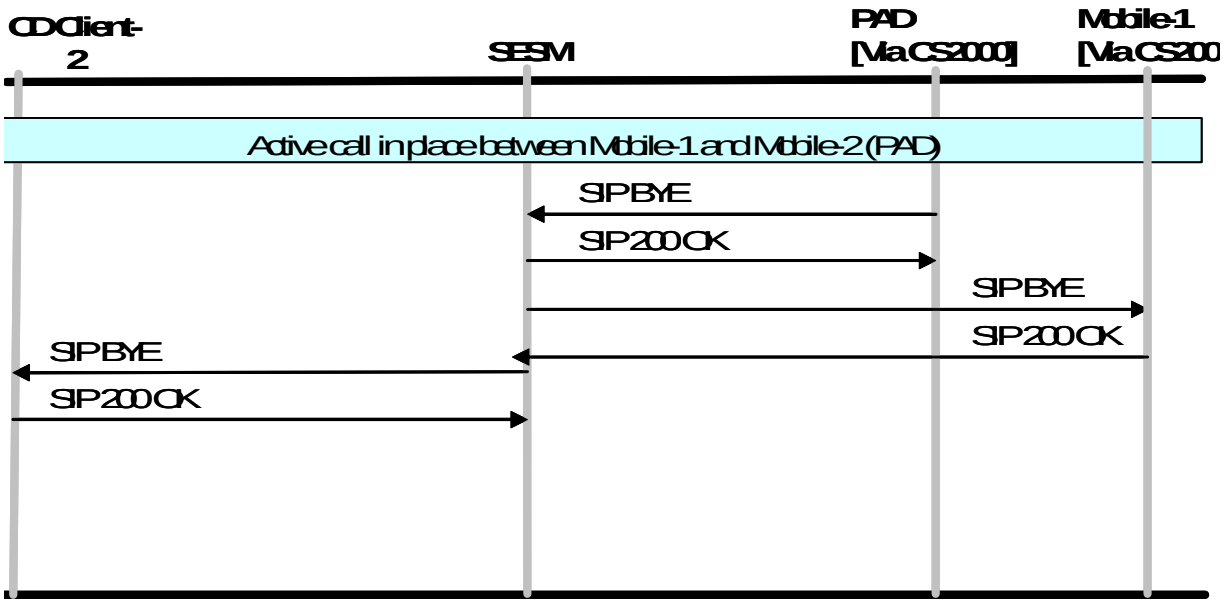
20.3.6 Release Scenarios

This section covers the situations in which a subscriber (mobile-1) disconnects established calls. Specifically, the scenarios presented are PAD Release, Network Release and Release from the MCD PC Client

20.3.6.1 PAD Release

The PAD release and the TDM network release appear identical from the MCS perspective. The call flow is shown below.

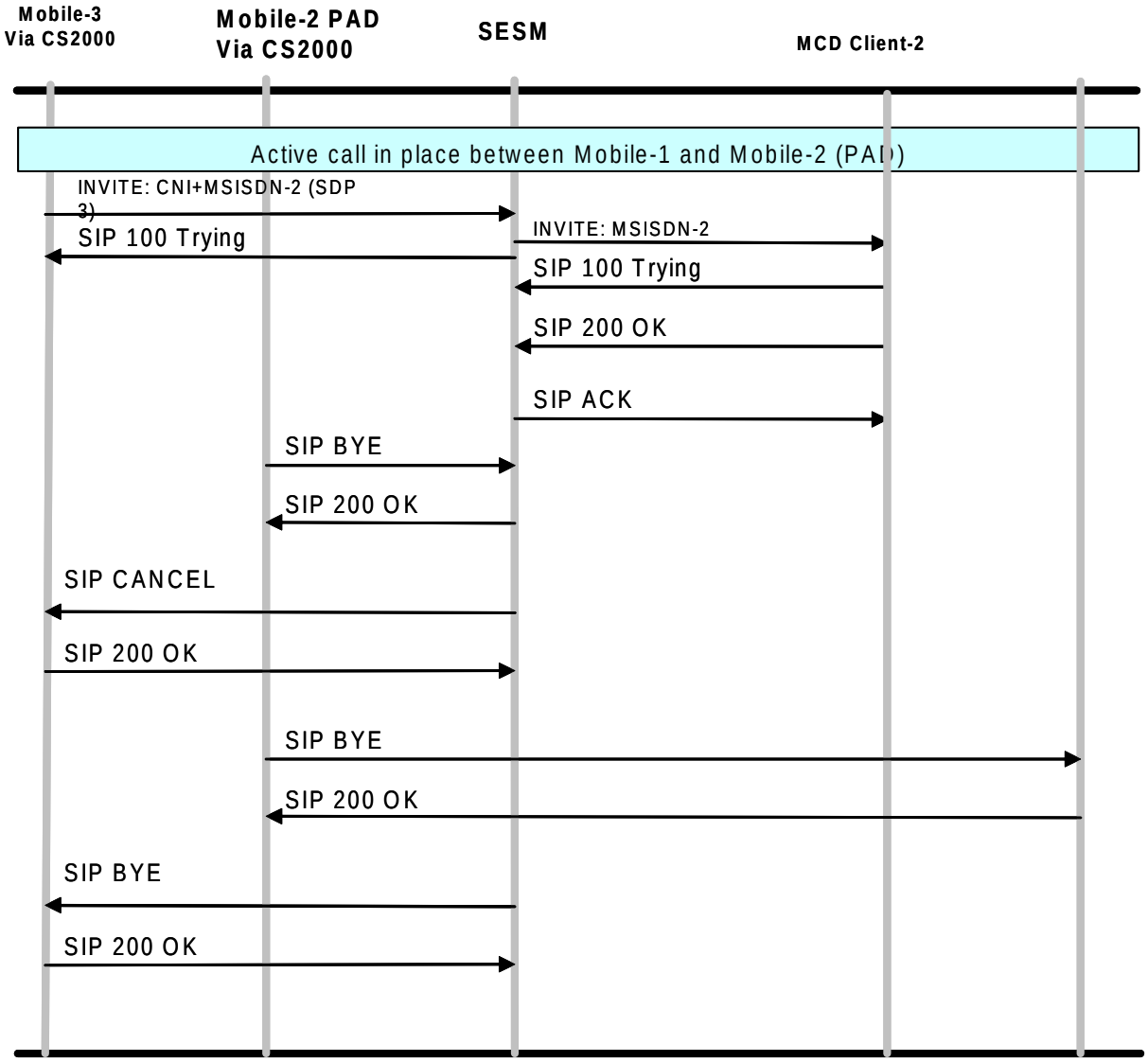
Figure 38 PAD Release



20.3.6.2 PAD Release for Inbound Call (multi-call)

The call flow for the PC Client new call is as follows.

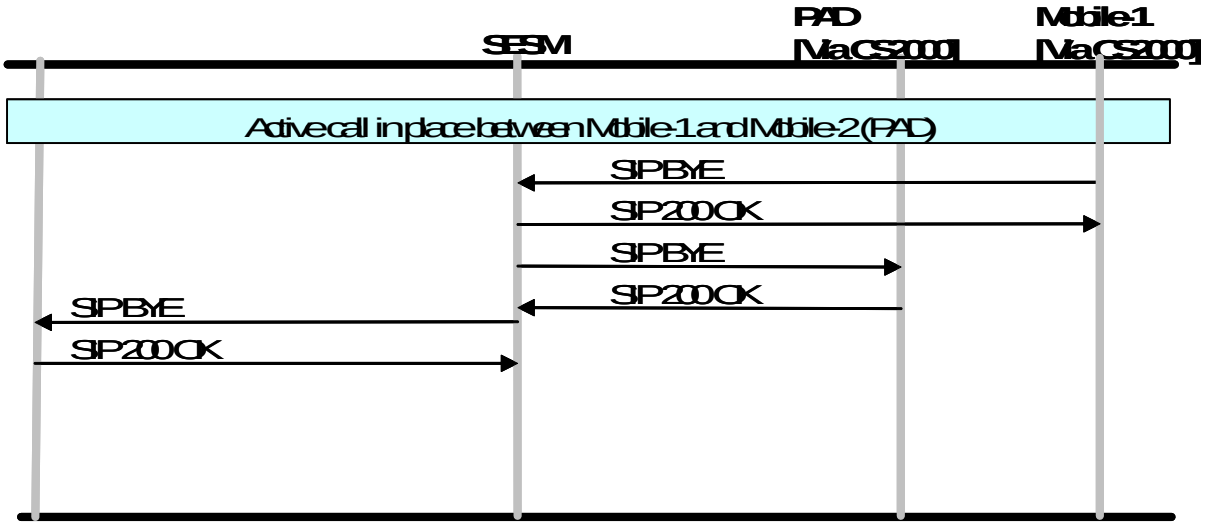
Figure 39 PAD Release for Inbound Call (multi-call)



20.3.6.3 Remote Party Release

The call flow for the PC Client new call is as follows.

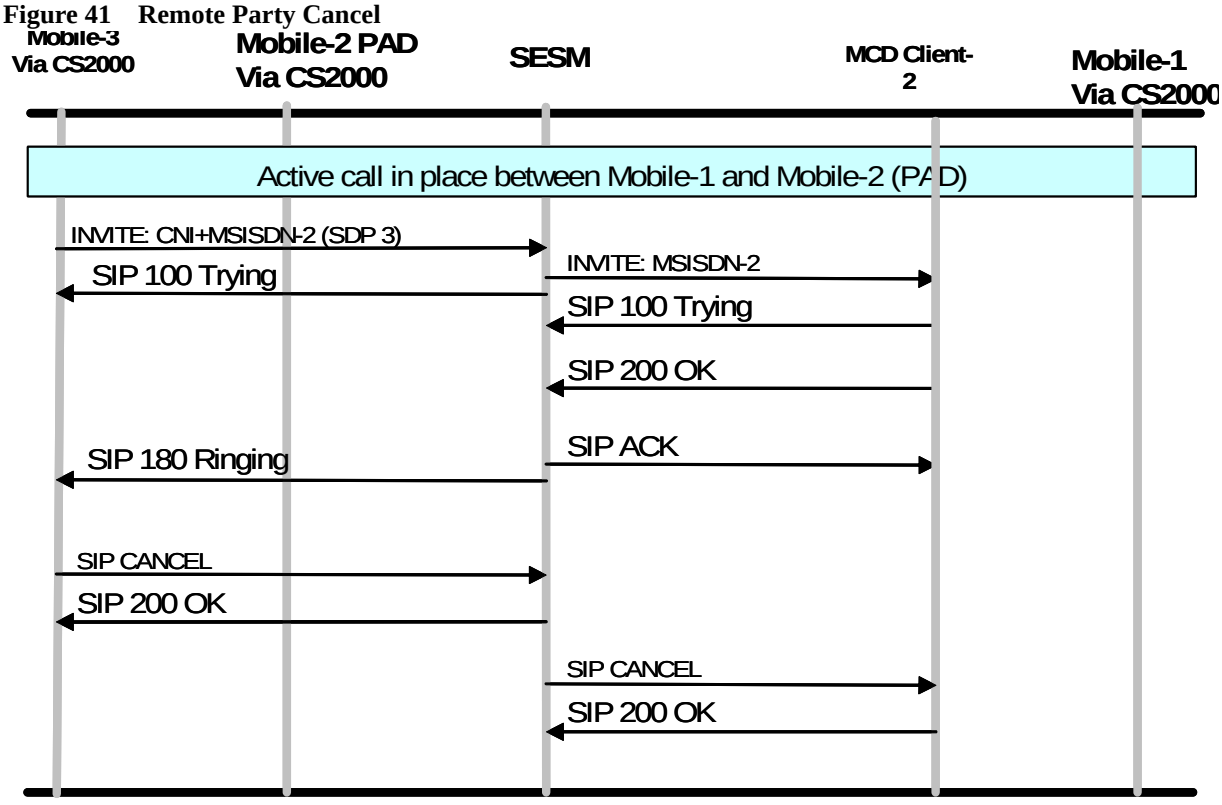
Figure 40 Remote Party Release



20.3.6.4 Remote Party Cancel

The call flow for the PC Client new call is as follows.

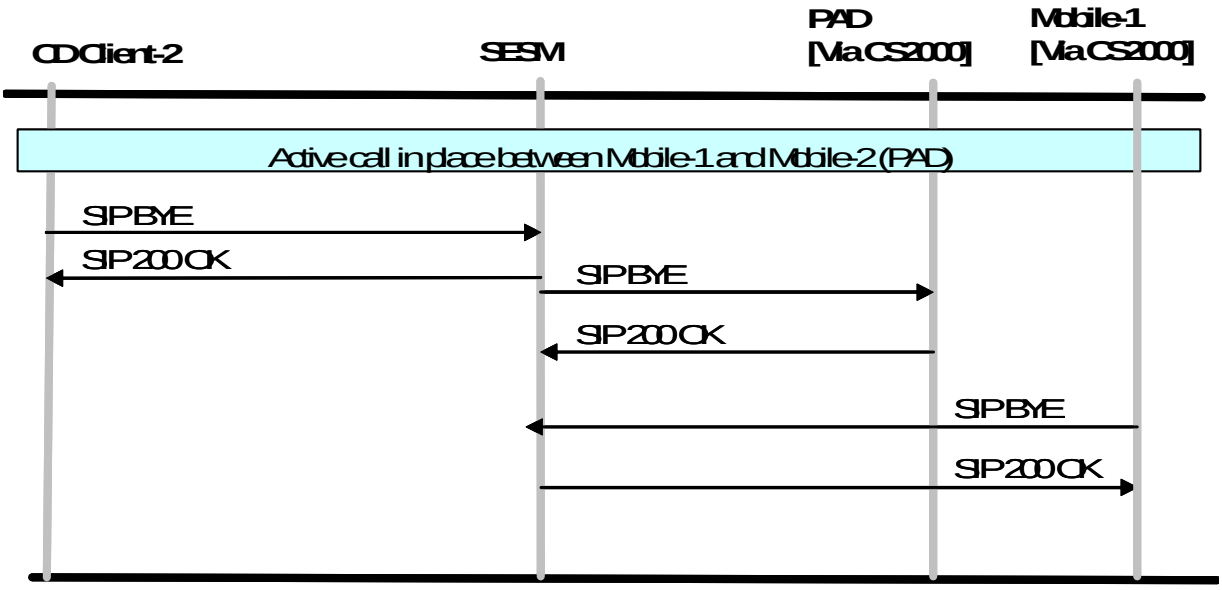
Figure 41 Remote Party Cancel



20.3.6.5 MCD PC Client Release

The PC Client release can occur for any active call leg. The call flow below illustrates the scenario where the establish call is released from the PC Client.

Figure 42 PAD Release



20.4 Hardware Requirements or Dependencies

The Nortel Communication Server 2000 (CS2000) is required to perform the features described.

20.5 Software Requirements or Dependencies

The following software is required to perform this feature.

MCS Component	MCS External Dependency	Description
Sip Application Module	Nortel CS2K or DMS Release ISN08 (or later)	The Wireless Converged Desktop service provides multimedia functionality to existing Mobile TDM switching systems. This entry lists the switch releases that the service supports.

20.6 Limitations and Restrictions

The following restrictions apply to this feature:

1. Video Calls are not supported in this release.

2. Functionality initiated by the PAD does not interact with the MCD feature, and call stated reflecting such services functionality will not be reflected by the MCD PC Client. For example, if a call is put on hold via the PAD, it will not appear to be put on hold as observed on the MCD PC Client, or a call originated by the PAD will have no call control window presented by the MCD PC Client.
3. Dual Hold is not supported on the MCD PC Client in this release. This scenario is when the client attempts to put a call on hold when the call has already been placed on hold by the far end. When the MCD Client has been put on hold (remote hold) and the hold button is blinking to indicate the call is on hold, clicking the hold button will have no effect and will not cause the client to attempt to hold the call again from the client's near end (local hold). Note that this restriction is only applicable when the far end is a SIP or MCD Client user; thus, if the far end is a mobile user and holds the call, as described in restriction 2, the MCD PC Client nor the MCD Service running on the Application Server will be unaware the call is on hold and will not prevent this dual hold scenario.
4. On-call-presence is not supported for PAD originations in this release.
5. The Converged Multimedia PC Client presence works only when the client is registered. If the user logs out of the MCD PC Client, or disconnects from the network, presence will not be correct until the PC Client re-registers.
6. Call Logs (including network call logs) will not be generated for PAD originations.
7. Call logs for MCD PC Client terminated calls contain the CLI provided by the CS2K. Prefixes may be required for call log originations to complete.
8. Call redirection (before answer) is not available in this release.
9. Consult transfer of established calls is not available in this release.
10. Call Park is not available on the Converged Multimedia Client.
11. CS2K overflow routing must be considered and engineered as part of the provisioning of this feature. This is because an MCS SESM outage can impact TDM call completion of converged users on the wireless (e.g. GSM) network. Overflow routing at the CS2K will allow an alternate route to ensure the GSM calls complete in the event the SIPT trunk connecting the MCS is detected as faulty.
12. The Converged Multimedia PC Client does not support Audio; must use the PAD.
13. A Converged User can only have one Multimedia PC Client active at any one time.
14. The MCS must interface a DMS based TDM switching system (CS2K).
15. A single Converged Phone Number can be assigned to a subscriber.

16. The Converged Multimedia PC Client is not aware of Service provided by the Switching System (e.g. Call Forward, Roll Over to Voice Mail).
17. Voicemail – A user should have one VM provisioned. For example, a user should not have VM provisioned on MCP and TDM switch. This can introduce unexpected behavior with the user's PA rules and VM pickup timing. For example, if a user has VM off of GSM network (for their mobile) and provisions a rule on their PA to ring their client (Mobile) 3 times, along with other destinations in their ring-list and their GSM VM is set for 3 rings, then their GSM VM could pick up and the remainder of the PA rules will not be run. The user may expect the PA rules to finish before their GSM VM picking up. Care must be taken on how ring-lists and VM are setup, so the desired behavior is seen.
18. Whenever Voicemail is hosted off TDM switch, MWI is not provided to converged users MCD PC Client.
19. When a MCD user appears in a Personal Agent ring-list the MCD user's redirect COS is not used when a call is extended to the user's converged phone. Instead, the MCD user's primary COS is used. This guarantees that a call to a MCD user will always be able to terminate to their converged phone. Because a MCD user's Preferred Audio Device (the number used to reach their converged phone) is provisioned by the administrator, fraud via redirect should not be a problem.
20. The mobile subscriber (PAD) cannot be part of a centrex group.
21. The mobile subscriber (PAD) can only have single line appearance. Either public or private but not both.
22. Client and network services provided on the wireless TDM network are not coordinated with those provided by the MCS 5200. Each network provides its services independently such that wireless features invoked on the CD Mobile (PAD) will not supervise the MCS Session Manager or its clients.
23. The only originating service supported in this release is click-to-call.
24. If Branding is provisioned, the mobile subscriber may hear branding multiple times during call setup on the PAD. Specifically, branding media files will be played for each call leg into the MCS application server.
25. Telephony translations that involve the prefixes CRD or CRA should be avoided. The CD service will prefix the destination accordingly.
26. Personal Agent routes can not be used to screen converged users PAD number or SIP user ID.
27. This feature does not support MCD PADs accessed from the MCS via a PRI gateway.
28. The Picture ID functionality will ONLY work if a call is made from an MCD PC Client SIP client using SIP addressing. If the call is routed through the GSM network then the picture ID information will be lost.

20.7 Feature Interaction

20.7.1 Service Compatibility

This feature is not compatible with various other MCS services. A summary of service compatibility is provided in the following Table. Service packages that contain the Converged Desktop feature can not be provisioned with any service indicated as ‘Not Compatible’ in the following table.

Table 21 Service Compatibility

MCS Service	Interaction with Converged Desktop Service
Ad Hoc Conference	Compatible - Subscribers can invoke MCS Conferencing by Joining established calls.
Advance Address book	Compatible - This is used by the “Converged” client to save other subscribers calling information. The address book can be used to originate calls.
Advance Screening	Compatible - This provides the advanced routing and screening capabilities from the MCS Personal Agent.
Allowed Clients – PCClient Set Control	Not Compatible
Assistant Console	Not Compatible - not used by MCD users
Assistant Support	Not Compatible - not used by MCD users
Call Park	Not Compatible - MCD users cannot park or retrieve calls while converged, but the call from a MCD user can be parked
CS2000 SIP Line	Not Compatible - not used by MCD users
Calling Line ID Restriction	Compatible - This service is applied when using the C2C in the “Converged Mode” or using another MCS client for origination of calls from the MCS system. If Calling line restriction is required from a TDM phone then this service would need to be provisioned on the TDM switch providing the service to the phone.
Call Waiting Disable	Not Compatible
Client Collaboration	Compatible – However, all forms of client collaboration are applicable to only MCS subscribers.
Colorful Ringback Tones	Not Compatible
Converged Desktop	Compatible - Set to the following for MCD service “Mobile converged”
Device Access Restrictions	Not Compatible
Hot Line	Not Compatible
Multiple Login Restriction	Not Compatible
Net6 Support on 2004	Not Compatible
IM Chatroom Meet Me conferencing	Compatible - can be assigned to a MCD user to access conferencing bridge and MCS chat room.

Table 21 Service Compatibility

MCS Service	Interaction with Converged Desktop Service
Music On Hold	Compatible – Can be used in most call scenarios where the call traverses the MCS system.
Network Call Logs	Compatible – However, call logs originated from the PAD will not be logged in the ‘outbox’. However calls originated from the MCD PC Client (via click-to-call) will be logged to the call log ‘outbox’.
Presence	Compatible – However, presence of a MCD user is based on the MCD Client registration. If the MCD Client is not registered, presence of the MCD user is not updated.
Qos	Not Compatible
Subscriber OPI	Compatible
Unified Communication	Compatible – MCS / MAS hosted voicemail
Video	Not Compatible
Voice Mail	Compatible - TDM based voice mail.
Wireless Client	Not Compatible
Wireless Gateway	Not Compatible

The following sections describe the interactions of Wireless Converged Desktop service with other supported features that may exist on a converged call. Services not listed are not supported in this release.

1.7.2 Advanced Routing

No special handling is required for sequential or simultaneous calls that include a Converged User.

1.7.3 Voice Mail

Calls that terminate to a MCD PC Client can forward to a Voice Mail system. There are two approaches that can be taken to accomplish this.

The first approach is to have the user continue to use their mobile based voicemail. In this configuration the MCS application server will release these call attempts and the CS2000 must map this release to an ISUP message REL w/ cause. The call can then be further processed on the mobile network to forward the call to a voicemail system.

The second approach is to transition users to an MCP based voice mail system. If an MCP based messaging system is used, then both call legs of the dual leg call to a MCD User are cancelled, and the call is rolled over to the voice messaging system.

1.7.3.1 Voice Mail Hosting

It is recommended that the MCP handle Voice Mail roll over instead of the mobile switching system. This will allow the Personal Agent to search the subscriber's other terminating devices before rolling over to Voice Mail. Doing this may take additional resources because the switching system will have to send all calls to the MCP so that voicemail can be handled.

1.7.3.2 Voice Mail Waiting Indicator (MWI)

If the voice messaging system is hosted off of the MCP the MCD Multimedia PC Client provides a voicemail indicator. The voicemail icon at the top will flash when a new unread message is in your inbox and will stay flashing until the message has been retrieved. VM MWI is not provided if VM is hosted on the TDM system.

1.7.3.3 Voice Mail Access

The MCD user can access their voicemail box by making a call to the voice mail number on the MCD Multimedia Client (which is through the click to call mechanism) or dialing the number on the Converged phone directly. After the call is established, the user can then navigate the voicemail system and retrieve their voicemails using their Converged Phone keypad. The MCD Multimedia Client cannot be used to do this (unlike the non-converged Multimedia PC Client which can). Double-clicking on the voice mail icon does not call the voice mail server on the mobile network.

1.7.4 Interaction with IM and Web push

Instant Messages or Web pushes received by a SIP user are directed to the MCD Multimedia PC Client only.

1.7.5 Multiple Call Restriction

The maximum number of simultaneous calls is enforced on the MCS Session Manager during call processing.

1.7.6 Presence

Presence is available only on the MCD Multimedia PC when registered. The enhancement called "On the Phone" presence (automatically changes state if the client is engaged in an active call) is not available in this release. For example, if a call originates from the CD Mobile the presence state will not change to "On the Phone" at the PC Client. However, presence states can be manually changed on the MCD PC Client. The standard list of presence states are supported along with any user defined states. Please refer to the "SIP Multimedia PC Client Fundamentals" user documentation for information on Presence for the Multimedia PC Client.

1.7.7 Call Redirect (before answer)

Redirect before answer is not available to a MCD PC Client, but the MCD PC Client and its Converged Phone (PAD) can be redirected by another MCP client before answer.

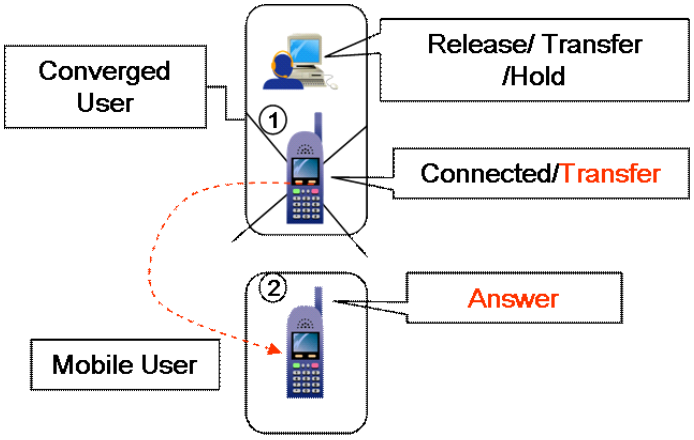
1.7.8 Call Transfer

Direct Transfer after answer is available to the MCD PC Client. When the 'transfer' button is clicked, the subscriber will be shown a window for entering the destination the call should be transferred to and only offers the option to perform a direct transfer. If a direct transfer is invoked, the client will send a SIP REFER message to direct the call to the transfer destination and the call on the PC client is released once the transfer is complete.

Consult Transfer is not available to the MCD PC Client. However the MCD PC Client and its Converged Phone (PAD) can be transferred by another MCP client.

The call-transfer features on the mobile phone may have undesirable side effects when used in conjunction with the MCD feature offered by MCS. Generally, the MCS will not have knowledge of the mobile invoked features. Consider the following scenario which may occur as these features intersect. Figure 43 shows Converged User already engaged in a conversation with a party B (not shown). However, when a transfer is invoked from Converged User's mobile phone to Mobile-2, the voice path will be modified on the mobile network without knowledge of this transition on the MCS network. Thus, resulting in a scenario where the MCD PC Client can control the audio stream of the transferred call even when the audio is changed over to Mobile-2.

Figure 43 Call Transfer from Mobile



1.7.9 Conference Calls

Conference calls are supported on the MCD PC Client.

1.7.10 Meet Me Conferencing

Meet me conference calls are supported on the MCD PC Client.

1.7.11 Caller Line ID (Privacy)

Caller Line ID Privacy is supported on the MCD PC Client and the MCS network. However, the feature must also be enabled on the TDM network at the same time to be effective.

1.7.12 Network Call Logs

1.7.12.1 Inbox

Inbound call attempts are recorded in the Inbox. The ability to successfully re-dial a caller from this call log depends on the calling line id provided by the adjacent switch (CS2K). The prefixing introduced in this feature will be automatically pre-pended by the application server during call routing.

1.7.12.2 Outbox

Only outbound call attempts made from the MCD PC Client are recorded in this Outbox. Outbound call originations from the PAD will not be recorded in this log.

1.7.13 Interaction with RTP Portal

RTP media portal will not be inserted even when the MCD PC Client is behind a firewall.

1.7.14 Interaction with Long Call Audit

Call audits that involve the PAD leg (CD mobile) will simply be forwarded to the CS2000. The MCS Session Manager will not release these call legs directly.

1.7.15 Interaction with Other Media Services

The following services depend on the MAS for providing media.

1.7.15.1 Branding

MAS hosted branding is supported on the MCD PC Client.

1.7.15.2 Colorful Ring-back Tones

CRBT is not supported the MCD PC Client.

1.7.15.3 Music On Hold

MAS hosted music-on-hold is played to all parties on hold (when provisioned).

1.7.15.4 Announcements and Treatments

MAS hosted announcements are not played to a gateway subscribers. Thus, mobile subscribers will not be able to hear these media files on the mobile.

1.7.16 Class of Service considerations for MCD Terminations

When a call terminates to a Converged User, a call leg is extended to the user’s converged phone over a gateway route using the Preferred Audio Device DN

that is provisioned for that user. The rules for determining the class of service and dial-plan for processing of the Preferred Audio Device DN are as follows.

When calling within the same domain or across different domains, translations uses the dial-plan of the domain that is being terminated to and the class of service of the Converged Desktop User that is being terminated to.

1.8 Accounting

1.8.1 Converged Desktop Supplementary Service

This feature introduces a new supplementary service to the IPDR. The serviceType field will be labeled “mobileConverged” if this service is running on the call leg that the record is generated on.

```
<ipdr:UE xsi:type="UE-VoIP-Type">
        <recTime>2005-08-04T21:43:51.361Z</recTime>
  <protocol>sip</protocol>
  <uID>058372efe9135810c17e69f7d9e71275f5d13b4@47.104.23.220</uID>
  <corrID>058372e6b11c90d3117e69f303e6ff078956bd7@47.104.23.220</
corrID>
  <connSubscriberID>u2149971915@nortel.com</connSubscriberID>
  <startTime>2005-08-04T21:43:32.079Z</startTime>
  <connParty>sip:2149971915 @nortel.com</connParty>
  <outpulsedDigits>sip:2149971915 @nortel.com</outpulsedDigits>
  <tMG>47.104.17.146</tMG>
  <ansInd>true</ansInd>
  <ansTime>2005-08-04T21:43:51.314Z</ansTime>
  <aband>false</aband>
  <supplementaryService>
    <sdpService>
    <sessionName>Phone-Call</sessionName>
       <media>
            <mediaName>audio</mediaName>
            <sdpProtocol>RTP/AVP</sdpProtocol>
            <origSdpPort>50082</origSdpPort>
            <origConnAddr>47.102.245.76</origConnAddr>
            <termSdpPort>45040</termSdpPort>
```

```
            <termConnAddr>47.104.17.146</termConnAddr>
            <dir>1</dir>
            <codecList>
            <codec>0 PCMU/8000</codec>
                    <codec>110 telephone-event/8000</codec>
            </codecList>
         </media>
   </sdpService>
</supplementaryService>
<supplementaryService>
   <mobileConverged>
            <directoryNumber>2149971915</directoryNumber>
            <subscriberID>u2149971915@nortel.com</subscriberID>
   </mobileConverged>
```

1.8.2 IPDR (Internet Protocol Detail Record)

There are some important aspects of the IPDR records generated by the Converged Desktop feature that need to be understood to ensure proper billing can be provided. The following sections describe how accounting for this service is different than normal MCP based calls.

1.8.2.1 Number of Billing records on a Converged Call

The general accounting rules for generating IPDRs apply to Mobile Converged Desktop. The only scenario where the MCD service deviates from the normal policy is when the MCP creates two separate legs for a ‘converged’ call (one for Mobile and one for PC Client). In that case, the two legs are treated as one and only one record set (i.e. CI/DI or CE/DE) is created to represent both legs of the call.

1.8.2.2 Mid-call (event based) SDP IPDR

On a converged call, when mid-call audio changes occur, each leg on a Dual Leg will generate an SDP IPDR for the stream type it handles. The audio leg will generate an SDP IPDR containing only audio SDP if the audio stream has changed. Additionally, when the PAD audio is modified through the CS2000 the MCS will generate SDP IPDR records.

1.8.2.3 MCP / TDM billing record correlation

All IPDR records generated by a converged call, including the extra IPDRs generated on a Dual Leg call, will have the “corrID” IPDR field set to the same value so that they can be records. This field can be used to correlate records from converged calls on the MCP and the TDM switch.

If a correlation ID is passed to the MCP via the “x-nt-corr-id” header in an SIP INVITE from a TDM switch, then all IPDRs generated on that call will have the “corrID” field set to the value of the received correlation ID. In addition, if the call is extended back to a TDM switch (same switch or another), the same correlation ID is passed in the SIP INVITE to that switch via the “x-nt-corr-id” header.

1.9 Fault Management

1.9.1 Logs

N/A

1.9.2 Operational Measurements

The following Operational Measurements are added:

1. Each time a CD call is originated by click-to-call

```
    Component: Session Manager
     OM group: CONVERGEDDESKTOP3_SERVICE
   Tuple Name: ConvergedDesktop_Service
Register Name: CDC2C
        Range: Integer
   Definition: Counts the number click-to-call
originations that were placed from a MCD PC Client.
```

2. Number of call attempts answered on the CD Mobile (PAD)

```
    Component: Session Manager
     OM group: CONVERGEDDESKTOP3_SERVICE
   Tuple Name: ConvergedDesktop_Service
Register Name: CDANSPAD
        Range: Integer
   Definition: Counts the number call attempts that
were answered on the CD Mobile (PAD). This scenario
occurs when the subscriber is registered on the MCD
PC Client and the CD Mobile answers the initial call.
Thus, can also be considered the number of 'initial
calls answered'. The counter is incremented on the
successful SIP Notify transaction sent to the PC
client. This register will not peg if the subscriber
is not registered on the MCD PC client.
```

3. Each time a call attempt is answered on the MCD PC Client

```
  Component: Session Manager
     OM group: CONVERGEDDESKTOP3_SERVICE
   Tuple Name: ConvergedDesktop_Service
Register Name: CDANSPCC
        Range: Integer
   Definition: Counts the number call attempts that
were answered on the MCD PC Client. This scenario
occurs when the MCD Client answers the initial call.
Thus, can also be considered the number of
'subsequent calls answered'.
```

4. Number of call attempts to MCD PC Client when client becomes network isolated

```
    Component: Session Manager
     OM group: CONVERGEDDESKTOP3_SERVICE
   Tuple Name: ConvergedDesktop_Service
Register Name: CDCOG
        Range: Integer
   Definition: Counts the number call-of-grace
terminations that were attempted on a MCD PC Client.
This scenario occurs when a MCD PC Client has a
registered contact on the MCS application server, yet
fails to auto-answer an incoming call attempt. The
behavior at the application server is to attempt this
call-of-grace 1 of N call attempts.
```

5. Number of call attempts redirected to PSTN when MCD PC Client is not registered

```
    Component: Session Manager
     OM group: CONVERGEDDESKTOP3_SERVICE
   Tuple Name: ConvergedDesktop_Service
Register Name: CDPXYCALL
        Range: Integer
   Definition: Counts the number call attempts that
were proxied back to the CS2000. This scenario occurs
when a MCD PC Client has not registered on the MCS
```

application server. All call attempts should be proxied back to the mobile network.

6. Each time a call attempt timer expires on the application server for a CD3 subscriber.

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDCATTEXP

Range: Integer

Definition: Counts the number of termination attempts presented to MCD PC Client, where the call attempt timer expired. The call was presented to the subscriber but no action was taken. The application server releases the call upon expiry.

7. Each time a call termination attempt is Rejected / Declined by a CD3 subscriber

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDDECLINE

Range: Integer

Definition: Counts the number of declined termination attempts that were presented to MCD PC Client. The subscriber must press ‘Decline’ for this register to increment.

8. Each time a call termination attempt is Ignored by a CD3 subscriber

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDIGNORE

Range: Integer

Definition: Counts the number of ignored termination attempts presented to MCD PC Client. The subscriber must press 'Ignore' for this to register to increment.

9. Each time a call hold / retrieve is attempted by a CD3 subscriber

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDHLDRT

Range: Integer

Definition: Counts the number of hold/retrieve attempts managed by the CD3 service.

10. Each time a call transfer is initiated by a CD3 subscriber

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDXFER

Range: Integer

Definition: Counts the number of call transfers managed by the CD3 service.

11. Each time a conference call is initiated by a CD3 subscriber

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDCONF

Range: Integer

Definition: Counts the number of conference calls managed by the CD3 service.

12. Each time MCD PC Client Register message is received

Component: Session Manager

```
      OM group: CONVERGEDDESKTOP3_SERVICE
   Tuple Name: ConvergedDesktop_Service
Register Name: CDREG
        Range: Integer
  Definition: Counts the number of register messages
that are sent by the MCD PC Client during Login,
updates, and Presence state changes.
```

1.10 Glossary

Term	Description
SME	Small to Medium Enterprise
CD	Converged Desktop
GUI	Graphical User Interface
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
PBX	Private Branch Exchange
IP	Internet Protocol
STP	SS7 Signal Transfer Point
SCP	SS7 Service Control Point
HLR	Home Location Register
ISUP	Signaling System 7 ISDN User Part
ISDN	Integrated Services Digital Network
SS7	Common Channel Signaling System No. 7
MAP	Mobile Application Part
MSC	Mobile Switching Center
CRD	Destination Call Leg Return Code – preferred audio device prefix
CRA	Associated Call Leg Return Code – click to call prefix
PAD	Preferred Audio Device

139: Functional Description (FN) A00012273

139.1 Feature name and Feature ID

A00012273 - SIP Lines: Call Forwarding Indication

139.2 Description

This activity provides the CS2K support for Call Forwarding Indicator and Call Forwarding Reminder for SIP agents that interface to the CS2K

Note that this functionality also requires SIP Client development in the SIP messaging arena, which is not covered by this activity.

Call Forwarding Indicator is provisioned using option CFIND. The SIP client provides a special dialtone (sometimes called “stuttered dialtone”) to a subscriber who goes offhook when the subscriber has had call forwarding activated.

Call Forwarding Reminder provides a brief one-time ringing (sometimes called “ring splash”) to a subscriber who is onhook when call forwarding is active and a call was attempted to the subscriber and forwarded.Enabling/ Disabling of Call Forwarding Reminder is not provisioned as a separate option, but is dependent upon the type of call forwarding and also possibly feature data for some call forwarding types. For example, Call Forward Busy (CFB) never has Call Forwarding Reminder, while Call Forward Universal (CFU) always does, and Selective Call Forwarding (SCF) has feature data indicating if it does.

139.3 Hardware Requirements or Dependencies

None

139.4 Software Requirements or Dependencies

None

139.5 SIP User Agent Interactions & Requirements

If the SIP User Agent (UA) is not registered, calls attempting to terminating to it are unaffected by this feature.

If the UA does not respond to an INVITE, calls attempting to terminating to it are unaffected by this feature.

If the UA rejects an INVITE, calls attempting to terminating to it are unaffected by this feature.

In order to support this feature, the UA must be compliant to draft-ietf-sipping-config-framework-07 (ua-profile event package). The ua-profile event package deals with the call forwarding indicator. Additionally, there is a new event package defined by this feature for the call forwarding reminder.

139.5.1 Call Forwarding Indicator

The syntax used for the call forwarding indicator:

SUBSCRIBE
Event: ua-profile
Accept: application/server-call-feature-status+xml

NOTIFY
Event: ua-profile
Content type: application/server-call-feature-status+xml
Content:
<ua-profile>
<feature>call-forward-indicator</feature>
<status>on | off</status>
</ua-profile>

When call forward is activated, every subsequent origination attempt should get a distinctive dial tone (stutter dialtone).

139.5.2 Call Forwarding Reminder

The new event package deals with the call forwarding reminder. The syntax:

SUBSCRIBE
Event: network-redirection-reminder
Accept: application/network-redirection

NOTIFY
Event: network-redirection-reminder
Content type: application/network-redirection
Content:
call-redirected | subscription-active | subscription-expired

When the call forwarding reminder is activated, if the UA has no calls, there should be a short alerting tone or message presented at the user interface.

139.6 Limitations and restrictions

Option CFIND (in SERVORD) for DPL lines must have feature data STN_TONE set to “CFT”. This is an existing limitation for all types of LGRP lines, which includes DPL lines.

139.7 Interactions

None.

139.8 Applicable customer facing sections

Fault Management

- Logs _N/A_
- Alarms _N/A_

Configuration

- Data Schema _N/A_
- User Interface _N/A_
- Element Management _N/A_
- Security _N/A_
- Service Order _N/A_
- Office Parameters _N/A_

Accounting (includes AMA billing) _N/A_

Performance (includes operational measurements) _N/A_

139.9 Glossary

Term	Description

139.10 Sample Datafill & Usage

For both call forwarding indicator and call forwarding reminder, it is necessary to have call forwarding datafilled on the line. A sample SERVORD command for call forwarding on DN 5200001 (assuming a RES line):

```
ADO $ 5200001 CFW C NSCR 1 $
```

For call forwarding indicator, it is also necessary to have the CFIND option datafilled. CFIND is a RES option. A sample SERVORD command for CFIND on DN 5200001 is:

```
ADO $ 5200001 CFIND CFT 1000 $
```

With the above datafill, after the subscriber activates call forwarding:

- A stuttered dial tone is given to the subscriber when going off-hook
- When a call is placed to 5200001 and is forwarded, the SIP device will generate a ring splash.

140: Functional Description (FN) A00012308

140.1 Feature name and Feature ID

A00012308 - SIP Lines Services: PRK, DPRK, CPU

140.2 Description

The purpose of this feature is to interwork a specific set of Session Initiation Protocol (SIP) clients into IBN/RES network based Call Park and Call Pickup services. See “Limitations and restrictions” on page 1397. for the specific list of Call Park and Call Pickup line options.

To activate this feature functionality the service set 1 patches need to be applied and DPL line option compatibilities removed (included in patches). Once applied, the setup and functionality of these services with SIP agents are seamless as compared to the functionality of the service on other Nortel supported agents For additional information reference Nortel NTPs for Park and Pickup NT-297-8001-808.

140.3 Hardware Requirements or Dependencies

There are no hardware dependencies required to execute this feature.

140.4 Software Requirements or Dependencies

Software Dependencies:

— XACore Succession release SN10 and SN09 patches

Firmware Dependencies:

— none

140.5 Limitations and restrictions

- Supports the following Call Park and Call Pickup line options:
  - — Call Park: PRK, DCPK
  - — Call Pickup: CPU, DCPU, DCPX, TAFAS
- Supports the following set of SIP devices:
  - — Motorola Outside Network Terminations (ONTs)
  - — Cisco SIP phones
  - — Nortel PC Soft clients

- Supports the existing Engineered Recommended and Absolute group member maximums for Call Pickup (CPU) when all members are SIP agents.
- This feature supports Parking a call if there is at most one other answered session when the Call Park vertical service code is processed.
- In the context of Call Pickup (CPU), the number of sessions which could be simultaneously alerting will vary based on the client. The CS2K Pickup service will always pickup the session which has been ringing the longest.
- In the context of TAFAS Pickup (TAFAS), if the TAFAS agent is a SIP agent, then multiple terminations are possible with the proper datafill. If more than 1 termination to the TAFAS SIP device is occurring, then the longest ringing TAFAS SIP session will be pickup.
- Activations for CPU, additional session invocation of CPU are subject to current CPU flash invocation restrictions.
- Activations for DCPU, additional session invocations of DCPU are not allowed if currently involved in a stable (talking) call. This matches current DCPU behaviors...i.e you cannot flash and invoke DCPU.
- Activations for TAFAS, additional session invocation of TAFAS are subject to current TAFAS flash invocation restrictions.
- Interactions with CPU, DCPU, and TAFAS, and call wait (CWT). A call waiting call will not be picked up. This is done to match historical behavior.
- Directed Call Pickup w/Barge-In and Directed Call Pickup w/Barge-In Exempt will be delivered in a separate activity. Until this is delivered, invoking of Barge-in via a SIP agent or Barging into a SIP agent is not supported.

140.6 Interactions

The following are the feature interactions for this feature:

- Features which this feature is dependant on:
  - — none
- Features which are dependent on this feature:
  - — A00012597 Music On Hold
  - — A00012323 Park/Pickup w/Barge-in
- Features which have an interaction with this feature:
  - — none

140.7 Applicable customer facing sections

Fault Management

Logs ___n/a___

Alarms ___n/a___

Configuration

Data Schema ___n/a___

User Interface ___n/a___

Element Management ___n/a___

Security ___n/a___

Service Order ___n/a___

Office Parameters ___n/a___

Accounting (includes AMA billing) ___n/a___

Performance (includes operational measurements) ___n/a___

140.8 Glossary

Term	Description
Features	in this context means design feature as opposed to central office features/services (ex. CFW, CWT, etc.)

141: Functional Description (FN) A00012310

141.1 Feature name and Feature ID

A00012310 - Hunt, SCMP, and CWT variant support for SIP Lines

141.2 Description

The purpose of this feature is to provide support for network based hunting, series completion and call waiting services for SIP user agents as part of the CS2K SIP Lines program.

In general,these services will behave in a manner consistent with their behavior in non-SIP configurations. Any exceptions are noted below.

141.2.1 Hunting

This feature provides support for the following hunt types on CS2K SIP Lines:

- DNH - Directory Number Hunt
- MLH - Multi-Line Hunt
- DLH - Distributed Line Hunt
- BNN - Bridged Night Number
- PRH - Preferential Hunt

In addition, the following hunt suboptions will be supported:

- CFGD/CFGDA - Call Forward Group Don’t Answer
- LOD- Line Overflow to DN
- LOR - Line Overflow to Route
- CIR - Circular Hunt
- SHU - Stop Hunt
- RMB - Remote Make Busy

SIP lines can be used in the same hunt group as non-SIP lines. There will be no restrictions on using SIP lines in hunt configurations beyond the normal customer group and line class code restrictions imposed by standard hunt provisioning.

The functionality for SIP lines being in hunt groups has been defined to be:

- Termination on a SIP line for hunt purposes will only be considered if that line is involved in no other calls at the time. That is, the SIP line will be

skipped in the hunt search algorithm if it is already involved in a call - even if it has the capability to engage in multiple call appearances.

Exceptions:

1.) CWT termination is allowed in DNH and PRH groups if the individual member has the CWT option. For SIP lines, if a DNH or PRH member has CWT, hunt calls will continue to be presented to the member until its maximum call appearances have been reached.

2.) In MLH configurations, if CWT is added to the pilot, extra call waiting calls are actually presented to the last member of the group. If that last member is a SIP line, calls will continue to be presented to that line until its maximum call appearances have been reached.

- If a hunt call terminates on a SIP line, and the SIP client declines the call (4XX or 6XX SIP response), the hunting search will continue to the next available hunt member. BNN groups are an exception to this rule. When a call terminates on a BNN and the SIP client declines the call, the call will receive busy treatment.
- If a hunt call terminates on a SIP line, and the SIP client redirects the call (3XX SIP response), the call will be forwarded to the redirection destination.
- Hunt suboptions CFGD/CFGDA, LOD, LOR, CIR, SHU, and RMB will function in the same manner as they do in non-SIP configurations.

141.2.2 Series Completion (SCMP)

This feature provides support for Series Completion on CS2K SIP Lines.

SIP lines can be in the same SCMP group as non-SIP lines. There will be no restrictions on using SIP lines in SCMP configurations beyond the normal restrictions imposed by standard SCMP provisioning.

In general, SCMP on a SIP line should function in exactly the same manner as it does for a non-SIP line. There are two items worth noting:

- SCMP takes precedence over CWT. Therefore, termination on a SIP line for SCMP purposes will only be considered if that line is involved in no other calls at the time, even if it has the capability to engage in multiple call appearances.
- SIP lines have the additional capability to decline calls after they have been presented to the line. If a SIP line with SCMP is idle but declines the call, the call will be directed to the SCMP DN rather than busy treatment.

141.2.3 Call Waiting Variants

This feature provides support for the following Call Waiting Variants on CS2K SIP Lines:

- CWI - Call Waiting Intragroup

- CWO - Call Waiting Originating
- CWD - Dial Call Waiting
- CWX - Call Waiting Exempt
- CWTACT - Call Waiting Activate
- SCWID - Spontaneous Call Waiting Identification

For SIP lines, a call waiting call is just a second call appearance being offered to the SIP client. The client is responsible for any tone application and the function of switching between the two calls via hold/restore. Therefore, for CS2K SIP lines, the presence of the above CWT options will be used to determine when it is appropriate to offer multiple call appearances to the terminating SIP line.

In that context, the function of the above CWT variants is the same for SIP lines as it is for non-SIP lines.

141.3 Hardware Requirements or Dependencies

CWD requires PMA (Packet Media Anchor) insertion when the CWD originator is a SIP line. The PMA is required to provide subsequent digit collection after the CWD feature access code. Without the PMA, CWD cannot be initiated by a SIP line.

141.4 Software Requirements or Dependencies

In order to provision hunt groups on CS2K SIP lines, there is a dependency on feature A00012223: “SESM Additional Provisioning for SIP Lines”. This feature adds support for hunt group provisioning commands such as EST, ADD, DEL, ABNN, DBNN, and CHDN via SESM.

141.5 Limitations and restrictions

- MPH (Multi-Position Hunt) is not supported by this feature.
- Hunt group provisioning commands EST and ADD, when applied via SESM, will be limited to only one len or gateway endpoint per command. See feature A00012223 “SESM Additional Provisioning for SIP Lines” for more information.
- CWR (Call Waiting Ringback) and CWTC (Call Waiting Conference) are not supported by this feature.
- If a SIP line has max_call_appearances set to 1, then no call waiting calls can be presented to that line by any call wait variant, regardless of CWT variant provisioning.
- If a SIP line is using all of it’s available call appearances (example: max_call_appearances = 4, and 4 calls are active), then no further calls can

be presented to that line by any call wait variant, regardless of CWT variant provisioning.

- Typically, core based features that impose call waiting on the terminating line (CWO, CWD) will override the use of Cancel Call Waiting (CCW) by the terminator. For SIP lines however, CCW is implemented in by the SIP client, so core based CWO and CWD cannot override it. This is a limitation of CWO and CWD for SIP lines.

141.6 Interactions

Not applicable.

141.7 Applicable customer facing sections.

Fault Management

Logs _N/A_

Alarms _N/A_

Configuration

Data Schema _N/A_

User Interface _N/A_

Element Management _N/A_

Security _N/A_

Service Order _N/A_

Office Parameters _N/A_

Accounting (includes AMA billing) _N/A_

Performance (includes operational measurements) _N/A_

141.8 Glossary

Term	Description
New term	Definition

142: Functional Description (FN) A00012315

142.1 Feature name and Feature ID

A00012315 - Telemetry for SIP Lines

142.2 Description

The SIP Lines Telemetry feature (A00012315) enables remote meter reading of SIP Lines. It allows utility companies to read utility meters remotely by establishing a media session with the Telemetry device at the subscriber's home.

This feature allows the functions of the UTS (Utility Telemetry Service) and SRA (Suppressed Ringing Access) CS2000 Core features to be extended to SIP Lines. UTS and SRA calls are established from automated systems owned by utility companies to TIU (Telemetry Interface Unit) devices that are attached to the subscriber's phone line. Both UTS and SRA suppress ringing of the subscriber's phone and allow the TIU to pick up the call.

To operate on SIP Lines, the customer has agreed that SIP INVITE messages will be sent to the ONT with appropriate headers added. The SIP User Agent, running inside the ONT, will route calls with the new telemetry headers to the TIU instead of the phone.

The media session of the Telemetry call is set up using the G.711 codec so that any specific in-band signalling between the utility company and the TIU can be transported.

The major requirement of this feature is flagging Telemetry calls so that appropriate headers can be added to the outgoing INVITE to the ONT.

The figure below illustrates the flow of a typical Telemetry call. The messages between the Utility Company Server and the CS200 are moving over either UT or ISUP trunks. Generic trunk messages are shown as UT and ISUP trunks use different messaging.

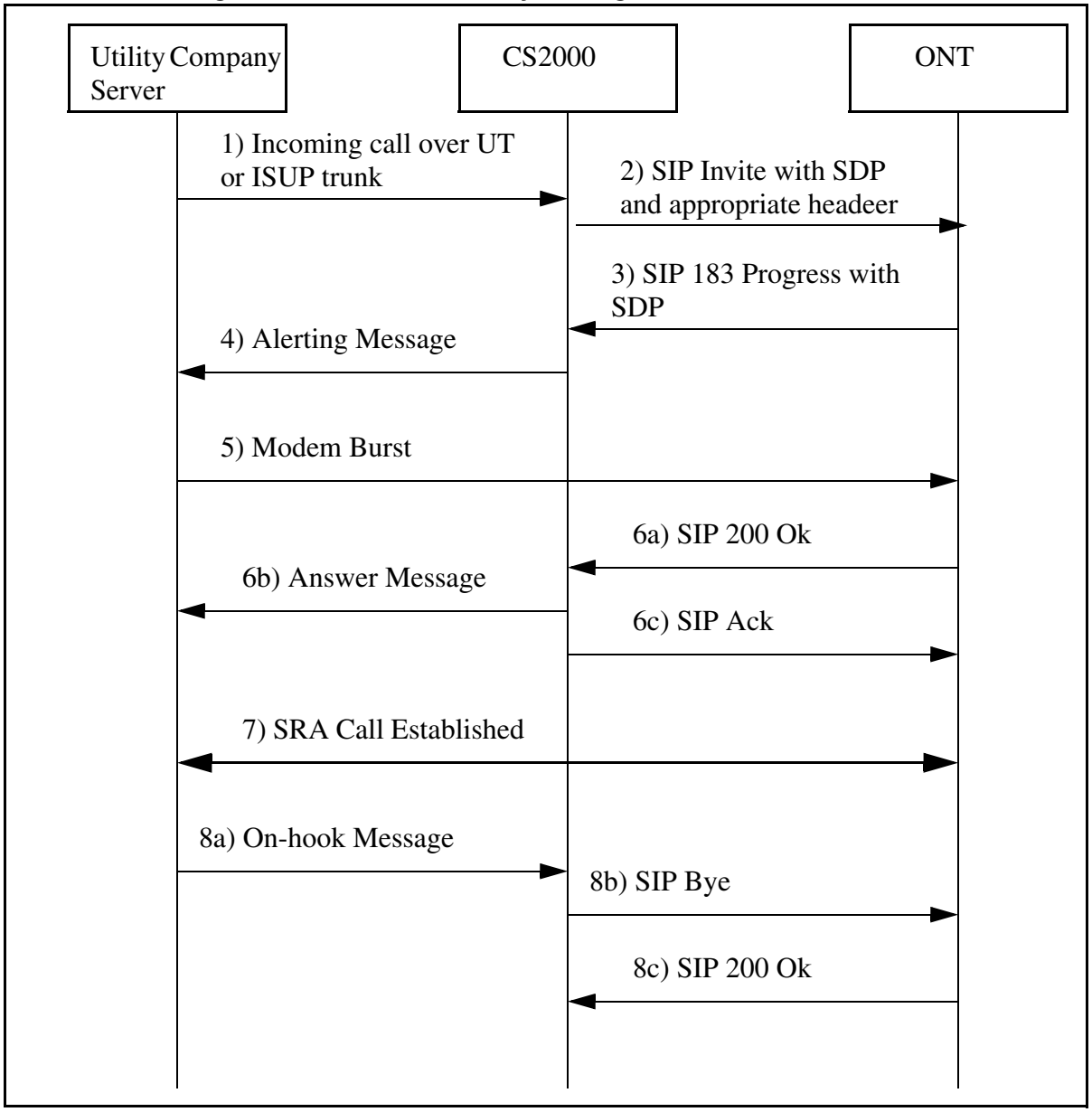
1. An incoming Telemetry call, which can either originate on a dedicated UTS-trunk or travel over an ISUP trunk, reaches the terminating CS2000. For ISUP trunks, this will be a IAM message; for UT trunks it will be an off-hook message followed by digits messages.
2. If the terminating line is a SIP line (has the DPL line option), a SIP Invite message is sent to the ONT. The INVITE contains the Require header "Require: x-suppressed-ringing". If the telemetry call is interruptible, resource-priority header will be added: "Resource-Priority: x-suppressed-

ringing.interruptible". If open-loop is configured, x-suppressed-ringing header will be added: "x-suppressed-ringing: open-loop=<value in seconds>"

The ONT, seeing the headers, knows this is a Telemetry call.

3. The media path must be established before the answer messages for Telemetry calls because the utility company servers send a modem burst which they expect to cause the ONT to go off-hook. For this reason, the initial SIP Invite will have SDP included. The ONT must send a 183 Progress message with SDP in response.
4. The CS2000 informs the originator that the media path is complete. For ISUP this will be a ACM message; for UT, a wink message is sent.
5. The originating server sends a modem burst to wake up the TIU off the ONT.
6. The ONT sends a 200 OK message which results in a answer message being sent to the originator. For ISUP, this is a ANM message; for UT, an off-hook. The CS2000 also sends an ACK back to the ONT.
7. At this point, the Telemetry call is up and the originating server interrogates the TIU.
8. In the usual case, the server initiates call shutdown by sending a on-hook message. This is communicated to the ONT via a SIP Bye message. The ONT acknowledges the Bye via a 200 Ok.

Figure 1 Common Telemetry Message Flow



142.2.1 CS2000 Core Provisioning

No new provisioning steps are introduced by this feature on the CS2000 Core. Some background on Telemetry may be useful however.

Telemetry calls are initiated from servers owned by utility companies. The calls can be completed in 2 ways: via the UTS or SRA methods.

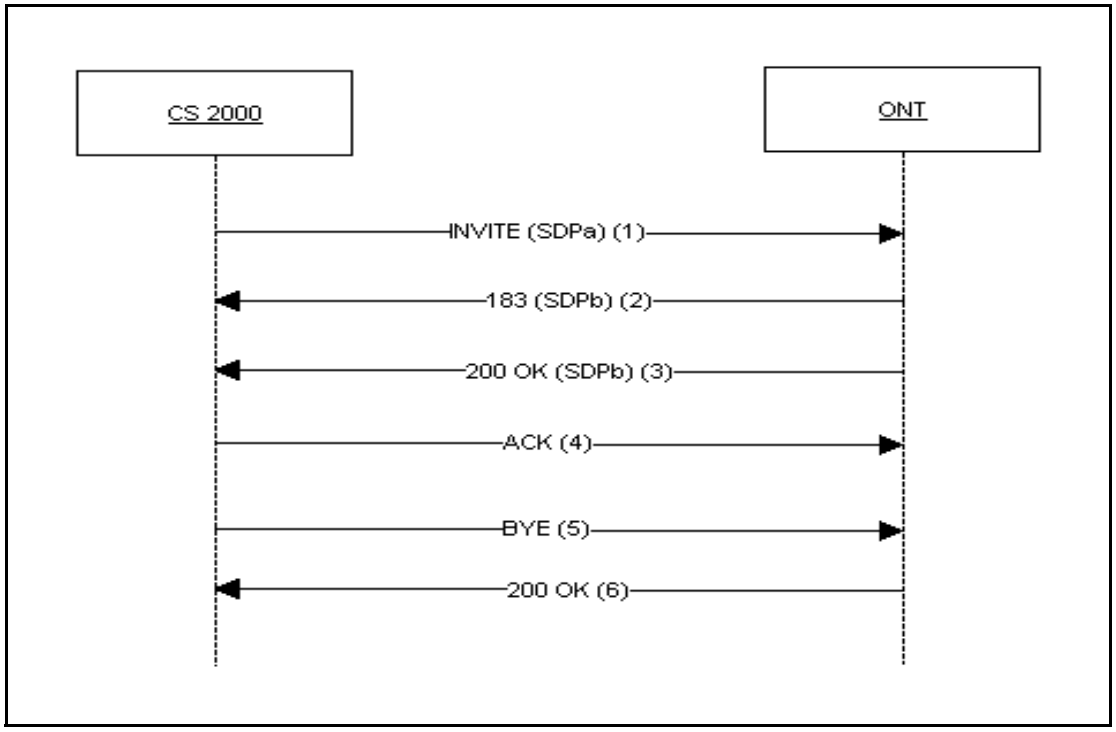
UTS Telemetry calls are made over dedicated UT trunks which directly connect the utility company servers to the terminating CS2000. When a call

arrives over a UT trunk, the UTS feature on the CS2000 suppresses ringing to the terminating line and connects the call.

SRA Telemetry calls have the same end result, suppressing ringing to the line, but can be initiated over ISUP trunks. In an SRA call, the originating server doesn't need to be directly connected to the terminating CS2000. SRA calls translate to a feature DN in table DNROUTE which starts the SRA feature. The SRA feature does some security screening, then extracts the subscriber's DN from the OCN parameter of the IAM message. It then ensures that the SRA line option is on the terminating line. Alternatively, Universal SRA can be enabled for the entire office.

142.2.2 Message Flow between CS2000 and the ONT

Figure 3: Telemetry Call Flows



The INVITE message will be changed as the part of this feature. The required changes are in bold text.

INVITE (from Session Manager to ONT), URI parameter and Require header added.

```
INVITE sip:sipln17@ssdv3.com:26052;maddr=47.104.26.178 SIP/2.0
 to: "sipln17 ssdev3" <sip:sipln17@ssdv3.com>
 from: <sip:sipln20@ssdv3.com>;tag=2072921334
```

call-id: 5fc6f0a2_1050c8843d0@zpvey0mg
cseq: 93972 INVITE
max-forwards: 20
x-nt-corr-id: 4114.010-15-31-36-38@127
x-nt-party-id: /sipln20
x-nt-location: 649
call-info: <http://zpvey0me:80/pa/direct/
pictureServlet?user=sipln20@ssdv3.com>;Purpose=icon
contact: <sip:sipln17@ssdv3.com:5060;maddr=47.104.26.180>
p-asserted-identity: <sip:1036320520@ssdv3.com>
remote-party-id: <sip:1036320520@ssdv3.com>;screen=yes;
party=calling;npi=NPI_UNKNOWN;ton=TON_NATIONAL
supported: com.nortelnetworks.firewall,p- 3rdpartycontrol,
nosec,com.nortelnetworks.im.encryption
Requires: x-suppressed-ringing
Resource-Priority: x-suppressed-ringing.interruptible //only when call is interruptible
x-Suppressed-Ringing: open-loop=30 // only when open-loop value is different than 0
content-length: 210
content-type: application/sdp

v=0
o=sipln20 3330185520 3330185520 IN IP4 47.102.245.46
s=-
e=unknown@invalid.net
t=0 0
m=audio 50002 RTP/AVP 0 8 18 110
c=IN IP4 47.102.245.46
a=rtpmap:18 G729/8000
a=rtpmap:110 telephone-event/8000

142.2.3 CPL Processing for telemetry call (Session Server)

CPL processing will be disabled for telemetry call since telemetry call is used do remote meter reading. It's not appropriate to forward Telemetry call to other devices such as cell phones or other telephone numbers.

142.3 Hardware Requirements or Dependencies

No new hardware dependencies are introduced beyond the existing requirements for Telemetry calls and SIP Lines.

142.4 Software Requirements or Dependencies

No new software dependencies are introduced beyond the existing requirements for Telemetry calls and SIP Lines.

142.5 Limitations and restrictions

- The CS2000 Session Server's branding/treatment will be disabled for Telemetry calls.
- The CS2000 Session Server's CPL processing will be disabled for Telemetry calls.

142.6 Interactions

Telemetry calls have documented interactions with other CS2000 voice features. Most of these interactions effectively disable other terminating features (such as Call Forwarding, SCRJ, etc). The UTS FN, found in PLS FMDOC under node NC0362FN, details these interactions.

The UTS and SRA Core features can be provisioned to be interruptible or non-interruptible. Traditionally, if a Telemetry call is interruptible, another incoming call to the terminating line will take precedence over the Telemetry call. This is accomplished by the CS2000 suspending the incoming call while it tears down the Telemetry call. However, SIP lines can support multiple call appearances. It has been decided, in agreement with the customer, that if a line is busy with a Telemetry call, subsequent incoming calls will always be offered to the line via a new SIP session.

The SRA Core feature has a *ACCESS* field in its DNROUTE tuple which can be set to NORING, OSI or RING. However, for DPL lines, the client (the ONT in this case) is responsible for ringing the line. As the values of the ACCESS tuple are not communicated to the client, the datafill in ACCESS will have no effect on DPL lines. It is expected that the clients will not ring the line for Telemetry calls.

A couple other interaction scenarios deserves mention. The first involves the Call Forward Don't Answer (CFD) feature. If a second call is established to a ONT line that is busy with a non-interruptible Telemetry call, the ONT will return a SIP 486 Busy message, not a 180 Ringing message. CFD will not be invoked and the call will not forward; the originator will not hear busy tone.

The second interaction involves a Telemetry call to a ONT line that is already busy with a call. Again, the ONT returns 486 Busy, not 180 Ringing. In this case the call will not complete; however, the originator will not get a busy tone.

Also note that call routing features (Personal Agent features) of the CS2K Session Server (MCS) are disabled on Telemetry calls.

142.7 Glossary

Term	Description
Telemetry	The science and technology of automatic measurement and transmission of data by wire, radio, or other means from remote sources, as from space vehicles, to receiving stations for recording and analysis.
UTS	Utility Telemetry Service
SRA	Suppressed Ringing Access
TIU	Telemetry Interface Unit

Term	Description
ONT	Optical Network Terminator

143: Functional Description (FN) A00012317

143.1 Feature name and Feature ID

A00012317 - Session Initiation Protocol (SIP) Services - Automatic Call Back (ACB) and Automatic Recall (AR)

143.2 Description

This activity provides support for Automatic Call Back (ACB) and Automatic Recall (AR), collectively called ACBAR, for Dynamic Packet Lines (DPL) using SIP.

The ACB service places a call to the last outgoing number dialed by the subscriber. The AR service places a call to the last incoming call to the subscriber. These numbers are stored in the outgoing and incoming call memories respectively.

If the number to be dialed (destination line) is busy, the CS2000 provides an announcement to the ACBAR subscriber, indicating that the line is busy, and that he will be notified with special ringing when the destination line is free. The CS2000 monitors the destination line until it goes idle. The CS2000 then rings the ACBAR subscriber, with a special ringing cadence indicating that it is an ACBAR recall notification. The number of the destination line may also be displayed on the ACBAR subscriber's phone, giving him an indication of which line is now free, as the ACBAR subscriber can have multiple ACBAR instances active.

When the ACBAR subscriber answers the notification, the CS2000 performs a final busy/idle check on the destination line, to make sure it has not gone busy within the interval of recalling the ACBAR subscriber. If the destination line is still idle, the CS2000 places the call to the destination line. If the destination line is busy again, the CS2000 provides an announcement indicating the condition, and that the ACBAR subscriber will be notified with special ringing when the destination line is free. This behavior continues until the call is placed successfully to the destination line, or the ACBAR subscriber cancels the ACBAR request, or the T6 or T10 timer expires indicating that the CS2000 has monitored the line for the maximum allowed time and automatically cancels the request.

Refer to BellCore/Telcordia TR-00215 and TR-00227 for information on the ACB and AR feature descriptions.

143.3 User Agent Requirements

In order to be integrated with the CS2000 ACB/AR service, the User Agent (UA) must be able to support the interface specified by this feature. A User Agent must be able to handle SIP Refer and Hold methods, and SIP Slow Start Termination procedures. To be able to provide the CS2000 ACB/AR service fully, they must also support caller id, distinctive ringing and name/number privacy. Supporting number privacy includes supporting a nested SIP p-asserted-identity header in the SIP REFER message.

The User Agent should not allow ACB/AR feature access codes to be used as the forward-to DN for User Agent based Redirection Services. The User Agent should not allow ACB/AR feature access codes to be used as the transfer-to DN as part of User Agent based Blind Call Transfer services.

143.4 Hardware Requirements or Dependencies

Not applicable.

143.5 Software Requirements or Dependencies

Not applicable.

143.6 Limitations and restrictions

143.6.1 AR To Busy Private Destinations

If the last number to call a SIP line was a private number, the SIP subscriber will be able to activate AR to that private destination DN if that DN is idle at the time of activation. If the destination DN is not idle at the time of AR activation by a SIP line, the AR request will not be honored, and the SIP subscriber will receive long term denial treatment. This is due to the fact that the REFER method is used to setup the call to a destination DN after that DN was busy, and subsequently went idle. The REFER method requires the destination DN be provided in the REFER method, as the REFER-TO number. This means that a private DN would be delivered to a User Agent, which is considered untrusted Customer Premise Equipment (CPE). Delivering Private DNs to CPE is an exposure to the privacy of the destination DN, and can lead to legal actions by the subscriber requiring privacy.

143.6.2 ACB To Busy Private Destinations

The same restriction described for AR in section 143.6.1, also applies to ACB. This is due to the fact that a SIP subscriber can successfully AR to a private destination DN. When this happens, the SIP subscribers outgoing call memory is updated with the destination's private DN. If the SIP subscriber subsequently activated ACB to the private destination DN, and that DN is idle, the ACB request will be honored and the call will go thru. However, if that private destination DN is busy at the time of ACB activation, the ACB request will not be honored, and the SIP subscriber will receive long term denial treatment for the same reasons described in section 143.6.1.

143.6.3 CNDB and ACB/AR For SIP Lines

If a SIP ACB subscriber has dialled the ACB access code to a busy destination, and either of the following conditions exists

1. prior to the last outgoing call, and the user dialed the CNDB access code, or,
2. prior to dialing the ACB access code, the user dialled the CNDB access code,

then ACB request will be honored, and the request will be queued. However, when the destination line goes idle, and the ACB user is recalled and answers the recall, the subsequent call that is setup to the destination line will have both the number and the name of the ACB user marked as private.

If a SIP AR subscriber has dialled the AR access code to a busy destination, and prior to dialling the AR access code the user dialled the CNDB access code, then AR request will be honored, and the request will be queued. However, when the destination line goes idle, and the AR user is recalled and answers the recall, the subsequent call that is setup to the destination line will have both the number and the name of the AR user marked as private.

143.6.4 ACBAR Provisioning Requirement

For ACBAR to be supported on a SIP User Agent, the User Agent must be provisioned with the SIP line option with at least at a value 2 for the MAX_NUM_CALLS field of the DPL Line option. This is a requirement due to the REFER mechanism used on Answer of the ACBAR recall ringing notification.

143.6.5 Redirect Attempts Using ACB/AR Vertical Service Codes

Use of ACB/AR feature access codes as the forward-to DN of a User Agent based Redirection Service is not supported by the CS2000.

143.6.6 User Agent Blind Transfer (REFER) Attempts Using ACB/AR Vertical Service Codes

Use of ACB/AR feature access codes as the transfer-to DN of a User Agent based Blind Transfer Service is not supported by the CS2000.

143.7 Interactions

143.7.1 ACBAR Interactions

Service Interactions involving SIP lines and ACBAR will be the same as those for non-SIP lines and ACBAR except where noted in this section.

143.7.2 Network Based Interactions

143.7.2.1 Destination Line - Network Determined Idle

If the CS2000 is monitoring a destination line for an ACBAR request, and that line is a SIP line, the line will be determined to be idle when there are no network based sessions for that line. User Agent based sessions and User Agent based services (e.g. Do Not Disturb) will not be taken into account by the CS2000.

143.7.2.2 ACB Subscriber - Network Determined Idle

If the CS2000 is about to recall notify a SIP ACBAR subscriber, that subscriber will be determined to be idle for recall when there are no network based sessions for that line. User Agent based sessions and User Agent based services (e.g. Do Not Disturb) will not be taken into account by the CS2000.

143.7.2.3 CLASS Call Memories

Incoming and Outgoing Call Memory (ICM, OCM) for a SIP subscriber will be updated in a consistent manner as normal CLASS and Centrex users. Only CS2000 handled originations and terminations will cause the Call Memories to be updated.

An exception is for User Agent based redirections. For User Agent based redirections (e.g. User Agent CFW), the OCM will not be updated by the extended leg to the remote DN. In other words, the OCM will not be updated to be the remote DN on a User Agent based redirection.

Click-to-Call feature operation will cause both the incoming and outgoing call memories to updated to the User Agent's own DN prior to answering the offered call at the User Agent's device. Once the offered call at the User Agent's device is answered, and call setup to the terminator occurs, the User Agent's OCM will be updated to the referred-to or dialed DN.

143.7.3 User Agent Interactions

143.7.3.1 ACBAR Distinctive Ringing

The ACBAR feature uses distinctive ringing for the recall notification to the ACBAR subscriber when the destination line is free. The distinctive ringing types used are specified in the following table:

Table 1 ACBAR Distinctive Ringing to SIP Alert Info mapping

SIP Alert Info Hdr	DMS Ring Code	NA Cadence (ms - 6 sec cycle)	UK & AUS Cadence (ms - 3 sec cycle)	DRING Datafill Ring Pattern
http://127.0.0.1/nortel/dst_ring_2	D	400 on, 200 off, 400 on, 200 off, 800 on, 4000 off	200 on, 200 off, 200 on, 400 off, 600 on, 1400 off	DRING 7

SIP Alert Info Hdr	DMS Ring Code	NA Cadence (ms - 6 sec cycle)	UK & AUS Cadence (ms - 3 sec cycle)	DRING Datafill Ring Pattern
http://127.0.0.1/nortel/dst_ring_6	4	1500 on, 500 off, 500 on, 3500 off	200 off, 800 on, 200 off, 200 on, 200 off, 400 on, 1000 off	DRING 3

The User Agent is responsible for generating distinctive ringing if it receives a SIP Alert Info Header with either of the above specifications.

143.7.3.2 Normal Call Termination Failure

If the CS2000 is attempting to terminate to a SIP line that the CS2000 has determined to be “network idle”, but the termination fails for any of the following reasons:

- User Agent not registered
- User Agent registered, but not responding
- User Agent registered, User Agent responds with busy indication (e.g. Do Not Disturb, or currently in dialing state),

the CS2000 will not offer the calling party the Special Delivery Service (SDS) busy service to activate ACB. The calling party will receive busy tone.

143.7.3.3 ACBAR Recall Notification Failure

If the CS2000 attempts to recall notify a SIP ACBAR subscriber, and that recall attempt fails due to any of the following:

- User Agent not registered
- User Agent registered, but not responding
- User Agent registered, User Agent responds with any response other than a “100 Trying” or “180 Ringing”, (e.g.busy indication due to Do Not Disturb, or currently in dialing state),

the CS2000 will check if the maximum number of recall notifications have been applied to the subscriber for the ACBAR request. If the maximum number of notifications have been applied for that request, the CS2000 will treat the request the same as any other request that has exhausted the recall applications, and terminate the ACBAR request. Otherwise the CS2000 will start the T2 timer, and upon timer expiration, will start the recall notification process again.

143.7.3.4 ACBAR Call Setup Failure

If the SIP ACBAR subscriber has answered the recall notification, and the CS2000 is attempting to setup the call to the destination line (using the REFER method), but the Call Setup request fails due to any of the following:

- User Agent not registered
- User Agent registered, but not responding
- User Agent registered, User Agent responds with anything other than a "202 Accepted" or "NOTIFY:Terminated" (e.g a busy/reject indication)

the CS2000 will check if the maximum number of recall notifications have been applied to the subscriber for the ACBAR request. If the maximum number of notifications have been applied for that request, the CS2000 will treat the request the same as any other request that has exhausted the recall applications and terminate the ACBAR request. Otherwise the CS2000 will start the T2 timer, and upon timer expiration, will start the recall notification process again.

143.7.3.5 ACB/AR Call Termination Failure

If the CS2000 is attempting to terminate to a SIP line because of an ACBAR request using Immediate processing, and the CS2000 has determined that SIP line to be "network idle", but the termination fails for any of the following reasons:

- User Agent not registered
- User Agent registered, but not responding
- User Agent registered, User Agent responds with busy indication (e.g. Do Not Disturb, or currently in dialing state),

the CS2000 will not offer the calling party the Special Delivery Service (SDS) busy service to activate ACB. The calling party will receive busy tone, and the request will be considered completed.

143.7.3.6 User Agent Consultative Transfer (REFER) Attempts Using ACB/AR Vertical Service Codes

If a SIP ACBAR User attempts to transfer a call using a User Agent Consult/ Transfer Capability, where the transfer-to DN dialed is an ACB/AR Vertical Service Code, the ACB/AR service will operate normally on the consult session of the SIP ACBAR User Agent.

For ACB, the number in the SIP User's outgoing call memory will be used as the transfer-to DN. If the transfer-to station is determined to be network idle by the ACB service, the consult session will be setup immediately. If the transfer-to station is determined to be network busy by the ACB service, the SIP ACBAR User Agent will receive the ACB confirmation treatment on the consult session. If the SIP ACBAR User attempted the transfer function (i.e. REFER) prior to or during the confirmation treatment, the transferred party will receive the ACB confirmation treatment. When both the SIP ACBAR User Agent and the transfer-to station are both idle, the SIP ACBAR User Agent will receive the recall notification.

For AR, the number in the SIP User's incoming call memory will be used as the transfer-to DN. If AR 2-level activation is in effect, the SIP ACBAR User Agent will receive the AR 2-level activation announcements on the consult session. If AR 1-level activation is in effect, or the SIP ACBAR User enters the acceptance digit for 2-level activation, and the transfer-to station is determined to be network idle by the AR service, the consult session will be setup immediately. If the transfer-to station is determined to be network busy by the AR service, the SIP ACBAR User Agent will receive the AR confirmation treatment. If the SIP ACBAR User attempted the transfer function (i.e. REFER) prior to or during two-level announcements, the transferred party will receive the AR two-level announcement and will be able to enter the acceptance digit. If the SIP ACBAR User attempted the transfer function (i.e. REFER) prior to or during the confirmation treatment, the transferred party will receive the confirmation treatment.When both the SIP ACBAR User Agent and the transfer-to station are both idle, the SIP ACBAR User Agent will receive the recall notification.

143.7.3.7 ACBAR Edge Condition Interaction Table

Table 2 ACBAR Edge Condition Interaction Scenario's

ACBAR Phase	ACBAR User Agent Network Line State	ACBAR User Agent Edge Condition	Description: A = ACBAR User B = Terminator	CS2000 non-SIP Line ACBAR User Equivalent	CS2000 SIP Line ACBAR User Result
Nodal and Internodal Activation using Immediate Processing Call Setup	IDLE	Not Registered or Registered but not responding	A is any line, B is SIP Line. A activates ACBAR to B. CS2000 attempts call setup with Immediate processing.	If the terminator becomes busy after the initial query but before call setup, the ACBAR user receives busy tone and the request is considered complete.	SIP ACBAR User receives busy tone and the request is considered complete.
Nodal and Internodal Delayed Processing Call Setup	IDLE	Not Registered or Registered but not responding	A is any line, B is SIP Line. A activates ACBAR to B. B is initially busy. B is queued on. B goes idle. A receives recall notification ringing, A answers recall. B loses network connectivity before CS2000 attempts call setup.	If the terminator becomes busy after the final busy/idle query but before call setup, the ACBAR user receives busy tone and the request is considered complete	SIP ACBAR User receives busy tone and the request is considered complete.

Table 2 ACBAR Edge Condition Interaction Scenario's

ACBAR Phase	ACBAR User Agent Network Line State	ACBAR User Agent Edge Condition	Description: A = ACBAR User B = Terminator	CS2000 non-SIP Line ACBAR User Equivalent	CS2000 SIP Line ACBAR User Result
Nodal and Internodal Activation using Immediate Processing Call Setup	IDLE	BUSY Dialing	A is any line, B is SIP Line. A activates ACBAR to B. CS2000 attempts call setup with Immediate processing. B is offhook dialing, User Agent responds with 486 BUSY.	If the terminator becomes busy after the initial query but before call setup, the ACBAR user receives busy tone and the request is considered complete.	SIP ACBAR User receives busy tone and the request is considered complete.
Nodal and Internodal Delayed Processing Call Setup	IDLE	BUSY Dialing	A is any line, B is SIP Line. A activates ACBAR to B. B is initially busy. B is queued on. B goes idle. A receives recall notification ringing, A answers recall. B goes offhook and begins dialling before CS2000 attempts call setup.	If the terminator becomes busy after the final busy/idle query but before call setup, the ACBAR user receives busy tone and the request is considered complete	SIP ACBAR User receives busy tone and the request is considered complete.
Nodal and Internodal Activation using Immediate Processing Call Setup	IDLE	BUSY (User Agent Do Not Disturb)	A is any line, B is SIP Line. A activates ACBAR to B. CS2000 attempts call setup with Immediate processing. B has User Agent Do Not Disturb activated. User Agent responds with 486 BUSY.	1) If the terminator has DND activated, the CS2000 will mark the response to the initial query with denied termination, which results in long term denial to the ACBAR User 2) If the terminator activates DND after the initial query but before call setup, the ACBAR User receives busy tone (or DND treatment) and the request is considered complete.	SIP ACBAR User receives busy tone and the request is considered complete.

Table 2 ACBAR Edge Condition Interaction Scenario's

ACBAR Phase	ACBAR User Agent Network Line State	ACBAR User Agent Edge Condition	Description: A = ACBAR User B = Terminator	CS2000 non-SIP Line ACBAR User Equivalent	CS2000 SIP Line ACBAR User Result
Nodal and Internodal Delayed Processing Call Setup	IDLE	BUSY (User Agent Do Not Disturb)	A is any line, B is SIP Line. A activates ACBAR to B. B is initially busy. B is queued on. B activates User Agent Do Not Disturb. B goes idle. A receives recall notification ringing, A answers recall. CS2000 attempts call setup. User Agent responds with 486 BUSY.	If the terminator activates DND during busy monitoring, the ACBAR User receives busy tone (or DND treatment) on the subsequent call setup and the request is considered complete.	SIP ACBAR User receives busy tone and the request is considered complete.
Nodal and Internodal Activation using Immediate Processing Call Setup	IDLE	Forwarded (User Agent Call Forwarding Active)	A is any line, B is SIP Line. A activates ACBAR to B. CS2000 attempts call setup with Immediate processing. B has User Agent Call Forwarding activated. User Agent responds with 302 Redirect.	1) If the terminator has CFV active or SCF active for the ACBAR User's number during the initial query process, the ACBAR User will receive short term denial annc. 2)If the terminator activates call forwarding after the initial query, but before the call setup, then on call setup, Call Forwarding procedures will take precedence, that is, the "ACBAR call setup" call will be forwarded to the remote station.	ACBAR Call Setup attempt from SIP ACBAR User to 'B' will be forwarded to the remote station.

Table 2 ACBAR Edge Condition Interaction Scenario's

ACBAR Phase	ACBAR User Agent Network Line State	ACBAR User Agent Edge Condition	Description: A = ACBAR User B = Terminator	CS2000 non-SIP Line ACBAR User Equivalent	CS2000 SIP Line ACBAR User Result
Nodal and Internodal Delayed Processing Call Setup	IDLE	Forwarded (User Agent Call Forwarding Active)	A is any line, B is SIP Line. A activates ACBAR to B. B is initially busy. B is queued on. B has User Agent Call Forwarding activated. B goes idle. A receives recall notification ringing, A answers recall. CS2000 attempts call setup. User Agent responds with 302 Redirect.	If the terminator activates call forwarding during busy monitoring then on the subsequent call setup, Call Forwarding procedures will take precedence, that is, the "ACBAR call setup" call will be forwarded to the remote station.	ACBAR Call Setup attempt from SIP ACBAR User to B will be forwarded to the remote station.
Nodal and Internodal Activation using Immediate Processing Call Setup	IDLE	User Agent SCRJ active or SCA active (resulting in rejection treatment)	A is any line, B is SIP line. A activates ACBAR to B. CS2000 attempts call setup. User Agent responds with 3xx redirect response, or 4xx busy response or connects to rejection announcement, depending on rejection treatment configuration	If the terminator has SCRJ active for the ACBAR User's DN during the initial query process, a call to the terminator will be set up immediately, resulting in the ACBAR User receiving rejection treatment.	SIP ACBAR User receives rejection treatment. This may be busy tone for 4xx response, or forwarding for 3xx response, or rejection announcement depending on rejection treatment configuration

Table 2 ACBAR Edge Condition Interaction Scenario's

ACBAR Phase	ACBAR User Agent Network Line State	ACBAR User Agent Edge Condition	Description: A = ACBAR User B = Terminator	CS2000 non-SIP Line ACBAR User Equivalent	CS2000 SIP Line ACBAR User Result
Nodal and Internodal Delayed Processing Call Setup	IDLE	User Agent SCRJ active or SCA active (resulting in rejection treatment)	A is any line, B is SIP Line. A activates ACBAR to B. B is initially busy. B is queued on. B has User Agent SCRJ or SCA activated. B goes idle. A receives recall notification ringing, A answers recall. CS2000 attempts call setup. SIP User Agent responds with 3xx redirect response, or 4xx busy response or connects to rejection announcement, depending on rejection treatment configuration	If the terminator activates SCRJ or SCA during busy monitoring then on the subsequent call setup, the Ragor will receive rejection treatment.	SIP ACBAR User receives rejection treatment. This may be busy tone for 4xx response, or forwarding for 3xx response, or rejection announcement depending on rejection treatment configuration
Notification Recall Ringing	IDLE	Not Registered or Registered but not responding	A is SIP line, B is any line. A activates ACBAR to B. B is busy and is queued on. A loses connectivity during busy monitoring. B goes idle, and the CS2000 attempts recall ring notification to A.	If the ACBAR User goes offhook just prior to recall ringing notification, then if the maximum number of recall notification applications has been attempted, the request is considered complete. Otherwise, timer T2 is started, and on T2 expiry, recall notification is attempted again.	If no response is received from the SIP User Agent on recall notification attempt, then if the maximum number of recall notification applications has been attempted, the request is considered complete. Otherwise, timer T2 is started, and on T2 expiry, recall notification is attempted again.

Table 2 ACBAR Edge Condition Interaction Scenario's

ACBAR Phase	ACBAR User Agent Network Line State	ACBAR User Agent Edge Condition	Description: A = ACBAR User B = Terminator	CS2000 non-SIP Line ACBAR User Equivalent	CS2000 SIP Line ACBAR User Result
Notification Recall Ringing	IDLE	BUSY	A is SIP line, B is any line. A activates ACBAR to B. B is busy and is queued on. A goes offhook and starts dialing. B goes idle, and the CS2000 attempts recall ring notification to A. A's User Agent responds with 4xx BUSY.	If the ACBAR User goes offhook just prior to recall ringing notification, then if the maximum number of recall notification applications has been attempted, the request is considered complete. Otherwise, timer T2 is started, and on T2 expiry, recall notification is attempted again.	If 4xx BUSY response is received for the recall notification attempt, then if the maximum number of recall notification applications has been attempted, the request is considered complete. Otherwise, timer T2 is started, and on T2 expiry, recall notification is attempted again
Notification Recall Ringing	IDLE	BUSY DND (Session Server Advanced Services Do Not Disturb)	A is SIP line, B is any line. A activates ACBAR to B. B is busy and is queued on. A has Session Server Do Not Disturb active. B goes idle, and the CS2000 attempts recall ring notification to A.	If the ACBAR User has CS2000 DND active at the time of recall notification, the CS2000 will continue with the recall notification and ring the line with ACBAR special ringing.	If the SIP ACBAR User has Session Server DND active at the time of recall notification, then the CS2000 will continue with the recall notification and ring the line with ACBAR special ringing. The notification will not be rejected.

Table 2 ACBAR Edge Condition Interaction Scenario's

ACBAR Phase	ACBAR User Agent Network Line State	ACBAR User Agent Edge Condition	Description: A = ACBAR User B = Terminator	CS2000 non-SIP Line ACBAR User Equivalent	CS2000 SIP Line ACBAR User Result
Notification Recall Ringing	IDLE	BUSY (User Agent DND)	A is SIP line, B is any line. A activates ACBAR to B. B is busy and is queued on. A has User Agent DND active. B goes idle, and the CS2000 attempts recall ring notification to A. A's User Agent responds with 4xx BUSY.	No equivalent scenario.	If 4xx BUSY response is received for the recall notification attempt, then if the maximum number of recall notification applications has been attempted, the request is considered complete. Otherwise, timer T2 is started, and on T2 expiry, recall notification is attempted again
Notification Recall Ringing	IDLE	Session Server Advanced Services CFW active	A is SIP line, B is any line. A activates ACBAR to B. B is busy and is queued on. A has Session Server CFW active. B goes idle, and the CS2000 attempts recall ring notification to A.	If the ACBAR User has CS2000 DND active at the time of recall notification, the CS2000 will continue with the recall notification and ring the line with ACBAR special ringing.	If the SIP ACBAR User has Session Server CFW active at the time of recall notification, then the CS2000 will continue with the recall notification and ring the line with ACBAR special ringing. The notification will not be forwarded.

Table 2 ACBAR Edge Condition Interaction Scenario's

ACBAR Phase	ACBAR User Agent Network Line State	ACBAR User Agent Edge Condition	Description: A = ACBAR User B = Terminator	CS2000 non-SIP Line ACBAR User Equivalent	CS2000 SIP Line ACBAR User Result
Notification Recall Ringing	IDLE	User Agent CFW active	A is SIP line, B is any line. A activates ACBAR to B. B is busy and is queued on. A has User Agent CFW active. B goes idle, and the CS2000 attempts recall ring notification to A. A's User Agent responds with 3xx REDIRECT	No equivalent scenario.	If 3xx REDIRECT response is received for the recall notification attempt, the redirect attempt will not be honored. If the maximum number of recall notification applications has been attempted, the request is considered complete. Otherwise, timer T2 is started, and on T2 expiry, recall notification is attempted again
Notification Recall Ringing	IDLE	Session Server Advanced Services Call Screening (SCRJ) active	A is SIP line, B is any line. A activates ACBAR to B. B is busy and is queued on. B is in A's Session Server SCRJ list. B goes idle, and the CS2000 attempts recall ring notification to A.	If the ACBAR User has CS2000 SCRJ active at the time of recall notification, and the terminator's DN is in the SCRJ list, the CS200 will continue with the recall notification and ring the line with ACBAR special ringing.	If the SIP ACBAR User has Session Server SCRJ active, with the terminator's DN on the SCRJ list, at the time of recall notification, then the CS2000 will continue with the recall notification and ring the line with ACBAR special ringing. The notification will not be rejected.

Table 2 ACBAR Edge Condition Interaction Scenario's

ACBAR Phase	ACBAR User Agent Network Line State	ACBAR User Agent Edge Condition	Description: A = ACBAR User B = Terminator	CS2000 non-SIP Line ACBAR User Equivalent	CS2000 SIP Line ACBAR User Result
Notification Recall Ringing	IDLE	User Agent Call Screening (SCRJ) active	A is SIP line, B is any line. A activates ACBAR to B. B is busy and is queued on. B is in A's SCRJ list on A's User Agent. B goes idle, and the CS2000 attempts recall ring notification to A. A's User Agent responds with 3xx redirect response, or 4xx busy response or connects to rejection announcement, depending on rejection treatment configuration	No equivalent scenario.	If 3xx REDIRECT response is received for the recall notification attempt, the redirect will not be honored.If a 3xx or 4xx BUSY response is received for the recall notification attempt, then if the maximum number of recall notification applications has been attempted, the request is considered complete. Otherwise, timer T2 is started, and on T2 expiry, recall notification is attempted again

143.1 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

143.2 Glossary

Term	Description
New term	Definition

144: Functional Description (FN) A00012321

144.1 Feature name and Feature ID

A00012321 - SIP Services: Long Distance Alerting (LDA)

144.2 Description

This feature integrates the LDA feature with SIP Lines. The LDA feature provides distinctive ringing patterns for calls determined to be long distance. Provisioning LDA has not been impacted, follow the existing LDA guidelines to configure LDA.

The following table shows the Nortel recommended cadences and SIP Alert Info Header for each of the configurable tones on the DMS.

Table 1 CM Ring Char to SIP Alert Info mapping

LDA RING_PATTERN (table OFCENG)	SIP Alert Info Hdr	DMS Ring Code	NA Cadence (ms - 6 sec cycle)	UK & AUS Cadence (ms - 3 sec cycle)
LONG	http://127.0.0.1/nortel/standard_ring	0	2000 on, 4000 off	400 on, 200 off, 400 on, 2000 off
LONG_LONG	http://127.0.0.1/nortel/dst_ring_5	3	1500 on, 500 off, 1500 on, 2500 off	600 on, 2400 off
LONG_SHORT	http://127.0.0.1/nortel/dst_ring_6	4	1500 on, 500 off, 500 on, 3500 off	200 off, 800 on, 200 off, 200 on, 200 off, 400 on, 1000 off
LONG_SHORT_SHORT	http://127.0.0.1/nortel/dst_ring_7	5	1500 on, 500 off, 500 on, 500 off, 500 on, 2500 off	400 on, 800 off, 200 on, 200 off, 400 on 200 off, 200 on, 200 off 400 on
LONG_SHORT_MEDIUM	http://127.0.0.1/nortel/dst_ring_8	6	1500 on, 500 off, 500 on, 500 off, 1000 on, 2000 off	unused
MEDIUM_MEDIUM	http://127.0.0.1/nortel/dst_ring_1	C	800 on, 400 off, 800 on, 4000 off	600 on, 400 off, 600 on, 1400 off

Table 1 CM Ring Char to SIP Alert Info mapping

LDA RING_PATTERN (table OFCENG)	SIP Alert Info Hdr	DMS Ring Code	NA Cadence (ms - 6 sec cycle)	UK & AUS Cadence (ms - 3 sec cycle)
SHORT_SHORT_MEDIUM	http://127.0.0.1/nortel/dst_ring_2	D	400 on, 200 off, 400 on, 200 off, 800 on, 4000 off	200 on, 200 off, 200 on, 400 off, 600 on, 1400 off
SHORT_MEDIUM_SHORT	http://127.0.0.1/nortel/dst_ring_3	E	300 on, 200 off, 1000 on, 200 off, 300 on, 4000 off	200 on, 200 off, 600 on, 200 off, 200 on, 1600 off

The SIP client is responsible for generating call wait tones if it receives a SIP Alert Info Header while a call is in progress. If SIP client receives an alert-info header not listed in this table then standard_ring should be assumed by the client device:

SIP Alert Info Hdr	NA Cadence (ms - 6 sec cycle)
http://127.0.0.1/nortel/standard_ring	300 on
http://127.0.0.1/nortel/dst_ring_1	100 on, 100 off, 100 on
http://127.0.0.1/nortel/dst_ring_2	100 on, 100 off, 100 on, 100 off, 100 on
http://127.0.0.1/nortel/dst_ring_3	100 on, 100 off, 300 on, 100 off, 100 on

144.3 Hardware Requirements or Dependencies

Any SIP client supported on CS2000.

144.4 Software Requirements or Dependencies

none

144.5 Limitations and restrictions

The tones are limited to the set of tones listed in the following table.

144.6 Interactions

N/A

144.7 Applicable Customer Facing Sections

Fault Management

Logs

Alarms _____

Configuration

Data Schema _____

User Interface _____

Element Manager _____

Security _____

Service Order _____

Office Parameters _____

Accounting (Includes AMA billing) _____

Performance (Includes OMs) _____

144.8 Glossary

Term	Description

145: Functional Description (FN) A00012322

145.1 Feature name and Feature ID

A00012322 - Session Initiation Protocol (SIP) Services - Busy Line Verification (BLV)

145.2 Description

This activity extends the CS2000 End Office (EO) switch's BLV and Barge In (BI) capability to support SIP Dynamic Packet Lines (DPL). BLV provides a Public Switch Telephone Network (PSTN) Operator with the ability to verify if a line is in an idle or busy state. Utilizing the BLV connection, the PSTN operator may proceed to perform an emergency barge-in of a busy line if required. To establish a BLV connection, an incoming call is initiated by the Operator from Traffic Operator Position System (TOPS) Access Tandem (AT) to the EO. The EO bridges the Operator to the line to be verified. A scrambler circuit is inserted at the TOPS AT to ensure privacy during BLV. The Operator can choose to move to a BI connection by stopping the voice scrambling, at which time the Operator can engage in a conversation with the BLV line. The EO has no knowledge a BI connection has been established as no additional signaling is sent to the EO. However, the line hears an intermittent Operator presence tone every 10 seconds while the BI connection exists. This tone is sent inband from the TOPS AT. The Operator makes a determination of whether the line is in an idle or busy state by listening for scrambled tones or speech. If no tone or speech is detected, the Operator may conclude the line is in an idle state and/or move to a BI connection. If scrambled tones or speech is detected, the Operator may conclude the line is in an idle or busy state based on the nature of the tones and/or move to a BI connection.

In the EO, a BLV call is originated on an Operator (OP) trunk group that can be dedicated to operator verification or can be a combined toll completing/ verification trunk group. With a dedicated verification trunk group, all incoming calls are assumed to be BLV/BI calls. A dedicated verification OP trunk group is configured by datafilling field MODE to "VF" in table TRKGRP. With a combined toll completing/verification trunk group, verification calls must include leading prefix digits to identify the call as BLV/ BI. A combined toll completing/verification OP trunk group is configured by datafilling field MODE to "CV" in table TRKGRP. This activity does not introduce new provisioning requirements for BLV/BI to SIP DPL.

For SIP DPL, H.248 OP trunk groups and OP trunk groups configured on CS2000 legacy peripherals (i.e. XPM, SPM) are supported.

If the Operator initiates a BLV/BI call to a line that is in a busy state, the Operator is bridged into the existing call. With TDM lines, the bridged connection can be established using a Metallic Test Access (MTA) unit or can be established using a conference 3-port circuit. With Voice Over Internet Protocol (VoIP) lines, the bridged connection is always established using a conference circuit. BLV/BI for SIP DPL will also use a conference circuit to bridge the Operator. Therefore, conference circuits must be configured for BLV/BI to SIP DPL. The type of conference circuit required depends on the switch configuration:

- In a hybrid CS2000, where TDM and packet agencies exist, there is an existing restriction that H.248 OP trunks can *not* be used for BLV/BI to a TDM line or to any line involved in a call with at least one TDM agent (line or trunk). This activity is not addressing this restriction. Therefore in a hybrid CS2000, OP trunks for BLV/BI must be configured on an XPM or SPM. In this case, TDM conference ports are always used for BLV/BI and must also be configured.

  In a hybrid CS2000, the OP trunks must be configured on an XPM or SPM.

- In a packet only CS2000, an H.248 OP trunk will be configured as all the agencies are packet based. In this case, packet conference ports are used for BLV/BI.

  Only Audio Media Server (AMS) conference ports will be supported for BLV/BI to SIP DPL. The Universal Audio Server (UAS) is not supported.

The behavior of SIP DPL differs slightly from TDM/VoIP lines. SIP DPL use the SIP application layer control (signaling) protocol to create, modify and terminate sessions. A SIP DPL may have multiple sessions active at any given time. BLV/BI support for SIP DPL needs to take these SIP DPL specific behaviors/capabilities into consideration. Therefore, the BLV/BI capability provided by this activity for SIP DPL differs from the existing BLV/BI capability for TDM/VoIP lines. The following sections describe the new BLV/BI capability provided by this activity for SIP DPL.

145.2.1 BLV/BI Capability for Idle SIP DPL

The existing BLV/BI capability for TDM/VoIP lines establishes a bridge-tap connection to the TDM/VoIP line when in an idle state (i.e. onhook). The Operator listens for tones and/or speech while bridged. If the TDM/VoIP line goes offhook, the subscriber is not permitted to dial a new call. The Operator may choose to advance from a BLV connection to a BI connection by stopping the voice scrambling and then initiate a conversation with the subscriber.

With SIP DPL, it is not possible to establish this type of bridge-tap connection and a different approach is required. Rather than a bridge-tap connection, if the SIP DPL is determined to be idle, the Operator will be provided silent tone. A

connection will not be established with the SIP DPL. When the Operator disconnects, the OP trunk will be released.

This approach provides a behavior that is very similar to the BLV behavior for idle TDM/VoIP lines. With idle TDM/VoIP lines, the Operator hears silence while bridged and concludes the line is idle based on the silence. By providing silent tone for SIP DPL, the Operator will also be able to determine the SIP DPL is idle by listening. Impacts to the Operator's practices and procedures for BLV should be minimal (if any).

Note that with BLV to idle TDM/VoIP lines, there is a low runner scenario where the subscriber could go offhook during a BLV connection. The Operator could choose to advance to a BI connection at this time. Due to the nature of SIP lines, this capability is not provided for SIP DPL.

145.2.2 BLV/BI Capability for Busy SIP DPL

The existing BLV/BI capability for TDM/VoIP lines bridges the Operator to the busy call using a conference circuit or MTA (for TDM lines only). The busy call must meet a set of criteria before the Operator is bridged. If the bridging criteria is not met, busy line treatment is provided to the Operator.

BLV/BI to a busy SIP DPL will behave similar to TDM/VoIP lines with one key difference. A SIP DPL can have one or more sessions established when BLV/BI occurs. If only one session exists, that session will be checked to see if it meets the bridging criteria. If multiple sessions exist, the list of sessions will be searched to find a session that meets the bridging criteria. The bridging criteria for BLV/BI is the same criteria used for TDM/VoIP lines, with two exceptions:

- SIP DPL sessions can be in either an active or held state. The bridging criteria checking for SIP DPL will include a new criteria for an *active* session. BLV/BI will not bridge the Operator to a session that is held. The Operator will be bridged to a session in the *active* state only.

  It is possible the Operator will be bridged to an active session which is subsequently held. In this case, the BLV/BI connection will be bridged to a held connection. If the session becomes active again, the BLV/BI connection will persist.

- The three-way calling service is provided by the SIP DPL and is no longer a CS2000 Core based service. For SIP DPL, the Operator can be bridged to a three-way call if this service is being provided by the SIP DPL.

In the event a session can not be found that passes the bridging criteria, the Operator will be provided busy line treatment. This is consistent with the BLV/BI capability for TDM/VoIP lines, which provides busy line treatment if the call is not suitable for bridging. Note that a maximum of 10 SIP DPL sessions will be searched to find a suitable session for bridging.

The existing TDM/VoIP bridging criteria checking that will also be used for SIP DPL consists of, but is not limited to:

- The busy call must be in an answered state.
- No Complex Call Service can be actively running on the busy call.
- The connected party in the busy call cannot be an OP trunk group or Emergency Services (ES) trunk group.
- The busy call does not include an Attendant console.

While the Operator is bridged to the call, any of the parties involved in the call can disconnect. The action taken upon the detection of a disconnect is dependent on which party initiates the disconnect:

- If the Operator disconnects from the bridged connection, the conference circuit is removed and the remaining two parties are bridged back into a 2-party call.
- If the connected party disconnects while the Operator is bridged, the conference circuit is removed and the Operator and SIP DPL are bridged into a 2-party call.
- If the SIP DPL disconnects while the Operator is bridged, the Operator is provided silent tone and the connected party is released.

  This behavior for BLV/BI to a SIP DPL is different than the behavior for BLV/BI to a TDM/VoIP line. With a TDM/VoIP line, the Operator is reconnected to the idle line after the disconnect. The Operator can listen to the connection and determine the line has disconnected. With SIP DPL, the same functional behavior is provided by applying silent tone to the Operator.

145.2.3 BLV/BI Interactions with SIP DPL Maintenance States

With the BLV/BI capability for TDM/VoIP lines, the Operator is provided treatment if the line is in a maintenance state. BLV/BI for SIP DPL is consistent with this approach. If the SIP DPL is in a maintenance state, the Operator is provided treatment. The standard treatment associated with the SIP DPL's state is provided. At this time, the line maintenance states that apply to a SIP DPL include:

System Busy (SB), Man Busy (MB), Offline (INB),

Call Processing Busy Deload (CPD), LCD Busy (LMB)

145.3 Hardware Requirements or Dependencies

TDM and/or AMS conference ports must be configured as described in section "144.2 Description" on page 1430.

145.4 Software Requirements or Dependencies

Not applicable.

145.5 Interactions

145.5.1 CS2000 Core based Service Interactions

This section describes the interaction between BLV/BI and Core based services. These interactions are handled in consistently with BLV/BI to TDM/ VoIP lines. The key service interactions are described below (other service interactions may exist).

- Advanced Intelligent Network (AIN) Terminating Call Model (TCM) and Originating Call Mode (OCM) triggers are bypassed for BLV/BI.
- The Denied Termination (DTM) line option has no impact on BLV/BI calls. The Operator is conferenced to verify a SIP DPL line when the DTM line option is assigned.
- BLV/BI will not bridge to a call that has an active Lawful Intercept connection. Busy Line treatment is provided to the Operator.
- A BLV/BI call is not supported to a SIP DPL that has service suspended via the Suspended Service (SUS) or Plug Up (PLP) line options. Trouble intercept treatment (TRBL) and terminator suspended service (TESS) treatment are provided to the Operator respectively.
- A BLV/BI call is not supported to a SIP DPL that is assigned the No Double Connect (NDC) line option. Busy Line treatment is provided to the Operator.
- BLV/BI calls will not series complete if the SIP DPL has the Series Completion (SCMP) line option assigned. If at least one session exists for the SCMP SIP DPL when the BLV/BI call is received, an attempt will be made to conference the Operator to an existing session as described in section 144.2.2. If the SIP DPL is idle, silent tone is provided to the Operator as described in section 144.2.1.
- For MLH and DLH hunt groups, the BLV/BI call is always attempted on the pilot DN for the hunt group. For DNH and BNN hunt groups, the BLV/ BI call is always attempted on the dialed DN. The BLV/BI request will not hunt.

  If at least one session exists for the SIP DPL when the BLV/BI call is received, an attempt will be made to conference the Operator to an existing session as described in section 144.2.2. If the SIP DPL is idle, silent tone is provided to the Operator as described in section 144.2.1.
- Call forwarding services that *unconditionally* forward the call are not supported for BLV/BI. If a BLV/BI call is requested to a SIP DPL configured with a call forwarding *always* service, the Operator is provided busy line treatment.
- If the SIP DPL is busy with a call forward *busy* feature activated, the BLV/ BI call is not forwarded. Rather, an attempt will be made to conference the Operator to an existing session as described in section 144.2.2.

- When a BLV/BI connection is established to a busy call involving a SIP DPL with the Call Park or Directed Call Park line option, the call park capability is disabled. The SIP DPL can not park the call while the Operator is bridged. Feature action nack (NACK) treatment is provided to the Operator.
- When a BLV/BI connection is established to a busy call involving a SIP DPL with the Call Park or Directed Call Park line option, the call park capability is disabled. The SIP DPL can not park the call while the Operator is bridged. Feature action nack (NACK) treatment is provided to the Operator.
- When a BLV/BI connection is established to a busy call involving a SIP DPL configured with the Account (Acct) Code feature, the Acct Code feature is disabled for Flash Entry. A Flash Entry occurs when the SIP DPL flashes during an active call, dials the Acct Code feature access code followed by the account code, then flashes to re-join the active call. If the active call has a BLV/BI connection established, the Flash Entry is ignored and an IBN110 log is output indicating a BLV connection was in progress. Refer to activity A00012326, Auth/Account Codes support for SIP Lines, for further information on the IBN110 log.
- When a BLV/BI connection is established to a busy call involving a SIP DPL configured with the Authorization (Auth) Code feature, the Auth Code feature is disabled for Flash Entry. A Flash Entry occurs when the SIP DPL flashes during an active call, dials the Auth Code feature access code followed by the auth code, then flashes to re-join the active call. If the active call has a BLV/BI connection established, the Flash Entry is ignored and an IBN110 log is output indicating a BLV connection was in progress. Refer to activity A00012326, Auth/Account Codes support for SIP Lines, for further information on the IBN110 log.
- When a BLV/BI connection is established to a busy call involving a SIP DPL, the Malicious Call Hold (MCH) feature is disabled. The SIP DPL can not activate the MCH feature. Feature action nack (NACK) treatment is provided to the Operator.
- BLV/BI requests to SIP DPL in a call pickup group will bridge the Operator to the SIP DPL's busy call, even if that call was established through the call pickup service. The following call pickup services are supported for SIP DPL:

  — Call Pickup (CPU)

  — Directed Call Pickup (DCPU)

  — Night Service Trunk Answer From Any Station (TAFAS)

  — Directed Call Pickup with Barge-In (DCBI)

  With DCBI, when a barge-in connection is established involving a SIP DPL, there are two active sessions. Both sessions are considered eligible

for BLV and will be included in the criteria checking search (as described in “144.2.2 BLV/BI Capability for Busy SIP DPL” on page 1432.

145.5.2 SIP DPL (SIP Client) Service Interactions

This section describes the interaction between BLV/BI and SIP DPL (i.e. SIP Client) based services.

- The SIP DPL Blind Transfer and Consult Transfer capability is denied if any call leg involved in the transfer is a BLV/BI call. This restriction applies if the Operator is verifying the SIP DPL or the connected party in either call leg. The only exception is if the Operator is verifying a connected TDM line using an MTA, in which case the transfer request is not denied. Examples include, but are not limited to:

  — SIP DPL is involved in a two-party call with a TDM line. A BLV/BI call to the SIP DPL results in the Operator being conferenced to the call using a conference port. The SIP DPL attempts to blind transfer the TDM line.

  — SIP DPL is involved in a two-party call with a TDM line. A BLV/BI call to the TDM results in the Operator being conferenced to the call using a conference port. The SIP DPL attempts to blind transfer the TDM line.

    If the BLV/BI connection to the TDM line is established using the MTA, the transfer request will not be denied.

  — SIP DPL is involved in two calls. The first call leg is a BLV/BI call. In the second call leg, the SIP DPL is connected to another party. The SIP DPL attempts to consult transfer the other party on the second leg to the Operator.

  — SIP DPL is involved in two calls. In the first call leg, the SIP DPL is connected to another party. The second call leg is a BLV/BI call. The SIP DPL attempts to consult transfer the Operator to the other party in the first call leg.

- With 3WC and 6WC[1] using the Media Application Server (MAS), there is no guarantee a BLV/BI request for a SIP DPL controller will result in a connection with the controller.

  — As each call leg of a 6WC is established by an ONT controller, each call leg becomes suitable for bridging after answer is received. The controller can then place these call legs on hold, leaving them in the conference, while the controller establishes another new call leg. In this case, there is no indication the controller has left the conference. All call legs remain suitable for BLV/BI bridging. If a BLV/BI call is received for the controller while in this state, the Operator will be

[1]The Optical Network Terminal (ONT) uses the MAS for 6WC only. The PC Client uses the MAS for all conference configurations (e.g. 3WC, 6WC).

bridged to one of the call legs that is on hold in the conference even though the controller is not actively connected.

– The same interaction applies to a 3WC or a 6WC established by a PC Client controller.

— When the controller of a 6WC is an ONT and the controller disconnects, the conference is taken down.

– If a BLV/BI connection was established to the controller, the Operator will receive silent tone when the controller disconnects.

– If a BLV/BI connection was established to one of the other parties in the conference (i.e. other than the controller), the BLV/BI connection will persist after the controller disconnects.

— When the controller of a 3WC or 6WC is a PC Client and the controller disconnects, the conference remains active until all parties involved in the conference disconnect. Although the controller has disconnected, the controller still has active call appearances for each call leg of the conference.

– If a BLV/BI connection was established to the controller before the controller disconnected, the Operator will remain connected to the conference even though the controller has disconnected.

– If a BLV/BI connection was established to the controller after the controller disconnected, the Operator will be connected to one of the call legs even though the controller had previously disconnected.

145.6 Limitations and restrictions

The following limitations and restrictions apply to BLV/BI for SIP DPL:

- Only H.248 OP trunks and OP trunks configured on CS2000 legacy peripherals (i.e. XPM, SPM) are supported for BLV/BI to SIP DPL.
- In a hybrid CS2000, with TDM and packet agencies, there is an existing restriction that H.248 OP trunks can *not* be used for BLV/BI to a TDM line or to any line involved in a call with at least one TDM agent (line or trunk). This activity is not addressing this restriction. Therefore in a hybrid CS2000 with SIP DPL, the OP trunks must be configured on a CS2000 legacy peripheral (i.e. XPM, SPM).
  — H.248 OP trunks for BLV/BI are not supported in a hybrid CS2000. The OP trunks must be configured on an XPM or SPM.
  — TDM conference ports must be configured in the hybrid switch for BLV/BI.
- In a packet based (non-hybrid) CS2000 switch, packet conference ports must be configured for BLV/BI.

Only AMS conference ports are supported for BLV/BI. The Universal Audio Server (UAS) is not supported.

- A BLV/BI call to a busy SIP DPL searches for a suitable session to bridge. A maximum of 10 sessions will be searched to find a suitable session.
- If a BLV/BI request conferences into a multi-media session for a SIP DPL, the session will drop to a voice only connection. If the Operator subsequently drops out of the call and the SIP DPL is reconnected into a 2-party call with the other party, the multi-media capability is re-negotiated.
- When a conference circuit is inserted, the session's remote held status is not conveyed through the conference resource. As a result, the session's remote held status is not conveyed while a BLV/BI connection is active.

  This scenario can occur during a race condition where a BLV connection is established at the same time a remote hold is applied. This scenario can also occur if the session is placed on hold after the BLV/BI connection is established.
- Calls on H.248 Per-Trunk Signaling (PTS) trunks receiving a tone (e.g. treatment tone) are taken down over a Core warm restart. This behavior also applies to BLV/BI calls when the H.248 OP trunk is provided silent tone (i.e. when the BLV line is idle).
- During a Core maintenance cold or reload swact, BLV/BI calls are among those calls cleared in the Core. This includes the BLV/BI call leg on the OP trunk and the original 2-party call that was established between the BLV line and the connected party. Additionally, during the swact, the Gateway Controller (GWC) marks all call processing busy (CPB) calls (including BLV/BI calls) to be taken down when the next internal or external event occurs. It is possible an internal event may occur during the swact resulting in an immediate tear down of the associated CPB call in the GWC. But an internal event may not occur, which can result in the BLV/BI call and original 2-party call being cleared in the Core but persist in the GWC. However, these calls will persist in the GWC no longer than five minutes following the swact. After five minutes, an audit in the GWC will clear the calls. Note that whether an internal event occurs during the swact is unpredictable.
- BLV/BI is not supported to a busy call that involves a Multiple Appearance Directory Number (MADN) SIP DPL. The Operator is provided busy line treatment if either the BLV line or the connected party is a MADN SIP DPL.

145.7 Applicable customer facing sections

Fault Management

Logs	__n/a__
Alarms	__n/a__

Configuration

- Data Schema __n/a__
- User Interface __n/a__
- Element Management __n/a__
- Security __n/a__
- Service Order __n/a__
- Office Parameters __n/a__

Accounting (includes AMA billing) __n/a__

Performance (includes operational measurements) __n/a__

145.8 Glossary

Term	Description
3WC	3-Way Calling
6WC	6-Way Calling
AIN	Advanced Intelligent Network
AMS	Audio Media Server
BI	Barge In
BLV	Busy Line Verification
BUSY	Busy Line Treatment
CPD	Line Call Processing Busy Deload
CPU	Call Pick Up
CS2000	Call Server 2000
CWT	Call Waiting
DCPU	Directed Call Pickup
DMS	Digital Multiplex System
DPL	Dynamic Packet Lines
DTM	Denied Termination
EO	End Office
FPE	Feature Processing Environment
GWC	Gateway Controller

Term	Description
INB	Offline
IP	Internet Protocol
LMB	Line LCD Busy
MADN	Multiple Appearance Directory Number
MAS	Media Application Server
MB	Man Busy
OP	Operator
PSTN	Public Switch Telephone Network
PTS	Per Trunk Signaling
SB	System Busy
SCA	Single Call Arrangement
SS	Session Server
TAFAS	Trunk Answer From Any Station
TCM	Terminating Call Model
UAS	Universal Audio Server
VoIP	Voice over IP

146: Functional Description (FN) A00012323

146.1 Feature name and Feature ID

Feature ID: A00012323

Session Initiation Protocol (SIP) Services:
- Directed Call Pickup with Barge-in (DCBI)
- Directed Call Pickup Barge-in Exempt (DCBX)

146.2 Description

This activity extends the CS2000 End Office (EO) switch's DCBI and DCBX capability to support Dynamic Packet Lines (DPL) using the SIP functional protocol.

Directed Call Pickup - Barge In (DCBI) permits an IBN station to pick up a ringing intragroup call without for a line within the same customer group. If the called station answers the call before the instigating party completes the call pickup sequence, the instigating party can barge in to the answered call, resulting in a conference state.

An optional warning tone can be applied to both parties of the existing call before the activating station is barged-in. Application of this tone is a customer group option in table CUSTSTN. The DCBI tone consists of 440 Hz at -13dbm.

A called station with directed call pickup barge-in exempt (DCBX) can block any attempts by another station with DCBI to barge in (the caller hears reorder tone).

A called station with directed call pickup exempt (DCPX) can block any attempts by another station to either barge in or pick up the call (the caller hears reorder tone).

Dynamic Packet Line (DPL) Support:

> ***Note:*** In this document, DPL lines are synonymous with Session Initiation Protocol User Agents (SIP UAs).

For the purposes of further discussion into the individual behaviors, the following terms are used:
- A - the calling party of the original call (originator)
- B - the barge-in target (BI target)
- C - the barge-in instigator (BI instigator)

146.2.1 Barge-in target is not DPL

If the BI target is not DPL, then the existing method of using CS2000 controlled 3 port conference circuits will be used. The type of conference circuit chosen, whether Audiocodes Media Server (AMS) or Maintenance Trunk Module (MTM) based, will depend on the agent type of the BI instigator. For SIP DPL lines, the preference will be AMS if available. The barge-in tone, if provisioned against the customer group in table CUSTSTN (DCBITONE) will be applied to the conference circuit.

All DCBI behavior will be consistent with TDM and packet agents, including the limitation that the BI target will not be considered the conference controller when the calls have reached a conferenced state. Flashes from the BI target will be ignored, and should any party disconnect, the call will collapse into a two party call between the remaining agents.

146.2.2 Bargein target is DPL

146.2.2.1 DCBI Behavior

If the barge-in target is a DPL line, the DCBI behavior is extended to make use of the Session Initiation Protocol's (SIP's) ability to request a new INVITE message to the BI target, with a JOIN header to remotely join this new call to the existing BI target call using the SIP A's conferencing abilities. Once the INVITE/JOIN request has been sent, the CS2000 will view the resulting topology as two independent active calls on two separate DPL instances.

When the BI target is DPL, it will be up to the SIP UA to either handle or reject the request. All subsequent messages following the INVITE/JOIN will be handled by standard call processing.

Once the barge-in request has been completed and a remote conference has been formed, the DPL BI target will become the conference controller. The SIP UA will then be in charge of the topology of the call, and can either:

- Drop one leg of the conference, either by refusing the request or by handling a flash request.
- Request that the originator be REFER'd to the instigator.

Barge-in Tone:

Barge-in tone must be provided by the SIP UA. The CS2000 will not.

> ***Note:*** Due to the nature of barge-in on SIP UAs that support remote conferencing, the application of the barge-in warning tone is not under the control of the CS2000. According to GR-590, the barge-in warning tone is only required to be played to the user being barged in on, which differs from the legacy DMS implementation of the DCBI service which played the tone to both users on the original call. The implementation of barge-in

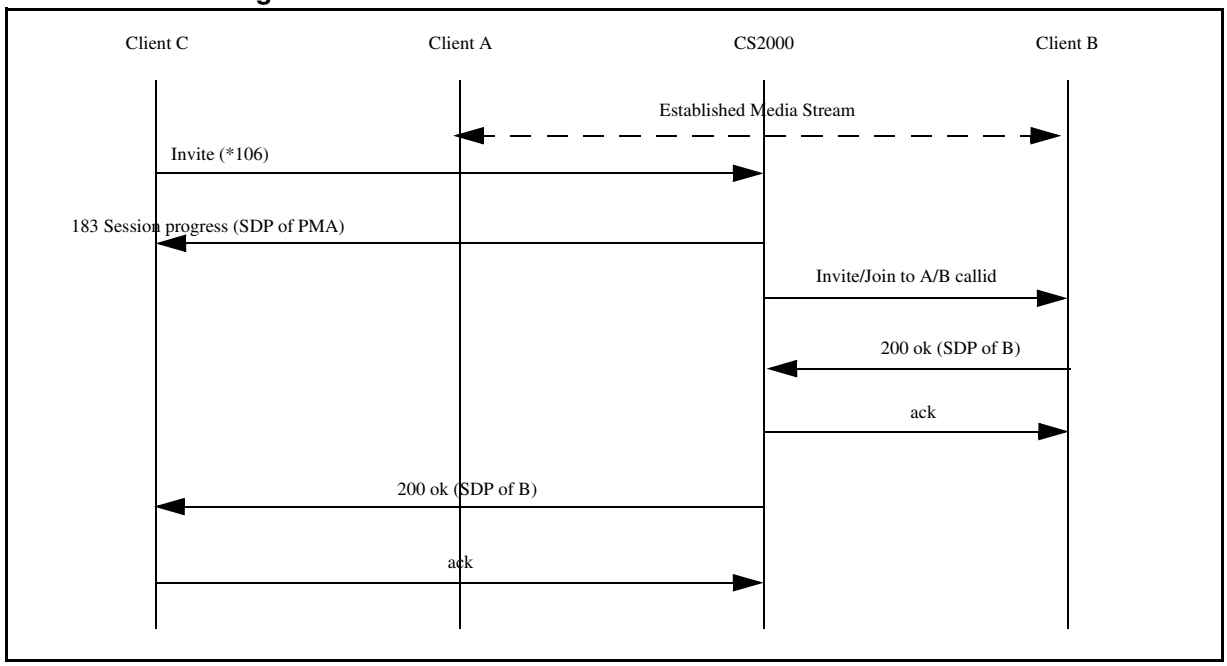
in the SIP UA is out of the control of the CS2000 and is likely to be more GR compliant than is the legacy DMS service.

Remote Conference Transcoding:

It will be a function of the SIP UA to handle SDP re-negotiation in the event that the transcoding (code and packetization rate) in use for existing call are incompatible with the SDP of the BI instigator. The customer should ensure that in all cases, there is a common transcoding algorithm that can apply to all parties.

146.2.2.2 DCBI Message Sequence Chart

Figure 1 Invite/Join MSC



146.2.3 DCPX/DCBX

If either Directed Call Pickup Exempt (DCPX) or Directed Call Pickup Barge-in Exempt (DCBX) is assigned to the BI target, the bargein attempt will not be allowed. The instigator will receive NACK treatment.

146.2.4 Provisioning

DCBI is provisioned in the core against the instigator's line. Once provisioned, DCBI can be used to either pick up or barge in on calls within the same customer group. To block DCBI, either DCPX or DCBX must be assigned to the target line.

146.3 Hardware Requirements or Dependencies

None.

146.4 Software Requirements or Dependencies

In order to use the DPL remote conferencing abilities, the SIP User Agent (UA) must support the following SIP messages:

- The INVITE message with a JOIN header as specified in the IETF Join RFC3911.

  - required in order to remotely join the instigating party to the existing call
- The REFER message as specified in the IETF Refer specification RFC3515.
- The ability to provision and apply a barge-in tone prior to joining the instigator to the existing call (if desired).

146.5 Limitations and restrictions

The following limitations and restrictions apply to DCBI/DCBX for SIP DPL:

- All limitations and restrictions for Directed Call Pickup (non barge-in) for SIP DPL lines as documented in a00012308 are inherited by this activity.
- All TDM DCBI/DCBX limitations and restrictions are inherited by this activity, unless otherwise noted.
- Limitations and restrictions for when the bargein target is SIP DPL:
  - The SIP UA will need to be configured to apply the bargein tone if required. The changing of the CS2000 provisioning of the DCBI warning tone will have no impact on the presence or absence of the tone when barging into a SIP UA agent.
  - Bargein will only be supported for SIP UAs that support the JOIN header in the INVITE message.
  - DCBI barge-in is only supported if there is at most one other active session on the BI target when the DCPU/DCBI VSC is processed. This is consistent with TDM in blocking the DCPU or DCBI of a CWT call, whether ringing or answered.
  - DCBI is not supported unless the SIP DPL BI target is assigned the DPL option with MAX_NUM_CALLS greater than one.
  - It will be up to the SIP UA to renegotiate SDP to address transcoding incompatibilities between the original call and the DCBI instigator when processing the INVITE/JOIN request if required.
  - In order for the bargein target to exit the call and collapse the remaining agents to a 2 party call, that SIP UA must support the REFER message.
  - A FRLS of the bargein target DN will tear down both call legs.
  - The CS2000 will make every attempt to not initiate a bargein session that is on hold, but that could occur in certain race conditions. This

can be avoided if the client rejects the INVITE w/JOIN if an attempt is made to JOIN a session that the client believes to be on hold.

— If the SIP UA does not properly support the JOIN header but does not reject the INVITE with the JOIN header the CS2000 will tear down the call and route the DCBI invoker to treatment upon receipt of an alerting indication in the CS2000. This is to prevent unexpected behavior of the service on non-compliant SIP UAs.

- Limitations and restrictions for when the instigator is SIP DPL:

  — DCBI instigation is allowed only if the instigator has no other calls, either active or held.

146.6 Interactions

146.6.1 Three way calling (3WC)

If the SIP DPL is involved in a 3WC, barge-in is not allowed.

146.6.2 Call Waiting

In TDM, DCBI cannot be used to barge in on a call where call waiting is being applied.

146.6.3 Session Server (SS) Service Interactions

Personal agent based services provided by the Session Server do not apply when a call is being terminated to a SIP DPL line for barge-in.

146.7 Applicable customer facing sections

Fault Management

Logs	___n/a___
Alarms	___n/a___

Configuration

Data Schema	___n/a___
User Interface	___n/a___
Element Management	___n/a___
Security	___n/a___
Service Order	___n/a___
Office Parameters	___n/a___

Accounting (includes AMA billing)	___n/a___
Performance (includes operational measurements)	___n/a___

146.8 Glossary

Term	Description
AMS	Audio Media Server
BI	Barge In
BLV	Busy Line Verification
BUSY	Busy Line Treatment
CPU	Call Pickup
CS2000	Call Server 2000
CWT	Call Waiting
DCPU	Directed Call Pickup
DCBX	Directed Call Pickup Bargein Exempt
DCPX	Directed Call Pickup Exempt (also blocks bargein)
DMS	Digital Multiplex System
DPL	Dynamic Packet Lines
DTM	Denied Termination
EO	End Office
FPE	Feature Processing Environment
INB	Offline
LMB	Line LCD Busy
MADN	Multiple Appearance Directory Number
MB	Man Busy
MTM	Maintenance Trunk Module
PSTN	Public Switch Telephone Network
SB	System Busy
SS	Session Server
TCM	Terminating Call Model
UAS	Universal Audio Server
VSC	Vertical Services Code (activation code)

147: Functional Description (FN) A00012325

147.1 Feature name and Feature ID

A00012325 - SIP Lines: Teen Line

147.2 Description

This activity provides CS2K support for SIP lines for Teen Service. Teen Service refers to the SDN option, which allows multiple DNs to be associated with one line - each such DN has an associated ringing pattern. The SDN option has additional sub-options available on a per-DN basis.

147.3 UA Interactions & Requirements

If the UA is not registered, calls attempting to terminating to it are unaffected by this feature.

If the UA does not respond to an INVITE, calls attempting to terminating to it are unaffected by this feature.

If the UA rejects an INVITE, calls attempting to terminating to it are unaffected by this feature.

The UA used for this feature must support all requirements placed on DPL UA. Additionally, since the UA provides the actual ringing and the call waiting tones, and Teen Line makes use of distinctive ringing patterns and distinctive call waiting tones, there must be a way of informing the UA agent of which ringing pattern/call waiting tone should be used.

The way is the SIP Alert Info header in the SIP INVITE method. The Session Server is responsible for mapping the GCP tone into the proper SIP tone based on the client device (vendor specific tones). The following tables describe the tone definitions and the default mapping, as well as two internal mappings.

The UA is responsible for generating the alerting tone if it receives a SIP Alert Info header in a SIP INVITE method if no call is already in progress.

The UA is responsible for generating call wait tones if it receives a SIP Alert Info header in a SIP INVITE method while a call is already in progress.

Table 1 SDN to SIP Alert Info mapping - ringing

SDN Provisioned Ring Value	NA Cadence (ms - 6 sec cycle)	UK & AUS Cadence (ms - 3 sec cycle)	DMS Ring Code	GCP Local New Call Data	Default SIP Alert Info Hdr
0	2000 on, 4000 off	400 on, 200 off, 400 on, 2000 off	0	standard_ring	http://127.0.0.1/ nortel/standard_ring
1	800 on, 400 off, 800 on, 4000 off	600 on, 400 off, 600 on, 1400 off	C	dst_ring_1	http://127.0.0.1/ nortel/dst_ring_1
2	400 on, 200 off, 400 on, 200 off, 800 on, 4000 off	200 on, 200 off, 200 on, 400 off, 600 on, 1400 off	D	dst_ring_2	http://127.0.0.1/ nortel/dst_ring_2
3	300 on, 200 off, 1000 on, 200 off, 300 on, 4000 off	200 on, 200 off, 600 on, 200 off, 200 on, 1600 off	E	dst_ring_3	http://127.0.0.1/ nortel/dst_ring_3

Table 2 SDN to SIP Alert Info mapping - call waiting tone

SDN Provisioned Ring Value	NA Cadence (one time)	DMS Ring Code	GCP Local New Call Data	Default SIP Alert Info Hdr
0	300 on	0	standard_ring	http://127.0.0.1/nortel/standard_ring
1	100 on, 100 off, 100 on	C	dst_ring_1	http://127.0.0.1/nortel/dst_ring_1
2	100 on, 100 off, 100 on, 100 off, 100 on	D	dst_ring_2	http://127.0.0.1/nortel/dst_ring_2
3	100 on, 100 off, 300 on, 100 off, 100 on	E	dst_ring_3	http://127.0.0.1/nortel/dst_ring_3

147.4 Hardware Requirements or Dependencies

None

147.5 Software Requirements or Dependencies

Activity A00012321 - SIP Services: Distinctive Ringing

147.6 Limitations and restrictions

None.

147.7 Interactions

None

147.8 Applicable customer facing sections

Fault Management

- Logs _N/A_
- Alarms _N/A_

Configuration

- Data Schema _N/A_
- User Interface _N/A_
- Element Management _N/A_
- Security _N/A_
- Service Order _N/A_
- Office Parameters _N/A_

Accounting (includes AMA billing) _N/A_

Performance (includes operational measurements) _N/A_

147.9 Glossary

Term	Description
CS2K	Call Server 2000
GWC	Gateway Controller
SDN	Secondary DN
SIP	Session Initiation Protocol
UA	User Agent

148: Functional Description (FN) A00012326

148.1 Feature name and Feature ID

A00012326 - SIP Lines: Authentication and Authorization

148.2 Description

This activity provides support for Authentication and Authorization account codes for Dynamic Packet Lines (DPL) using SIP. The Account code functionality allows a subscriber to enter a billing number into a Station Message Detail Recording (SMDR) record for charge-back purposes.

An authorization code is a specified set of digits assigned to and used by station end users. These codes can range in length from 2 to 14 digits. When set, the length does not change for the customer group. Authorization codes provide cost control. These codes control access to specified networks. Authorization codes raise or lower the network class of service (NCOS) of a call.

This feature supports Account/ Auth Codes Flash Entry for SIP Lines.

148.3 Hardware Requirements or Dependencies

Not applicable

148.4 Software Requirements or Dependencies

Not applicable

148.5 Limitations and restrictions

The following limitations and restrictions:

- When a call is in progress, and we try to dial Acct/Auth code in a new session, if the client starts a conference call, then the tones provided will be heard in the conference.
- Multiple call appearances are not supported.
- In case the Originator is SIP ONT, the special dialtone received when the originator dials Account/Auth FAC/VSC, is provided by the PMA and not the ONT.
- Account codes can range from 2 to 14 digits in length. The length of the account code is the validation method in the North American and the Canadian market.
- The reset dialing does network if the STARACPT suboption is set toY and the account code is entered voluntarily.

- The STARACPT subfield is set to N for the Asia Pacific CALA markets.
- The account code validation is by content when subfield STARACPT is set to N.
- The log AMAB150 displays a blank space for the asterisk as the valid digit for the voluntary account code.
- The functionality for POTS digit collection applies to the voluntary account code activation only.

148.6 Interactions

A description of the interactions between Acct/Auth codes flash entry and other functionalities appear in the following paragraphs.

- If the invoker of ACCT/AUTH or the connected party is being verified by the Operator, verified by the Operator, the request is denied. ACCT/AUTH is not permitted if an Operator Busy Line Verification (BLV) connection exists.
- In case of analog clients like the ONT where one call is already established and a new session is initiated to enter the FAC followed by the prompt for account/auth code, if the user invokes a client based conference, then the first session would hear the DN prompt and RODR treatment before the second leg is collapsed.

148.7 Glossary

Term	Description
FAC	Feature Activation Code
VSC	Vertical Service Code

149: Functional Description (FN) A00012385

149.1 Feature name and Feature ID

A00012385 - SIP Lines MADN Support

149.2 Description

The purpose of this feature is to interwork a specific set of Session Initiation Protocol (SIP) clients into IBN/RES network-based Multiple Appearance Directory Number (MADN) Single Call Arrangement (SCA) features.

SIP Line support is providing the following MDN line options, suboptions, and subfeatures:

— SCA - single call arrangement

— SCA Bridging

— PRL - MADN Privacy Release, PRLA and PRLC activation code

— SCA MREL - MADN Release of Bridging

149.3 Hardware Requirements or Dependencies

There are no hardware dependencies required to execute this feature.

149.4 Software Requirements or Dependencies

149.4.1 Feature Activity Dependencies

- A00012223 “SESM: Additional Provisioning for SIP Lines
- A00009528 “Call Pickup on Multimedia Communications Platform MCP 9.0”
- A00012273 “SIP Lines: Call Forward Indication”

149.4.2 Software Dependencies

- Succession release SN09 with drop 2 service set patches.
- GWC load GC091
- Session Server / Manager software load MCP_9.1.0.0

149.4.3 Firmware Dependencies

None

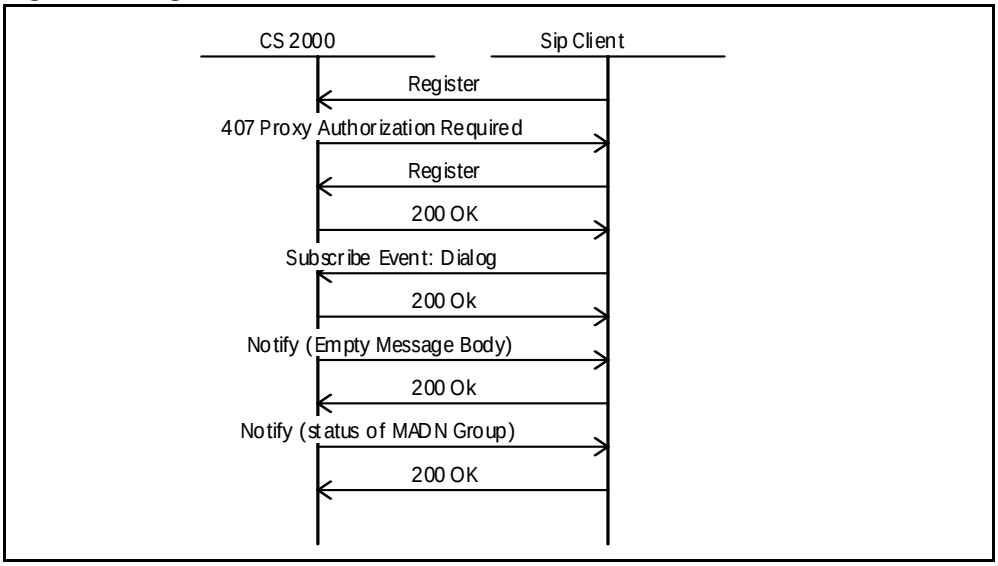
149.4.4 SIP Client Requirements

SIP Clients wishing to supply CS 2000 Network-Based MADN SCA Bridging functionality are expected to be compliant to RFC 3261, RFC 3265 and draft-ietf-sipping-dialog-package-06. The following information is provided so Client vendors will understand the message sequences of special importance.

149.4.4.1 Client Registration/Subscription and the Dialog Event Package

The ONT SIP clients must be provisioned with the MADN Dialog Event Package such that the client will properly register for the events. When a client supporting MADN registers, in addition to sending a SIP Registration to register the contact, it also needs to Subscribe to the Dialog event package. The message sequence is shown below. All of the Register and Subscribe messages should be authenticated by the SS. In the flow below the expectation is that the client is reusing the Proxy Authentication header.

Figure 1 Registration Call Flow



The Subscription to the dialog event should be subscribing to the user's own dialog status. The first Notify sent back will just contain the time out information for the subscription. The ONT should not treat an empty message body as anything other than a Notification of the status of the subscription. It should not cause a state change for the MADN group status. In order to change the group status the client must receive a message body in the Notify. Only two of the states are expected to be reported for the MADN group. If the group is busy the state of Confirmed will be sent. If the group is idle the state will be terminated.

The content type of the message body is that defined in the draft which is: application/dialog-info+xml. The message body for the active state will look like the following:

```
<?xml version="1.0"?>
  <dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info"
               version="0" state="full"
               entity="sip:MADNDN@example.com">
    <dialog id="as7d900as8">
      <state>confirmed</state>
    </dialog>
  </dialog-info>
```

The MADNDN in the above message body example will be replaced with the actual MADN.

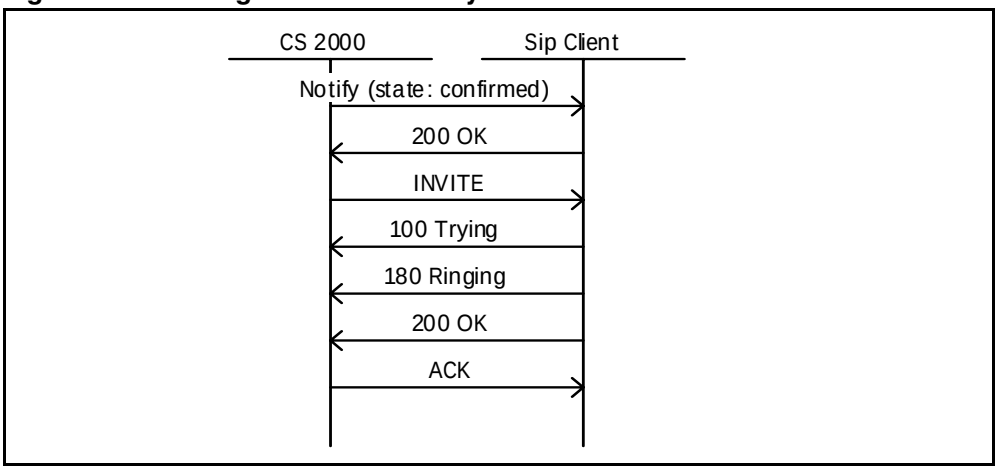
For the idle state the confirmed will be replaced with terminated. If the client has not received any indication of a state change it should assume that the state of the group is idle.

The reason that the state of the group is important is that any member of a MADN SCA group needs to treat an off-hook while the group is active as a bridging request unless a client is currently processing an inbound invite. The bridging request is discussed in section “148.4.4.3 Bridging Requests”

149.4.4.2 Incoming Call Processing

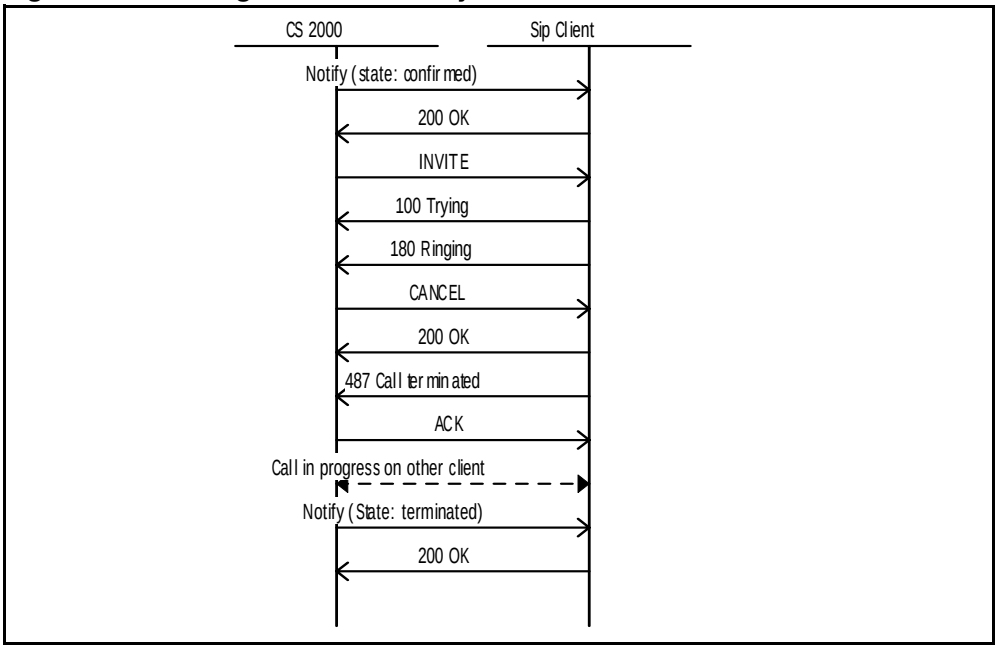
An inbound call to a client should be processed as any normal SIP invite inbound to the client. The state of the MADN group should not cause an inbound INVITE to be treated any differently. The Group will transition to the confirmed state either shortly before the Invite is received or shortly afterwards.

Figure 2 Incoming Call Answered by Client



If the call is answer by another member of the MADN group the call flow will look like any other abandoned call. The group will stay active until the call is released by all members of the MADN group.

Figure 3 Incoming call answered by another client



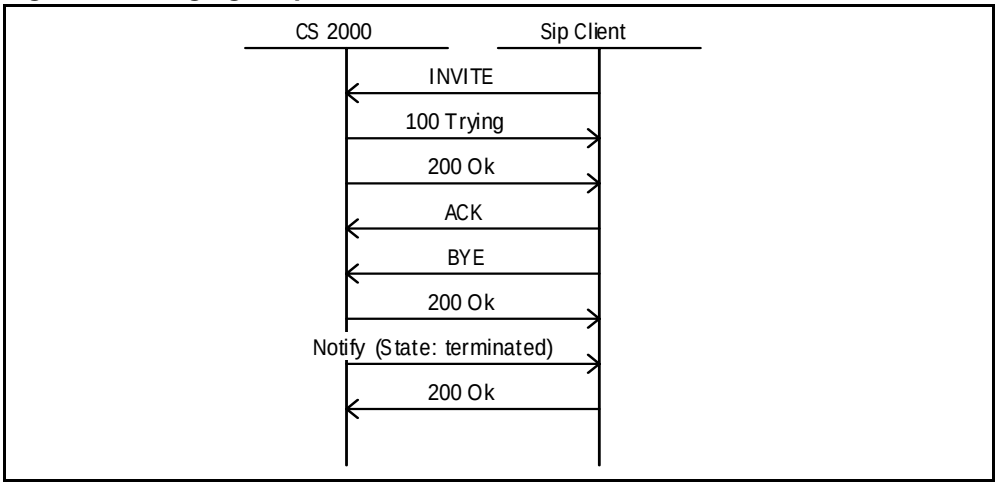
149.4.4.3 Bridging Requests

When a client is Idle but the group is busy and the user takes the handset off-hook the client should initiate an invite immediately without providing dial tone or letting the user input dtmf digits. This invite will be treated as a request to bridge the call into the active call. For this invite request it is recommended that the Invite look like the user is calling themselves. For example if the MADN dn is 555-1212 and the domain for the user is example.com the status line, to and from headers for the call would look like the following:

INVITE sip:5551212@example.com SIP/2.0
To: sip:5551212@example.com
From: sip:5551212@example.com;tag=3149adf0987

The rest of the INVITE would be formatted as any other initial INVITE request from the client. The call will be fast answered, meaning the client will receive a 200 Ok to the INVITE without any other provisional responses with the exception of the 100 trying.

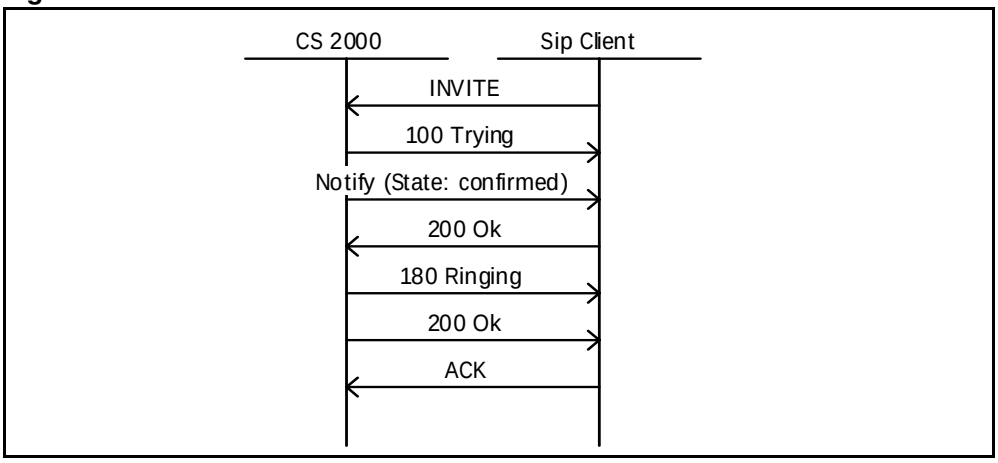
Figure 4 Bridging Request



149.4.4.4 Outbound Call

The normal outbound call case is when an idle client in an idle group sends an INVITE out. In this case the client will collect digits from the user and then send the INVITE. Shortly after sending the Invite a NOTIFY will be received marking the group as active.

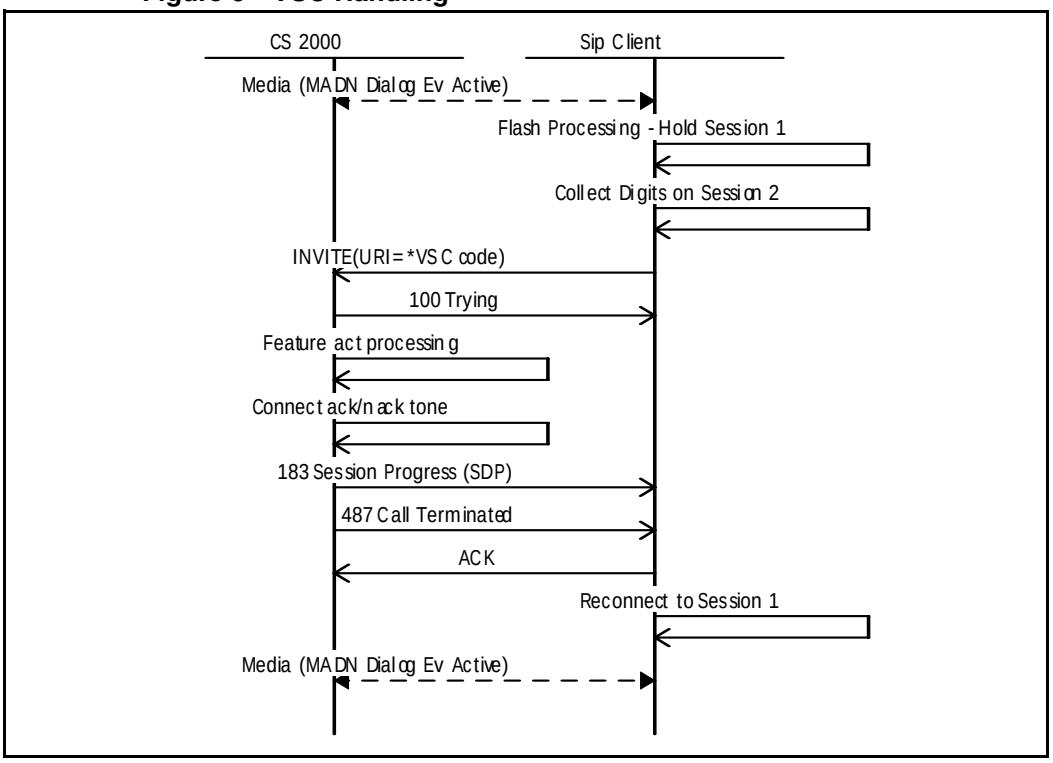
Figure 5 Outbound Call



149.4.5 VSC Call

MADN has imbedded features MHOLD and PRL which must be handled via Vertical Service Codes (VSCs) during active calls in the MADN group. For a MADN member participating in the MADN call (active media stream), the client is expected to handle Flash + digits processing, and send those digits to the CS 2000 for processing. The CS 2000 will evaluate the digits and process accordingly, connecting the VSC session to Ack or Nack tone, and then providing instruction to collapse the VSC call. The client is then expected to reconnect the media path to the original session.

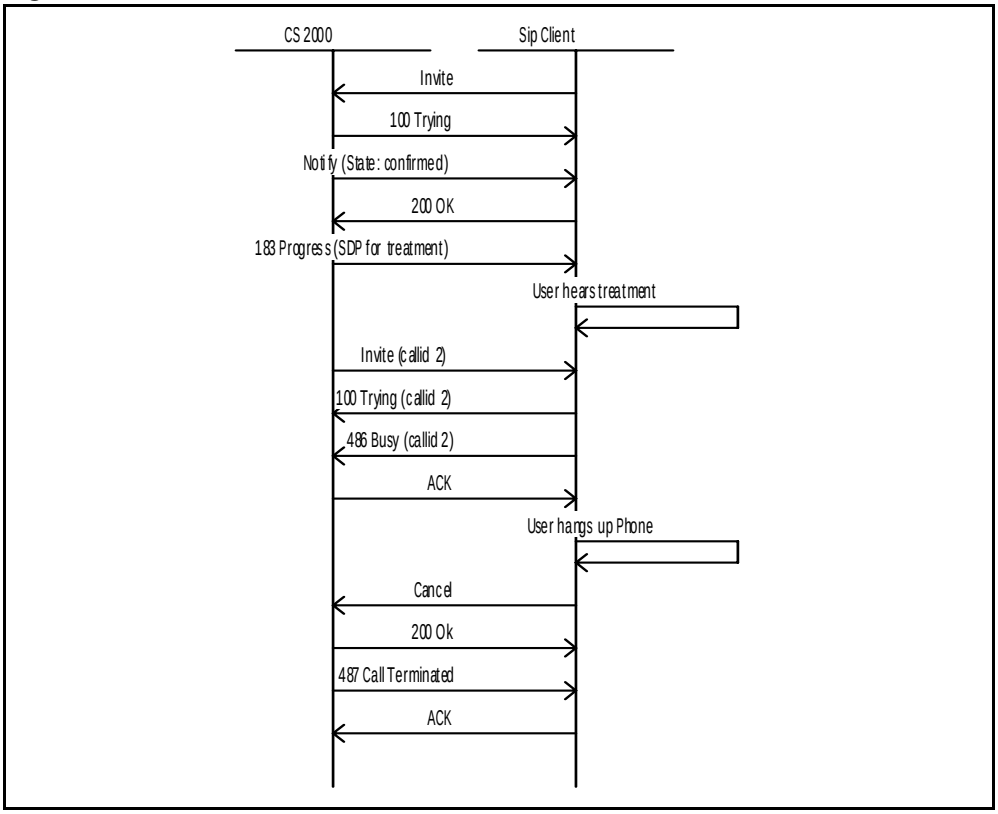
Figure 6 VSC Handling



149.4.5.1 Race Conditions

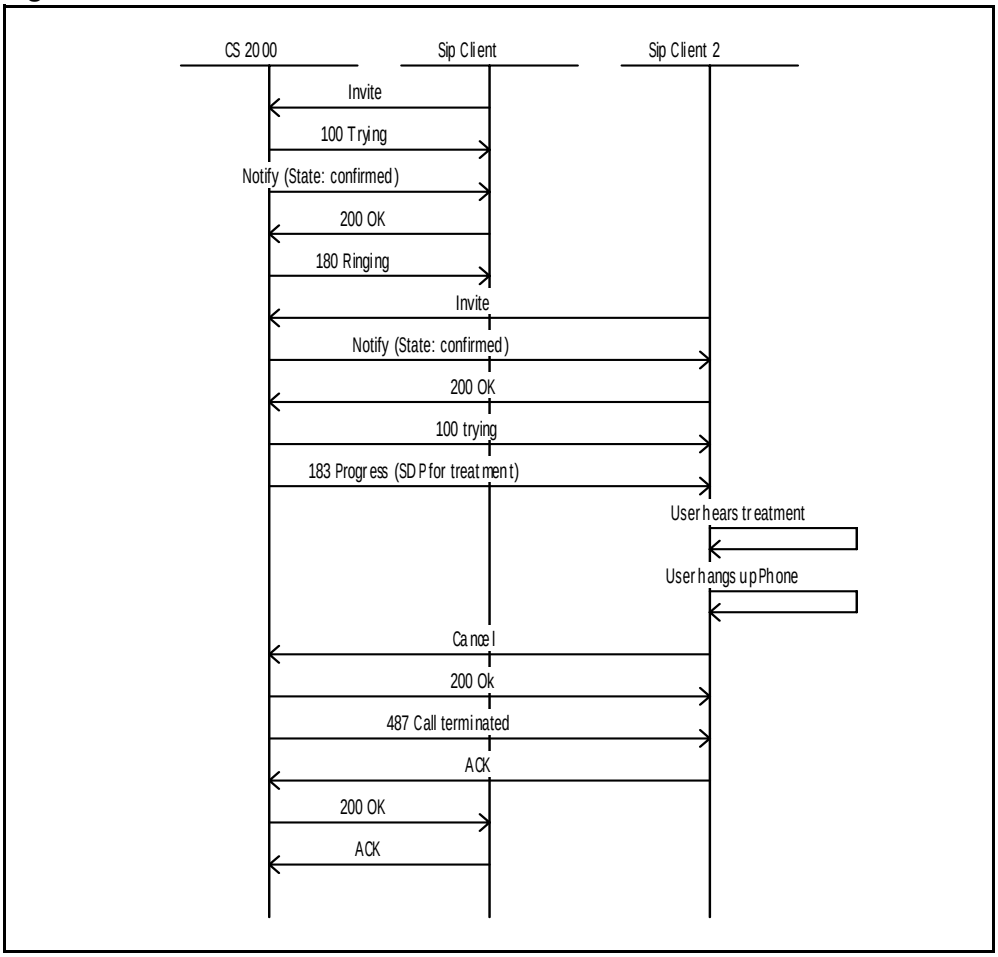
There are really two race conditions that will commonly occur. The first occurs when placing an Inbound call and an outbound call pass on the wire. The Outbound call will be given treatment. The inbound call will then be delivered to the client. How the client behaves depends on the client. The assumption is that the client will send 486 busy to the Inbound call and the user will hang up the call getting treatment. After hanging up the call if the user takes the phone off hook this should be treated as a bridging request and the user will end up answering the call. The call flow is shown below up to the point of the bridging request:

Figure 7 Inbound/Outbound Race



The other major race condition is two clients attempting to perform outbound calls simultaneously. In this case the clients call who arrives second will be given treatment and denied the origination. This case looks like the above but the call flow is a little different.

Figure 8 Dual Outbound call race



149.5 Limitations and restrictions

- This feature supports a limited set of SIP devices. Only SIP client devices which adhere to the SIP Client Requirements laid out in this document will be supported.
- MADN Engineering Rules as they apply to SIP Lines with the DPL option are as follows:
  - — MADN groups can have 32 members in either SCA arrangements
  - — no more than 16 members of the same MADN group can appear on a single GWC
  - — all members of a MADN group must belong to the same customer group

- No support for multiple SIP sessions with the exception of a second session invoking a Vertical Service Code (VSC) feature during an active / stable call
- The following MADN options, suboptions and subfeatures are not supported on SIP clients:
  - MCA - Multiple Call Arrangement
  - CACH - Call Appearance Call Handling
  - EXB - Extension Bridging
  - MRFM - MADN Ring Forward Manual
  - MRF - MADN Ring Forward
  - CFMDN - Call Forward MDN Secondary Members - MCA
  - MLAMP - MADN Lamp
  - PRV - MADN Privacy
  - MHOLD - MADN HOLD

Note: MHOLD is not supported in 09FF; however Hold will be supported through client based hold.

Note: MRF is not supported in 09FF; however RF will be supported through client based RF.

Note: MDNNAME and MEMDISP will be supported only for non-DPL lines.

149.6 Interactions

- If a SIP client is provisioned with MADN group and the client comes into service while the MADN group is ringing, that member will be notified the MADN dialog is active, but it will not be instructed to apply ringing.
- If a MADN group is comprised solely of SIP clients, there is the possibility that all members of the group could reject a call termination attempt. If this occurs, the originator of the call will be sent to reorder treatment. With non-functional originators (i.e. 2500 sets) there are scenarios where the originator may hear audible ringing and then be sent to treatment when the SIP line terminator rejects the call.

149.7 Query Commands

The query commands allow you to perform various existing queries.

Command format:

- qdn <DN>
- qlen <LEN>

- qsip <DN,LEN>

Command usage:

To Query a DN

>>qdn 6213101

```
-------------------------------------------------------------------------------
DN:     6213101     (NON-UNIQUE)
TYPE: MULTIPLE APPEARANCE DIRECTORY NUMBER
SNPA: 613   SIG: DT    LNATTIDX: N/A
XLAPLAN KEY : N/A                    RATEAREA KEY : N/A
LINE EQUIPMENT NUMBER:     SS    00 1 00 21
PRIMARY LEN:  SS    00 1 00 21
LINE CLASS CODE:  IBN
IBN TYPE:  MADN
MADN INFO - TYPE:SCA  PRIMARY:Y  RING:ALWAYS
MADN GROUP INFO - DENIAL_TRMT:   TONE   BRIDGING:Y
            CONF_SIZE: 3  BRIDGE_TONE:Y  INIT_STAT:NONPRIVATE
CUSTGRP:            BNR  SUBGRP:0  NCOS: 0
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: N
PM NODE NUMBER     :    214
PM TERMINAL NUMBER :    22
OPTIONS:
DGT DPL Y 10
OFFICE OPTIONS:
SRA
MADN MEMBER LENS INFO:
  SS    00 1 00 21           SCA   PRIMARY: Y   RING: ALWAYS
  SS    00 1 00 22           SCA   PRIMARY: N   RING: ALWAYS
  FUNC      101     KEY: 1   SCA   PRIMARY: N   RING: ALWAYS   NCOS: 0
  FUNC      102     KEY: 1   SCA   PRIMARY: N   RING: ALWAYS   NCOS: 0

-------------------------------------------------------------------------------
```

To Query a LEN

qlen SS   00 1 00 21

```
-------------------------------------------------------------------------------

LEN:     SS    00 1 00 21
TYPE: MULTIPLE APPEARANCE DIRECTORY NUMBER
SNPA: 613
DIRECTORY NUMBER:     6213101              (NON-UNIQUE)
LINE CLASS CODE:  IBN
IBN TYPE:  MADN
MADN INFO - TYPE:SCA  PRIMARY:Y  RING:ALWAYS
MADN GROUP INFO - DENIAL_TRMT:   TONE   BRIDGING:Y
            CONF_SIZE: 3  BRIDGE_TONE:Y  INIT_STAT:NONPRIVATE
```

CUSTGRP: BNR SUBGRP:0 NCOS: 0
SIGNALLING TYPE: DIGITONE
CARDCODE: RDTLSG GND: N PADGRP: PKNIL BNV: NL MNO: N
PM NODE NUMBER : 214
PM TERMINAL NUMBER : 22
OPTIONS:
DGT DPL Y 10
OFFICE OPTIONS:
SRA

To perform a sip query -- qsip <dn> or qsip <len>

>qsip 6213101

SIP USER DATA
==========
SIP URI: user21@rtp7ssb.com
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: N
NUMBER OF CONTACTS: 2
CONTACTS: 47.142.66.155:5060 user21@47.142.91.49:5060
SERVICE PACKAGE:
basic_package
SERVICES:
ALCLNT N IM SIPLN ADVSCR 5 9 N CLNTCO N N N N ADHOC 4 ADDRBK 50 PRES 10 N
null N VIDEO N N IMCHAT NWLOG 50 50

SIP LINE DATA
==========
ENDPT ID: SS/000/1/0021
VMG: rtp7ssb
ZONE ID(s):
CLIENT TYPE: ONT
STATIC CLIENT: Y

SIP CALL DATA
==========
ACTIVE CALL APPEARANCES:
NODENO TERMNO
NUMBER OF ACTIVE SESSIONS IN CS2000 SESSION SERVER: 0

To post a dn or len at the map
mapci;mtc;pm;lns;ltp

Posting a dn or len at the map yields the same results.
post <dn> or post <len>

XAC MS IOD Net PM CCS Lns Trks Ext APPL
AMDI RExByp NODLOG RExSch 2 SPM 2 RS SYSB 117C.. .
ATM_6+
M *C* *C* *C* *C* *C*
LTP
0 Quit POST DELQ BUSYQ PREFIX

```
 2 Post_     LEN SS   00 1 00 21                BEAR IP_P
 3         LCC PTY RNG                    STA F S LTA  TE  RESULT
 4         IBN              DN 613 621 3101 IDL
 5 Bsy
 6 RTS
 7 Diag
 8
 9 AlmStat
10 CktLoc    post d 6213101
11 Hold
12 Next
13
14
15 FullDn
16 Prefix
17 LCO_
18 Level_
```

LMM:
<dn> post

dn call server clli call server line state endpoint state gateway profile time
6136213101 rtp7 idl unsupported_gw sipvoice 14.44:33

149.8 Applicable customer facing sections

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

149.9 Glossary

Term	Description
New term	Definition

150: Functional Description (FN) A00012386

150.1 Feature name and Feature ID

A00012386 - Media Gateway 9000 Public Key Infrastructure

150.2 Description

This feature tracks the development and implementation of various Public Key Infrastructure features on the MG9K for IP security (IPsec).

IP security is employed to protect traffic flow between endpoints on a network. This standard protocol accomplishes this task by first authenticating the endpoint involved (verify endpoint identity) and also by encrypting the transmitted data. Public Key Infrastructure (PKI) is a standard that allows entities to establish trust relationships between endpoints and thereby aids authentication. For this feature, the MG9K IPsec interfaces will use a digital certificate to authenticate the peers with which it establishes IPsec sessions.

MG9K will use PKI to authenticate its IPsec sessions to the Element Manager (EM) and to the Gateway Controller (GWC). These channels are also known as the OAMP and signaling channels respectively.

150.3 Hardware Requirements or Dependencies

This feature is restricted to IP capable ITP controller cards.

150.4 Software Requirements or Dependencies

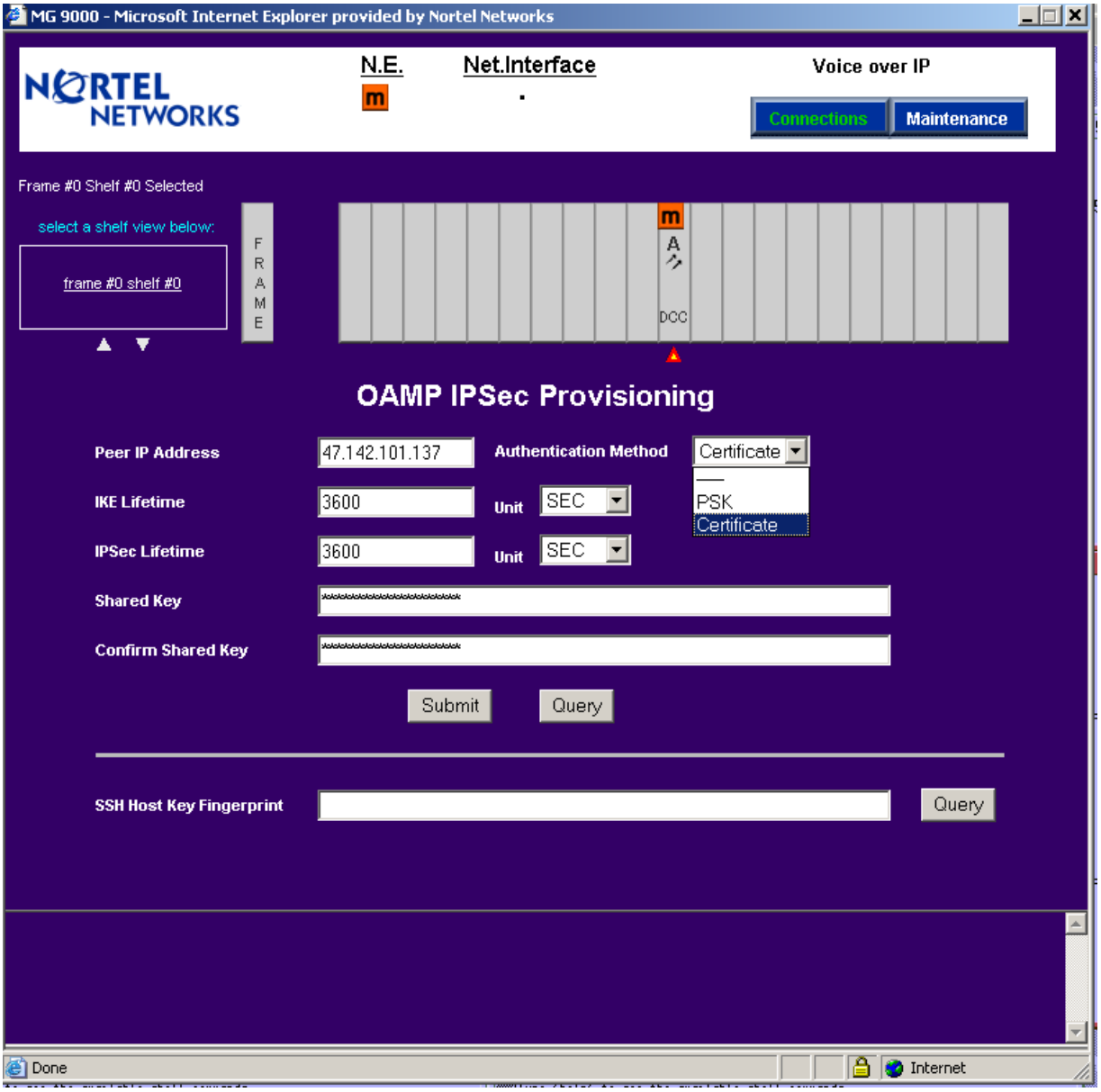
The Element Manager and the Gateway controller loads must be PKI capable.

150.5 Limitations and restrictions

None.

150.6 Interactions

As with previous releases, the user will use the Local Craft Interface (LCI) to configure IPsec on the DCC cards. The LCI screens were modified to allow the user to select the authentication method, the options being Pre-shared key and Digital certificate. A similar change was made to the MG9K EM VMG security view.



150.7 Glossary

Term	Description
PKI	Public Key Infrastructure

151: Functional Description (FN) A00012390

151.1 Feature name and Feature ID

A00012390 - Call Transfer Screening for SIP Lines

151.2 Description

This feature provides the call transfer screening support for the SIP Lines. The Call Transfer feature is developed in the DMS-CORE for SIP Lines under the DPL feature and this feature enhances the functionality by providing the screening functionality.

The screening service is provided for both the Blind and the Consultation Call Transfers.The screening will be specific to the DPL Lines agents or ONT. The Call Transfer and the screening function for TDM Line agents will remain unaffected.

The screening function will be triggered when the REFER(RFC 3515) message from the SIP Lines agent is conveyed to the CS2000 core as a feature message. The REFER message can be initiated when the user is in a single established call to make a Blind Transfer call or it can be initiated when the user is involved in two legs of call (the second one may be in a Ringing state).

The Call Transfer screening check components are discussed below.

151.2.1 Provisioning CXR for SIP Lines

Provisioning of the customer group or/and the SIP Line agent with specific screening suboptions. The subscription on the SIP Line agent will override the flavor of Call Transfer for the Customer Group to which the SIP Line agent belongs.

- The SIP Line provisioning is supported in the same way as it is for TDM Lines.
- The Call Transfer flavors will be processed only after checking if the call transfer type provisioned for the Line initiating the REFER. If the SIP Line is not provisioned with CXR option then the customer group provisioning is checked. A default value of CTINTRA for option CXFER is stored internally. Unless datafill is specified for this option, the default option is not displayed in the table CUSTSTN.
- The CXRRCL suboption is allowed while provisioning but ignored for CXR processing.

- The CXR method is allowed for provisioning, but only the STD method is supported for SIP Lines.The Figure 1 “CXR Provisioning for SIP Lines” on page 1468 shows an example for servord provisioning of the SIP Line.

Figure 1 CXR Provisioning for SIP Lines

```
> SERVORD
SO:
> ADO
SONUMBER: NOW 89 90 12 AM
>
DN_OR_LEN:
> 6216052
OPTION:
> CXR
CXFERTYP:
> CTALL
CXRRCL:[1]
> N
METHOD:
> STD
OPTION:
> $
COMMAND AS ENTERED:
ADO NOW 89 90 12 AM 6216052 (CXR CTALL N STD) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
> Y
```

1 - The CXRRCL option will be prompted for during provisioning of the SIP Lines, but the sub-option will be ignored in the CXR processing of the call.

151.2.2 Call Transfer Screening Process

- Checking first leg call type (Intragroup, Extragroup) whose party is being transferred to the second leg and its type.
- Compare them with the provisioned data for the flavour of call transfer.
- The Call transfer screening in case of Blind CXR will reject or allow the second leg origination after screening is done on receiving the REFER from the SIP Line agent.
- In case of consultation call transfer (when two call legs exist from the REFER initiating agent) the call transfer is just rejected and SIP Line

initiating the REFER will be appropriately notified. The call legs remains same as they were before the Call Transfer screening was initiated.

151.3 Hardware Requirements or Dependencies

N/A

151.4 Software Requirements or Dependencies

The call transfer screening development will be targeted to DPL Line agents. The Consultation Transfer call is NOT supported in Rel SN08 and its implementation in SN09 is out of scope for this feature. The CXR screening functionality will support the consultation transfer when it is available for SIP Lines.

151.5 Limitations and restrictions

- The Call Transfer service on the CORE for SIP Lines is a client or User agent initiated REFER handler service which will have all the interactions with the basic call as applicable to SIP Lines.
- The Call Transfer Recall functionality will not be supported for SIP Lines. The provisioning of CXRRCL sub option with the CXR option will be allowed, but the CXR Screening process will ignore the value of CXRRCL
- Consultation Call Transfer support for SIP Lines is not in the scope for the Call transfer Screening feature.

151.6 Interactions

The SIP Line call transfer screening will interact with all the services which SIP Lines supports.The Call Transfer service as implemented for the SIP Lines on the Core will have interactions as for a SIP Line basic call.

151.7 Glossary

Term	Description
CS2000	Call Server 2000
DPL	Dynamic Packet Line
ONT	Optical Network Terminal
CXR	Call Transfer (option)
CXRRCL	Call Transfer Recall (Sub-option)
DMS-Core	Digital Multiplex System-Core
REFER	SIP Method to accomplish Call Transfer (RFC 3515)
SIP	Session Initiation Protocol
UA	User Agent

152: Functional Description (FN) A00012402

152.1 Feature name and Feature ID

A00012402 - 911 Hold/Ringback Support on SIP Lines

152.2 Description

152.2.1 Overview

This activity will implement the support for the following two E911 features on SIP Lines in SN09:

- E911 Network Hold
- Ringback

The scope of this feature is provide implementation of the above mentioned features on SIP Lines for two types of SIP User Agents. First being a 911 Enabled SIP UA, such as an ONT (Optical Network Terminal) and the second being a generic SIP Client with no support for 911 specific behavior.

152.2.2 Brief description of 911 Hold and Ringback features

- **E911 Network Hold**

The Network Hold feature provides the ability to hold the Network of the 911 call in the event that the Network goes on-hook prior to disconnect from PSAP operator. If the Network Hold is present in the network the PSAP operator will hear a tone to indicate that a caller has gone on-hook and the hold has been activated.

The session and the call resources will be held in the network until ether:

- The PSAP operator releases the call.
- SIP Client reconnects to the original 911 session.
  - — For 911 Enabled SIP Users, since the session is also put on hold in the client, the client will be reconnected to the 911 session as soon as the off-hook is detected.
  - — In case of other generic SIP UAs, where all the media resources have been released, the user will be reconnected to the prior 911 session only when he attempts to make a new call.

In the CS2000 Network the Network Hold is a controlled by the ORIGHOLD subfield provisionable on the E911 incoming trunks to the E911 Tandem. Both

MF and ISUP IT with the E911 Option trunks provide the support for Network Hold.

Example of ORIGHOLD option datafilled on the ISUP IT incoming trunk to the E911 Tandem is as follows:

```
TABLE: TRKGRP
>pos e911ics7
E911ICS7 IT 0 ELO NCRT IC NIL MIDL 613 AT1 NSCR 613 613 000 N N
(E911 0747 113 E911_STD N Y 0 0 Y) $
                                   ORIGHOLD bool
```

- **Ringback**

Gives the E911 PSAP operator the ability to ring the 911 caller back who has gone on-hook and who is being held by the Network Hold Feature. It also provides the ability to, at any point, send the receive off hook (ROH) to the caller's phone set which is off hook.

Ringback is controlled by the RBACK feature option assignment in the E911 Tandem found in table IBNXLA.

152.2.3 E911 Call Setup.

152.2.3.1 E911 Call Setup with 911 Enabled as the SIP UA.

911 Enabled SIP UA Dial plan specifically identifies the digit string '911' as an Emergency call. For such calls a combination of "Resource-Priority" and "Priority:Emergency" headers will be included in all sip INVITE messages sent to and received from the CS2000.

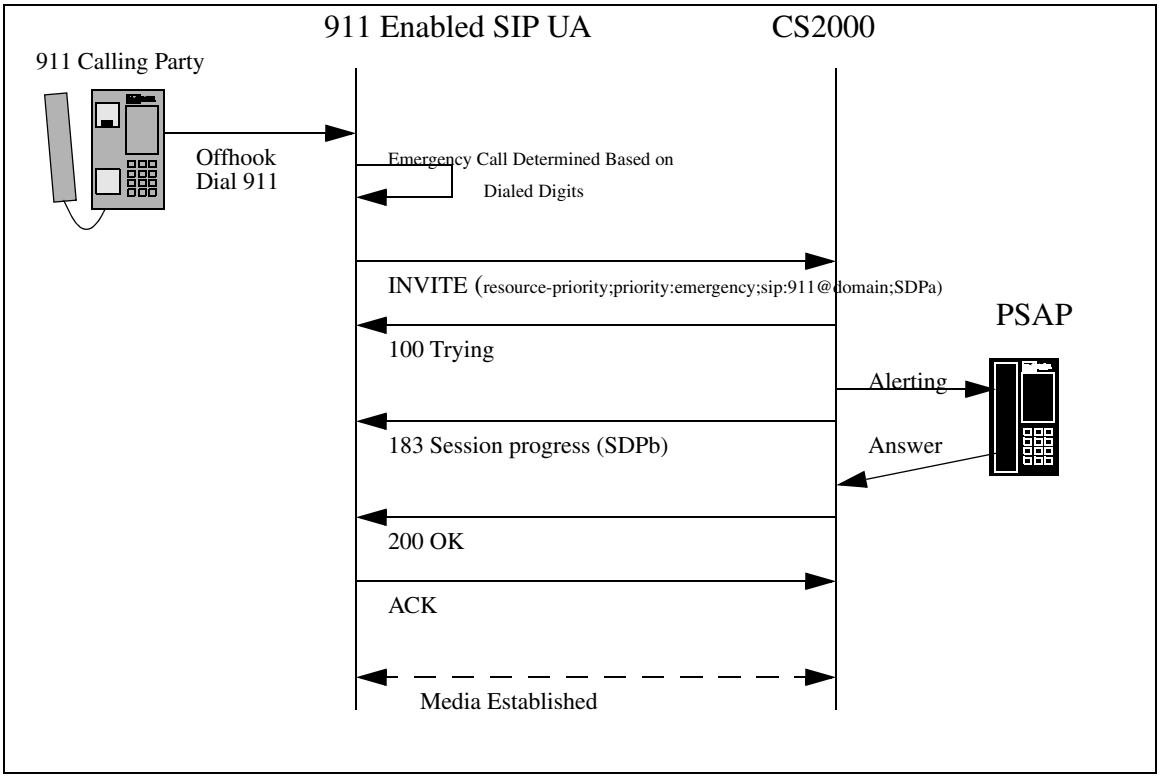
The Priority Header provided by the SIP UA client in the initial INVITE and all subsequent INVITEs will allow the CS2000 to differentiate between the 911 Enabled and generic SIP clients. The differences in 911 call processing by having Priority Header included in INVITE messaging are as follows:

- During the initial call setup, INVITE messages received with Resource and Priority Headers will receive preferential handling by CS2000 Overload Controls and thus will less likely to be rejected during overload times.
- INVITE with a 0 SDP and a Resource and Priority Headers received from a 911 Enabled SIP UA will be handled as a "Network Hold" Request for the 911 session and processed as such. The session and all its resources will be put on hold.
- An INVITE with 0 SDP and with NO Priority Header received during an established 911 session will be handled as a regular hold request (which are not supported on 911 calls) and thus will be denied. CS2000 will respond

with a 403 Forbidden message to deny the request. Figure 5 illustrates the message flow.

Figure 1 illustrates the messaging exchange occurring during the setup of the E911 Call when 911 Enabled SIP US is present in the network.

Figure 1 911 Call Setup with 911 Enabled SIP UA

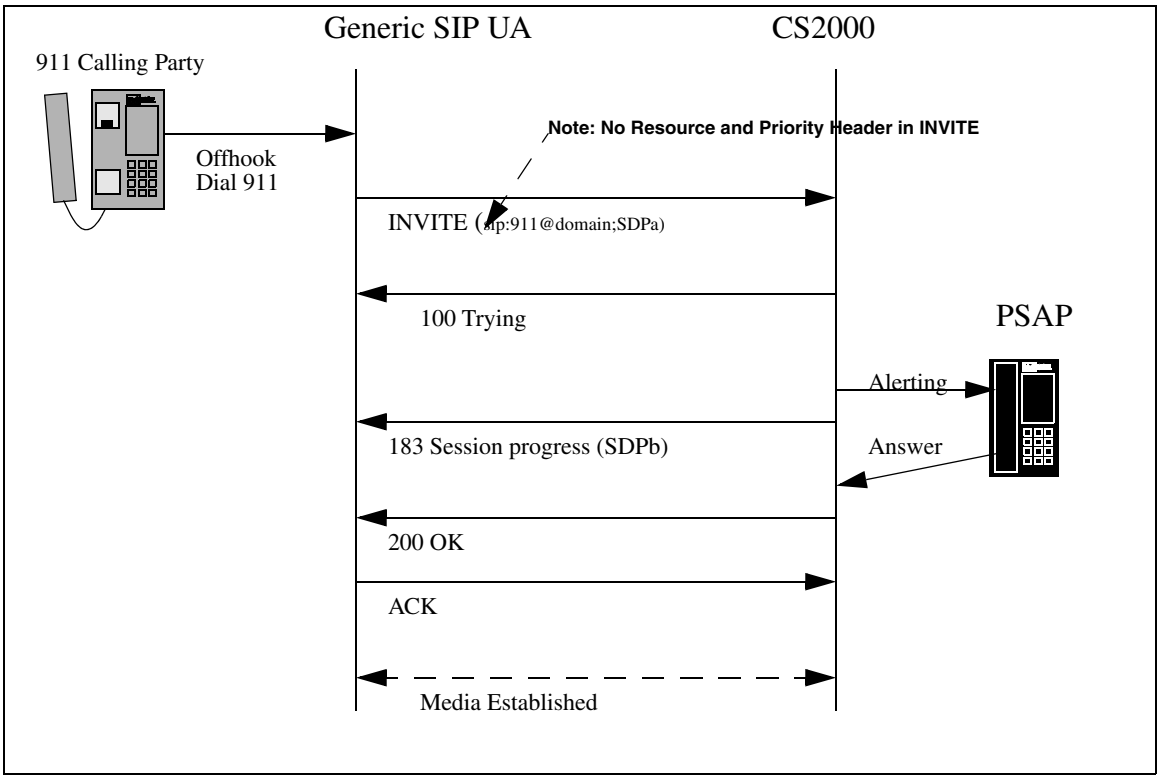


152.2.3.2 E911 Call Setup with a Generic SIP UA

Figure 2 illustrates the messaging exchange that occurs during the setup of the E911 call with a generic SIP UA. In contrast with the messaging received from the 911 Enabled SIP UA, there is no Resource-Priority and Priority:Emergency Headers in the sip INVITE received by the CS2000.

The main impact of not having these headers during the initial 911 call setup, is that the 911 call will NOT receive any preferential treatment from the CS2000 during the call setup stage.

Figure 2 911 Call Setup- Generic SIP UA



152.2.4 Caller Disconnect Message Handling

152.2.4.1 911 Caller Disconnect on 911 Enabled SIP UAs

Call flow in Figure 3 illustrates the disconnect/ message handling on the 911 Enabled SIP UA. The Handling of an invalid hold request is shown in Figure 4.

Upon detecting on hook from the 911 user, the SIP UA maintains all call resources and places the session on hold. An INVITE with 0 SDP and a combination of resource and priority headers is sent to CS2000 to request the session to be held. In the event that these headers are not included in the INVITE with 0 SDP, the hold request will be denied by the CS2000 and a sip 403 will be returned. See Figure 4.

Once the session has been successful put on hold, it will remain on hold until either the PSAP operator disconnects, or the 911 caller tries to re-connect to the session.

While the session is on hold, any incoming calls to the SIP user will receive BUSY Tone.

Figure 3 Disconnect Handling on the 911 Enabled SIP UA

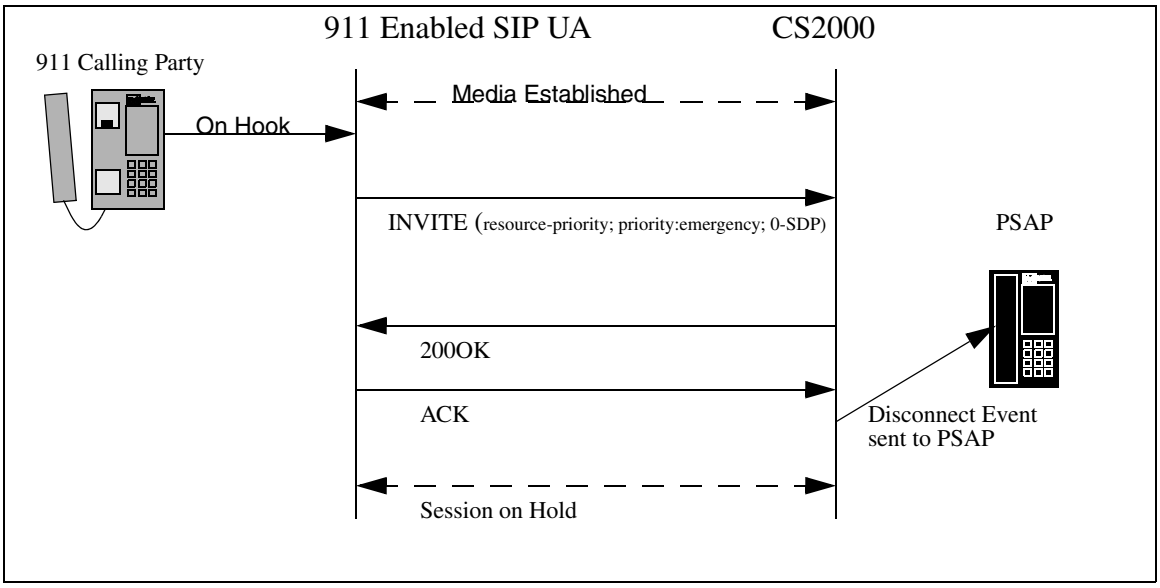
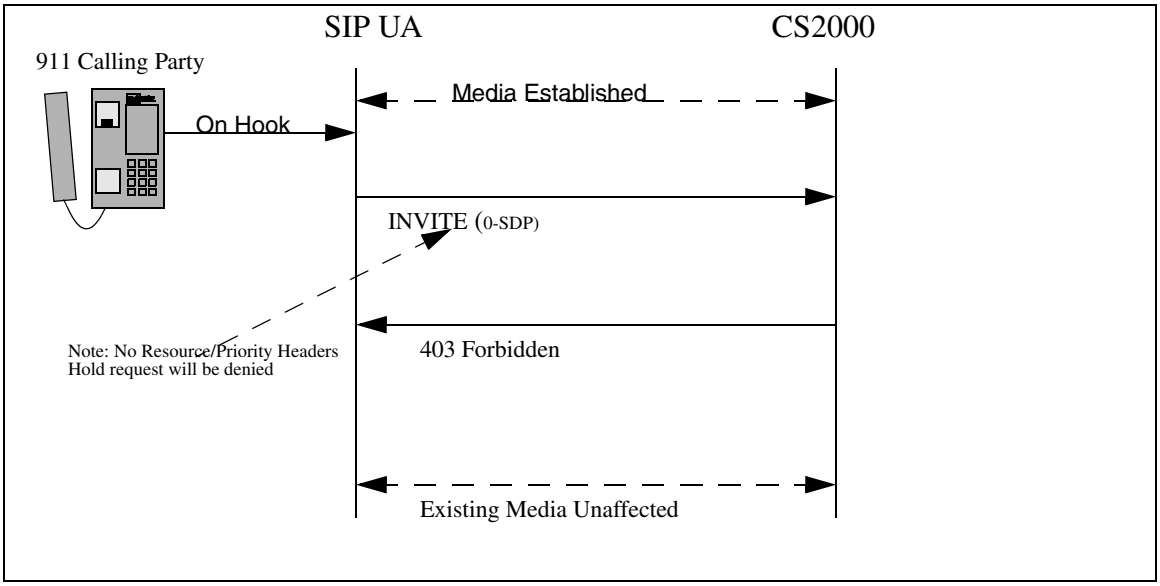


Figure 4 Invalid Hold Request



152.2.4.2 911 Caller Disconnect - Generic SIP UA Scenario

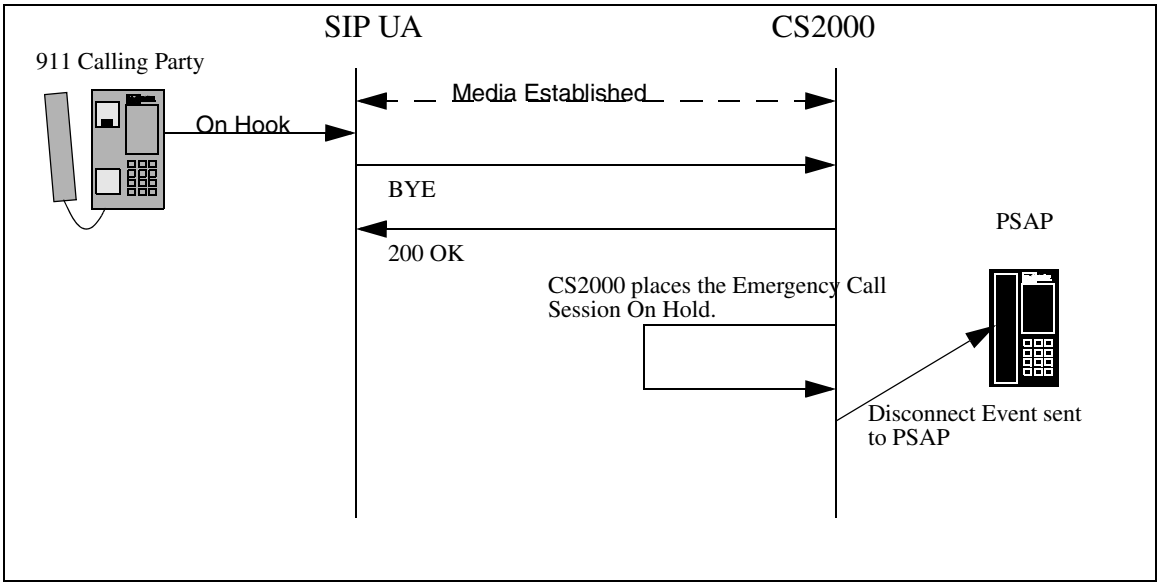
For generic SIP clients the user disconnect handling is illustrated in Figure 5. Typically SIP UA's don't have the logic to differentiate between 911 and regular calls and thus will take their media resources down as soon as the on-hook from the set is detected but prior to sending the BYE to the CS2000. This behavior makes it necessary for CS2000 to support the sip BYE message as a

request for network hold. Upon receipt of the BYE message the CS2000 session resources would be placed on hold and the PSAP operator notified of user's disconnect.

The session resources on the CS2000 will be held until either the PSAP operator disconnects, or the 911 caller goes off-hook and tries to originate a call.

While the session is on hold, any incoming calls to the SIP user will be sent to BUSY treatment.

Figure 5 Disconnect Handling - Generic SIP UA



152.2.5 Reconnect Following Activation of Network Hold

The 911 caller can "reconnect" to the existing 911 session by either of the following methods:

- If the SIP UA is 911 Enabled, simply going off-hook will re-establish the 911 session.
- In the Generic SIP UA scenario, the user will need to go off-hook and attempt to originate a call. SC2000 will respond to the incoming INVITE by reconnecting the client to the previous session.

Figures 6 and 7 illustrate the possible message flows for the reconnect scenarios.

Figure 6 Reconnect Handling with 911 Enabled SIP UA in the Network

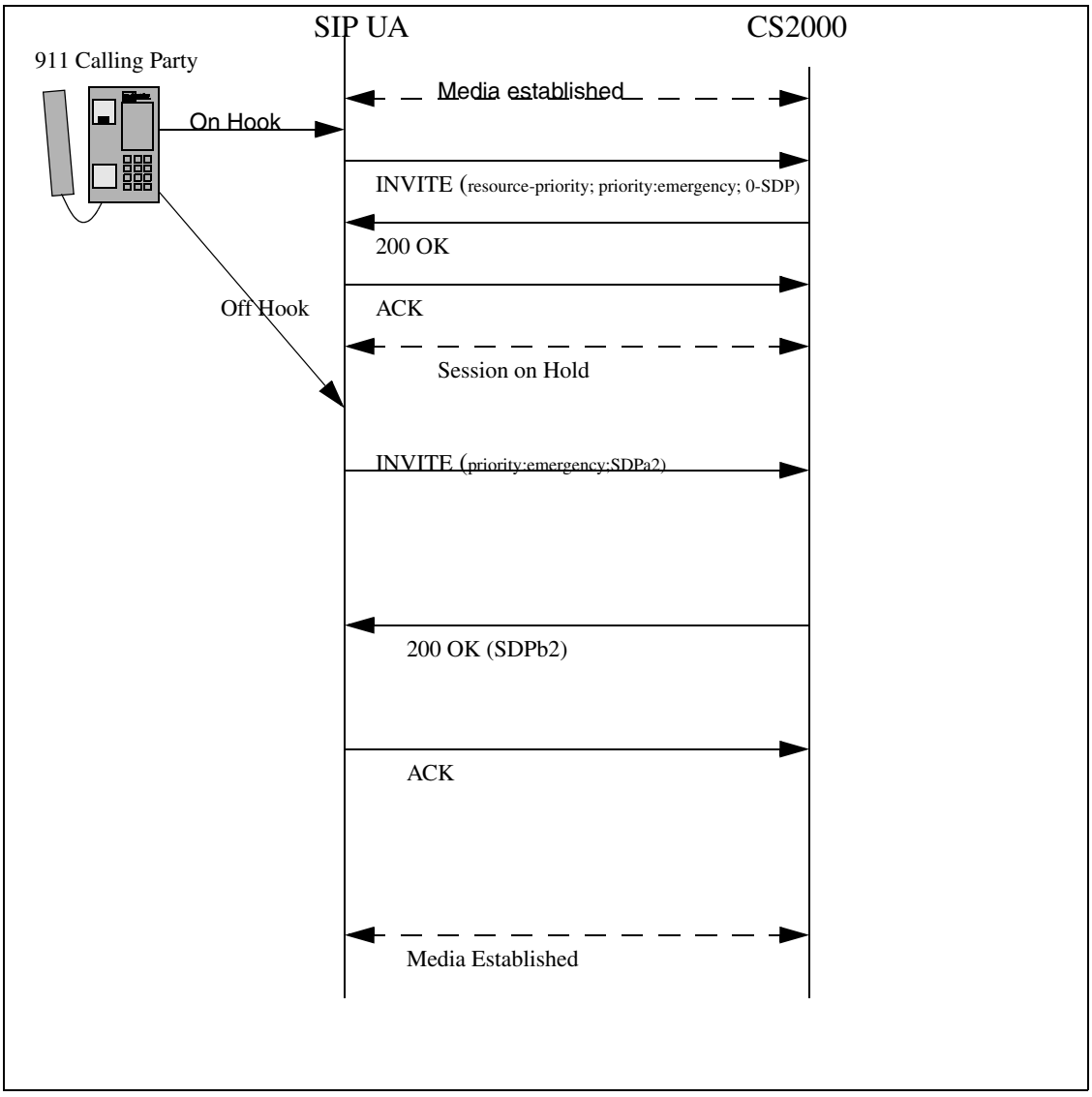
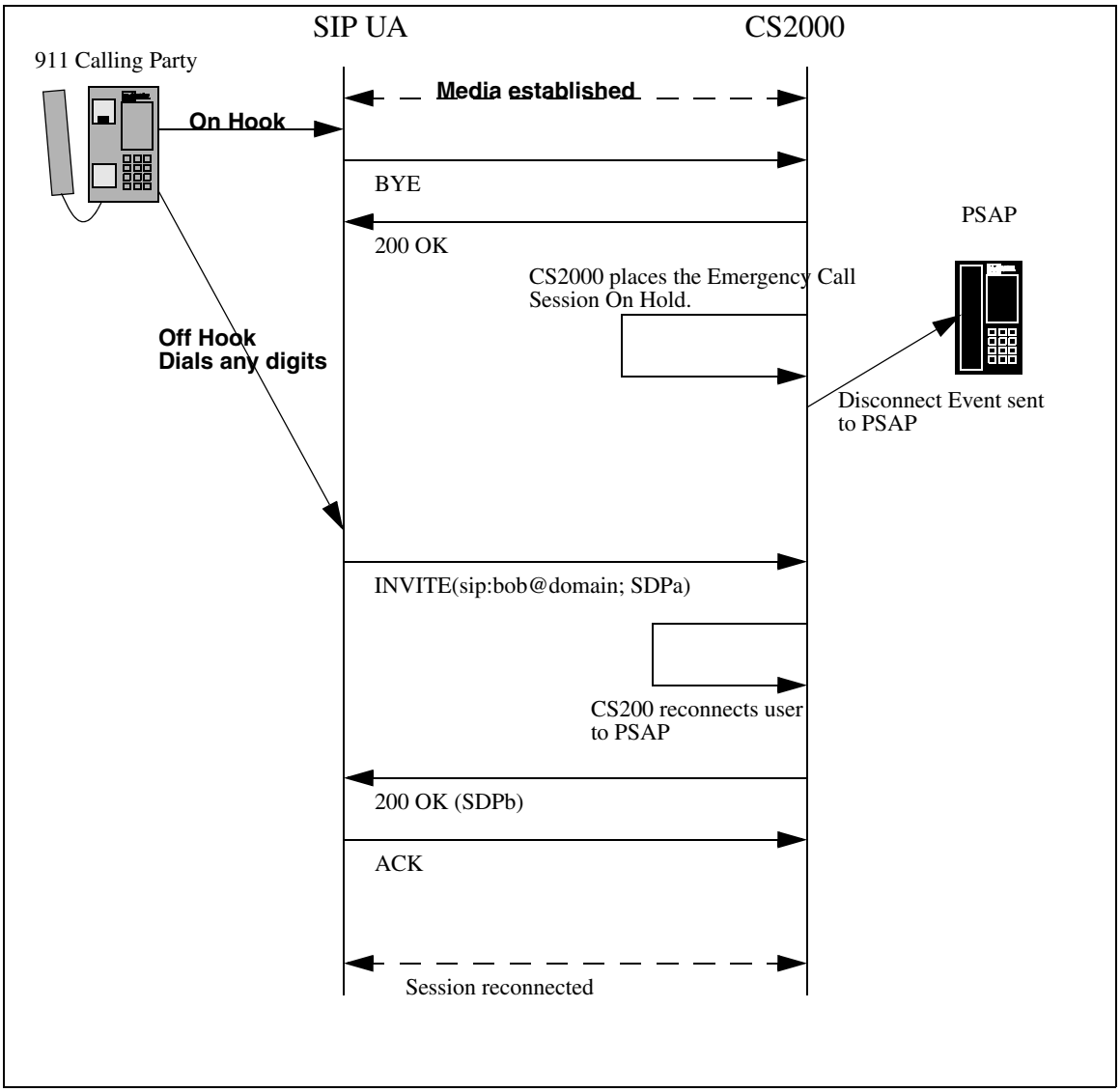


Figure 7 Reconnect Handling - Generic SIP UA

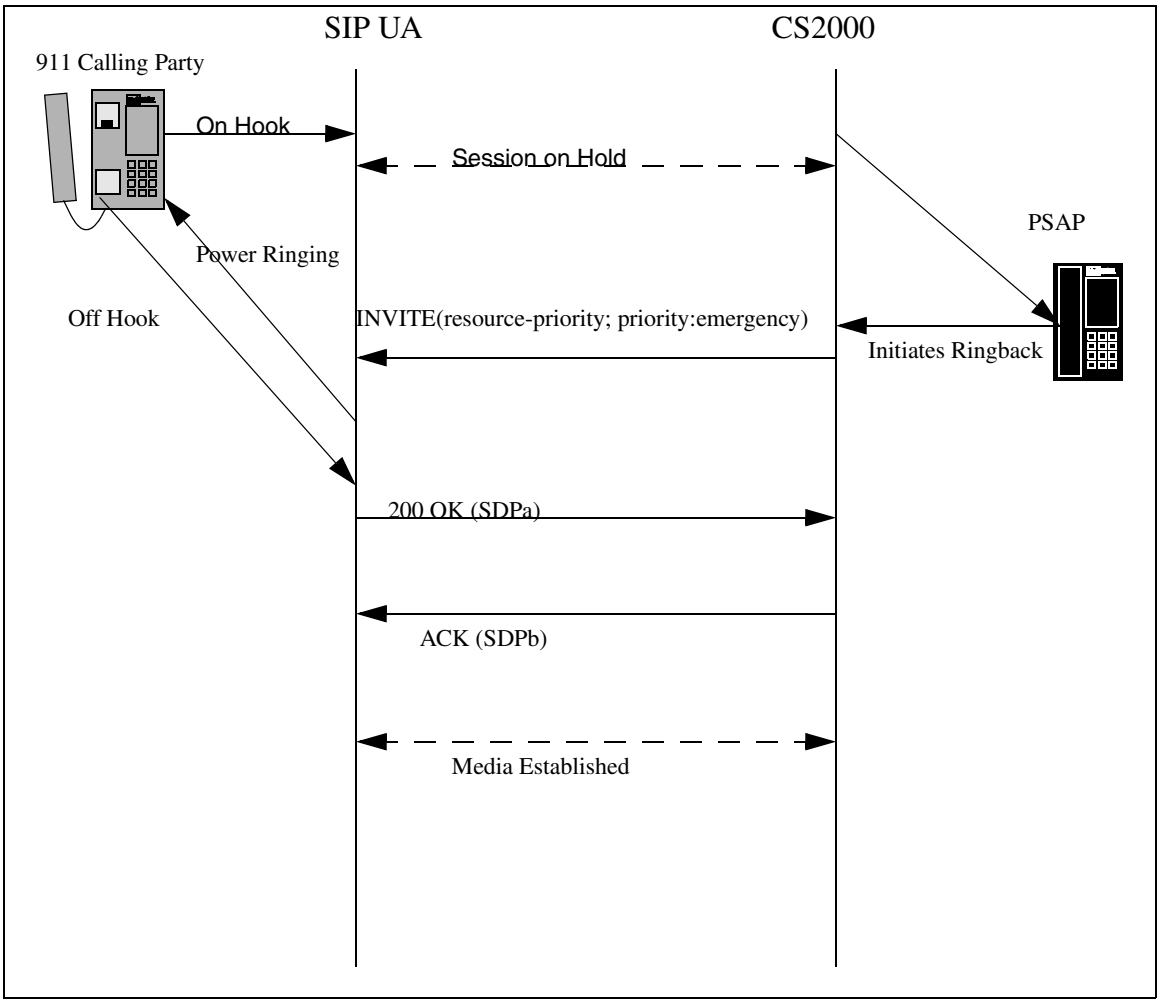


152.2.6 Ringback Activation following Network Hold

At any point while the call is being held the E911 PSAP operator can ring the 911 caller back. Once Ringback is activated, the CS2000 restores the held session and the SIP UA applies power ringing to the user's set.

Once the session is placed on hold, there is no difference in the message flows between the 911 Enabled SIP UA and other SIP UAs.

Figure 8 Ringback Handling in the Network

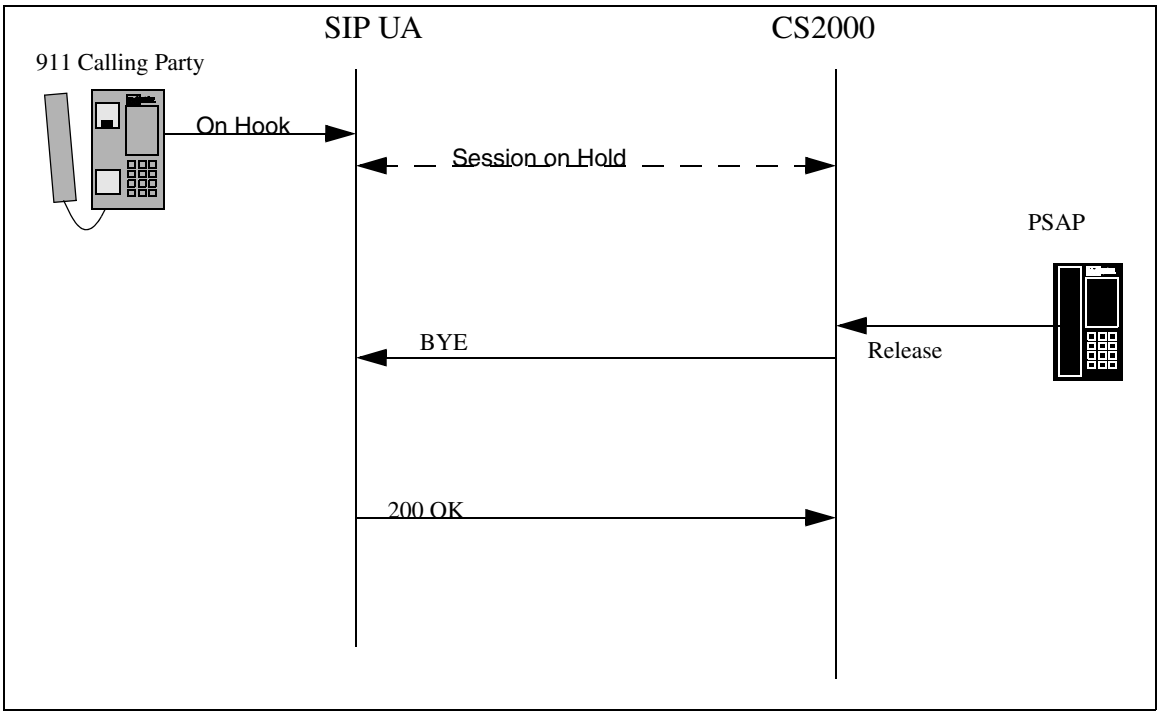


152.2.7 PSAP Disconnects following Network Hold

At any point while the call is being held the E911 PSAP operator can disconnect the session by going on hook

Figure 9 illustrates a Release received from the PSAP following the onhook from the SIP UA.

Figure 9 PSAP Disconnect Handling in the Network



152.3 Hardware Requirements or Dependencies

No new hardware dependencies are introduced beyond the general requirements for SIP Lines

152.4 Software Requirements or Dependencies

In addition to the general software requirements for SIP Lines and E911, this feature also introduces the support for the 911 Enabled SIP UA. Such a SIP UA differs from other Agents in that it has the smarts to identify emergency calls and handle them accordingly.

911 Enabled SIP UA's Dial plan specifically identifies the digit string '911' as an Emergency call. For such calls the "Resource-Priority" and "Priority:Emergency" Headers will be included in all sip INVITE messages sent to the CS2000.

The 911 Enabled SIP UA Service Profile will have the following a following provisionable boolean parameter: Emergency Call On-Hook Hold. If On-Hook Hold is set to true, then the on-hook from the 911 caller will be treated like a call hold and all session resources will be held. Once the On-Hook is detected an INVITE with the "Resource-Priority" and "Priority:Emergency" Headers and 0 SDP will be sent to CS2000 to request the hold.

Since PSAP can at any point request to alert the caller, the 911 Enabled SIP UA will either provide a distinctive power ringing if the Network's set is off-hook or a "howler" tone if the set is on-hook.

152.5 Limitations and restrictions

In case where a BYE message is received from SIP UA and the session is being held in the CS2000, simply going off hook by the user will not cause the session to be reconnected. The user will need to dial digits and an INVITE (sip:cdn@domain) will need to be received by CS2000 in order to reconnect the user to the PSAP operator.

152.6 Interactions

CS2000 will require the "911 Enabled" SIP UAs support all behaviors outlined above.

152.7 Applicable customer facing sections

none

152.8 Glossary

Term	Description
FTTP	Fiber-To-The-Premises
E911	Enhanced 911
UA	User Agent
PSAP	Public Safety Answering Point
ROH	Receive OffHook
911 Enabled	Optical Network Terminator
SIP	Session Initiated Protocol

153: Functional Description (FN) A00012403

153.1 Feature name and Feature ID

A00012403 - Data Protection for SIP Lines

153.2 Description

This feature inherits all functionality from legacy lines.

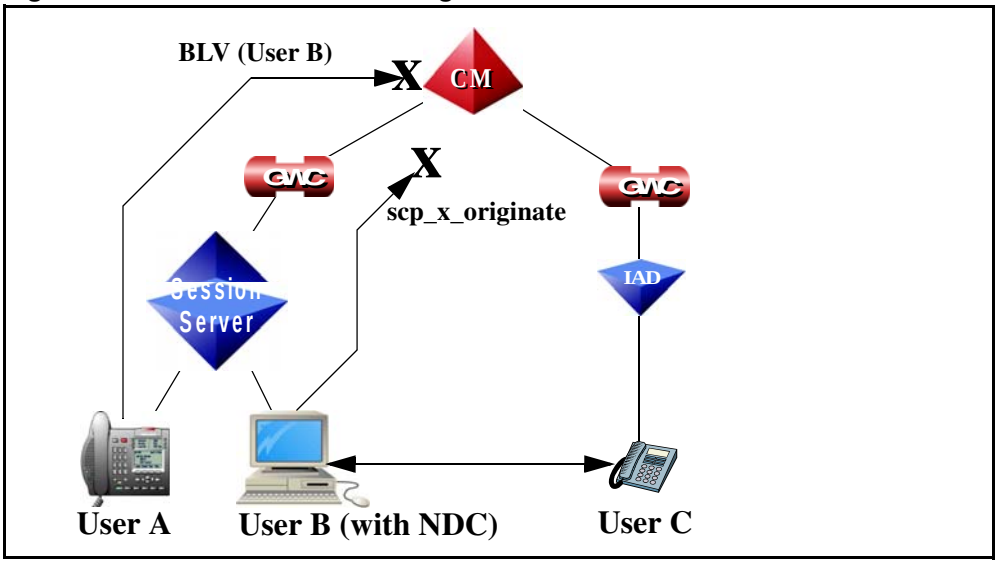
Data protection prevents interruption or mutilation of data calls caused by the application of warning tones and voice energy associated with attendant camp-on, busy verification, busy override and call waiting.

Data protection is provided by assigning the No Double Connect (NDC) option to a line. A line assigned NDC, cannot use the call transfer, or any of the conference features, nor participate when invoked from another subscriber. This option prevents the user of such a line from providing access to data or to computers from other, possibly unauthorized lines.

The NDC option is activated/deactivated via Data Modification Order (DMO).

No Double Connect (NDC) option has two roles: First is to prevent a user with NDC assigned from making multiple calls, Second is to ensure any feature that is incompatible with NDC does not operate on a user with NDC option.

Figure 1 Functional Behavior Diagram



User B (with NDC option) is in a call with User C. User A is prevented from activating a feature (e.g. Busy Line Verification) against User B. User B is prevented from making a new origination.

153.3 Hardware Requirements or Dependencies

None.

153.4 Software Requirements or Dependencies

None.

153.5 Limitations and restrictions

The NDC option is not compatible with the following line options:

This component is to validate the feature is compatible with the No Double Connect (NDC) option. Certain features cannot be assigned to a line with NDC option. These features are as follows:

3WC, 3WCPUB, CHD, CNF, CRT,CWD, CWI, CWO, CWT, CWTC, CWX, CXR, DCBX, DSCWID, FXR, HLD, LDSA, LDSO, LDSR, LDST, LNPTST, MPB, PCWT, PRK, VOWDN[1].

Incompatibility is assigned through table OPTOPT.

153.6 Interactions

Camp-on is not compatible with stations that have NDC assigned. If the customer group parameter is comp-on with tone, camp-on will not apply to stations assigned option NDC.

Call Transfer and Blind Call Transfer is not compatible with NDC.

Busy Verification is denied to stations assigned NDC.

Call Waiting, Call Waiting Origination, and Dial Call Waiting are incompatible with lines assigned NDC option.

Directed Call Pickup-Barge In is incompatible with lines assigned NDC option.

Executive Busy Override, also known as Executive Right of Way, Executive Busy Override, Executive Override, Override, Break-In, Barge-In, is incompatible with lines assigned NDC option.

Trunk Busy Verify is incompatible with NDC option, when the busy circuit is connected to a line with NDC option.

[1]See Glossary for Definition.

Click to Call, and PA Simring are not compatible with NDC. (These services must have 3WC option).

When the client device is programmed with 3xx/Redirect/Call Forward All, the NDC check will be made against the client as well as the target to which the redirect occurs.

153.7 Applicable customer facing sections

Fault Management

- Logs x_____
- Alarms _____

Configuration

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

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

153.8 Glossary

Term	Description
New term	Definition
3WC	Three Way Calling. The 3WC option allows the subscriber, on the assigned line, to place a call on hold. When the call is on hold, the subscriber can set up a request call to another subscriber. The subscriber that initiates the three-way call can switch speech paths between the held party and the talking party. The subscriber can connect all parties into a three port conference. When the three way call is in progress, the subscriber can drop the conference. When the subscriber drops the conference, the subscriber connects to a single-party call again.
3WCPUB	Three Way Calling Public Announcement. The 3WCPUB option allows all parties on a call extension from a 50B customer premises system (CPS) to bridge together. The parties do not wait for the controlling party to flash all the parties together.

Term	Description
CHD	Call Hold. The Call Hold (CHD) option allows a subscriber with a 500/2500 set to hold a call. If a party does not go off-hook, the subscriber can hold a call for any period of time. When this action occurs, the station with CHD can perform other tasks. These tasks include speed call programming or call pickup, as a call holds. The subscriber can only put one call on hold at a time.
CNF	Station Controlled Conference. The station Controlled Conference (CNF) option allows a station to have a conference call to a maximum of 30 parties. With the CNF option, the station does not require the help of an attendant for a conference call to a maximum of 30 parties. The members of the conference can belong to the same customer group or belong to different customer groups. The members also can belong to a station on a trunk. The JOIN option works with CNF to add a held party to a conference without having to hang up and redial the held party. CNF is a prerequisite to adding JOIN to the business set.
CRT	Call Redirect. Call Redirect (CRT) provides residential subscribers with the ability to transfer calls to a predefined routing directory number (DN) or to a voice mail DN. The transfer occurs when the subscriber flashes and dials the CRT access code during an established two-party call. After su8ccessful feature activation, the subscriber receives a confirmation treatment. Only the terminator in a two-party call can activate CRT. After activating, the terminator becomes the CRT controller.
CWD	The Dial Call Waiting (CWD) option allows a business set user to impose call waiting on a busy station. The busy station can be a 500/2500 set or a business set with a call waiting (CWT) feature key.
CWI	The Call Waiting Intragroup (CWI) option allows a subscriber to apply the CWT option to intragroup calls, in addition to those allowed with CWT.
CWO	The Call Waiting Originating (CWO) option allows an originating line to impose a call waiting tone automatically on a busy line.
CWT	The Call Waiting (CWT) option allows the system to alert a busy station when an incoming call attempts to reach the directory number (DN).
CWTC	The Call Waiting Conference (CWTC) option allows the subscriber to conference a waiting party.
CWX	The Call Waiting Exempt (CWX) option does not allow Dial Call Waiting (CWD) and Call Waiting Originating (CWO) to interrupt a business set user.
CXR	The call transfer option (CXR) allows the assignment of a call transfer type other than the type that the customer group has.

Term	Description
DCBX	The Directed Call Pickup Barge-In Exempt (DCBX) option allows a station to block the attempts of other stations with DCBI assigned to barge in.
DSCWID	Deluxe Spontaneous Call Waiting Identification (DSCWID) allows the subscriber to receive calling-party information during call waiting. The subscriber also receives this information with basic SCWID. The DSCWID presents the subscriber with a set of option to treat the incoming calls. These options include the following: - Answer the new call and put the current call on hold. - Disconnect the call. Answer the new call. - Forward the new call. - Connect the new call to a busy announcement. - Conference the new call with the current call.
FXR	The Fast Transfer (FXR) option reduces the number of keystrokes required to transfer a call. The user does not need o conference all parties before the user transfers calls.
HLD	The Permanent Hold (HLD) option allows a single-line set to put an active call on hold and return the handset to the handset cradle. The party on hold hears a ringback tone, a recorded announcement, music, or silence.
LDSA	The long distance signal activate (LDSA) line option (activation code *49 or 1149) allows the end user to activate or deactivate Long Distance Alerting (LDA) on a line. The operating company personnel can assign the LDSA line option through SERVORD.
LDSO	The Long Distance Signal Option (LDSO) option provides Long Distance Alerting (LDA) subscribers with a different ring and a different tone.
LDSR	The Long Distance Signal Ringing (LDSR) option provides Long Distance Alerting Enhancement (LDAE) subscribers with a a distinctive ring when the subscriber line is idle.
LDST	The Long Distance Signal Tone (LDST) option provides Long Distance Alerting Enhancement (LDAE) subscribers with a distinctive ring when the subscriber line is busy.
LNPTST	The system assigns the local number portability test (LNPTST) option to a single-party residential (1FR RES) line to allow a local number portability (LNP) test call. The system assigns this option through SERVORD. The SERVORD blocks subscription to this option by any other type of line. The only line option compatible with LNPTST is Digitone (DGT). The SERVORD does not allow assignment of LNPTST and line options that are not compatible on the same line.

Term	Description
MPB	The Multi-Party Bridging (MPB) option allows a multi-party group with a maximum of four subscribers with a different line equipment to associate in a multiparty group. The liens appear to the subscribers to be different parties of a multiparty line. Each member of a MPB group has a different directory number and a different line equipment number. The MPB option creates a bridge among subscriber lines that wires cannot bridge. Wires cannot bridge subscriber lines because these lines do not have analog appearance in the central office. An example of these lines are lines that connect to an integrated digital loop carrier.
PCWT	The Precedence Call Waiting Terminating
PRK	The Call Park (PRK) option allows a business user to park a call against the directory number (DN) of the user. Retrieval of the parked call can occur from any station. When the call is parked, the user can originate and receive calls on that DN.
VOWDN	The Virtual Office Worker (VOW) feature allows telecommuters who do not have dedicated physical phone sets to access their dedicated directory number (DN) and associated features and options. They do this by logging into their dedicated DN from any of a pre-designated group of phone sets. Once logged in, all features and options operate normally, and all calls to the dedicated DN terminate to the set on which the login occurred. All predesignated sets that are to be used by VOWs need to have the VOWDN line option assigned within the customer groups that are to offer VOW functionality. The VOWDN option is not compatible with any other line options/features except SETMODEL, DGT, DISP, M0200, and NAME.

154: Functional Description (FN) A00012410

154.1 Feature name and Feature ID

A00012410 - Support SIP lines for Malicious Call Hold

154.2 Description

This feature expands the existing Malicious Call Hold (which is datafilled as the CLF option), service supported in the CS2K Core to SIP Lines.

A line with the CLF (Calling Line Identification with Flash) option, activates and deactivates the CLF functionality with a flash and VSC (Vertical Service Code). The line is the terminating party of the call. The Core generates a log and records information about the Originator of the MCH caller.

When the terminating agent of the SIP lines, initiates the MCH feature, a message with an authorization code is sent to the CS2K The CS2K will terminate the call and service the request action.

154.3 Hardware Requirements or Dependencies

Not Applicable

154.4 Software Requirements or Dependencies

Not Applicable

154.5 Limitations and restrictions

The following are the restrictions and limitations of this service:

- This MCH feature will be initiated on a SIP Client that has only one call prior to invoking the malicious call feature.
- This MCH feature will only supported for 2 (two) calls on the same VSC. That is, if the client enter the VSC with more than 2 calls, then the feature will not be activated.
- This feature will support any client that has been integrated with the CS2K
- B party control in not part of NA MCH feature.

154.6 Interactions

All existing MCH interactions works the same way with the SIP Lines. No new interaction anticipated.

154.7 Glossary

Term	Description
CLF	Clear Line Identification with Flash
MCH	Malicious Call Hold
NA	North American
VSC	Vertical Service Code
SIP	Simple Internet Protocol

155: Functional Description (FN) A00012470

155.1 Feature name and Feature ID

A00012470 Compact Call Agent - Support for NA/Intl Hybrid Market

A00012766: SDM/CBM800 connected with BRISC to CBM850 connected with CCA cutover.

Note: The scope of the requirements has been expanded to include both North American and International markets.

155.2 Description

155.2.1 Overview

This activity supports the Packet Ready 2005 (PR-2005) marketing initiative to convert existing BRISC (SNSE70EM, SN70EM) core offices to CS-2000 Compact (CCA) based Hybrid offices.

The cutover activity builds on the procedures already supported for CS-2100 Compact (Enterprise) who have supported the BRISC to Compact cutover since the SE06 release.

The following additional components are supported over the CS-2100 Hybrid:

- SDM or CBM-800 on the BRISC are converted to CBM-850 connected to the Compact during the overall cutover process.
  This is developed as part of activity A00012766.
  (The requirement to cutover from an SDM on BRISC, to the same SDM on CCA is being addressed by the SDM/CBM team as a post-SN09FF activity.)
- ICM (Intelligent Call Manager) EIU application is supported over the cutover from BRISC to CS-2000 Compact. However, given the lack of a secure IP address on the CCA for use the ICM application, it is recommended that the use of this functionality be limited to ICM systems that are securely connected to the CCA (for example, the ICM system is in the same office, or connected to the same private network as the CCA).
- As part of ICM compact support, an additional external (publicly routable) IP address is supplied as the Core address for ICM. This IP address is hardened and filtered for security purposes. This is currently seen as an SN10 activity, and is not currently supported as part of this activity.
- There is no longer any need to migrate FLIS based SS7 links to a USP-Compact after the core cutover. FLIS based SS7 links are supported on the CCA after the cutover.

- Baseline for the cutover is (I)SN09. This requires that the TDM office be brought up to (I)SN09 baseline prior to beginning the compact cutover.
- The set of PMs and applications supported in CS 2000 Compact is slightly different than in CS2100 Compact.

155.2.2 Office Cutover\

155.2.2.1 Cutover Strategy

The strategy for performing the CM to Compact-Core cutover for the North American and International Markets is based on CM to XA-Core Cutover methodology and on previous development done to support CM to Compact Core in ISN06/SE06.

All of these procedures are based on the existing software upgrade methodology (One Night Process, or ONP). This core-to-core ONP is accomplished by having the Compact-Core behave as an “inactive” CPU, while the CM Core behaves as the “active” CPU. Data and activity can then be transferred to the new core by a TABXFR, PRESWACT, and NoRestartCutover, similar to those processes used during a standard ONP.

The cutover tools assist the personnel involved in installation and software delivery to manage the retrofit process throughout the entire retrofit. The tools are delivered on the *NONRES Installation/Commissioning Tools Tape or CD* as a set of loadable modules that and are loaded onto both the CM and Compact cores for the duration of the cutover. After the Compact-Core cutover has been completed, the tools are removed.

A special cutover hardware tool called the Cut-Over Device (COD) which was developed for the CM to XA-Core cutover is also used. The COD acts as a switchbox in the links from both the CM and Compact Cores to the MS. It performs conversion of the DS-512 and OC-3 protocols used between the CM and Compact-Core and the MS respectively. The COD simplifies and increases the reliability of the Cutover procedure by making it easy to switch individual links between the CM and Compact Cores, test for the correct link connectivity, setup a data transfer link between the two cores, and perform a switch of activity (SWACT) between the two cores.

In the CM to Compact Call Agent Cutover procedure, the CODs are installed in a portable XA-Core shelf. There are both SNSE and SN versions of the CODs. (Figure 4)

155.2.2.2 ICM Cutover Overview

To support ICM over the Core cutover requires that the ICM systems be shutdown briefly, and the Core IP address be changed to the CCA core address, and the system is restarted once the Core Cutover has occurred. There are many ICM configurations possible, involving Nortel or 3rd party ICM systems, which may or may not be operating through a proxy. These systems

are usually located on the ICM customer premises. There may be several ICM systems supported off the DMS.

As part of the planning activities for the cutover, the ICM customer(s) must be involved to capture the specifics of their ICM configurations, to review the plan for the cutover, and to secure their participation in the pre-testing and night of cutover activities. They must also participate in any changes required to firewall rules in order to support connectivity to the new Core IP address.

ICM connectivity pre-test will be performed a few days prior to the night of cutover. This involves testing ICM connectivity to the CCA from within the office, and also from the customer sites. It is recommended that each ICM customer should perform the steps to pretest ICM connectivity to the CCA from their site, in concert with the onsite tech.

On the night of cutover, the ICM customer will execute the ICM cutover steps for their ICM system, coordinated with the actual core cutover.

155.2.2.3 Synopsis

The purpose of this activity is to provide support to convert an office running (I)SN09 on a CM core to (I)SN09FF running on a Compact core.

Also, provides support to convert an SDM/CBM800 running in SN09 to CBM850 running SN09FF load in parallel with the conversion of CM core to Compact Call Agent.

There are many aspects to this cutover, (roughly in order of execution), including:

- Advance Planning and Preparation
- Bring office h/w to SN06 baseline, upgrade it to supported hardware and s/w to SN06 baseline, s/w upgrade to SN09, as required.
- Upgrading MS hardware and software to baseline as required during the procedure.
- Load and Tool Delivery
- Commissioning the new Compact Core (including the Core and IO blades, Disk storage server, and LAN).
- Installing and Commissioning/Configuring the new CBM850 and establish the communication to newly commissioned CCA (IMs and NTPs are provided in the section **3.2.3.4.3**).
- Installation of specialized cutover tools to aid in the process.
- Integration of Cutover devices (CODs)
- MS Boot Testing
- Integration of the DMS/TDM LAN with the CS-LAN IP network

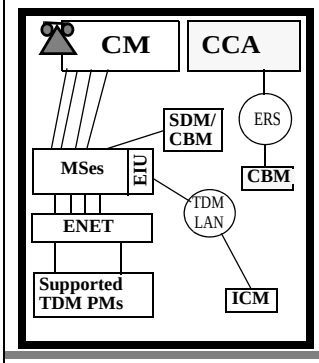
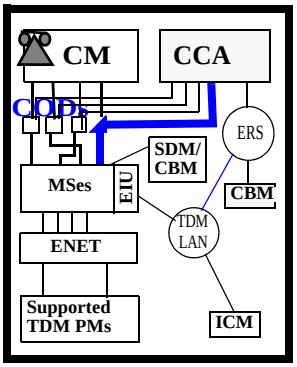
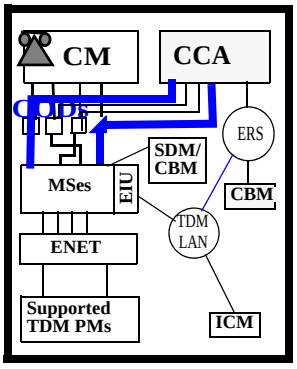
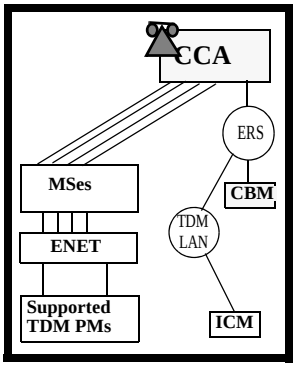
- Perform the downstream connectivity testing from CBM850.
- Perform the billing application pretest on CCA and CBM850.
- ICM connectivity pre-testing to the CCA
- ManB all the CBM850 applications.
- Transferring and converting switch data from the CM to the Compact Core.
- Rts all the CBM850 applications.
- Make sure that the SBA schedules are activated.
- Prepare ICM for cutover.
- Switching activity from the CM core to the Compact Core.
- Perform the billing application post test on CCA and CBM850.
- Switching ICM applications from communicating with the core via the TDM LAN EIU to the CCA. Bring ICM systems insv, and perform call testing.
- If downstream is configured on the SDM/CBM800, send the billing files to downstream.
- Bsy and OffL the DS512/OC3 card on the CCA, which is used for connecting the SDM/CBM800.
- Removal of the cutover tools, including CODs, upgrade the MS CMIC cards to OC-3.
- Removal of TDM EIU LAN equipment.
- Decommissioning the CM core.
- Optional consolidation of LAN equipment.

155.2.2.4 Procedure Overview

Figure 1, "Cutover Procedure Summary of Activities and Impact" below gives an overview of the end to end cutover procedure. Notice that there are activities occurring both before and after the Night of Cutover (Z-date). The overall time frame listed in the figure is an approximation only. Actual time frames are determined by the Installation team in consultation with the customer and are captured in the CM-Compact Cutovers Planning Guide.

The procedure supports Single Cabinet Compact configurations (Non-Geographic Survivable).

Figure 1 Cutover Procedure Summary of Activities and Impact

Office Configuration	Activity in Office	Impact to Customer	Timeline
	**Baselining/Installation/Commissioning**		
	• Upgrade office to h/w and s/w baseline for cutover: may include as required: - JNET to ENET conversion - Migrate to supported PMs - S/W upgrades	• Various, depending on upgrade procedure	• Z-30-Z-15 •
	• Upgrade MS hardware to baseline	• MS Simplex for h/w upgrade (1-2 hrs)	
	• Commission CCA & ERS	• No impact to inservice office	• Z-14
	• Install & Commission CBM850.	• No impact to inservice office	• Z-13 •
	**Integration/Data Transfer Phase**		
	• Integrate CODs in CMIC links	• Each MS Link OOS during integration	• Z-5
	• Perform MS Boot Testing	• Each MS in simplex for 2 hours	• Z-4, Z-3
	• Integrate ERS8600 into TDM-side LAN	• No impact to inservice ofc.	• Z-2
	• Appl pretest CCA-CBM850	•	•
	• ICM connectivity pre-test	No impact to inservice ofc.	• Z-2
	• Establish Data Transfer Config. - one COD is switched to CCA	• No impact to inservice ofc.	•
	• Transfer SLM data to CCA via SLMXFR	Office runs with three MS-core-links for duration of data transfer	Z (Day/ Night of Cutover)
	• Setup Volume mapping (volalias)		
	• Perform ONP TABXFR, EIU IP Tables not transferred	• CM remains InSync	
	**Switch of Activity Phase**		
	• Establish Cutover SWACT config.- Two CODs are switched to CCA	• Office runs with two MS-core-links	• Z (Day/ Night of Cutover)
	• Prepare ICM for cutover	•	
	• Prepare CBM-850 appls for cutover	•	
	• Switch activity to CCA via NoRestartCutover	• TSI < 15s; PSIs < 30;Two MS-core-links, EIU IP Applications < 5min.	
	• Switch Remaining CODs to CCA		
	• Verify CBM850 applications		
	• ICM cutover to new Core IP	•	
	• Remove NIIKEY Files	•	
	**De-Commissioning Phase**		
	• De-integrate CODs, install OC3 PB's on MS CMICs	• MS Simplex for 1 hour.	• Z+2, Z+3
	• De-Integrate TDM LAN from EIU		•
	• Remove EIU datafill from CCA		•
	• Decommission EIU		•
	•		• Z+4-5
	• Decommission CM/SLM		• Z+7
			• Z+7
	Z=Cutover Night		

155.2.2.5 Components

The following sections describe the components of the Hybrid cutover. They are roughly in order of execution,.

155.2.2.5.1 Software and Hardware Baseline

This portion of the activity identifies the Software and Hardware baseline required as the starting configuration. If necessary, activities may be needed pre-cutover to bring the office to baseline. For example, if a JNET office is to be converted, it would need to be upgraded to an ENET prior to applying the CM to Compact Cutover procedure.

Examples of upgrades that might be required:

- JNET to ENET conversion
- CM hardware upgrades to SN70EM or SNSE70EM
- Migration of services away from unsupported PMs to supported PMs (for example - moving from Series 1 PMs to XPMs)
- DPP/BMC conversion to CBM-800.
- Software upgrade of the entire office to (I)SN09 baseline

End goal is to have the office on the (I)SN09 s/w release with only hardware supported over the cutover.

Supported hardware:

- SNSE70EM or SN70EM BRISC processor
- ENET
- CBM800 or SDM
- IOM
- Series II peripherals: MTM, SMS, ESMU, SMU, ESMA, SMA, LGC, RSCS, LTC, LGCi, DTC, LTCi, SPM, DTCI, IW-SPM

155.2.2.5.2 MS Hardware and Software Upgrade

The following elements of the MS hardware are upgraded during the process, as required:

- MS Processor card upgraded to NT9X13DG (SN) or NT9X13NB (SNSE), (if required). This task is done as part of the office hardware base lining activities.
- MS CMIC Port cards upgraded to NT9X17AD (if required). This is done at the same time as the MS Processor card upgrade, during the hardware baselines phase.
- MS Mapper Card is updated if required.

- Each upgrade of the MS hardware requires the MS unit to be powered down during the card replacement.

155.2.2.5.3 Compact Core Commissioning

The compact core is installed and commissioned according to the installation IM. This portion of the system is commissioned prior to connecting it to the MS to begin the Cutover procedure.

Part of the commissioning process is to datafill the IP provisioning tables with the correct IP datafill for the Compact Core. The tables that need to be provisioned are:

- IPNETWRK[1]
- IPHOST

The other tables that were traditionally involved with IP provisioning on CM based cores are not required to be datafilled and are to be left empty. These are:

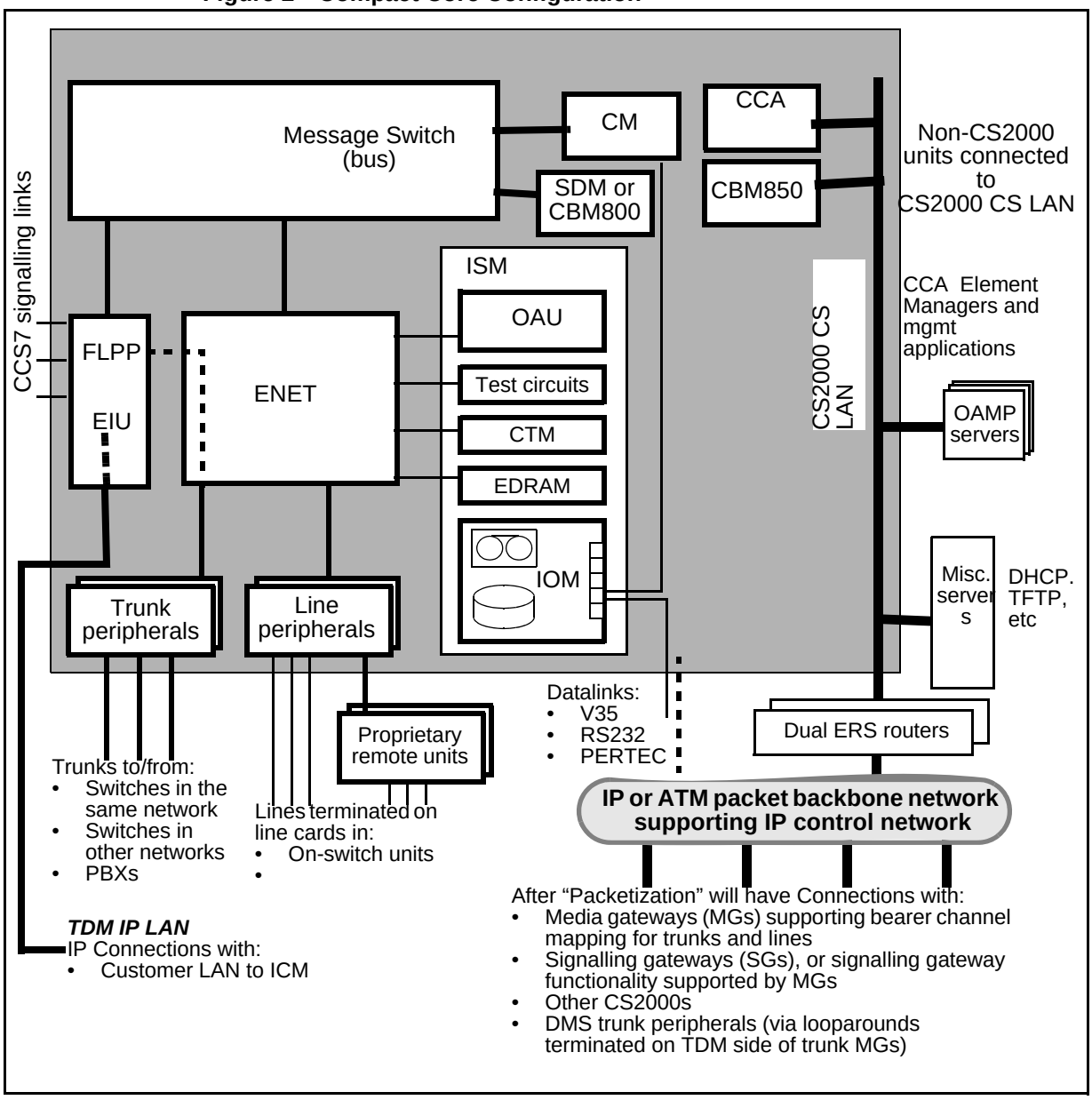
- IPROUTER
- IPTHRON
- IPPROTO
- RMCONFIG

At the end of this phase, and prior to COD and LAN integration, the Compact Core is set to be the Inactive Core using the NIIKEY files.

Figure 2, "Compact Core Configuration" shows the configuration after this step.

[1]The installer must be provided with he appropriate EFILEs to do this provisioning. IPNETWRK needs to have one IP address defined as well as the SCRNFLAG setting. The CM core can support up to 16 IP addresses. These will get collapsed down to one new Compact Core IP address.

Figure 2 Compact Core Configuration



155.2.2.5.4 CBM850 Commissioning and Configuring

The CBM850 is installed and configured according to the installation IM (24-2610) for the SN09 load. Establish the communication between newly commissioned Compact core and CBM850. Make sure that CBM850 communicates with Compact core.

Use the following NTPs/IMs to configure the applications on CBM850.

Table 1 CBM-850 Documents

Application	NTP/IM
CBM850 Commissioning	24-2610
Security and Administration	NN10358-611.03
SuperNode Billing Application	NN10363-811.03
GDD application	NN10353-511.03
Log Delivery Service	NN10353-511.03
OM Data Delivery	NN10361-711.03
Passport Log Streamer	NN10440-450
GR740PT	NN10440-450
DNBD Call Data Delivery (NA load)	NN10190-113
DNBD Call Data Delivery (International load)	NN10194-113 NN10449-113
DDMS	NN10347-461.03

Configure the DDMS applications on the CBM850. But, do not bring the DDMS applications (**OSS Comms Svcs & OSS and Application Svcs**) to InSv state on the CBM850.

Make sure all the other applications are inservice on the CBM850 after configuring them.

NOTE:

If downstream configuration required for the SBA and same downstream is used for both SDM/CBM800 and CBM850 systems, a new directory need to be created in the downstream for the CBM850 billing file transfer. While configuring the SBA schedules on CBM850 the new directory information has to be provided to avoid overwriting the billing files in the downstream.

SBA schedules can not be activated when there is no active stream running on CBM850. The schedules will be activated only during billing pretest.

WARNING

When SBA schedules are configured on CBM850, do not use the same downstream directory info used in SDM/CBM800 configurations. Create a new directory in the downstream system and configure the schedules with the new directory information to transfer the billing files to downstream.

155.2.2.5.5 Provisioning of New external Core IP address

A requirement for ICM on the CS 2000 Compact Hybrid is to have an externally visible IP address for the Core, to allow external ICM applications to communicate with the core. Since normally the Core IP address is only visible on the internal CS-LAN, the security of this new IP address is important.

This is currently being pursued as an SN10 activity.

In the interim, it is recommended that the cutover procedure be limited to offices with ICM systems that are either co-located with the CCA, or can be connected to the CS-LAN in a secure manner (for example, on the same private lan).

155.2.2.5.6 Load Delivery

Loads, and software tools are delivered on SLM tapes or CDs. The following are expected:

- CM cutover tools
- Compact-Core Cutover tools on CD.
- Compact-Core Loads on CD:
  - (I)SN09FF Compact-Core platform (LINUX) image and MC (Message Controller) image.
  - (I)SN09FF Compact-Core Application (SOS) and MS images.
- SN09FF CBM850

These loads, and software tools are transferred from tape or CD to SLM disk volume or Compact disk volume as appropriate.

155.2.2.5.7 Site Preparation

Site preparation includes activities such as:

- Verifying connectivity to the switch
- TABAUDIT - used to verify the validity and integrity of the table data

- PRECHECK - used to verify the switch preparedness for the ONP.

155.2.2.5.8 Cutover Software Tools Installation

During the Cutover Tools installation phase, the software tools are installed and initialized on both the CM and Compact cores. The software tools consist of loadable modules. Scripts are provided to facilitate the loading of the tools.

Two new modules (SDMCBMTG & CCACMDCM) are introduced in CM as part of the cutover tools for the SDM/CBM800 to CBM850 cutover activity. New loading and unloading scripts are introduced to load and unload the cutover tools on CM.

If billing pre-test need to be performed, then the following modules need to be transferred to the Compact Call Agent.

CRSGENUI
CRSGENP
CRSGENCI
BCRUGENI

loadcmtl: New script to load the cutover tools on the CM.

The list of modules require for the SN/SNSE CM core:
XARETNRG
XARCMDUI
XAMCLUI
XAMCLDAD
XAMCLKID
SLMXFRUI
SLMXFRBG
SLMXFRCI
VOLNAMUI
VOLNAMCI
CUTSWCT
CUTSWTCI
CUTTODTX
XARETCI
XAMCLCM
VOLNAMCM
CMMTCC
XARCMDCM
XARCLNCM
SDMCBMTG
CCACMDCM

unldcmtl: New script to unload the cutover tools on the CM

A brief summary of each of the commands, accessed via the XARETRO CI follows:

XARETINIT
This command initializes retrofit software and prepares the system software for an Compact Core retrofit.

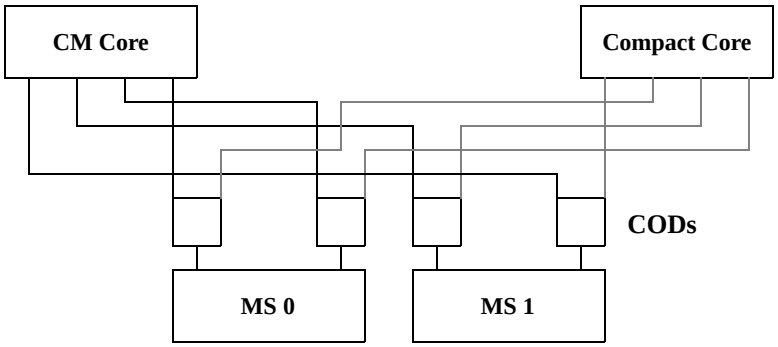
STATUS
This command provides a report of the state of the Compact Core retrofit. For each procedure within the retrofit procedure, a report is given on the progress which has been made.

LINKTEST
This command is used to test the CMIC links and to verify that they are able to carry messaging (see "Figure 3 Office Configuration with new CMIC links, CODs integrated" on page 1501 for a description of the links to be tested):

- the CM Core (Old Core) to COD links, the COD to MS links and the COD to Compact-Core (New Core) links for CM to Compact Cutovers.

Each link is tested separately, as the CODs are integrated.

Figure 3 Office Configuration with new CMIC links, CODs integrated



MATECORELINK
The MATECORELINK command is used to establish a communication path between the CM and CA cores. The communication path allows a graceful means to transfer office data and activity to the new core.

VOLALIAS
The VOLALIAS command is used to establish the name mapping from the CM SLM volume to the Compact Core disk volume. The SLM volume names are replaced with the corresponding Compact Core disk volume names.The SLM to Compact Core volume name translation mechanism is required to

eliminate mismatches in application data between the SLM volume name and the Compact Core disk volume name.

In addition to the above, Table Reformat support is provided to translate SLM volume names in office tables during TABXFR.

VOLNAMXFR
The VOLNAMXFR command is used to transfer the names of the SLM disk volume names from the CM to the Compact Core. This information is used to setup the FROM portion of the VOLALIAS volume mapping.

SLMXFR
This CI increment supports SLM file transfer activity from SLM disk to Compact Core disk during CM to Compact Core cutover. This is needed because the SuperNode/SNSE CM Core to Compact Core Retrofit will replace SLM disk and tape devices with NFS mounted disk volumes on the Compact Core.

CUTSWACTCI
This CI increment provides a mechanism similar to NORESTARTSWACT to be used for SuperNode/SNSE CM to Compact Core Cutover. Specifically the following commands are provided:

- NORESTARTCUTOVER - This performs the switch of activity from the old core to the new core. For Cutover, the NoRestartCutover switch of activity is from an insync SuperNode or SNSE CM core, to an insync Compact Core.

- SWACTTRAK - This provides a time trace of the activities occurring during the NoRestartCutover switch of activity.

RESET
The RESET command is used to reset the status of the policing software. This enables the user to begin a new retrofit without unloading and reloading the software tools.

CI@RTIF Function
A CIBINCOM interface is provided at the CM RTIF after the switch of activity to the compact core. This allows text based commands, including NODISP MAP commands, to be performed at the CM RTIF. This functionality allows executions of various commands required to prepare the CM core to initiate an abort cutover.

COREGOACTIVE
The COREGOACTIVE command can be performed on the CM core after a switch of activity to the compact core in order resume activity/callp on the CM core. This is used to support aborts back to the CM core. Impact is equivalent

to a COLD RESTART. It would be executed from the CI@RTIF prompt on the CM.

SUSPEND/RESUME
The SUSPEND and RESUME commands are used on the active CM core to either suspend or resume the cutover procedure respectively. The SUSPEND command is used by the TELCO to allow commands to be executed that would normally not be permitted during the retrofit window. Once these non-retrofit commands are completed, the cutover set of permissions can be resumed, via the RESUME command, without loss of cutover progress data. One example of commands that are normally disallowed during cutover is MATELINK RTS which would put the active CM core in splitting.

155.2.2.5.9 Cutover Device (COD) Integration

The cutover devices (CODs) are integrated into the MS links. The CODs are expected to be shipped to site in a Portable XA-Core cabinet. It is not necessary for the Compact cutover to have the portable XA-Core shelf populated with any of the XA-Core cards. Only the 4 CODs are needed in their correct slot positions.

“Figure 4 SuperNode COD” on page 1504 and “Figure 5 SNSE COD” on page 1505 show diagram of the SN and SNSE COD devices respectively. While the SN and SNSE CODs are very similar in appearance, they are not interchangeable. The type of COD is easily identified by the label **SN** or **SNSE** at the top of the COD. These labels are highlighted in the figures.

The toggle switch (S1) is used to switch the link from the CM to the XA positions. The XA position connects the MS to the Compact Core.

“Figure 6 COD locations on an XA-Core Shelf” on page 1506 shows a rear view of the XA-Core portable shelf showing the COD locations within the shelf. The CODs must be inserted in the correct slots:

- COD 0 - Slot 14R
- COD 1 - Slot 13R
- COD 2 - Slot 6R
- COD 3 - Slot 5R

Figure 4 SuperNode COD

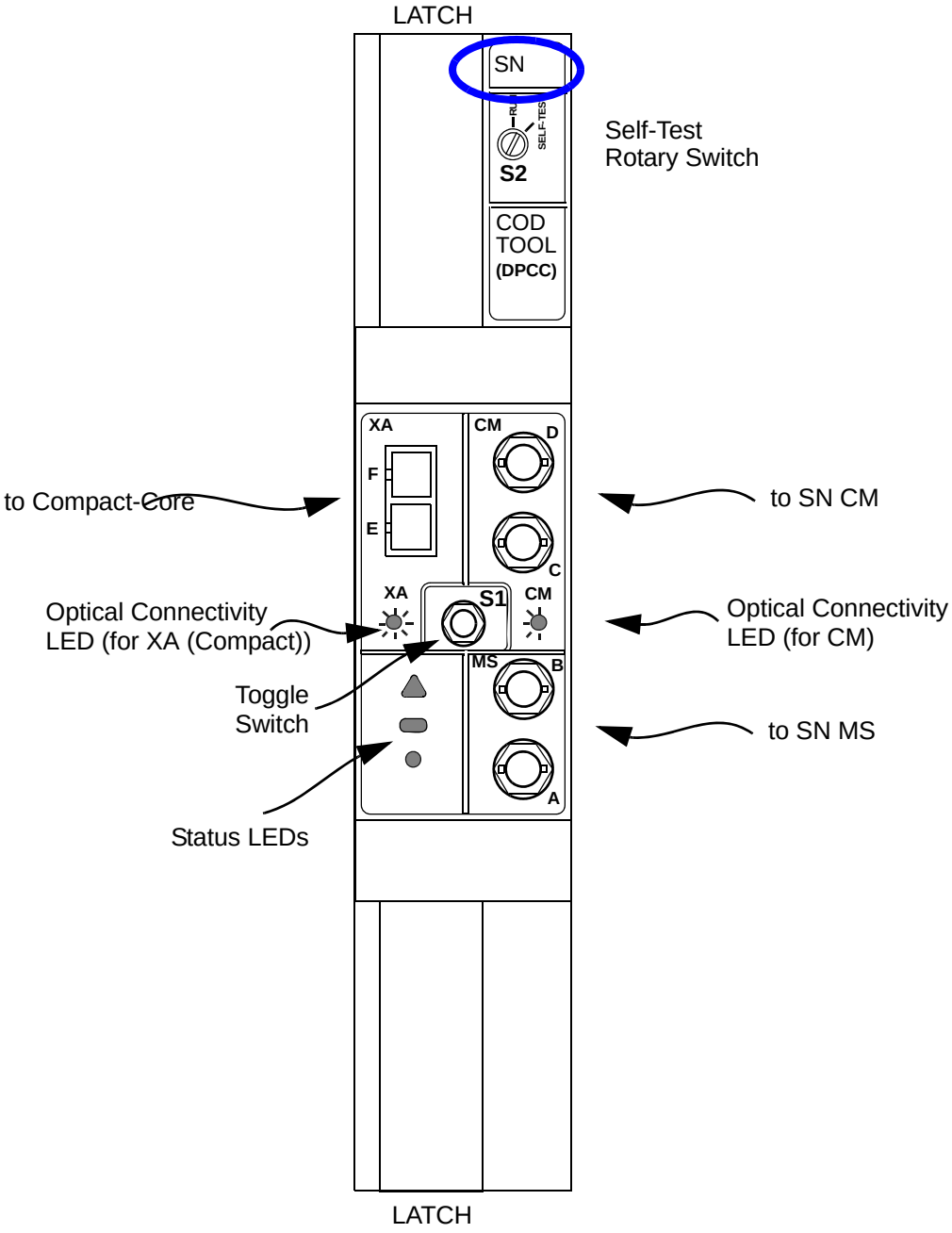


Figure 5 SNSE COD

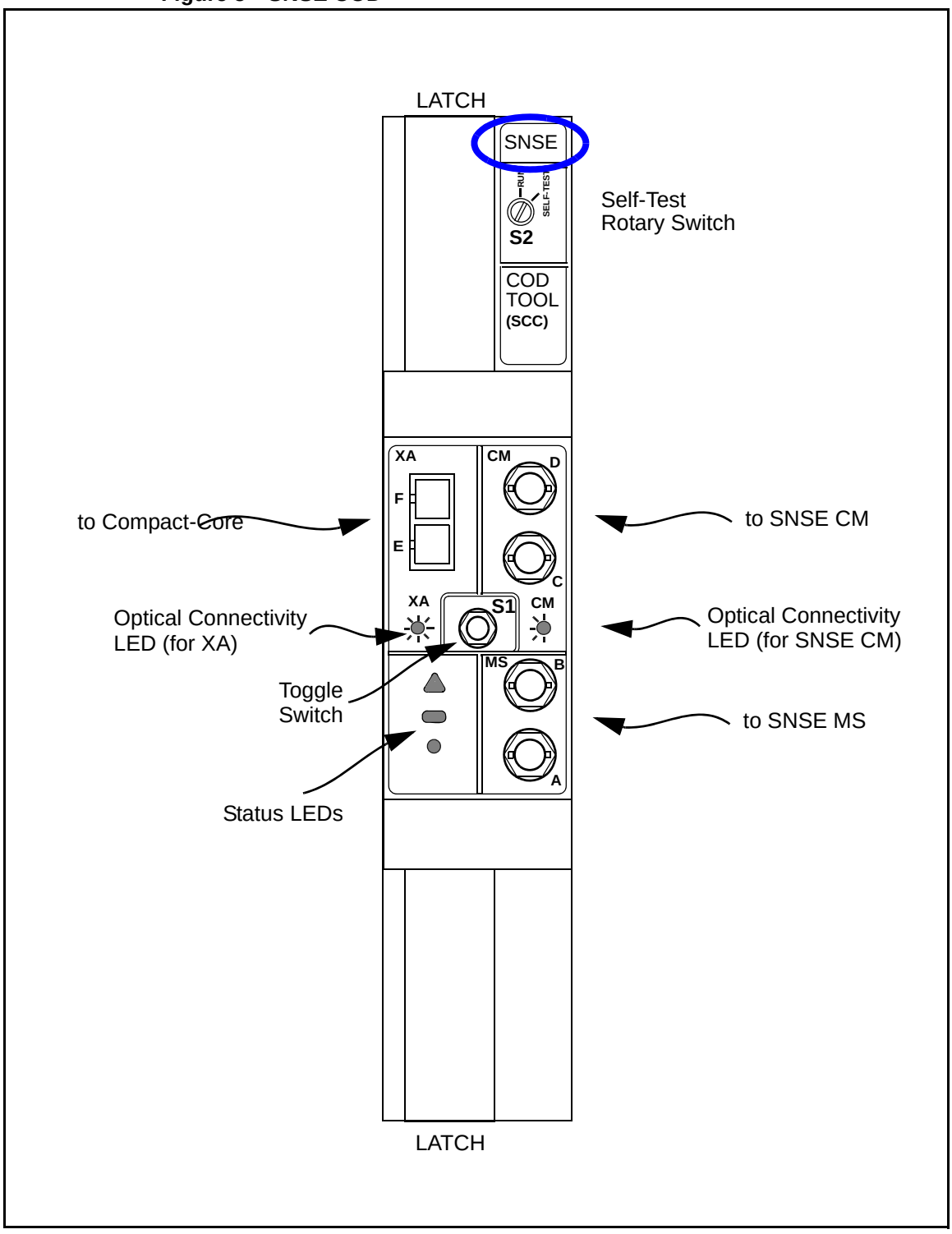
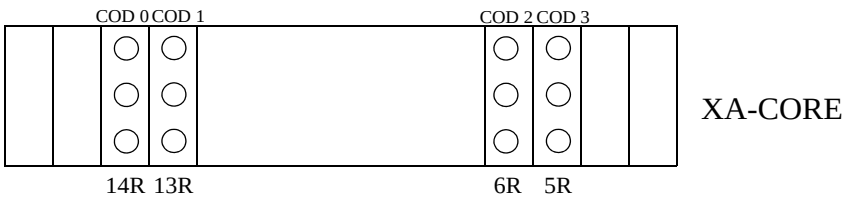


Figure 6 COD locations on an XA-Core Shelf



Rear View

155.2.2.5.10 MS BOOT testing

The MS boot testing procedure verifies connectivity between the Compact and the MSes, and ensures that the MSes can be loaded from the Compact.

In turn, each MS is BSYed on the CM side. The Compact core is booted active, with the appropriate CODs switched to the Compact side. The MS is booted over each CMIC link.

155.2.2.5.11 CBM-850 Application Pre-test

This procedure tests that the Compact can talk to the CBM-850 and that CBM applications can be successfully brought insv.

Make sure that all applications are InSv in the CBM850 except DDMS applications (**OSS Comms Svcs & OSS and Application Svcs**). This will ensure that the CBM850 applications are able to communicate with the CCA core.

Perform the downstream testing to make sure CBM850 can communicate with the downstream. Execute *ping* command on CBM850 with IP address of all the configured downstreams and make sure that the *ping* command works fine. This will ensure that CBM850 can communicate with all the configured downstream systems.

CBM850 Billing Pretest

This testing will be performed prior to the ONP to make sure billing records are transferred to CBM850 from CCA as well as to downstream from CBM850. Make sure that the applications on the CBM850 are configured and in-service.

- Setup of the MATECORELINK in the data transfer configuration (1 link to Compact).
- VOLNAMXFR to transfer the volume names from the CM to the Compact.
- VOLALIAS to provide a mapping from CM to Compact volume names.

Transfer Billing datafill
- Transfer the billing related tables from CM to Compact Core
ca_sos> tabxfr
ca_sos> stopif 1
ca_sos> limit 25
ca_sos> setup ca
ca_sos> status
ca_sos> xfronly OFCENG
ca_sos> xfronly CRSFMT
ca_sos> xfronly CRSMAP
ca_sos> xfronly SDMBILL

Disable MATECORELINK
- Bsy matecorelink
cm_map> xaretro
cm_map> matecorelink bsy

- Toggle the COD back to CM side
- Rts the CMIC port for the link on CM
  - SN CM : mapci;mtc;ms;shelf 0; card 25; rts 1 port 0
  - SNSE CM : mapci;mtc;ms;shelf 0; card 4; rts 1 port 1
- At this point all the COD switches should be toggled to CM.

Suspend XARETRO tool
- Suspend the tool until it is needed again.
cm_map> xaretro
cm_map> suspend

ca_sos> xaretro
ca_sos> suspend

Boot the CCA as Active
- Disable the NIIKEY
- Dump the IMAGE on CCA
- Set the boot file on CCA with the dumped image
- Reboot the Compact Call Agent blades

Perform the test
- Downloading of data dictionary successful
  >cbmmtc appl
    - verify that the application “tasl” is InSv
      (may take up to 15 minutes to download)
- Make sure that config data migration is done

Activate the SBA Schedules on CBM850:
- Follow the procedure given in **Appendix section 3.9.5** to activate the configured schedules.
- Verify that the schedules are activated using the procedure given in **Appendix section 3.9.6.**

Billing testing on CBM850 and Compact core:
- If AMA streams are configured
 - load the *crsgen* tool on Compact core (available as part of the cutover tools)
  ca_map> load crsgenui
  ca_map> load crsgenp
  ca_map> load crsgenci
  ca_map> load bcrugeni
  - with SBA InSv on the CBM850
  ca_map> crsgen ama setrate 200
  ca_map> crsgen ama start
  wait for 1 minute
  ca_map> crsgen ama stop

  - with SBA ManB on the CBM850
  ca_map> crsgen ama setrate 200
  ca_map> crsgen ama start
  wait for 1 minute
  ca_map> crsgen ama stop
 - RTS SBA on the CBM850 and perform the clean-up
 - unload the crsgen tool from CCA
  ca_map> unload bcrugeni
  ca_map> unload crsgenci
  ca_map> unload crsgenp
  ca_map> unload crsgenui
- If OCC stream is configured
  - with SBA InSv on the CBM850
  ca_map> cdrtst
  ca_map> cdrcrank 10 8 10

  - with SBA ManB on the CBM850
  ca_map> cdrtst
  ca_map> cdrcrank 10 8 10
 - RTS SBA on the CBM850 and perform the clean-up

Refer to the **Appendix section** of this feature for more detail on how to validate the Billing Normal and Backup modes.

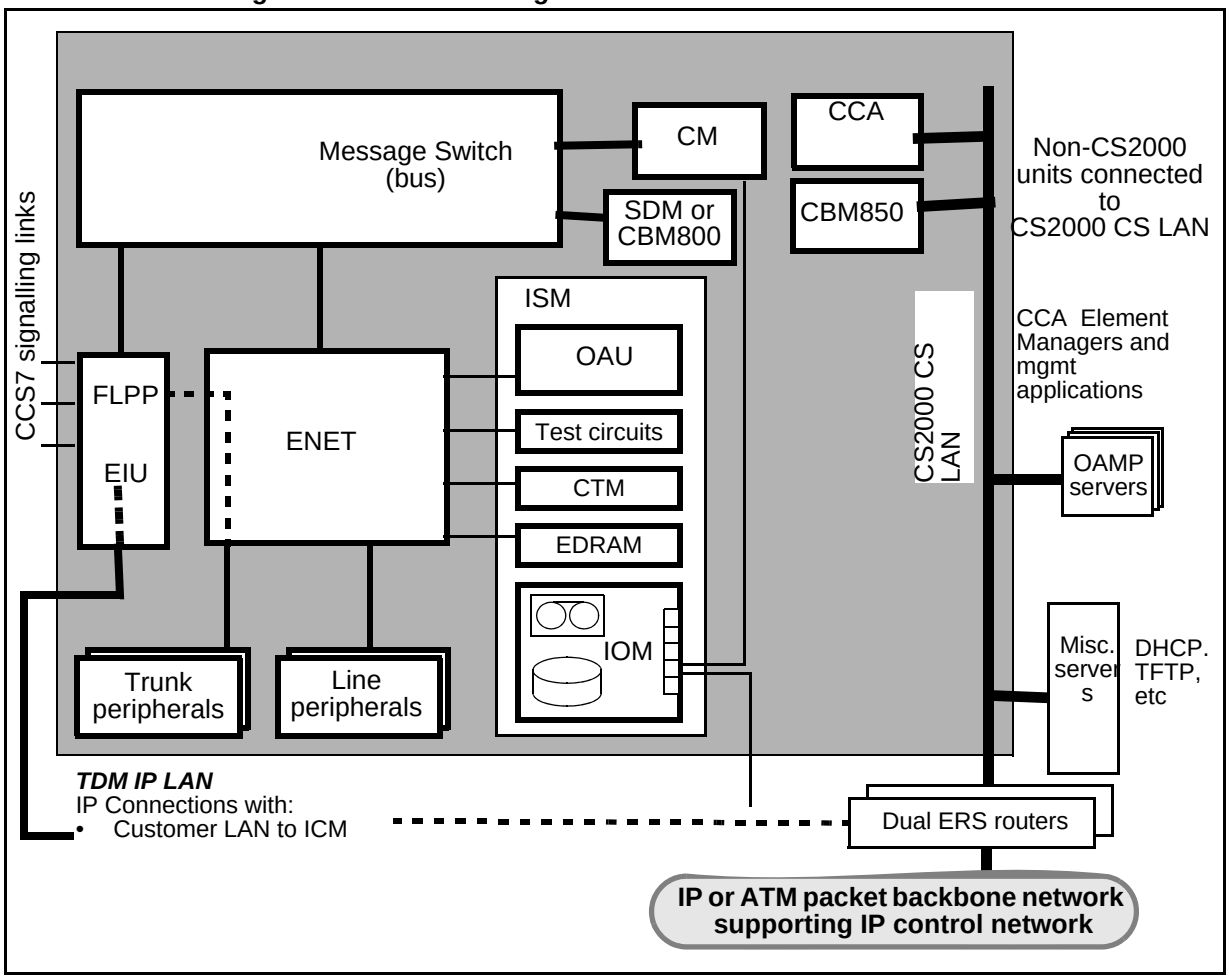
- Restore the matecore link back to CM (all the CODs are toggled to CM position).
- Boot the compact core as inactive with the patch current load prior to the ONP.

155.2.2.5.12 TDM LAN Integration with Packet LAN

During this phase any TDM LAN equipment is integrated into the packet LAN equipment.

Figure 7, "TDM LAN Integrated With Packet LAN" shows generically how the TDM LAN is integrated with the packet LAN. For each type of TDM LAN, the actual specifics will vary. A PC or other device should be used to test that the two LANs have been correctly integrated.After the integration, the IP traffic will continue to flow between the CM core and the down-stream IP application off of the EIU. No IP traffic will flow between the Compact Core and the down-stream IP application.

Figure 7 TDM LAN Integrated With Packet LAN



155.2.2.5.13 ICM connectivity pre-testing to the CCA

The intent of the pre-testing is to verify TCP connectivity on port 2500 to the CCA IP address. The tests will be performed a few days prior to the night of cutover.

TCP port scan of port 2500 on CCA IP address is used to pre-test the ICM connectivity.

Depending on how the ICM system is connected to the central office, additional rules on firewall(s) may be required to support ICM connectivity to the new core. In order to derisk ICM connectivity issues on the Night of Cutover, connectivity pre-testing should be performed from both:

1. Central Office site, on the TDM lan.

2. Customer ICM site(s)

Figure 8, "ICM connectivity Pre-testing" shows some example ICM systems connected to the Central office, and the connectivity testing done from each site.

TCP Port 2500 test

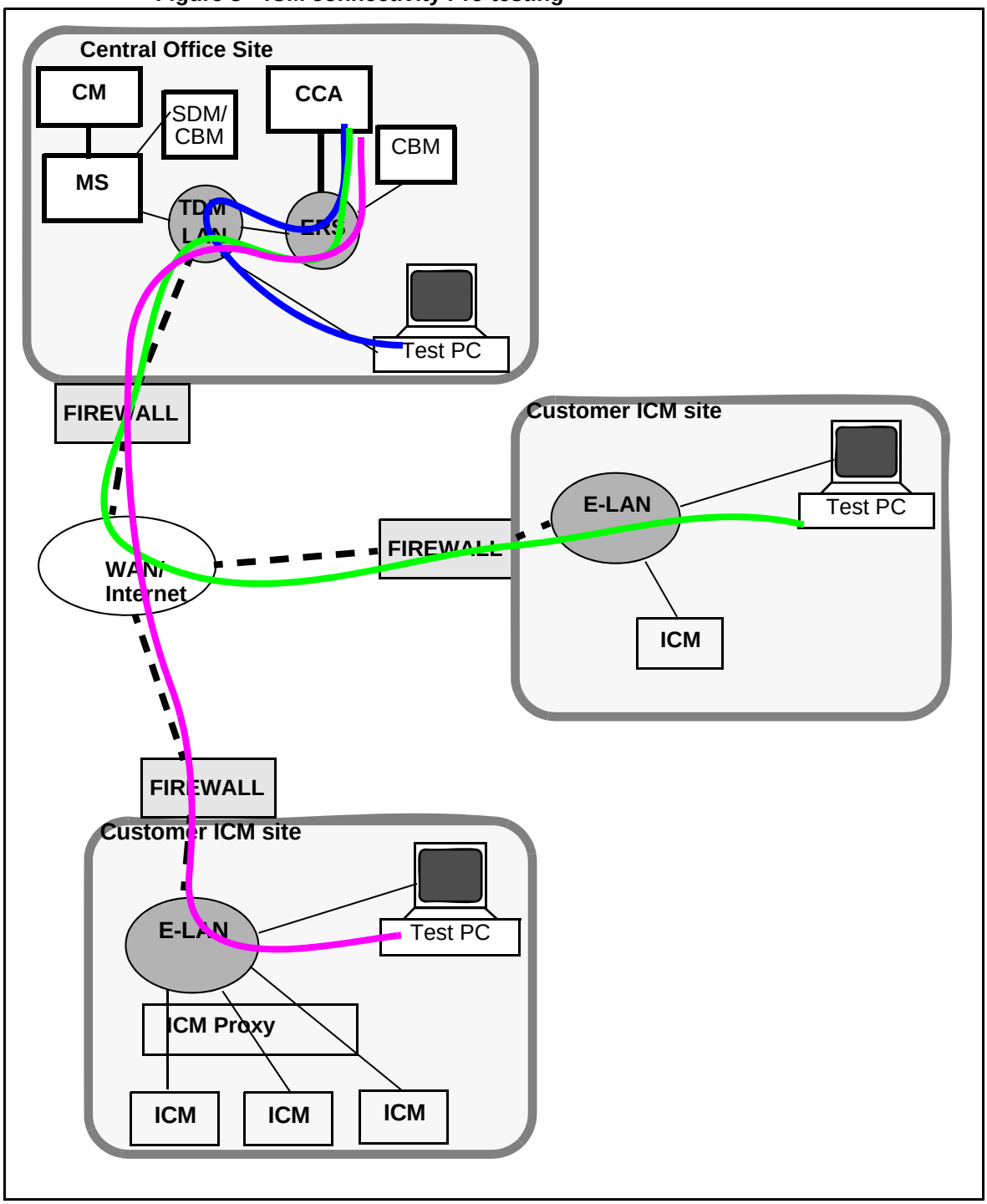
The TCP port test tests only TCP connectivity to port 2500 (port used by ICM/ SCAI); it does not validate any SCAI functionality in the SOS image, and does not require any special datafill in the SOS image, thus this is a much simpler test.

A port scan tool can be used to test the responsiveness of port 2500 on the CCA IP address. The desired response is that port 2500 is open on the CCA ip address.

Alternately, telnet can be used to attempt to test the connectivity to port 2500. (e.g. telnet <cca_ip_address> 2500)
Note that the desired response is that the telnet connection is rejected (since the CCA is not setup to support telnet on port 2500). If the request times out, this indicates that there is no connectivity to the CCA IP address.

Given the simplicity of the TCP port 2500 tests, and the easy availability of the software on the test PCs, the port scan or the telnet test is used to pre-test the ICM connectivity, at least for testing from the ICM customer site.

Figure 8 ICM connectivity Pre-testing



155.2.2.5.14 Transfer and Conversion of Switch data from CM to Succession CS-2000 Compact

This phase includes:

- Make sure that the Billing pretest is completed.
- ManB all the CBM850 applications (appctrl -b all)
- Setup of the MATECORELINK in the data transfer configuration (1 link to Compact).
- VOLNAMXFR to transfer the volume names from the CM to the Compact.
- VOLALIAS to provide a mapping from CM to Compact volume names.
- SLMXFR to transfer selected files from the CM to the Compact.
- TABXFR to transfer office datafill from the CM image to the compact image.

  Special steps are taken at this point to not transfer any of the office tables from the CM core that contain CM IP address and routing datafill. The following tables are not transferred:

  — IPNETWRK

  — IPHOST

  — IPROUTER

  — IPPROTO

  — IPTHRON

  — RMCONFIG

  The following tables are transferred:

  — ENSITES

  — ENTYPES

  — EXNDINV

- Software Optionality Control (SOC): As per ONP, any SOCs that are available on the active CM core are automatically transferred to the inactive Compact Core (Tables SOCOPT, SOCVAR, SOCFEAT). Any new software optionality control that need to be activated in the Compact Core that are not already active in the CM core, is not covered automatically and will need to be handled manually. [1]

155.2.2.5.15 Switching Activity from CM to Compact

The switching activity phase involves:

- Establishing the Switch of activity CMIC configuration - a second CMIC is toggled to the compact core for a total of 2 links, one from each MS. The MATECORELINK is then re-established on the second CMIC.

[1]SOCs for SMDR and SMDI may need to be handled manually, as SOC for these applications was introduced into Compact Core for these applications in SN04.

- Performing PRESWACT to prepare both cores for the switch of activity, and transfer dynamic data to the Compact.
- Prepare IP applications for cutover. Insure that all IP connections that are established over the EIU are properly disconnected.
  - The NETMAN tool can be used to insure that all IP connections are down.
- Do not run the **StatusCheck** under **bcsupdate; swactci** before the cutover.
- Rts all the applications on the CBM850 (appctrl -r all)
- If DDMS application is configured on CBM850, perform the following steps to bring up the DDMS applications.
  - unpermit the DDMS users on the CCA (e.g. unpermit sdm01)
  - permit the DDMS users on the CCA with default password
  - Bsy & Rts the DDMS applications (**OSS Comms Svcs & OSS and Application Svcs**) on the CBM850
- Make sure that all the SBA schedules are activated on the CBM850. Follow the procedure given in **Appendix section 3.9.6.**
  - If not activated, follow the procedure in **Appendix section 3.9.5** to activate the same.
- Make sure all the application on the CBM850 is InSv state (cbmmtc appl). It might take 10-15 minutes.
- ICM customers shut down their ICM systems and change IP address to CCA IP.
- Performing the NORESTARTCUTOVER to perform the actual switch of activity from the CM to the Compact, and recovery of the office.[1]
- Switching all CODs to the Compact Core.
- ICM customers restart their ICM systems, verify connectivity to the CCA Core, and proceed to test ICM calls.
- Performing office testing to ensure that the new load is running correctly.
- Perform the billing application posttest on CCA and CBM850. Refer **Appendix section 3.9.2** to run the test.
- If downstream is configured on the SDM/CBM800, send the billing files to the downstream. Refer **Appendix section 3.9.3** to transfer the billing files to downstream.
- Bsy and OffL the DS512/OC3 card on the CCA, which is used for connecting the SDM/CBM800.
- Performing POSTSWACT to cleanup after the switch of activity.

[1]As per all ONP's on CM, the applicator should be connected via the modem interface on the IOC and should not be using TELNET to connect to the CM.

- Soak min of 24 hours.

155.2.2.5.16 Cutover Tools Removal

This phase removes the COD devices from the MS links, integrating the NT9X63 OC3 paddleboards into the MS shelf. At this point, the Portable shelf can be removed from service.

Then, the Cutover software tools are removed from the Compact Core.

It is not necessary to remove the software Cutover tools from the CM core, as it will be decommissioned.

155.2.2.5.17 CM Core Decommissioning

This phase results in the CM core and SLM being removed from the CM shelf.

155.2.2.5.18 DMS TDM IP Hardware Decommissioning

This phase results in removal of all the DMS TDM IP hardware from the office and corresponding datafill from the compact image. The steps involved in this are:

- Removal of EIU hardware from the LPP/LIS/FLIS:
  - — Ethernet Interface Paddleboard Card - NT9X85AA,
  - — Ethernet Interface Card - NT9X84AA,
  - — Integrated PBUS and FBUS Card - NTEX22BB
  - — Media Access Unit (MAU) - a commercially available unit,
  - — Attachment unit interface cable.
- Removal of EIU datafill from table LIUINV.

155.2.2.6 Summary of changes to documentation

This section lists the documents used in the SL-100 CM to Compact cutover, and indicates in general the changes required to make documentation suitable for the NA and Intl CM to Compact cutover.

General changes required to multiple documents:

- Change references to MSL-100 product to DMS-100 Family product supported by this cutover procedure.
- Change references from SE06 to (I)SN09 (CM) or (I)SN09FF (Compact).
- References to IMs or other documents within these documents must be changed to refer to the new or changed documents.
- CCA software and tools are no longer delivered on DAT tape - most DAT tapes have been replaced by CD; SOS load comes on DVD.

The new procedures for CBM-850 application testing need to either be inserted at the appropriate points in existing documents, or have new documents created:

- CBM-850 application pre-test: (executed prior to the night of cutover) This could potentially be a new IM document.
- Billing pretest procedure for CCA/CBM850.
- Billing posttest procedure for CCA/CBM850.
- Billing testing Procedure for SDM/CBM800 during the abort. This is required for both the abort (prior and after switch activity)
- Sending the Billing files to downstream.

Table 2 MSL-100 Cutover Documentation

Document	Title	Changes Required
02-0526	SuperNode CM/SLM to Compact Hybrid Cutover Planning Guide	Bringing office hardware to SN06 baseline and upgrade it to supported h/w; s/w baseline to SN06 baseline, then upgrade it to SN09. The cutover will be done from SN09 to SN09FF
02-0872	SNSE CM/SLM to Compact Hybrid Cutover Planning Guide	Bringing office hardware to SN06 baseline and upgrade it to supported h/w; s/w baseline to SN06 baseline, then upgrade it to SN09. The cutover will be done from SN09 to SN09FF
24-1469	Compact Core Software Tools Loading	Need to add additional modules introduced for CM and new scripts to load and unload the modules on CM. Need to add the billing pre-test modules introduced for CCA. These tools need to be transferred only if billing pre-test is required.
24-0879	SLM Data Transfer for SNSE/CM to Compact Core Upgrades	
24-1471	SLM Data Transfer for SN/CM to Compact Core Upgrades	
24-0877	MS Boot Testing for SNSE CM/SLM to Compact Core Upgrades	
24-1470	MS Boot Testing for SN/CM to Compact Core Upgrades	

Document	Title	Changes Required
78-0534	COD Integration for SN/CM to Compact Core Upgrades	
78-0538	COD De-Integration for SN/CM to Compact Core Upgrades	
78-0874	COD Integration for SNSE/CM to Compact Core Upgrades	
78-0878	COD Deintegration for SNSE/CM to Compact Core Upgrades	
24-1626	Patch-Current S/W Loading for SN/ SNSE CM/SLM to Compact Core Upgrades	
78-0539	SN/CM to Compact Core Cutover	
78-0873	SNSE/CM to Compact Core Cutover	
78-0873	SuperNode MS System Upgrade for XA-CORE	
65-6131	SuperNode SE: MS System Upgrade for XA-CORE	
78-1466	Portable XA Installation/Removal for Compact Core Hybrid	
30-1473	Clean Up for CM to Compact Core Hybrid Upgrades	
24-0971	CS2000 Compact Call Agent/ STORM Software Installation and Commissioning	Not related to cutover, although used in installation/commissioning of CCA – should be no change.
555-4001-213	Meridian SL-100 SN/SNSE CM to Compact Core upgrade Method of Procedure	- Remove the DPP/BMC billing references. - Remove references to SMDR billing over EIU. - Remove the step and procedure used to perform the STATUSCHECK on CM core after the preswact and before the norestartcutover.

155.2.3 Cutover Aborts

Aborts of the procedure are provided for two main scenarios:

- Prior to switching activity to the Compact.
  Generally, the abort involves stopping the process, and switching all CODs back to the CM core.
  Make sure that all the applications on SDM/CBM800 becomes in-service after the abort.
  Perform the billing testing on SDM/CBM800. Refer **Appendix section 3.9.4** to test the billing on SDM/CBM800.
  If applications are in-service (appctrl -q all) in CBM850, bsy all the applications (appctrl -b all).

- After switching activity to the Compact.
  Once the switch of activity has occurred, up to the point where the new load has been accepted, abort back to the CM is possible using the following method:
  - If necessary, migrate SS7 links from USP-Compact back to FLIS.
  - Switch all CODs back to the CM side.
  - Perform a COREGOACTIVE command from the XARETRO CI on the CI@CM-RTIF.
  - Perform a COREGOINACTIVE command on the compact core.
  - For offices which have ICM, the core address on each of the ICM systems (or ICM proxy as appropriate) will need to be changed back to the old CM core IP address. Note that this requires coordination with the ICM customer(s) who have the ICM systems on their site(s).
  - Make sure that all the applications on SDM/CBM800 becomes in-service after the abort. It might take up to 15 minutes.
  - Perform the billing testing on SDM/CBM800. Refer **Appendix section 3.9.4** to test the billing on SDM/CBM800.
  - If downstream is configured and billing records are collected in the CBM850, send the billing files to the downstream. Refer **Appendix section 3.9.3** to transfer the billing files to downstream.
  - Bsy all the application on the CBM850 (appctrl -b all)

It is recommended that the office undergo a data freeze during the acceptance period, as Journal files from the compact core will not be applicable to the CM core.

Once the CODs have been removed, abort is no longer possible.

155.3 Hardware Requirements or Dependencies

The following table lists hardware needed for the core cutover procedure.

Table 3 Cutover Hardware Requirements

Part Number	Title/Description
DSLX22AA	CMIC DS-512 to OC-3 Switchbox (SuperNode)
DSLX22BA	CMIC DS-512 to OC-3 Switchbox (SuperNodeSE)
NTLX01DA	Portable XA-Core

The following table provides a description of the MS baseline requirements for support of the CM to Compact Core Cutovers. Where indicated the components may be upgraded as part of the procedure, otherwise the baseline requirements must be met prior to beginning the process.

Table 4 MS Hardware Baseline (MS):

PEC	PRODUCT DESCRIPTION	COMMENTS
NT9X13DG Rel 01+	MS Processor (16 Meg.)	Upgraded SN MS/LMS CPU (NT9X13DD/DC/DB*)
NT9X17AD Rel 06+	MS 4-PORT PCP	Upgraded NT9X17AA - Upgraded ONLY for CMIC links
NT9X53AD Rel 05+	MS Clock Card	Needed to I/F with NTLX44AA
NT9X63 AB Rel 01+	OC3 2-PORT Paddleboard (with E3MLIC)	Replaces NT9X20AA/ NT9X62AB. Upgraded during procedure.
9X15AA Rel 50+	Mapper card	
* Currently deployed standard product.		

SDM Hardware Baseline:
Please refer to the “SDM Hardware Baseline” document under the following link for the SN09 SDM hardware baseline information.

http://livelink-ott.ca.nortel.com/livelink/livelink.exe?func=ll&objId=7908447&objAction=browse&sort=name

CBM800/CBM850 Hardware Baseline:
Please refer to the “CBM Product Specification 22/09” document under the following link for the SN09 CBM800 hardware baseline information.

http://livelink-ott.ca.nortel.com/livelink/livelink.exe?func=ll&objId=11892249&objAction=browse&sort=name

Please refer to the “CBM Product Specification” document under the following link for the SN09FF CBM850 hardware baseline information.

http://livelink-ott.ca.nortel.com/livelink/livelink.exe/fetch/6809740/13197707/7331141/7330811/12172432/CBM_Product_Specification_23_9.1?nodeid=12172204&vernum=0

155.4 Software Requirements or Dependencies

SDM/CBM800 & CM Software Baseline:

- SDM/CBM800 running in SN09 software baseline. All the SN09 patches need to be applied on the SDM/CBM800 prior to the cutover.
- CM running in SN09 software baseline. All the SN09 core patches need to be applied on the CM prior to the cutover.

CBM850, CCA and Cutover tools Requirement:

- (I)SN09FF Compact Call Agent software baseline.
- CM cutover tools on SLM tape.
- Compact-Core Cutover tools on CDs.
- SSPFS CDs for the CBM850.
- SN09FF CDs for the CBM850.
- SN09FF Compact-Core platform (LINUX) image and MC (Message Controller) image on CDs.
- SAM21 Load on CD.
- SN09FF nodata Compact-Core Application (SOS) and MS images on DVD.

155.5 Limitations and restrictions

This activity supports the cutover of CM core to Compact TDM/Hybrid Core.

- Only offices containing ENET are supported. JNET is not supported.
- Offices containing SDM/CBM800 are supported in the FROM configuration. The SDM/CBM800 is converted to a CBM850 during the cutover.
- Only the ICM IP communication based application is supported during the cutover:
  Other IP based applications are not supported over the cutover, although in most cases the application may be restarted after the cutover using the new core IP address.
- Both Supernode and Supernode SE are supported.

- SN70EM and SNSE70EM CMs are supported. SN50, SN60 or previous CMs are not supported
- Only common applications between SDM/CBM800 and CBM850 are supported during the cutover.

155.6 Interactions

This activity interacts with activity A00012766 for the SDM/CBM conversion.

155.7 Glossary

Term	Description
SNSE	SuperNode Size Enhanced
CBM	Core and Billing Manager
COD	Cut Over Devices
3PC	Third-Party Core, now called CS-2000 Compact.
SN	SuperNode
CCA	Compact Call Agent
ONP	One Night Procedure
CM	Compact Module
SDM	Supernode Data Manager
SBA	Supernode Billing Application

155.8 Reference Documents

Document	Title/Description
MOP 555-4001-213	Meridian SL-100 SN/SNSE CM to Compact Core upgrade MOP

155.9 Appendix

155.9.1 Billing Pretest: Validating Billing Normal & Backup modes

Billing testing will be performed for the SMDR, BC and CDR250 billing records on the Compact Core.

CBM850 setup:
- On the CBM850 verify that TASL and SBA are InSv
  -- From the CBM850: cbmmtc appl

- Verify that the billing stream AMA on the CBM is Active
billmtc
CONFSTRM
list ama

Generate Billing records On Compact Core for AMA stream:
Load the *crsgen* tool on CCA (available as part of the cutover tools)
ca_map> load crsgenui
ca_map> load crsgenp
ca_map> load crsgenci
ca_map> load bcrugeni

crsgen ama setrate 200
crsgen ama start
wait for 1 minute
crsgen ama stop

Generate Billing records On Compact Core for OCC stream:
cdrtst
cdrcrank 10 8 10

Verify the billing for AMA streams:
Verify the CBM850 setup
From the steps above, Start generating billing records using **crsgen**

/cbmdata/00/billing/ama/open> query
AMA:
PrimarySubStream: InSv
Number of Records in Open Files: 1485
ClosedNotSent Files Available: 0
Records within the ClosedNotSent files: 0
Date of Last File Sent:
Date and time unavailable.

/cbmdata/00/billing/ama/open> closec ama
Closed 020001.030002.00001.01.2

/cbmdata/00/billing/ama/open> query
AMA:
PrimarySubStream: InSv
Number of Records in Open Files: 0
ClosedNotSent Files Available: 1
Records within the ClosedNotSent files: 1600

Date of Last File Sent:
Date and time unavailable.

If downstream is configured on CBM850,
Send billing files downstream from CBM850:
billmtc
filesys
sendfile ama
- Verify that the downstream is receiving the file.
Note: This billing file will have the dummy records so, this file should not be processed for any billing purpose on the downstream system. Also, cleanup the dummy billing files from the downstream.

To verify Billing in backup mode, do the following:
From the CBM “cbmmtc” manbusy SBA
>cbmmtc appl
>bsy <SBA appl number>

Take a snapshot on Compact core logical backup volume:

>diskut
>lv
>lf <backup volumes for the ama stream>

- Make sure that there no backup files in all the configured backup volumes for the ama stream.

From the steps above, Start generating billing records using **crsgen**

Verify on Compact core that the logical backup volume is receiving billing file:

>diskut
>lv
>lf <configured volumes>

Those logical volumes should have incremental backup files.

To verify Billing in backup mode can recover do the following:

From the CBM “cbmmtc” manbusy SBA
>cbmmtc appl
>rts <SBA appl number>

On the Core, go to the map level: *mapci;mtc;appl;sdmbil;post ama*

The ama billing state should change automatically to rcvry and then into InSv

```
      MS    IOD    Net     PM     CCS     Lns    Trks    Ext    APPL
     MSpair AMA  B   .      .      .      .      ...   1Crit   .
      *C*    *C*                                        *C*
           OAMAP  ATMFW   SDM   SPMCP  SWMTC  SDMBIL  PKT
TOPSIP
 0 Quit          .     .     .     .     .     .     .     .
 2 Post_
 3 Addvol_
 4 Remvol_        AMA :     InSv  Pri:      InSv  Rec:      InSv
 5                          Bkup:     InSv  Comm:     InSv
 6 TST
 7 Bsy
 8 RTS
 9 Conf_
10
11 DispAL
12
13 Status
14 Query
15
16
17 Audit
18
  OPERATOR
```

Note: Make sure that you are receiving the amount of billing files that were on the core (SCA). The amount of files generated from the tool should match the amount received on the CBM when billing recovered from backup mode.

Unload the crsgen tool from Compact core:

```
ca_map> unload bcrugeni
ca_map> unload crsgenci
ca_map> unload crsgenp
ca_map> unload crsgenui
```

Verify the billing for OCC streams:
To verify the CDR250 billing format, repeat the above steps for the OCC stream.

Billing cleanup to be ready for the cutover:
From “CBMMTC appl” map level, ManBsy SBA
From the unix prompt on the CBM active unit:
>cd /cbmdata/00/billing/ama
/cbmdata/00/billing/ama>ls -lrt (to list everything under the ama directory)
/cbmdata/00/billing/ama> rm -rf * (remove all files and directories under ama directory to cleanup everything)
From “CBMMTC appl” map level, RTS SBA

From the unix prompt on the CBM active unit, verify that all directories got recreated):
/cbmdata/00/billing/ama> ls -lrt (All directories should have been recreated)

Note:
- If AMA stream is tested, Make sure that the crsgen tool is unloaded from the Compact core.
- If downstream is tested, Make sure that the dummy billing files from the downstream is cleaned up.

WARNING
During the billing pre-test on CCA, the following swerrs may be observed. Please ignore the swerrs only during billing pre-test.

```
CSNNC09BS     SWER    DEC07 15:24:58 0700
      PROCID= #C50F #10C6: MTCMAINP, DATA= 0001000000010000
      007E5D94=MSCCKSWM.BK01:
                              MSC_CLOCK_SWMAST_SANITY_P+#03D4
    007E4F8C=MSCCKSWM.BK01:MSC_CLOCK_SWMAST_OP+#020C
      006F52F4=MSDBUI.CS01:MS_INVOK+#0674
      0078AF98=MSCSTRI.BC03:MSC_CARD_S+#09F8
      0078C01C=MSCSTRI.BC03:MSC_EX_M+#015C
      0066A66C=MTCBASI1.CV01:EXECUTE_M+#082C
      0065F75C=MTCMAINP.BG01:MTCMAIN_PROCESS_+#02DC
      0065F458=MTCMAINP.BG01:MTCMAIN_PROCESS+#0058
      004C46A0=MODULES.FS09:INITIALIZEP+#0020
      004A2E60=PROCS.HK03:LIVEANDD+#0020

CSNNC09BS     SWER    DEC07 15:24:58 0600
      PROCID= #C50F #10C6: MTCMAINP, DATA= 0000000000000001
    007E5D3C=MSCCKSWM.BK01:
                               MSC_CLOCK_SWMAST_SANITY_P+#037C
    007E4F8C=MSCCKSWM.BK01:MSC_CLOCK_SWMAST_OP+#020C
      006F52F4=MSDBUI.CS01:MS_INVOK+#0674
      0078AF98=MSCSTRI.BC03:MSC_CARD_S+#09F8
      0078C01C=MSCSTRI.BC03:MSC_EX_M+#015C
      0066A66C=MTCBASI1.CV01:EXECUTE_M+#082C
      0065F75C=MTCMAINP.BG01:MTCMAIN_PROCESS_+#02DC
      0065F458=MTCMAINP.BG01:MTCMAIN_PROCESS+#0058
      004C46A0=MODULES.FS09:INITIALIZEP+#0020
      004A2E60=PROCS.HK03:LIVEANDD+#0020
```

155.9.2 CBM850 Billing Posttest

This testing will be performed immediately after the *norestartcutover* to make sure billing records are transferred to CBM850 from CCA as well as to downstream from CBM850.

Verify the billing on CBM850 for configured streams:
Make sure that the SBA application is in-service in CBM850 (cbmmtc appl).

Run the following command to verify the billing record collection in cbm850:
query
AMA:
PrimarySubStream: InSv
Number of Records in Open Files: 9800
ClosedNotSent Files Available: 0
Records within the ClosedNotSent files: 0
Date of Last File Sent:
Date and time unavailable.

OCC:
PrimarySubStream: InSv
Number of Records in Open Files: 106
ClosedNotSent Files Available: 0
Records within the ClosedNotSent files: 0
Date of Last File Sent:
Date and time unavailable.

Run the query command again, if there are calls processed on the core, the number of records will increase for the streams.
#query

AMA:
PrimarySubStream: InSv
Number of Records in Open Files: 23912
ClosedNotSent Files Available: 0
Records within the ClosedNotSent files: 0
Date of Last File Sent:
Date and time unavailable.

OCC:
PrimarySubStream: InSv
Number of Records in Open Files: 420
ClosedNotSent Files Available: 0
Records within the ClosedNotSent files: 0
Date of Last File Sent:
Date and time unavailable.

If, downstream is configured, verify that the billing files are transferred to the downstream as per the configured schedules.

155.9.3 Sending billing files to Downstream

Procedure to send the unsent billing files from SDM/CBM800/CBM850 to the downstream.

```
# closec ama
billmtc
filesys
sendfile ama
```

- Repeat the above steps for all the configured streams.
- Verify that the downstream is received the billing file.

155.9.4 SDM/CBM800 Cutover abort Billing test

This testing will be performed immediately after the fallback to make sure billing records are transferred to SDM/CBM800 from SN/SNSE CM as well as to downstream from SDM/CBM800.

Make sure that the SBA application is in-service in SDM/CBM800.

Run the following command to verify the billing record collection in SDM/CBM800:

```
# query
AMA:
    PrimarySubStream:                   InSv
    Number of Records in Open Files:    2058
    ClosedNotSent Files Available:      0
    Records within the ClosedNotSent files: 0
    Date of Last File Sent:
        Fri Nov  4 10:27:11 2005

OCC:
    PrimarySubStream:                   InSv
    Number of Records in Open Files:    212
    ClosedNotSent Files Available:      0
    Records within the ClosedNotSent files: 0
    Date of Last File Sent:
        Fri Nov  4 10:28:42 2005
```

Run the query command again, if there are calls processed on the core, the number of records will increase for the streams.

```
#query

AMA:
    PrimarySubStream:                   InSv
    Number of Records in Open Files:    7154
    ClosedNotSent Files Available:      0
    Records within the ClosedNotSent files: 0
    Date of Last File Sent:
        Fri Nov  4 10:27:11 2005

OCC:
    PrimarySubStream:                   InSv
```

```
Number of Records in Open Files:        762
ClosedNotSent Files Available:          0
Records within the ClosedNotSent files: 0
Date of Last File Sent:
      Fri Nov  4 10:28:42 2005
```

If downstream is configured on the SDM/CBM800, verify that the billing files are transferred to downstream as per the schedules configured.

155.9.5 Activating the SBA Schedules on CBM850

Make sure that the SBA application is in-service in CBM850.

If there are any schedules configured for SBA, then follow the steps below.

Execute the following commands on CBM850 to activate the SBA schedules.

```
# billmtc
SCHEDULE
Change ama

File_Format_Type       : 'DNS'
Destination            : 'AMA1'
Protocol               : 'FTPW'
Primary_Destination    : '47.129.82.27'
Primary_Port           : '21'
Alternate_Destination  : '47.129.82.27'
Alternate_Port         : '21'
Start_Time             : '00:00'
Stop_Time              : '23:59'
Interval               : '120'
Remote_Storage_Directory: '/home/ksamy/CBMSBA'
Remote_Login           : 'ksamy'
Remote_Password        : '******'
Maximum_Retries        : '3'
Retry_Wait_Time        : '1'
File_Extension         : ''
Field_Separator        : '.'
Active                 : 'No'

Enter the field name to be changed. Stream, File_Format_Type and
Destination cannot be changed.

Enter 'All' to be prompted for all field names.
Press Enter to accept 'All'.
Enter Field_Name: Active

WARNING: Billing files associated with this tuple will not transfer
downstream when Active is set to No.
```

Valid active values are {'No', 'n', 'Yes', 'y'}.
Press Enter to accept 'No'.
Enter Active: **Yes**

Stream : 'AMA'
File_Format_Type : 'DNS'
Destination : 'AMA1'
Protocol : 'FTPW'
Primary_Destination : '47.129.82.27'
Primary_Port : '21'
Alternate_Destination : '47.129.82.27'
Alternate_Port : '21'
Start_Time : '00:00'
Stop_Time : '23:59'
Interval : '120'
Remote_Storage_Directory: '/home/ksamy/CBMSBA'
Remote_Login : 'ksamy'
Remote_Password : '******'
Maximum_Retries : '3'
Retry_Wait_Time : '1'
File_Extension : ''
Field_Separator : '.'
Active : 'Yes'

Valid actions are {'Save', 'Edit', 'Abort'}.
Press Enter to accept 'Edit'.
Enter Action: **Save**

Schedule tuple changed.

Press Return to Continue.

Repeat the above steps for all the configured schedules.

Activating the RTB Schedules:

If RTB is configured on CBM850, follow the below steps to activate.

billmtc
SCHEDULE
RTB

bsy OCC DIRP OCCCLNT
rts OCC DIRP OCCCLNT
Query OCC

Stream : OCC
Destination list :

DIRP OCCCLNT **INSV**

Repeat the above steps for all the RTB configurations.

155.9.6 Checking the SBA Schedule status on CBM850

Make sure that the SBA application is in-service in CBM850.

If there are any schedules configured for SBA, then follow the steps below.

Run the following commands on CBM850 to get the status of each configured schedules on CBM850.

billmtc
SCHEDULE
list OCC

Stream : 'OCC'
File_Format_Type : 'DIRP'
Destination : 'OCC1'
Protocol : 'RFTPW'
Primary_Destination : '47.129.82.27'
Primary_Port : '21'
Alternate_Destination : '47.129.82.27'
Alternate_Port : '21'
Start_Time : '00:00'
Stop_Time : '23:59'
Interval : '5'
Remote_Storage_Directory: '/home/ksamy/CBMRTB'
Remote_Login : 'ksamy'
Remote_Password : '******'
Maximum_Retries : '3'
Retry_Wait_Time : '1'
File_Extension : ''
Field_Separator : '.'
Active : 'Yes'
Press Enter to continue ('Abort' quits)...

Make sure that the Active field is set to “Yes”.

Repeat the list command for all the configured streams and make sure that the Active field is set to “Yes” for all of them.

Checking the RTB status:

```
# billmtc
SCHEDULE
RTB
Query OCC

Stream : OCC
Destination list :
-------------------------------------------------
DIRP OCCCLNT                    INSV
```

Make sure that the RTB status is INSV.

Repeat the above steps for all the configured RTB tuples.

156: Functional Description (FN) A00012478

156.1 Feature name and Feature ID

A00012478 - Compact Call Agent: Geo Support for GigE

This feature supports GigE interface for sparing or synchronizing data between the two MCG905-270 CCAs for both Geo and non-Geo configurations.

156.2 Description

This feature enables synchronization of data between two Compact Call Agent (CCA) blades over a Gigabit Ethernet link. The current design uses Fiber Channel (FC) for keeping data synchronized. This feature will provide an additional option of synchronization over Gigabit Ethernet (GigE) depending on the customers' needs.

GigE is an ethernet technology that provides an alternative for high-speed data transmission (1 gigabit per second) to achieve memory synchronization between active and inactive CCA. The principal benefits of GigE are:

- It provides a low cost, reliable and fast data transmission solution. GigE is based on the Ethernet protocol and Ethernet standards are the most deployed network backbone solution.
- It is scalable and upgradable. It may be possible to upgrade data synchronization over GigE to 10 GigE in the future.

Other benefits include:

- A GigE link has a lower cost to provision and maintain than a Fiber Channel link for Geo applications. For customers who do not own optical transport between geo sites, GigE has a lower lease cost then Fiber Channel.
- It is expected that a GigE link for Geo applications will allow greater distances between sites to be supported.

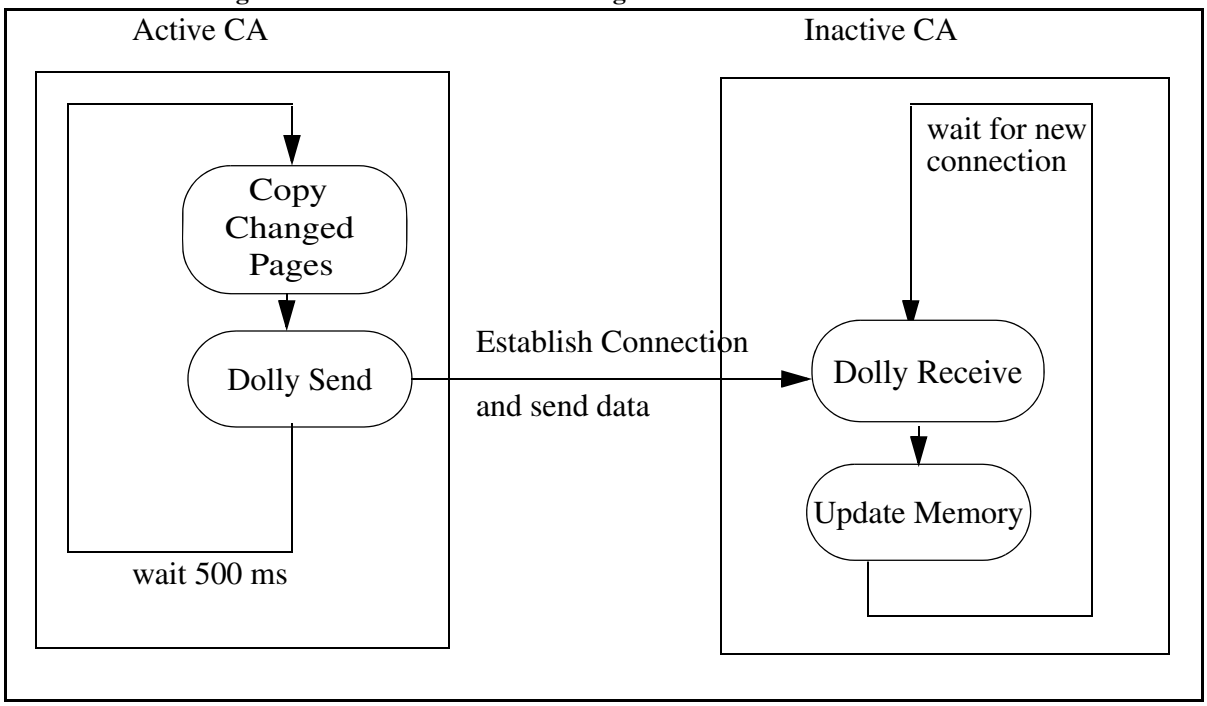
The desired behavior of this feature is to provide an ethernet transport option between two MCPN905-based CCA cards. The MCPN765-based CCA cards do not support the GigE ports and hence will continue to use Fiber Channel.

This feature will provide high synchronization bandwidth for the Dolly process. Dolly is a linux process running on both the active and inactive CCA. The instance of Dolly running on the active CCA is responsible for sending the "dirty" or "changed" memory pages to the inactive CCA. The instance of

Dolly running on the inactive CCA is responsible for receiving those changed pages and passing them to PEEL to update memory [Figure 1].

All changed pages are collected and copied into a buffer on the active CCA every 500 milliseconds. The Dolly process running on the active CCA will establish connection over the GigE link with the Dolly process running on the inactive CCA. Once the connection is established, data transmission will start. Any packet loss will be retransmitted to ensure that the inactive does not have a corrupt image due to loss of information. Upon completion of data transmission, the inactive CCA will copy the received data into memory and wait for the next new connection.

Figure 1 Functional Behavior Diagram



- This feature will provide an in-service method to change the FC connection to GigE (and vice-versa) for both Geo and non-Geo configurations with MCPN905-based CCA.
- Support to select either FC or GigE will be provided by the SAM21 Element Manager GUI. The work is documented in feat.A00012581.
  - — The EM GUI will have a separate Sparing Link Type tab to allow selection of either Fiber Channel or Gigabit Ethernet link for sparing or data synchronization between the CCA cards.

— Once the link selection has been made through the EM GUI, that information will be written in the *"extrainfo"* file on the configured Bootp server.

- The MCPN905-based software load will have support for both FC and GigE links between the CCA cards and it will be up to the customer to choose either of the two links (FC, only if they have FC PMC) but not both at the same time.
- This feature shall continue to support the FC links for MCPN765-based Compact Call Agent cards for both Geo and non-Geo configurations.
- For both Geo and non-Geo configurations, a new configuration path supported for upgrade will be

  — from MCPN905-based CCA with FiberChannel set up as synchronization link to MCPN905-based CCA with GigE set up as synchronization link; and vice-versa

156.2.1 Reference Configuration

The Gigabit Ethernet port of the PIM11 on the PrPMC815 card will be used for synchronizing data between the Call Agent cards.

The Fiber Channel connection will remain configurable as it is today, whenever the Fiber Channel hardware and driver are present.

156.2.1.1 Non-Geographic Survivability Mode Configuration

On a standard CS2000-Compact with MCPN905 (NTRX51HZ) CCA cards synchronization of data between the CCA units will be done over a direct and dedicated Gigabit Ethernet link (1000BaseT connection). This will be a point-to-point connection. An example is shown in Figure 2.

156.2.1.2 Geographic Survivability Mode Configuration

- On a Geographically Survivable CS2000-Compact with MCPN905 (NTRX51HZ) CCA cards synchronization of data between the two CCA units will be done via the CS-LAN router. An example is shown in Figure 2, using ERS 8600.
- Configuration of CCA interactions with the local CS-LAN router in each site will be configured on each CCA blade using the setgeoconfig script tool as it is done today. No changes are being made to that procedure.
- The internal architecture of the CS-LAN router should enable building secure VLANs. When port-based VLANs are configured, each VLAN is completely separated from another (broadcast domain). Its unique hardware architecture allows each packet to be analyzed independently of the preceding one. This mode guarantees complete traffic isolation by allowing discarding of untagged traffic on tagged port or tagged traffic on untagged ports. Even if a tagged port receives traffic with a VLAN Id

which identifies a VLAN from another customer configured on the switch, this traffic is completely discarded.

In other words - any traffic within this type of VLAN cannot exit the VLAN, nor can traffic from another VLAN be sent to a port within this VLAN when the IP default gateway is not set. This enables us to use an IP address for the sparing or synchronization of data on the MCPN905-based CCA GigE card without having to advertise it. Traffic will be confined between both CCA cards whether connected directly via a point-to-point fibre or via the CS-LAN router.

- The CS-LAN router must also support JUMBO frames. For example, the 8608SX(E), 8608GT(E), 8608GB(E), 10GE I/O modules and the 2 Gig ports of the 8632TXE board have the ability to forward 9600 (MTU) jumbo frames.
- The CS-LAN router may require an additional module (if it is not already equipped) with 1000BaseT GBIC support for Gigabit Ethernet transmission. For example, the ERS 8600 CS-LAN will require an additional 8608 module quipped with a 1000BaseT GBIC to support GigE. An example of the configuration procedure is shown in Figure 3.
- For configuring the GigE link on any CS-LAN router the engineering guidelines must be followed.
- Please refer to Appendix A for a step by step example in OTT3 about how to configure ERS 8600 to enable sparing over GigE in Geographic Survivable lab.

Figure 2 An example of data synchronization or sparing over GigE on MCPN905 CCA

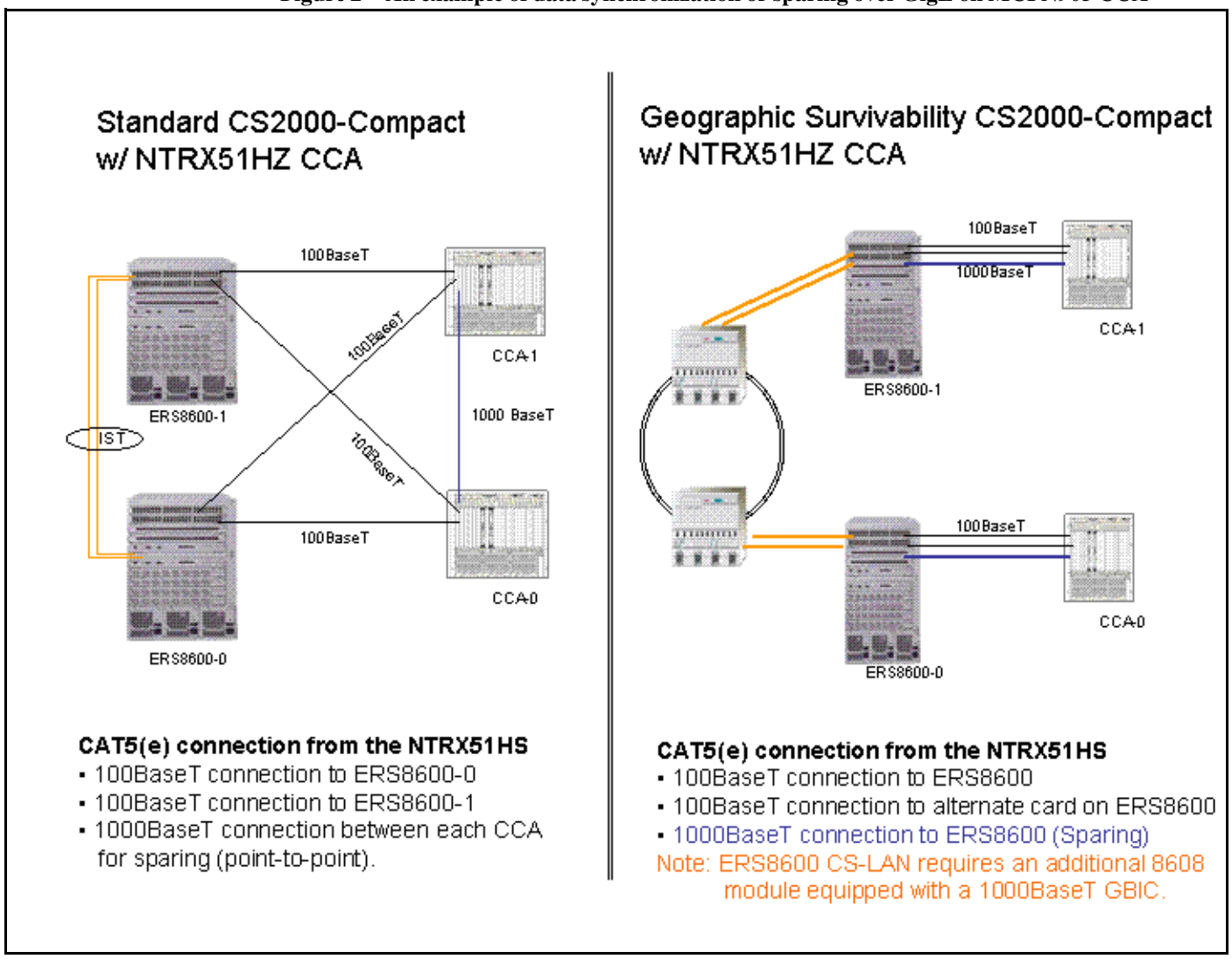


Figure 3 An Example of CSLAN configuration for sparing over GigE on MCPN905 CCA using ERS 8600 router

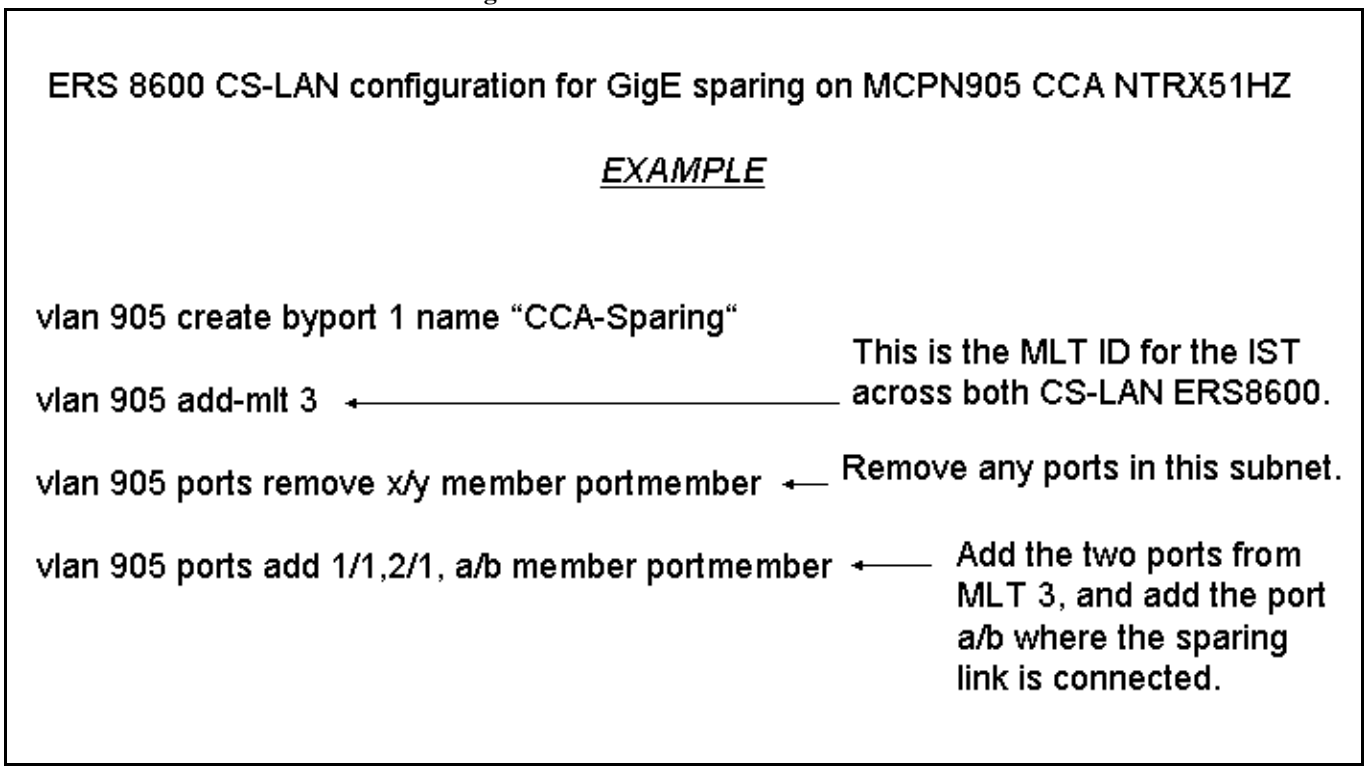
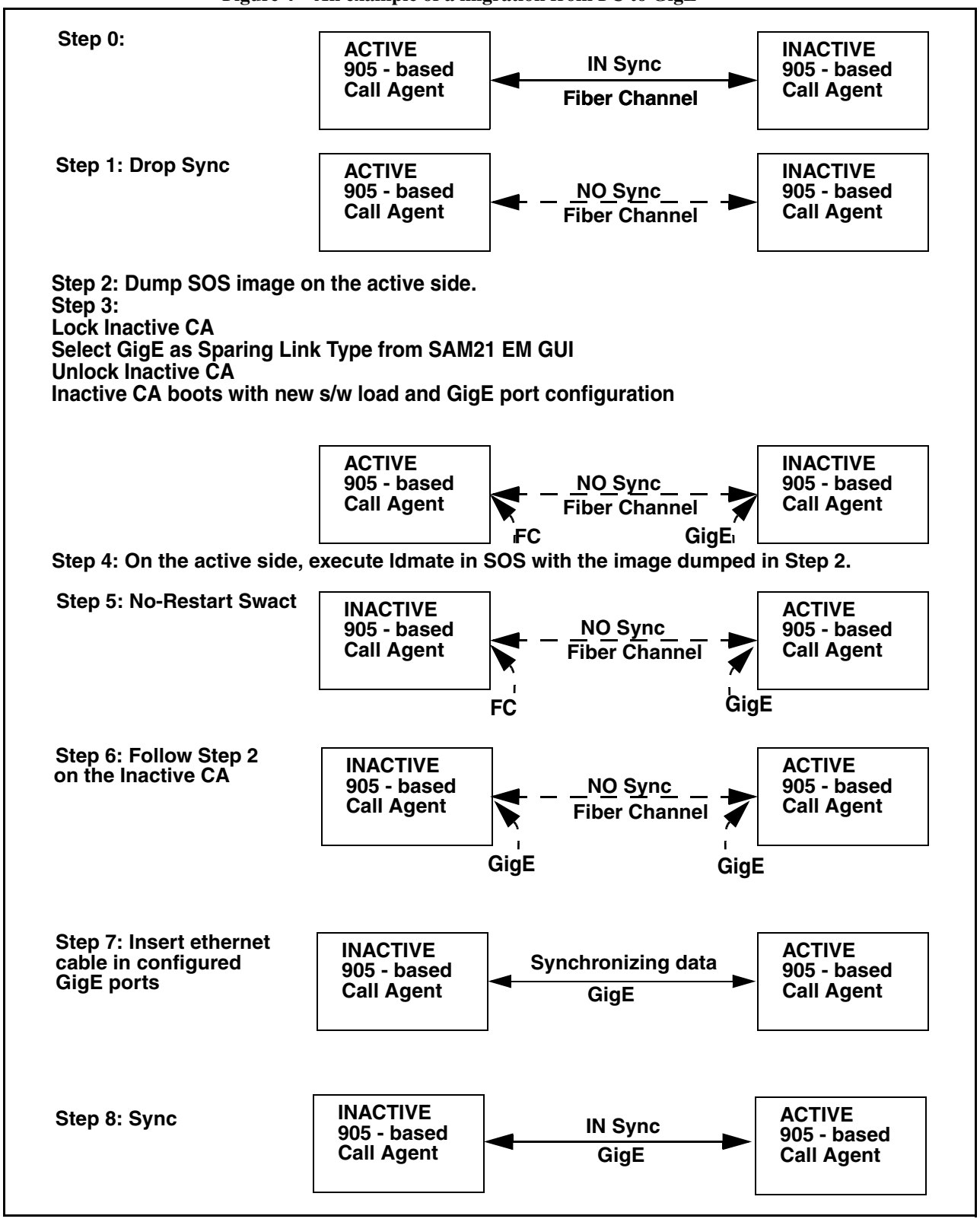


Figure 4 An example of a migration from FC to GigE

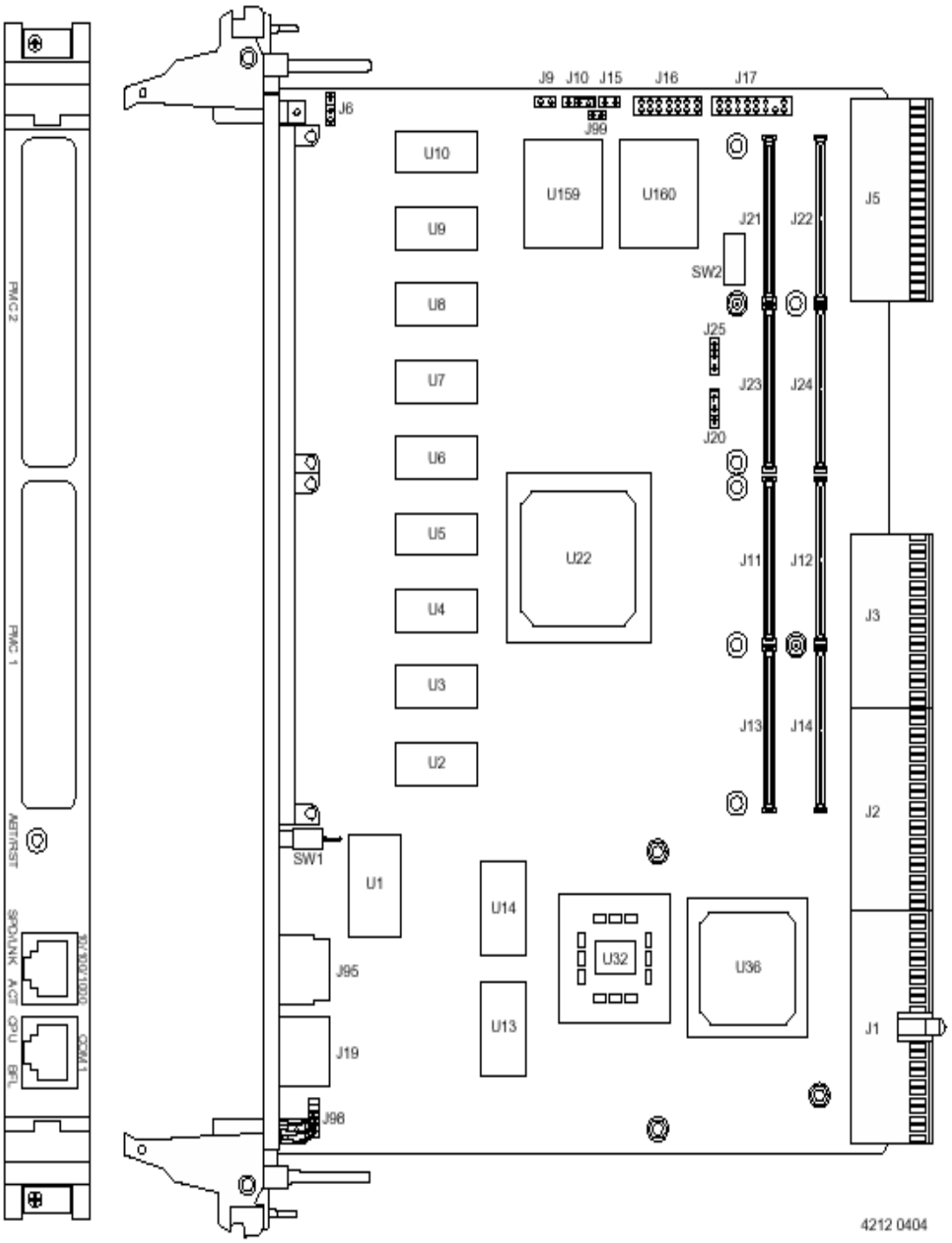


156.2.2 Upgrade scenario

The following upgrade scenarios are for both non-Geo and Geo survivable CS2000-CCA.

156.2.2.1 Hardware and Software upgrade

- In order to use Gigabit Ethernet for data synchronization or sparing, the two CCA blades must be MCPN905-based.
- The two MCPN905-based CCA blades must be equipped with a software load that supports data synchronization over Gigabit Ethernet link.
- The 1000BaseT cable must be inserted in the configured GigE ports on the PrPMC815 before attempting to bring the blades in synchronization.
- For geo configurations, a CS-LAN router is required that supports Gigabit Ethernet.
- It requires specific hardware configuration in order to enable the GigE port on the PrPMC815. On the 905 itself, PMC1 is at the middle of the board (connectors J11 to J14). PMC2 at the top (connectors J21 to J24). On the transition module the PIM for PMC1 is in the middle of the transition module J11. PIM2 is at the top J24.
  For 3pc-905 blade, if both PrPMC815 and FC PMC are present, PrPMC815 must be installed in PMC2 which is at the top of the board and FC PMC must be installed in PMC1 which is in the middle of the board. The rear transition module should be aligned with the position of PrPMC815 so it must be installed in PIM2 which is at the top of the board. If only PrPMC815 is present, PrPMC815 and rear transition module must be installed at the same position as described above.



156.2.2.2 System Impact of Failure Scenarios

In case, there is a fault in the 1000BaseT cable, there will no sparing of data over GigE link. This can cause a potential outage since the switch will be in simplex.

156.2.2.3 Recovery Behavior

If there a problem in the upgrade scenario above, the upgrade can be aborted and the system reverted back to the original configuration.

For example, if a failure happens during an upgrade from a MCPN905-based CCA with synchronization over Fiber Channel to an MCPN905-based CCA with synchronization over GigE, the failure can be corrected by reverting back to using Fiber Channel for synchronization on the MCPN905-based CCA by selecting Fiber Channel as the Sparing Link Type from the SAM21 EM GUI, since the new software load will support FC as well.

156.3 Hardware Requirements or Dependencies

1. For both Geo and non-Geo configurations, a 1000BaseT Gigabit Ethernet cable is required.
2. For Geo-Survivable configurations, the CS-LAN router must be equipped to support Gigabit Ethernet transmissions. For example, the ERS8600 CS-LAN will require an additional 8608 module equipped with a 1000BaseT GBIC.

156.4 Software Requirements or Dependencies

1. SN09FF load (or higher) for Call Agent
2. SN09FF load (or higher) for SAM21 Element Manager GUI

156.5 Limitations and restrictions

- To minimize loss of calls during a migration from FC to GigE, a no-restart swact may be used only
  - — when the CPU utilization is less than 40% and the number of changed pages count is less than 2200,
  - — on the same CCA software load on both CCA blades.

The CPU Utilization can be seen from the tool CAPCI. The number of changed pages can be calculated by checking the SLUTIL field in CAPCI. SLUTIL represents the number of changed pages divided by the maximum sparing link (or synchronization) bandwidth. The maximum sparing link bandwidth is usually set to 6000 pages unless specified otherwise.

$$\text{SLUTIL} = \frac{\text{number of changed pages}}{6000} \times 100$$

156.6 Interactions

Feature A00012581 is directly related to this feature. The SAM21 EM GUI which provides the customer to input the Sparing Link Type is covered under feature A00012581.

156.7 Applicable customer facing sections

Fault Management

— Logs _X_

— Alarms _X_

Configurations

— Element Management _X_

—

156.8 Appendix A

ERS 8600 Configure Example in OTT3 to Enable Sparing Over GigE in Geographic Suvivable Lab

```
OTT3 CSLAN P8600-1-B0:5# config vlan 12

OTT3 CSLAN P8600-1-B0:5/config/vlan/12# info


Sub-Context: create fdb-entry fdb-filter fdb-static ip ports srcmac
static-mcast

mac

Current Context:


        Vlan 12 is not created


OTT3 CSLAN P8600-1-B0:5/config/vlan/12# create byport 1 name "CA_GigE"

OTT3 CSLAN P8600-1-B0:5/config/vlan/12# info


Sub-Context: create fdb-entry fdb-filter fdb-static ip ports srcmac
static-mcast

mac

Current Context:
```

```
                          action : N/A
                        add-mlt :
                     addDsapSsap :
                  removeDsapSsap : N/A
                         agetime : N/A
                          delete : N/A
                        qoslevel : 1
                            name : CA_GigE


OTT3 CSLAN P8600-1-B0:5/config/vlan/12# ports
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# info


Sub-Context:
Current Context:


                           add :
                      portmember -
                      activemember -
                      staticmember -
                     notallowtojoin -
                    remove : N/A


OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# config ethernet 4/1
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1# info


Sub-Context: eapol ip lacp limit-fdb-learning mroute-limit multimedia
pcap remot
e-mirroring smlt stg unknown-mac-discard vlacp
Current Context:
Port 4/1 :
                              lock : false
                     block-traffic : false
                              name :
                    auto-negotiate : false
                            duplex : full
```

```
                    enable-diffserv : false
                    access-diffserv : false
                          qos-level : 1
                            routing : enable
                 unknown-mac-discard : disable
                        high-secure : false
                    default-vlan-id : 0
              untag-port-default-vlan : disable
               tagged-frames-discard : disable
                    perform-tagging : disable
                     svlan-porttype : normal
          untagged-frames-discard : disable
                        loop-detect : disable     action port-down
                              state : up
                           linktrap : enable
                multicast rate-limit : disabled
                broadcast rate-limit : disabled
                               sffd : disabled
                           cp-limit : enabled multicast-limit 15000
broadcast-limit 10000


OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1# name "CA_Cu_GigE"


OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1# config vlan 12 ports

OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# add 4/1 member
portmember

OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# info


Sub-Context:

Current Context:


                           add :
                              portmember - 4/1
                            activemember - 4/1
                            staticmember -
```

```
                              notallowtojoin -
                             remove : N/A

OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# config ethernet 4/6
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/6# info

Sub-Context:
Current Context:
Port 4/6 :
                                  lock : false
                        block-traffic : false
                                  name :
                       auto-negotiate : false
                                duplex : full
                      enable-diffserv : false
                      access-diffserv : false
                            qos-level : 1
                              routing : enable
                  unknown-mac-discard : disable
                             high-secure : false
                      default-vlan-id : 12
              untag-port-default-vlan : disable
               tagged-frames-discard : disable
                      perform-tagging : disable
                       svlan-porttype : normal
           untagged-frames-discard : disable
                           loop-detect : disable     action port-down
                                state : up
                              linktrap : enable
                 multicast rate-limit : disabled
                 broadcast rate-limit : disabled

                                  sffd : disabled
                               cp-limit : enabled multicast-limit 15000
broadcast-limit 10000
```

```
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/6# name "CA_Sx_GigE"

OTT3 CSLAN P8600-0-B0:5/config/ethernet/4/6# auto-negotiate enable

OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/6# config vlan 12 ports

OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# add 4/6 member
portmember

OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# info


Sub-Context:

Current Context:


                          add :
                             portmember - 4/1,4/6
                           activemember - 4/1,4/6
                           staticmember -
                         notallowtojoin -
                       remove : N/A


OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# .

OTT3 CSLAN P8600-1-B0:5/config/vlan/12# ip

OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ip# rip

OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ip/rip# info


Sub-Context:

Current Context:


                           rip : disable
          advertise-when-down : disable
             auto-aggregation : disable
                         cost : 1
               default-listen : disable
               default-supply : disable
                     holddown : 120
                    in-policy : N/A
                   out-policy : N/A
```

```
                        timeout : 180
                triggered-update : disable
                         listen : enable
                   manualtrigger : N/A
                         poison : disable
                         supply : enable

OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ip/rip# .
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ip# ospf
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ip/ospf# info

Sub-Context:
Current Context:

           advertise-when-down : disable
                          ospf : disable
                interface-type : broadcast
                hello-interval : 10
                 dead-interval : 40
                 poll-interval : 120
                      priority : 1
                        metric : 0
           authentication-type : none
            authentication-key :
                          area : 0.0.0.0

OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ip/ospf# config ethernet 4/1 ip
rip

OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip/rip# info

Sub-Context:
Current Context:

Port 4/1 :
```

```
                        rip : disable
          advertise-when-down : disable
             auto-aggregation : disable
                        cost : 1
              default-listen : disable
              default-supply : disable
                    holddown : 120
                   in-policy : N/A
                  out-policy : N/A
                     timeout : 180
             triggered-update : disable
                      listen : enable
                manualtrigger : N/A
                      poison : disable
                      supply : enable

OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip/rip# .
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip# ospf
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip/ospf# info

Sub-Context:
Current Context:
Port 4/1 :
          advertise-when-down : disable
                        ospf : disable
              interface-type : broadcast
              hello-interval : 10
               dead-interval : 40
               poll-interval : 120
                    priority : 1
                      metric : 0
          authentication-type : none
           authentication-key :
                        area : 0.0.0.0
```

```
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip/ospf# .
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1# stg 1
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/stg/1# info

Sub-Context:
Current Context:

Port 4/1 :
            change-detection : enable
                   faststart : disable
                    pathcost : 100
                    priority : 128
                         stp : disable

OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/stg/1# .
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip# arp
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip/arp-response# info

Sub-Context:
Current Context:

Port 4/6 :
                arp-response : enable



OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip/arp-response# top
OTT3 CSLAN P8600-0-A0:5# config sys
OTT3 CSLAN P8600-0-A0:5/config/sys# set ?

Sub-Context: action eapol flags msg-control record-reservation snmp
ssh
Current Context:

    clock-sync-time <minutes>
```

```
    contact <contact>
    ecn-compatibility <enable|disable>
    global-filter <enable|disable>
    info
    location <location>
    mgmt-virtual-ip <ipaddr/mask>
    mroute-stream-limit <enable|disable>
    mtu <bytes>
    name <prompt>
    portlock <on|off>
    sendAuthenticationTrap <true|false>
    smlt-on-single-cp <enable|disable> [timer <value>]
    topology <on|off>
    udp-checksum <enable|disable>
    udpsrc-by-vip <enable|disable>
    vlan-bysrcmac <enable|disable>
    wsm-direct-mode <enable|disable>
OTT3 CSLAN P8600-0-A0:5/config/sys# set mtu ?
set MTU (with CRC) to one of three values: 1522, 1950 and 9600 bytes
Required parameters:
<bytes>          = MTU value {1522..9600}
Command syntax:
mtu <bytes>
OTT3 CSLAN P8600-0-A0:5/config/sys# set
OTT3 CSLAN P8600-0-A0:5/config/sys/set# mtu 9600
OTT3 CSLAN P8600-0-A0:5/config/sys/set# info

Sub-Context: action eapol flags msg-control record-reservation snmp
ssh
Current Context:

               mgmt-virtual-ip : 0.0.0.0/0.0.0.0
                  udp-checksum : enable
                    udp-source : disable
               clock-sync-time : 60
```

```
            mroute-stream-limit : disable
                        contact : support@nortelnetworks.com
                       location : 4655 Great America Parkway, Santa
Clara, CA 950
54
                           name : OTT3 CSLAN P8600-0-A0
                       portlock : off
        sendAuthenticationTrap : false
                       topology : on
                  globalFilter : enable
                  vlanBySrcMac : disable
             ecn-compatibility : enable
               wsm-direct-mode : disable
             smlt-on-single-cp : disable timer 3
                    System MTU : 9600


OTT3 CSLAN P8600-0-A0:5/config/sys/set# .
OTT3 CSLAN P8600-0-A0:5/config/sys# top
OTT3 CSLAN P8600-0-A0:5# save config
Save config to file /flash/config.cfg successful.
```

156.9 Customer documentation impacts

This feature affects some logs, alarms, and element management as follows:

1. For the custom log changes all the appearnces of "FC" are renamed to "SL", i.e.

   Dec 5 15:35:17 172.16.16.70 logman: CCA335 MAJOR FLT Link Connectivity ^M Unit Number : 1, ACTIVE ^M Description : Link0: SYSB, mateCon: BAD, netCon: BAD; Link0 Mode: FULL_DUPLEX; Link1: INSV, mateCon: OK, netCon: OK; Link1 Mode: FULL_DUPLEX; BLink: INSV, mateCon: OK; **SL**: INSV;

2. Same for the alarm changes, all the appearances of "FC" are renamed to "SL", i.e.

```
Alarm Severity Description
2 CAMtc LnkCon major Link0: INSV, mateCon: OK, netCon: OK;
3 Sys Link0 Mode: FULL_DUPLEX;
4 Con Link1: INSV, mateCon: OK, netCon: OK;
5 Appl Link1 Mode: FULL_DUPLEX;
6 BLink: SYSB, mateCon: BAD;
7 SL: SYSB;
```

3. In CCAMTC, the "FC" for the carrier sparing state is replaced by "SL", i.e.

```
CallAgent SYS CON APPL Unit: 1
C MisM NTP . simplx
M
CoreMtc Jam: Link0: Link1: BLnk: SL: Appl:
0 Quit Unit0 Inact no . Act . Inact . . nosync /waiting
2 CAMtc Unit1 Act no . Act . Inact . . nosync .
```

4. There is a new query util "QuerySL" in CCAMTC slot 16 all mtc levels to query the type is sparing link, i.e.

```
CallAgent SYS CON APPL Unit: 1
C MisM NTP . simplx
M
CoreMtc Jam: Link0: Link1: BLnk: SL: Appl:
0 Quit Unit0 Inact no . Act . Inact . . nosync /waiting
2 CAMtc Unit1 Act no . Act . Inact . . nosync .
3 Sys
4 Con
5 Appl
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16 QuerySL
17 Help
18 Refresh Sparing Link (SL) Type: Gigabit Ethernet
root
```

5. In SAM21 EM, there is a new tab window for 905 card for the customer to choose which sparing link to use, "Fiber Channel" or "Gigbit Ethernet".

157: Functional Description (FN) A00012506

157.1 Feature name and Feature ID

A00012506 - Border Control Point (BCP) Operational Measurement (OM) Enhancements

157.2 Overview

157.2.1 Operational Measurements

Operational measurements (OMs) provide statistical information on the server operations and performances. OMs are represented in terms of groups, which contain registers (counters and gauges) that provide performance-related data. The Management Module (SysMgr) scans OM Group registers at configured intervals. The OM information associated with a selected component is then viewable by administrators in the OM Browser at any selected point in time (corresponding to the launching of the OM Browser). There are two types of OMs: active and holding. Active OMs are displayed as they are reported by the server to the management server/management console. Holding OMs have already been archived to files on the server hosting the active Management Module. The OM scan cycle is configurable using the OAM configuration options available in the System Management Console. OM scan cycles are configured per Network Element (NE). The configured value can be changed via the “Configuration Parameters” (see Figure 1: NE Configuration Parameters), under the “Parm Group: OM” shown in Figure 2: OM Parm Group Configuration Parameters.

Figure 1: NE Configuration Parameters

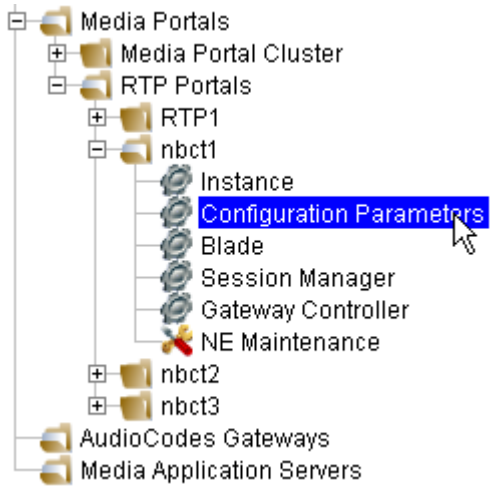
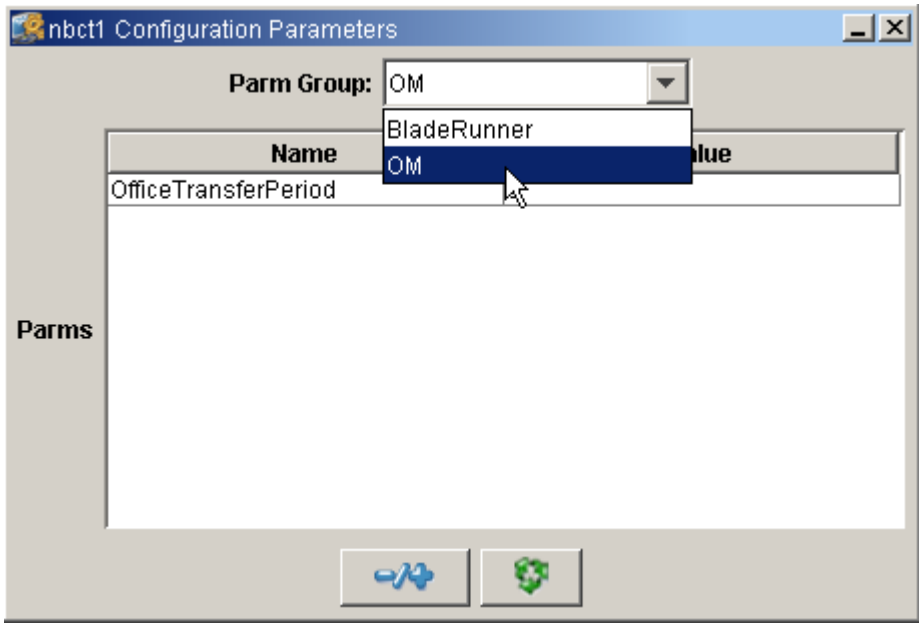
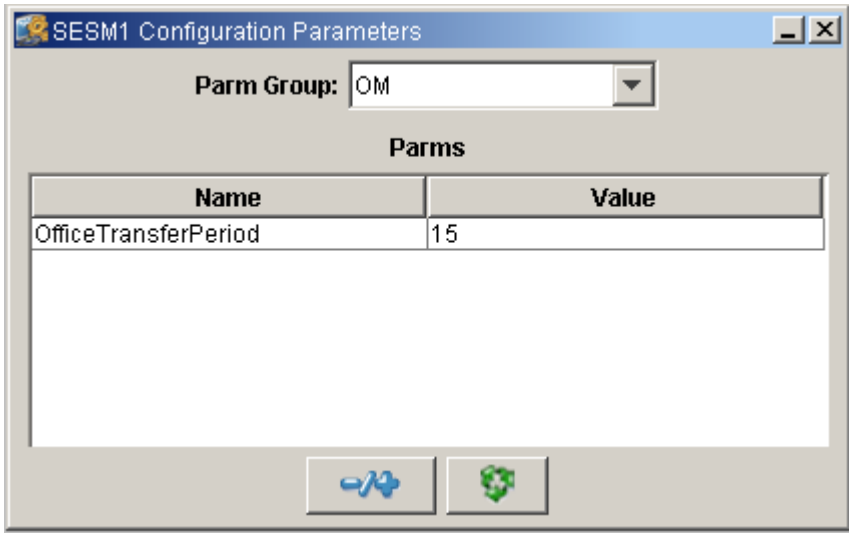


Figure 2: OM Parm Group Configuration Parameters



The parameter that controls how often OM's are collected is named "OfficeTransferPeriod" and the value is specified in minutes. Valid values for this parameter are 5, 15, 30 or 60 minutes.

Figure 3: OfficeTransferPeriodConfiguration Parameter



The OM Framework handles pushing OMs collected to IEMS.

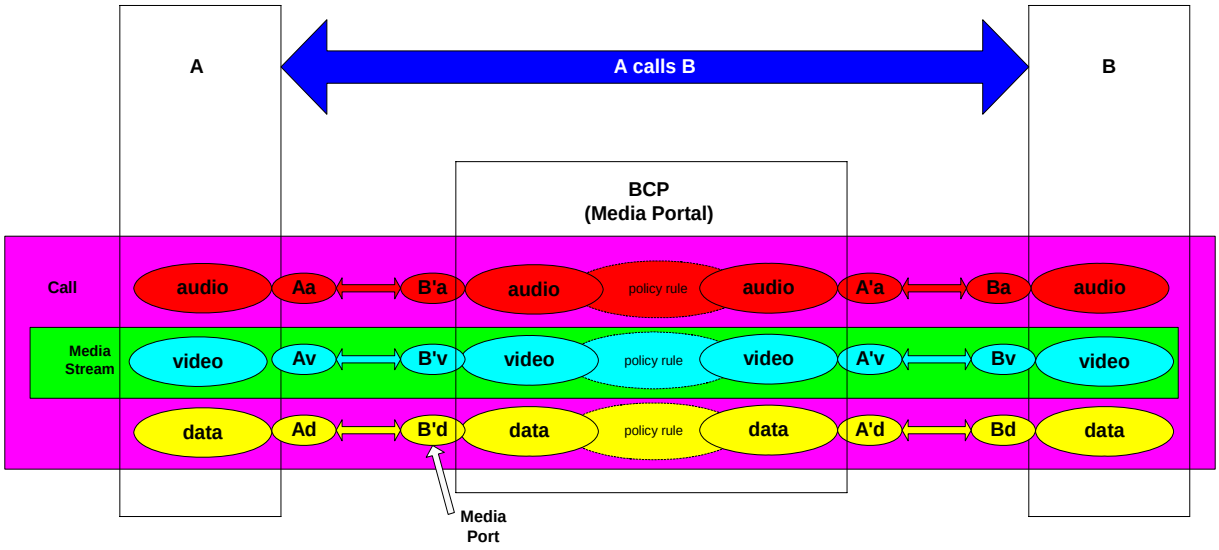
157.2.2 BCP

The BCP was previously referred to as the RTP Media Portal. Renaming existing references to RTP Media Portal is beyond the scope of this feature,

hence; the old terminology is used where needed to maintain consistency with what exists today.

BCP only understands ports and streams. Figure 4: BCP Media Streams shows an example of a basic “A calls B” scenario that involves three media streams. A media stream is successfully created once a policy rule connects two connections on the BCP. In the example shown below, the BCP knows that six ports have been allocated and that three policy rules have been created.

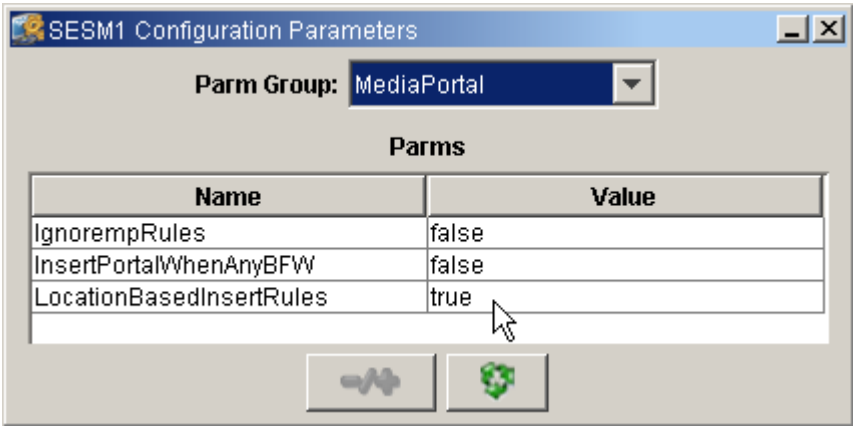
Figure 4: BCP Media Streams



157.2.2.1 BCP Insertion Configuration

The configuration parameters shown in Figure 5: SESM MediaPortal Configuration Parameters may need to be modified depending on network configuration for the Session Manager to insert a BCP for a given call.

Figure 5: SESM MediaPortal Configuration Parameters



IgnorempRules (default setting is false):
If set to true, the SESM would completely ignore BCP insertion rules, meaning the SESM would not insert any BCP to any call in the MCS system. This parameter should only be set to true when there is no BCPs configured in the MCS system. When this parameter is set to true, the settings for "InsertPortalWhenAnyBFW" and "LocationBasedInsertRules" are ignored.

InsertPortalWhenAnyBFW (default setting is false):
This parameter is only used when "LocationBasedInsertRules" is set to false. If "LocationBasedInsertRules" is not enabled, the SESM would use the non-"LocationBasedInsertRules" which is the default setting of the SESM BCP insertion rule. If non-"LocationBasedInsertRules" is used, by default, the SESM does not insert a BCP to a call unless one of the following criteria is met:

- If either or both of originating and terminating clients' domain configurations on the PROV have "AlwaysUseMediaPortal" set to true with this call.
- If either or both of the origination and terminating clients are behind the firewall or NAT (BFW). Basically, with the legacy insertion rule, if there is any BFW client in the call, a BCP should be inserted. However, due to the consideration of the effective usage of BCP resources, it is assumed that if both clients are BFW and in the same domain, most likely they are behind the same firewall or NAT, they should be able to communicate with each other without having to consume any BCP resources. Therefore, in this case, a BCP is not inserted unless the "InsertPortalWhenAnyBFW" is set to true to override the assumption.
- If the call is traversed through two interfaces (public/private), a BCP is inserted.
- If the call is originated from or terminated to a device which is unable to handle media changes, a BCP is inserted.
- If privacy is required for this call, a BCP is inserted.

LocationBasedInsertRules (default setting is false):
This is the enhanced BCP insertion rule that is based on the location infrastructure of the virtual network topology. If this parameter is set to true, the SESM would ignore the legacy BCP insertion rules (e.g. firewall clients, InsertPortalWhenAnyBFW, AlwaysUseMediaPortal domain, etc). By default, the SESM inserts a BCP to every call unless there is a Routability Group provisioned via the Provisioning Module for the call with the originating and terminating clients' location to suppress BCP insertion. Note that even though the originating and terminating clients are at the same location, a BCP is still inserted to the call if no Routability Group is configured with the location. When this parameter is set to true, the setting of "InsertPortalWhenAnyBFW" is ignored.

157.3 Description

This activity provides operational measurement enhancements for Border Control Point (BCP) usage. These enhancements are intended to provide some degree of parity between the GWC and the SIP Session Manager view of BCP performance measurements. Refer to Table 1: Session Manager vs GWC OMs for details on where the two diverge. This activity requests that additional Performance Measurements related to the BCP usage be generated on:

- Each controlling Session Manager
- Each Border Control Point

Table 1: Session Manager vs GWC OMs

OM	Session Manager	GWC
sesmSuccessCalls (GWC equivalent: “GWC successful calls” 5/10)	1 call = many BCPs Media streams for a single call may be distributed over multiple BCPs (e.g. audio + video + data).	1 call = 1 BCP Media streams for a single call are co-located on a single BCP.
sesmFailedCalls (GWC equivalent: “GWC failed calls” 5/10)	1 call = many BCPs Media stream for a single call may be distributed over multiple BCPs (e.g. audio + video + data) For example: a multimedia call (audio + video + data) would fail if any of the 3 policy rules on any of the BCPs suffered a failure.	1 call = 1 BCP Media streams for a single call are co-located on a single BCP.
mediaPortalCount (GWC equivalent: “Number of provisioned Media Proxies”)	The number of BCPs configured in the Management Console to support this Session Manager	The number of BCPs provisioned to support this GWC.
sesmSuccessStreams (GWC equivalent: “Media Proxy successful calls” 5/10)	(per-Stream) The number of stream setup requests (policy rules) that were successfully processed by this BCP.	(per-Call) The number of calls successfully setup by this BCP.
sesmFailedStreams (GWC equivalent: “Media Proxy failed calls” 5/10)	(per-Stream) The number of stream setup requests (policy rules) that were not successfully processed by this BCP.	(per-Call) The number of calls that failed to be setup by this BCP.

157.3.1 Session Manager OMs

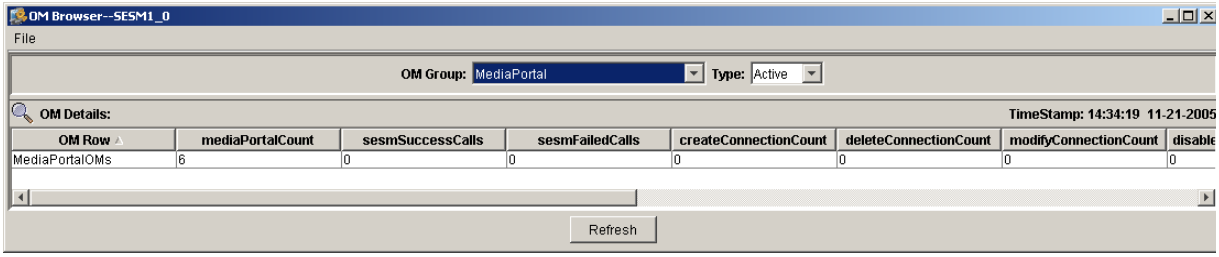
157.3.1.1 Media Portal

There are three new OM Registers added to the OM Group “MediaPortal” defined in Table 2: OM Group Media Portal - New OM Registers. Figure 6: Example GUI snapshot of MediaPortal OM Group shows the new OM Registers in the OM Browser GUI.

Table 2: OM Group Media Portal - New OM Registers

Register Name	Type	Description
sesmSuccessCalls	Counter	The number of calls that were successfully setup using any available BCP on this Session Manager in the last collection period.
sesmFailedCalls	Counter	The number of failed attempts to setup a call on any available BCP on this Session Manager in the last collection period.
mediaPortalCount	Usage	The number of BCPs configured to support this Session Manager from the Management Console. This counter will be updated when BCPs are added or removed via the Management Console.

Figure 6: Example GUI snapshot of MediaPortal OM Group



157.3.1.2 Media Portal Instances

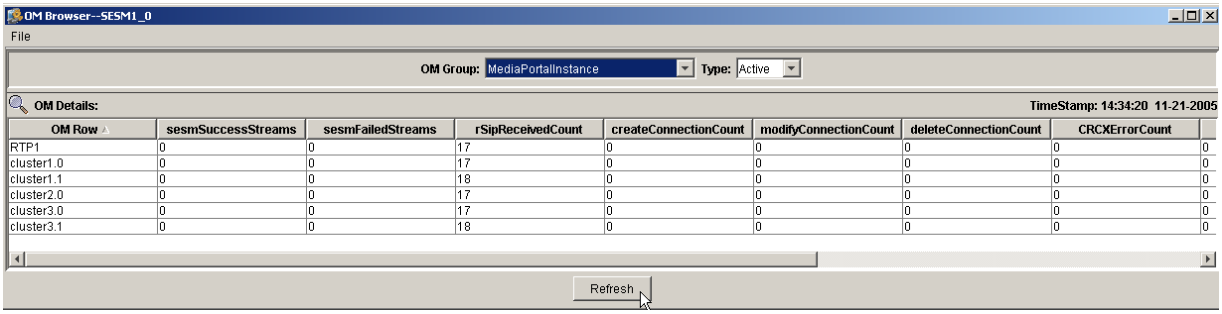
For OM Registers that are per-BCP, a new OM Group (“MediaPortalInstance”) is introduced. The OM Registers defined for this OM Group are described in Table 3: OM Group Media Portal Instance - New OM Registers. For each BCP configured to support this Session Manager, an OM Row is created. For CPX8216-T, the OM Row name is the NE-name. For BladeCenter-T, the OM Row name will be a label of the following form: <MediaPortalClusterName>.<ServiceID> (e.g. “MCP1.0”, “MCP1.7”, …). An example using BladeCenter-T is shown in Figure 7: Example GUI snapshot of MediaPortalInstance OM Group. The OM Row for a BCP is not

added to the OM Group until the BCP registers with the Session Manager (sends a RSIP message). If a BCPs' configuration is removed via the Management Console, its operational measurements for the current OTP are lost. The OM Row is not removed when the BCP deregisters with the Session Manager.

Table 3: OM Group Media Portal Instance - New OM Registers

Register Name	Type	Description
sesmSuccessStreams	Counter	The number of stream setups that were successfully processed by this media portal.
sesmFailedStreams	Counter	The number of stream setups that were not successfully processed by this media portal.

Figure 7: Example GUI snapshot of MediaPortalInstance OM Group

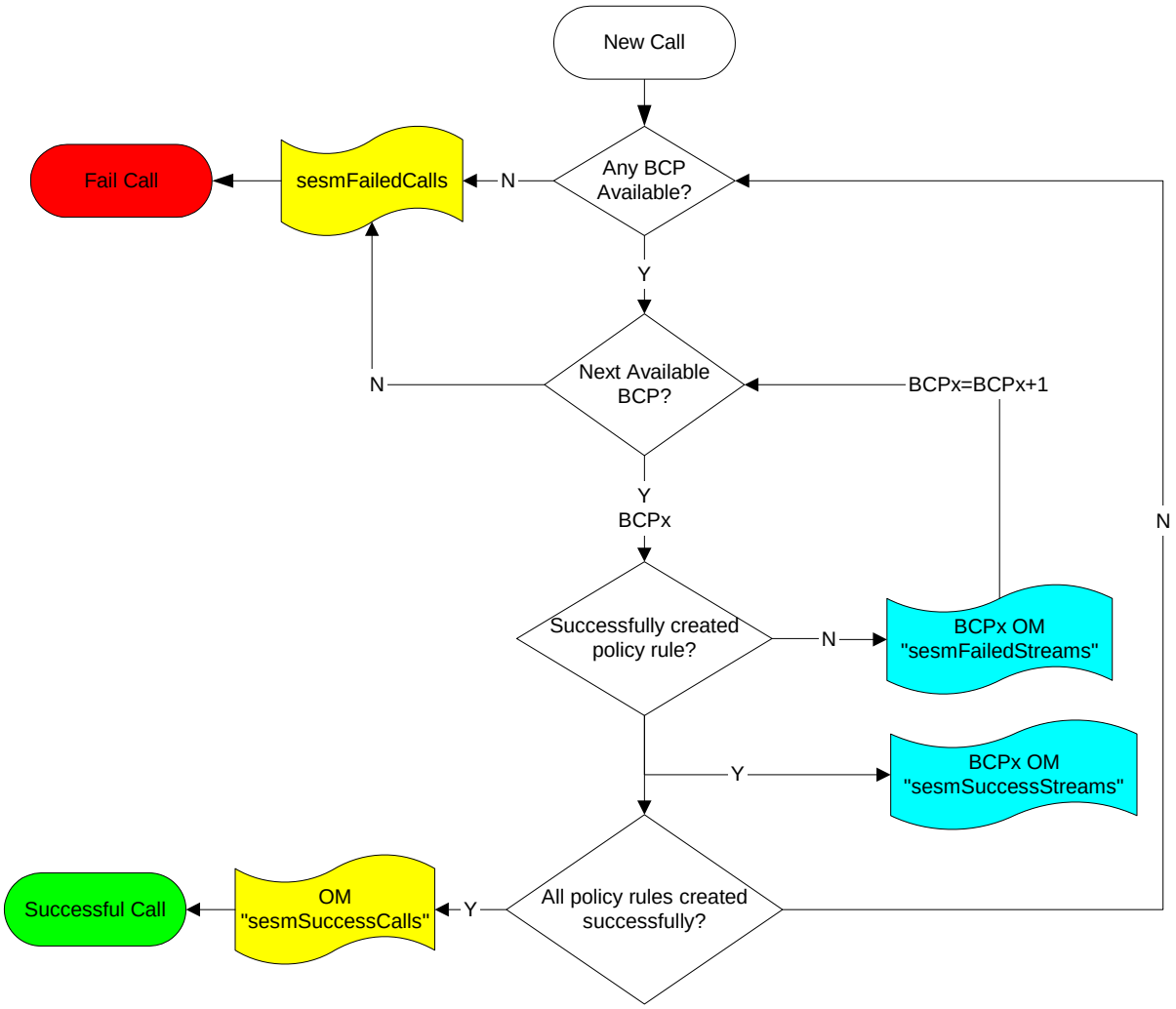


157.3.1.3 Session Manager Call Processing

The following diagram shows the flow for pegging the requested call related OMs on the Session Manager and the requested per-BCP OMs for that Session Manager. The new OMs are:

- Session Manager failed calls (sesmFailedCalls)
- Session Manager successful calls (sesmSuccessCalls)
- BCP failed streams (sesmFailedStreams)
- BCP successful streams (sesmSuccessStreams)

Figure 8: Session Manager "Call" OM Generation Logic



157.3.1.4 Session Manager Failed Calls

The Session Manager Failed Calls OM (“sesmFailedCalls”) represents the number of failed attempts to setup a call on any available BCPs on this Session Server in the last collection period. Unlike the GWC, media streams for a single call can be distributed over multiple BCPs. As Figure 8: Session Manager "Call" OM Generation Logic8 shows, for each new call, if a BCP is required for the call, the Session Manager will check to see if there are any BCPs available (registered with this Session Manager). If not, then the “sesmFailedCalls” OM Register is pegged. If there is a BCP available, the Session Manager will then attempt to create a policy rule for each media request for the call (e.g. audio, video, data). If there is a failure on one BCP, the Session Manager will attempt to use the next available BCP. If the Session Manager exhausts its pool of available BCPs before creating all the policy rules needed for the call, then the “sesmFailedCalls” OM Register is pegged.

157.3.1.5 Session Manager Successful Calls

The Session Manager Successful Calls OM (“sesmSuccessCalls”) represents the number of calls that were successfully setup using any available BCPs on this Session Manager in the last collection period. For a single call, unlike the GWC, media streams can be distributed over multiple BCPs. Figure 8: Session Manager "Call" OM Generation Logic illustrates the logic used in pegging this OM Register. This OM Register is incremented only if the Session Manager successfully creates a policy rule for each media. Note that it is possible for there to be a failure to create a policy rule for a media stream; however, the Session Manager will attempt to create it on the next available BCP (if not already exhausted its pool of BCPs).

157.3.1.6 BCP Failed Streams

The BCP Failed Streams OM (“sesmFailedStreams”) represents the number of stream setup requests that were not successfully processed per BCP. Unlike the GWC, the BCP does not have a notion of a call, but of ports and streams as shown in Figure 4: BCP Media Streams. As the figure shows, there are six ports allocated to the call for three media streams. A failure to allocate a port on the BCP or a failure to join the two ports via a policy rule in order to establish a media stream increments this OM register by one. This OM register is pegged per media stream and not per call as illustrated in Figure 8: Session Manager "Call" OM Generation Logic.

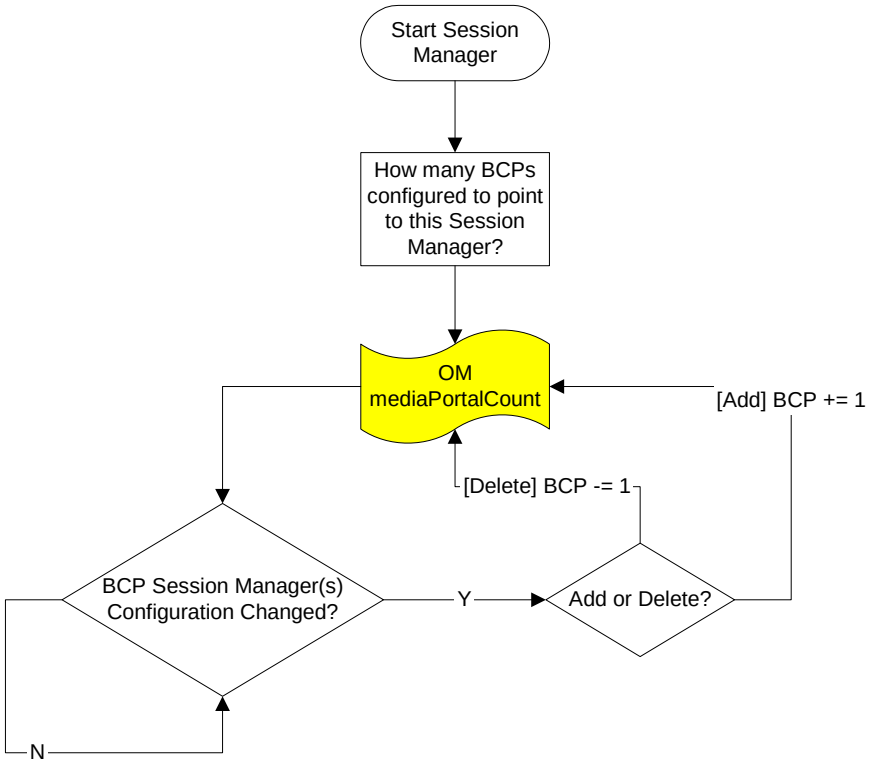
157.3.1.7 BCP Successful Streams

The BCP Successful Streams OM (“sesmSuccessStreams”) represents the number of media stream setup requests that were successfully processed per BCP. A media stream is considered successfully setup when the BCP establishes a logical connection via a policy rule between the two endpoints at which point the BCP Successful Streams is incremented by one. This OM register is pegged per media stream and not per call as illustrated in Figure 8: Session Manager "Call" OM Generation Logic.

157.3.2 Session Manager Configured BCPs

The following diagram shows the flow for pegging the mediaPortalCount OM Register on the Session Manager indicating the number of configured BCPs for this instance of the Session Manager. This register is only updated when a BCP configuration is either added or removed via the Management Console. If no BCP configurations exist, this register value is set to zero. A Session Manager only counts the BCPs that are associated with it via the “Session Manager(s)” data in the BCP configuration from the Management Console.

Figure 9: Session Server Configured BCPs OM Generation Logic



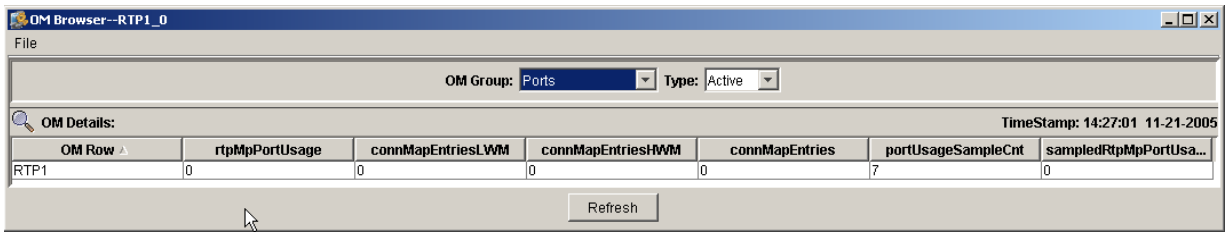
157.3.3 BCP OMs

Due to the large number of registers already existing in the MPCP OM Group, a new OM Group, named “Ports” has been created. There are four new OM Registers added to the OM Group “Ports” defined inTable 4: OM Group Ports - New OM Registers . Figure 6 shows the new OM Registers in the OM Browser GUI. The pre-existing OM Registers “rtpMpPortUsage” and “connMapEntries” has been moved out of the MPCP OM Group to the new Ports OM Group.

Table 4: OM Group Ports - New OM Registers

Register Name	Type	Description
sampledRtpMpPortUsage	Usage	Provides the summing of the in use ports every 100 seconds.
portUsageSampleCnt	Counter	The number of 100 second samples taken during this collection interval contributing to the averaged report.
connMapEntriesHWM	Usage	Highest number of simultaneous ports detected to be in use during this collection interval.
connMapEntriesLWM	Usage	Lowest number of simultaneous ports detected to be in use during this collection interval.

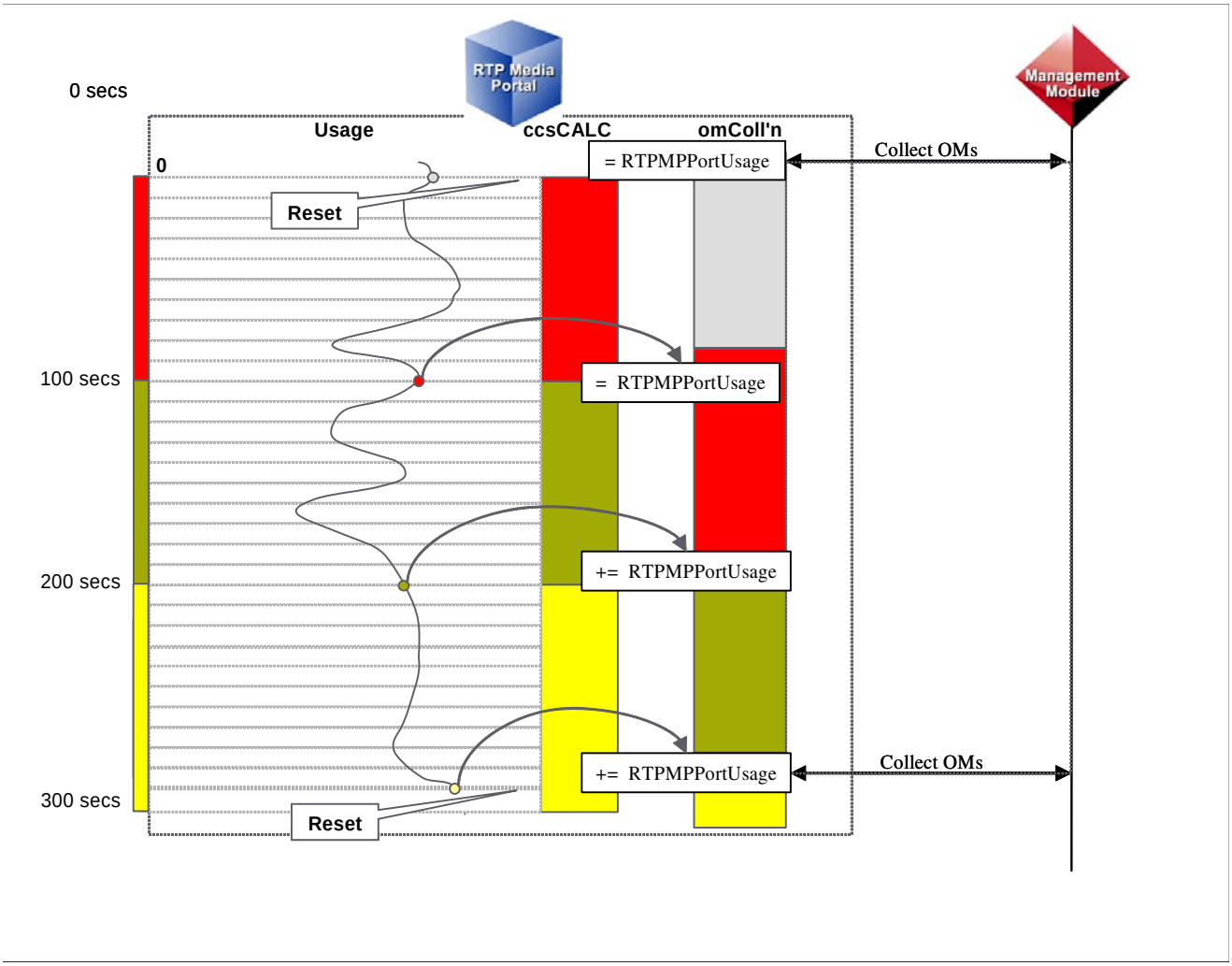
Figure 6:Example GUI snapshot of Ports OM Group



157.3.3.1 BCP Usage OM

The figure below illustrates the new sampledRtpMpPortUsage OM. This OM provides the summing of the in use ports every 100 seconds that gives a view of the CCS (hundred call seconds) of traffic. For example, in a five minute period, the BCP ports will be scanned three times (300 seconds/100 second scan). Each time there is a scan (every 100 seconds), and a port is in use, the count for that port is incremented. So for a five minute period, if a port is in use each time the scan occurs then a 3 is reported in the measurement. This measurement can then be plugged into traffic tables, like Erlang B, to compute the number of ports required for a given blocking probability. The number of 100 second reports sampled during the collection cycle will also be reported.

Figure 7 BCP: New "RTPMPPortUsage" OM



157.3.3.2 Port Usage Sample Count OM

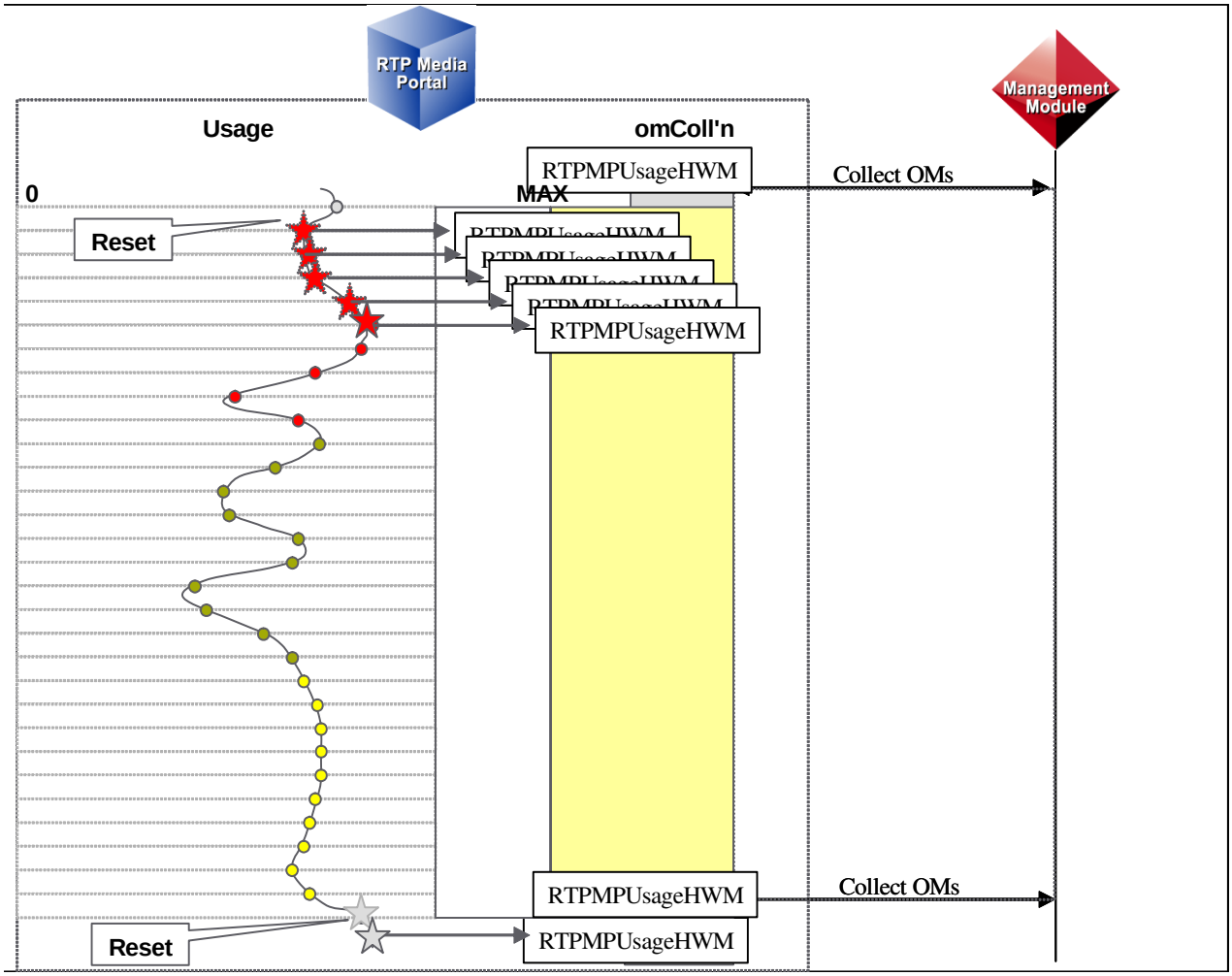
The Port Usage Sample Count OM (“portUsageSampleCnt”) represents the number of 100 second port usage samples taken during a collection cycle. For example, for a five minute collection cycle, the value should be 3. This value can be used to determine if the “sampledRtpMpPortUsage” OM Register should be thrown out or not when used with traffic tables. There is the possibility of a Java Garage Collection delaying a 100 second report.

157.3.3.3 BCP Usage High Water Mark OM

The figure below illustrates the new connMapEntriesHWM OM. This OM provides a high water mark of the ports in use on the BCP for a collection cycle. Each time a port is allocated, the number of ports in use is compared to the current value of the connMapEntriesHWM OM. If the current number of ports in use exceeds the value stored in the OM Register, then the OM

Register’s value is set to the current usage value. At the beginning of each collection cycle, the HWM register is reset to the current usage level.

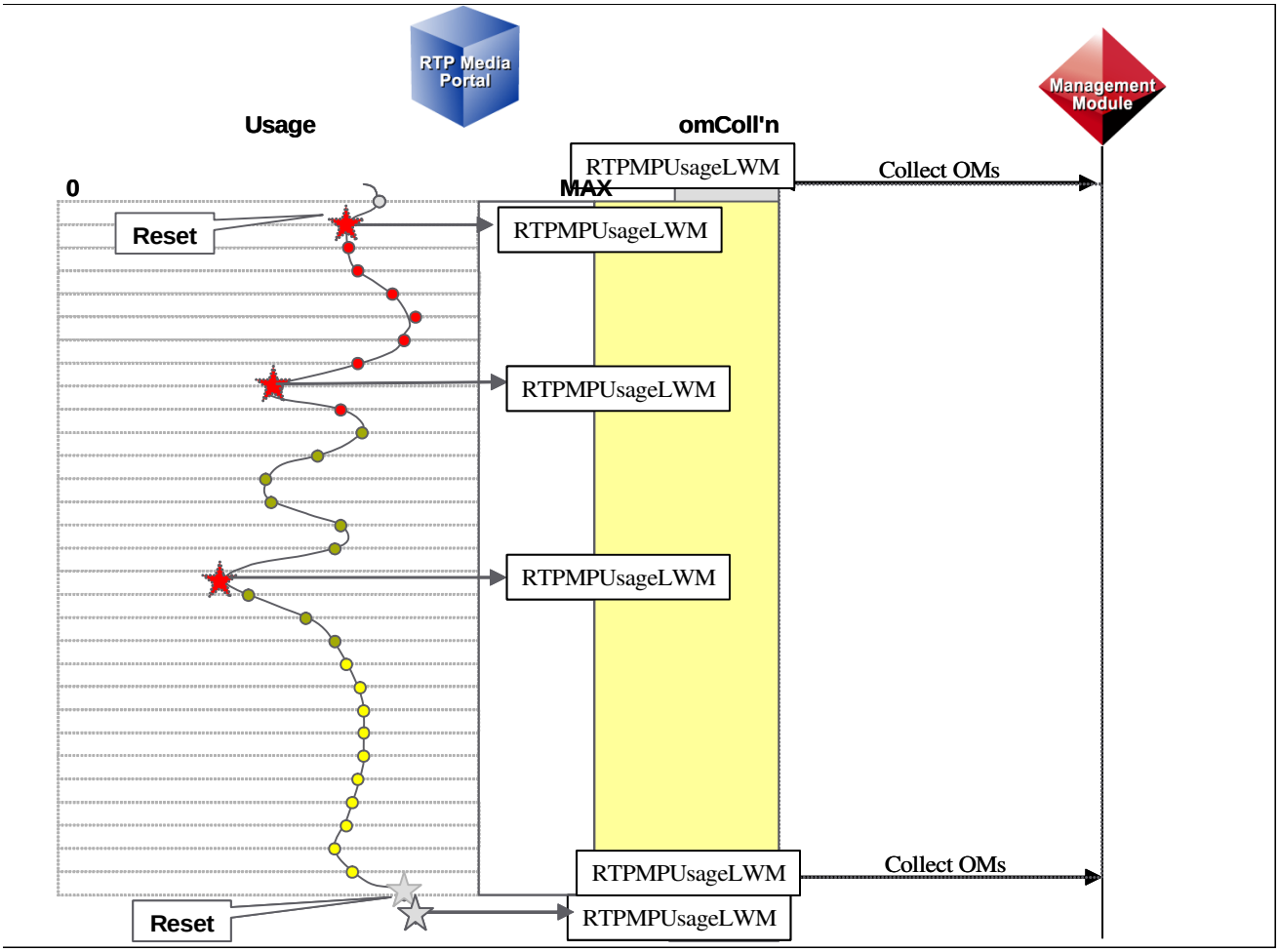
Figure 8: BCP: New "RTPMPUsageHWM" OM



157.3.3.4 BCP Usage Low Water Mark OM

The figure below illustrates the new connMapEntriesLWM OM. This OM provides a low water mark of the ports in use on the BCP for a collection cycle. At the beginning of each collection cycle, the LWM register is reset to the current usage level.

Figure 8: BCP: New "RTPMPUsageLWM" OM



157.4 Hardware Requirements or Dependencies

None

157.5 Software Requirements or Dependencies

None

157.6 Limitations and restrictions

If a BCPs configuration is removed via the Management Console, its operational measurements for the current OTP are lost.

The accuracy of reporting port usage every 100 seconds is at the mercy of the Java Garbage Collector.

157.7 Interactions

This feature will have negligible capacity and real time impact.

157.8 Glossary

Term	Description
Call	A communication context that involves two endpoints that are communicating using one or more forms of media.
Media Port	An entity repressenting one of the endpoints for a media stream..
Media Stream	A single media channel for conveyance of media (audio, video or data) between endpoints
OTP	Office Transfer Period.
Policy Rule	Refers to the internal connection between two proper connections on the BCP.

158: Functional Description (FN) A00012526

158.1 Feature name and Feature ID

A00012526 - TDM Call Recording Feature

158.2 Description

This feature provides trunk information in the ICM (Intelligent Call Management) protocol to facilitate call recording functionality in a TDM environment. It depends on feature A00012527: 'Provisioning of CS2K trunks on GW and Carrier basis' to access the trunk information.

158.2.1 Background

ICM is a SCAI (Switch-Computer Applications Interface) protocol.

SCAI specifies an architecture and an Open Systems Interconnection (OSI) application layer protocol suite for peer-to-peer data communication between host computer applications and switch applications, thereby enabling the functional integration of computer systems and telephony switching systems.[1]

Remote Operation Service Element (ROSE) is used to support the interactive communication between the switch and host application.

Currently, ICM services exist for the use of four types of customers.

- Automatic Call Distribution (ACD) customers
- Meridian Digital Centrex (MDC) customers
- Residential (RES) customers
- SL-100 Private Branch Exchange (PBX) customers

ICM uses the following Operation Classes.

- Class 1: Synchronous, reporting success or failure
- Class 2: Asynchronous, reporting success or failure
- Class 5: Asynchronous, outcome not reported

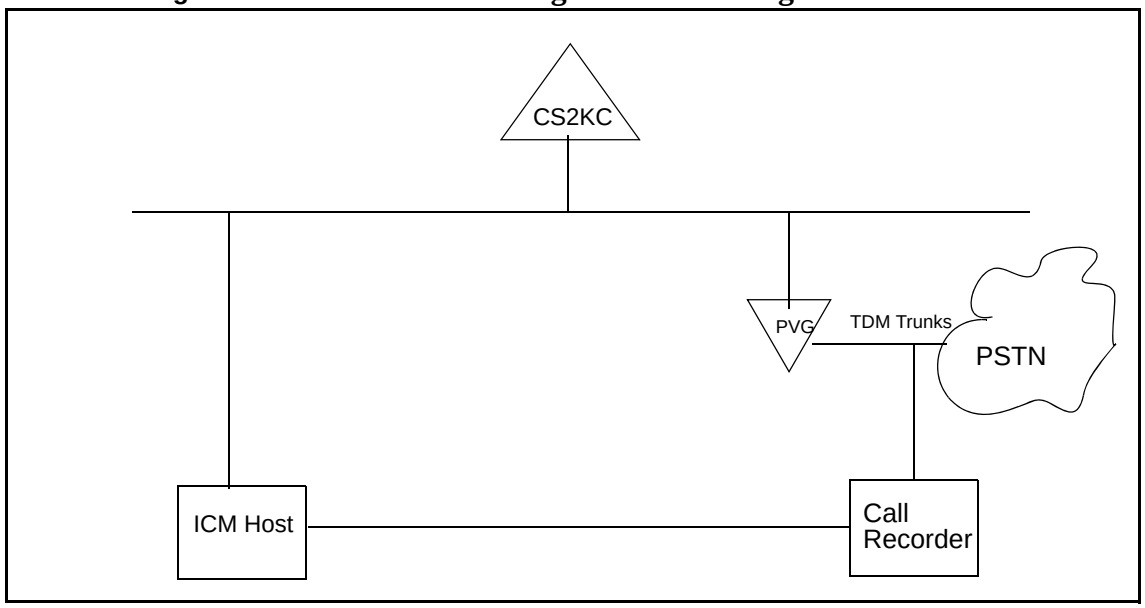
158.2.2 Functionality Overview

Call recording functionality for TDM trunks utilizes the ICM protocol and a call recording device which taps into the TDM trunk involved in the call. A high-level diagram is shown below.

[1]Taken from the ANSI SCAI Standard document: ANSI TI.626-1993

The CS2KC switch sends the ICM messages to the ICM Host (which is a Genesys CTI server for this case). The ICM Host will then relay required information to the Call Recorder, which will then start recording on the trunk.

Figure 1 TDM Call Recording Functional Diagram for CS2KC



To properly record calls and retrieve recorded calls, the system needs the following trunk information:

- PM Type
- PM Number
- Carrier Number
- Channel Number

This feature will provide this additional trunk information in the following ICM messages:

- dv_call_offered_U
- dv_call_queued_U

158.2.3 Feature Overview

To provide the trunk information in ICM messages, the following is required:

- SOC to control functionality
- SCAISSRV Table Control to subscribe for the trunk information
- ICM Enhancements including new SCAI protocol version SCAI19
- Call Processing and Error Handling
- New Log SCAI600

158.2.4 SOC

This feature will have a state controlled SOC, ICM00085.

— With the SOC turned on, the switch will attempt to send trunk information in the appropriate ICM messages. Reference the call processing section of this document for a complete description of the requirements to send trunk information.

— With the SOC turned off, the switch does not attempt to send trunk information in ICM.

Please reference the CN section of this document for more information.

158.2.5 Table SCAISSRV Subscription Changes

The following changes in the table SCAISSRV are required to provide subscription to the changed SCAI/ICM messages.

158.2.5.1 Subscription for ACD

A new default tuple ACDEVENT19$ will be created with the new parameter TRNKINFO in functions CALLQUED and CALLOFFR.

158.2.5.2 Subscription for Residential and Centrex lines

- A new default tuple RESEVENT19$ will be created with the new parameter TRNKINFO in function CALLOFFR.
- A new default tuple CTXEVENT19$ will be created with the new parameter TRNKINFO in function CALLOFFR.

Please reference the CN section of this document for more information on table SCAISSRV.

158.2.6 ICM Message Enhancements

This feature introduces a new parameter, **TRNKINFO,** in the following ICM call related messages.

- DV_Call_Queued_U
- DV_Call_Offered_U

The ASN.1 notations for the these messages are shown in the Appendix of this document.

The new parameter, TRNKINFO, is added with the following information:

- PM Type: string {PVG, GW}
- PM Number: integer {0-1023}
- Carrier Number: integer {1-168}
- Channel Number: integer {1-31}

The changes are included in a new SCAI protocol version, SCAI19, as described in the next section.

158.2.6.1 Application Logon SCAI Service Version

The dv-Appl-Logon message contains a parameter, Service Version, which uniquely identifies the version of messages which will be sent during the session. A new Service Version value will be created to uniquely identify the stream of messages which are new or changed during this software release. The new Service Version will be SCAI19.

This new Service Version (SCAI19) must be specified in the dv-Appl-Logon message for the host application to receive the enhanced messages. If a Service Version lower than SCAI19 is specified, the TRNKINFO parameter will not be contained in the above two SCAI messages sent to the Host.

The Service Version is upward compatible. This means all of the functionality enabled and provided with any of the previous Service Versions will be provided in SCAI19. Future DMS/CS2K/Cs2Kc software releases will provide additional ICM functionality but will continue to allow the specification of the SCAI19 Service Version. Therefore, applications written to use SCAI19 will not require rewriting to continue to work properly.

158.2.7 Call Processing and Error Handling

Throughout call processing, any time one of the two modified ICM messages is to be sent out, the switch will attempt to include the new TRNKINFO parameter. The following conditions must be met in order for this to occur:

1. SOC ICM00085 must be set to ON.
2. The SCAI Service Version is at least SCAI19.
3. An ICM switch-host session is established. A successful dv-Appl-Logon request was sent by the host computer.
4. The line which the host application is monitoring must be associated to the session via dv-DN-Associate.
5. For Centrex/Res lines the line option ECM with suboption CALL_EVENTS and SCAIRDIR must be set to ‘Y’.
6. The switch-host session is subscribed to the new default tuples, ACDEVENT19$, CTXEVENT19$ or RESEVENT19$.

For call which meet all of the above criteria, the trunk information will be sent if available. If the trunk information is not available then it cannot be sent and a new SCAI600 log is generated.

> ***Note:*** Nodal calls do not have a trunk involved in the call and therefore, have no trunk information. No log is generated for these calls.

For calls which do not meet the above criteria, the TRNKINFO parameter will not be sent. No log is generated.

Trunk information is obtained from tables created and altered by feature A00012527: Provisioning of CS2K trunks on GW and Carrier basis. The tables include GATWYINV and GWEPCARR. Please reference feature documentation for A00012527 for more information on these tables.

158.2.8 Log SCAI600

A new SCAI log, SCAI600, is created to indicate when a call should have sent the trunk information parameter, TRNKINFO, in the ICM message but was not able to because it was not available. The trunk information may not be available for a number of reasons including incorrect or missing datafill. The action is to check the datafill in table GATWYINV and GWEPCARR.

Please reference the FM section of this document for more information on this log.

158.3 Hardware Requirements or Dependencies

N/A

158.4 Software Requirements or Dependencies

If the trunk information is not available to the SCAI environment due to no manual entry of the SESM datafill in appropriate tables (look at activity A00012527: Provisioning of CS2K trunks on GW and carrier basis) the TRNKINFO parameter cannot be sent in the SCAI messages and log SCAI600 is generated.

158.5 Limitations and restrictions

New option TRNKINFO cannot be sent in ICM messages if no trunk information is available for the call.

158.6 Interactions

None of the existing interactions will be affected or changed by this activity. No new interactions will be introduced by this activity

158.7 Glossary

Term	Description
ACD	Automatic Call Distribution
ASN	Abstract Syntax Notation
CTI	Computer Telephone Integration
DN	Directory Number
ICM	Intelligent Call Management
MDC	Meridian Digital Centrex
RES	Residential Enhanced Services
SCAISSRV	Switch Computer Application Interface SCAI Service

158.8 Appendix: ASN.1 Notations for Modified ICM Messages

This sections shows the ASN.1 notations for the following modified ICM messages in SCAI19:

- DV_Call_Queued_U
- DV_Call_Offered_U

The new parameter, TRNKINFO, is added with the following information:

- Gateway Type: string {PVG, GW}
- Gateway Number: integer {0-1023}
- Carrier Number: integer {1-168}
- Channel Number: integer {1-31}

The parameters below which are ***italicized and bold*** are new to these messages.The letter ‘U’ in the message name indicates that the message is unconfirmed, i.e., this operation requires no outcome to be reported by the host. The letter ‘**C**’ at the end of the message’s name indicates that the message requires confirmation from the host.

158.8.1 DV_Call_Queued_U message

The switch sends this RO of Operation Class 5 to the host when a call to an ACD DN associated with the current session is received by the switch and placed in the Incoming Call Queue.

158.8.1.1 Changed DV_Call_Queued_U ASN.1 definition.

ASN.1 Encoding

dv-CALL-QUEUED-U ARGUMENT OPERATION

```
                                        ARGUMENT CallQueuedArgument ::= 6

CallQueuedArgument                      ::=     SEQUENCE
 {networkCallID             [0] IMPLICIT SEQUENCE
    {networkNodeID                  [0] IMPLICIT INTEGER OPTIONAL,
    localCallID                     [1] IMPLICIT INTEGER OPTIONAL}
                                    OPTIONAL,

acdDN                       [1] IMPLICIT OCTET STRING OPTIONAL,
origCallingNumber           [2] IMPLICIT OCTET STRING OPTIONAL,
origChargeNumber            [3] IMPLICIT OCTET STRING OPTIONAL,
callHistoryInfo             [4] IMPLICIT SEQUENCE

    {callType                       [0] IMPLICIT  ENUMERATED
        {callTransferred                (1),
        callOverflowed                  (2),
        callRedirected                  (3),
        callForwarded                   (4)
        callConsult                     (5),
        callConference                  (6),
        callReturnedToQueue             (7),
        callRouted                      (8)} OPTIONAL,

    origInboundDN               [1] IMPLICIT OCTET STRING OPTIONAL,
    prevApplicationID           [2] IMPLICIT INTEGER OPTIONAL,
    hostCallData                [3] IMPLICIT OCTET STRING OPTIONAL}
                                    OPTIONAL,

acdGroup                    [5] AddressType OPTIONAL,
forwardingParty             [6] ForwardingPartyType OPTIONAL,
cpadigs                     [7] IMPLICIT OCTET STRING OPTIONAL,
uuiParameter                [8] IMPLICIT OCTET STRING OPTIONAL,

trnkInfo                    [9] IMPLICIT SEQUENCE

{Gateway Type                       [0] IMPLICIT OCTET STRING OPTIONAL,

 Gateway Number                     [1] IMPLICIT INTEGER OPTIONAL,

 Carrier Number                     [2] IMPLICIT INTEGER OPTIONAL,

 Channel Number                     [3] IMPLICIT INTEGER OPTIONAL}

                                    OPTIONAL

}

    AddressType:: = CHOICE
```

```
{positionID                    [0] IMPLICIT INTEGER,
 dialedDigits                  [1] IMPLICIT IA5STRING,
 stationNumber                 [2] IMPLICIT OCTET STRING,
 q931Address                   [3] Q931AddressType}

Q931 AddressType               :: =     SEQUENCE
{numberTypeNumberPlan          [0] OCTET STRING OPTIONAL,
 presentationScreeningIndicator [1] OCTET STRING OPTIONAL,
 digits                        [2] IA5 STRING OPTIONAL}


ForwardingPartyType            :: =     IMPLICIT SEQUENCE
{firstFwdNumber                [0] AddressType OPTIONAL,
 firstFwdReason                [1] IMPLICIT ENUMERATED
 {unknown                      (0),
 userBusy                      (1),
 noReply                       (2),
 unconditional                 (3)  }   OPTIONAL,
 lastFwdNumber                 [2] AddressType OPTIONAL,
 lastFwdReason                 [3] IMPLICIT ENUMERATED
 {unknown                      (0),
 userBusy                      (1),
 noReply                       (2),
 unconditional                 (3)  }   OPTIONAL},
```

158.8.1.2 DV_Call_Queued_U:Coded example.

An ACD call has been initiated from the OrigCallingNumber 6136217703 6134444444 and offered over a trunk to an ACD group with Primary DN 6136212111, for which no agent is available, the call is placed in the Incoming Call Queue and the switch sends DV-CALL-QUEUED-U to the host. No Return Result is required or received by the switch from the host.

INVOKE **CS2K** ===== > **HOST**

Hex Dump			Information Element	Comments
Tag	**Length**	**Content**		
a1	54		INVOKE	Message length is 84 bytes decimal
02	02	03 ff	InvokeID	The InvokeID is 1023
02	01	06	Operation	Operation value for DV-CALL-QUEUED-U is decimal 6
30	4b		Argument	CallQueued argument is of Sequence type and is 75 bytes long decimal

Hex Dump			Information Element	Comments
Tag	**Length**	**Content**		
a0	09		NetworkCallId	The NetworkCallId is a constructor of 9 bytes long
80	04	03 38 d0 90	NetworkNodeId	The NetworkNodeId is 54055056
81	01	0d	LocalCallId	The LocalCallId is 13
81	0a	36 3133 36 32 31 32 31 31 31	ACDDN	The called ACDDN of the Group is 6136212111
82	0c	00 83 36 31 33 36 32 31 37 37 30 33	Original Calling Number	The first 2 bytes are fixed and must not be read at present. The original calling number is 6136217703
A5	0c		Acd group	The ACDGroup is of type Constructor and is 12 bytes long
82	0a	36 31 33 36 32 31 32 31 31 31	Station number	The station number of the ACDGroup is 6136212111
87	0a	36 31 33 34 34 34 34 34 34 34	CPADIGS	The CPA value is 6134444444
A9	**0E**		**trnkInfo**	**is a constructor of 14 bytes long.**
80	**03**	**50 56 47**	**Gateway Type**	**PVG**
81	**01**	**39**	**Gateway Number**	**decimal 57**
82	**01**	**54**	**Carrier Number**	**decimal 84**
83	**01**	**10**	**Channel Number**	**decimal 16**
Hex Dump= a1 54 02 02 03 ff 02 01 06 30 4b a0 09 80 04 03 38 d0 90 81 01 0d 81 0a 36 31 33 36 32 31 32 31 31 31 82 0c 00 83 36 31 33 36 32 31 37 37 30 33 a5 0c 82 0a 36 31 33 36 32 31 32 31 31 31 87 0a 36 31 33 34 34 34 34 34 34 34 a9 0E 80 03 50 56 47 81 01 39 82 01 54 83 01 10				

158.8.2 DV_Call_Offered_U message

This section describes the DV-CALL-OFFERED-U message the switch uses to notify the host that a ICM Party has been selected for ACD. The party has been selected to handle an incoming call to one of the DNs belonging to the associated environment of the current switch-host session when the call is about to be offered to the ICM Party. This call comes in over a trunk.

158.8.2.1 Changed DV_Call_Offered_U ASN.1 definition.

ASN.1 Encoding

```
dv-CALL-OFFERED-U                   OPERATION

                                ARGUMENT CallOfferedArgument ::= 5

CallOfferedArgument             ::=     SEQUENCE
 {networkCallID             [0] IMPLICIT SEQUENCE
    {networkNodeID                  [0] IMPLICIT INTEGER OPTIONAL,
     localCallID                    [1] IMPLICIT INTEGER OPTIONAL}
                                    OPTIONAL,
acdDN                       [2] IMPLICIT OCTET STRING OPTIONAL,
origCallingNumber           [3] IMPLICIT OCTET STRING OPTIONAL,
origChargeNumber            [4] IMPLICIT OCTET STRING OPTIONAL,
callHistoryInfo             [5] IMPLICIT SEQUENCE

 {callType                  [0]  IMPLICIT  ENUMERATED
    {callTransferred        (1),
     callOverflowed         (2),
     callRedirected         (3),
     callForwarded          (4)
     callConsult            (5),
     callConference         (6),
     callReturnedToQueue (7),
      callRouted             (8)} OPTIONAL,

 origInboundDN    [1] IMPLICIT DeviceAddressType OPTIONAL,
 prevApplicationID[2] IMPLICIT INTEGER OPTIONAL,
 hostCallData       [3] IMPLICIT OCTET STRING OPTIONAL}
                                OPTIONAL,

acdGroup            [6] AddressType OPTIONAL,
callMode            [7] IMPLICIT ENUMERATED

{callWaited         (1)}    OPTIONAL,
destDeviceID        [8] AddressType OPTIONAL,
forwardingParty     [9] ForwardingPartyType OPTIONAL,
cpadigs             [10] IMPLICIT OCTET STRING OPTIONAL,
```

uuiParameter [11]IMPLICIT OCTET STRING OPTIONAL,

trnkInfo [12] IMPLICIT SEQUENCE

{Gateway Type [0] IMPLICIT OCTET STRING OPTIONAL,

Gateway Number [1] IMPLICIT INTEGER OPTIONAL,

Carrier Number [2] IMPLICIT INTEGER OPTIONAL,

Channel Number [3] IMPLICIT INTEGER OPTIONAL}

OPTIONAL

}

AddressType :: = CHOICE
{positionID [0] IMPLICIT INTEGER,
dialedDigits [1] IMPLICIT IA5STRING,
stationNumber [2] IMPLICIT OCTET STRING,
q931Address [3] Q931AddressType}

Q931AddressType :: = SEQUENCE
{numberTypeNumberPlan [0] OCTET STRINGOPTIONAL,
presentationScreeningIndicator [1] OCTET STRINGOPTIONAL,
digits [2] IA5 STRING OPTIONAL}

ForwardingPartyType :: = IMPLICIT SEQUENCE
{firstFwdNumber [0] AddressTypeOPTIONAL,
firstFwdReason [1] IMPLICIT ENUMERATED
{unknown (0),
userBusy (1),
noReply (2),
unconditional (3)} OPTIONAL,

lastFwdNumber [2] AddressType OPTIONAL,
lastFwdReason [3] IMPLICIT ENUMERATED
{unknown (0),
userBusy (1),
noReply (2),
unconditional (3) } OPTIONAL}

158.8.2.2 DV_Call_Offered_U: Coded example.

An ACD call is initiated from the OrigCallingNumber 6136217703 by dialing 6134444444 and is assigned a LocalCallID = 9. The call is offered over a trunk to an acd agent with posid 7707 of the acd group with primary DN 613621111.

The switch sends DV-CALL-OFFERED-U to the host. No Return Result is required or received by the switch from the host.

INVOKE **CS2K** ===== > **HOST**

Hex Dump			Information Element	Comments
Tag	**Length**	**Content**		
a1	5a		INVOKE	this message is 90 bytes decimal
02	02	03 f9	InvokeID	the InvokeID is 1017
02	01	05	Operation	the operation is DV-CALL-OFFERED-U [5]
30	51		Argument	CallOffered argument is of Sequence type and is 81 bytes long decimal
a0	09		NetworkCallId	The NetworkCallId is a constructor 9 bytes
80	04	03 38 d0 90	NetworkNodeId	The NetworkNodeId is 54055056
81	01	09	LocalCallId	The LocalCallId is 9 decimal
82	0a	36 31 33 36 32 31 32 31 31 31	acd_dn	6136212111
83	0c	00 83 36 31 33 36 32 31 37 37 30 33	OrigCallingNumber	The first two bytes are fixed and presently must not be read.The customer's OrigCallingNumber is 6136217703
a6	0c		acd_grp	
82	0a	36 31 33 36 32 31 32 31 31 31	StationNumber	The called DN is 6136212111
a8	04		DeviceID	The DeviceID is of type Constructor and is 4 bytes long
80	02	1e 1b	pos_id_2	7707
8a	0a	36 31 33 34 34 34 34 34 34 34	CPADIGS	The CPA value is 6134444444
Ac	**0E**		**trnkInfo**	**is a constructor of 14 bytes long.**

Hex Dump			Information Element	Comments
Tag	Length	Content		
80	03	50 56 47	Gateway Type	PVG
81	01	64	Gateway Number	decimal 100
82	01	1E	Carrier Number	decimal 30
83	01	0A	Channel Number	decimal 10
Hex Dump = a1 5a 02 02 03 f9 02 01 05 30 51 a0 09 80 04 03 38 d0 90 81 01 09 82 0a 36 31 33 36 32 31 32 31 31 31 83 0c 00 83 36 31 33 36 32 31 37 37 30 33 a6 0c 82 0a 36 31 33 36 32 31 32 31 31 31 a8 04 80 02 1e 1b 8a 0a 36 31 33 34 34 34 34 34 34 34 Ac 0E 80 03 5056 47 81 01 64 82 01 1E 83 01 0A				

159: Functional Description (FN) A00012527

159.1 Feature name and Feature ID

A00012527 - Provisioning of CS2K trunks on GW and Carrier basis

159.2 Description

This activity allows mapping of trunk TID's on CS2K core based on GW and carrier, using CM tables GATWYINV and GWEPCARR.

Currently, provisioning of GWs and carriers for CS2000 trunking is done in the CS2K EM (SESM). Provisioning of trunk groups and individual trunk members is done in the CS2K CM. A trunk member in the CM is mapped to a channel on a carrier in SESM using a node and terminal number (TID). No GW or carrier information is currently available on the CM for trunks configured on gateways. Because of this data split, existing OA&M on the CM can only identify the TID of a trunk to the craftsperson by giving the physical circuit location. This has resulted in

1. a multi-step process for the craftsperson to locate a physical GW and pack (CM -> SESM -> GW element manager or physical hardware).
2. the inability to provide maintenance services on GW or carrier from the CM.
   - — post by GW or carrier in TTP
   - — OMs on a GW basis
   - — GW alarm

As part of this activity, changes will be made in the following areas:

- Support for PVG and GW profiles for table GATWYINV
- Introduction of new table GWEPCARR
- Modification of CktLoc command in MAPCI, TTP level to display Gateway and Carrier information.

This activity will support both North American and International loads.

Figure 1 Trunk Carrier / GW data in core

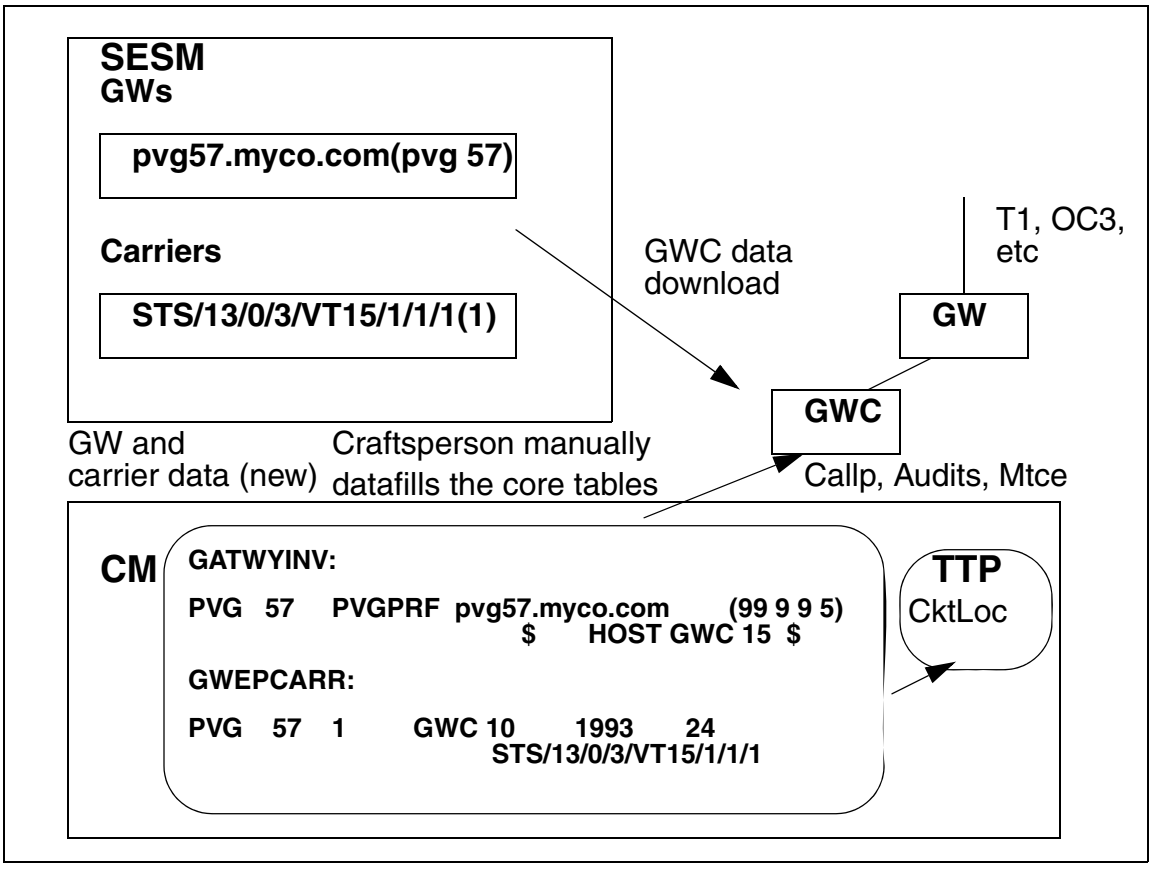


Figure 2 TTP Display with Modified CktLoc Command

```
XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
AMDI      .     DLOG E    .       1 SPM     .    SYSB     57C..     .     SDM
  M                              *C*             CR C    *C*             M
TTP
 0 QUIT      POST     1  DELQ           BSYQ         DIG
 2 Post_     TTP  6-0000
 3 SEIZE     CKT TYPE     PM NO.          COM LANG STA S R  DOT TE  RESULT
 4           2W S7 S7 GWC  15    12       TEST   0 INB
 5 BSY                                                  R
 6 RTS
 7 TST
 8
 9 CktInfo
10 CktLoc
11 Hold       CktLoc
12 NEXT       GW          Ckt  Chnl
13 RLS        PVG   57    1      1
14 Ckt_
15 TrnslVf_   GW Name
16 StkSdr_    PVGRTP1023
17 Pads       Endpoint Name
18 Level_       STS/13/0/3/VT15/1/1/1/1
  ADMIN
Time  15:59  >
```

Note 1: Automatic upload from SESM to GATWYINV and GWEPCARR tables in core is not supported as part of this activity. The craftsperson has to manually datafill the tables by looking into the SESM details.

159.2.1 GW Data - Table GATWYINV

Table GATWYINV is an existing table that houses the gateway related information. It currently allows only ABI GWs which are provisioned in parallel in the CM and SESM. This activity shall allow support for PVG and GW profiles in table GATWYINV.

Datafill each gateway in table GATWYINV prior to datafill in table GWEPCARR. Deleting of tuple in GATWYINV is not allowed if the Gateway type and number are being referenced in table GWEPCARR.

For details on what/how this is provisioned, refer to “12.5.2 Table GATWYINV Database Schema information” in the CN chapter of this book.

159.2.2 Carrier Data - Table GWEPCARR

Table GWEPCARR is a new table that shall hold the mapping from GW and carrier number to the TID range used by trunks on the carrier. The key to table GWEPCARR is the GW type and number and the carrier number. The number of channels on a carrier is restricted to 24 for North America and 31 for International. The table will also hold the carrier name information.

The internal representation of GWEPCARR shall be used to map GW and carrier group number to the TIDs used for that carrier. There shall also be a mapping from TID to GW and carrier.

Datafilling table GWEPCARR with a gateway, that does not exist in table GATWYINV, is not allowed.

For details on what/how this is provisioned, refer to “12.5.3 Table GWEPCARR Database Schema information” in the CN chapter of this book.

159.2.3 Trunk Test Position (TTP - CM)

At MAPCI, TTP level, the CktLoc command is not currently supported for GWC trunks. This component shall support GWC for CktLoc and shall display the gateway and carrier information for the trunk member currently being posted, if the TID to Carrier mapping exists in Table GWEPCARR.

If the posted trunk does not have TID to Carrier mapping in table GWEPCARR, then a message “CARRIER INFO NOT PRESENT IN TABLE GWEPCARR” would be displayed.

The CktLoc will not be supported for GWC audio nodes as part of this activity.

For details on what/how this is done, refer to the CN section of this feature.

159.3 Hardware Requirements or Dependencies

N/A

159.4 Software Requirements or Dependencies

This feature requires the Core load to be a succession load.

159.5 Limitations and restrictions

Craftsperson should provision the Gateway and carrier information in SESM. The same information must be manually datafilled in core as well.

159.6 Interactions

N/A

159.7 Glossary

Term	Description
CM	Computing Module (also known as “Core”)
CS2K	Call Server 2000
EM	Element Manager
GATWYINV	Gateway Inventory Table
GW	Gateway
GWC	Gateway Controller
GWEPCARR	Gateway Endpoint Carrier Table
PM	Peripheral Module
PVG	Packet Voice Gateway
SESM	Succession Element Sub-element Manager
TID	Terminal Identifier
TRKMEM	Trunk Member Table
TTP	Trunk Test Position
CktLoc	Circuit Location
MAPCI	Maintenance and Administration Position Command Interpreter

160: Functional Description (FN) A00012528

160.1 Feature name and Feature ID

A00012528 - ICM Queue Expansion

160.2 Description

160.2.1 ICM Work queue

For every ICM link datafilled through Table SCAICOMS, one incoming and one outgoing ICM work queue is allocated. All messages coming from the host computer are queued by the transport into the incoming ICM work queue. Messages sent by the switch are queued by the ICM application into the outgoing ICM work queue. When the ICM work queue becomes full, the messages coming into it are lost. This scenario may arise during high traffic. This feature increases the ICM temporary queue size and hence enhances its capability to handle messages during high traffic. The ICM temporary queue size is being increased from 512 to 1024. Refer to Section 2.3 for further details on ICM temporary queue size increase.

160.2.2 Invoke ID

An Invoke ID is used each time an ICM message is sent or received. This Invoke ID remains in use until the message is responded to. Currently, the Invoke ID range is 0 - 1024. The messages originated by the switch to the Host will use Invoke IDs from 1023 down to 512 while the Host will use Invoke IDs from 0 up to 511. This feature also increases the Invoke ID range from 0 -1024 to 0 -3072 to support the increase of the ICM temporary queue. Refer to Section 2.4 for further details on Invoke ID expansion.

160.3 ICM Temporary Queue Expansion

Feature A59006731 introduced the concept of temporary work queues. This is an allocated pool of ten incoming/outgoing queues which is created at the time of datafilling the first ten links in Table SCAICOMS. As of now, the temporary work queues are capable of handling 512 messages. This pool of ten temporary incoming/outgoing queues will be available to any of the 351 links which experience high traffic. This pool of ten temporary queues is in addition to the SCAI Incoming/Outgoing work queue for each of the 351 links which is capable of handling up to 128 messages at a time. When the item count of an ICM Work queue (incoming or outgoing) reaches the threshold value of 128, a temporary queue (incoming or outgoing) from the allocated pool of ten temporary queues will be made available. So a total of 640 messages can be queued at a time. During high traffic, if the number of messages goes beyond 640, then the message is lost.

This activity increases the size of the ICM temporary queue to support 1024 messages at a time. This ensures that during high traffic conditions, message loss will be minimized to a large extent. The temporary queue size will be increased for both X.25 and TCP/IP links.

160.4 Invoke ID Expansion

Even with the increased size of the ICM message queue it will only be possible to queue a maximum of 512 messages without the expansion in the Invoke ID range. So this feature also increases the Invoke ID range from 0 -1024 to 0 - 3072 to support the increase of the ICM temporary queue. The messages originated by the switch to the host will use Invoke IDs from 3071 down to 1536 while the host will use Invoke IDs from 0 up to 1535.

The Invoke ID expansion will be controlled by the scai protocol version. For protocol version scai19 and above the Invoke ID range will be 0 - 3072. So the range of Invoke IDs for a session is determined at the time of session logon and by the scai protocol version. For session logons with scai protocol version less than scai19, the old range of Invoke IDs are retained.

The table below shows the Invoke ID range corresponding to the scai protocol version in the application logon message.

Table 1: Invoke ID range dependent on the Scai version

Affected ranges	Protocol version >= scai19	Protocol version < scai19
Invoke ID Range	0 to 3072	0 to 1024
Host to Switch Invoke ID range	0 to 1535	0 to 511
Switch to Host Invoke ID range	3071 to 1536	1023 to 512

160.5 Hardware Requirements or Dependencies

N/A

160.6 Software Requirements or Dependencies

N/A

160.7 Limitations and restrictions

N/A

160.8 Interactions

N/A

160.9 Glossary

Term	Description
ICM	Intelligent Call Management
SCAI	Switch-Computer Applications Interface

161: Functional Description (FN) A00012538, A00012537, A00012539

161.1 Feature name and Feature ID

A00012538, A00012537, A00012539--SIP Lines Support - Part 2

161.2 Description

This activity, SIP Lines Support - Part 2, consists of 3 features:

- A00012538 - Additional Provisioning for SIP Lines
- A00012537 - SIP Lines - Data Sync Audit
- A00012539 - SIP Lines - Maintenance Enhancements

These features deal with meeting the Configuration and Provisioning requirements on CS2K SS for support of SIP Lines. It provides new OPI and OMI interfaces for configuration and provisioning. In addition new OPI methods are added for audit - which can be used by the clients to ensure that data on MCS is in sync with Data on other systems unknown to MCS.

The responsibility for audit and data correction is that of the client (SESM). The server provides mechanism to retrieve the data that exists on SS and use that for maintaining data consistency.

The requirements fall into the following work areas.

HUNT/MADN Group Provisioning

OPI methods for Data Audit

Version Service

Client Jars

Backward/ Forward compatibility

Number of simultaneous Endpoint postings

161.3 HUNT/ MADN Group Provisioning

The activity “A00009528 - Call Pickup” introduces a concept of grouping users on the Provisioning System. The group provisioning is generic and is associated with a group type. The group type defines what Call Processing Service the group is used for.

This feature requires addition on new group types such as MADN and Hunt Groups. Please refer to the “A00009528 - Call Pickup” FN for details.

The interfaces defined by the Call Pickup feature is leveraged for Group Provisioning. No additional methods are required for the same.

161.4 OPI methods for Data Audit

Several new methods are required to carry out the audit functionality for SIP Lines data on the client (SESM).

SIP Line Data Audit - SIP Line provisioning functionality was introduced as part of A00009043 SIP Lines Provisioning Support feature. Several new methods are required for auditing this data from the client.

The following methods are added to OPI web service.

1) public int getUserCountInSubDomain(String subDomainName) throws ProvisionException

Could be the root domain name. The output is the number of users in the actual domain specified.

2) public int getUserCountInDomain(String domainName) throws ProvisionException

Returns user count in the domain tree starting with the specified domain.

A new web service called “SIPLines” is added and the following methods will be exposed via this service.

1) public String[] getDomainsForVMG(String vmgName) throws ProvisionException

2) public String[] getVMGForDomain(String subDomainName) throws ProvisionException

This takes in the actual subdomain name.

3) public SipLineAuditData[] getSIPLineAuditDataByDomain(String domainName, int start, int stop) throws ProvisionException

Returns the users available in the actual domain specified.

The SIPLineAuditData object contains the following fields:

String endpointId
String vmg
String[] clientType
String userName (user@root domain only. Actual subdomain does not matter).
String dirNum

4) public SipLineAuditData[] getSIPLineAuditDataByDomainByVMG(String domainName, String vmgName, int start, int stop) throws ProvisionException

Returns the users available in the actual domain specified.

5) public String[] getUsersByRegistrationState(String domainName, boolean registered)

Returns the usernames in the actual domain specified.

This method returns the list of usernames in the domain specified that have any contacts registered if registered boolean is set to true.

It returns the list of users that are not registered at all if the registered boolean is set to false.

6) public String[] getUsersByRegistrationState(String domainName, boolean registrationState, String clientType)

Returns the usernames in the actual domain specified.

The client type is the name from the ClientType object that is returned by the getClientTypes() method.

Returns the same list as in the previous method, except that it is also filtered by the client Type. The client type check is done against the provisioned data and has no bearing to what client actually registered. (No way of knowing that).

Group Data Audit - Refer to the Call Pickup FN for APIs.

161.5 Version Service

A new web service “VersionService” will run on the SM and Prov Mgr.

Interface: VersionService

Method: getLoadVersion() returns Version

Version {

int majorReleaseNum

int minorReleaseNum

int maintenanceReleaseNum

}

This service would be used by OPI and OMI clients to handle versions for maintenance releases. Refer to Backward/ Forward Compatibility section for more details.

161.6 Client Jars

The client jar (built based on the wsdl) for SIPLines web service will be available in the “OPIClient.jar”.

The client jar (built based on the wsdl) for OMI services will be available in “OMIClient.jar”.

These jars will be available as part of the MCS load. The location of these jars for SESM loadbuild is TBD.

161.7 Backward/ Forward Compatibility

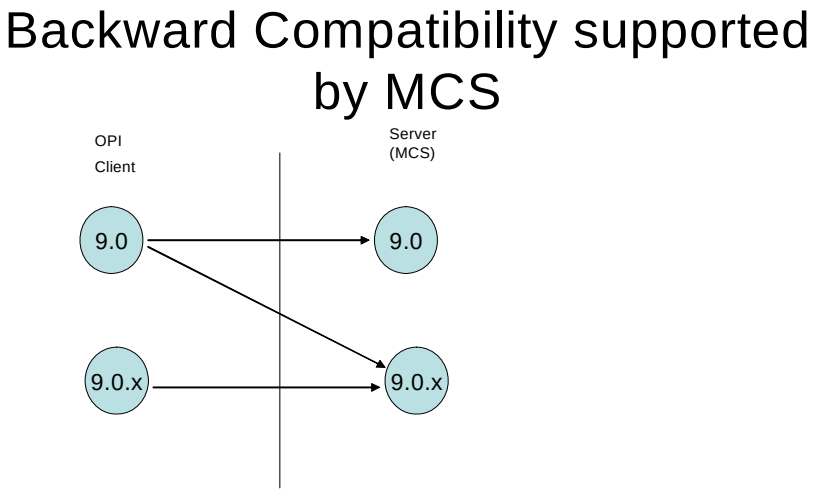
There are new OPI and OMI interfaces as part of this feature. Existing interfaces work as is and do not get affected.

OPI and OMI web services support backward compatibility for 1 release. This section describes SESM’s specific requirement for forward compatibility. The details are based on the fact that these features are delivered in a maintenance release for MCS09.

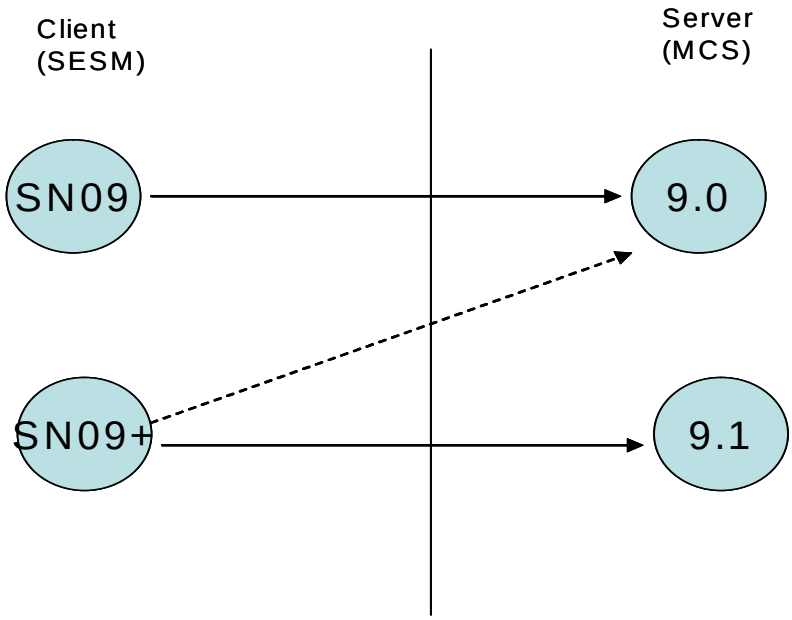
In the SIPLines solution, for provisioning and configuration using OPI and OMI services, MCS is a server and SESM works as a client. Since the client (SESM) would be upgraded prior to MCS (server), there is a risk that a forward release client talks to the older MCS09 load for the new functionality.

It is the client’s job to ensure that appropriate methods are called on the respective servers.

MCS Supported Backward Compatibility for major and minor releases:

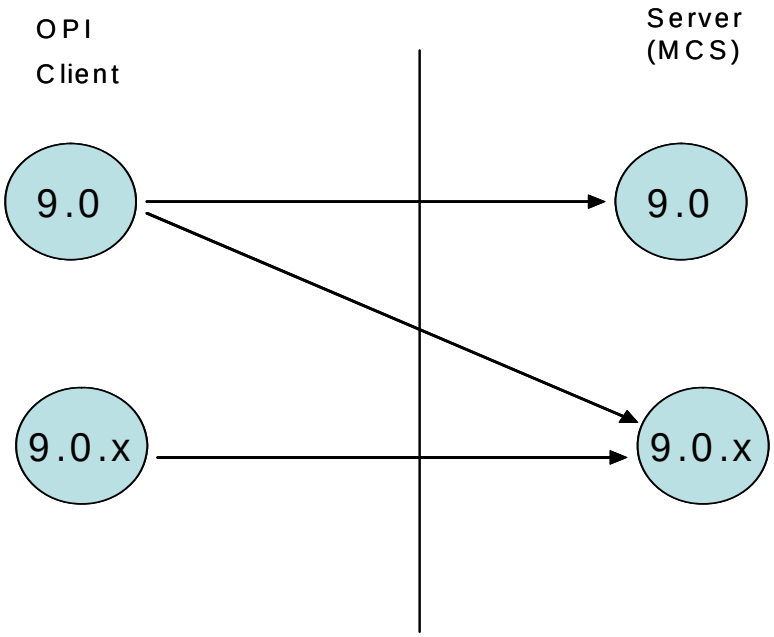


Forward Compatibility for major and minor releases:

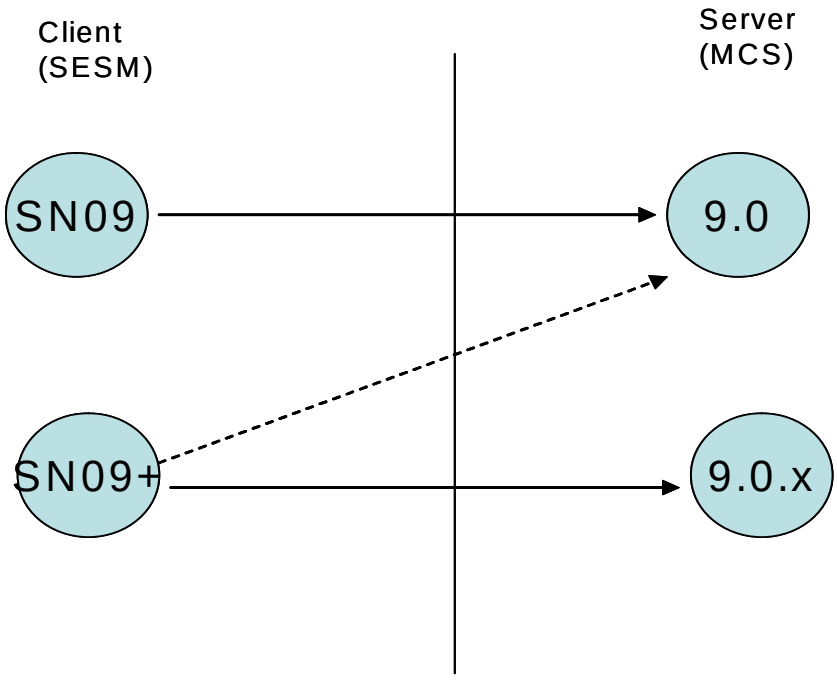


SESM would call the method getCurrentOPIVersion and based on the servers version, call the appropriate methods. The server would return the strings “9.0” and “9.1” respectively.

MCS Supported Backward Compatibility for maintenance releases:



Forward Compatibility for maintenance releases:



SESM would use VersionService to determine the MR number. Based on the MR number, SESM determines which methods to call. The server still expects the string “9.0” as the version number for any OPI method calls.

161.8 Number of simultaneous Endpoint posting

In the first release of SIP Lines on MCS (MCS 09) the number of endpoints which could be simultaneously posted from a single OMI login was limited to five. Since live monitoring of endpoint state must be done at the component which is aware of that state, endpoint state information is retrieved from the MCS Session Manager, which is responsible for Call Processing. This number was chosen as one which would not impact traffic rates on the Session Manager. However, it may be possible to increase the number without adversely affecting Call Processing. This feature will provide a mechanism to engineer the number of simultaneous endpoint posting per Session Manager via a configuration parameter against the System Manager.

161.9 Software Requirements or Dependencies

161.10 Limitations and restrictions

Interactions

A00009043 SIP Lines Provisioning Support

A00009528 Call Pickup

161.11 Glossary

Term	Description
Accounting Manager	CS2K MSM component which formats and stores billing records from the Session Manager. Turned off in MSM 9.0
AM	Accounting Manager
CPB	Call Processing Busy. Used to indicate that a SIP Line Subscriber is in the middle of a call.
Endpoint	Refers to a SIP Line Subscriber. In the context of SIP Lines, an endpoint does not actually refer to an IP port pair, but to a subscriber who may have registrations at multiple locations.
GCP	Gateway Control Protocol. Used for communication with GWCs
GWC	Gateway Controller. CS2K component to which Session Managers communicate for call processing
MCS	Multimedia Communication Server
MSM	Multimedia Session Manager
NCAS	Non Call Associated Signalling

Term	Description
NE	Network Element. A managed component of CS2K MSM. Includes Accounting Manager, Session Manager, and System Manager.
OAM	Operations, Accounting, and Management.
OID	Object Identifier. Unique ID used in the CS2K MSM database as a primary key.
OMI	Open Management Interface
Provisioning Manager	CS2K MSM component which manages CS2K MSM provisioning, including subscribers.
Session Manager	CS2K MSM component which manages SIP Sessions and call processing
SIP	Session Initiation Protocol
System Manager	CS2K MSM component which manages CS2K MSM configuration and maintenance.
VMG	Virtual Media Gateway. CS2K view of the CS2K MSM Session Manager.

162: Functional Description (FN) A00012569

162.1 Feature name and Feature ID

A00012569 - NI2 PRI/ ISUP UUI over SCAI

162.2 Description

162.2.1 User-to-User Service (UUI) Information Element (IE)

The PRI User-to-User Signalling (UUS) supplementary service enables a user to send/receive a limited amount of information to/from another user.This information is passed transparently without modification of content through the network over the signalling channel in association with the call.

UUS allows communication of ISDN users by transferring user-to-user information (UUI) during call establishment, call confirmation and/or call clearing phases of a call, within call control messages. Maximum 128 octets of user-to-user information can be transferred in each message. The UUI is already supported in Setup message for PRI NI2 GWC trunks.

This feature will support UUI for Setup Q931 messages i.e call establishment phase for

- DTCI and SPM peripherals for NI2 PRI trunk
- GWC, SPM and DTCI peripherals for NTNA PRI Trunks

UUS option will be enabled by datafilling in table LTDATA.

The UUI data from the setup will be tandemed to ISUP IAM (Initial address message) without any modification to the UUI data field. Similarly, UUI data from the ISUP IAM will be tandemed to PRI setup message without any modification to the UUI field.

162.2.2 UUI over SCAI

SCAI (Switch Computer Application Interface) is a messaging link provided by the CS2K to a host computer. The information carried across the X.25/TCP-IP link allows applications running on the CS2K to communicate with applications running on the host computer.

This feature will support delivery of UUI in the following SCAI messages:

- DV_Call_Received_C
- DV_Call_Queued_U
- DV_Call_Offered_U

In order to support UUI, the size of outgoing ICM messages will be increased from 256 bytes to 512 bytes. The support of UUI over the SCAI link will be supported only for SCAI19 and later service versions.

162.3 User-to-User Service (UUI) Information Element (IE)

162.3.1 Functional overview

In order to provide the User to User service on an NI2 PRI / NTNA PRI variant, two levels of requirements need to be met.

- There are 2 possibilities of UUS subscription, “Required” or “Preferred”. This feature will support only “Preferred” subscription.
- The second level is the request for a call. This is accomplished by the presence of a UUI IE in a received SETUP message.

The user to user data in any subsequent messages (Alert, Connect & Disconnect) is discarded.

This feature supports only the “Preferred UUS” option. The UUS is an existing option in table LTDATA.

User-to-User Service (UUS) starts with UUS option datafilled against a given LTID in table LTDATA. The UUS option is already available for tuples in table LTDATA. At present, it is enabled for NI-2 LTIDS on GWC. This feature enables UUS as an option for NI-2 LTIDs on SPM and XPM(DTCI). The Feature also supports UUS as an option for NTNA PRI LTIDs on SPM, XPM(DTCI) and GWC.

A call initiated with a Q.931 SETUP message having no UUI IE proceeds as non-UUS call.

This feature also supports mapping of UUI and UUS related messages for the following interworking:

- NI-2 PRI to/from NI-2 PRI
- NI-2 PRI to/from ANSI ISUP
- NTNA PRI to/from NTNA PRI
- NI-2 PRI to NTNA PRI

This feature will support UUS for NI-2 variant PRI and NTNA PRI100 variant on the following peripherals:

- A legacy XPM (DTCI)
- A SPM (DMSCP/MG4K)
- A GWC that hosts an H.248 trunk GW (PVG)

162.3.2 Delivery of UUS:

The Subscription of UUS has the following two possibilities:

- Preferred UUS
- Required UUS

162.3.2.1 Preferred UUS

Preferred UUS indicates that originating ISDN user can send a UUI IE in the Q.931 SETUP message to activate the service. If the UUI IE cannot be delivered to the far end user, due to a failure scenario the call continues without UUS active.

Preferred UUS subscription is obtained by datafilling table LTDATA with service option 'UUS' as shown in example below.

Preferred UUS will be supported by this feature.

Figure 1 External view of tuple in Table LTDATA with Preferred option

```
TABLE LTDATA
LTDKEY LTDRSLT
-----------------
ISDN 641 SERV SERV N N ALWAYS ALWAYS (UUS) $
```

162.3.2.2 Required UUS

REQUIRED UUS indicates that the originating ISDN user can send an UUI IE in the Q.931 SETUP message to activate the service. If the UUI IE cannot be delivered to the far end user due to a failure scenario, the call is cleared at the originating switch.

REQUIRED UUS will not be supported as part of this feature.

162.3.3 Message Protocols

162.3.3.1 ISDN UUI IE

The ISDN User to User Information Element structure is based upon the CCITT Recommendation Q.931 ISDN user-network interface layer 3 specification. The ISDN User to User Information Element structure will be as follows:

Table 1 User-user information element, coded #7E

Byte	8	7	6	5	4	3	2	1
1	0	1	1	1	1	1	1	0
		User-User Information Element Identifier						
2	Length of user-user contents							
3	Protocol Discriminator							
4	User Information							
:	:							
n	:							

- "n" can be a maximum of 131 bytes, which means up to 128 bytes of user information may be included.
- Protocol Discriminator is coded as 0 0 0 0 0 0 0 0 to indicate User Specific protocol.
- The User to User Information Element must be at least 3 bytes long in order for the UUS functionality to be invoked.
- The length of the UUI IE information is not regarded in the above 3 bytes limit check. Thus the presence of the first three bytes is mandatory for the UUI IE to be accepted.

162.3.3.2 User-to-User information parameter (UUI) on ISUP

The purpose of the User-to-user information parameter is to convey information between ISDN users. This information is not interpreted by the network, but rather is carried transparently and delivered to the remote user(s).

The format of the user-to-user information parameter is shown in the table below:

Table 2 User-user information parameter, coded #20

	8	7	6	5	4	3	2	1
1	User-user							
	0	0	1	0	0	0	0	0
	Information Parameter Identifier							
2	Length of user-user contents							
3	Protocol discriminator							
4etc	User information							

162.3.4 PRI to PRI/ISUP messaging

The UUS functionality is requested by including UUI IE in the SETUP message. When the originating CS2K receives the UUI IE in the SETUP message, table LTDATA static data will be checked. If Table LTDATA is NOT datafilled to support Preferred UUS, then the UUI IE will be stripped from the SETUP message and a STATUS message with Cause value of 50 “Requested Facility Not Subscribed” will be sent to the originator and the call will continue. If table LTDATA is datafilled to support Preferred UUS, then the ISDN UUI IE in the SETUP message will be carried across the network, the UUI IE will be mapped to the SETUP message for PRI to PRI calls and delivered to the ISDN end user.

The UUI data from the setup will be tandemed to ISUP IAM (Initial address message) without any modification to the UUI data field. Similarly, UUI data from the ISUP IAM will be tandemed to PRI setup message without any modification to the UUI field.

162.3.5 Preferred UUS Behavior

The Preferred UUS functionality will be requested by including UUI IE in the Q.931 SETUP message. When the Originator receives the UUI IE in the Q.931 SETUP message, Table LTDATA static data will be checked for subscription.

- **Preferred UUS Provisioning Phase**:

If table LTDATA is datafilled to support Preferred UUS, then the UUI IE in the Q.931 SETUP message will be carried across the network. The UUI IE will be mapped to the Q.931 SETUP message for PRI to PRI calls and/or PRI to ISUP calls, delivered to the end user.

- **Preferred UUS Call Request Phase:**

A call with specific parameters is requested by the calling party. If the (calling party) Originator sending the Q.931 setup message containing the UUI parameter, and if the Originator subscribes to the UUS service, then the UUI is mapped to SCP_X_Originate message. Otherwise the PM (DTCI, XPM, SPM) will send a Q.931 STATUS message to the Originator to indicate that the UUS facility was NOT subscribed. The Q.931 STATUS message with Cause value of 50 “Requested Facility Not Subscribed” will be sent to the originator and the call will continue without the UUI information.

Table 3 Error Scenario Handling

EVENT	ACTION BY SPCS/CS2K
UUS in Setup, but calling party has not subscribed to UUS option in LTDATA table.	Discard UUS; return STATus (cause #50) to calling party; continue call processing
UUS in SETUP cannot be further conveyed due to unsupported signaling. (Delivery of UUS is “Preferred”)	Discard UUS; continue call processing; return STATus (cause #69) to calling party.
User-User Information Element too long (excessive of 131 octets)	Discard UUS; continue call processing; Return STATus (cause #43) to sending party
UUS in CONNect,	Discard UUS; continue call processing;
UUS in DISConnect,	Discard UUS
UUS is present in an inappropriate clearing message (RELease)	Discard UUS; return RELease COMplete (cause #43) to sending party; continue call clearing
SETUP message length exceeds maximum supported number of octets	Discard UUS; continue call processing; return STATus (cause #43) to sending party

162.3.6 Information Element and Parameter Summary

A ‘X’ in Table 4 indicates that the IE, or parameter, can be included in the message identified in the column on the left. A blank entry indicates inclusion of the IE, or parameter, is invalid or not applicable.

Table 4 Information Element and Parameter Summary

Message	UUI IE	UUI Parm	Notes	UUI Supported
Setup (SETUP)	X		Call Request message	Yes
Alerting (ALERT)	X			No
Connect (CONNECT)	X		Call Confirmation message	No
Disconnect (DISC)	X		Call clearing message	No
Initial Address Message (IAM)		X	Call Request message	Yes
Address Complete Message (ACM)		X		Yes
Answer Message (ANM)		X	Call Confirmation message	Yes
Release (ISUP REL)		X	Call Clearing message	Yes

162.3.7 Hardware Requirements or Dependencies

None.

162.3.8 Limitations and restrictions

- The maximum length supported for the ISDN UUI IE is 131 bytes.
- The maximum length supported for the ISUP UUI Parameter is 131 bytes.
- The scope of this feature is limited to UUS enhancement for NI-2 PRI variant and NTNA PRI variant only.
- Only “Preferred” UUS option is supported by this feature.
- The protocol specifics outlined in this document reflect UUS for the Nortel North American PRI variant (NI-2 PRI and NTNA DMS PRI) only.
- The CS2K validates UUS subscription for ISDN PRI call originations only.
- When the CS2K receives a UUI IE in a message that does not support UUI, the CS2K sends a Q.931 STATUS message response.
- When the CS2K discards the UUI IE from a Q.931 message, indication of this is only communicated to the far end (FE) of the PRI. Indication that the UUI IE was discarded (a Q.931 STATUS message) is not propagated along adjacent PRI trunk connections.

162.4 UUI over SCAI

162.4.1 Description

The first PRI SETUP message (Initial Address message; IAM in the case of ISUP) sent from the originating switch can contain UUI (User to User Information) parameter. The UUI is used by the terminating switch as call related data.

This feature ensures that UUI arriving over the following trunks is delivered to the ICM environment.

1. NI2 PRI

2. NTNA PRI

3. ANSI ISUP

This activity will provide the UUI in ICM messages for the following agent types:

1. ACD agents
2. MDC agents
3. RES agents.

UUI IE from CS2K to the SCAI host will only be reflected in all the will be in every DV_Call_Queued_U, DV_Call_Offered_U and DV_Call_Received_C message.

162.4.2 Modified ICM Messages

This feature introduces a new parameter, namely **UUIPARM** in the following ICM call related messages.

- DV_Call_Queued_U
- DV_Call_Offered_U
- DV_Call_Received_C

The ASN.1 notations for the above mentioned three messages for ACD customer provided by this activity are shown in this section. The length fields are variable because the length depends on the variable contents. The tag values are taken from the Remote Operation Service Element (ROSE) protocol.

The maximum length of UUI supported by the new parameter is 128 bytes. The new parameter will show up in the above said messages on the basis of the appropriate subscription which will be discussed later.

The UUI is supported in the above-mentioned four messages for a SCAI-monitored terminator only.

- **SCAI19 Service Version**
  - — The ICM application Logon message contains a parameter; service Version, which is used to identify the stream of messages which will be allowed across the link. This service version is used as a method of protecting the integrity of host applications which choose not to upgrade their software to accept new message types after a switch has been upgraded to a new service version.
  - — The new service version SCAI19 needs to be added to the current list of SCAI service versions to receive modified messages with new parameter. The new service version is accepted at application logon processing time. The processing of individual messages which are introducing new encoding / decoding, adheres to the Service Version of ICM.

Note: *The parameters which are* ***italicized and bold*** *are new to these messages.The letter 'U' in the message name indicates that the message is unconfirmed, i.e., this operation requires no outcome to be reported by the host. The letter '****C****' at the end of the message's name indicates that the message requires confirmation from the host.*

162.4.2.1 DV_Call_Queued_U message

The switch sends this Remote Operation of Class 5 to the host when a call to an ACD DN associated with the current session is received by the switch and placed in the Incoming Call Queue.

162.4.2.1.1 Changed DV_Call_Queued_U ASN.1 definition.

ASN.1 Encoding

```
dv-CALL-QUEUED-U ARGUMENT        OPERATION

                                 ARGUMENT CallQueuedArgument ::=
6

    CallQueuedArgument                  ::=     SEQUENCE
     {networkCallID          [0] IMPLICIT SEQUENCE
     {networkNodeID                  [0] IMPLICIT INTEGER OPTIONAL,
     localCallID                     [1] IMPLICIT INTEGER OPTIONAL}
                                     OPTIONAL,

    acdDN                   [1] IMPLICIT OCTET STRING OPTIONAL,
    origCallingNumber       [2] IMPLICIT OCTET STRING OPTIONAL,
    origChargeNumber        [3] IMPLICIT OCTET STRING OPTIONAL,
    callHistoryInfo         [4] IMPLICIT SEQUENCE

     {callType              [0] IMPLICIT  ENUMERATED
          {callTransferred          (1),
          callOverflowed            (2),
          callRedirected            (3),
          callForwarded             (4)
          callConsult               (5),
          callConference            (6),
          callReturnedToQueue       (7),
          callRouted                (8)} OPTIONAL,

    origInboundDN           [1] IMPLICIT OCTET STRING OPTIONAL,
    prevApplicationID       [2] IMPLICIT INTEGER OPTIONAL,
    hostCallData            [3] IMPLICIT OCTET STRING OPTIONAL}
                            OPTIONAL,

    acdGroup                [5] AddressType OPTIONAL,
    forwardingParty         [6] ForwardingPartyType OPTIONAL,
    cpadigs                 [7] IMPLICIT OCTET STRING OPTIONAL
    uuiParameter            [8] IMPLICIT OCTET STRING OPTIONAL}


    AddressType:: = CHOICE
    {positionID             [0] IMPLICIT INTEGER,
```

```
 dialedDigits                [1] IMPLICIT IA5STRING,
 stationNumber               [2] IMPLICIT OCTET STRING,
 q931Address                 [3] Q931AddressType}

Q931 AddressType                    :: =     SEQUENCE
{numberTypeNumberPlan               [0] OCTET STRING OPTIONAL,
 presentationScreeningIndicator     [1] OCTET STRING OPTIONAL,
 digits                             [2] IA5 STRING OPTIONAL}


ForwardingPartyType                 :: =     IMPLICIT SEQUENCE
{firstFwdNumber                     [0] AddressType OPTIONAL,
 firstFwdReason                     [1] IMPLICIT ENUMERATED
 {unknown                           (0),
 userBusy                           (1),
 noReply                            (2),
 unconditional                      (3)  }   OPTIONAL,
 lastFwdNumber                      [2] AddressType OPTIONAL,
 lastFwdReason                      [3] IMPLICIT ENUMERATED
 {unknown                           (0),
 userBusy                           (1),
 noReply                            (2),
 unconditional                      (3)  }   OPTIONAL},
```

162.4.2.1.2 DV_Call_Queued_U:Coded example.

An ACD call has been initiated from the OrigCallingNumber 6136217703 with UUI '01 02 03 04 05 06 07 08 09 0a', by dialing 6134444444 and assigned a LocalCallID = 13, and offered it to an ACD group with Primary DN 6136212111, for which no agent is available, the call is placed in the Incoming Call Queue and the switch sends DV-CALL-QUEUED-U to the host. No Return Result is required or received by the switch from the host.

INVOKE **CS2K ===== > HOST**

Hex Dump			Information Element	Comments
Tag	**Length**	**Content**		
a1	54		INVOKE	Message length is 84 bytes decimal
02	02	03 ff	InvokeID	The InvokeID is 1023
02	01	06	Operation	Operation value for DV-CALL-QUEUED-U is decimal 6
30	4b		Argument	CallQueued argument is of Sequence type and is 75 bytes long decimal

Hex Dump			Information Element	Comments
Tag	**Length**	**Content**		
a0	09		NetworkCallId	The NetworkCallId is a constructor of 9 bytes long
80	04	03 38 d0 90	NetworkNodeId	The NetworkNodeId is 54055056
81	01	0d	LocalCallId	The LocalCallId is 13
81	0a	36 3133 36 32 31 32 31 31 31	ACDDN	The called ACDDN of the Group is 6136212111
82	0c	00 83 36 31 33 36 32 31 37 37 30 33	Original Calling Number	The first 2 bytes are fixed and must not be read at present. The original calling number is 6136217703
A5	0c		Acd group	The ACDGroup is of type Constructor and is 12 bytes long
82	0a	36 31 33 36 32 31 32 31 31 31	Station number	The station number of the ACDGroup is 6136212111
87	0a	36 31 33 34 34 34 34 34 34 34	CPADIGS	The CPA value is 6134444444
88	**0a**	**01 02 03 04 05 06 07 08 09 0a**	**UUI**	**The UUI IE data is '01 02 03 04 05 06 07 08 09 0a'.**
Hex Dump= a1 54 02 02 03 ff 02 01 06 30 4b a0 09 80 04 03 38 d0 90 81 01 0d 81 0a 36 31 33 36 32 31 32 31 31 31 82 0c 00 83 36 31 33 36 32 31 37 37 30 33 a5 0c 82 0a 36 31 33 36 32 31 32 31 31 31 87 0a 36 31 33 34 34 34 34 34 34 34 88 0a 01 02 03 04 05 06 07 08 09 0a				

162.4.2.2 DV_Call_Offered_U message

This section describes the DV-CALL-OFFERED-U message the switch uses to notify the host that a ICM Party has been selected for ACD. The party has been selected to handle an incoming call to one of the DNs belonging to the associated environment of the current switch-host session when the call is about to be offered to the ICM Party.

162.4.2.2.1 Changed DV_Call_Offered_U ASN.1 definition.

ASN.1 Encoding

```
dv-CALL-OFFERED-U                    OPERATION

                                     ARGUMENT CallOfferedArgument ::= 5

CallOfferedArgument                  ::=     SEQUENCE
 {networkCallID                  [0] IMPLICIT SEQUENCE
 {networkNodeID                      [0] IMPLICIT INTEGER OPTIONAL,
 localCallID                         [1] IMPLICIT INTEGER OPTIONAL}
                                     OPTIONAL,
acdDN                            [2] IMPLICIT OCTET STRING OPTIONAL,
origCallingNumber                [3] IMPLICIT OCTET STRING OPTIONAL,
origChargeNumber                 [4] IMPLICIT OCTET STRING OPTIONAL,
callHistoryInfo                  [5] IMPLICIT SEQUENCE

 {callType                       [0]  IMPLICIT  ENUMERATED
    {callTransferred             (1),
     callOverflowed              (2),
     callRedirected              (3),
     callForwarded               (4)
     callConsult                 (5),
     callConference              (6),
     callReturnedToQueue         (7),
      callRouted                 (8)} OPTIONAL,

 origInboundDN    [1] IMPLICIT DeviceAddressType OPTIONAL,
 prevApplicationID[2] IMPLICIT INTEGER OPTIONAL,
 hostCallData     [3] IMPLICIT OCTET STRING OPTIONAL}
                      OPTIONAL,

acdGroup         [6] AddressType OPTIONAL,
callMode         [7] IMPLICIT ENUMERATED

{callWaited      (1)}    OPTIONAL,
destDeviceID     [8] AddressType OPTIONAL,
forwardingParty  [9] ForwardingPartyType OPTIONAL,
cpadigs          [10] IMPLICIT OCTET STRING OPTIONAL
uuiParameter     [11]IMPLICIT OCTET STRING OPTIONAL}


AddressType                          :: =    CHOICE
{positionID      [0] IMPLICIT INTEGER,
dialedDigits     [1] IMPLICIT IA5STRING,
stationNumber    [2] IMPLICIT OCTET STRING,
```

```
q931Address        [3] Q931AddressType}

Q931AddressType                 :: =      SEQUENCE
{numberTypeNumberPlan           [0] OCTET STRINGOPTIONAL,
 presentationScreeningIndicator [1] OCTET STRINGOPTIONAL,
 digits                         [2] IA5 STRING OPTIONAL}

ForwardingPartyType             :: =      IMPLICIT SEQUENCE
{firstFwdNumber                 [0] AddressTypeOPTIONAL,
 firstFwdReason                 [1] IMPLICIT ENUMERATED
{unknown                        (0),
 userBusy                       (1),
 noReply                        (2),
 unconditional                  (3)} OPTIONAL,

 lastFwdNumber                  [2] AddressType OPTIONAL,
 lastFwdReason                  [3] IMPLICIT ENUMERATED
{unknown                        (0),
 userBusy                       (1),
 noReply                        (2),
 unconditional                  (3)  }   OPTIONAL}
```

162.4.2.2.2 DV_Call_Offered_U: Coded example.

An ACD call is initiated from the OrigCallingNumber 6136217703 with UUI '01 02 03 04 05 06 07 08 09 0a' in setup message by dialing 6134444444 and is assigned a LocalCallID = 9. The call is offered to an acd agent with posid 7707 of the acd group with primary DN 613621111. The switch sends DV-CALL-OFFERED-U to the host. No Return Result is required or received by the switch from the host.

INVOKE **CS2K ===== > HOST**

Hex Dump			Information Element	Comments
Tag	**Length**	**Content**		
a1	5a		INVOKE	this message is 90 bytes decimal
02	02	03 f9	InvokeID	the InvokeID is 1017
02	01	05	Operation	the operation is DV-CALL-OFFERED-U [5]
30	51		Argument	CallOffered argument is of Sequence type and is 81 bytes long decimal
a0	09		NetworkCallId	The NetworkCallId is a constructor 9 bytes

Hex Dump			Information Element	Comments
Tag	**Length**	**Content**		
80	04	03 38 d0 90	NetworkNodeId	The NetworkNodeId is 54055056
81	01	09	LocalCallId	The LocalCallId is 9 decimal
82	0a	36 31 33 36 32 31 32 31 31 31	acd_dn	6136212111
83	0c	00 83 36 31 33 36 32 31 37 37 30 33	OrigCallingNumber	The first two bytes are fixed and presently must not be read.The customer's OrigCallingNumber is 6136217703
a6	0c		acd_grp	
82	0a	36 31 33 36 32 31 32 31 31 31	StationNumber	The called DN is 6136212111
a8	04		DeviceID	The DeviceID is of type Constructor and is 4 bytes long
80	02	1e 1b	pos_id_2	7707
8a	0a	36 31 33 34 34 34 34 34 34 34	CPADIGS	The CPA value is 6134444444
8b	**0a**	**01 02 03 04 05 06 07 08 09 0a**	**UUI**	**The UUI IE data is '01 02 03 04 05 06 07 08 09 0a'.**
Hex Dump = a1 5a 02 02 03 f9 02 01 05 30 51 a0 09 80 04 03 38 d0 90 81 01 09 82 0a 36 31 33 36 32 31 32 31 31 31 83 0c 00 83 36 31 33 36 32 31 37 37 30 33 a6 0c 82 0a 36 31 33 36 32 31 32 31 31 31 a8 04 80 02 1e 1b 8a 0a 36 31 33 34 34 34 34 34 34 34 8b 0a 01 02 03 04 05 06 07 08 09 0a				

162.4.2.3 DV_Call_Received_C message

The switch uses the DV-CALL-RECEIVED-C message to notify the host that a call to an ACD group belonging to an Associated environment with which the host has an established session has been received. This allows the host to "redirect" the call.

162.4.2.3.1 Changed DV_CALL_Received_C ASN.1 definition.

ASN.1 Encoding

```
dv-CALL-RECEIVED-C          OPERATION
                            ARGUMENT  CallReceivedArgument
                            RESULT
                            ERRORS      {call-Received-Error}
                            LINKED {dv-CALL-REDIRECT} ::=
10

CallReceivedArgument              ::=       SEQUENCE
 {networkCallID             [0] IMPLICIT SEQUENCE
 {networkNodeID                   [0] IMPLICIT INTEGER OPTIONAL,
 localCallID                      [1] IMPLICIT INTEGER OPTIONAL}
                           OPTIONAL,
acdDN                      [1] IMPLICIT OCTET STRING OPTIONAL,
origCallingNumber          [2] IMPLICIT OCTET STRING OPTIONAL,
origChargeNumber           [3] IMPLICIT OCTET STRING OPTIONAL,
callHistoryInfo            [4] IMPLICIT SEQUENCE

 {callType                 [0]  IMPLICIT  ENUMERATED
    {callTransferred       (1),
     callOverflowed        (2),
     callRedirected        (3),
     callForwarded         (4)
     callConsult           (5),
     callConference        (6),
     callReturnedToQueue (7),
      callRouted           (8)} OPTIONAL,
          origInboundDN                                  [1]
IMPLICIT OCTET STRING
OPTIONAL,
prevApplicationID                [2] IMPLICIT INTEGER OPTIONAL,
hostCallData                     [3] IMPLICIT OCTET STRING
                                                  OPTIONAL}
                           OPTIONAL,
acdGroup                   [5] AddressType OPTIONAL,
forwardingParty            [6] ForwardingPartyType OPTIONAL,
cpadigs                    [7]IMPLICIT OCTET STRING OPTIONAL
uuiParameter               [8]IMPLICIT OCTET STRING
OPTIONAL}


AddressType                      :: =      CHOICE
 {positionID               [0] IMPLICIT INTEGER,
 dialedDigits              [1] IMPLICIT IA5STRING,
 stationNumber             [2] IMPLICIT OCTET STRING,
 q931Address               [3] Q931AddressType}

Q931AddressType                  :: =      SEQUENCE
```

```
{numberTypeNumberPlan          [0] OCTET STRING OPTIONAL,
presentationScreeningIndicator [1] OCTET STRING OPTIONAL,
digits                         [2] IA5 STRING OPTIONAL}

ForwardingPartyType            :: =     IMPLICIT SEQUENCE
{firstFwdNumber                [0] AddressType OPTIONAL,
firstFwdReason                 [1] IMPLICIT ENUMERATED
{unknown                       (0),
userBusy                       (1),
noReply                        (2),
    unconditional               (3)  }  OPTIONAL,
lastFwdNumber                  [2] AddressType OPTIONAL,
lastFwdReason                  [3] IMPLICIT ENUMERATED
{unknown                       (0),
userBusy                       (1),
noReply                        (2),
unconditional                  (3)  }   OPTIONAL}

call-Received-ErrorERROR::= 0
```

162.4.2.3.2 DV_Call_Received_C: Coded example.

An ACD call has been initiated from the OrigCallingNumber 9192466001, with UUI in setup by dialing 9197224444 and assigns a LocalCallID = 4 to the call meant for ACD group with Primary DN of the ACD group =9194815200. The switch sends DV-CALL-RECEIVED-C message to the host which responds with either Return Result message or Return Error message.

INVOKE CS2K ===== > HOST

Hex Dump			Information Element	Comments
Tag	**Length**	**Content**		
a1	51		INVOKE	this message is 81 bytes decimal
02	02	03 f9	InvokeID	the InvokeID is 1017 decimal
02	01	0a	Operation	the operation is DV-CALL-RECIEVED-C[10] decimal
30	48		Argument	CallReceived argument is of Sequence type and is 72 bytes long decimal
a0	06		NetworkCallId	the NetworkCallId is a constructor 6 bytes
80	01	00	NetworkNodeId	the NetworkNodeId is 0
81	01	04	LocalCallId	the LocalCallId is 4

Hex Dump			Information Element	Comments
Tag	**Length**	**Content**		
81	0a	39 31 39 34 38 31 35 32 30 30	ACDDN	the called ACDDN is 9194815200
82	0c	00 83 39 31 39 32 34 36 36 30 30 31	OrigCallNumber	the first two bytes are fixed and presently unused. The customer's OrigCallNumber is 9192466001
a5	0c		ACDGroup	the ACDGroup is a type constructor 12 bytes
82	0a	39 31 39 34 38 31 35 32 30 30	StationNumber	the customer group's Primary ACDDN is 9194815200
87	0a	39 31 39 37 32 32 34 34 34 34	CPADIGS	The CPA value is 9197224444
88	**0a**	**01 02 03 04 05 06 07 08 09 0a**	**UUI**	**The UUI IE data is '01 02 03 04 05 06 07 08 09 0a'**
Hex Dump= a1 51 02 02 03 f9 02 01 0a 30 48 a0 06 80 01 00 81 01 04 81 0a 39 31 39 34 38 31 35 32 30 30 82 0c 00 83 39 31 39 32 34 36 36 30 30 31 a5 0c 82 0a 39 31 39 34 38 31 35 32 30 30 87 0a 36 31 33 37 32 32 34 34 34 34 88 0a 01 02 03 04 05 06 07 08 09 0a				

162.4.3 Size expansion of ICM messages

The size of outgoing ICM messages will be increased from the existing 256 bytes to 512 bytes. The increased size will be available for TCP/IP link set only. For X.25 link sets, the maximum available size will be 241 bytes.

If the size of a message with UUI parameter becomes greater than 241 bytes in X.25 link set, then the UUI will be discarded from the message and the message will be sent with the remaining parameters. In such scenarios, a SCAI LOG 304 will be generated indicating the removal of UUI.

Note: It is recommended to upgrade from X.25 to TCP/IP to get the full use of UUI over the SCAI link.

162.4.4 Subscription

The following changes in table SCAISSRV are required to provide subscription to receive ICM messages with the new parameter. Preconditions to be satisfied by a party in order to receive all the messages with new parameter are also given in this section.

162.4.4.1 Changes in table SCAISSRV

The changes in table SCAISSRV are made for the following SCAI messages:

- DV_Call_Received_C
- DV_Call_Queued_U
- DV_Call_Offered_U

An optional parameter UUIPARM is added to the existing parameters in the function CALLQUED, CALLOFFR and CALLRECDC which are present in the following categories: CTXEVENT, RESEVENT, ROUTING and ACDEVENT messages in table SCAISSRV.

During the software upgrade, the existing tuples of table SCAISSRV which are present in loads prior to the introduction of the aforementioned four tuples, would be modified by reformat procs during table transfer to reflect UUIPARM parameter in the functions CALLQUED, CALLOFFR and CALLRECDC as ‘N’.

Following are the sample tuples shown:

```
TABLE SCAISSRV
 SUBSERV SPROFILE
 ------------------------------------------------
 ACDEVENT15$ ACDEVENT (CALLQUED Y Y Y Y Y Y Y Y Y Y Y N)
 (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y N)
 (CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLREL Y Y Y Y Y Y) (AGTLGDIN Y Y Y) (AGTLGDOUT Y Y)
 (AGTREADY Y Y)
 (AGTNREADY Y Y N) (LOBEVENT Y Y Y) (EMKEVENT Y Y Y Y Y Y)
```

```
TABLE SCAISSRV
 SUBSERV SPROFILE
 ------------------------------------------------

ROUTING15$ ROUTING (CALLRECDC Y Y Y Y Y Y Y Y Y Y Y N)
(CALLREDIR Y Y Y) $
```

A new default tuple CTXEVENT19$ under category CTXEVENT will be created with the optional parameter UUIPARM of the function CALLOFFR set to Y. Prior to this, the latest default tuple in the category CTXEVENT is CTXEVENT13$.

A new default tuple RESEVENT19$ under category RESEVENT will be created with the optional parameter UUI of the function CALLOFFR set to Y. Prior to this, the latest default tuple in the category RESEVENT is RESEVENT13$.

A new default tuple ROUTING19$ under category ROUTING will be created with the optional parameter UUI of the function CALLRECDC set to Y. Prior to this, the latest default tuple in the category ROUTING is ROUTING15$.

A new default tuple ACDEVENT19$ under category ACDEVENT will be created with the optional parameter UUIPARM of the function CALLQUED, and CALLOFFR set to Y. Prior to this, the latest default tuple in the category ACDEVENT is ACDEVENT15$.

Table 5 SCAISSRV table changes

Category	Function	Added Parameters	New/Same
CTXEVENT	CALLOFFER / CALLANSWR	UUIPARM	Old function and new parameter
RESEVENT	CALLOFFER / CALLANSWR	UUIPARM	Old function and new parameter
ROUTING	CALLRECDC	UUIPARM	Old function and new parameter
ACDEVENT	CALLQUED / CALLOFFER / CALLANSWR	UUIPARM	Old function and new parameter

```
TABLE SCAISSRV
 SUBSERV SPROFILE
 ------------------------------------------------
 CTXEVENT19$ CTXEVENT (SETOFFHK Y Y Y)
 (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLREL Y Y Y Y)
 (CALLNAME Y Y Y Y Y) $



TABLE SCAISSRV
 SUBSERV SPROFILE
 ------------------------------------------------
 RESEVENT19$ RESEVENT (SETOFFHK Y Y)
 (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLREL Y Y Y)
 (CALLNAME Y Y Y Y Y) $



TABLE SCAISSRV
 SUBSERV SPROFILE
 ------------------------------------------------

 ROUTING19$ ROUTING (CALLRECDC Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLREDIR Y Y Y) $



TABLE SCAISSRV
 SUBSERV SPROFILE
 ------------------------------------------------
 ACDEVENT19$ ACDEVENT (CALLQUED Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLREL Y Y Y Y Y Y) (AGTLGDIN Y Y Y) (AGTLGDOUT Y Y)
 (AGTREADY Y Y)
 (AGTNREADY Y Y N) (LOBEVENT Y Y Y) (EMKEVENT Y Y Y Y Y Y)
```

162.4.4.2 Preconditions to receive the modified ICM messages.

- The state SOC ICM00083 should be ON.
- A party must be a ACD DN or ECM associated in order to get the modified messages.
- The Service Version should at least be SCAI19.
- The ICM session on which the DV_Call_Queued_U message is to be sent with the new parameter must subscribe to the ACDEVENT category and CALLQUED function. Also the parameter ***UUIPARM*** in the function CALLQUED must be set to ***Y***.
- The ICM session on which the DV_Call_Offered_U message is to be sent with the new parameter must subscribe to either ACDEVENT, CTXEVENT or RESEVENT category and CALLOFFR function. Also the parameter ***UUIPARM*** in the function CALLOFFR must be set to ***Y*** and ***UUIPARM*** in function CALLQUED and CALLRECDC must be set to N.
- The ICM session on which the DV_Call_Received_C message are to be sent with the new parameter must subscribe to the ROUTING category and CALLRECDC function. Also the parameter ***UUIPARM*** in the function CALLRECDC must be set to ***Y***.

162.4.5 Message Flow Scenarios

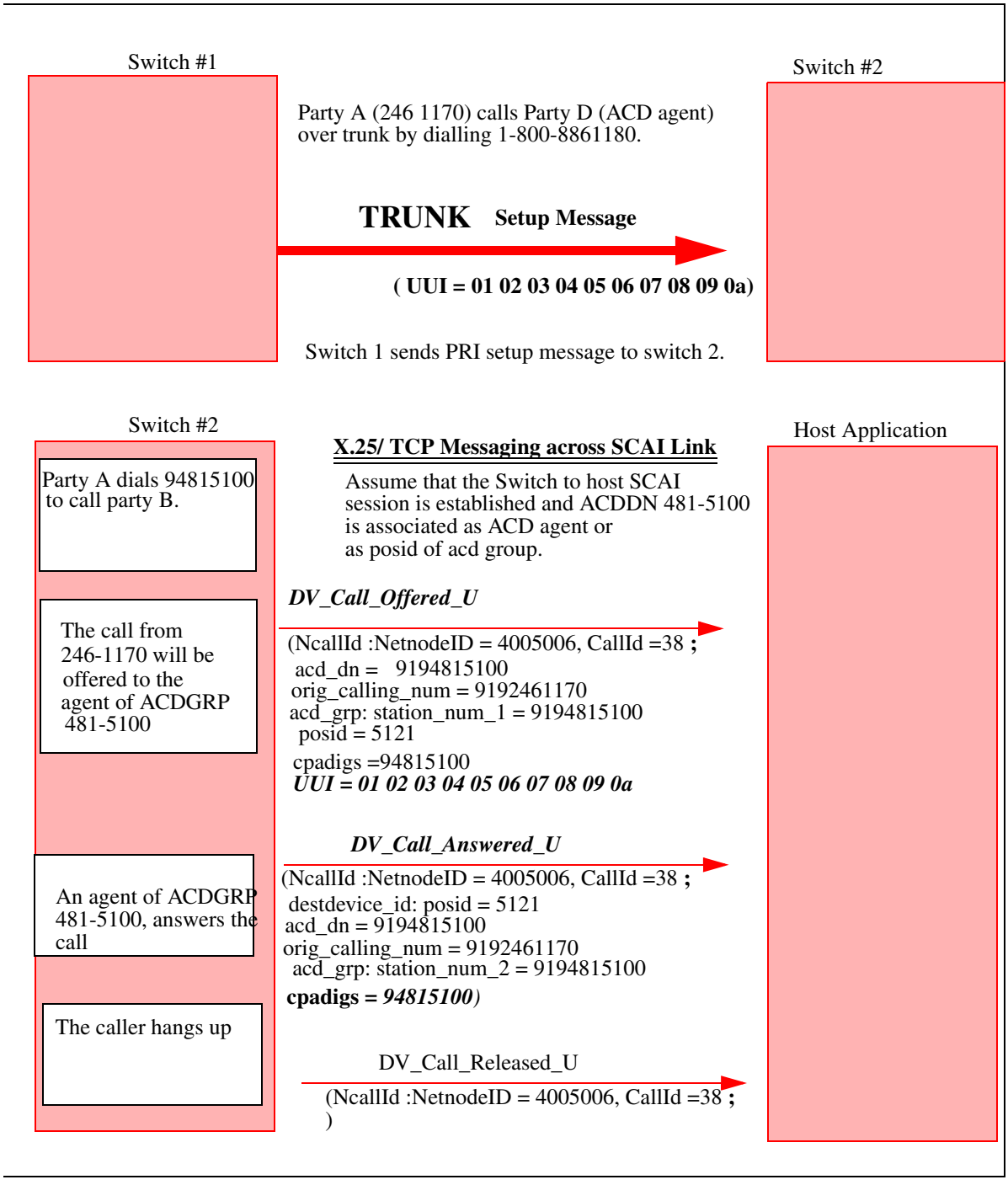
Consider some message flow scenarios to get better understanding of the feature. In all the scenarios mentioned below, assume the following, unless stated otherwise:

1. *Parties B, C and D are always ECM associated ACD/MDC/RES agents.*
2. *Parties B and C belong to same switch.*
3. *Party A is any agent that requires service from a call centre and may be on the same network or a different network.*
4. *All the preconditions mentioned in section Please refer to "161.4.4.2 Preconditions to receive the modified ICM messages." on page 1616. are satisfied by all the parties.*
5. *The modified messages are shown in bold and italics.*
6. *The messaging that remains the same may not been shown explicitly.*
7. *The term trunks mean any of the trunks mentioned in section Please refer to "161.4.1 Description" on page 1602..*
8. *In all the scenarios, the statement 'party A calls party B/D' is to be interpreted as 'party A dials to reach a call centre and the call terminates to agents B/D within that call centre'.*

162.4.5.1 Example 1: UUI IE in DV_Call_Offered_U

Party A (2461170) calls party B (ACD agent of ACDGRP 4815100, posid: 5121) over PRI/ISUP trunk and party B answers.

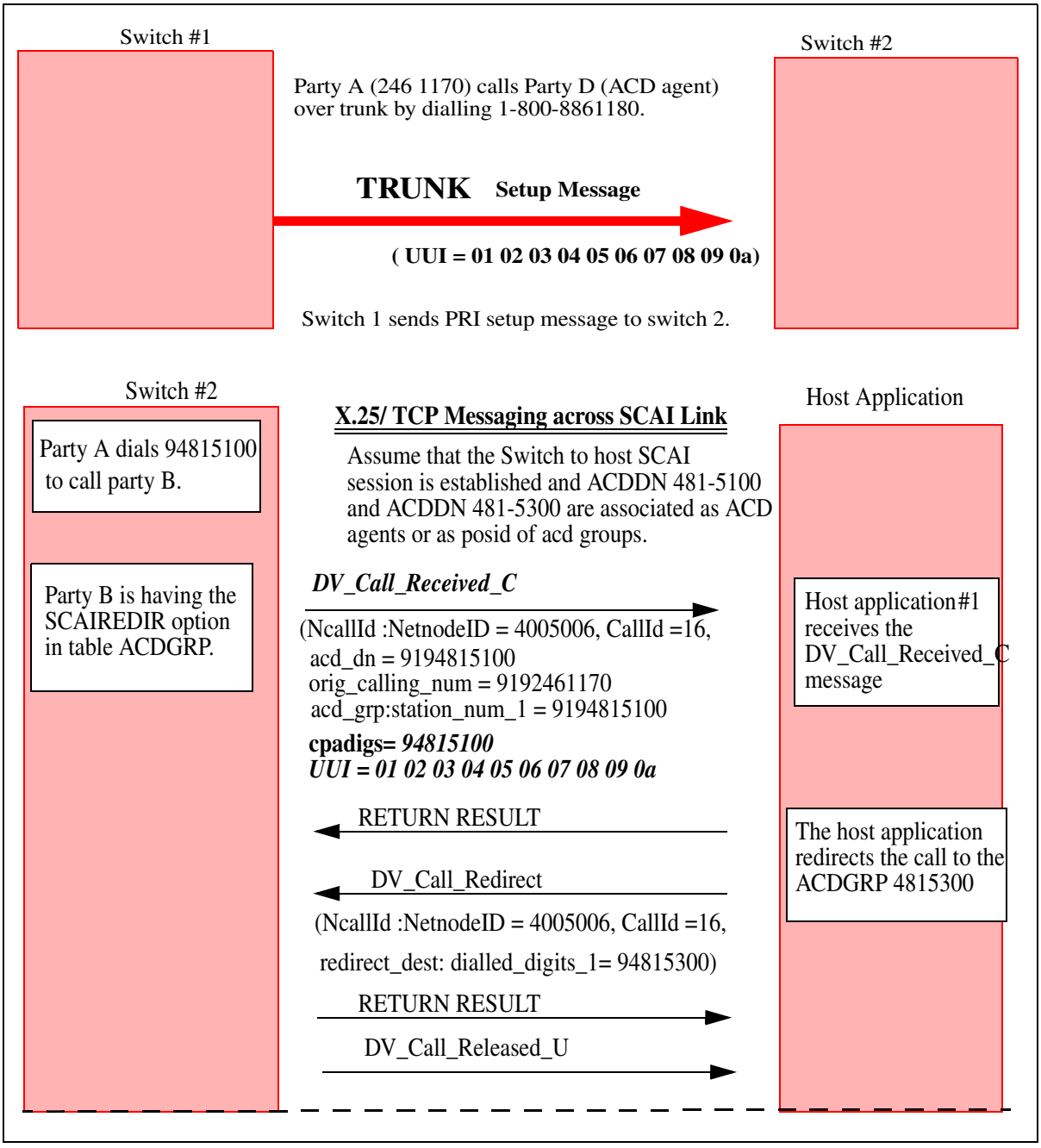
Figure 2 UUI in DV_Call_Offered_U



162.4.5.2 Example 2: UUI IE in DV_Call_Received_C message

Party A (2461170) calls party B (ACD agent of ACDGRP 4815100, posid: 5121) over PRI/ISUP trunk and party B answers.

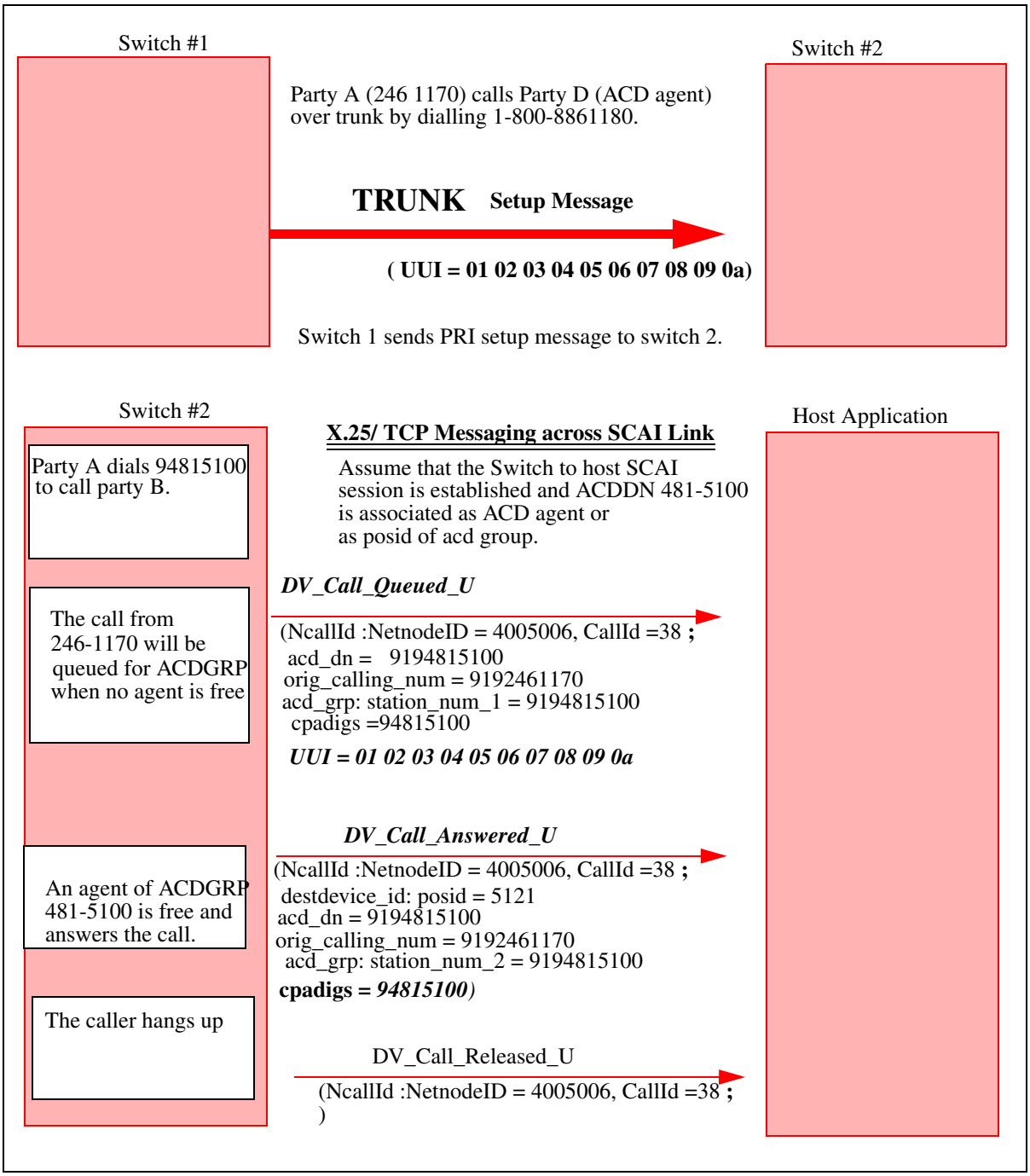
Figure 3 UUI in DV_Call_Received_C message



162.4.5.3 Example 3: UUI IE in DV_Call_Queued_U

Party A (2461170) calls party B (ACD agent of ACDGRP 4815100, posid: 5121) over ISUP/PRI and party B answers.

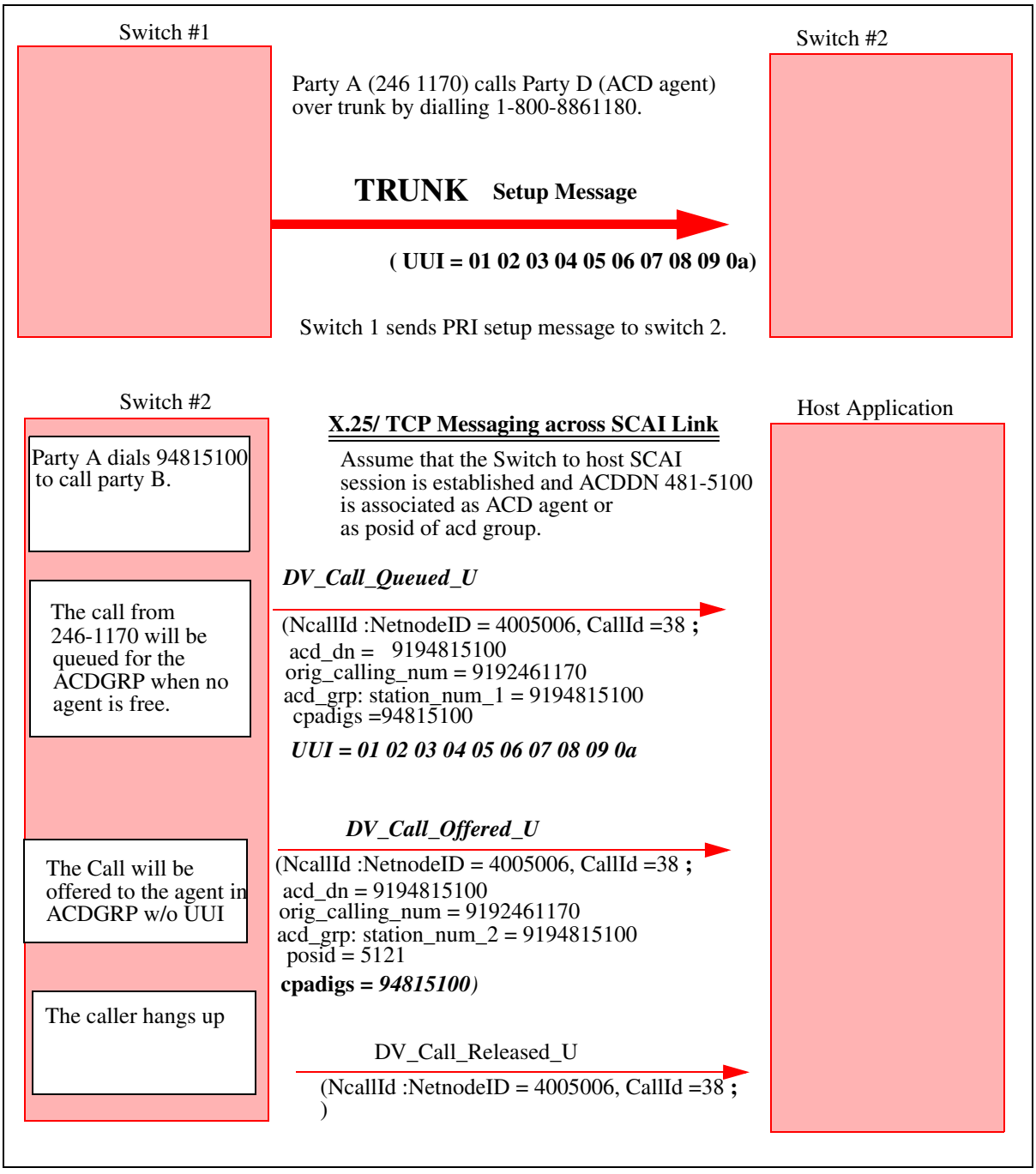
Figure 4 UUI in DV_Call_Queued_U



162.4.5.4 Example 4: UUI IE not in DV_Call_Offered_U

Party A (2461170) calls party B (ACD agent of ACDGRP 4815100, posid: 5121) over ISUP/PRI and party B answers.

Figure 5 UUI in DV_Call_Queued_U



162.4.6 SOC

The UUI IE data delivery to SCAI is controlled by state SOC ICM00083. The UUI IE data is delivered to the SCAI host only if the SOC is turned on and the sub service supporting UUI is subscribed.

In case a call over a ISUP/NI2 PRI trunk with UUI IE terminates on a SCAI monitored agent and the SOC ICM00083 is IDLE, the UUI shall not be delivered to the SCAI host even if the profile in SCAIPROF is subscribed to the subservice with support for UUI.

The SOC functionality shall be available in SN10 and SN09 Drop II shall have the functionality as an activatable patch. When CS2K with patch CFZ40 activated on SN09 upgrades to SN10 or higher release, the SOC Option ICM00083 will be automatically turned ON during ONP.

Note: The delivery of UUI IE over incoming NI-2 PRI or ANSI ISUP messages will not be SOC controlled.

162.4.7 Logs

If the total size of the outgoing ICM message with UUI exceeds the maximum supported size of outgoing ICM message then the UUI IE will be discarded and LOG SCAI 304 will be generated.

162.5 Hardware Requirements or Dependencies

Not Applicable

162.6 Software Requirements or Dependencies

Not Applicable

162.7 Limitations and restrictions

This feature does not ensure the correct UUI IE population for the protocol variants other than those specified

162.8 Interactions

Not Applicable

162.9 Applicable customer facing sections

162.9.1 Fault Management

162.9.1.1 Logs (LG)

SCAI 304: The snapshot of the log is given below:

RSNN10AG SCAI304 JAN14 22:30:56 5348 INFO UUIPARM DISCARDED
MESSAGE: DV-CALL-QUEUED-U

LINK ID : DNA: 000000000000000 PROTOCOL: 1 1 1 1
DEVICE : MPC: 0 LINK: 3
SCAI GROUP: SCAI_GRP1
LINKSET NAME: X25_LNK1

SCAI304 log limitation: There are certain scenarios in which the SCAI304 log will be generated with LINK ID, DEVICE ID and LINKSET NAME set as unavailable. This happens when the queue used to transmit the message to the SCAI host is decided at a later stage. That is, the queue information is available only at a later stage after the UUI parameter is discarded. The queue information is needed to get the LINK ID, DEVICE ID and LINKSET NAME details.

162.9.2 Configuration

162.9.2.1 Data schema (DS)

Figure 6 Data Schema changes in Tables LTDATA and SCAISSRV

```
 TABLE LTDATA
LTDKEY LTDRSLT
-----------------
ISDN 641 SERV SERV N N ALWAYS ALWAYS (UUS) $


TABLE SCAISSRV
 SUBSERV SPROFILE
 ------------------------------------------------
 CTXEVENT19$ CTXEVENT (SETOFFHK Y Y Y)
 (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLREL Y Y Y Y)
 (CALLNAME Y Y Y Y Y) $


TABLE SCAISSRV
 SUBSERV SPROFILE
 ------------------------------------------------
 RESEVENT19$ RESEVENT (SETOFFHK Y Y)
 (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLREL Y Y Y)
 (CALLNAME Y Y Y Y Y) $


TABLE SCAISSRV
 SUBSERV SPROFILE
 ------------------------------------------------

 ROUTING19$ ROUTING (CALLRECDC Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLREDIR Y Y Y) $


TABLE SCAISSRV
 SUBSERV SPROFILE
 ------------------------------------------------
 ACDEVENT19$ ACDEVENT (CALLQUED Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLREL Y Y Y Y Y Y) (AGTLGDIN Y Y Y) (AGTLGDOUT Y Y)
 (AGTREADY Y Y)
```

162.9.2.2 User Interface

Not applicable

162.9.2.3 Element Management
Not applicable

162.9.2.4 Alarms
Not applicable

162.9.2.5 Security
Not applicable

162.9.2.6 Office Parameters
Not applicable

162.9.2.7 Service orders (SO)
Not applicable.

162.9.3 Man machine interface (MM)
Not applicable.

162.9.4 Operational measurements (OM)
Not Applicable.

162.9.5 AMA/Billing information (AM)
Not Applicable.

162.9.6 Real-time
Not Applicable.

162.9.7 Engineering Information
Not Applicable

162.10 Glossary

Term	Description
UUI	User to User Information
UUS	User to User signalling
ACD	Automatic Call Distribution
SCAI	Switch-Computer Applications Interface
ICM	Intelligent Call Management
PRI	Primary Rate Interface
NI-2	National ISDN 2

Term	Description
XPM	eXtended Peripheral Module
GWC	GateWay Controller
SPM	Service Peripheral Module
SPCS	Stored Program Controlled switching System
IAM	Initial Address Message
ACM	Address Complete Message
ANM	ANswer Message
IAM	Initial Address Message
REL	RELease message
REL COM	RELease COMplete message
RO	Remote Operation
RES	Residential Enhanced Services
MDC	Meridian Digital Centrex
LCS	Local Concrete Syntax.
ISUP	ISDN User Part

163: Functional Description (FN) A00012570

163.1 Feature name and Feature ID

A00012570 - Disabling Non-secure Network Services in SSPFS

163.2 Description

When non-secure services within the operating system are not used, they should be disabled to close down any port(s) used by these services and reduce the exposures to security threats. Non-secure services such as ftp, tftp, telnet, SNMP and NFS may have secure equivalents. Therefore the use of the non-secure services can be disabled altogether when not in use. A configuration tool is required to selectively disable the non-secure services.

This activity provides some configuration tools to assist customers in configuring the server based on their security policy. Upon completion of the fresh system installation or upgrade, the customer (security administrator) has the possibility to apply the security policy on the server via a command line interface.

As part of this feature, non-secure network services not required by our product offerings (such as rpc in inetd.conf) will be disabled by default during initial system installation and upgrades.

This feature is targeted for all SSPFS platforms and profiles.

163.3 Hardware Requirements or Dependencies

Not applicable.

163.4 Software Requirements or Dependencies

Not applicable

163.5 Limitations and Restrictions

The following operating system services will be configurable/disabled by default on fresh install:

- List the RPC post IT.

This feature only provides configuration tools for services registered in the inetd.conf and the proftpd.conf files.

The configuration tools are only available to the root user.

Any services started under inittab, initd or the rpcd deamons are not affected.

163.6 Interactions

This feature interacts with any applications already deployed that makes use of the services listed above in section 2.5.

164: Functional Description (FN) A00012571

164.1 Feature name and Feature ID

A00012571 - CBM User Group Improvements

164.2 Description

This feature builds on two other CBM23 security features:

- A00012465 - CBM User Authorization Integration with a Nortel Central Security Server (Wireless application).
- A00012729 - CBM Application GID Migration.

A number of CBM maintenance commands require *root* (superuser) privileges. This is a security concern because it results in the wide distribution of the *root* password. This feature will eliminate the requirement to be the *root* user in order to do CBM maintenance procedures[1].

Currently there are only two authorization levels on the CBM: 1) the *root* user and 2) users belonging to the *maint* group. In this feature two new user groups will be created to eliminate the requirement for the *root* user and enable increased authorization granularity. The new groups are **emsadm** for system administration and **secadm** for security administration. While just these two groups will be added at this time, it will be possible to extend this feature in future releases and add additional groups.

The following table has a general summary of the CBM maintenance functions and the required authorization level. For more detail refer to later sections.

Table 1: Summary of Authorization Levels

Function	Root	emsadm	secadm	maint
Initial system installation	* *(1)*			
Application software install	*	*		
Software patching	*	*		
System upgrade	*			

[1]Initial installation of a CBM will still require the use of the root account (limitation imposed by Solaris).

Table 1: Summary of Authorization Levels

Function	Root	emsadm	secadm	maint
User Administration (create users, add users to groups, etc.)	*		*	
Application Configuration	*	*		*
Application State Change	*	*	*	*
view security logs	*		*	
Backup	*	*	*	*

This feature will extend the CBM maintenance MAP screens for user administration, including additional screens to:

- display list of groups and the users in a group
- display list of users and the groups they belong to
- create, change and remove users
- add/delete users to groups.

164.3 CBM User Shells

All CBM users regardless of their authorization levels will obtain a restricted shell after login to a CBM. The only exception to a restricted login shell is the root user.

A restricted shell will limit a user's ability to preform many system commands. A non-restricted shell is needed for administrative users to perform their functions. For users with administrative authorizations, they will able to obtain a non-restricted shell from a restricted login shell. For maintenance users who don't have administrative authorizations, they will be denied access to obtain a non-restricted shell.

The following shows how an emsadm user can obtain non-restricted shell access from the restricted login shell.

Figure 1 Get non-restricted shell from a restricted login shell

```
> ssh hems@47.135.214.81
Password:
Your password will expire in 29 days.
Last login: Sun Aug 21 21:15:47 2005
**************************************************************
**                                                          **
**                  This is a private database.             **
**                All activity is subject to monitoring.    **
**          Any UNAUTHORIZED access or use is PROHIBITED.   **
**                                                          **
**************************************************************
Rsh> fash
$
```

Security logs are generated when a user attempts to access a non-restricted shell from within the restricted login shell. Both successful and failure attempts are logged. The security logs for both the successful and failure scenarios are displayed as follows:

Successful access to non-restricted shell:

Aug 23 11:31:09 CBMDRY3 gen_security_log[21486]: class_security.ver02 EVENT.TYPE="USER_ACT_Security_Login" DOC="fash" STAT="Success" DST="CBMDRY3" DST.USR="hsec" SRC.OFFEND="47.129.112.179" HOST.TYPE="application" TTY="pts/4" MESSAGE=Access to non-restricted shell is granted MID="SDM_MID_defn.security.0010"

Failure attempt to access a restricted shell:

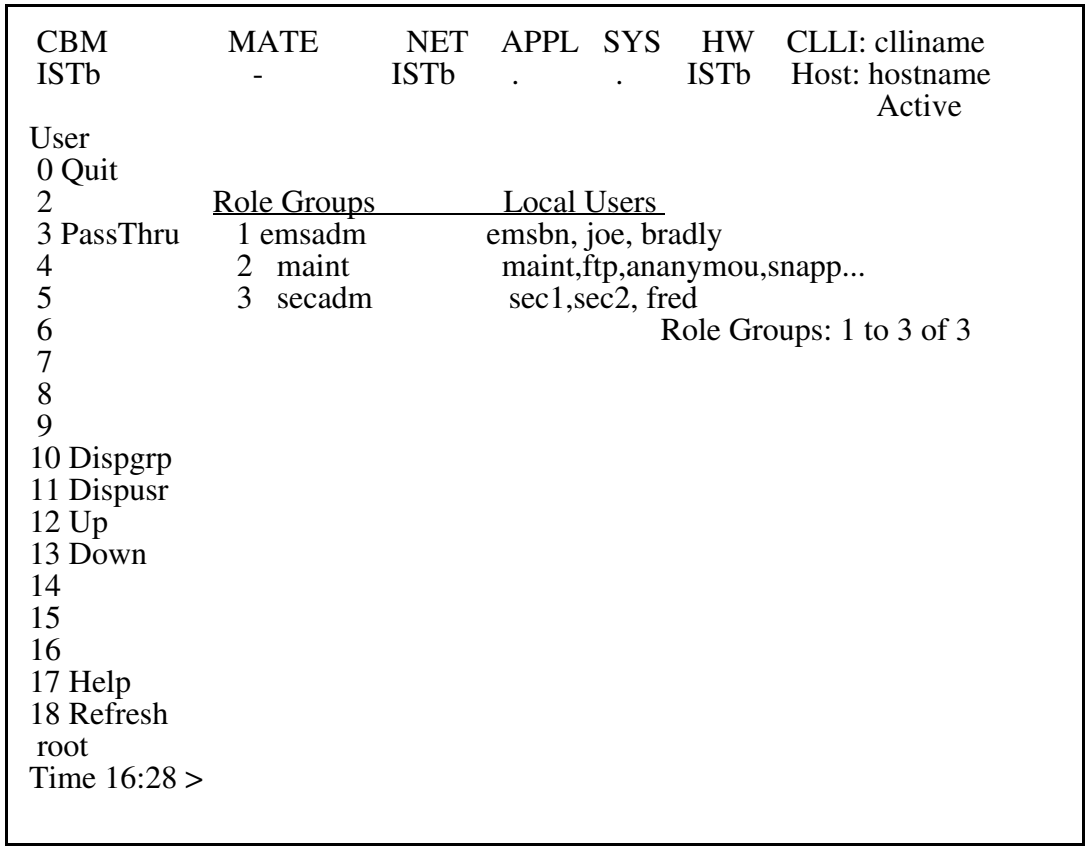
Aug 23 11:31:19 CBMDRY3 gen_security_log[21525]: class_security.ver02 EVENT.TYPE="USER_ACT_Security_Login" DOC="fash" STAT="Failure" DST="CBMDRY3" DST.USR="hmaint" SRC.OFFEND="47.129.112.179" HOST.TYPE="application" TTY="pts/3" MESSAGE=Access to non-restricted shell is denied MID="SDM_MID_defn.security.0010"

Note: The syntax of the above displayed logs is not finalized.

164.4 CBMMTC- User Menu Changes

The main menu for the user level of the CBMMTC will be changed to display all the Role groups and their users. From this menu “add”, “change” and delete will still be done as it was in previous releases. Some new commands have also been added to display more information about the role groups and users of the roles groups.

Figure 2 CBM user menu

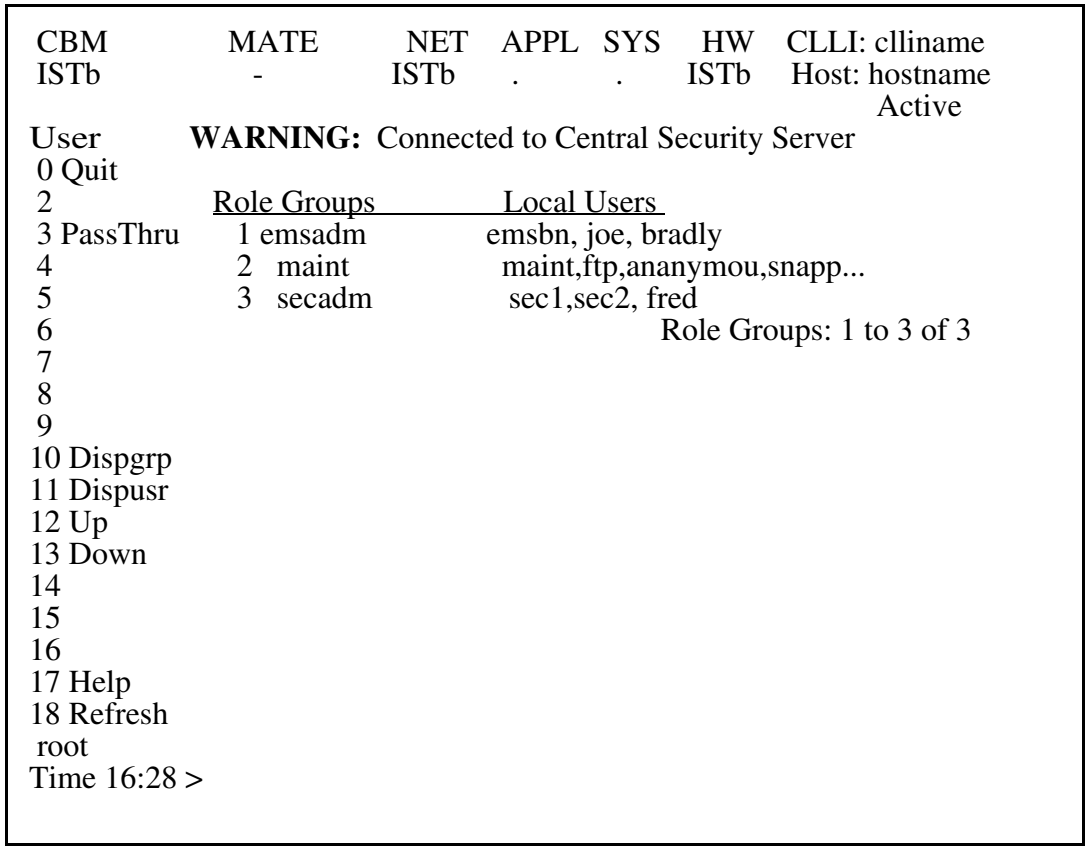


With this menu a user can be added, changed or deleted. To add a user to a group type: “add <username>”. If the user already exists locally or remotely, an error will be returned stating this. The user will be required to enter the main role group for the user as well as any other role groups the user is to belong to. To change the users information including password type “change <user>”. The user’s groups and/or password can now be changed. To remove the user from a group type: “delete <username>”. If the user does not exist, a error will be displayed. Only local user can be deleted from the RMI.

If a central security server is installed in the system a special warning will be displayed on the screen so that the user will know that any users create on the CBM are local to that CBM and will not appear on the Central security server.

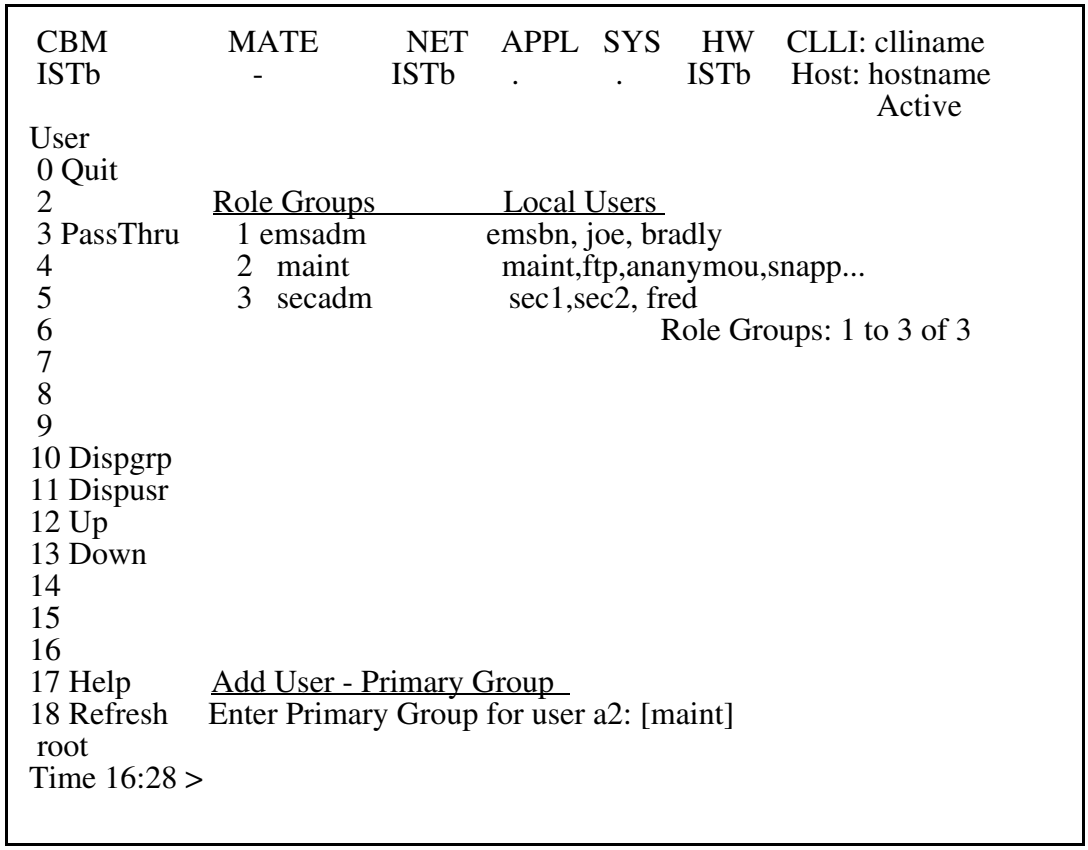
Also, any users that are created on the central security server will not appear on the local CBM menus. That is, remote users can not be viewed, added, changed or deleted. However, if a user is attempted to be created locally and it already exists on the central security server, the command will fail.

Figure 3 CBM user menu



The add and change options for users will display a new group of screens to allow the primary group, secondary groups and password for a new user to be added or changed. The following screens will be displayed for the add or change commands:

Figure 4 CBM "Add/Change" Primary Group prompt



At this prompt the user can either type a carriage return to accept the default which is "maint" in this case, as the user's primary group or type a different primary group. At this time the other choices are "secadm" and "emsadm".

The user will now be prompted to enter the secondary groups. The following screen will be displayed:

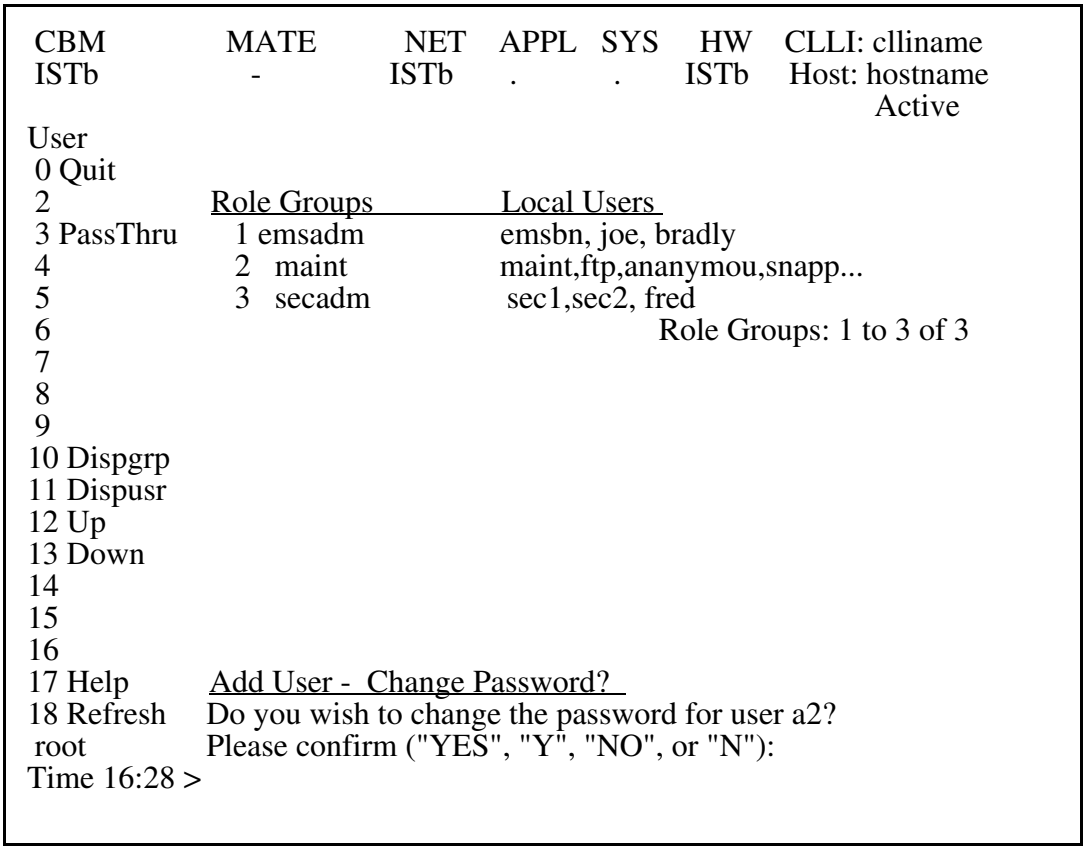
Figure 5 CBM "Add/Change" Secondary Groups prompt

```
CBM          MATE       NET   APPL  SYS   HW    CLLI: clliname
ISTb           -        ISTb   .     .    ISTb   Host: hostname
                                                      Active
User
 0 Quit
 2              Role Groups          Local Users
 3 PassThru      1 emsadm            emsbn, joe, bradly
 4               2  maint            maint,ftp,ananymou,snapp...
 5               3  secadm           sec1,sec2, fred
 6                                                Role Groups: 1 to 3 of 3
 7
 8
 9
10 Dispgrp
11 Dispusr
12 Up
13 Down
14
15
16
17 Help        Add User -  Secondary Groups
18 Refresh     Enter Secondary groups for user a2, type 'none' to remove: [none]
 root
Time 16:28 > secadm,emsadm
```

At this prompt the user can either type carriage return to accept the default which is "none" in this case or type one or more groups. The possible groups are "maint', "secadm" and/or "emsadm". The primary group can not be a part of this list. So in the above example since "maint" is the maint group the secondary groups can be none, secadm, emsadm of both secadm and emsadm. To add both type the names separated by a comma, as shown above.

The user will then be asked if he wants to change the password of the new user.

Figure 6 CBM "Add/Change" Password prompt



If you choose "y" you will then be prompted to enter the password for the user. If "n" is chosen then you will get the "command complete" and you will see the display change to add your user.

A security log is generated to capture the password change event. The password change security log will look as follows:

Aug 24 13:49:40 CBMDRY3 gen_security_log[20718]: class_security.ver02 EVENT.TYPE="USER_ACT_Security_Passwd" DOC="cbmmtc" STAT="Success" DST="CBMDRY3" DST.USR="root" SRC.OFFEND="47.129.112.179" HOST.TYPE="application" TTY="pts/1" MESSAGE=user A reset password for user B MID="SDM_MID_defn.security.0018"

Note: The syntax of the above displayed log is not finalized.

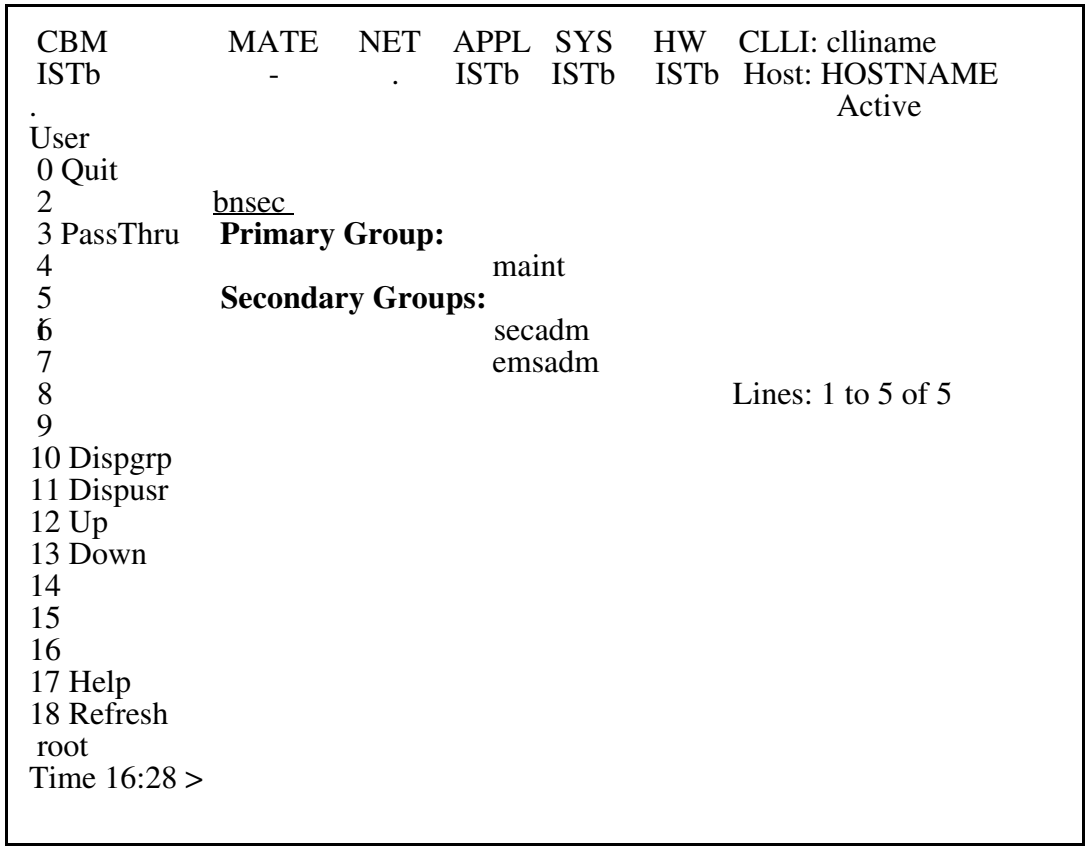
To display all users on the local CBM type either option 11 or “dispusr”. The display user command will give the following screen:

Figure 7 CBM user Menu Dispusr “all”

```
CBM          MATE    NET   APPL  SYS   HW   CLLI: clliname
ISTb           -      .    ISTb  ISTb  ISTb  Host: hostname
                                                    Active
User
 0 Quit
 2              Local Users              Groups
 3 PassThru      1  maint                maint
 4               2  Bradly               maint, emsadm
 5               3  Brenda               emsadm
 6               4  joe                  maint, secadm
 7               5  mark                 emsadm
 8               6  patrick              emsadm
 9
10 Dispgrp
11 Dispusr                    Users: 1 to 6 of 6
12 Up
13 Down
14
15
16
17 Help
18 Refresh   .
 root
Time 16:28 >
```

To display the information for a particular user type: 11 <username> or “dispusr <username>”. The display for a user will appear as:

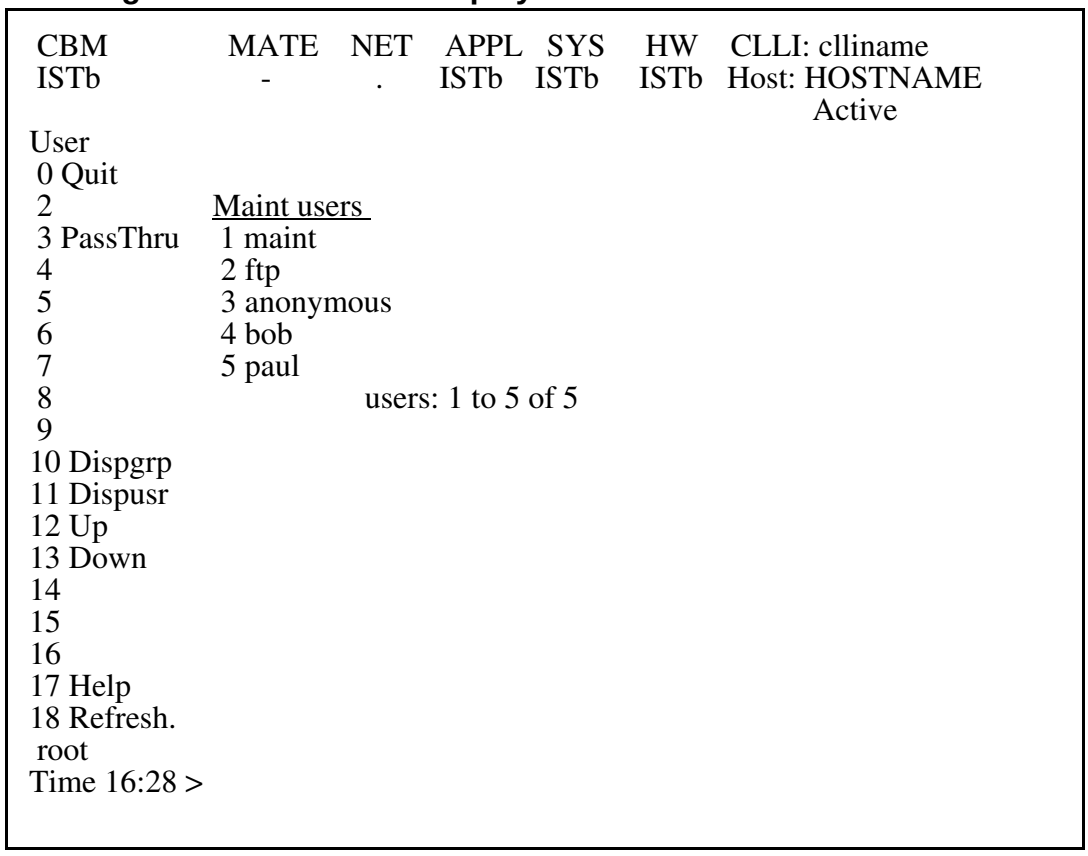
Figure 8 CBM user display menu



This menu differs from the SDM menu of this level slightly as it does not show the home directory or shell for the user. In this release we thought it was better not to allow the user to change these fields since it required more knowledge on the user’s behave.

The Group information can also be displayed. If option 10 or “dispgrp” is typed without parameters, all the groups with their users is type as in figure 3. If you type “11 maint” or “dispgrp maint” you will get the following screen:

Figure 9 CBM Maint display menu



The actions that a certain group can perform can also be displayed. This may be done by typing “10 <groupname> act” or “dispgrp <groupname> act”. The following is a display for maint:

Figure 10 CBM dispgrp maint act display

```
CBM          MATE   NET   APPL  SYS   HW    CLLI: clliname
ISTb          -      .    ISTb  ISTb  ISTb  Host: HOSTNAME
                                                    Active
User
 0 Quit
 2              Allowed actions for role group maint:
 3 PassThru          performance-manage
 4                   performance-view
 5                   accounting-manage
 6                   accounting-view
 7                   config-manage
 8                   config-view
 9                   fault-manage
10 Dispgrp           fault-view
11 Dispusr                              Lines: 1 to 8 of 8
12 Up
13 Down
14
15
16
17 Help
18 Refresh.
 root
Time 16:28 >
```

164.5 CBM Commands Authorization

The following tables contain the commands authorizations for CBM tools (cbmmtc and billmtc) and some of the commands from SPFS CLI tool that are used on a CBM.

Note: When the new authorization level is “ALL”, it indicates that users in all groups (maint, emsadm and secadm) and the root user have access to that command.

Table 2: CBMMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
cbmmtc				root, maint	ALL

Table 2: CBMMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	Mtc		Enter the maintenance level	root, maint	ALL
	Mtc>Net		Enter the Network connectivity status level.	root, maint	ALL
	Mtc>Net	Logs	Display the last event reported on each of the connectivity status indeicators.	root, maint	ALL
	Mtc>Net	QueryCBM	Query information about the CBM including Faults, status and mate faults.4	root, maint	ALL
	Mtc>Net>Core		Go to the Core level.	root, maint	ALL
	Mtc>Net>Core	Logs	Display the last Core communication event reported.	root, maint	ALL
	Mtc>Net>Core	QueryCBM	Query information about the CBM including Faults, status and mate faults.	root, maint	ALL
	Mtc>Net>NTP		Go to the NTP level.	root, maint	ALL
	Mtc>Net>NTP	Query	Display the details of an NTP server.	root, maint	ALL
	Mtc>Net>NTP	Logs	Display the last NTP event reported (if any).	root, maint	ALL
	Mtc>Net>NTP Note: The command is disabled in cbmmtc	Add	Add NTP server(s) and peer(s)	n/a	n/a
	Mtc>Net>NTP Note: The command is disabled in cbmmtc	Change	Change NTP server/peer.	n/a	n/a
	Mtc>Net>NTP Note: The command is disabled in cbmmtc	Delete	Delete NTP server(s) and peer(s)	n/a	n/a
	Mtc>Appl		Enter the software applications status level.	root, maint	ALL
	Mtc>Appl	logs	Display the last event reported (if any) on each of the application status indicators.	root, maint	ALL

Table 2: CBMMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	Mtc>Appl	Bsy	Busy an application.	root, maint	ALL
	Mtc>Appl	RTS	Return an application to service.	root, maint	ALL
	Mtc>Appl	OffL	Offline an application.	root, maint	ALL
	Mtc>Sys		Enter the operating system software status level.	root, maint	ALL
	Mtc>Sys	Logs	Display the last event reported on each of the connectivity status indei-cators.	root, maint	ALL
	Mtc>Sys	QueryCBM	Query information about the CBM including Faults, status and mate faults.	root, maint	ALL
	Mtc>Sys> Note: The command is disabled in cbmmtc	Change	Change the alarm threshold for a system software status indicator.	n/a	n/a
	Mtc>Hw		Enter the hardware status level.	root, maint	ALL
	Mtc>Hw	logs	Display the last event reported (if any) on each of the hardware status indicators.	root, maint	ALL
	Mtc>Hw	QueryCBM	Query information about the CBM including Faults, status and mate faults.	root, maint	ALL
	Mtc	Quit	Quit the current level or exit the CBM maintenance interface.	root, maint	ALL
	Mtc	Help	Displays help for a single command or all valid	root, maint	ALL
	Mtc	Refresh	Refresh the current screen.	root, maint	ALL
	Admin		Enter the system administration level.	root, maint	ALL
	Admin>User		Enter the user administration level.	root, maint	ALL
	Admin>User>PassThru		Go to PassThru level.	root, maint	ALL

Table 2: CBMMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	Admin>User>PassThru	**Change**	**Change a PassThru user.**	**root**	**root, secadm**
	Admin>User>PassThru	**Add**	**Add a new PassThru user.**	**root**	**root, secadm**
	Admin>User>PassThru	**Delete**	**Delete a PassThru user.**	**root**	**root, secadm**
	Admin>User	**Add**	**Add a new maintenance class user id.**	**root**	**root, secadm**
	Admin>User	**Delete**	**Delete a maintenance class user id.**	**root**	**root, secadm**
	Admin>User	**Change**	**Change the password for the user specified.**	**root**	**root, secadm**
	Admin>SWIM		Enter the software inventory management level.	root, maint	ALL
	Admin>SWIM>packages		Enter the software packages level.	root, maint	ALL
	Admin>SWIM>packages	**Apply**	**Apply package on this CBM.**	**root**	**root, emsadm**
	Admin>SWIM>packages	Select	Select a package.	root, maint	ALL
	Admin>SWIM>packages	**Remove**	**Remove software.**	**root**	**root, emsadm**
	Admin>SWIM>packages	Search	Search the list for the given text	root, maint	ALL
	Admin>SWIM>packages	Filter	Filter the list of software.	root, maint	ALL
	Admin>SWIM>Packages	View	Toggle between showing the software description and the software fileset name.	root, maint	ALL
	Admin>SWIM>Config		Enter the software configuration level.	root, maint	ALL
	Admin>SWIM>Config	Select	Selects a package.	root, maint	ALL
	Admin>SWIM>Config	**Config**	**Configure packages.**	**root**	**root, emsadm**

Table 2: CBMMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	Admin>SWIM>Config	Search	Search the list for the given text.	root, maint	ALL
	Admin>SWIM>Config	Filter	Filter the list of software.	root, maint	ALL
	Admin>SWIM>Config	View	Toggle between showing the software description and the software fileset name.	root, maint	ALL
	Admin>SWIM>Options		Enter the options level.	root, maint	ALL
	Admin>SWIM>Options	**Change**	**Change default values for SWIM.**	**root**	**root, emsadm**
	Admin>SWIM>History		Enter the software history level.	root, maint	ALL
	Admin>SWIM>History	ViewLog	View the log for the given history entry.	root, maint	ALL
	Admin>SWIM>History	Search	Search the list for the given text.	root, maint	ALL
	Admin>SWIM>History	Filter	Filter the list of software.	root, maint	ALL
	Admin>SWIM>History	View	Toggle between showing the software description and the software fileset name.	root, maint	ALL

Wireless SBA billing application's BILLMTC is different than the Wireline version. The following is the authorization summary for Wireless SBA BILLMTC.

Note: The root user have access to all the commands under billmtc and it is not shown in the authorization levels in the following table.

Table 3: Wireless BILLMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
billmtc			Enter billing maintenance level.	maint	emsadm, maint
	billmtc	Quit	Quits the current level	maint	emsadm, maint

Table 3: Wireless BILLMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	billmtc	Set	Sets context	maint	emsadm, maint
	billmtc	CONF-STRM	Enters CONFSTRM level	maint	emsadm, maint
	billmtc	APPL	Enters APPL level	maint	emsadm, maint
	billmtc	Query	Displays current state of streams	maint	emsadm, maint
	billmtc	Mib	Sets and gets MIB objects	maint	emsadm, maint
	billmtc	Dispal	Displays all current CBM alarms	maint	emsadm, maint
	billmtc	Displogs	Displays logs not yet sent to CM	maint	emsadm, maint
	billmtc	FILESYS	Enters FILESYS level	maint	emsadm, maint
	billmtc	SCHED-ULE	Enters SCHEDULE level	maint	emsadm, maint
	billmtc	Help	Available commands with syntax	maint	emsadm, maint
	billmtc	Refresh	Refreshes the screen	maint	emsadm, maint
	billmtc	Clli	Displays core CLLI	maint	emsadm, maint
	CONFSTRM	Quit	Quits the current level	maint	emsadm, maint
	CONFSTRM	Set	Sets context.	maint	emsadm, maint
	CONFSTRM	Add	Configures a new stream	maint	emsadm, maint
	CONFSTRM	Change	Changes an existing stream configu-ration	maint	emsadm, maint
	CONFSTRM	Delete	Deletes a stream	maint	emsadm, maint
	CONFSTRM	List	Lists configuration of a (or all) stream(s)	maint	emsadm, maint

Table 3: Wireless BILLMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	CONFSTRM	CLEANUP	Configure the closedSent cleanup process	maint	emsadm, maint
	CONFSTRM> CLEANUP	Quit	Quits the current level	maint	emsadm, maint
	CONFSTRM> CLEANUP	Set	Sets context.	maint	emsadm, maint
	CONFSTRM> CLEANUP	Change	Change closedSent cleanup config	maint	emsadm, maint
	CONFSTRM> CLEANUP	List	List closedSent cleanup config	maint	emsadm, maint
	APPL	Quit	Quits the current level	maint	emsadm, maint
	APPL	Set	Sets Context	maint	emsadm, maint
	APPL	cdrView	Displays CDR records from DIRP formatted onto the screen.	maint	emsadm, maint
	APPL	AFT	Enters AFT level	maint	emsadm, maint
	APPL	BACKUP	Enter DVD backup level.	maint	emsadm, maint
	APPL	ALM	Enters ALM level	maint	emsadm, maint
	APPL	TOOLS	Enters Tools level	maint	emsadm, maint
	APPL>AFT	Quit	Quits the current level	maint	emsadm, maint
	APPL>AFT	Set	Command inapplicable	maint	emsadm, maint
	APPL>AFT	AFT-CONFG	Enters AFT Session configuration level	maint	emsadm, maint
	APPL>AFT	Query	Query info on file transfer lists for sessions	maint	emsadm, maint
	APPL>AFT	Setfile	Set an override file, delete a file from the list	maint	emsadm, maint
	APPL>AFT	Rsetfile	Reset a file from partial to pending	maint	emsadm, maint

Table 3: Wireless BILLMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	APPL>AFT	AFTRESND	Enters AFT resend level	maint	emsadm, maint
	APPL>AFT	Start	Start an AFT session that was stopped	maint	emsadm, maint
	APPL>AFT	Stop	Stop an AFT session file transfer	maint	emsadm, maint
	APPL>AFT	Alarm	Query or cancel AFT session alarms	maint	emsadm, maint
	APPL>AFT>AFT-CONFG	Set	Sets context	maint	emsadm, maint
	APPL>AFT>AFT-CONFG	Add	Add AFT tuples to the MIB	maint	emsadm, maint
	APPL>AFT>AFT-CONFG	Delete	Delete AFT tuples from the MIB	maint	emsadm, maint
	APPL>AFT>AFT-CONFG	Change	Change number of retry attempts for a session	maint	emsadm, maint
	APPL>AFT>AFT-CONFG	List	List AFT tuples in the MIB	maint	emsadm, maint
	APPL>AFT>AFT-CONFG	almChg	Configure ALM	maint	emsadm, maint
	APPL>AFT>AFTRESND	Quit	Quits the current level	maint	emsadm, maint
	APPL>AFT>AFTRESND	Set	Sets context	maint	emsadm, maint
	APPL>AFT>AFTRESND	Listfile	Lists processed files	maint	emsadm, maint
	APPL>AFT>AFTRESND	Addfile	Add processed files to a session	maint	emsadm, maint
	APPL>BACKUP	Set	Sets Context	maint	emsadm, maint
	APPL>BACKUP	Backup	Perform a manual backup	maint	emsadm, maint
	APPL>BACKUP	SCHED-ULE	Enters scheduled backup level	maint	emsadm, maint
	APPL>BACKUP>SCHELDULE	Set	Sets Context	maint	emsadm, maint

Table 3: Wireless BILLMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	APPL>BACKUP>SCHELDULE	Add	Adds a tuple to the backup schedule	maint	emsadm, maint
	APPL>BACKUP>SCHELDULE	Change	Changes a tuple in the backup schedule	maint	emsadm, maint
	APPL>BACKUP>SCHELDULE	Delete	Deletes tuple(s) from the backup schedule	maint	emsadm, maint
	APPL>BACKUP>SCHELDULE	List	Lists tuple(s) in the backup schedule	maint	emsadm, maint
	APPL>ALM	Set	Sets Context	maint	emsadm, maint
	APPL>ALM	CONFIG	Enters CONFIG level	maint	emsadm, maint
	APPL>ALM	QApps	Query applications registered to ALM	maint	emsadm, maint
	APPL>ALM	QStreams	Query streams registered to ALM	maint	emsadm, maint
	APPL>ALM>CONFIG	Set	Sets Context	maint	emsadm, maint
	APPL>ALM>CONFIG	almReq	Register an application to ALM	maint	emsadm, maint
	APPL>ALM>CONFIG	almDereq	Deregister an application from ALM	maint	emsadm, maint
	APPL>ALM>CONFIG	almChg	Change an application registration from ALM	maint	emsadm, maint
	APPL>TOOLS	Set	Sets Context	maint	emsadm, maint
	APPL>TOOLS	tmbConf	Set tmbConf to on/off	maint	emsadm, maint
	FILESYS	Set	Sets context	maint	emsadm, maint
	FILESYS	Sendfile	Sends billing file(s) per stream to downstream	maint	emsadm, maint
	FILESYS	Listfile	Lists stored billing file(s) per stream	maint	emsadm, maint
	FILESYS	Closec	Closes currently open billing file(s) per stream	maint	emsadm, maint

Table 3: Wireless BILLMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	SCHEDULE	Set	Sets Context	maint	emsadm, maint
	SCHEDULE	Add	Adds a tuple to the schedule	maint	emsadm, maint
	SCHEDULE	Change	Changes a tuple in the schedule	maint	emsadm, maint
	SCHEDULE	Delete	Deletes tuple(s) from the schedule	maint	emsadm, maint
	SCHEDULE	List	Lists tuple(s) in the schedule	maint	emsadm, maint
	SCHEDULE	RTB	Enters RTB level	maint	emsadm, maint
	SCHEDULE>RTB	Set	Sets context	maint	emsadm, maint
	SCHEDULE>RTB	Rts	Returns RTB to service for a stream.	maint	emsadm, maint
	SCHEDULE>RTB	Bsy	Busies RTB for a stream.	maint	emsadm, maint
	SCHEDULE>RTB	Offl	Offlines RTB for a stream.	maint	emsadm, maint
	SCHEDULE>RTB	Query	Queries the state of RTB for a stream.	maint	emsadm, maint
	SCHEDULE>RTB	IPTest	Tests the IP address used by RTB for a stream.	maint	emsadm, maint
	SCHEDULE>RTB	CONFRTB	Enters the RTB configuration level.	maint	emsadm, maint
	SCHED-ULE>RTB>CON-FRTB	Set	Set context	maint	emsadm, maint
	SCHED-ULE>RTB>CON-FRTB	Add	Adds RTB to a stream.	maint	emsadm, maint
	SCHED-ULE>RTB>CON-FRTB	Change	Changes the RTB configuration for a stream.	maint	emsadm, maint

Table 3: Wireless BILLMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	SCHED-ULE>RTB>CON-FRTB	Delete	Deletes RTB from a stream.	maint	emsadm, maint
	SCHED-ULE>RTB>CON-FRTB	Query	Query the RTB configured destina-tions.	maint	emsadm, maint
	SCHED-ULE>RTB>CON-FRTB	Autorec	Turns Autorecovery on or off for RTB.	maint	emsadm, maint
	SCHED-ULE>RTB>CON-FRTB	LagTimer	Set the RTB Lag Timer	maint	emsadm, maint

The following is the authorization summary for Wireline SBA BILLMTC.

Note: The root user have access to all the commands under billmtc and it is not shown in the authorization levels in the following table.

Table 4: Wireline BILLMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
billmtc			Enter billing maintenance level.	maint	emsadm, maint
	billmtc	Quit	Quits the current level	maint	emsadm, maint
	billmtc	Set	Sets context	maint	emsadm, maint
	billmtc	CONF-STRM	Enters CONFSTRM level	maint	emsadm, maint
	billmtc	APPL	Enters APPL level	maint	emsadm, maint
	billmtc	Query	Displays current state of streams	maint	emsadm, maint
	billmtc	Mib	Sets and gets MIB objects	maint	emsadm, maint
	billmtc	Dispal	Displays all current CBM alarms	maint	emsadm, maint

Table 4: Wireline BILLMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	billmtc	Displogs	Displays logs not yet sent to CM	maint	emsadm, maint
	billmtc	FILESYS	Enters FILESYS level	maint	emsadm, maint
	billmtc	SCHED-ULE	Enters SCHEDULE level	maint	emsadm, maint
	billmtc	TOOLS	Enters TOOLS level	maint	emsadm, maint
	billmtc	Help	Available commands with syntax	maint	emsadm, maint
	billmtc	Refresh	Refreshes the screen	maint	emsadm, maint
	billmtc	Clli	Displays core CLLI	maint	emsadm, maint
	CONFSTRM	Quit	Quits the current level	maint	emsadm, maint
	CONFSTRM	Set	Sets context.	maint	emsadm, maint
	CONFSTRM	Add	Configures a new stream	maint	emsadm, maint
	CONFSTRM	Change	Changes an existing stream configu-ration	maint	emsadm, maint
	CONFSTRM	Delete	Deletes a stream	maint	emsadm, maint
	CONFSTRM	List	Lists configuration of a (or all) stream(s)	maint	emsadm, maint
	CONFSTRM	Act	Activates a filtered stream	maint	emsadm, maint
	CONFSTRM	Deact	Deactivates a filtered stream	maint	emsadm, maint
	CONFSTRM	Update	Updates a filtered stream’s criteria.	maint	emsadm, maint
	CONFSTRM	Start	Resume receiving records on a fil-tered stream.	maint	emsadm, maint
	CONFSTRM	Stop	Stop receiving records on a filtered stream.	maint	emsadm, maint

Table 4: Wireline BILLMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	CONFSTRM	Help	Available commands with syntax	maint	emsadm, maint
	CONFSTRM	Refresh	Refreshes the screen	maint	emsadm, maint
	CONFSTRM	clli	Displays core CLLI	maint	emsadm, maint
	APPL	Quit	Quits the current level	maint	emsadm, maint
	APPL	Set	Command inapplicable	maint	emsadm, maint
	APPL	AFT	Enters AFT level	maint	emsadm, maint
	APPL	SFP	Enters SFP level	maint	emsadm, maint
	APPL	Help	Available commands with syntax	maint	emsadm, maint
	APPL	Refresh	Refreshes the screen	maint	emsadm, maint
	APPL	clli	Displays core CLLI	maint	emsadm, maint
	APPL>AFT	Quit	Quits the current level	maint	emsadm, maint
	APPL>AFT	Set	Command inapplicable	maint	emsadm, maint
	APPL>AFT	AFT-CONFG	Enters AFT Session configuration level	maint	emsadm, maint
	APPL>AFT	Query	Query info on file transfer lists for sessions	maint	emsadm, maint
	APPL>AFT	Setfile	Set an override file, delete a file from the list	maint	emsadm, maint
	APPL>AFT	Rsetfile	Reset a file from partial to pending	maint	emsadm, maint
	APPL>AFT	AFTRESND	Enters AFT resend level	maint	emsadm, maint
	APPL>AFT	Start	Start an AFT session that was stopped	maint	emsadm, maint

Table 4: Wireline BILLMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	APPL>AFT	Stop	Stop an AFT session file transfer	maint	emsadm, maint
	APPL>AFT	Alarm	Query or cancel AFT session alarms	maint	emsadm, maint
	APPL>AFT	Help	Available commands with syntax	maint	emsadm, maint
	APPL>AFT	Refresh	Refreshes the screen	maint	emsadm, maint
	APPL>AFT	clli	Displays core CLLI	maint	emsadm, maint
	APPL>AFT>AFT-CONFG	Quit	Quits the current level	maint	emsadm, maint
	APPL>AFT>AFT-CONFG	Set	Sets context	maint	emsadm, maint
	APPL>AFT>AFT-CONFG	Add	Add AFT tuples to the MIB	maint	emsadm, maint
	APPL>AFT>AFT-CONFG	Delete	Delete AFT tuples from the MIB	maint	emsadm, maint
	APPL>AFT>AFT-CONFG	Change	Change number of retry attempts for a session	maint	emsadm, maint
	APPL>AFT>AFT-CONFG	List	List AFT tuples in the MIB	maint	emsadm, maint
	APPL>AFT>AFTRESND	Quit	Quits the current level	maint	emsadm, maint
	APPL>AFT>AFTRESND	Set	Sets context	maint	emsadm, maint
	APPL>AFT>AFTRESND	Listfile	Lists processed files	maint	emsadm, maint
	APPL>AFT>AFTRESND	Addfile	Add processed files to a session	maint	emsadm, maint
	APPL>SFP>	Quit	Quits the current level	maint	emsadm, maint
	APPL>SFP>	Set	Sets context	maint	emsadm, maint
	APPL>SFP>	Query	Queries the SFP status	maint	emsadm, maint

Table 4: Wireline BILLMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	APPL>SFP>	**Act**	**Activates SFP**		**emsadm**
	APPL>SFP>	**Deact**	**De-activates SFP**		**emsadm**
	FILESYS	Quit	Quits the current level	maint	emsadm, maint
	FILESYS	Set	Sets context	maint	emsadm, maint
	FILESYS	Sendfile	Sends billing file(s) per stream to downstream	maint	emsadm, maint
	FILESYS	Listfile	Lists stored billing file(s) per stream	maint	emsadm, maint
	FILESYS	Closec	Closes currently open billing file(s) per stream	maint	emsadm, maint
	SCHEDULE	Quit	Quits the current level	maint	emsadm, maint
	SCHEDULE	Set	Sets Context	maint	emsadm, maint
	SCHEDULE	Add	Adds a tuple to the schedule	maint	emsadm, maint
	SCHEDULE	Change	Changes a tuple in the schedule	maint	emsadm, maint
	SCHEDULE	Delete	Deletes tuple(s) from the schedule	maint	emsadm, maint
	SCHEDULE	List	Lists tuple(s) in the schedule	maint	emsadm, maint
	SCHEDULE>RTB		**Enters RTB level**	**maint**	**maint**
	SCHEDULE>RTB	Set	Sets context	maint	emsadm, maint
	SCHEDULE>RTB	Rts	Returns RTB to service for a stream.	maint	emsadm, maint
	SCHEDULE>RTB	Bsy	Busies RTB for a stream.	maint	emsadm, maint
	SCHEDULE>RTB	Offl	Offlines RTB for a stream.	maint	emsadm, maint
	SCHEDULE>RTB	Query	Queries the state of RTB for a stream.	maint	emsadm, maint

Table 4: Wireline BILLMTC Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	SCHEDULE>RTB	IPTest	Tests the IP address used by RTB for a stream.	maint	emsadm, maint
	SCHEDULE>RTB	CONFRTB	Enters the RTB configuration level.	maint	emsadm, maint
	SCHED-ULE>RTB>CON-FRTB	Set	Set context	maint	emsadm, maint
	SCHED-ULE>RTB>CON-FRTB	Add	Adds RTB to a stream.	maint	emsadm, maint
	SCHED-ULE>RTB>CON-FRTB	Change	Changes the RTB configuration for a stream.	maint	emsadm, maint
	SCHED-ULE>RTB>CON-FRTB	Delete	Deletes RTB from a stream.	maint	emsadm, maint
	SCHED-ULE>RTB>CON-FRTB	Query	Query the RTB configured destina-tions.	maint	emsadm, maint
	SCHED-ULE>RTB>CON-FRTB	Autorec	Turns Autorecovery on or off for RTB.	maint	emsadm, maint
	SCHED-ULE>RTB>CON-FRTB	**LagTimer**	**Set the RTB Lag Timer**	**maint**	**maint**
	TOOLS	Quit	Quits the current level	maint	emsadm, maint
	TOOLS	Set	Sets Context	maint	emsadm, maint
	TOOLS	Amadump	Displays record information	maint	emsadm, maint

The following table lists the commands from SPFS CLI tool that are used on a CBM and supported by this feature.

Table 5: SPFS CLI Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
cli	cli		Enter the system command line interface level.	root	root emsadm secadm
	cli>view		Enter the view level	root	root emsadm secadm
	cli>view	sspfs_soft	Display Software Installation Level Of SSPFS	root	root emsadm secadm
	cli>view	chk_ssfps	Check SSPFS Processes	root	root emsadm secadm
	cli>view	sw_conf	The software configuration of the system	root	root emsadm secadm
	cli>view	cpu_util	Overall CPU utilization	root	root emsadm secadm
	cli>view	cpu_util_proc	CPU utilization by process	root	root emsadm secadm
	cli>view	port_util	I/O port utilization	root	root emsadm secadm
	cli>view	disk-util	Filesystem utilization	root	root emsadm secadm
	cli>configure		Enter the configuration level	root	root emsadm secadm
	cli>configure>NTP configuration		Enter the NTP configuration level	root	root emsadm secadm
	cli>configure>NTP configuration	ntp_conf	Configure the NTP daemon	root	root emsadm
	cli>configure>NTP configuration	ntp_unconf	Unconfigure the NTP daemon	root	root emsadm

Table 5: SPFS CLI Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	cli>configure>NTP configuration	ntp_remove	Remove an NTP server	root	root emsadm
	cli>configure>NTP configuration	ntp_view	View ntp configuration information.	root	root emsadm
	cli>configure>OAMP Application Configuration		Enter OAMP Application Configuration level	root	root emsadm secadm
	cli>configure>OAMP Application Configuration	sdm_conf	Configure SDM IP Address	root	root emsadm
	cli>configure>OAMP Application Configuration	sdm_unconf	Unconfigure SDM IP Address	root	root emsadm
	cli>configure>OAMP Application Configuration	sdmuser_conf	Configure SDM User	root	root emsadm
	cli>configure>OAMP Application Configuration	sdmuser_unconf	Unconfigure SDM User	root	root emsadm
	cli>configure>OAMP Application Configuration	cmClli_rediscovery	Re-discovery the CM CLLI by SDM IP	root	root emsadm
	cli>configure>OAMP Application Configuration	cmClli_conf	Configure CM_CLLI Address	root	root emsadm
	cli>configure>OAMP Application Configuration	cmClli_unconf	Unconfigure CM_CLLI IP Address	root	root emsadm
	cli>configure>OAMP Application Configuration	cm_conf	Configure CM IP Address	root	root emsadm
	cli>configure>OAMP Application Configuration	cm_unconf	Unconfigure CM IP Address	root	root emsadm
	cli>configure>IP Configuration		Enter IP Configuration level	root	root emsadm secadm
	cli>configure>IP Configuration	config_router	Configure Default Router and Netmask	root	root emsadm

Table 5: SPFS CLI Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	cli>configure>IP Configuration	config_data	Configure System Data IP Addresses	root	root emsadm
	cli>configure>IP Configura-tion>ipsecike_config		enter ipsecike_config level	root	root emsadm
	cli>configure>IP Configura-tion>ipsecike_config >IPSec		enter IPSec configuration level	root	root emsadm
	cli>configure>IP Configura-tion>ipsecike_config >IPSec	**Add IPSec Entry**	**Add IPSec Entry**	**root**	**root**
	cli>configure>IP Configura-tion>ipsecike_config >IPSec	**Delete IPSec entry**	**Delete IPSec entry**	**root**	**root**
	cli>configure>IP Configura-tion>ipsecike_config >IPSec	List All IPSec entries	List All IPSec entries	root	root emsadm
	cli>configure>IP Configura-tion>ipsecike_config >IKE		enter IKE configuration level	root	root emsadm
	cli>configure>IP Configura-tion>ipsecike_config >IKE	**Add IKE Entry**	**Add IKE Entry**	**root**	**root**
	cli>configure>IP Configura-tion>ipsecike_config >IKE	**Delete IKE entry**	**Delete IKE entry**	**root**	**root**
	cli>configure>IP Configura-tion>ipsecike_config >IKE	List IKE entries	List IKE entries	root	root emsadm
	cli>IP Configura-tion>ipsecike_config >IKE	**Change**	**Change Preshared Key for IKE entry**	**root**	**root**

Table 5: SPFS CLI Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	cli>configure>Syslog Configuration		Enter Syslog Configuration level	root	root emsadm secadm
	cli>configure>Syslog Configuration	list_syslog	List a system's syslog configuration	root	root emsadm
	cli>configure>Syslog Configuration	add_syslog	Add a syslog configuration entry	root	root emsadm
	cli>configure>Syslog Configuration	del_syslog	Remove a syslog configuration entry	root	root emsadm
	cli>configure>Syslog Configuration	route_syslog_on	Route syslog to remote host	root	root emsadm
	cli>configure>Syslog Configuration	route_syslog_off	Turn off syslog re-direction to a remote host	root	root emsadm
	cli>configure>Security Services Configuration		Enter Security Services Configuration level	root	root emsadm secadm
	cli>configure>Security Services Configuration>Socks Configuration		Enter Socks Configuration level	root	root emsadm secadm
	cli>configure>Security Services Configuration>Socks Configuration	config_socks	Modify Socks Security Service	root	root emsadm
	cli>configure>Security Services Configuration>Socks Configuration	list_socks	List Socks Security Service	root	root emsadm secadm
	cli>configure>Security Services Configuration>IEMS Server Location Configuration		Enter IEMS Server Location Configuration level	root	root emsadm secadm
	cli>configure>Security Services Configuration>IEMS Server Location Configuration	iems_ip	Configure IEMS Server IP	root	root emsadm

Table 5: SPFS CLI Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	cli>configure>Security Services Configuration>PAM Configuration		Enter PAM Configuration level	root	root emsadm secadm
	cli>configure>Security Services Configuration>PAM ConfigurationCentral Security Client Configuration>		Enter Central Security Client Configuration level	root	root emsadm secadm
	cli>configure>Security Services Configuration>PAM ConfigurationCentral Security Client Configuration>	pam_orig	Use Default PAM Configuration	root	root emsadm
	cli>configure>Security Services Configuration>PAM ConfigurationCentral Security Client Configuration>	pam_radius	Use Security Server	root	root emsadm
	cli>configure>Security Services Configuration>PAM ConfigurationCentral Security Client Configuration>	saml_passwd_conf	Configure saml password	root	root emsadm
	cli>configure>Location Configuration		Enter Location Configuration level	root	root emsadm secadm
	cli>configure>Location Configuration	chg_tz	Change Timezone	root	root emsadm
	cli>configure>Location Configuration	sys_loc	System Location	root	root emsadm
	cli>configure>Succession Element Configuration		Enter Succession Element Configuration level	root	root emsadm secadm
	cli>configure>Succession Element Configuration	NPM Application	NPM Application Configuration	root	root emsadm

Table 5: SPFS CLI Command Authorization Summary

CBM Tool	Level	Commands	Description	Old auth. level	New auth. level
	cli>configure>Succession Element Configuration	PSE Application	PSE Application Configuration	root	root emsadm
	cli>Other		Enter Other Configuration level	root	root emsadm secadm
	cli>Other>log rotation		Enter Log rotation configuration level	root	root emsadm secadm
	cli>Other>Log Rotation	exec_rlog	Execute The Rotatelog Function	root	root emsadm secadm
	cli>Other>Log Rotation	view_rlog	View The Rotatelog Configuration File	root	root emsadm secadm
	cli>Other	capt_files	Capture Various SSPFS Files/Logs For Debugging Purposes	root	root emsadm
	cli>Other	sun_explorer	Execute the Sun Explorer Data Gathering Tool	root	root emsadm
	cli>Other	mount_image	Mount A Generic Iso Image To The SSPFS Unit	root	root emsadm
	cli>Other	umount_image	Un-Mount A Generic Iso Image From The SSPFS Unit	root	root emsadm

164.6 CBM NTP Procedures

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Customer doc: NN10347-461 Core and Billing Manager 850: Application Installation and Upgrade Guide					
Upgrading the CBM850			root	root	This procedure include other procedures (listed in this table) that require root access.

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Verifying the state of a cluster			root	root,	The following commands are executed: • ubmstat • ubmstat • CheckConfiguration • init 6 • cli, other, capt_files
Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server			root	root,	The following commands are executed: • df -k / • ftp <repository_server_ip> • ftp> ls • ftp> get <iso_image> • mv • gzip -d • tar -xvf • cd • mv • cli, other, mount_image This procedure is required only during an install and upgrade.

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Upgrading SSPFS software			root	root	The following commands are executed: **Using CDROM:** • cd / • /cdrom/cdrom0/s0/pre_upgrade • /liveupgrade.ksh • cli, view, sspfs_soft **Using ESD:** • df -k /opt • cd /opt • ftp • ftp> get • cli, other, mount_image • /tmpmnt/pre_upgrade • cli, other, umount_image • mv • /liveupgrade.ksh
Performing a backup of oracle data on an SSPFS-based server			root	root	The following commands are executed: • servstop IEMS • /opt/nortel/iems/current/bin/purge-TempData.sh • servstart IEMS • mt -f /dev/rmt/0 rewind • /opt/nortel/sspfs/bks/bkdata • tar tvf /dev/rmt/0 • tar tvf /cdrom/*bkdata*/*.tar • cd / • eject cdrom • /etc/init.d/volmgt stop • /etc/init.d/volmgt stop **This procedure is not required for CBM.**

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Performing a backup of file system on an SSPFS-based server		config-admin	root	root, emsadm	The following commands are executed: • mt -f /dev/rmt/0 rewind • /opt/nortel/sspfs/bks/bkfullsys • gtar -tvMf /dev/rmt/0 • gtar -tvMf /cdrom/*bkfullsys*/*.tar • cd / • eject cdrom **root only (These steps are not needed for this procedure unless error occurs when ejecting a CD:** • **/etc/init.d/volmgt stop** • **/etc/init.d/volmgt start**
Verifying group IDs and user IDs on an SSPFS-based server			maint, root	ALL	The following commands are executed: • cut -f1,3 -d':' /etc/group • cut -f1,3 -d':' /etc/passwd
Executing a fallback during an SSPFS-based server upgrade			root	root	The following commands are executed: • /SSPFS_Upgrade.fallback • udstat
Applying patches to a CBM		Config-admin	root	root, emsadm	The following commands are executed: • Calls “Configuring PSE on a CBM”. • Calls “Configuring NPM on an SSPFS server”. • Calls “Applying patches using the NPM”.

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Removing patches from a CBM		Config-admin	root	root, emsadm	The following commands are executed: • Calls “Configuring PSE on a CBM”. • Calls “Configuring NPM on an SSPFS server”. • Calls “Removing patches using the NPM”.
Configuring PSE on a CBM		Config-admin	root	root, emsadm	The following commands are executed: • cli, configuration, Succession Element Configuration, PSE Application Configuration, Configure_PSE (Configure the Patching Server Element) • pse start
Configuring NPM on an SSPFS server		Config-admin	root	root, emsadm	The following commands are executed: • cli, configuration, Succession Element Configuration, NPM Application Configuration • servstart npm
Setting up local user accounts on an SSPFS-based server			root	root	The following commands are executed: • useradd -g succssn <userid> • passwd -r files <userid> • groups <userid> • usermod -g succssn -G <groupA,groupB,...> <userid>

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Patching the inactive node of a cluster during an upgrade			root	root	The following commands are executed: • Follow procedure “Applying patches using the NPM” if NPM does not reside on CBM -> should not worry about in this case. • patchUpToDate - directory <directory_name> **Note: CBM upgrade will be performed by root users. This procedure is invoked during an upgrade, and therefore will be executed as root.**
Starting the PSE server application on an SSPFS-based server		Config-admin	root	root, emsadm	The following commands are executed: • pse start • pse status
Starting the NPM server application		Config-admin	root	root, emsadm	The following commands are executed: • servman query -status -group NPM • servstart NPM

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Transferring patches to the NPM database manually			root	root	The following commands are executed: • ubmstat • mkdir /data/npm/tmp • chmod 777 /data/npm/tmp • find /cdrom -name '*.patch' > /data/npm/tmp/current.patchlist • cd /data/npm/tmp • mkdir /data/npm/patch_upgrade • chmod 777 /data/npm/patch_upgrade • cd /data/npm/patch_upgrade • ftp <ESD_server> • ls • chmod 777 * • servquery -status -group NPM • servstart NPM • npm • getpatch patchlist • cd / • eject cdrom • /etc/init.d/volmgt stop • /etc/init.d/volmgt start **Note: As it currently stands, this procedure will be executed by root. However, this procedure could be split into two procedure:** **1- Procedure one will create the patch directory structure and this will be required just once after a fresh install or upgrade (will be executed by root).** **2- Procedure two will provide the steps to transfer the patches to the NPM server. This is the procedure that will be often run by customers prior to patch apply. This procedure will be executed by emsadm.**

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Applying patches using the NPM			root	root emsadm secadm	The following commands are executed: • npm (calling procedure “Accessing the Network Patch Manager CLUI” - calling npm commands). • The rest of the procedure called within this procedure requires invoking the GUI from outside the CBM.
Removing patches using the NPM			root	root emsadm secadm	The following commands are executed: • npm (calling procedure “Accessing the Network Patch Manager CLUI” - calling npm commands). • The rest of the procedure called within this procedure requires invoking the GUI from outside the CBM.
Deactivating patches using the NPM			root	root emsadm secadm	The following commands are executed: • npm (calling procedure “Accessing the Network Patch Manager CLUI”) • The rest of the procedure called within this procedure requires invoking the GUI from outside the CBM.

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Performing a device audit using the NPM			root	root emsadm secadm	The following commands are executed: • npm (calling procedure “Accessing the Network Patch Manager CLUI”) • The rest of the procedure called within this procedure requires invoking the GUI from outside the CBM.
Defining NPM patching reports			root	root emsadm secadm	The following commands are executed: • npm (calling procedure “Accessing the Network Patch Manager CLUI”) • The rest of the procedure called within this procedure requires invoking the GUI from outside the CBM.
Accessing the Network Patch Manager CLUI			root	root emsadm secadm	The following commands are executed: • npm
Restarting a device using the NPM			root	root emsadm secadm	The following commands are executed: • npm (calling procedure “Accessing the Network Patch Manager CLUI”) • The rest of the procedure called within this procedure requires invoking the GUI from outside the CBM.

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Launching CS 2000 Management Tools and NPM client applications			root	root emsadm secadm	The following commands are executed: • npm (calling procedure “Accessing the Network Patch Manager CLUI” • The rest of the procedure called within this procedure requires invoking the GUI from outside the CBM.
Confirming the upgrade on a cluster			root	root	The following commands are executed: • /SSPFS_Upgrade.accept • /SSPFS_Upgrade.fallback • OK boot • GetRunningClusterNodeNames • udstat

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Cloning the image of one node in a cluster to the other node			root	root	The following commands are executed: • udstat • cli, view, • sspfs_soft • servquery -status all • servstart <app_name> • pse status • pse start • ptmctl status • cp • cd • ./ configure_s1isext.sh -replica disable • init 0 • OK banner • startb <Ethernet address> • OK boot net -image • finishb

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Installing optional software on a CBM 850			root	root emsadm	The following commands are executed: • May need to create logical volumes depending on the application • init 6 (if logical volume created) • Insure that system is patch current (refer to patching procedures) • Perform system clone. DDMS: • makelv /cbmdata/00/osscomms 16 • chmod 755 /cbmdata/00/osscomms • chown maint:maint /cbmdata/00/osscomms • cbmmtc apply, source, select, apply • cbmmtc config, select, config • All the rest of the applications follow the same process. **If changing ownership/ permission of a logical volume is required for application apply, then a root user is required. Else an emsadm user can perform the procedure otherwise.**
Removing software packages from a CBM 850		Config-admin	root	root emsadm	The following commands are executed: • cbmmtc packages, select, remove
Viewing software transaction history and logs on the CBM 850			root, maint	ALL	The following commands are executed: • cbmmtc • history • ViewLog <#>

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Using the Queryloads tool to display patches and packages applied on the CBM 850			root, maint	ALL	The following commands are executed: • queryloads
Customer Doc: NN10353-511 Core and Billing Manager 850 Configuration Management					
Configuring a virtual IP on an SSPFS-based server			root	root	The following commands are executed: • Cli, Configuration, IP Configuration,config_data. • shutdown • **boot** This procedure requires a reboot and therefore must be executed by root.
Configuring log delivery destinations			root, maint	ALL	The following commands are executed: • logroute
Modifying a log device using logroute			root, maint	ALL	The following commands are executed: • logroute
Deleting a device using logroute			root, maint	ALL	The following commands are executed: • logroute
Configuring log delivery for MDM/PPEM security and audit logs			root, maint	ALL	The following commands are executed: • logroute
Excluding MDM/PPEM audit and security logs from other log devices			root, maint	ALL	The following commands are executed: • logroute
Specifying the logs delivered from the CM to the core manager			root, maint	ALL	The following commands are executed: • logroute
Configuring log delivery global parameters			root, maint	ALL	The following commands are executed: • logroute

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Configuring the GDD parameter using logroute			root, maint	ALL	The following commands are executed: • logroute
Configuring outbound connection security for OMDD			root	root	The following commands are executed: • cd ~maint • ls -lad .ssh • mkdir .ssh • chown maint:maint .ssh • chmod u+rwx .ssh • su maint • ssh -l maint <nn.nn.nn.nn>
Configuring core access for SBRM through the CBM 850		config-admin	root	root, emsadm	The following commands are executed: • cd /opt/nortel/bkresmgr/cbm/scripts • ./bkmgr_config.sh
Creating the backup user ID on the core for SBRM	N/A	N/A	N/A	N/A	This procedure is executed on the Core.
Commissioning or decommissioning Network Time Protocol (NTP)		Config-admin	root	root, emsadm	The following commands are executed: • Cli, configuration, NTP configuration • cbmmtc ntp
Adding or removing an NTP server or peer		Config-admin	root	root, emsadm	The following commands are executed: • Cli, configuration, NTP configuration • cbmmtc ntp
Installing the logreceiver tool on a client workstation			root, maint	ALL	The following commands are executed: ftp <CBM_IP_address> ftp> cd /swd/client ftp> binary ftp> get logreceiver ftp> bye

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Installing the CMFT on a client workstation			root, maint	ALL	The following command is executed from the client workstation, connecting to the CBM as root: scp root@<coremanager_ip_address>:/sdm/scft/cmft.
Customer doc: NN10358-611 Core and Billing Manager 850 Security and Administration					
Performing a backup of oracle data on an SSPFS-based server			root	root	The following commands are executed: • servstop IEMS • /opt/nortel/iems/current/bin/purgeTempData.sh • servstart IEMS • mt -f /dev/rmt/0 rewind • /opt/nortel/sspfs/bks/bkdata • tar tvf /dev/rmt/0 • tar tvf /cdrom/*bkdata*/*.tar • cd / • eject cdrom • /etc/init.d/volmgt stop • /etc/init.d/volmgt stop **This procedure is not required for CBM.**

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Performing a backup of file system on an SSPFS-based server		config-admin	root	root, emsadm	The following commands are executed: • mt -f /dev/rmt/0 rewind • /opt/nortel/sspfs/bks/bkfullsys • gtar -tvMf /dev/rmt/0 • gtar -tvMf /cdrom/*bkfullsys*/*.tar • cd / • eject cdrom **root only (These steps are not needed for this procedure unless error occurs when ejecting a CD:** • **/etc/init.d/volmgt stop** • **/etc/init.d/volmgt start**
Preparing a CD-RW or DVD-RW for use			root	root emsadm secadm	The following commands are executed: • cdrw -l • cdrw -b all • cdrw -l • cd / • eject cdrom **root only (These steps are not needed for this procedure unless error occurs when ejecting a CD:** • **/etc/init.d/volmgt stop** • **/etc/init.d/volmgt start**

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Adding a file system using the makelv command		Config_admin	root	root emsadm	The following commands are executed: • makelv <file system name><file system size>
Increase the size of a file system on an SSPFS-based server			root	root	The following commands are executed: Single server CBM: • cli, View, disk_util • echo '/opt/nortel/sspfs/fs/meta.pl fs' 2048 / 5000 - p | dc • filesys grow -m <mount_point> -s <size>m CBM HA: • ubmstat • Udstat • Cli, view, disk_util • GrowClusteredFileSystem.ksh <mount_point> <size>m • init 6 • StopCluster
Migrating core manager user accounts to IEMS NOTE: The procedure shouldn't be in SN09 NTP since the feature wasn't available in SN09			root	root	The following commands are executed (duplicate commands are not displayed twice): • cd <directory path> • ls -IRa • exportLocalUser <directory path> <IEMS server domain name> • cat • sftp <IP address>, put • rm • Cbmmtc, admin, user, delete <userID> • mkdir • cp • chown • rm -rf

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Adding or removing a program from the maintenance class users' access		config-admin	root	root, emsadm	The following commands are executed: • custprog -a <program name> • custprog -d <program name>
Connecting to the CM passthru			passthru	passthru	The following commands are executed: • telnet or ssh with passthru userid
Adding or removing a maintenance user		Security_admin	root	root, secadm	The following commands are executed: • cbmmtc, user, add <userID>, change <userID>, delete <userID>
Adding or removing a passthru user		Security_admin	root	root, secadm	The following commands are executed: • cbmmtc, pasthru, add, delete <userID>,
Setting up local user accounts on an SSPFS-based system			root	root	The following commands are executed: • useradd -g succssn <userid> • passwd -r files <userid> • groups <userid> • usermod -g succssn -G <groupA,groupB,...> <userid> **This procedure must be removed from the customer documentation (should use cbmmtc to setup users)**

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Configuring an SSPFS-based central security client NOTE: The procedure shouldn't be in SN09 NTP since central security server is not supported on CBM in SN09.		Config_admin	root	root, emsadm	The following commands are executed: • userdel <userid> • Cli, Configuration, Security Services Configuration, IEMS Server Location Configuration, iems_ip, x, PAM Configuration, Central Security Client Configuration, pam_radius, x, saml_passwd_conf **Note: This procedure should be performed through cbmmtc with secadm access.**
Configuring IPSec and IKE on the CBM 850			root	root	This procedure calls procedure "Configuring IPSec and IKE on an SSPFS-based server" (no other commands invoked).
Transferring files as a core user using FTPProxy NOTE: The procedure is out of date since site cm is no longer available.			passthru	passthru	The following commands are executed: • ftp <cbm IP address> • ftp> site cm • ftp> get output
Starting an SCFT client session			root maint	ALL	The following commands are executed: Invoke procedures: • Displaying help for SCFT • Listing volumes on Core using SCFT • Removing a file from Core using SCFT • Transferring files from Core using SCFT • Transferring files to Core using SCFT

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Transferring files from Core using SCFT			root maint	ALL	The following commands are executed: • ssh <user>@<cbm host> "scft <-b|-a> -s <reclen> -g /<volume>/<corefile>" > <localfile>
Transferring files to Core using SCFT			root maint	ALL	The following commands are executed: • ssh <user>@<host> "scft <-b|-a> -s <reclen> -p /<volume>/<corefile>" < <localfile>
Removing a file from Core using SCFT			root maint	ALL	The following commands are executed: • ssh <user>@<host>"scft -r /<volume>/<filename>"
Displaying help for SCFT			root maint	ALL	The following commands are executed: • ssh <user>@<cbm host> "scft -h"
Listing volumes on Core using SCFT			root	ALL	The following commands are executed: • ssh <user>@<host>"scft -1 /"
Configuring the time zone on an SSPFS-based server		Config_admin	root	root, emsadm	The following commands are executed: • Cli, Configuration, Location Configuration, chg_tz

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Changing a user password on an SSPFS-based system			root	root	The following commands are executed: • passwd -r files <userid> **This procedure must be removed from the customer documentation (should use cbmmtc to change user password)**
Changing a passthru user password			passthru	passthru	No commands invoked. Just login to the system as a passthru user.
Setting the threshold for file system on an SSPFS-based server		Config_admin	root	root, emsadm	The following commands are executed: • filesys update -m <mount_point> -a <threshold>
Starting an application			root, maint	ALL	The following commands are executed: • Cbmmtc, appl, bsy/rts
Starting the application group			root, maint	ALL	The following commands are executed: • Cbmmtc, appl, bsy group/rts group
Stopping an application			root, maint	ALL	The following commands are executed: • Cbmmtc, appl, bsy
Stopping the application group			root, maint	ALL	The following commands are executed: • Cbmmtc, appl, bsy group
Stopping and restarting an application			root, maint	ALL	The following commands are executed: • Cbmmtc, appl, bsy, rts

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Offlining an application			root, maint	ALL	The following commands are executed: • Cbmmtc, appl, bsy, offl
Offlining the application group			root, maint	ALL	The following commands are executed: • Cbmmtc, appl, bsy group, offl group
Displaying the CLLI from the command line			root, maint	ALL	The following commands are executed: • clli
Displaying the CLLI from BILL-MTC			root, maint	ALL	The following commands are executed: • billmtc, clli
Configuring IPSec and IKE on an SSPFS-based server			root	root	The following commands are executed: • Cli, Configuration, IP Configuration, ipsecike_config, IPSec Configuration, Add IPSec entry, x, Delete IPSec entry, x, List All IPSec entries, x, x, IKE Configuration, Add IKE entry, x, Delete IKE entry, List IKE entries, x, Change Preshared key for IKE entry
Customer doc: NN10361-711 Core and Billing Manager 850 Performance Management					
OMUI operations			root, maint	ALL	This document include only OMUI configuration procedures. These procedures are all allowed by maint users.
Customer doc: NN10355-111 Core and Billing Manager 850 Basics					

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
No procedures defined					This document provides a detailed description of the CBM and its applications.
Customer doc: NN10351-911.03.01_Core_and_Billing_Manager_850_Fault_Management (Note: all maint authorizations can run as root, emsadm and secadm)					
Clearing a CBM850 fault condition			root maint	ALL	The following commands are executed: • querycbm flt • cbmmtc, appl, bsy, rts
Clearing a CBM application Alarm			root maint	ALL	The following commands are executed: • querycbm flt • cbmmtc, appl, bsy, rts
Clearing a GDD logical volume size threshold violation			root (1) maint (2)	root (1) ALL (2)	This procedure describe two ways of fixing the problem: 1- Increase the size of the logical volume. 2- Decrease the number of days to keep the logs. The following commands are executed: 1) • cli, view, disk_util • echo '/opt/nortel/sspfs/fs/meta.pl fs' 2048 / 5000 - p | dc • filesys grow -m <mount_point> -s <size>m 2) • logroute
Clearing a major heartbeat alarm					No commands (HW check)
Replacing a failed power supply					No commands (HW check)

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Replacing failed Ethernet Interface			root	root	The following commands are executed: • mapci;mtc;appl;sdmbil;post <stream_name> • bsy • cbmmtc, appl • bsy group • offl group • **shutdown system** • Replace hardware • cbmmtc, appl • bsy group • rts group
Accessing TCP and TCP-IN log devices from a remote location			root maint	ALL	The following commands are executed: • logreceiver <port_number> • logroute
Accessing the mate			root	ALL	The following commands are executed: • GetCurrentHostName • ping <mate hostname> **root only:** • **ssh root@ <mate hostname>**
Clearing Mate alarm			root	ALL	The following commands are executed: • Access the mate • cbmmtc
Displaying SBA log reports		accounting-manage	root maint	root maint emsadm	The following commands are executed: • billmtc • displogs **procedure indicates that root user is required, however I don't see the need for root user. The document must be changed.**

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Displaying SBA alarms		fault-view	root maint	root maint emsadm	The following commands are executed: • billmtc • dispal **procedure indicates that root user is required, however I don't see the need for root user. The document must be changed.**
Collecting Debug information using the CBMGATHER command		fault-admin	root	emsadm (1) root (2)	The following commands are executed on both nodes of a CBM850 (1): • cbmgather • cd /var/adm • tar cvf varadm_active.tar *.day* *.log **root only (2):** • **compress varadm_active.tar** • **rm -f /var/adm/cbmgather_<machine>_<date_and_time>.tar.Z**
Controlling the SDM Billing Application		fault-manage	root maint	root maint emsadm	The following commands are executed: • cbmmtc, appl, bsy/rts • billmtc, schedule, rtb, bsy stream/rts stream
Displaying or storing log records using logreceiver					No commands. This procedure is performed on the client workstation.
Retrieving and viewing log records		fault-manage	root maint	root maint emsadm	The following commands are executed: • logquery

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Troubleshooting AFT alarms		fault-manage	root maint	root maint emsadm	The following commands are executed: • billmtc, appl, aft, alarm cancel <session_name>, aftconfg, delete <session_name>, start <session_name>
Troubleshooting Log Delivery problems on a CBM			root	root	The following commands are executed: • cbmmtc, appl, bsy, rts • querycbm flt • cd /cbmdata/00/gdd • ls -l • rm <file> • filesys grow -m /cbmdata/00/gdd -s <size>{m,g}
Clearing a BAK50 alarm					No commands. Procedure performed on the core.
Clearing a BAK70 alarm					No commands. Procedure performed on the core.
Clearing a BAK90 alarm					No commands. Procedure performed on the core.
Clearing a BAKUP alarm					No commands. Procedure performed on the core.
Adjusting disk apace in response to SBA backup file system alarms					No commands. Procedure performed on the core.
Clearing a CDRT alarm					No commands. Procedure performed on the core.

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Clearing a DSKWR alarm on a CBM			root	root	The following commands are executed: • Invoked procedure "Viewing customer logs on an SSPFS-based server" • Invoked procedure "Verifying disk utilization on an SSPFS-based server" • billmtc, filesys, sendfile <stream_name • ls /<stream>/ <stream_name>/ orphan • chmod 755 <directory> • chown maint:maint <directory>
Clearing an FTPW alarm		accounting-admin	root	root, emsadm	The following commands are executed: • perform procedure "Verifying the file transfer protocol"-> require root/ emsadm access
Clearing an inbound file transfer alarm			root	root	The following commands are executed: • chmod 777 /home/ maint/ftpdir • rm /<rcLogicalVolumeDirectory>/ftpdir
Clearing on LODSK alarm		accounting-admin	root	root, emsadm	The following commands are executed: • perform procedure "Verifying the file transfer protocol"-> require root/ emsadm access • Perform procedure "Verifying the FTP Schedule"

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Clearing a NOBAK alarm					No commands. Procedure performed on the core.
Clearing a NOCLNT alarm					No commands. Procedure performed on the core.
Clearing a NOREC alarm					No commands. Procedure performed on the core.
Clearing a NOSTOR alarm		accounting-manage	root maint	root maint emsadm	The following commands are executed: • Perform procedure "Clearing a major SBACP alarm"
Clearing a NOVOL alarm		accounting-manage	root maint	root maint emsadm	The following commands are executed: • Perform procedure "Clearing a major SBACP alarm"
Clearing a RTBCF alarm					No commands
Clearing an RTBER alarm					No commands
Clearing an RTBFM alarm					No commands
Clearing an RTBPD alarm					No commands
Clearing an RTBST alarm					No commands
Clearing a major SBACP alarm		accounting-manage	root maint	root maint emsadm	The following commands are executed: • cbmmtc, appl, bsy/rts • billmtc, schedule, rtb, by stream/rts stream
Clearing a minor SBACP alarm					No commands. Procedure performed on the core.

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Verifying the file transfer protocol		accounting-admin	root	root, emsadm	The following commands are executed: • billmtc, filesys, closec, listfile, sendfile, schedule, list, change, save • cp /<logical_vol>/ closedNotSent/ <file> /tmp • cd /tmp • ftp <address> <port> • ftp> stru f • ftp> put <file> <file.tmp> • ftp> rename <file.tmp> <file>
verifying the FTP Schedule		accounting-manage	root maint	root maint emsadm	The following commands are executed: • billmtc, schedule, list, change, save.
Replacing one or more failed disk drives on a SSPFS-based server			root	root	The following commands are executed: Replace the hardware • metadb -d c0t0d0s7 • prtvtoc -h /dev/ rdsk/c0t1d0s2 | fmthard -s - /dev/ rdsk/c0t0d0s2 • metareplace -e d2 c0t0d0s1 • Clone the system
Shutting down an SSPFS-based server			root	root	The following commands are executed: • init 0 • metadb -d c0t0d0s7 • prtvtoc -h /dev/ rdsk/c0t1d0s2 | fmthard -s - /dev/ rdsk/c0t0d0s2 • metareplace -e d2 c0t0d0s1 • Clone the system

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
preparing a CD_RW or DVD_RW for use		config-admin	root	root, emsadm	The following commands are executed: The following commands are executed: • cdrw -l • cdrw -b all • Cd / • eject cdrom • /etc/init.d/volmgt stop • /etc/init.d/volmgt start
Increasing the size of a file system on a SSPFS-based server			root	root	The following commands are executed: Single server CBM: • cli, View, disk_util • echo '/opt/nortel/sspfs/fs/meta.pl fs' 2048 / 5000 - p | dc • filesys grow -m <mount_point> -s <size>m CBM HA: • ubmstat • Udstat • Cli, view, disk_util • GrowClusteredFileSystem.ksh <mount_point> <size>m • init 6 • StopCluster

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Performing a backup of file systems on an SSPFS-based server		config-admin	root	root, emsadm	The following commands are executed: • mt -f /dev/rmt/0 rewind • /opt/nortel/sspfs/bks/bkfullsys • gtar -tvMf /dev/rmt/0 • gtar -tvMf /cdrom/*bkfullsys*/*.tar • cd / • eject cdrom • /etc/init.d/volmgt stop • /etc/init.d/volmgt start
Verifying disk utilization on an SSPFS-based server		config-admin	root	root, emsadm	The following commands are executed: • cli, view, disk_util
Replacing a DVD drive on an SSPFS-based server			root	root	The following commands are executed: • init 0 • replace hardware
Initiating a manual fallover on a Sun Netra 240 server pair			root	root	The following commands are executed: • swact
Viewing Customer logs on a SSPFS-based server			root	root emsadm secadm	The following commands are executed: • cd /var/log • ls • cat <log_filename> |more • cat <log_filename> |grep <search_string>
Customer doc: NN10363-811 Core and Billing Manager 850 Accounting					
Configuring a billing stream on the core manager		accounting-manage	maint root	maint root emsadm	The following commands are executed: • billmtc, confstrm, add stream, edit, save, change, save, delete stream

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Configuring a DMS-GSP CDR billing stream		accounting-manage	maint root	maint root emsadm	The following commands are executed: • mib cdr set typeofcdr gsp
Activating a billing stream on the Core					This is a core procedure
Configuring the outbound file transfer schedule		accounting-manage	maint root	maint root emsadm	The following commands are executed: • billmtc, schedule, add, save, change stream, save, delete stream,
Configuring SBA outbound connection security			root	root	The following commands are executed: • cd ~maint • ls -lad .ssh • mkdir .ssh • chown maint:maint .ssh • chmod u+rwx .ssh • su maint • ssh -l maint <nn.nn.nn.nn>
Configuring RTB for a billing stream		accounting-manage	maint root	maint root emsadm	The following commands are executed: • billmtc, schedule, rtb, confrtb, add, edit, save, change, delete
Querying the status of RTB for a billing stream		accounting-view	maint root	maint root emsadm	The following commands are executed: • billmtc, schedule, rtb, query
Returning RTB stream instance to service		accounting-manage	maint root	maint root emsadm	The following commands are executed: • billmtc, schedule, rtb, rts

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Turning auto-recovery on		accounting-manage	maint root	maint root emsadm	The following commands are executed: • cbmmtc, appl, bsy, offl • billmtc, schedule, rtb, confrtb, autorec on • cbmmtc, appl, bsy, rts
Turning auto-recovery off		accounting-manage	maint root	maint root emsadm	The following commands are executed: • cbmmtc, appl, bsy, offl • billmtc, schedule, rtb, confrtb, autorec off • cbmmtc, appl, bsy, rts
Retrieving billing files for a stream set to inbound file transfer mode			maint only	maint only	The following commands are executed: • ftp <core manager's IP address> • ftp> cd ftpdir/ <stream name> • ftp> ls • ftp> get <file-name.extension> • ftp> rename <file-name>.pri <file-name>.sec
Activating or deactivating secondary file processing		accounting-admin	root	root emsadm	The following commands are executed: • cbmmtc, appl, bsy • billmtc, appl, sfp, act/deact

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Copying billing files to DVD using SBADVDWRITE		accounting-admin	root	root, emsadm	The following commands are executed: • /usr/bin/cdrw -l • /usr/bin/eject cdrom **root only (These steps are not needed for this procedure unless error occurs when ejecting a CD:** • **/etc/init.d/volmgt stop** • **/etc/init.d/volmgt start** • sbadvdwrite • cd cdrom/cdrom0/ <stream name>/ <directory name> • ls -lA
Copying billing files to DVD manually			root	root	The following commands are executed: • /usr/bin/cdrw -l • /usr/bin/eject cdrom • /etc/init.d/volmgt stop • /etc/init.d/volmgt start • cd <directory> • /usr/bin/ls -l • /usr/bin/mkisofs -o <destination file> -a -J -L -R <path-spec> • /usr/bin/mkisofs -o <destination file> -a -J -L -R <path-spec> • /usr/bin/cdrw -C -i <ISO9660 file> • /usr/bin/rm <ISO9660 file>

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Preparing a CD_RW or DVD_RW for use		config-admin	root	root, emsadm	The following commands are executed: The following commands are executed: The following commands are executed: • cdrw -l • cdrw -b all • Cd / • eject cdrom **root only (These steps are not needed for this procedure unless error occurs when ejecting a CD:** • **/etc/init.d/volmgt stop** • **/etc/init.d/volmgt start**
Adding a logical volume for SBA through the command line		config-admin	root	root, emsadm	The following commands are executed: • makelv <logical_volume_name> <logical_volume_size>
Configure an AFT session		accounting-manage	maint root	maint root emsadm	The following commands are executed: • billmtc, appl, aft, aftconf, add OCC <session_name> <destination> [RETRY <retry_attempts>, quit, start <session_name>
Querying a billing stream		accounting-manage	maint root	maint root emsadm	The following commands are executed: • billmtc, query stream, query all

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Searching and viewing billing records		accounting-view	maint root	maint root emsadm	The following commands are executed: • billmtc, tools, amadump <stream-name>, AMADUMP>> dump <display_mode> [sum] [numout <numout_value>] [numsrch <numsearch_value>] [numblk <numblock_value>] [filter <filter_string> or <%filter_number>] [fname <file-name>] [btime <start_time>] [etime <end_time>] • listfile <stream-name>
Listing billing files		accounting-view	maint root	maint root emsadm	The following commands are executed: • billmtc, filesys, • listfile <stream_name> <optional_parameters>,
Listing billing streams		accounting-view	maint root	maint root emsadm	The following commands are executed: • billmtc, confstrm, • list {<stream_name> | ALL},
closing billing files		accounting-manage	maint root	maint root emsadm	The following commands are executed: • billmtc, filesys, • closec <stream_name>

Table 6: Authorization Summary - CBM NTP Customer Documentation

Operation/ Command	Current Action	New Action	Current auth. level	New auth. level	Note
Sending billing files from disk		accounting-manage	maint root	maint root emsadm	The following commands are executed: • billmtc, filesys, • sendfile <stream_name> [<optional_parameters>]

Note: When the new authorization level is “ALL”, it indicates that users in all groups (maint, emsadm and secadm) and the root user have access to that command.

164.7 Hardware Requirements or Dependencies

There are no hardware requirements for this feature.

164.8 Software Requirements or Dependencies

This feature builds on two other CBM23 security features:

- A00012465 - CBM User Authorization Integration with a Nortel Central Security Server (Wireless application).
- A00012729 - CBM Application GID Migration.

164.9 Limitations and restrictions

No user interface is provided to create additional authorization levels.

Only commands that are specified in this document will be supported by this feature. In the future, other applications or commands will be revised to use this authorization scheme.

Some commands do not check for authorizations, and therefore these commands would be accessible by all users.

164.10 Interactions

This feature will change the RMI for user creation.

164.11 Glossary

Term	Description
API	Application Program Interface
CBM	Core and Billing Manage
CNM	CDMA Network Manager
CLI	Command Line Interface
IEMS	Integrated Element Manager System
MS	Management System
MSAP	Management System Application
MSOS	Management System Operating System
NE	Network Element
NE/MS	NE or MS
PAM	Pluggable Authentication Modules
RBAC	Role Based Access Control
RMI	Resource Manager Interface
SBA	SuperNode Billing Application
SDM	Super Node Data Manager
SPFS	Succession Platform Foundation Software

165: Functional Description (FN) A00012622

165.1 Feature name and Feature ID

A00012622 - Platform HW Alarm Reporting

165.2 Description

This activity provides the capability for the MCS System Manager to monitor HP CC3310 servers, IBM blade servers, and the IBM BladeCenter chassis for hardware faults.

Alarms are generated for four kinds of hardware faults.

Power Supply. A minor alarm raised when any power supply operates outside of specifications or any voltage sensor reports a value outside of specifications.

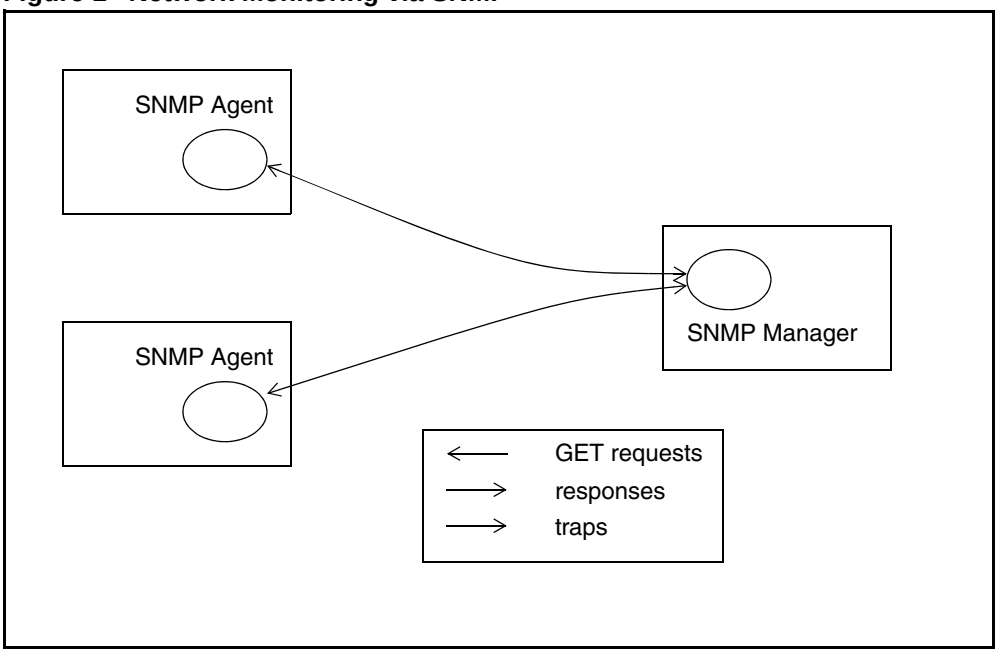
Cooling Device. A minor alarm is raised when any cooling device (fan or blower) operates outside of specifications.

Temperature. A minor alarm is raised when any temperature sensor exceeds its specified threshold.

Processor. A minor alarm is raised when a CPU failure is detected (available on the BC-T only).

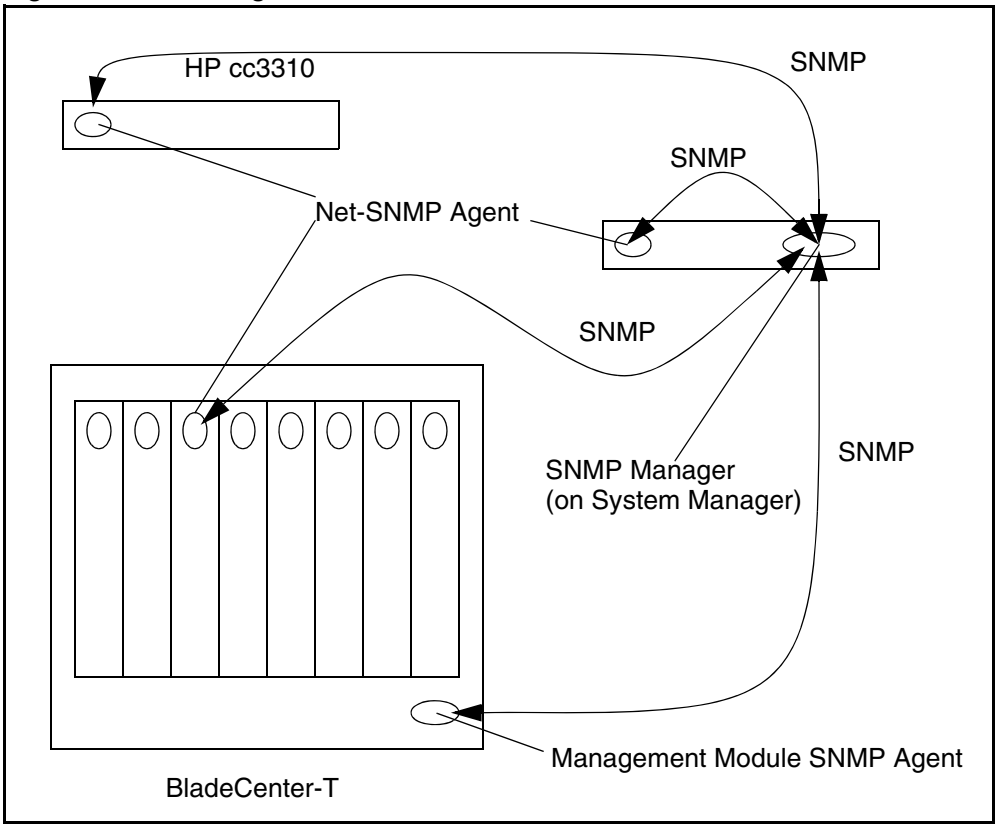
The System Manager monitors configured servers using the SNMP protocol. A high level depiction of the use of SNMP is shown in Figure 1. The SNMP protocol is exchanged between an SNMP Agent and an SNMP Manager. An SNMP agent is responsible for reporting the values of variables defined by one or more Management Information Base specification documents. An SNMP manager is an entity capable of requesting MIB variable values from SNMP Agents. An SNMP agent may also be configured to spontaneously report events to an SNMP Manager; these event reports are called *traps*.

Figure 1 Network Monitoring via SNMP



The SNMP protocol provides a mechanism enabling the SNMP Manager to cause an SNMP Agent to alter the values of some MIB variables. This mechanism, referred to as “SNMP Set”, justifies the term “management” in SNMP. This capability is disabled under MCS for security reasons. The MCS therefore *monitors* servers, but does not *manage* them.

Figure 2 Monitoring the CC3310 and BC-T

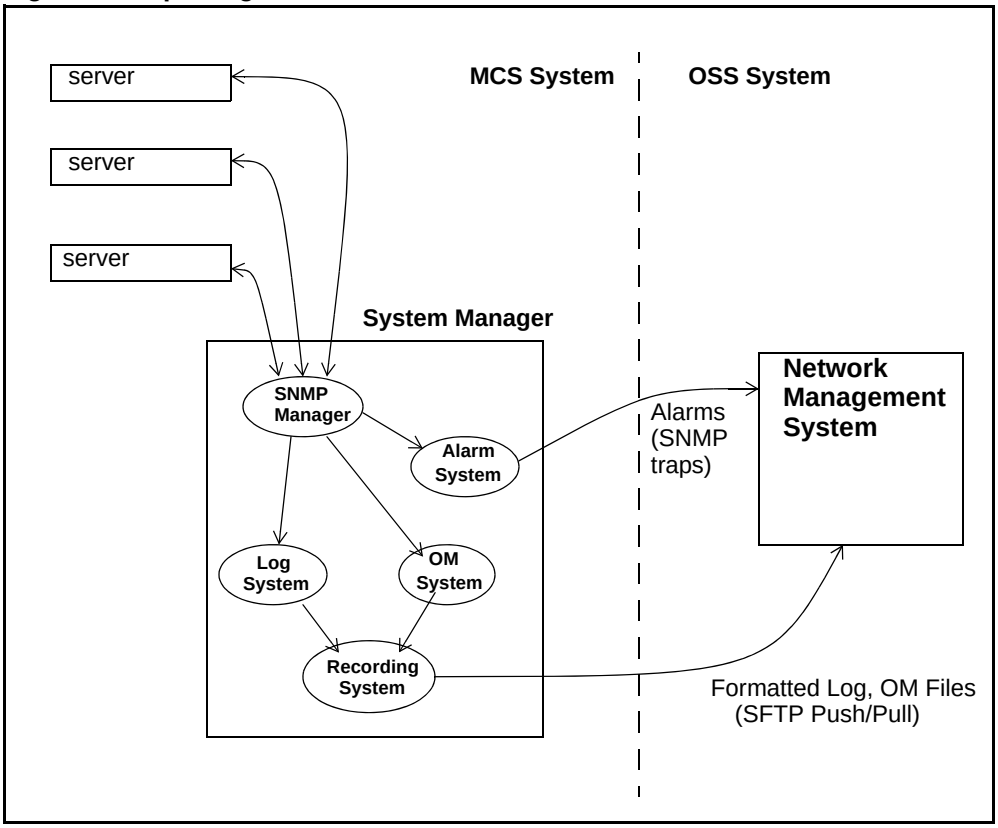


A more detailed view is shown in Figure 2. The open source Net-SNMP agent is installed on all MCS servers. Resource utilization measurements are available from these agents under the well known MIB-2 standard.

On the HP CC3310, hardware faults are reported through the Net-SNMP agent using the mapbase4 MIB provided by HP.

BladeCenter servers do not report their own hardware faults; this function is provided by an SNMP agent running in the BladeCenter Management Module using the mmblade MIB provided by IBM.

Figure 3 Reporting to the NMS



The general flow of network management information is shown in Figure 3. The System Manager polls SNMP agents running on monitored servers for the raw data from which to generate operational measurements. Some of these measurements are instrumented with configured alarm thresholds. The System Manager raises and clears alarms when these thresholds are crossed. Alarms are reported to registered parties as SNMP traps defined under the Nortel Reliable MIB. A log is generated whenever an alarm is raised or cleared.

Formatted logs and OMs are reported to the recording system on the System Manager which persists them in the local file system. Formatted record files are available via SFTP pull.

165.3 Hardware Requirements or Dependencies

The hardware fault reporting implemented under this activity is available only for the CC3310 and BC-T.

165.4 Software Requirements or Dependencies

The CC3310 implementation relies upon the dmi2snmp process supplied by HP and the SMUX capability of Net-SNMP.

165.5 Limitations and restrictions

Processor failure is reported only for the BC-T.

Monitoring must be started manually (from the System Management Console). Once started, the administrative state of the monitor is maintained over System Manager restarts so that monitoring will automatically resume.

165.6 Interactions

The Oracle SNMP agent must be configured not to use the well-known TCP port 199 for the SMUX protocol.

165.7 Glossary

Term	Description
BC-T	BladeCenter -Telco. A NEBS-compliant version of the IBM BladeCenter.
BIST	Built-In Self Test. A capability for equipment to test itself for defects by comparing self-administered known inputs to expected outputs.
DMI	Desktop Management Interface. A standard for remote computer maintenance.
DMTF	Distributed Management Task Force. The standards organization responsible for defining the Desktop Management Interface.
ITU	International Telecommunication Union
MIB	Management Information Base. A data structure and documentation describing the information accessible via SNMP
MM	Management Module. The BladeCenter management module.
PDU	Protocol Data Unit. A data packet formatted according to some particular protocol.
SMUX	SNMP Multiplexing. A standard for instructing an SNMP agent to delegate processing of a MIB subtree to another process.
SNMP	Simple Network Management Protocol. A standard networking protocol. UDP is unreliable, meaning that data may be lost, duplicated, or received out of order.

166: Functional Description (FN) A00012635

166.1 Feature name and Feature ID

A00012635 - Netra 240 146 GB Disk Drive Upgrade

166.2 Description

Due to the increasing foot print of data stored by the applications on SPFS, the servers are running out of available disk drive space. To resolve this disk space need, the field grade Netra 240 servers can be upgraded with 146 GB drives, replacing the existing two 72 GB drives. Although the existing servers can be manually upgraded today, this feature provides an automated upgrade utility to greatly reduce the complexity and interaction required by the personnel performing the disk drive upgrade.

166.2.1 Performing the 146GB Upgrade - High level view

Below is a high level description of the manual steps required to perform this procedure and then a session of the output when the automated utility is invoked. The automated process will log all steps below to the /var/adm/ messages file for ease of GNPS to debug any error or interruption in the field. Note, most of the user's time will be spent waiting for disk mirrors to synchronize.

Simplex unit or Cluster active unit high level description

1. Invoke the disk upgrade utility from cli. Provide a description of the action to be taken, warn user about implications of aborting procedure, and finally get user's confirmation to continue.
2. Perform Prechecks:

- System must be field grade N240 with existing 2 x 72 GB drives
- All mirrors must have full redundancy, in an 'Okay' state.
- Warn the user if the utility is not invoked from the console. Force confirmation if the console is not used for this upgrade.
- Check for the existence of the /Mtce InProgress file which indicates other significant SPFS maintenance is in progress such as a software upgrade or clone. If the file exists, do not continue.
- Set mtce in progress so other SPFS maintenance actions are aware of this activity in progress.

3. Obtain and persist metastat information.
4. Select first disk and remove it from the boot device list.

5. Detach submirrors for selected disk.
6. Clear metastat information for detached submirrors.
7. Remove selected disk device from meta database.
8. Unconfigure selected disk device (blue light on chassis is now lit indicating which disk should be removed).
9. Instruct user to remove old disk and insert new 146 GB disk drive.
10. Ensure 146 GB disk drive is inserted. Selected disk is now 146 GB disk drive.
11. Configure selected disk.
12. Format selected disk.
13. Meta initialize submirrors with selected disk.
14. Attach the submirrors one at a time, displaying synchronization status periodically.
15. Update boot device list with selected device.
16. Perform disk state checks again.
17. Repeat steps 4 - 15 for the other disk device.
18. Create a customer log indicating the upgrade is complete.
19. Instruct user to take a full system backup immediately.

Cluster Mate Unit Upgrade high level description

For an SPFS cluster only, upgrading the inactive node would be slightly more than the time it takes to perform a clone. These steps are manual and would consist of the following:

1. Put the inactive node at the ‘ok’ prompt.
2. Replace both 72 GB disks with the 146 GB disks.
3. Follow the existing documented procedure to perform a clone.

166.2.2 Example Session of a Successful 146 GB Upgrade

The following is an example of the commands the user would enter to invoke the 146 GB upgrade. Shown below are the messages displayed for a successful upgrade along with the expected input required by the user. Additionally, sample design logs are also displayed which would be used in the event an unexpected error occurred and additional support was needed.

spfs-server:/> cli
Command Line Interface
 1 - View

```
 2 - Configuration
 3 - Other

 X - exit

select - 2

Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Disk Drive Upgrade
16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)


 X - exit

select - 15

Disk Drive Upgrade
 1 - disk_drive_upgrade_146gb (Perform 146 GB Disk Drive Upgrade)

 X - exit

select - 1
```

```
################################################################################
##
#####                        Hard Drive Upgrade Utility                    #####
################################################################################
##
This program is an automated utility which will assist with upgrading the disk drives in this
server to 146 GB disk drives. This procedure will disable the disk mirroring one disk at a time,
which means one of the redundant disks will be out of service or not fully capable of providing
service until this procedure is complete. If the other disk fails or is removed inadvertently, sig-
nificant recovery time should be expected.

It is highly recommended that this procedure be invoked from the system console. Due to the
length of time to synchronize the mirrors each time a disk is replaced, expect this procedure to
take at least 4 hours to complete. Any interruption to the automated utility (i.e. loss of connec-
tion, terminating the process) will require the user to manually complete the disk drive upgrade
or recover from the disk drive upgrade.

Lastly, a recent system and data backup should be available before continuing with this disk
drive upgrade procedure. These will be needed if an unexpected restore is required.
Do you want to continue? [no] y


************************************************************
*                  Removing disk 0 from the boot device list           *
************************************************************
The boot device list has been updated to: disk1:b


************************************************************
*                  Detaching Submirrors on disk 0                      *
************************************************************
d11: submirror d9 is detached
d8: submirror d6 is detached
d5: submirror d3 is detached
d2: submirror d0 is detached
d100: submirror d101 is detached


************************************************************
*                  Clearing Submirrors on disk 0                       *
************************************************************
d9: Concat/Stripe is cleared
d6: Concat/Stripe is cleared
```

```
d3: Concat/Stripe is cleared
d0: Concat/Stripe is cleared
d101: Concat/Stripe is cleared


************************************************************
*                  Deleting disk 0 from the meta database  *
************************************************************
Deleted device c1t0d0s7 from the Meta database.


************************************************************
*                  Unconfiguring disk 0                    *
************************************************************
Unconfigured disk device c1::dsk/c1t0d0


************************************************************
*                  Removing disk 0                         *
*          * Manual Action Is Required For This Step *     *
*      **Warning** Removing the wrong disk will most likely *
*                  result in extended service loss.        *
************************************************************

Please replace disk 0 with the new 146 GB disk drive. The disk to be replaced
is labeled "HDD 0" on the chassis. The blue removal lamp should be lit on
the chassis, adjacent to the disk drive to be removed. Confirm below when the
disk drive has been replaced.
Has the disk drive been replaced? [no] y


************************************************************
*    Scanning for all current system devices               *
************************************************************
System device scan finished.


************************************************************
*    Checking that disk 0 is present                       *
************************************************************
Disk 0 is present.
```

```
************************************************************
*       Configuring disk 0                                 *
************************************************************
Configured disk device c1::dsk/c1t0d0


************************************************************
*       Checking that disk 0 is the expected size          *
************************************************************
Disk 0 size is correct, 146 GB


************************************************************
*       Formatting disk 0                                  *
************************************************************
Disk format completed for /dev/rdsk/c1t0d0s2
fmthard:  New volume table of contents now in place.


************************************************************
*       Adding disk 0 to the meta database                 *
************************************************************
Added device c1t0d0s7 to the Meta database.


************************************************************
*       Initializing Submirrors on disk 0                  *
************************************************************
d9: Concat/Stripe is setup
d6: Concat/Stripe is setup
d3: Concat/Stripe is setup
d0: Concat/Stripe is setup
d101: Concat/Stripe is setup


************************************************************
*                                                          *
*       Updating disk id for disk 0 in the meta database   *
*                                                          *
************************************************************
Updating Solaris Volume Manager device relocation information for c1t0d0
Old device reloc information:
     id1,sd@SFUJITSU_MAT3147N_SUN146G000510C00NCY____AAC0P5300NCY
```

```
New device reloc information:
      id1,sd@SFUJITSU_MAT3147N_SUN146G000510C00NCY____AAC0P5300NCY
Meta device id updated for c1t0d0


************************************************************
*       Attaching Submirrors on disk 0                     *
*  *Note* Synchronizing of the Mirrors will take several   *
*              minutes per mirror to complete.             *
************************************************************
d11: submirror d9 is attached
Waiting for Mirror d11 to synchronize:    Resync in progress: 0 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 3 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 7 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 11 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 15 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 19 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 23 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 27 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 31 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 35 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 39 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 43 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 48 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 52 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 56 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 60 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 64 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 68 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 72 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 75 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 79 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 83 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 87 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 91 % done
Waiting for Mirror d11 to synchronize:    Resync in progress: 95 % done
Synchronization of Mirror d11 is complete
d8: submirror d6 is attached
Waiting for Mirror d8 to synchronize:    Resync in progress: 0 % done
Waiting for Mirror d8 to synchronize:    Resync in progress: 9 % done
Waiting for Mirror d8 to synchronize:    Resync in progress: 20 % done
Waiting for Mirror d8 to synchronize:    Resync in progress: 30 % done
Waiting for Mirror d8 to synchronize:    Resync in progress: 40 % done
```

```
Waiting for Mirror d8 to synchronize:    Resync in progress: 51 % done
Waiting for Mirror d8 to synchronize:    Resync in progress: 61 % done
Waiting for Mirror d8 to synchronize:    Resync in progress: 72 % done
Waiting for Mirror d8 to synchronize:    Resync in progress: 82 % done
Waiting for Mirror d8 to synchronize:    Resync in progress: 92 % done
Synchronization of Mirror d8 is complete
d5: submirror d3 is attached
Waiting for Mirror d5 to synchronize:    Resync in progress: 0 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 4 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 9 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 15 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 20 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 25 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 31 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 36 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 42 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 47 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 53 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 58 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 63 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 69 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 74 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 79 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 85 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 90 % done
Waiting for Mirror d5 to synchronize:    Resync in progress: 96 % done
Synchronization of Mirror d5 is complete
d2: submirror d0 is attached
Waiting for Mirror d2 to synchronize:    Resync in progress: 0 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 4 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 9 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 14 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 20 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 25 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 30 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 36 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 41 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 46 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 52 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 57 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 62 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 68 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 73 % done
```

```
Waiting for Mirror d2 to synchronize:    Resync in progress: 78 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 83 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 89 % done
Waiting for Mirror d2 to synchronize:    Resync in progress: 94 % done
Synchronization of Mirror d2 is complete
d100: submirror d101 is attached
Waiting for Mirror d100 to synchronize:    Resync in progress: 0 % done
Waiting for Mirror d100 to synchronize:    Resync in progress: 10 % done
Waiting for Mirror d100 to synchronize:    Resync in progress: 20 % done
Waiting for Mirror d100 to synchronize:    Resync in progress: 30 % done
Waiting for Mirror d100 to synchronize:    Resync in progress: 40 % done
Waiting for Mirror d100 to synchronize:    Resync in progress: 51 % done
Waiting for Mirror d100 to synchronize:    Resync in progress: 60 % done
Waiting for Mirror d100 to synchronize:    Resync in progress: 70 % done
Waiting for Mirror d100 to synchronize:    Resync in progress: 80 % done
Waiting for Mirror d100 to synchronize:    Resync in progress: 90 % done
Synchronization of Mirror d100 is complete


************************************************************
*       Updating boot device list with disk 0                                *
************************************************************
The boot device list has been updated to: disk1:b disk0:b
```

At this point, similar actions and output would be displayed for disk 1, starting with “Removing disk 1 from the boot device list”. Upon completion of the disk 1 upgrade, the following message would be displayed:

```
*** Disk drive upgrade procedure has completed successfully. ***
*** Please take a new full system backup as soon as possible. ***
```

Example logs from /var/adm/messages recording the progression of the upgrade.

```
Oct  3 13:15:30 nbound HD_Upgrade: Beginning the Hard Drive Upgrade Procedure
Oct  3 13:15:30 nbound HD_Upgrade: The boot device list has been updated to: disk1:b
Oct  3 13:15:33 nbound HD_Upgrade: d11: submirror d9 is detached
Oct  3 13:15:36 nbound HD_Upgrade: d8: submirror d6 is detached
Oct  3 13:15:38 nbound HD_Upgrade: d5: submirror d3 is detached
Oct  3 13:15:40 nbound HD_Upgrade: d2: submirror d0 is detached
Oct  3 13:15:42 nbound HD_Upgrade: d100: submirror d101 is detached
Oct  3 13:15:47 nbound HD_Upgrade: d9: Concat/Stripe is cleared
Oct  3 13:15:49 nbound HD_Upgrade: d6: Concat/Stripe is cleared
Oct  3 13:15:52 nbound HD_Upgrade: d3: Concat/Stripe is cleared
Oct  3 13:15:54 nbound HD_Upgrade: d0: Concat/Stripe is cleared
```

Oct 3 13:15:56 nbound HD_Upgrade: d101: Concat/Stripe is cleared
Oct 3 13:16:01 nbound HD_Upgrade: Deleted device c1t0d0s7 from the Meta database.
Oct 3 13:16:05 nbound unix: /pci@1c,600000/scsi@2/sd@0,0 (sd0) offline
Oct 3 13:16:05 nbound HD_Upgrade: Unconfigured disk device c1::dsk/c1t0d0
Oct 3 13:16:09 nbound unix: DISK @ HDD0 has been removed.
Oct 3 13:16:17 nbound unix: DISK @ HDD0 has been inserted.
Oct 3 13:16:22 nbound HD_Upgrade: Disk 0 is present.
Oct 3 13:16:24 nbound unix: sd0 at glm0: target 0 lun 0
Oct 3 13:16:24 nbound unix: sd0 is /pci@1c,600000/scsi@2/sd@0,0
Oct 3 13:16:24 nbound unix: /pci@1c,600000/scsi@2/sd@0,0 (sd0) online
Oct 3 13:16:24 nbound HD_Upgrade: Configured disk device c1::dsk/c1t0d0
Oct 3 13:16:29 nbound HD_Upgrade: Disk 0 size is correct, 146 GB
Oct 3 13:16:32 nbound HD_Upgrade: Disk format completed for /dev/rdsk/c1t0d0s2
Oct 3 13:16:32 nbound HD_Upgrade: fmthard: New volume table of contents now in place.
Oct 3 13:16:36 nbound HD_Upgrade: Added device c1t0d0s7 to the Meta database.
Oct 3 13:16:39 nbound HD_Upgrade: d9: Concat/Stripe is setup
Oct 3 13:16:41 nbound HD_Upgrade: d6: Concat/Stripe is setup
Oct 3 13:16:44 nbound HD_Upgrade: d3: Concat/Stripe is setup
Oct 3 13:16:46 nbound HD_Upgrade: d0: Concat/Stripe is setup
Oct 3 13:16:48 nbound HD_Upgrade: d101: Concat/Stripe is setup
Oct 3 13:16:53 nbound HD_Upgrade: d11: submirror d9 is attached
Oct 3 13:16:54 nbound HD_Upgrade: Waiting for Mirror d11 to synchronize: Resync in progress: 0 % done
Oct 3 13:17:24 nbound HD_Upgrade: Waiting for Mirror d11 to synchronize: Resync in progress: 3 % done
Oct 3 13:17:54 nbound HD_Upgrade: Waiting for Mirror d11 to synchronize: Resync in progress: 7 % done
Oct 3 13:18:24 nbound HD_Upgrade: Waiting for Mirror d11 to synchronize: Resync in progress: 11 % done
.
.
.

Oct 3 13:28:58 nbound HD_Upgrade: Waiting for Mirror d11 to synchronize: Resync in progress: 95 % done
Oct 3 13:29:28 nbound HD_Upgrade: Synchronization of Mirror d11 is complete
Oct 3 13:29:29 nbound HD_Upgrade: d8: submirror d6 is attached
Oct 3 13:29:29 nbound HD_Upgrade: Waiting for Mirror d8 to synchronize: Resync in progress: 0 % done
Oct 3 13:29:59 nbound HD_Upgrade: Waiting for Mirror d8 to synchronize: Resync in progress: 9 % done

Oct 3 13:30:29 nbound HD_Upgrade: Waiting for Mirror d8 to synchronize: Resync in progress: 20 % done
.
.
.
Oct 3 13:34:00 nbound HD_Upgrade: Waiting for Mirror d8 to synchronize: Resync in progress: 92 % done
Oct 3 13:34:31 nbound HD_Upgrade: Synchronization of Mirror d8 is complete
Oct 3 13:34:31 nbound HD_Upgrade: d5: submirror d3 is attached
Oct 3 13:34:31 nbound HD_Upgrade: Waiting for Mirror d5 to synchronize: Resync in progress: 0 % done
Oct 3 13:35:01 nbound HD_Upgrade: Waiting for Mirror d5 to synchronize: Resync in progress: 4 % done
Oct 3 13:35:31 nbound HD_Upgrade: Waiting for Mirror d5 to synchronize: Resync in progress: 9 % done
Oct 3 13:36:01 nbound HD_Upgrade: Waiting for Mirror d5 to synchronize: Resync in progress: 15 % done
.
.
.

OOct 3 13:43:33 nbound HD_Upgrade: Waiting for Mirror d5 to synchronize: Resync in progress: 96 % done
Oct 3 13:44:04 nbound HD_Upgrade: Synchronization of Mirror d5 is complete
Oct 3 13:44:04 nbound HD_Upgrade: d2: submirror d0 is attached
Oct 3 13:44:04 nbound HD_Upgrade: Waiting for Mirror d2 to synchronize: Resync in progress: 0 % done
Oct 3 13:44:34 nbound HD_Upgrade: Waiting for Mirror d2 to synchronize: Resync in progress: 4 % done
Oct 3 13:45:05 nbound HD_Upgrade: Waiting for Mirror d2 to synchronize: Resync in progress: 9 % done
.
.
.
Oct 3 13:53:07 nbound HD_Upgrade: Waiting for Mirror d2 to synchronize: Resync in progress: 94 % done
Oct 3 13:53:37 nbound HD_Upgrade: Synchronization of Mirror d2 is complete
Oct 3 13:53:38 nbound HD_Upgrade: d100: submirror d101 is attached
Oct 3 13:53:38 nbound HD_Upgrade: Waiting for Mirror d100 to synchronize: Resync in progress: 0 % done
Oct 3 13:54:08 nbound HD_Upgrade: Waiting for Mirror d100 to synchronize: Resync in progress: 10 % done

Oct 3 13:54:38 nbound HD_Upgrade: Waiting for Mirror d100 to synchronize: Resync in progress: 20 % done
.
.
.

Oct 3 13:58:10 nbound HD_Upgrade: Waiting for Mirror d100 to synchronize: Resync in progress: 90 % done
Oct 3 13:58:40 nbound HD_Upgrade: Synchronization of Mirror d100 is complete
Oct 3 13:58:43 nbound HD_Upgrade: The boot device list has been updated to: disk1:b disk0:b
.
.
Disk 1 logs are output...
.
.

Oct 3 14:43:43 nbound HD_Upgrade: Disk drive upgrade procedure has completed successfully

166.2.3 Examples of Possible Error Messages

Below are examples of error messages that could occur during the upgrade.

New disk is not inserted even though it was confirmed.

The following message would be seen if the user confirmed the disk was changed but the disk was not inserted:

.
.
```
************************************************************
*         Checking that disk 0 is present                  *
************************************************************

"Error: Disk 0 is not detected.

** Warning ** Because of the failure above that occurred after disk 0
replacement, it must be replaced or reseated again.
If yould would like to replace or reseat the disk drive, enter 'yes' below.
Enter 'no' if you want to abort the upgrade procedure.
Do you want to retry this action?


************************************************************
*                       Removing disk 0                    *
*                * Manual Action Is Required For This Step *                *
```

```
*            **Warning** Removing the wrong disk will most likely          *
*                          result in extended service loss.                *
************************************************************************
```

Please replace disk 0 with the new 146 GB disk drive. The disk to be replaced is labeled "HDD 0" on the chassis. The blue removal lamp should be lit on the chassis, adjacent to the disk drive to be removed. Confirm below when the disk drive has been replaced.
Has the disk drive been replaced? [no] y
.

.Upgrade program is not invoked by the root user.

The following message would be seen if the user invoking the upgrade procedure is not root:

```
##############################################################################
##
#####                        Hard Drive Upgrade Utility                  #####
##############################################################################
##
```

This program is an automated utility which will assist with upgrading the disk drives in this server to 146 GB disk drives. This procedure will disable the disk mirroring one disk at a time, which means one of the redundant disks will be out of service or not fully capable of providing service until this procedure is complete. If the other disk fails or is removed inadvertently, significant recovery time should be expected.

It is highly recommended that this procedure be invoked from the system console. Due to the length of time to synchronize the mirrors each time a disk is replaced, expect this procedure to take at least 4 hours to complete. Any interruption to the automated utility (i.e. loss of connection, terminating the process) will require the user to manually complete the disk drive upgrade or recover from the disk drive upgrade.

Lastly, a recent system and data backup should be available before continuing with this disk drive upgrade procedure. These will be needed if an unexpected restore is required.
Do you want to continue? [no] y

This program requires it to be invoked by the root user, exiting the program.

Disk drive upgrade utility exiting because of precheck failures.
Correct the failure(s) displayed above before retrying.

The current server does not have 72 GB disks currently installed.

The following message would be seen if the server didn't have the required 72 GB disk drives currently installed:

```
.#############################################################################
###
#####                        Hard Drive Upgrade Utility                  #####
#############################################################################
##
```

This program is an automated utility which will assist with upgrading the disk drives in this server to 146 GB disk drives. This procedure will disable the disk mirroring one disk at a time, which means one of the redundant disks will be out of service or not fully capable of providing service until this procedure is complete. If the other disk fails or is removed inadvertently, significant recovery time should be expected.

It is highly recommended that this procedure be invoked from the system console. Due to the length of time to synchronize the mirrors each time a disk is replaced, expect this procedure to take at least 4 hours to complete. Any interruption to the automated utility (i.e. loss of connection, terminating the process) will require the user to manually complete the disk drive upgrade or recover from the disk drive upgrade.

Lastly, a recent system and data backup should be available before continuing with this disk drive upgrade procedure. These will be needed if an unexpected restore is required.
Do you want to continue? [no] y

Error: Disk 0 size is 36 GB. This value is less than the minimum required disk size which is 72 GB.

Disk drive upgrade utility exiting because of precheck failures.
Correct the failure(s) displayed above before retrying.

166.2.4 146 GB Disk Drive Rollback to 72 GB disk drive

It is possible but not expected to rollback one or both of the 146 disk drives to the 72 GB drives.

Rolling back one of the 72 GB drives

The only for seeable reason why a 146 GB drive would have to be rolled back during the upgrade procedure is a disk failure. It is impossible to predict at what point a failure could occur. An automated recovery mechanism does not exist to recover from a disk failure during the upgrade.

The automated utility persists information about the upgrade to facilitate any manual recovery. One important piece of persisted information is the output of the meta data prior to beginning the upgrade, stored in file /var/tmp/

meta_backup. Other important persisted data is found in the /var/adm/ messages. This file will contain all of the messages from the upgrade utility when a change or modification is attempted by the utility. It contains success and failure messages which allows the user to observe the progression of the upgrade if their console session is not available.

By using the meta data prior to the upgrade and knowing at which point the upgrade failed, the user can attempt to manually finish the 146 GB upgrade or rollback to the 72 GB disk drive.

Example: New 146 GB disk drive fails right after insertion for disk 0 (i.e. configuration fails) and the on-site personnel doesn't have three new drives on hand so they want to back out. This utility may fail to configure the drive and the user chooses to abort the upgrade after the configuration failure.

The persisted meta data that shows the mirror and submirror mappings in file /var/tmp/meta_data looks like:

```
d11 -m d9 d10 1
d9 1 1 c1t0d0s4
d10 1 1 c1t1d0s4
d8 -m d6 d7 1
d6 1 1 c1t0d0s3
d7 1 1 c1t1d0s3
d5 -m d3 d4 1
d3 1 1 c1t0d0s0
d4 1 1 c1t1d0s0
d2 -m d0 d1 1
d0 1 1 c1t0d0s1
d1 1 1 c1t1d0s1
d100 -m d101 d102 1
d101 1 1 c1t0d0s5
d102 1 1 c1t1d0s5
```

Using the /var/adm/messages logs (or the users session), the following logs were found for the upgrade of disk 0:

```
Oct  3 13:15:30 nbound HD_Upgrade: Beginning the Hard Drive Upgrade Procedure
Oct  3 13:15:33 nbound HD_Upgrade: d11: submirror d9 is detached
Oct  3 13:15:36 nbound HD_Upgrade: d8: submirror d6 is detached
Oct  3 13:15:38 nbound HD_Upgrade: d5: submirror d3 is detached
Oct  3 13:15:40 nbound HD_Upgrade: d2: submirror d0 is detached
Oct  3 13:15:42 nbound HD_Upgrade: d100: submirror d101 is detached
Oct  3 13:15:47 nbound HD_Upgrade: d9: Concat/Stripe is cleared
Oct  3 13:15:49 nbound HD_Upgrade: d6: Concat/Stripe is cleared
```

```
Oct  3 13:15:52 nbound HD_Upgrade: d3: Concat/Stripe is cleared
Oct  3 13:15:54 nbound HD_Upgrade: d0: Concat/Stripe is cleared
Oct  3 13:15:56 nbound HD_Upgrade: d101: Concat/Stripe is cleared
Oct  3 13:16:01 nbound HD_Upgrade: Deleted device c1t0d0s7 from the Meta database.
Oct  3 13:16:05 nbound unix: /pci@1c,600000/scsi@2/sd@0,0 (sd0) offline
Oct  3 13:16:05 nbound HD_Upgrade: Unconfigured disk device c1::dsk/c1t0d0
Oct  3 13:16:09 nbound unix: DISK @ HDD0 has been removed.
Oct  3 13:16:17 nbound unix: DISK @ HDD0 has been inserted.
Oct  3 13:16:22 nbound HD_Upgrade: Disk 0 is present.
Oct  3 13:16:24 nbound HD_Upgrade: Failed to configure disk device c1::dsk/c1t0d0
```

The user would then have to manually recover/rollback to the 72 GB by doing the following (which is basically a reverse of what was done):

1. Replace the failed 146 GB drive with the original 72 GB drive.
2. Configure the disk: *cfgadm -c configure c1::dsk/c1t0d0*
3. Add the disk to the meta database: *metadb -af c1t0d0s7*
4. Initialize each of the submirrors that were cleared (from the logs above, message “d9: Concat/Stripe is cleared”) by using the meta data from above:
   a. *metainit d9 1 1 c1t0d0s4*
   b. *metainit d6 1 1 c1t0d0s3*
   c. *metainit d3 1 1 c1t0d0s0*
   d. *metainit d0 1 1 c1t0d0s1*
   e. *metainit d101 1 1 c1t0d0s5*
5. Attach the submirrors one at a time, waiting for each mirror to finish synchronization prior to starting the next one. The synchronization status can be checked by invoking ‘metastat <mirror>’.
   a. *metattach d11 d9*
   b. *metattach d8 d6*
   c. *metattach d5 d3*
   d. *metattach d2 d0*
   e. *metattach d100 d101*
6. Add the disk back to the boot list: *eeprom boot-device=”disk0:b disk1:b”*

Rolling back both 146 GB drives to 72 GB drives

It is unforeseeable why the 146 GB drives would be rolled back to the 72 GB drives. The following is the high level description of how to rollback the 146 GB drives to the original 72 GB drives after the upgrade.

Simplex:

7. Locate the latest full system backup taken with the 72 GB drives.
8. Put the unit at the ‘ok’ prompt.
9. Replace the 146 GB drives with the 72 GB drives that were removed from the system.
10. Follow the existing procedure for restoring from a full system backup for a simplex server, using the backup taken when the drives were 72 GB.
11. Restore the latest data backup using the existing procedure for a simplex server.

Cluster Rollback

1. Locate the latest full system backup taken with the 72 GB drives.
2. Put both units of the cluster at the ok prompt.
3. Replace the 146 GB drives in both units with the 72 GB drives that were removed from the units.
4. Follow the existing procedure for restoring from a full system backup for a cluster, using the backup taken when the drives were 72 GB.
5. Restore the latest data backup using the existing procedure for a cluster.

166.3 Hardware Requirements or Dependencies

The 146 GB disk drive upgrade utility is only supported on SPFS servers with two 72 GB drives.

166.4 Software Requirements or Dependencies

The 146 GB disk drive upgrade is performed after the server upgrade to SN09FF.

166.5 Limitations and restrictions

Limitations and restrictions include:

- A new full system backup is required to be taken after completion of the upgrade.
- If a remote backup server is in use, it must be re-installed with 146 GB drives after the target server is upgraded with 146GB drives.
- Synchronization of the mirrors must be performed one at a time. The amount of time it takes to fully synchronize one of the 146 GB drives is at least 2 hours.
- Interruption of the automated upgrade utility will require the user to either manually complete the upgrade or manually recover the server.

166.6 Interactions

Not applicable.

166.7 Glossary

Term	Description
New term	Definition

167: Functional Description (FN) A00012735

167.1 Feature name and Feature ID

A00012735 - Session Server Fault Handling Enhancements

167.2 Description

This activity extends the coverage of hardware faults handled by the Session Server NCGL Platform Manager software and thus increases the reliability of the Session Server platform. This activity involves the detection and reporting of hardware faults in the following areas:

- Power Supplies
- Fan Speeds
- System Temperature
- System Voltage
- Miscellaneous Hardware Elements

167.3 Hardware Requirements or Dependencies

The software of activity interacts with functions of the existing SAM XTS (HP CC3310) hardware of the Session Server platform. No new hardware is required.

167.4 Software Requirements or Dependencies

No new software or firmware dependencies are introduced by this activity.

167.5 NCGL Platform Web Pages

An Element Management web based interface is provided to perform the platform or application maintenance and monitoring of logs and alarms. The platform web interface resides under the Communication Server 2000 NCGL Platform Manager link on the Session Server EM web login page. This web interface can be accessed from either the Succession IEMS or a general web browser running on a client machine.

This activity introduces enhancements to the fault handling of the NCGL software within the NGSS platform. These enhancements include the monitoring and alarming of the various hardware resident sensors. These sensor monitors are displayed in a new Sensors page of the Succession Communication Server 2000 NCGL Platform Manager web pages. When mate connectivity exists, data for both units are shown on the Sensors page.

The sensors are categorized as either primary or secondary sensors. The primary sensors are always reported on the Sensors page while the value of a secondary sensor is only reported when the sensor is reporting a failure. In terms of alarms and customer logs, no such distinction between primary and secondary sensors applies - all sensors are treated the same.

The sensors are also categorized into the following sensor groups for purposes of sensor display, logging and alarming:

1. Power Supplies:

   There are two power supply modules, labelled “A” and “B”, per unit. Sensors report module presence and operational status. There is one primary and 2 secondary sensors per power supply module.

2. Fan Speed:

   There are 4 internal fan speed sensors and no secondary sensors per unit.

3. System Temperature:

   There are 4 primary temperature sensor plus 6 secondary sensors per unit.

4. System Voltage:

   There are 3 primary power line sensors plus 13 secondary sensors per unit.

5. Miscellaneous Hardware Elements:

   There are no primary sensors reported but up to 29 secondary sensors might be reported per unit.

The format of sensor information for a single unit of the new Sensors web page appears below in Table 1 on page 1724. Where applicable the units of the sensor readings appear in the Sensor Status column. In the cases of sensors with thresholds, the current value of the sensor plus associated thresholds are provided. Note that these thresholds are established in the hardware and this activity does not provide a method to change the threshold values. Where applicable the severity of the threshold (minor or major) is shown indicating that the exceeding the threshold will result in the assignment of the respective severity or higher.

The alarm severity column allows easier identification of the failed sensors and correlation with alarm indicators and customer log reports. A higher severity may appear in the alarm severity column in comparison to the minor threshold. This might happen if multiple sensors with the same replaceable component (FRU) are reporting failures. Please see the alarm subsection for more information.

If the secondary sensors report a failure indication, then the senors records will appear in the “<any other sensor failure reports>” fields. Reports for one or

more failed secondary sensors could appear on the Sensor page. If no secondary sensors report failures, then no additional records appear.

Table 1: Unit Sensor Format

Sensor Group		Sensor Status
Unit 0 Chassis Sensors		**Alarm:** <chassis alarm severity>
Fan Speed	80mm, Left	<current RPM plus thresholds>
	80mm, Right	<current RPM plus thresholds>
	40mm, Left:	<current RPM plus thresholds>
	40mm, Right	<current RPM plus thresholds>
System Temp	Baseboard	<status plus current degrees C>
	Processor 1	<status plus current degrees C>
	Processor 2	<status plus current degrees C>
	Front Panel	<status plus current degrees C>
	Other	<any other sensor failure reports>
System Voltage	3.3V	<current Volts plus hi/low thresholds>
	5V	<current Volts plus hi/low thresholds>
	12V	<current Volts plus hi/low thresholds>
	Other	<any other sensor failure reports>
Miscellaneous H/W Elements		<any other sensor failure reports>
Unit 0 Power Supply Module A		**Alarm:** <power supply A alarm severity>
Power Supply	A	<PS present and status> <any other sensor failure reports>
	Other	<any other sensor failure reports>
Unit 0 Power Supply Module B		**Alarm:** <power supply B alarm severity>
Power Supply	B	<PS present and status> <any other sensor failure reports>
	Other	<any other sensor failure reports>

The Sensors page provides the latest values of the last sensor sample. No history of sensor readings or failures is provided. The customer logs may be used to identify such a history.

Here is an example Sensor page display for a single unit

Sensor Group		Sensor Status
Unit 0 Chassis Sensors		**MAJOR**
Fan Speed	80mm,Left	Current = 4029.00 RPM Low Minor/Major = 1989.00/1836.00 RPM
	80mm,Right	Current = 3315.00 RPM Low Minor/Major = 1989.00/1836.00 RPM
	40mm,Left	Current = 9537.00 RPM Low Minor/Major = 3774.00/3264.00 RPM
	40mm,Right	Current = 8925.00 RPM Low Minor/Major = 3774.00/3264.00 RPM
System Temp	Baseboard	Current = 87.00 C Low Minor/Major = 10.00/5.00 C High Minor/Major = 60.00/65.00 C
	Processor1	Current = 33.00 C Low Minor/Major = 0.00/-10.00 C High Minor/Major = 75.00/80.00 C
	Processor2	Current = 32.00 C Low Minor/Major = 0.00/-10.00 C High Minor/Major = 75.00/80.00 C
	Front Panel	Current = 25.00 C Low Minor/Major = 10.00/5.00 C High Minor/Major = 40.00/45.00 C
	Other	OK
System Voltage	3.3V	Current = 3.41 volts Low Minor/Major = 3.08/2.99 volts High Minor/Major = 3.54/3.64 volts
	5V	Current = 5.01 volts Low Minor/Major = 4.68/4.52 volts High Minor/Major = 5.33/5.49 volts
	12V	Current = 16.03 volts Low Minor/Major = 11.16/10.79 volts High Minor/Major = 12.71/13.08 volts
	Other	OK
Miscellaneous H/W Elements		OK
Unit 0 Power Supply Module A		**MAJOR**
Power supply	A	presence detected
	Other	minor 22 performance lags; minor 23 performance lags;
Unit 0 Power Supply Module B		**minor**
Power supply	B	presence detected
	Other	minor 26 performance lags;

167.6 Alarms

This activity introduces new alarms for reporting faults due to:

1. Power Supply related failure
2. Fan Speed threshold exceeded
3. System Temperature threshold exceeded
4. System Voltage threshold exceeded
5. Miscellaneous hardware sensors reporting failure

The new alarms are associated with an field replaceable unit (FRU). There are two FRU types involved with the sensor monitoring:

1. the server chassis and contained baseboard
2. the power supply module

There are two power supply FRUs, A (left when viewed from rear) and B (right), per session server module.

For the new alarms:

1. An XTS382 alarm and log signifies the occurrence of a server chassis/ baseboard sensor alarm condition.
2. An XTS383 alarm and log signifies the occurrence of a power supply module alarm condition

For each unit, at any time at most one alarm should be raised for each FRU.

Once raised, the severity of an alarm might escalate if:

- the number of failed primary or secondary sensors in the group detecting failure increases or
- the nature of the sensor failure changes (e.g. both minor and major thresholds are crossed)

When raised these alarms may be viewed on the Alarms page of the NCGL Platform Manager web pages. Note that the Alarms page is refreshed approximately every 45 seconds.

The NCGL platform also supports the reporting of alarm events to an SNMP host target. These SNMP traps are typically configured to route to the Succession IEMS. Traps for the new alarms follow the same format, fields values and behavior as existing platform alarm traps. When raising an alarm, the SNMP traps are associated with the XTS382 and XTS383 identifiers. Once all sensor conditions associated with an FRU are cleared, the alarm is cleared and an XTS682 or XTS683 SNMP trap and customer log are generated.

Alarms are formatted and displayed as follows:

<Type> <ID> <Timestamp> <Host> <Severity> <Description>

167.6.1 Alarm Type

The alarm type specifies the alarm category for the given alarm. Each of the new alarms are associated with the Equipment Alarm type.

Table 2: Alarm Type Selection

Log Number	Elements	Type
XTS382/XTS682	Chassis/Baseboard Sensor	Equipment alarm
XTS383/XTS683	Power Supply Sensor	Equipment alarm

167.6.2 Alarm ID

The alarm ID specifies, in general terms, why the given alarm was raised. The alarm ID choices for the new alarms are:

1. Cooling system problem:
2. Processor Problem:
3. Threshold Crossed
4. Power Problem
5. Equipment Malfunction

For cases of multiple, diverse alarm conditions against the same FRU, the equipment malfunction identifier is used.

167.6.3 Alarm Timestamp

The alarm timestamp specifies the date and time when the given alarm was raised.

167.6.4 Alarm Host

The host field contains the Session Server host name from where alarm was raised.

167.6.5 Alarm Severity

The alarm severity specifies the seriousness of the given alarm.

The following alarm severities apply to the alarms introduced by this activity:

- Minor

  Indicates the detection of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious fault.

- Major

  Indicates a service affecting condition has developed and a timely corrective action is required.

- Cleared

  Note that ‘cleared’ will not be seen on the Alarms Panel, since the Alarms Panel only shows alarms that are currently raised.

For severity selections of the new alarms of this activity please refer to table 1.

167.6.6 Alarm Description

The alarm description provides specific details about the given alarm. For the alarms introduced by this activity, the description field includes:

- location:

  For the power supply module alarms, this indicates either “A” (left when viewed from rear) or “B” (right when viewed from rear) for the applicable FRU.

- sensor counts:

  The number of sensor reporting failure for the FRU is also given.

Here are example fields from the Alarms Panel on the platform web pages:

Type: Equipment

ID: Threshold Crossed

Date: Monday December 12th 2005 04:17:46 AM

Host: NGSS0

Severity: Minor

Description: Chassis sensor alarm raised. 1 sensor is reporting a failure.

167.7 Customer Logs

The Session Server Element Manager provides a web page for viewing of customer logs. The customers log panel displays a historical view of customer logs that have been generated on the Session Server unit.

This activity adds new customer logs to the existing platform (XTS) logs. The new customer logs are associated with the types of field replaceable units where the hardware sensors reside.

The Session Server customer logs are generated using syslog. Here is the format for the new logs.

<time stamp> <host name> <process name> <Name> <Number> <Severity> <Event type> <Label> <Description>

The log description field follows the same format as the alarm description field described in “Alarm Description” on page 1728.

Here are the field values for these new customer logs.

Table 3: Fields of the New Logs

Name	Number	severity	Event Type	Label	Description
XTS	382	MINOR	FLT	Chassis Sensor Fault	Chassis sensor alarm raised. <#> sensor <is/are> reporting a failure.
XTS	382	MAJOR	FLT	Chassis Sensor Fault	Chassis sensor alarm raised. <#> sensor <is/are> reporting a failure.
XTS	682	CLEARED	INFO	Chassis Sensor Condition Cleared	Chassis sensor condition cleared.
XTS	383	MINOR	FLT	Power Supply Sensor Fault	Power supply alarm raised in module <A/B>. <#> sensor <is/are> reporting a failure.
XTS	383	MAJOR	FLT	Power Supply Sensor Fault	Power supply alarm raised in module <A/B>. <#> sensor <is/are> reporting a failure.

Table 3: Fields of the New Logs

Name	Number	severity	Event Type	Label	Description
XTS	683	CLEARED	INFO	Power Supply Sensor Condition Cleared	Power supply condition cleared in module <A/B>.

167.8 Limitations and restrictions

This activity does not introduce further limitations or restrictions to the NGSS platform. Please note that this activity addresses the failure monitoring documented in the FN section of A00004005. Please refer to A00004005 for other limitations and restrictions of the NGSS platform.

167.9 Interactions

Not applicable.

167.10 Glossary

Term	Description
New term	Definition

168: Functional Description (FN) A00012843

168.1 Feature name and Feature ID

A00012843 - IEMS support for MDM security Interface changes

168.2 Description

In SN09 MDM changes their security interface, MDM client is moving from a PAM Radius client to a PAM IS Client, so it will no longer require a Radius secret configuration in IEMS.

To support this change in MDM, IEMS requires the following design changes:

1. Remove the Radius Secret field from the MDM Mgr Addition wizard when adding a new SN09 or later MDM Element Manager. See Figure 1.

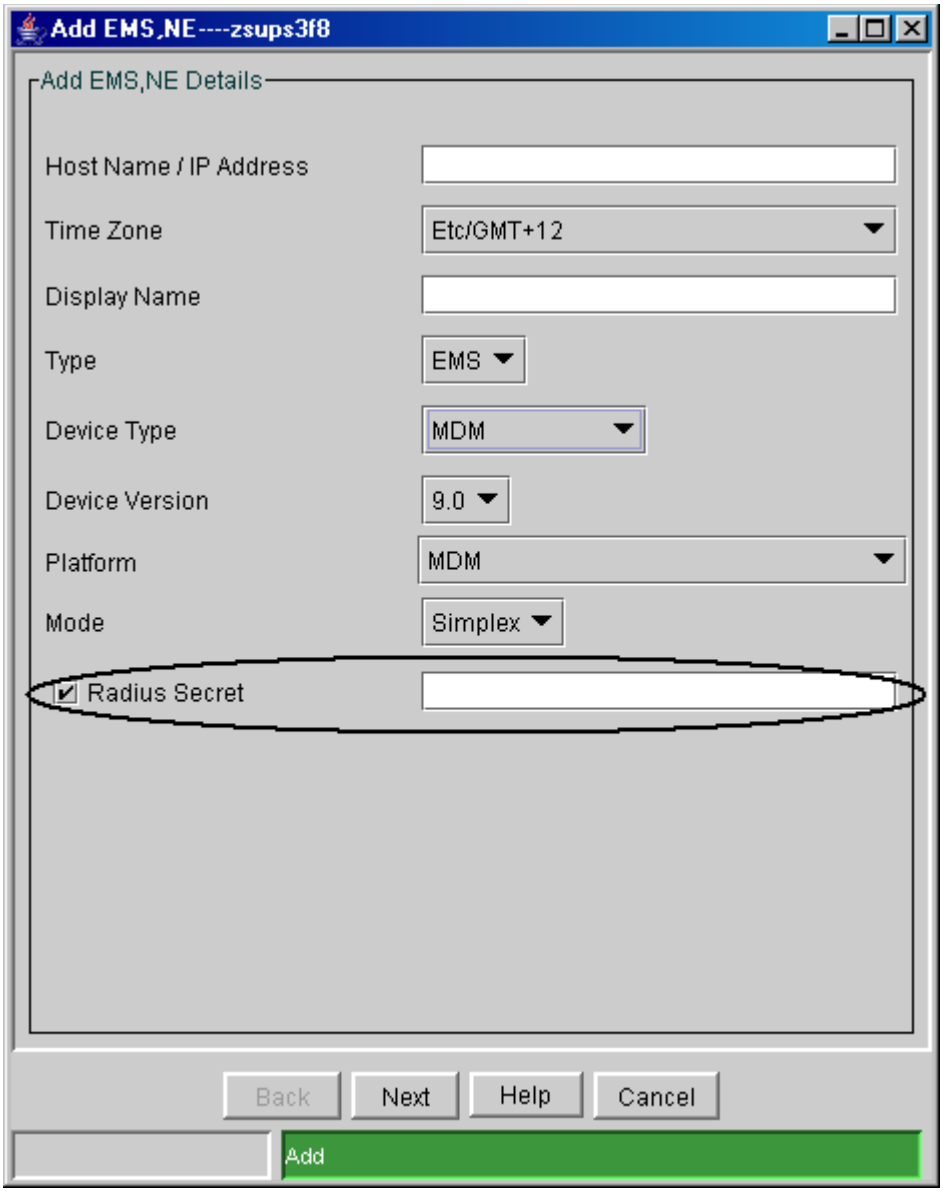


Figure 1 MDM Addition wizard

2. Disable the Update Radius Secret menu item from the MDM Element Manager's menu when it is a SN09 or later MDM Element Manager. See Figures 2 and 3.

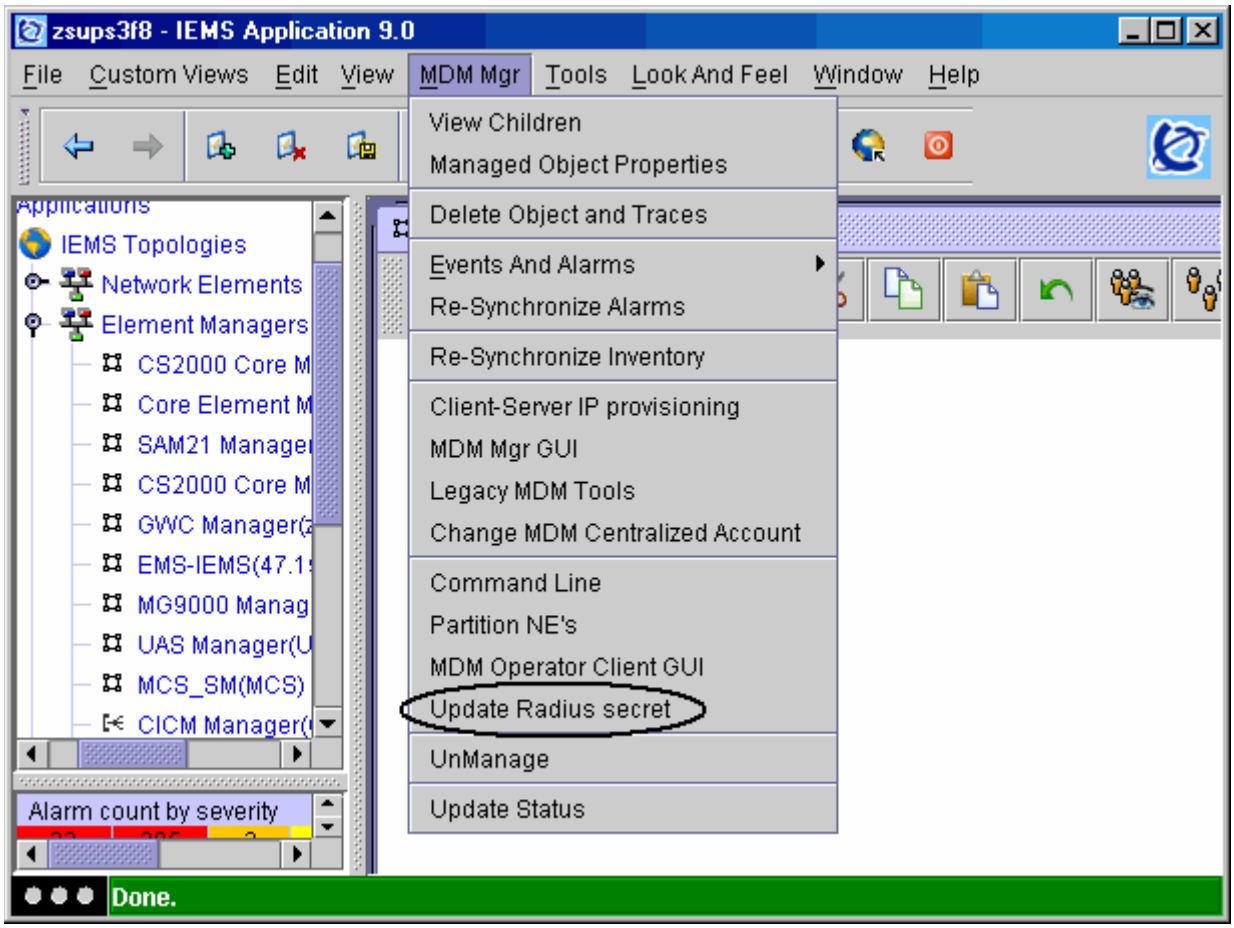


Figure 2 MDM Mgr Menu

Figure 3 MDM Mgr Right Click Popup Menu

52.1 Hardware Requirements or Dependencies

N/A

52.2 Software Requirements or Dependencies

This Feature requires the following applications:

- IEMS Application Server SN09.1
- IEMS Security Server, MFT V1.1.0
- SN09 MDM Mgr R15.3
- SN08 MDM Mgr R15.2

52.3 Limitations and restrictions

N/A

52.4 Interactions

There are no interactions between this feature and existing features.

52.5 Glossary

RADIUS - Remote Authentication Dial-In User Service

IEMS - Integrated Element Management System

GUI - Graphical User Interface

EM - Element Manager

NE - Network Element

CLI - Command Line Interface

PAM - Pluggable Authentication Module

169: Functional Description (FN) A00012889

169.1 Feature name and Feature ID

A00012889 - Passphrase Protected Keys for SSH

169.2 Description

The applications (SBA and OMDD) on the SDM/CBM, use either standard FTP (insecure) or OpenSSH SFTP (secure) to perform outbound file transfers to the downstream machine.

Currently, for secure outbound file transfer, only password-based authentication is supported.

This feature enhances the existing secure outbound file transfer functionality by introducing the key-based (public key) authentication.

The key-based authentication mechanism is provided as an additional option for the user. Hence, the user can select to use either the password-based or the key-based authentication while adding and changing the secure file transfer schedules in the SBA (billmtc) or OMDD (omui) user interface programs. The actual configuration details are documented in the configuration section.

When the user configures secure file transfer schedule with key-based authentication, the keypair (public/private key files) will be automatically generated with a random passphrase. The keypair will be stored under ~maint/ .ssh/ directory and the passphrase will be stored in the Private Data Manager in an encrypted format.

If there is a failure in generating the cryptographic keys, an info log SDM666 will be generated.
Ex:
SDM666 Oct 12 04:33:59 1234 NONE INFO Failed to generate cryptographic keys for user=maint, app_name=OMDD, index=ftd1

169.3 Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced by this feature.

169.4 Software Requirements or Dependencies

The customer's downstream machine (OSS) should be running a SSH-2 server compatible with SFTP client of OpenSSH. The OpenSSH software should be installed on the SDM/CBM too.

169.5 Limitations and restrictions

- The initial host key acceptance of the downstream processor should be done manually before it can use the SSH protocol to transfer the files from SDM/CBM. Figure 1 shows an example of how to accept a host key manually. The .ssh/known_hosts file in maint user's home directory will be edited by SSH software to include the host key. After that, the applications (SBA/OMDD) can use SSH to send files to the downstream OSS as maint/root. This procedure must be performed for each downstream destination.
- Automatic dumping of the public key file on the remote system is NOT supported by this feature. All users have to manually dump the contents of the public key file into the user's authorization file on the remote system.

  Note: If the remote system is running OpenSSH server, the public key should be appended to .ssh/authorized_keys or .ssh/authorized_keys2 file of the user. Figure 2 shows an example of how to append the public key to .ssh/authorized_keys file of the user.
- The SSH-2 server running on the downstream OSS must be compatible with OpenSSH sftp client.
- The data transfers of AFT, RTB and sendtape applications are not secured.

Figure 1 Host key acceptance

On SDM/CBM

```
> login: root
> root's Password: xxxx
> su maint
> ssh user1@47.135.214.66
> The authenticity of host '47.135.214.66 (47.135.214.66)' can't be established.
> RSA key fingerprint is fd:3b:18:27:1f:85:55:83:ff:e6:16:7e:fd:5e:33:f8.
> Are you sure you want to continue connecting (yes/no)? yes
> Warning: Permanently added '47.135.214.66' (RSA) to the list of known hosts.
```

Figure 2 Appending public key to authorized_keys file of the user on the downstream machine

On SDM/CBM

```
> login: root
> root's Password: xxxx
> cd ~maint/.ssh
> ssh root@47.135.214.66 'cat >> .ssh/authorized_keys' < sba:occ:dirp:oss_rsa.pub
> Password:
>
```

169.6 Interactions

None

169.7 Applicable customer facing sections

Fault Management

- Logs __X__
- Alarms __X__

Configuration

- Data Schema _N/A_
- User Interface __X__
- Element Management _N/A_
- Security __X__
- Service Order _N/A_
- Office Parameters _N/A_

Accounting (includes AMA billing) _N/A_

Performance (includes operational measurements) _N/A_

169.8 Glossary

Term	Description
SDM	Supernode Data Manager
CBM	Core Billing Manager
SBA	SDM/CBM Billing Application
OMDD	Operational Measurements Data Delivery
OMUI	OMDD User Interface
SSH	Secure Shell
FTP	File Transfer Protocol
SFTP	Secure File Transfer Protocol (SSH internal protocol)
OSS	Operations Support System

170: Functional Description (FN) A00012893

170.1 Feature name and Feature ID

A00012893 - BCP 7200 VLAN Tagging

170.2 Description

This feature provides support for IEEE 802.1Q VLAN-tagging on the BCP7200.

The introduction of IEEE 802.1Q VLAN-tagging on the BCP7200 simplifies the Service Network Interconnect of the BCP7200 by supporting direct interconnect into VLAN-tagged network topologies.

Simplification of BCP7200 Service Network Interconnect has transitive benefits in terms of:

- reduced cost: due the elimination of the need for specialized Interconnect Equipment containing advanced packet analysis functions.
- deployability: the BCP7200 can now be deployed directly into a broader array of networks (i.e. tagged and untagged topologies).
- simplification: the BCP7200 network interconnect no longer requires complex configuration of advanced functions on Service Network Interconnect Equipment.

170.3 Background

170.3.1 The Media Portal Component

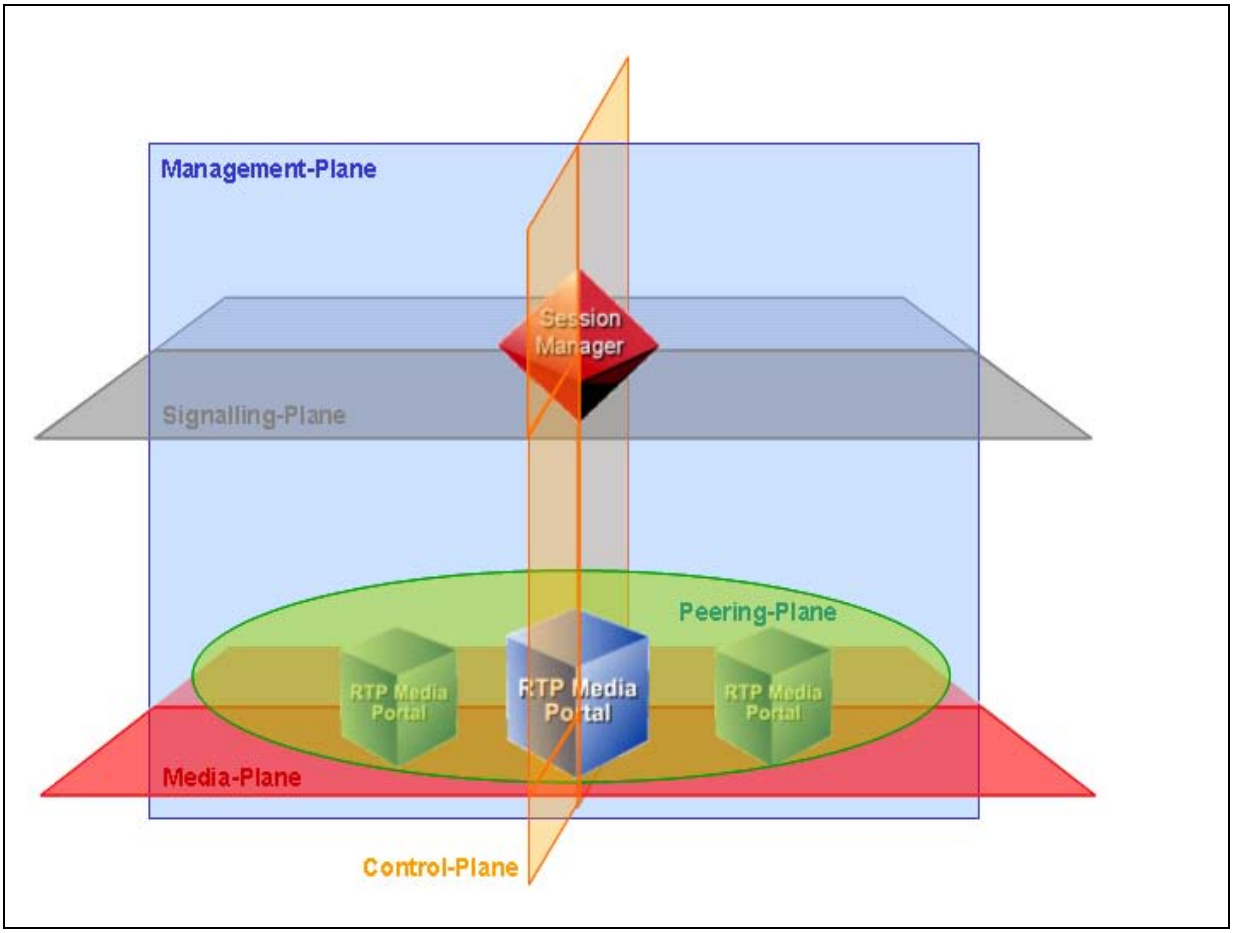
The Media Portal Component is the part of the Multimedia Communications Portfolio (MCP) whose primary function is to extend the reach of multimedia services so that they are accessible to obscured endpoints - devices residing behind a firewall (FW), or a Network Address Translation (NAT) and/or Network Address Port Translation (NAPT) device.

The Media Portal Component is also employed as a media NAPT point that shields internal Service Network components from external exposure - and is used to provide media anchoring and media pivot capabilities.

In order to provide these advanced media functions the Media Portal Component must reside in the following planes of operation (refer to “Media Portal Component - Presence in Service-planes.” on page 1741):

- the **Management-plane**, over which the Media Portal Component is deployed to a target platform – and over which command/control and telemetry can flow to aid in operation, administration, and maintenance.
- the **Control-plane**, through which a Call Server (e.g. a CS2000 Gateway Controller, GWC – or a MCS Session Manager) can utilize the Media Portal Control Protocol (MPCP) to control participation of the Media Portal Component in calls as required.
- the **Media-plane**, over which media streams converge on the Media Portal for relay to their associated endpoints.
- *and the **Peering-plane**, in which the Service Instances participating in a Fault Tolerant Service Cluster maintain synchrony (through heartbeat and Checkpointing mechanisms) and detect failures.* ***(this service-plane is only applicable to the BCP7200).***

Figure 1 Media Portal Component - Presence in Service-planes.



In addition to its logical presence in the service–planes, the Media Portal Component can be configured for physical presence in either one, or two separate, media networks. These two types of network topology are known as:

- **Single Network Topology**: in this topology the Media Portal Component is connected to a single network space in the Media-plane (refer to “Media Portal Component – Single Network Topology.” on page 1742). In this topology, the Service Network is protected by Access Control Lists (ACLs) on the routers. This topology occurs in Multimedia Communications System (MCS) deployments.
- **Dual Network Topology**: in this topology the Media Portal Component is connected into two separate Media-plane network spaces – and can relay media packets between the two (refer to “Media Portal Component – Dual Network Topology.” on page 1743). In this topology, the Service Network also benefits from an extra layer of protection in the Media-plane as a result of the Media Portal’s operation. This topology is used throughout Communications Server 2000 (CS2K) deployments.

Figure 2 Media Portal Component – Single Network Topology.

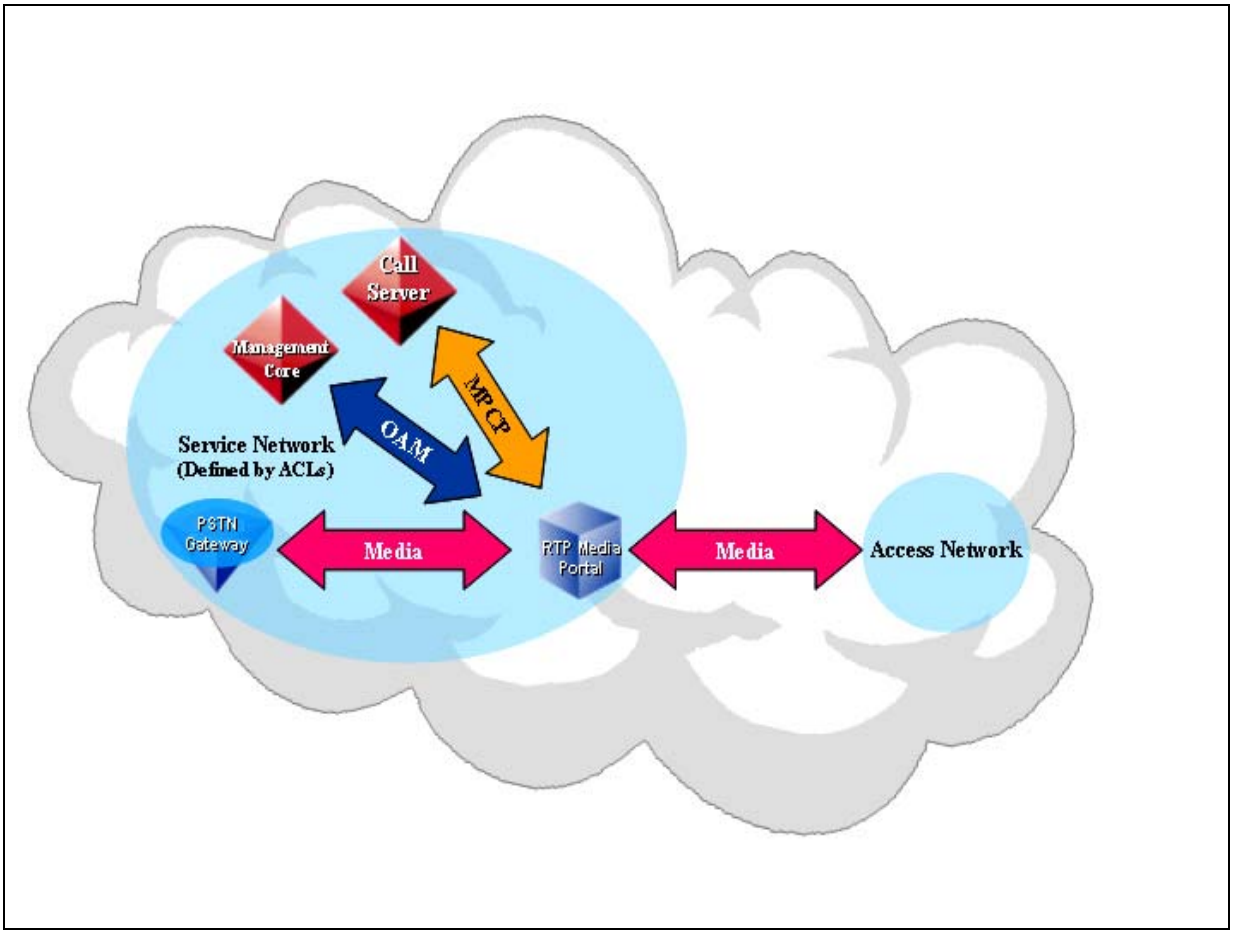
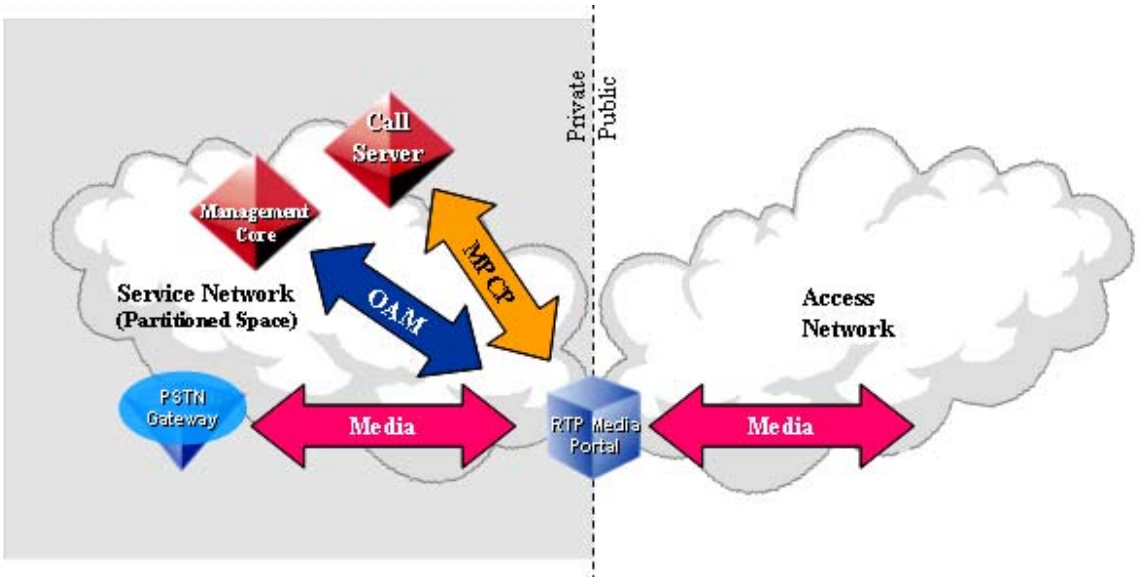


Figure 3 Media Portal Component – Dual Network Topology.

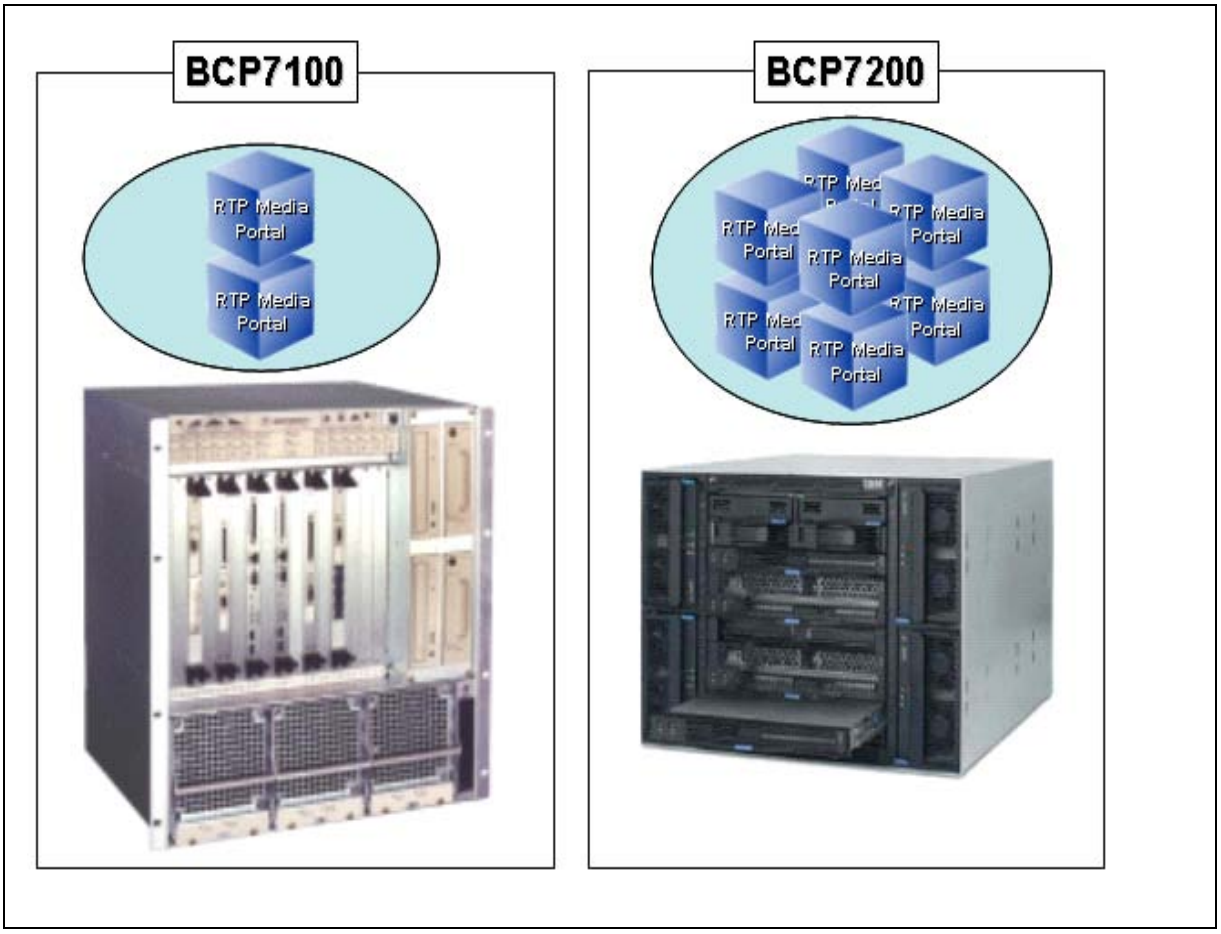


170.4 Border Control Point (BCP)

The Border Control Point (BCP) is the nomenclature used to identify particular packaging of the Media Portal Component (refer to “The Border Control Point (BCP) Family” on page 1744):

- The BCP7100 describes the original packaging of the Media Portal component onto the Motorola CPX8216T platform. The BCP7100 supports a maximum of two (2) simplex RTP Media Portal Service Instances.
- The newer BCP7200 is the packaging of the Media Portal Component onto the IBM BladeCenterT chassis. The BCP7200 supports a maximum of eight (8) simplex RTP Media Portal Service Instances (for “1+0” stand-alone configurations), and a maximum of seven (7) redundant RTP Media Portal Service Instances (for the maximum “7+1” Fault Tolerant Service Cluster configuration).

Figure 4 The Border Control Point (BCP) Family



While the physical packaging of these two platforms differs significantly, the basic operation of the RTP Media Portal Component software is the same on both platforms[1]. In fact, both platforms present a consistent logical view of the RTP Media Portal Service owing to its consistent presence in the Service-planes. It is at the point of Network Interconnect where the distinguishing architectural differences between the platforms is most visible. A summary of these differences (hardware/software, and physical/logical) are presented below (refer to "Border Control Point (BCP) Family – Service Network Connectivity" on page 1746):

- BCP7100: in this packaging a distributed hardware architecture is closely matched to a distributed RTP Media Portal Component software architecture (management and control functions reside on the Host Card,

[1]From a logical perspective, both BCP7100/BCP7200 support the same suite of functionality in the Management-plane (OAM), the Control-plane (MPCP), and the Media-plane (Address and Port Discovery, Anchor/Pivot, QoS Reporting, Asynchronous Event Reporting, …). Also, both BCP7100/7200 support single- or dual-network operation. ***Caveat: the BCP7200 provides "N+1" Fault Tolerance capabilities that are not available on the BCP7100.***

and media processing is performed separately across many distributed Media Blades). This close mapping between distributed hardware and software components makes for a simpler interconnect into the Service Network(s) since the physical links connect to hardware subcomponents that are dedicated to hosting specific software subcomponents (i.e. the physical links carry only the traffic of the hosted software subcomponent). As a result, the BCP7100 hardware platform is interconnected into the Service Network(s) using the available physical links (on the Host Card and the Media Blades) to establish presence in the Service-planes as follows:

- The Host Card utilizes an active/standby Network Interface Card (NIC) Teaming configuration to provide a redundant physical link through which the Media Portal can establish presence in both the Management- and Control-planes.
- Each Media Blade has two separate non-redundant physical links to establish presence in the Media-plane. If the Media-plane consists of a single-network space (i.e. Single Network Topology) then only one of these physical links (Net1) is connected to establish Media-plane presence. However; if the Media-plane consists of partitioned network spaces then each physical link on the Media Blades (Net1 and Net2) is connected into each network space.
- The Service Interconnect Equipment can then utilize simple functions (e.g. port-based VLAN) to classify the traffic flow for each physical link and drop it into the appropriate network space.

- BCP7200: in this packaging the Media Portal Component software architecture is no longer distributed, but has become a monolithic whole (the Host and Media Blade functions are melded together) that executes as a single logical instance on a non-distributed hardware platform (i.e. BladeServer). As well, the BCP7200 hardware architecture contains an integrated Ethernet Switch Module (ESM) that interconnects the BladeServers and the Service Network(s) together using Layer-2 link aggregation (for reliability and capacity requirements). As a result, the BCP7200 interconnect into the Service Network(s) is an aggregate flow of multi-netted traffic[1] (Management-, Control- , and Media-plane traffic are all intermixed on the ESM's external links). For some Service Network topologies, interconnect of this sort requires advanced functions in the Service Network Interconnect Equipment that can classify traffic flows (e.g. the subnet-based VLAN functions available on the Passport 8600, refer to "BCP7200 – Service Network Interconnect" on page 1747). This makes for a more complex Service Network Interconnect that relies on advanced functions to analyze all incoming/outgoing packets and to place them in the proper network space:

[1]Multi-netted traffic consists of flows that are comprised of frames belonging to multiple subnets.

- The BCP7200 Service Network Interconnect Point consists of up to six (6) separate physical links grouped together at Layer-2 into a Link Aggregation Group (which provides a single logical link with a total capacity of the constituent physical links).
- All traffic emitted/admitted from/to the BCP7200 is multi-netted traffic.
- The Service Network Interconnect Equipment cannot simply classify traffic according to physical link (since all traffic flows appear on all ESM external physical links). Therefore the Service Network Interconnect equipment must have advanced traffic processing functions if it is desired to separate the multi-netted traffic and drop it into the appropriate network space.

Figure 5 Border Control Point (BCP) Family – Service Network Connectivity

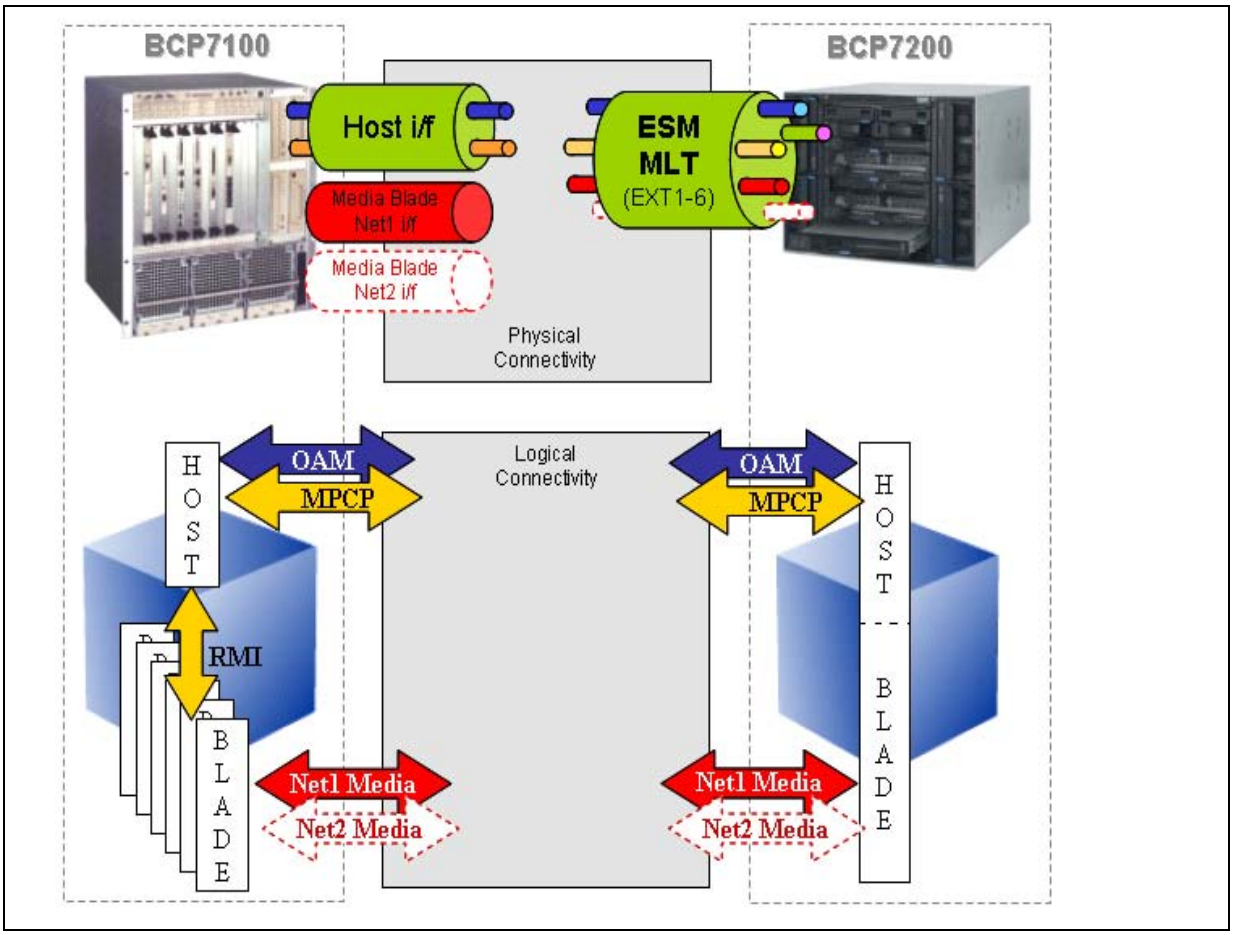
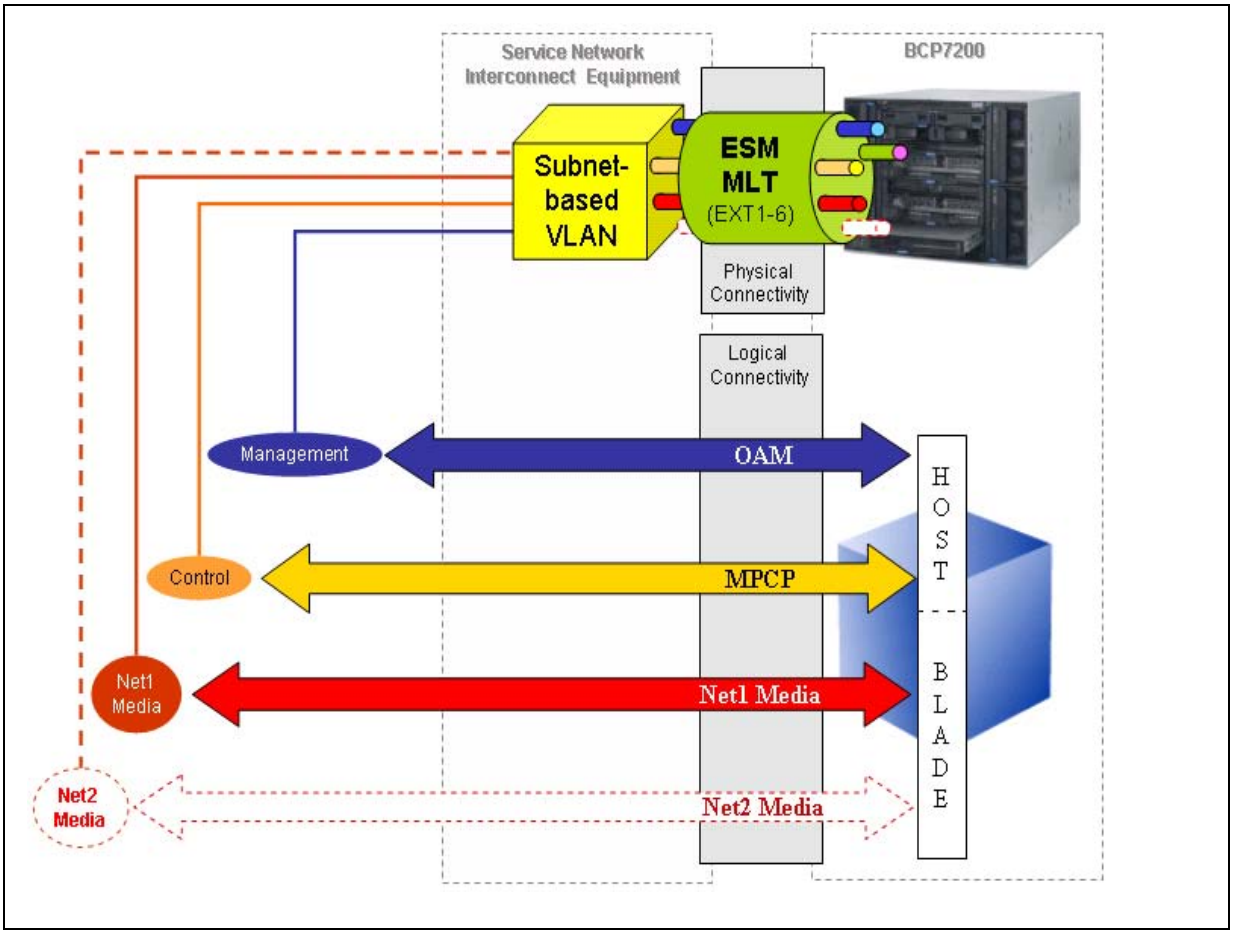


Figure 6 BCP7200 – Service Network Interconnect



170.5 IEEE 802.1Q VLAN-tagging

170.6 IEEE 802.1Q Ethernet Frame

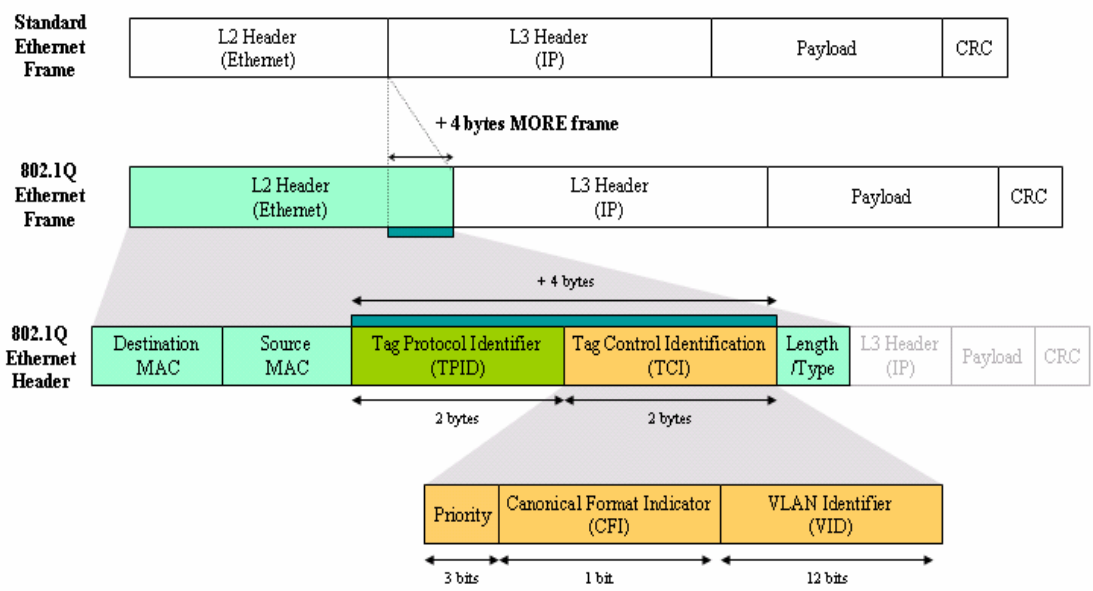
A summary of IEEE 802.1Q VLAN-tagging functionality is presented in this section, and a more comprehensive description can be found in the specification that can be found in "802.1Q™, IEEE Standards for Local and metropolitan area networks, Virtual Bridged Local Area Networks".

Originally, IEEE 802 Local Area Networks (LANs) were connected together with Media Access Control (MAC) Bridges that operated according to physical connectivity: all connected devices were implicitly part of the same broadcast domain (with routers providing network connectivity between broadcast domains).

As network topologies evolved into ever more complex structures to meet a growing array of requirements, the physical dependencies constraining broadcast domains became unwieldy and the concept of virtual broadcast domains came into being. The IEEE 802.1Q standard defines the operation of Virtual LAN (VLAN) Bridges that permit the definition, operation and administration of Virtual LAN topologies within a Bridged LAN infrastructure.

The key re-tooling that enables VLAN-tagging to occur is the extension of the Ethernet frame (Layer-2) by 4-bytes to accommodate the new tagging data structures placed in the L2 Header (refer to “802.1Q – Ethernet Frame Extensions” on page 1748 [1]). This feature enables the BCP7200 to be configured to support the new 802.1Q Ethernet Frame – including properly populating its VLAN Identifier (VID) field.

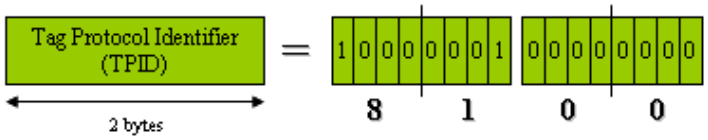
Figure 7 802.1Q – Ethernet Frame Extensions



The new fields that distinguish an 802.1Q Ethernet Frame from a Standard Ethernet Frame are (the italicized data structures are not explicitly addressed by this feature but are included for completeness):

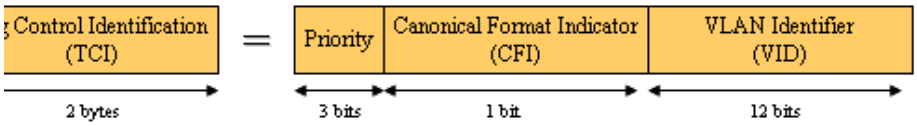
- The 2-byte Tag Protocol Identifier (TPID):

[1]Expanding the Ethernet Frame size by 4-bytes implicitly requires other interconnecting network components (hardware and software) to be able to distinguish 802.1Q Ethernet Frames –AND- to be able to properly process such frames.



- The TPID has a defined value of 8100 in hex.
- When a frame has a TPID (also known as “EtherType”) equal to 8100, the frame carries the tag information for IEEE 802.1Q / 802.1P.

- The 2-byte Tag Control Identification (TCI) field:



  - The first three bits of the TCI define user priority.
    - These bits provide eight (2^3) priority levels.
    - IEEE 802.1P defines the operation for these 3 user priority bits.
  - The Canonical Format Indicator (CFI) is a single-bit flag that is always set to zero for Ethernet switches.
    - CFI is used for compatibility between Ethernet type network and Token Ring networks.
    - If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as CFI=1 indicates an untagged port.
  - **VLAN ID is the identification of the VLAN, which is basically used by the standard 802.1Q.**
    - 12 bits allow the identification of 4096 (2^12) VLANs.
    - VID of 0 is used to identify priority frames*, and a VID of 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

      ***NOTE:** A frame with a VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is used as the VID of the frame*

170.7 IEEE 802.1Q Terminology

Presented below is some common terminology used in reference to IEEE 802.1Q tagging functionality:

- o VLAN identifier (VID) - the 12-bit portion of the VLAN tag in the frame header that identifies an explicit VLAN.
- o Untagged frame - a frame that does not carry any VLAN tagging information in the frame header.
- o Tagged frame - a frame that carries VLAN tagging information in the header. This VLAN tagging information is a 32-bit field (VLAN tag) in the frame header that identifies the frame as belonging to a specific VLAN.
- o Port VLAN identifier (PVID) - a classification mechanism that associates a port with a specific VLAN. For example, a port with a PVID of 3 (PVID =3) assigns all untagged frames received on this port to VLAN 3.
- o Untagged member - a port that has been configured as an untagged member of a specific VLAN. When an untagged frame exits the switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.
- o Tagged member - a port that has been configured as a tagged member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame header is modified to include the 32-bit tag associated with the PVID. When a tagged frame exits the switch through a tagged member port, the frame header remains unchanged (original VID remains).

NOTE: *If an 802.1Q VLAN-tagged frame is sent to a port that has VLAN-tagging disabled, then the frames are dropped at that ingress port.*

170.8 IEEE 802.1Q Frame Processing

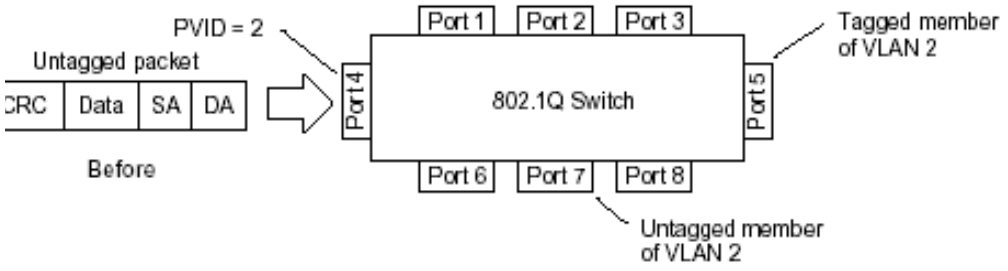
Each port on an IEEE 802.1Q-enabled switch can belong to one or more VLANs, and each VLAN can have any number of switch ports in its membership.

When configuring port-based VLANs, the switch ports are configured as tagged or untagged members of specific VLANs. Any port that belongs to multiple VLANs, however, must have VLAN tagging enabled. Any untagged frames (those with no VLAN specified) are classified with the sending port's PVID.

170.8.1 Untagged Frame Processing:

This example describes the processing of untagged frames (*Port 5 is configured as a tagged member of VLAN 2, and port 7 is configured as an untagged member of VLAN 2*):

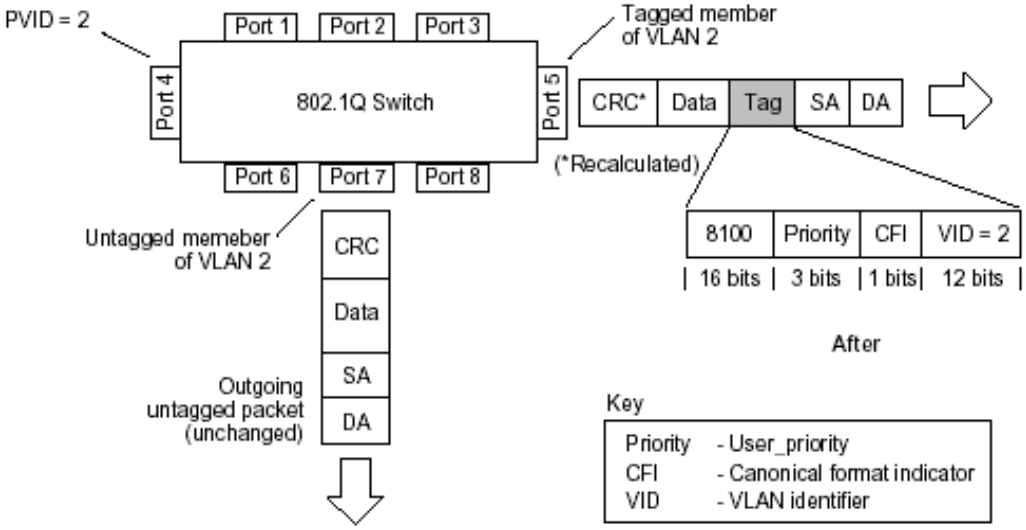
1. Untagged incoming frames arriving on Port 4 are assigned directly to VLAN 2 (port 4 has a PVID = 2).



2. The untagged frame traverses the logical broadcast domain in the 802.1Q Switch and is:

    a. marked (tagged) as it leaves the switch through port 5 (which is configured as a tagged member of VLAN 2).

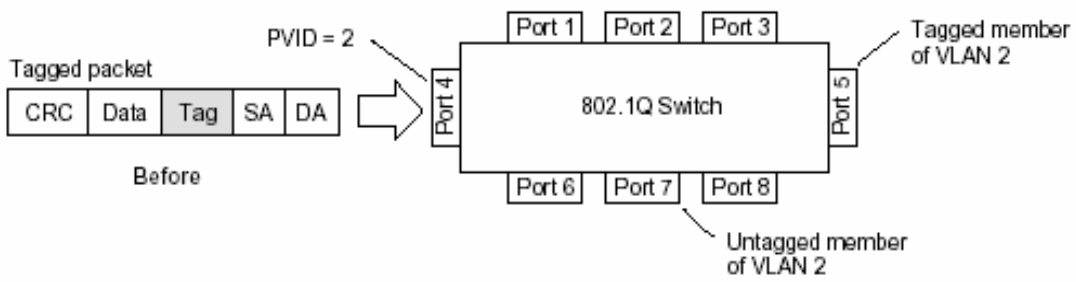
    b. unchanged as it leaves the switch through port 7 (which is configured as an untagged member of VLAN 2).



170.8.2 Tagged Frame Processing:

This example describes the processing of tagged frames (*Port 5 is configured as a tagged member of VLAN 2, and port 7 is configured as an untagged member of VLAN 2*):

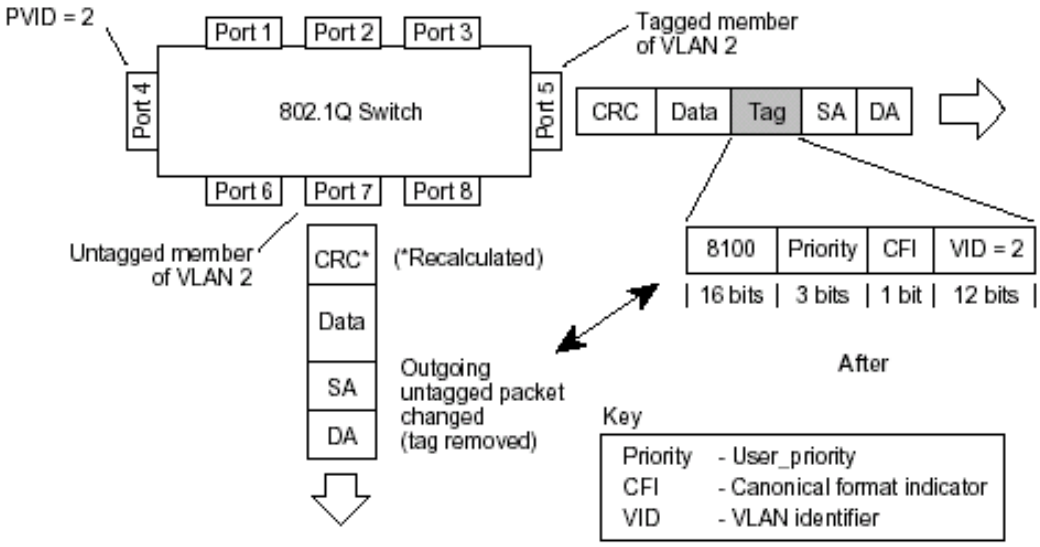
1. VLAN-tagged incoming frames arrive on Port 4 and (assuming the VLAN ID in the frame was “VLAN 2”) are relayed across VLAN 2.



2. The VLAN-tagged frame remains unchanged as it traverses the logical broadcast domain in the 802.1Q Switch and:

    a. remains unchanged as it leaves the switch through port 5 (which is configured as a tagged member of VLAN 2).

    b. Becomes untagged as it leaves the switch through port 7 (which is configured as an untagged member of VLAN 2).



170.9 Overview

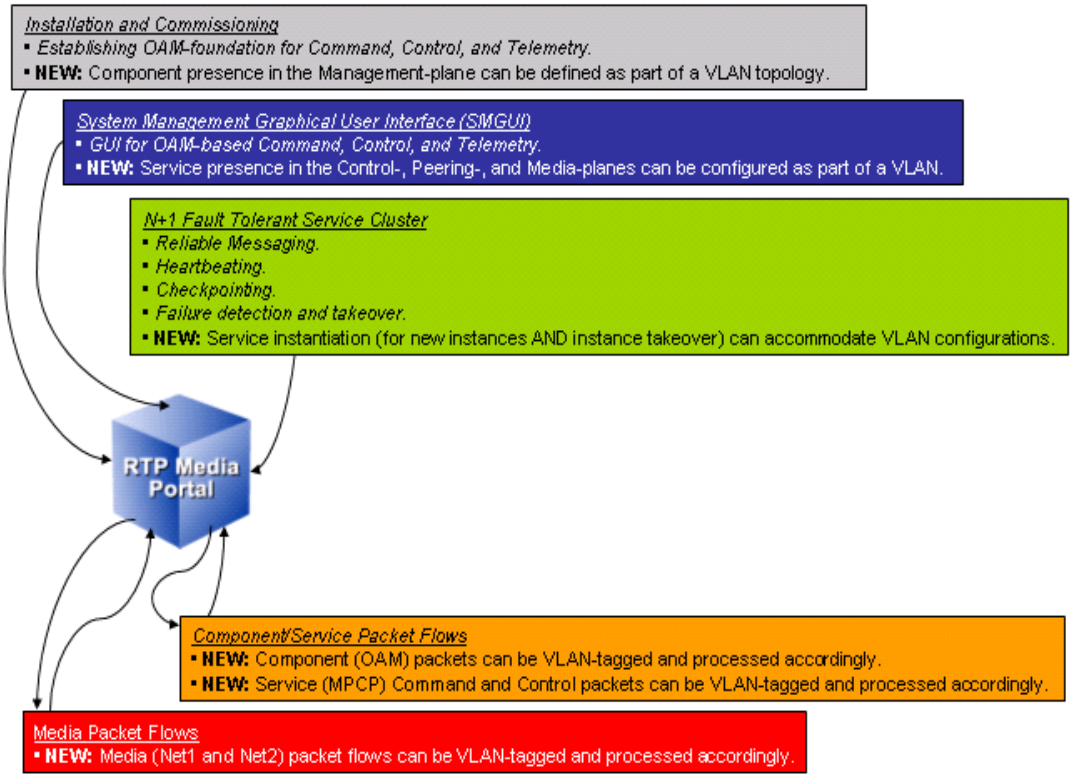
The BCP7200 is enhanced to provide IEEE 802.1Q VLAN-tagging functionality.

This is accomplished by providing means to configure and utilize the available IEEE 802.1Q capabilities that were previously dormant in the platform - NOT implementing IEE802.1Q itself since support for this was already available, but latent, in the underlying platform hardware and Operating System.

The scope of this feature encompasses the following areas (refer to “BCP7200 VLAN Tagging – Feature Overview” on page 1754):

- Installation and Commissioning Procedures (I&C): these procedures are enhanced to support configuration for logical- and physical-partitioning of VLAN-tagged traffic at the point of Service Network Interconnect, and to accommodate specification of the Management-plane (OAM) presence in a VLAN-tagged network topology.
- System Management Graphical User Interface (SMGUI): this interface is enhanced to provide the capability to specify VLAN membership for Control- and Media-plane points of presence. There are also changes made to Static Route datafill that permit association of Static Routes to VLANs.
- N+1 Fault Tolerant Cluster: the fault tolerance mechanisms are enhanced to accommodate service instantiation in VLAN topologies (for both the Control- and Media-planes).

Figure 8 BCP7200 VLAN Tagging – Feature Overview



170.9.1 Installation and Commissioning (I&C)

There are two Installation and Commissioning procedures utilized to prepare the BCP7200 to host the RTP Media Portal Component:

- the “MCP09 BCT RTP MP - I&C MOP” [2], which sets up the IBM BladeCenterT platform. This MOP is enhanced to include a description of how the Nortel Networks Layer-2/3 Gigabit Ethernet Switching Module (ESM) can be configured to support logical partitioning of traffic, and how it can be configured to achieve a degree of physical separation between the various types of traffic.
- and the “RTP Portal Installation MOP” [3], which installs and configures the Linux Operating System on each of the service nodes (an IBM HS20 BladeServer that will host a RTP Media Portal Service Instance). This procedure is enhanced to collect optional VLAN information for the IP-address configured on the BladeServer (used to properly establish presence in the Management-plane for VLAN-tagged network topologies).

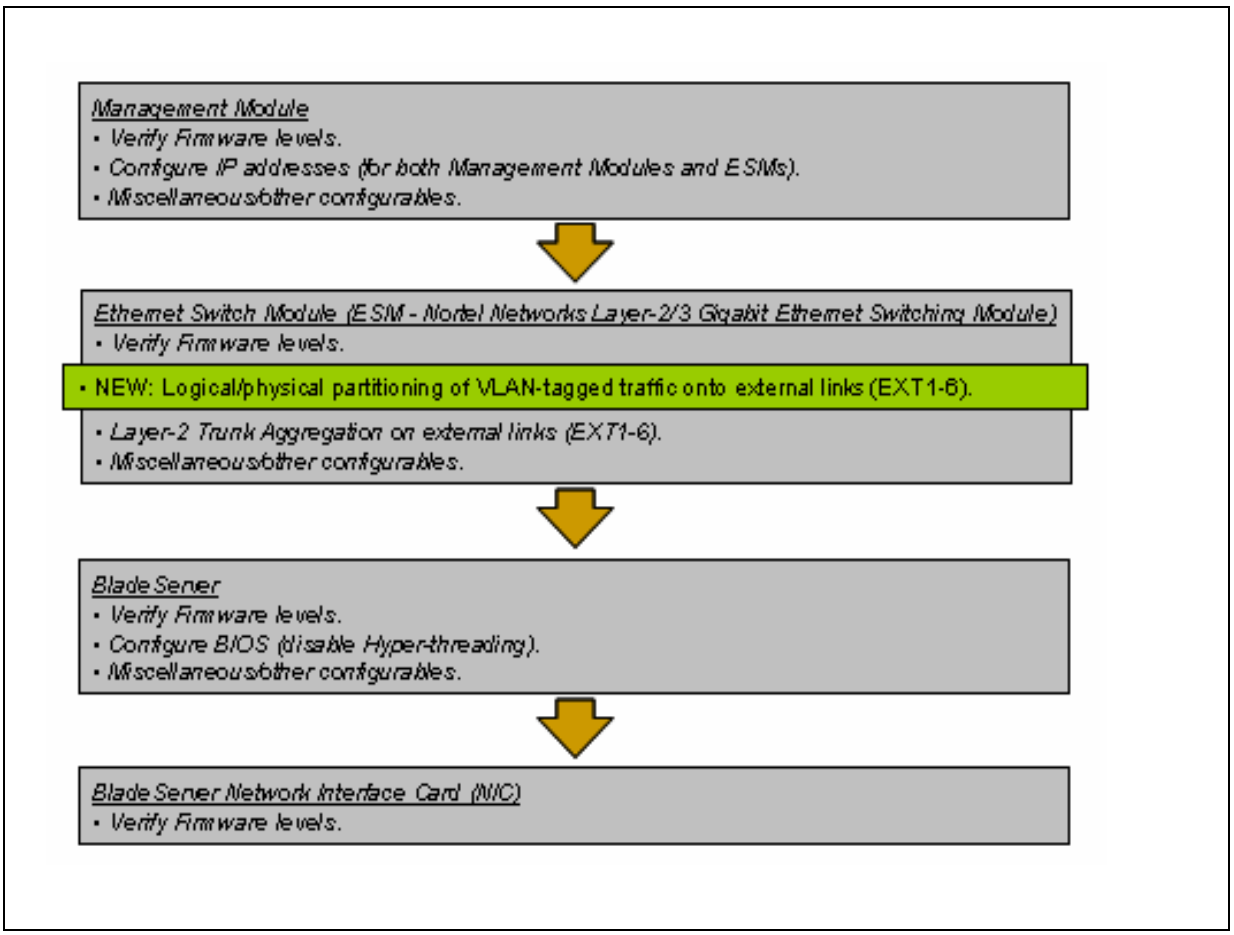
170.9.2 MCP09 BCT RTP MP - I&C MOP

170.9.3 Traffic Partitioning Overview

The “MCP09 BCT RTP MP - I&C MOP” [2] describes methods for ensuring that the subcomponents of the IBM BladeCenterT chassis are properly configured.

There is a new section added to this procedure that describes the methods that should be employed on the Nortel Networks Layer-2/3 Gigabit Ethernet Switching Module (ESM) to achieve the desired level of traffic partitioning for the various types of traffic traversing the network interconnect point between the BCP7200 and the Service Network (refer to ““MCP09 BCT RTP MP – I&C MOP” – Additions ” on page 1755).

Figure 9 “MCP09 BCT RTP MP – I&C MOP” – Additions

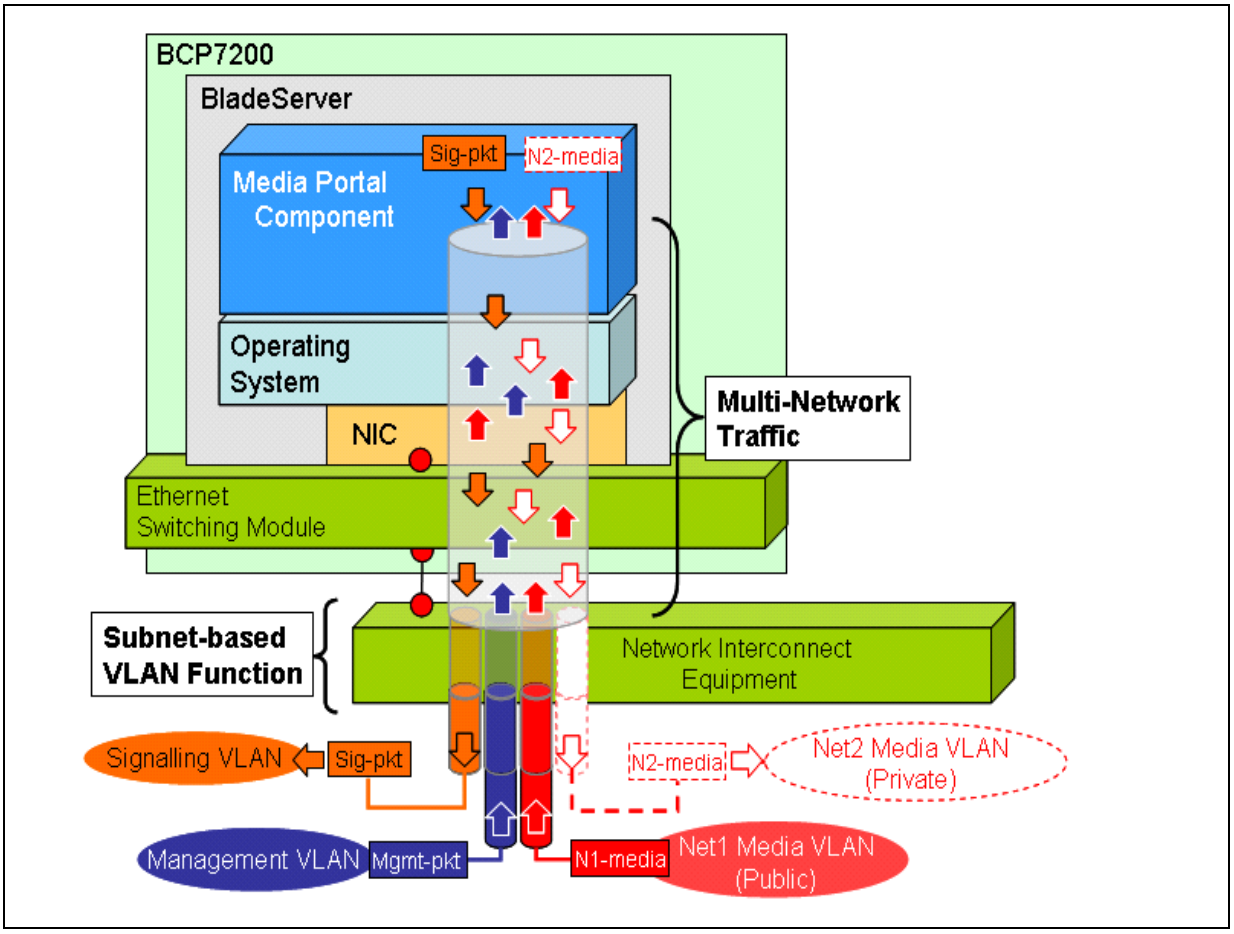


The Nortel Networks Layer-2/3 Gigabit Ethernet Switching Module (ESM) resides in-chassis and provides the switch fabric between the BladeServers (the service nodes that host the RTP Media Portal Service Instances) as well as

network interconnect to the Service Networks. As such, the ESM provides the point at which the BCP7200 interconnects into the Service Network.

Prior to the introduction of this feature the ESM could only be configured for non-tagged operation[1] (refer to “BCP7200 Service Network Interconnect – Multi-netted Flows ” on page 1756): all traffic was delivered as a multi-netted flow over the Layer-2 trunk connecting the BCP7200 to the Service Network. In certain configurations (typically for CS2K deployments) the multi-netted flow was later partitioned onto separate VLANs by some other network equipment outside of the BCP7200 (e.g. Network Interconnect Equipment providing Subnet-based VLAN functionality).

Figure 10 BCP7200 Service Network Interconnect – Multi-netted Flows



With the introduction of VLAN-tagging by this feature, it is now possible to configure the ESM to logically and/or physically partition the traffic flows

[1]When configured to operate in an untagged mode, the BCP7200 utilizes Standard Ethernet Frames for packet carriage.

delivered between the BCP7200 RTP Media Portal Service Instances and the Service Network (refer to “BCP7200 Service Network Interconnect – Logical Partitioning of Flows ” on page 1757, and “BCP7200 Service Network Interconnect – Physical Partitioning of Flows” on page 1758).

NOTE: *All configuration parameters will continue to default to the multi-netted configuration in order to preserve backwards compatability.*

Figure 11 BCP7200 Service Network Interconnect – Logical Partitioning of Flows

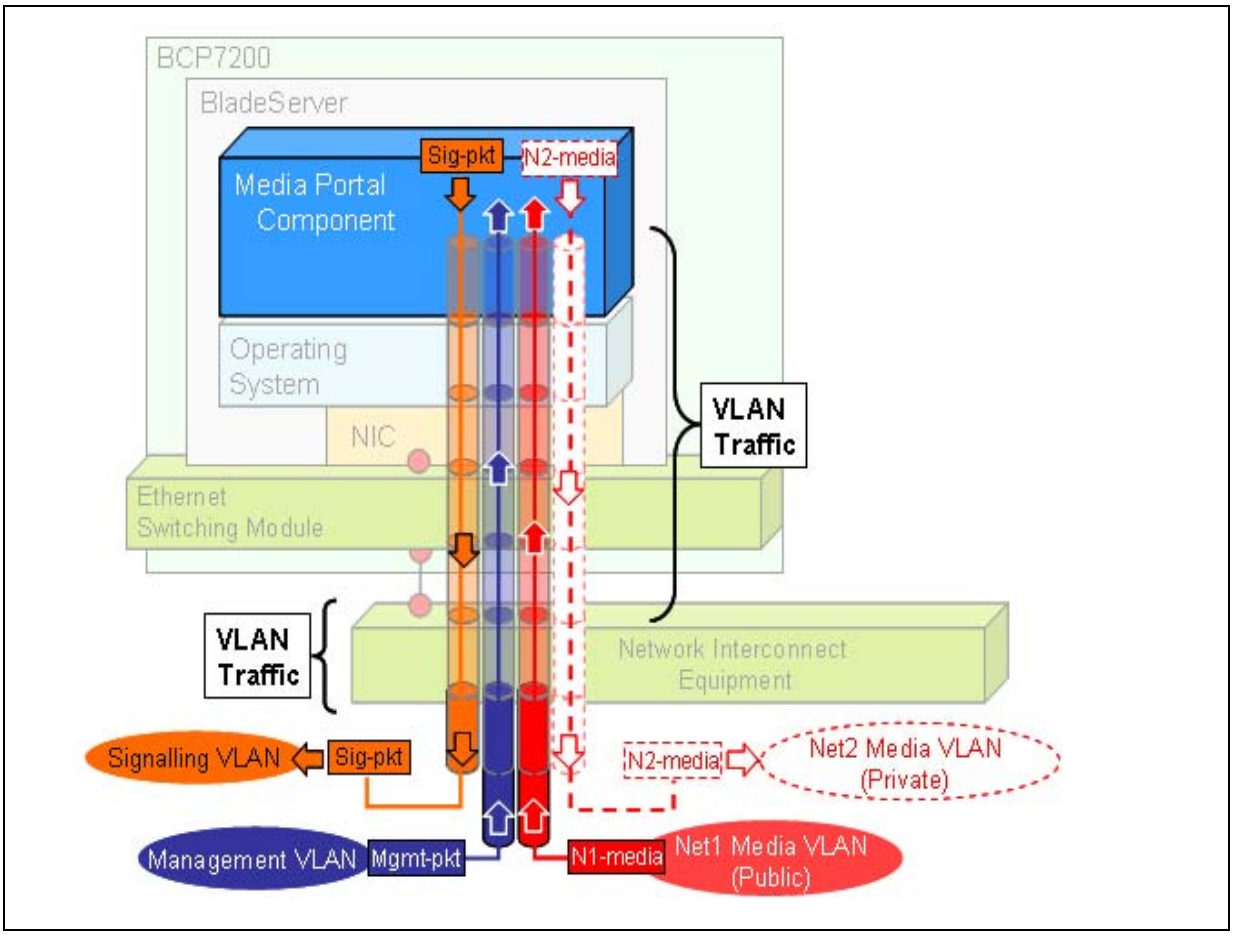
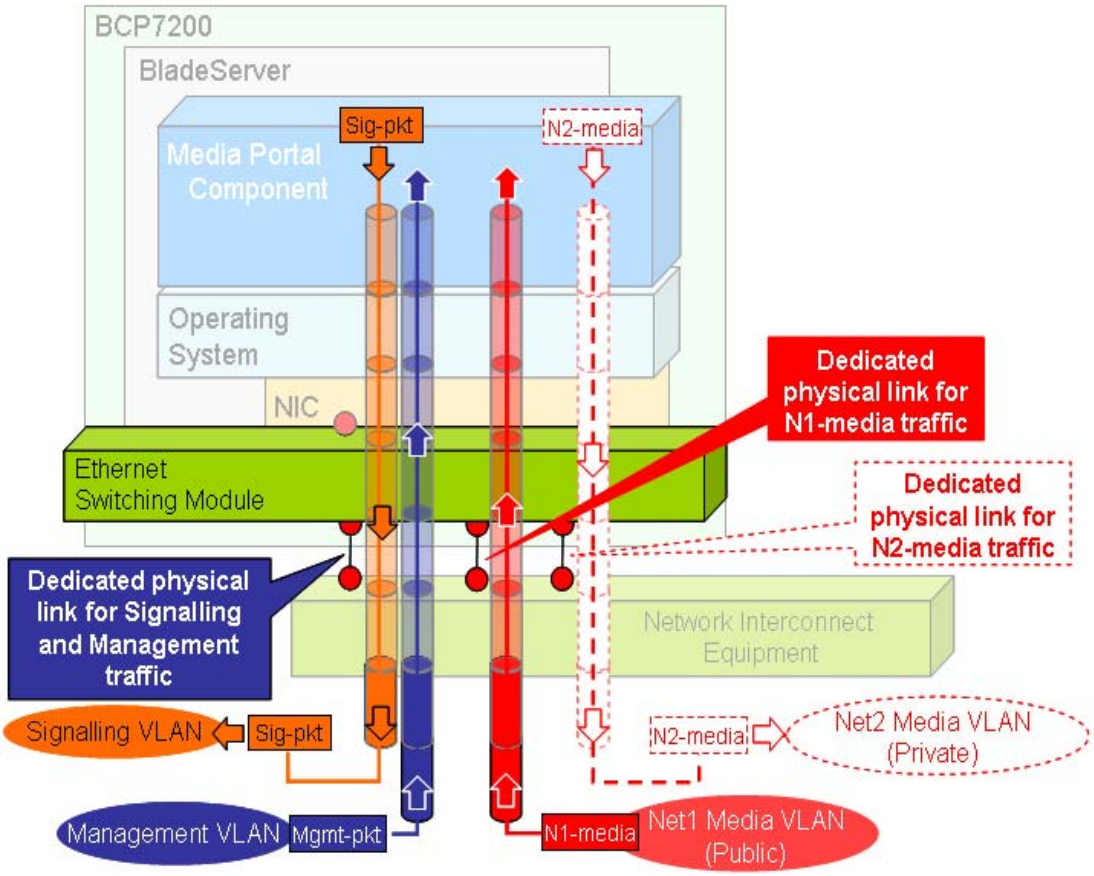


Figure 12 BCP7200 Service Network Interconnect – Physical Partitioning of Flows



170.9.4 ESM Configuration for IEEE 802.1Q VLAN-tagging

The ESM supports IEEE 802.1Q VLAN-tagging.

The Alteon OS running in the ESM supports up to 128 VLANs per switch. Even though the maximum number of VLANs supported at any given time is 128, each can be identified with any number between 1 and 4095.

In order to properly interconnect and convey VLAN-tagged packets to their destination, the ESM must be configured to support the intended broadcast domains and to provide the desired degree of partitioning between those broadcast domains.

Each port on the ESM can belong to one or more VLANs, and each VLAN can have any number of ESM ports in its membership. Any port that belongs to multiple VLANs, however, must have VLAN tagging enabled. Any untagged frames (those with no VLAN specified) are classified with the sending port's PVID.

It is through the association of ESM ports to VLANs that logically and physically partitioned traffic is able to traverse the BCP7200 interconnect with the Service Network.

170.9.4.1 Multi-Network/Unpartitioned Flows (Default)

The ESM factory default configuration makes use of an internal VLAN configuration (all external ESM ports are untagged) where:

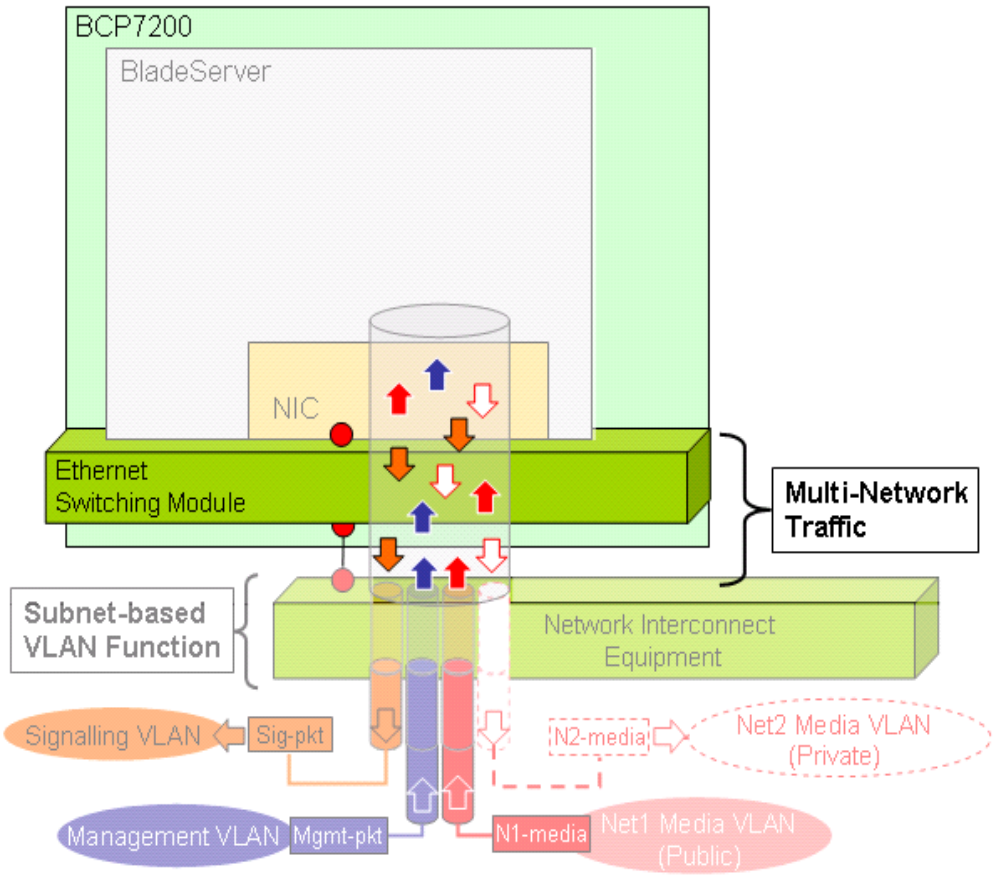
- VLAN 1 is the default service VLAN for connecting the external ports (EXT1-6) and the internal blade ports (INT1-8).
- VLAN 4095 is used by the out-of-band management network for chassis/ platform administration.

The factory default setting places all non-management ports (i.e. ports EXT1-6, and ports INT1-8) on the same VLAN initially - although each port's PVID is configurable to any VLAN number between 1 and 4094. Each port on the ESM is also configured with a default VLAN number, known as its PVID (default PVID = 1).

The factory default configuration for the ESM also has all external ports set as untagged members of VLAN 1.

This factory default ESM configuration enables theBCP7200 to handle multi-netted traffic (untagged) to flow across the Service Network interconnect (refer to "ESM – Configuration for Multi-Network Traffic (Default)" on page 1760).

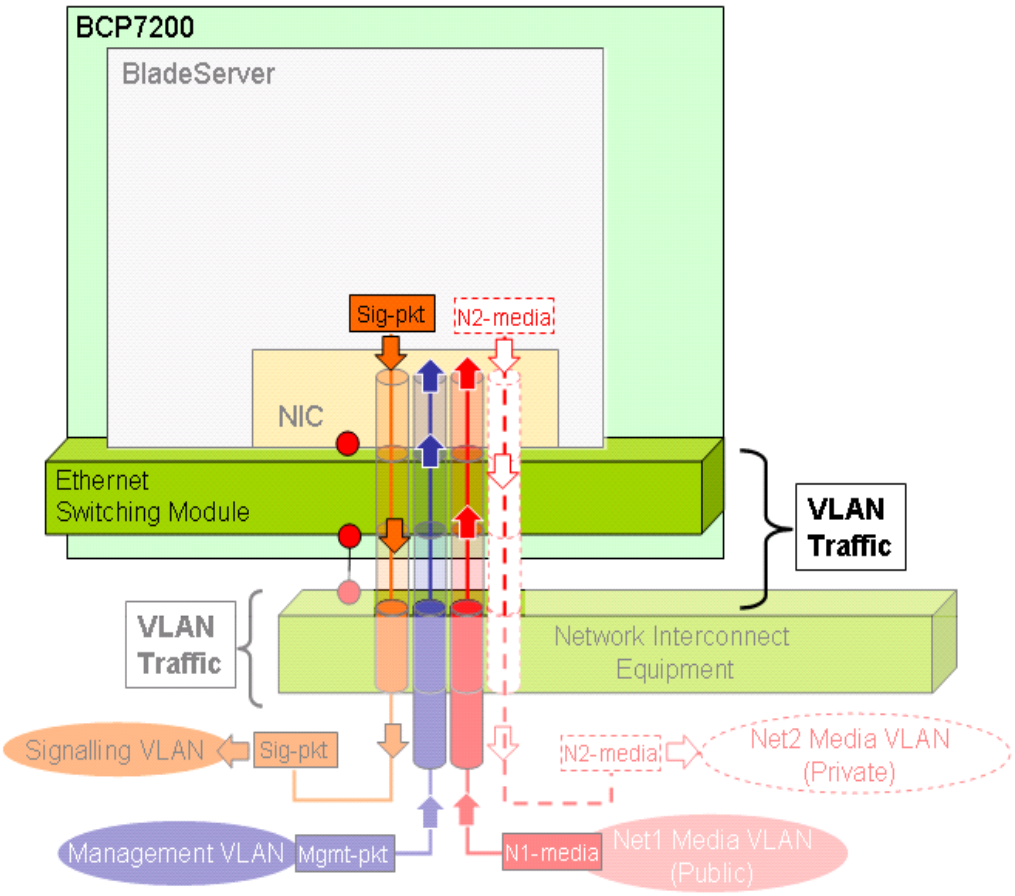
Figure 13 ESM – Configuration for Multi-Network Traffic (Default)



170.9.4.2 Logical Partitioning of Flows

Logical Partitioning of traffic flows between the BCP7200 and the Service Network (refer to “ESM – Configuration for Logical Partitioning of Traffic” on page 1761) is accomplished by configuring the ESM for membership in the desired Service Network VLANs – and by enabling VLAN tagging on the ESM service ports (EXT1-6, and INT1-8). This extends the logically partitioned Service Network VLANs to the service nodes (Blade Servers) that will eventually host a running Media Portal Service Instance.

Figure 14 ESM – Configuration for Logical Partitioning of Traffic



It is assumed in a VLAN-tagged network topology that only VLAN-tagged frames will traverse the Service Network Interconnect. However; the PVID associated with the EXT ports on the ESM can be set to a desired value to accommodate handling of untagged frames (should such be encountered).

When preparing for I&C of the BCP7200 into a VLAN-tagged network, it is important to understand the underlying topology. Of relevance to the logical partitioning of traffic are (refer to Table 3 VLAN Network Topology Information for Logical Separation3 on page 1762): the number of Service Network VLANs in which the BCP7200 must participate, and the specific Service-planes and network spaces that these VLANs occupy. It is the existing Service Network Topology into which the BCP7200 must interconnect (i.e. the presence of, and values for: x, y, z1and z2) that dictates how traffic is logically partitioned. This information is required in order to configure the proper interconnect between the ESM and the Service Network.

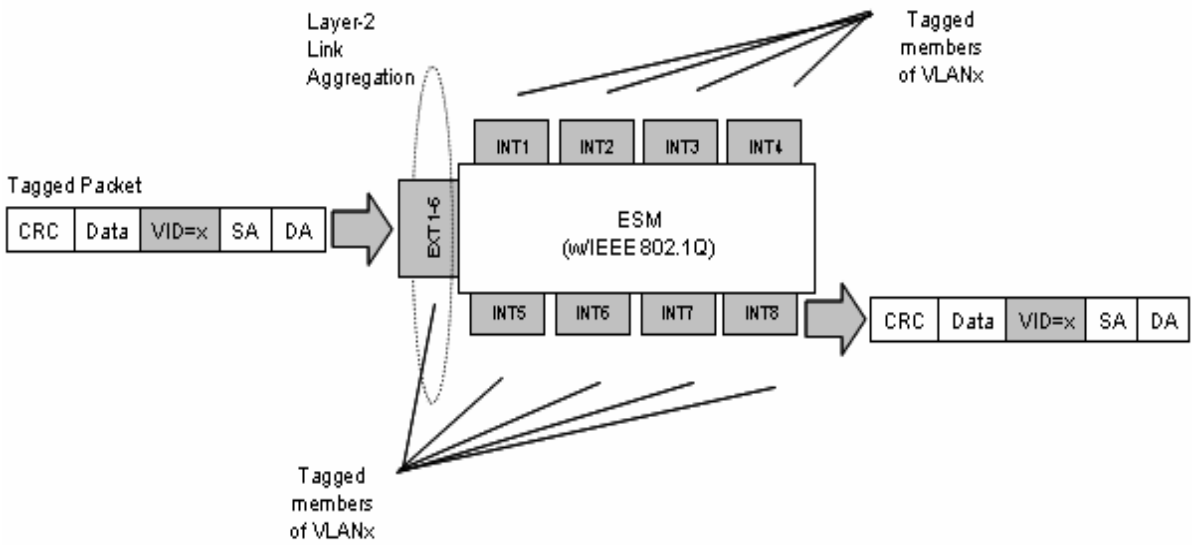
Table 3 VLAN Network Topology Information for Logical Separation

Service Plane / Network Space	VID
Management-Plane (OAM)	x
Control-Plane (MPCP)	y
Media-Plane (Net1 media)	z1
Media-Plane (Net2 media)	z2
Peering-Plane	*Not Applicable*

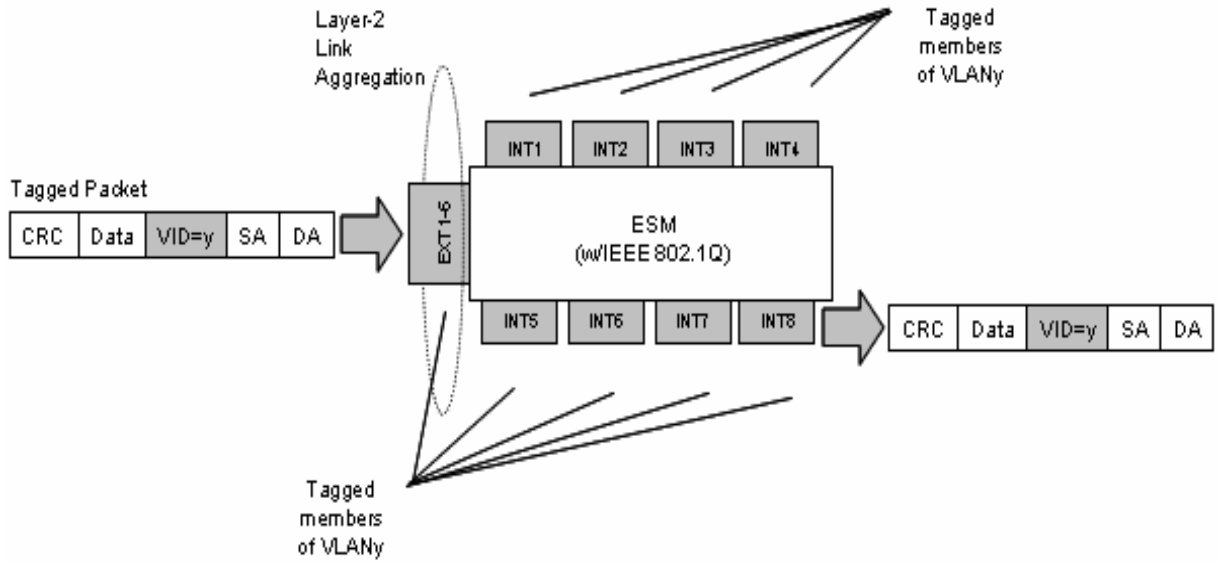
The Service Network's VIDs must be accounted for in both: the platform configuration during I&C (to provide an ESM configuration that supports proper interconnect and relay between the Service Network and the Blade Servers), and the service configuration in the SMGUI (to provide the RTP Media Portal Service with the topological knowledge required for participation in VLAN-tagged Service Networks).

The following permutations of VLAN-tagged network topologies are possible:

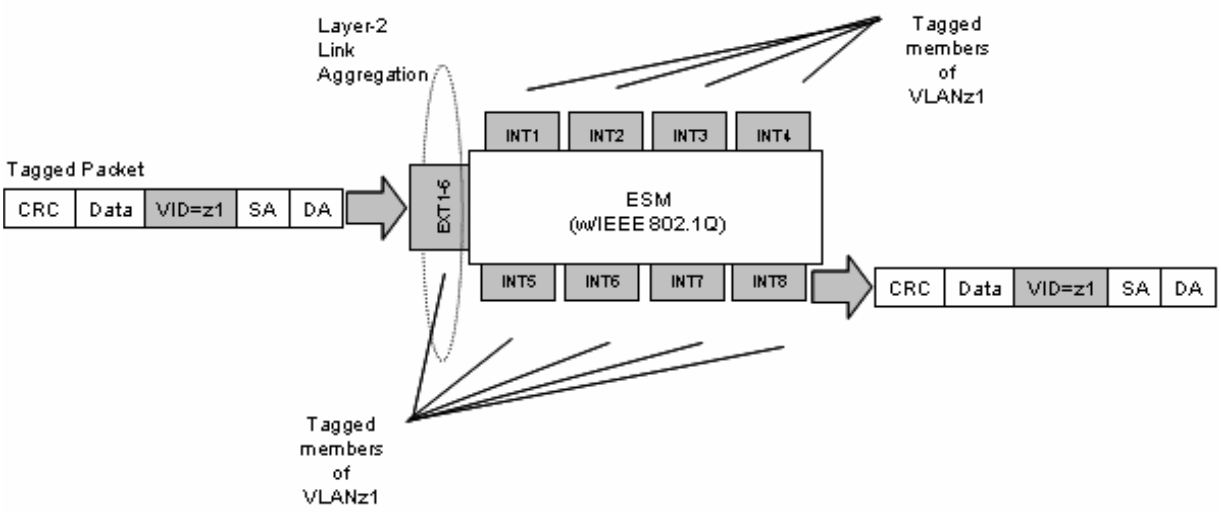
- **Unique VIDs (xyz1z2)** – there is a unique VID for each network space, and all ESM service ports (EXT1-6 and INT1-8) are configured for membership in each of these VLANs. Thus, service traffic can traverse the ESM switching fabric between the Service Network and the Service Node(s). For example:
  - OAM traffic (tagged with "VID=x") from the Service Network arrives at the ESM (on the Layer-2 trunk formed by ports EXT1-6) and traverses VLANx for delivery to the appropriate Service Node (e.g. INT8). Similar processing occurs for tagged frames originating on the Service Node and destined for the Service Network.

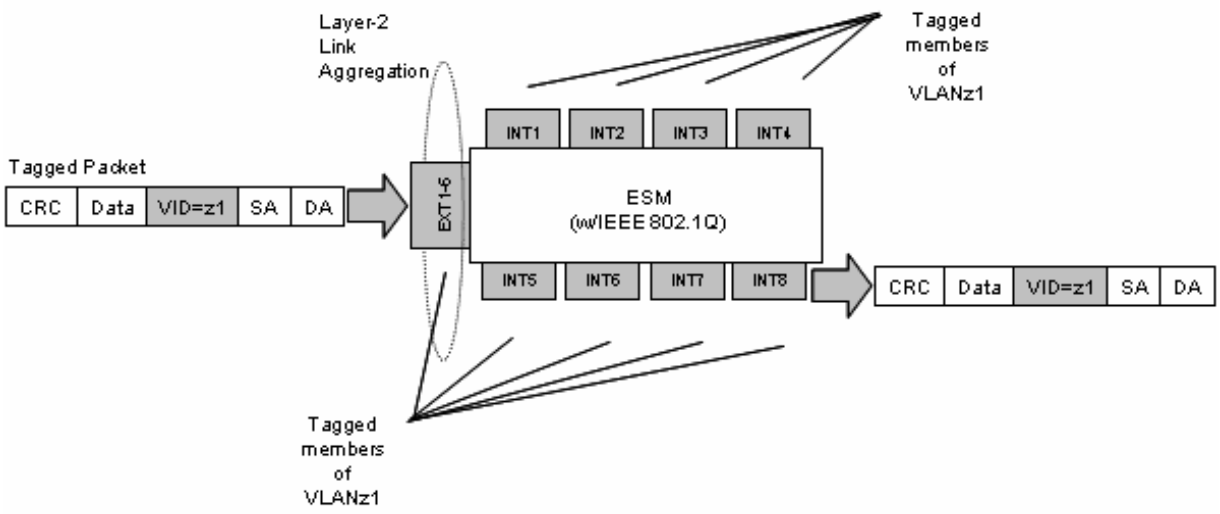


- MPCP traffic (tagged with "VID=y") from the Service Network arrives at the ESM (on the Layer-2 trunk formed by ports EXT1-6) and traverses VLANy for delivery to the appropriate Service Node (e.g. INT8). Similar processing occurs for tagged frames originating on the Service Node and destined for the Service Network.



- Media traffic (tagged with either "VID=z1" or "VID=z2") from the Service Network arrives at the ESM (on the Layer-2 trunk formed by ports EXT1-6) and traverses VLANz1/VLANz2 for delivery to the appropriate Service Node (e.g. INT8). Similar processing occurs for tagged frames originating on the Service Node and destined for the Service Network.





- **Shared VIDs (x=y, or x=z1, y=z1, etc.)** – some VIDs are common to multiple network spaces, and all ESM service ports (EXT1-6 and INT1-8) are configured for membership in each of the required VLANs. Thus, service traffic can traverse the ESM switching fabric between the Service Network and the Service Node(s).
- **Common VID (x=y=z1=z2)** – there is one single VID for all service plane traffic, and all ESM service ports (EXT1-6 and INT1-8) are configured as members of this VLAN. Thus, service traffic can traverse the ESM switching fabric between the Service Network and the Service Node(s).

NOTE: *This Common VID topology is similar to originally existing multi-netted traffic flows, except in this configuration the multi-netted traffic is delivered inside tagged frames.*

In order to configure the ESM to support such VLAN-tagged topologies, the following ESM commands are used:

- To add VLAN topology knowledge into the ESM:

    1. Access the ESM configuration menu for each Service Network VLAN:

       /cfg/l2/vlan <x>

       where:

       <x> = the Service Network VID.

    2. Add ESM ports to a specific VLAN:

       /cfg/l2/vlan <x>/add <port>

       where:

<x> = the Service Network VID.

<port> = the service port (EXT1-6, or INT1-8).

- To enable VLAN-tagging on ESM ports:

  /cfg/port <port>/tag e

  where:

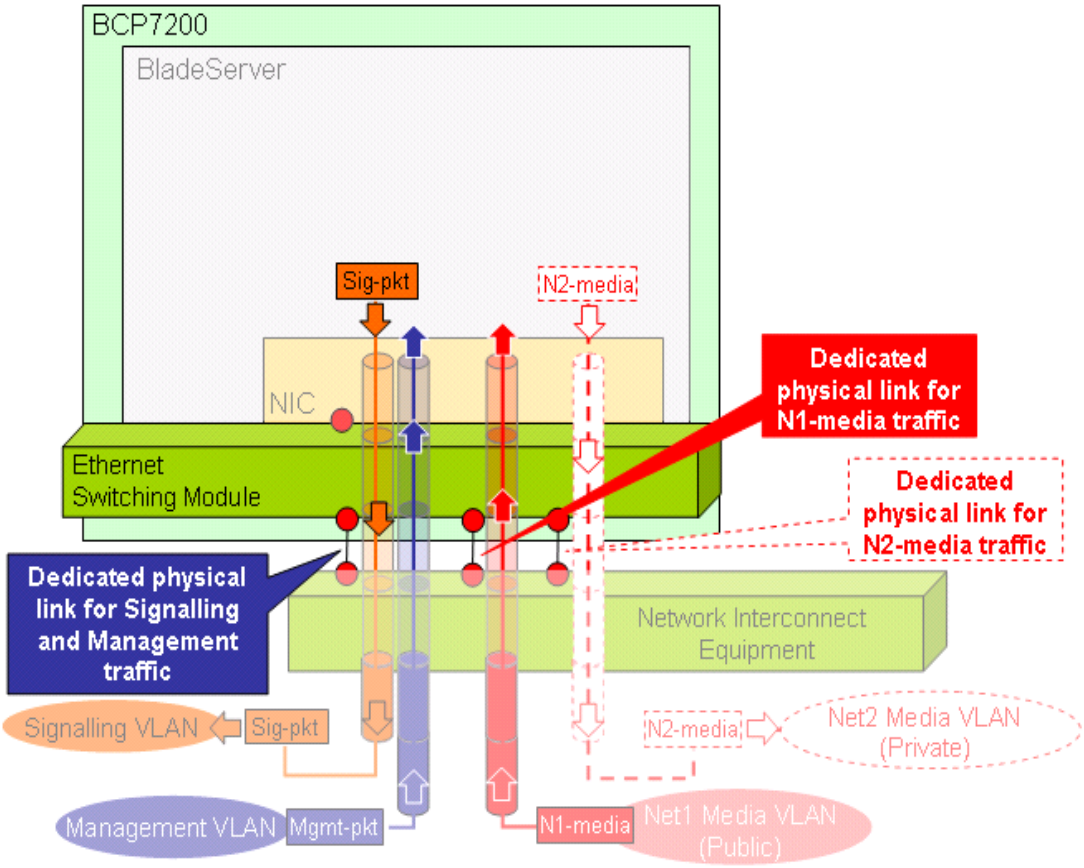
  <port> = the target service port (EXT1-6, or INT1-8).

170.9.4.3 Physical Partitioning of Flows

In addition to being able to support the logical partitioning of service flows, the ESM can also be configured to provide a degree of physical separation between flows at the Service Network Interconnect.

Physical partitioning is accomplished through the dedicated membership of certain external physical service ports (EXT1-6) to a specific VLAN(s). Once this association is made, only traffic from that specific VLAN(s) will traverse that physical link(s). Refer to “ESM – Configuration for Physical Partitioning of Traffic” on page 1766.

Figure 15 ESM – Configuration for Physical Partitioning of Traffic



Once again, when preparing for I&C of the BCP7200 into a network, it is important to understand the underlying topology. However; in addition to the information required to maintain the logical separation of traffic flows (the number of VLANs in which the BCP7200 must participate – and the specific Service-planes and network spaces that these VLANs occupy), the degree of physical separation must also be determined (refer to Table 4 VLAN Network Topology Information for Physical Separation). The additional External Service Port information is required in order to configure the proper physical/ logical interconnect between the ESM and the Service Network.

Table 4 VLAN Network Topology Information for Physical Separation

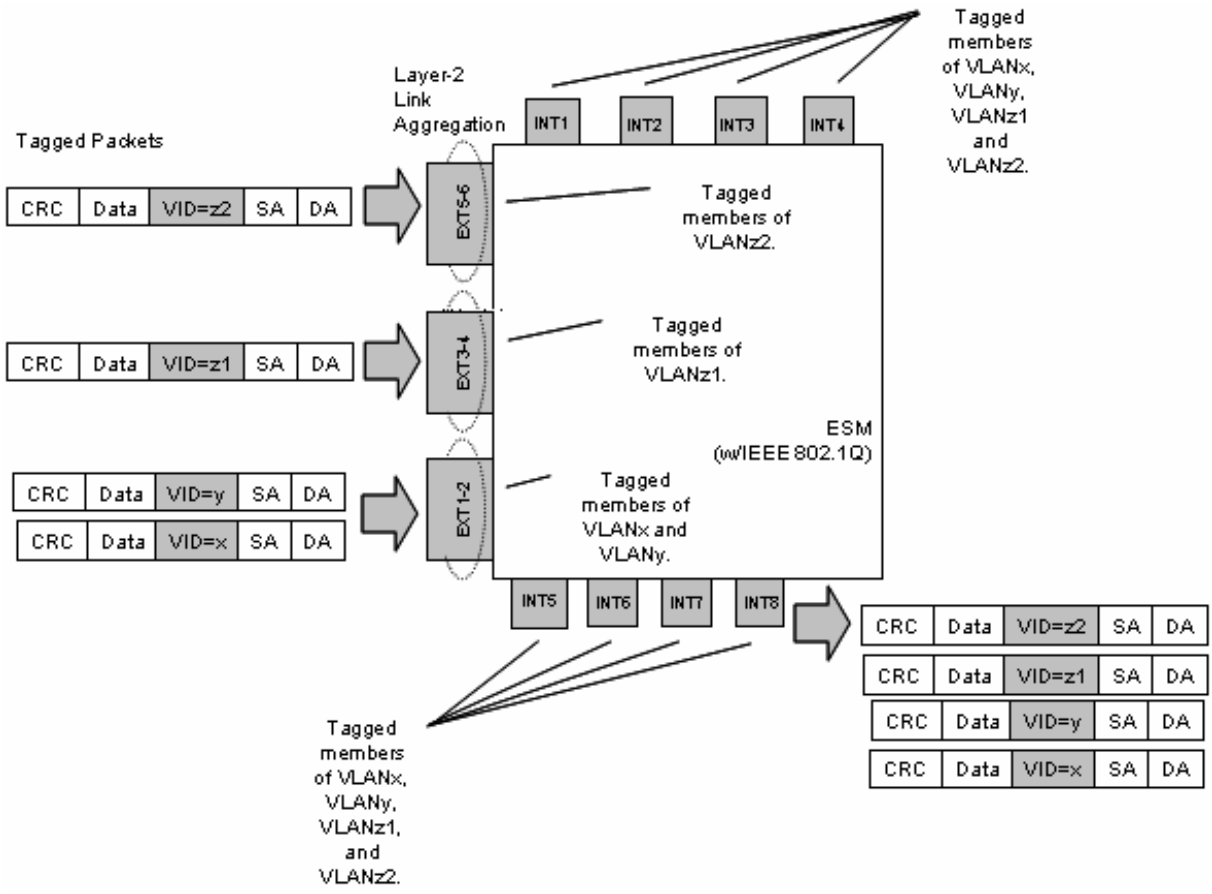
Service Plane / Network Space	VID	External Service Port(s)
Management-Plane (OAM)	x	{EXT1-EXT6}
Control-Plane (MPCP)	y	{EXT1-EXT6}
Media-Plane (Net1 media)	z1	{EXT1-EXT6}
Media-Plane (Net2 media)	z2	{EXT1-EXT6}
Peering-Plane	*Not Applicable*	{EXT1-EXT6}

NOTE: *The ESM can support a maximum of three (3) separate Layer-2 Link Aggregation trunks. This will limit the number of physically partitioned configurations possible that support Layer-2 Fault Tolerance using Link Aggregation.*

An example is provided below of an ESM configured for physical separation of traffic at the Service Network Interconnect where there are three degrees of physical separation:

- OAM and MPCP traffic only traverses links EXT1-2 (EXT1-2 are configured as members of both VLANx and VLANy),
- Net1 media traffic only traverses links EXT3-4 (EXT3-4 are configured as members of only VLANz1),
- and Net2 media traffic only traverses links EXT5-6 (EXT5-6 are configured as members of only VLANz2).

All service traffic appears on all internal ESM service ports (INT1-8 are configured as members of VLANx, VLANy, VLANz1, and VLANz2). Thus, service traffic can traverse the ESM switching fabric between the Service Network and the Service Node(s) using physically separate external links:

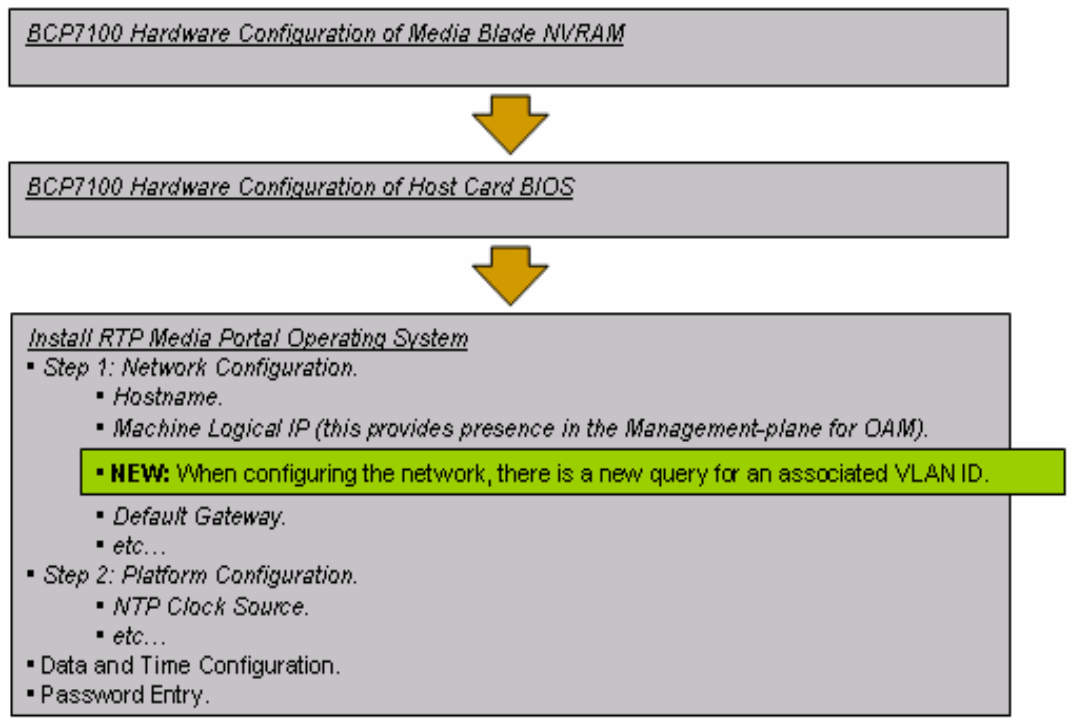


170.9.4.4 RTP Portal Installation MOP

The “RTP Portal Installation MOP” [3] includes a procedure that describes the installation and configuration of the Operating System which prepares the platform for hosting an RTP Media Portal Service Instance.

There is a new step added to this procedure that queries for information regarding the potential presence of VLAN-tagged Service Network topologies when configuring presence in the Management-plane (refer to ““RTP Portal Installation MOP” – Additions ” on page 1769). The default value for the possible Management-plane VLAN ID is “<none>” in order to provide backwards compatibility with existing multi-netted configurations.

Figure 16 "RTP Portal Installation MOP" – Additions

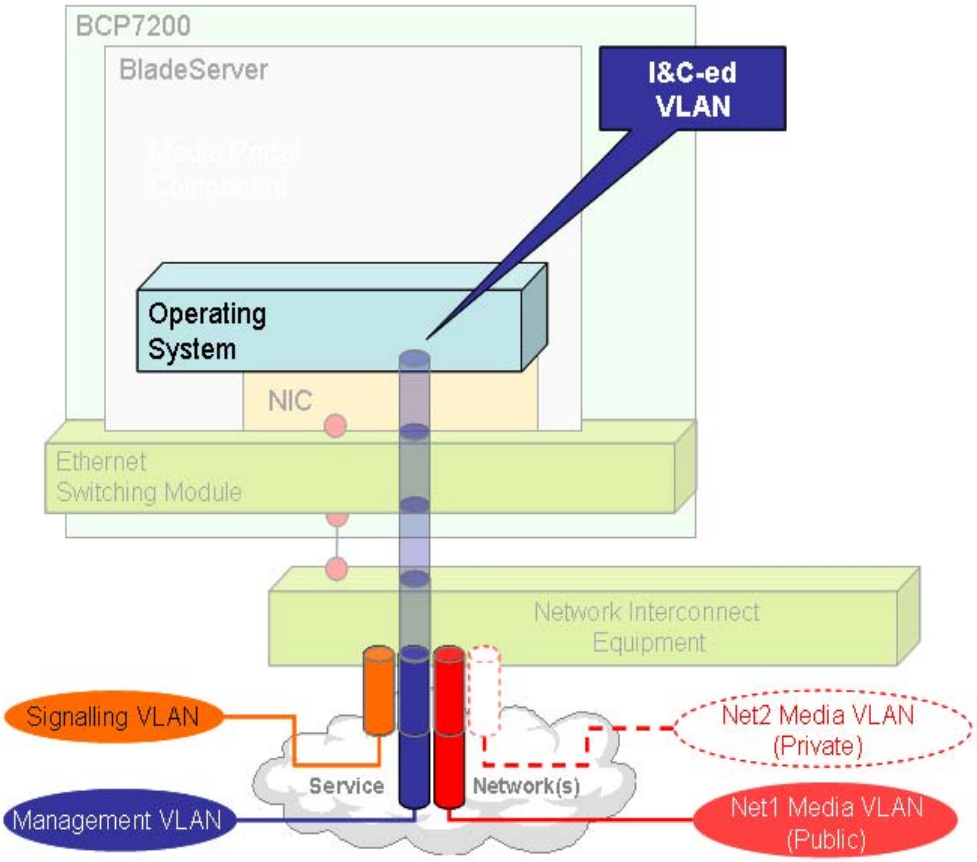


The new query added to this procedure is:

> **Enter associated VLAN? <none>**
>
> (If this BCP7200 does not reside in an IEEE 802.1Q VLAN-tagged network topology, then press the <Enter-key> to proceed with the default configuration "<none>" to establish operation in an untagged environment)

This new VLAN information is used to establish Management-plane presence in an IEEE 802.1Q VLAN-tagged network topology (refer to "BCP7200 – I&C of Management-plane VLAN " on page 1770).

Figure 17 BCP7200 – I&C of Management-plane VLAN



170.10 System Management Graphical User Interface (SMGUI)

170.10.1 Overview

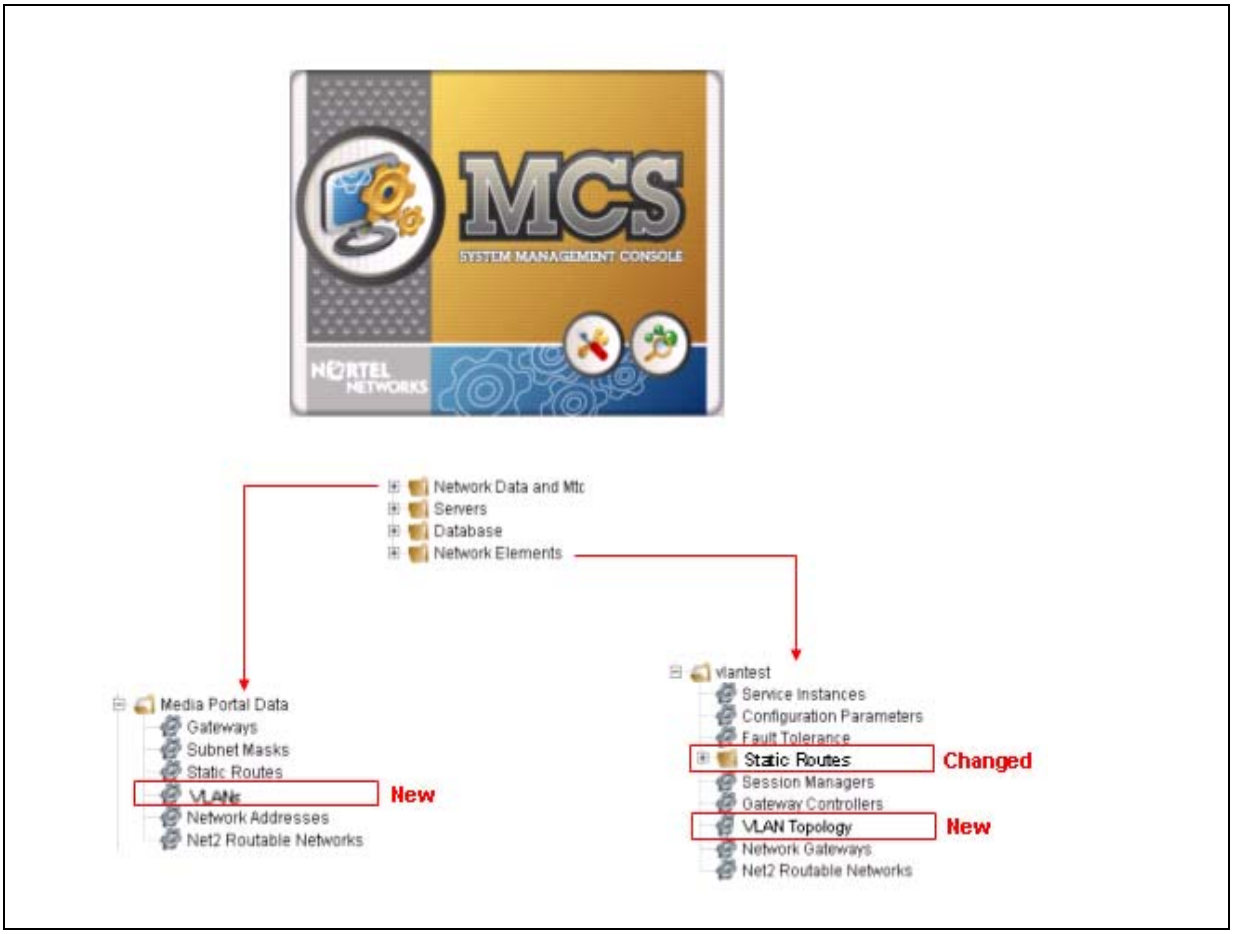
The System Management Graphical User Interface (SMGUI) is enhanced to accommodate configuration of the BCP7200 RTP Media Portal service for operation in VLAN-tagged Service Network topologies.

This new configuration information relates to (refer to “BCP7200 SMGUI – Support for VLAN-tagged Service Network Topologies ” on page 1771):

- Service Network VLAN Topology:
  - New “VLAN” configuration parameter added to “Network Data & Mtc” to permit specification of Service Network VLAN information.
  - New “VLAN Topology” configuration parameter added to the “Media Portal Cluster” data to permit association of an RTP Media Portal Service Instance’s network spaces to specific VLANs.
- Static Route VLAN Assignments:

- Changed the “Static Routes” configuration parameter in the “Media Portal Cluster” data into a data structure that permits more granular assignment of Static Routes to specific VLANs.

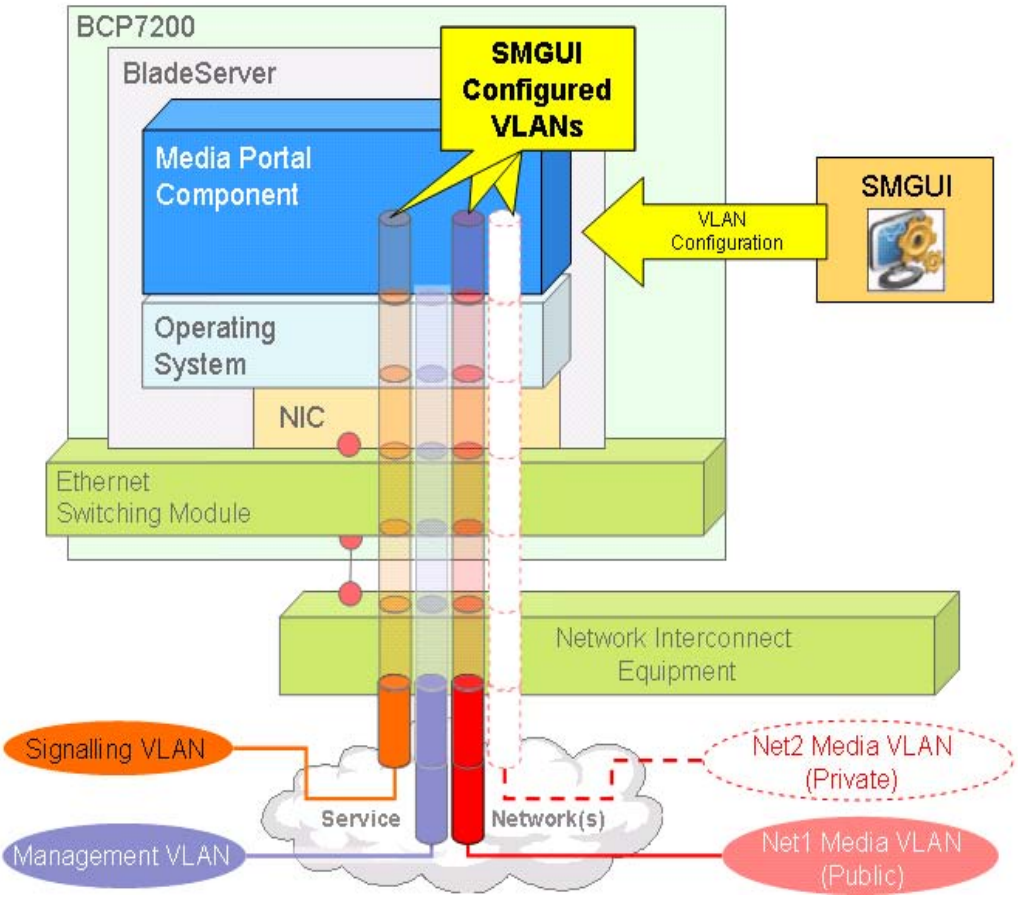
Figure 18 BCP7200 SMGUI – Support for VLAN-tagged Service Network Topologies



The introduction of VLAN information into the system enables RTP Media Portal Service Instances hosted on the BCP7200 to be configured with presence in separate VLANs that represent (refer to “BCP7200 – SMGUI Configuration of Control- and Media-plane VLANs ” on page 1772):

- a distinct network space for Control-plane traffic,
- and two separate network spaces for Media-plane traffic (one for Net1 media, and the other for Net2 media).

Figure 19 BCP7200 – SMGUI Configuration of Control- and Media-plane VLANs



170.10.1.1 SMGUI - Service Network VLAN Topology

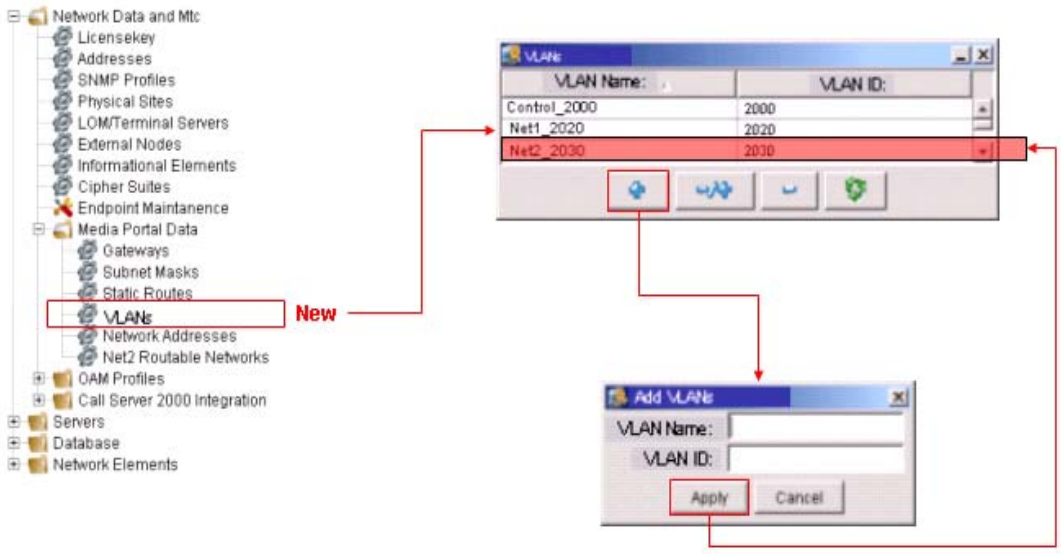
Knowledge of the Service Network VLAN Topology is entered into the system using the new “VLAN” configuration parameter added to “Network Data & Mtc”.

Every VLAN in the Service Network that is intended to be extended to the BCP7200 must be datafilled into the system as follows (refer to “SMGUI - Configuration of Service Network VLANs ” on page 1773):

1. Open the System Management Console to view the System Management GUI (SMGUI).
2. In the navigation pane (left-side) click on the “Network Data & Mtc” folder to view its contents.
3. In the navigation pane (left-side) find the “Media Portal Data” folder inside of “Network Data & Mtc” and click it to view its contents. There is a new configuration parameter (“VLANs”) present in the “Media Portal Data” folder.

4. In the navigation pane (left-side) find the new “VLANs” configuration parameter in the “Media Portal Data” folder. Click on the “VLANS” configuration parameter to open the “VLANs” configuration window in the work area (right-side pane). In the “VLANs” configuration window use:
    - the “+” button to add new Service Network VLANs into the system.
    - the “-“ button to remove Service Network VLANs from the system.
    - the “+/-“ button to edit data for Service Network VLANs already existing in the system.
5. In the “VLANs” configuration window click the “+” button to open the “Add VLANs” window and add new Service Network VLAN information into the system:
    - “VLAN Name” – a unique name in the system that represents this particular data element.
    - “VLAN ID” – this is the VLAN Identifier (VID) that defines this VLAN in the Service Network.

Figure 20 SMGUI - Configuration of Service Network VLANs

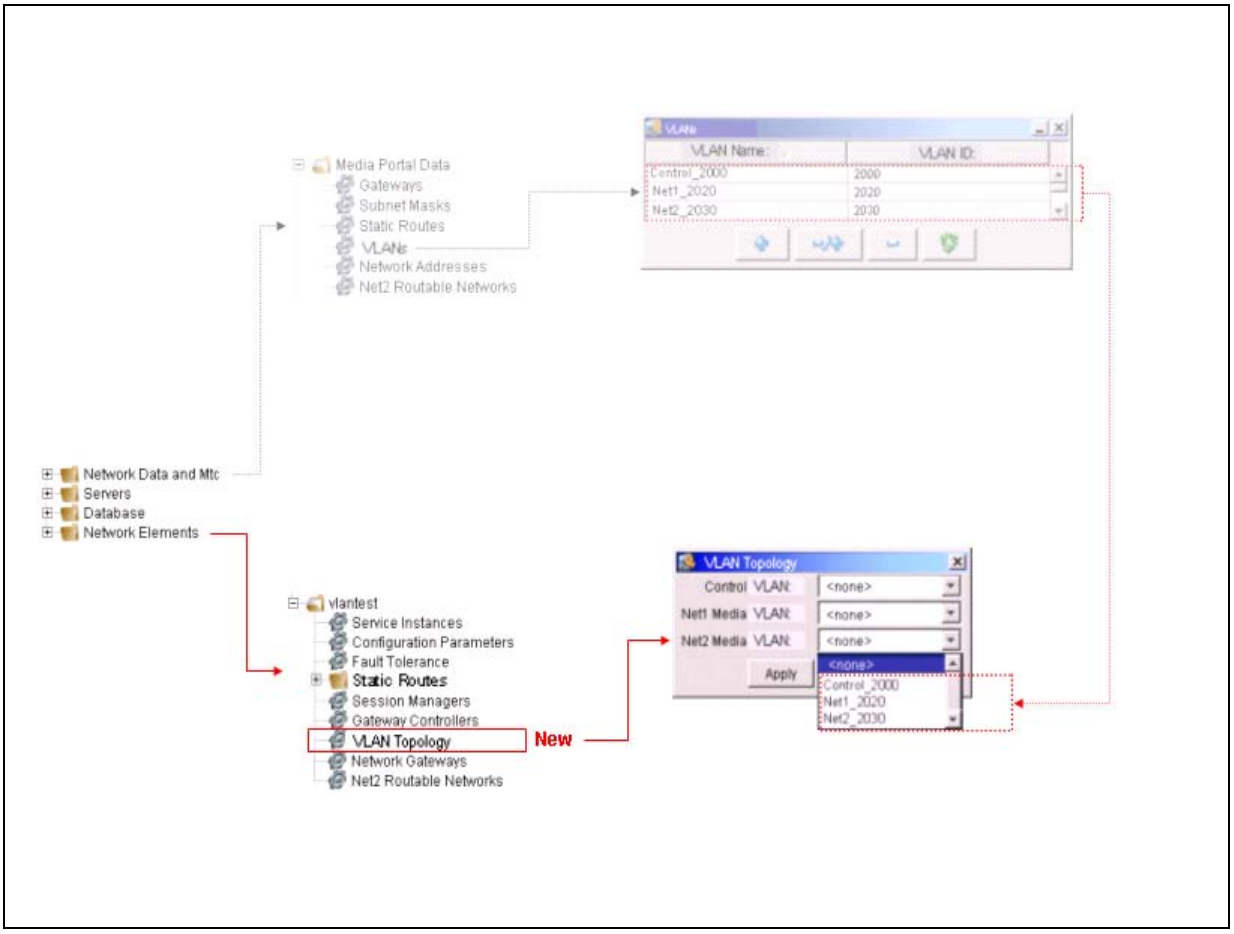


Once all of the required Service Network VLANs are defined in the system, they can be associated with any combination of BCP7200 RTP Media Portal Service Instances using the new “VLAN Topology” configuration parameters present in the “Media Portal Cluster” data as follows (refer to “SMGUI – Association of RTP Media Portal Service Instances with Service Network VLANs ” on page 1775):

1. Open the System Management Console to view the System Management GUI (SMGUI).
2. In the navigation pane (left-side) click on the “Network Elements” folder to view its contents.
3. In the navigation pane (left-side) find the “Media Portals” folder inside of “Network Elements” and click it to view its contents.
4. In the navigation pane (left-side) find the “Media Portal Cluster” folder inside of “Media Portals” and click it to view all of the BCP7200 RTP Media Portal Service Clusters datafilled in the system. Each BCP7200 RTP Media Portal Cluster has a new configuration parameter (“VLAN Topology”) that can be used to associate these entities with Service Network VLANs (when adding/editing specific “Media Portal Cluster” instances).
5. In the navigation pane (left-side) add/edit a “Media Portal Cluster” instance (i.e. open the folder to view the available configuration parameters). The new “VLAN Topology” configuration parameter is present.
6. In the navigation pane (left-side) click on the new “VLAN Topology” configuration parameter to open the “VLAN Topology” window for this “Media Portal Cluster” in the work-area (right-side pane). The “VLAN Topology” window contains three information elements (all defaulted to “<none>” to represent configuration for untagged operation):
   - “Control VLAN”: this element is used to associate a Service Network VLAN to the Control IP address.
   - “Net1 Media VLAN”: this element is used to associate a Service Network VLAN to the Net1 Media IP address.
   - “Net2 Media VLAN”: this element is used to associate a Service Network VLAN to the Net2 Media IP address.
7. In the “VLAN Topology” window (located in the right-side pane work-area) select the Service Network VLAN intended for association using the pick-list. The pick-list is populated with the Service Network VLAN information that was entered into the system using the new “VLAN” data structure located in “Network Data & Mtc”.
8. Once all desired associations are made, click the “Apply” button in the “VLAN Topology” window to submit this information into the system.

Note: *The BCP7200 does not support live update of configuration changes, so configuration data does not get picked up in run-time until the BCP7200 is cycled (e.g. Stop+Start, Kill+Start, or Restart).*

Figure 21 SMGUI – Association of RTP Media Portal Service Instances with Service Network VLANs



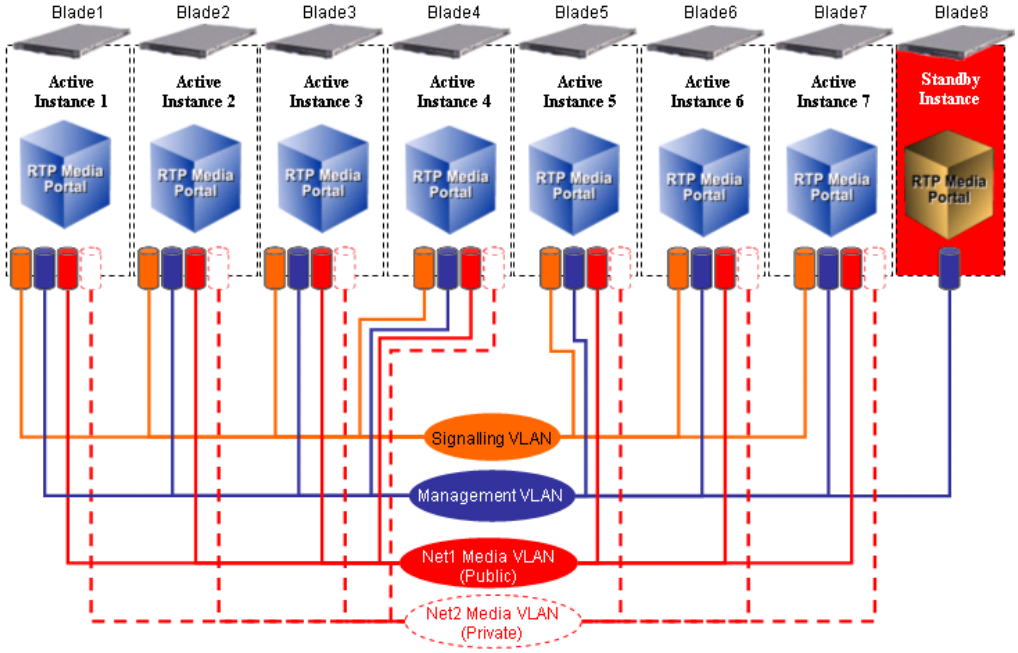
170.10.2 N+1 Fault Tolerant Service Cluster

The BCP7200 RTP Media Portal Fault Tolerant Service Cluster is enhanced to accommodate utilization of the Service Network VLAN topology during takeover actions. Thus, when the standby RTP Media Portal Service Instance detects a failure and begins running the active Service Instance, it will reconnect into the Service Network using the VLAN topology associated with the RTP Media Portal Service Instance (i.e. a Control VLAN, a Net1 Media VLAN, and a Net2 Media VLAN).

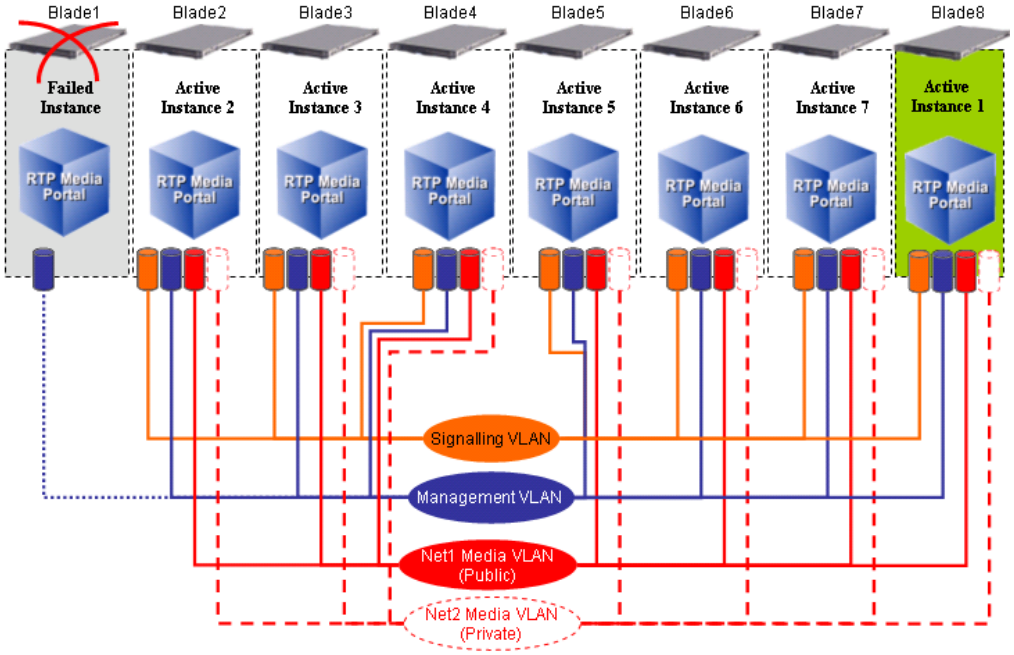
For example:

1. Assuming a stable BCP7200 “7+1” RTP Media Portal Fault Tolerant Service Cluster (Active Instances 1-7 running on Blade Servers 1-7, and the Standby

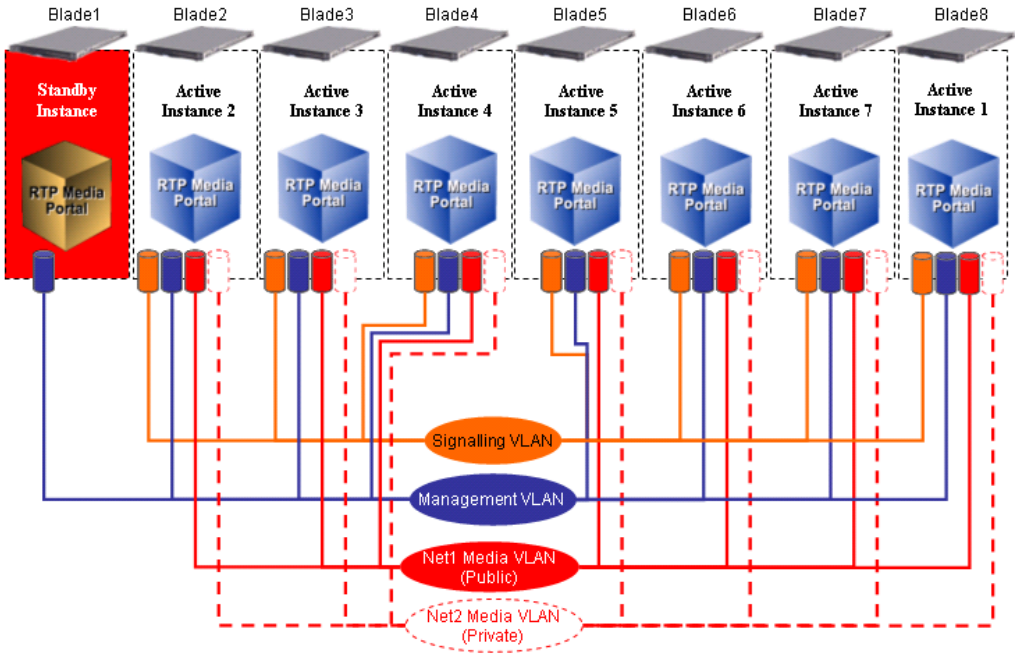
Instance running on Blade Server 8) interconnected into a VLAN-tagged Service Network:



2. In the event of a failure affecting an active RTP Media Portal Service Instance (e.g. Blade Server 1 fails destroying Active Instance 1), then the standby RTP Media Portal Service Instance will immediately instantiate itself as the affected RTP Media Portal Service Instance (Active Instance 1 begins running on Blade Server 8 – and interconnects with the Service Network using the configured VLAN network topology). The Service Cluster will continue to provide non-redundant service until the system recovers from the failure:



3. When the system recovers, the affected RTP Media Portal Service Instance (e.g. the instance running on Blade Server 1) attempts to re-join the Service Cluster and determines that it must now run as the standby Service Instance (e.g. the Standby Instance is now running on Blade Server 1). At this point, the Service Cluster is once again providing fully redundant service:

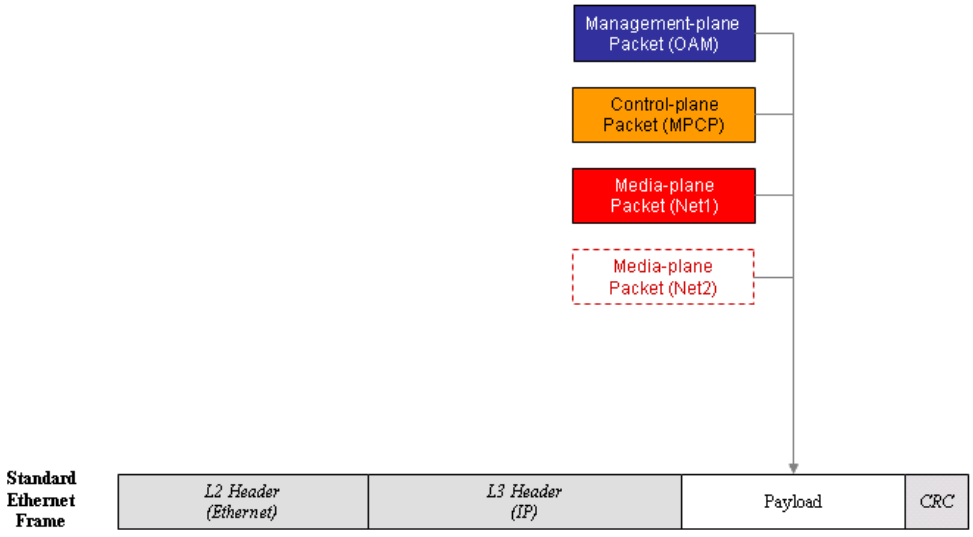


170.11 Service Packet Flows

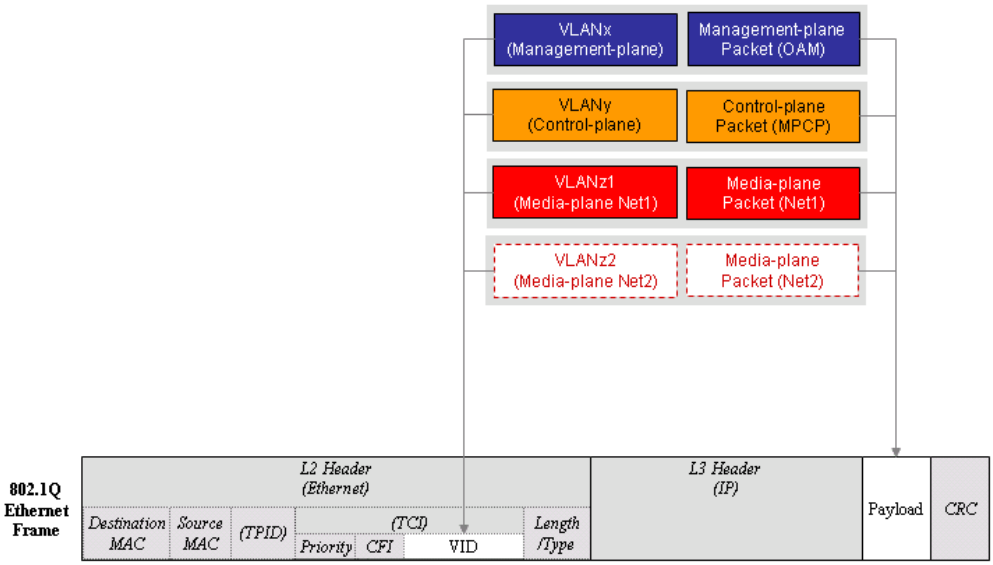
This feature provides new configuration parameters and procedures for enabling the BCP7200 to operate in IEEE 802.1Q VLAN-tagged Service Network topologies.

IEEE 802.1Q VLAN-tagged topology support is provided in addition to the previously supported untagged configuration – so the BCP7200 can now be configured for interconnect to either tagged or untagged Service Networks:

- When configured for untagged operation, the BCP7200 conveys its service packets (packets traversing each of the Service-planes: Management-plane, Control-plane, and Media-plane) in standard Ethernet frames that travel in a multi-netted flow from/to the Service Network.



- When configured for tagged operation, the BCP7200 conveys its service packets in 802.1Q Ethernet frames that are logically partitioned into separate network spaces by placing the associated VID configuration information into the VLAN Identifier (VID) field in the L2 header. In such configurations it is possible to segregate service traffic into distinct logical network spaces dedicated to conveyance of specific traffic types (e.g. Management, Control, and Media – which can be further distinguished into a Net1 Media and Net2 Media address space). In addition to placing service packets into properly tagged frames, BCP7200 RTP Media Portal Service Instances are also able to “bridge” media packets from one network space (Net1 Media) to another (Net2 Media) – and vice-versa – as a consequence of the normal operation of Media-plane functionality that the Media Packet Engine provides.



170.12 Hardware Requirements or Dependencies

This feature only applies to the BCP7200 – which is an IBM BladeCenterT (BCT) hardware platform.

170.13 Software Requirements or Dependencies

The following software changes are not required by this feature, but will occur as part of the normal course of product development:

- Upgrade to JVM 1.4.2_09 (moves the RTP Media Portal Component software onto the version of the Java Virtual Machine used across other product components).
- Upgrade to ESM firmware (up-version to collect bug-fixes, and to gain access to enhancements in the Layer-2 Trunk Failover mechanism that provide configurable control over the failover-trigger).
- Upgrade to IBM BladeCenterT (BCT) subcomponent firmware (up-version to collect bug-fixes).

170.14 Limitations and restrictions

1. IEEE 802.1Q VLAN-tagging support is only provided for the BCP7200.
2. IEEE 802.1Q VLAN-tagging support is only provided for the service traffic on the BCP7200 – there is no tagging of the out-of-band platform management traffic traversing the Management Modules in the chassis.
3. Since VLAN-tagging fundamentally changes the format of frames transmitted on a tagged port, carefully planned network designs are needed to prevent tagged frames from being transmitted to devices that do not support IEEE 802.1Q VLAN tags, or devices where tagging is not enabled.

4. The BCP7200 does not support live update of configuration changes, so configuration data does not get picked up in run-time until the BCP7200 is cycled (e.g. Stop+Start, Kill+Start, or Restart).
5. Configuration parameter default values (i.e. “<none>”) target operation in untagged topologies.
6. There are also restrictions and limitations as to the ESM’s functions and capabilities with respect to support of IEEE 802.1Q VLAN-tagging. Some of these are listed below, but please refer to most recent ESM documentation for most accurate listing:
    - The ESM can support a maximum of 128 VLANs at a time.
    - By default, the Alteon OS software is configured so that management ports are configured to the default VLAN 4095.
    - The ESM can support a maximum of three (3) separate Layer-2 Link Aggregation trunks. This will limit the number of physically partitioned configurations possible that support Layer-2 Fault Tolerance using Link Aggregation.
    - All ESM ports configured as members of a Layer-2 trunk must have the same VLAN configuration. Also,
        - all trunk member ports must be assigned to the same VLAN configuration before the trunk can be enabled.
        - changes to the VLAN settings of any trunk member cannot be applied until the VLAN settings of all trunk members have been similarly changed.

170.15 Interactions

Not Applicable.

170.16 Glossary

Term	Description
ACL	Access Control List
802.1Q	IEEE Standard for Virtual Local Area Networks
BCT	IBM BladeCenterT
CS2000	Communications Server 2000
CS2K	Communications Server 2000
CFI	Canonical Format Indicator
CRC	Cyclic Redundancy Code

ESM	Ethernet Switch Module. *(The official product name for this hardware subcomponent is "Nortel Networks Layer 2/3 Gigabit Ethernet Switch Module")*
eth0/eth1	Physical Ethernet Port designations
EXT1-6	External Alteon ESM ports connecting the internal BCT subcomponents to the service network(s)
FW	Firewall
Gbps	Gigabits per second
GbE	Gigabit Ethernet
GHz	GigaHerz (frequency: 10^{-9} seconds)
GPS	Global Product Support
GUI	Graphical User Interface
GWC	CS2K Gateway Controller
I&C	Installation and Commissioning
IBM	International Business Machines
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
INT1-8	Internal Alteon ESM ports connecting to the BCT Blade Servers
IO	Input / Output
IP	Internet Protocol
L2	Layer-2
L3	Layer-3
LAN	Local Area Network
MAC	Media Access Control
MB	Megabytes
Mbps	Megabits per second
MCP	Multimedia Communications Platform
MCP09	Technology stream for MCP
MCS	Multimedia Communications Server (solution built on MCP technology)
MGCP	Media Gateway Control Protocol
Mgmt	Management
MGT1-2	Internal Alteon ESM ports connecting to the BCT Management Modules
MHz	MegaHerz (frequency: 10^{-6} seconds)

MPCP	Media Proxy Control Protocol (for control of RTP Media Portal)
MP	Media Portal
ms	Milliseconds
N	Representation of the number of active service instances in a fault tolerant configuration
N+1	Representation of all service instances (all active, and the one standby) in a fault tolerant configuration
N1-media	Net1 Media
N2-media	Net2 Media
NAT	Network Address Translation
NAPT	Network Address and/or Port Translation
NE	Network Element
NIC	Network Interface Card
OAM	Operations, Administration, Maintenance
OAM&P	Operations, Administration, Maintenance, & Provisioning
OM	Operational Measurement
PSTN	Public Switched Telephony Network
PVID	Port VID
RSIP	Restart In Progress (an MPCP message)
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
Sig	Signalling
SIP	Session Initiation Protocol
SMGUI	System Management Graphical User Interface
SN08/SN09	Software delivery streams for the CS2000/CS2K
TCI	Tag Control Identification
TPID	Tag Protocol Identifier
UDP	User Datagram Protocol
VID	VLAN Identifier
VLAN	Virtual Local Area Network

171: Functional Description (FN) A00012905

171.1 Feature name and Feature ID

Corrective CAF: A00012905: ERS8600 Alarm Mapping Correction in IEMS

171.2 Description

This feature corrects ERS8600 alarm mappings defined in IEMS system. No user interfaces will be changed in this corrective CAF.

From SN08, some ERS8600 traps have an incorrect mapping relationship with IEMS fault code. This causes unknown and misunderstanding alarms or events in IEMS system. Refer to the FM section of this feature for the content changes of some alarms and events.

This feature will be delivered in SN09-FF release. Refer to the FM section of this feature for more details.

171.3 Hardware Requirements or Dependencies

N/A

171.4 Software Requirements or Dependencies

This Feature requires the following applications:

- IEMS Application Server SN09-FF
- SN09 ERS 8600 V3.7.2.2

171.5 Limitations and restrictions

N/A

171.6 Interactions

There are no interactions between this feature and existing features.

171.7 Glossary

IEMS - Integrated Element Management System

ERS 8600 – Ethernet Routing Switch 8600

172: Functional Description (FN) A00012974

172.1 Feature name and Feature ID

Corrective CAF: A00012974: Correct Execdata mismatch between GWC EM and Core

172.2 Purpose

Prior to SESM SN07 there is a TRUNK250 GWC profile which exec data include “ABTRK DTCEX” and “PRAB UTR250”. From SN07 the TRUNK250 profile is being changed to TRUNKNA, and “ABTRK DTCEX” becomes “ABTRK GWCEX”. Also, a valid TRUNKNA GWC has 3 pairs of exec data. That is, “AB250 GWC250” is added by A89007187. Therefore, when both SESM and Core upgrade from SN6.2 or below to SN7.0 or above, both sides need to change the TRUNK250 profile to TRUNKNA profile.

This feature provides customers a function to change the execdata of a GWC from the GWCEM GUI. If the execdata of a GWC is changed, then both the SESM database table and Core table will be updated.

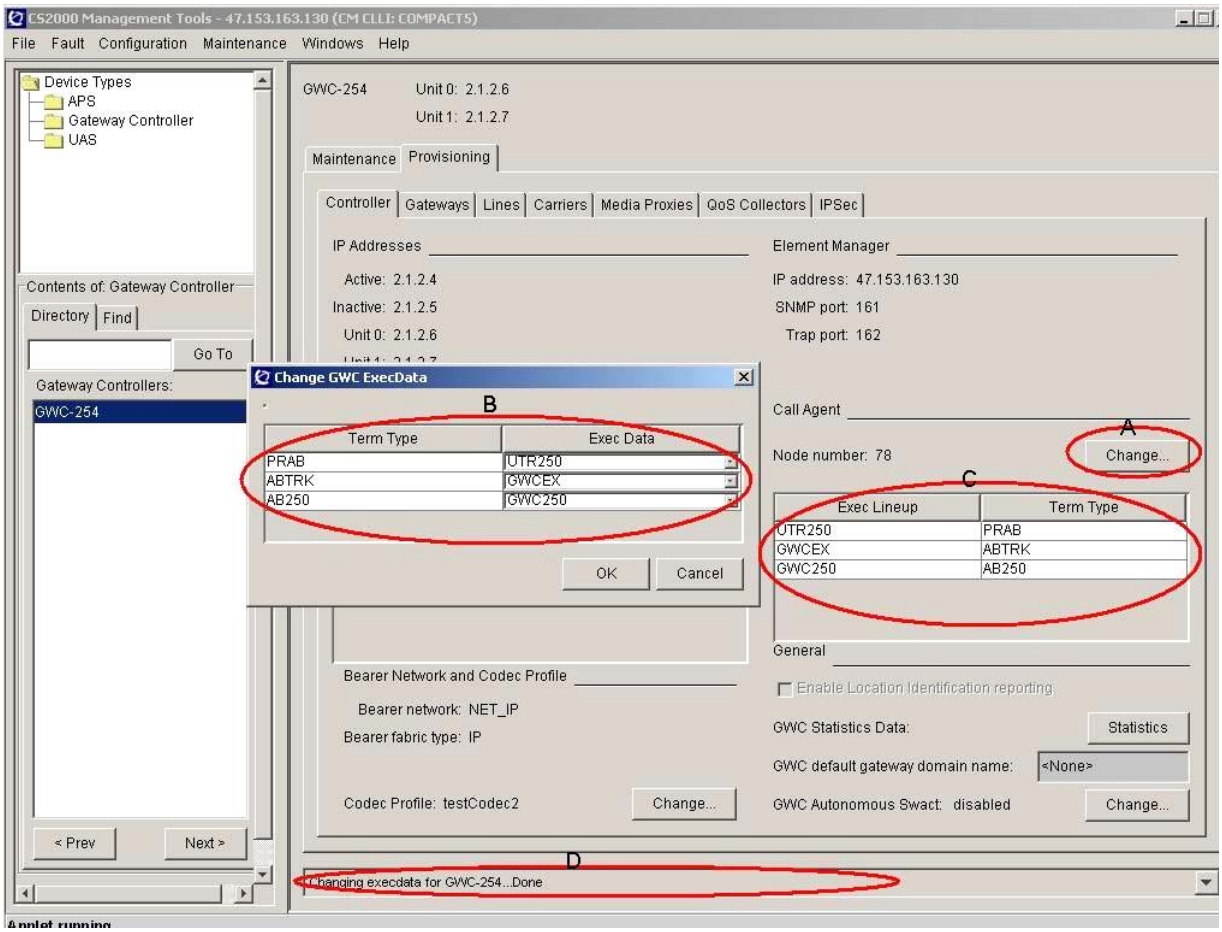
Since it is required for a GWC to have static data reloaded after a change of the exec data, a MN alarm will be generated to the IEMS for each GWC unit of a GWC pair until new static data is sent by locking and unlocking the cards.

172.3 Problem symptoms

Previously customers could choose execdata of a GWC profile for a GWC only when adding a new GWC. If the GWC has already been added into SESM the only way to change the GWC execdata is to delete the GWC and add it again. This is extremely service impacting.

This feature will introduce a new function which let customers change execdata of an existing GWC through the SESM GUI. After successful changing only a GWC, BSY/RTS operations are needed to make the new configuration valid on the GWC pair. Thus it is not necessary to delete and add a GWC in order to change the GWC execdata.

For example: Areas in red circles in the figure that follows show modification of this feature on the GUI.

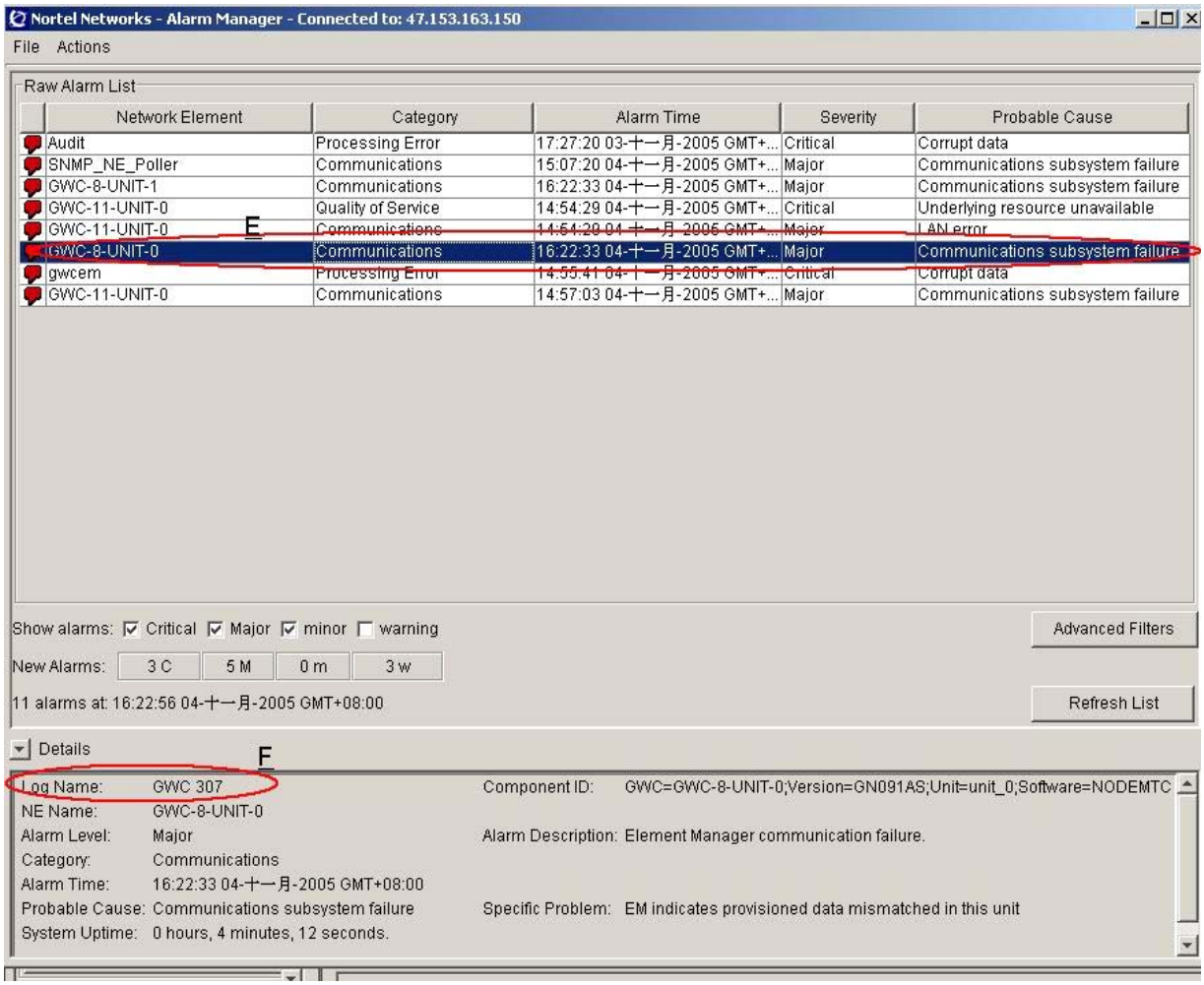


A: Add a “Change…” button

B: Pop up a new dialogue when clicking the A button

C: The fields will be refreshed after successfully changing the ExecData

D: Messages will be prompted in the status bar during the operation



E: Alarm is raised after successful change of EXECDATA

F: The Alarm type is GWC 307, which means communication with the CS 2000 GWC Manager need to be restored. This alarm can be cleared by BSY/ RTS of GWC unit.

172.4 Related documentation

N/A

173: Functional Description (FN) A00013063

173.1 Feature name and Feature ID

A00013063: PacketCable Multimedia for MCS and Carrier

173.2 Description

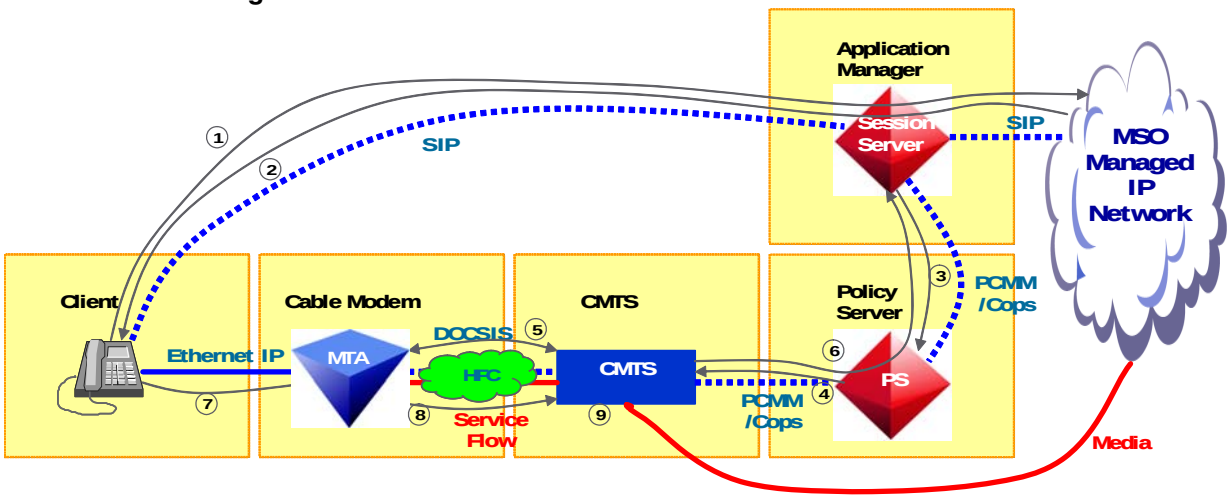
173.2.1 Functional Overview

PacketCable Multimedia is an architecture developed by CableLabs to enable MultiService Operating Companies to deliver Quality of Service enabled multimedia services over DOCSIS networks. PacketCable Multimedia extends the Dynamic Quality of Service architecture developed as part of PacketCable 1.X to allow Application Managers in the MSO network to request and obtain Quality of Service treatment for multimedia traffic flows on behalf of an end user.

The PCMM signaling implementation is compliant with PacketCable specification PKT-SP-MM-I02-040930.

The following diagram illustrates a high level call flow for a PacketCable Multimedia (PCMM) SIP call.

Figure 1 PCMM SIP Call Flow



1. SIP Client originates a session application (SIP Invite) to the Session Server and into the network to a destination client
2. The destination responds with an OK (200 OK) to the SIP Client through the Session Server
3. The application manager on the session server requests managed QoS on behalf of the SIP client by signaling to the policy server
4. The Policy Server makes policy decision and sends the request to the CMTS
5. The CMTS uses DOCSIS signaling to create service flow in the Cable Modem
6. The CMTS responds with a gate-id, which is passed via Policy Server to Session Server
7. The SIP Client sends data/media to the Cable Modem
8. Cable Modem puts data on the appropriate managed service flow to the CMTS based on classifier (e.g. IP address, port)
9. CMTS enforces policy for data on the service flow and network using the gate

Signaling
Media
High QoS Media

Activity A000011740 provided the PacketCable Multimedia (PCMM) service for the CS2K and can be referred to for the provisioning and activation of PCMM. This activity enables the use of PCMM in an MCS5200 environment. It also provides the following enhancements which apply to both the MCS and CS2K implementations except where otherwise noted:

Emergency Support - Raises the priority of the PCMM messages when a SIP call is made to an emergency number. Not supported for CS2K configuration.

Video Codec Flowspec Mapping - Allows the setting of the RSVP values for video codecs in order to communicate the bandwidth requirements for an instance of a given video session from the AM to the PS and CMTS. Audio codecs always use the values defined in PacketCable PKT-SP-CODEC specification.

Failover Support For PCMM - If the active Session Manager fails and the standby Session Manager takes over, then stable PCMM service flows (gates) are retained.

173.2.2 Emergency Support

The priority contained in the PCMM Gate-Set message is raised to the highest level when a SIP call is made to an emergency number. The Policy Server and the CMTS may use the priority value to implement priority based admission and to defend the resulting flow from being preempted. Provisioning of emergency number is accomplished using the Provisioning Client's Emergency Number and Emergency Alias Lists.

173.2.3 Failover Support For PCMM

If the AM's active Session Manager fails, and the standby Session Manager takes over, then the newly active Session Manager can communicate with the Policy Server. Also, the newly active Session Manager has knowledge of all stable PCMM service flows (gates) so it can delete them when the session ends. A stable PCMM service flow is defined as a session that was answered and the AM has received acknowledgement from the Policy Server that the PCMM service flow request was successful.

173.2.4 Video Codec FlowSpec Mapping

The following sections describe how to configure the FlowSpec video codec values which will be delivered as part of this activity. Please refer to activity A000011740 to understand how to configure the Policy Server and assign the PCMM feature to subscribers. These steps must be taken first in order to make use of the FlowSpec data described in the following sections.

173.2.4.1 Configuring FlowSpec Data

FlowSpec RSVP values are used to determine how much bandwidth is provided for video calls. Audio codecs always use the values defined in PacketCable PKT-SP-CODEC specification.

The customer is allowed to adjust video quality through modifications of the FlowSpec RSVP values for a specific codec and frame rate. A customer may configure up to 32 codec name / frame rate combinations.

Configuration of these codec values is system wide and will be used in determining video bandwidth for PCMM calls. The subscribers service package must have the Video option selected before an attempt to use the video codec FlowSpec data described in this section is made.

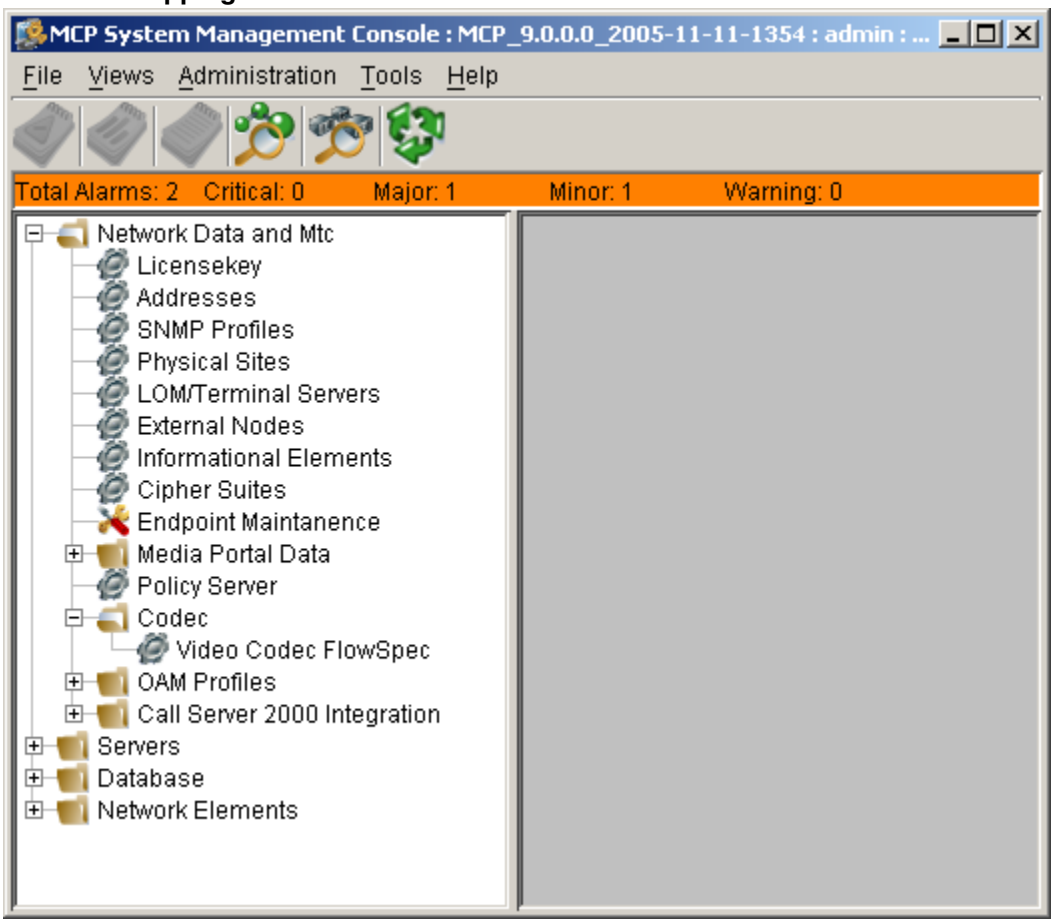
If a video codec is supplied by a SIP client during call setup and it has not been configured as part of PCMM Codec configuration, then the call will receive Best Effort service (no PCMM Service Flow) and will not render the best video quality.

Two supported video codecs are pre-provisioned in the system and they contain default FlowSpec RSVP values as follows:

Frame Rate	**Bucket Rate**	**Bucket Size**	**Peak**	**Min**	**Max**	**Rate**	**Slack**
10	30000	3000	30000	50	3000	30000	800

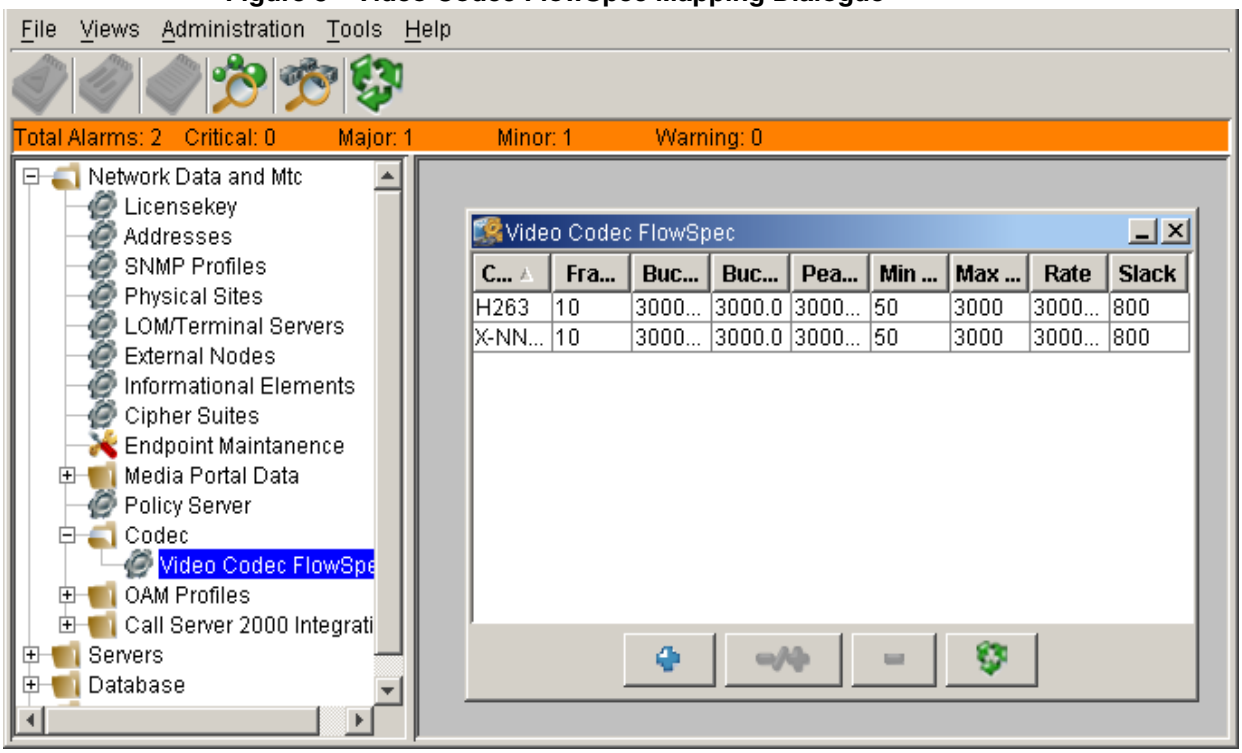
To configure the vide codec FlowSpec mappings from the MCP System Management Console expand the “Network Data and Mtc” folder and expand the “Codec” folder:

Figure 2 MCP System Management Console for Video Codec FlowSpec Mapping



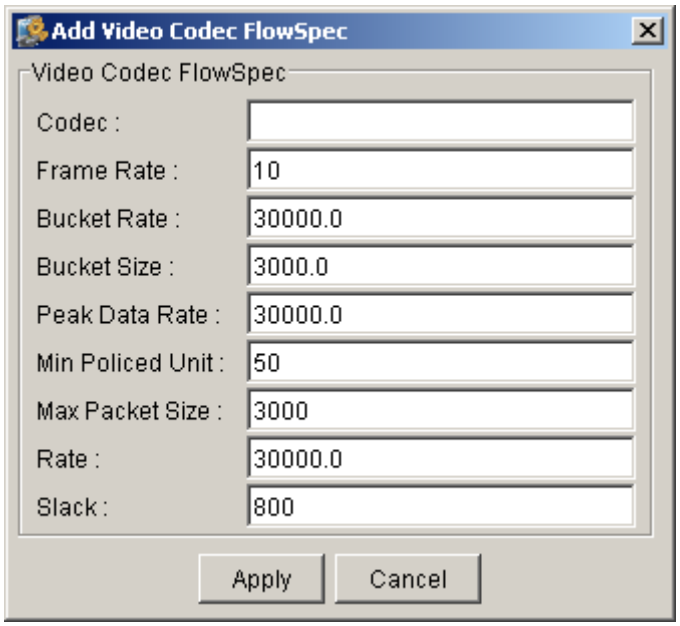
- Select the “Video Codec FlowSpec Mapping” item and the following screen appears:

Figure 3 Video Codec FlowSpec Mapping Dialogue



- Select the '+' icon and a new window appears. Enter the following fields:

Figure 4 Add Video Codec



a. **Codec**: Customer defined codec name up to 16 characters

b. Frame Rate: Video frame rate. The default is 10

c. **Bucket Rate:** Token bucket rate that the traffic conforms to in bytes per second**.** The default is 30000

d. **Bucket Size**: Size of each token in bytes. The default is 3000

e. Peak: Peak rate at which the source will send in bytes per second. The default is 30000

f. Min Unit: Minimum policed unit, usually the smallest packet size that the source will generate, in bytes. The default is 50

g. Max Units: Maximum packet size generated by the source in bytes. The default is 3000

h. Reserved Rate: Reserved rate in bytes per second. The default is 30000

i. Slack: Slack term in microseconds. The default is 800

Once these fields are entered, click “Apply” and the video codec will be configured.

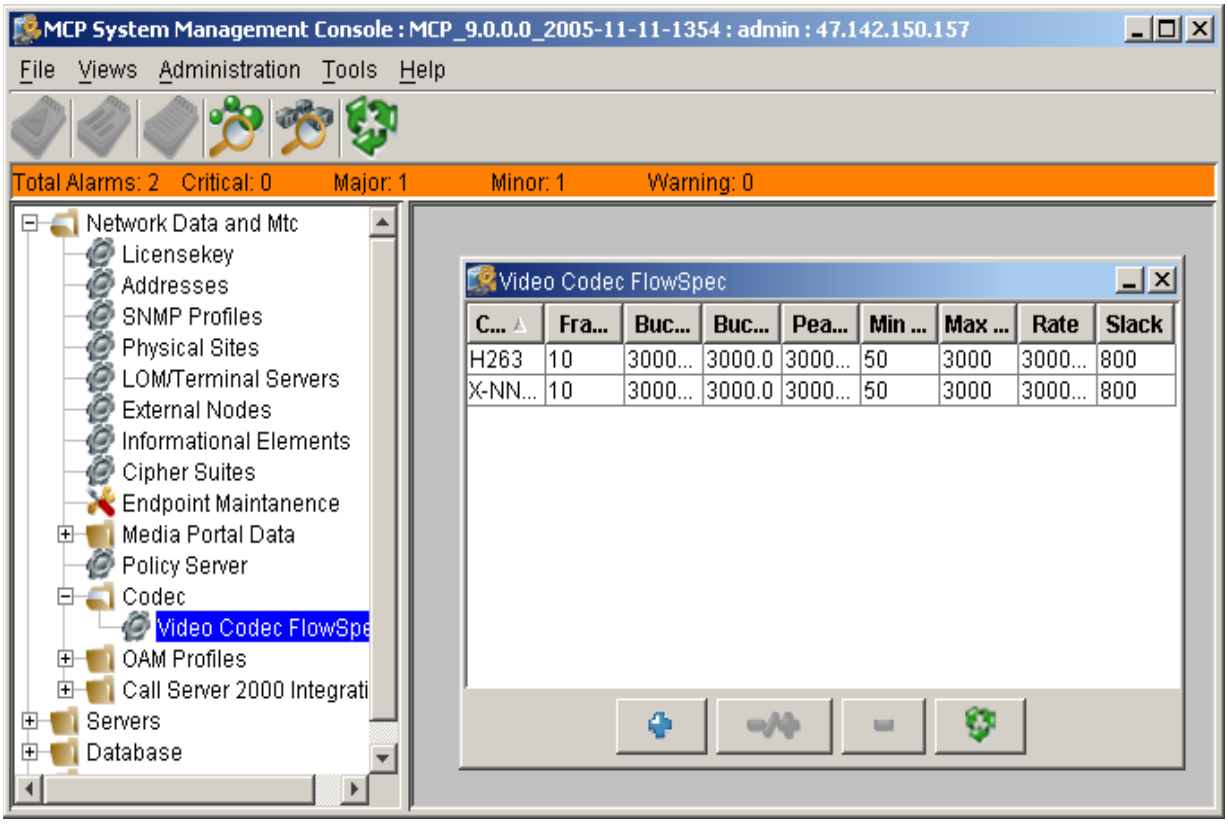
173.2.4.2 Deleting a PCMM Codec

A video codec maybe deleted using the MCS System Management Console.

In order to delete a PCMM codec entry:

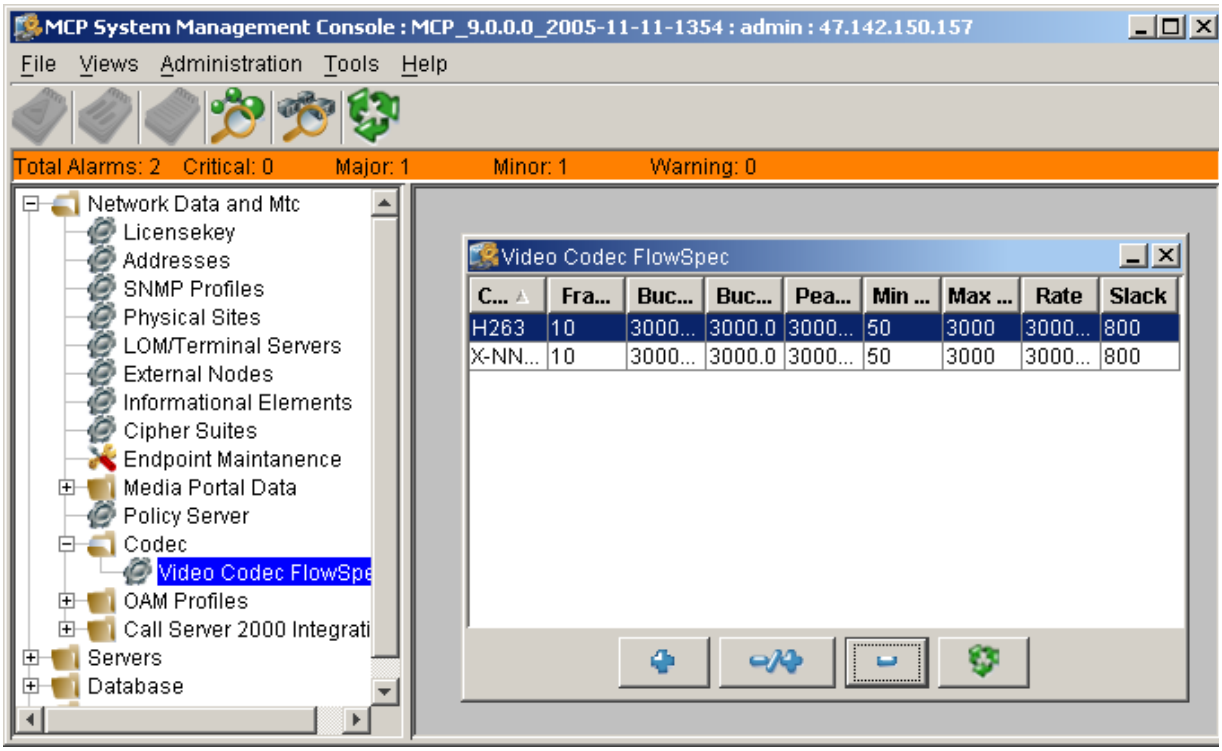
- Expand the “Network Data and Mtc” and “Codec” folders.

Figure 5 System Management for Video Codec FlowSpec Mapping



- Select the “Video Code FlowSpec Mapping” item and a new screen will appear as follows:

Figure 6 Video Codec FlowSpec Mapping Selected



- Highlight the PCMM codec to be deleted and click the “-” (minus) button
- A confirmation screen will appear- select ‘yes’ to delete, ‘no’ to cancel.

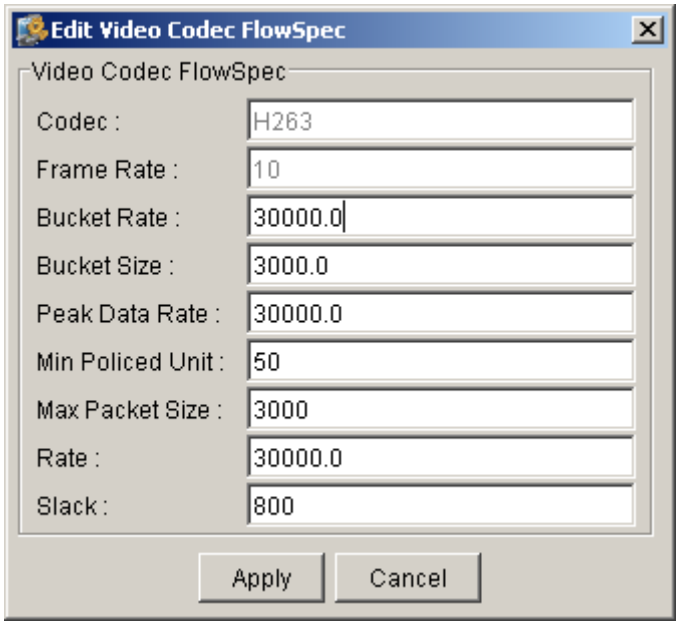
173.2.4.3 Modifying a PCMM Codec

A PCMM codec maybe modified using the MCS System Management Console.

Modifications of any field will take affect only on new calls which are established after the data is modified. Existing calls will retain their current video quality.-i.e video quality will not be renegotiated on active calls.

In order to modify a PCMM codec entry:

- Expand the “Network Data and Mtc” and “Codecs” items
- Select the “Video Code FlowSpec Mapping” item and the same screen as mentioned in the “Deleting a PCMM Codec” will appear.
- Highlight the PCMM codec to be modified and click the “+/-” button.
- The following screen will appear: Note that the codec name and framerate values cannot be modified. If a different codec/ framerate is desired you must add a new codec/framerate combination. All other fields can be modified.



- Modify any field which are allowed and depress apply. The new values will be modified stored.

173.3 Hardware Requirements or Dependencies

To deploy the PC-MM feature, the MSO needs to have PC-MM compliant cable network elements that are not supplied by Nortel. These third-party elements include cable modems, CMTSs, and a policy server.

173.4 Software Requirements or Dependencies

The policy server and CMTSs in the cable network must support PacketCable Multimedia specification PKT-SP-MM-I02-040930. The cable modems must support DOCSIS 1.1 or greater.

173.5 Limitations and restrictions

Failover for PCMM does not support the processing of unsolicited messages received from the Policy Server after the switch of activity. Therefore, the following scenario could occur:

1. A SIP session is answered and it has a PCMM service flow.
2. The active Session Manager fails and the standby Session Manager takes over.
3. Something happens on the network causing the CMTS to detect and report a loss of packets (through the Policy Server) to the Session Manager for the SIP session.

4. The call will lose it's PCMM service flow and resort to Best Effort quality of service.

173.6 Interactions

The PCMM feature sets up managed quality of service for SIP calls originating from or terminating to the cable network. PCMM operates on a half-call basis. This means that PCMM signaling and managed QoS happen only for the half of the call that is in the cable network. For example, an on-net to off-net call will only do PCMM signaling for the originating line half of the call. The trunk half of the call is not touched by PCMM.

173.6.1 Basic Call

The PCMM feature attempts to set up managed quality of service when the SDP information is known for both of the media endpoints (originating and terminating). Therefore, application of the PC-MM protocol procedures will not cause call failures, but it is possible that under some network error conditions a call might receive "best effort" QoS rather than managed QoS.

173.7 Glossary

Term	Definition
AM	Application Manager - logical network element defined in the PacketCable Multimedia architecture responsible for making bandwidth requests on behalf of a cable agnostic client.
Best effort	The default service flow. The characteristics for this service flow are defined in the cable modem config file. If a packet does not match any classifier then it is assigned to the best effort service flow.
CableLabs	A standards body that writes interface specifications and defines functional behavior for cable network elements.
Classifier	The set of parameters by which a media packet is judged to determine which service flow the packet belongs on.
Client	A SIP client
CM	Cable Modem - a cable network device that provides access to the cable network from an ethernet IP network.
CM	Call Manager - an MCS architecture component responsible for managing call-halves.
CMTS	Cable Modem Termination System - gateway between the cable HF/C network and the ethernet IP network. The CMTS receives the PCMM messages and communicates with the cable modem via DOCSIS to set up managed service flows.
COPS	Common Open Policy Service - a protocol defined in RFC 2748 that sets up a master/slave relationship between network elements for policy decisions. The PCMM protocol is an extension of COPS.
CS2M	CS2000 Management Tools - the CS2K GWC provisioning GUI

Term	Definition
DOCSIS	Data Over Cable System Interface Specification - the protocol used between cable modems and their CMTS to set up service flows and classifiers.
DIFFSERV	Differentiated Services - an IP packet marking scheme that allows IP packets to be treated differently in the network
DSCP	DIFFSERV Code Point - the bit pattern used for DIFFSERV
GETS	Government Emergency Telephone Service - a telephony service that gives higher priority to some callers so that government services can function in the presence of extremely high call loads
HF/C	Hybrid-Fiber/Coax
KRS	Key Registration System
NAT	Network Address Translator - a device that translates between public network addresses and private network addresses.
PacketCable	A subdivision of CableLabs that focuses on standards for VoIP over cable and multimedia over cable.
PC	Personal Computer (in this case)
PCMM	PacketCable Multimedia - an architecture and protocol for managing cable network bandwidth on behalf of cable agnostic clients.
PDP	Policy Decision Point - the COPS network element responsible for formulating network policy. The AM is a PDP. The PS is a PEP w.r.t. the AM and a PDP w.r.t. the CMTS.
PEP	Policy Enforcement Point - the COPS network element responsible for enforcing policies created by the PDP. The CMTS is a PEP. The PS is a PEP w.r.t. the AM and a PDP w.r.t. the CMTS.
Policy	A policy in the context of PCMM defines the access to and level of managed QoS available to a PCMM subscriber.
PS	Policy Server - network element defined in the PacketCable Multimedia architecture responsible for receiving PCMM signaling from and AM and forwarding it to the correct CMTS.
QoS	Quality of Service - the set of network characteristics that determine how a media packet is treated
SA	IPSec or IKE Secure Association
Service Flow	A managed QoS pipeline through the cable HF/C network defined by the quality of service given to the packets that transit the service flow.
SIP	Session Initiation Protocol - a VoIP signaling protocol
Socket	The IP address and port number used to communicate over an IP network to a particular service.
SS-L	Session Server Lines - a name for the MCS application server when used with CS2000

Term	Definition
TOS	Type Of Service - a set of bits in the IP header that can be used to mark IP packets for different treatment in the network. Some of the TOS bits are used for DSCP.

174: Functional Description (FN) A00013457

174.1 Feature name and Feature ID

A00013457: Message Waiting Indication using SIP VM/UM based on RFC 3842

174.2 Description

This development supports both North American and International markets.

This development is the expansion of the SN09 actid A00007544. The actid A00007544 was not tested with a SIP based UM/VM system. Also, the SN09 development was limited to the direct networking between two CS2K using SIP network. This development addresses the following three main aspects:

- Session Initiation Protocol (SIP) based network message waiting service (NMS) support based on RFC 3842 interworking with tandem solutions.
- Testing of message waiting indication (MWI) and NMS with RFC 3842 compliant SIP based 3rd party VM/UM.
- Testing of the MWI and NMS with RFC 3842 compliant SIP based open source VM/UM system.

174.2.1 SIP NMS based on RFC 3842 interworking with tandem Solutions

There are a large number of customers who are deploying the VM/UM connection with the CS2K Core or equivalent class 5 switches in a network mode. In this case, the customers have to maintain only one VM for multiple customers served via different class 5 switches (including CS2K). The existing software in CS2K Core already provide this service using NMS based on GR-866-Core using the SS7 network for public purpose and the INTERWORK subsystem network for private purpose. Also, NMS based on GR-866 is widely used with NTNA PRI connections as well as H.323 connections to the enterprise based PBX (or equivalent).

The existing software limitations were such that the tandem solutions where, the SIP based VM/UM is connected to a CS2K via SIP network and line is connected to a remote node (class 5 switch, PBX, etc.) was not supported. This

design is removing this limitation and allow the interworking between traditional network (public or private) and SIP based network VM/UM.

This feature does not cover development needed in SIP clients, SIP compliant remote node and SIP compliant VM.

Based on the converged network needs and support for multiple interfaces, the following end user devices are supported:

- Traditional Phones (e.g POTS, RES, IBN, KSET etc.)
- CICM IP sets
- Traditional Lines off of a remote switch
- Traditional Lines off of a remote SIP domain
- Traditional Lines off of a PBX
- SIP lines served by CS2K.
- SIP Lines served by a remote CS2K.

Also, the following interfaces to a message server (Voicemail) system are supported:

- Traditional SMDI and UCD/HUNT group to VM.
- Traditional VM using public SS7 network for NMS (North American market only).
- Traditional VM using private NTNA PRI for NMS (North American market only).
- Traditional VM using Interwork subsystem for NMS (North American market only).
- Traditional VM using public ETSI ISUP network for NMS (INTL market only).
- Traditional VM using private ETSI PRI network for NMS (INTL market only).
- Traditional VM using SIP NMS based on RFC 3842.

- Commercial 3rd party RFC 3842 compliant SIP VM/UM network to CS2K.
- Open Source RFC 3842 compliant SIP VM/UM network to CS2K.
- Enterprise hosted 3rd party (e.g. IP Unity) RFC 3842 compliant SIP VM/UM network to CS2K.
- Tandem solution between two CS2K interconnecting via an INTERWORK subsystem networking with a SIP VM/UM connected to one CS2K (North American market only)
- Tandem solution between two CS2K interconnecting via NTNA PRI based networking with a SIP VM/UM connected to one CS2K (North American market only).
- Tandem solution between two CS2K interconnecting via SS7 based networking with a SIP VM/UM connected to one CS2K (North American market only).
- Tandem solution between a CS2K and a PBX interconnecting via an H.323 (MCDN) based networking with a SIP VM/UM connected to the CS2K (North American market only).
- Tandem solution between two CS2K interconnecting via ETSI ISUP based networking with a SIP VM/UM connected to one CS2K (INTL market only).
- Tandem solution between two CS2K interconnecting via ETSI PRI based networking with a SIP VM/UM connected to one CS2K (INTL market only).

The combination of above user devices and VM interfaces are supported with following interoperability limitation:

The design is generic and based on RFC 3842 standards, Nortel is unable to test every possible interoperability using different hardware and different vendor equipment. Therefore, Nortel can only be able to claim the support for the tested networks. In order to make other hardware and different vendor equipment supported, proper interoperability testing must be done in Nortel-approved interoperability lab. After the complete testing, appropriate support will be provided for them as per the relationship defined in Nortel's Developer Partner Program.

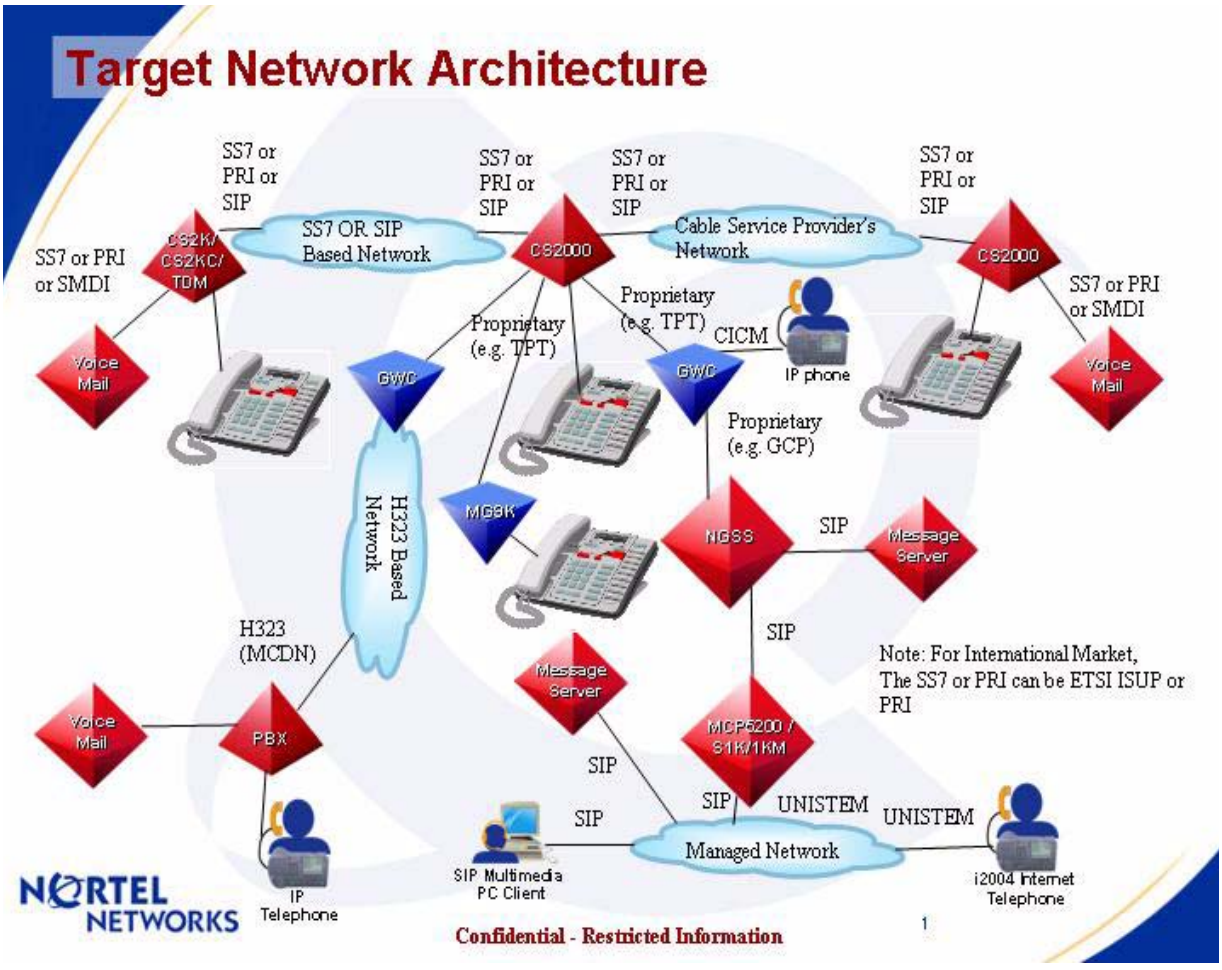
The DPNSS support for the INTL market has been developed by companion feature A00009409 and A00012847. Therefore, details for the DPNSS support please refer to A00009409 and A00012847.

The H.323 MCDN for INTL market is not covered by this actid.

174.2.2 Target Network Architecture

The feature develops a converge network architecture. In this architecture of the Message Waiting (MWT) service the VM or Message Server (MsgSrv) can reside in any network and the user device can reside in any network. The communication required for MWT service is supported by this architecture. The following figure (Figure 1) is a pictorial representation of the target architecture.

Figure 1 Target Architecture



With this development, MWT is provided across the different type of networks within a Service Provider’s network. The following are the advantages to the service provider:

- Support of MWI on end user device (i.e. terminals, phone etc.)
- Consolidation of the VM system in service provider's network
- Converged network support
- MWI to S1K/1KM and BCM

In above configuration, the Call Pilot is another type of traditional VM/UM system. The call pilot uses SMDI connectivity for VM connections.

For other topologies and how MWT service provided are described in See "Supported Configurations" on page 1803.

174.2.3 Supported Configurations

The connection and communication bases the supported configurations are separated in two categories: (1) Configurations of Voicemail or MsgSrv systems, and (2) Configurations of Lines or clients.

The configurations described here are specific to MWT service and VM communications for MWT service. These configurations assumes that the call related communications and signalling are provided prior to the MWT service and exists in the given configuration.

174.2.3.1 Configurations of Voicemail or MsgSrv Systems

The following configurations are separated by the protocol used for communication between CS2K and VM system:

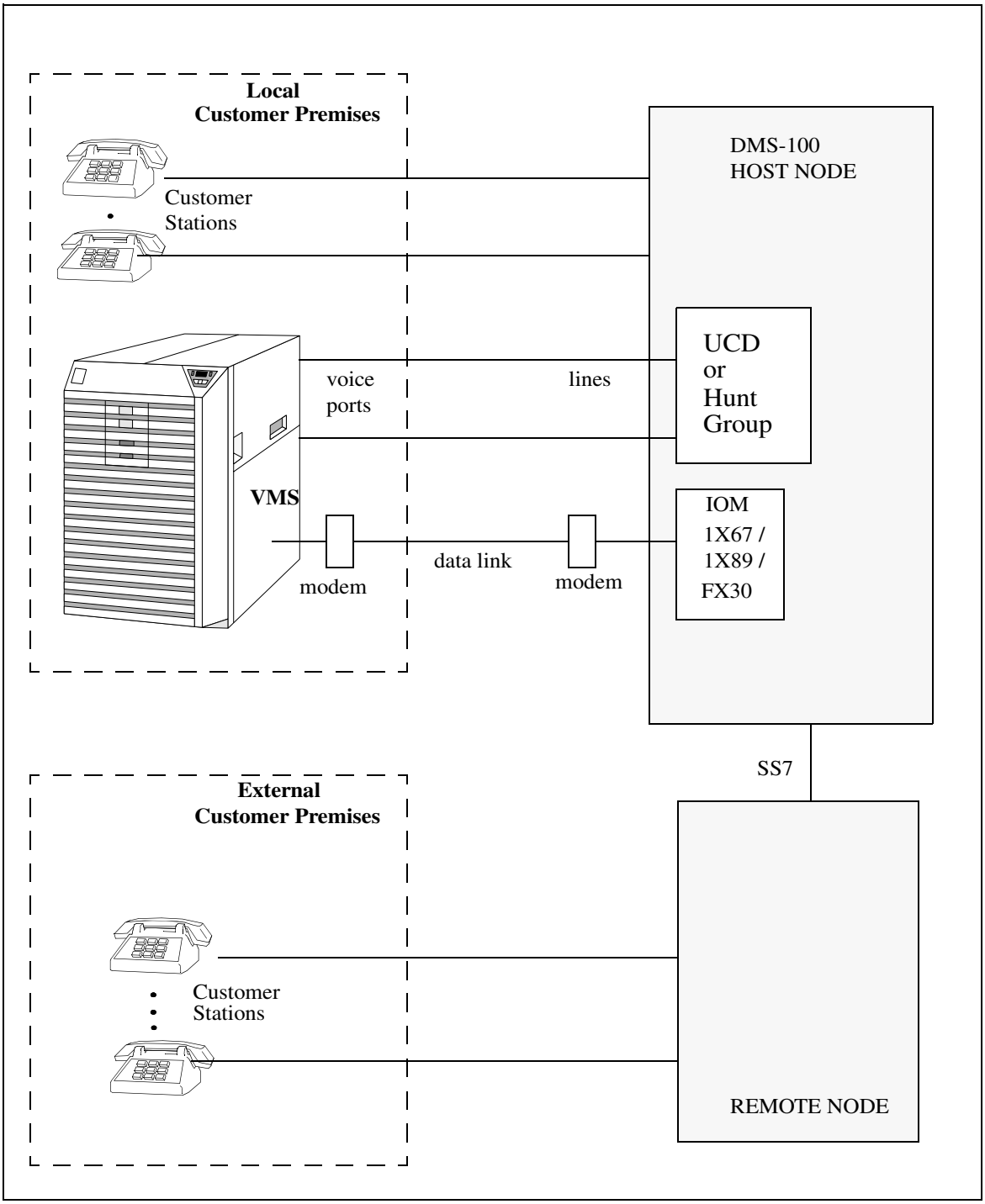
174.2.3.1.1 Traditional VM communication using UCD/HUNT group and SMDI link

This is an existing and supported configuration in CS2K/DMS. For details on this configuration, please look in the NTP 297-2051-104- SMDI Setup and Operation.

This configuration is applicable to both North American and INTL markets.

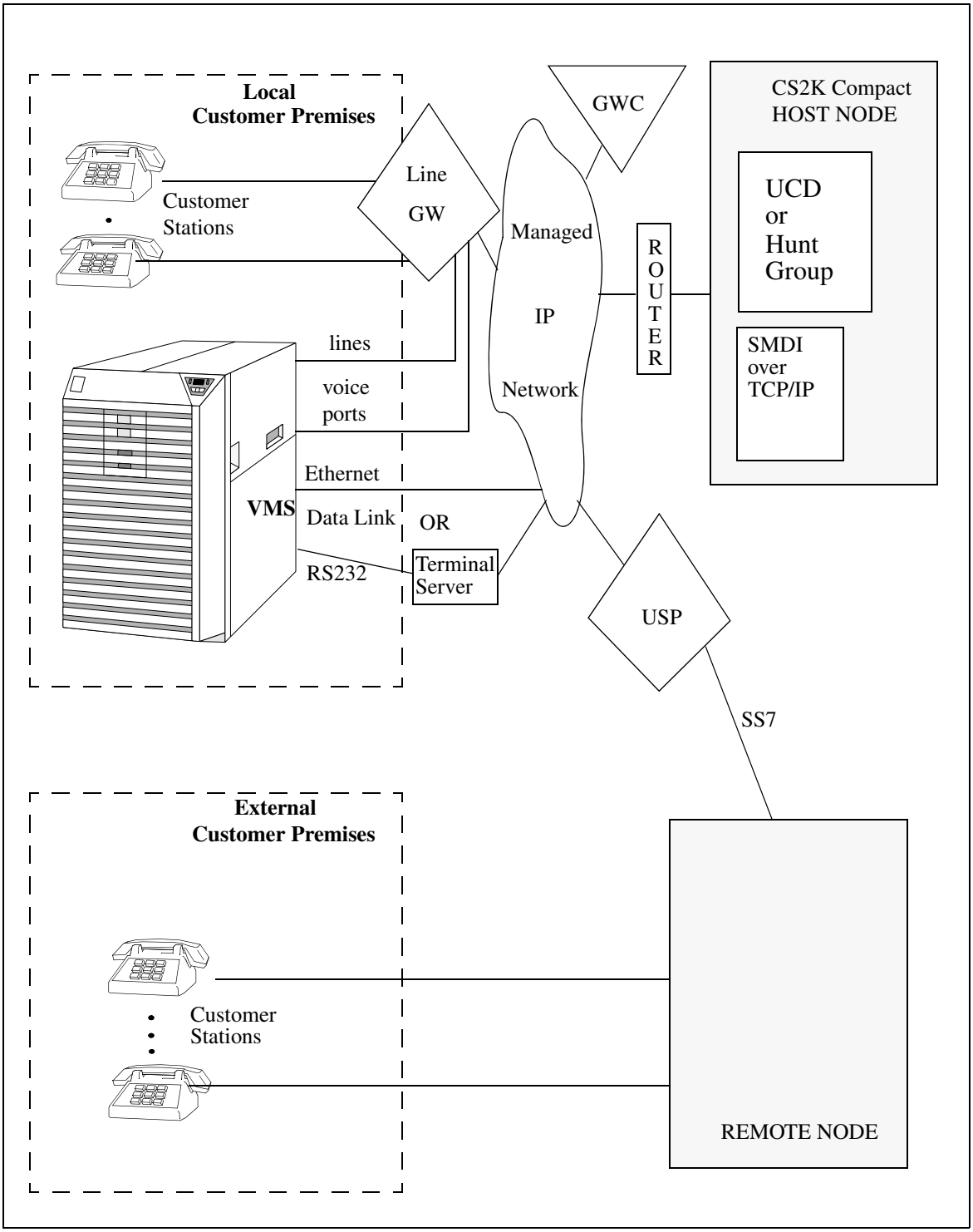
The following figure is a generic view of this configuration in DMS:

Figure 2 Simple VM Configuration in DMS



The data link in above Figure 2 is based on SMDI specifications described in the GR- 283- Core. The following figure provides a view of a simple VM configuration in the CS2K Compact:

Figure 3 Simple VM Configuration is CS2K Compact



In Figure 3 , the communication between the CS2K Compact and VM is SMDI based on GR- 283- Core. However, the transport medium is TCP/IP.

The details of this configuration can also be found in the NTP 297-2051-104 - SMDI Setup and Operation.

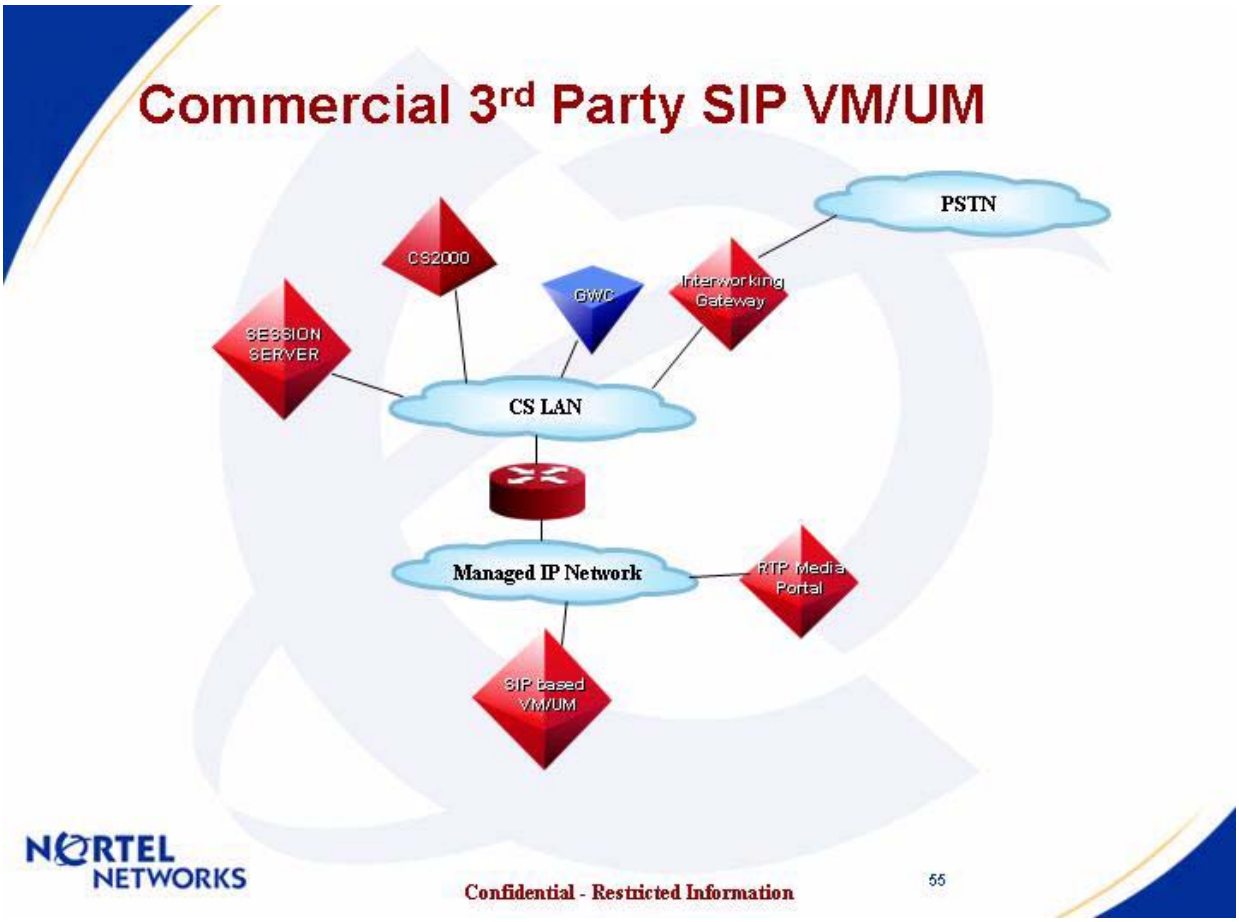
174.2.3.1.2 Network VM communication using the SS7 network

Figure 2 and Figure 3 also describe the configuration of the VM communication using the SS7 network between host node and remote node. For details, please see NTP 297-2051-104 - SMDI Setup and Operation; and NTP 297-8021-350v13 - North American Translation Guide Volume 13 of 25.

174.2.3.1.3 Commercial 3rd Party SIP UM/VM system communicating with CS2K

Figure 4 shows the configuration of the Commercial 3rd party SIP VM/UM communicating with CS2K. The commercial 3rd party SIP VM/UM can be provided by any commercial vendor. In this case, the SIP VM/UM system can reside on any location within the intranet of the customer. The SIP VM/UM system is logically connected to a Session Server. The communication between SIP VM/UM and Session Server is SIP messages defined in RFC 3261, RFC 3262, RFC 3263, RFC 3264, and RFC 3842. The RFC 3842 provides the MWI capability of SIP to the customer network.

Figure 4 Commercial 3rd Party SIP VM/UM system communicating with CS2K

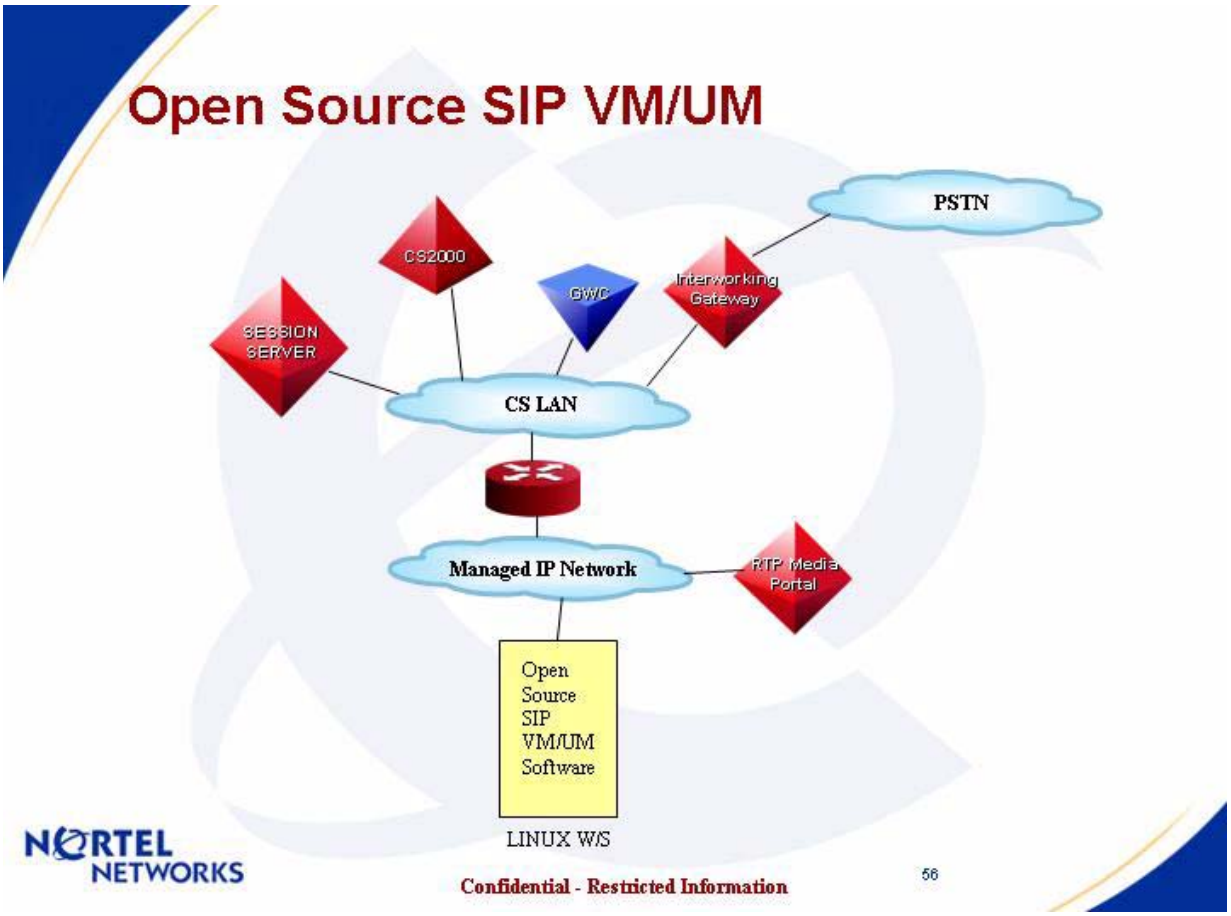


This configuration is applicable to both North American and INTL markets.

174.2.3.1.4 Open Source SIP VM/UM system with CS2K

Figure 5 shows the configuration of the Open Source SIP VM/UM communicating with CS2K. The Open Source SIP VM/UM is based on the open source software and independent from hardware or a specific 3rd party vendor. In this case the SIP VM/UM system can reside on any location within the intranet of the customer. The SIP VM/UM system is logically connected to a Session Server. The communication between SIP VM/UM and Session Server is SIP messages defined in RFC 3261, RFC 3262, RFC 3263, RFC 3264, and RFC 3842. The RFC 3842 provides the MWI capability of SIP to the customer network.

Figure 5 Open Source SIP VM/UM system communicating with CS2K

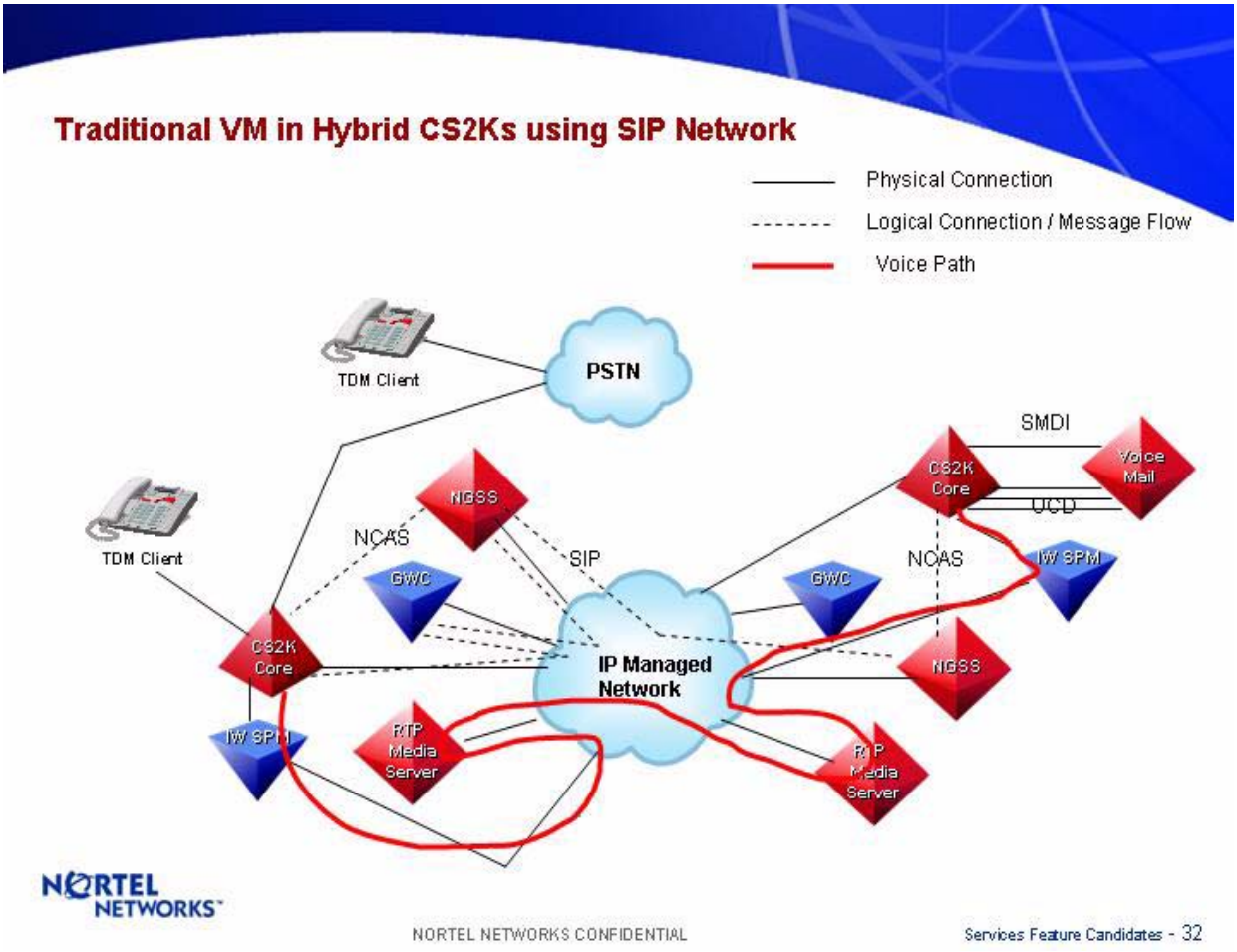


This configuration is applicable to both North American and INTL markets.

174.2.3.1.5 Traditional VM communication using SIP network

For this configuration, the VM is a traditional VM connected to one CS2K via SMDI and UCD/HUNT group. The line is on another CS2K. The RFC 3842 based SIP messages are used between two CS2K to pass MWI information for NMS.

Figure 6 Traditional VM communication using SIP network

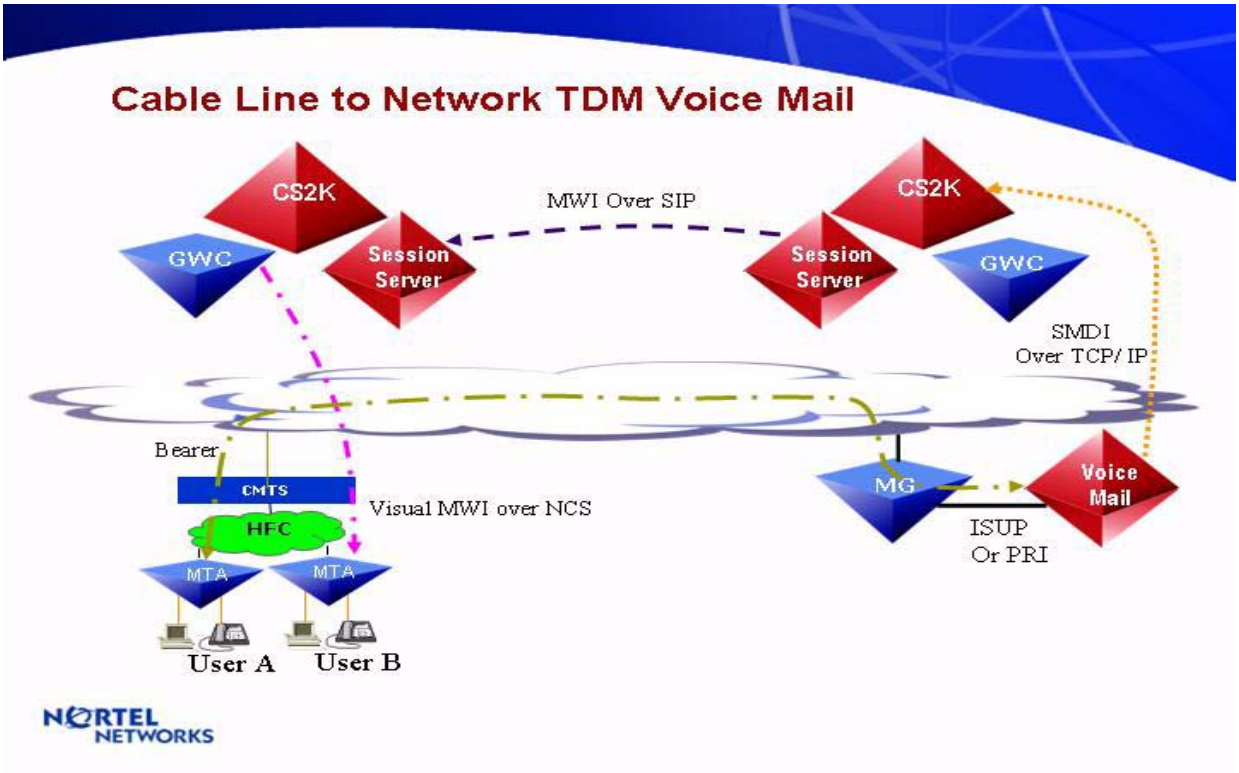


This configuration is applicable to both North American and INTL markets.

174.2.3.1.6 Network VM communication using SIP for Cable Service Providers

In cable service provider networks, the VM is connected to a CS2K compact as described in previous section 173.2.3.1.1 (Figure 3). As indicated in section 173.2.3.1.1, the communication between two CS2K Compact is based on the managed IP network using SIP signalling.

Figure 7 VM in Cable Network



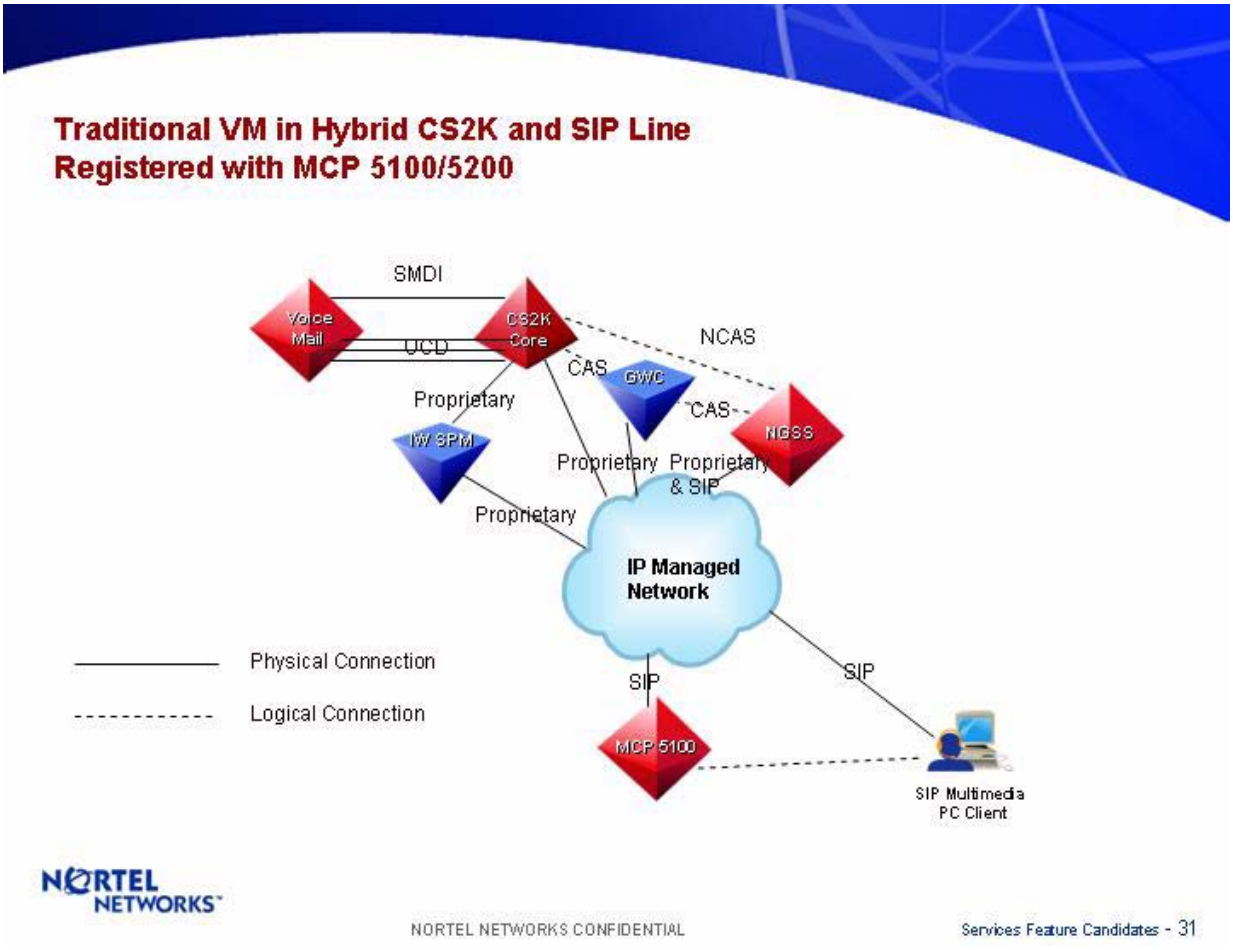
Note: The complete interoperability and compliance depends on the availability of the design lab. This configuration is quite similar to configuration describe by Figure 6 in section 173.2.3.1.5. The only major difference is the usage of MTA and conformance testing for cable lab specifications.

This configuration is applicable to both North American and INTL market.

174.2.3.1.7 VM support for MCP 5100/5200 Platform using SIP network

For this configuration, the VM is a traditional VM connected to one CS2K via SMDI and UCD/HUNT group. The SIP line is registered with the MCP 5100/ 5200 platform and the SIP line is served by the traditional VM. The CS2K is sending RFC 3842 defined SIP messages to MCP 5100/5200 platform to provide network based MWI service.

Figure 8 VM support for MCP 5100/5200 using SIP network



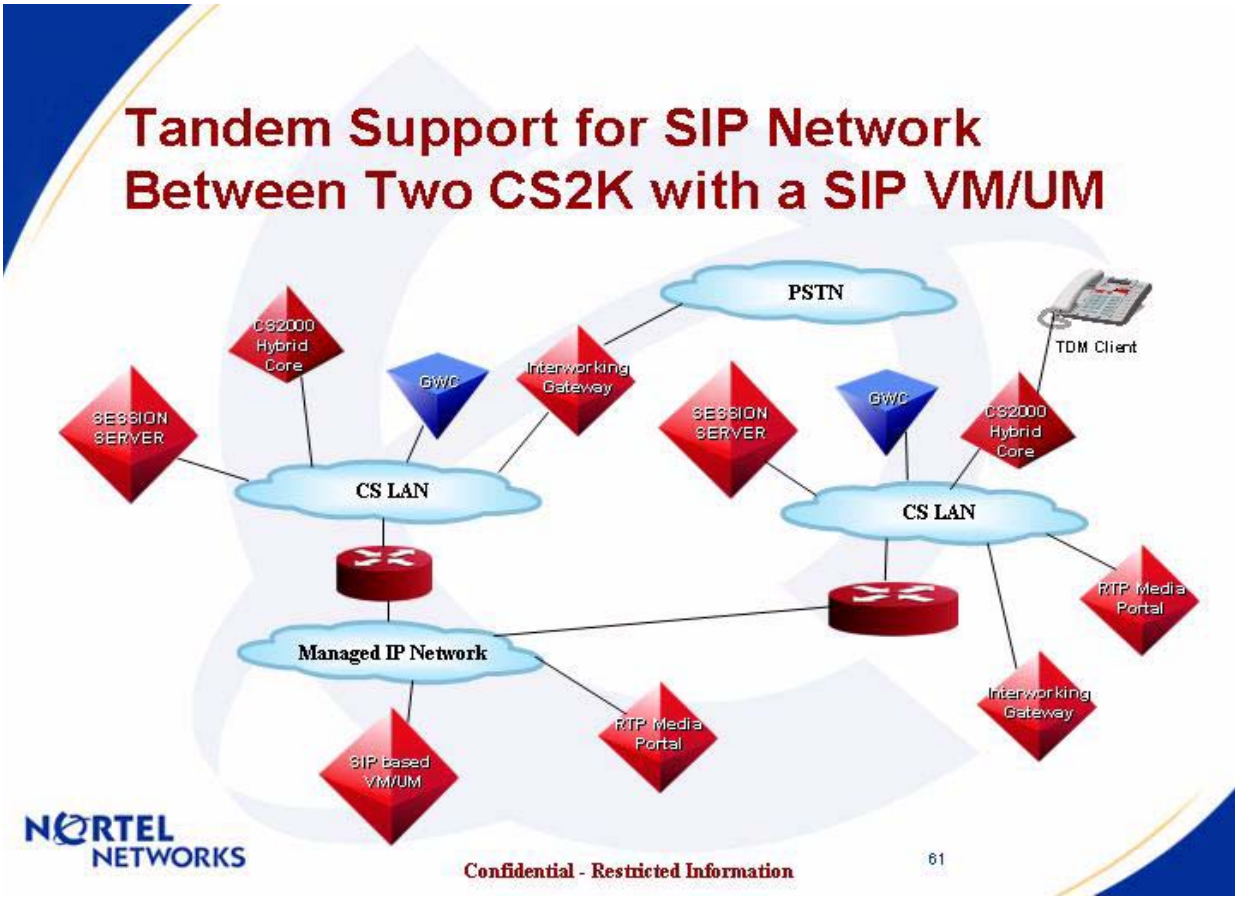
Note: In this configurations, the partial RFC 3842 supported. The CS2K send the NOTIFY messages to the remote MCP 5100/5200 only for the lines behind the MCP 5100/5200. This limitation attributes to the MCP 5100/5200 not forwarding the SUBSCRIBE message from the line to the CS2K.

This configuration is applicable to both North American and INTL market.

174.2.3.1.8 Tandem Support for Two CS2K via SIP Network and SIP VM/UM

In a hybrid network, the customer can have SIP network connections between a CS2K and remote CS2K using NGSS. With the support of the SIP VM/UM, which is network VM/UM to the one CS2K, the CS2K become a tandem switch for the NMS traffic between SIP VM/UM and lines connected to remote CS2K (See Figure 9).

Figure 9 tandem Support for SIP Network between two CS2K and SIP VM/UM

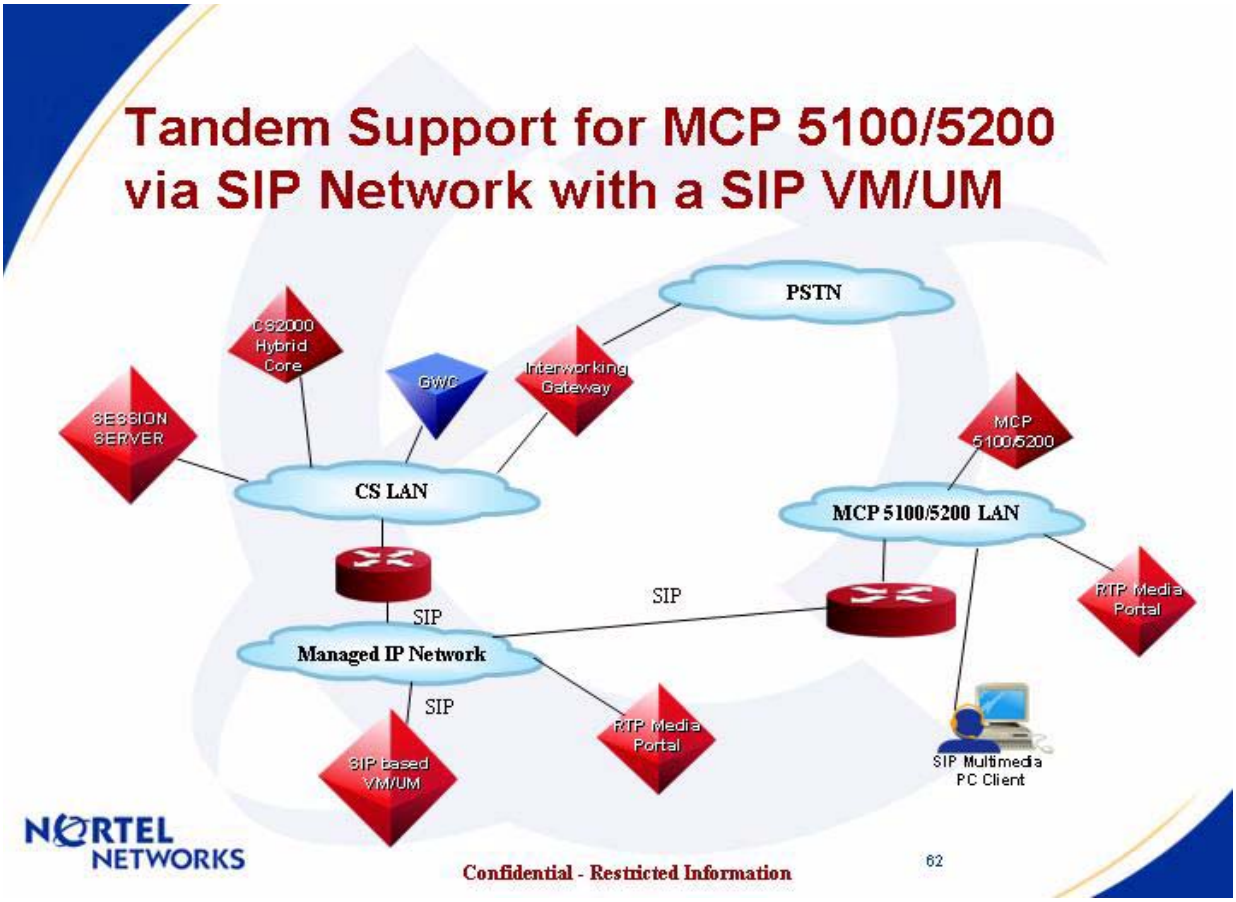


This configuration is applicable to both North American and INTL market.

174.2.3.1.9 Tandem Support for MCP 5100/5200 via SIP Network and SIP VM/UM

In a hybrid network, the customer can have SIP network connections between a CS2K and remote MCP 5100/5200 using NGSS. With the support of the SIP VM/UM, which is network VM/UM to the CS2K, the CS2K become a tandem switch for the NMS traffic between SIP VM/UM and lines connected to remote MCP 5100/5200 (See Figure 10).

Figure 10 tandem Support for MCP 5100/5200 via SIP Network and SIP VM/UM



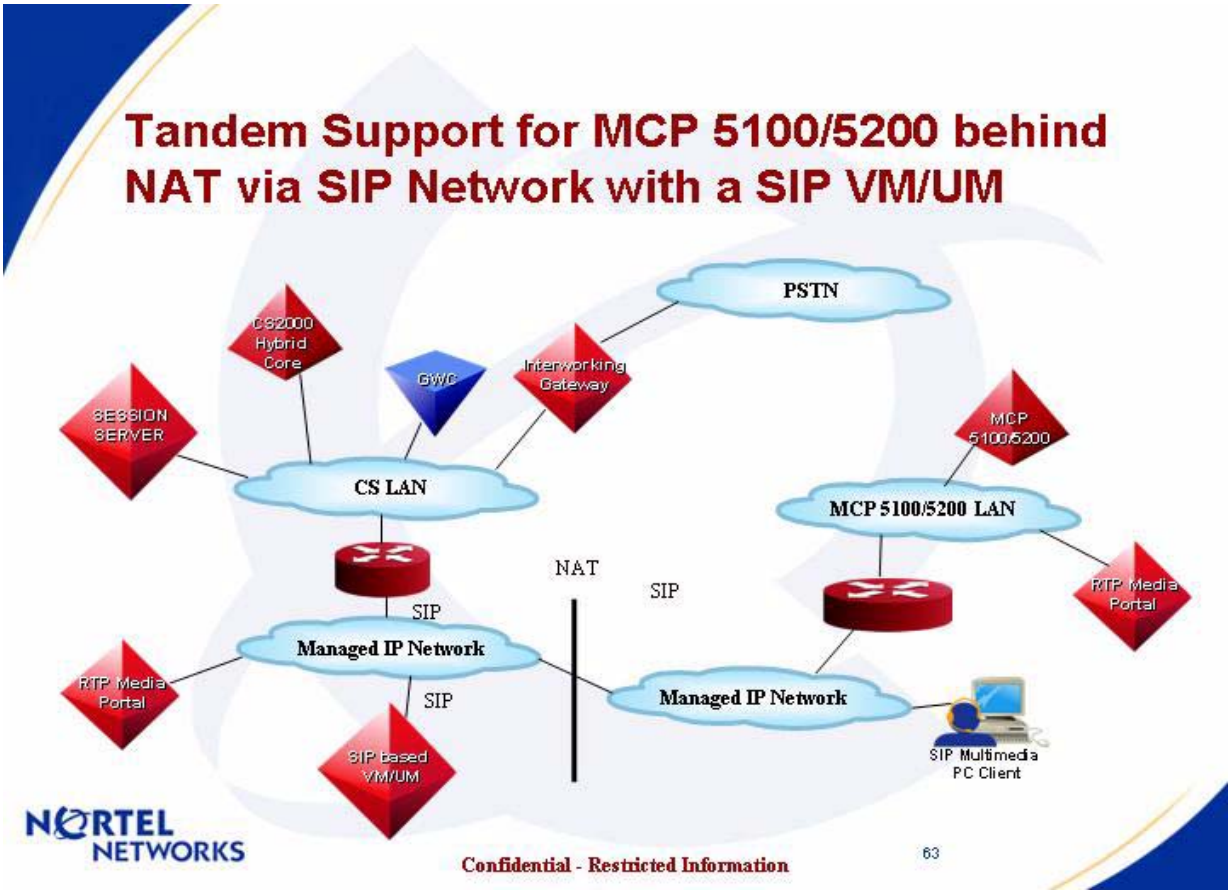
Note: In this configuration, the partial RFC 3842 supported. The CS2K send the NOTIFY messages to the remote MCP 5100/5200 only for the lines behind the MCP 5100/5200. This limitation attributes to the MCP 5100/5200 not forwarding the SUBSCRIBE message from the line to the CS2K.

This configuration is applicable to both North American and INTL market.

174.2.3.1.10 Tandem Support for a MCP 5100/5200 behind NAT and SIP VM/UM

In a hybrid network, the customer can have SIP network connections between a CS2K and remote MCP 5100/5200 behind a NAT using NGSS. With the support of the SIP VM/UM, which is network VM/UM to the CS2K, the CS2K become a tandem switch for the NMS traffic between SIP VM/UM and lines connected to remote MCP 5100/5200 behind a NAT (See Figure 11).

Figure 11 Tandem Support for MCP 5100/5200 behind NAT via SIP Network and SIP VM/UM



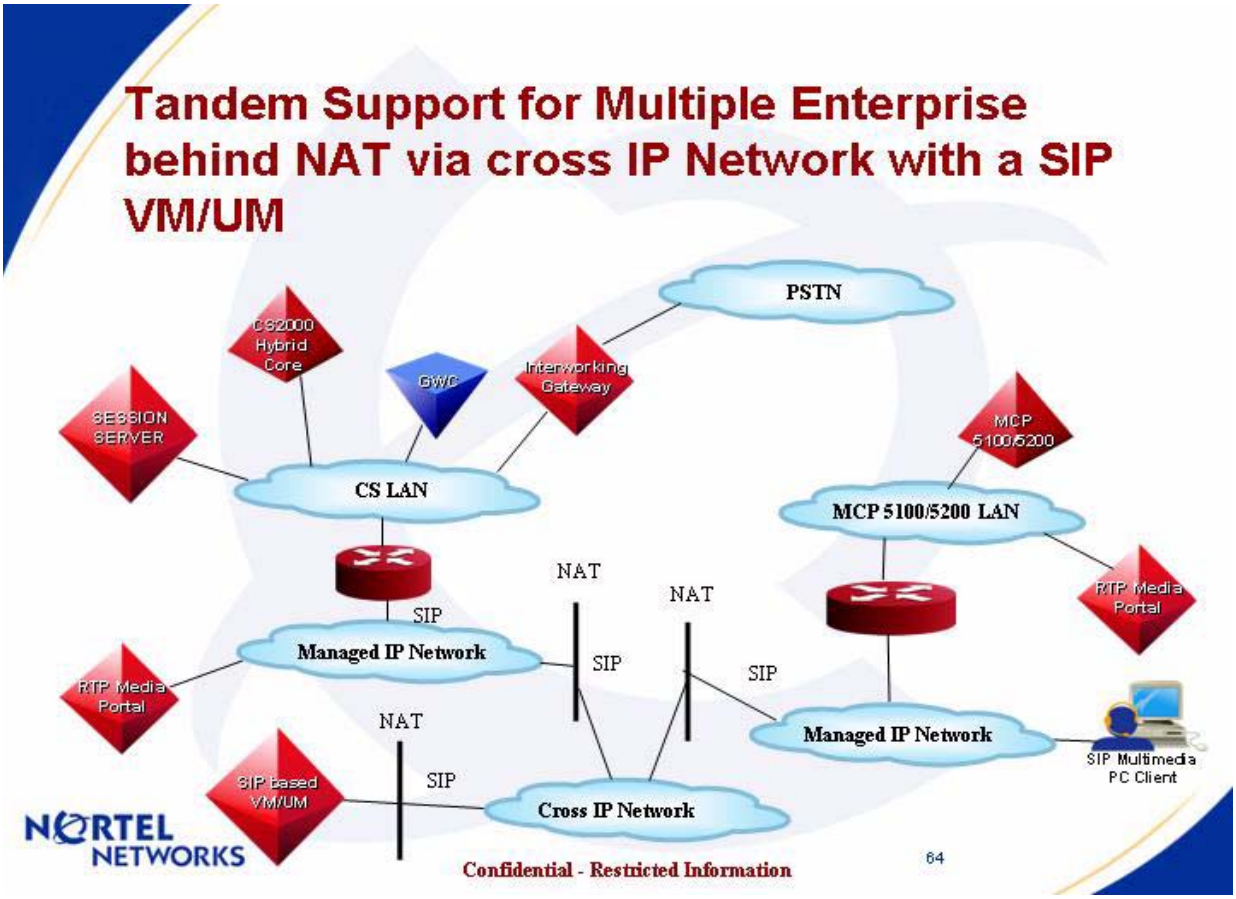
Note: In this configurations, the partial RFC 3842 supported. The CS2K send the NOTIFY messages to the remote MCP 5100/5200 only for the lines behind the MCP 5100/5200. This limitation attributes to the MCP 5100/5200 not forwarding the SUBSCRIBE message from the line to the CS2K.

This configuration is applicable to both North American and INTL market.

174.2.3.1.11 Tandem Support for Multiple Enterprise in cross IP Internet network and SIP VM/UM

In a hybrid network, the customer can have SIP network connections between one CS2K and remote CS2K behind a NAT using NGSS. With the support of the SIP VM/UM, which is network VM/UM to the CS2K behind a NAT, the CS2K become a tandem switch for the NMS traffic between SIP VM/UM behind NAT and lines connected to remote CS2K behind a NAT (cross IP Internet network) (See Figure 12).

Figure 12 Tandem Support for Multiple Enterprise in cross IP Internet network and SIP VM/UM

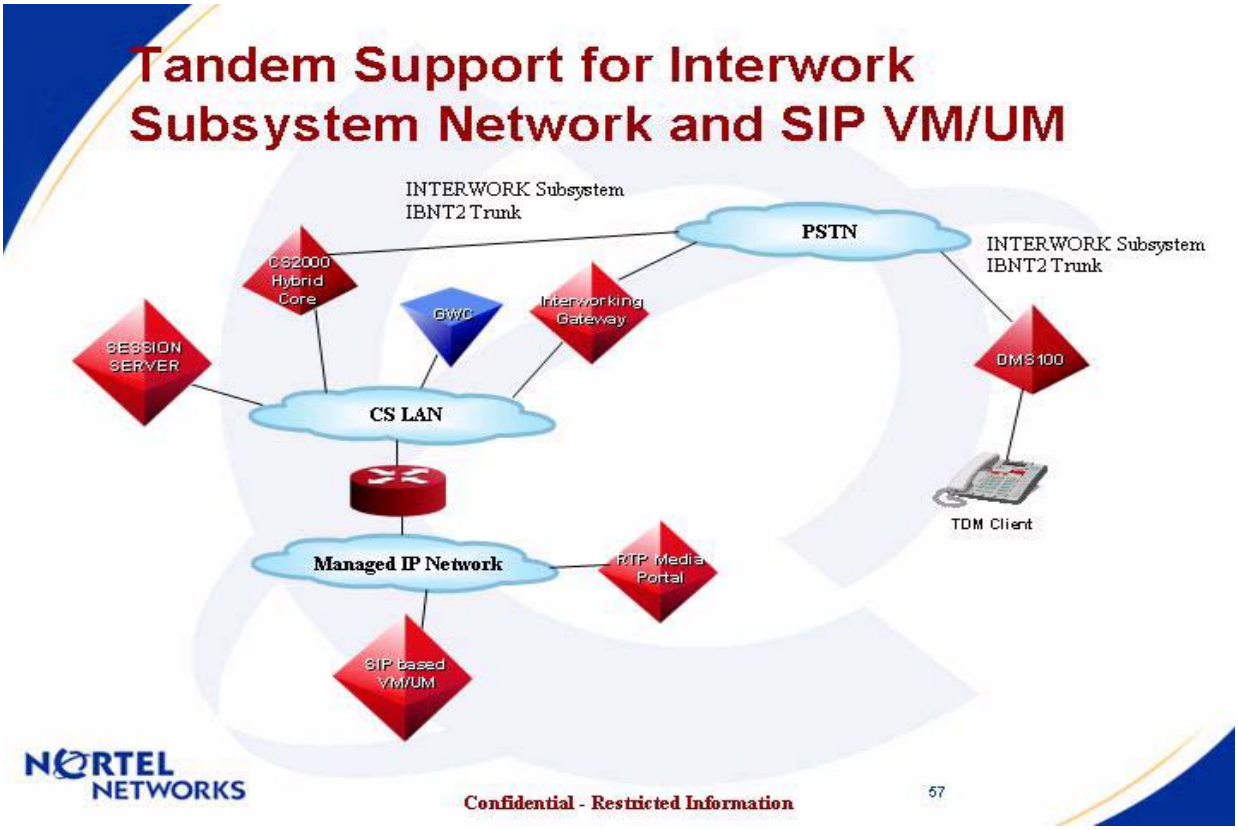


This configuration is applicable to both North American and INTL market.

174.2.3.1.12 tandem Support for INTERWORK Subsystem Network and SIP VM/UM

In a hybrid network, the customer can have private network connections between CS2K and DMS100/CS2K/CS2100 using INTERWORK subsystem based network. With the support of the SIP VM/UM, which is network VM/UM to the CS2K, the CS2K become a tandem switch for the NMS traffic between SIP VM/UM and lines connected to remote DMS100/CS2K/CS2100 (See Figure 13).

Figure 13 tandem Support for Interwork Subsystem Network and SIP VM/UM

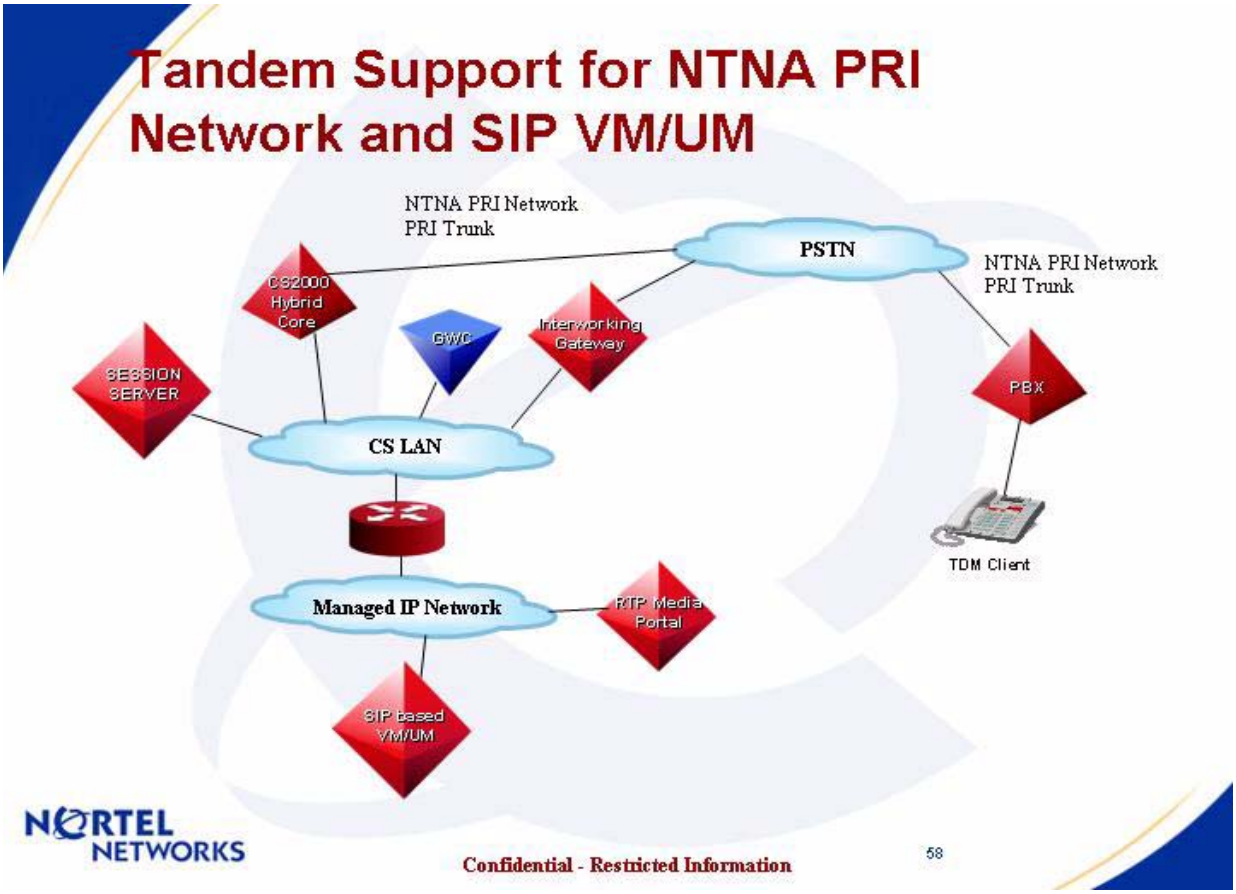


This configuration is only applicable to North American market.

174.2.3.1.13 tandem Support for NTNA PRI Network and SIP VM/UM

In a hybrid network, the customer can have private network connections between CS2K and MSL100/CS2100/CS1K/BCM/PBX using NTNA PRI based network. With the support of the SIP VM/UM, which is a network VM/UM connected to the CS2K, the CS2K become a tandem switch for the NMS traffic between SIP VM/UM and lines connected to remote PBX (See Figure 14).

Figure 14 tandem Support for NTNA PRI Network and SIP VM/UM

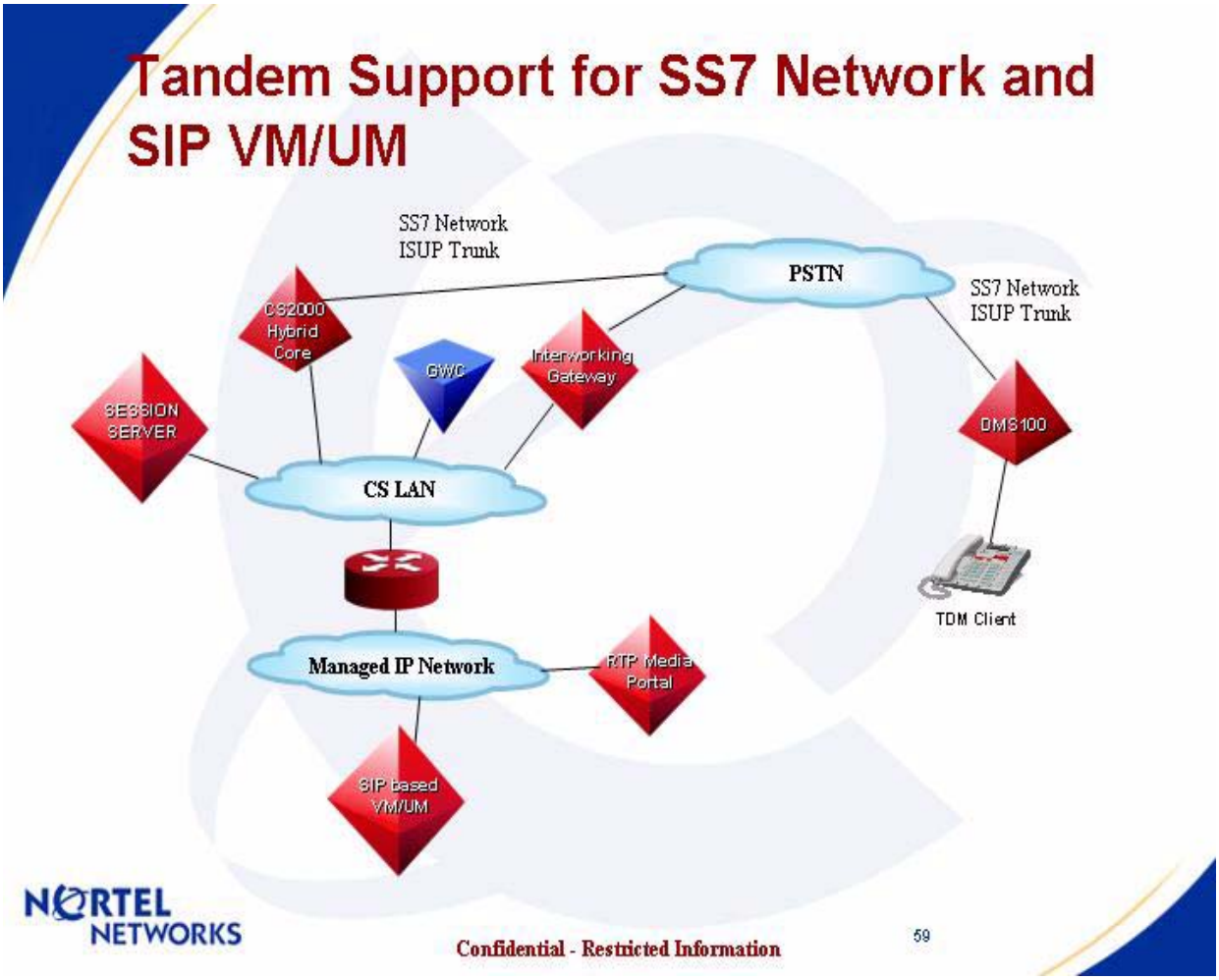


This configuration is only applicable to North American market.

174.2.3.1.14 tandem Support for SS7 Network and SIP VM/UM

In a hybrid network, the customer can have public network connections between CS2K and a remote class 5 switch interconnected via SS7 based networking. With the support of the SIP VM/UM, which is network VM/UM to the CS2K, the CS2K become a tandem switch for the NMS traffic between SIP VM/UM and lines connected to remote class 5 switch (See Figure 15).

Figure 15 tandem Support for SS7 Network and SIP VM/UM

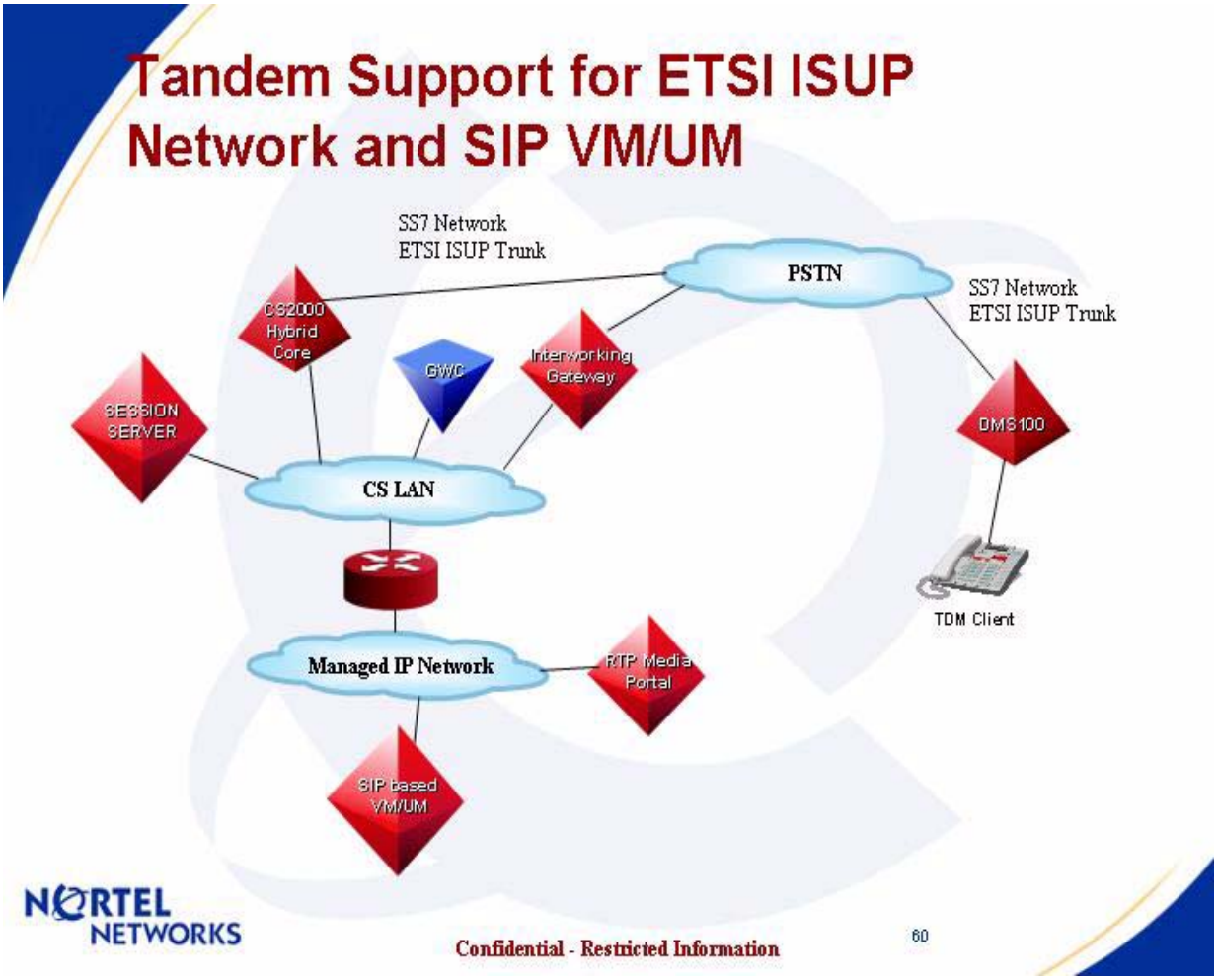


This configuration is only applicable to North American market.

174.2.3.1.15 tandem Support for ETSI ISUP Network and SIP VM/UM

In a hybrid network, the customer can have public network connections between CS2K and remote switch using ETSI ISUP based network. With the support of the SIP VM/UM, which is network VM/UM to the CS2K, the CS2K become a tandem switch for the NMS traffic between SIP VM/UM and lines connected to remote switch (See Figure 16).

Figure 16 tandem Support for ETSI ISUP Network and SIP VM/UM

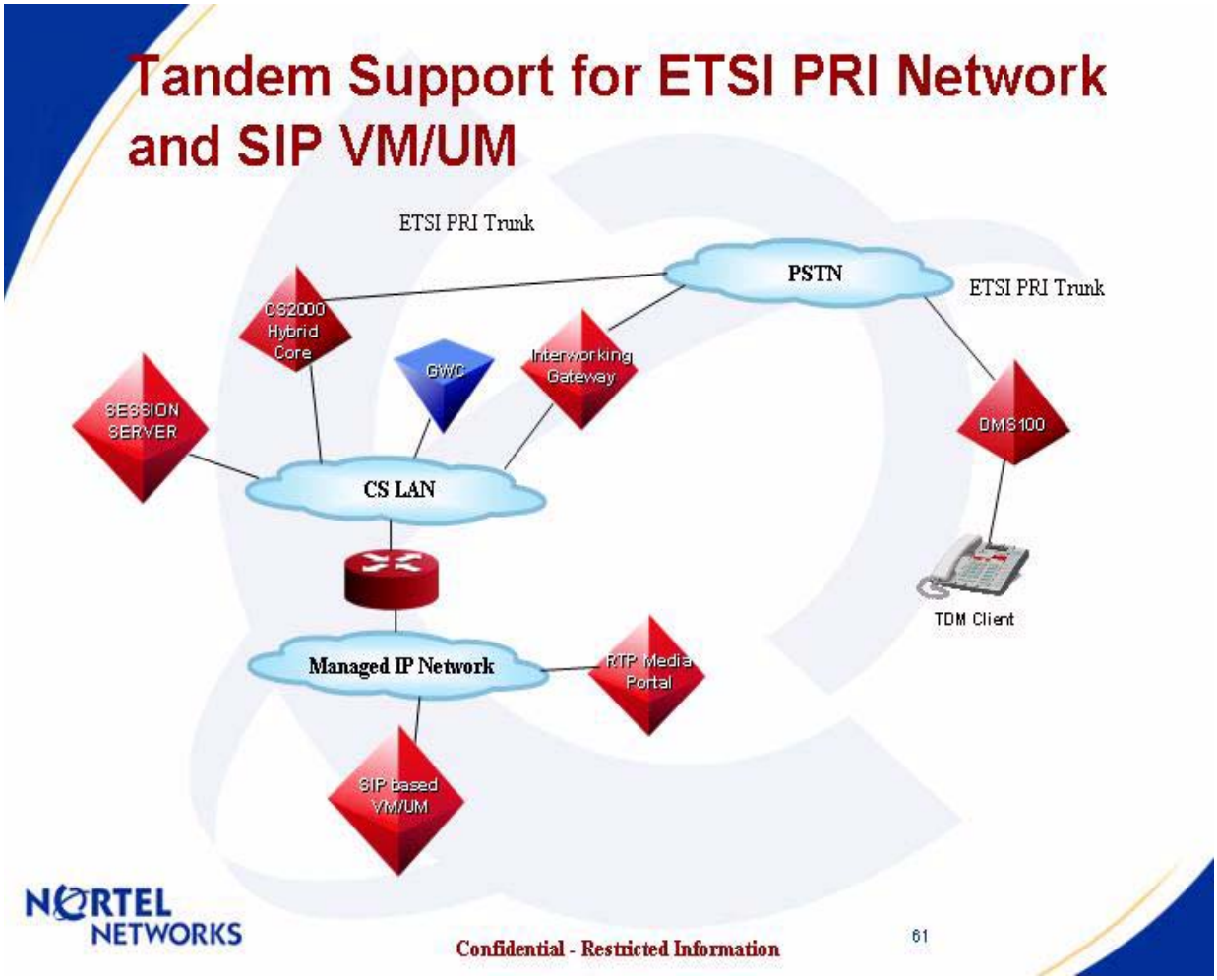


This configuration is only applicable to INTL market.

174.2.3.1.16 tandem Support for ETSI PRI Network and SIP VM/UM

In a hybrid network, the customer can have public network connections between CS2K and remote switch using ETSI PRI based network. With the support of the SIP VM/UM, which is network VM/UM to the CS2K, the CS2K become a tandem switch for the NMS traffic between SIP VM/UM and lines connected to remote switch (See Figure 17).

Figure 17 tandem Support for ETSI PRI Network and SIP VM/UM

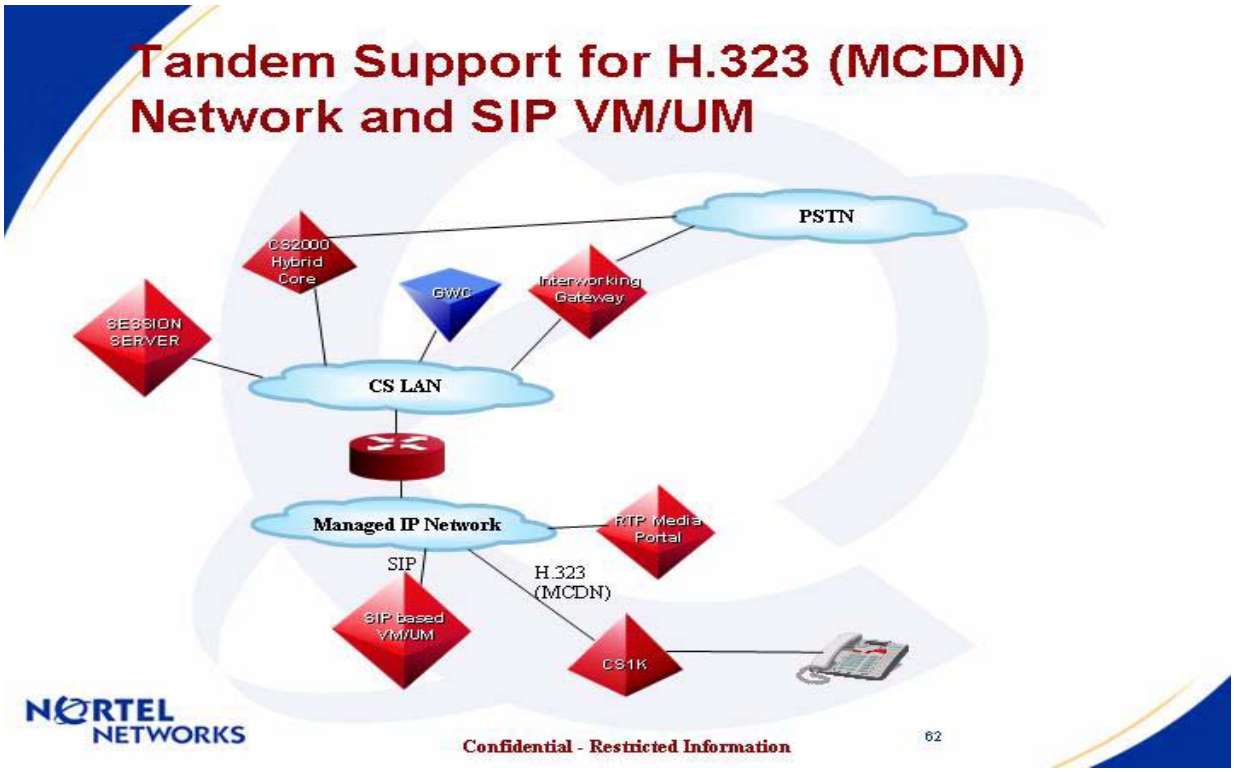


This configuration is only applicable to INTL market.

174.2.3.1.17 tandem Support for H.323 (MCDN) Network and SIP VM/UM

In a hybrid network, the customer can have private network connections between the CS2K and a CS1K/M1/BCM interconnecting via H.323 (MCDN) based networking. With the support of the SIP VM/UM, which is a network VM/UM connected to the CS2K, the CS2K become a tandem switch for the NMS traffic between SIP VM/UM and lines connected to a remote CS1K/M1/BCM via H.323 (MCDN) (See Figure 18).

Figure 18 tandem Support for H.323 (MCDN) Network and SIP VM/UM



This support is only applicable to North American market.

For INTL market, appropriate QSIG to MCDN support is required. Once the QSIG to MCDN support is fully developed, this configuration should be verified with testing under interoperability testing requirements prior to define as supported configuration.

174.2.3.2 Configurations of Lines or clients

The details of these configurations (data fill and setup) are described in the CN section of the feature. The following configurations are separated by the protocol used for communication between CS2K and line/client:

174.2.3.2.1 Lines connected via LCM/XPM

The phone line which is connected via LCM/XPM using PSTN network to the host node are supported today. In case of the SIP VM, these type of lines are considered as non-SIP lines and appropriate additional configuration is required in the Session Server.

174.2.3.2.2 CS2K hosted SIP Lines

In SN09, the CS2K hosted SIP lines support has been developed. These lines are designed such that they use implicit SUBSCRIBE to the CS2K. Therefore, these lines behave the same as lines connected via LCM/XPM for MWI perspective only.

In the future, if CS2K hosted SIP lines will be able to perform explicit SUBSCRIBE, additional work will need to be done to pass these SUBSCRIBE messages to the SIP VM/UM system. The additional work for the explicit SUBSCRIBE is not provided by this feature.

174.2.3.2.3 Lines connected via Gateways

The phone lines which are connected via a H.248-based access devices (e.g. MG9000, Calix, etc.) and MGCP-based IAD behave the same as traditional line connected to the CS2K via LCM/XPM. There is no change anticipated in this configuration. The CICM lines which are connected via an IP gateway behave the same. There is no impact to their setup and operation. In case of the SIP VM, these type of lines are considered as non-SIP lines and appropriate additional configuration is required in the Session Server.

174.2.3.2.4 Lines connected to a remote node

The lines connected to a remote node (e.g. PBX, another switch, MCP etc.) are considered as network lines. For these lines network message waiting (NMS) service is provided. The CS2K does not store any data associated with these remote lines.

174.2.3.2.5 Media Terminal Adaptor

The Media Terminal Adaptor (MTA) is used in the cable network to provide media (voice) services. From the CS2K perspective, the MTA is same as a line in the CS2K supported via gateways and gateway controller. The MWT service is provided to the MTA same way it is provided to lines connected via gateways.

> ***Note:*** The complete interoperability and compliance depends on the availability of a cable-focussed configuration in the design lab. The availability of MTA devices will allow us to perform this cable network requirement. However, it will not be overtly tested, if no lab or MTA available. Since Nortel assume that the MTA cable line is another line in the CS2K and behave same way as any other line with MWT service assignment, than this design will support the MTA.

174.2.3.2.6 Single Physical Line with Multiple VM Access

Current design of MWT service in the CS2K does not restrict a single physical line from having access to multiple VM systems. With this design, there is no change to such support. The support is provided using the data fill of the Call Forwarding on the single physical line. The following example explain how this works:

Line B is a KSET line with two different DN keys and has MWT service assigned to it.

The first key's DN is datafilled with call forwarding busy (CFB) and call forwarding do not answer (CFD) and call forwarding number to DN of VM 1.

The second key's DN is datafilled with call forwarding busy (CFB) and call forwarding do not answer (CFD) and call forwarding number to DN of VM 2.

Now let say first call to DN Key 1 encounters busy condition and forwards to the VM 1. The VM 1 records the message and send a message to CS2K to turn MWT light on for the DN Key 1. The MWT light is now lit for the first message from VM 1.

During the first call, a second call come to the DN key 2 and encounters no answer condition and forwards to the VM 2. The VM 2 records the message and send a message to CS2K to turn MWT light on for the DN Key 2. The request is now enqueued for the VM 2.

When user of Line B retrieves the message from the VM 1, the MWT light will remain lit for the second message.

Please note that the MWT request from each VM will be treated as two separate requests in the MWT service.

174.2.3.2.7 Multiple Lines with Single VM Access

The multiple lines in a given CS2K are supported by a single VM. In this case the VM has each line provisioned as individual user. This is already supported functionality. This functionality is not changed by this feature.

Some VM systems are capable to assign multiple DNs against a single mailbox (e.g. an end user with multiple phones). Therefore, when a message is recorded in the mailbox and VM is capable to provide a MWI message for each DN assigned against the mailbox. This configuration is also supported because for each DN CS2K receive a separate MWI message.

174.2.3.2.8 Multiple Lines with Multiple VM Access

This configuration is also supported in current design. The following example describes how this is supported.

Line A is a RES line with MWT service and datafilled with CFB and CFD forwarding to DN of VM 1. The VM 1 is on a remote node.

Line B is an IBN line with MWT service and datafilled with CFB and CFD forwarding to DN of VM 2. The VM 2 is on host node.

Line C is a SIP Line with MWT service and datafilled with CFB and CFD forwarding to DN of VM 3. The VM 3 is a SIP VM. The Line C is not registered.

Originator A calls Line A and Line A is busy. The call forwards to VM 1 on remote node. The VM 1 records the message from Originator A. The remote node sends a MWT message to the host node. The request of network MWT is now queued to Line A from VM 1.

Originator B calls Line B and Line B is busy. The call forwards to VM 2. The VM 2 records the message from Originator B. The VM 2 sends a MWT message to the host node. The request of local MWT is now queued to Line B from VM 2.

Originator C calls SIP Line C and SIP Line C is not registered. The call forwards to VM 3. The VM 3 records the message from Originator C. The VM 3 sends a MWT message to the host node. The request of network MWT is now queued to Line C from VM 3. The MWT notification is not sent to the Line C because it is not register. When the user of Line C sends a subscribe message for MWT after registration, the CS2K sends the current status of the MWT service in the CS2K to the line C.

174.2.4 Sample Message Details for SIP

The message details are based on the SIP Line configuration described above.

Step 1: The SIP Line SUBSCRIBE for MWT service.

Figure 19 SIP Line Register with CS2K - SUBSCRIBE Message

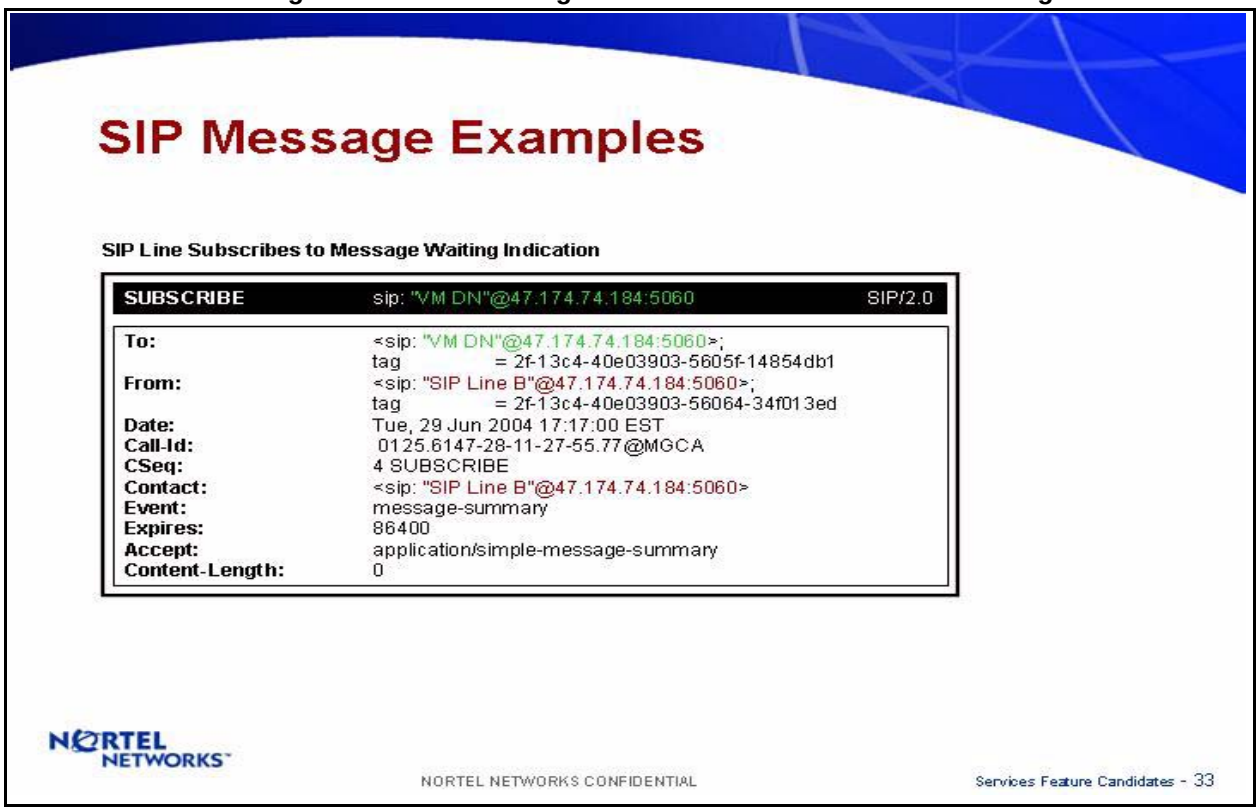


Figure 20 SIP Line Register with CS2K - OK Response

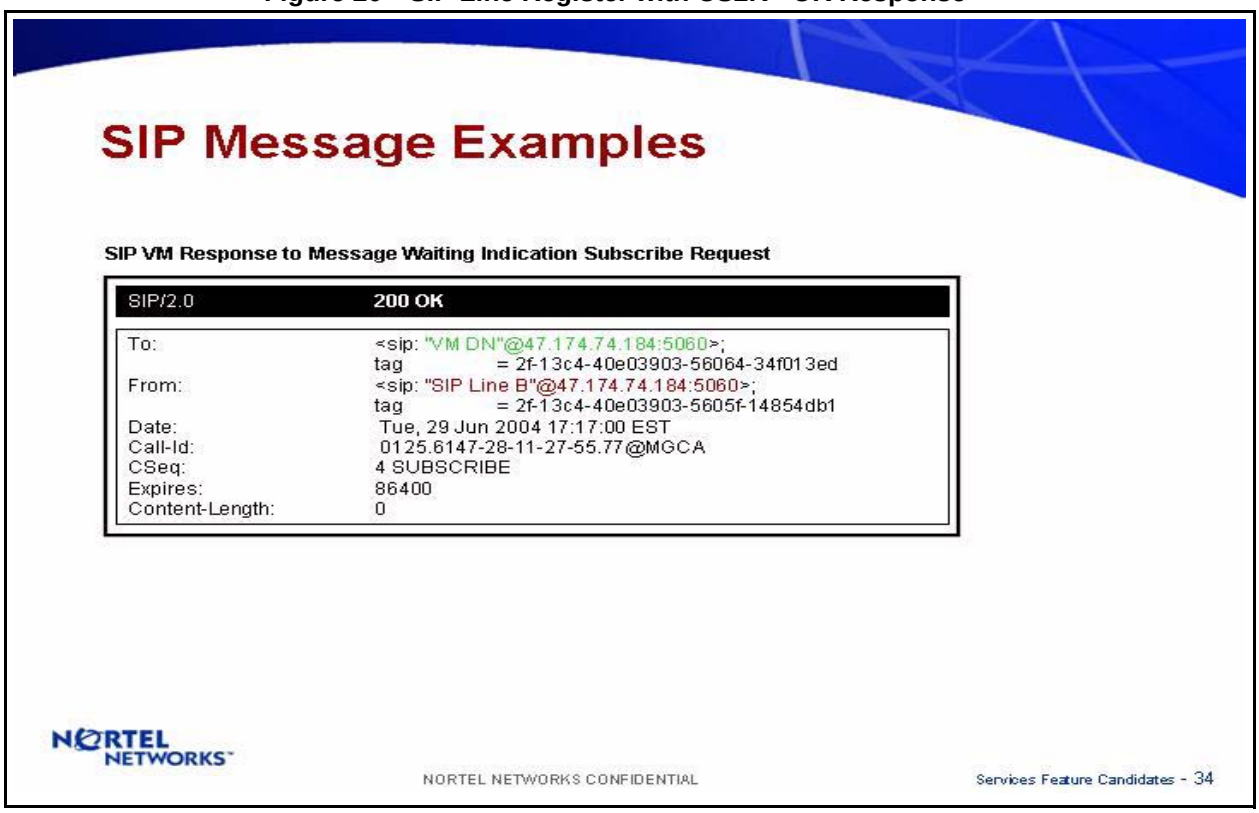


Figure 21 SIP Line Register with CS2K - NOTIFY Message

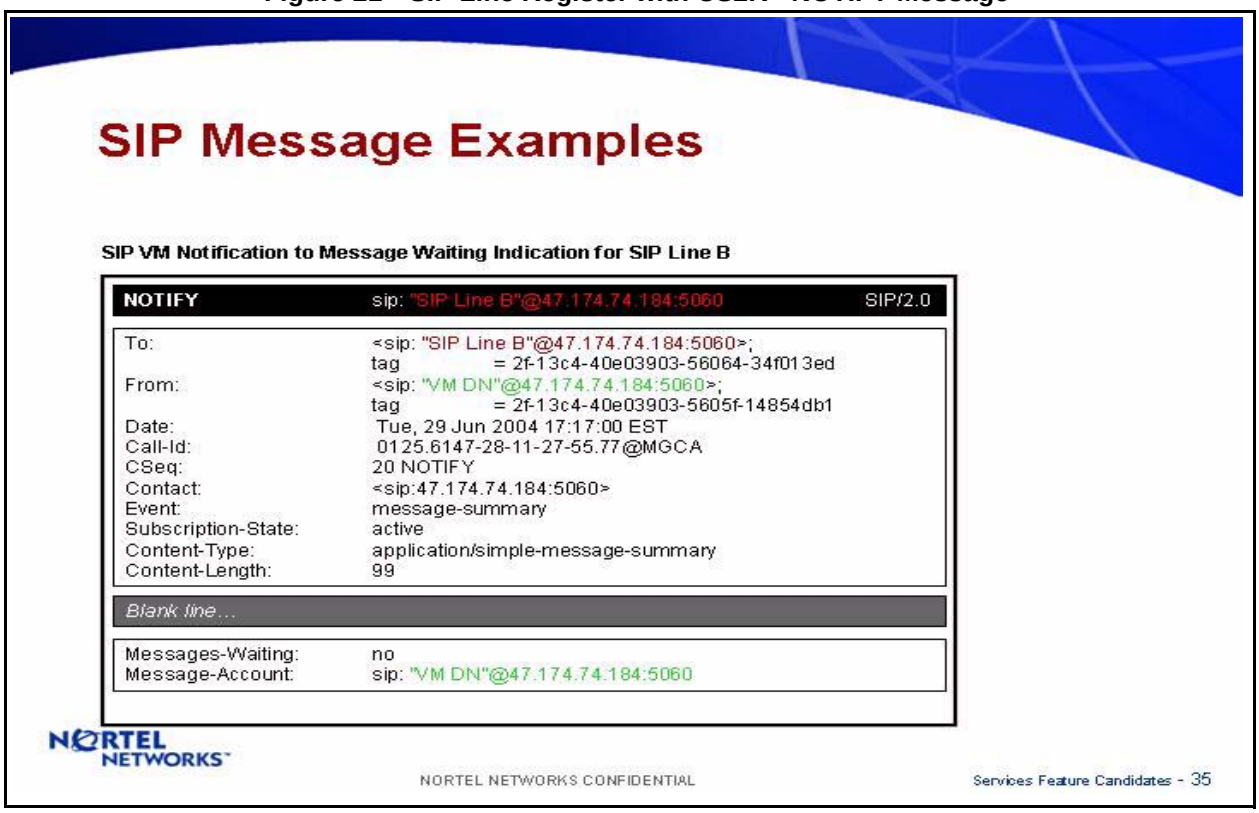
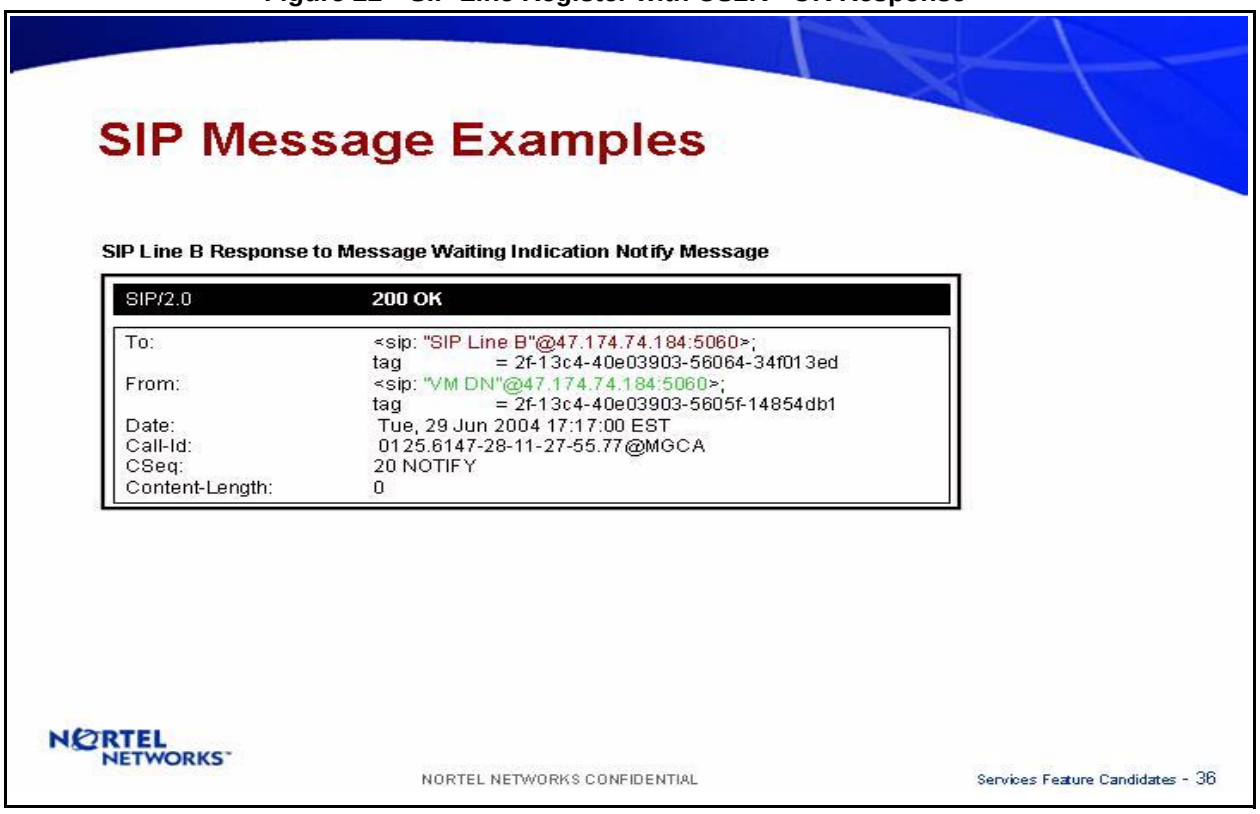


Figure 22 SIP Line Register with CS2K - OK Response



Step 2: Line A Calling SIP Line B and Forwarded to VM using SIP network

Figure 23 Call Termination to SIP VM DN - INVITE Message

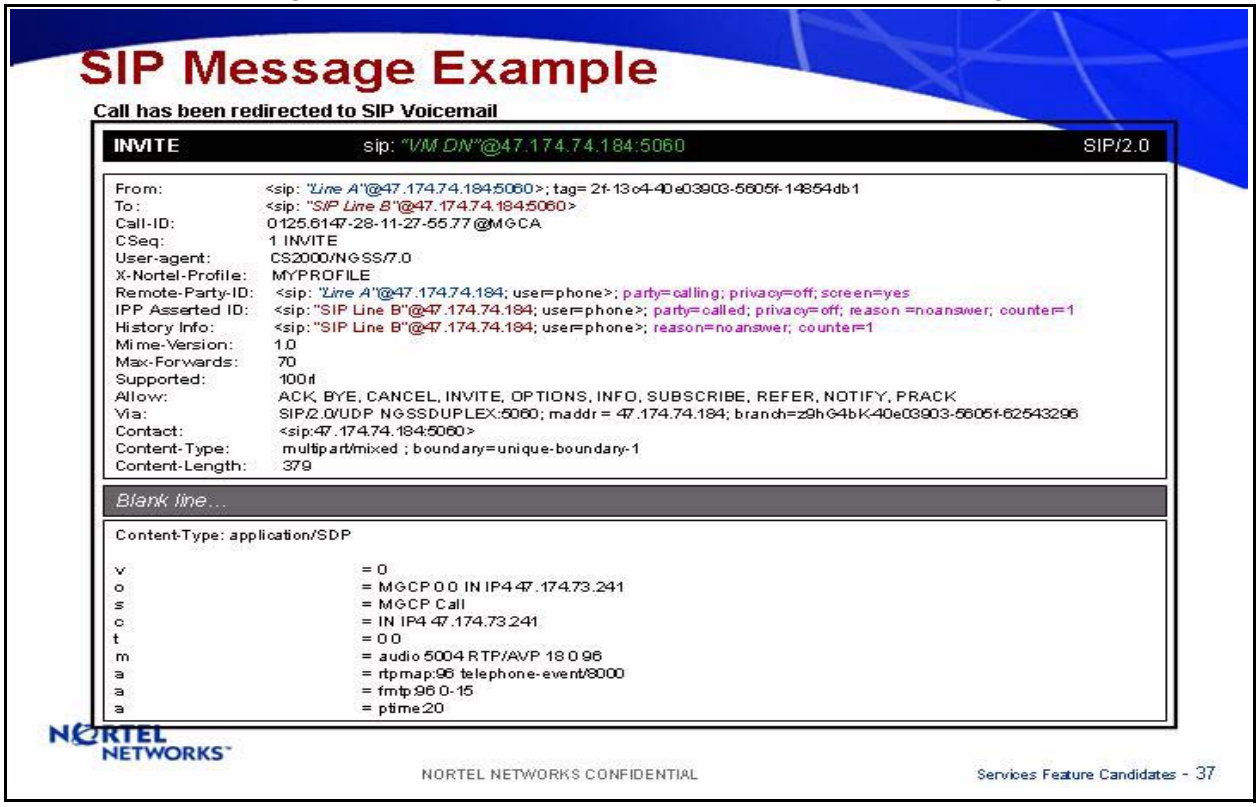


Figure 24 Call Termination to VM DN - 100 Trying Response

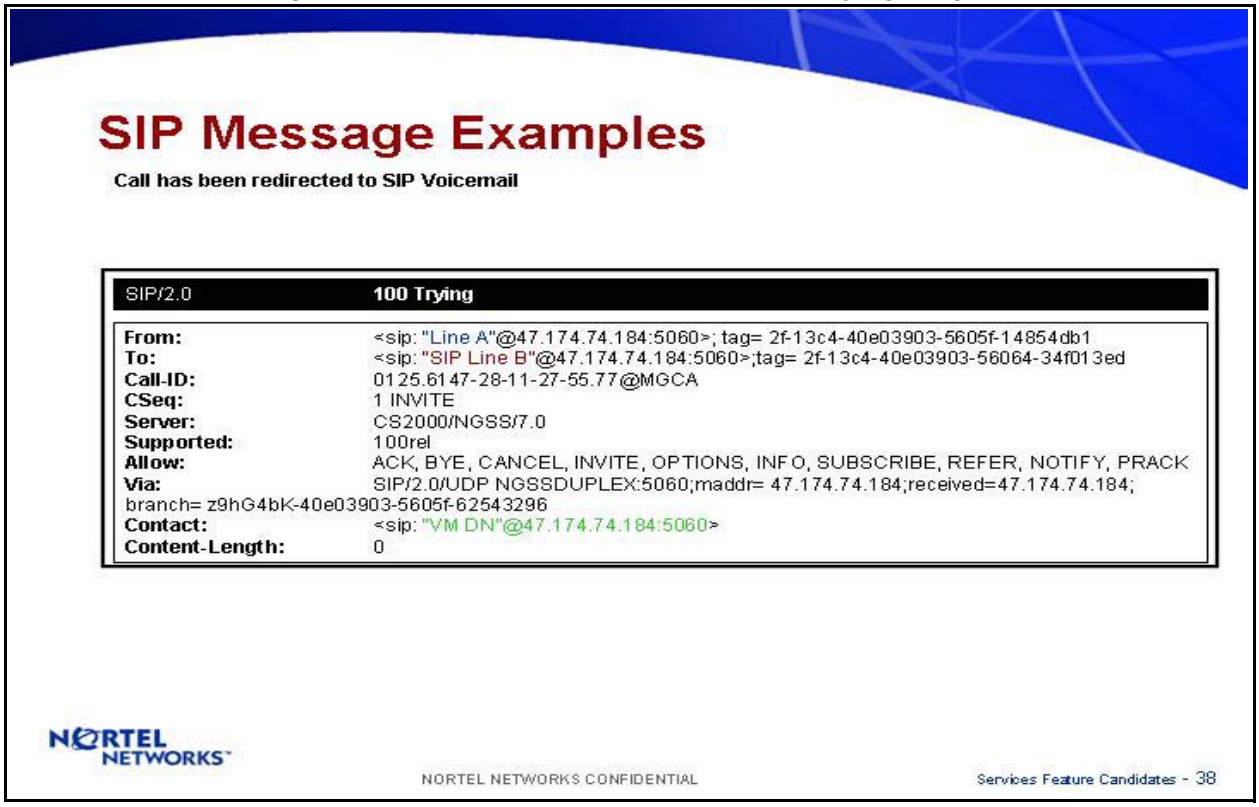


Figure 25 Call Termination to VM DN - 180 Ringing Response

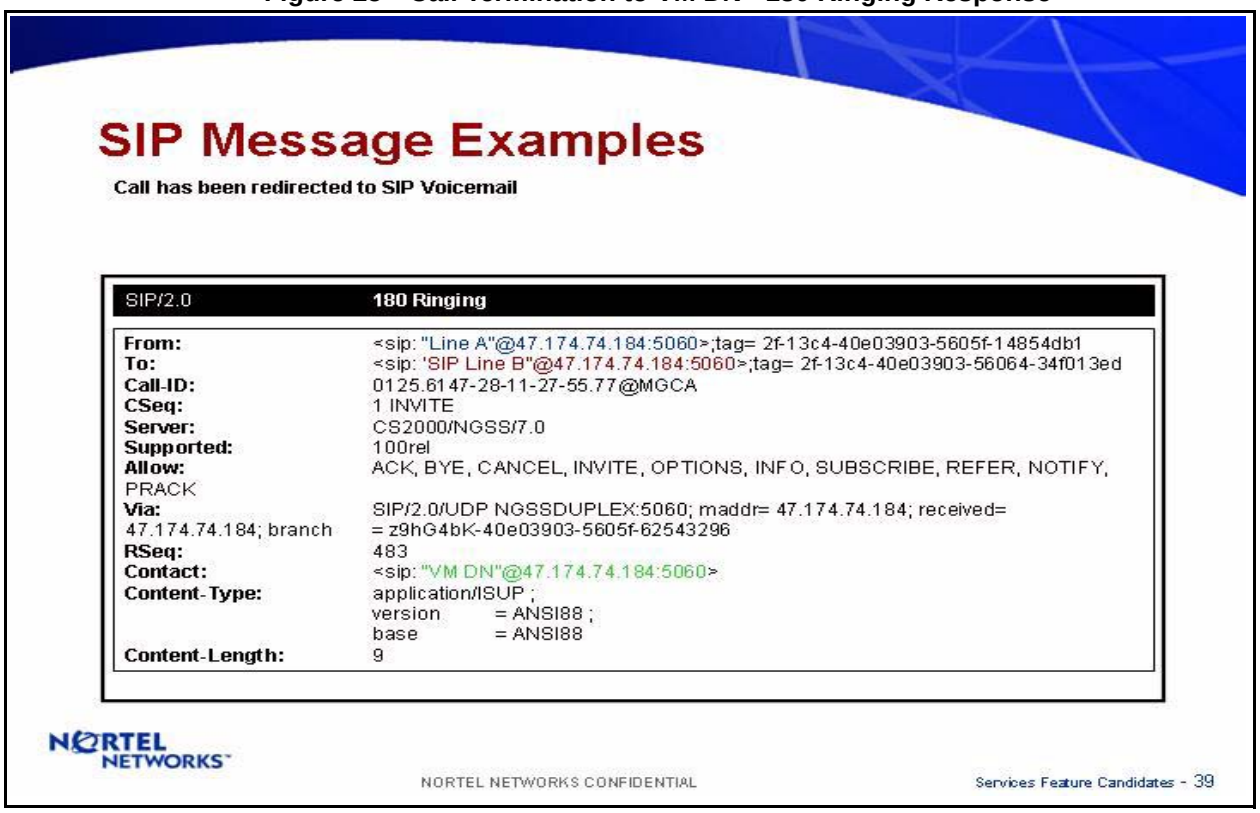


Figure 26 Call Termination to VM DN - 200 OK Response

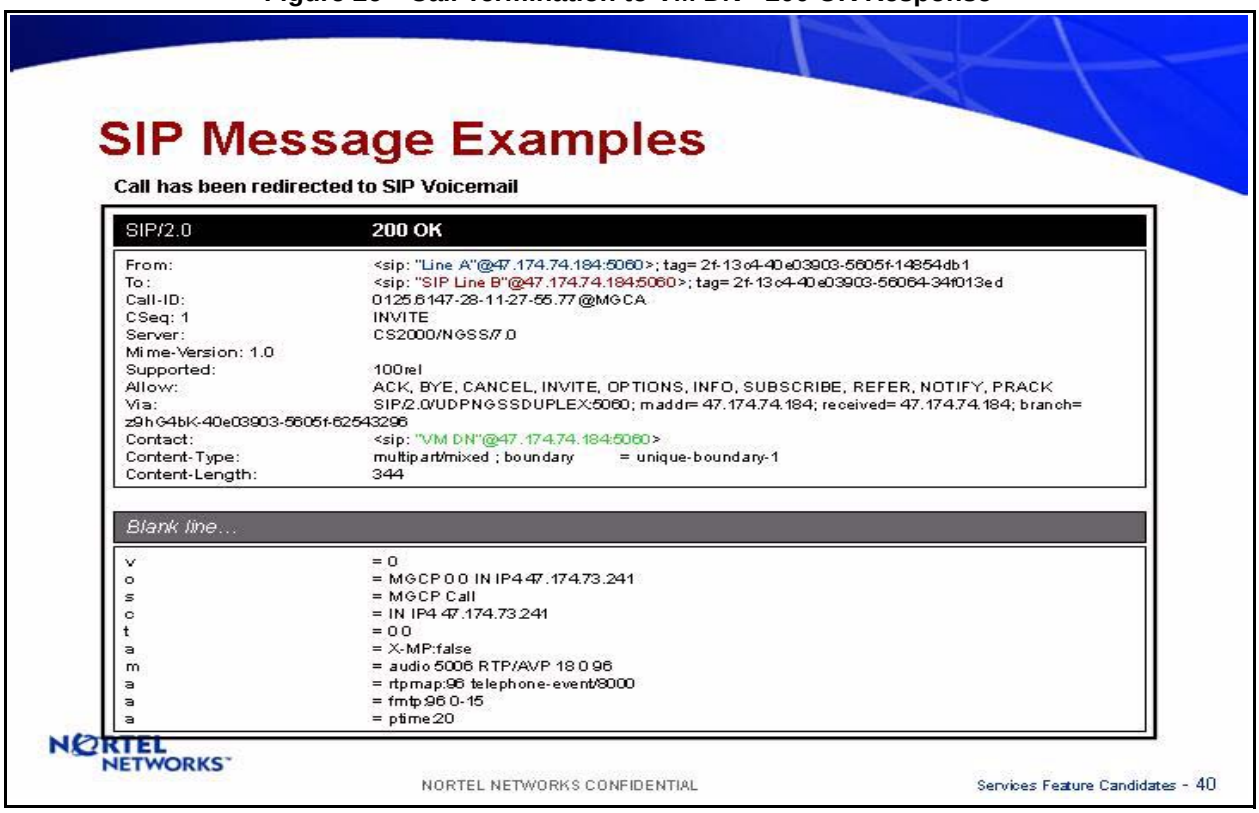
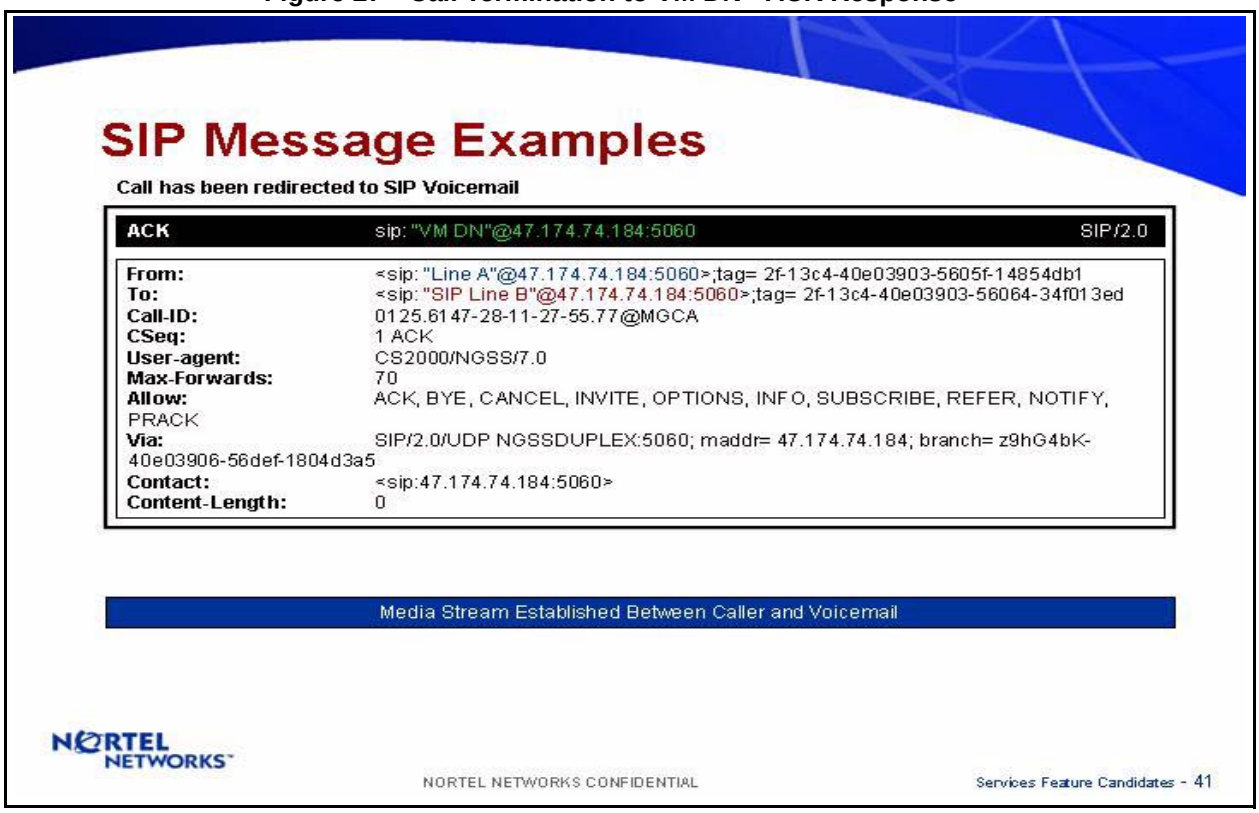


Figure 27 Call Termination to VM DN - ACK Response



Step 3: Caller Records Message and hang-up

Figure 28 Call Release from Caller - BYE Message

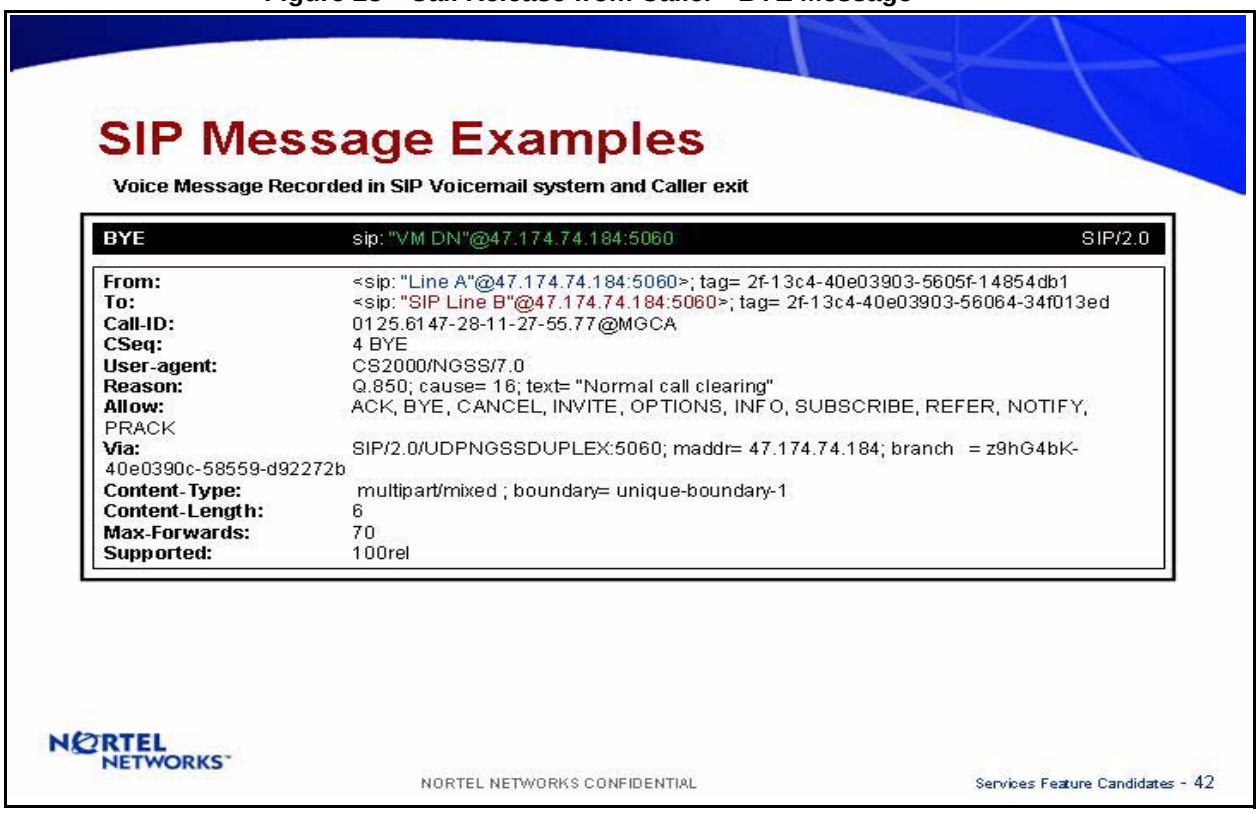
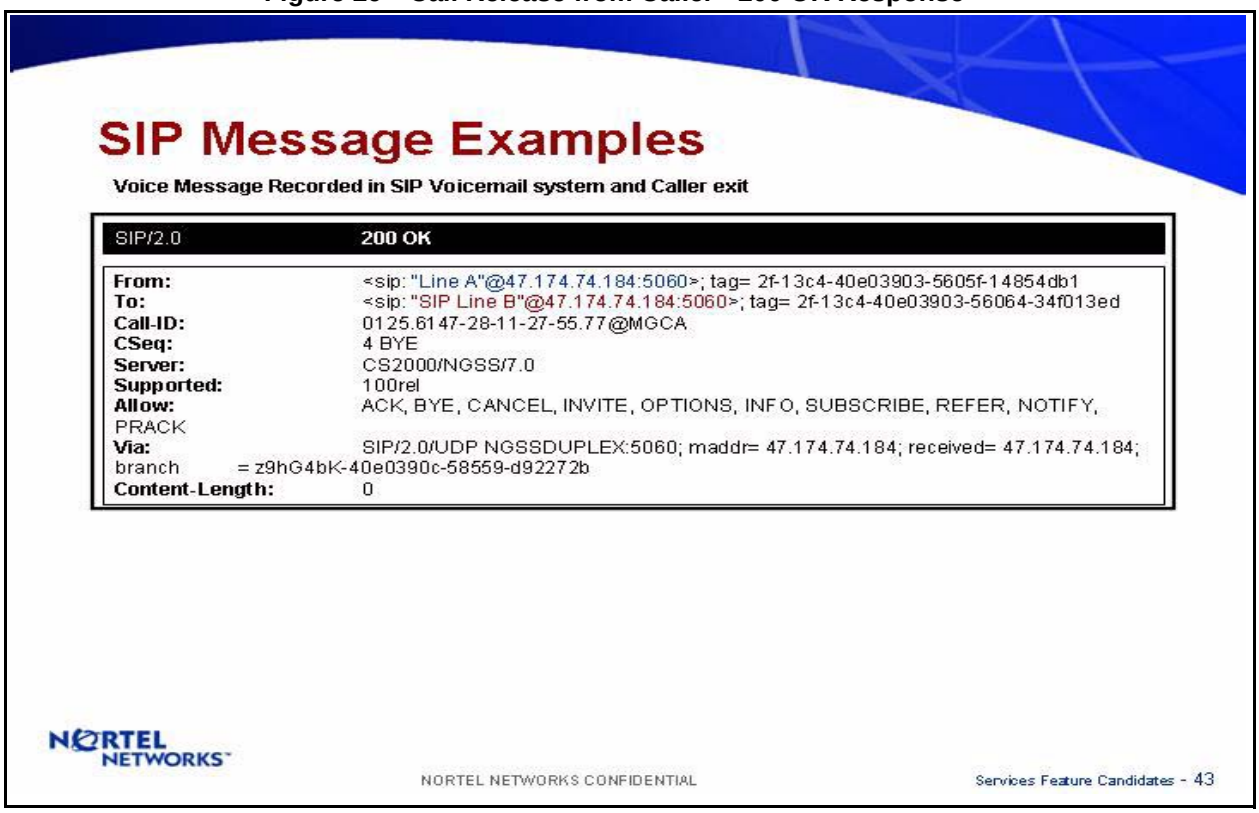


Figure 29 Call Release from Caller - 200 OK Response



Step 4: CS2K sends a NOTIFY Message

Figure 30 CS2K sends NOTIFY Message

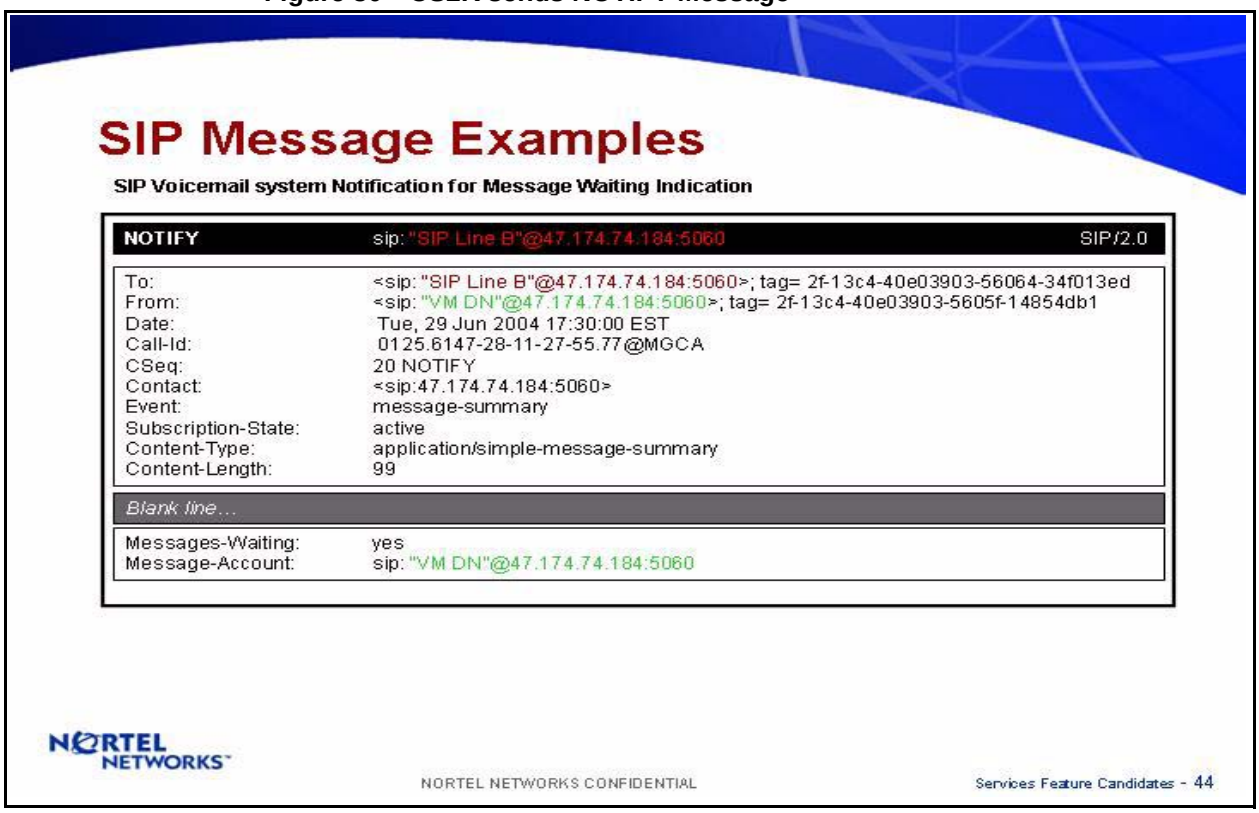
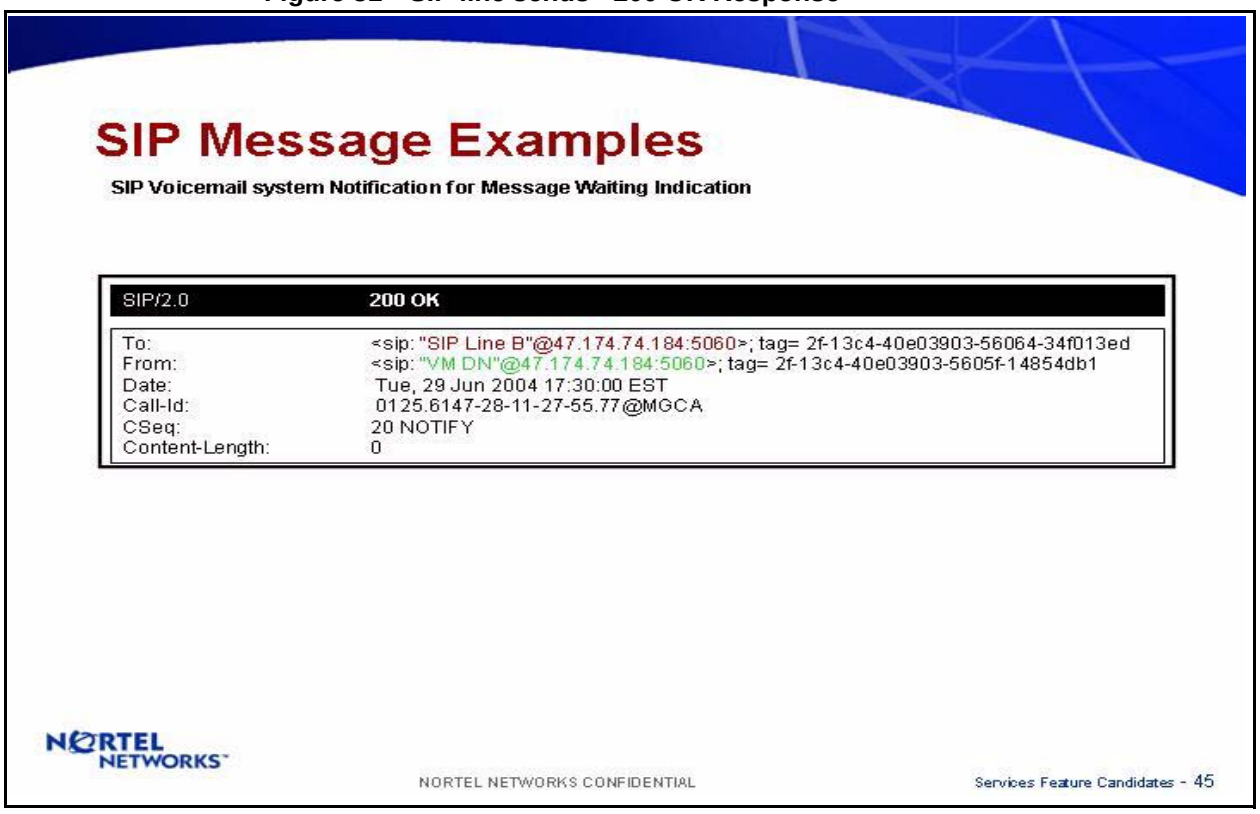


Figure 31 SIP line sends - 200 OK Response



Step 5: SIP Line retrieves the Messages from the VM using SIP network

Note: The SIP messages are related to basic SIP call.

Figure 32 SIP Line B Calling VM DN - INVITE Message

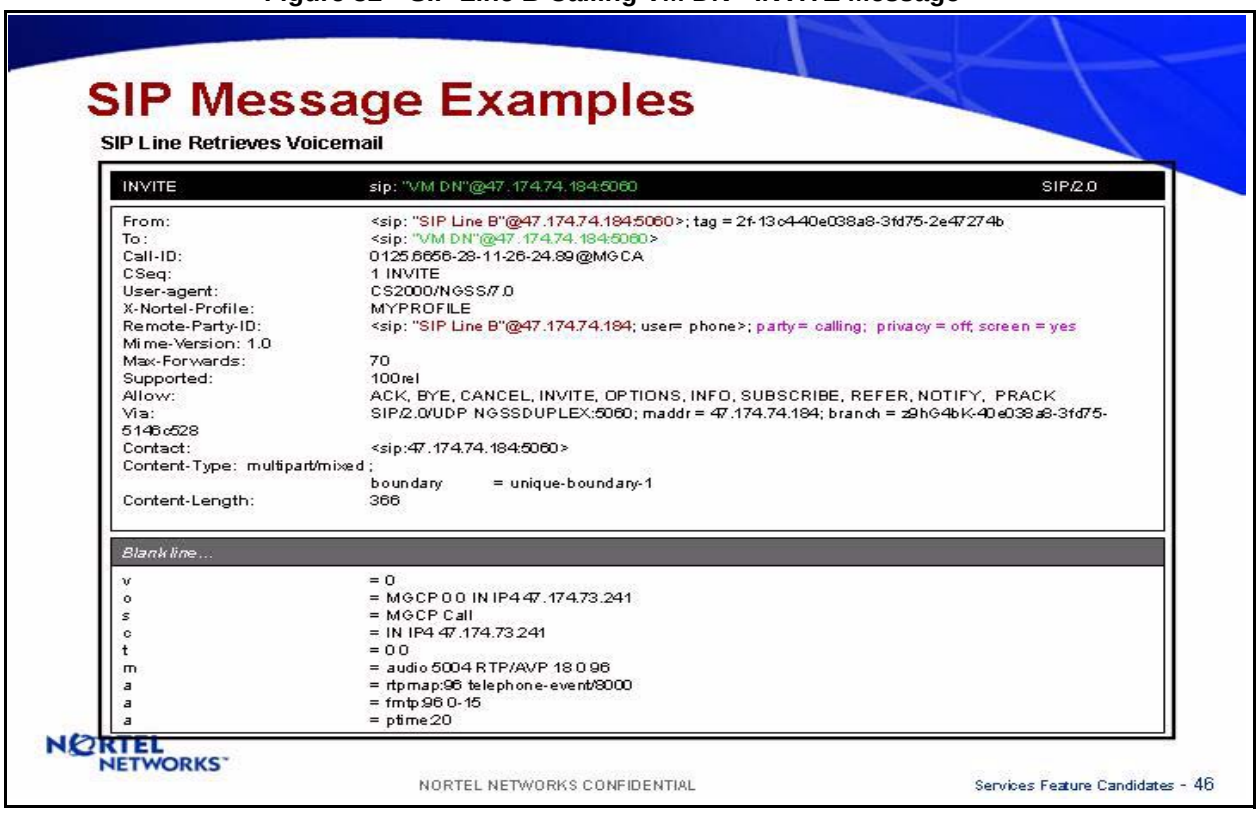


Figure 33 SIP Line B Calling VM DN - TRYING Message

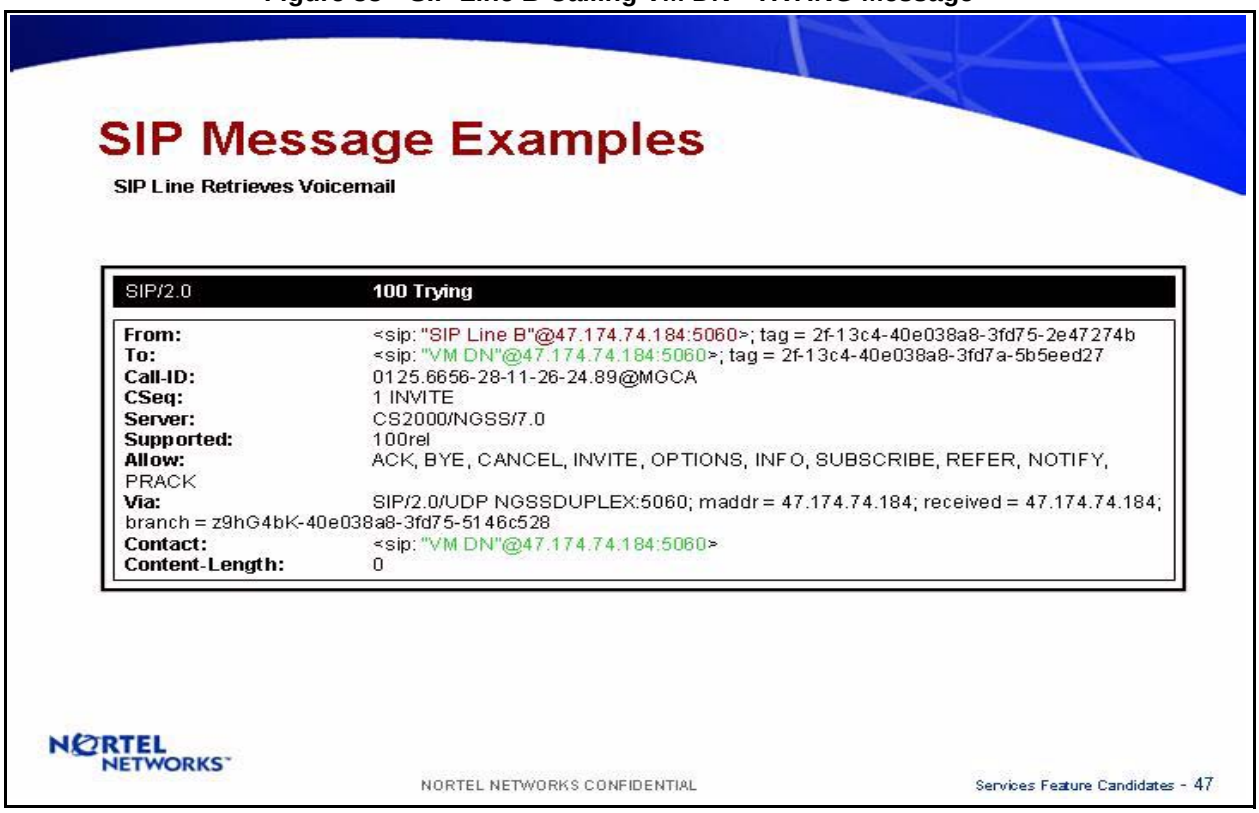


Figure 34 SIP Line B Calling VM DN - RINGING Message

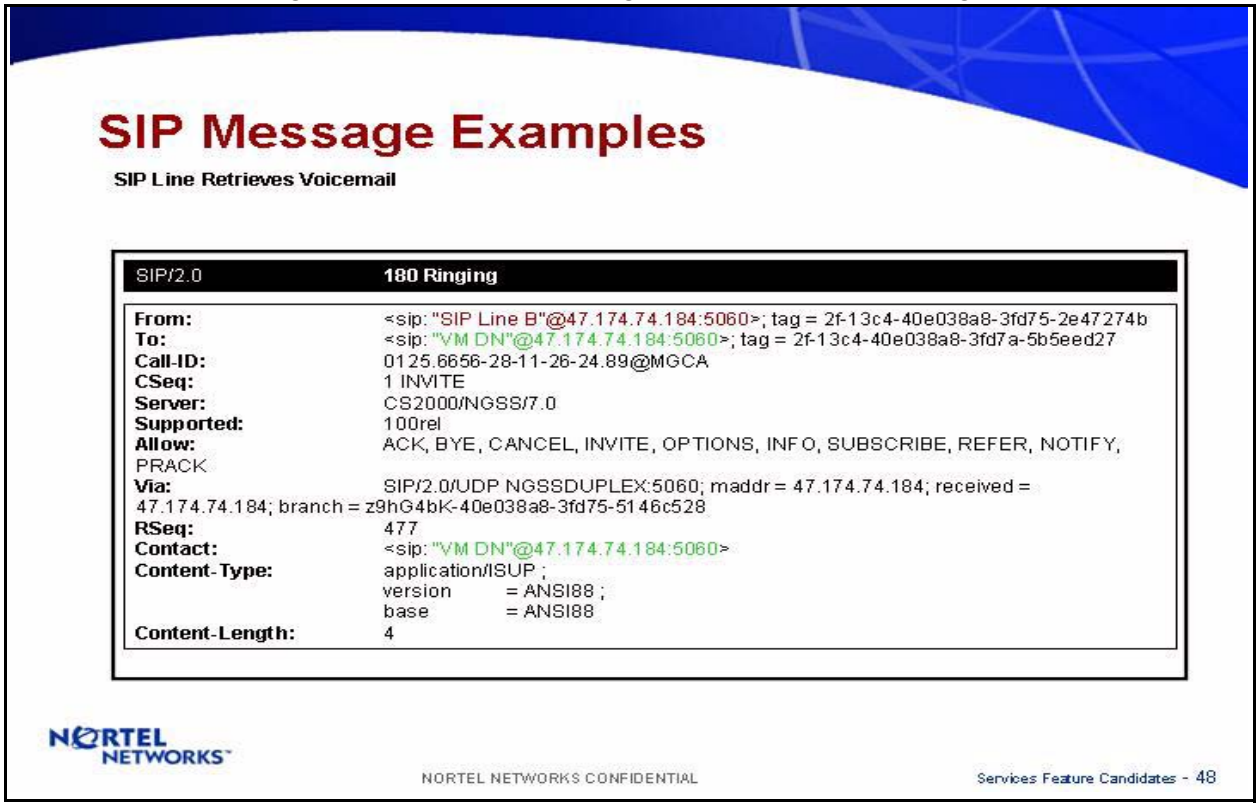


Figure 35 VM Answers - CS2K sends OK Response Message

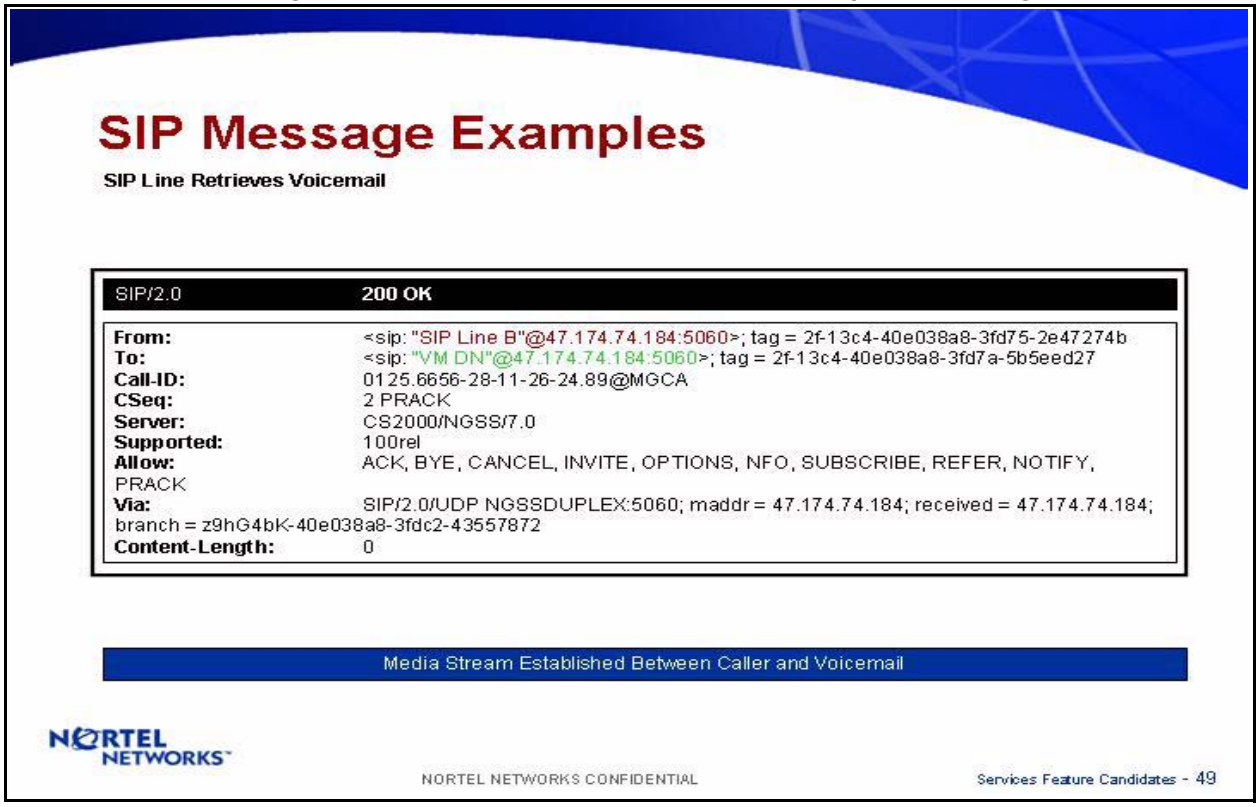


Figure 36 SIP Line B Accepts - ACK Response Message

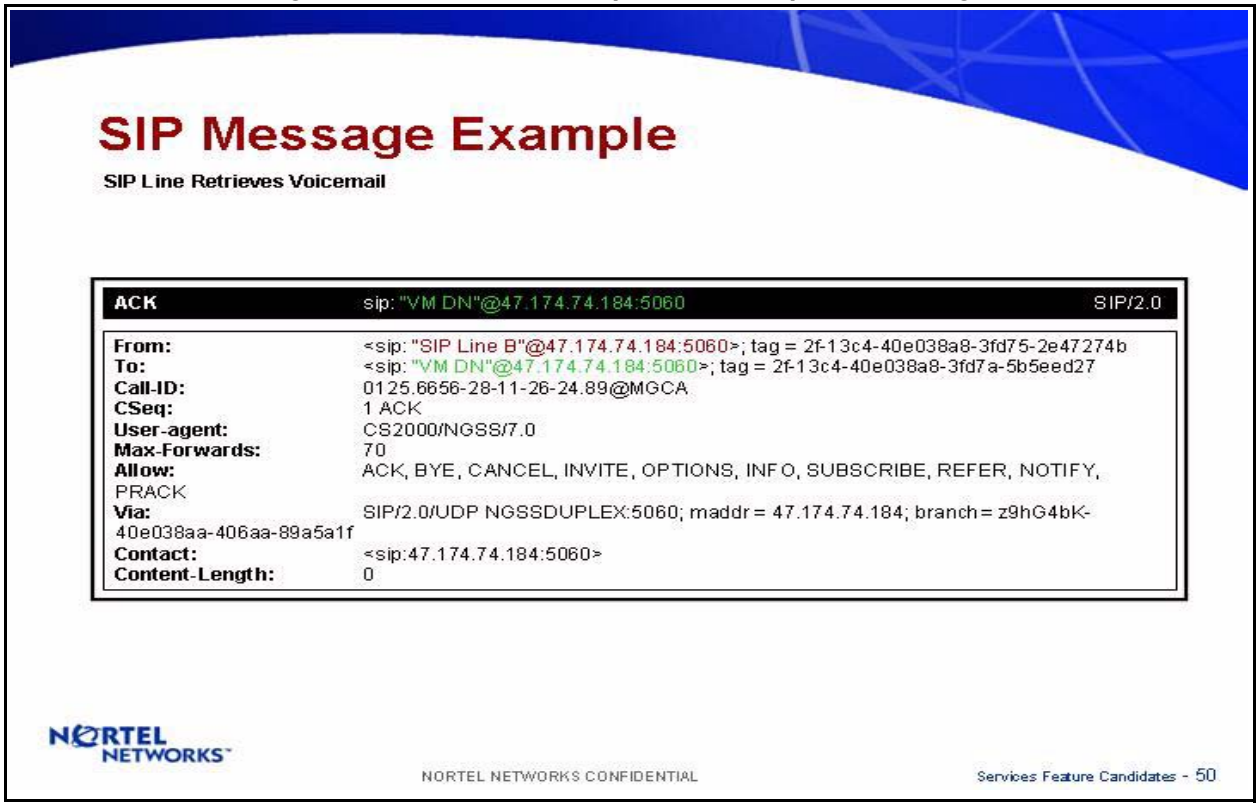


Figure 37 SIP Line B Exit from the Call - BYE Message

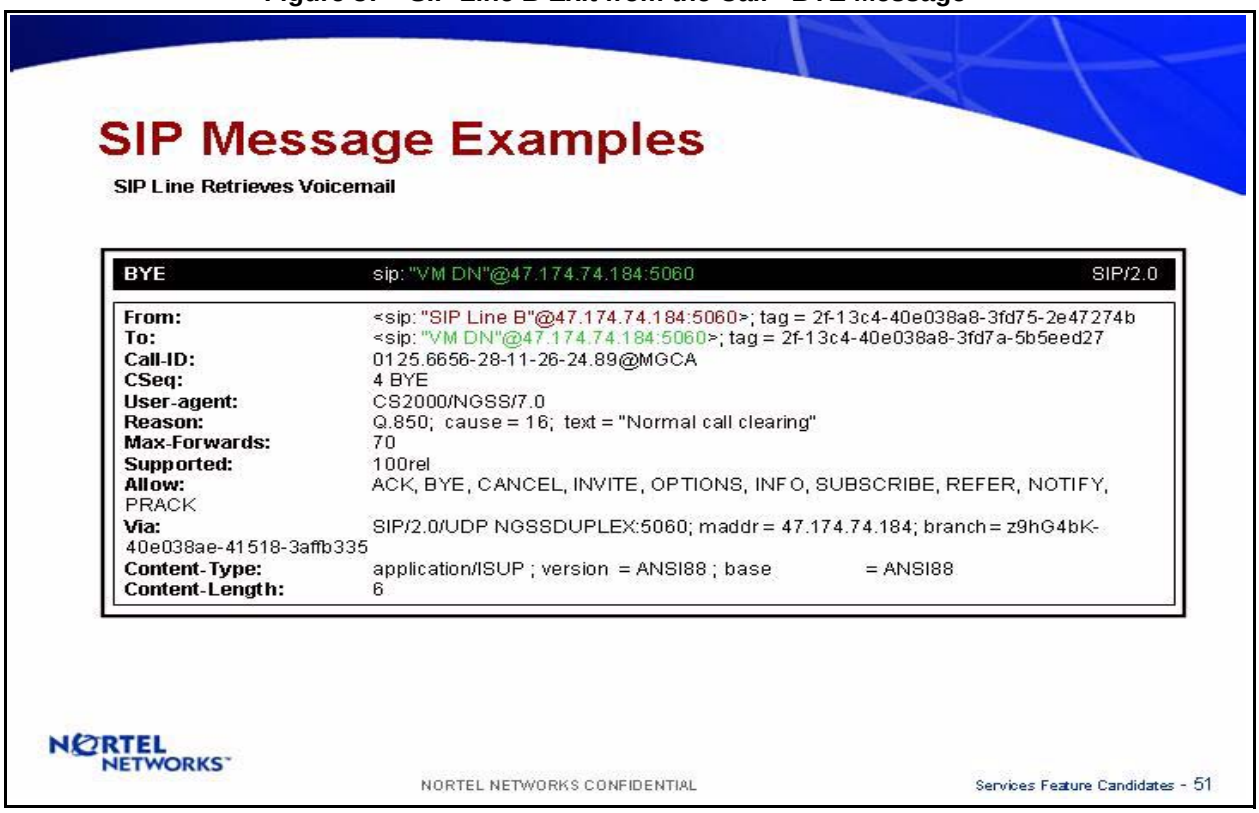
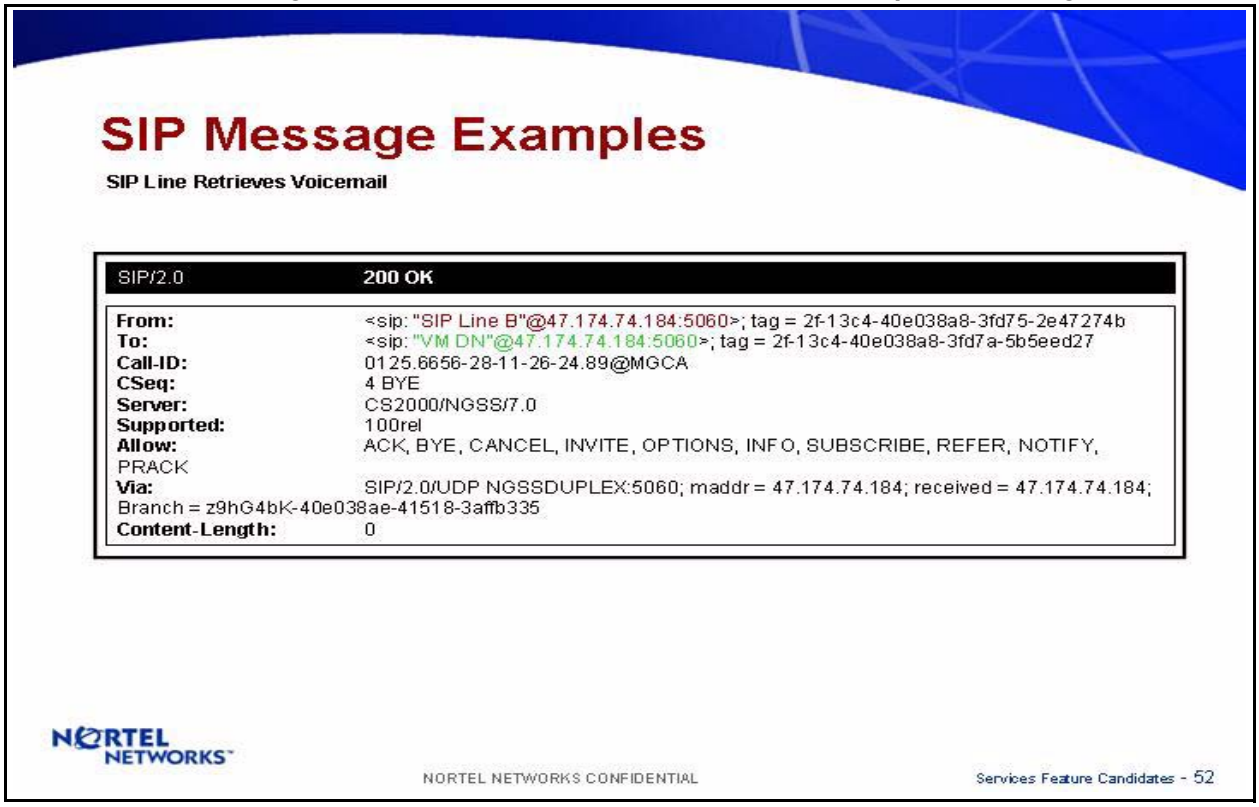


Figure 38 VM disconnects - CS2K sends OK Response Message



Step 6: CS2K sends NOTIFY message.

Figure 39 CS2K sends NOTIFY Message

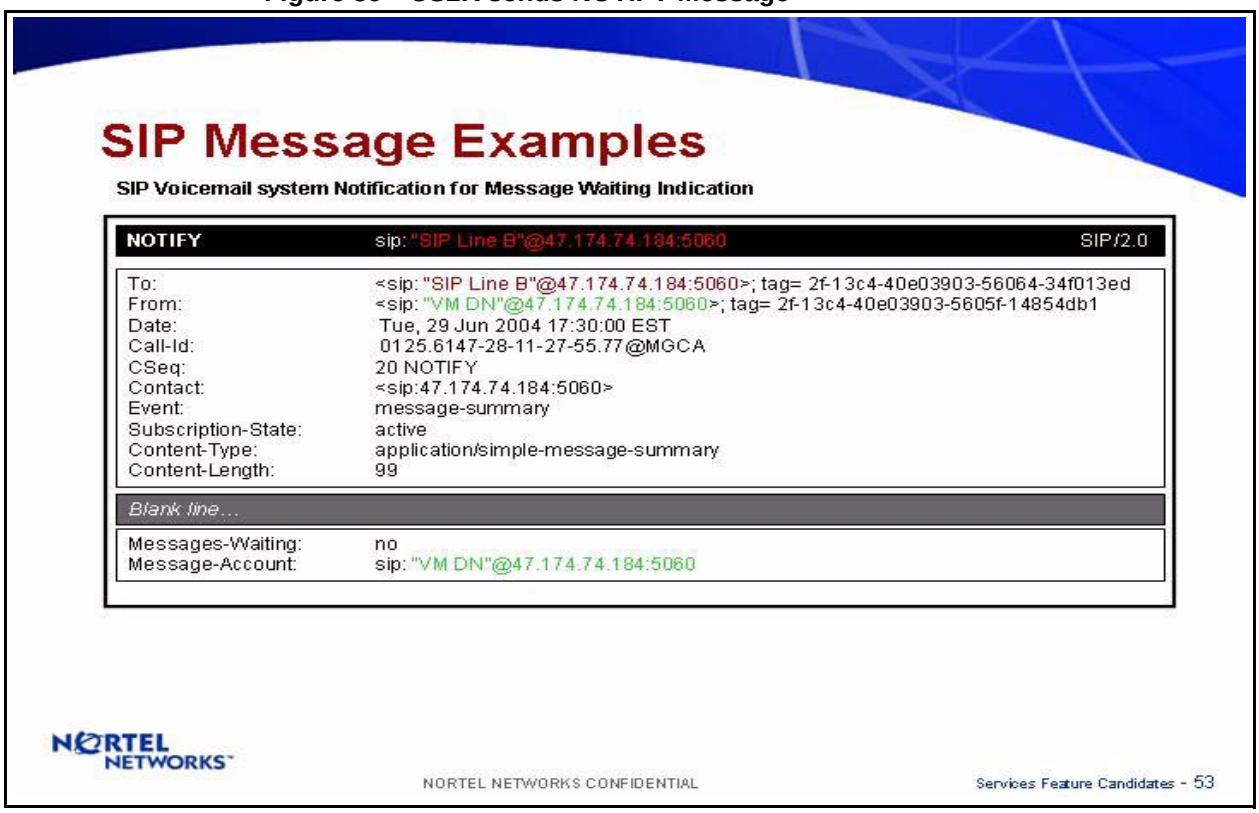
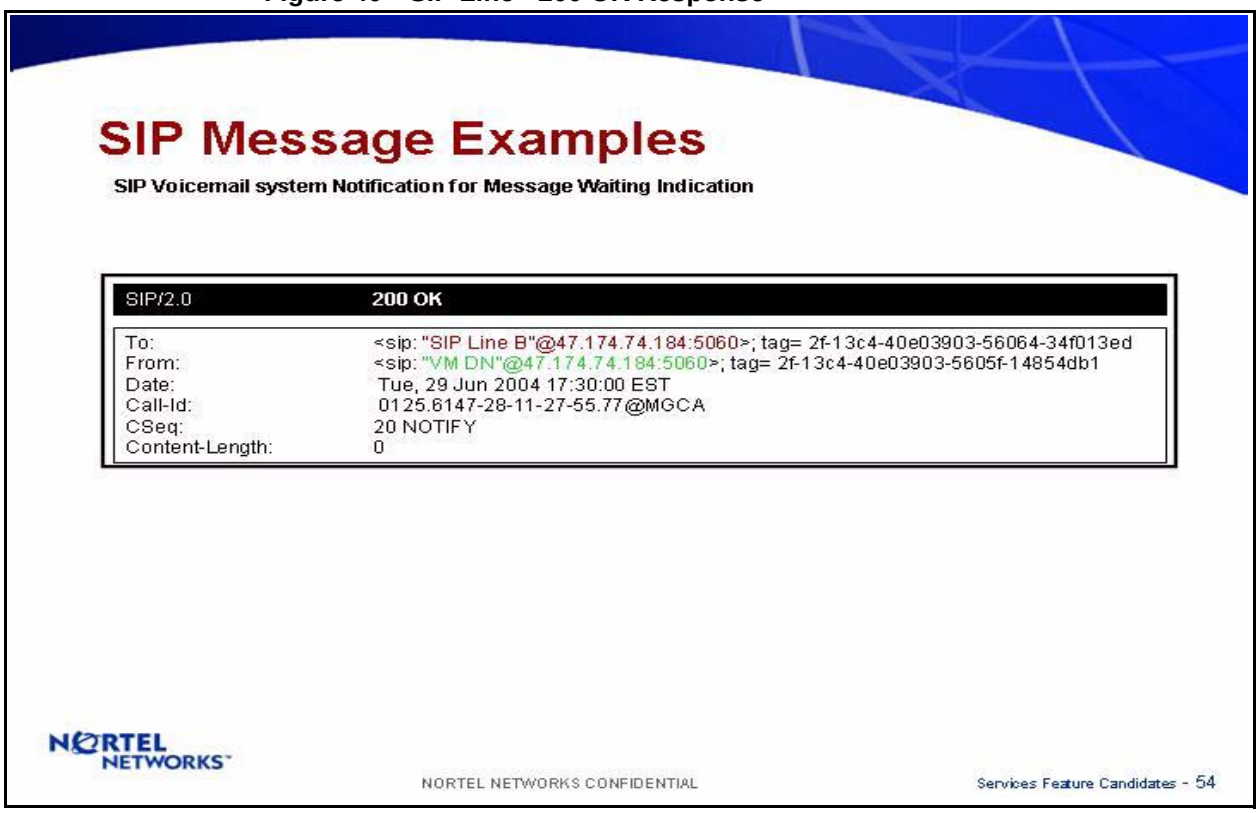


Figure 40 SIP Line - 200 OK Response



174.3 Hardware Requirements or Dependencies

This feature uses the existing hardware of CS2K Core and Session Server. The Session Server provides a standard-based SIP interface. Therefore, all commercially available 3rd party hardware and Voicemail systems are directly supported.

The commercial 3rd party VM/UM box will be used from a remote lab in Ottawa for testing purpose.

The Open Source VM/UM system is run on a LINUX platform. Therefore, it does not need any separate hardware. Lab based LINUX box will be used to create a Open Source VM/UM.

There is no new hardware dependency or requirement for this feature.

174.4 Software Requirements or Dependencies

The development depends on following 3rd party software currently exists in respective platform:

- SIP Stack from RADVISION in Session Server

The usage of this service depends on SOC MDC00078. Also, the H.323 network connectivity depends on two SOC CS2B0004 and CS2C0004.

174.5 Limitations and restrictions

The following limitations and restrictions apply to the feature:

- The NMS service sends MWI ON/OFF for the remote lines. It is assumed that the remote node or SIP Client will provide appropriate indication to the end user for the MWI. The MWI indication can not be enforced from the CS2K.
- The Call Request Retrieval (CRR) functionality can not be invoked as second leg of Three way call (TWC). This limitation is for fraud prevention.
- The Call Request Retrieval (CRR) functionality can not be invoked as second or subsequent leg of a conference (CNF) call. This limitation is for fraud prevention.
- The MWT functionality is only provided to multiple appearance directory number (MADN) primary member.
- The MWT functionality is only provided to HUNT group primary member.
- All existing MWT and NMS service limitations apply to this feature except as overtly noted in feature documentation.
- The optional data defined in the RFC 3842 are not supported by current feature. The support for the optional data can be developed in future releases.
- In cases where a Line is connected to a CS2K, the VM is connected to a remote node (e.g. MCS) via SIP network, and a G729 compatible codec is used for interconnect voice paths, the remote node or device must support RFC 2833 for out of band DTMF signalling.
- When the line is connected to a remote node (e.g. MCS) via SIP network, VM is connected to a CS2K, and a G729 compatible codec is used for interconnect voice paths than remote node or device must support RFC 2833 for out of band DTMF signalling.
- The design is generic and based on RFC 3842 standards. Testing limitations does not allow for testing every possible interoperability scenarios using different hardware and vendor equipment in a network. In order to make different hardware and vendor equipment supported, proper interoperability testing must be done in Nortel approved interoperability lab. After the complete testing, appropriate support will be provided. The configurations defined in this document are tested generically.
- The design supports maximum of 10 digit DN in form of North American and Universal DN.

- The only IP devices supported in Table IPAPPL for SOC MDC00078 (NMS over SCTP) are EIU and HIOP.
- The SETPRIME and MULTIHOMING options in Table IPAPPL are allowed to add in Table IPAPPL. However, their usage is ignored.
- The MODE option in Table IPAPPL is always SERVER. If not added by the craft person, it will be added automatically.
- The option NEWTOR in table MSGRTE is not supported.
- For international markets, only ETSI ISUP and ETSI PRI interworking is supported by this feature. The DPNSS based interworking will be supported under companion features A00012847 and A00009409.
- The digit manipulation allowed in Table MSGRTE manipulates the source or destination digits only. For SCTP selector, the source or destination digits does not have any meaning. Therefore, digit manipulation via Table MSGRTE is not supported.
- For CS2k- hosted SIP lines, the implicit subscribe has been assumed. No SUBSCRIBE message are forwarded from CS2K hosted SIP line to the SIP VM/UM. The Session Server design assumes that for these SIP lines, only the implicit SUBSCRIBE supported.
- The NOTIFY message to the MCP 5100/5200 is only supported due to limitation on MCP5100/5200 to forward the SUBSCRIBE message from the SIP device to CS2K.
- The MCP 5100/5200 based MAS as VM/UM is not supported. The MCP 5100/5200 is not capable to send/receive the NOTIFY/SUBSCRIBE messages from/to MAS for the SIP Network. It only supports the SIP device register with the MCP 5100/5200.

174.6 Interactions

The service is controlled by the CS2K Core. The Session Server and GWC only provides access to various networks and protocol conversions. Therefore, CS2K Core interactions are applicable to this service.

The existing MWT and NMS service software is used for the development of this feature. Therefore, all existing interactions apply to this expansion of service. There is no new interaction anticipated at the time of this writing.

174.7 Glossary

Term	Description
CFB	Call Forward Busy
CFD/CFDA	Call Forward Do Not Answer

Term	Description
CFU	Call Forwarding Unconditional / Call Forwarding Universal
CICM	Centrex IP Line
CRR	Call Request Retrieval
CS2K	Communication Server 2000
DMS	Digital Multiplex Switch
DN	Directory Number
EO	End Office
ETSI	European Telecommunications Standards Institute
GCP	Generic Call Protocol
GW	Gateway
GWC	Gateway Controller
IAD	IP Analog Gateway
IBN	Integrated Business Line
IP	Internet Protocol
ISDN	Integrated Services Digital Network
KSET	Key Set Line
MCDN	Meridian Customer Defined Networking
MG9K	Media Gateway 9000
MS	Message Switch
MsgSrv	Message Server
MWI	Message Waiting Indication
MWT	Message Waiting
NCAS	Non-Call-Associated Signaling
NGSS	Session Server
NMS	Network Message Waiting

Term	Description
PBX	Private Branch Exchange
PC	Personal Computer
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephony Network
PVG	Packet Voice Gateway
RES	Residential Line
S1K/1KM	Type of IP PBX
SCTP	Session Control Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMDI	Simplified Message Desk Interface
SOC	Software Optionality Control
SS7	Signaling System No. 7
TCAP	Transaction Capabilities Application Part
TDM	Time Division Multiplexing
TEL URI	Telephony URI
TPT	Terminal Processing Task
UCD	Uniform Call Distribution
UM	Unified Messaging
URI	Uniform Resource Identifiers
VM	Voicemail System
VoIP	Voice over Internet Protocol

175: Functional Description (FN) A00013508

175.1 Feature name and Feature ID

A00013508: System Manager Auto-Failover Support

175.2 Description

This feature gives an overall design level changes required in the IEMS Software to integrate the System Manager Auto-Failover Support functionality in to IEMS. System Manager is already being managed by the IEMS, but due to a requirement, System Manager is going to include the Auto-Failover functionality on it, which will lead to certain changes in the Data Exchange between the IEMS and the System Manager. This document captures all such changes and the necessary IEMS side modifications required to perform the System Manager Management as expected.

The major changes with respect to the IEMS data exposure due to the Auto-Failover support will be

- SNMP Traps (Faults from the System Manager) will have the Logical IP Address as their source address instead of the physical unit IP address.
- SNMP Requests should be coming to the Logical IP Address of the System Manager to retrieve any fault or performance data.
- No Stranded data should be passed on to the OSS from the System Manager via IEMS

175.3 Customer Visible Changes in IEMS due to this Activity:

1. While Provisioning the System Manager in to IEMS, the user will have to specify the Logical IP of the System Manager in the Hostname/IP Address text field of the initial Add Node screen.

2. With this feature introduction, IEMS will be listening for Traps from the Logical IP only.

3. The Resync Alarms Menu will be enabled in the Parent System Manager Object and the same will be disabled in the Physical Unit Objects, which is the opposite of what exists now.

4. The OSS will see a new Performance major alarm and log EMJS351 if there are problems with the login details specified for collecting the PM Files from the System Manager and the same will be cleared if the problem is resolved. The problem description is one of two types:

- Unable to login to the Device: <Device Name> with the specified Username and password to collect PM data (If login fails)
- Insufficient privileges for the specified Username and password to rename the PM files on the Device: <Device Name> (If file renaming fails)

This alarm will be generated only once and will be cleared once the log situation is rectified. One important thing to note is that, if the above log situation arises, IEMS will not collect any data from the System Manager to avoid processing the same files again and again.

5. Customers should avoid configuring a direct FTP PUSH OM Collection directly from the SM/FPM to Performance data collection; otherwise, it will lead to loss of data on both the feeds (data being sent from IEMS and the data directly being pushed by the SM/FPM).

176: Functional Description (FN) A00013935

176.1 Feature name and Feature ID

A00013935: PKMTA Extraction for DPT Call

176.2 Description

This feature, A00013935: PKMTA Extraction for DPT Calls, extends the Packet Media Anchor (PktMA) removal software developed for SIP Lines to allow it to be used by Dynamic Packet Trunks (DPTs).

In SN09, a DPT call never releases the PktMA resources once one has been added to the bearer path. This means that for DPTs agents the network had to be engineered to have PktMA resources for the duration of the DPT call, whether the call was using the resource or not.With the extension of the ability to remove the PktMA to DPTs, a CS2000 network requires significantly fewer AMS 2010 gateways for the PktMA function. This results in a decreased cost for the CS2000 SIP-T solution.

The removal of the PktMA for SIP and SIP-T DPT is triggered by monitoring the functions the PktMA is currently performing and by the state of the call. Once the PktMA is no longer needed in the call it is removed from the bearer path.

Calls that will now be able to remove the PktMA are:

- Calls where the PktMA supplies audible ring back after answer such as with bind call transfer and call park
- Calls where the PktMA is used to collect addition routing information such as DISA and DMS-250 Calling Card Services (MCCS)

Services that use continuous scanning, for example reorigination, like what is provided by the STR card on an XPM will continue to require the PktMA resource for the duration of the call.

176.3 Hardware Requirements or Dependencies

This feature adds no new hardware dependencies to the system. The feature does have all the dependencies of the features it builds on. Please reference the feature documentation for A00007120 PktMA dependencies

This feature does change the number of AMS gateways that will be needed to support the PktMA function in a network. Please refer to the relevant engineering documentation to determine the number of AMS a network requires.

176.4 Software Requirements or Dependencies

This feature adds no new software dependencies to the system. The feature does have all the dependencies of the features it builds on. Please reference the feature documentation for A00007120 PMA dependencies.

176.5 Limitations and restrictions

The PktMA removal functionality provided by this feature is disabled for BICC DPTs. In addition the feature does has all the limitations and restrictions of the features it builds on. Please reference the feature documentation for A00007120 PMA limitations and restrictions.

176.6 Interactions

The CS2000 system puts all PktMA resources in to the same PktMA pools. Since a PktMA can only be used by one SIP Line or DPT at a time the PktMA resource pool must be sized to support both functions in the system.

176.7 Glossary

Term	Description
DPT	Dynamic Packet Trunk
PktMA	Packet Media Anchor

177: Functional Description (FN) A00014049

177.1 Feature name and Feature ID

A00014049: GWC and SESM support for AAL2-G726-32 codec in IP Network

177.2 Description

This Corrective CAF activity enables the Gateway Controller and SESM to support the new codec AAL2-G726-32 in the SN09.1 Release. This activity also modifies SESM provisioning rules for IP network profiles.

The AAL2-G726-32 codec can be provisioned in the SESM GUI for IP network profiles only. To facilitate rapid deployment, the AAL2-G726-32 codec is replacing the ILBC codec in codec lists on SESM and GWC. ILBC codec is removed from codec lists from SN09FF onward.

From SN09.1 release onward, an IP network codec profile list will consist of 2 or 3 valid IP codecs, one of which MUST be PCMU or PCMA codec.

177.3 Hardware Requirements or Dependencies

VSP3 and VSP3-o cards support AAL2-G726-32 codec and the prior versions of VSP cards are not compatible with this SN09.1 functionality.

177.4 Software Requirements or Dependencies

For the integrated functionality in CS2K, the PVG image which supports AAL2-G726-32 codec is required.

177.5 Limitations and restrictions

This activity removes the existing iLBC codec and introducesAAL2-G726-32 codec in Gateway Controller and SESM. Hence in SN09.1 release, iLBC codec will not be available for network provisioning.

Note: The AAL2-G726-32 codec support will be patched back to SN08 and SN09 Gateway Controller releases. Till the Gateway Controller patches are available, the Gateway Controller will interpret AAL2-G726-32 codec provisioned in SESM as iLBC.

177.6 Interactions

None.

177.7 Glossary

Term	Description
AAL2	ATM Adaptation Layer-2
ATM	Asynchronous Transfer Mode
CAF	Content Application Form
CS2K	Call Sever 2000.
FN	Functional Description
GWC	Gateway Controller
iLBC	internet Low Bitrate Codec
PVG	Passport Voice Gateway
SAM21	Services Application Module (21 slots)
SESM	Succession Element and Sub-Element Manager

178: CR Description Q01333369

178.1 Applicable Solution(s)

This applies to a CS2K running SN09FF having GWCs with one or more TGCP gateways provisioned.

178.2 Description

Toggling of T.38 from “OFF” to “ON / LOOSE”, OR from “ON/LOOSE” to “OFF” in the “Network Codec Profile” using CMT, will trigger a GW capabilities audit on all ENABLED TGCP gateways.

The gateways’ response to the GW capabilities audit will be used to update a GWC’s knowledge of gateways’ capabilities (including the TGCP packages supported on the gateways). The GWC will not include T.38 codec-options nor monitor for T.38 events in further TGCP messages if the gateways’ response doesn’t include the FXR package.

178.3 Limitations and restrictions

Craftspersons need to take specific care while deactivating T.38 in the “Network Codec Profile”. They must ensure that T.38 has been deactivated on all provisioned TGCP gateways before deactivating it on CS2K. An outage could be caused if this order of deactivating T.38 is not followed.

Note that the outage caused by the deactivation procedure is due to limitations set by T.38 specifications; that is:

- the dynamic nature in which the GW can alter its capabilities (i.e., in-service upgrades, toggling of T.38 support within the gateway EM)
- it is necessary for the GWC to discover the capabilities of the GW.
- if the GW receives a request for T.38 and it is not enabled on the GW, that request must be NACKed.

Fault Management List (FMs)

Introduction

This chapter describes impacts to fault management, such as logs and alarms, for the features planned for this release. Only those features with fault-management impacts are listed.

Featid	Title
A00007544	NCAS Link and SIP NMS Support based on RFC 3842
A00007547	SIP Lines Core Call Processing Support
A00007703	SDM/CBM Log Capacity & Robustness
A00007814.V2	REX testing for MG9000 (Media Gateway 9000) from Element Manager
A00008740	SN09 Clock Sync Robustness
A00009012.AA10	TOPS OSSAIN Service Enhancements
A00009013.AA09	TOPS announcements via UAS/AMS
A00009227	NPM Robustness
A00009235.AA09	TLS for SIP
A00009280.V3	MG9K Line Circuit Enhancements
A00009282	Emergency Stand Alone (ESA) Multiple Level Precedence and Preemption (MLPP) for MG9KEM
A00009315	Alarm Logging Failure
A00009353.AA10	GWC Unit Availability/ Health Monitoring

A00009470.AA09	SuperNode Data Manager (SDM) to support Security Assertion Markup Language (SAML) NSSwitch client
A00009515.AA14	Out-of-Band Interop with MCS
A00009532	Support host to host tunnels for all northbound OSS connections
A00009610	IEMS Calix Integration
A00009611	IEMS Keymile Integration
A00009614	Tamper-proof Key Storage and Event Generation
A00009777	IEMS Mediant 2000 Integration
A00009822	General Security Log When the User Logs Out
A00009893	Session Server Call Processing Overload
A00011827.AB14	GWC Autonomous SWACT
A00012183	Public Key Manager
A00012199	MG9K EM CPR Robustness
A00012326.AA03	SIP Lines: Authentication and Authorization
A00012403.AA08	Data Protection for SIP Lines
A00012526.AA12	TDM Call Recording Feature
A00012622	Platform HW Alarm Reporting
A00012735.AA13	Session Server Fault Handling Enhancements
A00012905	ERS8600 Alarm Mapping Correction in IEMS

1: Fault Management (FM): A00007544

1.1 Feature Name

NCAS Link and SIP NMS Support based on RFC 3842

1.2 Fault management strategy

The fault management information is provided using LOGs. The LOGUTIL CI provide the access to the LOGs generated by MWT and NMS software. The LOG are generated based on LOG framework. This feature uses the existing framework to add new LOGs in MWT and NMS software.

1.3 Fault management tools and utilities

1.3.1 Faults, Alarms and Logs

The LOGUTIL CI command is used as tools in the CS2K Core software. All existing tools and utilities are applicable in case of CS2K Core software.

The LOG generated in the GWC are passed to the CS2K Core via maintenance logs. Therefore, they are also available as part of the CS2K Core tools and utilities.
The Session Server (NGSS) LOGs are independent and uses the new mechanism to pass the LOG information to the remote system. The existing LOG tools and utilities are used in the NGSS.

1.4 Logs (For CS2K only)

The following Logs are aded in DMS/C22K Core as part of this activity:

- NMSS115: It is generated if an error occurs while sending NMS TCAP messages to SCTP
- NMSS116: It is generated if an erro occurs while receiving NMS TCAP messages from SCTP
- NMSS117: It is generated if an error occurs while sending NMS REJ messages to SCTP

- NMSS118: It is generated if an eror occurs while receiving NMS REJ messages from SCTP.

1.5 Log Title/Log ID: NMSS115

1.5.1 Formats

<Switch ID> NMSS115 <DATE> <TIME> INFO
SCTPNMS_ERR_SNT_REPORT

Error occured while sending NMS messages over SCTP.

Example:

RSNN08AZ NMSS115 NOV25 09:40:46 0800 INFO SCTPNMS_ERR_SNT_REPORT

Error occured while sending NMS messages over SCTP.

1.5.1.1 NTSTD

Not Applicable

1.5.1.2 SCC2

Not Applicable

1.5.1.3 Syslog

Not Applicable

1.5.1.4 SNMP

Not Applicable

Table 1: NTSTD/SCC2 Optional Header Fields

Field Name	Used (Y/N)	Value	Fixed/ Variable	type	size	Description
Event Label						
Equipment ID						

Table 2: Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Location:				
Notification Id:				
State:				
Category:				
Cause:				
Time:				
Component Id:				
Specific Problem:				
Description:				
Fabric				
Frame Location				

1.5.1.5 Integrated Element Manager GUI Fields

For each new log, populate the following table with the values displayed in the IEMS Alarm Manager GUI. (Non-legacy logs only).

Table 3: IEMS Alarm GUI Field descriptions

Field	Value
Category	
Severity	
LogName	
LogNumber	
EventType	
EventLabel	
ProbableCause	*see*
SpecificProblem	
BodyText	

1.5.2 Explanation

Description: This log is generated in association with a OM PEG. It provides information regarding a problem in sending Non-CallP messages to the SCTP. When this log is generated, it indicates that the MWI service is broken for a subscriber in the SCTP.

1.5.3 Field descriptions

There are no fileds in the log. The string is self explanatory.

Table 4: Field descriptions

Field	Value	Description

1.5.4 Action

1.5.5 Associated Operational Measurements or Performance Measurements

This log is generated when the SCTPNMSS OM is not pegged.

1.5.6 Additional information

N/A

1.6 Log Title/Log ID: NMSS116

1.6.1 Formats

<Switch ID> NMSS116 <DATE> <TIME> INFO SCTPNMS_ERR_RCV_REPORT

Error occured while receiving NMS messages over SCTP.

Example:

RSNN08AZ NMSS116 NOV25 09:41:25 0800 INFO SCTPNMS_ERR_RCV_REPORT

Error occured while receiving NMS messages over SCTP.

1.6.1.1 NTSTD

Not Applicable

1.6.1.2 SCC2

Not Applicable

1.6.1.3 Syslog

Not Applicable

1.6.1.4 SNMP

Not Applicable

Table 5: NTSTD/SCC2 Optional Header Fields

Field Name	Used (Y/N)	Value	Fixed/ Variable	type	size	Description
Event Label						
Equipment ID						

Table 6: Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Location:				
Notification Id:				
State:				
Category:				
Cause:				
Time:				
Component Id:				
Specific Problem:				
Description:				
Fabric				

Table 6: Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Frame Location				

1.6.1.5 Integrated Element Manager GUI Fields

For each new log, populate the following table with the values displayed in the IEMS Alarm Manager GUI. (Non-legacy logs only).

Table 7: IEMS Alarm GUI Field descriptions

Field	Value
Category	
Severity	
LogName	
LogNumber	
EventType	
EventLabel	
ProbableCause	*see*
SpecificProblem	
BodyText	

1.6.2 Explanation

Description: This log is generated in association with a OM PEG. It provides information regarding a problem in receiving Non-CallP messages from the SCTP. When this log is generated, it indicates that the MWI service is broken for a subscriber in the CS2K. The NMS TCAP message received is corrupted.

1.6.3 Field descriptions

There are no fileds in the log. The string is self explanatory.

Table 8: Field descriptions

Field	Value	Description

1.6.4 Action

1.6.5 Associated Operational Measurements or Performance Measurements

This log is generated when the SCTPNMSR OM is not pegged.

1.6.6 Additional information

N/A

1.7 Log Title/Log ID: NMSS117

1.7.1 Formats

<Switch ID> NMSS117 <DATE> <TIME> INFO SCTPREJ_ERR_SNT_REPORT

Error occured while sending REJ messages over SCTP.

Example:

RSNN08AZ NMSS117 NOV25 09:45:23 0800 INFO SCTPREJ_ERR_SNT_REPORT

Error occured while sending REJ messages over SCTP.

1.7.1.1 NTSTD

Not Applicable

1.7.1.2 SCC2

Not Applicable

1.7.1.3 Syslog

Not Applicable

1.7.1.4 SNMP

Not Applicable

Table 9: NTSTD/SCC2 Optional Header Fields

Field Name	Used (Y/N)	Value	Fixed/ Variable	type	size	Description
Event Label						
Equipment ID						

Table 10: Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Location:				
Notification Id:				
State:				
Category:				
Cause:				
Time:				
Component Id:				
Specific Problem:				
Description:				
Fabric				
Frame Location				

1.7.1.5 Integrated Element Manager GUI Fields

For each new log, populate the following table with the values displayed in the IEMS Alarm Manager GUI. (Non-legacy logs only).

Table 11: IEMS Alarm GUI Field descriptions

Field	Value
Category	
Severity	

Table 11: IEMS Alarm GUI Field descriptions

Field	Value
LogName	
LogNumber	
EventType	
EventLabel	
ProbableCause	*see*
SpecificProblem	
BodyText	

1.7.2 Explanation

Description: This log is generated in association with a OM PEG. It provides information regarding a problem in sending Non-CallP messages to the SCTP. When this log is generated, it indicates that the MWI service is broken for a subscriber in the SCTP.

1.7.3 Field descriptions

There are no fileds in the log. The string is self explanatory.

Table 12: Field descriptions

Field	Value	Description

1.7.4 Action

1.7.5 Associated Operational Measurements or Performance Measurements

This log is generated when the SCTPREJS OM is not pegged.

1.7.6 Additional information

N/A

1.8 Log Title/Log ID: NMSS118

1.8.1 Formats

<Switch ID> NMSS118 <DATE> <TIME> INFO
SCTPREJ_ERR_RCV_REPORT

Error occured while sending NMS messages over SCTP.

Example:

RSNN08AZ NMSS118 NOV25 09:47:26 0800 INFO SCTPREJ_ERR_RCV_REPORT

Error occured while receiving REJ messages over SCTP.

1.8.1.1 NTSTD

Not Applicable

1.8.1.2 SCC2

Not Applicable

1.8.1.3 Syslog

Not Applicable

1.8.1.4 SNMP

Not Applicable

Table 13: NTSTD/SCC2 Optional Header Fields

Field Name	Used (Y/N)	Value	Fixed/ Variable	type	size	Description
Event Label						
Equipment ID						

Table 14: Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Location:				
Notification Id:				
State:				
Category:				
Cause:				
Time:				
Component Id:				
Specific Problem:				
Description:				
Fabric				
Frame Location				

1.8.1.5 Integrated Element Manager GUI Fields

For each new log, populate the following table with the values displayed in the IEMS Alarm Manager GUI. (Non-legacy logs only).

Table 15: IEMS Alarm GUI Field descriptions

Field	Value
Category	
Severity	
LogName	
LogNumber	
EventType	
EventLabel	
ProbableCause	*see*
SpecificProblem	
BodyText	

1.8.2 Explanation

Description: This log is generated in association with a OM PEG. It provides information regarding a problem in sending Non-CallP messages to the SCTP. When this log is generated, it indicates that the MWI service is broken for a subscriber in the CS2K.The REJECT message received is corrupted.

1.8.3 Field descriptions

There are no fileds in the log. The string is self explanatory.

Table 16: Field descriptions

Field	Value	Description

1.8.4 Action

1.8.5 Associated Operational Measurements or Performance Measurements

This log is generated when the SCTPREJR OM is not pegged.

1.8.6 Additional information

N/A

1.8.6.1 Integrated Element Manager GUI Fields

For each new log, populate the following table with the values displayed in the IEMS Alarm Manager GUI. (Non-legacy logs only).

Table 17: IEMS Alarm GUI Field descriptions

Field	Value
Category	
Severity	
LogName	
LogNumber	
EventType	
EventLabel	
ProbableCause	*see*

Table 17: IEMS Alarm GUI Field descriptions

Field	Value
SpecificProblem	
BodyText	

1.8.7 Explanation

Description: This log is generated in association with a OM PEG. It provides information regarding a problem in sending Non-CallP messages to the SCTP. When this log is generated, it indicates that the MWI service is broken for a subscriber in the the CS2K. The REJECT message received is corrupted.

1.8.8 Field descriptions

There are no fileds in the log. The string is self explanatory.

Table 18: Field descriptions

Field	Value	Description

1.8.9 Action

1.8.10 Associated Operational Measurements or Performance Measurements

This log is generated when the SCTPREJR OM is not pegged.

1.8.11 Additional information

N/A

1.9 Logs (For NGSS only)

The following logs are added on NGSS as a part of this activity. These logs can be viewed using the NGSS web interface.

1 NCAS601 : This log is raised when a new NCAS Link is created.

2. NCAS325 : This log is generated when an alarm is generated when the NCAS Link goes down.It is also generated when the alarm is cleared when the NCAS Link comes up.

1.10 Log Title/Log ID: NCAS601

1.10.1 Formats

<MMM dd hh:mm:ss> <device name> <prog name>: <Log Name> <alarm value> <event type><label><text format>

<MMM dd hh:mm:ss> : Current date and time.

<device name> : The name assigned to the session server.

<prog name> : The name of the program that generates the log.

<Log Name> : Log Name - NCAS601

<alarm value> : None

<event type> : INFO

<label> : NCAS Link created

<text format> : A new SCTP connection -LINK1 has been established between SCPLite and the core

Here LINK1 is the name given to the new NCAS Link created.

Example:
Feb 7 08:54:56 rtptngss0-1 a.out: NCAS601 NONE INFO NCAS Link Created A new SCTP connection -LINK1 has been established between SCPLite and the core

1.10.1.1 NTSTD

Not Applicable

1.10.1.2 SCC2

Not Applicable

1.10.1.3 Syslog

Not Applicable

1.10.1.4 SNMP

Not Applicable

Table 19: NTSTD/SCC2 Optional Header Fields

Field Name	Used (Y/N)	Value	Fixed/ Variable	type	size	Description
Event Label						
Equipment ID						

Table 20: Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Location:				
Notification Id:				
State:				
Category:				
Cause:				
Time:				
Component Id:				
Specific Problem:				
Description:				
Fabric				
Frame Location				

1.10.1.5 Integrated Element Manager GUI Fields

For each new log, populate the following table with the values displayed in the IEMS Alarm Manager GUI. (Non-legacy logs only).

Table 21: IEMS Alarm GUI Field descriptions

Field	Value
Category	Customer Logs
Severity	NONE

Table 21: IEMS Alarm GUI Field descriptions

Field	Value
LogName	NCAS
LogNumber	601
EventType	INFO
EventLabel	NCAS link created
ProbableCause	
SpecificProblem	
BodyText	A new SCTP connection -LINK1 has been established between SCPLite and the core

1.10.2 Explanation

Description:This log is generated when a new NCAS Link is created.

1.10.3 Field descriptions

There are no fileds in the log. The string is self explanatory.

Table 22: Field descriptions

Field	Value	Description

1.10.4 Action

None.

1.10.5 Associated Operational Measurements or Performance Measurements

N/A.

1.10.6 Additional information

N/A

1.11 Alarms

The new alarms will be added in the NGSS for the SCTP link between NGSS and CM. The alarm NCAS325 is raised when the NCAS Link connection is lost. .

1.11.1 Integrated Element Manager GUI Fields

For each new log, populate the following table with the values displayed in the IEMS Alarm Manager GUI. (Non-legacy logs only).

Table 23: IEMS Alarm GUI Field descriptions

Field	Value
Severity	CRIT
Category	Communications
LogName	NCAS
LogNumber	325
EventType	TBL
EventLabel	NCAS Link Down
ProbableCause	outOfService
SpecificProblem	NCAS Link Connection between the core and Scplite is lost
BodyText	SCTP connection -LinkName between SCPLite and the core is lost

1.11.2 SNMP Northbound Alarm Event (Non-legacy logs only)

Table 24: Alarm Trap Field descriptions

Field	Value
nnExtAlarmActiveSequenceNumber	this field is defined by the system and not specific to this alarm
alarmActiveResourceDescription	
nnExtAlarmActiveEventType	<M3100 Event Type>
alarmActiveDescription	
alarmActiveDateAndTime	this field is defined by the system and not specific to this alarm
nnExtAlarmActiveProbableCause	<M3100 Probable Cause>
nnExtAlarmActiveAdditionalText	
alarmActiveResourceId	this field is defined by the system and not specific to this alarm

1.11.3 Explanation

Description: NCAS325 Alarm is raised when the SCTP connection between the SCPLite and the core is lost.. When the alarm is raised an NCAS325 log is generated and can be found in the customer logs.Severity: Critical

1.11.4 Action

The SCTP Connection between the SCPLite and the core has to be restored.

1.11.5 Corresponding Clear Log

Log Title: NCAS325 - SCTP Connection Restored.

This log is generated when the NCAS Link down trouble alarm is lowered.

1.11.5.1 Format

<Date> <Time> <DeviceName> alarmd: NCAS325 <AlarmSeverity> TBL NCAS Link Down: <DeviceInfo> <AlarmRaiseLowerText>

<Date> : Current Date

<Time> : Current Time

<DeviceName> : The name assigned to the session server.

<AlarmSeverity>: The current severity of the alarm.

CRIT

NONE

<DeviceInfo> : Info which specifies the device to which the alarm pertains

<AlarmRaiseLowerText> :

SCTP Connection between SCPLite and core is lost

SCTP Connection between SCPLite and core is lost - Alarm Cleared

Feb 7 08:55:06 rtptngss0-1 alarmd: NCAS206 NONE TBL NCAS Link NCGL=rtptngss0-1;Unit=1;SCTP Connection Link1 between the SCPLite and core is lost - Alarm cleared

1.11.5.2 NTSTD

1.11.5.3 SCC2

1.11.5.4 Syslog

1.11.5.5 SNMP

Table 25: NTSTD/SCC2 Optional Header Fields

Field Name	Used (Y/N)	Value	Fixed/ Variable	type	size	Description
Event Label		*NCAS Link Down*				
Equipment ID						

Table 26: Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Location:				
Notification Id:				
State:				
Category:		*Communication*		
Cause:		*outOfService*		
Time:				
Component Id:		*NCAS*		
Specific Problem:		*NCAS Link Connection between the core and Scplite is lost*		
Description:		*SCTP Connection Link1 between the SCPLite and core is lost - Alarm cleared*		
Fabric				

Table 26: Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Frame Location				

1.12 Related documentation

Appropriate NTP contains the details of various existing logs.

2: Fault Management (FM): A00007547

2.1 Feature Name

SIP Lines Core Call Processing Support

2.2 Fault management strategy

Logs are used for fault management.

2.3 Fault management tools and utilities

Not applicable

2.3.1 Faults, Alarms and Logs

2.4 Logs

DPL100

DPL101

2.4.1 Formats

Note:

2.4.1.1 NTSTD

Examples:

```
RTPF08BZ   DPL100 SEP21 07:30:32 0301 INFO DPL FREE QUEUE REBUILD START
RTPF08BZ   DPL101 SEP21 07:30:33 0302 INFO DPL FREE QUEUE REBUILD FINISH
```

There is no variable text in the log body in all these logs

2.4.1.2 SCC2

2.4.1.3 Syslog

2.4.1.4 SNMP

2.4.2 Associated Operational Measurements or Performance Measurements

2.4.3 Additional information

2.5 Alarms

2.6 Related documentation

3: Fault Management (FM): A00007703

3.1 Feature Name

SDM/CBM Log Capacity & Robustness

3.2 Fault management strategy

The fault management strategy for A00007703 (Log Capacity Enhancements) shall be consistant with the existing fault management in the LOGDEV system. No new logs or alarms will be introduced. Where necessary, SWERs may be used to alert users to error conditions that cannot be addressed via software or which can be addressed via software but which should also be communicated to support staff for debugging and troubleshooting purposes.

3.3 Fault management tools and utilities

Not applicable.

3.4 Faults, Alarms and Logs

Not applicable -- no new alarms or logs are introduced as part of A00007703.

3.5 Logs

Not applicable -- no logs will be introduced or changed by this feature.

3.6 Alarms

Not applicable -- no alarms will be introduced or changed by this feature.

3.7 Related documentation

None.

4: Fault Management (FM): A00007814

4.1 Feature Name

REX testing for MG9000 (Media Gateway 9000) from Element Manager

4.2 Fault management strategy

There are no faults generated by this feature.

4.3 Fault management tools and utilities

This feature generates the customer logs.

4.4 Logs

4.4.1 Log Title/Log ID: REX 600

4.4.1.1 Formats

REX Start/Completed log:

MSH10_I06BR REX600 JUN5 14:12:56 2164 INFO MG9K Card REX LOG NOTIFICATION
NE Number: 2 NE Name: HS9K
Card.frame0.shelf3.slot15.ITX REX completed on:
Time: Thu Jun 05 14:12:56 EDT 2003

4.4.1.2 Explanation

Description: Log report REX600 indicates the start or completion of REX on a card/card-pair. The cards under consideration are ITP, ITX and DCC.

4.4.1.3 Field Descriptions

This log report has no selected fields.

4.4.1.4 Action

None

4.4.1.5 Associated Operational Measurements or Performance Measurements

None

4.4.1.6 Additional information

None

4.4.2 Log Title/Log ID: REX 601

4.4.2.1 Formats

REX Success/Failure log:

MSH10_I06BR REX601 JUN5 14:12:56 2164 INFO MG9K Card REX LOG NOTIFICATION
NE Number: 2 NE Name: HS9K
Card.frame0.shelf3.slot15.ITX REX successful on:
Time: Thu Jun 05 14:12:56 EDT 2003

4.4.2.2 Explanation

Description: Log report REX601 indicates the success or failure of REX on a card/card-pair. The cards under consideration are ITP, ITX and DCC.

4.4.2.3 Field Descriptions

This log report has no selected fields.

4.4.2.4 Action

None

4.4.2.5 Associated Operational Measurements or Performance Measurements

None

4.4.2.6 Additional information

REX601 is generated for the failure conditions also. When the diagnostics of the card fails, REX is failed for the card under consideration.

4.4.3 Log Title/Log ID: REX 602

4.4.3.1 Formats

REX Skipped log:
MSH10_I06BR REX602 JUN5 14:12:56 2164 INFO MG9K Card REX LOG NOTIFICATION
NE Number: 2 NE Name: HS9K
Card.frame0.shelf3.slot15.ITX REX skipped on:
Time: Thu Jun 05 14:12:56 EDT 2003

4.4.3.2 Explanation

Description: Log report REX602 indicates that the REX for the card/card-pair under consideration has been skipped. The card types considered are ITP, ITX and DCC.

4.4.3.3 Field Descriptions

This log report has no selected fields.

4.4.3.4 Action

None

4.4.3.5 Associated Operational Measurements or Performance Measurements

None

4.4.3.6 Additional information

Various reasons for which REX is skipped on a card/card-pair are:

1. Unable to SWACT the card.

2. In the case of a card-pair if the REX on inactive card fails, REX for the card-pair is skipped.

3. If the duration for REX specified by the user exceeds, REX for the card/card-pair is skipped.

4.5 Alarms

NA

5: Fault Management (FM): A00008740

5.1 Feature Name

SN09 Clock Sync Robustness

5.2 Fault management strategy

Six new alarms are defined for the MG9000 ABI circuit pack by this feature. These alarms will be reported from the ABI to the DCC and subsequently to the MG9000 Element Manager is the normal way.

5.3 Fault management tools and utilities

5.3.1 Fault, Alarms, and Logs

5.4 Logs

A new MG9K ABI footprint log will be created by this feature. The purpose of the log is to capture the pertinent clock sync data that occurs during an unusual clock sync event. This data is only useful in determining if clock event were associated with XPM DS512 link closure that may have lead to an outage. This data would not be viewed by the customer for analysis. The only users of this data would be Nortel design team and possibly field support personnel.

A new MG9K ABI aer buffer is defined for capturing additional data not covered by the footprint log.

5.4.1 Formats

An example of the new footprint log is listed below:

```
CLKR643  ABI clock registers   DEC-17  14:41:39.850
 INDXCLK  DACV   ABS    REL    512    Slew   Msg    Linear Phase  Target ITP512
          ERROR  PHASE  PHASE  TX/RX  rate   links  mode   diff   phase  Rxphase
    4     0      d72    acc    1      6f4    11     3      3      1ffe   acc    6f3
    5     0      d75    acb    1fff   6f4    11     3      3      2      acc    6f3
    6     0      d75    acb    1fff   6f3    11     3      3      2      acc    6f3
    7     0      d75    acb    1fff   6f3    11     3      3      2      acc    6f3
    8     0      d75    acb    1fff   6f4    11     3      3      2      acc    6f3
    9     0      d75    acb    1fff   6f3    11     3      3      0      acc    6f2
    10    0      d72    acc    1      6f4    11     3      3      1ffe   acc    6f3
    114   d72    acc    1      6f4    11     3      3      1ffe   acc    6f3
    12    4      d75    acb    1fff   6f4    11     3      3      2      acc    6f3
    13    4      d75    acb    1fff   6f3    11     3      3      2      acc    6f3
    14    4      d75    acb    1fff   6f3    11     3      3      2      acc    6f3
    15    4      d75    acb    1fff   6f4    11     3      3      2      acc    6f3
```

0	4	d75	acb	1fff	6f3	11	3	3	0	acc	6f2
1	0	d72	acc	1	6f4	11	3	3	1ffe	acc	6f3
20	d75	acb	1fff	6f4	11	3	3	2	acc	6f3	
3	0	d75	acb	1fff	6f3	11	3	3	0	acc	6f2

An example of the new aer buffer is listed below. The contents of the buffer can be accessed by using the following dSH command on the Mg9000 ABI card

/aer/display clksync

Date	Time	CLK ERROR	DACV	ABS PHASE	REL PHASE	512 TX/RX	Slew rate	Msg links	Linear Phase mode	Phase diff	Target phase	ITP512 Rxphase
12/27/1990	00:00:00.430	0	c64	ac7	1ffc	3c9	11	0	3	0	acb	3ca
12/27/1990	00:00:00.930	0	c67	ac9	1ffe	3ca	11	0	3	1	acb	3cb
2/ 7/2005	10:36:57.850	4	c67	aca	1fff	3ca	11	0	3	1ffe	acb	3ca
2/ 7/2005	10:37:22.850	0	c71	acb	1	3cb	11	0	3	0	acb	3cb

5.4.2 Explanation

See DSUM section of this document a better explaination of the content of these logs.

5.4.3 Field descriptions

The data fields listed in the footprint and aer logs are essentially the same except the aer buffer log contains a time stamp of when a specific field exceeded its allowable data range. The data collected is the raw data contained in hardware registers on the ABI Vazaelle Field Programmable Gate Array (FPGA). The meaning of these register values is too detailed to address here and this data is only intended for the Nortel design team.

5.4.4 Action

No action is required by any customer, craft or field support personnel based on these logs. This data will be gathered and analyzed by the design team as needed to determine the root cause of any system outage.

5.4.5 Associated Operational Measurements or Performance Measurements

5.4.6 Additional information

5.5 Alarms

Six new alarms are defined for the MG9000 ABI circuit pack by this feature. These alarms will be reported from the ABI to the DCC and subsequently to the MG9000 Element Manager is the normal way.

Maj This alarm should clear within a few seconds, if this alarm is in a steady alarm condition then it indicates that the ITPs or ABI card should be replaced.

Maj

This alarm should clear within a few seconds, if this alarm is in a steady alarm condition then it indicates that the ITPs or ABI card should be replaced.

This alarm should only occur during brief periods of maintenance actions and should clear on it own. If this alarm is in a steady alarm condition then it indicates that the indicated ITP card should be replaced.

This alarm should only occur during brief periods of maintenance actions and should clear on it own. If this alarm is in a steady alarm condition then it indicates that the indicated ITP card should be replaced.Major

If this alarm occurs it indicates that both ITPs in the shelf are having clock issues and immediate analysis into the ITP alarms should be undertaken.Critical

5.5.1 Integrated Element Management GUI fields

The MG9000 Element Manager will report these six alarms in its Alarm Browser in the standard manner.

FM_List Int'l-SN09.fm

6: Fault Management (FM): A00009012

6.1 Feature Name

TOPS OSSAIN Service Enhancements

6.2 Fault management strategy

Not applicable.

6.3 Fault management tools and utilities

Not applicable

6.4 Logs

Log Title/Log ID: TEOL100

6.4.1 Formats

If OSSAIN Broadcast Announcements were used during a week, a TEOL100 log will be generated at midnight the following Sunday with the "OSSAIN Broadcast Announcements" functionality listed (other functionality may also be listed). For example:

```
TEOL100 mmdd hh:mm:ss ssdd INFO TOPS End Of Life Notification
  Use of functionality scheduled for removal:
    Functionality Used                  Scheduled Removal
    ------------------                  ---------------------
    OSSAIN Broadcast Announcements          SN10
```

6.4.2 Explanation

Description: A TEOL100 log identifies functionality no longer supported in an upcoming load. A log is generated only when a functionality is used while scheduled for removal within 3 releases. All such functionalities used in the previous week are listed in that week's EOL log.

6.4.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
Functionality Used	OSSAIN Broadcast Announcements	This field identifies the functionality that is scheduled for removal yet is being used.

Table 1 Field descriptions

Field	Value	Description
Schedule Removal	SN10	This field identifies the release in which the functionality is scheduled to be removed.

6.4.4 Action

If there is a plan in place to transition off of the identified functionality prior to upgrading to the identified release (or beyond), then the notification logs can be ignored. If there is no such plan in place, then the next level of support should be contacted to initiate an appropriate transition plan.

6.4.5 Additional information

The log indicates only that the functionality was used one or more times in the previous week. It does not indicate when the functionality was used (i.e. the time of the log itself is not at all related to the time of the usage), nor does it indicate the number of times it was used.

Log Title/Log ID: OAIN306

6.4.6 Formats

OAIN306 is generated to indicate a call routed to treatment because too many DA recalls have already been performed and the call was attempting to go to yet another DARECALL function.

Figure 1 Example log report for OAIN306

```
OAIN306 FEB28 07:46:17 8701 INFO TRMT: MAX DA RECALLS REACHED
CALLID: 0302 0011
FUNCTION: DA_RECALL
CALLING: CKT T907TI00 1
```

6.4.7 Explanation

Description: A call routed to treatment because it was routed to a function with DARECALL setup and too many DA recalls had already been processed.

6.4.8 Field descriptions

Table 2 Field descriptions

Field	Description
CALLID	Call ID of the call
FUNCTION	Function the call was routing to when it failed and routed to treatment instead.

6.4.9 Action

Check table VROPT maximum_da_recalls to ensure count is as desired. Note this will include TOPS operator DA recalls also.

Check table OAFUNDEF to ensure the function datafill DARECALL is set as desired.

Change transfer or trigger information to route to different function.

Maintain a count in context block to route appropriately.

Log Title/Log ID: OAIN301

6.4.10 Formats

OAIN301 is generated to indicate a service change over a SN transition did not happen because of an error. Errors can include called party attached and call orig of country direct.

Figure 2 Example log report for OAIN301

```
OAIN301 FEB28 07:46:17 8701 TBL OSSAIN RESOURCE PROBLEM
CALLID: 0302 0011
TROUBLE: SERVICE CHANGE FAILED
```

6.4.11 Explanation

Description: Service change attempt over transition to SN failed because called party attached or call origination is country direct.

6.4.12 Field descriptions

Table 3 Field descriptions

Field	Description
CALLID	Call ID of the call

6.4.13 Action

SN needs to release called party and then request service change via OAP.

6.5 Alarms

Not applicable.

6.6 Related documentation

A00009012 - TOPS OSSAIN Service Enhancements

7: Fault Management (FM): A00009013

7.1 Feature Name

TOPS announcements via UAS/AMS

7.2 Fault management strategy

This activity does not introduce any new element for which a fault management strategy is needed. It adheres to the existing fault management strategy for Succession announcements and for TOPS.

7.3 Fault management tools and utilities

Existing fault management tools and utilities for Succession announcements apply to the announcements for this activity.

7.3.1 Faults, Alarms and Logs

This activity makes minor changes in two existing legacy DMS logs.

7.4 Log: TOPS113

Log Title/Log ID: TOPS113

This is an existing legacy DMS log, documented in Log Report Reference Manual. The log can also be generated by the CS 2000 CM. This feature changes the fixed string in the Event Label field. This activity changes that string from

```
TOPS DRAM PLAY TRBL
```

to

```
ANNOUNCEMENT PLAY TRBL
```

7.4.1 Formats

7.4.1.1 NTSTD

Format:

```
<Office Id>     TOPS113 <MMMDD hh:mm:ss> <seq #> INFO ANNOUNCEMENT PLAY TRBL
        CKT <trkid>
        CHECK FOR INCOMPLETE DATAFILL IN TABLE ANNPHLST
```

Example:

```
RTPC09AZ     TOPS113 JAN03 01:16:53 7985 INFO ANNOUNCEMENT PLAY TRBL
        CKT         TOPCOMAMF 0
        CHECK FOR INCOMPLETE DATAFILL IN TABLE ANNPHLST
```

7.4.1.2 SCC2

Standard for CM.

7.4.1.3 Syslog

N/A

7.4.1.4 SNMP

N/A

7.4.1.5 Integrated Element Manager GUI Fields

N/A

7.4.2 Explanation

Unchanged.

7.4.3 Field descriptions

Unchanged.

7.4.4 Action

Unchanged.

7.4.5 Associated Operational Measurements or Performance Measurements

Unchanged.

7.4.6 Additional information

In SN06 the last line of the log body was changed from

```
CHECK FOR INCOMPLETE DATAFILL IN TABLE DRMUSERS
```

to

```
CHECK FOR INCOMPLETE DATAFILL IN TABLE ANNPHLST
```

This was done under a CR and was not documented in NTPs. The reason for the change was that activity A19013546 introduced table ANNPHLST, which replaced table DRMUSERS. All NTP references to DRMUSERS in the description of this log should be changed to refer to ANNPHLST.

7.5 Log: TOPS104

Log Title/Log ID: TOPS104

This is an existing legacy DMS log, documented in Log Report Reference Manual. The log can also be generated by the CS 2000 CM. The only change made by this activity is in the TROUBLE CODE field.

7.5.1 Formats

7.5.1.1 NTSTD

Format:

```
<Office Id>     TOPS104 <MMMDD hh:mm:ss> <seq #> INFO ACTS TROUBLE
        CKT <trkid1>
        CKT <trkid2> CKT <trkid3> CKT <trkid4>
```

```
INCOMING TRK = CKT <trkid>
OUTGOING TRK = CKT <trkid>
CLGNO = <dn> CLDNO = <dn>
TROUBLE CODE = <trouble text>
```

Example:

```
RTPC09AZ     TOPS104 APR01 12:00:00 2112 INFO ACTS TROUBLE
   CKT         ACTSTOPS 111
   CKT        ACTSTOPS 111 CKT         ACTSTOPS 111 CKT         RCVRCOIN 12
   INCOMING TRK = CKT          LNTOPSI  4
   OUTGOING TRK = CKT          LNTOPSO  4
   CLGNO = 613-621-1002         CLDNO = 212-220-1111
   TROUBLE CODE = MISCELLANEOUS_ACTS_TRBL
```

7.5.1.2 SCC2

Standard for CM.

7.5.1.3 Syslog

N/A

7.5.1.4 SNMP

N/A

7.5.1.5 Integrated Element Manager GUI Fields

N/A

Table 1 NTSTD/SCC2 Optional Header Fields

Field Name	Used (Y/N)	Value	Fixed/ Variable	type	size	Description
Event Label	Y	ACTS TROUBLE	Unchanged; see Log Report Reference Manual.			
Equipment ID	N					

Table 2 Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Other fields are unchanged.				

Table 2 Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
TROUBLE CODE	Y	CDC_DSP1_FAIL CDC_DSP2_FAIL CDC_DSP3_FAIL CDC_RAM_FAIL CDC_ROM_FAIL CDC_TRAP MISCELLANEOUS_ACTS_TRBL MISC_CDC_FAIL MISC_ANNOUNCEMENT_FAIL RECEIVER_SUSPECTED		Indicates the trouble.

7.5.2 Explanation

The Traffic Operator Position System (TOPS) subsystem generates this report when the operator keys “suspect CDC” trouble at the operator position, or when unexpected messages are received from the coin detector circuit (CDC), the digital recorded announcement machine (DRAM) cards, or the packet media server (UAS or MS 2000 Series).

7.5.3 Field descriptions

The TROUBLE CODE field is the only one changed by this activity.

Table 3 Field descriptions

Field	Value	Description
TROUBLE CODE	NO_REPLY_FROM_DRAM	This value can no longer be generated.
TROUBLE CODE	MISC_DRAM_FAIL	This value can no longer be generated.
TROUBLE CODE	MISC_ANNOUNCEMENT_FAIL	Indicates a miscellaneous problem with an announcement used for an ACTS call. Probably an unexpected message has been received from the announcement machine. When this trouble code is generated, the TOPS104 log is most often accompanied by another log that provides more detailed information.
TROUBLE CODE	*other values*	The meaning of the other values is unchanged. See Log Report Reference Manual.

7.5.4 Action

Most often this log indicates a hardware problem, and the action is to diagnose the indicated circuit cards from the MAP (maintenance and administration position) and replace cards if necessary. The first CKT field in the log body is the agent reporting the problem.

If the agent reporting the problem is an ACTS announcement, check for other logs that may accompany this one and may provide more specific information. If the problem cannot be diagnosed using other logs, then check CM table ANNMEMS to determine whether it is a DRAM announcement (HDWTYPE = DRAM) or a packet announcement (HDWTYPE = UAS). Packet announcement members do not correspond to specific hardware circuits. Table ANNMEMS will identify the logical AUD node that was controlling the announcement, and table SERVSINV will associate that AUD node with a Gateway Controller. Follow standard troubleshooting procedures for the media servers that are controlled by that Gateway Controller.

7.5.5 Associated Operational Measurements or Performance Measurements

Unchanged.

7.6 Alarms

N/A

7.7 Related documentation

Log Report Reference Manual.

8: Fault Management (FM): A00009227

8.1 Feature Name

Feature A00009227 - NPM Robustness

8.2 Fault management strategy

The standard MG9K EM Fault Management strategy will apply to the NPM Patch Alarm. The alarm will by displayed by the MG9K EM Alarm Browser, logged in NT standard format to the SSPFS CUST logs and forwarded to northbound OSS.

8.3 Fault management tools and utilities

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

8.4 Logs and Alarms

There will be a single new patch alarm fault raised and cleared by the MG9000 to indicate when a restart is required for a patch on a specific card. The MG9000 will manage both raise and clear actions based on its own patching implementation.

8.4.1 Explanation

8.4.1.1 patchAlarmFault

Title: patchAlarmFault

Name: PATC

Description: This log is generated when a patchAlarmFault is received from an MG9000 DCC card.

Severity: MAJOR

Event Type: Trouble

8.4.2 Format

The Log Delivery application for this feature generates logs in the Number 2 Switch Control Center (SCC2) format and the NT standard (STD) format.

8.4.2.1 patchAlarmFault

PATC 301APR17 09:31:13 1806 TROUBLE MG9K nnPatchAlarm
Location: 8-co8-Frame000.Shelf2.Slot13
Notification Id: 952
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Apr 17 09:31:13 2003
Component Id: Card.frame0.shelf2.slot11.OC3
Specific Problem: Patch Alarm - Patch(es) require a restart primary to instrument changes.
Patch ID: Patch N
Description: Patch(es) require a restart primary to instrument changes
Site Flr RPos Bay_id Cary 02 H02 MG9F 012

8.4.3 Field descriptions

8.4.3.1 Patch Alarm Fault

Table 1 Field descriptions PATC 300

Field	Value	Description
office identification	String	Identifies the switch that generates the log. This field is optional. The maximum length of this field is 12 characters.
alarm	***,**,*, or blank	Indicates the alarm type of the log report. ***=critical, **=major, *=minor, blank = no alarms/warning
threshold	+ or blank	Indicates if a threshold is set for the log report. Plus (+) sign indicates that a threshold was set; if a blank, a threshold was not set.

Table 1 Field descriptions PATC 300

Field	Value	Description
report identification	AAAA nnn	Identifies the log subsystem that generates the report. This field uses 2-4 alphabetical characters and the number 100-999 of the log report in this subsystem. For this log AAAA= MGC and nnn=300.
day	String	Identifies the day of the week.
mmmmdd	January-December (01-31)	Identifies the month and date the report generates.
hh:mm:ss	00-23 00-59 00-59	Identifies the hour, the minute, and the second the report generates.
zone	PST, EST, MST, CST, AST	Identifies the time zone.
yyyy	0000-9999	Year
ssdd	0000-9999	Defines a different sequence number for each log report generated.
event type	TBL, INFO, etc	Trouble, Service Summary, State Change, Information, Threshold and Expert. Threshold for this log.
patch id	String	Patch identification.
event id	String	The Log Title.
NE Number	integer	Number of the NE
NE Name	string	Name of the NE
nnUemgEventTime	DateandTime	The Date and Time the event occurred in the following format: day mmmmdd hh:mm:ss zone yyyy

Table 1 Field descriptions PATC 300

Field	Value	Description
nnUemgAlarmSeverity	String	warning
Description	string	Patch(es) require a restart primary to instrument changes

8.4.4 Action

PATC 301 - Restart primary to instrument changes.

8.4.5 Associated Operational Measurements or Performance Measurements

- None.

8.5 Related documentation

1. NORTEL-PATCHING-MIB - MG9000's Enterprise MIB, contains patching definitions

2. PLOA and SLOA Logs and Alarms for UE9kMG EM (DID) - MG9000s design documentation for logs and alarms on the MG9000 Element Manager.

3. Logs and Alarms Strategy for WUA Components - MG9000 Alarm strategy guide - version 1.4

3. Reliable Alarms and Alarm Robustness Design Intent Document (DID) - MG9000 Element Manager design document.

4. PLOA and SLOA Alarm Forwarding to OSS(DSUM) - MG9000 Alarm forwarding feature.

9: Fault Management (FM): A00009235

9.1 Feature Name

Feature A00009235 - TLS for SIP

9.2 Fault management strategy

The TLS security feature for the SIP Gateway application on the CS2000 Session Server includes new logs and alarms to be defined. This section details the logs and alarms that the TLS security feature has defined.

An alarm monitoring process will be used to compare thresholds values with current operating conditions. As alarmable conditions occur, the process will ensure that the appropriate alarm is raised.

9.3 Fault management tools and utilities

This feature utilizes the current log and alarm display mechanisms in use by the SS-Trunks. There will be new alarms and logs defined, but there will not be any new display mechanisms. Refer the to documented activity (in pls fmdoc) A00003933 (Succession Communication Server (SCS) 2000 - Session Server Manager 2000 - SIP Gateway application) for the overall log and alarm tools and utilities.

This feature generates logs and alarms under the purview of the SIP Gateway application Call Processing. These logs and alarms are only generated and reported on the SIP Gateway application.

They can be viewed via the SIP Gateway Maintenance web browser interface on the Session Server Manager - SIP Gateway application web page. The body of log formats shown in this document are the format for the Session Server logs if viewed from the IEMS (Integrated Element Manager System). Log formats may differ if logs are viewed from the Session Server Web Interface. The content will not differ, just the format and/or the headers.

References to TLS-based logs and alarms not found in this document will be found in the documentation to feature A00006893 in PLS FMDOC.

9.3.1 Faults, Alarms and Logs

9.4 Logs

All logs and associated alarms will have the name start with SIPS (for SIP Security).

The following new logs have been created/modified:

- SIPS608 - TLS Certificate Policy failure (new).
- SIPS609 - Security Parameter Changed (new).
- SIPS604 - TLS Initialization Logs (changed).

The following new alarm related logs have been created/modified:

- SIPS303 - Certificate Mismatch in Server Certificate
- SIPS305 - TLS Initialization Failure (changed from previous release)
- SIPS308 - Failed Certificate Policy Check

9.4.1 SIPS608 - TLS Certificate Policy failure log

9.4.1.1 Formats

9.4.1.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> sipgwyappln: SIPS608 <Severity> <Type> TLS ^M Certificate Policy failure, <IP Address>:<Port>^M

Following are values/explanations of the variable values presented above:

- <Date>: Current date
- <Time>: Current time
- <Severity>: The Severity of the log (MINOR).
- <Type>: The type of log (INFO)
- <DeviceName>: The name assigned to the Session Server
- <IP Address> : The IP address of the remote side of the connection
- <Port> : The port number of the connection

Example:

```
 Mar 2 09:53:57 NGSS sipgwyappln: SIPS608 MINOR INFO TLS Certificate Policy
failure, 172.16.172.104:55263
```

9.4.1.2 Explanation

The SIPS608 log is generated when the remote side of the connection presents a certificate that does not conform to the selected local certificate policy.

9.4.1.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
<DATE>	<Mon> <DD>	Current date when the log occurred.
<Time>	<HH>:<MM>:<SS>	Current time when the log occurred.
<DeviceName>		Name of the session server.
<Severity>	MINOR	Severity level of the log
<Type>	INFO	informational or initialization log.
<IP Address>	<a>.<b>.<c>.<d>	IP address of remote side of connection
<Port>	<xxx>	The Port number of the connection

9.4.1.4 Action

There are two courses of action. The first would be to remove the certificate policy that is preventing the certificate from the Security Parameters Configuration Web Page on the SS-Trunks. The second course of action (and the preferred one) would be to enforce the local certificate policy throughout the network (forcing the Remote SIP Server to present a certificate that conforms to the certificate policy).

See “Certificate Policy Check Failure Alarm” on page 1922 for more details.

9.4.1.5 Associated Operational Measurements or Performance Measurements

None for this log.

9.4.1.6 Additional information

None.

9.4.2 SIPS609 - TLS Security Parameter Changed log

9.4.2.1 Formats

9.4.2.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> sipgwyappln: SIPS609 <Severity> <Type> TLS ^M Security Parameter <SecParmName> updates^M OLD: <OldText>^M NEW: <NewText>

Following are values/explanations of the variable values presented above:

<Date>: Current date

<Time>: Current time

<DeviceName>: The name assigned to the Session Server

<Severity>: The Severity of the log (NONE).

<Type>: The type of log (“TLS”)

<process>: process class that raised the log (either sipgwyappln: or certClass:)

<Unit#>: The unit number assigned (either 0 or 1)

<SecParmName>: One of:

- "MaxTLSSessions",
- "localTLSport",
- "numOfTLSEngines",
- "SessionCachingEnabled",
- "SessionCacheValidDuration",
- "SessionCacheSize",
- "SelfSignedCertificatesAllowed",
- "TLSAllowedCipherSuites",
- "TLSServerCertPath",
- "TLSServerKeyPath",
- "TLSTrustedCertsPath",
- "ThrottleEnabled",
- "ThrottleBurstDurationinSecs",
- "ThrottleSustainedDurationinSecs",
- "ThrottleBurstEventThreshold",
- "ThrottleSustainedEventThreshold",
- "TlsEnabled",

- "ExitOnFailTLSInitialization",
- "RequireLocalCertificatePolicy",
- "RequirekeyUsage",
- "RequireauthorityKeyIdentifier",
- "RequiresubjectKeyIdentifier",
- "RequireprivateKeyUsagePeriod",
- "RequiresubjectAltName",
- "RequireissuerAltName",
- "RequirebasicConstraints",
- "RequireextKeyUsage",
- "AlarmMinimumDisplayTimeMinutes",
- "AlarmThresholdDroppedConnections",
- "AlarmThresholdAuthenticationFailure",
- "AlarmThresholdCertExpiryDays",
- "AlarmThresholdLocalCertificatePolicy"

<OldText>: One of

- For the non-AlarmThreshold logs: “<value>”, where:
  - <value>: the old value of the entry
- For the AlarmThreshold logs: “Minor = <min>, Major = <maj>, Critical = <crit>”, where:
  - <min>: the old minor threshold value
  - <maj>: the old major threshold value
  - <crit>: the old critical threshold value

<NewText>: One of

- For the non-AlarmThreshold logs: “<value>”, where:
  - <value>: the new value of the entry
- For the AlarmThreshold logs: “Minor = <min>, Major = <maj>, Critical = <crit>”, where:
  - <min>: the new minor threshold value
  - <maj>: the new major threshold value
  - <crit>: the new critical threshold value

Example:

```
Mar 11 12:31:12 NGSS sipgwyappln: SIPS609 NONE      TLS Security Parameter
AlarmThresholdAuthenticationFailure updated OLD: Minor = 2, Major = 4, Critical =
6 NEW: Minor = 2, Major = 4, Critical = 5
Mar 11 12:31:37 NGSS sipgwyappln: SIPS609 NONE      TLS Security Parameter
ExitOnFailTLSInitialization updated OLD: 1 NEW: 0
```

9.4.2.2 Explanation

The SIPS609 logs are generated whenever a TLS Security Parameter is changed by the user.

9.4.2.3 Field descriptions

Table 2 Field descriptions

Field	Value	Description
<DATE>	<Mon> <DD>	Current date when the log occurred.
<Time>	<HH>:<MM>:<SS>	Current time when the log occurred.
<DeviceName>		Name of the session server.
<Severity>	CRIT	Severity level of the log
<Type>	“ “	Informational log
<SecParmName>	<SecParmName>	Name of the parameter as seen from the Security Parameters Configuration web page.
<OldText>	<OldText>	The text representation of the old value of the parameter(s)
<NewText>	<NewText>	The text representation of the new value of the parameter(s)

9.4.2.4 Action

None. Informational log only.

9.4.2.5 Associated Operational Measurements or Performance Measurements

None.

9.4.2.6 Additional information

None.

9.4.3 SIPS604: Certificate Information Logs

These logs were originally implemented in SN08. The Certificate Effective Date log is the new content being documented here. Everything else remains the same as in SN08.

9.4.3.1 Formats

9.4.3.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> sipgwyappln: SIPS604 <Severity> <Type> TLS <Log Message>

Following are values/explanations of the variable values presented above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <Severity>: The Severity of the log (NONE).
- <Type>: The type of log (INFO)
- <Log Message>: one of:
  - — none/info: "^M Local Certificate Effective: Year=<YYYY>, Month = <MM>, Day = <DD>^M"
  - — none/info: "^M Local Certificate Expires: Year=<YYYY>, Month = <MM>, Day = <DD>^M"

Examples:

```
Oct  8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS604 NONE INFO TLS ^M    Local
Certificate Effective: Year=2004, Month = 10, Day = 8^M

Oct  8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS604 NONE INFO TLS ^M    Local
Certificate Expires: Year=2005, Month = 10, Day = 8^M
```

9.4.3.2 Explanation

The SIPS604 log is generated twice during the initialization of the Call Processing application (i.e. during the unlock). These logs indicates when the current local certificate will become effective, and when it will expire.

9.4.3.3 Field descriptions

Table 3 Field descriptions

Field	Value	Description
<DATE>	<Mon> <DD>	Current date when the log occurred.

Table 3 Field descriptions

Field	Value	Description
<Time>	<HH>:<MM>:<SS>	Current time when the log occurred.
<DeviceName>		Name of the session server.
<Severity>	NONE	Severity level of the log
<Type>	INFO	informational.
<Log Message>	see bulleted list	Log message text.

9.4.3.4 Action

On an info log, no immediate action is required.

9.4.3.5 Associated Operational Measurements or Performance Measurements

Not applicable to this log.

9.4.3.6 Additional information

None.

9.4.4 SIPS303 - TLS Certificate Mismatch alarm log

9.4.4.1 Formats

9.4.4.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> sipgwyappln: SIPS303 <Severity> <Type> TLS ^M Certificate Mismatch in Server Certificate NCGL=<DeviceName>;Unit=<UnitNumber>;SIPS = Certificate Mismatch in Server Certificate ^M

Following are values/explanations of the variable values presented above:

- <Date>: Current date
- <Time>: Current time
- <Severity>: The Severity of the log (CRITICAL).
- <Type>: The type of log (INFO)
- <DeviceName>: The name assigned to the Session Server
- <UnitNumber>: The node {0 or 1} where the alarm was generated.

Example:

```
Apr  7 16:38:21 yang alarmd: SIPS303 CRIT TBL  Certificate Mismatch in Server
Certificate NCGL=yang;Unit=0;SIPS = Certificate Mismatch in Server Certificate
```

9.4.4.2 Explanation

Every minute, the SS-Trunks compares the data in the certificate and key files on the active side, to those on the inactive side. The SIPS303 log is generated if the two sets of files do not match each other. An alarm is also raised.

If the two files do not match each other, a number of consequences may occur, depending on the nature of the changes made to the files.

Effects may include:

- Inability to use the EM Web Server after the next swact or reboot.
- Inability to run TLS-based calls after the next swact or reboot.
- Dropping of all TLS-based calls after the next swact.

Needless to say, this is a log/alarm that should be acted on immediately. See the “Action” section below for more details.

9.4.4.3 Field descriptions

Table 4 Field descriptions

Field	Value	Description
<DATE>	<Mon> <DD>	Current date when the log occurred.
<Time>	<HH>:<MM>:<SS>	Current time when the log occurred.
<DeviceName>		Name of the session server.
<Severity>	CRITICAL	Severity level of the log
<UnitNumber>	0 or 1	which one of the two units generated the log.
<Type>	INFO	informational or initialization log.

9.4.4.4 Action

The proper certificate and key files must be restored to their place on both the active and inactive nodes. Check to ensure that the Certificate and Key provided to the call processing application are in the correct directory (as pointed to by the Database entry). It may be that the database entry is incorrect or corrupt.

The location of the files for the certificate and key are specified by the values stored in the database.

Root access to the SS-Trunks is normally required to correct this condition. This is because the server.key file is readable and writeable only by root.

Obtain the backup copies of these files made during install or upgrade, or during certificate replacement. Install them on *both* nodes using the cert_mgnt tool. Details on the backup/restore using cert_mgnt or other means can be found in the CN for this feature or the SS-Trunks install/upgrade NTP NN10346-611.

If the backup copies are not immediately available, it may be possible to copy the files from one node to the other. The sipgwyappln application must be running in a normal state on the node with the complete fileset for this to happen. Details on copying files between nodes can be found in the CN for this feature or the NTP quoted above.

In the worst case, if no backup copies exist, the user may wish to create or import an entirely new set of certificate and key files. Be warned: creating new self-signed certificates will likely require datafilling of the certificate on every peer SIP server in the network. And it will require the user to restart CallP on both nodes during a maintenance window.

The user will want to determine who has damaged or removed these files, because this may be the result of a security breach in the user's network.

The SS-Trunks produces CRT700 and CRT701 customer logs that are produced when the system cert_mgnt tool creates these files; look for these logs to determine if someone has made recent changes.

The user will want to ensure that the certificate and key files are meant to be together (by running the cert_mgnt tool).

9.4.4.5 Associated Operational Measurements or Performance Measurements

None for this log.

9.4.4.6 Additional information

None.

9.4.5 SIPS305 - TLS Engine failure log

These logs are output by TLS when it fails to initialize, and by the TLS alarm code when an alarm is raised to flag TLS initialization failure.

9.4.5.1 Formats

9.4.5.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> sipgwyappln: SIPS305 <Severity> <Type> NCGL=<DeviceName>;Unit=<UnitNumber> TLS <Log Message>

Following are values/explanations of the variable values presented above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <Severity>: The Severity of the log (CRIT).
- <Type>: The type of log (INIT)
- <UnitNumber>: The number {0,1} of the SS-Trunks.
- <Log Message>:
  - crit/init: “^M TLS Local Key and Cert do not match^M”
  - crit/init: “^M TLS Failed client init^M”
  - crit/init: “^M TLS Failed Server init^M”
  - crit/init: “^M TLS Failed to load Certificate^M”
  - crit/init: “^M TLS Failed to load Key^M”
  - crit/init: “^M TLS Failed to Init^M”
  - crit/init: “^M TLS Failed to get pointer^M”
  - crit/init: “^M TLS Failed to create thread^M”
  - crit/init: “^M TLS Failed Local Certificate Policy^M”
  - crit/init: “^M TLS is Not Enabled NCGL=<DeviceName>;Unit=<UnitNumber> TLS is Not Enabled^M” where <UnitNumber> is the number of the unit where the alarm was generated.

Examples:

```
Mar  1 10:06:53 NGSS sipgwyappln: SIPS305 CRIT INIT TLS ^M    TLS Failed Local
Certificate Policy^M
Mar  1 10:06:53 NGSS alarmd: SIPS305 CRIT TBL  TLS is Not Enabled
NCGL=NGSS;Unit=0;SIPS TLS is Not Enabled
```

9.4.5.2 Explanation

The SIPS305 log is generated during the initialization of the Call Processing application (i.e. during the unlock). If one of the critical logs come out, it

means that there is a problem with the initialization, and the application is unable to start.

9.4.5.3 Field descriptions

Table 5 Field descriptions

Field	Value	Description
<DATE>	<Mon> <DD>	Current date when the log occurred.
<Time>	<HH>:<MM>:<SS>	Current time when the log occurred.
<DeviceName>		Name of the session server.
<Severity>	CRIT	Severity level of the log
<Type>	INIT or TBL	initialization log / trouble log.
<UnitNumber>	0 or 1	which one of the two units generated the log.
<Log Message>	see bulleted list	Log message text.

9.4.5.4 Action

On a critical severity log, check to ensure that the Certificate and Key provided to the call processing application are in the correct directory (as pointed to by the Database entry). Then ensure that the Certificate and Key files themselves are not corrupted or tampered with. Ensure that the certificate and key files are meant to be together (by running the cert_mgnt tool). See “SIPS604: Certificate Information Logs” on page 1910 for more information.

Alternatively contact the next level of support.

Once the problem is resolved, and the user ‘unlocks’ the application again, there will be 3 logs indicating resolution.

- SIPM500

```
Feb  9 13:15:40 comit.ngss.unit1 sipgwymtc: SIPM500 NONE INFO SIP Gateway
Application Maintenance State Change ^M        [Administrative : Locked          -
> Unlocked      ]^M       [Operational    : Enabled        -> Enabled       ]^M
[Control         : Not Suspended    -> Not Suspended  ]^M        [Procedural      :
Not Terminating -> Not Terminating]^M      [User Requested : Yes]^M      [Reason
: Unlock command issued]^M         [Web User ID     : mtc]^M
```

- SIPS605
- SIPS604 (2 of them: one for certificate effective date; one for certificate expiry date)

9.4.5.5 Associated Operational Measurements or Performance Measurements

Not applicable to this log.

9.4.5.6 Additional information

Normally, the cert_mgnt CLI will provision the certificate and key files properly. If this interface has not been run prior to the attempt to bring the call processing application in service, or has been run improperly, unexpected results could occur. Extra information as to the cause of the problem will likely reside in the initialization trace logs provided in the /opt/apps/logs directory (look for siptrace.<date>.server.<pid>).

9.4.6 SIPS308 - Failed Certificate Policy Check Alarm Log

9.4.6.1 Formats

9.4.6.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> sipgwyappln: SIPS308 <Severity> <Type> ^M TLS Local Certificate Policy Mismatch NGSS=NCGL;Unit=<UnitNumber>;SIPS Failed <count> certificate policy checks.^M

Following are values/explanations of the variable values presented above:

- <Date>: Current date
- <Time>: Current time
- <Severity>: The Severity of the log.
- <Type>: The type of log (INFO)
- <DeviceName>: The name assigned to the Session Server
- <UnitNumber>: The number {0,1} of the SS-Trunks.
- <count>: The number of certificate policy checks that have failed.

Example:

```
Mar  2 14:44:46 NGSS alarmd: SIPS308 MINOR TBL  TLS Local Certificate Policy
Mismatch NCGL=NGSS;Unit=0;SIPS Failed 1 certificate policy checks
```

9.4.6.2 Explanation

The SIPS308 log is generated when enough certificate policy failures have occurred to generate an alarm. See 9.5.3 “Certificate Policy Check Failure Alarm” on page 1922 for more information.

9.4.6.3 Field descriptions

Table 6 Field descriptions

Field	Value	Description
<DATE>	<Mon> <DD>	Current date when the log occurred.
<Time>	<HH>:<MM>:<SS>	Current time when the log occurred.
<DeviceName>		Name of the session server.
<Severity>	MINOR	Severity level of the log
<UnitNumber>	0 or 1	which one of the two units generated the log.
<Type>	INFO	informational or initialization log.

9.4.6.4 Action

There are two courses of action. The first would be to remove the certificate policy that is preventing the certificate from the Security Parameters Configuration Web Page on the SS-Trunks.

The second course of action (and the preferred one) would be to enforce the local certificate policy throughout the network (forcing the Remote SIP Server to present a certificate that conforms to the certificate policy).

9.4.6.5 Associated Operational Measurements or Performance Measurements

None for this log.

9.4.6.6 Additional information

None.

9.5 Alarms

The following list of alarms has been created or changed for this feature:

- Fail to construct TLS client or server engine (changed).
- Certificate mistmatch between active/inactive host (new).
- Failed Certificate Policy Check (new).

The following alarms have not changed in SN09, but now have provisionable alarm thresholds. Consult this feature's CN document for more details.

- Connection Requests Dropped Alarm.
- Connection Handshake Failure Alarm.
- TLS Local Certificate Expiration Alarm.

9.5.1 Certificate Mismatch Alarm

Many of the details on this alarm and the appropriate response are documented in section 9.4.4 “SIPS303 - TLS Certificate Mismatch alarm log” on page 1911.

9.5.1.1 Integrated Element Manager GUI Fields

Table 7 IEMS Alarm GUI Field descriptions

Field	Value
Severity	NONE, or CRIT
Category	*Certificate Mismatch*
LogName	SIPS
LogNumber	303
EventType	TBL
EventLabel	TBL
ProbableCause	*versionMismatch*
SpecificProblem	TLS Certificate Mismatch
BodyText	Certificate Mismatch in Server Certificate

The original alarm log is not refreshed.

9.5.1.2 Explanation

Description: The SIPS303 log is generated whenever the certificate or private key files on the SS-Trunks do not match between the active and inactive nodes .

Severity: Critical. A certificate mismatch means that a SWACT could lead to the dropping of TLS calls, or that TLS CallP may not be active on the next reboot. It may also mean that the EM web server is inoperative, or will become inoperative on the next SWACT or node reboot. See 9.4.4.2 “Explanation” on page 1912 for more information.

9.5.1.3 Action

See 9.4.4.4 “Action” on page 1912 for detailed instructions on how to respond.

9.5.1.4 Corresponding Clear Log

Log Title: SIPS303 with severity NONE.

9.5.2 TLS Engine Failure Alarm

This alarm has been changed in SN09; it was first implemented in SN08. Please reference feature documentation for A00006893 for details on the SN08 implementation.

9.5.2.1 Integrated Element Manager GUI Fields

Table 8 IEMS Alarm GUI Field descriptions

Field	Value
Severity	NONE or CRIT
Category	*TLS Engine Failure*
LogName	SIPS
LogNumber	305
EventType	TBL
EventLabel	TBL
ProbableCause	*fileError*
SpecificProblem	TLS has failed to initialize properly, and needs to be restarted.
BodyText	TLS is Not Enabled

9.5.2.2 Explanation

The TLS Engine has failed to initialize when SS-Trunks CallP started. This may or may not have resulted in the termination of CallP on the SS-Trunks.

The SIPS305 customer log is generated during the alarming of TLS Engine failure. This log will inform the user of the exact reason that the TLS engine failed to start.

This alarm will only occur when the exitOnFailTLSinitialization security parameter is set to ‘N’. We recommend that exitOnFailTLSinitialization always be set to ‘Y’, and ‘Y’ is the default value.

9.5.2.3 Action

It is recommended that exitOnFailTLSinitialization be set to 'Y'. After that parameter is set to 'Y', this alarm will not occur in future cases of TLS initialization failure. Instead, the CallP application will not run if TLS cannot initialize properly.

The text of the associated SIPS305 customer log dictates the action.

The following error messages may be output in the SIPS305 customer log:

1. "TLS Failed to load Key"

2. "TLS Failed to load Certificate"

3. "TLS Failed Server init"

4. "TLS Local Key and Cert do not match"

5. "TLS Failed client init"

6. "TLS Failed to create thread"

7. "TLS Failed to get pointer"

8. "TLS Failed to Init"

9. "TLS Failed Local Certificate Policy"

The appropriate actions for these messages are as follows:

For messages 1, 2, and 4:

a. Check for the existence and validity of the certificate and key files. Restore these from backup if necessary. See 9.4.4.4 "Action" on page 1912 for a detailed method of validating these files.

b. If CallP is running, and the exitOnFailTLSinitialization security parameter is set to 'N', then: Change the value of parameter TlsEnabled to "Y" on the SecurityParmConfig EM web page. This will attempt a restart of TLS.

c. Else: Manually suspend/lock (if required) and unsuspend/unlock CallP from the Maintenance EM web page.

d. If the alarm is not cleared after this, contact Nortel Technical Support.

For messages 3, 5, 6, 7, and 8:

a. If CallP is running, and the exitOnFailTLSinitialization security parameter is set to 'N', then: Change the value of parameter TlsEnabled to "Y" on the SecurityParmConfig EM web page. This will attempt a restart of TLS.

b. Else: Manually suspend/lock (if required) and unsuspend/unlock CallP from the Maintenance EM web page.

c. If the alarm is not cleared after this, contact Nortel Technical Support.

For message 9, there are two alternatives:

a. Set the “RequireLocalCertificatePolicy” parameter on the SecurityConfigParms EM web page to “N”. This is a stopgap measure that will allow TLS to come up even if the certificate defies the local certificate policy.

   i. If CallP is running, and the exitOnFailTLSinitialization security parameter is set to ‘N’, then: Change the value of parameter TlsEnabled to “Y” on the SecurityParmConfig EM web page. This will attempt a restart of TLS.

   ii. Else: Manually suspend/lock (if required) and unsuspend/unlock CallP from the Maintenance EM web page.

b. Provision a new certificate that follows the established security policy. This is usually the preferred option, but may take a significant amount of time to accomplish, depending on the Public Key Infrastructure policy of the customer.

   i. If the customer allows self-signed certificates, a new self-signed certificate may be provisioned on this SS-Trunks using the cert_mgnt tool. However, this new self-signed certificate will have to be provisioned as a trusted certificate on all the SS-Trunks’s peer SIP servers.

   ii. If CallP is not running: Manually suspend/lock and unsuspend/unlock CallP from the Maintenance EM web page.

   iii. If CallP is running: Change the value of parameter TlsEnabled to “Y” on the SecurityParmConfig EM web page. This will attempt a restart of TLS.

c. If steps a and/or b do not work, contact Nortel Technical Support

9.5.2.4 Corresponding Clear Log

Log Title: SIPS305 with severity NONE.

9.5.3 Certificate Policy Check Failure Alarm

9.5.3.1 Integrated Element Manager GUI Fields

Table 9 IEMS Alarm GUI Field descriptions

Field	Value
Severity	NONE, MINOR, MAJOR, or CRIT
Category	*Certificate Policy Check Failure*
LogName	SIPS
LogNumber	308
EventType	TBL
EventLabel	TBL
ProbableCause	*thresholdCrossed*
SpecificProblem	A number of certificates violating the provisioned certificate policy on the SS-Trunks have been submitted by peer SIP servers.
BodyText	Failed <certificate_count> certificate policy checks <updatetext>

BodyText explanation: The BodyText entry for the log will contain “Failed <number> certificate policy checks”. However, over time, other events may occur, and the alarm BodyText will be updated with “Failed <number> certificate policy checks in the last minute<updatetext>”, where <updatetext> is one of:

- “, <numberminor> Minor events since alarm creation” for Minor alarms
- “, <numbermajor> Major, <numberminor> Minor events since alarm creation” for Major alarms or
- “, <numbercritical> Critical, <numbermajor> Major, <numberminor> Minor events since alarm creation” for Critical alarms.

The original alarm log is not refreshed.

9.5.3.2 Explanation

The customer has the option of setting requirements on TLS certificates submitted by other servers, using certain parameters provisionable on the SecurityParmsConfig web page on the EM.

If certificates are submitted by remote SIP servers that violate the policy set by the customer, the remote servers' certificates will be rejected, and calls from that server will not be allowed.

If a certain number of remote servers' certificates are failed, an alarm is generated. The number of failures that trigger an alarm is provisionable via the AlarmThresholdLocalCertificatePolicy parameter on the SecurityParmsConfig web page.

The default provisioned values for this alarm are minor=1, major=2, critical=5.

The log/alarm will be raised at least 30 minutes, and if the problem has ceased, the clear alarm log will be generated.

9.5.3.3 Action

The customer has two options here:

1. Disable the certificate policy restrictions set on the SecurityParmsConfig web page. The policy restrictions can be turned off by setting the RequireLocalCertificatePolicy parameter to 'N'.
    a. This option is intended as a stopgap, so that the customer can permit calls from offending servers while new certificates are issued to those servers.
2. Provision new certificates on the offending servers, that meet the customer's certificate policy. If self-signed certificates are used on the offending servers, the certificates will require datafilling on multiple peer SIP servers.
    a. This is the preferred option, but it may take significant time to complete this task.

9.5.3.4 Corresponding Clear Log

Log Title: SIPS308 with severity NONE.

9.6 Related documentation

NTP NN10346-611.

A00006893 FM section, in PLS FMDOC.

A00009235 CN section, in PLS FMDOC.

10: Fault Management (FM): A00009280

10.1 Feature Name

MG9K Line Circuit Enhancements

10.2 Fault management strategy

This feature does not introduce new faults.

10.3 Fault management tools and utilities

10.3.1 Faults, Alarms and Logs

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

10.4 Logs

The Log Delivery application for this feature generates logs in the Number 2 Switch Control Center (SCC2) format and the NT standard (STD) format.

There is no change in the existing format of Line Circuit alarms, except that the description part has an added statement about the DN number associated with the Line circuit alarm. If no DN is associated, then the 'DN Affected: None' would be displayed.

Once an alarm is reported, any subsequent changes to the DN would not get reflected in the alarm log of that line circuit or in the description part of the line circuit alarm on the Alarm Browser.

10.4.1 Formats

10.4.1.1 NTSTD

NorLineFault
SWLN301 ***Jan12 01:02:40 3409 TBL MG9K NorLineFault
Location: 18-c018-FrameFFF.Shelf3.Slot21.SAAL.p7
Notification Id: 399
State: not acknowledged
Category: equipment

Cause: Equipment Malfunction
Time: Jan 12 01:02:40 1970
Component Id: Card.frame0.shelf3.slot21.SAAL.p7
Specific Problem:norLineFault
Description: linefault
DN Affected: 6195210102
Site Flr RPos Bay_id
Cary 02 H02 MG9F 012

10.4.1.2 SCC2

NorLineFault
*** SWLN301 3409 TBL MG9K NorLineFault
Location: 18-c018-FrameFFF.Shelf3.Slot21.SAAL.p7
Notification Id: 399
State: cleared
Category: equipment
Cause: Equipment Malfunction
Time: Jan 12 01:02:40 1970
Component Id: Card.frame0.shelf3.slot21.SAAL.p7
Specific Problem: NorLineFault
Description: linefault
DN Affected: 6195210102
Site Flr RPos Bay_id
Cary 02 H02 MG9F012

10.5 Alarms

No new alarms are added as a part of this CCAF.

The Description part of a line circuit alarm would have an added statement namely:

DN Affected: <Associate DN>

If no DN is associated with a line circuit then the below statement would be appended to the description part of the line circuit alarm:

DN Affected: None

Once alarm is reported any subsequent changes to DN would not get reflected in the alarm log of that line circuit or in the description part of the line circuit alarm on the Alarm Browser.

10.6 Related documentation

None.

11: Fault Management (FM): A00009282

11.1 Feature Name

Emergency Stand Alone (ESA) Multiple Level Precedence and Preemption (MLPP) for MG9KEM

11.2 Fault management strategy

The standard MG9k EM Fault Management strategy will apply to the faults for this feature. Alarms will be displayed by the MG9K EM Alarm Browser, logged in NT standard format to the SSPFS CUST logs and forwarded to northbound OSS.

11.3 Fault management tools and utilities

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

11.4 Logs and Alarms

No new alarms will be added. A new alarm reason will be generated for ESA download problems from the Core when the timestamp of the Core file is more than 48 hours old.

The alarm will be displayed at the Alarm Browser at the subnet as well as the well as the alarm browser for each corresponding network element. A log is also generated. Both are NE level alarms.

11.4.1 Explanation

11.4.1.1 ESA311

Title: Core Download Failed

Name: ESA

Description: This log is generated by the EM in when a problem is detected when trying to download the datafile from the core.

This new condition is when the Core datafile is more than 48 hours old, indicating that the file on the Core is not being generated nightly.

Severity: Minof

Event type: ESA Core Data Download

11.4.2 Field descriptions

11.4.2.1 ESA311 (nnEsaCoiFault)

Table 1 Field descriptions ESA304

Field	Value	Description
office identification	String	Identifies the switch that generates the log. This field is optional. The maximum length of this field is 12 characters.
alarm	***,**,*, or blank	Indicates the alarm type of the log report. ***=critical, **=major, *=minor, blank = no alarms/warning
threshold	+ or blank	Indicates if a threshold is set for the log report. Plus (+) sign indicates that a threshold was set; if a blank, a threshold was not set.
report identification	AAAA nnn	Identifies the log subsystem that generates the report. This field uses 2-4 alphabetical characters and the number 100-999 of the log report in this subsystem. For this log AAAA= MGC and nnn=600.
day	String	Identifies the day of the week.
mmmmdd	January-December (01-31)	Identifies the month and date the report generates.

Table 1 Field descriptions ESA304

Field	Value	Description
hh:mm:ss	00-23 00-59 00-59	Identifies the hour, the minute, and the second the report generates.
zone	PST, EST, MST, CST, AST	Identifies the time zone.
yyyy	0000-9999	Year
ssdd	0000-9999	Defines a different sequence number for each log report generated.
event type	TBL, INFO, etc	Trouble, Service Summary, State Change, Information, Threshold and Expert. TBL for this log.
event id	String	The Log Title.
NE Number	integer	Number of the NE
NE Name	string	Name of the NE
Fault Type	string	The type of the fault: ESA Community of Interest
nnUemgEventTime	DateandTime	The Date and Time the event occurred in the following format: day mmmmdd hh:mm:ss zone yyyy
nnUemgAlarmSeverity	String	Major
Description	string	Failed to ping members of communityof interest

11.4.2.2 ESA312 (Internodal ESA Provisioning Fault)

Table 2 Field descriptions ESA304

Field	Value	Description
office identification	String	Identifies the switch that generates the log. This field is optional. The maximum length of this field is 12 characters.
alarm	***,**,*, or blank	Indicates the alarm type of the log report. ***=critical, **=major, *=minor, blank = no alarms/warning
threshold	+ or blank	Indicates if a threshold is set for the log report. Plus (+) sign indicates that a threshold was set; if a blank, a threshold was not set.
report identification	AAAA nnn	Identifies the log subsystem that generates the report. This field uses 2-4 alphabetical characters and the number 100-999 of the log report in this subsystem. For this log AAAA= MGC and nnn=600.
day	String	Identifies the day of the week.
mmmmdd	January-December (01-31)	Identifies the month and date the report generates.
hh:mm:ss	00-23 00-59 00-59	Identifies the hour, the minute, and the second the report generates.
zone	PST, EST, MST, CST, AST	Identifies the time zone.
yyyy	0000-9999	Year
ssdd	0000-9999	Defines a different sequence number for each log report generated.

Table 2 Field descriptions ESA304

Field	Value	Description
event type	TBL, INFO, etc	Trouble, Service Summary, State Change, Information, Threshold and Expert. TBL for this log.
event id	String	The Log Title.
NE Number	integer	Number of the NE
NE Name	string	Name of the NE
Fault Type	string	The type of the fault: Processing Error
nnUemgEventTime	DateandTime	The Date and Time the event occurred in the following format: day mmmmdd hh:mm:ss zone yyyy
nnUemgAlarmSeverity	String	Major
Description	string	Internodal ESA provisioning failure

11.4.3 Action

ESA304 (nnEsaCoiFault):

Check failure cause in alarm or log text and perform corrective action This will typically require network route troubleshooting. The MG9000 will clear the alarm autonomously once the root cause is fixed.

ESA312 (Internodal ESA provisioning failure):

Check failure log in the alarm or log text (most common is communication failure between the MG9000 EM and the MG9000). Once the root cause is fixed the alarm can be cleared by running and audit on the affected NE, or hitting “Apply” button on the Internodal ESA configuration GUI.

11.4.4 Associated Operational Measurements or Performance Measurements

None.

11.5 Related documentation

1. NORTEL-UEMG-BASE-MIB - MG9000's Enterprise MIB, contains the Alarm Log Table.

2. PLOA and SLOA Logs and Alarms for UE9kMG EM (DID) - MG9000s design documentation for logs and alarms on the MG9000 Element Manager.

3. Logs and Alarms Strategy for WUA Components - MG9000 Alarm strategy guide - version 1.4

3. Reliable Alarms and Alarm Robustness Design Intent Document (DID) - MG9000 Element Manager design document.

4. PLOA and SLOA Alarm Forwarding to OSS(DSUM) - MG9000 Alarm forwarding feature.

12: Fault Management (FM): A00009315

12.1 Feature Name

Alarm Logging Failure

12.2 Fault management strategy

ISSPFS will generate an alarm to detect that the logging system is no longer writing logs

12.3 Fault management tools and utilities

The scope of this feature is to provide a mechanism to immediately notify, in real-time, the MSAP administrator (e.g., alarm) if the MSAP security log fails to record the events that are required to be recorded.

12.4 Logs

None

12.5 Alarms

12.5.1 Logging has stopped Alarm

```
Component Id     :
cbm850=wnc0s0rv;NODE=wnc0s0rv,CLASS=SYS,SYSTYPE=Syslog,File=monitor_syslog.csh
Severity         : Major
State            : ISTb
Report Name      : SPFS
Report Number    : 380
Application      : SSPFS_RES_MON
Algorithm Used   : Algorithm1
Category         : QualityOfService
Event Type       : INFO
Probable Cause   : unspecifiedReason
Description      : The Logging system is not writing logs
Specific Problem : syslogd not writing marklog logs
User Data        :
Recovery Action  :
Time When Raised : Wed Mar 2 11:51:28 2005
```

12.5.2 Logging has stopped Alarm Clearing

```
Component Id     :
cbm850=wnc0s0rv;NODE=wnc0s0rv,CLASS=SYS,SYSTYPE=Syslog,File=monitor_syslog.csh
Severity         : Cleared
State            : InSv
Report Name      : SPFS
Report Number    : 380
Application      : SSPFS_RES_MON
Algorithm Used   : Algorithm1
Category         : QualityOfService
```

```
Event Type       : INFO
Probable Cause   : unspecifiedReason
Description      : The Logging system is now writing logs
Specific Problem : syslogd is now writing marklog logs
User Data        :
Recovery Action  :
Time When Raised : Wed Mar 2 11:53:34 2005
```

12.6 Related documentation

13: Fault Management (FM): A00009353

13.1 Feature Name

GWC Unit Availability/ Health Monitoring

13.2 Fault management strategy

None

13.3 Fault management tools and utilities

None

13.4 Logs

None

13.5 Alarms

An alarm will be raised whenever the PreSwact audit fails for two consecutive cycles.The text of the alarm describes which component has led to the failure.It will be reflected in the SESM as well as in the GWC with the available status of the GWC in the SESM reflecting “DEGRADED”. The audit runs periodically and raises alarm for PSA fail on error conditions. A duplicate alarm for the same reason as that of an existing one will not be raised. Following are the alarm details:

- **Alarm format** - The alarm will be having the following characteristics

Description	: PreSwact Audit Failure
Component	: NODEMTC
Category	: QualityOfService
ProbableCause	: ‘resourceAtOrNearingCapacity’ for resource exhaust. ‘performanceDegraded’ for Unit Jam.

- **Severity** - Major
- **Cause or condition** — PreSwactAudit Failure
- **Duration** — The alarm will be raised when ever the PreSwact Audit fails on error conditions and gets cleared when the error condition is cleared.

The alarm will also have a specific reason for the alarm apart from a generic description. This will describe which component has led to the failure.

13.5.1 Causes for the Alarm

The PreSwact Audit alarm will be raised under the following conditions:

1. Monitored base resource reaches the threshold level.
2. Monitored application resource reaches the threshold level.
3. Existing PreSwact Audit check fails for an error condition.
4. When the standby unit is jammed to prevent it from taking up the activity.

13.5.2 Clearing the Alarm

PreSwact Audit alarm will be raised whenever PreSwact Audit fails.This alarm will be cleared when the fault is cleared as PSA will be running periodically other than running during Swacts.The PSA will pass for a resource when its usage comes down with in limits.

For example, if the Request resource remains exhausted over two consecutive PreSwact Audit cycles, the PSA will fail and the alarm with corresponding failure reason will be raised. If in the subsequent cycles the Request resource level comes down within limits, PSA will pass and hence the alarm will be cleared for the resource.

13.5.3 Integrated Element Manager GUI Fields

None

13.6 Related documentation

None

14: Fault Management (FM): A00009470

14.1 Feature Name

SuperNode Data Manager (SDM) to support Security Assertion Markup Language (SAML) NSSwitch client

14.2 Fault management strategy

The feature will log SAML client configuration changes to SDM Security Logs.

Note: Please refer to SN08 IEMS Integration feature document in PLS FMDOC (a00007489) for detail information on SDM Security Logs for SN08 functionality.

14.3 Fault management tools and utilities

14.3.1 Faults, Alarms and Logs

SDM Security Logs utility will be used by this feature.

14.4 Logs

Log Title/Log ID: USER_ACT_Security_Naming_Service/ SDM_MID_defn.security.0012

14.4.1 SDM Security log

The existing SN08 security log will be used for naming service configuration changes. The following is an example of a security log when naming service is changed from LOCAL to SAML.

Feb 4 11:12:20 wcary2p4 sdmmtc[19512]: class_security.ver02 EVENT.TYPE="USER_ACT_Security_Naming_Service" DOC="RMI" STAT="Success" DST="wcary2p4" DST.USR="root" SRC.OFFEND="47.129.112.179" HOST.TYPE="application" TTY="pts/4" MESSAGE="Naming Service was changed - Current: LOCAL New: SAML" MID="SDM_MID_defn.security.0012"

Both USER_ACT_Security_Naming_Service and SDM_MID_defn.security.0012 are an existing security log EVNT.TYP and MID.

14.5 Alarms

Not applicable to this feature.

14.6 Related documentation

None

15: Fault Management (FM): A00009515

15.1 Feature Name

Out-of-Band Interop with MCS

15.2 Fault management strategy

15.3 Logs

New NCAS class log will be generated by the SIP Gateway Application under this activity. It will be generated for the following event: OOB Refer is Rejected

This log can be viewed via the SIP Gateway Maintenance web browser interface on the Session Server Manger - SIP Gateway application web page.

No alarms will be generated in connection with this

15.3.1 NCAS LOGS

New customer log that will be generated by this feature:

- NCAS501 - OOB REFER REJECTED

15.3.1.1 NCAS501 OOB REFER Rejected

Log NCAS501 “OOB REFERREJECTED” is generated when an Out-of-Band REFER Request that has been received by the Session Server does not validate and this the request can not be accepted.

Log Title: OOB

Name: NCAS 501

Description: OOB REFER REJECTED

Event Type: Trouble

FORMAT: For the NCAS 501 log, the following are values/explanations of the variable values:

- alarmLevel = NONE
- componentID = NCAS
- category = Communications
- description = OOB Refer Rejected

- probable cause = Incorrect Header
- specific cause = ReferTo or ReferBy Header Incorrect
- correlationIdList = None
- neVendorSpecificInfo = None
- technologySpecificInfo = None
- reportName = NCAS
- reportNum= 501
- eventType = TBL
- label = OOB

ACTION: Verify Header Population

16: Fault Management (FM): A00009532

16.1 Feature Name

Support host to host tunnels for all northbound OSS connections

16.2 Fault management strategy

Not applicable.

16.3 Fault management tools and utilities

Not applicable.

16.4 Logs

No new logs are being added because of this feature. The following section is added for informational purposes.

16.4.1 IPsec syslog messages

The Solaris implementation of IPsec automatically sends all failure logs to syslog /var/adm/messages. We do not have control over this. However when the Server Security Manager (SSM) makes any changes to the IPsec security rules, the wrapper scripts will output any attempted changes to /var/log/securitylog.

The Solaris IPsec itself does not seem to generate any failure messages because security could be compromised, however IKE does seem to generate failure messages to syslog.

Sample IKE failure message would look like the following:

```
messages.0:Mar 25 15:40:04 wnc1s01h /usr/lib/inet/in.iked: [ID
313954 daemon.notice] IKE_DELETE_PAYLOAD_RECEIVED:
20040325204004:   Source addr:47.142.217.23 Destination
addr:47.142.217.22 SPI:0x0100005d350a7d6c0100006b743037d4
Description:Received delete notification
```

All other possible failure messages that could get generated to syslog is shown below for IKE.

```
IKE_AH_IP_FRAGMENT

IKE_AH_SA_LOOKUP_FAILURE

IKE_AH_SEQUENCE_NUMBER_FAILURE

IKE_AH_ICV_FAILURE

IKE_ESP_SEQUENCE_NUMBER_OVERFLOW

IKE_ESP_IP_FRAGMENT
```

IKE_ESP_SA_LOOKUP_FAILURE,

IKE_ESP_SEQUENCE_NUMBER_FAILURE

IKE_ESP_ICV_FAILURE

IKE_INVALID_COOKIE

IKE_INVALID_ISAKMP_VERSION

IKE_INVALID_EXCHANGE_TYPE

IKE_INVALID_FLAGS

IKE_INVALID_MESSAGE_ID

IKE_INVALID_NEXT_PAYLOAD

IKE_INVALID_RESERVED_FIELD

IKE_INVALID_DOI

IKE_INVALID_SITUATION

IKE_INVALID_PROPOSAL

IKE_INVALID_SPI

IKE_INVALID_TRANSFORM

IKE_INVALID_ATTRIBUTES

IKE_INVALID_KEY_INFORMATION

IKE_INVALID_ID_INFORMATION

IKE_INVALID_CERTIFICATE

IKE_INVALID_CERTIFICATE_TYPE

IKE_INVALID_CERTIFICATE_AUTHORITY

IKE_INVALID_HASH_INFORMATION

IKE_INVALID_HASH_VALUE

IKE_INVALID_SIGNATURE_INFORMATION

IKE_INVALID_SIGNATURE_VALUE

IKE_INVALID_PROTOCOL_ID

IKE_INVALID_MESSAGE_TYPE

IKE_CERTIFICATE_TYPE_UNSUPPORTED

IKE_CERTIFICATE_UNAVAILABLE

IKE_NOTIFICATION_PAYLOAD_RECEIVED

IKE_DELETE_PAYLOAD_RECEIVED

```
IKE_UNEQUAL_PAYLOAD_LENGTHS

IKE_BAD_PROPOSAL_SYNTAX

IKE_RETRY_LIMIT_REACHED
```

16.5 Alarms

No new alarms are being added because of this feature.

16.6 Related documentation

17: Fault Management (FM): A00009610

17.1 Feature Name

IEMS Calix Integration

17.2 Fault management strategy

17.3 Active Alarm List

In order to retrieve the active alarm list for a C7 shelf IEMS will query the calixAllAlarmTable from the CALIX-FAULT-MIB. This will happen for the following conditions

1 After the discovery for C7 network is completed while provisioning a C7 Network

2 A cold start trap is received from the C7 shelf or network

3 User issues a manual Re-Synchronize Alarms command from the IEMS client

4 System time is less that the previous system time for a calix trap

To query, IEMS will use the C7 network's configured IP address and the UDP port assigned for that shelf.

Following table lists the mapping between the columns of the alarm table and the IEMS event and also other properties of the IEMS event

Alarm Table Field	***IEMS Event Field***
CalixAllAlarmObjIndex	Entity*
CalixAllAlarmCntIndex	NotificationID
calixAllAlarmObjTl1Aid	Entity*, ComponentID#,location(bodyText) with only the shelf name
CalixAllAlarmObjClass	-
CalixAllAlarmSeverity	Severity critical(3) – critical major(2) – major minor(1) – minor unknown(4) – minor
CalixAllAlarmType	Entity*,SpecificProblem

CalixAllAlarmSrvEffect	LogNumber unknown – 300 serviceAffecting – 301 nonServiceAffecting – 302
CalixAllAlarmLocation	ComponentID# nearEnd(1), farEnd(2),bothEnds(3),notApplicable(4)
CalixAllAlarmDateTime	Time
calixAllAlarmTimeStamp	-
Calix Resync Alarm	Text
Other	ProbableCause
Other	Category
FLT	EventType
Fault	EventLabel

* - An entity uniquely identifies an alarm. Entity for an alarm is formed by combining ipAddress(C7 network), calixAllAlarmObjTl1Aid, calixAllAlarmType and calixAllAlarmObjIndex.

- componentID is formed combining calixAllAlarmObjTl1Aid and calixAllAlarmLocation. If location value is 'notApplicable' then componentID is calixAllAlarmObjTl1Aid or else it is calixAllAlarmObjTl1Aid (calixAllAlarmLocation)

Note: As there is no column in the alarm table that can be used as the text for the IEMS alarm it is set to 'Calix Resync Alarm'.

17.3.1 Calix trap handling

The following traps from the C7 device will be handled in IEMS

17.3.1.1 Cold Start Trap

On receiving a cold start trap from the calix device, IEMS will re-synchronize the C7network and the C7 Shelf alarms.

17.3.1.2 Calix Alarm Raise Notification Trap

This trap is recognized as an alarm in IEMS. The severity of the alarm is based on the value of the CalixTrapAlarmSeverity varbind.

The following table lists the mapping of varbinds of this trap to IEMS event.

CalixTrapAlarm varbind	***IEMS Event Field***
calixTrapTl1Aid	entity*, componentID#, location(bodyText) only the node and shelf part
CalixTrapAlarmTransition	determines whether alarm is raised or cleared

CalixTrapAlarmSeverity	Severity critical(3) – critical major(2) – major minor(1) – minor unknown(4) – minor
CalixTrapAlarmType	entity*, specificProblem
CALX	LogName
calixTrapSrvEffect	LogNumber unknown – 300 serviceAffecting – 301 nonServiceAffecting - 302
calixTrapCondDescr	text
calixTrapLocation	ComponentID# nearEnd(1), farEnd(2),bothEnds(3),notApplicable(4)
calixTrapObjClass	-
calixTrapObjIndex	entity*
calixTrapSerialNr	sequenceNumber
There is no varbind to get the alarm generated time. Will use the current IEMS time while adding the alarm.	time
Other	probableCause
Other	category
Fault – For rising alarm Cleared – For falling alarm	eventLabel
FLT – For rising alarm INFO – For falling alarm	eventType

17.3.1.3 Threshold Crossing Alert Trap

The TCA traps will be added in IEMS with a severity of MINOR. The following table lists the mapping of varbinds of this trap to IEMS event

TCA Trap Varbind	*IEMS Event Field*
calixTrapTl1Aid	entity*, componentID#,location(bodyText) only the node and shelf part
calixTrapCondType	entity, specificProblem
Minor	severity
CALX	logName

calixTrapCondState	*logNumber* cleared(1) – 800 standing(2) – 801 transient(3) – 802 notApplicable(4) - 803 *state*(bodyText) cleared(1) – Cleared standing(2) – Raised transient(3) –Transient notApplicable(4) – N/A
calixTrapCondDescr	text
calixTrapLocation	componentID nearEnd(1), farEnd(2),bothEnds(3),notApplicable(4)
calixTrapMonValue	-
calixTrapThLevel	-
calixTrapTmPeriod	-
calixTrapObjClass	-
calixTrapObjIndex	entity
calixTrapSerialNr	sequenceNumber
Other	probableCause
Other	category
TCA	eventLabel
THR	eventType

17.3.1.4 Remove/Restore Traps

The remove/restore traps will be added as informational events in IEMS. The following table shows the mapping of the varbinds of this trap to the fields in IEMS event

Remove/Restore TrapVarbind	***IEMS Event Field***
calixTrapTl1Aid	entity,location(bodyText) only the node and shelf part
calixTrapObjState	text
calixTrapObjClass	-
calixTrapObjIndex	entity
calixTrapSerialNr	sequenceNumber

CALX	logName
501 – For calixRemoveEvent 502 – For calixRestoreEvent	logNumber
INFO	eventType
EntityRemove – For calixRemoveEvent EntityRestore – For calixRestoreEvent	eventLabel

17.3.2 Alarm Correlation & Propagation

All the traps are associated with the C7 shelf, except the cold start trap, based on the calixTrapTl1Aid varbind. If the pattern for this varbind doesn't match the standard pattern, then the traps are associated with the C7 network.

The cold start trap is not associated with any of the calix objects. When this trap is received in IEMS then all the existing alarms for the C7 network, including the shelves, are cleared and an IEMS 609 INFO event is generated that is associated with the C7 network.

All the traps are propagated from the C7 shelf to the C7 node and to the C7 network.

17.3.3 Trap Loss Detection

Whenever IEMS detects a trap loss, i.e. when the sequenceNumber in the trap is greater than the previous sequenceNumber plus one, then IEMS would generate an informational event to notify this trap loss. It is desirable that the user performs a manual resync for the alarms once the count of this alarm increases. Following are the properties of the IEMS event that will be generated

IEMS Event Field	***Value***
Entity	Name of the C7 network as generated by IEMS
logName	IEMS
logNumber	603
severity	INFO
eventType	INFO
eventLabel	Missed Notifications
category	Other
location	C7 network IP address
componentID	IEMS=name of the C7 network as generated by IEMS

text	Notification(s) missed in ML (comma separated missed sequenceNumbers

17.3.4 Sample Northbound Trap Format

Chennai *** CALX301 JAN27 12:50:17 0001 TBL C7 Fault
Location: N1-1
Notification Id: 1
State: Raised
Category: other
Cause: other
Time: Jan 27 12:50:17 2005
Component Id: N1-1-IG1-EOC(farEnd)
Specific Problem: embeddedOperChanDuplexFail
Description: Calix Resync Alarm

The properties for the above trap are

Event Field	***Value***
calixAllAlarmObjIndex	2360320
calixAllAlarmCntIndex	1
calixAllAlarmObjTl1Aid	N1-1-IG1-TMC
calixAllAlarmObjClass	igDataLink(17)
calixAllAlarmSeverity	Critical(3)
calixAllAlarmType	timeSlotMgmtChannelDuplexFail(126)
calixAllAlarmSrvEffect	serviceAffecting(2)
calixAllAlarmLocation	FarEnd(2)
calixAllAlarmDateTime	01-27-2005,12:50:17
calixAllAlarmTimeStamp	15 days, 14 hours, 35 minutes, 28 seconds.

17.4 Menu Handling

The menu for any of the C7 objects will appear on right-clicking any of these objects in the respective maps. Following table shows the menu items for each of these objects.

C7 Network	Managed Object Properties Delete Object and Traces Re-Synchronize Inventory Re-Synchronize Alarms Events And Alarms Launch Calix iMS Launch TL1 Command Line UnManage Update Status
C7 Node	Managed Object Properties Re-Synchronize Alarms Events And Alarms Launch Calix iMS Launch TL1 Command Line
C7 Shelf	Managed Object Properties Re-Synchronize Alarms Events And Alarms Launch Calix iMS Launch TL1 Command Line

The Delete Object And Traces menu will be provided only for C7 network. This is because the C7 Shelf and C7 Nodes are auto discovered from the C7 network. On deleting the C7 network the respective nodes and shelves will also be deleted.

17.5 Configuring Radius Secrets

User will be given the option of configuring the radius secrets. If he configures then it will be applied for both the Calix GUI Launch IP address as well as the Command Line IP address. This will be provided in the C7 Provisioning screen. Only the users that are part of the secadm group would be able to modify the secrets.

Also default radius secret for Calix devices can be configured from Edit --> Default Secrets option in the Security Administration. A new type will be added for Calix in this GUI.

17.6 Launch

The iMS GUI launch as well as the TL1 Command Line launch would be permissible only to the users that belong to the MG domain.

17.6.1 Launch Calix iMS

The following steps are taken in order to launch the Calix IMS

1 User executes the 'Launch Calix IMS' by right clicking the network,node or shelf

2 IEMS requests https://<IEMS IP>/<Calix IP>/func/launchIMS.jnlp passing the userName, password TTL token,IEMS IP, Calix IP and the telnet wrapper command

3 The SSPFS apache proxy forwards the request to Calix and the necessary jars are downloaded to the IEMS client

4 Calix iMS client runs

5 The Calix iMS connects to the IEMS server using SSH and executes the command specified. This is actaully the telnet wrapper that is getting invoked.

6 The telnet wrapper queries the IEMS database using the Calix network IP to determine the actual logon script.

7 The necessary acccess control is performed and security and audit logs are generated.

8 On successful verification the logon script is invoked. The expect script uses the userName and SU token passed to the telnet wrapper to perform an SSH command line port forwarding to the Calix device.

9 IMS GUI becomed operational

Note: The final launch url has to be finalized

17.6.2 Launch TL1 Command Line

The following steps are taken in order to launch the TL1 Command Line

1 User executes the 'TL1 Command Line' by right clicking the network,node or shelf

2 IEMS client obtains two SU tokens

3 Using mindterm IEMS client will SSH to the IEMS server using the userName and an SU Token and execute the telnet wrapper command passing the necessary parameters

4 The telnet wrapper queries the IEMS database using the Calix network IP to determine the expect script.

5 The necessary acccess control is performed and security and audit logs are generated.

6 On successful verification the expect script is invoked. The expect script uses the userName and SU token passed to the telnet wrapper to perform an SSH command line port forwarding to the Calix device.

7 TL1 Command Line is operational

17.6.3 Telnet Wrapper

The telnet wrapper is a generic script that can be used to perform command line proxy to a device. The arguments that have to be passed to the script are

- IP Address of the target device
- Any additional parameters that are required by the actual logon script

Using the passed IP address of the target device the telnet wrapper will query the IEMS DB to obtain the type and version of the device. Using this informationa it would obtain the necessary logon script to be invoked.

Necessary access control is performed to identify if the user has permissions to invoke this operation. Security and audit logs are generated. A new operation named 'Command Line Proxy' will be added in the Security Administration to represent the launches that would require commandline proxy. This would be used to perform access control for the Calix iMS Launch and the TL1 Command Line Launch that would be using the command line proxy.

On successful verification the actual logon script in invoked to login to the device.

The telnet wrapper gets executed as part of the restricted shell. For this purpose during the installation of IEMS server the telnet wrapper would be registered with servman.

Note: As the IP address in the only parameter used to obtain actual logon script there may be a possibility that multiple devices are running in the same IP address. Then currently there is no way to determine the correct logon script. Currently for Calix this may not be a problem since the IP for a C7 network is unique.

17.7 Peformance Collection

In order to perform data collection for Calix, provision will be given in the existing Add Job and Report Job screen to select the Calix objects. In the Device Type list box 'C7 Shelf' option would be provided. On selecting this all the discovered calix shelf objects would be listed in the Device List. The user can select the shelves for which data has to be collected.

To get the data the calix network IP address and the corresponding shelf port will be used.

18: Fault Management (FM): A00009611

18.1 Feature Name

IEMS Keymile Integration

18.2 Fault management strategy

The Fault management interface employed by IEMS for the Keymile UNEM and UMUX devices will be based on SNMP. The design uses the fault data that the UNEM server sends on behalf of the UMUX devices it manages as well as itself in the northbound direction and makes the required conversions into a well-defined format at the IEMS layer. The IEMS does not provide a one-to-one mapping between the Keymile UNEM and UMUX alarms, rather it groups the alarms based on X.733 categories.

18.3 Northbound Events (Alarm and Logs)

18.3.1 Communication Alarms

The UNEM proxy agent sends an alarmRaisedTrap when an event on a UNEM managed entity (i.e. a managed UMUX NE or the UNEM itself) causes a standing communication condition and has immediate or potential impact on the operation or performance of the entity in question.

Table 27: Communication Alarm

Field	Value
Log Name	UNEM or UMUX
Log Number	300
Severity	Minor, Major, or Critical
Event Type	TBL
State	Raised
Category	Communication
Probable Cause	Please refer to the alarm text
Description	Please refer to the alarm text
Action	Please refer to the alarm text and consult the appropriate UNEM or UMUX User Guide for the appropriate action.

18.3.1.1 NTSTD Format Sample

wnc0s0jn *** UMUX300 MAR29 05:09:44 0482 TBL UMUX FLT

Location: OTT_UMUX_1200
Notification ID: 0
State: Raised
Category: communication
Cause: others
Time: Mar 29 05:09:44 2005
Component Id: LOMIF <12> 2Mbit/s-1 / E12
Specific Problem: others
Description: AIS Received

18.3.1.2 SCC2 Format Sample

**46 UMUX300 0009 TBL UMUX FLT
Location: OTT_UMUX_1200
Notification ID: 0
State: Raised
Category: communication
Cause: others
Time: Mar 17 13:46:27 2005
Component Id: LOMIF <12> 2Mbit/s-1 / E12
Specific Problem: others
Description: Loss of Signal

18.3.1.3 Syslog Format Sample

Apr 8 01:27:24 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9447~~ UMUX300 CRIT TBL UMUX FLT^M Location: OTT_UMUX_1200^M Notification ID: 0^M State: Raised^M Category: communication^M Cause: others^M Time: Apr 08 01:54:45 2005^M Component Id: LOMIF <12> 2Mbit/s-1 / E12^M Specific Problem: others^M Description: AIS Received

18.3.1.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 11 minutes, 8 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.305:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10: STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.18.50.48.48.53.45.52.45.56.44.54.58.51.52.58.48.46.48.44.23905:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.2: 07 d5 04 08 06 22 00 00:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11: STRING:
DeviceSpecificInfo=;AIS Received:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1: INTEGER: 5:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2: INTEGER: 1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3: STRING: :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4: STRING:
UMUX300:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:

.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.6: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7: INTEGER: 16:

18.3.2 Equipment Alarms

The UNEM proxy agent sends an alarmRaisedTrap when an event on a UNEM managed entity (i.e. a managed UMUX NE or the UNEM itself) causes a standing equipment condition and has immediate or potential impact on the operation or performance of the entity in question.

Table 28: Equipment Alarm

Field	Value
Log Name	UNEM or UMUX
Log Number	301
Severity	Minor, Major, or Critical
Event Type	TBL
State	Raised
Category	Equipment
Probable Cause	Please refer to the alarm text
Description	Please refer to the alarm text
Action	Please refer to the alarm text and consult the appropriate Keymile UNEM or UMUX User Guide for the appropriate action.

18.3.2.1 NTSTD Format Sample

wnc0s0jn *** UMUX301 MAR23 08:36:30 0483 TBL UMUX FLT
Location: RTP_UMUX_1500
Notification ID: 0
State: Raised
Category: equipment
Cause: others
Time: Mar 23 08:36:30 2005
Component Id: COBUX <11> Board / Network Element
Specific Problem: others
Description: SW Installation Error

18.3.2.2 SCC2 Format Sample

*C16 UMUX301 0011 TBL UMUX FLT
Location: RTP_UMUX_1500
Notification ID: 0

State: Raised
Category: equipment
Cause: others
Time: Mar 30 08:16:32 2005
Component Id: COBUX <12> Board
Specific Problem: others
Description: Unit Not Available

18.3.2.3 Syslog Format Sample

Apr 8 01:22:48 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9442~~ UMUX301 CRIT TBL UMUX FLT^M Location: OTT_UMUX_1200^M Notification ID: 0^M State: Raised^M Category: equipment^M Cause: others^M Time: Apr 08 01:49:02 2005^M Component Id: LOMIF <12> Board^M Specific Problem: others^M Description: Unit Not Available

18.3.2.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 7 minutes, 51 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.305:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10: STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48.48.53.45.52.45.56.44.54.58.51.48.58.52.51.46.48.44.23882:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.2: 07 d5 04 08 06 1e 2b 00:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11: STRING:
DeviceSpecificInfo=;Unit Not Available:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1: INTEGER: 5:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2: INTEGER: 1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3: STRING: :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4: STRING:
UMUX301:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.6: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7: INTEGER: 15:

18.3.3 Environmental Alarms

The UNEM proxy agent sends an alarmRaisedTrap when an event on a UNEM managed entity (i.e. a managed UMUX NE or the UNEM itself) causes a

standing environmental condition and has immediate or potential impact on the operation or performance of the entity in question.

Table 29: Environmental Alarm

Field	Value
Log Name	UNEM or UMUX
Log Number	302
Severity	Minor, Major, or Critical
Event Type	TBL
State	Raised
Category	Environmental
Probable Cause	Please refer to the alarm text
Description	Please refer to the alarm text
Action	Please refer to the alarm text and consult the appropriate UNEM or UMUX User Guide for the appropriate action.

18.3.3.1 NTSTD Format Sample

wnc0s0jn *** UMUX302 MAR23 08:36:32 0483 TBL UMUX FLT
Location: RTP_UMUX_1500
Notification ID: 0
State: Raised
Category: environmental
Cause: others
Time: Mar 23 08:36:30 2005
Component Id: COBUX <11> Board / Network Element
Specific Problem: others
Description: Alarm Active

18.3.3.2 SCC2 Format Sample

24 UMUX302 0001 TBL UMUX FLT
Location: OTT_UMUX_1200
Notification ID: 0
State: Raised
Category: environmental
Cause: others
Time: Mar 17 00:24:26 2005
Component Id: COBUX <11> Board / External Input-1
Specific Problem: others
Description: Alarm Active

18.3.3.3 Syslog Format Sample

Apr 8 01:38:28 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9452~~ UMUX302 TBL UMUX FLT^M Location: OTT_UMUX_1200^M Notification ID: 0^M State: Raised^M Category: environmental^M Cause: others^M Time: Apr 08 02:05:48 2005^M Component Id: COBUX <11> Board / External Input-1^M Specific Problem: others^M Description: Alarm Active

18.3.3.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 16 minutes, 50 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.302:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10: STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48.48.53.45.52.45.56.44.54.58.51.57.58.51.56.46.48.44.23930:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.2: 07 d5 04 08 06 27 26 00:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11: STRING:
DeviceSpecificInfo=;Alarm Active:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1: INTEGER: 5:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2: INTEGER: 1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3: STRING: :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4: STRING:
UMUX302:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.6: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7: INTEGER: 18:

18.3.4 Processing Error Alarms

The UNEM proxy agent sends an alarmRaisedTrap when an event on a UNEM managed entity (i.e. a managed UMUX NE or the UNEM itself) causes a standing processing error condition and has immediate or potential impact on the operation or performance of the entity in question.

Table 30: Processing Error Alarm

Field	Value
Log Name	UNEM or UMUX
Log Number	303
Severity	Minor, Major, or Critical
Event Type	TBL
State	Raised

Table 30: Processing Error Alarm

Field	Value
Category	Processing Error
Probable Cause	Please refer to the alarm text
Description	Please refer to the alarm text
Action	Please refer to the alarm text and consult the appropriate UNEM or UMUX User Guide for the appropriate action.

18.3.4.1 NTSTD Format Sample

wnc0s0jn *** UMUX303 APR21 09:39:32 0483 TBL UMUX FLT
Location: SIMULATED
Notification ID: 0
State: Raised
Category: processingError
Cause: others
Time: Apr 21 08:55 2005
Component Id: SIMULATED
Specific Problem: others
Description: SIMULATED

18.3.4.2 SCC2 Format Sample

34 UMUX303 0001 TBL UMUX FLT
Location: SIMULATED
Notification ID: 0
State: Raised
Category: processingError
Cause: others
Time: Mar 17 10:24:26 2005
Component Id: SIMULATED
Specific Problem: others
Description: SIMULATION

18.3.4.3 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 4 hours, 16 minutes, 55 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.302:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10: STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48.48.53.45.52.45.56.44.54.58.51.57.58.51.56.46.48.44.23930:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.2: 07 d5 04 08 06 27 26 00:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11: STRING:
DeviceSpecificInfo=;Alarm Active:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1: INTEGER: 5:

.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2: INTEGER: 1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3: STRING: :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4: STRING: UMUX303:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5: STRING: IEMS=SIMULATED;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.6: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7: INTEGER: 18:

18.3.5 Quality of Service Alarms

The UNEM proxy agent sends an alarmRaisedTrap when an event on a UNEM managed entity (i.e. a managed UMUX NE or the UNEM itself) causes a standing quality of service condition and has immediate or potential impact on the operation or performance of the entity in question.

Table 31: Quality of Service Alarm

Field	Value
Log Name	UNEM or UMUX
Log Number	304
Severity	Minor, Major, or Critical
Event Type	TBL
State	Raised
Category	Quality of Service
Probable Cause	Please refer to the alarm text
Description	Please refer to the alarm text
Action	Please refer to the alarm text and consult the appropriate UNEM or UMUX User Guide for the appropriate action.

18.3.5.1 NTSTD Format Sample

wnc0s0jn * UMUX304 MAR29 05:40:44 0499 TBL UMUX FLT
Location: OTT_UMUX_1200
Notification ID: 0
State: Raised
Category: qualityOfService
Cause: others
Time: Mar 29 05:40:44 2005
Component Id: LOMIF <12> 2Mbit/s-1 / E12
Specific Problem: others
Description: Near End Degraded Performance

18.3.5.2 SCC2 Format Sample

45 UMUX304 0001 TBL UMUX FLT
Location: OTT_UMUX_1200
Notification ID: 0
State: Raised
Category: qualityOfService
Cause: others
Time: Mar 17 12:24:26 2005
Component Id: COBUX <11> Board / External Input-1
Specific Problem: others
Description: Near End Degraded Performance

18.3.5.3 Syslog Format Sample

Apr 8 01:28:28 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9449~~ UMUX304 MINOR TBL UMUX FLT^M Location: OTT_UMUX_1200^M Notification ID: 0^M State: Raised^M Category: qualityOfService^M Cause: others^M Time: Apr 08 01:55:49 2005^M Component Id: LOMIF <12> 2Mbit/s-1 / E12^M Specific Problem: others^M Description: Near End Degraded Performance

18.3.5.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 12 minutes, 24 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.303:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10: STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48.48.53.45.52.45.56.44.54.58.51.53.58.49.51.46.48.44.23909:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.2: 07 d5 04 08 06 23 0d 00:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11: STRING:
DeviceSpecificInfo=;Near End Degraded Performance:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1: INTEGER: 5:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2: INTEGER: 1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3: STRING: :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4: STRING:
UMUX304:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.6: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7: INTEGER: 17:

18.3.6 Alarm Clear

The UNEM proxy agent sends an alarmClearedTrap when a standing condition on a UNEM managed entity (i.e. a managed UMUX NE or the UNEM itself) has been removed.

Table 32: Alarm Clear Event

Field	Value
Log Name	UNEM or UMUX
Log Number	500
Event Type	INFO
State	Cleared
Description	The standing alarm condition has been cleared
Action	N/A

18.3.6.1 NTSTD Format Sample

wnc0s0jn UMUX500 DEC31 19:00:00 0503 INFO UMUX Clear
Location: OTT_UMUX_1200
State: Cleared
Time: Mar 29 05:37:27 2005
Component Id: COBUX <11> Board / External Input-1
Description: Alarm Active

18.3.6.2 SCC2 Format Sample

00 UMUX500 0018 INFO UMUX Clear
Location: OTT_UMUX_1200
State: Cleared
Time: Mar 31 03:48:34 2005
Component Id: LOMIF <12> 2Mbit/s-1 / E12
Description: Loss of Signal

18.3.6.3 Syslog Format Sample

Apr 8 01:25:04 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9445~~ UMUX500 NONE INFO
UMUX Clear^M Location: OTT_UMUX_1200^M State: Cleared^M
Time: Apr 08 01:25:04 2005^M Component Id: LOMIF <12> Board^M
Description: Unit Not Available

18.3.6.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 2 minutes, 31 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.301:

.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10: STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.11
6.18.50.48.48.53.45.52.45.56.44.51.58.57.58.51.52.46.48.44.23459:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.2: 07 d5 04 08 03 09 22 00:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11: STRING:
DeviceSpecificInfo=;H.248 Association Failure:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1: INTEGER: 5:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2: INTEGER: 1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3: STRING: :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4: STRING:
UMUX500:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-33;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7: INTEGER: 14:

18.3.7 Operational State Change

The following notification type defines the neOpStatModified trap. It indicates a change in the operational state of a UMUX NE.

Table 33: Operation State Change Event

Field	Value
Log Name	UMUX
Log Number	501
Event Type	INFO
State	INFO
Description	The operational state of a UMUX NE has changed
Action	Please refer to the UMUX User Guide for the appropriate action.

18.3.7.1 NTSTD Format Sample

wnc0s0jn UMUX501 MAR29 05:37:27 0515 neOperationalState Change
Location: OTT_UMUX_1200_Test
State: INFO
Time: Mar 29 05:37:27 2005
Component Id: OTT_UMUX_1200_TestOTT_UMUX_1200_Test
Description: op state has transitioned

18.3.7.2 SCC2 Format Sample

33 UMUX501 0014 INFO neOperationalState Change
Location: OTT_UMUX_1200
State: INFO
Time: Mar 31 03:33:27 2005

Component Id: OTT_UMUX_1200OTT_UMUX_1200
Description: op state has transitioned

18.3.7.3 Syslog Format Sample

Apr 8 00:58:13 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9433~~ UMUX501 NONE INFO neOperationalState Change^M Location: OTT_UMUX_1200^M State: INFO^M Time: Apr 08 00:58:13 2005^M Component Id: OTT_UMUX_1200OTT_UMUX_1200^M Description: OTT_UMUX_1200 op state has transitioned 52

18.3.7.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 41 minutes, 42 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING: IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: 07 d5 04 08 06 25 0a 00:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING: UMUX501:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 37 UMUX501 0000 INFO neOperationalState Change :
OTT_UMUX_1200_TESTING op state has transitioned 52:

18.3.8 Polling State Change

The following notification type defines the nePollStatModified trap. It indicates that the UNEM's polling status of the UMUX NE has been modified

Table 34: Polling State Change Event

Field	Value
Log Name	UMUX
Log Number	502
Event Type	INFO
State	INFO
Description	The Polling state of a UMUX NE has changed
Action	Please refer to the UMUX User Guide for the appropriate action.\

18.3.8.1 NTSTD Format Sample

wnc0s0jn UMUX502 MAR29 05:26:57 0508 nePollState Change

Location: OTT_UMUX_1200
State: INFO
Time: Mar 29 05:26:57 2005
Component Id: OTT_UMUX_1200OTT_UMUX_1200
Description: op state has transitioned

18.3.8.2 SCC2 Format Sample

24 UMUX502 0006 INFO nePollState Change
Location: OTT_UMUX_1200
State: INFO
Time: Mar 31 03:24:15 2005
Component Id: OTT_UMUX_1200OTT_UMUX_1200
Description: op state has transitioned

18.3.8.3 Syslog Format Sample

Apr 8 00:44:59 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9430~~ UMUX502 NONE INFO nePollState Change^M Location: RTP_UMUX_1500^M State: INFO^M Time: Apr 08 00:44:59 2005^M Component Id: RTP_UMUX_1500RTP_UMUX_1500^M Description: RTP_UMUX_1500 polling state has transitioned 1

18.3.8.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 2 hours, 28 minutes, 48 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING: IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: 07 d5 04 08 05 18 10 00:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING: UMUX502:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 24 UMUX502 0000 INFO nePollState Change :
OTT_UMUX_1200 polling state has transitioned 1:

18.3.9 Alarm Acknowledgment

The UNEM proxy agent sends an alarmAckedTrap when an outstanding alarm has been acknowledged. IEMS will simply forward the event northbound. IEMS will not reflect this trap in its alarm list.

Table 35: Alarm Acknowledgment

Field	Value
Log Name	UNEM or UMUX

Table 35: Alarm Acknowledgment

Field	Value
Log Number	600
Event Type	INFO
State	INFO
Description	This informational log is sent when an alarm is acknowledged by the UNEM system.
Action	N/A

18.3.9.1 NTSTD Format Sample

wnc0s0jn UMUX600 MAR29 05:38:44 0485 INFO UMUX Ack
Location: OTT_UMUX_1200
State: INFO
Time: Mar 29 05:38:44 2005
Component Id: LOMIF <12> 2Mbit/s-1 / E12
Description: AIS Received

18.3.9.2 SCC2 Format Sample

00 UMUX600 0016 INFO UMUX Ack
Location: OTT_UMUX_1200
State: INFO
Time: Mar 31 03:48:34 2005
Component Id: LOMIF <12> 2Mbit/s-1 / E12
Description: Loss of Signal

18.3.9.3 Syslog Format Sample

Apr 8 01:25:44 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9446~~ UMUX600 NONE INFO
UMUX Ack^M Location: OTT_UMUX_1200^M State: INFO^M
Time: Apr 08 03:52:32 2005^M Component Id: LOMIF <12> Board^M
Description: Unit Not Available

18.3.9.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 8 minutes, 43 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: 07 b1 0c 1f 07 00 00 00:

.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING:
UMUX600:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 00
UMUX600 0057 INFO UMUX Ack :
Unit Not Available:

18.3.10 NE Add

The UNEM proxy agent sends an neAdded trap when a UMUX NE has been added to the UNEM topology inventory. In addition to adding the NE to it's topology, IEMS forwards the informational event NB.

Table 36: Communication Alarm

Field	Value
Log Name	UMUX
Log Number	601
Event Type	INFO
State	INFO
Description	<UMUX Name> NE Added
Action	N/A

18.3.10.1 NTSTD Format Sample

wnc0s0jn UMUX601 MAR29 05:35:35 INFO UMUX Added
Location: OTT_UMUX_1200_Test
State: INFO
Time: Mar 29 05:35:35 2005
Component Id: OTT_UMUX_1200_Test797322492
Description: OTT_UMUX_1200_Test NE Added

18.3.10.2 SCC2 Format Sample

54 UMUX601 0023 INFO UMUX Added
Location: OTT_UMUX_TESTING
State: INFO
Time: Mar 31 03:54:48 2005
Component Id: OTT_UMUX_TESTING 47.134. 44.110
Description: OTT_UMUX_TESTING NE Added

18.3.10.3 Syslog Format Sample

Apr 8 00:59:37 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9434~~ UMUX601 NONE INFO
UMUX Added^M Location: MYTest^M State: INFO^M Time:

Apr 08 00:59:37 2005^M Component Id: MYTest 10. 1. 5. 1^M
Description: MYTest NE Added

18.3.10.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 2 hours, 48 minutes, 38 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING: IEMS=wcarhw4e.ca.nortel.com-UMUX-37;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: STRING: ^G^E,^F^B:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING: UMUX601:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 44 UMUX601 0047 INFO UMUX Added :
UMUX_TESTING(10. 10. 1. 1) NE Added :

18.3.11 NE Deleted

The UNEM proxy agent sends an neDeleted trap when a UMUX NE has been deleted from the UNEM topology inventory. In addition to adding the NE to it's topology, IEMS forwards the informational event NB.

Table 37: Communication Alarm

Field	Value
Log Name	UMUX
Log Number	602
Event Type	INFO
State	INFO
Description	<UMUX Name> NE Deleted
Action	N/A

18.3.11.1 NTSTD Format Sample

wnc0s0jn UMUX602 MAR29 05:40:38 0524 INFO UMUX Deleted
Location: OTT_UMUX_1200_Test
State: INFO
Time: Mar 29 05:40:38 2005
Component Id: OTT_UMUX_1200_Test797322492
Description: OTT_UMUX_1200_Test NE Deleted

18.3.11.2 SCC2 Format Sample

33 UMUX602 0051 INFO UMUX Deleted
Location: RTP_UMUX_1500_TEST
State: INFO
Time: Mar 31 04:33:36 2005
Component Id: RTP_UMUX_1500_TEST 47.142. 87.102
Description: RTP_UMUX_1500_TEST NE Deleted

18.3.11.3 Syslog Format Sample

Apr 8 01:00:18 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9435~~ UMUX602 NONE INFO UMUX Deleted^M Location: MYTest^M State: INFO^M Time: Apr 08 01:00:18 2005^M Component Id: MYTest 10. 1. 5. 1^M Description: MYTest NE Deleted

18.3.11.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 2 hours, 50 minutes, 9 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING: IEMS=wcarhw4e.ca.nortel.com-UMUX-37;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: STRING: ^G^E-%:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING: UMUX602:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 45 UMUX602 0048 INFO UMUX Deleted :
UMUX_TESTING(10. 10. 1. 1) NE Deleted :

18.3.12 NE Name Modified

The UNEM proxy agent sends an neNameModified trap when a UMUX NE Name is changed in the UNEM. IEMS forwards this information event northbound.

Table 38: Communication Alarm

Field	Value
Log Name	UMUX
Log Number	603
Event Type	INFO
State	INFO
Description	<UMUX Name> NE Name Change

Table 38: Communication Alarm

Field	Value
Action	N/A

18.3.12.1 NTSTD Format Sample

wnc0s0jn UMUX603 MAR29 05:36:25 0514 INFO UMUX Name Change
Location: OTT_UMUX_1200_Test
State: INFO
Time: Mar 29 05:36:25 2005
Component Id: OTT_UMUX_1200_Test 47.134. 44.252
Description: OTT_UMUX_1200_Test NE Name Change

18.3.12.2 SCC2 Format Sample

31 UMUX603 0013 INFO UMUX Name Change
Location: OTT_UMUX_1200
State: INFO
Time: Mar 31 03:31:50 2005
Component Id: OTT_UMUX_1200 47.134. 44.252
Description: OTT_UMUX_1200 NE Name Change

18.3.12.3 Syslog Format Sample

Apr 8 01:01:54 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9436~~ UMUX603 NONE INFO
UMUX Name Change ^M Location: RTP_UMUX_1500_MYTEST^M
State: INFO^M Time: Apr 08 01:01:54 2005^M Component Id:
RTP_UMUX_1500_MYTEST 47.142. 87.102^M Description:
RTP_UMUX_1500_MYTEST NE Name Change

18.3.12.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 2 hours,
46 minutes, 45 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: STRING: ^G^E*
:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING:
UMUX603:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 42
UMUX603 0045 INFO UMUX Name Change :
OTT_UMUX_1200_TESTING(797322492) NE Name Changed :

18.3.13 Card Added

The UNEM proxy agent sends a cardAdded event when a card has been added to a managed UMUX inventory. IEMS forwards the event northbound as an informational.

Table 39: Communication Alarm

Field	Value
Log Name	UMUX
Log Number	604
Event Type	INFO
State	INFO
Description	<Card Name> has been added to <NE Name> at <Slot No.>
Action	N/A

18.3.13.1 NTSTD Format Sample

wnc0s0jn UMUX604 APR21 02:54:35 0190 INFO UMUX Card Added
Location: IPSMG
State: INFO
Time: Apr 21 02:54:35 2005
Component Id: IPSMGRTP_UMUX_1500
Description: IPSMG has been added to RTP_UMUX_1500 at 19

18.3.13.2 SCC2 Format Sample

28 UMUX604 0004 INFO UMUX Card Added
Location: RTP_UMUX_1500
State: INFO
Time: Apr 06 00:28:39 2005
Component Id: RTP_UMUX_1500
Description: ISBUQ has been added to RTP_UMUX_1500 at 17

18.3.13.3 Syslog Format Sample

Apr 8 01:09:27 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9440~~ UMUX604 NONE INFO UMUX Card Added^M Location: ISBUQ^M State: INFO^M Time: Apr 08 01:09:27 2005^M Component Id: ISBUQRTP_UMUX_1500_MYTEST^M Description: ISBUQ has been added to RTP_UMUX_1500_MYTESTat 17

18.3.13.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 2 hours, 57 minutes, 19 seconds.:

.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-33;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: STRING: ^G^E4/
^B:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING:
UMUX604:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 52
UMUX604 0000 INFO UMUX Card Added :

18.3.14 Card Deleted

The UNEM proxy agent sends a cardDeleted event when a card has been deleted from a managed UMUX inventory. IEMS forwards the event northbound as an informational.

Table 40: Communication Alarm

Field	Value
Log Name	UNEM or UMUX
Log Number	605
Event Type	INFO
State	INFO
Description	<Card Name> has been deleted from <NE Name> at <Slot No.>
Action	N/A

18.3.14.1 NTSTD Format Sample

wnc0s0jn UMUX605 APR21 02:54:35 0190 INFO UMUX Card Deleted
Location: IPSMG
State: INFO
Time: Apr 21 02:54:35 2005
Component Id: IPSMGRTP_UMUX_1500
Description: IPSMG has been deleted from RTP_UMUX_1500 at 19

18.3.14.2 SCC2 Format Sample

30 UMUX605 0004 INFO UMUX Card Deleted
Location: RTP_UMUX_1500
State: INFO
Time: Apr 06 00:38:35 2005
Component Id: RTP_UMUX_1500
Description: ISBUQ has been deleted from RTP_UMUX_1500 at 17

18.3.14.3 Syslog Format Sample

Apr 8 01:07:18 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9437~~ UMUX605 NONE INFO
UMUX Card Deleted^M Location: ISBUQ^M State: INFO^M
Time: Apr 08 01:07:18 2005^M Component Id:
ISBUQRTP_UMUX_1500_MYTEST^M Description: ISBUQ has been
deleted from RTP_UMUX_1500_MYTESTat 17

18.3.14.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 2 hours,
54 minutes, 12 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-33;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: STRING: ^G^E1(
:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING:
UMUX605:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 49
UMUX605 0000 INFO UMUX Card Deleted :

19: Fault Management (FM): A00009614

19.1 Feature Name

Tamper-proof Key Storage and Event Generation

19.2 Fault management strategy

IEMS and SSPFS will create logs and alarms for:

- Expiration of certificates, expiration of system and local accounts and the passwords for system and local accounts.
- Attempts to add/modify/delete key material including cryptographic keys, userids, passwords, and SNMP community strings.

19.3 Fault management tools and utilities

The scope of this feature in perspective to fault management is to provide a method of reporting information to the end-user; all tools and utilities for the analysis and handling procedures are controlled and maintained by the SESM Alarm Manager or IEMS.

19.4 Logs

Security logs will be created for both successful and failed attempts to add/ modify/ delete key material. Security log examples are shown below.

19.4.1 Database Password Change Logs

<date and time> PROG=pfsora_set_pwd SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=Change_password MESSAGE="Database password change for: <user>"

<date and time> PROG=pfsora_set_pwd SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_EMS_Prov CMD=Change_password MESSAGE="Invalid user for database password change: <user>"

<date and time> PROG=pfsora_set_pwd SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_EMS_Prov CMD=Change_password MESSAGE="Invalid machine used for database password change:< networkId>"

19.4.2 Certificate Creation and Change Logs

<date and time> PROG=apache.sh SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=CERT_Add MESSAGE="Fresh certificate installed"

<date and time> PROG=apache.sh SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=CERT_Mod MESSAGE="Certificate changed"

19.4.3 ssh Key Creation/Change Logs

<date and time> PROG=keygen.sh SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=KEY_Mod MESSAGE="ssh key change"

<date and time> PROG=keygen.sh SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=KEY_Mod MESSAGE="Invalid user for ssh key change: <user>"

<date and time> PROG=keygenWithoutBoopTransferr.sh SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=KEY_Mod MESSAGE="ssh key change"

<date and time> PROG=keygenWithoutBoopTransferr.sh SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=KEY_Mod MESSAGE="Invalid user for ssh key change: <user>"

19.4.4 IPSec IKE Policy Creation and Deletion Logs

Currently, when an IKE policy is added or deleted, a security log is generated. Those logs will be replaced with logs in the new format, shown below. Also, logs will be generated from the server (utility) level.

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IKE rule added. Rule: <IKE rule> "

<date and time> PROG=IKEUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IKE entry added"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE rule deleted. Rule: <IKE rule> "

<date and time> PROG=IKEUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE entry deleted"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="Problem occurred loading IPSec rules on other cluster unit"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="Could not Sync IPSec data”

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IKE rule could not be added. Rule: <IKE rule> ”

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IKE configuration data could not be updated”

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IKE preshared key data could not be updated”

<date and time> PROG=IKEUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IKE entry could not be added"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE key could not be deleted. Rule: <IKE rule>"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE rule could not be deleted. Rule: <IKE rule>"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE rules could not be updated"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE key could not be updated"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE configuration data could not be updated"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE preshared key data could not be updated"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="Problem occurred loading IPSec rules on other cluster unit"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="Could not Sync IPSec data"

<date and time> PROG=IKEUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE entry could not be deleted""

19.4.5 IPSec Key Change Log

Currently, when an IPSec key is changed, a security log is generated. Those logs will be replaced with logs in the new format, shown below. Also, logs will be generated from the server (utility) level.

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Preshared key modified"

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Attempt to modify Preshared key"

<date and time> PROG=IKEUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Preshared key modified"

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Attempt to modify Preshared key"

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Could not change Preshared key"

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="IKE preshared key data could not be updated"

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Problem occurred loading IPSec rules on other cluster unit"

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Could not Sync IPSec data"

<date and time> PROG=IKEUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Could not modify preshared key"

19.4.6 IPSec IPSec Policy Creation and Deletion Logs

Currently, when an IPSec policy is added or deleted, a security log is generated. Those logs will be replaced with logs in the new format, shown below. Also, logs will be generated from the server (utility) level.

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IPSec rule added. Rule: <IPSec rule> "

<date and time> PROG=IPSecUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IPSec entry added"

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IPSec rule deleted. Rule: <IPSec rule> "

<date and time> PROG=IPSecUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IPSec entry deleted"

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="Problem occurred loading IPSec rules on other cluster unit"

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="Could not Sync IPSec data”

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IPSec rule could not be added. Rule: <IPSec rule> ”

<date and time> PROG=IPSecUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IPSec entry could not be added"

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IPSec rule could not be deleted. Rule: <IPSec rule>"

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="Problem occurred loading IPSec rules on other cluster unit"

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="Could not Sync IPSec data"

<date and time> PROG=IPSecUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IPSec entry could not be deleted""

19.5 Alarms

19.5.1 Password Expiration Warning Alarm

```
Component Id     :
cbm850=wnc0s0rv;NODE=wnc0s0rv,CLASS=SEC,SECTYPE=Expiration,OBJECT=password,USER=maint
Severity         : Warn
State            : ISTb
Report Name      : SPFS
Report Number    : 350
Application      : IEMS_EXPIRATION_CHECKER
Algorithm Used   : Algorithm1
Category         : QualityOfService
Event Type       : INFO
Probable Cause   : unspecifiedReason
Description      : password expiry
Specific Problem : The password for user 'maint' will expire in 5 day(s)
User Data        :
Recovery Action  :
Time When Raised : Mon Jan 17 12:57:10 2005
```

19.5.2 Password Expiration

```
Component Id     :
cbm850=<SERVER>;NODE=<SERVER>,CLASS=SEC,SECTYPE=Expiration,OBJECT=password,USER=maint
Severity         : Minor
State            : ISTb
Report Name      : SPFS
Report Number    : 350
Application      : IEMS_EXPIRATION_CHECKER
Algorithm Used   : Algorithm1
Category         : QualityOfService
Event Type       : TBL
Probable Cause   : unspecifiedReason
Description      : password expiry
Specific Problem : The password for user 'maint' has expired
User Data        :
```

```
Recovery Action  :
Time When Raised : <DATE and TIME>
```

19.5.3 Account Expiration Warning Alarm

```
Component Id     :
cbm850=<SERVER>;NODE=<SERVER>,CLASS=SEC,SECTYPE=Expiration,OBJECT=account,USER=maint
Severity         : Warn
State            : ISTb
Report Name      : SPFS
Report Number    : 350
Application      : IEMS_EXPIRATION_CHECKER
Algorithm Used   : Algorithm1
Category         : QualityOfService
Event Type       : INFO
Probable Cause   : unspecifiedReason
Description      : account expiry
Specific Problem : The account for user 'maint' will expire in 5 day(s)
User Data        :
Recovery Action  :
Time When Raised : <DATE and TIME>
```

19.5.4 Account Expiration Alarm

```
Component Id     :
cbm850=<SERVER>;NODE=<SERVER>,CLASS=SEC,SECTYPE=Expiration,OBJECT=account,USER=maint
Severity         : Minor
State            : ISTb
Report Name      : SPFS
Report Number    : 350
Application      : IEMS_EXPIRATION_CHECKER
Algorithm Used   : Algorithm1
Category         : QualityOfService
Event Type       : TBL
Probable Cause   : unspecifiedReason
Description      : account expiry
Specific Problem : The account for user 'maint' has expired
User Data        :
Recovery Action  :
Time When Raised : <DATE and TIME>
```

19.5.5 Certificate Expiration Alarm

```
Component Id     :
cbm850=<SERVER>;NODE=<SERVER>,CLASS=SEC,CLASSTYPE=EXPIRED,SUBTYPE=HTTPSCERT,FILE=<FILE>
Severity         : Minor
State            : ISTb
Report Name      : SPFS
Report Number    : 350
Application      : SSPFS_RES_MON
Algorithm Used   : Algorithm1
Category         : QualityOfService
Event Type       : TBL
Probable Cause   : unspecifiedReason
Description      : certificate expiration
Specific Problem : https certificate has expired
User Data        :
```

```
Recovery Action  :
Time When Raised : <DATE and TIME>
```

19.5.6 Certificate Expiration Alarm Clearing

```
Component Id     :
cbm850=<SERVER>;NODE=<SERVER>,CLASS=SEC,CLASSTYPE=EXPIRED,SUBTYPE=HTTPSCERT,FILE=<FILE>
Severity         : Cleared
State            : InSv
Report Name      : SPFS
Report Number    : 350
Application      : SSPFS_RES_MON
Algorithm Used   : Algorithm1
Category         : QualityOfService
Event Type       : INFO
Probable Cause   : unspecifiedReason
Description      : certificate expiration
Specific Problem : https certificate is no longer expired
User Data        :
Recovery Action  :
Time When Raised : <DATE and TIME>
```

19.6 Related documentation

20: Fault Management (FM): A00009777

20.1 Feature Name

IEMS Mediant 2000 Integration

20.2 Fault management strategy

MG 3200 behaves in a similar way as that of MS2000 devices except for a few new Traps. IEMS will use a similar kind of approach as that of MS2000 to handle the faults form MG 3200 and the additional faults.

SNMP Fault Mapping would remain the same as that of MS2000 for the AcBoard Traps (mentioned on the DID - referenced), coldStart and authenticationFailure traps.

A new Trap named dsx1LineStatusChange will also be forwarded from MG 3200 device. This trap will be mapped to an INFO event in the IEMS.

It is expected that MG 3200 will not send ATM MIB Traps which are a part of MS2000 device.

IEMS will take care of synchronizing the alarms between the IEMS and MG 3200 device. Re-synchronization of Alarms will happen using the IETF MIB support and Notification Log MIB Support available in the MG 3200 device. IEMS assumes that everything relating to this implementation is similar to MS200 device. Re-sync Operation will be invoked under following situations:

1. While Configuring the MG 3200 in to IEMS

2. If IEMS misses a Trap (This will be sequence number based and IEMS assumes that MG 3200 supports alarm retrieval based on its sequence number as in MS2000)

3. When invoking re-synchronization Manually.

4. When ever a coldStart trap is received from the MG 3200

5. During IEMS restart (if the device is present in the db)

The Fault Mapping for the MG 3200 traps are as mentioned below,

Trap Name	OID	LogKey
acBoardFatalError	.1.3.6.1.4.1.5003.9.10.1.21.2.0.1	MGTH301
acBoardConfigurationError	.1.3.6.1.4.1.5003.9.10.1.21.2.0.2	MGTH302

acBoardTemperatureAlarm	.1.3.6.1.4.1.5003.9.10.1.21.2.0.3	MGTH303
acBoardEvBoardStarted	.1.3.6.1.4.1.5003.9.10.1.21.2.0.4	MGTH500
acBoardEvResettingBoard	.1.3.6.1.4.1.5003.9.10.1.21.2.0.5	MGTH300
acgwAdminStateChange	.1.3.6.1.4.1.5003.9.10.1.21.2.0.7	MGTH501
acBoardEthernetLinkAlarm	.1.3.6.1.4.1.5003.9.10.1.21.2.0.10	MGTH307
acActiveAlarmTableOverflow	.1.3.6.1.4.1.5003.9.10.1.21.2.0.12	MGTH309
acOperationalStateChange	.1.3.6.1.4.1.5003.9.10.1.21.2.0.15	MGTH312
acKeepAlive	.1.3.6.1.4.1.5003.9.10.1.21.2.0.16	MGTH313
acNATTraversalAlarm	.1.3.6.1.4.1.5003.9.10.1.21.2.0.17	MGTH314
acEnhancedBITStatus	.1.3.6.1.4.1.5003.9.10.1.21.2.0.18	MGTH600
acPerformanceMonitoringThresholdCrossing	.1.3.6.1.4.1.5003.9.10.1.21.2.0.27	MGTH800
dsx1LineStatusChange	.1.3.6.1.2.1.10.18.15.0.1	MGTH601
coldStart	.1.3.6.1.6.3.1.1.5.1	Will not be sent to NB All prior alarms from the device will be cleared and "Re-sync" operation will be invoked as the device has been reset.
authenticationFailure	.1.3.6.1.6.3.1.1.5.5	Will not be sent to NB

Apart from these, the Trap VarBinds will be parsed and mapped in to event properties as follows,

IEMS Event Property	**Values associated for the Property**
Name	From Trap Varbind: *acBoardTrapGlobalsName*
LogName	MGTH
LogNumber	As specified in Fault Mapping table provided above
Source	From Trap Varbind: *acBoardTrapGlobalsSource*
Unique ID	acBoardTrapGlobalsUniqID

Severity	From Trap Varbind: *acBoardTrapGlobalsSeverity* (based on its value severity will vary) dsx1LineStatusChangeTrap will be given a INFO severity
EventType	FLT for "Raise" events and INFO for "Clear" events
State	Will be based on the severity value. For traps with severity Clear (i.e. severity =5) the state will be "*Clear*" , for all other severity the state will be "*Raise*".
Category	From Trap Varbind: *acBoardTrapGlobalsType* (communications | qualityOfService | processingError | equipment | environmental | other)
Probable Cause	From Trap Varbind: *acBoardTrapGlobalsProbableCause*.
Specific Problem	Value to be provided
Description	From Trap Varbind: *acBoardTrapGlobalsTextualDescription*.
Info1	From Trap Varbind: *acBoardTrapGlobalsAdditionalInfo1*
Info2	From Trap Varbind: *acBoardTrapGlobalsAdditionalInfo2*
Info3	From Trap Varbind: *acBoardTrapGlobalsAdditionalInfo3*
Time	From Trap Varbind: *acBoardTrapGlobalsDateAndTime*

NorthBound SCC2 Log format:

*C32 MGTH301 0001 FLT MG3200 FAULT
Location: MG;192.168.113.144
State: Raised
Category: communications
Cause: congestion
Time: Apr 08 12:32:34 2005
Component Id: MG 3200
Trap Name: 1
Description: Fake trap generated for the trap acBoardFatalError

NorthBound NTSTD Log format:

Nortel *** MGTH301 APR08 12:32:34 0001 FLT MG3200 FAULT
Location: MG;192.168.113.144
State: Raised
Category: communications
Cause: congestion
Time: Apr 08 12:32:34 2005
Component Id: MG 3200
Trap Name: 1
Description: Fake trap generated for the trap acBoardFatalError

21: Fault Management (FM): A00009822

21.1 Feature Name

General Security Log When the User Logs Out

21.2 Fault management strategy

This feature logs the interaction with Client Session Monitor. A security log is generated when the Client Session Monitor processes the notification of the authentication and client lifetime events. Logs are generated as per the MFT Logging Guidelines(FW3.3 Loggin Service Guidelines).

21.3 Fault management tools and utilities

21.3.1 Faults, Alarms and Logs

The logs output are information only logs.

Security logs are generated for registering successful authentications to the Client Session Monitor. If the Client Session Monitor can not decrypt the information received to register authentication or client lifetime events, an information log is output. Security logs are generated when the clients indicate a successful login and logout.

21.4 Logs

21.4.1 Formats

The format of a security log is

Date Logger Src_usr Src Dst Stat Evnt_type Cmd Message

21.4.2 Explanation

21.4.2.1 Authentication

When the Client Session Monitor interface is called to register an authentication event, the following example log is output to the security log

Mar 31 18:27:48 wnc0y0nr PROG=CSNotifierEngine.java SRC.USR=rtpu SRC=47.142.122.200 STAT=Success EVNT.TYPE=USER_ACT_Security CMD=SESSION_AUTHENTICATED MESSAGE="User Authenticated: SID = 53, LastLoggedIn=Last login: Thu Mar 31 18:28:00 EST 2005 from 47.142.211.68 to 47.142.122.200"

This is an information log only, no action is required.

21.4.2.2 Client start

When the Client Session Monitor interface is called to register a client start event, the following example log is output to the security log:

Mar 31 18:18:10 wnc0y0nr PROG=CSNotifierEngine.java SRC.USR=rtpu SRC=47.142.122.200 STAT=Success EVNT.TYPE=USER_ACT_Security CMD=SESSION_START MESSAGE="doSessionStart Successful: SID = 52"

This is an information log only, no action is required.

21.4.2.3 Client stop

When the Client Session Monitor interface is called to register a client stop event, the following example log is output to the security log:

Mar 31 17:55:19 wnc0y0nr PROG=CSNotifierEngine.java SRC.USR=UNKNOWN SRC=47.142.122.200 STAT=Success EVNT.TYPE=USER_ACT_Security CMD=SESSION_STOP MESSAGE="doSessionEnd Stopped: SID = 42, Reason = User Exit"

This is an information log only, no action is required.

21.4.2.4 Could not decrypt

When the Client Session Monitor interface can not decrypt the information received, the following example log is output to the security log:

Feb 21 18:30:33 comp5iems CSM:class_security.ver02 SRC_USR="rtpo" STAT=”Fail”EVNT_TYPE=”USER_ACT_Security” CMD=”SESSION_Authentication” MESSAGE=”RegisterClientSessionStopCould not decrypt message”

21.4.2.5 Mark done

When the Client Session Monitor receives a request to manually mark an active session as stopped (.e.g. the Mark Done from the GUI is executed), the following example log is output to the security log:

Apr 2 07:17:28 wnc0y0nr PROG=CSNotifierEngine.java SRC.USR=UNKNOWN SRC=47.142.211.35 STAT=Success EVNT.TYPE=USER_ACT_Security CMD=SESSION_STOP MESSAGE="doSessionEnd Stopped: SID = 237, Reason = Admin Marked Done"

21.4.2.6 SID not valid

When the Client Session Monitor interface is called to register a client start or stop event and the session Id is not valid, the following example log is output to the security log:

Feb 21 18:30:33 comp5iems CSM:class_security.ver02 SRC_USR="rtpo" STAT=”Fail”EVNT_TYPE=”USER_ACT_Security”

CMD=”SESSION_Stop” MESSAGE=”RegisterClientSessionStop dropping invalid session stop because SID not valid: SID=5678”

21.4.3 Field descriptions

Table 41: MFT Security Log Fields

Field Name	Type	Max	Max length Syslog	Definition	Required
Date	*Date*		*15 +1*	*ISO 8601 standard format expressed as yyyyMMddhhmmssZ in java.text.Simple-DateFormat notation. This field is expected in all logs*	*Mandatory*
Level	*String*	*16*	*5*	*ASCII expression of logging level and not an integer.*	*Mandatory*
Logger	*String*	*256*		*ASCII expression of the logger name as chosen by the application that does the logging*	*Mandatory*
Src_usr	*String*	*128*	*8+32+3*	*The source user name or identification*	*Mandatory*
Src	*String*	*256*	*39+1*	*The value should contain the source device’s host name, or its IP address and (optionally) the port number.*	*Mandatory*
Process	*String*	*32*	*32+1*	*The value should contain the process name and process ID for the process on the device that generated the message.*	*Mandatory*
Msg	*String*	*1024*	*4+64+3*	*The log message itself.*	*Mandatory*
Stat	*String*	*32*	*5+7+3*	*The state or status of the process. Possible values: Failure, Success, Start or End*	*Mandatory*
Log_type	*String*	*64*	*9+11+3*	*Type of the log message. Possible values: Trace, Application, Security, Exception*	*Mandatory*
Dst	*String*	*256*	*4+39+3*	*The address of the destination in the same format as the source*	*Mandatory*
Doc	*String*	*1024*	*4+64+3*	*The name of the accessed resource*	*Mandatory*
Mid	*String*	*64*	*4+64+3*	*The concept is to log message identifiers instead of actual messages so that the message identifier can be used to look up a language specific form of the message in display tools*	*Mandatory*

Table 41: MFT Security Log Fields

Field Name	Type	Max	Max length Syslog	Definition	Required
Src_offend	*String*	*256*	*11+39+3*	*The address of the originating device generating information which triggered a security log event in the same format as the source*	*Optional*
Dst_usr	*String*	*128*	*8+32+3*	*The destination user name or identification*	*Optional*
Src_mail	*String*	*128*	*9+32+3*	*The source email address*	*Optional*
Vol	*Integer*		*4+10+1*	*The number of bytes*	*Optional*
Vol_sent	*Integer*		*9+10+1*	*The number of bytes sent*	*Optional*
Vol_rcvd	*Integer*		*9+10+1*	*The number of bytes received*	*Optional*
Cnt	*Integer*		*4+10+1*	*The number of articles, files, events*	*Optional*
Cnt_sent	*Integer*		*9+10+1*	*The number of articles, files, events sent*	*Optional*
Cnt_rcvd	*Integer*		*9+10+1*	*The number of articles, files, events received*	*Optional*
Host	*String*	*256*	*5+39+3*	*The name of the host that issues the log*	*Optional*
Host_type	*String*	*64*	*10+32+3*	*The device type from which the log was generated*	*Optional*
Prog_file	*String*	*256*	*10+32+3*	*The name of the program source file from which the log was generated*	*Optional*
Prog_line	*Integer*		*10+10+1*	*The line number of the Prog_source file*	*Optional*
Tty	*String*	*16*	*4+16+3*	*The tty field describes the user's physical connection to the host*	*Optional*
Prot	*String*	*64*	*5+8+3*	*The protocol field specifies the protocol used*	*Optional*
Cmd	*String*	*1024*	*4+64+3*	*The command field is an issued command*	*Optional*
Evnt_type	*String*	*64*	*10+32+3*	*The evnet type field specifies the type or classification of the event*	*Optional*
Src_oid	*String*	*64*	*8+64+3*	*The object identifier is a unique registration number for a device, which will be part of the X.500 directory*	*Optional*

Table 41: MFT Security Log Fields

Field Name	Type	Max	Max length Syslog	Definition	Required
Log_date	*String*		*15+1*	*The original date of the log message. Used when logs are spooled and held before being sent by the logging service to the final destination*	*Optional*

21.4.4 Action

No immediate action required

21.4.5 Associated OMs or PMs

None

21.4.6 Additional information

None

21.5 Alarms

None

21.6 Related documentation

FW3.3 Logging Service Guidelines

22: Fault Management (FM): A00009893

22.1 Feature Name

Session Server Call Processing Overload

22.2 Fault management strategy

To provide notification of SIP Gateway application overload-related events on the Session Server, new logs and alarms are created by this activity.

22.3 Fault management tools and utilities

22.3.1 Faults, Alarms and Logs

New STGW700 logs are added to cover various scenarios:

- Generated when the Flow Control Rate changes. Note that this log can be generated when the application is not in overload, such as when it is still recovering from an earlier overload state.
- Generated when an IP address is either removed from or re-added to the Access Control List as a result of babbling node isolation.
- Generated when a critical, major or minor CPU occupancy level has been reached.

22.4 STGW700 SIP Gateway Application FCR Change Log

22.4.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	NONE
Event Type	INFO
Label	SIPOVLD
Component ID	SIPC
Description	FCR Change OLD FCR: <0-100> NEW FCR: <0-100>

22.4.2 Action

None.

22.4.3 Associated Operational Measurements or Performance Measurements

OM group SIPGW_OVERLOAD

22.4.4 Additional information

22.5 STGW700 Babbling node detected log

22.5.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	NONE
Event Type	INFO
Label	SIPOVLD
Component ID	SIPC
Description	Babbling node detected, <server name> <IP addresss> IP disabled

22.5.2 Action

None

22.5.3 Associated Operational Measurements or Performance Measurements

None

22.5.4 Additional information

22.6 STGW700 Babbling node timeout Log

22.6.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	NONE
Event Type	INFO
Label	SIPOVLD

Component ID	SIPC
Description	Babbling node timeout, <server name> <IP addresss> IP enabled

22.6.2 Action

None

22.6.3 Associated Operational Measurements or Performance Measurements

None

22.6.4 Additional information

22.7 STGW700 Babbling node initialization Log

22.7.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	NONE
Event Type	INFO
Label	SIPOVLD
Component ID	SIPC
Description	All babbling node IPs re-enabled due to initialization

22.7.2 Action

None

22.7.3 Associated Operational Measurements or Performance Measurements

None

22.7.4 Additional information

22.8 STGW700 CPU occupancy critical alarm Log

22.8.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	CRITICAL
Event Type	TBL
Label	SIPOVLD
Component ID	SIPC
Description	CPU occupancy critical alarm

22.8.2 Action

None

22.8.3 Associated Operational Measurements or Performance Measurements

OM group SIPGW_OVERLOAD

22.8.4 Additional information

22.9 STGW700 CPU occupancy major alarm Log

22.9.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	MAJOR
Event Type	TBL
Label	SIPOVLD
Component ID	SIPC
Description	CPU occupancy major alarm

22.9.2 Action

None

22.9.3 Associated Operational Measurements or Performance Measurements

OM group SIPGW_OVERLOAD

22.9.4 Additional information

22.10 STGW700 CPU occupancy minor alarm Log

22.10.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	MINOR
Event Type	TBL
Label	SIPOVLD
Component ID	SIPC
Description	CPU occupancy minor alarm

22.10.2 Action

None

22.10.3 Associated Operational Measurements or Performance Measurements

OM group SIPGW_OVERLOAD

22.10.4 Additional information

22.11 Alarms

22.11.1 CPU Occupancy Critical

This alarm is generated when the CPU occupancy reaches the critical alarm threshold level.

Table 1 NGSS Alarm GUI Field descriptions

Field	Value
Severity	Critical
Category	Quality of Service Alarm

Table 1 NGSS Alarm GUI Field descriptions

Field	Value
Description	CPU Occupancy reached critical threshold level
LogName	STGW
LogNumber	700
EventType	TBL
EventLabel	SIPOVLD
ProbableCause	No Probable Cause

22.11.2 CPU Occupancy Major

This alarm is generated when the CPU occupancy reaches the major alarm threshold level.

Table 2 NGSS Alarm GUI Field descriptions

Field	Value
Severity	Major
Category	Quality of Service Alarm
Description	CPU Occupancy reached major threshold level
LogName	STGW
LogNumber	700
EventType	TBL
EventLabel	SIPOVLD
ProbableCause	No Probable Cause

22.11.3 CPU Occupancy Minor

This alarm is generated when the CPU occupancy reaches the minor threshold level.

Table 3 NGSS Alarm GUI Field descriptions

Field	Value
Severity	Minor
Category	Quality of Service Alarm
Description	CPU Occupancy reached minor threshold level

Table 3 NGSS Alarm GUI Field descriptions

Field	Value
LogName	STGW
LogNumber	700
EventType	TBL
EventLabel	SIPOVLD
ProbableCause	No Probable Cause

22.12 Related documentation

23: Fault Management (FM): A00011827

23.1 Feature Name

GWC Autonomous SWACT

23.2 Fault management strategy

Two new critical CMT alarms are introduced by this activity. The new alarms identify the following conditions:

- Communication with the GWC's associated gateways is down
- Autonomous SWACT initiated

The first alarm is raised if communication to the GWC's associated gateways is lost. This alarm is cleared when communication is detected with at least one associated gateway. It is also cleared when the GWC is manually or automatically SWACT and is raised again on the newly active unit if communication is still lost with all the associated gateways.

The second alarm is raised when an autonomous SWACT is initiated due to a loss of communication to all the associated media gateways. This alarm indicates that the system has taken action in an attempt to restore communication. This alarm remains active until manually cleared or gets automatically cleared when the GWC is SWACT back to the original active unit.

These alarms are raised in addition to the existing major alarms raised against each gateway that loses communication with the GWC. These alarms are raised prior to the SWACT and cleared as communication is restored to each individual gateway after the SWACT.

23.3 Fault management tools and utilities

23.3.1 Faults, Alarms and Logs

New logs and alarms are generated as tools to identify a potential network outage. The new alarms are:

- GWC 318 - Indicates that an autonomous SWACT has been initiated
- GWC 319 - Indicates that communication with the GWC's associated gateways is down

Along with the alarms the following logs are generated.

- PM181 - GWC SWACT indication with reason

23.4 Logs

23.4.1 Log Title/Log ID: PM181

23.4.1.1 Formats

23.4.1.1.1 NTSTD

Row 1:<Log Header>
Row 2:<Event>
Row 3:<Reason>

23.4.1.2 Example

RTPY09AW PM181 APR27 08:13:20 2502 INFO GWC 7
GWC activity dropped.
Reason: no GW communication

23.4.1.3 Explanation

The existing PM181 is used to report a GWC SWACT has occurred. The format of this log is unchanged.

The Autonomous SWACT activity adds a new reason to the PM181 log to indicate the cause of the autonomous SWACT. In this case, the reason indicates that a SWACT has occurred due to loss of communication with all associated media gateways.

23.4.1.4 Field descriptions

Table 42: Field descriptions

Field	Value	Description
Reason	no GW communication	Communication with all associated media gateways has been lost.

23.4.1.5 Action

This log indicates a problem in the network exists. The Element Managers for related network components should be used to identify the root cause.

23.4.1.6 Associated Operational Measurements or Performance Measurements

N/A

23.4.1.7 Additional information

None

23.5 Alarms

23.5.1 GWC 318

23.5.1.1 Integrated Element Manager GUI Fields

Table 43: IEMS/SESM Alarm GUI Field descriptions: GWC 318

Field	Value
Severity	Critical
Category	Communications
LogName	GWC
LogNumber	318
ProbableCause	Underlying resource unavailable
SpecificProblem	<Element Name>: No communication with associated media gateway(s)
BodyText	Autonomous SWACT initiated

23.5.1.2 Example of Alarm in CMT Alarm Manager

Log Name:GWC 318
NE Name:GWC-9-UNIT-0
Alarm Level:Critical
Category:Communications
Alarm Time:15:17:33 16-Nov-2005 EST
Probable Cause:Underlying resource unavailable
SystemUptime:23 hours, 10 minutes, 4 seconds.
Component ID: GWC=GWC-9-UNIT-0;Version=GN91AWJK; Unit=unit_0;Soft-ware=AUTOSWACT
Alarm Description: Autonomous SWACT initiated
Specific Problem: GWC-9-UNIT-0: No communication with associated media gateway(s)

23.5.1.3 Explanation

Description: This log indicates that the autonomous SWACT has been initiated to restore communication with the GWC's associated media gateways.

Severity: Critical

23.5.1.4 Action

The Element Managers for related network components should be consulted to identify failures within the network. This alarm can be manually cleared or gets automatically cleared when the GWC is swact back to the original active unit.

23.5.1.5 Corresponding Clear Log

GWC 399

23.5.1.6 Syslog Format of Alarm Clear

Nov 17 01:48:39 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=1510~~ GWC399 NONE INFO GWC Fault^M Location: GWC-9-UNIT-0^M NotificationID: 5^M State: Clear^M Time: Nov 16 15:17:54 2005^M Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK;Unit=unit_0; Software=AUTOSWACT^M Description: Autonomous SWACT initiated

23.5.1.7 NTSTD

znc0s0jh *** GWC 318 NOV16 15:17:33 0126 TBL GWC Fault
Location: GWC-9-UNIT-0
NotificationID: 5
State: Raise
Category: communications
Cause: underlyingResourceUnavailable
Time: Nov 16 15:17:33 2005
Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK; Unit=unit_0;Software=AUTOSWACT
Specific Problem: GWC-9-UNIT-0: No communication with associated media gateway(s)
Description: Autonomous SWACT initiated

23.5.1.8 SCC2

*C17 GWC 318 0115 TBL GWC Fault
Location: GWC-9-UNIT-0
NotificationID: 5
State: Raise
Category: communications
Cause: underlyingResourceUnavailable
Time: Nov 16 15:17:33 2005
Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK; Unit=unit_0;Software=AUTOSWACT
Specific Problem: GWC-9-UNIT-0: No communication with associated media gateway(s)
Description: Autonomous SWACT initiated

23.5.1.9 Syslog

Nov 17 01:48:18 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=1500~~ GWC318 CRIT TBL GWC Fault^M Location: GWC-9-UNIT-0^M NotificationID: 5^M State: Raise^M Category: communications^M Cause: underlyingResourceUnavailable^M Time: Nov 16 15:17:33 2005^M Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK;Unit=unit_0;Software=AUT^M OSWACT^M Specific Problem: GWC-9-UNIT-0: No communication with associated media g^M ateway(s)^M Description: Autonomous SWACT initiated

23.5.1.10 SNMP

sysUpTime. => 12:46:43
snmpTrapOID. => nnExtAlarmCritical
mib-2. =>
1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.28.50.48.48.53.45.49.49.45.49.54.44.49.53.58.51.48.58.52.53.46.48.44.45.48.53.58.48.48.5565
mib-2. => <bel>i<vt><dle><si><rs>-<nul>-<enq><nul>
mib-2. => Autonomous SWACT initiated
nnExtAlarmActiveEventType => 2
nnExtAlarmActiveProbableCause => 554
nnExtAlarmActiveAdditionalText => GWC-9-UNIT-0: No communication with associated media gateway(s)
nnExtAlarmActiveDocumentationPointer => GWC318
nnExtAlarmActiveResourceDescription => IEMS=0x00000063000000a12f8e809a-GWC-9-UNIT-0;GWC=GWC-9-UNIT-0;Version=GN91AWJK;Unit=unit_0;Software=AUTOSWACT
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 1208

23.5.2 GWC 319

23.5.2.1 Integrated Element Manager GUI Fields

Table 44: IEMS/SESM Alarm GUI Field descriptions: GWC 319

Field	Value
Severity	Critical
Category	Communications
LogName	GWC
LogNumber	319
ProbableCause	Underlying resource unavailable
SpecificProblem	<Element Name>: No communication with associated media gateway(s)
BodyText	GWC communication loss with associated media gateway(s)

23.5.2.2 Example of Alarm in CMT Alarm Manager

Log Name:GWC 319
NE Name:GWC-9-UNIT-0
Alarm Level:Critical
Category:Communications
Alarm Time: 15:17:23 16-Nov-2005 EDT
Probable Cause:Underlying resource unavailable
SystemUptime:22 hours, 38 minutes, 51 seconds.
Component ID: GWC=GWC-9-UNIT-0;Version=GN91AWJK; Unit=unit_0;Software=SSC
Alarm Description: GWC communication loss with associated media gateway(s)
Specific Problem: GWC-9-UNIT-0: No communication with associated media gateway(s)

23.5.2.3 Explanation

Description: This log indicates that communication to the GWC's associated media gateways is down.

Severity: Critical

23.5.2.4 Action

The Element Managers for related network components should be consulted to identify failures within the network. This log will be cleared after a swact but is raised again on the newly active unit if communication is still lost with all the associated gateways.This log will be cleared when communication to at least one gateway is restored.

23.5.2.5 Corresponding Clear Log

GWC 399

23.5.2.6 Syslog Format of Alarm Clear

Nov 17 01:48:39 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=1510~~ GWC399 NONE INFO GWC Fault^M Location: GWC-9-UNIT-0^M NotificationID: 4^M State: Clear^M Time: Nov 16 15:17:54 2005^M Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK;Unit=unit_0;Software=SSC^M Description: GWC communication loss with associated media gateway(s)

23.5.2.7 NTSTD

znc0s0jh *** GWC319 NOV16 15:17:23 0125 TBL GWC Fault
Location: GWC-9-UNIT-0
NotificationID: 4
State: Raise
Category: communications
Cause: underlyingResourceUnavailable
Time: Nov 16 15:17:23 2005
Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK; Unit=unit_0;Software=SSC
Specific Problem: GWC-9-UNIT-0: No communication with associated media gateway(s)
Description: GWC communication loss with associated media gateway(s)

23.5.2.8 SCC2

*C17 GWC 319 0114 TBL GWC Fault
Location: GWC-9-UNIT-0
NotificationID: 4
State: Raise
Category: communications
Cause: underlyingResourceUnavailable
Time: Nov 16 15:17:23 2005
Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK; Unit=unit_0;Software=SSC
Specific Problem: GWC-9-UNIT-0: No communication with associated media gateway(s)
Description: GWC communication loss with associated media gateway(s)

23.5.2.9 Syslog

Nov 17 01:48:09 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=1499~~ GWC319 CRIT TBL GWC Fault^M Location: GWC-9-UNIT-0^M NotificationID: 4^M State: Raise^M Category: communications^M Cause: underlyingResourceUnavailable^M Time: Nov 16 15:17:23 2005^M Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK;Unit=unit_0;Software=SSC^M Specific Problem: GWC-9-UNIT-0: No communication with associated media g^M ateway(s)^M Description: GWC communication loss with associated media gateway(s)

23.5.2.10 SNMP

sysUpTime. => 12:46:33
snmpTrapOID. => nnExtAlarmCritical
mib-2. =>
1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.28.50.48.48.53.45.49.49.45.49.54.44.49.53.58.51.48.58.51.53.46.48.44.45.48.53.58.48.48.5563
mib-2. => <bel>i<vt><dle><si><rs>#-<nul>-<enq><nul>
mib-2. => GWC communication loss with associated media gateway(s)
nnExtAlarmActiveEventType => 2
nnExtAlarmActiveProbableCause => 554
nnExtAlarmActiveAdditionalText => GWC-9-UNIT-0: No communication with associated media gateway(s)
nnExtAlarmActiveDocumentationPointer => GWC319
nnExtAlarmActiveResourceDescription => IEMS=0x00000063000000a12f8e809a-GWC-9-UNIT-0;GWC=GWC-9-UNIT-0;Version=GN91AWJK;Unit=unit_0;Software=SSC
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 1206

24: Fault Management (FM): A00012183

24.1 Feature Name

Public Key Manager

24.2 Fault management strategy

This document describes the fault management details for all the components of feature A00012183 - IPSEC PKI Support. This document includes the following components:

- PKManager
- GWCEM
- MG9kEM
- SSM

PKManager applies the following strategy:

- Security logs are monitored by security personnel and are first to be notified of impending expiring certificates via logs. Alarms are monitored by maintenance / fault personnel so alarms are last resort signals.
- Security logs are generated for any changes to alarm level or alarm threshold configuration. PKManager certificate generation activity or replacement (distribution) activities, revocation and certificate request generation.
- Generate standard audit logs and SSPFS security logs for all operations that involve security parameters, any key input by an operator, any change to which key to use (imported vs. internally generated).
- Generate major alarm when key generation fails and when certificate distribution fails.
- Generate security logs and escalating alarms as indicated below when certificate approaches its expiration date based on configured major alarm in advance time and configured minor alarm in advance time.
- PKManager will alarm imported certificate expirations only. Expiration of internally generated certificate results in generation and distribution of new certificate to EM. A log is generated not an alarm.
- Clear alarm and generate security log when alarmed certificate is replaced.

Thresholds for alarm level escalation for certificates with impending expiration dates are listed below. The maximum severity for non-call process service affecting certificates is a major alarm. Only certificates whose expiration is impending that are used as part of call control or call processing operations are to escalate to a critical alarm level.

Minor alarm - default threshold is 168 hours. This time is configurable by an operator at the PKGUI.

Major alarm - default threshold is 72 hours. This time is configurable by an operator at the PKGUI but must be less than minor alarm. Highest level for non-call control related certificates i.e. OAM&P, HTTPS

Critical alarm - call control related certificate has expired.

GWCEM applies the following strategy:

GWCEM uses existing SESM fault management structure.

MG9kEM applies the following strategy:

Existing Mg9kEM fault management framework and structure is followed.

SSM applies the following strategy:

The existing Fault Management strategy will apply to the faults for SSM PKI.

24.3 Fault management tools and utilities

PKManager -

The PKI GUI provides the ability for users to browse outstanding alarms generated by the PKManager.

GWCEM -

GWCEM uses existing SESM Alarm Manager to support alarm reporting, alarm history retrieval and browsing.

Mg9kEM -

MG9kEM alarms can be viewed from the Alarm Browser GUI.

SSM -

No special tools required for SSM logs.

24.4 Logs

PKManager Log Section:

Security logs are generated for any changes to alarm level or alarm threshold configuration or replacement (distribution) activities, revocation and certificate request generation. A log is generated when an internally generated certificate expires. Security personnel and are notified of impending expiring certificates via logs.

Security Log location
The Security Log file is stored at:

/var/log/securitylog

24.4.1 PKManager Certificate Generation Logs

24.4.1.1 Certificate Request Created
PKManager will log creation of a certificate request for export.

24.4.1.1.1 Security Log output
Sep 23 16:58:54 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS CMD="Generate CSR" MESSAGE="Certificate signing request was created for CN, GWC-10 47.142.33.5"

24.4.1.2 Certificate Request Received
PKManager will log reception of a certificate request from integrated client applications.

24.4.1.2.1 Security Log output
Sep 28 14:25:37 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER SRC=wnc0s0jd STAT=Start EVNT.TYPE=SYSTEM_EVENT_EMS CMD="Generate Certif" MESSAGE="Processing a request to create a certificate for CN, wnc0s0r8.us.nortel.com 47.142.148.6"

24.4.1.3 Certificate Created
PKManager will log successful creation of an X509 certificate.

24.4.1.3.1 Security Log output

Sep 30 14:57:15 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS CMD="Certif Created" MESSAGE="Certificate was created for CN, TestCert1 47.133.32.16"

24.4.1.4 Certificate Delivered
PKManager will log successful delivery of an X509 certificate.

24.4.1.4.1 Security Log output

Sep 28 14:30:49 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS CMD="Certif Delivered" MESSAGE="Certificate was created for CN, wnc0s0jd.us.nortel.com 47.142.94.74"

24.4.1.5 Certificate Request Rejected

PKManager will log invalid and rejected certificate requests.

24.4.1.5.1 Security Log output

Sep 28 14:24:50 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER SRC=wnc0s0jd STAT=Failure EVNT.TYPE=SYSTEM_EVENT_EMS CMD="Generate Certif" MESSAGE="Invalid certificate request for CN, wnc0s0r8.us.nortel.com 47.142.148.6"

24.4.2 Certificate Revocation and Replacement

24.4.2.1 Certificate Revoked

PKManager will log revocation of certificates.

24.4.2.1.1 Security Log output

Sep 30 15:49:55 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS CMD="Revoke Certif" MESSAGE="Revoked certificate CN, TestCert1 47.133.32.16"

24.4.2.2 Replacement Certificate Request

PKManager will log X509 certificate replacement requests.

24.4.2.2.1 Security Log output

Sep 30 15:53:22 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER SRC=wnc0s0jd STAT=Start EVNT.TYPE=SYSTEM_EVENT_EMS CMD="Replace Certif" MESSAGE="Processing request to replace certificate for CN, GWC-10 47.142.33.5"

24.4.3 Invalid, Expiring and Expired Certificate

24.4.3.1 Invalid Certificate

PKManager will log certificates that fail validation.

24.4.3.1.1 Security Log output

Sep 28 14:24:50 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER SRC=wnc0s0jd STAT=Failure EVNT.TYPE=SYSTEM_EVENT_EMS CMD="Validate Certificate" MESSAGE="Certificate serial number 262 CN, wnc0s0r8.us.nortel.com 47.142.148.6 is invalid"

24.4.3.2 Approaching Certificate Expiration

PKManager will log certificates approaching expiration in advance of expiration as configured in the system.

24.4.3.2.1 Security Log output

Sep 28 16:58:45 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS CMD="Advance Notice" MESSAGE="Certificate serial number 261, CN, GWC-10 47.142.33.5 will expire on 2005-10-04 00:00:00.0"

24.4.3.3 Last Notice Before Certificate Expiration

PKManager will log a final notice in advance of expiration as configured in the system.

24.4.3.3.1 Security Log output

Sep 28 17:10:47 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS CMD="Last Notice" MESSAGE="Certificate serial number 261, CN, GWC-10 47.142.33.5 will expire on 2005-10-01 00:00:00.0"

24.4.3.4 Expired Certificate

PKManager will log expired X509 certificates.

24.4.3.4.1 Security Log output

Sep 28 17:18:49 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS CMD="Certif Expired" MESSAGE="Certificate serial number 261, CN, GWC-10 47.142.33.5 has expired"

GWCEM Log Section:

No new customer logs.

MG9kEM Log Section:

24.4.4 New MGEM715 audit log

24.4.4.1 Formats

This audit log is generated whenever a user attempts to set or clear the “Use Certificate” indicator for the NE. The audit can be found at: /var/log/auditlog.

Here is an example of the new MGEM715 log:

```
Jun 25 15:07:28 wnc1s04n MGEM: joeuser 704
Clearing use certificate indicator MG9K: co33 [33]
```

Here is the description of the fields:

Table 1 Field descriptions

Field	Description	Example
Date/Time	Date and Time stamp of the log	Jun 25 15:07:28
Host Name	Host machine name	wnc1s04n
Application Name	Specifies the application producing the log.	MGEM
User Name	User name attempting the action	joeuser
Log number	The log number	704
Log Text	Specifies the action attempted and any associated details.	Clearing use certificate indicator MG9K: co33 [33]

24.4.4.2 Action

This log is informational, no action is required.

SSM Log Section:

24.4.5 SSPFS IPsec syslog messages

The Solaris implementation of IPsec automatically sends all failure logs to syslog /var/adm/messages. We do not have control over this. However when the servlet makes any changes to the IPsec security rules, the wrapper scripts will output any attempted changes to /var/log/securitylog.

The Solaris IPsec itself does not seem to generate any failure messages because security could be compromised, however IKE does seem to generate failure messages to syslog.

Sample IKE failure message would look like this.

```
messages.0:Mar 25 15:40:04 wnc1s01h /usr/lib/inet/in.iked: [ID
313954 daemon.notice] IKE_DELETE_PAYLOAD_RECEIVED:
20040325204004:   Source addr:47.142.217.23  Destination
addr:47.142.217.22  SPI:0x0100005d350a7d6c0100006b743037d4
Description:Received delete notification
```

All other possible failure messages that could get generated to syslog is shown below for IKE.

```
IKE_AH_IP_FRAGMENT

IKE_AH_SA_LOOKUP_FAILURE
```

IKE_AH_SEQUENCE_NUMBER_FAILURE

IKE_AH_ICV_FAILURE

IKE_ESP_SEQUENCE_NUMBER_OVERFLOW

IKE_ESP_IP_FRAGMENT

IKE_ESP_SA_LOOKUP_FAILURE,

IKE_ESP_SEQUENCE_NUMBER_FAILURE

IKE_ESP_ICV_FAILURE

IKE_INVALID_COOKIE

IKE_INVALID_ISAKMP_VERSION

IKE_INVALID_EXCHANGE_TYPE

IKE_INVALID_FLAGS

IKE_INVALID_MESSAGE_ID

IKE_INVALID_NEXT_PAYLOAD

IKE_INVALID_RESERVED_FIELD

IKE_INVALID_DOI

IKE_INVALID_SITUATION

IKE_INVALID_PROPOSAL

IKE_INVALID_SPI

IKE_INVALID_TRANSFORM

IKE_INVALID_ATTRIBUTES

IKE_INVALID_KEY_INFORMATION

IKE_INVALID_ID_INFORMATION

IKE_INVALID_CERTIFICATE

IKE_INVALID_CERTIFICATE_TYPE

IKE_INVALID_CERTIFICATE_AUTHORITY

IKE_INVALID_HASH_INFORMATION

IKE_INVALID_HASH_VALUE

IKE_INVALID_SIGNATURE_INFORMATION

IKE_INVALID_SIGNATURE_VALUE

IKE_INVALID_PROTOCOL_ID

IKE_INVALID_MESSAGE_TYPE

```
IKE_CERTIFICATE_TYPE_UNSUPPORTED

IKE_CERTIFICATE_UNAVAILABLE

IKE_NOTIFICATION_PAYLOAD_RECEIVED

IKE_DELETE_PAYLOAD_RECEIVED

IKE_UNEQUAL_PAYLOAD_LENGTHS

IKE_BAD_PROPOSAL_SYNTAX

IKE_RETRY_LIMIT_REACHED
```

24.5 Alarms

PKManager Alarm Section:

24.5.1 Key/Certificate Generation Failure Major Alarm Log

Log Title:PKM300

24.5.1.1 Formats

NTSTD log format:

RTP2 ** PKM300 SEP23 17:25:00 0401 TBL PKM Certificate generation failure
Location: PKManager=wnc0s0jd
NotificationID: 2000091
State: Raise
Category: Processing Error
Cause: Failed to create X509 certificate
Time: SEP23 17:25:00 2005
Component Id: PKManager
Specific Problem: Failed to create valid certificate for CN, GWC-1 42.45.123.56
Description: Attempt to create and validate an X509 certificate failed.

Table 2 Log Field descriptions

Field	Value
Category	Trouble
Severity	MAJ
LogName	PKM
LogNumber	300
Day Time	mmmdd hh:mm:ss

Table 2 Log Field descriptions

Field	Value
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate generation failure
Location	PKManager=hostname
Notification Id	0-65535
Category	Processing error
Cause	Failed to create X509 certificate
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	PKManager
SpecificProblem	Failed to create valid certificate for CN, GWC-1 42.45.123.56
Description	Attempt to create and validate an X509 certificate failed

24.5.1.2 Explanation

This Log is generated when an attempt to create and validate an X509 certificate has failed.

24.5.1.3 Action

Verify that the PKManager has been installed and initially configured properly. Review installation procedures and initial configuration procedures.

24.5.2 Key/Certificate Generation Failure Alarm Cleared Log

Log Title:PKM300

24.5.2.1 Formats

NTSTD log format:

RTP2 PKM300 SEP23 17:35:00 0401 TBL PKM Certificate generation failure

Location: PKManager=wnc0s0jd
NotificationID: 2000091
State: Cleared
Time: SEP23 17:35:00 2005

Table 3 Log Field descriptions

Field	Value
Category	Trouble
Severity	INFO
LogName	PKM
LogNumber	300
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate generation failure
Location	PKManager=hostname
NotificationID	0-65535
State	Cleared
Day Time Year	MMMdd hh:mm:ss YYYY

24.5.2.2 Explanation

This Log is generated when a X509 certificate creation and validation succeeded after previously having failed.

24.5.2.3 Action

None.

24.5.3 Key/Certificate Delivery Failure Major Alarm Log

Log Title:PKM301

24.5.3.1 Formats

NTSTD log format:

RTP2 ** PKM301 SEP23 18:25:00 0401 TBL PKM Certificate delivery failure

Location: PKManager=wnc0s0jd
NotificationID: 2000092
State: Raise
Category: Processing Error
Cause: Failed to deliver an X509 certificate
Time: SEP23 18:25:00 2005
Component Id: PKManager

Specific Problem: Failed to deliver a certificate for CN, GWC-2 42.45.123.16

Description: Attempt deliver a certificate to an application for a device failed.

Table 4 Log Field descriptions

Field	Value
Category	Trouble
Severity	MAJ
LogName	PKM
LogNumber	301
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate delivery failure
Location	PKManager=hostname
Notification Id	0-65535
Category	Processing error
Cause	Failed to deliver a certificate
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	PKManager
SpecificProblem	Failed to deliver a certificate for CN, GWC-2 42.45.123.16
Description	Attempt deliver a certificate to an application for a device failed

24.5.3.2 Explanation

This Log is generated when an attempt to deliver an X509 certificate to an application has failed.

24.5.3.3 Action

Verify that network communication among the system servers is operational. Retry provisioning the device.

24.5.4 Key/Certificate Delivery Failure Major Alarm Cleared Log

Log Title:PKM301

24.5.4.1 Formats

NTSTD log format:

RTP2 PKM301 SEP23 18:35:00 0401 TBL PKM Certificate delivery failure
Location: PKManager=wnc0s0jd
NotificationID: 2000092
State: Cleared
Time: SEP23 18:35:00 2005

Table 5 Log Field descriptions

Field	Value
Category	Trouble
Severity	INFO
LogName	PKM
LogNumber	301
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate delivery failure
Location	PKManager=hostname
NotificationID	0-65535
State	Cleared
Day Time Year	MMMdd hh:mm:ss YYYY

24.5.4.2 Explanation

This Log is generated when delivery of an X509 certificate has succeeded after previously having failed.

24.5.4.3 Action

None.

24.5.5 Certificate Expired Critical Alarm Log

Log Title:PKM302

24.5.5.1 Formats

NTSTD log format:

RTP2 *** PKM302 SEP24 18:25:00 0401 TBL PKM Certificate expired
Location: PKManager=wnc0s0jd
NotificationID: 2000192
State: Raise
Category: Processing Error
Cause: An X509 certificate has expired
Time: SEP24 18:25:00 2005
Component Id: PKManager
Specific Problem: Expired certificate for CN, GWC-2 42.45.123.16
Description: A certificate used during call control operations has expired

Table 6 Log Field descriptions

Field	Value
Category	Trouble
Severity	CRT
LogName	PKM
LogNumber	302
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate expired
Location	PKManager=hostname
Notification Id	0-65535
Category	Processing error
Cause	An X509 certificate has expired
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	PKManager
SpecificProblem	Expired certificate for CN, GWC-2 42.45.123.16
Description	A certificate used during call control operations has expired

24.5.5.2 Explanation

This Log is generated when an X509 certificate used by a device to authenticate itself during call control operations has expired. The device cannot send or receive call control messages.

24.5.5.3 Action

Verify the status for the device's certificate. if the certificate is PKManager generated certificate and the status is delivery failure. Determine why it has failed to be delivered. If the certificate is an imported certificate and the status is expired. Generate a new certificate for the device, import the certificate, verify the PKManager successfully delivers the certificate.

24.5.6 Certificate Expired Critical Alarm Cleared Log

Log Title:PKM302

24.5.6.1 Formats

NTSTD log format:

RTP2 PKM302 SEP24 19:35:00 0401 TBL PKM Certificate expired
Location: PKManager=wnc0s0jd
NotificationID: 2000192
State: Clear
Time: SEP24 19:35:00 2005

Table 7 Log Field descriptions

Field	Value
Category	Trouble
Severity	INFO
LogName	PKM
LogNumber	302
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate expired
Location	PKManager=hostname
NotificationID	0-65535
State	Clear
Day Time Year	MMMdd hh:mm:ss YYYY

24.5.6.2 Explanation

This Log is generated when a X509 certificate for a call control device that was expired has been replaced with a new valid certificate.

24.5.6.3 Action

None.

24.5.7 Certificate Expired Major Alarm Log

Log Title:PKM305

24.5.7.1 Formats

NTSTD log format:

RTP2 ** PKM305 SEP28 18:25:00 0401 TBL PKM Certificate expired
Location: PKManager=wnc0s0jd
NotificationID: 2001192
State: Raise
Category: Processing Error
Cause: An X509 certificate has expired
Time: SEP24 18:25:00 2005
Component Id: PKManager
Specific Problem: Expired certificate for CN, GWC-26 42.45.123.32
Description: A certificate used for OAM&P functions has expired

Table 8 Log Field descriptions

Field	Value
Category	Trouble
Severity	MAJ
LogName	PKM
LogNumber	305
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate expired
Location	PKManager=hostname
Notification Id	0-65535

Table 8 Log Field descriptions

Field	Value
Category	Processing error
Cause	An X509 certificate has expired
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	PKManager
SpecificProblem	Expired certificate for CN, GWC-26 42.45.123.32
Description	A certificate used for OAM&P functions has expired

24.5.7.2 Explanation

This Log is generated when an X509 certificate used by a device to authenticate itself for OAM&P functions has expired. The device cannot send or receive OAM&P commands.

24.5.7.3 Action

Verify the status for the device's certificate. if the certificate is PKManager generated certificate and the status is delivery failure. Determine why it has failed to be delivered. If the certificate is an imported certificate and the status is expired. Generate a new certificate for the device, import the certificate, verify the PKManager successfully delivers the certificate.

24.5.8 Certificate Expired Major Alarm Cleared Log

Log Title:PKM305

24.5.8.1 Formats

NTSTD log format:

RTP2 PKM305 SEP28 19:35:00 0401 TBL PKM Certificate expired
Location: PKManager=wnc0s0jd
NotificationID: 2001192
State: Cleared
Time: SEP28 19:35:00 2005

Table 9 Log Field descriptions

Field	Value
Category	Trouble
Severity	INFO

Table 9 Log Field descriptions

Field	Value
LogName	PKM
LogNumber	305
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate expired
Location	PKManager=hostname
NotificationID	0-65535
State	Cleared
Day Time Year	MMMdd hh:mm:ss YYYY

24.5.8.2 Explanation

This Log is generated when a X509 certificate for an OAM&P device that was expired has been replaced with a new valid certificate.

24.5.8.3 Action

None.

24.5.9 Certificate Forewarning of Expiration Major Alarm Log

Log Title:PKM303

24.5.9.1 Formats

NTSTD log format:

RTP2 ** PKM303 SEP25 18:25:00 0401 TBL PKM Last Alarm Before a Certificate Expiration
Location: PKManager=wnc0s0jd
NotificationID: 2000392
State: Raise
Category: Advanced Warning
Cause: Last alarm before X509 certificate expires
Time: SEP25 18:25:00 2005
Component Id: PKManager
Specific Problem: A certificate will expire soon CN, GWC-2 42.45.123.16
Description: Last forewarning of an impending certificate expiration

Table 10 Log Field descriptions

Field	Value
Category	Trouble
Severity	MAJ
LogName	PKM
LogNumber	303
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Last Alarm Before a Certificate Expiration
Location	PKManager=hostname
Notification Id	0-65535
Category	Advanced Warning
Cause	Last alarm before X509 certificate expires
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	PKManager
SpecificProblem	A certificate will expire soon CN, GWC-2 42.45.123.16
Description	Last forewarning of an impending certificate expiration

24.5.9.2 Explanation

This Log is generated when the expiration date of an X509 certificate has reached the forewarning date for the last alarm before expiration. A previous forewarning date has already passed. The alarm raised at that time has being escalated.

24.5.9.3 Action

1) Check that the in advance of expiration thresholds are configured properly. If not correct these.(ie. they are invalid or set too soon)

2) Verify the status and expiration date for the device's certificate. If the certificate is a PKManager generated certificate and the status is delivery

failure. Determine why it has failed to be delivered. If the certificate is an imported certificate. Generate a new certificate for the device, import the certificate, verify the PKManager successfully delivers the certificate.

24.5.10 Certificate Forewarning of Expiration Major Alarm Cleared Log

Log Title:PKM303

24.5.10.1 Formats

NTSTD log format:

RTP2 PKM303 SEP24 19:35:00 0401 TBL PKM Last Alarm Before a Certificate Expiration
Location: PKManager=wnc0s0jd
NotificationID: 2000392
State: Cleared
Time: SEP24 19:35:00 2005

Table 11 Log Field descriptions

Field	Value
Category	Trouble
Severity	INFO
LogName	PKM
LogNumber	303
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Last Alarm Before a Certificate Expiration
Location	PKManager=hostname
NotificationID	0-65535
State	Cleared
Day Time Year	MMMdd hh:mm:ss YYYY

24.5.10.2 Explanation

This Log is generated when an X509 certificate has been replaced and delivered successfully to the device after the replaced certificate had reached the last alarm before expiration date.

24.5.10.3 Action

None.

24.5.11 Certificate Forewarning of Expiration Minor Alarm Log

Log Title:PKM304

24.5.11.1 Formats

NTSTD log format:

RTP2 * PKM304 SEP26 18:25:00 0401 TBL PKM First Alarm Forewarning of a Certificate Expiration

Location: PKManager=wnc0s0jd
NotificationID: 2000492
State: Raise
Category: Advanced Warning
Cause: First alarm warning of impending X509 certificate expiration
Time: SEP26 18:25:00 2005
Component Id: PKManager
Specific Problem: A certificate will expire soon CN, GWC-2 42.45.123.16
Description: Initial forewarning of an impending certificate expiration

Table 12 Log Field descriptions

Field	Value
Category	Trouble
Severity	MINOR
LogName	PKM
LogNumber	304
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate expired
Location	PKManager=hostname
Notification Id	0-65535
Category	Advanced Warning
Cause	First Alarm Forewarning of a Certificate Expiration

Table 12 Log Field descriptions

Field	Value
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	PKManager
SpecificProblem	A certificate will expire soon CN, GWC-2 42.45.123.16
Description	Initial forewarning of an impending certificate expiration

24.5.11.2 Explanation

This Log is generated when the expiration date of an X509 certificate has reached the date for initial alarm forewarning its expiration.

24.5.11.3 Action

1) Check that the in advance of expiration thresholds are configured properly. If not correct these.(ie. they are invalid or set too soon)

2) Verify the status and expiration date for the device's certificate. If the certificate is a PKManager generated certificate and the status is replaced then check the status again in an hour. Should the status change to delivery failure. Determine why it has failed to be delivered. If the certificate is an imported certificate. Generate a new certificate for the device, import the certificate, verify the PKManager successfully delivers the certificate.

24.5.12 Certificate Forewarning of Expiration Minor Alarm Cleared Log

Log Title:PKM304

24.5.12.1 Formats

NTSTD log format:

RTP2 PKM304 SEP24 19:35:00 0401 TBL PKM First Alarm Forewarning of a Certificate Expiration
Location: PKManager=wnc0s0jd
NotificationID: 2000492
State: Cleared
Time: SEP24 19:35:00 2005

Table 13 Log Field descriptions

Field	Value
Category	Trouble

Table 13 Log Field descriptions

Field	Value
Severity	INFO
LogName	PKM
LogNumber	304
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	First Alarm Forewarning of a Certificate Expiration
Location	PKManager=hostname
NotificationID	0-65535
State	Cleared
Day Time Year	MMMdd hh:mm:ss YYYY

24.5.12.2 Explanation

This Log is generated when an X509 certificate has been replaced and delivered successfully to the device after the replaced certificate had triggered the initial forewarning alarm before expiration log.

24.5.12.3 Action

None.

GWCEM Alarm Section:

24.5.13 New Alarm: GWCEM fail to retrieve the cert.

This new alarm will be raised when GWCEM fail to retrieve the certificates from PKBClient.

24.5.13.1 Cause and condition

This scenario will happen if the PKBM is not ready for certificate retrieve or communication errors.

24.5.13.2 Alarm format

The format of this alarm should be:

Network Element: CS2K Config Manager

Alarm Level: Critical

Category: Environment

Alarm Time: <Data and time when the alarm was raised>

Probable Cause: PKBM is not ready for certificate retrieve or communication errors.

Description: GWCEM fail to retrieve the certificates.

24.5.13.3 Response Action

Action is required to check the communication between GWCEM and PKBClient or between PKBClient and PKBroker.

Mg9kEM Alarm Section:

24.5.14 New IPSC 307 - 312 alarms

24.5.14.1 Formats

The following alarms are raised or cleared when the Mg9kEM receives the "nnIpsecCertifFault" trap from the gateway:

Alarm ID	Fault Type Description
IPSC 307	certificate has expired
IPSC 308	certificate is about to expire in 4 days
IPSC 309	certificate has invalid from date
IPSC 310	remote certificate verification failed
IPSC 311	certificate is missing Subject Alt. Name
IPSC 312	time of date not set at the gateway

The above alarms have the same basic format. The fault type received from the "nnIpsecCertifFault" determines the alarm id and fault description. Here is an example of a IPSC 310 alarm:

MSH10_I06BR IPSC 310 JUN2 13:35:15 6550 Major TBL MG9K nnIpsecCertifFault

Location: 1-RM9K-Frame007.Shelf1.Slot13
Notification Id: 57493
State: cleared
Category: Equipment Alarm

Cause: remote certificate verification failed
Time: May 30 15:18:48 2003
Component Id: Card.frame0.shelf1.slot13.ITP
Specific Problem: Ipsec Cert Fault
Description: remote certificate verification failed

Site	Flr	RPos	Bay_id
CARY	***02***	***BB17***	***MG9F 007***

Here are the descriptions of the fields:

Field	Value
LogName	IPSC
LogNumber	307 - 312
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
Severity	Major
Alarm Category	Trouble
Device ID	Mg9k
EventType	nnIpsecCertifFault
Location	equipment location
NotificationID	0-65535
State	Raise or Clear
Day Time Year	MMMdd hh:mm:ss YYYY
Category	Equipment alarm
Cause	reason for fault
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	Equipment description
SpecificProblem	problem description
Description	fault description
Frame location Info	physical location of the equipment

24.5.14.2 Action

Correct the reported error condition associated with the alarm. For example, ensure the certificates used are current and valid.

24.5.15 New IPSC 313 alarm

24.5.15.1 Formats

The IPSC 313 alarm is raised when the EM attempts but fails to deliver certificates to the gateway. This alarm is cleared when subsequent delivery attempt succeeds.

Here is an example of a IPSC 313 alarm:

MSH10_I06BR IPSC 313 JUN2 13:35:15 6551 Major TBL MG9KEM CERT DELIVERY ERROR

Location: 1-RM9K-Frame007.Shelf1.Slot13
Notification Id: 57494
State: raised
Category: System Alarm
Cause: error delivering certificates
Time: May 30 15:18:48 2003
Component Id: Card.frame0.shelf1.slot13.ITP
Specific Problem: delivery error
Description: error delivering certificates

Site	Flr	RPos	Bay_id
CARY	***02***	***BB17***	***MG9F 007***

Here are the descriptions of the fields:

Field	Value
LogName	IPSC
LogNumber	313
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
Severity	Major
Alarm Category	Trouble
Device ID	MG9KEM
EventType	CERT DELIVERY ERROR
Location	equipment location
NotificationID	0-65535
State	Raise or Clear

Field	Value
Day Time Year	MMMdd hh:mm:ss YYYY
Category	System alarm
Cause	reason for fault
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	Equipment description
SpecificProblem	problem description
Description	fault description
Frame location Info	physical location of the equipment

24.5.15.2 Action

Correct the reported error condition associated with the alarm then retry the download request.

SSM Alarm Section:

No new or changed alarms.

25: Fault Management (FM): A00012199

25.1 Feature Name

MG9K EM CPR Robustness

25.2 Fault management strategy

No additional fault management is provided by this feature.

25.3 Fault management tools and utilities

25.3.1 Faults, Alarms and Logs

Customer logs will be generated whenever EM user opts for “clear persist and discover” functionality. Existing Reinitalize Gateway log will be used.

25.4 Logs

NE606

25.4.1 Formats

Jun 3 02:18:19 wnc0s0pe MG9kEMFactory_9:_V2_~I=MG9K~H=wnc0s0pe~A=MG9kEMFactory_9~S=2663~~ NE606 NONE INFO MG9K Reinitialize Gateway Event Description: Reinitialize Gateway Event Sent Time: Fri Jun 03 02:18:19 EDT 2005

25.4.2 Explanation

Each time user clicks on “Clear persist and discover” button in NE Discovery View, NE606 log will be generated.

25.4.3 Field descriptions

Table 1:

Field	Description	Example
Date/Time	Date and time stamp of the log	Jun 3 02:18:19
Host Name	Host machine name	wnc0s0pe
Application Name	The application producing the log	MG9kEMFactory_9
User Name	MG9K EM User name	rtpu
Log Number	The log number	NE606
Log Text	The action being taken	Reinitialize Gateway Event

25.4.4 Action

This is information log only. No action required.

25.4.5 Associated Operational Measurements or Performance Measurements

None

25.4.6 Additional information

None

25.5 Alarms

None

25.6 Related documentation

None

26: Fault Management (FM): A00012326

26.1 Feature Name

SIP Lines: Authentication and Authorization

26.2 Fault management strategy

The fault management information is provided using LOGs. The LOGUTIL CI provide the access to the LOGs generated. The LOGs are generated based on LOG framework. This feature uses the existing framework to add new LOGs.

26.3 Fault management tools and utilities

26.3.1 Faults, Alarms and Logs

The LOGUTIL CI command is used as tools in the CS2K Core software. All existing tools and utilities are applicable in case of CS2K software.

26.4 Logs (For CS2K only)

The following reasons have bee added in the existing LOG IBN110 as part of this activity.

- AUTH_ACCT_ON_MULTIPLE_SESSIONS: Reason added to LOG IBN110. It is generated when Multiple sessions are present while invoking the Acct/Auth codes flash entry feature.
- BLV_IN_PROGRESS: Reason added to existing LOG IBN110. It is generated if the invoker of ACCT/AUTH or the connected party is being verified by the Operator.

26.5 Log Title/Log ID, Log Reason: IBN110, AUTH_ACCT_ON_MULTIPLE_SESSIONS

26.5.1 Formats

<Switch ID> IBN110 <DATE> <TIME> INFO AUTH_ABUSE
<LEN> <DN> <KEY>
TYPE=AUTH ACCT ON MULTIPLE SESSIONS
<CUSTOMER_GROUP>
<DIGITS_DIALLED>

Example:

```
RTPT08BM      IBN110 SEP29 11:25:56 0425 INFO AUTH_ABUSE
      SS   00 0 00 27    DN 6136215077     KEY  1
       TYPE = AUTH ACCT ON MULTIPLE SESSIONS
       CUSTOMER_GROUP =          IBNTST
```

DIGITS_DIALLED = BB

26.5.1.1 NTSTD
Not Applicable

26.5.1.2 SCC2
Not Applicable

26.5.1.3 Syslog
Not Applicable

26.5.1.4 SNMP
Not Applicable

26.5.2 Explanation
Description: This log provides information regarding behavior of Acct/Auth codes flash entry on Multiple sessions (More than 2 sessions). When multiple sessions are present, this log is generated to indicate that Acct/Auth codes flash entry is not allowed.

26.5.3 Field descriptions

Table 1: Field descriptions

Field	Value	Description
TYPE	AUTH ACCT ON MULTIPLE SESSIONS	This reason in AUTH_ABUSE_KIND indicates why the LOG has been generated.

26.5.4 Associated Operational Measurements or Performance Measurements
None

26.5.5 Additional information
None

26.6 Log Title/Log ID, Log Reason: IBN110, BLV_IN_PROGRESS

26.6.1 Formats
<Switch ID> IBN110 <DATE> <TIME> INFO AUTH_ABUSE
<LEN> <DN> <KEY>
TYPE=BLV IN PROGRESS
<CUSTOMER_GROUP>
<DIGITS_DIALLED>

Example:

```
RTPT08BM      IBN110 SEP29 11:25:56 0425 INFO AUTH_ABUSE
      SS   00 0 00 27    DN 6136215077     KEY  1
       TYPE = BLV IN PROGRESS
       CUSTOMER_GROUP =          IBNTST
       DIGITS_DIALLED = BB
```

26.6.1.1 NTSTD

Not Applicable

26.6.1.2 SCC2

Not Applicable

26.6.1.3 Syslog

Not Applicable

26.6.1.4 SNMP

Not Applicable

26.6.2 Explanation

Description: This log provides information regarding interaction of Acct/Auth codes flash entry with BLV. This log is generated to indicate that Acct/Auth is not permitted if an Operator Busy Line verification (BLV) connection exists.

26.6.3 Field descriptions

Table 2: Field descriptions

Field	Value	Description
TYPE	BLV IN PROGRESS	This reason in AUTH_ABUSE_KIND indicates why the LOG has been generated.

26.6.4 Action

26.6.5 Associated Operational Measurements or Performance Measurements

None

26.6.6 Additional information

26.7 Alarms

Not Applicable

26.8 Related documentation

None

27: Fault Management (FM): A00012403

27.1 Feature Name

Data Protection for SIP Lines

27.2 Fault management strategy

This feature will inherit all the functionality currently available with legacy implementation.

27.3 Fault management tools and utilities

27.4 Logs

27.4.1 Explanation

Log Title: Aud501

Name: Data Dump for a Local Test Desk (LTD) extension block

Description: The Audit subsystem generates this report when there is a data dump for a local test desk (LTD) extension block. Extension blocks are used to provide additional data space for a call condense block (CCB), which stores only enough data to describe a basic call.

Event type: The log is encountered when performing a test against a line with NDC option.

Please refer to the North American DMS-100 Log Report Reference Manual Volume 2 for a description of this log.

27.4.2 Format

27.4.3 Field descriptions

27.4.4 Action

27.4.5 Associated Operational Measurements or Performance Measurements

27.4.6 Explanation

Log Title: TRMT 22

Name: NDC_IN_EFFECT

Description: Busy Verify fails because there is no double connection call.

Event type: The log is encountered when performing a test against a line with NDC option.

Please refer to the North American DMS-100 Log Report Reference Manual Volume 2 for a description of this log.

27.4.7 Format

27.4.8 Field descriptions

27.4.9 Action

28: Fault Management (FM): A00012526

28.1 Feature Name

TDM Call Recording Feature

28.2 Log SCAI600

Log Title/Log ID: SCAI600

28.2.1 Formats

X.25 Format:

```
RTP210AM    SCAI600 NOV11 17:11:00 2800 INFO MISSING TRNKINFO
    TABLES      : GATWYINV/GWEPCARR
    TRUNK       : TEST 0
    NODENO      : 12
    TRMNO       : 340
    MESSAGE     : DV-CALL-OFFERED-U
    LINK ID     : DNA:  000000000000000 PROTOCOL:  1  1  1  1
    DEVICE      : MPC:  0 LINK:  3
    SCAIGRP     : TCP_JG
    LINKSET     : SCAI_X25
```

TCP Format:

```
RTP210AM    SCAI600 NOV11 10:03:30 4500 INFO MISSING TRNKINFO
    TABLES      : GATWYINV/GWEPCARR
    TRUNK       :TEST 0
    NODENO      : 12
    TRMNO       : 340
    MESSAGE     : DV-CALL-OFFERED-U
    LINK ID     : IP_ADDR: 103  2  1  7
    DEVICE      : Not Applicable
    SCAIGRP     : TCP_JG
    LINKSET     : SCAI_TCP
```

28.2.2 Explanation

When TDM Call Recording TRNKINFO criteria is met, if the trunk information is not accessible by SCAI, the new parameter, TRNKINFO, will not be sent and SCAI600 will be generated.

28.2.3 Field descriptions

Table 3: Field descriptions

Field	Value	Description
INFO	MISSING TRNKINFO	TRNKINFO missing from tables listed in log and could not be sent in ICM message also noted in log.
TABLES	GATWYINV/GWEPCARR	Tables where datafill is missing.
TRUNK	CLLI	Incoming trunk
NODENO	Int	Node number of incoming trunk

Table 3: Field descriptions

Field	Value	Description
TRMNO	Int	Term number of incoming trunk
MESSAGE	{DV-CALL-OFFERED-U, DV-CALL-QUEUED-U}	The ICM message for which the log SCAI600 is generated.
LINK ID		Identifies link in table SCAICOMS to which the ICM corresponds. For X.25: Identifies the calling data network address (DNA). Subfields Protocol, MPC, and Link are included. For TCP: Identifies the internet protocol (IP) address.
DEVICE		*For X.25:* MPC # and the Link # *For TCP:* Not Applicable
SCAI GROUP		Identifies the scai group as datafilled in SCAIGRP Table with which the ECM session is established.
LINKSET NAME		Name of linkset.

28.2.4 Action

Check the datafill in tables GATWYINV and GWEPCARR.

29: Fault Management (FM): A00012622

29.1 Feature Name

Platform HW Alarm Reporting

29.2 Hardware alarms

Hardware alarms are reported under new alarm family HWER. Both the server and chassis monitors are capable of raising these alarms. Initially these four new reports are created.

HWER 701 - Cooling Device Malfunction

- For the BC-T platform: HWER 701 is derived from the monitors.blowers table. The alarm is raised when one or more blowers have any state value other than “good”. The alarm severity is Critical if both blowers are faulty, otherwise the severity is Major.
- For the Langley platform: HWER 701 is derived from the tCoolingDevice and tOperationalState tables. The alarm is raised when one or more cooling devices have an operational state not equal to vEnabled. The alarm severity is Critical if any of the faulty cooling devices are unspared, otherwise the severity is Major.

HWER 702 - Power Supply Malfunction

- For the BC-T platform: HWER 702 is derived from the powerModuleHealthTable table. The alarm is raised when one or more power modules have a state not equal to “good”. The alarm severity is Critical if any of the faulty power modules are unspared, otherwise the severity is Major.
- For the Langley platform: HWER 702 is derived from the tPowerSupply and tOperationalState tables. The alarm is raised when one or more power supplies have an operational state not equal to vEnabled. The alarm severity is Critical if any of the faulty power supplies are unspared, otherwise the severity is Major.

HWER 703 - Temperature Threshold Exceeded

- For the BC-T platform: HWER 703 is derived from the bladeTemperaturesTable and bladeTemperatureThresholdsTable tables. The alarm is raised when one or more bladeSensorNTemp probes report a value greater than the corresponding warning threshold. The sensor value table in the report text consists an inequality (“actual > expected” and the sensor name for each sensor out of spec. The alarm severity is Major.
- For the Langley platform: HWER 703 is derived from the tTemperatureProbe table. The alarm is raised when one or more

temperature probes report that a55TemperatureStatus is any value other than vOk. The sensor value table in the report text consists of the a55TemperatureStatus and the a55TemperatureProbeDescription variables for each sensor out of spec. The alarm severity is Major

HWER 704 - Processor Malfunction

- For the BC-T platform: HWER 704 is not reported for BC-T.
- For the Langley platform: HWER 704 is derived from the tProcessor and tOperationalState tables. The alarm is raised when one or more processors have an operational state not equal to vEnabled. The alarm severity is Major.

29.3 Alarm templates

The template for HWER 701 appears in Table 1. The device state table consists of two columns containing the device name and the device state as reported through the relevant MIB. The severity is Major if the malfunction results in loss of redundancy, Critical if it results in total loss of cooling.

Table 1: HWER 701 Report Format

Property Name	Property Value
Report Number	HWER 701
Description Text	Cooling Device Malfunction <device-state-table>
Clear Condition	All cooling devices are functioning normally.
Corrective Action	Replace defective cooling devices.

The template for HWER 702 appears in Table 2. The device state table consists of two columns containing the device name and device state as reported through the relevant MIB. The severity is Major if the malfunction results in loss of redundancy, Critical if it results in loss of power.

Table 2: HWER 702 Report Format

Property Name	Property Value
Report Number	HWER 702
Description Text	Power Supply Malfunction <device-state-table>
Clear Condition	All power supplies are functioning normally.

Table 2: HWER 702 Report Format

Property Name	Property Value
Corrective Action	Replace defective power supplies.

The template for HWER 703 appears in Table 3. The sensor value table consists of two columns containing the problem text and description of each sensor for which the reported value exceeds the threshold. Sensors reporting normal values are not shown.

Table 3: HWER 703 Report Format

Property Name	Property Value
Report Number	HWER 703
Description Text	Temperature Threshold Exceeded <sensor-value-table>
Clear Condition	All temperature sensors report normal values.
Corrective Action	Restore effective cooling for this equipment.

The template for HWER 704 appears in Table 4. The device state table consists of two columns containing the device name and device state as reported through the relevant MIB. The severity is Critical.

Table 4: HWER 704 Report Format

Property Name	Property Value
Report Number	HWER 704
Description Text	Processor Malfunction <device-state-table>
Clear Condition	All processors are functioning normally.
Corrective Action	Replace defective processors.

30: Fault Management (FM): A00012735

30.1 Feature Name

Session Server Fault Handling Enhancements

30.2 Fault management strategy

This section provides information on logs and alarms for the features under the Session Server Fault Handling elements. This activity builds upon the fault management services and software of NCGL Platform Manager in A00004005 introducing support for managing some new fault conditions.

30.3 Fault management tools and utilities

No new tools and utilities are introduced by this activity. The current approach to fault management applies.

30.4 Session Server Fault Handling Logs and Alarms.

This section describes the logs and alarms introduced by this activity.

The logs and alarms can be viewed via the web browser interface on the Succession Communication Server 2000 NCGL Platform Manager - via Alarms panel and Customer Logs panel.

This activity introduces the following logs:

30.4.1 Fault Handling Alarms/Logs

- XTS382, XTS682: Chassis Sensor Fault
- XTS383, XTS683: Power Supply Sensor Fault

30.4.2 Field Description

The new logs follow the existing XTS log format and are composed of the fields shown in the table given below.

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log.

Process Name	Alphanumeric	Identifies the NCGL or application process that generated the report.
Log Number	Alphanumeric	The component prefix and number of the log
Severity	Alphanumeric	The log severity (may be related to alarm severity)
Event Type	Alphanumeric	The type of trouble recorded
Label	Alphanumeric	Title label for the log.
Component Id	Alphanumeric	The component id is the unit hostname.
Description	Alphanumeric	Description of the log including location information when applicable and sensor details.

Here is an example platform /var/log/custlog entry:

Dec 9 06:22:41 NGSS0 alarmd: XTS382 MAJOR FLT Chassis Fault Detected NGSS0 Chassis sensor alarm raised. 2 sensors are reporting failures.

Here is an example alarm entry from the platform web pages:

Type: Equipment

ID: Threshold Crossed

Date: Friday December 8, 2005 02:39:06 PM

Host: NGSS1

Description: Chassis sensor alarm raised. 1 sensor is reporting a failure.

Here is a sample from an IEMS resident log file.

Dec 9 15:00:35 rtpo-cmt IEMS: _V2_~I=~H=rtpo-cmt~A=IEMS~S=1017~~ XTS383 MAJOR FLT XTS Fault Location: RTPOSST0-Unit-1;172.18.164.14 Notification Id: 17^M State: Raised^M Category: equipment Cause: thresholdCrossed(51) Time: Dec 09 15:00:19 2005 Component Id: RTPOSST0_1 Specific Problem: Description: Power supply alarm raised in module A. 1 sensor is reporting a failure.

Dec 9 15:07:00 rtpo-cmt IEMS: _V2_~I=~H=rtpo-cmt~A=IEMS~S=2218~~ IEMS607 NONE INFO IEMS Autogenerated Clear^M Location: RTPOSST0-Unit-1;172.18.164.14^M NotificationID: 17^M State: Clear^M Time: Dec 09 15:07:00 2005^M Specific Problem: ^M Category: equipment^M Component Id: RTPOSST0_1^M Description: Raised log: XTS383; Power supply alarm raised in module A. ^M 1 sensor is reporting a failure.

30.4.3 Fault Handling Alarms/Logs

The fault handling elements produces the following alarm and logs.

30.4.3.1 XTS382

30.4.3.1.1 Explanation When there is a sensor reports a failure condition, an XTS382 alarm is raised on the Alarms panel of the NCGL Session Server unit. An XTS382 log is generated.

30.4.3.1.2 Format Alarm/Log: Power Supply Failure Alarms/Logs

Type: Equipment

ID: equipmentMalfunction

Event: FLT

Label: Chassis Sensor Fault

Severity:

- Minor: a single, minor sensor fault has been detected by the hardware sensors for the unit's power supplies
- Major: either multiple, minor or at least one major sensor fault has been detected
- Critical: not currently generated

30.4.3.1.3 Field descriptions See section 30.4.2 Field Description.

30.4.3.1.4 Action On the NCGL Platform Manager web pages view the Sensor Information, System Information panels. Examine existing alarms and associated logs.

Inspect the environmental conditions of the unit.

If the Sensor Status field of the Sensor Information page indicates that presence is not detected, confirm that all drives and FRUs are correctly seated and latched into the chassis.

Consider chassis replacement or contact technical support if the condition continues.

30.4.3.1.5 Associated Operational Measurements or Performance Measurements

None.

30.4.3.1.6 Additional information None.

30.4.3.2 XTS682

30.4.3.2.1 Explanation When XTS382 Chassis Sensor fault condition and alarm is cleared. An alarm trap and INFO log XTS682 are generated.

30.4.3.2.2 Format Alarm/Log: Power Supply Alarm Cleared

Type: Equipment

ID: equipmentMalfunction

Event: INFO

Label: Power Supply Alarm Cleared

Severity: None

30.4.3.2.3 Field descriptions See Section 30.4.2 Field Description.

30.4.3.2.4 Action None.

30.4.3.2.5 Associated Operational Measurements or Performance Measurements None.

30.4.3.2.6 Additional information None.

30.4.3.3 XTS383

30.4.3.3.1 Explanation When there is one or more sensors report failure conditions with either power supply module A or B, an XTS383 alarm is raised on the Alarms panel of the NCGL Session Server unit.

30.4.3.3.2 Format >> Alarm/Log: Fans Failure Alarms/ Logs

----> Type: Equipment

---->ID: equipmentMalfunction

---->Event: FLT

---->Label: Fans Problem

---->Severity: Minor, Major

30.4.3.3.3 Field descriptions

See Section 30.4.2 Field Description.

30.4.3.3.4 Action

On the NCGL Platform Manager web pages view the Sensor Information, System Information panels. Examine existing alarms and associated logs.

Inspect the environmental conditions of the affected power supplies in the unit.

If the Sensor Status field of the Sensor Information page indicates that presence is not detected, confirm that the power supply module is correctly seated and latched into the chassis.

Consider chassis replacement or contact technical support if the condition continues.

If the alarm is critical, contact Nortel Networks support personnel for assistance.

30.4.3.3.5 Associated Operational Measurements or Performance Measurements

None

30.4.3.3.6 Additional information

None

30.4.3.4 XTS683

30.4.3.4.1 Explanation

When XTS383 Minor/Major Power Supply Sensor Fault alarm condition is cleared. a INFO alarm/log XTS683 is generated.

30.4.3.4.2 Format

>>Alarm/Log: Fans Problem Alarm Cleared

---->Type: Equipment

---->ID: EquipmentMalfunction

---->Event: INFO

---->Label: Power Supply Condition Cleared

---->Severity:None

30.4.3.4.3 Field descriptions

See Section 30.4.2 Field Description

30.4.3.4.4 Action

None

30.4.3.4.5 Associated Operational Measurements or Performance Measurements

None

30.4.3.4.6 Additional information

None

31: Fault Management (FM): A00012905

31.1 Feature Name

ERS8600 Alarm Mapping Correction in IEMS

31.2 Fault management strategy

The ERS8600 faults descriptions in IEMS was outstanding until now. In SN09-FF feature A00012905, several ERS8600 faults severities were changed. This feature is intended to enhance the existing mapping of the ERS8600 events and provide the associated customer documentation in the "Carrier Voice over IP Fault Management Logs Reference manual (NN10275-909)" and the "Carrier VOIP OSS Guide Advanced Feature Guide" for ERS8600 faults.

In this document, all the ERS8600 faults will be described in the following.

31.3 Fault management tools and utilities

In a Carrier VOIP CS2000 central office the ERS8600s should be configured to forward their SNMP traps to the IEMS. The IEMS mediates these SNMP traps converting them into normalized customer log events. This normalization process provides the following:

- Converts the ERS8600 SNMP TRAPs into an alarm raise, alarm clear or an info customer log event.

- These normalized events are forwarded to the IEMS northbound interfaces (SCC2, NTstd, custlog, SNMP). Please refer to the "OSS Guide Advance Feature Guide" (PLN-i09-OSS) for a description of these northbound interfaces.

- Correlates these incoming SNMP TRAPs to a ERS8600 configured in the IEMS inventory.

- Persists these normalized events in the IEMS server allowing the craftperson to view them in the IEMS event browser (which provides both a real-time and historical view of all ERS8600 normalized events) and alarm browser (which provides a real-time view of the incoming ERS8600 alarms).

31.4 ERS8600 alarm clearing policy

When working with the ERS8600 faults in the IEMS it is important to understand how these alarms are cleared. The ERS8600 does not support an interface that allows a northbound manager (i.e, the IEMS) the ability to resync with the ERS8600 alarm states. In addition, the ERS8600 does not support a direct mapping between all of its alarm raise events and clear events it sends.

As a result the ERS8600 alarms can be cleared one of six ways from the IEMS alarm view (i.e., the IEMS alarm browser). These include:

- The ERS8600 sends a clear for an associated alarm that it previously raised. The IEMS performs the correlation between raise and clear and removes the associated alarm form the IEMS alarm view. It is important to note that the ERS8600 does not send an explicit clear event for all the ERS8600 alarms that are raised.

- Performing a manual clear in the IEMS alarm browser. This allows a craftperson to remove an alarm in the IEMS view that is no longer active in the ERS8600 (Note: This only clears the alarm in the IEMS).

- Performing a manual delete in the IEMS alarm browser. This allows a craftperson to remove an alarm in the IEMS view that is no longer active in the ERS8600 (Note: This only clears the alarm in the IEMS).

- IEMS Age based clearing Policy: This mechanism utilizes an automated alarm ageing clearing policy in the IEMS server. The alarm clearing job (refer to the 'administration tools | jobs | alarm clearing policy' in the IEMS JWS client) clears all alarms from the IEMS view for the configured device types based upon the alarms age. By default this policy is configured to clear all alarms that are older then 7 days. In addition, by default, the ERS8600 device type is included in this policy. This policy ensures that ERS8600 alarms do not continue to accumulate in the IEMS alarm view (Note: This only removes the alarm in the IEMS).

- IEMS NB SNMP Agent clear request. (Note: This only removes the alarm in the IEMS).

- Executing the /opt/nortel/iems/current/bin/purgeTempData.sh script on the IEMS server. Please note that this clears all alarm, event and performance data history for all devices on the IEMS server.

31.5 Alarms brief overview

This table contains all the ERS8600 alarms in the IEMS side. They will be described in the following sections.

Alarm Index	Alarm Name	Trap OID (v2c)	MDM Fault Code (Hex)	IEMS Event (severity)	SN09 IEMS log	Correction in IEMS SN09-FF
1	risingAlarm	1.3.6.1.2.1.16.0.1	S C1220008	minor	PP 310	
2	fallingAlarm	1.3.6.1.2.1.16.0.2	S C1220008	clear	PP 311	
3	Default Trap	DEFAULT	S C1229999	indeterminate	PP 312	
4	coldStart	1.3.6.1.6.3.1.1.5.1.0	S C0000000	clear	PP 313	info

Alarm Index	Alarm Name	Trap OID (v2c)	MDM Fault Code (Hex)	IEMS Event (severity)	SN09 IEMS log	Correction in IEMS SN09-FF
5	warmStart	1.3.6.1.6.3.1.1.5.2.0	S C0000001	clear	PP 315	info
6	linkDown	1.3.6.1.6.3.1.1.5.3.0	S C0000002	major	PP 317	
7	linkUp	1.3.6.1.6.3.1.1.5.4.0	S C0000002	clear	PP 318	
8	authenticationFailure	1.3.6.1.6.3.1.1.5.5.0	S C0000004	warning	PP 319	
9	rcnChasPowerSupplyDown	1.3.6.1.4.1.2272.1.21.0.6	S C1220007	critical	PP 322	
10	rcnChasPowerSupplyUp	1.3.6.1.4.1.2272.1.21.0.14	S C1220007	clear	PP 323	
11	rcnChasFanDown	1.3.6.1.4.1.2272.1.21.0.7	S C1220006	critical	PP 324	
12	rcnChasFanUp	1.3.6.1.4.1.2272.1.21.0.21	S C1220006	clear	PP 325	
13	rcn2kCardDown	1.3.6.1.4.1.2272.1.21.0.11	S C1220001	major	PP 326	critical
14	rcn2kCardUp	1.3.6.1.4.1.2272.1.21.0.12	S C1220001	clear	PP 327	
15	rcn2kTemperature	1.3.6.1.4.1.2272.1.21.0.13	S C1220003	critical	PP 328	critical/ clear
16	rcnErrorNotification	1.3.6.1.4.1.2272.1.21.0.3	S C1220009	warning, major, critical	PP 329	
17	rcnLinkOscillation	1.3.6.1.4.1.2272.1.21.0.8	S C122000A	major	PP 330	
18	rcnMacViolation	1.3.6.1.4.1.2272.1.21.0.9	S C122000B	warning	PP 331	critical
19	rcnSonetTrap	1.3.6.1.4.1.2272.1.21.0.10	S C1220051	warning	PP 332	
20	rcnStpNewRoot	1.3.6.1.4.1.2272.1.21.0.4	S C122000C	warning	PP 333	
21	rcnStpTopologyChange	1.3.6.1.4.1.2272.1.21.0.5	S C122000D	warning	PP 334	
22	rcnStpTCN	1.3.6.1.4.1.2272.1.21.0.16	S C1220017	warning	PP 335	
23	rcn2kAtmPvcLinkStateChange	1.3.6.1.4.1.2272.1.21.0.15	S C1220012	info, minor, major/ clear	PP 336	
24	rcnSmltIstLinkUp	1.3.6.1.4.1.2272.1.21.0.17	S C1220014	clear	PP 337	
25	rcnSmltIstLinkDown	1.3.6.1.4.1.2272.1.21.0.18	S C1220014	major	PP 338	
26	rcnSmltLinkUp	1.3.6.1.4.1.2272.1.21.0.19	S C1220020	clear	PP 339	
27	rcnSmltLinkDown	1.3.6.1.4.1.2272.1.21.0.20	S C1220020	major	PP 340	
28	rcnPasswordChange	1.3.6.1.4.1.2272.1.21.0.22	S C1220022	warning	PP 341	
29	rcnPcmciaCardRemoved	1.3.6.1.4.1.2272.1.21.0.25	S C1220049	warning	PP 342	critical
30	rcnSmartCpldTimerFired	1.3.6.1.4.1.2272.1.21.0.26	S C1220024	major	PP 343	
31	rcnCardCpldNotUpDate	1.3.6.1.4.1.2272.1.21.0.27	S C1220025	warning	PP 344	major
32	rcnIgapLogFileFull	1.3.6.1.4.1.2272.1.21.0.28	S C1220026	major	PP 345	
33	rcnCpLimitShutDown	1.3.6.1.4.1.2272.1.21.0.29	S C1220027	major	PP 346	
34	rcnSshServerEnabled	1.3.6.1.4.1.2272.1.21.0.30	S C1220028	clear	PP 347	

Alarm Index	Alarm Name	Trap OID (v2c)	MDM Fault Code (Hex)	IEMS Event (severity)	SN09 IEMS log	Correction in IEMS SN09-FF
35	rcnSshServerDisabled	1.3.6.1.4.1.2272.1.21.0.31	S C1220028	major	PP 348	
36	rcnSshSessionLogin	1.3.6.1.4.1.2272.1.21.0.32	S C1220029	clear	PP 349	info
37	rcnSshSessionLogout	1.3.6.1.4.1.2272.1.21.0.33	S C1220029	major	PP 350	info
38	rcnSshUnauthorizedAccess	1.3.6.1.4.1.2272.1.21.0.34	S C1220030	major	PP 351	critical
39	rcnHaCpuState	1.3.6.1.4.1.2272.1.21.0.35	S C1220031	warning	PP 352	critical
40	rcnInsufficientMemory	1.3.6.1.4.1.2272.1.21.0.36	S C1220032	warning	PP 353	critical
41	rcnSaveConfigAction	1.3.6.1.4.1.2272.1.21.0.37	S C1220033	info	PP 354	
42	rcnLoopDetectOnPort	1.3.6.1.4.1.2272.1.21.0.38	S C1220034	warning	PP 355	critical
43	vrrpTrapStateTransition	1.3.6.1.2.1.46.1.3.0.3.0	S C1220048	warning	PP 356	critical
44	rcnEmError	1.3.6.1.4.1.2272.1.21.0.23	S C1220023	warning	PP 357	
45	ospfVirtIfStateChange	1.3.6.1.2.1.14.16.2.1	S C1220015	warning/ clear	PP 358	
46	ospfNbrStateChange	1.3.6.1.2.1.14.16.2.2	S C1220011	warning/ clear	PP 359	
47	ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2.3	S C1220016	minor/ clear	PP 360	
48	ospfIfConfigError	1.3.6.1.2.1.14.16.2.4	S C122000F	major	PP 361	critical
49	ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2.5	S C1220021	major	PP 362	critical
50	ospfIfAuthFailure	1.3.6.1.2.1.14.16.2.6	S C122000E	major	PP 363	critical
51	ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2.7	S C1220013	major	PP 364	critical
52	ospfIfStateChange	1.3.6.1.2.1.14.16.2.16	S C1220010	warning/ clear	PP 365	
53	rcnCardDown	1.3.6.1.4.1.2272.1.21.0.1		major	PP 366	critical
54	rcnCardUp	1.3.6.1.4.1.2272.1.21.0.2		clear	PP 367	
55	rcnbgpEstablished	1.3.6.1.4.1.2272.1.21.0.39	S C1220039	clear	PP 368	clear
56	rcnbgpBackwardTransition	1.3.6.1.4.1.2272.1.21.0.40	S C1220040	critical	PP 369	
57	rcnAggLinkUp	1.3.6.1.4.1.2272.1.21.0.41	S C1220041	clear	PP 370	
58	rcnAggLinkDown	1.3.6.1.4.1.2272.1.21.0.42	S C1220041	clear	PP 371	major
59	rcnIgmpNewGroupMember	1.3.6.1.4.1.2272.1.21.0.43	S C1220042	clear	PP 372	info
60	rcnIgmpLossGroupMember	1.3.6.1.4.1.2272.1.21.0.44	S C1220042	clear	PP 373	info
61	rcnIgmpNewQuerier	1.3.6.1.4.1.2272.1.21.0.45	S C1220043	clear	PP 374	info
62	rcnIgmpQuerierChange	1.3.6.1.4.1.2272.1.21.0.46	S C1220044	clear	PP 375	info
63	rcnDvmrpIfStateChange	1.3.6.1.4.1.2272.1.21.0.47	S C1220045	clear	PP 376	info

Alarm Index	Alarm Name	Trap OID (v2c)	MDM Fault Code (Hex)	IEMS Event (severity)	SN09 IEMS log	Correction in IEMS SN09-FF
64	rcnDvmrpNewNbrChange	1.3.6.1.4.1.2272.1.21.0.48	S C1220046	clear	PP 377	info
65	rcnDvmrpNbrLossChange	1.3.6.1.4.1.2272.1.21.0.49	S C1220046	clear	PP 378	info
66	rcnFdbProtectViolation	1.3.6.1.4.1.2272.1.21.0.59	S C1220047	clear	PP 379	info
67	rcnLogMsgControl	1.3.6.1.4.1.2272.1.21.0.60	S C1220050	clear	PP 380	info
68	rcnSaveConfigFile	1.3.6.1.4.1.2272.1.21.0.61	S C1220052	clear	PP 381	info
69	rcnDNSRequestResponse	1.3.6.1.4.1.2272.1.21.0.62	S C1220057	clear	PP 382	info
70	pingProbeFailed	1.3.6.1.2.1.80.0.1.0	S C1220053	clear	PP 383	info
71	pingTestFailed	1.3.6.1.2.1.80.0.2.0	S C1220054	clear	PP 384	info
72	pingTestCompleted	1.3.6.1.2.1.80.0.3.0	S C1220054	clear	PP 385	info
73	traceRoutePathChange	1.3.6.1.2.1.81.0.1.0	S C1220055	clear	PP 386	info
74	traceRouteTestFailed	1.3.6.1.2.1.81.0.2.0	S C1220056	clear	PP 387	info
75	traceRouteTestComplete	1.3.6.1.2.1.81.0.3.0	S C1220056	clear	PP 388	info
76	UDPEapSessionEndTrap	1.3.6.1.4.1.562.42.5.1.3.2.2		clear	PP 389	info
77	UDPEapSessionStartTrap	1.3.6.1.4.1.562.42.5.1.3.2.1		clear	PP 390	info
78	rcnDuplicateIpAddress	.1.3.6.1.4.1.2272.1.21.0.63		major	PP 391	critical
79	rcnLoopDetectPortDown	.1.3.6.1.4.1.2272.1.21.0.64		major	PP 392	critical

Note: IEMS severity definition:

severity = 6|5|4|3|2|1

Critical = 1

Major = 2

Minor = 3

Warning = 4

Clear = 5

Info = 6

An Example entry of ERS8600TrapList.xml

<TRAP
oid = ".1.3.6.1.4.1.2272.1.21.0.45"

```
        name = "rcnIgmpNewQuerier">
        <PROPERTIES>
            <eventprop name = "severity" value = "6"/>
            <eventprop name = "logName" value = "PP"/>
            <eventprop name = "logNumber" value = "374"/>
            <eventprop name = "eventType" value = "INFO"/>
            <eventprop name = "eventLabel" value = "PP Fault"/>
            <eventprop name = "category" value = "communications"/>
            <eventprop name = "entity" value = "$ip_Querier_$1"/>
            <eventprop name = "componentID" value = "ERS8600=$ip; igmpInterfaceIfIndex=$1"/>
            <eventprop name = "alarmClear" value = "3"/>
            <eventprop name = "probableCause" value = "New Querier in interface"/>
            <eventprop name = "description" value = "New Querier in interface: igmpInterfaceIfIndex = $1
(igmpInterfaceQuerier = $2 )"/>
            <eventprop name = "specificProblem" value = "New Querier in interface"/>
        </PROPERTIES>
        <VARBINDS>
            <varbind name = ".1.3.6.1.3.59.1.1.1.1.1" property = "$1"/>
            <varbind name = ".1.3.6.1.3.59.1.1.1.1.5" property = "$2"/>
        </VARBINDS>
    </TRAP>
```

This table is the ERS8600 raise-clear mappings.

ERS 8600 Trap Raise-Clear Mapping:

Index	Raise Alarm	Clear Alarm
1	RisingAlarm(PP310)	FallingAlarm(PP311)
2	LinkDown (PP317)	LinkUp(PP318)
3	RcnChasPowerSupplyDown / RcChasPowerSupplyDown (PP322)	RcnChasPowerSupplyUp / RcChasPowerSupplyUp (PP323)
4	RcnChasFanDown / RcChasFanDown (PP324)	RncChasFanUp / RnChasFanUp (PP325)
5	Rcn2kCardDown / Rc2kCardDown (PP326)	Rcn2kCardUp / Rc2kCardUp (PP327)
6	RcnSmltIstLinkDown(PP338)	RcnSmltIstLinkUp(PP337)
7	RcnSmltLinkDown / RcSmltLinkDown (PP340)	RcnSmltLinkUp / RcSmltLinkUp (PP339)
8	RcnSshServerDisabled(PP348)	RcnSshServerEnabled(PP347)
9	Rcn2kTemperature(PP328)	Rcn2kTemperature(PP328)
10	RcnCardDown / RcCardDown (PP366)	RcnCardUp / RcCardUp (PP367)
11	rcn2kAtmPvcLinkStateChange(PP336)	rcn2kAtmPvcLinkStateChange(PP336)
12	ospfVirtIfStateChange(PP358)	ospfVirtIfStateChange(PP358)
13	ospfNbrStateChange(PP359)	ospfNbrStateChange(PP359)
14	ospfVirtNbrStateChange(PP360)	ospfVirtNbrStateChange(PP360)
15	ospfIfStateChange(PP365)	ospfIfStateChange(PP365)
16	rcnAggLinkDown (PP371)	rcnAggLinkUp (PP370)
17	rcnbgpBackwardTransition (PP369)	rcnbgpEstablished (PP368)

About the alarm clearing rule, IEMS judges it from the severity level. If the severity level is 5, IEMS considers it is a clear alarm. For those alarms without explicit corresponding clear alarm, IEMS will clear them when it reaches the age time or the alarms are cleared manually.

31.6 Alarm (PP310)

risingAlarm, Trap OID is1.3.6.1.2.1.16.0.1

31.6.1 Explanation

The PP310 alarm signifies that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.

This alarm is set when an alarm threshold is crossed. The text of the alarm message identifies the alarm value that triggered the alarm, the item that was being monitored, and the threshold level.

A rising alarm indicates that the alarm is triggered when the alarm value rises above the threshold value.

A falling alarm indicates that the alarm is triggered when the alarm value falls below the threshold value.

The falling alarm clears the rising alarm.

31.6.2 Action

Please refer to ERS8600 Fault Management document.

31.6.3 Corresponding Clear Log

PP311.

31.6.3.1 Format

31.6.3.2 NTSTD

Not available.

31.6.4 Field descriptions

This alarm has no selected fields.

31.6.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.6.6 Additional information

This alarm requires no additional information.

31.7 Alarm (PP311)

fallingAlarm, Trap OID is1.3.6.1.2.1.16.0.2

31.7.1 Explanation

The PP311 alarm signifies that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.

31.7.2 Action

Please refer to ERS8600 Fault Management document.

31.7.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.7.3.1 Format

31.7.3.2 NTSTD

Not available.

31.7.4 Field descriptions

This alarm has no selected fields.

31.7.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.7.6 Additional information

This alarm requires no additional information.

31.8 Alarm (PP313)

coldStart, Trap OID is1.3.6.1.6.3.1.1.5.1.0

31.8.1 Explanation

The PP313 alarm signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.

31.8.2 Action

Please refer to ERS8600 Fault Management document.

31.8.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.8.3.1 Format

31.8.3.2 NTSTD

zsups3f8 PP313 OCT26 01:28:48 0009 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: operator
Cause: Agent reinitialized itself with default settings
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Agent reinitialized itself with default settings
Description: A coldStart trap signifies that the snmp agent is reinitializing itself with default settings.
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.1.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.8.4 Field descriptions

Table 5: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.8.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.8.6 Additional information

This alarm requires no additional information.

31.9 Alarm (PP315)

warmStart, Trap OID is1.3.6.1.6.3.1.1.5.2.0

31.9.1 Explanation

The PP315 alarm signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.

31.9.2 Action

Please refer to ERS8600 Fault Management document.

31.9.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.9.3.1 Format

31.9.3.2 NTSTD

zsups3f8 PP315 OCT26 01:28:48 0011 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: operator
Cause: Agent reinitialized itself with its configuration unaltered.
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Agent reinitialized itself with its configuration unaltered.
Description: A warmStart trap signifies that the SNMPv2 agent is reinitializing itself such that its configuration is unaltered.
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.2.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.9.4 Field descriptions

Table 6: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.9.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.9.6 Additional information

This alarm requires no additional information.

31.10 Alarm (PP317)

linkDown, Trap OID is1.3.6.1.6.3.1.1.5.3.0

31.10.1 Explanation

The PP317 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to transition into the down state.

31.10.2 Action

Please refer to ERS8600 Fault Management document.

31.10.3 Corresponding Clear Log

PP318.

31.10.3.1 Format

31.10.3.2 NTSTD

zsups3f8 ** PP317 OCT26 01:28:48 0013 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: communications
Cause: loss of communication
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ifIndex=100
Specific Problem: Generic Link Status
Description: Link Down: ifIndex = 100(AdminStatus = up OperationStatus = down Port = 37 Slot = 1)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.3.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.10.4 Field descriptions

Table 7: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, `ifIndex` and node ID of the device.
OperationStatus	character string	Can be one of {up (1), down (2), testing (3)}

Table 7: Field descriptions

Field	Value	Description
PhysicalInfo	character string	Indicates the phsyical information appended to OperationStatus. The actual physical information is determined by ifIndex. ifIndex >= 64 and ifIndex <= 703 the information is: Port = ‘(ifIndex & 0x3f) + 1‘ Slot = ‘ifIndex >>6‘ ifIndex >= 832 and ifIndex <= 863 the information is: Circuitless IP = ‘ifIndex - 832 + 1‘ ifIndex >= 2048 and ifIndex <= 4095 the information is: VLAN = ‘ifIndex - 2048 + 1‘ ifIndex >= 4096 and ifIndex <= 4127 the information is: MLT = ‘ifIndex - 4096 + 1‘ ifIndex >= 4352 and ifIndex <= 5351 the information is: Tunnel = ‘ifIndex - 4352 + 1‘ An ifIndex not within the above ranges, the information is: unknown of ifIndex meaning Note: The content in ‘‘ part will be calculated out.

31.10.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.10.6 Additional information

This alarm requires no additional information.

31.11 Alarm (PP318)

linkUp, Trap OID is1.3.6.1.6.3.1.1.5.4.0

31.11.1 Explanation

The PP318 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links has transitioned out of the down state.

31.11.2 Action

Please refer to ERS8600 Fault Management document.

31.11.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.11.3.1 Format

31.11.3.2 NTSTD

zsups3f8 PP318 OCT26 01:28:48 0016 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: communications
Cause: communication regained
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ifIndex=100
Specific Problem: Generic Link Status
Description: Link Up: ifIndex = 100(AdminStatus = up OperationStatus = up Port = 37 Slot = 1)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.4.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.11.4 Field descriptions

Table 8: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, `ifIndex` and node ID of the device.
OperationStatus	character string	Can be one of {up (1), down (2), testing (3)}

Table 8: Field descriptions

Field	Value	Description
PhysicalInfo	character string	Indicates the phsyical information appended to OperationStatus. The actual physical information is determined by ifIndex. ifIndex >= 64 and ifIndex <= 703 the information is: Port = ‘(ifIndex & 0x3f) + 1‘ Slot = ‘ifIndex >>6‘ ifIndex >= 832 and ifIndex <= 863 the information is: Circuitless IP = ‘ifIndex - 832 + 1‘ ifIndex >= 2048 and ifIndex <= 4095 the information is: VLAN = ‘ifIndex - 2048 + 1‘ ifIndex >= 4096 and ifIndex <= 4127 the information is: MLT = ‘ifIndex - 4096 + 1‘ ifIndex >= 4352 and ifIndex <= 5351 the information is: Tunnel = ‘ifIndex - 4352 + 1‘ An ifIndex not within the above ranges, the information is: unknown of ifIndex meaning Note: The content in ‘‘ part will be calculated out.

31.11.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.11.6 Additional information

This alarm requires no additional information.

31.12 Alarm (PP319)

authenticationFailure, Trap OID is1.3.6.1.6.3.1.1.5.5.0

31.12.1 Explanation

The PP319 alarm signifies an authenticationFailure on the device.

31.12.2 Action

Please refer to ERS8600 Fault Management document.

31.12.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.12.3.1 Format

31.12.3.2 NTSTD

zsups3f8 PP319 OCT26 01:28:48 0017 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: security
Cause: Authentication failure
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Authentication failure
Description: Authentication failure occurred
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.5.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.12.4 Field descriptions

Table 9: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.12.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.12.6 Additional information

This alarm requires no additional information.

31.13 Alarm (PP322)

rcnChasPowerSupplyDown, Trap OID is1.3.6.1.4.1.2272.1.21.0.6

31.13.1 Explanation

The PP322 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcChasPowerSupplyOperStatus object for one of its power supply unit is about to transition into the down state.

This alarm is set when the power supply unit goes down. The alarm is cleared when the power supply comes up again.

31.13.2 Action

Please refer to ERS8600 Fault Management document.

31.13.3 Corresponding Clear Log

PP323.

31.13.3.1 Format

31.13.3.2 NTSTD

zsups3f8 *** PP322 OCT26 01:28:49 0045 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Power Supply down
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; SupplyId=1
Specific Problem: Power Supply Status
Description: Power Supply Status: SupplyId = 1(OperationStatus = down)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.6
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.13.4 Field descriptions

Table 10: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.

Table 10: Field descriptions

Field	Value	Description
Component Id	character string	Indicates the IP address, supplyId and node ID of the device.
OperationStatus	character string	Can be one of {unknown (1), empty (2), up (3), down (4)}

31.13.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.13.6 Additional information

This alarm requires no additional information.

31.14 Alarm (PP323)

rcnChasPowerSupplyUp, Trap OID is1.3.6.1.4.1.2272.1.21.0.14

31.14.1 Explanation

The PP323 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcChasPowerSupplyOperStatus object for one of its power supply unit is about to transition into the up state.

31.14.2 Action

Please refer to ERS8600 Fault Management document.

31.14.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.14.3.1 Format

31.14.3.2 NTSTD

zsups3f8 PP323 OCT26 01:28:49 0057 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: equipment
Cause: Power supply up
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; SupplyId=1
Specific Problem: Power Supply Status
Description: Power Supply Status: SupplyId = 1(OperationStatus = up)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.14
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.14.4 Field descriptions

Table 11: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, supplyId and node ID of the device.
OperationStatus	character string	Can be one of {unknown (1), empty (2), up (3), down (4)}

31.14.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.14.6 Additional information

This alarm requires no additional information.

31.15 Alarm (PP324)

rcnChasFanDown, Trap OID is1.3.6.1.4.1.2272.1.21.0.7

31.15.1 Explanation

The PP324 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcChasFanOperStatus object for one of its power supply unit is about to transition into the down state.

This trap is set when the fan goes down. The alarm is cleared when the fan comes up again.

For 3 slot and 6 slot chassis, there is a single fan.

A 10 slot chassis has two fans; one that cools the top 5 slots and the other that cools the bottom 5 slots.

The chassis will overheat even if a single fan goes down. So both the fans are needed for the chassis to be operational.

31.15.2 Action

Please refer to ERS8600 Fault Management document.

31.15.3 Corresponding Clear Log

PP325.

31.15.3.1 Format

31.15.3.2 NTSTD

zsups3f8 *** PP324 OCT26 01:28:49 0047 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Fan status down
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; fanId=1
Specific Problem: Fan down
Description: Fan Down: fanId= 1(OperationStatus = down)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.7
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.15.4 Field descriptions

Table 12: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, fanId and node ID of the device.
OperationStatus	character string	Can be one of {unknown (1), up (2), down (3)}

31.15.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.15.6 Additional information

This alarm requires no additional information.

31.16 Alarm (PP325)

rcnChasFanUp, Trap OID is1.3.6.1.4.1.2272.1.21.0.21

31.16.1 Explanation

The PP325 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcChasFanOperStatus object for one of its power supply unit is about to transition into the up state.

31.16.2 Action

Please refer to ERS8600 Fault Management document.

31.16.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.16.3.1 Format

31.16.3.2 NTSTD

zsups3f8 PP325 OCT26 01:28:49 0077 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: equipment
Cause: Fan Status Up
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; fanId=1
Specific Problem: Fan Up
Description: Fan Up: fanId= 1(OperationStatus = up)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.21
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.16.4 Field descriptions

Table 13: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, fanId and node ID of the device.

Table 13: Field descriptions

Field	Value	Description
OperationStatus	character string	Can be one of {unknown (1), up (2), down (3)}

31.16.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.16.6 Additional information

This alarm requires no additional information.

31.17 Alarm (PP326)

rcn2kCardDown, Trap OID is1.3.6.1.4.1.2272.1.21.0.11

31.17.1 Explanation

The PP326 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcCardOperStatus object for one of its cards is about to transition into the down state.

31.17.2 Action

Please refer to ERS8600 Fault Management document.

31.17.3 Corresponding Clear Log

PP327.

31.17.3.1 Format

31.17.3.2 NTSTD

zsups3f8 *** PP326 OCT26 01:28:49 0051 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Rc 2k Card Down
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; cardIndex=1
Specific Problem: RC 2k Card Status
Description: Card Down: cardIndex = 1(AdminStatus = down
OperationStatus = down)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.11
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.17.4 Field descriptions

Table 14: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, cardIndex and node ID of the device.
AdminStatus	character string	Can be one of {up (1), down (2), testing (3)}
OperationStatus	character string	Can be one of {up (1), down (2), testing (3), unknown (4), dormant (5)}

31.17.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.17.6 Additional information

This alarm requires no additional information.

31.18 Alarm (PP327)

rcn2kCardUp, Trap OID is1.3.6.1.4.1.2272.1.21.0.12

31.18.1 Explanation

The PP327 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcCardOperStatus object for one of its cards is about to transition into the up state.

31.18.2 Action

Please refer to ERS8600 Fault Management document.

31.18.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.18.3.1 Format

31.18.3.2 NTSTD

```
zsups3f8      PP327 OCT26 01:28:49 0053 INFO PP Fault
    Location: ERS8600_RTP;47.142.106.1
    State: Cleared
    Category: equipment
    Cause: Card status Up
    Time: Oct 26 01:28:49 2005
    Component ID: ERS8600=47.142.106.1; cardIndex=1
    Specific Problem: RC 2k Card Status
    Description: Card Up: cardIndex = 1(AdminStatus = up OperationStatus
    = up)
    .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.12
    .1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

31.18.4 Field descriptions

Table 15: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, cardIndex and node ID of the device.
AdminStatus	character string	Can be one of {up (1), down (2), testing (3)}
OperationStatus	character string	Can be one of {up (1), down (2), testing (3), unknown (4), dormant (5)}

31.18.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.18.6 Additional information

This alarm requires no additional information.

31.19 Alarm (PP328)

rcn2kTemperature, Trap OID is1.3.6.1.4.1.2272.1.21.0.13

31.19.1 Explanation

The PP328 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected the chassis is over-heating.

The chassis is overheating. This trap is generated at a threshold temperature of 48 degrees centigrade.

31.19.2 Action

Please refer to ERS8600 Fault Management document.

31.19.3 Corresponding Clear Log

PP328.

31.19.3.1 Format

31.19.3.2 NTSTD

zsups3f8 *** PP328 OCT26 01:28:49 0055 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Over-heating of the chassis detected
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: RC 2K Chassis Temperature
Description: Chassis over-heating: rc2kChassisTemperature = 50
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.13
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.19.4 Field descriptions

Table 16: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.
Status	Raised/Cleared	Indicated the alarm severity. It is determined by the temperature.

Table 16: Field descriptions

Field	Value	Description
rc2kChassisTemperature	character string	Indicates the temperature of the chassis. When the temperature is >= 48 degree, a critical alarm will be raised. Once the temperature is <48 degree, raise a corresponding clear alarm.

31.19.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.19.6 Additional information

This alarm requires no additional information.

31.20 Alarm (PP329)

rcnErrorNotification, Trap OID is1.3.6.1.4.1.2272.1.21.0.13

31.20.1 Explanation

The PP329 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that an error condition has occurred.

31.20.2 Action

Please refer to ERS8600 Fault Management document.

31.20.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.20.3.1 Format

31.20.3.2 NTSTD

zsups3f8 PP329 OCT26 01:28:48 0023 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: Error condition occurred
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: RC 2K Error
Description: Error occurred: Error Level = 0(Error Code = 1 Error Text =)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.3
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.20.4 Field descriptions

Table 17: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.
Severity	warning/major/critical	Indicated the alarm severity. It is determined by the Error level.
Error Level	character string	Error level = 0 or 1, indicates warning alarm. Error level = 2 or 3, indicates major alarm. Error level = 4, indicates critical alarm.

31.20.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.20.6 Additional information

This alarm requires no additional information.

31.21 Alarm (PP330)

rcnLinkOscillation, Trap OID is1.3.6.1.4.1.2272.1.21.0.8

31.21.1 Explanation

The PP330 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected an excessive number of link state transitions on the specified port.

31.21.2 Action

Please refer to ERS8600 Fault Management document.

31.21.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.21.3.1 Format

31.21.3.2 NTSTD

zsups3f8 ** PP330 OCT26 01:28:49 0049 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Link Oscillation detected
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; portIndex=1
Specific Problem: RC Link Oscillation
Description: LinkOscillation: portIndex = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.8
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.21.4 Field descriptions

Table 18: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, portIndex and node ID of the device.

31.21.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.21.6 Additional information

This alarm requires no additional information.

31.22 Alarm (PP331)

rcnMacViolation, Trap OID is1.3.6.1.4.1.2272.1.21.0.9

31.22.1 Explanation

The PP331 alarm signifies that the SNMPv2 entity, acting in an agent role, has received a PDU with an invalid source MAC address.

31.22.2 Action

Please refer to ERS8600 Fault Management document.

31.22.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.22.3.1 Format

31.22.3.2 NTSTD

zsups3f8 *** PP331 OCT26 01:28:49 0061 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: RC Mac Violation
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; portIndex=1
Specific Problem: RC Mac violation
Description: RC Mac Violation: portIndex= 1(rcErrorText =)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.9
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.2.2.1.1.0: 0

31.22.4 Field descriptions

Table 19: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, portIndex and node ID of the device.

31.22.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.22.6 Additional information

This alarm requires no additional information.

31.23 Alarm (PP332)

rcnSonetTrap, Trap OID is1.3.6.1.4.1.2272.1.21.0.10

31.23.1 Explanation

The PP332 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected a change of status on a Sonet port.

31.23.2 Action

Please refer to ERS8600 Fault Management document.

31.23.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.23.3.1 Format

31.23.3.2 NTSTD

zsups3f8 PP332 OCT26 01:28:49 0059 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: Sonet port status change
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; portIndex=1
Specific Problem: Sonet port status change
Description: Sonet Trap: portIndex = 1(TrapType = sectionAlarm Trap Indication = sectionLossOfSignal)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.10
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.23.4 Field descriptions

Table 20: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, portIndex and node ID of the device.

Table 20: Field descriptions

Field	Value	Description
TrapType	character string	Can be one of {sectionAlarm (1), lineAlarm (2), pathAlarm (3)}
Trap Indication	character string	Can be one of {noDefect (1), sectionLossOfSignal (2), sectionLossOfFrame (3), lineAlarmIndication (4), lineRemoteDefectIndication (5), pathLossOfPointer (6), pathAlarmIndication (7), pathRemoteDefectIndication (8), pathUnequipped (9), pathSignalLabelMismatch (10), pathTraceMismatch (11)}

31.23.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.23.6 Additional information

This alarm requires no additional information.

31.24 Alarm (PP333)

rcnStpNewRoot, Trap OID is1.3.6.1.4.1.2272.1.21.0.4

31.24.1 Explanation

The PP333 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected the Spanning Tree Protocol has declared the device to be the new root of the spanning tree.

31.24.2 Action

Please refer to ERS8600 Fault Management document.

31.24.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.24.3.1 Format

31.24.3.2 NTSTD

zsups3f8 PP333 OCT26 01:28:48 0025 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other

Cause: Stp New Root
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; stgId=1
Specific Problem: Stp New Root
Description: Stp New Root: stgId = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.4
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.24.4 Field descriptions

Table 21: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, stgId and node ID of the device.

31.24.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.24.6 Additional information

This alarm requires no additional information.

31.25 Alarm (PP334)

rcnStpTopologyChange, Trap OID is1.3.6.1.4.1.2272.1.21.0.5

31.25.1 Explanation

The PP334 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected the Spanning Tree Protocol has gone due to a topology change event.

31.25.2 Action

Please refer to ERS8600 Fault Management document.

31.25.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.25.3.1 Format

31.25.3.2 NTSTD

zsups3f8 PP334 OCT26 01:28:48 0027 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: Stp Topology change
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; stgId=1
Specific Problem: Stp Topology change
Description: Stp Topology change: stgId= 1(portIndex = 1)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.5
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.25.4 Field descriptions

Table 22: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, stgId and node ID of the device.

31.25.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.25.6 Additional information

This alarm requires no additional information.

31.26 Alarm (PP335)

rcnStpTCN, Trap OID is1.3.6.1.4.1.2272.1.21.0.16

31.26.1 Explanation

The PP335 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected the Spanning Tree Protocol has gone due a topology change event.

31.26.2 Action

Please refer to ERS8600 Fault Management document.

31.26.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.26.3.1 Format

31.26.3.2 NTSTD

zsups3f8 PP335 OCT26 01:28:49 0067 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: Stp TCN
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; portIndex=1
Specific Problem: Stp TCN
Description: Stp TCN: portIndex= 1(stgId= 1 BridgeAddress= 00-08-74-F0-3C-EC)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.16
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.26.4 Field descriptions

Table 23: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, portIndex and node ID of the device.

31.26.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.26.6 Additional information

This alarm requires no additional information.

31.27 Alarm (PP336)

rcn2kAtmPvcLinkStateChange, Trap OID is1.3.6.1.4.1.2272.1.21.0.15

31.27.1 Explanation

The PP336 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the rc2kAtmPvcOamVcStatus object for one of PVC is about to transition into different state, either from up to down or from down to up.

31.27.2 Action

Please refer to ERS8600 Fault Management document.

31.27.3 Corresponding Clear Log

PP336.

31.27.3.1 Format

31.27.3.2 NTSTD

zsups3f8 PP336 OCT26 01:28:49 0065 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: environmental
Cause: PVC link status change
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; rc2kAtmPvcIfIndex=0
Specific Problem: PVC link status change
Description: Atm Pvc Link State Change: AtmPvcIfIndex = 0(AtmPvcVpi = 0 AtmPvcVci = 0 AtmPvcOamVcStatus = notManaged)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.15
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.27.4 Field descriptions

Table 24: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address,rc2kAtmPvcIfIndex and node ID of the device.

Table 24: Field descriptions

Field	Value	Description
Severity	info/minor/major/clear	Indicated the alarm severity. It is determined by the AtmPvcOamVcStatus.
AtmPvcOamVcStatus	character string	AtmPvcOamVcStatus = "notManaged", indicates info alarm. AtmPvcOamVcStatus = "downVerify" or "upVerify", indicates minor alarm. AtmPvcOamVcStatus = "down", indicates major alarm. AtmPvcOamVcStatus = "up", indicates clear alarm.

31.27.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.27.6 Additional information

This alarm requires no additional information.

31.28 Alarm (PP337)

rcnSmltIstLinkUp, Trap OID is1.3.6.1.4.1.2272.1.21.0.17

31.28.1 Explanation

The PP337 alarm signifies that the split MLT link is from down to up.

31.28.2 Action

Please refer to ERS8600 Fault Management document.

31.28.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.28.3.1 Format

31.28.3.2 NTSTD

zsups3f8 PP337 OCT26 01:28:49 0069 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: other

Cause: Split MLT link status up
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Split MLT link status up
Description: Split MLT link status up
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.17
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.28.4 Field descriptions

Table 25: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.28.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.28.6 Additional information

This alarm requires no additional information.

31.29 Alarm (PP338)

rcnSmltIstLinkDown, Trap OID is1.3.6.1.4.1.2272.1.21.0.18

31.29.1 Explanation

The PP338 alarm signifies that the split MLT link is from up to down.

31.29.2 Action

Please refer to ERS8600 Fault Management document.

31.29.3 Corresponding Clear Log

PP337.

31.29.3.1 Format

31.29.3.2 NTSTD

zsups3f8 ** PP338 OCT26 01:28:49 0071 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: Split MLT Link Status Down
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Split MLT Link Status Down
Description: Split MLT Link Status Down
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.18
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.29.4 Field descriptions

Table 26: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.29.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.29.6 Additional information

This alarm requires no additional information.

31.30 Alarm (PP339)

rcnSmltLinkUp, Trap OID is1.3.6.1.4.1.2272.1.21.0.19

31.30.1 Explanation

The PP339 alarm signifies that the split SMLT link is up.

31.30.2 Action

Please refer to ERS8600 Fault Management document.

31.30.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.30.3.1 Format

31.30.3.2 NTSTD

zsups3f8 PP339 OCT26 01:28:49 0073 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: other
Cause: Split SMLT link up
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; rcMltSmltId=1
Specific Problem: Split SMLT Link status
Description: Split SMLT link up: rcMltSmltId = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.19
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.30.4 Field descriptions

Table 27: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcMltSmltId and node ID of the device.

31.30.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.30.6 Additional information

This alarm requires no additional information.

31.31 Alarm (PP340)

rcnSmltLinkDown, Trap OID is1.3.6.1.4.1.2272.1.21.0.20

31.31.1 Explanation

The PP340 alarm signifies that the split SMLT link is down.

31.31.2 Action

Please refer to ERS8600 Fault Management document.

31.31.3 Corresponding Clear Log

PP339.

31.31.3.1 Format

31.31.3.2 NTSTD

zsups3f8 ** PP340 OCT26 01:28:49 0075 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: Split SMLT Link down
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; rcMltSmltId=1
Specific Problem: Split SMLT link status
Description: Split SMLT link down: rcMltSmltId = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.20
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.31.4 Field descriptions

Table 28: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcMltSmltId and node ID of the device.

31.31.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.31.6 Additional information

This alarm requires no additional information.

31.32 Alarm (PP341)

rcnPasswordChange, Trap OID is1.3.6.1.4.1.2272.1.21.0.22

31.32.1 Explanation

The PP341 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the one of the cli password is changed.

31.32.2 Action

Please refer to ERS8600 Fault Management document.

31.32.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.32.3.1 Format

31.32.3.2 NTSTD

zsups3f8 PP341 OCT26 01:28:49 0081 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: security
Cause: CLI password changed
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: CLI password has been changed
Description: CLI password changed (PasswordChange = ssladmin PassChangeResult = success)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.22
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.32.4 Field descriptions

Table 29: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.

Table 29: Field descriptions

Field	Value	Description
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.
PasswordChange	character string	Can be one of {ro (1), l1 (2), l2 (3), l3 (4), rw (5), rwa (6), slboper (7), l4oper (8), oper (9), slbadmin (10), l4admin (11), ssladmin (12), commStrRo (13), commStrRw (14), commStrl3 (15), commStrl2 (16), commStrl1 (17), webPassWdRo (18)}
PassChangeResult	character string	Can be one of {success (1), fail (2)}

31.32.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.32.6 Additional information

This alarm requires no additional information.

31.33 Alarm (PP342)

rcnPcmciaCardRemoved, Trap OID is1.3.6.1.4.1.2272.1.21.0.25

31.33.1 Explanation

The PP342 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the PCMCIA card is being removed.

31.33.2 Action

Please refer to ERS8600 Fault Management document.

31.33.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.33.3.1 Format

31.33.3.2 NTSTD

zsups3f8 *** PP342 OCT26 01:28:49 0085 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: PCMCIA card is being removed.
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: PCMCIA card removed.
Description: PCMCIA card is being removed.
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.25
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.33.4 Field descriptions

Table 30: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.33.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.33.6 Additional information

This alarm requires no additional information.

31.34 Alarm (PP343)

rcnSmartCpldTimerFired, Trap OID is1.3.6.1.4.1.2272.1.21.0.26

31.34.1 Explanation

The PP343 alarm signifies that the cpld timer fired.

31.34.2 Action

Please refer to ERS8600 Fault Management document.

31.34.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.34.3.1 Format

31.34.3.2 NTSTD

zsups3f8 ** PP343 OCT26 01:28:49 0087 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: cpld timer fired
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; CardIndex=1
Specific Problem: cpld timer fired
Description: cpld timer fired: CardIndex = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.26
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.34.4 Field descriptions

Table 31: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, CardIndex and node ID of the device.

31.34.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.34.6 Additional information

This alarm requires no additional information.

31.35 Alarm (PP344)

rcnCardCpldNotUpDate, Trap OID is1.3.6.1.4.1.2272.1.21.0.27

31.35.1 Explanation

The PP344 alarm signifies that the cpld is not up to date.

31.35.2 Action

Please refer to ERS8600 Fault Management document.

31.35.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.35.3.1 Format

31.35.3.2 NTSTD

zsups3f8 ** PP344 OCT26 01:28:49 0089 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: cpld is not up to date
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; CardIndex=1
Specific Problem: cpld not up to date
Description: cpld is not up to date: CardIndex = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.27
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.35.4 Field descriptions

Table 32: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, CardIndex and node ID of the device.

31.35.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.35.6 Additional information

This alarm requires no additional information.

31.36 Alarm (PP345)

rcnIgapLogFileFull, Trap OID is1.3.6.1.4.1.2272.1.21.0.28

31.36.1 Explanation

The PP345 alarm signifies that the Igap accounting time-out Log File reached the maximum.

31.36.2 Action

Please refer to ERS8600 Fault Management document.

31.36.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.36.3.1 Format

31.36.3.2 NTSTD

zsups3f8 ** PP345 OCT26 01:28:49 0091 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: processingError
Cause: Igap Log file full
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Igap Log file full
Description: Igap accounting time-out Log File reach the maximum.
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.28
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.36.4 Field descriptions

Table 33: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.

Table 33: Field descriptions

Field	Value	Description
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.36.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.36.6 Additional information

This alarm requires no additional information.

31.37 Alarm (PP346)

rcnCpLimitShutDown, Trap OID is1.3.6.1.4.1.2272.1.21.0.29

31.37.1 Explanation

The PP346 alarm signifies that the cp limit for the port is shutting down.

31.37.2 Action

Please refer to ERS8600 Fault Management document.

31.37.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.37.3.1 Format

31.37.3.2 NTSTD

```
zsups3f8  **   PP346 OCT26 01:28:50 0093 TBL  PP Fault
      Location: ERS8600_RTP;47.142.106.1
      State: Raised
      Category: equipment
      Cause: cp limit for the port is shutting down
      Time: Oct 26 01:28:50 2005
      Component ID: ERS8600=47.142.106.1; PortIndex=1
      Specific Problem: cp limit for the port is shutting down
     Description: Cp limit for port is shutting down: PortIndex= 1(AdminStatus
      = up OperStatus = down CpLimitShutDown = true)
      .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.29
      .1.3.6.1.4.1.2272.1.21.0.29: 0
      .1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

31.37.4 Field descriptions

Table 34: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, PortIndex and node ID of the device.
AdminStatus	character string	Can be one of {up (1), down (2), testing (3)}
OperationStatus	character string	Can be one of {up (1), down (2), testing (3), unknown (4), dormant (5)}
CpLimitShutDown	character string	Can be one of {true (1), false (2)}

31.37.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.37.6 Additional information

This alarm requires no additional information.

31.38 Alarm (PP347)

rcnSshServerEnabled, Trap OID is1.3.6.1.4.1.2272.1.21.0.30

31.38.1 Explanation

The PP347 alarm signifies that the SSH server is enabled.

31.38.2 Action

Please refer to ERS8600 Fault Management document.

31.38.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.38.3.1 Format

31.38.3.2 NTSTD

zsups3f8 PP347 OCT26 01:28:50 0097 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: communications
Cause: SSH server is enabled
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; SshGlobalPort=1
Specific Problem: SSH server enabled
Description: SSH server is enabled: SshGlobalPort = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.30
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.38.4 Field descriptions

Table 35: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, SshGlobalPort and node ID of the device.

31.38.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.38.6 Additional information

This alarm requires no additional information.

31.39 Alarm (PP348)

rcnSshServerDisabled, Trap OID is1.3.6.1.4.1.2272.1.21.0.31

31.39.1 Explanation

The PP348 alarm signifies that the SSH server is disabled.

31.39.2 Action

Please refer to ERS8600 Fault Management document.

31.39.3 Corresponding Clear Log

PP347.

31.39.3.1 Format

31.39.3.2 NTSTD

zsups3f8 ** PP348 OCT26 01:28:50 0095 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: communications
Cause: SSH server is disabled
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; SshGlobalPort=1
Specific Problem: SSH server disabled
Description: SSH server is disabled: SshGlobalPort = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.31
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.39.4 Field descriptions

Table 36: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, SshGlobalPort and node ID of the device.

31.39.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.39.6 Additional information

This alarm requires no additional information.

31.40 Alarm (PP349)

rcnSshSessionLogin, Trap OID is 1.3.6.1.4.1.2272.1.21.0.32

31.40.1 Explanation

The PP349 alarm signifies that there is a SSH session login.

31.40.2 Action

Please refer to ERS8600 Fault Management document.

31.40.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.40.3.1 Format

31.40.3.2 NTSTD

zsups3f8 PP349 OCT26 01:28:50 0099 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: SSH Session login
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1;
SshGlobalHostIpAddr=47.142.106.60
Specific Problem: SSH Session login
Description: SSH session login occurred: SshGlobalHostIpAddr = 47.142.106.60
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.32
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.40.4 Field descriptions

Table 37: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, SshGlobalHostIpAddr and node ID of the device.

31.40.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.40.6 Additional information

This alarm requires no additional information.

31.41 Alarm (PP350)

rcnSshSessionLogout, Trap OID is1.3.6.1.4.1.2272.1.21.0.33

31.41.1 Explanation

The PP350 alarm signifies that there is a SSH session logout.

31.41.2 Action

Please refer to ERS8600 Fault Management document.

31.41.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.41.3.1 Format

31.41.3.2 NTSTD

zsups3f8 PP350 OCT26 01:28:50 0101 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: SSH session logout
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1;
SshGlobalHostIpAddr=47.142.106.60
Specific Problem: SSH session logout
Description: SSH session logout occurred: SshGlobalHostIpAddr = 47.142.106.60
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.33
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.41.4 Field descriptions

Table 38: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.

Table 38: Field descriptions

Field	Value	Description
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, SshGlobalHostIpAddr and node ID of the device.

31.41.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.41.6 Additional information

This alarm requires no additional information.

31.42 Alarm (PP351)

rcnSshUnauthorizedAccess, Trap OID is1.3.6.1.4.1.2272.1.21.0.34

31.42.1 Explanation

The PP351 alarm signifies that an unauthorized access has occurred.

31.42.2 Action

Please refer to ERS8600 Fault Management document.

31.42.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.42.3.1 Format

31.42.3.2 NTSTD

zsups3f8 *** PP351 OCT26 01:28:50 0103 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: security
Cause: Unauthorized access
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1;
SshGlobalHostIpAddr=47.142.106.60
Specific Problem: Unauthorized access
Description: Unauthorized access occurred: SshGlobalHostIpAddr = 47.142.106.60

.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.34
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.42.4 Field descriptions

Table 39: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, SshGlobalHostIpAddr and node ID of the device.

31.42.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.42.6 Additional information

This alarm requires no additional information.

31.43 Alarm (PP352)

rcnHaCpuState, Trap OID is1.3.6.1.4.1.2272.1.21.0.35

31.43.1 Explanation

The PP352 alarm signifies that the state of the HA-CPU.

31.43.2 Action

Please refer to ERS8600 Fault Management document.

31.43.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.43.3.1 Format

31.43.3.2 NTSTD

zsups3f8 *** PP352 OCT26 01:28:50 0105 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised

Category: equipment
Cause: State of the HA-CPU
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; CardIndex=1
Specific Problem: State of the HA-CPU
Description: State of the HA-CPU: CardIndex = 1 (HaCpuState = initialization)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.35
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.43.4 Field descriptions

Table 40: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, CardIndex and node ID of the device.
HaCpuState	character string	Can be one of {initialization (0), oneWayActive (1), twoWayActive (2), synchronized (3), remoteIncompatible (4), error (5), disabled (6), peerNotConnected (7), peerConnected (8), lostPeerConnection (9), notSynchronized (10)}

31.43.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.43.6 Additional information

This alarm requires no additional information.

31.44 Alarm (PP353)

rcnInsufficientMemory, Trap OID is1.3.6.1.4.1.2272.1.21.0.36

31.44.1 Explanation

The PP353 alarm signifies that insufficient memory on CPU blade for proper operation. Recommended memory = 256 MB available through Nortel Networks upgrade kit.

31.44.2 Action

Please refer to ERS8600 Fault Management document.

31.44.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.44.3.1 Format

31.44.3.2 NTSTD

zsups3f8 *** PP353 OCT26 01:28:50 0107 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: environmental
Cause: Insufficient memory on CPU blade for proper operation
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; CardIndex=1
Specific Problem: Insufficient memory on CPU
Description: Insufficient memory: CardIndex = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.36
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.44.4 Field descriptions

Table 41: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, CardIndex and node ID of the device.

31.44.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.44.6 Additional information

This alarm requires no additional information.

31.45 Alarm (PP354)

rcnSaveConfigAction, Trap OID is 1.3.6.1.4.1.2272.1.21.0.37

31.45.1 Explanation

The PP354 alarm signifies that the switch run time or boot configuration is being saved.

31.45.2 Action

Please refer to ERS8600 Fault Management document.

31.45.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.45.3.1 Format

31.45.3.2 NTSTD

zsups3f8 PP354 OCT26 01:28:50 0109 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: processingError
Cause: Switch run time or boot configuration is saved
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Switch configuration saved
Description: Switch configuration saved: SysAction = none
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.37
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.45.4 Field descriptions

Table 42: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.

Table 42: Field descriptions

Field	Value	Description
Component Id	character string	Indicates the IP address and node ID of the device.
SysAction	character string	Can be one of {none (1), hardReset (2), softReset (3), saveToNVRAM (4), resetCounters (5), saveToStandbyNVRAM (6), cpuSwitchOver (7), checkSwInFlash (8), checkSwInPcmcia (9), resetConsole (10), resetModem (11), flushIpRouteTbl (12), saveRuntimeConfig (13), saveRuntimeConfigToSlave (14), saveBootConfig (15), saveSlaveBootConfig (16), resetIstStatCounters (17)}

31.45.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.45.6 Additional information

This alarm requires no additional information.

31.46 Alarm (PP355)

rcnLoopDetectOnPort, Trap OID is1.3.6.1.4.1.2272.1.21.0.38

31.46.1 Explanation

The PP355 alarm signifies that a loop has been detected on a port. The vlan on that port will be disabled.

31.46.2 Action

Please refer to ERS8600 Fault Management document.

31.46.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.46.3.1 Format

31.46.3.2 NTSTD

zsups3f8 *** PP355 OCT26 01:28:50 0111 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised

Category: communications
Cause: Loop detected on port. The vlan on that port will be disabled
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; PortIndex=1
Specific Problem: Loop detected on port.
Description: Loop detected on port: PortIndex = 1 (rcVlanId = 1)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.38
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.46.4 Field descriptions

Table 43: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, PortIndex and node ID of the device.

31.46.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.46.6 Additional information

This alarm requires no additional information.

31.47 Alarm (PP356)

vrrpTrapStateTransition, Trap OID is1.3.6.1.2.1.46.1.3.0.3.0

31.47.1 Explanation

The PP356 alarm signifies that a state transition has occurred on a particular vrrp interface. Implementation of this trap is optional. 'vrrpOperIpAddr' contains the IP address of the vrrp interface while 'ipAdEntAddr' contains the IP address assigned to physical interface.

31.47.2 Action

Please refer to ERS8600 Fault Management document.

31.47.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.47.3.1 Format

31.47.3.2 NTSTD

zsups3f8 *** PP356 OCT26 01:28:49 0063 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: communications
Cause: State transition has occurred on vrrp interface
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; ifIndex=100
Specific Problem: Trap state transition
Description: State Transition: ifIndex = 100 (TransitionType = masterToBackup TransitionCause = shutdownReceived Port = 37 Slot = 1)
.1.3.6.1.2.1.4.20.1.1.0: 0.0.0.0
.1.3.6.1.2.1.46.1.1.10.1.3.0: 0.0.0.0
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.46.1.3.0.3.0
.1.3.6.1.2.1.46.1.1.10.1.2.0: 0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.47.4 Field descriptions

Table 44: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ifIndex and node ID of the device.
TransitionType	character string	Can be one of {none (1), masterToBackup (2), backupToMaster (3), initializeToMaster (4), masterToInitialize (5), initializeToBackup (6), backupToInitialize (7),backupToBackUpMaster (8), backUpMasterToBackup (9)}

Table 44: Field descriptions

Field	Value	Description
TransitionCause	character string	Can be one of {none (1),higherPriorityAdvertizeReceived (2), shutdownReceived (3), vrrpAddrAndPhysicalAddrMatch (4), masterDownInterval (5), preempted (6), criticalIPFail (7), usrConfig (8), syncFromPrimary (9), iPInterfaceDown (10), lowerPioAdvReceived (11), higherSrcIPEqualPrioAdvReceived (12), lowerSrcIPEqualPrioAdvReceived (13), startVR (14), other (15)}
PhysicalInfo	character string	Indicates the phsyical information appended to TransitionCause. The actual physical information is determined by ifIndex. ifIndex >= 64 and ifIndex <= 703 the information is: Port = ‘(ifIndex & 0x3f) + 1‘ Slot = ‘ifIndex >>6‘ ifIndex >= 832 and ifIndex <= 863 the information is: Circuitless IP = ‘ifIndex - 832 + 1‘ ifIndex >= 2048 and ifIndex <= 4095 the information is: VLAN = ‘ifIndex - 2048 + 1‘ ifIndex >= 4096 and ifIndex <= 4127 the information is: MLT = ‘ifIndex - 4096 + 1‘ ifIndex >= 4352 and ifIndex <= 5351 the information is: Tunnel = ‘ifIndex - 4352 + 1‘ An ifIndex not within the above ranges, the information is: unknown of ifIndex meaning Note: The content in ‘‘ part will be calculated out.

31.47.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.47.6 Additional information

This alarm requires no additional information.

31.48 Alarm (PP357)

rcnEmError, Trap OID is1.3.6.1.4.1.2272.1.21.0.23

31.48.1 Explanation

The PP357 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected Em error.

31.48.2 Action

Please refer to ERS8600 Fault Management document.

31.48.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.48.3.1 Format

31.48.3.2 NTSTD

zsups3f8 PP357 OCT26 01:28:49 0079 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Em error detected
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; CardIndex=1
Specific Problem: Em error detected
Description: Em error: CardIndex = 1 (Em Error = none)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.23
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.48.4 Field descriptions

Table 45: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, CardIndex and node ID of the device.

Table 45: Field descriptions

Field	Value	Description
Em Error	character string	Can be one of {none (1), non128KCardOffLine (2), checkSlaveConfigNResetForEmMMode (3), mismatchResetForEmMode (4), mismatchEmModeMasterSlave (5), incompatMasterResetForEmMode (6), putSlaveOffEmImcompat (7), slave8690EmIncompatGoingOffline (8), cpu8690DisableEm (9)}

31.48.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.48.6 Additional information

This alarm requires no additional information.

31.49 Alarm (PP358)

ospfVirtIfStateChange, Trap OID is1.3.6.1.2.1.14.16.2.1

31.49.1 Explanation

The PP358 alarm signifies that there has been a change in the state of an OSPF virtual interface. This trap should be generated when the interface state regresses (e.g., goes from Point-to-Point to Down) or progresses to a terminal state (i.e., Point-to-Point).

31.49.2 Action

Please refer to ERS8600 Fault Management document.

31.49.3 Corresponding Clear Log

PP358.

31.49.3.1 Format

31.49.3.2 NTSTD

zsups3f8 PP358 OCT26 01:28:48 0043 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: environmental
Cause: OSPF virtual interface state change
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70

Specific Problem: OSPF virtual interface state change
Description: OSPF virtual interface state change: ospfRouterId = 47.142.106.70 (AreaId = 0.0.0.0 Neighbor = 0.0.0.0 State = pointToPoint)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.1
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.49.4 Field descriptions

Table 46: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.
Severity	warning/clear	Indicated the alarm severity. It is determined by the State value.
State (In the Description)	character string	State = “down”, indicates warning alarm. State = “pointToPoint”, indicates clear alarm.

31.49.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.49.6 Additional information

This alarm requires no additional information.

31.50 Alarm (PP359)

ospfNbrStateChange, Trap OID is1.3.6.1.2.1.14.16.2.2

31.50.1 Explanation

The PP359 alarm signifies that there has been a change in the state of a non-virtual OSPF neighbor. This trap should be generated when the neighbor state

regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., 2-Way or Full). When an neighbor transitions from or to Full on non-broadcast multi-access and broadcast networks, the trap should be generated by the designated router. A designated router transitioning to Down will be noted by ospfIfStateChange.

31.50.2 Action

Please refer to ERS8600 Fault Management document.

31.50.3 Corresponding Clear Log

PP359.

31.50.3.1 Format

31.50.3.2 NTSTD

zsups3f8 PP359 OCT26 01:28:48 0029 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Non-virtual neighbor state change
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
Specific Problem: Non-virtual OSPF neighbor state change
Description: Non-virtual neighbor state change: RouterId = 47.142.106.70 (NbrIpAddr = 47.154.182.56 NbrRouter = 47.154.182.1 State = loading)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.2
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.14.10.1.2: 0

31.50.4 Field descriptions

Table 47: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.

Table 47: Field descriptions

Field	Value	Description
Severity	warning/clear	Indicated the alarm severity. It is determined by the State value.
State (In the Description)	character string	State = “down”, “attempt”, “init”, “twoWay”, “exchangeStart”, “exchange”, “loading”, indicates warning alarm. State = “full”, indicates clear alarm.

31.50.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.50.6 Additional information

This alarm requires no additional information.

31.51 Alarm (PP360)

ospfVirtNbrStateChange, Trap OID is1.3.6.1.2.1.14.16.2.3

31.51.1 Explanation

The PP360 alarm signifies that there has been a change in the state of an OSPF virtual neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).

31.51.2 Action

Please refer to ERS8600 Fault Management document.

31.51.3 Corresponding Clear Log

PP360.

31.51.3.1 Format

31.51.3.2 NTSTD

zsups3f8 * PP360 OCT26 01:28:48 0037 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1

State: Raised
Category: environmental
Cause: Virtual OSPF neighbor state change
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
Specific Problem: Virtual OSPF neighbor state change
Description: Virtual neighbor state change: RouterId = 47.142.106.70 (NbrArea = 47.154.182.56 NbrRouter = 47.154.182.1 State = loading)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.3
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.51.4 Field descriptions

Table 48: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.
Severity	minor/clear	Indicated the alarm severity. It is determined by the State value.
State (In the Description)	character string	State = “down”, “attempt”, “init”, “twoWay”, “exchangeStart”, “exchange”, “loading”, indicates warning alarm. State = “full”, indicates clear alarm.

31.51.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.51.6 Additional information

This alarm requires no additional information.

31.52 Alarm (PP361)

ospfIfConfigError, Trap OID is1.3.6.1.2.1.14.16.2.4

31.52.1 Explanation

The PP361 alarm signifies that a packet has been received on a non-virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. Note that the event option Mismatch should cause a trap only if it prevents an adjacency from forming.

31.52.2 Action

Please refer to ERS8600 Fault Management document.

31.52.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.52.3.1 Format

31.52.3.2 NTSTD

zsups3f8 *** PP361 OCT26 01:28:48 0031 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Configuration error
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
Specific Problem: configuration error
Description: IfConfig Error: ospfRouterId = 47.142.106.70 (IpAddress = 47.154.182.56)
.1.3.6.1.2.1.14.7.1.2: 0
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.4
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.52.4 Field descriptions

Table 49: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.

Table 49: Field descriptions

Field	Value	Description
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.

31.52.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.52.6 Additional information

This alarm requires no additional information.

31.53 Alarm (PP362)

ospfVirtIfConfigError, Trap OID is1.3.6.1.2.1.14.16.2.5

31.53.1 Explanation

The PP362 alarm signifies that a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. Note that the event optionMismatch should cause a trap only if it prevents an adjacency from forming.

31.53.2 Action

Please refer to ERS8600 Fault Management document.

31.53.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.53.3.1 Format

31.53.3.2 NTSTD

zsups3f8 *** PP362 OCT26 01:28:48 0039 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Virtual interface configuration error
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
Specific Problem: Virtual interface configuration error
Description: VirtIfConfigError: ospfRouterId = 47.142.106.70 (AreaId = 47.154.182.1 Neighbor = 47.154.182.56 ErrorType =badVersion)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.5

.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.53.4 Field descriptions

Table 50: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.
ErrorType	character string	Can be one of {badVersion (1), areaMismatch (2), unknownNbmaNbr (3), unknownVirtualNbr (4), authTypeMismatch (5), authFailure (6), netMaskMismatch (7), helloIntervalMismatch (8), deadIntervalMismatch (9), optionMismatch (10), crcCheckFailed (11)}

31.53.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.53.6 Additional information

This alarm requires no additional information.

31.54 Alarm (PP363)

ospfIfAuthFailure, Trap OID is1.3.6.1.2.1.14.16.2.6

31.54.1 Explanation

The PP363 alarm signifies that a packet has been received on a non-virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.

31.54.2 Action

Please refer to ERS8600 Fault Management document.

31.54.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.54.3.1 Format

31.54.3.2 NTSTD

```
zsups3f8 ***   PP363 OCT26 01:28:48 0033 TBL  PP Fault
     Location: ERS8600_RTP;47.142.106.1
     State: Raised
     Category: security
     Cause: ospf If authentication failure
     Time: Oct 26 01:28:48 2005
     Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
     Specific Problem: ospf If authentication failure
     Description: ospf If authentication failure: ospfRouterId = 47.142.106.70
     (ConfigErrorType =authTypeMismatch)
     .1.3.6.1.2.1.14.7.1.2: 0
     .1.3.6.1.2.1.14.7.1.1: 0.0.0.0
     .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.6
     .1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

31.54.4 Field descriptions

Table 51: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.
ConfigErrorType	character string	Can be one of {badVersion (1), areaMismatch (2), unknownNbmaNbr (3), unknownVirtualNbr (4), authTypeMismatch (5), authFailure (6), netMaskMismatch (7), helloIntervalMismatch (8), deadIntervalMismatch (9), optionMismatch (10), crcCheckFailed (11)}

31.54.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.54.6 Additional information

This alarm requires no additional information.

31.55 Alarm (PP364)

ospfVirtIfAuthFailure, Trap OID is1.3.6.1.2.1.14.16.2.7

31.55.1 Explanation

The PP364 alarm signifies that a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.

31.55.2 Action

Please refer to ERS8600 Fault Management document.

31.55.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.55.3.1 Format

31.55.3.2 NTSTD

zsups3f8 *** PP364 OCT26 01:28:48 0041 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: security
Cause: ospf virtual interface authentication failure
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
Specific Problem:
Description: ospfVirtIfAuthFailure: ospfRouterId = 47.142.106.70 (AreaId = 47.154.182.1 Neighbor = 47.154.182.56 ErrorType =authTypeMismatch)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.7
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.55.4 Field descriptions

Table 52: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.

Table 52: Field descriptions

Field	Value	Description
ErrorType	character string	Can be one of {badVersion (1), areaMismatch (2), unknownNbmaNbr (3), unknownVirtualNbr (4), authTypeMismatch (5), authFailure (6), netMaskMismatch (7), helloIntervalMismatch (8), deadIntervalMismatch (9), optionMismatch (10), crcCheckFailed (11)}

31.55.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.55.6 Additional information

This alarm requires no additional information.

31.56 Alarm (PP365)

ospfIfStateChange, Trap OID is1.3.6.1.2.1.14.16.2.16

31.56.1 Explanation

The PP365 alarm signifies that there has been a change in the state of a non-virtual OSPF interface. This trap should be generated when the interface state regresses (e.g., goes from Dr to Down) or progresses to a terminal state (i.e., Point-to-Point, DR Other, Dr, or Backup).

31.56.2 Action

Please refer to ERS8600 Fault Management document.

31.56.3 Corresponding Clear Log

PP365.

31.56.3.1 Format

31.56.3.2 NTSTD

zsups3f8 PP365 OCT26 01:28:48 0036 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: equipment
Cause: Non-virtual OSPF interface state change
Time: Oct 26 01:28:48 2005

Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
Specific Problem: Non-virtual OSPF interface state change
Description: Non-virtual OSPF interface state change: ospfRouterId = 47.142.106.70 (IpAddress = 47.154.182.56 State =pointToPoint)
.1.3.6.1.2.1.14.7.1.2: 0
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.16
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.56.4 Field descriptions

Table 53: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.
Severity	warning/clear	Indicated the alarm severity. It is determined by the State value.
State (In the Description)	character string	State = “down”, “loopback”, “waiting”, indicates warning alarm. State = “pointToPoint”, “designedRouter”, “backupDesignatedRouter”, “otherDesignatedRouter”, indicates clear alarm.

31.56.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.56.6 Additional information

This alarm requires no additional information.

31.57 Alarm (PP366)

rcnCardDown, Trap OID is1.3.6.1.4.1.2272.1.21.0.1

31.57.1 Explanation

The PP366 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcCardOperStatus object for one of its cards is about to transition into the down state.

31.57.2 Action

Please refer to ERS8600 Fault Management document.

31.57.3 Corresponding Clear Log

PP367.

31.57.3.1 Format

31.57.3.2 NTSTD

zsups3f8 *** PP366 OCT26 01:28:48 0019 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: RC Card status down
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; rcCardIndex=1
Specific Problem: RC Card status
Description: RC card status down: CardIndex = 1 (AdminStatus = up OperStatus = down)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.1
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.57.4 Field descriptions

Table 54: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcCardIndex and node ID of the device.

Table 54: Field descriptions

Field	Value	Description
AdminStatus	character string	Can be one of {up (1), down (2), testing (3)}
OperStatus	character string	Can be one of {up (1), down (2), testing (3), unknown (4), dormant (5)}

31.57.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.57.6 Additional information

This alarm requires no additional information.

31.58 Alarm (PP367)

rcnCardUp, Trap OID is1.3.6.1.4.1.2272.1.21.0.2

31.58.1 Explanation

The PP367 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the rcCardOperStatus object for one of its cards is about to transition into the up state.

31.58.2 Action

Please refer to ERS8600 Fault Management document.

31.58.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.58.3.1 Format

31.58.3.2 NTSTD

zsups3f8 PP367 OCT26 01:28:48 0021 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: equipment
Cause: RC card status up
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; rcCardIndex=0
Specific Problem: RC Card Status
Description: RC card status up: CardIndex = 0 (AdminStatus = up OperStatus = up)

.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.2
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.58.4 Field descriptions

Table 55: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcCardIndex and node ID of the device.
AdminStatus	character string	Can be one of {up (1), down (2), testing (3)}
OperStatus	character string	Can be one of {up (1), down (2), testing (3), unknown (4), dormant (5)}

31.58.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.58.6 Additional information

This alarm requires no additional information.

31.59 Alarm (PP368)

rcnbgpEstablished, Trap OID is1.3.6.1.4.1.2272.1.21.0.39

31.59.1 Explanation

The PP368 alarm is generated when the BGP FSM enters the ESTABLISHED state.

31.59.2 Action

Please refer to ERS8600 Fault Management document.

31.59.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.59.3.1 Format

31.59.3.2 NTSTD

zsups3f8 PP368 OCT26 01:28:50 0113 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: communications
Cause: BGP FSM entered the ESTABLISHED state
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1;
rcIpBgpPeerIpAddress=47.142.106.70
Specific Problem: BGP FSM entered the ESTABLISHED state
Description: BGP FSM entered ESTABLISHED state: PeerIpAddress = 47.142.106.70 (PeerLastError = 1 PeerState =active)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.39
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.59.4 Field descriptions

Table 56: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcIpBgpPeerIpAddress and node ID of the device.
PeerState	character string	Can be one of {idle (1), connect (2), active (3), opensent (4), openconfirm (5), established (6)}

31.59.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.59.6 Additional information

This alarm requires no additional information.

31.60 Alarm (PP369)

rcnbgpBackwardTransition, Trap OID is1.3.6.1.4.1.2272.1.21.0.40

31.60.1 Explanation

The PP369 alarm is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.

31.60.2 Action

Please refer to ERS8600 Fault Management document.

31.60.3 Corresponding Clear Log

PP368.

31.60.3.1 Format

31.60.3.2 NTSTD

zsups3f8 *** PP369 OCT26 01:28:50 0115 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: communications
Cause: BGP FSM backward transition
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1;
rcIpBgpPeerIpAddress=47.142.106.70
Specific Problem: BGP FSM backward transition
Description: BGP FSM backward transition: PeerIpAddress = 47.142.106.70 (PeerLastError = 1 PeerState = active)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.40
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.60.4 Field descriptions

Table 57: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.

Table 57: Field descriptions

Field	Value	Description
Component Id	character string	Indicates the IP address, rcIpBgpPeerIpAddress and node ID of the device.
PeerState	character string	Can be one of {idle (1), connect (2), active (3), opensent (4), openconfirm (5), established (6)}

31.60.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.60.6 Additional information

This alarm requires no additional information.

31.61 Alarm (PP370)

rcnAggLinkUp, Trap OID is 1.3.6.1.4.1.2272.1.21.0.41

31.61.1 Explanation

The PP370 alarm is generated when the operational state of the aggregator changes from down to up.

31.61.2 Action

Please refer to ERS8600 Fault Management document.

31.61.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.61.3.1 Format

31.61.3.2 NTSTD

zsups3f8 PP370 OCT26 01:28:50 0117 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: communications
Cause: Aggregator up
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; rcMltId=1
Specific Problem: Aggregator status

Description: Aggregator up: rcMltId = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.41
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.61.4 Field descriptions

Table 58: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcMltId and node ID of the device.

31.61.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.61.6 Additional information

This alarm requires no additional information.

31.62 Alarm (PP371)

rcnAggLinkDown, Trap OID is 1.3.6.1.4.1.2272.1.21.0.42

31.62.1 Explanation

The PP371 alarm is generated when the operational state of the aggregator changes from up to down.

31.62.2 Action

Please refer to ERS8600 Fault Management document.

31.62.3 Corresponding Clear Log

PP370.

31.62.3.1 Format

31.62.3.2 NTSTD

zsups3f8 ** PP371 OCT26 01:28:50 0119 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1

State: Raised
Category: communications
Cause: Aggregator Down
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; rcMltId=1
Specific Problem: Aggregator status
Description: Aggregator Down: rcMltId = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.42
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.62.4 Field descriptions

Table 59: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcMltId and node ID of the device.

31.62.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.62.6 Additional information

This alarm requires no additional information.

31.63 Alarm (PP372)

rcnIgmpNewGroupMember, Trap OID is 1.3.6.1.4.1.2272.1.21.0.43

31.63.1 Explanation

The PP372 alarm signifies that a new member has come on an interface.

31.63.2 Action

Please refer to ERS8600 Fault Management document.

31.63.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.63.3.1 Format

31.63.3.2 NTSTD

zsups3f8 PP372 OCT26 01:28:50 0127 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: New Group member in interface
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; rcIgmpGroupIfIndex=0
Specific Problem: New Group member in interface
Description: New Group member in interface: rcIgmpGroupIfIndex = 0 (GroupIpAddress = 47.142.106.70 Port = 0 Members 47.142.106.71)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.43
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.63.4 Field descriptions

Table 60: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcIgmpGroupIfIndex and node ID of the device.

31.63.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.63.6 Additional information

This alarm requires no additional information.

31.64 Alarm (PP373)

rcnIgmpLossGroupMember, Trap OID is 1.3.6.1.4.1.2272.1.21.0.44

31.64.1 Explanation

The PP373 alarm signifies that a group member has been lost on an interface.

31.64.2 Action

Please refer to ERS8600 Fault Management document.

31.64.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.64.3.1 Format

31.64.3.2 NTSTD

zsups3f8 PP373 OCT26 01:28:50 0129 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Group member lost on interface
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; rcIgmpGroupIfIndex=0
Specific Problem: Group member lost on interface
Description: Group member lost on interface: rcIgmpGroupIfIndex = 0 (GroupIpAddress = 47.142.106.70 Port = 0 Members 47.142.106.71)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.44
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.64.4 Field descriptions

Table 61: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcIgmpGroupIfIndex and node ID of the device.

31.64.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.64.6 Additional information

This alarm requires no additional information.

31.65 Alarm (PP374)

rcnIgmpNewQuerier, Trap OID is 1.3.6.1.4.1.2272.1.21.0.45

31.65.1 Explanation

The PP374 alarm signifies that a new querier has come up on an interface.

31.65.2 Action

Please refer to ERS8600 Fault Management document.

31.65.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.65.3.1 Format

31.65.3.2 NTSTD

zsups3f8 PP374 OCT26 01:28:50 0131 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: New Querier in interface
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; igmpInterfaceIfIndex=0
Specific Problem: New Querier in interface
Description: New Querier in interface: igmpInterfaceIfIndex = 0
(igmpInterfaceQuerier = 47.142.106.70)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.45
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.65.4 Field descriptions

Table 62: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.

Table 62: Field descriptions

Field	Value	Description
Component Id	character string	Indicates the IP address, igmpInterfaceIfIndex and node ID of the device.

31.65.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.65.6 Additional information

This alarm requires no additional information.

31.66 Alarm (PP375)

rcnIgmpQuerierChange, Trap OID is1.3.6.1.4.1.2272.1.21.0.46

31.66.1 Explanation

The PP375 alarm signifies that the querier has changed.

31.66.2 Action

Please refer to ERS8600 Fault Management document.

31.66.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.66.3.1 Format

31.66.3.2 NTSTD

zsups3f8 PP375 OCT26 01:28:50 0133 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Querier changed
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; igmpInterfaceIfIndex=0
Specific Problem: Querier changed
Description: Querier changed: igmpInterfaceIfIndex = 0 (NewQuerier = 47.142.106.70 igmpInterfaceQuerier = 47.142.106.71)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.46
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.66.4 Field descriptions

Table 63: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, igmpInterfaceIfIndex and node ID of the device.

31.66.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.66.6 Additional information

This alarm requires no additional information.

31.67 Alarm (PP376)

rcnDvmrpIfStateChange, Trap OID is 1.3.6.1.4.1.2272.1.21.0.47

31.67.1 Explanation

The PP376 alarm signifies that there has been a change in the state of a DVMRP interface.

31.67.2 Action

Please refer to ERS8600 Fault Management document.

31.67.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.67.3.1 Format

31.67.3.2 NTSTD

zsups3f8 PP376 OCT26 01:28:50 0121 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications

Cause: DVMRP interface state change
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; dvmrpInterfaceIfIndex=0
Specific Problem: DVMRP interface state change
Description: DVMRP interface state change: dvmrpInterfaceIfIndex = 0 (OperState = up)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.47
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.67.4 Field descriptions

Table 64: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, dvmrpInterfaceIfIndex and node ID of the device.
OperState	character string	Can be one of {up (1), down (2)}

31.67.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.67.6 Additional information

This alarm requires no additional information.

31.68 Alarm (PP377)

rcnDvmrpNewNbrChange, Trap OID is1.3.6.1.4.1.2272.1.21.0.48

31.68.1 Explanation

The PP377 alarm signifies that a new neighbor has come up on a DVMRP interface.

31.68.2 Action

Please refer to ERS8600 Fault Management document.

31.68.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.68.3.1 Format

31.68.3.2 NTSTD

zsups3f8 PP377 OCT26 01:28:50 0123 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: New neighbor is up on DVMRP interface
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; dvmrpNeighborIfIndex=0
Specific Problem: New neighbor is up on DVMRP interface
Description: New neighbor is up on DVMRP interface:
dvmrpNeighborIfIndex= 0 (NeighborAddress = 47.142.106.70)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.48
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.68.4 Field descriptions

Table 65: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, dvmrpNeighborIfIndex and node ID of the device.

31.68.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.68.6 Additional information

This alarm requires no additional information.

31.69 Alarm (PP378)

rcnDvmrpNbrLossChange, Trap OID is1.3.6.1.4.1.2272.1.21.0.49

31.69.1 Explanation

The PP378 alarm signifies that a new neighbor has gone down on a DVMRP interface.

31.69.2 Action

Please refer to ERS8600 Fault Management document.

31.69.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.69.3.1 Format

31.69.3.2 NTSTD

zsups3f8 PP378 OCT26 01:28:50 0125 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Neighbor gone down on DVMRP interface
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; dvmrpNeighborIfIndex=0
Specific Problem: Neighbor gone down on DVMRP interface
Description: Neighbor gone down on DVMRP interface:
dvmrpNeighborIfIndex= 0 (NeighborAddress = 47.142.106.70)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.49
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.69.4 Field descriptions

Table 66: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, dvmrpNeighborIfIndex and node ID of the device.

31.69.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.69.6 Additional information

This alarm requires no additional information.

31.70 Alarm (PP379)

rcnFdbProtectViolation, Trap OID is 1.3.6.1.4.1.2272.1.21.0.59

31.70.1 Explanation

The PP379 alarm signifies that the system has violated the user configured limit for total number of fdb-entries learned on that port.

31.70.2 Action

Please refer to ERS8600 Fault Management document.

31.70.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.70.3.1 Format

31.70.3.2 NTSTD

zsups3f8 PP379 OCT26 01:28:50 0151 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: fdb-entries limit violation
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; PortIndex=1
Specific Problem: fdb-entries limit violation
Description: fdb-entries limit violation: PortIndex = 1 (VlanId = 1)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.59
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.70.4 Field descriptions

Table 67: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.

Table 67: Field descriptions

Field	Value	Description
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, PortIndex and node ID of the device.

31.70.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.70.6 Additional information

This alarm requires no additional information.

31.71 Alarm (PP380)

rcnLogMsgControl, Trap OID is 1.3.6.1.4.1.2272.1.21.0.60

31.71.1 Explanation

The PP380 alarm signifies whether or not the number of repetitions of the particular Log message has exceeded the particular frequency/count or not.

31.71.2 Action

Please refer to ERS8600 Fault Management document.

31.71.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.71.3.1 Format

31.71.3.2 NTSTD

zsups3f8 PP380 OCT26 01:28:50 0157 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: equipment
Cause: Log Message control trap
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Log Message control trap
Description: rcnLogMsgControl: SysMsgLogFrequency = 2
(SysMsgLogText =)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.60

.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.71.4 Field descriptions

Table 68: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.71.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.71.6 Additional information

This alarm requires no additional information.

31.72 Alarm (PP381)

rcnSaveConfigFile, Trap OID is 1.3.6.1.4.1.2272.1.21.0.61

31.72.1 Explanation

The PP381 alarm signifies that either the runtime config or the boot config has been saved on the switch.

31.72.2 Action

Please refer to ERS8600 Fault Management document.

31.72.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.72.3.1 Format

31.72.3.2 NTSTD

zsups3f8 PP381 OCT26 01:28:50 0153 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: equipment

Cause: Run time / boot config saved on switch
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Run time / boot config saved on switch
Description: Config saved on switch: SysAction = none
(SysConfigFileName = boot.conf)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.61
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.72.4 Field descriptions

Table 69: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.
SysAction	character string	Can be one of {none (1), hardReset (2), softReset (3), saveToNVRAM (4), resetCounters (5), saveToStandbyNVRAM (6), cpuSwitchOver (7), checkSwInFlash (8), checkSwInPcmcia (9), resetConsole (10), resetModem (11), flushIpRouteTbl (12), saveRuntimeConfig (13), saveRuntimeConfigToSlave (14), saveBootConfig (15), saveSlaveBootConfig (16), resetIstStatCounters (17)}

31.72.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.72.6 Additional information

This alarm requires no additional information.

31.73 Alarm (PP382)

rcnDNSRequestResponse, Trap OID is 1.3.6.1.4.1.2272.1.21.0.62

31.73.1 Explanation

The PP382 alarm signifies that the switch had sent a query to the DNS server or it had received a successful response from the DNS Server.

31.73.2 Action

Please refer to ERS8600 Fault Management document.

31.73.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.73.3.1 Format

31.73.3.2 NTSTD

zsups3f8 PP382 OCT26 01:28:50 0155 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Request/Response from DNS server
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Request/Response from DNS server
Description: Request sent to or response got from DNS server:
DnsServerLastIpAddr = 47.154.182.1 (DnsRequestType = request)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.62
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.73.4 Field descriptions

Table 70: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.
DnsRequestType	character string	Can be one of {request (0), response (1)}

31.73.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.73.6 Additional information

This alarm requires no additional information.

31.74 Alarm (PP383)

pingProbeFailed, Trap OID is 1.3.6.1.2.1.80.0.1.0

31.74.1 Explanation

The PP383 alarm is generated when a probe failure is detected when the corresponding pingCtlTrapGeneration object is set to probeFailure(0) subject to the value of pingCtlTrapProbeFailureFilter. The object pingCtlTrapProbeFailureFilter can be used to specify the number of successive probe failures that are required before this notification can be generated.

31.74.2 Action

Please refer to ERS8600 Fault Management document.

31.74.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.74.3.1 Format

31.74.3.2 NTSTD

zsups3f8 PP383 OCT26 01:28:50 0135 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Probe failure is detected
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Probe failure is detected
Description: Probe failure is detected: (ping TargetAddress = 47.154.182.56)
.1.3.6.1.2.1.80.1.3.1.8.0: 0
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.80.0.1.0
.1.3.6.1.2.1.80.1.3.1.4.0: 2485256176
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.80.1.3.1.9.0: 0
.1.3.6.1.2.1.80.1.3.1.5.0: 1208611943
.1.3.6.1.2.1.80.1.3.1.10.0:
.1.3.6.1.2.1.80.1.3.1.6.0: 941686800
.1.3.6.1.2.1.80.1.3.1.7.0: 1208902023
.1.3.6.1.2.1.80.1.3.1.3.0: 8a

31.74.4 Field descriptions

Table 71: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.74.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.74.6 Additional information

This alarm requires no additional information.

31.75 Alarm (PP384)

pingTestFailed, Trap OID is 1.3.6.1.2.1.80.0.2.0

31.75.1 Explanation

The PP384 alarm is generated when a ping test is determined to have failed when the corresponding pingCtlTrapGeneration object is set to testFailure(1). In this instance pingCtlTrapTestFailureFilter should specify the number of probes in a test required to have failed in order to consider the test as failed.

31.75.2 Action

Please refer to ERS8600 Fault Management document.

31.75.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.75.3.1 Format

31.75.3.2 NTSTD

zsups3f8 PP384 OCT26 01:28:50 0137 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications

Cause: Ping test failed
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Ping test failed
Description: Ping test failed: (ping TargetAddress = 47.154.182.56)
.1.3.6.1.2.1.80.1.3.1.8.0: 0
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.80.0.2.0
.1.3.6.1.2.1.80.1.3.1.4.0: 2485256176
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.80.1.3.1.9.0: 0
.1.3.6.1.2.1.80.1.3.1.5.0: 1208611943
.1.3.6.1.2.1.80.1.3.1.10.0:
.1.3.6.1.2.1.80.1.3.1.6.0: 941686800
.1.3.6.1.2.1.80.1.3.1.7.0: 1208902023
.1.3.6.1.2.1.80.1.3.1.3.0: 8a

31.75.4 Field descriptions

Table 72: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.75.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.75.6 Additional information

This alarm requires no additional information.

31.76 Alarm (PP385)

pingTestCompleted, Trap OID is 1.3.6.1.2.1.80.0.3.0

31.76.1 Explanation

The PP385 alarm is generated at the completion of a ping test when the corresponding pingCtlTrapGeneration object is set to testCompletion(4).

31.76.2 Action

Please refer to ERS8600 Fault Management document.

31.76.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.76.3.1 Format

31.76.3.2 NTSTD

zsups3f8 PP385 OCT26 01:28:50 0139 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Ping test completed
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Ping test completed.
Description: Ping test completed: (ping TargetAddress = 47.154.182.56)
.1.3.6.1.2.1.80.1.3.1.8.0: 0
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.80.0.3.0
.1.3.6.1.2.1.80.1.3.1.4.0: 2485256176
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.80.1.3.1.9.0: 0
.1.3.6.1.2.1.80.1.3.1.5.0: 1208611943
.1.3.6.1.2.1.80.1.3.1.10.0:
.1.3.6.1.2.1.80.1.3.1.6.0: 941686800
.1.3.6.1.2.1.80.1.3.1.7.0: 1208902023
.1.3.6.1.2.1.80.1.3.1.3.0: 8a

31.76.4 Field descriptions

Table 73: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.76.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.76.6 Additional information

This alarm requires no additional information.

31.77 Alarm (PP386)

traceRoutePathChange, Trap OID is 1.3.6.1.2.1.81.0.1.0

31.77.1 Explanation

The PP386 alarm signifies that the path to a target has changed.

31.77.2 Action

Please refer to ERS8600 Fault Management document.

31.77.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.77.3.1 Format

31.77.3.2 NTSTD

zsups3f8 PP386 OCT26 01:28:50 0141 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: The path to a target has changed
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: The path to a target has changed
Description: The path to a target has changed: (TargetAddress = 47.154.182.56)
.1.3.6.1.2.1.81.1.3.1.4.0: unknown
.1.3.6.1.2.1.81.1.2.1.3.0: unknown
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.81.0.1.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.81.1.3.1.5.0: 0.0.0.0

31.77.4 Field descriptions

Table 74: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.77.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.77.6 Additional information

This alarm requires no additional information.

31.78 Alarm (PP387)

traceRouteTestFailed, Trap OID is 1.3.6.1.2.1.81.0.2.0

31.78.1 Explanation

The PP387 alarm signifies that the system could not determine the path to a target.

31.78.2 Action

Please refer to ERS8600 Fault Management document.

31.78.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.78.3.1 Format

31.78.3.2 NTSTD

zsups3f8 PP387 OCT26 01:28:50 0143 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Could not determine the path to a target
Time: Oct 26 01:28:50 2005

Component ID: ERS8600=47.142.106.1
Specific Problem: Could not determine the path to a target
Description: Could not determine the path to a target: (TargetAddress = 47.154.182.56)
.1.3.6.1.2.1.81.1.3.1.4.0: unknown
.1.3.6.1.2.1.81.1.2.1.3.0: unknown
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.81.0.2.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.81.1.3.1.5.0: 0.0.0.0

31.78.4 Field descriptions

Table 75: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.78.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.78.6 Additional information

This alarm requires no additional information.

31.79 Alarm (PP388)

traceRouteTestComplete, Trap OID is 1.3.6.1.2.1.81.0.3.0

31.79.1 Explanation

The PP388 alarm signifies that the path to a target has just been determined.

31.79.2 Action

Please refer to ERS8600 Fault Management document.

31.79.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.79.3.1 Format

31.79.3.2 NTSTD

```
zsups3f8       PP388 OCT26 01:28:50 0145 INFO PP Fault
     Location: ERS8600_RTP;47.142.106.1
     State: None
     Category: communications
     Cause: The path to a target has just been determined.
     Time: Oct 26 01:28:50 2005
     Component ID: ERS8600=47.142.106.1
     Specific Problem: The path to a target has just been determined.
    Description: The path to a target has just been determined: (TargetAddress
     = 47.154.182.56)
     .1.3.6.1.2.1.81.1.3.1.4.0: unknown
     .1.3.6.1.2.1.81.1.2.1.3.0: unknown
     .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.81.0.3.0
     .1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
     .1.3.6.1.2.1.81.1.3.1.5.0: 0.0.0.0
```

31.79.4 Field descriptions

Table 76: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.79.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.79.6 Additional information

This alarm requires no additional information.

31.80 Alarm (PP389)

UDPEapSessionEndTrap, Trap OID is 1.3.6.1.4.1.562.42.5.1.3.2.2

31.80.1 Explanation

The PP389 alarm signifies that the UDPEap session has ended.

31.80.2 Action

Please refer to ERS8600 Fault Management document.

31.80.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.80.3.1 Format

31.80.3.2 NTSTD

zsups3f8 PP389 OCT26 01:28:50 0149 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: other
Cause: Session end trap
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Session end trap
Description: UDPEapSession end trap
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.562.42.5.1.3.2.2
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.4.1.562.42.5.1.3.1.1.9: 0
.1.3.6.1.4.1.562.42.5.1.3.1.1.8: 0
.1.3.6.1.4.1.562.42.5.1.3.1.1.7: 0
.1.3.6.1.4.1.562.42.5.1.3.1.1.4:
.1.3.6.1.4.1.562.42.5.1.3.1.1.3:
.1.3.6.1.4.1.562.42.5.1.3.1.1.2:
.1.3.6.1.4.1.562.42.5.1.3.1.1.1: 0

31.80.4 Field descriptions

Table 77: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.80.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.80.6 Additional information

This alarm requires no additional information.

31.81 Alarm (PP390)

UDPEapSessionStartTrap, Trap OID is 1.3.6.1.4.1.562.42.5.1.3.2.1

31.81.1 Explanation

The PP390 alarm signifies that the UDPEap session has started.

31.81.2 Action

Please refer to ERS8600 Fault Management document.

31.81.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.81.3.1 Format

31.81.3.2 NTSTD

zsups3f8 PP390 OCT26 01:28:50 0147 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: other
Cause: Session start trap
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Session start trap
Description: UDPEapSession start trap
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.562.42.5.1.3.2.1
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.4.1.562.42.5.1.3.1.1.7: 0
.1.3.6.1.4.1.562.42.5.1.3.1.1.6:
.1.3.6.1.4.1.562.42.5.1.3.1.1.5:
.1.3.6.1.4.1.562.42.5.1.3.1.1.10: 0
.1.3.6.1.4.1.562.42.5.1.3.1.1.4:
.1.3.6.1.4.1.562.42.5.1.3.1.1.3:
.1.3.6.1.4.1.562.42.5.1.3.1.1.2:
.1.3.6.1.4.1.562.42.5.1.3.1.1.1: 0

31.81.4 Field descriptions

Table 78: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.81.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.81.6 Additional information

This alarm requires no additional information.

31.82 Alarm (PP391)

rcnDuplicateIpAddress, Trap OID is 1.3.6.1.4.1.2272.1.21.0.63

31.82.1 Explanation

The PP391 alarm signifies that a duplicate IP address is detected on the subnet.

31.82.2 Action

Please refer to ERS8600 Fault Management document.

31.82.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.82.3.1 Format

31.82.3.2 NTSTD

zsups3f8 *** PP391 OCT26 01:28:50 0159 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: communications
Cause: More than one host with the same IP address have been detected on a subnet.
Time: Oct 26 01:28:50 2005

Component ID: ERS8600=47.142.106.1
Specific Problem: Duplicate IP address detected on the subnet.
Description: Duplicate IP address detected on subnet:
NetAddress=47.154.182.56 (PhysicalAddress= 00-08-74-F0-3C-EC)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.63
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.82.4 Field descriptions

Table 79: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

31.82.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.82.6 Additional information

This alarm requires no additional information.

31.83 Alarm (PP392)

rcnLoopDetectPortDown, Trap OID is 1.3.6.1.4.1.2272.1.21.0.64

31.83.1 Explanation

The PP392 alarm signifies that a loop has been detected on a port and the port is going to shut down.

31.83.2 Action

Please refer to ERS8600 Fault Management document.

31.83.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

31.83.3.1 Format

31.83.3.2 NTSTD

zsups3f8 *** PP392 OCT26 01:28:50 0161 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: communications
Cause: A network configuration error is creating a loop between ports in a vlan
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; portIndex=1
Specific Problem: Loop detected on a port and port is going to shut down
Description: Loop detected on port: PortIndex=1 (AdminStatus=up OperStatus=down)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.64
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

31.83.4 Field descriptions

Table 80: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, portIndex and node ID of the device.
AdminStatus	character string	Can be one of {up (1), down (2), testing (3)}
OperationStatus	character string	Can be one of {up (1), down (2), testing (3), unknown (4), dormant (5)}

31.83.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

31.83.6 Additional information

This alarm requires no additional information.

Configuration Management List (CNs)

Introduction

This chapter describes impacts to configuration management, such as hardware/software requirements, data schemas, and service orders for the features planned for this release. Only those features with configuration-management impacts are listed.

Featid	Title
A00007217	ITRANS Media Proxy Selection
A00007544.AB06	NCAS Link and SIP NMS Support based on RFC 3842
A00007547.AB12	SIP Lines Core Call Processing Support
A00007814.V3	REX testing for MG9000 (Media Gateway 9000) from Element Manager
A00008090.AA14	SBA: Alternate Scheduled Closure of Billing Files
A00008522	SESM Support for SIP Lines
A00008601.AA03	IW-SPM-IP Fully Provisionable Codec Lists for G.711/G.729
A00008629.AA08	GEM-II AAL2 IW-SPM SN09 Core Preparation Work
A00009011.AA02	TOPS Internet Protocol (IP) Security Enhancements
A00009012.AA10	TOPS OSSAIN Service Enhancements
A00009013.AA09	TOPS announcements via UAS/AMS
A00009036.AA07	Table HOMELRN Option SITE Expansion
A00009078.AA11	ICM Dual CTI
A00009085.AA06	ACD & ICM Capacity Expansion

A00009091.AA33	Equal Access (EA) LPIC Privilege Routing
A00009129.AA11	Controlled Hot Swact
A00009189	SESM Support for 64 Character FQDN
A00009190.AA23	Universal Carrier Protocol (UCP) C7UPTMR Enhancements
A00009200.AA14	Packet Trunking Trunk Test: Milli-watt Tone Swap
A00009207.AA05	DPT Trunk Testing Support
A00009218	MG9K Data Audit Robustness
A00009227	NPM Robustness
A00009235.AA09	TLS for SIP
A00009280.V3	MG9K Line Circuit Enhancements
A00009282	Emergency Stand Alone (ESA) Multiple Level Precedence and Preemption (MLPP) for MG9KEM
A00009339.AA16	Packet Cable T.38 Support
A00009375 & 9376	CICM Third-party Corrective Content Patching & CICM Selective Binary Component Patching
A00009463.AA08	CBM to Support Centralized User Authentication with IEMS
A00009470.AA09	SDM to support Security Assertion Markup Language (SAML) NSSwitch client
A00009520	Trunk blocking tools for MG4K and GWC on SN09
A00009532	Support host to host tunnels for all northbound OSS connections
A00009576.AC04	H.323 RASLess Provisioning
A00009611	IEMS Keymile Integration
A00009655	BladeCenter-T RTP Media Portal
A00009822	General Security Log When the User Logs Out
A00009839	Ability to apply patches during ESUP upgrade
A00009840	CBM IPSec Northbound Interface

A00009890	Provisioning for Media Proxy insertion for SIP lines
A00010303	Map Level Service Control Application Programming Interface
A00010742	GWC EM Enhancements to Support SIREN
A00010880	ABI SMU Support
A00011167	MG9KEM Central Userid and Password Support
A00011281	MS2000 IPSec Configuration via IEMS
A00011827.AB14	GWC Autonomous SWACT
A00012001.V5	IEMS Call Server 2000 SIP Integration
A00012183	Public Key Manager
A00012198.V2	GLC12 Coin Card Support from EM
A00012199	MG9K EM CPR Robustness
A00012215	Global Line Card Field Programmable Gate Array
A00012223, A00012217, A00012225	SESM Support for SIP Lines, Part 2
A00012526.AA12	TDM Call Recording Feature
A00012527.AA21	Provisioning of CS2K trunks on GW and Carrier basis
A00012570	Disabling Non-secure Network Services in SSPFS
A00012889	Passphrase Protected Keys for SSH

1: Configuration (CN): A00007217

1.1 Feature Name

ITRANS Media Proxy Selection

1.2 Initial Configuration

N/A

1.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

1.4 Upgrade Considerations

There are two sets of upgrade consideration. Upgrade of a GWC to SN09 and the upgrade of the CS2000 Management Tool Element manager to SN09.

For the CS2000 MT the impact is as follows:

On an upgrade of the CS2000MT to SN09, Media Proxies already provisioned on a GWC (as GWC Media Proxies) will remain as GWC default media proxies, whether or not the GWC is upgraded to SN09. If a GWC has been upgraded to SN09, The GWC media proxies will be sent to the GWC with an additional field indicating that they are GWC media Proxies.

The Media Proxies already on the system can be used after upgrade to create Media Proxy Groups regardless of whether they have been allocated to a GWC as a GWC Media Proxy.

One effect of an upgrade of the CS2000MT to SN09 will be to change the ID of all Media Proxies to use the new global ID structure. The Global ID is a unique ID across call servers representing a Network element. Each type of network element (eg Media Proxy) is allocated a set range of available IDs. The upgrade will convert the ID of any existing Media Proxies and Network Zones to the new format. New VPNs that are added will also use the new global ID format.

On the CS2000 MT User interface, the result of the upgrade will be to display the new gui panels for Media Proxy Groups and associated actions.

Upgrades of the CS2000MT from SN07 and SN08 to SN09 will be supported.

For a GWC upgrade the impact is as follows:

Once the CS2000 MT has been upgraded, the user can then begin to provision MP Groups and associate them with Network Zones (in order that the media Proxy Groups be used during call processing) as appropriate. However these changes will only be added to GWCs that are at SN09. GWCs with older loads will not be sent the Media Proxy Group or VPN data.

If a GWC is upgraded to SN09 on a newly upgraded SN09 CS2000MT, the Itrans NAT and LBL Network Zones will be sent to the GWC(s) with a "none" or "0" value for the Media Proxy group and VPN fields.

The upgrade should not have any additional impact on call processing.

SN07 and SN08 based GWCs will not support the Media Proxy Group and VPN functionality.

1.4.1 Dump and Restore (CM)

1.4.2 Element Management Upgrade

1.4.3 Downgrade impact

If the upgrade of a GWC to SN09 is aborted, the Media Proxy Group and VPN data will be removed from the GWC and all Media Proxies will revert back to being GWC default Media Proxies only.

1.5 Data schema (DS) (CM, MIBS, RDB)

1.5.1 MIB Interface

The mib is used to communicate provisioning information to the GWC. The design of the mib takes into account restrictions imposed by GWC architecture and SESM architecture.

This section describes the changes that will be made to the Mibs in order to enable the feature functionality. The Mibs that will be changed are the GWC-MIDDLE-BOX-MIB and the GWC-MEDIA-PROXY-MIB.

1.5.1.1 GWC-MIDDLE-BOX-MIB

GWC-MIDDLE-BOX-MIB adds two new fields:

- The **MiddleBoxMPGroupId** field is used to identify the preferred MediaProxyGroup for the middle box. The value of this field is used to index into the MediaProxyGroup table on the GWC. A GWC can have a maximum of 8 groups and there may be up to 512 MP groups in the system. The design component determines what range the above field can take in the mib.
- The **MiddleBoxVpnGID** field represents a global Identifier indicating the VPN that the MiddleBox is part of (applies to NATs only). If this field is set to 0, it means that the NAT does not belong to any provisioned or shared VPN.

MIB Definition

```
-- DMS Call Server GateWay Controller Middle Box Table Data MIB


GWC-MIDDLE-BOX-MIB DEFINITIONS ::= BEGIN
    IMPORTS
       OBJECT-TYPE, MODULE-IDENTITY, enterprises, IpAddress, Integer32
            FROM SNMPv2-SMI
        DisplayString, RowStatus
            FROM SNMPv2-TC
        GWCDeviceType, GWCDeviceProtocol, GWCDeviceProtVersion
            FROM NORTEL-GWC-COMMON-TC;


--
-- Define the location of this MIB within the MIB tree
--

nortel    OBJECT IDENTIFIER ::= { enterprises 562 }
voip      OBJECT IDENTIFIER ::= { nortel 28 }
ptn             OBJECT IDENTIFIER ::= { voip 0 }
serviceControlOBJECT IDENTIFIER ::= { ptn 1 }
legacyCallServerOBJECT IDENTIFIER ::= { serviceControl 4 }
lcsGateWayController OBJECT IDENTIFIER ::= { legacyCallServer 1 }

--
-- Define the elements in the GWC Middle Box Table Data MIB
--

gwcMiddleBoxTblMIB MODULE-IDENTITY
      LAST-UPDATED "200209240000Z"   -- 24th September 2002
      ORGANIZATION "Nortel DMS Call Server"
      CONTACT-INFO "Eman Jado-Adham
           Nortel Networks Inc.
                    1285 Baseline Road
                    Ottawa, Canada
                    Phone: (613) 763-3089
                    email: emanjado@nortelnetworks.com"
      DESCRIPTION  "The MIB module defines information about
           the Middle Box table(s) provision supported
                    by the GateWay Controller (GWC)."

      REVISION     "200209240000Z"
      DESCRIPTION  "add new fields for Internet Transparency
                    functionality (CAC, NAT traversal)"

      REVISION     "200409080000Z"
      DESCRIPTION  "Add new PORT field for support of ALG\par
                    Middle box"
```

```
      REVISION     "200411010000Z"
      DESCRIPTION  "Correct the MiddleBox GID to expand the
                    range greater than 65535.  This is required
                    for the larger ids that can result with the
                    CallAgent Id being set."

  ::= { lcsGateWayController 18 }

middleBoxTable OBJECT-TYPE
    SYNTAX SEQUENCE OF MiddleBoxEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
       "This table contains Middle Box data.
        The number of entries in this table
        depends on the type of the Middle Box
        for this GWC."
    ::= { gwcMiddleBoxTblMIB 1 }

--
-- Define the row objects in the table middleBoxTable
--

middleBoxEntry OBJECT-TYPE
    SYNTAX MiddleBoxEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "An entry describes the characteristics of the
         Middle Box, e.g. Policy Enforcement Point (PEP),
              needed for setting up calls with DQoS or Admission
              Control quality, .... ."
      INDEX { middleBoxGID }
    ::= { middleBoxTable 1 }

-- Define the fields

MiddleBoxEntry ::= SEQUENCE {
    middleBoxGID           Integer32,
    middleBoxName          DisplayString (SIZE(1..32)),
    middleBoxAddress       IpAddress,
    middleBoxType          GWCDeviceType,
    middleBoxStatus         INTEGER,
    middleBoxEntryStatus    RowStatus,
    middleBoxProtocol       GWCDeviceProtocol,
    middleBoxProtVers       GWCDeviceProtVersion,
    middleBoxCacType        INTEGER,
    middleBoxRUfactor       Integer32(0..255),
    middleBoxMaxCount       Integer32,
    middleBoxNatType        INTEGER,
    middleBoxParentMB       Integer32,
    middleBoxPort           Integer32(0..65535),
    middleBoxMPGroupId      Integer32(0..512),
    middleBoxVPNGID         Integer32
     }

middleBoxGID OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Middle Box Global Identifier."
    ::= { middleBoxEntry 1 }

middleBoxName OBJECT-TYPE
    SYNTAX DisplayString (SIZE(1..32))
    MAX-ACCESS read-create
```

```
    STATUS current
    DESCRIPTION
        "String that identifies FQDN of theMiddle Box."
    ::= { middleBoxEntry 2 }

middleBoxAddress OBJECT-TYPE
        SYNTAX IpAddress
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
            "IP Address of the Middle Box."
        DEFVAL { '00000000'h }
        ::= { middleBoxEntry 3 }

middleBoxType OBJECT-TYPE
    SYNTAX GWCDeviceType
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Type of device in the GWC defined in GWC-TC."
    ::= { middleBoxEntry 4 }

middleBoxStatus OBJECT-TYPE
    SYNTAX INTEGER { unintialized (0),
                         connecting   (1),
                         connected    (2),
                         initializing (3),
                         initalized   (4),
                         deleting     (5) }
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Status of Middle Box."
    ::= { middleBoxEntry 5 }

middleBoxEntryStatus  OBJECT-TYPE
    SYNTAXRowStatus
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Status column for row entry."
    ::= { middleBoxEntry 6 }

middleBoxProtocol OBJECT-TYPE
        SYNTAX GWCDeviceProtocol
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
            "Comms protocol supported by the middlebox.
             This enumerated list matches the list of supported
             protocols as defined in the GWC."
        DEFVAL { 0 }
        ::= { middleBoxEntry 7 }

middleBoxProtVers OBJECT-TYPE
        SYNTAX GWCDeviceProtVersion
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
       "Version of the comms protocol supported
        by the middlebox."
        DEFVAL { "0.0" }
        ::= { middleBoxEntry 8 }

middleBoxCacType OBJECT-TYPE
    SYNTAX INTEGER { none         (0),
                         internal     (1) }
    MAX-ACCESS read-create
```

```
    STATUS current
    DESCRIPTION
        "Type of Connection Admissions Control (CAC)
         for a given middlebox. Internal indicates that
         the GWC must provide a virtual CAC function."
         DEFVAL { 0 }
    ::= { middleBoxEntry 9 }

middleBoxRUfactor OBJECT-TYPE
    SYNTAX Integer32(0..255)
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Resource Usage factor, used in carrying out
         virtual CAC."
         DEFVAL { 0 }
    ::= { middleBoxEntry 10 }

middleBoxMaxCount OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Max resource value for a link on which virtual
         CAC will be performed."
         DEFVAL { 0 }
    ::= { middleBoxEntry 11 }

middleBoxNatType OBJECT-TYPE
    SYNTAX INTEGER { none            (0),
                     noncontrolled   (1) }
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "NAT capability of a given middlebox.
         non_controlled indicates that NAT is present
         but that we don't control it directly,
         therefore need to resort to other means"
         DEFVAL { 0 }
    ::= { middleBoxEntry 12 }

middleBoxParentMB OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "GID of next middlebox between this one and the
         the network core."
         DEFVAL { 0 }
    ::= { middleBoxEntry 13 }

middleBoxPort OBJECT-TYPE
        SYNTAX Integer32
        MAX-ACCESS  read-create
        STATUS current
        DESCRIPTION
            "ALG Middle Box UDP Port Number used by GWC
         to communicate to ALG."
        DEFVAL { 0 }
        ::= { middleBoxEntry 14 }


middleBoxMPGroupId OBJECT-TYPE
    SYNTAX Integer32(0..512)
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
```

```
       "ID of MPG group that is associated with this middlebox. 0
indicate
        no MPG is assigned."
        DEFVAL { 0 }
   ::= { middleBoxEntry 15 }

middleBoxVPNGID OBJECT-TYPE
        SYNTAX Integer32(0..64)
        MAX-ACCESS  read-create
        STATUS current
        DESCRIPTION
            "GID to indicate which VPN a NAT is part of. Used when
multiple
            NATs are in a single VPN. 0 indicates this NAT is the only
             NAT in this VPN"
        DEFVAL { 0 }
        ::= { middleBoxEntry 16 }

middleBoxLastOperationErrorMessage OBJECT-TYPE
        SYNTAX DisplayString (SIZE(1..128))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
           "Error Message holds a descriptive error message
            in case of an snmp failure of the last operation."
        ::= { gwcMiddleBoxTblMIB 2 }

middleBoxLastOperationErrorType OBJECT-TYPE
    SYNTAX INTEGER { information    (0),
                     warning        (1),
                     error          (2) }
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
           "This value contains the type of error that occurred on
           the last SET failure on any variable in a middleBox table.
             The combination of this type and the error message give
             the manager enough information to process the failure."
        ::= { gwcMiddleBoxTblMIB 3 }

END
```

1.5.1.2 GWC-MEDIA-PROXY-MIB

GWC-MEDIA-PROXY-MIB adds two new fields.

MediaProxyInGWCGroup is used to indicate whether or not the Media proxy has been provisioned as a media Proxy on the GWC. This field can be set to Y or N. A value of Y indicates that the Media Proxy belongs to the group of default media Proxies on the GWC (it may or may not be in one or more MP groups as well). A value of N means that the Media Proxy is not part of the group of default media Proxies but that it must be in at least one MP group because it is present on the GWC.Service Orders (SO) (CM & SESM).

MediaProxyGlobalID This fields represents a unique global ID for a specific MediaProxy within the system.

There is also a new table added to the GWC-MEDIA-PROXY-MIB. This is a new table to convey MediaProxy Group Data to the GWC. The new structure is defined as follows:

mediaProxyGroupTable - table containing data on MediaProxyGroups. Each Entry in the table consists of a sequence of the following sets of fields:
mediaProxyGroupID - The global id of the Media Proxy Group.
mediaProxyID - The global id that identifies a Media Proxy in the Media Proxy Group.

mediaProxyGroupEntryStatus - the entry status of the row.

The table has been designed to accommodate any number of media proxies in a group, however, the number of media proxies in a group in SN09 is restricted to a maximum of 5.

MIB Definition

```
-- DMS Call Server GateWay Controller Media Proxy MIB


GWC-MEDIA-PROXY-MIB DEFINITIONS ::= BEGIN
    IMPORTS
       OBJECT-TYPE, MODULE-IDENTITY, enterprises, IpAddress, Integer32
            FROM SNMPv2-SMI
        RowStatus, DisplayString
            FROM SNMPv2-TC
        GWCDeviceProtocol, GWCDeviceProtVersion
            FROM NORTEL-GWC-COMMON-TC;

--
-- Define the location of this MIB within the MIB tree
--

nortel    OBJECT IDENTIFIER ::= { enterprises 562 }
voip      OBJECT IDENTIFIER ::= { nortel 28 }
ptn             OBJECT IDENTIFIER ::= { voip 0 }
serviceControlOBJECT IDENTIFIER ::= { ptn 1 }
legacyCallServerOBJECT IDENTIFIER ::= { serviceControl 4 }
lcsGateWayController OBJECT IDENTIFIER ::= { legacyCallServer 1 }

--
-- Define the elements in the GWC Media Proxy MIB
--

gwcMediaProxyMIB MODULE-IDENTITY
      LAST-UPDATED "200210220000Z"   -- 22nd October 2002
      ORGANIZATION "Nortel DMS Call Server"
      CONTACT-INFO "Mike Fryars
           Nortel Networks UK Limited
                    Maidenhead Office Park, Westacott Way
                    Maidenhead, Berks, SL6 3QH
                    United Kingdom
                    Phone: +44 (0)1628 431603
                    email: mfryars@nortelnetworks.com"
      DESCRIPTION  "The MIB module defines information about
           Media Proxy Devices."

  ::= { lcsGateWayController 23 }


mediaProxyTable OBJECT-TYPE
   SYNTAX SEQUENCE OF MediaProxyEntry
   MAX-ACCESS not-accessible
```

```
    STATUS current
    DESCRIPTION
       "Table containing data on Media Proxy devices."
    ::= { gwcMediaProxyMIB 1 }

--
-- Define the row objects in the table middleboxRsrcUsageTable
--

mediaProxyEntry OBJECT-TYPE
    SYNTAX MediaProxyEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table entry containing data on a particular Media
              Proxy device."
      INDEX { mediaProxyName }
    ::= { mediaProxyTable 1 }

-- Define the fields

MediaProxyEntry ::= SEQUENCE {
    mediaProxyName         DisplayString (SIZE(1..32)),
    mediaProxyAddress      IpAddress,
    mediaProxyProtocol     GWCDeviceProtocol,
    mediaProxyProtVersion  GWCDeviceProtVersion,
    mediaProxyEntryStatus  RowStatus,
    mediaProxyInGWCGroup   DisplayString (SIZE (1)),
    mediaProxyGlobalID     Integer32
    }


mediaProxyName OBJECT-TYPE
    SYNTAX DisplayString (SIZE(1..32))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "String that identifies the Media Proxy."
    ::= { mediaProxyEntry 1 }

mediaProxyAddress OBJECT-TYPE
        SYNTAX IpAddress
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
            "IP Address of the Media Proxy."
        DEFVAL { '00000000'h }
        ::= { mediaProxyEntry 2 }

mediaProxyProtocol OBJECT-TYPE
    SYNTAX GWCDeviceProtocol
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
            "Comms protocol supported by the Media Proxy.
             This enumerated list matches the list of supported
             protocols as defined in the GWC."
    ::= { mediaProxyEntry 3 }

mediaProxyProtVersion OBJECT-TYPE
    SYNTAX GWCDeviceProtVersion
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Version of the comms protocol supported
         by the Media Proxy."
    ::= { mediaProxyEntry 4 }
```

```
mediaProxyEntryStatus  OBJECT-TYPE
    SYNTAXRowStatus
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Status column for row entry."
    ::= { mediaProxyEntry 5 }

mediaProxyInGWCGroup  OBJECT-TYPE
    SYNTAX DisplayString (SIZE (1))
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
       "A character indicating if this MP is part of the GWC's default
list. Y if it is in the list N if not."
    ::= { mediaProxyEntry 6 }

mediaProxyGlobalID  OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "A unique ID within the system identifying a specific MP."
    ::= { mediaProxyEntry 7 }


mediaProxyLastOperationErrorMessage OBJECT-TYPE
        SYNTAX DisplayString (SIZE(1..128))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
           "Error Message holds a descriptive error message
            in case of an snmp failure of the last operation."
        ::= { gwcMediaProxyMIB 2 }

mediaProxyLastOperationErrorType OBJECT-TYPE
    SYNTAX INTEGER { information    (0),
                     warning        (1),
                     error          (2) }
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
           "This value contains the type of error that occurred on
             the last SET failure on any variable in the resource
            usage table. The combination of this type and the error
             message give the manager enough information to process
             the failure."

        ::= { gwcMediaProxyMIB 3 }

mediaProxyGroupTable OBJECT-TYPE
    SYNTAX SEQUENCE OF MediaProxyGroupEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
       "Table containing data on Media Proxy Groups."
    ::= { gwcMediaProxyMIB 4 }

mediaProxyGroupEntry OBJECT-TYPE
    SYNTAX MediaProxyGroupEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table entry containing data on a particular MediaProxy
group"
    INDEX { mediaProxyGroupID}
    ::= { mediaProxyGroupTable 1 }
```

```
-- Define the fields

MediaProxyGroupEntry ::= SEQUENCE {
      mediaProxyGroupID      Integer32 (0..512),
      mediaProxyID1      Integer32 ,
      mediaProxyID2      Integer32 ,
      mediaProxyID3      Integer32 ,
      mediaProxyID4      Integer32 ,
      mediaProxyID5      Integer32 ,
      mediaProxyID6      Integer32 ,
      mediaProxyID7      Integer32 ,
      mediaProxyID8      Integer32 ,
      mediaProxyID9      Integer32 ,
      mediaProxyID10     Integer32 ,
      mediaProxyGroupEntryStatus      RowStatus
   }

mediaProxyGroupID OBJECT-TYPE
   SYNTAX Integer32 (0..512)
   MAX-ACCESS read-create
   STATUS current
   DESCRIPTION
       "Media Proxy Group ID."
        DEFVAL { 0 }
   ::= { mediaProxyGroupEntry 1 }

mediaProxyID1 OBJECT-TYPE
   SYNTAX Integer32
   MAX-ACCESS read-create
   STATUS current
   DESCRIPTION
      "ID that identifies the Media Proxy. 0 indicate no Media Proxy."
       DEFVAL { 0 }
   ::= { mediaProxyGroupEntry 2 }

mediaProxyID2 OBJECT-TYPE
   SYNTAX Integer32
   MAX-ACCESS read-create
   STATUS current
   DESCRIPTION
      "ID that identifies the Media Proxy. 0 indicate no Media Proxy."
       DEFVAL { 0 }
   ::= { mediaProxyGroupEntry 3 }

mediaProxyID3 OBJECT-TYPE
   SYNTAX Integer32
   MAX-ACCESS read-create
   STATUS current
   DESCRIPTION
      "ID that identifies the Media Proxy. 0 indicate no Media Proxy."
       DEFVAL { 0 }
   ::= { mediaProxyGroupEntry 4 }

mediaProxyID4 OBJECT-TYPE
   SYNTAX Integer32
   MAX-ACCESS read-create
   STATUS current
   DESCRIPTION
      "ID that identifies the Media Proxy. 0 indicate no Media Proxy."
   DEFVAL { 0 }
   ::= { mediaProxyGroupEntry 5 }

mediaProxyID5 OBJECT-TYPE
   SYNTAX Integer32
   MAX-ACCESS read-create
   STATUS current
   DESCRIPTION
      "ID that identifies the Media Proxy. 0 indicate no Media Proxy."
```

```
    DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 6 }

-- mediaProxyIDs 6-10 are reserved for furture expansion in SN09 the
-- customer will only be allowed to provision 5 MediaProxies per group.

mediaProxyID6 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Reserved for future expansion"
         DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 7 }

mediaProxyID7 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Reserved for future expansion"
         DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 8 }

mediaProxyID8 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Reserved for future expansion"
       DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 9 }


mediaProxyID9 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Reserved for future expansion"
    DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 10 }

mediaProxyID10 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Reserved for future expansion"
       DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 11 }

mediaProxyGroupEntryStatus  OBJECT-TYPE
    SYNTAXRowStatus
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Status column for row entry."
    ::= { mediaProxyGroupEntry 12 }

mediaProxyGroupLastOperationErrorMessage OBJECT-TYPE
    SYNTAX DisplayString (SIZE(1..128))
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
       "Error Message holds a descriptive error message
```

```
            in case of an snmp failure of the last operation."
        ::= { gwcMediaProxyMIB 5 }

    mediaProxyGroupLastOperationErrorType OBJECT-TYPE
        SYNTAX INTEGER { information    (0),
                warning    (1),
                error    (2) }
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
            "This value contains the type of error that occurred on
             the last SET failure on any variable in the resource
             usage table. The combination of this type and the error
             message give the manager enough information to process
             the failure."

        ::= { gwcMediaProxyMIB 6 }

END
```

1.6 Service Orders (SO) (CM & SESM)

N/A

1.7 Software optionality control (SOC)

N/A

1.8 Element Management

The GWC Element manager part of the CS2M Configuration Management Tools will be used to perform the configuration procedures for this component.

1.8.1 New/modified GUIs

All new and modified GUIs are part of the CS2M Configuration Management Tool GUI.

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Add Media Proxy Group dialog	New
Change Media Proxy Group Dialog	New
Media Proxies Tab	Changed
Media Proxies Details Dialog	New
Media Proxy Groups Tab	New
Media Proxy Group Details Dialog	New
Add Nat Dialog	Changed

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Add NAT/LBL Dialog	Changed
Nat Network Zone Panel	Changed
NAT/LBL Network Zone Panel	Changed
Change Nat Dialog	Changed
Change NAT/LBL Dialog	Changed
Zone Details	New
VPN Details	New
Zone GWCID Details	Changed
Zone GW Report Details	Changed
GWC Media Proxies Tab	Changed

1.8.1.1 GUI name:AddMPGroup

Add Media Proxy Group Dialog

1.8.1.1.1 Functional description

The purpose of this Dialog is to add a new Media Proxy group and add up to five Media Proxies to the group. Only previously provisioned Media Proxies can be added to a Media Proxy group. A Media Proxy can be added to more than one group.

There are a maximum of 512 Media Proxy Groups allowed in the system. A Media Proxy group may be selected from the left hand list and the “Add>>” button used to transfer it to the right hand list of selected media Proxies for the Group.

A Media Proxy group may be selected from the right hand list and the “<<Rem” button used to transfer it to the list of available Media Proxies on the left.

A name must be entered in the dialog box at the top. This should be a unique and meaningful name.

When an appropriate number of Media Proxies have been selected and the name filled in, the ok button can be selected.

1.8.1.1.2 GUI usage and implications

This gui is used to create a new group containing a subset of the Media Proxies on the system. The group can then be allocated to an ITRANs Middlebox and

in turn associated with a gateway. When this happens the GWC for the gateway is provisioned with details of the Media Proxies in the group.

A group must have been provisioned using this dialog before an ITRANs Middlebox can be associated with a group.

The Media Proxies must have been provisioned on the system prior to this GUI being invoked. If this is not the case then no Media Proxies will be available to be added to the group.

1.8.1.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
AddMPGroup	0	1	N/A

1.8.1.1.4 GUI fields

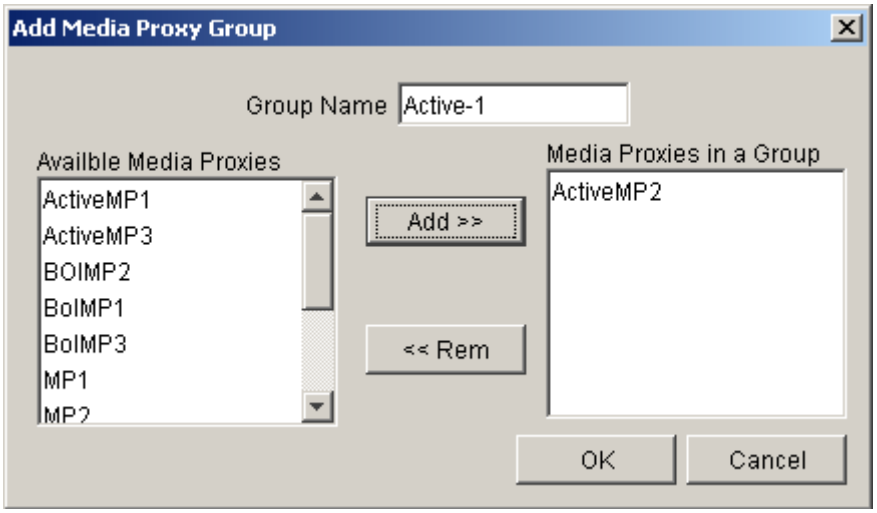
The following table lists fields for GUI AddMPGroup.Media Proxies must have been provisioned before the AddMPGroup dialog is invoked.

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Group Name	New	none	media proxy group name	This field holds the name of the media proxy group.	
Media Proxies	New	none	range of Media proxies	This displays the media proxies which can be added to the group	
Media Proxy Group	New	none	selected media proxies (max of 5)	This box shows the list of media proxies which have been selected for the group.	

1.8.1.1.5 Usage example

The following example shows sample datafill or menu selection for GUI AddMPGroup:



1.8.1.1.6 GUI release history update

This is a new GUI. First release.

1.8.1.1.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

1.8.1.1.8 Supplementary information

NONE

1.8.1.2 GUI name: ChangeMPGroup

Change Media Proxy Group Dialog

1.8.1.2.1 Functional description

The Change Media Proxy Group Dialog is a new Dialog to allow the alteration of the Media Proxies contained within a selected Media Proxy group. It is similar in appearance to the AddMPGroup Dialog.

A Media Proxy group may be selected from the left hand list and the “Add>>” button used to transfer it to the right hand list of selected Media Proxies for the Group.

A Media Proxy group may be selected from the right hand list and the “<<Rem” button used to transfer it to the list of available Media Proxies on the left.

The name of the group may not be changed.

1.8.1.2.2 GUI usage and implications

This Gui is to be used when any changes to the number of media proxies in the group are to be made (subject to the maximum limit). It is also to be used when one or more of the Media Proxies in the group is to be replaced with another.

Any additional Media Proxies must exist prior to this GUI being invoked. If this is not the case then no additional Media Proxies will be available to be added to the group. The addMediaProxy dialog enables Media Proxies to be added.

Media Proxies cannot be deleted from the system if they are in a Media Proxy group.

1.8.1.2.3 GUI size

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
ChangeMPGroup	0	1	N/A

1.8.1.2.4 GUI fields

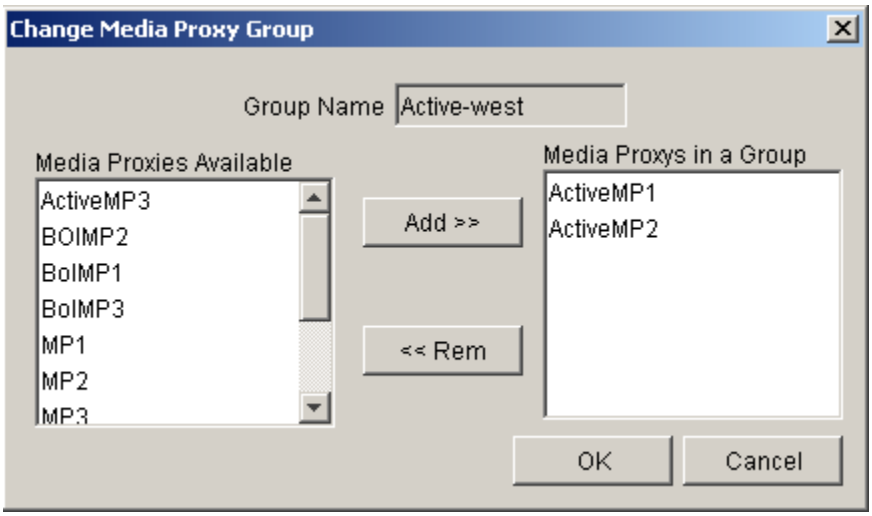
The following table lists fields for GUI ChangeMPGroup.Media Proxies must have been provisioned before the ChangeMPGroup dialog is invoked.

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Media Proxies	New	none	range of Media proxies	this displays the media proxies which can be added to the group	
Media Proxy Group	New	none	selected media proxies (max of 5)	This box shows the list of media proxies which have been selected for the group.	

1.8.1.2.5 Usage example

The following example shows sample datafill or menu selection for GUI ChangeMPGroup:



1.8.1.2.6 GUI release history update
New Dialog, first release.

1.8.1.2.7 Context sensitive launching information
This is launched using the CS2000 Management Tools interface

1.8.1.2.8 Supplementary information
NONE

1.8.1.3 GUI name: MPGroupTab
Media Proxy Groups Tab

1.8.1.3.1 Functional description
This tab is designed to show a list of Media Proxy Groups along with a comma separated list of the Media Proxies belonging to that group.

The tab also displays the following buttons:

Add - to add a new Media Proxy Group. When clicked this will launch the AddMPGroup Dialog described in section 12.8.2.3.

Delete - to delete a Media Proxy Group that has been selected from the list. When selected a dialog will ask for confirmation that the selected Media proxy group is to be deleted. This delete will fail if the Media Proxy Group is associated with any ITRANs Middleboxes that are on a GWC.

Change - to change the Media Proxies listed against a selected Media Proxy Group. When selected this will launch the ChangeMPGroup" Dialog described in section 12.8.2.4.

Properties - The properties button will launch the “Describe Media Proxy Group.”

1.8.1.3.2 GUI usage and implications

This GUI is used for display purposes and to provide a central point of access for all Media Proxy Group operations.

1.8.1.3.3 GUI size

Table 6 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
MPGTab	1	1	N/A

1.8.1.3.4 GUI fields

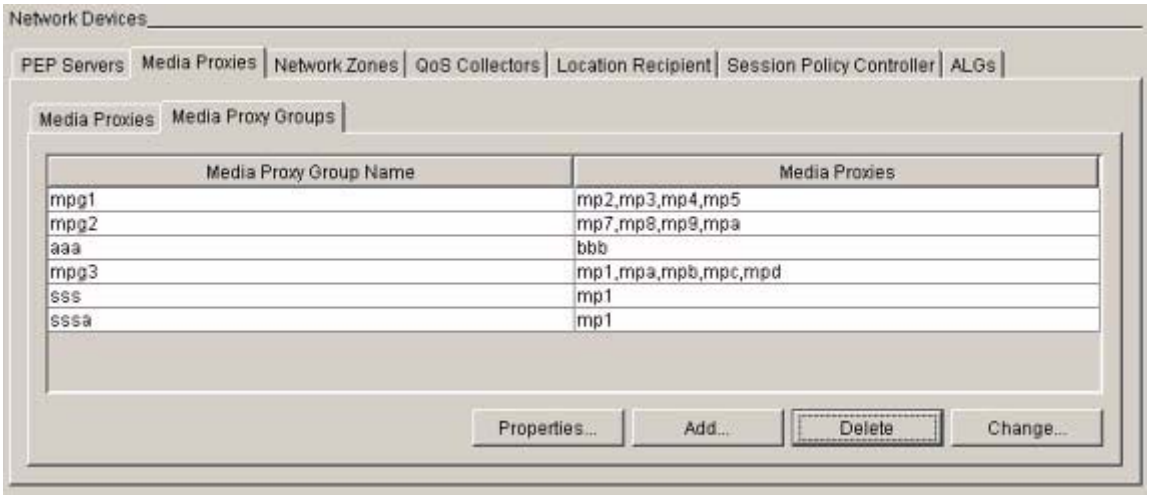
The following table lists fields for the MPGroup Tab

Table 7 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Media Proxy Group Name	New	none	values of media proxy groups	A column showing the list of media proxy groups	
Media Proxies	New	None	values of the selected media Proxies	a column showing a comma separated list of the media proxies which have been selected for the Group in column one.	

1.8.1.3.5 Usage example

The following example shows sample datafill or menu selection for GUI MPGroupTab:



1.8.1.3.6 GUI release history update
New Tabbed panel. First release

1.8.1.3.7 Context sensitive launching information
This is launched using the CS2000 Management Tools interface

1.8.1.3.8 Supplementary information
NONE

1.8.1.4 GUI name: MP Tab
Media Proxies Tab

1.8.1.4.1 Functional description
The Media Proxies tab has been modified to contain two sub-tabbed panels. The first sub tab will contain the content of the existing Media Proxy tabbed panel.

The second sub panel will contain the new Media Proxy Group tabbed panel.

The purpose of the Media Proxies tab is to make available information relating to the Media Proxies provisioned on the system. This tab is visible in the Network devices domain.

1.8.1.4.2 GUI usage and implications
This is the first gui to go to when viewing or performing operations involving system Media Proxies or Media Proxy Groups.

1.8.1.4.3 GUI size

Table 8 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
MPTab	1	1	N/A

1.8.1.4.4 GUI fields

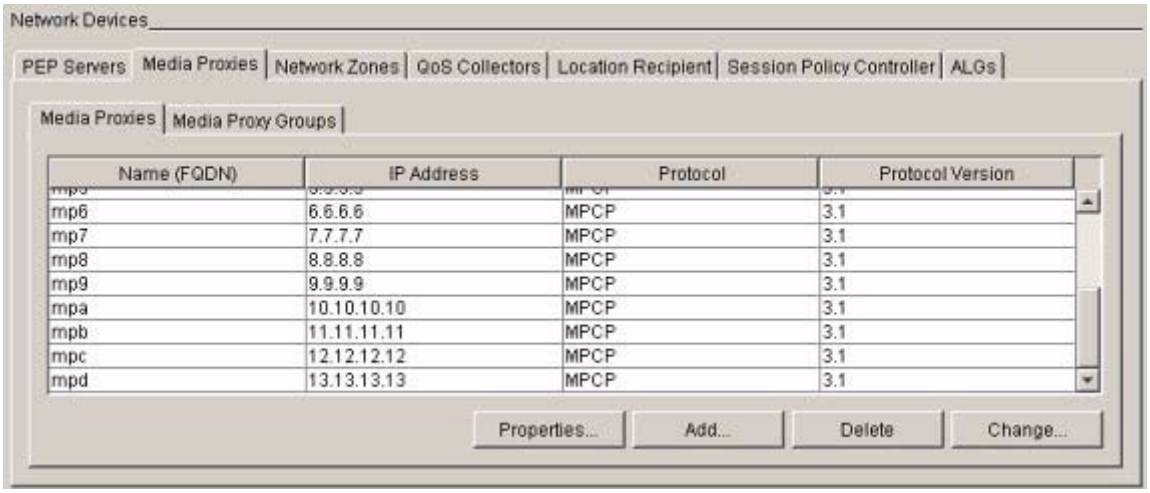
The following table lists fields for the MP tab.

Table 9 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

1.8.1.4.5 Usage example

The following example shows sample datafill or menu selection for GUI MP Tab:



1.8.1.4.6 GUI release history update

Two sub tabs have been added to this tabbed Panel. The first contains the original content of the tab and the second contains information about the Media Proxy Groups.

1.8.1.4.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

1.8.1.4.8 Supplementary information

NONE

1.8.1.5 GUI name: Media Proxy Description

Media Proxies Description Dialog

1.8.1.5.1 Functional description

The Media Proxy description dialog is there to provide handy information about what is using the Media Proxy.

The dialog will contain lists of all of the gateway controllers that are using the Media Proxy and the Media Proxy Groups that contain the selected Media Proxy.

The button that displays this dialog is available on the Media Proxy panel. A Media Proxy must be selected from the panel for the details to be shown.

1.8.1.5.2 GUI usage and implications

This GUI is used when the user wishes to find out more information on a specific Media Proxy group without having to navigate to the gateway controller GUI or the Media Proxy group GUI.

1.8.1.5.3 GUI size

Table 10 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Media Proxy Description Dialog	1	1	N/A

1.8.1.5.4 GUI fields

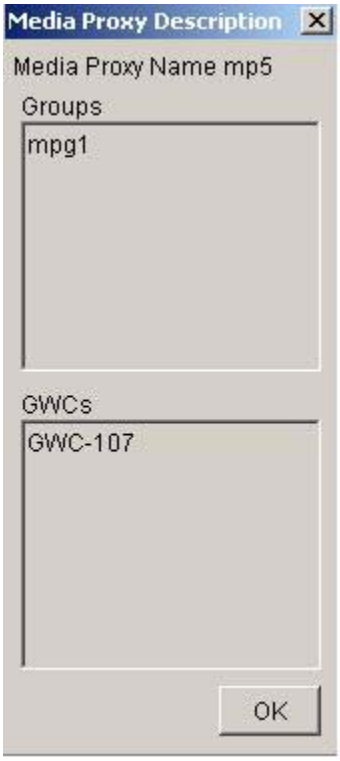
The following table lists fields for the MP tab.

Table 11 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

1.8.1.5.5 Usage example

The following example shows a sample Media Proxy that is used in two Media Proxy Groups:



1.8.1.5.6 GUI release history update

1.8.1.5.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

1.8.1.5.8 Supplementary information

NONE

1.8.1.6 GUI name: Media Proxy Groups Description

Media Proxy Groups Description

1.8.1.6.1 Functional description

The Media Proxy Group description dialog is there to provide handy information about what is using the Media Proxy Group.

The dialog will contain lists of all of the gateway controllers and the NATs that are using the Media Proxy Group.

The button that displays this dialog is available on the Media Proxy Group panel. A Media Proxy Group must be selected from the panel for the details to be shown.

1.8.1.6.2 GUI usage and implications

This GUI is used when the user wishes to find out more information on a specific Media Proxy Group without having to navigate to the gateway controller GUI or the Media Proxy GUI.

1.8.1.6.3 GUI size

Table 12 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Media Proxy Group Details Dialog	1	1	N/A

1.8.1.6.4 GUI fields

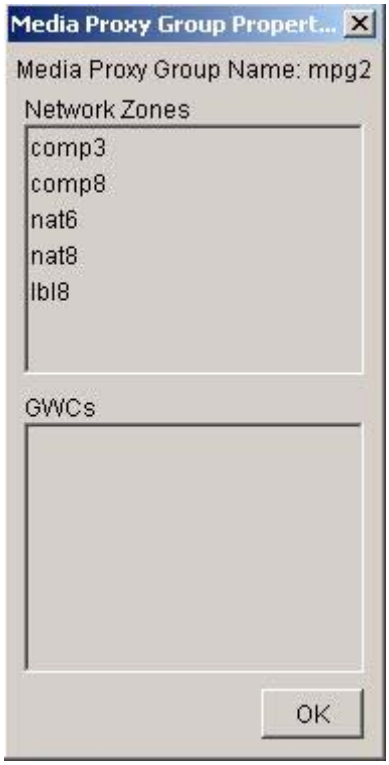
The following table lists fields for the MP tab.

Table 13 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

1.8.1.6.5 Usage example

The following example shows a sample Media Proxy Group that is used by a NAT and is present on a GWC.



1.8.1.6.6 GUI release history update
This is a new dialog.

1.8.1.6.7 Context sensitive launching information
This is launched using the CS2000 Management Tools interface

1.8.1.6.8 Supplementary information
NONE

1.8.1.7 GUI name: NAT Panel
NAT Panel

1.8.1.7.1 Functional description
Two new fields have been added to the list in the NAT Panel. The first displays any selected Media Proxy Group name and the second any chosen VPN name. Two new buttons have also been added to the panel. The first, called “VPN” is the link the VPN details dialog. This displays details of the VPNs.

The “details” button is the replacement for the buttons to display the zone ID and the gateway report.

1.8.1.7.2 GUI usage and implications

This GUI will now display Media Proxy Group and VPN names for NATs.

1.8.1.7.3 GUI size

Table 14 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
NATMiddlebox Panel	1	1	N/A

1.8.1.7.4 GUI fields

The following table lists fields for the MP tab.

Table 15 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Media Proxy Group	New			Displays the selected media proxy group.	?
VPN	New			Displays the selected VPN.	?

1.8.1.7.5 Usage example

The following example shows sample NAT and LBL Zones with Media Proxy Groups and/or a VPN :

1.8.1.7.6 GUI release history update
Two fields have been added to display the chosen Media Proxy Group and the chosen VPN.

Two buttons have been added - “ VPN” and “details”

1.8.1.7.7 Context sensitive launching information
This is launched using the CS2000 Management Tools interface

1.8.1.7.8 Supplementary information
NONE

1.8.1.8 GUI name: Add NAT
Add NAT Middlebox Dialog

1.8.1.8.1 Functional description
The add NAT dialog box has been modified to allow the selection of a Media Proxy Group and the option of adding a NAT to a VPN.

A new drop down box has been added which displays the list of the datafilled Media Proxy Groups. The default option is no Media Proxy Group.

The default display also includes a VPN check box. VPN information is only available if this tick box is selected. Selection of this box gives the user the choice of either selecting an existing VPN or creating a new one. Choosing the “create VPN” button will display a further dialog.

1.8.1.8.2 GUI usage and implications
This gui is used when a new NAT is created. It can also be used to create a new VPN.

1.8.1.8.3 GUI size

Table 16 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
AddNat	1	1	N/A

1.8.1.8.4 GUI fields
The following table lists fields for the MP tab.

Table 17 GUI field descriptions

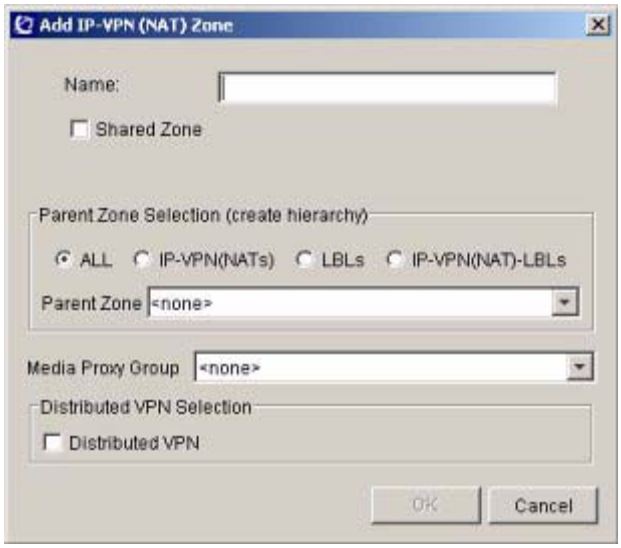
Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Media Proxy Group	New			To select a media proxy group	

Table 17 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
VPN	New			To select a VPN	

1.8.1.8.5 Usage example

The following example shows a new NAT being added which uses the London Media Proxy Group and is part of VPN1.



1.8.1.8.6 GUI release history update

The Media Proxy Group combo box has been added along with the Use VPN checkbox, VPN combo box and create vpn button.

1.8.1.8.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

1.8.1.8.8 Supplementary information

NONE

1.8.1.9 GUI name:Change NAT

Change NAT

1.8.1.9.1 Functional description

Please see Add NAT for details.

1.8.1.9.2 GUI usage and implications

Please see Add NAT for details.

1.8.1.9.3 GUI size

Table 18 New or modified GUIs

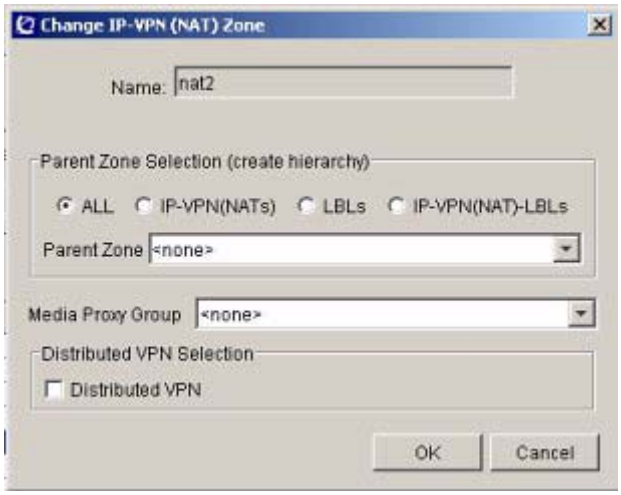
Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
ChangeNAT	1	1	N/A

1.8.1.9.4 GUI fields

Please see Add NAT for details.

1.8.1.9.5 Usage example

The following example shows a media proxy group and a VPN being added to an existing NAT.



1.8.1.9.6 GUI release history update

Please see Add NAT for details.

1.8.1.9.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

1.8.1.9.8 Supplementary information

NONE

1.8.1.10 GUI name: Add VPN

Add VPN Dialog.

1.8.1.10.1 Functional description

This is a new dialog box that is used when a new VPN is being created. The dialog contains a text box in which the user adds a new VPN name. On clicking the OK button the VPN is created but is not assigned to any NAT. The new VPN will automatically be added to the VPN combo box on the addnat dialog.

An optional check box “Shared Id” will display a field into which a specific Global ID can be entered for the VPN. This is to be used when the VPN is shared across Element managers. It does reuire that the ID to be shared is not already allocated to another VPN.

This dialog can only be called from the Add NAT dialog or the “Add” Button on the VPN details dialog.

1.8.1.10.2 GUI usage and implications

This dialog can only be called from the Add NAT dialog or by clicking the “Add” button on the VPN Details Dialog. It is used to create a new VPN.

1.8.1.10.3 GUI size

Table 19 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Add VPN	1	1	N/A

1.8.1.10.4 GUI fields

The following table lists fields for the addVPN dialog.

Table 20 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Name	New			Contains the new VPN name	

1.8.1.10.5 Usage example

The following example shows the default dialog with no data yet entered.

1.8.1.10.6 GUI release history update
This is a new dialog.

1.8.1.10.7 Context sensitive launching information
This is launched using the CS2000 Management Tools interface

1.8.1.10.8 Supplementary information
NONE

1.8.1.11 GUI name: Details
NAT Details

1.8.1.11.1 Functional description
This GUI will replace existing dialogs to display the GWC ID and GW information for Zones.

A new details button will be added to the network zone panels and the Display ID and Retrieve GW buttons will be removed. On clicking the details button the details dialog will be presented.

This will contain a pull down containing up to two items. The dialog choices are to display the GWC NAT ID and the gateway report. These options will only be available if the user selected a specific Network Zone. The original dialogs have been changed to panels and included in this dialog.

1.8.1.11.2 GUI usage and implications
This GUI is used to display Zone information, including GWC IDs and Gateways using the Zones.

1.8.1.11.3 GUI size

Table 21 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
NATDetails	1	1	N/A

1.8.1.11.4 GUI fields
The following table lists fields for the Details dialog.

Table 22 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Detail selection	New			Chooses NAT information.	

1.8.1.11.5 Usage example
The following example shows the default dialog.

1.8.1.11.6 GUI release history update
This is a new dialog.

1.8.1.11.7 Context sensitive launching information
This is launched using the CS2000 Management Tools interface

1.8.1.11.8 Supplementary information
NONE

1.8.1.12 GUI name: Details - VPN
VPN Details Dialog

1.8.1.12.1 Functional description
The dialog panel will show a table containing all VPNs and the NATs which make them up. An add and delete button will also be included to allow the user to manage the VPNs.

1.8.1.12.2 GUI usage and implications
This gui is selected by pressing the “VPN” button on the NAT or composite NAT/LBL tabbed panels.

1.8.1.12.3 GUI size

Table 23 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
VPN Details	1	1	N/A

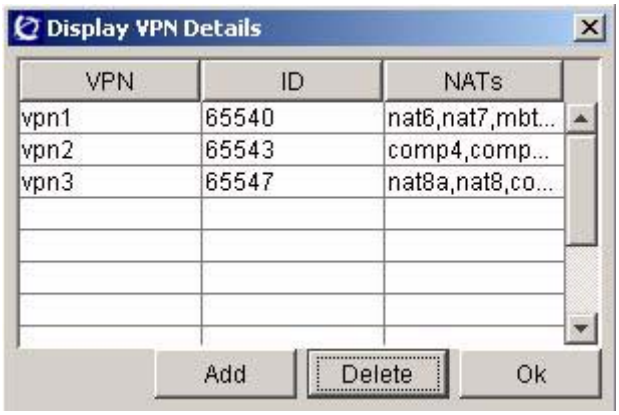
1.8.1.12.4 GUI fields
The following table lists fields for the VPN dialog.

Table 24 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
VPN Table	New			Displays VPN information.	

1.8.1.12.5 Usage example

The following example shows VPNs and the NATs that they consist of.



1.8.1.12.6 GUI release history update

This is a new panel.

1.8.1.12.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

1.8.1.12.8 Supplementary information

NONE

1.8.1.13 GUI name: Details GWC ID

GWC ID panel part of the details dialog

1.8.1.13.1 Functional description

This panel displays the NAT ID in the GWC.

Please note this is existing functionality which has been included in the details dialog.

1.8.1.13.2 GUI usage and implications

This gui displays the NAT ID which is GWC uses.

1.8.1.13.3 GUI size

Table 25 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GWCID	1	1	N/A

1.8.1.13.4 GUI fields

Table 26 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

1.8.1.13.5 Usage example

The following example shows the ID of the selected Zone.

1.8.1.13.6 GUI release history update

This is a new panel that contains existing information.

1.8.1.13.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

1.8.1.13.8 Supplementary information

NONE

1.8.1.14 GUI name: Details Gateway Report

Gateway report panel part of the Zone details dialog.

1.8.1.14.1 Functional description

This panel contains the gateway report table that was previously in its own dialog.

1.8.1.14.2 GUI usage and implications

This gui is obtained from the NAT details dialog.

1.8.1.14.3 GUI size

Table 27 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GWReport	1	1	N/A

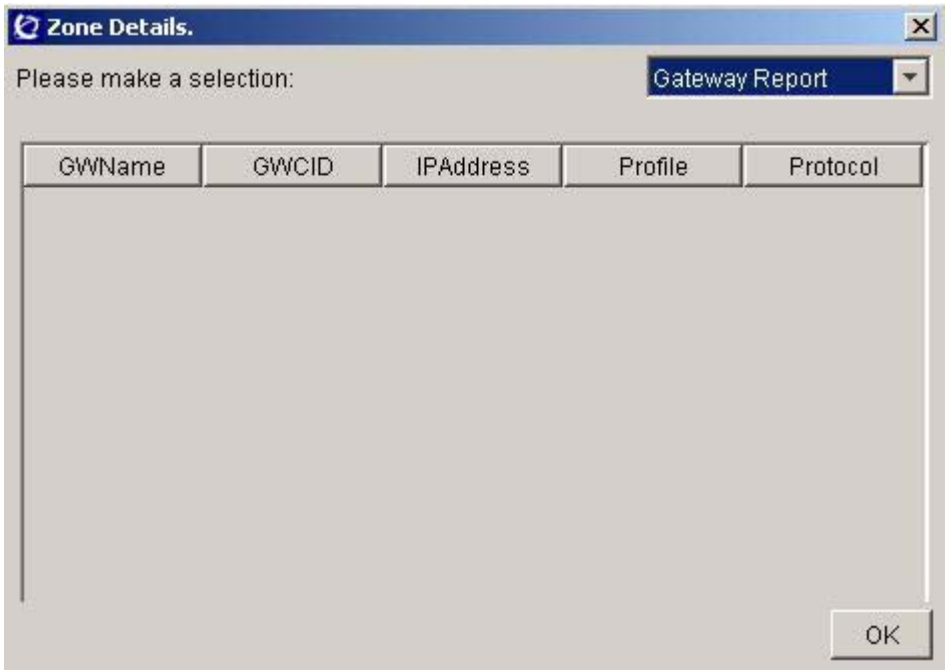
1.8.1.14.4 GUI fields

Table 28 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

1.8.1.14.5 Usage example

The following example shows the panel embedded in the details dialog.



1.8.1.14.6 GUI release history update

This is an existing GUI that's been moved to the details dialog box.

1.8.1.14.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

1.8.1.14.8 Supplementary information
NONE

1.8.1.15 GUI name: GWC Media Proxies Tab
Gateway controller media proxy tab.

1.8.1.15.1 Functional description
This panel contains the list of media proxies that are provisioned on a GWC. New group information has been added.

1.8.1.15.2 GUI usage and implications
This gui is obtained from the GWC provisioning panel.

1.8.1.15.3 GUI size

Table 29 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GWCMPPanel	1	1	N/A

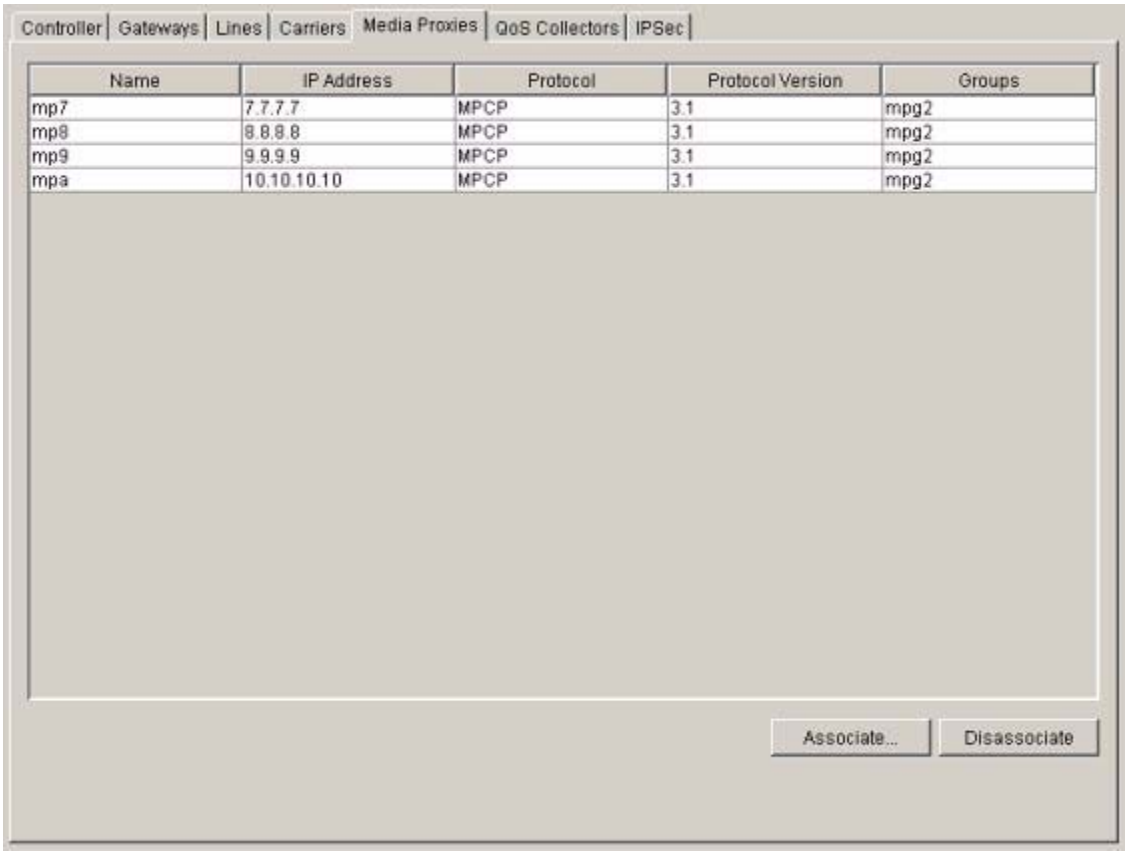
1.8.1.15.4 GUI fields

Table 30 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
MP Groups	New			Shows whether the media proxy is part of a group.	

1.8.1.15.5 Usage example

The following example shows the added groups column to the media proxy panel.



1.8.1.15.6 GUI release history update

This is an existing GUI that has been extended.

1.8.1.15.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

1.8.1.15.8 Supplementary information

NONE

1.8.2 CLUI Interface

None

1.9 User interface changes

None

1.10 OSSGate Interface Changes

1.10.1 XML Command Changes

The following new interfaces introduced in SN09 to manage Media Proxy Groups:

- Add Media Proxy Group - Add a new Media Proxy Group and the Media Proxys associated with that group.
- Query Media Proxy Group. - There are three types of query:
  - — List all the Media Proxys within a Media Proxy Group.
  - — List all Media Proxy Groups assigned against a Gateway Controller.
  - — List all the Media Proxy Groups that a Media Proxy belongs to.
- Change Media Proxy Group - Modify the list of Media Proxys assigned to a group.
- Delete Media Proxy Group - Delete a Media Proxy group.

The following new interfaces introduced in SN09 to manage VPNs.

- Add VPN - Add a new VPN with the specified name.
- Delete VPN - Delete a VPN from the list of VPNs.

The following interfaces will be modified in SN09 to make use of Media Proxy groups:

- Add Network Zone - When a Network zone is created, allow it to be optionally associated with a Media Proxy Group and/or a VPN. This requires changes to Add NAT and add LBL.
- Add NAT - When a Nat middlebox is created, allow it to be optionally associated with a Media Proxy Group and/or a VPN.
- Add LBL - When a LBL middlebox is created, allow it to be optionally associated with a Media Proxy Group.
- Query Network Zone - Extend the query to return the Media Proxy Group and VPN.
- Query Nat - Extend the query to return the Media Proxy Group and VPN.
- Query LBL - Extend the query to return the Media Proxy Group.
- Change Network Zone - Change the Media Proxy Group and/or VPN assigned to a middlebox.
- Change NAT - Change the Media Proxy Group and/or VPN assigned to a Middlebox.
- Change LBL - Change the Media Proxy Group assigned to a Middlebox.

1.10.1.1 Add MP Group XML command

Add Media Proxy Group is a new command in SN09. The command defines a new group and adds between one and five Media Proxies to that group.

The XML for this command is shown in Figure 1, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 1 XML command to Add Media Proxy Group

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <addMPGroup usn="1" version="1.0">
      <Parameters>
       <MPGroupName>aGroup</MPGroupName>
       <MPname>mp1</MPname>
       <MPname>mp11</MPname>
       <MPname>mp111</MPname>
       <MPname>mp1111</MPname>
       <MPname>mp11111</MPname>
     </Parameters>
     </addMPGroup>
    </Methods>
  </Command>
 </CommandList>
```

1.10.1.2 Response XML

Example:

```
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<addMPGroup usn="1" version="1.0"><ReturnData><ReturnCode value="0"
text="Successful result" /></ReturnData></AddMPGroup> </Methods>
  </Response>
</CommandList>
```

1.10.1.3 Query MP Group XML command

Query Media Proxy Group is a new command in SN09. Three versions of the command provide queries to return the following information:

- The list of Media Proxies contained in a Media Proxy Group
- List all Media Proxy Groups
- The list of Media Proxy Groups a Media Proxy belongs to
- The list of Media Proxy Groups associated with a Gateway Controller

The three versions of XML for this command are shown in Figure 2, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 2 XML command to Query MP Group

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryMPGroup usn="1" version="1.0">
      <Parameters>
       <MPGroupName>aGroup</MPGroupName>
      </Parameters>
     </queryMPGroup>
    </Methods>
  </Command>
 </CommandList>
## get all MPG entries
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryMPGroup usn="1" version="1.0">
      <Parameters>
      </Parameters>
     </queryMPGroup>
    </Methods>
  </Command>
 </CommandList>
## get MPGs that MP belongs to
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryMPGroup usn="1" version="1.0">
      <Parameters>
       <MPname>mp1</MPname>
      </Parameters>
     </queryMPGroup>
    </Methods>
  </Command>
 </CommandList>
## get MPGs that are on a GWC
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryMPGroup usn="1" version="1.0">
      <Parameters>
       <GWCname>GWC-1</GWCname>
      </Parameters>
     </queryMPGroup>
    </Methods>
  </Command>
 </CommandList>
```

1.10.1.4 Response XML

Two types of response are provided, the detailed single MPG response, and the multiple MPG name response. The single response is only provided when a single MPG is request.

```
## single MPG response
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<queryMPGroup usn="1" version="1.0"><ReturnData><MPGGroupName>MPG-ABC</
MPGGroupName><MPname>MP-ABC</MPname><MPname></MPname><MPname></
MPname><MPname></MPname><MPname></MPname><ReturnCode value="0" text="Successful result" /></
ReturnData></queryMPGroup>    </Methods>
  </Response>
</CommandList>

## multiple MPG response
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<queryMPGroup usn="1" version="1.0"><ReturnData><MPGGroupName>MPG-ABC</
MPGGroupName><ReturnCode value="0" text="Successful result" /></ReturnData></queryMPGroup>    </
Methods>
  </Response>
</CommandList>
```

1.10.1.5 Change MP Group XML command

Change Media Proxy Group is a new command in SN09. The command redefines the list of Media Proxies contained within a Media Proxy Group. The new list will replace the previous list.

The XML for this command is shown in Figure 3, the schema is defined in Appendix B and error messages returned are described in Appendix C.Appendix D provides a description of each tag.

Figure 3 XML Command to Change MP Group

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <changeMPGroup usn="1" version="1.0">
      <Parameters>
       <MPGroupName>aGroup</MPGroupName>
       <MPname>mp1</MPname>
       <MPname>mp2</MPname>
      </Parameters>
     </changeMPGroup>
    </Methods>
  </Command>
 </CommandList>
```

1.10.1.6 Response XML

```
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<changeMPGroup usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful
result" /></ReturnData></ChangeMPGroup>      </Methods>
  </Response>
</CommandList>
```

1.10.1.7 Delete MP Group XML command

Delete Media Proxy Group is a new command in SN09. The command deletes the definition of a Media Proxy Group.

The XML for this command is shown in Figure 4, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 4 XML Command to Delete MP Group

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <deleteMPGroup usn="1" version="1.0">
      <Parameters>
       <MPGroupName>aGroup</MPGroupName>
      </Parameters>
     </deleteMPGroup>
    </Methods>
  </Command>
 </CommandList>
```

1.10.1.8 Response XML

```
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<deleteMPGroup usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful
result" /></ReturnData></deleteMPGroup>     </Methods>
  </Response>
</CommandList>
```

1.10.1.9 Add VPN XML command

Add VPN is a new command in SN09. The command adds the definition of a new VPN.

The XML for this command is shown in Figure 5, the schema is defined in Appendix B and error messages returned are described in Appendix C.Appendix D provides a description of each tag.

Figure 5 XML Command to Add VPN

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <addVPN usn="1" version="1.0">
     <Parameters>
         <vpnName>VPN11</vpnName>
      </Parameters>
     </addVPN>
    </Methods>
  </Command>
 </CommandList>
```

1.10.1.10 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<addVPN usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful result" /
></ReturnData></addVPN>      </Methods>
  </Response>
</CommandList>
```

1.10.1.11 Delete VPN XML command

Delete VPN is a new command in SN09. The command deletes the definition of a VPN.

The XML for this command is shown in Figure 6, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 6 XML Command to Delete VPN

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <deleteVPN usn="1" version="1.0">
     <Parameters>
         <vpnName>VPN11</vpnName>
      </Parameters>
     </deleteVPN>
    </Methods>
  </Command>
 </CommandList>
```

1.10.1.12 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<deleteVPN usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful
result" /></ReturnData></deleteVPN>      </Methods>
  </Response>
</CommandList>
```

1.10.1.13 Add Network Zone XML command

The existing Add Network Zone command is extended in SN09. The additional tag <preferredMPGroup> allows a Media Proxy Group to be optionally associated with a Network Zone when a Network Zone is created. The additional tag <vpnName> allows a VPN to be optionally be associated with a Network Zone providing its type is NAT or Composite Nat.

The XML for this command is shown in Figure 7, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 7 XML Command to Add a Network Zone

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <addNetworkZone usn="1" version="1.0">
     <Parameters>
         <Name>NZ1</Name>
         <Service>NAT</Service>
        <PreferredMPGroup>MPG1</PreferredMPGroup>
      </Parameters>
     </addNetworkZone>
    </Methods>
  </Command>
</CommandList>
```

1.10.1.14 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<addNetworkZone usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful
result" /></ReturnData></addNetworkZone>      </Methods>
  </Response>
</CommandList>
```

1.10.1.15 Add NAT XML command

The existing Add NAT command is extended in SN09. The additional tag <preferredMPGroup> allows a Media Proxy Group to be optionally associated with a NAT when a NAT is created. The additional tag <vpnName> allows a VPN to be optionally be associated with a NAT.

The XML for this command is shown in Figure 8, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 8 XML Command to Add a NAT middlebox

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <addNAT usn="1" version="1.0">
     <Parameters>
        <NATname>MkI</NATname>
            <PreferredMPGroup>MPG1</PreferredMPGroup>
      </Parameters>
     </addNAT>
    </Methods>
  </Command>
</CommandList>
```

1.10.1.16 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<addNAT usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful result" /
></ReturnData></addNAT>      </Methods>
  </Response>
</CommandList>
```

1.10.1.17 Add LBL XML command

The existing Add LBL command is extended in SN09. The additional tag <preferredMPGroup> allows a Media Proxy Group to be optionally associated with a LBL middlebox when a LBL middlebox is created.

The XML for this command is shown in Figure 9, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 9 XML Command to Add a LBL middlebox

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
 <Command>
  <Interface>ITransIf</Interface>
   <Methods>
    <addLBL usn="1" version="1.0">
    <Parameters>
       <LBLname>LBL1</LBLname>
            <RUDescription>SPC_Default_RU</RUDescription>
            <MaxCount>10</MaxCount>
            <PreferredMPGroup>MPG1</PreferredMPGroup>
    </Parameters>
   </addLBL>
  </Methods>
 </Command>
</CommandList>
```

1.10.1.18 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<addLBL usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful result" /
></ReturnData></addLBL>      </Methods>
  </Response>
</CommandList>
```

1.10.1.19 Query Network Zone XML command

The existing Query Network Zone command is extended in SN09. When either individual or multiple network Zones are queried the response is extended to include the Media Proxy Group and VPN, if any, the Network Zone has.

- List all Network Zoness
- The details of a single network Zone.
- The list of Network Zones having a specified Media Proxy Group.

The optional tag <preferredMPGroup> is used to allow the query to be based on a specified Media Proxy Group.

The XML for this command is shown in Figure 10, the schema is defined in Appendix B and error messages returned are described in Appendix C.

Figure 10 XML Command to Query Network Zone

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryNetworkZone usn="1" version="1.0">
     <Parameters>
      </Parameters>
     </queryNetworkZone>
    </Methods>
  </Command>
 </CommandList>
```

1.10.1.20 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
     <Interface>ITransIf</Interface>
     <Methods>
<queryNetworkZone usn="1" version="1.0"><ReturnData>
<NetworkZone>
       <ID>10</ID>
       <Name>COMP1</Name>
       <ParentID>0</ParentID>
</NetworkZone>
<NetworkZone>
       <ID>11</ID>
       <Name>NZ1</Name>
       <ParentID>0</ParentID>
</NetworkZone><ReturnCode value="0" text="Successful result" /></ReturnData></
queryNetworkZone>     </Methods>
  </Response>
</CommandList>
```

1.10.1.21 Query NAT XML command

The existing Query NAT command is extended in SN09. When either individual or multiple NAT middleboxes are queried the response is extended to include the Media Proxy Group and VPN, if any, that each NAT has.

- List all NATs
- The details of a single NAT.
- The list of NATs having a specified Media Proxy Group.

The optional tag <preferredMPGroup> is used to allow the query to be based on a specified Media Proxy Group.

The XML for this command is shown in Figure 11, the schema is defined in Appendix B and error messages returned are described in Appendix C.

Figure 11 XML Command to Query NAT Middlebox

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
 <Command>
  <Interface>ITransIf</Interface>
   <Methods>
    <queryNAT usn="1" version="1.0">
    <Parameters>
       <NATname>Nat1</NATname>
     </Parameters>
    </queryNAT>
   </Methods>
 </Command>
</CommandList>
```

1.10.1.22 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<queryNAT usn="1" version="1.0"><ReturnData><NATname>ssssss</
NATname><NATType>1</NATType><ParentMB></
ParentMB><PreferredMPGroup>LONDON</PreferredMPGroup><VPNname>UK<VPNname>
<ReturnCode value="0" text="Successful result" /></ReturnData></queryNAT>     </Methods>
  </Response>
</CommandList>
```

1.10.1.23 Query LBL XML command

The existing Query LBL command is extended in SN09. When either individual or multiple LBL middleboxes are queried the response is extended to include the Media Proxy Group, if any, each LBL has. There are three types of query for this element:

- List all LBLs
- The details of a single LBL.
- The list of LBLs having a specified Media Proxy Group.

The optional tag <PreferredMPGroup> enables this extended query.

The XML for this command is shown in Figure 12, the schema is defined in Appendix B and error messages returned are described in Appendix C.

Figure 12 XML Command to Query LBL Middlebox

```
Query single LBL:
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryLBL usn="1" version="1.0">
     <Parameters>
        <LBLname>LBL1</LBLname>
      </Parameters>
     </queryLBL>
    </Methods>
  </Command>
 </CommandList>

 Query All LBLs:
  <?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryLBL usn="1" version="1.0">
     <Parameters>
      </Parameters>
     </queryLBL>
    </Methods>
  </Command>
 </CommandList>

  MPG based query:
 <?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryLBL usn="1" version="1.0">
     <Parameters>
       <PreferredMPGroup>MPG1</PreferredMPGroup>
      </Parameters>
     </queryLBL>
    </Methods>
  </Command>
 </CommandList>
```

1.10.1.24 Response XML

```
single response:
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<queryLBL usn="1" version="1.0"><ReturnData><LBLname>LBL1</LBLname><CounterGWC>0</
CounterGWC><RUDescription>SPC_Default_RU</RUDescription><MaxCount>10</
MaxCount><ParentMB></ParentMB><PreferredMPGroup>MPG2</PreferredMPGroup><ReturnCode value="0"
text="Successful result" /></ReturnData></queryLBL>    </Methods>
  </Response>
</CommandList>

multiple response:
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<queryLBL usn="1" version="1.0"><ReturnData><LBLname>LBL1</LBLname><LBLname>LBL2</
LBLname><ReturnCode value="0" text="Successful result" /></ReturnData></queryLBL>    </Methods>
  </Response>
</CommandList>

response for MPG query:
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<queryLBL usn="1" version="1.0"><ReturnData><LBLname>LBL2</LBLname><ReturnCode value="0"
text="Successful result" /></ReturnData></queryLBL>    </Methods>
  </Response>
</CommandList>
```

1.10.1.25 Change Network Zone XML command

The existing Change Network Zone command is extended in SN09. When the MediaProxyGroup of the network Zone is to be changed the optional tag <preferredMPGroup> is used to specify the new Media Proxy Group. The optional tag <vpnName> is used to specify the VPN name.

The XML for this command is shown in Figure 13, the schema is defined in Appendix B and error messages returned are described in Appendix C.

Figure 13 XML Command to Change Network Zone

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <changeNetworkZone usn="1" version="1.0">
     <Parameters>
        <Name>NZ1</Name>
        <PreferredMPGroup>MPG2</PreferredMPGroup>
      </Parameters>
     </changeNetworkZone>
    </Methods>
  </Command>
 </CommandList>
```

1.10.1.26 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<changeNetworkZone usn="1" version="1.0"><ReturnData><ReturnCode value="0"
text="Successful result" /></ReturnData></changeNetworkZone> </Methods>
  </Response>
</CommandList>
```

1.10.1.27 Change NAT XML command

The existing Change NAT command is extended in SN09. When the MediaProxyGroup or VPN associated with the NAT is to be changed the optional tag <preferredMPGroup> is used to specify the new Media Proxy Group. The optional tag <vpnName> is used to specify the new VPN name.

The XML for this command is shown in Figure 14, the schema is defined in Appendix B and error messages returned are described in Appendix C.

Figure 14 XML Command to Change NAT

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <changeNAT usn="1" version="1.0">
     <Parameters>
        <NATname>MkI</NATname>
             <PreferredMPGroup>MPG2</PreferredMPGroup>
      </Parameters>
     </changeNAT>
    </Methods>
  </Command>
 </CommandList>
```

1.10.1.28 Response XML

```
<?xml version='1.0'?>
<CommandList>
   <Response>
      <Interface>ITransIf</Interface>
      <Methods>
<changeNAT usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful
result" /></ReturnData></changeNAT>      </Methods>
   </Response>
</CommandList>
```

1.10.1.29 Change LBL XML command

The existing Change LBL command is extended in SN09. When the MediaProxyGroup associated with the LBL is to be changed the optional tag <preferredMPGroup> is used to specify the new Media Proxy Group.

The XML for this command is shown in Figure 15, the schema is defined in Appendix B and error messages returned are described in Appendix C.

Figure 15 XML Command to Change LBL

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <changeLBL usn="1" version="1.0">
     <Parameters>
        <LBLname>LBL1</LBLname>
                <PreferredMPGroup>MPG2</PreferredMPGroup>
      </Parameters>
     </changeLBL>
    </Methods>
  </Command>
 </CommandList>
```

1.10.1.30 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<changeLBL usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful
result" /></ReturnData></changeLBL>     </Methods>
  </Response>
</CommandList>
```

1.10.2 Additional OSSGate Changes

The Network Zone xml interface is common to both the CS2KMT and the SPC. Any changes added made to the network Zone xml must be implemented for the SPC as well as the CS2KMT. As this feature has introduced changes to the network Zone xml files shared by the SPC, the expectation is that there will be a feature on the SPC to absorb the impact of these changes.

1.11 Configuration Walkthrough

1.11.1 Creating a Media Proxy Group

A MPG is allocated as follows using the CS2000 Management tools GUI:

1) In the main network devices Panel, select the Media Proxies Tab.

2) In the “Media Proxies” Tab select the “Media Proxy Groups” Tab.

3) Click on the “Add” button to display the “Add Media Proxy Group” dialog.

4) Enter the name of the Media Proxy Group in the field at the top of the dialog

5) Select in turn up to 5 media proxies to add to the group by highlighting each and pressing the “add>>” button. If a MP is added in error it can be removed using the “<<rem” button.

6) If the creation fails, a message window will be displayed and the media proxy group will not be added.

1.11.2 Changing a Media Proxy Group

A MPG is modified as follows using the CS2000 Management tools GUI:

1) In the main network devices Panel, select the Media Proxies Tab.

2) In the “Media Proxies” Tab select the “Media Proxy Groups” Tab.

3) Select (highlight) the Media Proxy Group to be changed.

4) Click on the “Change” button to display the “Change Media Proxy Group” dialog.

5) Select any media proxies to be removed from the group by highlighting each and pressing the “<<rem” button. If a MP needs to be added it can be added using the “add>>” button.

6) If the change fails, a message box will be displayed and the change will not take effect.

A Media Proxy Group may not be modified in this way if it is associated with a Network Zone that is associated with a Gateway on a Gateway Controller. If such a Media Proxy Group must be changed, the Media Proxy Group must first be disassociated from the Gateway Controller. This can be achieved by changing the Group on the Network Zone, then changing the Media Proxy Group, before changing the network zone to have the group again.

WARNING: If the Media Proxy Group on the network Zone is changed or removed, this will affect the media proxies that are available for call processing for the duration of the change.

1.11.3 Deleting a Media Proxy Group

A MPG is deleted as follows using the CS2000 Management tools GUI:

1) In the main network devices Panel, select the Media Proxies Tab.

2) In the “Media Proxies” Tab select the “Media Proxy Groups” Tab.

3) Select the Media Proxy Group to be deleted.

4) Click on the “Delete” button at the bottom of the panel to delete the selected media Proxy Group.

5) if the deletion fails, a message box will be displayed.

A Media Proxy Group cannot be deleted if it is associated with a Network Zone.

1.11.4 Assigning a media Proxy Group

When a Network Zone is created using the CS2000 Management Tools Gui, a Media Proxy Group can be assigned to it as follows:

1) From the relevant Network Zone tab (NAT, LBL or composite) click the “Add..” button.

2) Using the “Media Proxy Group” drop down box, select a preferred media proxy group from the list of groups available.

3) proceed with the rest of the provisioning of the network Zone as normal.

4) If the creation fails, the details will be displayed in a message pane. The Network Zone will not be added.

When the Network Zone has been created, it can be used by a gateway as follows:

5) When provisioning a Media Gateway on a GWC, select an ITrans capable profile for the Media Gateway.

6) The Network Zone having the Media Proxy Group should be set as the adjacent middlebox for the media gateway. If the Network Zone is part of a chain of middleboxes then, in order for the gateway to use its Media Proxy Group, the network Zones closer to the media gateway in the chain must not have a preferred Group.

1.11.5 Changing the associated Media Proxy Group

To change the media proxy group associated with a Network Zone the following steps must be followed:

1) In the appropriate Network Zones tab, highlight the Network Zone that you wish to change.

2) Hit the “change” button to display the “Change Network Zone” Dialog

3) Select the new Media proxy Group from the drop down list box that appears on the Change Network Zone dialog and click on ok to action the change.

5) If the change fails, details will be displayed in a message pane. The change will not take effect.

WARNING: Changing a Media Proxy Group on a Network Zone that is provisioned on a gateway controller may affect call processing. Media Proxies may be made unavailable for the duration of the change.

1.11.6 Assigning a shared VPN when creating a Network Zone

When a Network Zone is created using the CS2000 Management Tools Gui, a VPN can be assigned to it as follows:

1) From the relevant Network Zone tab (NAT, LBL or composite) click the “Add..” button.

2) If available Click the “use VPN” check (tick) box.

3) From the drop down list which is made visible, select a VPN name. Or click the “create VPN” button to create a new one.

4) A specific VPN ID may be selected. This is used when a VPN spans multiple Call Servers.

5) Proceed with the rest of the provisioning of the network Zone as normal.

6) If the creation fails, the details will be displayed in a message pane. The Network Zone will not be added.

1.12 Appendix A for A00007217: Authorisation groups

The table below shows the Authorisation groups and permissions given for the new methods and operations that are being introduced for this feature. The access rights are aligned with those of the existing Itrans functionality (Media Proxies and Network Zones). Existing authorisation groups remain unchanged by this feature.

Command	**User Group**				
	mgcadm	**mgcrw**	**mgcmtc**	**mgcsprov**	**mgcro**
addMPGroup	X	X			
changeMPGroup	X	X			
queryMPGroup	X	X	X	X	X
deleteMPGroup	X	X			
addVPN	X	X			
deleteVPN	X	X			
queryVPN	X	X	X	X	X

1.13 Appendix B for A00007217: XML validation schemas

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define addMPGroup Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="addMPGroupmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="addMPGroupparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addMPGroupparamsType">
```

```
    <xsd:sequence>
      <xsd:element name="MPGroupName" type="NoSpaceNameType" />
      <xsd:element name="MPname" type="NoSpaceNameType" minOccurs="1" maxOccurs="5" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************************** -->
  <!-- * Define queryMPGroup Method Parameters -->
  <!-- ********************************************************************************************************** -->
  <xsd:complexType name="queryMPGroupmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="queryMPGroupparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="queryMPGroupparamsType">
   <xsd:choice minOccurs="0">
      <xsd:element name="MPGroupName" type="NoSpaceNameType" />
      <xsd:element name="MPname" type="NoSpaceNameType" />
      <xsd:element name="GWCname" type="GWCNameType"  />
   </xsd:choice>
  </xsd:complexType>
</xsd:schema>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************************** -->
  <!-- * Define changeMPGroup Method Parameters -->
  <!-- ********************************************************************************************************** -->
  <xsd:complexType name="changeMPGroupmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="changeMPGroupparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="changeMPGroupparamsType">
    <xsd:sequence>
      <xsd:element name="MPGroupName" type="NoSpaceNameType" />
      <xsd:element name="MPname" type="NoSpaceNameType" minOccurs="0" maxOccurs="5" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************************** -->
  <!-- * Define deleteMPGroup Method Parameters -->
```

```
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="deleteMPGroupmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="deleteMPGroupparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="deleteMPGroupparamsType">
    <xsd:all>
      <xsd:element name="MPGroupName" type="NoSpaceNameType" />
    </xsd:all>
  </xsd:complexType>
</xsd:schema>


<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define addVPN Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="addVPNmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="addVPNparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addVPNparamsType">
    <xsd:sequence>
      <xsd:element name="vpnName" type="NoSpaceNameType" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>


<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define deleteVPN Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="deleteVPNmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="deleteVPNparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="deleteVPNparamsType">
    <xsd:all>
      <xsd:element name="vpnName" type="NoSpaceNameType" />
    </xsd:all>
  </xsd:complexType>
</xsd:schema>
```

```
<xsd:schema version="1.0" xml:lang="en" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <!-- **** Warning! This module is cloned from SPC module addNZ.xsd       **** -->
        <!-- **** All changes to the master SPC module should be replicated here **** -->
    <xsd:include schemaLocation="SPCcommon.xsd"/>
    <!-- ***************************************** -->
    <!-- * Define Add Network Zone Method Parameters * -->
    <!-- ***************************************** -->
    <xsd:complexType name="addNetworkZoneMethodType">
        <xsd:all>
            <xsd:element name="Parameters" type="addNetworkZoneParamsType"/>
        </xsd:all>
        <xsd:attributeGroup ref="Usn_VersionAttrbGroup"/>
    </xsd:complexType>
    <xsd:complexType name="addNetworkZoneParamsType">
        <xsd:sequence>
            <xsd:element ref="ID" minOccurs="0"/>
            <!-- only for SESM, the ID is optional -->
            <xsd:element ref="Name"/>
            <xsd:element name="Service" type="NZServiceType" minOccurs="0"/>
            <xsd:element name="Parent" type="ParentType" minOccurs="0"/>
           <xsd:element name="IntraZoneBWInfo" type="BWInfoType" minOccurs="0"/>
            <xsd:element name="LogicalNetworkLink" type="AddLogicalLinkType" minOccurs="0"/>
   <xsd:element name="PreferredMPGroup" type="NoSpaceNameType" minOccurs="0"/>
     <xsd:element name="VPNname" type="NoSpaceNameType" minOccurs="0"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:schema>


<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define addNAT Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="addNATmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="addNATparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addNATparamsType">
    <xsd:all>
      <xsd:element name="NATname" type="NoSpaceNameType" />
      <xsd:element name="NATid" type="MiddleBoxIndexType" minOccurs="0"/>
      <xsd:element name="ParentMB" type="NoSpaceNameType" minOccurs="0"/>

   <xsd:element name="PreferredMPGroup" type="NoSpaceNameType" minOccurs="0"/>
      <xsd:element name="VPNname" type="NoSpaceNameType" minOccurs="0"/>
    </xsd:all>
  </xsd:complexType>
</xsd:schema>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
```

```
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define addLBL Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="addLBLmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="addLBLparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addLBLparamsType">
    <xsd:all>
      <xsd:element name="LBLname" type="NoSpaceNameType" />
      <xsd:element name="CounterGWC" type="IPAddressType" minOccurs="0" />
      <xsd:element name="RUDescription" type="xsd:string" />
      <xsd:element name="MaxCount" type="RUMaxCountType" />
      <xsd:element name="ParentMB" type="NoSpaceNameType" minOccurs="0" />
      <xsd:element name="LBLid" type="MiddleBoxIndexType" minOccurs="0" />
   <xsd:element name="PreferredMPGroup" type="NoSpaceNameType" minOccurs="0"/>
    </xsd:all>
  </xsd:complexType>
</xsd:schema>


<xsd:schema version="1.0" xml:lang="en" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <!-- **** Warning! This module is cloned from SPC module changeNZ.xsd    **** -->
        <!-- **** All changes to the master SPC module should be replicated here **** -->
    <xsd:include schemaLocation="SPCcommon.xsd"/>
    <!-- ****************************************** -->
    <!-- * Define Change Network Zone Method Parameters * -->
    <!-- ****************************************** -->
    <xsd:complexType name="changeNetworkZoneMethodType">
        <xsd:all>
            <xsd:element name="Parameters" type="changeNetworkZoneParamsType"/>
        </xsd:all>
        <xsd:attributeGroup ref="Usn_VersionAttrbGroup"/>
    </xsd:complexType>
    <xsd:complexType name="changeNetworkZoneParamsType">
        <xsd:sequence>
            <xsd:group ref="IDNameGroup"/>
            <xsd:sequence>
                <xsd:element name="Parent" type="ParentType" minOccurs="0"/>
        <xsd:element name="IntraZoneBWInfo" type="IntroZoneBWInfoType" minOccurs="0"/>
        <xsd:element name="LogicalNetworkLink" type="ChangeLogicalLinkType" minOccurs="0"/>
   <xsd:element name="PreferredMPGroup" type="NoSpaceNameType" minOccurs="0"/>
      <xsd:element name="VPNname" type="NoSpaceNameType" minOccurs="0"/>
            </xsd:sequence>
        </xsd:sequence>
    </xsd:complexType>
</xsd:schema>


<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
```

```
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define changeNAT Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="changeNATmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="changeNATparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="changeNATparamsType">
    <xsd:all>
      <xsd:element name="NATname" type="NoSpaceNameType" />
      <xsd:element name="ParentMB" type="NoSpaceNameType" minOccurs="0"/>
<xsd:element name="PreferredMPGroup" type="NoSpaceNameType" minOccurs="0"/>
      <xsd:element name="VPNname" type="NoSpaceNameType" minOccurs="0"/>
    </xsd:all>
  </xsd:complexType>
</xsd:schema>


<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define changeLBL Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="changeLBLmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="changeLBLparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="changeLBLparamsType">
    <xsd:all>
      <xsd:element name="LBLname" type="NoSpaceNameType" />
      <xsd:element name="CounterGWC" type="IPAddressType" minOccurs="0" />
      <xsd:element name="RUDescription" type="xsd:string" minOccurs="0" />
      <xsd:element name="MaxCount" type="RUMaxCountType" minOccurs="0" />
      <xsd:element name="ParentMB" type="NoSpaceNameType" minOccurs="0" />
   <xsd:element name="PreferredMPGroup" type="NoSpaceNameType" minOccurs="0"/>
    </xsd:all>
  </xsd:complexType>
</xsd:schema>


<xsd:schema version="1.0" xml:lang="en" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <!-- **** Warning! This module is cloned from SPC module queryNZ.xsd     **** -->
        <!-- **** All changes to the master SPC module should be replicated here **** -->
    <xsd:include schemaLocation="SPCcommon.xsd"/>
    <!-- ****************************************** -->
    <!-- * Define Query/QueryAll Network Zone Method Parameters * -->
    <!-- ****************************************** -->
    <xsd:complexType name="queryNetworkZoneMethodType">
```

```
        <xsd:all>
            <xsd:element name="Parameters" type="queryNetworkZoneParamsType" nillable="true"/>
        </xsd:all>
        <xsd:attributeGroup ref="Usn_VersionAttrbGroup"/>
    </xsd:complexType>
    <xsd:complexType name="queryNetworkZoneParamsType">
        <xsd:sequence>
            <xsd:choice minOccurs="0">
                <xsd:element ref="ID"/>
                <xsd:element ref="Name"/>
            </xsd:choice>
            <xsd:element name="IDMin" type="xsd:unsignedInt" minOccurs="0"/>
            <xsd:element name="IDMax" type="xsd:unsignedInt" minOccurs="0"/>
            <xsd:element name="MaxZones" type="xsd:unsignedInt" minOccurs="0"/>
                        <xsd:choice minOccurs="0">
        <xsd:element name="PreferredMPGroup" type="NoSpaceNameType"/>
                        </xsd:choice>
        </xsd:sequence>
    </xsd:complexType>
</xsd:schema>



<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define queryNAT Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="queryNATmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="queryNATparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="queryNATparamsType">
    <xsd:sequence>
      <xsd:choice minOccurs="0">
        <xsd:element name="NATname" type="NoSpaceNameType" />
        <xsd:element name="GWCname" type="GWCNameType" />
      </xsd:choice>
      <xsd:choice minOccurs="0">
        <xsd:element name="ListNATid" type="NoSpaceNameType" />
      </xsd:choice>
      <xsd:choice minOccurs="0">
        <xsd:element name="PreferredMPGroup" type="NoSpaceNameType"/>
      </xsd:choice>
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>



<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
```

```
                xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define queryLBL Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="queryLBLmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="queryLBLparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="queryLBLparamsType">
    <xsd:all>
      <xsd:element name="LBLname" type="NoSpaceNameType" minOccurs="0" />
      <xsd:element name="GWCname" type="GWCNameType" minOccurs="0" />
    </xsd:all>
    <xsd:choice minOccurs="0">
        <xsd:element name="PreferredMPGroup" type="NoSpaceNameType"/>
    </xsd:choice>
  </xsd:complexType>
</xsd:schema>
```

1.14 Appendix C for A00007217: Error codes and messages

Table 31 Return codes when command is unsuccessful

Cause of error	Return code	Example return messages
Incorrect command version in query	301	Unsupported version
Platform applications internal error: OSS Interface applications cannot connect to required server application	302	Interfacing error

Error codes have not yet been assigned. This section will need completing. before the feature completes.

1.14.1 Example Error Message

```
<?xml version='1.0'?>
   <CommandList>
      <Response>
        <Interface>ITransIf</Interface>
          <Methods>
             <queryNAT usn="1.0" version="1.0">
              <ReturnData>
                 <NATname>nat1111</NATname>
                  <ReturnCode value= "305" text="NAT not found"/>
              </ReturnData>
             </queryNAT usn="1.0">
```

```
        </Methods>
    </Response>
</CommandList>
```

1.15 Appendix D for A00007217: XML Commands: description of method parameters

1.15.1 Parameter definitions (new in SN09)

- **MPGroupName** - The unique name of the Media Proxy Group. TYPE *NoSpaceNameType*.
- **itransMPGroupName** - The same MPGroupName as defined above. This tag is used in the non-Itrans operations to give the context of Internet Transparency. TYPE *NoSpaceNameType*.
- **preferredMPGroup** - The id of the media Proxy Group.
- **vpnName** - The unique name of the VPN. TYPE *NoSpaceNameType*.

1.15.2 Method Parameters

Method parameters are defined below. Input data is mandatory except where indicated otherwise.

1. **addMPGroup** - Method to create a new Media Proxy Group. This method has the following parameters:

- Input data:
  - usn
  - version
  - MPGroupName. The unique name of the Media Proxy Group.
  - MPname. A list of between one and five Media Proxies which belong to the group that is being created.
- Output data:
  - usn (value should be the same as the input)
  - version (value should be the same as the input)
  - ReturnCode - indicates via an integer value if the command has been successful or, if not, the error type and includes a brief textual message with further information.

2. **queryMPGroup** - A set of methods to query Media Proxy Groups. This method has the following parameters, one of the three optional parameters must be supplied:

- Input data:

– usn

– version

– MPGroupName (optional). Query to return the list of Media Proxies in a the group.

– MPname (optional). Query to list the Media Proxy Groups the Media Proxy belongs to.

– GWCName (optional). Query to list the Media Proxy Groups assigned against the Gateway controller.

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– MPname (returned when the MPGroupName option is used)

– MPGroupName (returned when either the MPname or GWCName options are used)

– ReturnCode - indicates via an integer value if the command has been successful or, if not, the error type and includes a brief textual message with further information.

3. **changeMPGroup** - Method to change the list of Media Proxies assigned to a Media Proxy Group. This method has the following parameters:

• Input data:

– usn

– version

– MPGroupName. The unique name of the Media Proxy Group which must already exist.

– MPname. A list of between one and five Media Proxies which are now to be assigned to that group.

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

4. **deleteMPGroup** - Method that deletes a Media Proxy Group. This method has the following parameters:

• Input data:

– usn

– version

– MPGroupName. The name of the existing Media Proxy Group that is to be deleted.

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

5. **addVpn** - Method to Add a new VPN identifier. This method has the following parameters:

• Input data:

– usn

– version

– vpnName. The name of the VPN which is being created.

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

6. **deleteVpn** - Method to delete an existing VPN identifier. This method has the following parameters:

• Input data:

– usn

– version

– vpnName. The name of the VPN which is being deleted.

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

2: Configuration (CN): A00007544

2.1 Feature Name

NCAS Link and SIP NMS Support based on RFC 3842

2.2 Hardware and Software Requirements

The design depends on the RADVISION stack in Session Server (NGSS) for SIP. There is no additional hardware or software requirements.

If the remote node/system/VM/switching entity complies with the standard protocols supported by this design, then it will be able to interwork with the CS2K. Appropriate changes should be developed in the remote systems and this design have no specific information on configurations of the remote systems.

2.3 Initial Configuration

By default the SOC for the design are at idle state. Therefore, no service will be provided by this design. At initial configurations, it is assumed that standard datafill exists in the DMS/CS2K, GWC and NGSS. The new configurations associated with this feature do not exist.

For supported configurations, please See “Configuration Walkthrough” on page 2241.

2.4 Office/Subnet parameters (OP/SP) (CM & SESM)

This design does not require any office parameter or subnet parameter. However, it does requires definition of appropriate IP address, Port number and application name for the NCAS link. For details, please See “Data schema (DS) (CM, MIBS, RDB)” on page 2230. No details are added here.

2.4.1 New/modified office/subnet parameters

Not applicable.

2.5 Upgrade Considerations

2.5.1 Dump and Restore (CM)

Not Applicable.

2.5.2 Element Management Upgrade

Not Applicable.

2.5.3 Downgrade impact

Not Applicable.

2.6 Data schema (DS) (CM, MIBS, RDB)

2.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
IPAPPL	CHANGED	UNCHANGED
MSGRTE	CHANGED	UNCHANGED

2.6.2 Table/MIB/Remote Database Schema information

2.6.2.1 Name: IPAPPL

IP APPLICATION TABLE

2.6.2.1.1 Functional description

This table contains information about the IP addresses and Port numbers of remote system needed for the SCTP communication. This table also contains information about what application this tuple is datafilled.

2.6.2.1.2 Usage sequence and implications (CM Only)

This table should be datafilled first to create a NCAS link.

2.6.2.1.3 Size

Not changed.

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory

2.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for IPAPPL.

<conditional information>

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPT	Changed	SERVICE	NMS	New added service

2.6.2.1.5 Datafill example

The following example shows sample datafill for table IPAPPL.

2 NCAS SCTP EIU (IPV4 47 142 160 171) (IPV4 47 142 160 172) $ 4990

(APPLICATION NMS) $

2.6.2.1.6 Table release history update

The NMS is added in this release. The Table was created in SN07 release.

2.6.2.1.7 Supplementary information

None.

2.6.2.1.8 Translation verification and other tools

The Table IPAPPL does not use translation verification tools.

2.6.2.2 Name: MSGRTE

MESSAGE ROUTING TABLE

2.6.2.2.1 Functional description

This table provides the routing of the message based on the selector in the table.

2.6.2.2.2 Usage sequence and implications (CM Only)

The datafill for the NCAS link should be done in Table IPAPPL prior to datafilling this table.

2.6.2.2.3 Size

Not changed.

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory

2.6.2.2.4 Fields/OIDs

The following table lists fields/OIDs for MSGRTE

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
MSGRTRES	Changed	MSGRTE_SEL	NCAS instance H323 H323GWC	New selector SCTP is added.

2.6.2.2.5 Datafill example

The following example shows sample datafill for table MSGRTE:

PUBLIC 6137221440 6137221540 (SCTP 2) $

2.6.2.2.6 Table release history update

New selectors are added.

2.6.2.2.7 Supplementary information

None.

2.6.2.2.8 Translation verification and other tools

Not Applicable.

2.7 Service Orders (SO) (CM & SESM)

Not Applicable.

2.8 Software optionality control (SOC)

Based on PLM input this section will be updated.

Table 6 SOC

SOC option name:	MDC00078
SOC option title:	NMS Over IP (SCTP)
SOC option control type:	State
New SOC option?	Yes
SOC option order code	00041296
Option defined in DRU:	CCM
Affected products:	All

2.9 Element Management

2.9.1 New/modified GUIs

Table 7 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Remote SIP Server	Changed
Config Data	Changed

2.9.2 GUI information

2.9.2.1 GUI name: Remote SIP Server

Remote SIP Server

2.9.2.1.1 Functional description

A remote SIP Server is a remote SIP device that the Session Server Manager communicates with via the session initiation protocol. Two examples are other Call Server 2000s or a Multimedia Communication Server (MCS).

2.9.2.1.2 GUI usage and implications

SIP Gateway remote SIP server provisioning is performed by opening the "Remote SIP Server" folder in the left menu. Once there, the following may be performed:

- Remote SIP Server datafill may be added by clicking on the "Add Server" link.
- Remote SIP Servers may also be listed by clicking on "List Servers".
- After listing the Remote SIP servers, the user may choose to delete a particular remote SIP server or modify the data for a particular SIP server.

2.9.2.1.3 GUI size

Not Applicable.

Table 8 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory

2.9.2.1.4 GUI fields

Table 9 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Server Type	New		- Session Server - VRDN - Message Server - Select the Server Type	If the Server Type = Message Server, a SUBSCRIBE message will be sent out to the Remote Server.	
Auto Subscribe	New		Yes / No	If the Auto-Subscribe = 'Y', the Remote Server will be subscribed for accepting MWT notification.	

2.9.2.1.5 Usage example

Figure 1 Provisioning of Server Type on Remote SIP Server

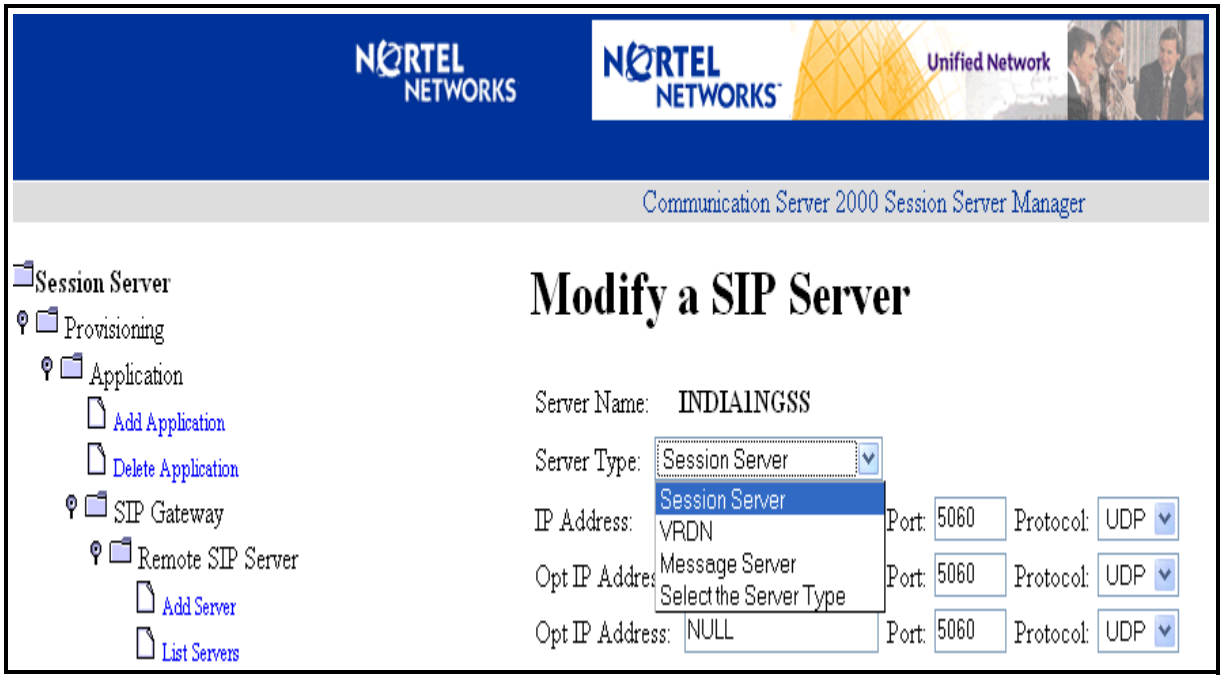
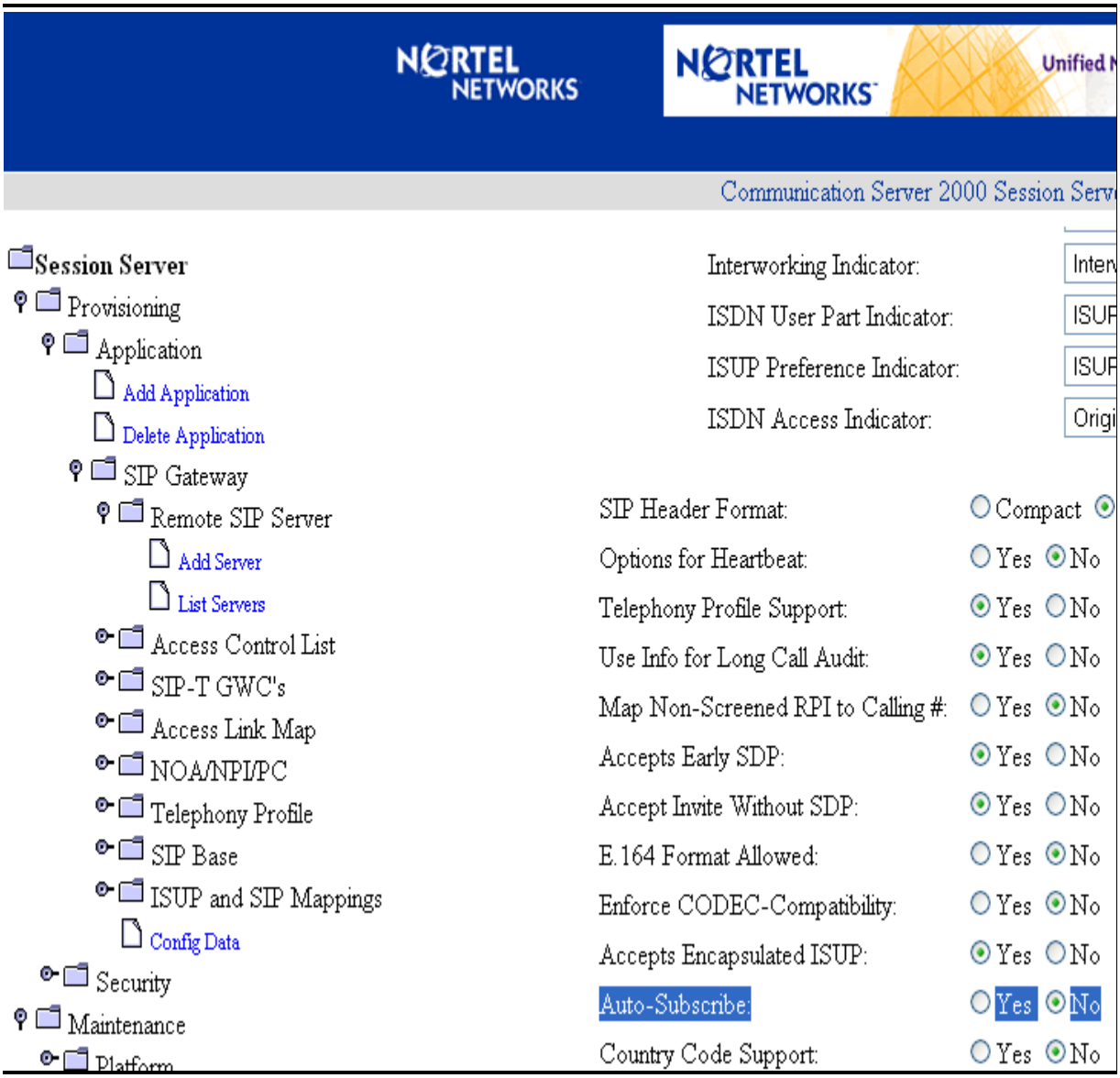


Figure 2 Provisioning of Auto-Subscribe on Remote SIP Server



2.9.2.1.6 GUI release history update

Not Applicable.

2.9.2.1.7 Context sensitive launching information

Not Applicable.

2.9.2.1.8 Supplementary information

Not Applicable.

2.9.2.2 GUI name: Config Data

Configurable Parameter

2.9.2.2.1 Functional description

Before the SIP Gateway application is brought into service, base configuration parameters should be modified to appropriate values.

While many parameters exist on the “Config Data” page, **care** must be taken when changing any of them.

2.9.2.2.2 GUI usage and implications

All the configurable parameters are found on the **Configurable Parameters** page. That page is reached from the Session Server Manager main page via:

- Click on the Provisioning folder
- Click on the Application folder
- Click on the SIP Gateway folder
- Click on **Config Data**

2.9.2.2.3 GUI size

Not Applicable.

Table 10 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory

2.9.2.2.4 GUI fields

Table 11 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
subsRetryTmr	New		Range 0 - 50000 milliseconds	If subsRetryTmr = 0, SUBSCRIBE will not be retried.	

2.9.2.2.5 Usage example

Figure 3 Provisioning of SubsRetryTimer on Session Server

2.9.2.2.6 GUI release history update

Not Applicable.

2.9.2.2.7 Context sensitive launching information

Not Applicable.

2.9.2.2.8 Supplementary information

Not Applicable.

2.9.3 CLUI Interface

2.10 User interface changes

Not Applicable.

2.10.1 Directory: <directory name/MAP level>

2.10.1.1 Directory description

2.10.1.2 Accessing directory: <directory name>

2.10.1.2.1 Access to directory or MAP level and return to CI

2.10.2 Command: <command name>

2.10.2.1 Command type: <NON-MENU, Listed MENU, Unlisted MENU>

2.10.2.2 Command target: <NT40, SUPERNODE, BRISC, All, Other>

2.10.2.3 Command availability: <RES, NONRES or OTHER>

2.10.2.4 Command description

2.10.2.5 Command syntax

Table 12 <CommandName> command parameters and variables

Command	Parameters and variables
<command name> for example, CNTRS	<Plane Number> (0,1) <Display what> Card (0 to 10) All Proc
Parameters and variables	Description
Card	Displays ECC error counts for the specified card only
All	Displays ECC error counts for all the cards on the specified plane. This includes the processor ECC error counts.
Proc	Displays ECC error counts for only the processor memory

2.10.2.6 Qualifications and warnings

2.10.2.7 Responses

2.10.2.7.1 <response>

Table 13 MAP outputs with associated meanings and actions

Command
<RESPONSE>: <description> **Meaning:** **System or user actions:** Example: WARNING: The CPUs are out of sync due to a problem with mismatches. The mismatch logs and minfo should be analysed before a manual resyncing is performed. Do you wish to continue? Please confirm ("Yes", "Y", "No", "N"). **Meaning:** <description> for example "This response warns users that the CPUs are out of sync due to a mismatch and that the cause of the mismatch should be determined before resyncing." **System or user actions:** <description> for example "You should analyze the mismatch logs and minfo to determine the type of faults in the system and deal with those problems before resyncing."
<RESPONSE>: <description> **Meaning:** **System or user actions:**

2.10.2.8 Example

Table 14 Usage examples for <CommandName> command

Description of task:	
Description of task	Synchronize the two CPUs of the CM without matching memory after synchronization and without displaying any warnings regarding possible side effects beforehand.
Command: MAP response:	Example: SYNC Nomatch Noprompt Example: SYNCHRONIZATION SUCCESSFUL

2.11 OSSGate Interface Changes

Not Applicable.

2.12 Security

Not Applicable.

2.13 Configuration Walkthrough

TBA based on the FN sections.

3: Configuration (CN): A00007547

3.1 Feature Name

SIP Lines Core Call Processing Support

3.2 Hardware and Software Requirements

No new hardware or software requirements are created by this activity.

3.3 Initial Configuration

Standard configuration applies.

3.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

3.5 Upgrade Considerations

None.

3.6 Data schema (DS) (CM, MIBS, RDB)

Not applicable.

3.7 Service Orders (SO) (CM & SESM)

Not Applicable. Service Order changes for the support of CS2K SIP Lines are documented under feature A00008556.

3.8 Software optionality control (SOC)

Not Applicable. SOC Control information for the support of CS2K SIP Lines is documented under feature A00008556.

3.9 Element Management

Not applicable.

3.10 OSSGate Interface Changes

Not applicable.

3.11 Security

Not applicable.

3.12 Configuration Walkthrough

4: Configuration (CN): A00007814

4.1 Feature Name

REX testing for MG9000 (Media Gateway 9000) from Element Manager

4.2 Hardware and Software Requirements

None.

4.3 Initial Configuration

NA

4.4 Office/Subnet parameters (OP/SP) (CM & SESM)

NA

4.5 Upgrade Considerations

NA

4.6 Data schema (DS) (CM, MIBS, RDB)

4.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
REX_SCHEDULE	NEW	OLD

4.6.2 Table/MIB/Remote Database Schema information

4.6.2.1 Name: REX_SCHEDULE

Routine EXercise Schedule database table.

4.6.2.1.1 Functional description

Table REX_SCHEDULE lists the schedule assignments for every NE that has to undergo REX.

REX_SCHEDULE table is used to store the schedule information for the NEs that have to execute REX. This table is updated when the user inputs a schedule to execute REX on an NE, removes the REX for an NE, after the execution of REX on an NE.

4.6.2.1.2 Usage sequence and implications (CM Only)

None.

4.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
REX_SCHEDULE	0	Number of NEs present in a subnet	TBD

4.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for REX_SCHEDULE

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SUBNETID	NEW	N/A	1	
NEID	NEW	N/A	1 to 999	
NENAME	NEW	N/A	1 to 32 characters	
STARTTIME	NEW	N/A	00:00 to 23:59	
PERIOD	NEW	N/A	00:00 to 23:59	
DURATION	NEW	N/A	00:00 to 23:59	
WEEKDAYS	NEW	N/A	It can be either of: 1.Sunday 2. Monday 3. Tuesday 4. Wednesday 5. Thursday 6.Friday 7. Saturday	
MODE	NEW	N/A	1. Without SWACT 2. With SWACT	

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CARD_TYPE	NEW	N/A	It can be a combination of the below given cards: 1. DCC 2. ITP 3. ITX	This field contains the selection of card types on which REX will be executed.

4.6.2.1.5 Datafill example
None.

4.6.2.1.6 Table release history update
A new table REX_SCHEDULE is introduced in SN09 to store the REX schedule information of all the NEs under a given subnet.

4.6.2.1.7 Supplementary information
None.

4.6.2.1.8 Translation verification and other tools
None.

4.7 Service Orders (SO) (CM & SESM)
NA

4.8 Software optionality control (SOC)
NA

4.9 Element Management
MG9000 Element manager will be used to execute REX on a given NE.

The EM user will be able to schedule REX and view the progress details of REX on a given NE. REX GUI can be launched from the configuration menu of Subnet view. User will be able to monitor the progress details of REX on the REX GUI and in NE Specific Desktop View.

REX views are similar to that of audit in MG9000 EM.

4.9.1 New/modified GUIs

Table 4 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
REX NE View	NEW
NE Specific Desktop View	CHANGED

4.9.2 GUI information

4.9.2.1 GUI name: REX NE View

4.9.2.1.1 Functional description

REX NE View: This new GUI is introduced under the submenu option MG9KEM NE Specific Desktop view ->Configuration. This GUI allows the user to schedule REX and also view the progress details on the selected NE.

User is allowed to “Add” an NE to be REXed. During “Add” of NE for REX, user inputs the schedule for an NE, by checking the day of the week, hour and minutes on the day of the week when the REX will be executed and duration of REX to be executed and mode of REX.

User can also remove the REX scheduled for an NE.

Progress details of the REX on the selected NE is made available to the user on this GUI.

Note: *REX GUI is subject to change in its appearance to match the enhanced Audit GUI. This change will happen after the IT completion of REX feature. It will be done as part of a CR.*

4.9.2.1.2 GUI usage and implications

To schedule an NE for REX

1 “Add” button is pressed to add the NE for REX.

2 On pressing “Add”, a new panel is opened which will list all the NEs in the given subnet. Select the NE. select mode of REX, select card types on which REX has to be executed, select the day of the week, hour and minutes on the day of the week selected, duration of REX on the selected NE.

3 “Apply” button has to be pressed. On pressing Apply, NE is scheduled for REX with user input data. Newly opened panel closes and the user is in REX NE View.

4 REX NE View lists all the NEs whose schedule is already input by the user. On selecting the NE, state of REX and the progress details are displayed on REX NE View.

To remove REX on already scheduled NE

1 Select the NE from the NE list of REX NE View.

2 On pressing “Remove” button, REX for the selected NE is aborted.

To View the Progress details of REX

1 Select the NE from the NE list of REX NE View.

2 Text area called “Progress details” of REX NE View shows the status of REX on the selected NE.

4.9.2.1.3 GUI size

Table 5 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
REX NE View	1	1	TBD

4.9.2.1.4 GUI fields

The following table lists fields for GUI REX NE View.

Table 6 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
“Add” Button	New	-	-	1. “Add” button is pressed to add the NE for REX. 2. On pressing “Add”, a new panel is opened which will list all the NEs in the given subnet. Select the NE. Select the day of the week, hour and minutes on the day of the week selected, duration of REX on the selected NE. On pressing “Add” button, a check is made if an Audit schedule exists on the current NE 3. “Apply” button has to be pressed. On pressing Apply, NE is scheduled for REX. Newly opened panel closes and the user is in REX NE View. On pressing “Apply” button, validations on the fields are done and prompted to the user. If an Audit schedule on this NE is scheduled at the same instant as REX, a warning message is prompted to the user. If the user confirms REX is scheduled. 4. REX NE View lists all the NEs whose schedule is already input by the user. On selecting the NE, state of REX and the progress details are displayed on REX NE View.	NA

Table 6 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Remove Button	New	-	-	1. Select the NE from the NE list of REX NE View. 2. On pressing “Remove” button, REX for the selected NE is aborted.	NA
Suspend Button	New	-	-	1. Select the NE from the NE list of REX NE View. 2. On pressing “Suspend” button, REX for the selected NE is Disabled/suspended.	NA
Resume Button	New	-	-	1. Select the NE from the NE list of REX NE View. 2. On pressing “Resume” button, REX for the selected NE is Resumed/enabled.	NA
REX Mode	New	-	1. Without SWACT 2. With SWACT	1. If the user selects “without SWACT” option, in that case, REX is executed only on the inactive card of the card pair. 2. If the selected option is “with SWACT”, REX is executed on both the cards of a pair. Inactive card undergoes REX execution, followed by a SWACT on active card and REX on newly inactive card.	NA

Table 6 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Card Types	New	1. DCC 2. ITP 3. ITX	-	1. On selecting DCC, REX will be executed on DCC cards of the NE under consideration which otherwise will be skipped. 2. On selecting ITP, REX will be executed on ITP cards of the NE under consideration which otherwise will be skipped. 3. On selecting ITX, REX will be executed on ITX cards of the NE under consideration which otherwise will be skipped.	NA
REX Schedule	New	Run Immediately	-	If run immediately option is chosen, Day of week, Hour and minute fields are disabled. On clicking on Apply, REX is immediately executed on the given NE.	NA
Day of Week	New	1. Sunday 2. Monday 3. Tuesday 4. Wednesday 5. Thursday 6. Friday 7. Saturday 8. Hour 9. Minutes	-	If Run immediately is deselected, Day of Week, Hour and Minute is enabled. User is able to select the day of the week on which the REX needs to be executed. Hour and Minute would enable user to input the time at which, REX will be executed on the day(s) of week selected.	NA
Current State	New	-	-	This field is a non editable field. It informs the user the state of the REX on the selected NE. State of the REX being “Ready to run”, “Running REX”, “Completed REX”.	NA

Table 6 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Progress Details	New	-	-	This text area displays the success/failure of the operations performed during REX on the selected NE. Operations during REX being, LOCK, UNLOCK, SWACT and Diagnose.	NA
REX Duration	New	1. Hour 2. Minutes	-	The fields Hour and Minutes enable the user to input the duration for which the REX can execute at its maximum limit. If the duration of REX exceeds the input value, REX is failed for such an NE	NA

4.9.2.1.5 Usage example

The following Figure-1 shows the GUI for REX NE View. Figure-2 shows the Create Schedule View which is displayed when “Add” button of REX NE View is clicked.

Figure 1: REX NE View

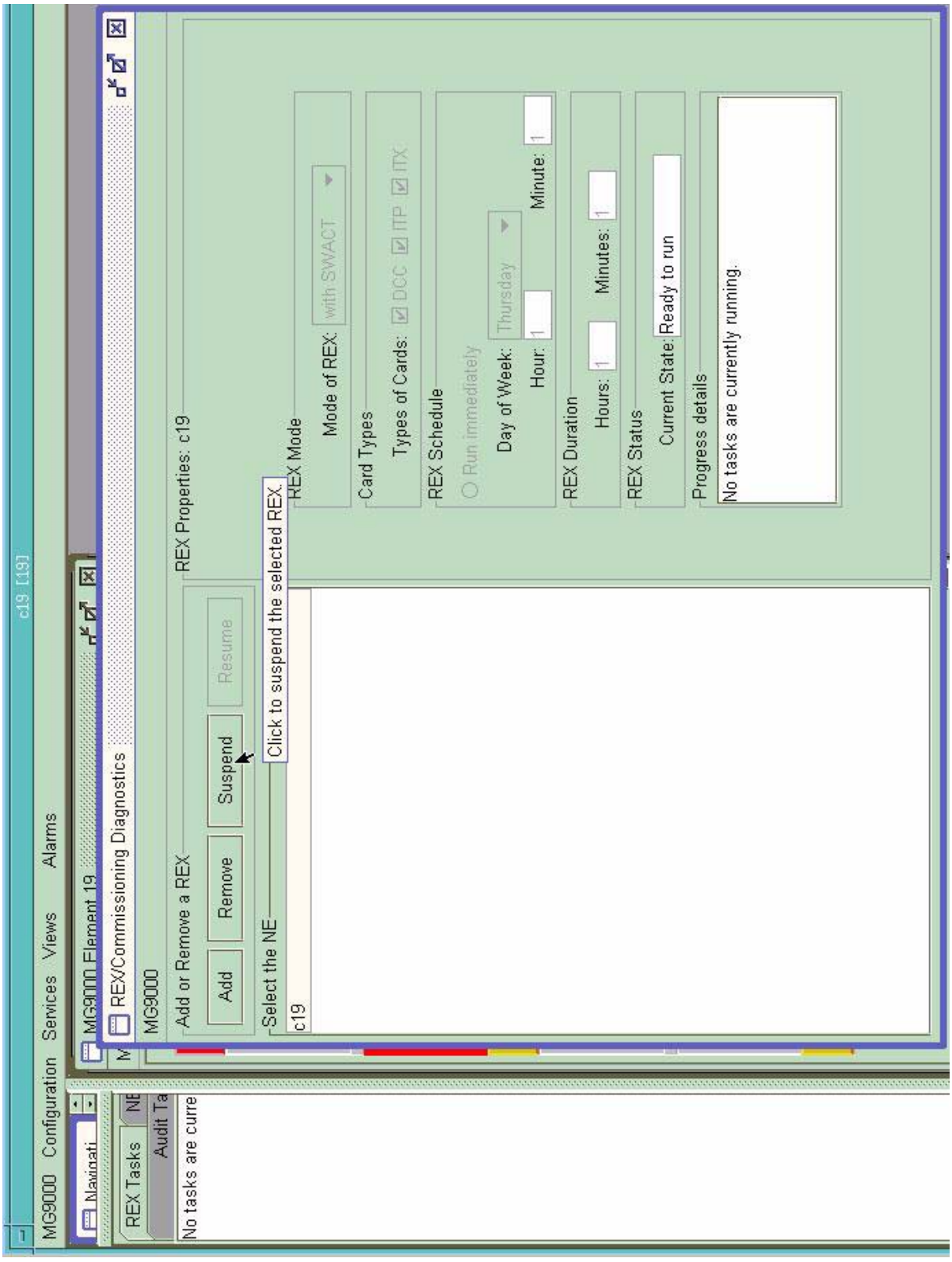


Figure 1.1 -Warning message if an Audit schedule exists at the same instant when REX is being scheduled.

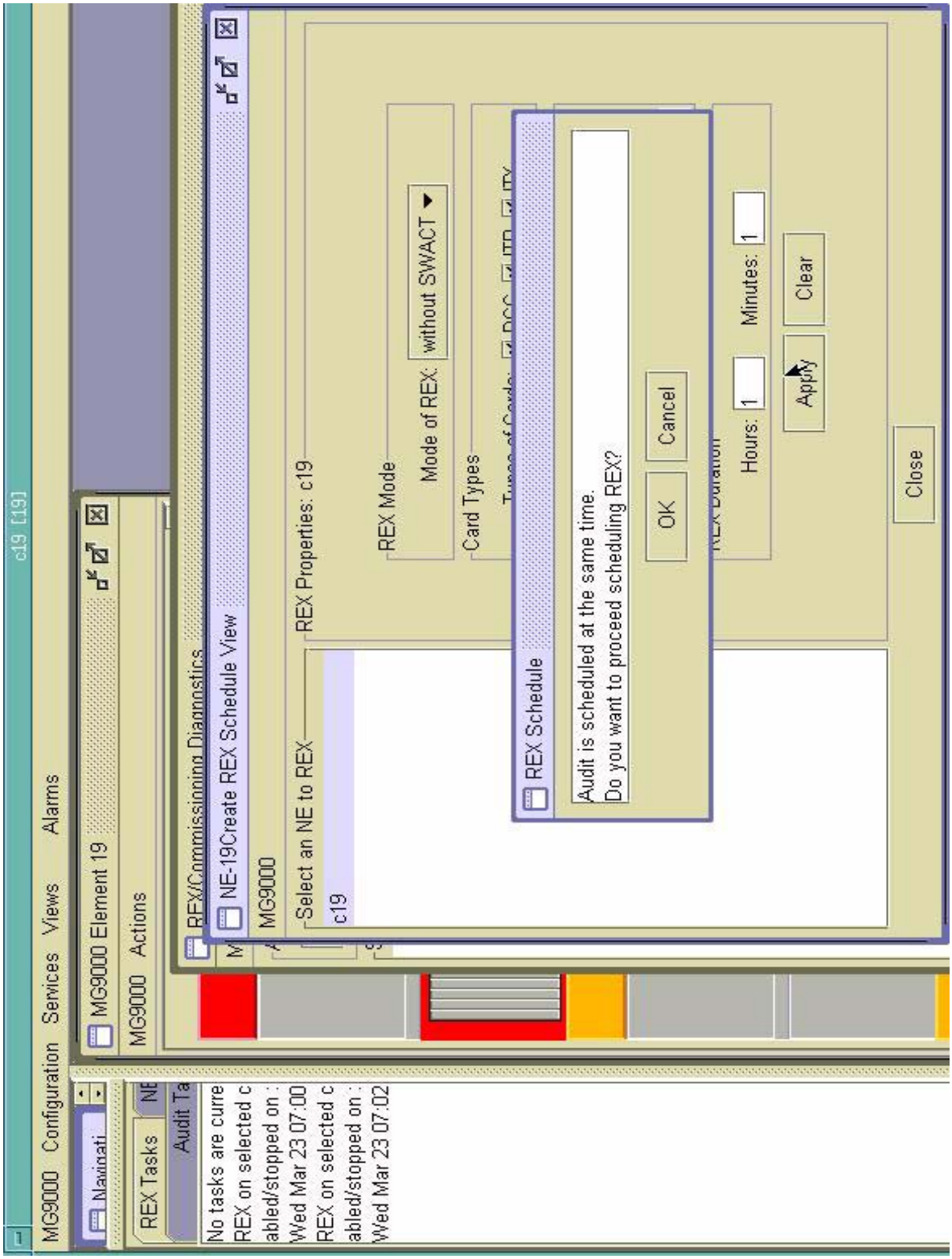
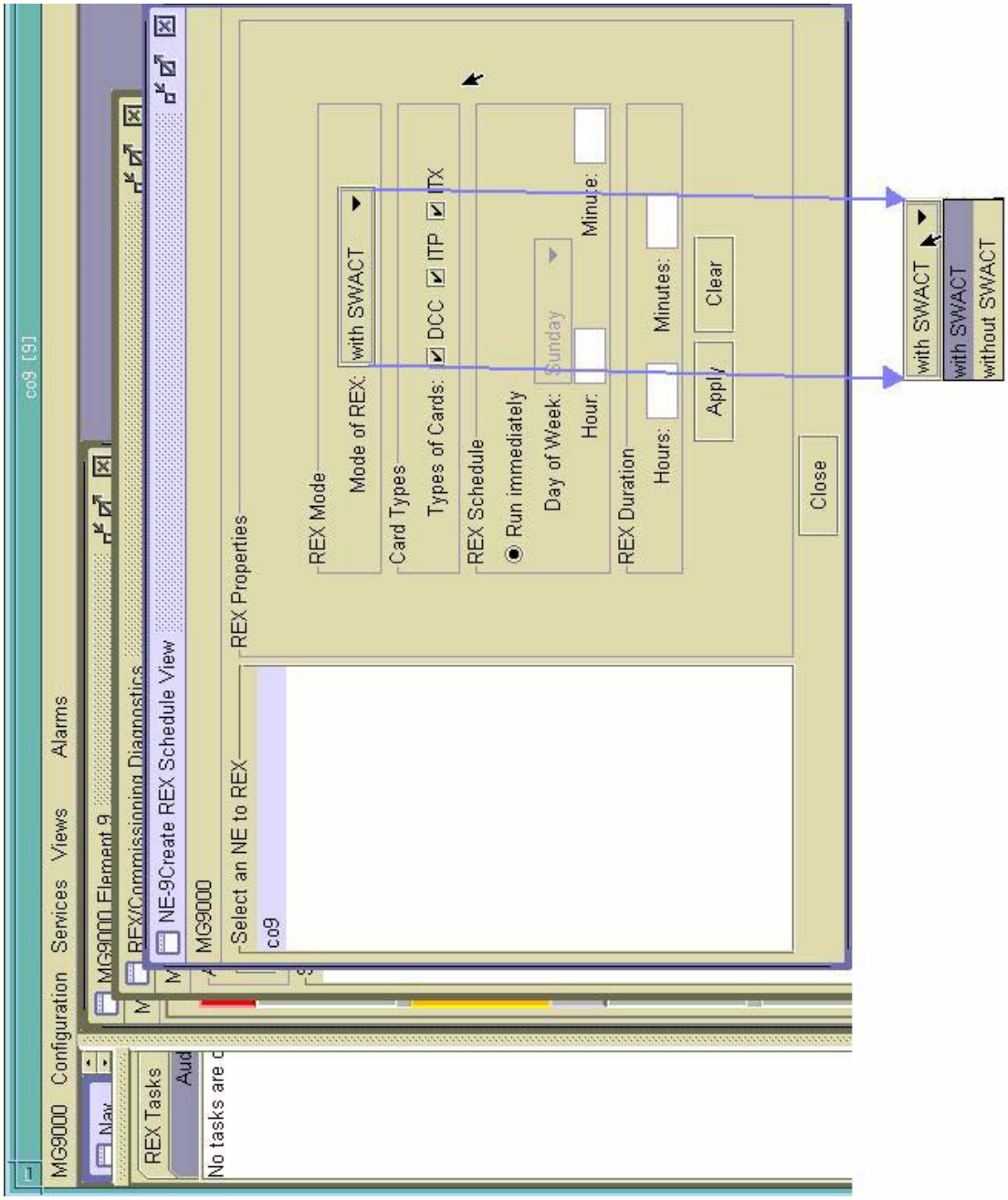


Figure-2 Create Schedule View



4.9.2.1.6 GUI release history update

A new GUI is introduced to schedule REX. REX NE View allows the user to schedule REX on an NE.

4.9.2.1.7 Context sensitive launching information

On clicking “REX NE” of Configuration menu from NE Specific Desktop view, REX NE View is launched. On clicking the “Add” button of REX NE View, Create Schedule View is launched.

4.9.2.1.8 Supplementary information

None.

4.9.2.2 GUI name: NE Specific Desktop View

NE Specific Desktop View provides REX progress details on its left panel.

4.9.2.2.1 Functional description

NE Specific Desktop View opens on clicking on MG9000 from subnet view. The configuration submenu of this view contains a new menu item “REX NE” as shown in Figure-3. This option enables user to launch REX GUI.

A tab is added on the left of NE Specific Desktop View to display the status of REX. Progress details of REX such as success/failure of operations like LOCK, UNLOCK, SWACT, Diagnose are displayed to the user.

4.9.2.2.2 GUI usage and implications

On clicking the NE from the Subnet view, NE Specific Desktop View is launched.

Following Figure-3 shows the GUI when the configuration menu item is clicked from NE Specific Desktop view. Menu item “REX NE” is introduced, which, when clicked, launches REX GUI.

4.9.2.2.3 GUI size

Table 7 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
NE Specific Desktop View	1	1	TBD

4.9.2.2.4 GUI fields

The following table lists fields for GUI NE Specific Desktop View that are related to REX.

Table 8 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
REX NE	New	-	-	On clicking REX NE option of Configuration menu, REX NE View is launched	NA

Table 8 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
REX Tasks tab	New	-	-	A text area that provides the status of REX to the user on the current NE. Status such as success/failure of LOCK, UNLOCK, SWACT and Diagnose are displayed to the user.	NA

4.9.2.2.5 Usage example

Figure -3 shows the NE Specific Desktop View with the “REX NE” option in configuration menu.

Figure -4 shows the “REX Tasks” tab of NE Specific Desktop View.

Figure -3 REX NE menu option

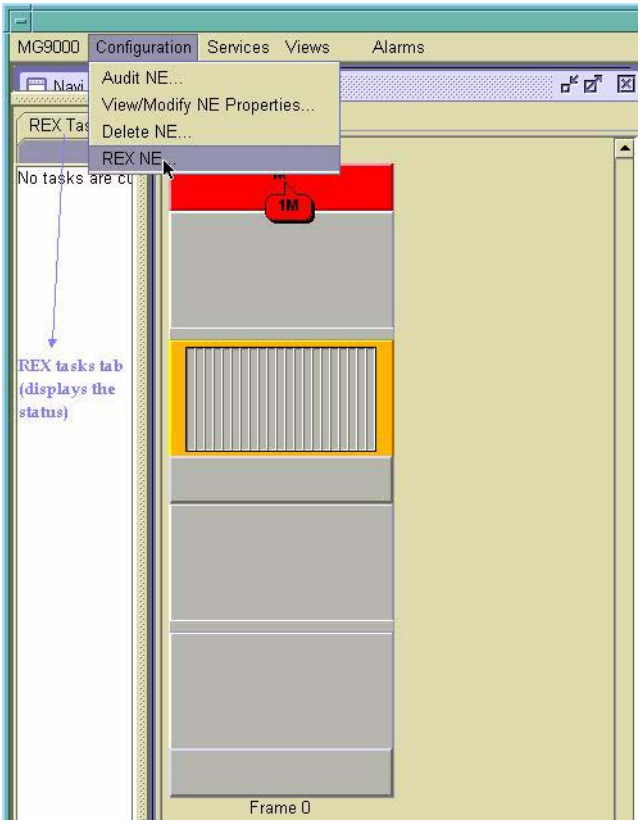
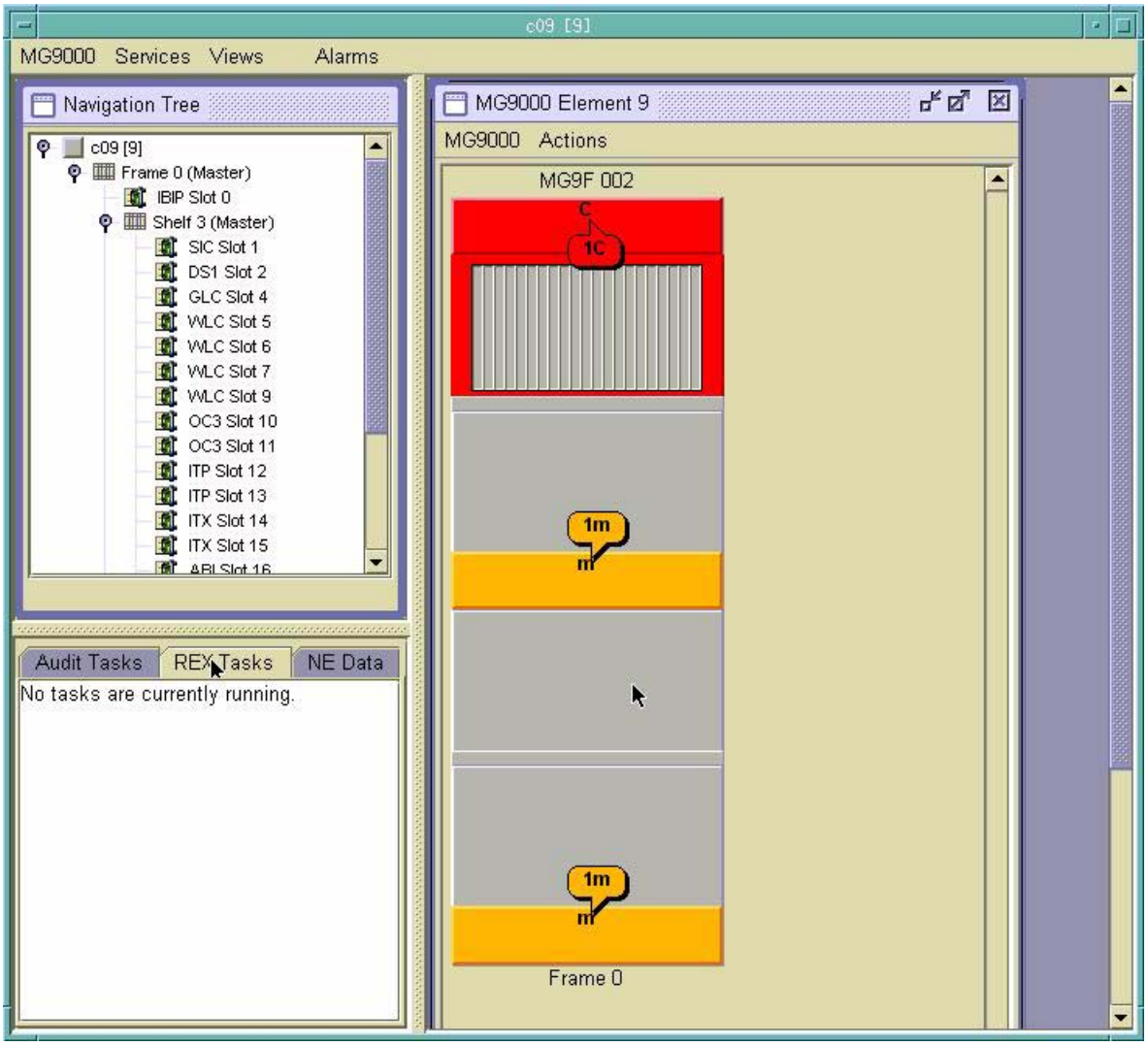


Figure -4 REX tasks tab on NE Specific Desktop View



4.9.2.2.6 GUI release history update

A new submenu item “REX NE” is added to Configuration menu of NE Specific Desktop View

A new tab is introduced on the left panel of NE Specific Desktop View to display the status of REX on the current NE.

4.9.2.2.7 Context sensitive launching information

REX NE option and the REX tasks tab is present only if the EM release is SN09 or higher.

4.9.2.2.8 Supplementary information

None.

4.9.3 CLUI Interface

None

4.10 User interface changes

NA

4.11 OSSGate Interface Changes

None

4.12 Security

NA

4.13 Configuration Walkthrough

None.

5: Configuration (CN): A00008090

5.1 Feature Name

SBA: Alternate Scheduled Closure of Billing Files

5.2 Hardware and Software Requirements

SBA installed and InSv

5.3 Initial Configuration

N/A

5.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

5.5 Upgrade Considerations

5.6 Data schema (DS) (CM, MIBS, RDB)

5.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)

5.6.2 Table/MIB/Remote Database Schema information

5.6.2.1 Name: rcSchFileCloseIntervalValid

5.6.2.1.1 Functional description

To enable the functionality of 'Alternate Scheduled Closure of Billing Files' a new BASE MIB entry namely 'rcSchFileCloseIntervalValid' is introduced. By default the value of this field will be '0'

During the Stream Configuration, user is prompted for

" Do you want Files closed at scheduled intervals from midnight[NO]{NO YES}:"

If user is providing any of the valid values that it has prompted then the MIB variable will get updated. For eg if 'Yes' is suplied then the variable 'rcSchFileCloseIntervalValid' will be set to '1' .

5.6.2.1.2 Usage sequence and implications (CM Only)
N/A

5.6.2.1.3 Size
N/A

5.6.2.1.4 Fields/OIDs
N/A

5.6.2.1.5 Datafill example
N/A

5.6.2.1.6 Table release history update
N/A

5.6.2.1.7 Supplementary information
N/A

5.6.2.1.8 Translation verification and other tools
N/A

5.6.2.2 Name: rcSchFileCloseInterval

5.6.2.2.1 Functional description
A new MIB variable ‘rcSchFileCloseInterval’ is introduced to store the Scheduled Closure Time if the functionality of ’Files closed at scheduled intervals from midnight’ is enabled.

During the Stream Configuration, if user choose ’Yes’ when it is prompted "Do you want Files closed at scheduled intervals from midnight[NO]{NO YES}:" then user will be prompted for providng any of the following options for the Scehduled Time.

Options:

1) Close billing files every 24 hour

2) Close billing files every 12 hour

3) Close billing files every 6 hour

4) Close billing files every 2 hour

5) Close billing files every 1 hour

6) Close billing files every 30 minutes

7) Close billing files every 15 minutes

8) Close billing files every 10 minutes

9) Close billing files every 5 minutes

Scheduled File Closure time Option [5] {1 - 9}:

When user provides any of the valid options that has prompted, the variable 'rcSchFileCloseInterval' will get updated. The default value is '5'.i.e the scheduled rotation will be 1 hour daily.

5.6.2.2.2 Usage sequence and implications (CM Only)

N/A

5.6.2.2.3 Size

N/A

5.6.2.2.4 Fields/OIDs

N/A

5.6.2.2.5 Datafill example

N/A

5.6.2.2.6 Table release history update

N/A

5.6.2.2.7 Supplementary information

N/A

5.6.2.2.8 Translation verification and other tools

N/A

5.6.2.3 Name: rcResetDIRPSeqNumber

5.6.2.3.1 Functional description

This MIB variable is introduced for enabling the functionality of Resetting the DIRP Billing File Sequence Number to '0' at Midnight.

During the Stream Configuration, if the File Format is chosen as 'DIRP , then user will be prompted for

"Do you want the files renamed with close date [NO] {NO YES }:"

If the answer is 'NO' then it will prompt the following.

"Do you want to reset DIRP Sequence Number at Midnight[NO]{NO YES}" :

If user is providing any of the valid values that it has prompted then the MIB variable 'rcResetDIRPSeqNumber' will get updated. For eg if the answer is'YES' then the variable will be set to '1'. The default value of this field is '0'.

5.6.2.3.2 Usage sequence and implications (CM Only)

N/A

5.6.2.3.3 Size

N/A

5.6.2.3.4 Fields/OIDs

N/A

5.6.2.3.5 Datafill example

N/A

5.6.2.3.6 Table release history update

N/A

5.6.2.3.7 Supplementary information

N/A

5.6.2.3.8 Translation verification and other tools

N/A

5.7 Service Orders (SO) (CM & SESM)

N/A

5.8 Software optionality control (SOC)

N/A

5.9 Element Management

N/A

5.10 User interface changes

Figure 1 SBA Stream Configuration (Alternate Scheduled Closure of Billing Files)

Stream Name [] {} : ama

Is this a Filter Stream [NO] {NO YES } :

Stream Record Format [] {SMDR BC CDR300 CDR250 } : BC

File Format Type [] {DNS DIRP } : DIRP

Please specify the logical Volume [/sba/ama] {} :

File Transfer Mode [OUTBOUND] {INBOUND OUTBOUND } :

Do you want the files renamed with close date [NO] {NO YES } :

Do you want to reset DIRP Sequence Number at Midnight[NO]{NO YES}:

Do you want the files closed for file transfer and writetape [YES] {NO YES } :

Do you want DIRP blocks closed based on time [NO] {NO YES } : NO

Do you want Files closed based on a time limit [NO] {NO YES } : NO

Do you want Files closed at scheduled intervals from midnight[NO]{NO YES}: YES

Options:

1) Close billing files every 24 hours

2) Close billing files every 12 hours

3) Close billing files every 6 hours

4) Close billing files every 2 hours

5) Close billing files every 1 hour

6) Close billing files every 30 minutes

Figure 2 SBA Stream Configuration (Alternate Scheduled Closure of Billing Files) Contd....

7) Close billing files every 15 minutes

8) Close billing files every 10 minutes

9) Close billing files every 5 minutes

Scheduled File Closure time option [5] {1 - 9}:

Number of records per day [0] {} :

Maximum Number of records per file [500000] {10000 - 500000} :

Maximum Number of bytes per file [20000000] {1000000 - 2^{1}0000000} :

Figure 3 Change Stream from the billmtc -> CONFSTRM level

Stream Name [AMA] {} :

File Transfer Mode [OUTBOUND] {INBOUND OUTBOUND } :

Do you want the files renamed with close date [NO] {NO YES } :

Do you want to reset DIRP Sequence Number at Midnight [NO] {NO YES } :

Do you want the files closed for file transfer and writetape [NO] {NO YES } :

Do you want DIRP blocks closed based on time [NO] {NO YES } :

Do you want Files closed based on time [NO] {NO YES } :

Do you want Files closed at scheduled intervals from midnight [NO] {NO YES } : YES

Options:

1) Close billing files every 24 hours

2) Close billing files every 12 hours

3) Close billing files every 6 hours

4) Close billing files every 2 hours

5) Close billing files every 1 hour

6) Close billing files every 30 minutes

7) Close billing files every 15 minutes

8) Close billing files every 10 minutes

9) Close billing files every 5 minutes

Scheduled file closure time option [5] {1 - 9} :

Number of records per day [0] {} :

Maximum Number of records per file [500000] {10000 - 500000} :

Maximum Number of bytes per file [20000000] {1000000 - 2^{1}0000000} :

Figure 4 billmtc -> CONFSTRM -> List ama

Stream Name [AMA] {} :

Displaying stream(s) AMA

Stream Name -> AMA

Stream Running status -> YES

Is this a Filter Stream -> NO

Stream Record Format -> BC

File Format Type -> DIRP

Logical Volume Name -> /cbmdata/00/billing/ama

File Transfer Mode -> OUTBOUND

Do you want the files renamed with close date -> NO

Do you want to Reset DIRP Sequence Number at Midnight -> NO

Do you want the files closed for file transfer and writetape -> NO

Do you want DIRP blocks closed based on time -> NO

Do you want Files closed based on time -> NO

Do you want Files closed at scheduled intervals from midnight -> YES

Scheduled File Closure time option -> 5 (every hour)

Maximum Number of records per file -> 500000

Maximum Number of bytes per file -> 20000000

Press Return to Continue...

Figure 5 billmtc -> CONFSTRM -> Delete ama

Stream Name -> AMA

Stream Running status -> NO

Is this a Filter Stream -> NO

Stream Record Format -> BC

File Format Type -> DIRP

Logical Volume Name -> /cbmdata/00/billing/ama

File Transfer Mode -> OUTBOUND

Do you want the files renamed with close date -> NO

Do you want to Reset DIRP Sequence Number at Midnight -> NO

Do you want the files closed for file transfer and writetape -> NO

Do you want DIRP blocks closed based on time -> NO

Do you want Files closed based on time -> NO

Do you want Files closed at scheduled intervals from midnight -> YES

Scheduled File Closure time option -> 5 (every hour)

Maximum Number of records per file -> 500000

Maximum Number of bytes per file -> 20000000

Verifying that no filter streams exist for this stream...

Verifying that no scheduled events exist for this stream

None exist

Are you sure you want to delete the stream? [No] {Yes/No, Y/N} : Y

Press Return to Continue...

5.11 OSSGate Interface Changes

N/A

5.12 Security

N/A

5.13 Configuration Walkthrough

5.13.1 Scheduled Closure of Billing Files

Since the new functionality of ‘closure of billing Files at scheduled intervals from midnight’ is mutually exclusive with the existing functionality of File Closed based on a time limit, this feature can be availed only when the ’File Closed based on a time limit ’ is disabled. That can be achieved by giving ’NO’ when it prompts for " Do you want Files closed based on a time limit [NO] {NO YES } : " during the Stream Configuration

The ’Alternate Schedule Closure of billing File’ feature can be enabled/ activated by giving ‘YES’ when user will be prompted the following during the stream configuration:

Do you want Files closed at scheduled intervals from midnight [NO] {NO YES} :

On enabling this feature, user is prompted with the following time interval options for scheduling the file closure:

Options:

1) Close billing files every 24 hours

2) Close billing files every 12 hours

3) Close billing files every 6 hours

4) Close billing files every 2 hours

5) Close billing files every 1 hour

6) Close billing files every 30 minutes

7) Close billing files every 15 minutes

8) Closes billing files every 10 minutes

9) Close billing files every 5 minutes

Scheduled File Closure time option [5] {1 - 9}:

By default, the files will be rotated an hourly (1 Hr) basis. Users can set any one of the options prompted depending on their requirement

5.13.2 Reset DIRP Sequence Number at Midnight

During the Stream Configuration, if user chooses the DIRP file format and if user is not choosing the functionality of renaming the file based on close date. That means if user is choosing 'NO' to the prompt

'Do you want the files renamed with close date [NO] {NO YES } :' then user will be prompted the following.

"Do you want to reset DIRP Sequence Number at Midnight[NO]{NO YES}:"

If the answer to the above prompt is 'YES' then the functionality will be enabled.

Figure 6 SBA Stream Configuration (Reset DIRP Sequence Number at Midnight)

Stream Name [] {} : ama

Is this a Filter Stream [NO] {NO YES } :

Stream Record Format [] {SMDR BC CDR300 CDR250 } : BC

File Format Type [] {DNS DIRP } : DIRP

Please specify the logical Volume [/sba/ama] {} :

File Transfer Mode [OUTBOUND] {INBOUND OUTBOUND } :

Do you want the files renamed with close date [NO] {NO YES } :

Do you want to reset DIRP Sequence Number at Midnight[NO]{NO YES}:YES

Do you want the files closed for file transfer and writetape [YES] {NO YES } :

Do you want DIRP blocks closed based on time [NO] {NO YES } : NO

Do you want Files closed based on time [NO] {NO YES } : NO

Do you want Files closed at scheduled intervals from midnight[NO]{NO YES}: YES

Figure 7 SBA Stream Configuration (Reset DIRP Sequence Number at Midnight) contd...

Options:

1) Close billing files every 24 hours

2) Close billing files every 12 hours

3) Close billing files every 6 hours

4) Close billing files every 2 hours

5) Close billing files every 1 hour

6) Close billing files every 30 minutes

7) Close billing files every 15 minutes

8) Close billing files every 10 minutes

9) Close billing files every 5 minutes

Scheduled File Closure time option [5] {1 - 9}:

Number of records per day [0] {} :

Maximum Number of records per file [500000] {10000 - 500000} :

Maximum Number of bytes per file [20000000] {1000000 - 20000000} :

6: Configuration (CN): A00008522

6.1 Feature Name

SESM Support for SIP Lines

6.2 Hardware and Software Requirements

This feature requires the 905-240 GWC card, pec code NTRX51DL. It also requires that the CM, GWC SESM and MCS gateways are on a SN09 load.

6.3 Initial Configuration

6.3.1 SESM-CS2K Prov Mgr EM Server Configuraion

In the SESM, the /opt/nortel/NTsesm/admin/bin/configure tool should be used to configure SESM access to the Session Server Element Manager (SS-EM).

The configuration tool will prompt the user to enter the following:

- Transport protocol to SS-EM server (http/https - default is https). In SN09, only HTTPS is supported by the SS-EM, however flexibilty to choose HTTP is provided to meet possible future needs.
- IP address / host name of primary SS-EM server
- IP address / host name of secondary SS-EM server. Some configurations may not include a secondary SS EM server. If so, configure the same information provided for the primary server (by default this should be the case).
- HTTP/HTTPS communication port to SS EM server (default 8080 for http, 8443 for https).
- The OPIClient version. This is mapped to the SS EM load version. In SN09, the appropriate value will be “9.0”. The OPIClient version should be incremented each release in steps of 1.0 i.e, 9.0, 10.0...15.0
- SS-EM Provisioning Manager administrator user name
- SS-EM Provisioning Manager administrator password

The IP address and port will be used to generate the SS-EM Provisioning Manager URL which in turn will be added to sesm.properties file.

As part of the configuration, the IP address will be validated for format, range and reachability. Other user entered data will be validated for format, range, values etc.

The user name will be added to sesm.properties as clear text.

The password will be stored separately and accessible only to the root user.

All configuration information (url, username, etc.) except password can be displayed by using the SESM "/opt/nortel/NTsesm/admin/bin/configure" tool.

6.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

6.5 Upgrade Considerations

TBD.

6.5.1 Dump and Restore (CM)

Not Applicable.

6.5.2 Element Management Upgrade

The MSM gateway is new to SN09. Upgrading from SN08 or fresh install of SN09 will add the required fields necessary to support the MSM Gateway.

6.5.3 Downgrade impact

No impact - works as per current process.

6.6 Data schema (DS) (CM, MIBS, RDB)

6.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SERVRINV	CHANGED	N/A
LGRPINV	CHANGED	N/A
LNINV	CHANGED	N/A
GWC-PROFILE_MIB	CHANGED	N/A
NORTEL-GWC-COMMON-TC	CHANGED	N/A

6.6.2 Table/MIB/Remote Database Schema information

6.6.2.1 Name: SERVRINV

Server Inventory

6.6.2.1.1 Functional description

In SN09, the field TERM_EXEC_TC_TAB of the table SERVRINV includes DPLEX with a DLP termtype for GWCs defined with Large_LineNA_v2 and Large_LineINTL_v2 GWC profiles.

6.6.2.1.2 Usage sequence and implications (CM Only)

The table SERVRINV is provisioned by the SESM. No manual datafill or change is allowed. Manual changes to this table will cause data corruption.

6.6.2.1.3 Size

Not applicable.

6.6.2.1.4 Fields/OIDs

Not applicable. This feature will use an already defined and supported field.

6.6.2.1.5 Datafill example

The following example shows sample datafill for table SERVRINV:

GWC 167 IP 47 4 4 4 DPL DPLEX POTS POTSEX KEYSET KSETEX $ NORTHAA $ NET_IP Y $ $

6.6.2.1.6 Table release history update

Not applicable.

6.6.2.1.7 Supplementary information

Not applicable.

6.6.2.1.8 Translation verification other tools

Not applicable.

6.6.2.2 Name: LGRPINV

Logical Group Inventory

6.6.2.2.1 Functional description

In SN09, the field GRPTYPE of the table LGRPINV is set to “SSDPL” for SIP; logical groups will be used to indicate that the logical group is assigned to a CS2K SS gateway.

6.6.2.2.2 Usage sequence and implications (CM Only)

The table LGRPINV is provisioned by the SESM. No manual datafill or change is allowed. Manual changes to this table will cause data corruption.

6.6.2.2.3 Size

Not applicable.

6.6.2.2.4 Fields/OIDs

Not applicable. This feature will use an already defined and supported field.

6.6.2.2.5 Datafill example

The following example shows sample datafill for table LGRPINV.

Preprovisioned SIP Lines : SITE 00 0 GWC 3 DPL_GRP $

Where SITE represents an entry from the table SITE in the CM.

6.6.2.2.6 Table release history update
Not applicable.

6.6.2.2.7 Supplementary information
Not applicable.

6.6.2.2.8 Translation verification other tools
Not applicable.

6.6.2.3 Name: LNINV
Line Inventory

6.6.2.3.1 Functional description
There are no software/functional changes to table LNINV. This section will describe the datafill.

```
(GRPTYPE SITE)  SITE                        4 char name

(GRPTYPE DPL_GRP) FRAME NUMBER              {0 TO 511}

(GRPTYPE DPL_GRP) LINE SUBGROUP             {0 TO 9}

(GRPTYPE DPL_GRP) SLOT                      {00 TO 10}

(GRPTYPE DPL_GRP) CIRCUIT                   {00 TO 99}*

*00 - 23 when SLOT = 10
```

6.6.2.3.2 Usage sequence and implications (CM Only)
Entries will be automatically configured by SESM at MSM gateway provisioning time.

6.6.2.3.3 Size
Not applicable.

6.6.2.3.4 Fields
Not Applicable.

6.6.2.3.5 Datafill example
The following example shows sample datafill for table LNINV.

Preprovisioned SIP line (North American):

SITE 00 0 21 31 RDTLSG PKLNL HASU N NL N NIL

Preprovisioned SIP line (International):

SITE 00 0 21 31 GWLPOT PKLNL HASU N NL N NIL

6.6.2.3.6 Table release history update
Not applicable.

6.6.2.3.7 Supplementary information
Not applicable.

6.6.2.3.8 Translation verification other tools
Not applicable.

6.7 Service Orders (SO) (CM & SESM)
No new service orders are created under this activity, however several new options are defined which can be used in NEW/CHF commands applicable to SIP lines hosted off of MSM VMGs.

All listed may also be used via the Bulk Provisioning Tool.

6.7.1 Service order change details
LCC and options

(SESM)
A new SIP_DATA option is introduced by this feature. The SIP_DATA option is a SERVORD+ option which is not presented to XACore SERVORD (it is removed from the command prior to XACore SERVORD command processing).

6.7.1.1 Option Format:
SIP_DATA sub-options-and-values $

where

sub-options = SIP_CLIENT_TYPE, SIP_URI, SIP_PASSWD, SIP_PACKAGE, SIP_LOCATION

The SIP_DATA option and sub-option **tags** (but not their values, see later restrictions) may be entered in either lower or upper case transparently.

> ***Note:*** sub-option values have external case restrictions. See "Usage/ Format Validation and Rules" in a subsequent section.

6.7.1.2 Sub-option value formats:
SIP_CLIENT_TYPE option value format = {one or more token_string_values}

SIP_URI option value format = {token_string_value, format uservalue@domainnamevalue}

SIP_PASSWD option value format = {token_string_value}

SIP_PACKAGE option value format = {one or more token_string_values}

SIP_LOCATION option value format = {one or more token_string_values}

6.7.1.3 SIP_DATA Sub-option and Value Examples:

"SIP_DATA SIP_PACKAGE test package $"

"SIP_DATA SIP_PACKAGE test package SIP_URI someone@somecompany.com $"

"SIP_DATA SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD test1password $"

6.7.1.4 Usage/Format Validation and Rules

OSSGate/SERVORD+ SIP_DATA validation will be limited. SessionServer-EM will be responsible for validating the actual value contents.

6.7.1.4.1 Rules Enforced for SIP Data by OSSGate/SERVORD+

Breaking these rules causes immediate command failure/rejection by OSSGate/SERVORD+:

- One or more sub-options are REQUIRED when the SIP_DATA option is specified.
- Sub-option tags are reserved words and may not be used as values for other sub-options or for any non-related types (eg. CM customer group, gateway names, etc.). For example, “SIP_PASSWORD sip_password” is an invalid option and value pair. “sip_password” may not be used as the value specified for the SIP_PASSWORD sub-option. “sip_password” may not be used as a part or whole value for any other sub-option (e.g. “SIP_LOCATION sip_passwd” will be rejected).
- The SIP_DATA terminator, “$”, is a reserved token and may not be used as a value of any SIP_DATA sub-option. If a sub-option is present in the SIP_DATA options list, then it must have a valid value other than “$”.
- The tag-value pair relationship for the options/sub-options will be enforced from a simple format perspective. All sub-options must have associated values. The overall SIP_DATA option must be terminated by a “$”.
- Multiple/extraneous SIP_DATA options or sub-options found in a single NEW/CHF/etc command, will result in rejection of the command by OSSGate/SERVORD+.
- SIP_URI must be of the format user@domain. The domain information is parsed from the URI value. A missing domain (e.g. missing @ delimiter or domain information) will cause immediate command failure. An invalid

domain name specified will be rejected by the Session Server Provisioning Manager.

- SIP_LOCATION must be included in the SIP_DATA option when the command issued results in the creation of a new user on the Session Server. In SN09, this applies only to the NEW command.

6.7.1.4.2 Rules NOT Explicitly Enforced for SIP Data by OSSGate/SERVORD+

These rules are not explicitly enforced by OSSGate/SERVORD+. Breaking these rules may cause command failures or other unintended consquences:

- SIP_DATA and the associated sub-option tags are reserved words and may not be used as values for any non-related types (eg. CM customer group, gateway names, etc.). Use of the reserved keywords in this manner may cause unexpected problems when attempting to use OSSGate/SERVORD+ for provisioning ANY type of line.
- CHF commands affecting SIP_DATA on SIP lines requires that gateway/termination names (or associated LEN) be used in the command instead of DN. Use of DN will result in the command being processed only by the CM, which is undesirable when SIP_DATA is present in the command.
- Use of the SIP_DATA option is not supported in commands which do not affect SIP lines or in commands which are not supported for flowthrough **for** SIP lines. Use of the SIP_DATA option in these commands may cause unintended command failures.
- The SIP_DATA option may fall anywhere in the command string except as the first token (which is reserved for the command name), however it is ***highly recommended*** that the SIP_DATA option be placed in the normal option field range of the command.
- The values assigned to sub-options SIP_CLIENT_TYPE, SIP_PACKAGE, and SIP_LOCATION are ***automatically normalized to lower case by OSSGate/SERVORD+*** (e.g. SIP_CLIENT_TYPE value “SIP Line” received at OSSGate will be normalized to “sip line” prior to transfer to the Session Server Provisioning Manager). **When commissioning these associated values on the Session Server Provisioning Manager, you MUST use lower case text.** Failure to commission these values in the Session Server Provisioning Manager using lower case text will result in command failures at OSSGate/SERVORD+.
- SIP_URI is normalized to lower case by the Session Server Provisioning Manager when received from OSSGate/SERVORD+. Caseless comparisons are performed by the Session Server Provisioning Manager when determining if a URI entered at OSSGate is already in use (e.g. “Slynch@Nortel.com” is considered identicle to “slynch@nortel.com” from the Session Server Provisioning Manager’s perspective). Only the normalized/lower-case URI is stored by the Session Server Provisioning

Manager (e.g. “USERname1@Domain1.net” received from OSSGate/ SERVORD+ would be stored as “username1@domain1.net” in the Session Server Provisioning Manager).

6.7.1.5 Data Mapping Example

In the following command,

LEN: MSM1 00 0 00 00

is mapped to

VMG: TestMSMVMG.1

termination/endpoint: MSM1/000/0/0000

OSSGate command:

NEW $ 9195200500 IBN PRADEFAULT 0 0 LATA1 0 MSM1 00 0 00 00 + DPL Y 10 SIP_DATA SIP_PACKAGE test package SIP_PASSWD + test1Password SIP_URI someone@somecompany.com + SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP $ $

XACore SERVORD command derived from OSSGate command:

NEW $ 9195200500 IBN PRADEFAULT 0 0 LATA1 0 MSM1 00 0 00 00 + DPL Y 10 $

Data sent to SS-EM:

VMG: TestMSMVMG.1

termination: MSM1/000/0/0000

Domain: somecompany.com

User: someone

Password: test1Password

firstName: SIPLineUser (default value)

lastName: SIPLineUser (default value)

Package: test package

locale: English (default value)

timezone: Eastern Standard Time (default value)

clientType: SIP Line

DN: 9195200500

location: Nortel Networks.RTP

status: ACTIVE (default value)

6.7.2 New commands

Not Applicable.

6.7.3 Line equipment format changes

6.7.3.1 LEN

No LEN format changes are introduced by this feature. Typical LEN format for SS LENs:

SITE FFF G TT tt

SITE = SITE name

FFF = frame number, 0-511

G = group number, 0-9

TT tt = terminal, 00 00 - 10 23

6.7.3.2 Media gateway endpoint format

No gateway/endpoint format changes are introduced by this feature. Typical SS VMG and endpoint formats:

VMG = 64 character free-form string (eg. TestSSVMG.1)

endpoint/termination = SITE/FFF/G/TTtt

where SITE, FFF, G, and TTtt value are as specified in the SS LEN format.

- The LEN's individual TT tt values will always be zero-padded to 2 digits when converted to an endpoint/termination name (e.g. TT tt value "2 7" would be converted to an endpoint/termination TTtt value of "0207").
- The LEN's FFF value will always be zero-padded to 3 digits (e.g. FFF value "6" would be converted to endpoint/termination FFF value "006").

6.8 Software optionality control (SOC)

6.9 Element Management

SESM

6.9.1 New/modified GUIs

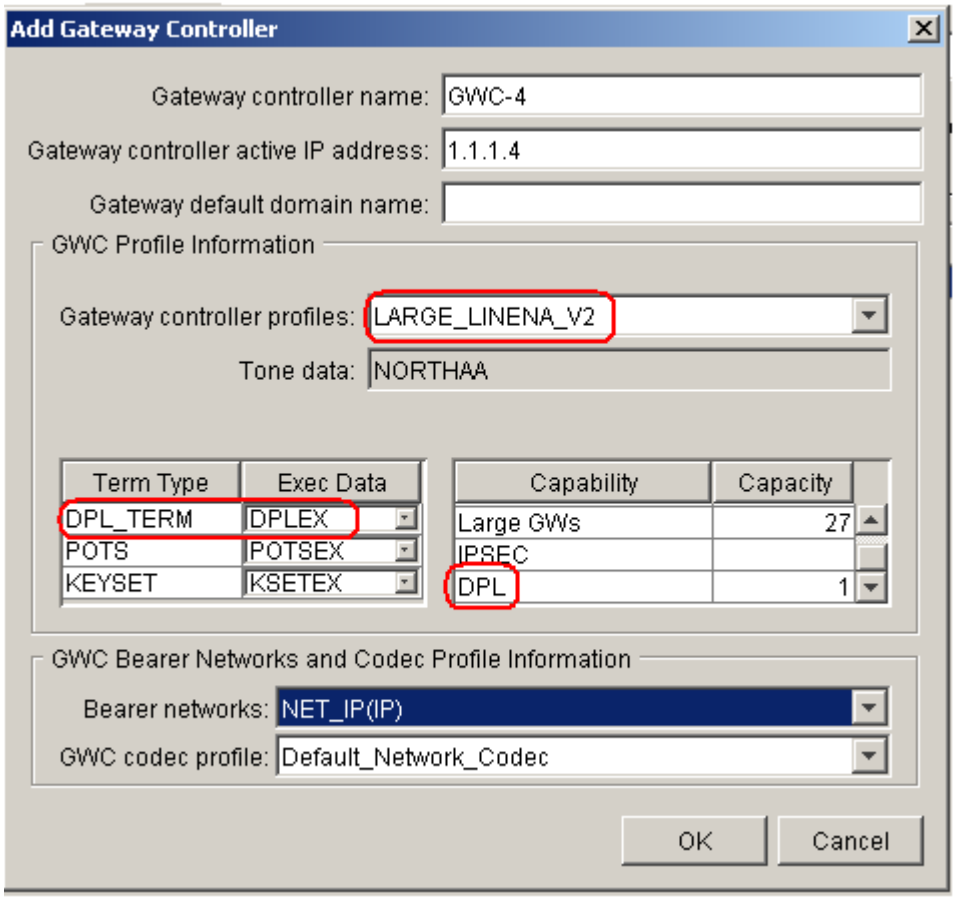
Table 2 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Associate Gateway	**CHANGED**
Change Gateway	**CHANGED**
View Current Audits	**NEW**
Line Data Integrity Audit	**NEW**
Run Audit	**CHANGED**

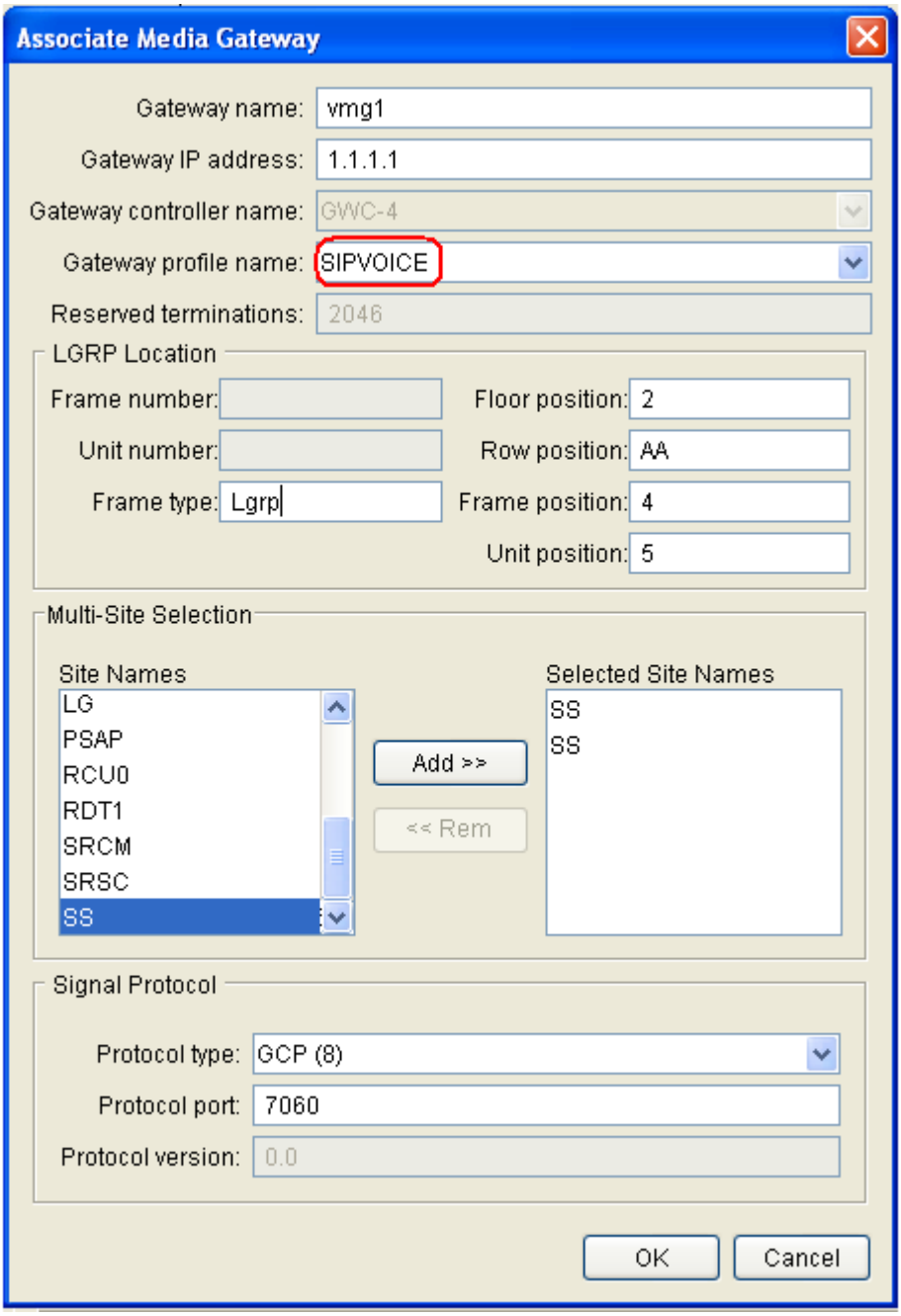
6.9.2 GUI information

6.9.2.1 GUI Name: Add GWC

GWCs for CS2K Session Server gateways are provisioned using either the Large_LineNA_v2 or Large_LineINTL_v2 GWC profile. These GWC profiles will cause a GWC to be added to the CM, table SERVRINV, with the exec lineup of DPLEX/DPL, POTSEX/POT and KSETEX/KEYSET)refer to diagram below).


Add Gateway Controller
Gateway controller name: GWC-4
Gateway controller active IP address: 1.1.1.4
Gateway default domain name:
GWC Profile Information
Gateway controller profiles: LARGE_LINENA_V2
Tone data: NORTHAA
Term Type
Exec Data
DPL_TERM
DPLEX
POTS
POTSEX
KEYSET
KSETEX
Capability
Capacity
Large GWs
27
IPSEC
DPL
1
GWC Bearer Networks and Codec Profile Information
Bearer networks: NET_IP(IP)
GWC codec profile: Default_Network_Codec
OK
Cancel

6.9.2.2 GUI name: Associate Gateway



6.9.2.2.1 Functional description

Adding a GW involves identifying a gateway name, IP address and selecting the MSM profile from the Gateway profile name list. The MSM selection causes a Multi-Site Selection panel to appear.

The LGRP Location panel is used to provide the physical equipment location of the GW. LGRP_type is a string. Floor position, frame position and unit positions are all integers while row position is a char ‘A’ - ‘Z’, ‘AA’ or ‘AB’.

Below the LGRP Location panel is the Multi-Site Selection panel. Within this panel is a Site Names list and a Selected Site Names list. The Site Names list consists of all of the site names from table SITE in the CM. Site names are selected (placed in the Selected Site Name list) by simply clicking on the site name and selecting Add.

For SN09, a maximum of 12 site names can be selected.

Each site name represents one LGRP as defined by:

<site>/frame/group

Each LGRP is provisioned in table LGRPINV (CM) and represents 1023 endpoints. Each endpoint is added to table LNINV as:

<site> frame group terminal

where the terminal number ranges from 00 00 to 10 22.

The Root Zone Selection panel is used to provision middleboxes.

The reserved termination field is updated once the OK button is selected. The entries in the Signal Protocol panel are fixed (cannot be changed).

Note: Adding a fully provisioned CS2KSS GW will take about 45 mins (12 LGRPs).

Note: Provisioning SIP GWs can only be performed one at a time. Attempts to provision multiple SIP GWs at the same time may cause all provisioning sessions to fail.

6.9.2.2.2 GUI usage and implications

This GUI is used only to add an MSM gateway.

6.9.2.2.3 GUI size

Not applicable.

6.9.2.2.4 GUI fields

The Multi site Selection panel is only visible if the MSM profile is selected from the Gateway Profile list.

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Site Names	New	none	Site name values from the CM	Site Names	None
Selected Site Names	New	none	Site names selected from the Site Name list	Selected Site Names	None

6.9.2.2.5 Usage example

There are two ways to access the above Associate Gateway GUI:

- From the CS2000 Management Tools GUI, select Configuration from the top menu and select Associate Media Gateway from the pull down
- From the Gateway tab, in the lower portion of the GUI, select the "Associate.." button

From the Associate Gateway panel:

1. Add the gateway name - up to 64 characters, can be "." or "/" delineated,
2. Input the IP address of the MSM Service Manager,
3. If the Associate Gateway panel was opened via the CS2000 Management Tools menu bar then the Gateway Controller name will need to be entered,
4. Select MSM from the Gateway profile name. The Site name box will disappear and will be replaced with a Multi Site Selection panel.
5. From the list of Site Names on the left, select a site name then clich on the "Add" button. This will add the site name to the Selected Site Name list on the right. For SN09, a maximum of 6 entries can be on the right side. These entries can be the same or different (same site name can be used multiple times). These site names will be used to name the line groups (LGRPs).
6. If a site name was selected in error, from the list on the right, select the site name and the "Rem" button. This will remove the site name from the list on the right.
7. The protocol, version and port have been defaulted, no changes are needed

8. Select OK to start the process. The association process may take up to 15 minutes. This process includes adding a GW to the GWC, adding a LGRP to table LGRPINV in the CM, adding the endpoints to the GWC, then adding the LENs to LNINV in the CM. The LGRP addition process is repeated until all selected LGRPs have been added.

6.9.2.2.6 GUI release history update
Modification to the Associate Gateway GUI

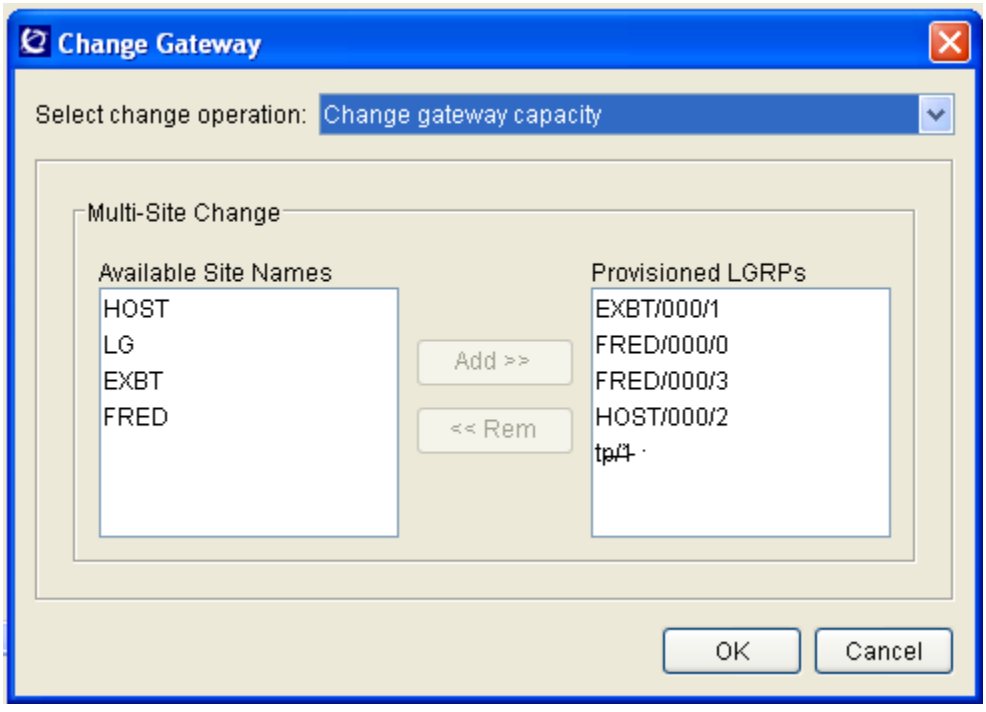
6.9.2.2.7 Context sensitive launching information
Not impacted, no changes

6.9.2.2.8 Supplementary information
None

6.9.2.2.9 CLUI Interface
No impact.

6.9.2.3 GUI name: Change Gateway

6.9.2.3.1 Functional description
This GUI allows the user to change the capacity of a gateway - this capability currently exists. Should the gateway be a MSM, a different Change Gateway GUI is presented.



A gateway using the MSM profile will have a dialog box in displayed. Similar to the AssocGW dialog box, this box contains two lists, Available Site Names on the left, which is a list of site names from the table SITE in the CM.

The second list, “Provisioned LGRPs”, is a list of site names already used and assigned. These site names have LGRPs and LENs assigned to it, therefore they show up with there respective frame and group numbers.

From this dialog box, the user can add additional site names (a maximum of 6 LGRP/Site names) are permitted in the Provisioned LGRPs list.

Additionally, the user can select to remove LGRP/Site names from the provisioned list simply by selecting them and the remove button.

Once the site names have been added, and OK selected, this diialog box will close and another panel will appear to display the progress and responses. The first item to display is the timeout value.

Cancel will close the box without executing any operation.

> ***Note:*** currently only single operations may be performed from thie Change Gateway dialog; in other words, the user cannot add one site and remove another site in the same operation.

6.9.2.3.2 GUI usage and implications

6.9.2.3.3 GUI fields

Table 4 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Site Names	New	none	Site name values from the CM	Site Names	None
Selected Site Names	New	none	Site names selected from the Site Name list	Selected Site Names	None

6.9.2.3.4 Usage example - Removing an LGRP

Reference the above figure, if the user wishes to remove HOST/000/2 from the currently configured, the following steps are performed:

1. From the Provisioning panel, Gateway Tab, click on the MSM gateway (there should only be one).

2. Select the Change button from the bottom of the Gateway Tab. A Change dialog box opens.
3. From the Change Dialog, the pull down, select Change Gateway Capacity
4. The above dialog box opens.
5. The user selects HOST/000/2 from the Provisioned LGRPs List, then selects the Rem. This will remove the HOST/000/2 from the Provisioned LGRPs List and place in the Available Site Names List.
6. Click on the OK and the operation will begin.
7. A Status box will open and indicate the expected time that the operation may take. This box will also indicate any success or error encountered during this operation.

6.9.2.3.5 Usage example - Adding an LGRP

Reference the above figure, if the user wishes to add another FRED LGRP/site name, the following steps are performed:

1. From the Provisioning panel, Gateway Tab, click on the MSM gateway (there should only be one).
2. Select the Change button from the bottom of the Gateway Tab. A Change dialog box opens.
3. From the Change Dialog, the pull down, select Change Gateway Capacity
4. The above dialog box opens.
5. The user selects FRED from the Available Site Names List, then selects the Add. This will add FRED from the Provisioned LGRPs List.
6. Click on the OK and the operation will begin.
7. A Status box will open and indicate the expected time that the operation may take. This box will also indicate any success or error encountered during this operation.

6.9.2.3.6 Usage example - Cancel

At any time, the user may cancel the pending operation without executing the operation. Simply select Cancel.

6.9.2.3.7 GUI release history update

Not Applicable.

6.9.2.3.8 Context sensitive launching information

Not impacted, no changes.

6.9.2.3.9 Supplementary information

Not Applicable.

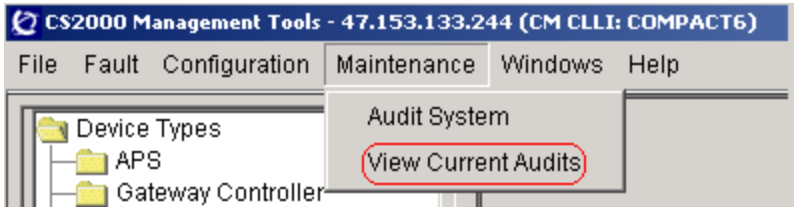
6.9.2.3.10 CLUI Interface

No Impact.

6.9.2.4 GUI name: View Current Audits

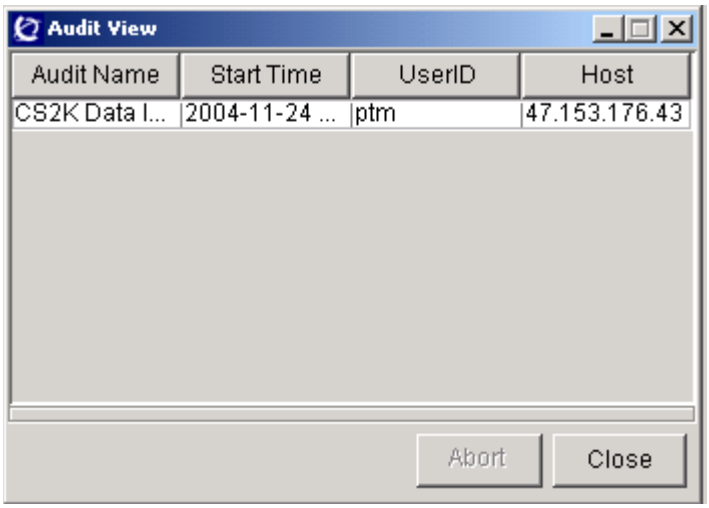
6.9.2.4.1 Functional description

- Add a new menu in Maintenance of Cs2kmt to provide the new function “Abort Audit”.



When user selected the menu “View Current Audits”, another new gui will be displayed. Detail info refer to the following gui.

- Add a new gui to provide the new function “Abort Audit”.



The running audits will be displayed in this gui. The datas of the audits include: Audit Name, Start Time, UserID, Host.

User can selected a running sudit and press the “Abort” button to abort the audit.

6.9.2.4.2 GUI usage and implications

This GUI is used only to view and abort the running audits.

6.9.2.4.3 GUI size

Not applicable

6.9.2.4.4 GUI fields

Not applicable

6.9.2.4.5 Usage example

From the CS2000 Management Tools GUI, select Maintenance from the top menu and select Audit System from the pull down.

6.9.2.4.6 GUI release history update

Add a new gui to view and abort the running audits.

6.9.2.4.7 Context sensitive launching information

Not impacted.

6.9.2.4.8 Supplementary information

None

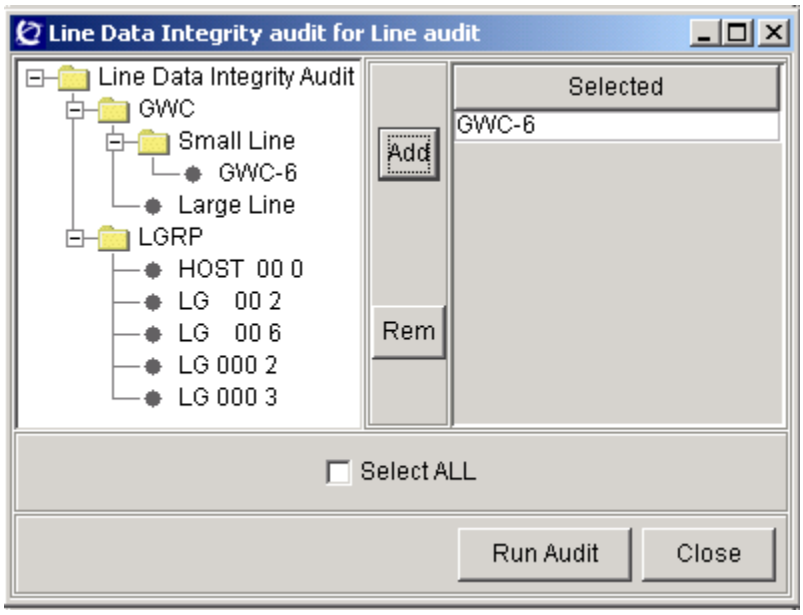
6.9.2.4.9 CLUI Interface Not Impacted

6.9.2.5 GUI name: Line Data Integrity Audit

6.9.2.5.1 Functional description

- Add a new gui to provide support for audit by GWCs, GWs or LGRPs. Only support Line Data Integrity audit now.

When user select “Line Data Integrity Audit” and press the “Run Audit” button in Audit System gui, the following gui will be displayed.



User can selected the GWCs, GWs or LGRPs in the left tree and add them to the right table by press the “->” button.

The button “<-” is used to delete the data that user selected in the right table.

User can select all datas to do audit by select checkbox “Select All”.

After user selected the data and press “Run Audit” button, the audit will be run as before.

6.9.2.5.2 GUI usage and implications
This GUI is used only to provide support for running line audit per GWCs, GWs, or LGRPs.

6.9.2.5.3 GUI size
Not Applicable.

6.9.2.5.4 GUI fields
Not Applicable.

6.9.2.5.5 Usage example
From the CS2000 Management Tools GUI, select Maintenance from the top menu and select Audit System from the pull down.

6.9.2.5.6 GUI release history update
Add a new gui to provide support for running line audit per GWCs, GWs, or LGRPs.

6.9.2.5.7 Context sensitive launching information
Not impacted.

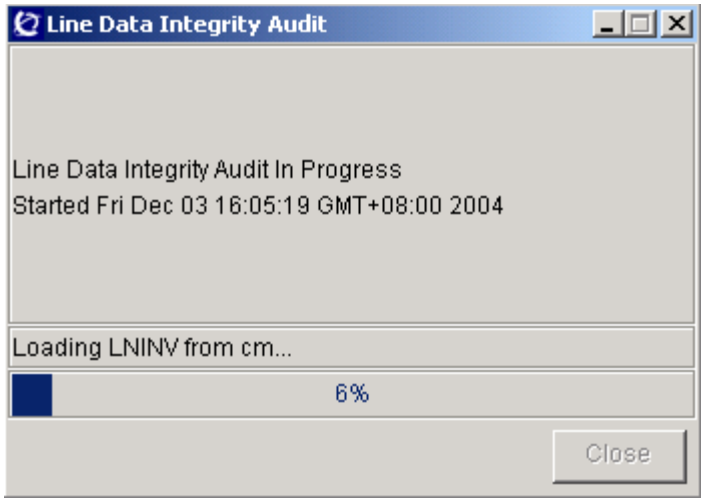
6.9.2.5.8 Supplementary information
None

6.9.2.5.9 CLUI Interface Not Impacted

6.9.2.6 GUI name: Run Audit

6.9.2.6.1 Functional description

6.9.2.6.2 GUI usage and implications
This GUI is used only to provide support for indicating process of running audit.



The progress bar was used to indicate the progress of the running audit.

The label was used to show the current operation.

6.9.2.6.3 GUI size
Not Applicable

6.9.2.6.4 GUI fields
Not Applicable

6.9.2.6.5 Usage example
From the CS2000 Management Tools GUI, select Maintenance from the top menu and select Audit System from the pull down.

6.9.2.6.6 GUI release history update
Add a new gui to provide support for indicating process of running audit.

6.9.2.6.7 Context sensitive launching information
Not impacted.

6.9.2.6.8 Supplementary information
None

6.9.2.7 CLUI Interface
Not Impacted

6.10 User interface changes
Not Applicable

7: Configuration (CN): A00008601

7.1 Feature Name

IW-SPM-IP Fully Provisionable Codec Lists for G.711/G.729

7.2 Hardware and Software Requirements

This functionality requires SN09 load in the Call Server, IW-IP CEM and GEM RM.

7.3 Initial Configuration

Not Applicable

7.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable

7.5 Upgrade Considerations

7.5.1 Dump and Restore (CM)

During the upgrade[ONP] from SN07/SN08 to SN09, in the following two cases the DFCODEC and PRFCODEC values will convert as shown:

Figure 1 Case1: DFCODEC-G711ULAW, PRFCODEC-NONE, RFC2833-

```
Before upgrade [SN07/SN08]:
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
--------------------------------------------------------------------------
IWSPM G711ULAW NONE 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
BOTTOM

After upgrade [SN09]:
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
--------------------------------------------------------------------------
IWSPM G729 G711ULAW 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
BOTTOM
```

ENABLE

Figure 2 Case 2: DFCODEC-G711ALAW, PRFCODEC-NONE, RFC2833-

```
Before upgrade [SN07/SN08]:
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
------------------------------------------------------------------------
IWSPM G711ALAW NONE 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
BOTTOM

After upgrade [SN09]:
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
------------------------------------------------------------------------
IWSPM G729 G711ALAW 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
BOTTOM
```

ENABLE.

7.6 Data schema (DS) (CM, MIBS, RDB)

7.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MNIPPARM	CHANGED	UNCHANGED

7.6.2 Table/MIB/Remote Database Schema information

7.6.2.1 Name: MNIPPARM

Multiservice Node Internet Protocol PARaMeters.

7.6.2.1.1 Functional description

Table MNIPPARM contains customer provisionable parameters applicable to the IW IP SPM peripheral. This table has no logical dependencies on other tables and each tuple is applicable to all SPMs of the specified type (i.e. all parameters in the tuple for IWSPM apply to every IW IP SPM configured as a BRIDGE ONLY SPM in the office).

7.6.2.1.2 Usage sequence and implications (CM Only)

There are no requirement to datafill tables in a specific order. However, the values specified in MNIPPARM will have no meaning unless an SPM of the IWIPBRG type is datafilled and operational in the office.

7.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNIPPARM	Unchanged	Unchanged	Unchanged

7.6.2.1.4 Fields

The following table lists fields for table MNIPPARM.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
MNKEY	Unchanged	None	IWSPM, DPTSPM	T_MNPARM_KEY. This is the tuple key, no default value provided.
DFCODEC	**Changed**	**None**	**G711ALAW, G711ULAW, G729**	**DEFAULT_CODEC. This specifies the default codec to be used in call processing. The default offered is G711ULAW.** **As part of this feature G729 can be provisioned as DFCODEC**
PRFCODEC	**Changed**	**None**	**NONE, G729, G711ALAW, G711ULAW**	**PREFERRED_CODEC. This specifies the preferred codec to be used in call processing. The default offered is NONE.** **As part of this feature G711ALAW or G711ULAW can be provisioned as PRFCODEC**
PKTRATE	Unchanged	None	10, 20	PACKETIZATION_RATE. This specifies the packetization rate in milliseconds to be used for voice packets. The default offered is 10.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
INGRESS	Unchanged	None	-6 TO 6	GAIN. This specifies the gain to be applied to the ingress side of the call. The default offered is 0.
EGRESS	Unchanged	None	-6 TO 6	GAIN. This specifies the gain to be applied to the egress side of the call. The default offered is 0.
JITMIN	Unchanged	None	0 TO 300	JITTER. This specifies the minimum jitter setting in milliseconds. The default offered is 100.
JITMAX	Unchanged	None	0 TO 300	JITTER. This specifies the maximum jitter setting in milliseconds. The default offered is 100.
JITTARG	Unchanged	None	0 TO 300	JITTER. This specifies the target jitter setting in milliseconds. The default offered is 100.
ECAN	Unchanged	ECHOLOSS, ECHOTAIL	ENABLE, DISABLE	STATUS. This specifies if Echo Cancellation is active or inactive. The default offered is DISABLE. The following subfields are given when ENABLE is specified.
		ECHOLOSS	0, 3, 6	ECHO_RETURN_LOSS. This subfield specifies the loss on the echo return signal.
		ECHOTAIL	16, 24, 32, 64, 96, 128	ECHO_TAIL_LENGTH. This subfield specifies the echo tail length in milliseconds.
VOICE	Unchanged	None	OFF, CONSERV, AGGRESS	VOICE_DETECTION. This specifies the level of voice detection. The default offered is OFF.
CMFNOISE	Unchanged	None	ENABLE, DISABLE	CMFNOISE. This specifies if comfort noise is provided. The default offered is DISABLE.
T38	Unchanged	None	ENABLE, DISABLE	T38. This specifies if T38 fax is supported. The default offered is DISABLE.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RFC2833	Unchanged	None	ENABLE, DISABLE	RFC2833. This specifies if RFC2833 is supported. The default offered is DISABLE.
RTCP	Unchanged	INTERVAL	N,Y	RTCP. This specifies if RTCP is active. The default offered is N.
		INTERVAL	1 TO 60	INTERVAL. This subfield specifies the RTCP interval when field RTCP is set to Y.
TONESET	Unchanged	None	NORTHAMERICA,SPAIN,UK,FRANCE,PORTUGAL,BELGIUM,GERMANY,NETHERLANDS,SWEDEN,AUSTRIA,ITALY,SWITZERLAND,AUSTRALIA,BRAZIL,IRELAND,MEXICO,ISRAEL,ROMANIA,TURKEY,CZECH,CHINA,TAIWAN,KOREA,JAPAN,PANAMA,ARGENTINA,GREECE,POLAND,NEWZEALAND,SINGAPORE,VENEZUELA,CHILE,HONGKONG,MALAYSIA,PHILIPPINES,THAILAND,INDIA	TONESET. This specifies the unique tonset to be utilized based on the resident country. The default offered in NORTHAMERICA.
LOGINT	Unchanged	None	1 TO 120	LOGINT. This specifies the log interval. The default offered is 5.
CRCERROR	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for CRC error logs. The default offered is 20, 10.
USIZEPKT	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the undersize packet logs. The default offered is 20, 10.
OSIZEPKT	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the oversized packet logs. The default offered is 20, 10.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FRAGMENT	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the fragments logs. The default offered is 20, 10.
JABBER	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the jabber logs. The default offered is 20, 10.
DROPEVNT	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the drop event logs. The default offered is 20, 10.
BRDCAST	Unchanged	RISE, FALL	0 T0 100	MNPARM_THRESHOLD. This specifies the settings for the broadcast logs. The default offered is 20, 10.
JITTER	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the jitter logs. The default offered is 20, 10.
LATENCY	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the latency logs. The default offered is 20, 10.
VPKTLOST	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the voice packets lost logs. The default offered is 20, 10.
MINLOG	Unchanged	None	0 TO 1000000	LOG_REPORT_MIN_VOLUME. This specifies the minimum packet volume for log reporting. The default offered is 1000.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OMPARMS	Unchanged	RTPLOSTE, JTREXC, LATEXC	1 TO 100, 1 TO 3000, 1 TO 3000	OMPARMS. This specifies operational measurement parameters. RTPLOSTE specifies the threshold value of RTP packets lost for pegging a particular OM. JTREXC specifies the threshold jitter value for pegging a particular OM. LATEXC specifies the threshold latency value for pegging a particular OM.
DIFFSERV	Unchanged	EF_CODEPOINT	6-bits as ASCII, prefixed by “CP” for CodePoint, ie:CP101110	The codepoint for voice band defaults to CP101110
	Unchanged	EF_PRIORITY	0 TO 7	The priority for voice defaults to 6
	Unchanged	CS5_CODEPOINT	6-bits as ASCII, prefixed by “CP” for CodePoint, ie: CP101000	The codepoint for signalling data defaults to CP101000
	Unchanged	CS5_PRIORITY	0 TO 7	The priority for signalling defaults to 6
MEDINTEG	Unchanged	None	ENABLE or DISABLE	Indicates the state of Media Integrity on this GEM card, defaults to DISABLE

7.6.2.1.5 Datafill example

The following example shows sample datafill for table MNIPPARM.

Figure 3 Datafill for table MNIPPARM

```
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
------------------------------------------------------------------------
IWSPM G729 G711ULAW 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
BOTTOM
```

Codec information is already provisionable in default codec[DFCODEC] and preferred codec[PRFCODEC] fields of MNIPPARM table. This feature only adds new values to support full provisioning of codec.

Following new values are added in default codec and preferred codec fields in MNIPPARM table as shown in Figure 4, “New codec values.’

Table 4 New codec values.

Field	Entry values prior to this feature	Entry values after this feature.
DFCODE	G711ALAW, G711ULAW	G711ALAW, G711ULAW, G729
PRFCODEC	NONE, G729	NONE, G729, G711ALAW, G711ULAW

Provisioning of both DFCODEC and PRFCODEC fields with the same values are blocked. The error message is displayed as shown in Figure 4, “Error msg display when same value given to both DFCODEC and PRFCODEC fields.’

Figure 4 Error msg display when same value given to both DFCODEC and PRFCODEC fields.

```
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
------------------------------------------------------------------------
IWSPM G711ULAW NONE 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
>cha
>JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
DFCODEC: G711ULAW
>G711ULAW
PRFCODEC: NONE
>G711ULAW
.........
.........
.........
.........
ERROR: DFCODEC and PRFCODEC values should be unique.
TUPLE TO BE CHANGED:
IWSPM G711ULAW G711ULAW 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE
ENABLE N NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
20 10 1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
```

Provisioning of both DFCODEC and PRFCODEC fields with the G711 values are blocked. The error message is displayed as shown in Figure 4, “Error msg display when same value given to both DFCODEC and PRFCODEC fields.’

Figure 5 Error msg display when G711 given in both DFCODEC and PRFCODEC fields.

```
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
------------------------------------------------------------------------
IWSPM G711ULAW NONE 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
>cha
>JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
DFCODEC: G711ULAW
>G711ULAW
PRFCODEC: NONE
>G711ALAW
.........
.........
.........
.........
ERROR: Both DFCODEC and PRFCODEC should not have G711 value.
TUPLE TO BE CHANGED:
IWSPM G711ULAW G711ALAW 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE
ENABLE N NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
20 10 1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
```

Following combinations are allowed to provision in DFCODEC and PRFCODEC fields of MNIPPARM table.

Table 5 DFCODEC and PRFCODEC in MNIPPARM table.

Preferred codec	Default codec
None	G711ALAW
None	G711ULAW
None	G729
G711ALAW	G729
G711ULAW	G729
G729	G711ALAW
G729	G711ULAW

7.6.2.1.6 Table release history update

Table MNIPPARM was created in the SN06 software release.

7.6.2.1.7 Supplementary information

None.

7.6.2.1.8 Translation verification and other tools

MNIPPARM does not use translation verification tools.

8: Configuration (CN): A00008629

8.1 Feature Name

GEM-II AAL2 IW-SPM SN09 Core Preparation Work

8.2 Hardware and Software Requirements

Since AAL2 IW-SPM is a new product introduction, there will be no discussion of how to upgrade an AAL1 or IP IW-SPM to AAL2.

8.3 Initial Configuration

1. To initially configure an AAL2 IW-SPM, first equip an IW-SPM with two NTLX82BA or later CEM packs in slots 7 and 8, and NTLZ20DA GEM-II packs in slots 9 and 10. Only the lower shelf will be used; no other cards should appear on the lower shelf (e.g. No DSP cards since GEM-II has built-in DSP). The upper shelf should be empty.
2. Equip 4 ENET links to each CEM. Four will be needed to realize a capacity 2016 bridges on the IW-SPM (less than 2016 if ECAN used).
3. Plug in OC3 SFP (Small Form Pluggable) connector into the front of each GEM-II card, then connect the SONET TX/RX fibers to this connector. Other end of fiber will connect to AAL2 port on a Passport.
4. Datafill following tables in the order given:
5. Insure network is mu-law as used in North America. A-law (for International) is not currently supported for ATM AAL2.
6. Office parm ECAN_EDGE_STRATEGY in OFCENG should be set to "Y" (same as needed for IP) so DPT GWCs, MG4Ks, and line GWCs will request ECAN on the IW-SPM.
7. Office parm AAL2_ATM_ENABLE in OFCENG should be set to "Y" so NTLZ20DA ATM RM can be added to an AAL2 IW-SPM.
8. CLLI: add ENET_TO_AAL2 tuple with ADMININF ENET_TO_AAL2_POOL.
9. BEARNETS: add an AAL2 network fabric.
10. NETBRDGE: add an ENET_TO_AAL2 BRDGCLLI that connects TDM_ENET to ATM_AAL2 with DISPLAY of E_A2.
11. NETPATH: specify path that will use the desired bridge by adding this tuple: "2 (ENET_TO_AAL2) $"
12. NET2NET: show that ENET and AAL2 can connect by changing CONNNETS of NET_AAL2 tuple to: "(TDM_ENET 2) $".
13. MNNODE: add an IW class SPM that is BRDG_ONLY with BRDGCLLI of ENET_TO_AAL2.

14. MNSHELF: add lower and upper NTLX51BA shelves to a NTLX91BA frame; the lower shelf will house the CEM and ATM packs for the IW-SPM, while the upper shelf will remain empty.

15. MNPRTGRP: add ATM_GRP and STS3L_GRP protection groups with revertive N+1 sparing for the IW-SPM.

16. PMLOADS: add AL2xxx load for the AAL2 NTLZ20DA. Insure IWSxxx load available for CEM cards on the IW-SPM.

17. MNCKTPAK: add two NTLX82BA (or later) CEMs in slots 8 and 9. Add two NTLZ20DA GEM-II packs in slots 7 and 8 with AL2xxx load name.

18. ENCDINV: add four ENET crosspoints for the IW-SPM.

19. MNLINK: add four C-side ENET links for the IW-SPM.

20. MNATMIF: add AAL1 and AAL2 parameters by adding a new tuple for IW-SPM.

21. MNMGPIP: add IP over AAL5 signalling info by adding a new tuple for IW-SPM.

22. MNIPPARM: add DIFFSERV for IP over AAL5 signalling by addiing a new tuple for IW-SPM.

23. MNHSCARR: add the 5 ATM carriers to the IW-SPM: two OC3S, two STS3L, and one STS3cP.

24. MAPCI;MTC;NET;SHELF <nn>;CARD <nn> BSY/RTS front and back of the ENET card, then BSY/RTS the 4 ENET links to the IW-SPM.

25. MAPCI;MTC;PM;POST SPM <nn>;SELECT CEM 0: BSY/ LOADMOD/RTS each CEM card.

26. MAPCI;MTC;PM;POST SPM <nn>;SELECT ATM 0; BSY/ LOADMOD/RTS each ATM RM.

27. MAPCI;MTC;TRKS;CARRIER;POST SPM <nn>;BSY/RTS the five ATM carriers on the IW-SPM, finishing with the STS3cP carriers which will create the bridges.

28. MAPCI;MTC;APPL;BRGMTCE;POST SPM <nn>;BSY ALL;RTS ALL to RTS the bridges on the 4 C-side ENET links and make the bridges available for CallP.

8.4 Office/Subnet parameters (OP/SP) (CM & SESM)

CM

8.4.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	AAL2_ATM_ENABLE	New	CM

8.4.2 Parameter information

8.4.2.1 AAL2_ATM_ENABLE

Enable AAL2 ATM bearer fabric over IW-SPM with NTLZ20DA GEM-II card.

8.4.2.1.1 Functional description

The AAL2_ATM_ENABLE parameter is required to enable the AAL2 ATM IW-SPM feature, which utilizes the new NTLZ20DA GEM-II card. The parameter is disabled by default. While disabled, the user will not be allowed to datafill an ATM RM with NTLZ20DA PEC code. When enabled, the datafill is allowed.

Here's the warning message shown when user enables this parm:

WARNING: Ensure that production IWSxxx and AL2xxx local loads'

are available for AAL2 IW-SPM before LoadMod/RTS.'

and here's the info message shown when parm is disabled:

INFO: Will no longer be able to datafill AAL2 IW-SPM.

Reason for parm is to control introduction of this new feature where the Core part will be available first in SN09, followed by the Local part in SN10. Once the production IWSxxx AL2xxx loads are available in SN10, this parameter can be enabled by customers wanting to deploy ATM AAL2 traffic.

8.4.2.1.2 Provisioning rules

User should insure that a working/verified AL2xxx load is available before enabling this parameter. Should only be enabled for mu-law networks (i.e. North America). The AAL2 IW-SPM feature does not currently support A-law (e.g. for International).

8.4.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
N	Y	N

8.4.2.1.4 Activation
Immediate activation. No restart required.

8.4.2.1.5 Dependencies
MNCKTPAK: will not be allowed to datafill NTLZ20DA as ATM RM until this parameter is enabled.

8.4.2.1.6 Consequences
None.

8.4.2.1.7 Verification
Confirm NTLZ20DA can be datafilled as ATM RM.

8.4.2.1.8 Memory requirements
No memory impact.

8.4.2.1.9 Parameter release history update
None.

8.5 Upgrade Impact

8.5.1 Dump and Restore
None. Parameter will default to “N” when dumping from pre-SN09 loads to SN09 or later loads.

8.5.2 Element Management Upgrade
None

8.6 Data schema (DS) (CM, MIBS, RDB)

8.6.1 New/modified tables, MIBs, or Database Schema

Table 3 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
NETBRDGE	Changed	Unchanged
MNCKTPAK	Changed	Unchanged

Table 3 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MNATMIF	Changed	Unchanged
MNMGPIP	Changed	Unchanged
MNIPPARM	Changed	Unchanged

8.6.2 Table/MIB/Remote Database Schema information

8.6.2.1 Name: NETBRDGE

Network Fabric Bridges

8.6.2.1.1 Functional description

Existing table.

8.6.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS

NETBRDGE

NETPATH

NET2NET

MNNODE

8.6.2.1.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NETBRDGE	0	15	Memory is automatically allocated for 16 tuples.

8.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for NETBRDGE.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BEARNETS	Changed	none	Select two tuples from table BEARNETS.	Allows selection of the two interfacing network types. For AAL2 IW-SPM, this would be TDM_ENET to NET_AAL2.

8.6.2.1.5 Datafill example

The following example shows sample datafill for table NETBRDGE, NETPATH, and NET2NET:

```
TOP
         BRDGCLLI    BRDGTYPE DISPLAY           BEARNETS
-----------------------------------------------------------
     ENET_TO_AAL2 CORE_BRDGE     E_A2 TDM_ENET NET_AAL2
       ENET_TO_IP CORE_BRDGE     E_IP TDM_ENET   NET_IP
BOTTOM

TOP
PATHIDX                                    NETBRDGE
-----------------------------------------------
       0                                          $
       1                        (       ENET_TO_IP)$
       2                        (     ENET_TO_AAL2)$
BOTTOM

TOP
BNETNAME
                                                                                CONNNETS
--------------------------------------------------------------------------------------
TDM_ENET
                                                  (  NET_IP    1) (NET_AAL2    2)$
  NET_IP
                                                                  (TDM_ENET    1)$
NET_AAL2
                                                                  (TDM_ENET    2)$
BOTTOM
```

8.6.2.1.6 Table release history update

Modify NETBRDGE to allow AAL2 network type.

8.6.2.1.7 Supplementary information

Cannot delete a tuple in NETBRDGE until all references to it in MNNODE have been deleted.

Cannot change a tuple network type to/from AAL2 until all references to in MNNODE have been deleted.

8.6.2.1.8 Translation verification other tools

The following example shows the output from MAPCI when it is used to verify Table NETBRDGE.

mapci;mtc;pm;post spm <nn>

```
 XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
Baseln  RExByp  NO AMA    .     3 SPM  5   RS    .     205C..  1 Maj  ATM_8+
  M              *C*            *C*    *C*             *C*     M      *C*
                                SysB    ManB    OffL    CBsy    ISTb    InSv
 0 Quit         PM                1       0      25       0      11      28
 2 Post_        SPM               0       0       2       0       7       0
 3 ListSet
 4 ListRes   SPM    8  ISTb  Class: IW        BRG_Only  NETBRDGE: E_A2
 5 Trnsl
 6           Shlf0 SL A Stat  Shlf0 SL A Stat  Shlf1 SL A Stat  Shlf1 SL A Stat
 7 ATMConn   -----  1 - ----  CEM 1  8 I ISTb  -----  1 - ----  -----  8 - ----
 8 IPConn    -----  2 - ----  ATM 0  9 A ISTb  -----  2 - ----  -----  9 - ----
 9 OfClk     -----  3 - ----  ATM 1 10 I SysB  -----  3 - ----  ----- 10 - ----
10           -----  4 - ----  ----- 11 - ----  -----  4 - ----  ----- 11 - ----
11 Disp_     -----  5 - ----  ----- 12 - ----  -----  5 - ----  ----- 12 - ----
12 Next      -----  6 - ----  ----- 13 - ----  -----  6 - ----  ----- 13 - ----
13 Select_   CEM 0  7 A ISTb  ----- 14 - ----  -----  7 - ----  ----- 14 - ----
14 QueryPM
15 ListAlm
16 Clock
17 SPERFORM
18 Upgrade_
  RLYNCH4
```

8.6.2.2 Name: MNCKTPAK

SPM Circuit Pack

8.6.2.2.1 Functional description

Existing table.

8.6.2.2.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

MNNODE

MNCKTPAK

ENCDINV

8.6.2.2.3 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNCKTPAK	0	?	Memory is dynamically allocated.

8.6.2.2.4 Fields/OIDs

The following table lists fields/OIDs for MNCKTPAK.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PEC	Changed	none	NTLZ20DA	Specifies the new GEM-II pack that can operate as AAL2 (for ATM RM) or IP (for GEM RM)
LOAD	Changed	none	AL2nnnn GM2nnnn	Select valid tuple from table PMLOADS. New AL2nnnn load for AAL2 ATM, or new GM2nnnn load for IP GEM.

8.6.2.2.5 Datafill example

The following example shows sample AAL2 datafill for table MNCTKPAK.

```
        CPKKEY                                                    CPKINFO
                        PEC  RELEASE       LOAD
SPM  8 0  9 ATM 0 1 WORKING (SYSB CR RPT) (MANB MJ RPT)
              (ISTB MN RPT) (PROTFAIL CR RPT) (PATCHFAIL MJ RPT) $
              NTLZ20DA       01    AL220AD
SPM  8 0 10 ATM 1 1 SPARE (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT)
              (PROTFAIL CR RPT) (PATCHFAIL MJ RPT) $
              NTLZ20DA       01    AL220AD
```

and this shows sample of NTLZ20DA configured a IP GEM:

```
TOP
        CPKKEY                                                    CPKINFO
                        PEC  RELEASE       LOAD
-------------------------------------------------------------------------
SPM  0 0  9 GEM 0 1 WORKING (SYSB CR RPT) (MANB MJ RPT)
              (ISTB MN RPT) (PROTFAIL CR RPT) (PATCHFAIL MJ RPT) $
              NTLZ20DA       01    GM221BG
SPM  0 0 10 GEM 1 1 SPARE (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT)
              (PROTFAIL CR RPT) (PATCHFAIL MJ RPT) $
              NTLZ20DA       01    GM221BG
```

8.6.2.2.6 Table release history update

Modify MNCKTPAK to allow NTLZ20DA GEM-II pack for GEM (IP) and ATM (AAL2) RM types.

8.6.2.2.7 Supplementary information

For GEM RMs, the NTLZ20DA acts as a replacement for the earlier NTLZ20BA and NTLZ20CA packs which are being discontinued due to parts obsolesence. Standard upgrade practice is used to go from NTLZ20BA/CA to the newer DA: BSY GEM, change PECCODE to NTLZ20DA and LOAD to GM2xxxx, LoadMod, RTS GEM.

For ATM RMs, the NTLZ20DA is allowed on IW-SPM class node assigned as BRDG_ONLY with BEARNETS field (in MNNODE) that supports AAL2 fabric. OFCENG parameter AAL2_ATM_ENABLE must be enabled before NTLZ20DA can be assigned as an AAL2 ATM RM.

8.6.2.2.8 Translation verification other tools

The following example shows the output from MAPCI when it is used to verify Table MNCKTPAK.

mapci;mtc;pm;post spm <nn>;select atm <n>

```
            XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
Baseln   RExByp   NO AMA     .       3 SPM   5    RS     .      205C..    1 Maj   ATM_8+
  M                *C*              *C*      *C*                *C*       M       *C*
                                    SysB     ManB     OffL     CBsy     ISTb     InSv
 0 Quit          PM                   1        0       25        0       11       28
 2               SPM                  0        0        2        0        7        0
 3 ListSet         ATM                1        0        0        0        1        0
 4
 5            SPM 8    ATM 0    Act    ISTb
 6 Tst
 7 Bsy        Loc : Row M  FrPos 40 ShPos  6 ShId 0 Slot  9   Prot Grp : 1
 8 RTS        Default Load: AL220AD                          Prot Role: Working
 9 OffL
10 LoadMod
11
12 Next
13 Select_
14 QueryMod
15 ListAlm
16 Prot
17 SPERFORM
18
  RLYNCH4
```

Here's an example for the GEM RM:

mapci;mtc;pm;post spm <nn>;select gem <n>

```
 XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
Baseln   RExByp   NO AMA     .      3 SPM   5   RS     .      205C..   1 Maj   ATM_8+
  M                *C*              *C*     *C*              *C*       M       *C*
                                     SysB    ManB    OffL     CBsy     ISTb     InSv
 0 Quit           PM                  1       0       25       0        11       29
 2                SPM                 0       0        2       0         7        0
 3 ListSet          GEM               0       0        1       0         1        0
 4
 5            SPM    0 GEM   0  Act    ISTb
 6 Tst
 7 Bsy        Loc : Row N  FrPos 31 ShPos  6 ShId 0 Slot  9   Prot Grp : 1
 8 RTS        Default Load: GM221BG                          Prot Role: Working
 9 OffL
10 LoadMod
11
12 Next
13 Select_
14 QueryMod
15 ListAlm
16 Prot
17
18
  RLYNCH
```

8.6.2.3 Name: MNATMIF

SPM ATM Protocol Interface Parameters

8.6.2.3.1 Functional description

Existing table that specified AAL1 ATM protocol parameters. Adding AAL2 ATM protocol parameters. An AAL2 RM will need both the AAL1 and AAL2 protocol parameters.

8.6.2.3.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

MNLINK

MNATMIF

MNMGPIP

8.6.2.3.3 Size

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNATMIF	0	86	Memory is dynamically allocated as each ATM node is added.

8.6.2.3.4 Fields/OIDs

The following table lists fields/OIDs added to table MNATMIF for AAL2 IW-SPMs.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CIDPRSVC	New	none	1..247	Specifies the maximum number of AAL2 CIDs that may be allocated on an AAL2 SVC. The local node may allocate no more than this number of trunks. Default value is 10. Note: value used in IW-SPM will be 10 (despite setting here) till a follow-up notice issued indicated IW-SPM will follow this table value.
PRECREAT	New	none	Y or N	Specifies whether Pre-creation of SVCs is enabled. If svcPreCreation is enabled, then an SVC set up is initiated when the bandwidth available in existing VCCs (between two NSAP addresses) is such that a new SVC would be required for the next call. Default Y for enabled.
TIMERCU	New	none	0..15875 nsec in 125 usec steps	Maximum period of time in usec (micro seconds) before a partially filled AAL2 packet is scheduled for transmission. Default 0 usec. Note 1000 usec = 1 msec.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SVCHOLD	New	none	0..600 sec in 1 sec steps	Length of time that an AAL2 SVC is kept up after the last narrowband call to use it has been deleted. This attribute is used to modify the SVC caching system. Longer values result in larger caches of SVCs. Default 180 sec to match PVG.
SRVCAT	New	none	CBR (Constant Bit Rate) or VBR (Variable Bit Rate)	ATM Service Category for SVC. Default is VBR.
PKCLRT	New	none	0..353207	Peak cell rate of the ATM connection on a per SVC basis. Default is 800 cells per sec.
SUSTCR	New	none	0..353207	Sustained cell rate of the ATM connection on a per SVC basis. Default is 800 cells per sec
MAXBURSZ	New	none	0..353207	Maximum burst size of the ATM connection on a per SVC basis. This “burst” defines how far beyond PKCLRT the connection will go before cells are dropped. Default is 0 cells
REMADDR	New	none	40 character address	ATM address of the node that may be reached.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CODEC	New	none	G711 (other values to be added in future)	Type of on-board CODEC in-use. Allows up to 16 different CODECs to be specified. Default is G711.
SILSUP	New	none	Y or N	Whether silence suppression is enabled or not. Default is Y for enabled.
MAXBRI	New	none	0..2016	Max number of bridges provided by an AAL2 IW. If silence suppression (SILSUP) is disabled, the max bridges possible is 1865. Allows telco to limit the traffic over an AAL2 IW-SPM. Default is 2016.

8.6.2.3.5 Datafill example

The following example shows sample datafill for table MNATMIF.

ATMKEY

ATMDATA

SPM 8

V40 PRIV BOTH 1 2300 8 16 255 32 2048 2048 PASSPORT RTPH_SPM_8 Y USER N NSAP

39345678901234567890A4A4A4F402F678901200 4 25 67 16 2048 2048 1000 2000 7000

15000 750 180 4 30 30 4 4 10 110 110 4 Y 0 180 VBR 800 800 0

39345678901234567890A4A4A4F402F678901201 Y G711 Y 2016

8.6.2.3.6 Table release history update
Modify MNATMIF to add AAL2 protocol parameters.

8.6.2.3.7 Supplementary information

Cannot CHAnge or DELete a tuple for AAL2 IW-SPM unless that node is OOS.

8.6.2.3.8 Translation verification other tools

None

8.6.2.4 Name: MNMGPIP
SPM IP Protocol Parameters

8.6.2.4.1 Functional description
Existing table. Normally applies to IP nodes, but AAL2 IW-SPM needs it to specify parameters for IP over AAL5 signalling.

8.6.2.4.2 Usage sequence and implications (CM Only)
Tables must be datafilled in the following sequence:

MNATMIF

MNMGPIP

MNHSCARR

8.6.2.4.3 Size

Table 10 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNMGPIP	0	86	Memory is dynamically allocated as each IP/AAL2 node is added.

8.6.2.4.4 Fields/OIDs
The following table lists fields/OIDs for MNMGPIP.

Table 11 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GEMSIGIP	Changed	none	same	Change to allow this field for AAL2 IW-SPM.
SIGMASK	Changed	none	same	Change to allow this field for AAL2 IW-SPM.
SIGGWIP	Change	none	same	Change to allow this field for AAL2 IW-SPM.

8.6.2.4.5 Datafill example

The following example shows sample datafill for table MNMGPIP.

```
            MGPKEY
          GEMSIGIP           SIGMASK           SIGGWIP
-------------------------------------------------------------------
       SPM  0 0  9
   172  16 121  11  255 255 255   0  172  16 121   1
       SPM  0 0 10
   172  16 121  11  255 255 255   0  172  16 121   1
```

8.6.2.4.6 Table release history update

Modify MNMGPIP to add AAL2 parameters.

8.6.2.4.7 Supplementary information

Cannot CHAnge or DELete a tuple for AAL2 IW-SPM unless that node is OOS.

8.6.2.4.8 Translation verification other tools

None.

8.6.2.5 Name: MNIPPARM

SPM IP Protocol Parameters

8.6.2.5.1 Functional description

Existing table. Normally applies to IP nodes, but AAL2 IW-SPM needs it to specify parameters for IP over AAL5 signalling.

8.6.2.5.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

MNMGPIP

MNIPPARM

MNHSCARR

8.6.2.5.3 Size

Table 12 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNIPARM	0	86	Memory is dynamically allocated once when first .

8.6.2.5.4 Fields/OIDs

The following table lists fields/OIDs for MNIPPARM.

Table 13 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DIFFSERV	Changed	none	same	Change to allow this field for AAL2 IW-SPM.

8.6.2.5.5 Datafill example

The following example shows sample datafill for table MNIPPARM.

```
MNKEY  DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG
         ECAN   VOICE CMFNOISE     T38 RFC2833 RTCP      TONESET LOGINT
CRCERROR USIZEPKT OSIZEPKT FRAGMENT  JABBER DROPEVNT BRDCAST  JITTER LATENCY
VPKTLOST  MINLOG         OMPARMS              DIFFSERV
              MEDINTEG
-------------------------------------------------------------------------------
IWSPM G711ULAW     NONE      10       0      0      0    100       0
     DISABLE      OFF  DISABLE DISABLE  ENABLE   N  NORTHAMERICA      5
  20  10   20  10   20  10   20  10  20  10   20  10  20  10  20  10  20  10
  20  10    1000  50  1000  1000 CP101110 6 CP101000 6
             DISABLE
```

8.6.2.5.6 Table release history update

Modify MNIPPARM for AAL2 IW-SPM.

8.6.2.5.7 Supplementary information

Cannot CHAnge or DEL ete an IW-SPM tuple unless all IW-SPM nodes are OOS.

8.6.2.5.8 Translation verification other tools

None.

8.7 Service Orders (SO) (CM & SESM)

None.

8.8 Software optionality control (SOC)

No SOC. Feature activation will be controlled thru AAL2_ATM_ENABLE office parameter in OFCENG.

8.9 Element Management

None

8.10 Command interface changes

IWCOMMCI is the only user tool changed by this feature. Two designer-only tools are also impacted (IWBMCI and IWSELCI), but they will not be covered in this user section.

8.10.1 Directory: IWCOMMCI

8.10.1.1 Directory description

Resident tool for commissioning and IW-SPM.

8.10.1.2 Accessing directory: IWCOMMISSION

8.10.1.2.1 Access to directory or MAP level and return to CI

To access IWCOMMISSION from the CI environment, enter IWCOMMCI.

To return to the CI environment, enter QUIT.

8.10.2 Command: BSY_IW

8.10.2.1 Command type: NON-MENU

8.10.2.2 Command target: All

8.10.2.3 Command availability: RES

8.10.2.4 Command description

Manually Busy bridges on a select ENET link on the IW-SPM.

8.10.2.5 Command syntax

Table 14 BSY_IW command parameters and variables

Command	Parameters and variables
BSY_IW	<SPM number> (0..85) ~~<Bridging type> (ATM, IP)~~ <Link number> (0..3) <Keep CPB calls up> (KEEP, KILL)
Parameters and variables	Description
Link number	The ENET link on the IW-SPM
Keep CPB calls up	Whether bridges with CPB calls should remain up or busied out. Optional parameter that defaults to KILL

The only change to the BSY_IW command is removal of the “Bridging type” parameter. The system will now rely on the setting in MNNODE’s BEARCLLI field to determine if the IW-SPM is ATM AAL1, ATM AAL2, or IP.

No change to the output of these commands, so no further info needs to be provided.

8.10.3 Command: RTS_IW

8.10.3.1 Command type: NON-MENU

8.10.3.2 Command target: All

8.10.3.3 Command availability: RES

8.10.3.4 Command description

Manually Return-to-Service bridges on a select ENET link on the IW-SPM.

8.10.3.5 Command syntax

Table 15 BSY_IW command parameters and variables

Command	Parameters and variables
RTS_IW	<SPM number> (0..85) ~~<Bridging type> (ATM, IP)~~ <Link number> (0..3)

Table 15 BSY_IW command parameters and variables

Command	Parameters and variables
Parameters and variables	Description
Link number	The ENET link on the IW-SPM

The only change to the RTS_IW command is removal of the “Bridging type” parameter. The system will now rely on the setting in MNNODE’s BEARCLLI field to determine if the IW-SPM is ATM AAL1, ATM AAL2, or IP.

No change to the output of this command, so no further info needs to be provided.

8.11 SECURITY

None.

8.12 Configuration Walkthrough

Earlier section on “Initial Configuration” describes the equipment and provisioning required to setup this feature. Setting up CallP to route calls over IW-SPM bridges has not changed (same as IP and AAL1 ATM), so it will not be covered here.

9: Configuration (CN): A00009011

9.1 Feature Name

TOPS Internet Protocol (IP) Security Enhancements

9.2 Hardware and Software Requirements

This feature does not introduce any new hardware requirements.

This feature requires new loads in the IP-XPM (SX05DA) and in the NT7X07AA. These loads interpret and act on the SNMP and Telnet configuration data downloaded from new datafill in the CM.

The applicable loads are as follows:

- IP-XPM (SX05DA): QTP22
- 7X07AA: TGWYM004

9.3 Initial Configuration

The new SNMP settings have default values such that behavior of the IP-XPM (SX05DA) and 7X07AA is unchanged following an upgrade from a pre-SN09 (TOPS22) load to an SN09 or higher load. For security, however, Telnet on a 7X07AA is always disabled following an upgrade from a pre-SN09 (TOPS22) load to an SN09 or higher load.

9.4 Office parameters (OP)

This feature adds four new office parameters. These office parameters affect 7X07AA cards defined in Table IPINV as TOPS IPGWs (`GW_TYPE` = `TOPS`). These parameters do not affect non-TOPS IPGWs.

When the craftsperson modifies these parameters, the Succession core displays the following warnings:

- This parameter applies to TOPS IPGWs only.
- All IPGWs must be reloaded for this change to take effect.

9.4.1 New/modified office parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management)
OFCENG	IPGW_SNMP_COMMUNITY_NAME	New	CM
OFCENG	IPGW_SNMP_MANAGER	New	CM
OFCENG	IPGW_SNMP_ENABLED	New	CM
OFCENG	IPGW_TELNET_ENABLED	New	CM

9.4.2 Parameter information

9.4.2.1 IPGW_SNMP_COMMUNITY_NAME

Internet Protocol Gateway Simple Network Management Protocol Community Name

9.4.2.1.1 Functional description

This parameter allows the craftsperson to configure one SNMP community name for SNMP read, write, and trap operations on the 7X07AA.

9.4.2.1.2 Provisioning rules

The craftsperson defines the community name (up to 16 characters) then datafills it in Table OFCENG, using single quotes to allow entry of lowercase letters or non-alphanumeric symbols.

9.4.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
One letter, digit, or non-alphanumeric symbol	Sixteen letters, digits, non-alphanumeric symbols, or any combination thereof	The string “public” (lowercase, and without the quotation marks) is the default. This is a customary default community name, and it is what currently deployed 7X07AAs use.

9.4.2.1.4 Activation

The new community name does not take effect on a 7X07AA until the card is PMRESET from the MAPCI;MTC;PM level. For all cards to be updated, all cards must be PMRESET. This should be done sequentially using the existing IPGW DRAIN command such that traffic is off-loaded (drained) from each 7X07AA before the card is PMRESET. This minimizes the effect on calls in progress.

9.4.2.1.5 Dependencies
None.

9.4.2.1.6 Consequences
This parameter should be set to a value other than “public.” If the parameter is set to “public” it is easier for a hacker to guess the community name and use SNMP to modify data on the 7X07.

9.4.2.1.7 Verification
To verify the change, the craftsperson can update the community name on their SNMP manager client, then attempt SNMP operations on the changed 7X07AAs. If the SNMP operations succeed, the new community name is in use by the 7X07AAs.

9.4.2.1.8 Memory requirements
20 bytes

9.4.2.1.9 Parameter release history update
SN09 (TOP22): Creation

9.4.2.2 IPGW_SNMP_MANAGER
Internet Protocol Gateway Simple Network Management Protocol Manager

9.4.2.2.1 Functional description
This parameter allows the craftsperson to configure the IP address of one SNMP manager (also known as a trap manager). The 7X07AA cards will send traps to this IP address.

Prior to SN09 (TOPS22), the 7X07AA allowed entry of up to four SNMP manager IP addresses. The default SNMP manager is obtained using DHCP, while up to three additional SNMP managers can optionally be defined using PMDEBUG on the 7X07AA. This feature allows a fifth SNMP manager IP address to be configured.

9.4.2.2.2 Provisioning rules
The craftsperson datafills the IPv4 address in Table OFCENG. The IPv4 address consists of four numbers, each in the range 0 to 255.

9.4.2.2.3 Range information

Table 3 Range Information

No SNMP manager	SNMP manager	Default
IPGW_SNMP_MANAGER set to N.	IPGW_SNMP_MANAGER set to Y. In this case a second field, IPADDR, appears. The craftsperson datafills the IP address of the SNMP manager. For example, IP address 47.142.225.193 would be datafilled as: Y 47 142 225 193	N (no manager datafilled)

9.4.2.2.4 Activation

The new SNMP manager does not take effect on a 7X07AA until the card is PMRESET from the MAPCI;MTC;PM level. See "9.4.2.1.4 Activation" on page 2324 for more information.

9.4.2.2.5 Dependencies

None.

9.4.2.2.6 Consequences

The telco should employ SNMP manager IP address validation to make it harder for a hacker to use SNMP to alter data on the 7X07.

9.4.2.2.7 Verification

To verify the change, the craftsperson can attempt SNMP write operations[1] using an SNMP manager client on a host whose IP address was not previously set on the 7X07AA using DHCP or PMDEBUG. If the write operations succeed, the new SNMP manager IP address is in use.

A subsequent security test would be to set the office parameter back to N, PMRESET the card, and try a second set of SNMP write operations using the same host as in the first test. The host is no longer in the valid SNMP manager list on the 7X07AA, so the 7X07AA should reject SNMP write attempts.

9.4.2.2.8 Memory requirements

8 bytes

9.4.2.2.9 Parameter release history update

SN09 (TOP22): Creation

[1]The SNMP manager IP address is only checked for write operations, not read operations.

9.4.2.3 IPGW_SNMP_ENABLED

Internet Protocol Gateway Simple Network Management Protocol Enabled

9.4.2.3.1 Functional description

This Y/N parameter allows the craftsperson to enable or disable SNMP on the 7X07AA.

9.4.2.3.2 Provisioning rules

No special provisioning rules.

9.4.2.3.3 Range information

Table 4 Range Information

Minimum	Maximum	Default
This is a Y/N field	This is a Y/N field	Defaults to N unless TOPS IPGWs are present in Table IPINV on the pre-SN09 dump side, in which case this parameter defaults to Y.

9.4.2.3.4 Activation

The SNMP enabled/disabled status does not take effect on a 7X07AA until the card is PMRESET from the MAPCI;MTC;PM level. See “9.4.2.1.4 Activation” on page 2324 for more information.

9.4.2.3.5 Dependencies

None.

9.4.2.3.6 Consequences

If the telco is not using SNMP on the 7X07, this parameter should be set to N. This will prevent a hacker from using SNMP to alter data on the 7X07.

9.4.2.3.7 Verification

To verify the change, the craftsperson can attempt SNMP operations on the changed 7X07AAs. If the operations succeed, SNMP is enabled. If the operations time out, SNMP is disabled.

9.4.2.3.8 Memory requirements

2 bytes

9.4.2.3.9 Parameter release history update

SN09 (TOP22): Creation

9.4.2.4 IPGW_TELNET_ENABLED

Internet Protocol Gateway Telnet Enabled

9.4.2.4.1 Functional description

This Y/N parameter allows the craftsperson to enable or disable Telnet on the 7X07AA.

9.4.2.4.2 Provisioning rules

No special provisioning rules.

9.4.2.4.3 Range information

Table 5 Range Information

Minimum	Maximum	Default
This is a Y/N field	This is a Y/N field	Defaults to N.

9.4.2.4.4 Activation

The Telnet enabled/disabled status does not take effect on a 7X07AA until the card is PMRESET from the MAPCI;MTC;PM level. See "9.4.2.1.4 Activation" on page 2324 for more information.

9.4.2.4.5 Dependencies

None.

9.4.2.4.6 Consequences

If the telco is not using Telnet on the 7X07, this parameter should be set to N. This will prevent a hacker from logging on to the card and causing problems. This will also prevent authorized personnel from inadvertently logging on to a heavily loaded card. A card can have up to 48 calls in progress, and Telnetting on to a heavily loaded card might cause it to crash, ending its calls.

9.4.2.4.7 Verification

To verify the change, the craftsperson can attempt to Telnet onto the changed 7X07AAs. If the craftsperson receives the login prompt, Telnet is enabled. If the attempt times out, Telnet is disabled.

9.4.2.4.8 Memory requirements

2 bytes

9.4.2.4.9 Parameter release history update

SN09 (TOP22): Creation

9.5 Upgrade Considerations

9.5.1 Dump and Restore (CM)

The following actions occur on dump and restore from a pre-SN09 load to an SN09 or higher load.

- IPGW_SNMP_COMMUNITY_NAME: This parameter is set to “public” (without quotation marks).
- IPGW_SNMP_MANAGER: This parameter is set to N.
- IPGW_SNMP_ENABLED: Table IPINV on the dump side is consulted. If any TOPS IPGWs are datafilled (GW_TYPE = TOPS), this parameter is set to Y. Otherwise this parameter is set to N.
- IPGW_TELNET_ENABLED: This parameter is set to N.

9.5.2 Element Management Upgrade

Not applicable.

9.5.3 Downgrade impact

If data has already been downloaded to the 7X07AAs and the core is downgraded to a pre-SN09 release, the 7X07AAs retain the last settings from the core prior to the downgrade.

If a 7X07AA is PMRESET at a later time, data download occurs again. The 7X07AA checks the release level of the downloaded information, and if it is prior to SN09, the 7X07AA reverts to pre-SN09 settings as follows:

- SNMP community name is “public”
- SNMP manager IP address from CM is removed from manager list
- SNMP is enabled
- Telnet is enabled

9.6 Data schema (DS)

9.6.1 New/modified tables

Table 6 New or modified tables

Table	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
XPMIPMAP	Changed	Unchanged

9.6.2 Table information

9.6.2.1 Name: XPMIPMAP

eXtended Peripheral Module Internet Protocol Mapping

9.6.2.1.1 Functional description

This existing table defines the IP-XPMs and allows configuration of IP capabilities on the redundant SX05DA processor cards.

This feature adds a new field, SNMP, which indicates whether SNMP is enabled on the IP-XPM. If SNMP is enabled, the craftsperson must also datafill an SNMP community name in new subfield COMMNAME.

9.6.2.1.2 Usage sequence and implications

Unchanged.

9.6.2.1.3 Size

Table 7 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
XPMIPMAP	Unchanged	Unchanged	New SNMP datafill adds 20 bytes per tuple

9.6.2.1.4 Fields

Table 8 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
XPMNAME	Unchanged	N/A	N/A	N/A
AUTONEG	Unchanged	N/A	N/A	N/A
SUBNMASK	Unchanged	N/A	N/A	N/A
IPCONFIG	Unchanged	N/A	N/A	N/A
SNMP	New	This field is refined based on the value datafilled.	Y/N	If SNMP is Y, datafill the SNMP community name in the additional field COMMNAME. If SNMP is N, no additional fields can be datafilled.
COMMNAME	New	Subfield of field SNMP This field appears when field SNMP is set to Y.	Vector of one to sixteen characters Non-alpha-numeric symbols and lowercase letters can be entered using single quotes.	This field indicates the SNMP community name for SNMP read and write operations on the IP-XPM. The IP-XPM does not send traps so this community name is not currently used for SNMP traps.

9.6.2.1.5 Datafill example

The following example shows sample datafill for Table XPMIPMAP.

```
TABLE: XPMIPMAP
XPMNAME AUTONEG SUBNMASK IPCONFIG SNMP
--------------------------------------
DTC 11 AUTO 255 255 255 0 CM 95 64 10 164 95 64 10 165 95 64 10 166
95 64 10167 (4) (5) $ N N
DTC 12 AUTO 255 255 255 0 CM 95 92 9 132 95 92 9 133 95 92 9 134
95 92 9 135(3) (2) $ N Y public
```

9.6.2.1.6 Table release history update

TOPS13: Creation

SN09 (TOPS22): Addition of field SNMP

9.6.2.1.7 Supplementary information

On dump and restore from a pre-SN09 Succession core load to an SN09 or later load, new field SNMP is set to Y and new field COMMNAME is set to "public" (without quotation marks). These settings cause IP-XPM behavior to be unchanged from pre-SN09 loads.

9.6.2.1.8 Translation verification and other tools

Not applicable.

9.7 Service Orders (SO)

Not applicable.

9.8 Software optionality control (SOC)

Table 9 SOC

SOC option name:	OSB00101
SOC option title:	Basic Operator Services
SOC option control type:	State
New SOC option?	No
SOC option order code	OSB00101
Option defined in DRU:	TOPS
Affected products:	TOPS

9.9 Element Management

Not applicable.

9.10 User interface changes

Not applicable.

9.11 OSSGate Interface Changes

Not applicable.

9.12 Security

9.12.1 Network configuration

TOPS-IP network configuration recommendations are unchanged.

9.12.2 Key management

Not applicable.

9.12.3 Protocol

Not applicable.

9.12.4 Authentication

This feature allows the SNMP community name to be changed from “public” to a customer-specified name. This feature also allows the SNMP manager to be datafilled in the CM. The community name is used to authenticate incoming read and write requests on both the IP-XPM (SX05DA) and the 7X07AA. The

SNMP manager is used to authenticate incoming write requests on the 7X07AA.

This feature also allows SNMP to be completely disabled on the IP-XPM (SX05DA) and the 7X07AA. In addition, Telnet can be disabled on the 7X07AA. These measures provide additional security if the customer is not using SNMP and Telnet.

9.13 Configuration Walkthrough

To configure new SNMP settings on the IP-XPM (SX05DA):

- Set the appropriate fields in the Table XPMIPMAP tuple corresponding to the desired IP-XPM.
- Perform a LoadPM or Bsy/RTS to download the settings to the desired units of the IP-XPM.

To configure new SNMP and Telnet settings on the 7X07AA:

- Set the appropriate office parameters in the Table OFCENG.
- Perform a PMRESET on the desired cards to download the settings. The settings do not take affect on a card until it has been PMRESET.

10: Configuration (CN): A00009012

10.1 Feature Name

TOPS OSSAIN Service Enhancements

This section discusses the datafill changes, the SOC which controls the feature, and a brief discussion of the changes to the MAPCI command TST for SNs.

10.2 Data schema (DS) (CM)

10.2.1 Modified tables Schema

Table 1 Modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
OAFUNDEF	CHANGED	UNCHANGED
TOPSFTR	CHANGED	UNCHANGED

10.2.2 Table Schema information

10.2.2.1 Name: OAFUNDEF

OSSAIN Function Definitions

10.2.2.1.1 Functional description

The table's functionality is unchanged.

10.2.2.1.2 Size

Unchanged with a maximum tuple range of 1022.

10.2.2.1.3 Fields

The following table lists fields/OIDs for OAFUNDEF.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FUNCAREA	FUNCAREA is unchanged but has two new subfields and a change to an existing subfield			
	New	USESERV	Y, N	**Use ORIGSERV** N means to allow the switch to change the DA service to TA when an operator transfers the call to an SN. All other transition scenarios will retain the service of the call. Y means to ensure the service datafilled in field ORIGSERV of OAFUNDEF is used when transferring or triggering to the function. If a service switch occurs, then other fields may be effected based on service switch rules defined in the OAP Specification document. This field is not needed to set the service with ORIGSERV for initial call processing. It is used for transitions only.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
	New	DARECALL	Y, N	**DA Recall** N is not a DA recall Y means the call going to the function is a DA recall and the switch will increment the DA recall counter and set operator indicators for recall if going to an operator. This field is not used for initial call processing.
	Changed	AUTOSYS	MCCS, DAS	**Automated Systems** MCCS will route the call to MCCS. If MCCS is not available for the call then it is routed to operator.

10.2.2.1.4 Datafill example

The following example shows sample datafill for table OAFUNDEF.

Table 3 New Table OAFUNDEF

FUNCID	FUNCNAME	FUNCAREA
1	DA_SN	SN DASERV Y N N N N N Y CQ17 N
2	DA_TOPSOPER	TOPSOPER N OSSAIN_TO_DA_OPR N
3	TA_AUTO	TOPSAUTO MCCS 0_PLUS
4	TA_SN	SN TASERV N N N N Y Y CQ0 N
5	DA_SN_RCL	SN DASERV Y Y N N N N Y CQ17 N
6	DA_TOPSOPER_RCL	TOPSOPER Y OSSAIN_TO_DA_OPR N
7	TA_AUTO_RCL	TOPSAUTO MCCS 0_PLUS
8	TA_SN_RCL	SN TASERV Y N N N Y Y CQ0 N

10.2.2.1.5 Table release history update

In SN09, table OAFUNDEF added fields USESERV, DARECALL, removed TOPSAUTO option AABS and added TOPSAUTO option MCCS.

10.2.2.1.6 OAFUNDEF error messages

New error messages for table OAFUNDEF are noted below:

Table 1 Error messages for table OAFUNDEF

Error message	Explanation
`MCCS and DAS are the only TOPS automated system that are currently supported for OSSAIN.`	The user tries to datafill the AUTOSYS refinement with an automated system other than MCCS or DAS.

10.2.2.1.7 ONP Processing

Over a pre-SN09 to SN09+ ONP, the following fields/sub-fields will be populated as shown:

- USESERV will be set to N.
- DARECALL will be set to N.
- AUTOSYS AABS functions will be changed to MCCS.

10.2.2.2 Name: TOPSFTR

TOPS Features

10.2.2.2.1 Functional description

The table's function has not changed.

10.2.2.2.2 Size

Increased by 1

10.2.2.2.3 Datafill example

The following example shows sample datafill for table TOPSFTR.

Table 4 Table TOPSFTR

FTRNAME	FTRENABL
OSSAIN_RELEASE_22	Y

10.2.2.2.4 Table release history update

In SN09, table TOPSFTR added OSSAIN_ENHANCEMENTS_22 to the range.

10.2.2.2.5 Supplementary Information

TOPSFTR entry, OSSAIN_RELEASE_22 is tied to SOC option OSAN0102 for OSSAIN Enhancements and activates the following portions of feature A00009012:

- Transfer to SN function service
- DA Recall function

Although the functionality is controlled by this parameter, the associated datafill can be entered prior to activation.

10.3 Software optionality control (SOC)

Portions of feature A00009012 are activated by SOC option OSAN0102 and TOPSFTR entry OSSAIN_ENHANCEMENTS_22.

Table 5 SOC

SOC option name:	OSSAIN Enhancements
SOC option title:	Yes

Table 5 SOC

SOC option control type:	state
New SOC option?	No
SOC option order code	OSAN0102
Option defined in DRU:	TOPS

10.4 User interface changes

10.4.1 Command: TST

10.4.1.1 Command type: unchanged

10.4.1.2 Command target: unchanged

10.4.1.3 Command availability: unchanged

10.4.1.4 Command description

TST is a command used for OSNM, OSN and OSAC nodes posted at the MAP. When a node is posted at the PM level of the MAP, the TST command is available. The TST command remains unchanged by this feature; however, the functionality of the command is changed and one new response message is provided.

- When TST is entered for a node, a ping is no longer sent. For OSN however, the Node Connectivity Test message is now sent to the OSN node in place of the ping to verify connectivity.
- When TST PING is entered for a node on a platform that does not support ping from SOS, the following new response message is provided: “Use TST without PING.”.

10.4.1.5 Command syntax

Unchanged

10.4.1.6 Qualifications and warnings

Unchanged

10.4.1.7 Responses

10.4.1.7.1 “Use TST without PING.”

Table 6 MAP outputs with associated meanings and actions

TST PING
“Use TST without PING.” **Meaning:** TST PING has been used on a switch which does not support pings from MAP. **System or user actions:** Use command TST without the PING option. Ping from another platform.

11: Configuration (CN): A00009013

11.1 Feature Name

TOPS announcements via UAS/AMS

11.2 Hardware and Software Requirements

This activity has the following prerequisite requirements:

- Hybrid Communication Server 2000 (CS 2000) with ENET and IP network fabrics
- Interworking Spectrum Peripheral Module(s) (IW SPM IP)

  Note: An interworking bridge is required for each connection of a TOPS call to a packet announcement.
- Gateway Controller(s) (GWC) configured with Audio Controller profile
- Media Server 2010 (MS 2010) or Universal Audio Server (UAS) media server(s)
- Succession element managers for maintenance of the above components. This includes the Announcement Provisioning Server (APS).
- TOPS equipment (such as operator positions)

In an office that is migrating from DRAM-based announcements to packet-based announcements for TOPS, datafill for the applications that use the announcements (for example, Branding or ACTS) will already be present when the migration begins. For new offices, that datafill will not be present, and it may be added after the announcements have been provisioned. This DDOC does not attempt to re-document the data schema for all of the TOPS applications that use announcements. Refer to your Translations Guide (297-nnnn-350) and Data Schema Reference Manual (297-nnnn-351) for more information about basic TOPS datafill.

The following documents include other important prerequisite configuration information.

Table 2: References for Configuration Prerequisites

Document Number	Title
NN10193-511	Communication Server 2000 Configuration Management
NN10100-511	IW SPM IP Configuration Management
NN10205-511	Gateway Controller Configuration Management
NN10095-511	Universal Audio Server Configuration Management

Table 2: References for Configuration Prerequisites

Document Number	Title
NN10323-111	Media Server 2000 Series Basics
NN10340-511	Media Server 2000 Series Configuration Management
See Helmsman for other related documentation.	

11.3 Initial Configuration

This section assumes, for the most part, that the office is already using DRAM-based announcements for TOPS and is migrating some or all of the TOPS applications to use packet-based announcements. For new TOPS offices, it is necessary to consult both this document and the NTPs that explain the TOPS applications.

11.3.1 Basic configuration steps

The steps for configuring packet-based announcements for TOPS are as follows:

1. Determine what audio segments will be needed for the TOPS applications, and what voice content you want the segments to have.

   For **standard announcements** (ANTYPE = STND in CM table ANNS) this is straightforward. If you are migrating from DRAM-based to packet announcements, you will want to identify and determine the content of the standard announcements already in use.

   The number of standard announcements in the office may be small enough that you can look at table ANNS and immediately know how each of the standard announcements is used. Otherwise, look in the following tables.

   — CLLIs for SPID-based branding announcements are datafilled in the TAANN and DAANN fields of CM table SPIDDB.

   — CLLIs for carrier-based and NBEC-based branding announcements are datafilled in the TAANN, DAANN, and CDANN fields of CM table BRANDANN.

   — Announcement CLLIs for Music and Announcement in Queue are datafilled with the ANN selector in the route lists of tuples in CM table TOPAUDIO.

   — TOPS-specific treatment announcement CLLIs are datafilled in subtable TREAT of the TOPSTKGP tuple of CM table TMTCNTL. Depending on the office configuration, the OFFTREAT tuple may be used for TOPS calls, or tuples for other trunk group types may be used.

   Once the announcement CLLIs are known, determine the external phrase names that are associated with them. To do this in an existing TOPS office, consult table ANNMEMS for the DRAM track number(s), and then look

in table ANNPHLST for the mapping from CLLI + track number to a list of external phrase names. Each of these phrase names must have a segment provisioned on the packet media servers.

Note: Packet-based announcement members cannot have multiple tracks datafilled in the CM. Refer to the Configuration Guide for your media server for information about configuring the media server itself to play announcements in multiple languages.

If you want to hear the content that a DRAM plays for a phrase, look in table DRAMPHRS to determine where the phrase is stored on the DRAM. Then use the DRAMREC utility to listen to the recording that is currently in use.

For **custom announcements** (ANTYPE other than STND in table ANNS), determining what segments need to be recorded for the media servers can be a little harder. This is partly because some of the announcement numbers and phrase names for custom announcement applications are pre-determined by Nortel, while others may be defined by the operating company. Also, custom announcements can use placeholder phrase names, and these are handled differently for packet-based announcements than for DRAM announcements. Refer to "TOPS custom announcement considerations" on page 2347 for specific information about determining the segments that must be provisioned on the media servers for ACTS and MCCS.

2. Record the phrases that were determined in step 1 to be needed, or have them professionally recorded. Refer to the Configuration Management document for your media server for information about the required format.
3. Upload the audio files to the Announcement Provisioning Server (APS), and import corresponding physical segments into the APS database. Note the segment ID associated with each. Refer to "Media Server 2000 Series Configuration Management" for more information.
4. Ensure that the segments are made available to all appropriate media servers.

   Note: You must provision the same set of audio segments for all media servers controlled by the same GWC.
5. In CM table ANNAUDID, associate the MS 2000 / UAS audio segment ID with each external announcement phrase name that will be used with this feature.
6. Ensure that CM tables CLLI, ANNS, ANNMEMS, and ANNPHLST are correctly datafilled for the announcements that will use this feature. They should be datafilled in that order.
   — CLLI - Datafill the CLLI codes for the announcements.

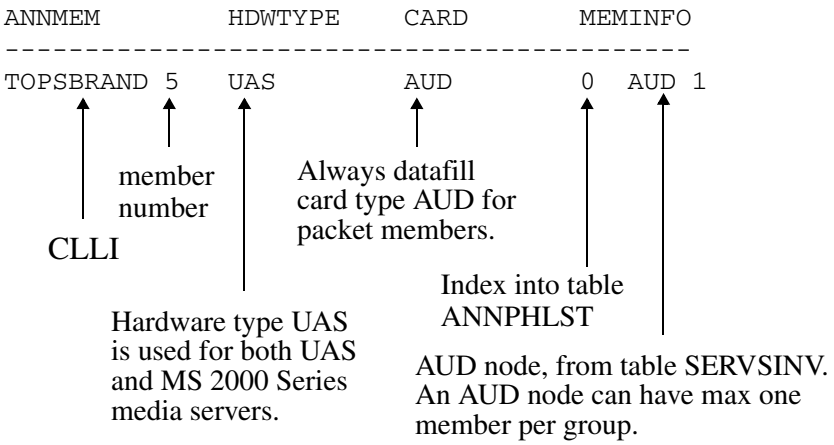
This table will already be datafilled if you are migrating from DRAM to packet announcements. In that case, no changes are needed.

— ANNS - Specify the characteristics of the announcement groups.

This table will already be datafilled if you are migrating from DRAM to packet announcements. In that case, no changes are needed.

— ANNMEMS - Specify the announcement members.

Add member tuples for all the announcements that will use packet-based media servers. The following figure shows an example.



The index into table ANNPHLST applies only to standard announcements type. It is present but ignored for custom announcement types.

Normally, all packet members of a standard announcement group are datafilled with the same index into table ANNPHLST. If the group also has DRAM members, the index for the packet members may or may not be the same as one of the track numbers of a DRAM member tuple. If it is the same, then the DRAM and AUD members will share a tuple in table ANNPHLST. If it is different, a tuple for the new index must be added to table ANNPHLST.

Note: For custom announcements, it is not possible for DRAM and packet members to use different tuples in table ANNPHLST.

— ANNPHLST - Specify the list of external phrase names that make up the announcement.

For custom announcement types, table ANNPHLST is indexed by the announcement CLLI and the application-specific custom announcement number. For standard DRAM announcements, it is indexed by the CLLI and track number. For standard packet announcements, it is indexed by the CLLI and the phrase list index from table ANNMEMS.

If you are migrating from DRAM-based to packet announcements for TOPS, and if you datafilled table ANNMEMS so that packet and DRAM members of standard announcement groups share the same ANNPHLST tuple, then table ANNPHLST needs no additional datafill.

If you are datafilling TOPS announcement applications from scratch, or if you are migrating but datafilled table ANNMEMS so that packet and DRAM members of a standard announcement group would not share the same ANNPHLST tuple, then datafill must be added to table ANNPHLST. A tuple is needed for each standard announcement member that has its own phrase list index, and for each custom announcement used by supported custom announcement applications (ACTS, MCCS).

Refer to your Translations Guide, Customer Data Schema Reference Manual, and later sections of this document for more information about datafilling table ANNPHLST.

7. Run TABAUDIT on tables ANNS, ANNMEMS, ANNPHLST, and ANNAUDID, and correct any errors found.
8. Ensure that the TOPS applications that are to use packet announcements are fully datafilled, if you are adding new applications rather than migrating existing ones. Refer to your Translation Guide and Customer Data Schema Reference Manual for more information about TOPS application datafill.
9. Bring new packet announcement members into service. This is done at the TTP level of the Maintenance and Administration Position (MAP) in the CM. If the Gateway Controller and/or the media servers are not in service, they must first be returned to service using CS 2000 OAM&P tools.

   Note: It is strongly recommended that test calls be made using the packet announcement members. See “Verifying provisioning” on page 2346 for more information.
10. For at least several days, monitor the applications carefully. Look for the following switch logs, which may indicate provisioning problems: XPKT340, TOPS104, and TOPS113. Also monitor logs and alarms on the media servers themselves. Procedures for doing that are described in the Fault Management document (NNnnnnn-911) for your media server.

11.3.2 Verifying provisioning

When commissioning new TOPS applications that use only packet-based announcements, it is strongly recommended that test calls be made before general TOPS traffic is routed to the announcements.

Test calls should also be made when migrating from DRAM-based to packet-based announcements for TOPS. To minimize the impact of the testing on live calls, the testing must be done at a time of very low traffic. The only way to ensure that a test call will get a packet announcement member is to busy out all DRAM members of the announcement group.

Specific provisioning problems that can cause trouble include (a) failure to provision all of the required phrases on some or all of the media servers, (b) mismatches between the segment identifiers provisioned on the media servers and the ones datafilled in CM table ANNAUDID, (c) failure to add an ANNAUDID tuple for some phrase name that the application uses, (d) failure to add an ANNPHLST tuple for an announcement member that the application uses, and (e) failure to provision the announcement ports on the media server.

Because of the potential disruptiveness of making test calls in a live office that is migrating from DRAM-based to packet-based announcements, it is important to check and double-check the provisioning before bringing packet members into service.

11.3.3 TOPS custom announcement considerations

To plan the audio segments that will be provisioned on the media servers for custom announcement applications such as MCCS and ACTS, it is useful to think backwards from the order in which the provisioning is actually done.

1. First, identify the announcements (announcement numbers) that the application uses. Both MCCS and ACTS predefine most of their announcement numbers, but both allow the operating company to define additional announcement numbers.
2. Second, determine the list of external phrase names that the CM uses (if migrating), or will use (if configuring the new application from scratch), for each of these announcement numbers. Nortel provides detailed recommendations on external phrase name lists to use for the pre-defined MCCS and ACTS announcement numbers. The operating company determines the phrase names for announcement numbers that the operating company defines. Also, the operating company may want to define some of its own phrase names to use with some of the pre-defined MCCS and/or ACTS announcement numbers, rather then using only the phrase names that Nortel suggests. If both legacy and packet members are used for the application, bear in mind that the CM uses the same external phrase name lists for both legacy and packet members.
3. Third, determine the content that will correspond to each phrase name. Nortel provides specific content suggestions for the phrase names that we recommend for the pre-defined announcement numbers. The operating company may choose to record different content, and in any case, the

operating company must determine the content for MCCS and ACTS announcements that the operating company defines.

4. Plan the provisioning of audio segments on the media servers. As described in the subsections below, there may not be a one-to-one relationship between physical audio segments on the media servers and phrase names datafilled in the CM. For ACTS, you must take into account the way variable substitution works for placeholder phrases.

When the above steps have been completed, configuration continues as described in "Basic configuration steps" on page 2343. The following subsections provide more detail about MCCS and ACTS.

11.3.3.1 MCCS

Refer to Table 3 on page 2358 for a concise summary of the pre-defined MCCS announcement numbers. For each pre-defined announcement number, the table shows suggested phrase names and content for the phrases.

The operating company can define additional MCCS announcement numbers that are used to brand the "thank-you" acknowledgment for correct card number entry. These operating company defined MCCS announcement numbers are datafilled in CM tables EAMCCSAN and MCCSNBEC.

If you are migrating from DRAM-based to packet-based announcements for MCCS, the easiest way to determine all the phrase names used for MCCS is to consult the MCCS tuples already datafilled in table ANNPHLST. If MCCS is being initially commissioned in the office, however, table ANNPHLST will be datafilled only after the audio segments have been provisioned on the media servers and datafilled in table ANNAUDID and other announcement tables.

MCCS does not use placeholder phrase names. Every phrase name in an MCCS tuple of table ANNPHLST must be mapped in table ANNAUDID to a segment identifier that will be sent to the media server when the corresponding announcement is to be played. MCCS has no requirement for media server provisioning for variable substitution.

The most straightforward way—but not necessarily the best way—to provision the media servers for MCCS is with a single, separate audio file for each MCCS phrase defined in the CM. This would mirror the way MCCS works with DRAMs. Alternatively, it is possible to save space on the media servers by decomposing some of the MCCS announcements into sub-phrases. Each sub-phrase would be a separate voice file on the media servers, and would have its own physical segment ID. A sequence type segment would then be defined in the APS to identify the sequence of physical segments that constitute the announcement. The segment ID of the sequence would be the one datafilled in CM table ANNAUDID against the MCCS external phrase name. The fact that the media server constructs the announcement from a sequence of physical

segments would be transparent to the CM. For more information about using audio sequences, refer to "Media Server 2000 Series Configuration Management."

11.3.3.2 ACTS

Table 5 on page 2362 summarizes the pre-defined ACTS announcement numbers. For each pre-defined announcement number, the table explains when the announcement is used and shows a list of suggested phrase names for the announcement. Content for the non-variable phrase names is suggested in Table 6 on page 2366.

The operating company can define additional ACTS announcement numbers that are used to brand the initial correct deposit and initial overdeposit "thank-you" acknowledgments for coin calls. These operating company defined ACTS announcement numbers are datafilled in CM tables SPIDDB, EAACTSAN and ACTSNBEC.

Because ACTS uses placeholder phrases, it is not possible for migrating offices to determine all the phrase names that ACTS uses simply by consulting existing datafill in table ANNPHLST. The remainder of this section is primarily concerned with how placeholder variable substitution works for ACTS, and the implications for provisioning the media servers. Provisioning the media servers is compared and contrasted to provisioning DRAMs for ACTS.

ACTS pre-defines four placeholder, or variable, phrase names in the CM. These are used for

- monetary amounts (ACTS_VAR_CHARGE and ACTS_VAR_CREDIT),
- time durations (ACTS_VAR_PERIOD), and
- coin denominations (ACTS_VAR_COIN).

The placeholder phrase names are not datafilled in table DRAMPHRS (legacy) or ANNAUDID (packet), and they do not directly correspond to recordings provisioned on DRAMs or media servers.

During call processing, the placeholder phrase names are resolved using call-specific information. For coin denominations (used only by the ACTS Coin Tone Generation Test feature), variable substitution works in much the same way for packet and legacy announcement members. For monetary amounts and time durations, variable substitution works very differently for packet members.

Coin denominations

Placeholder phrases for the ACTS Coin Tone Generation Test feature are handled in much the same way for packet members as for DRAM members. Internal logic in the CM maps the placeholder phrase ACTS_VAR_COIN to one of the pre-defined phrase names shown below:

Phrase Name	Recommended Content
ACTS_NICKEL	“nickel”
ACTS_DIME	“dime”
ACTS_QUARTER	“quarter”
ACTS_DOLLAR	“dollar”

The CM then looks in table ANNAUDID (if a packet member was selected) or DRAMPHRS (if a legacy member was selected), and it expects to find a mapping from that pre-defined phrase name to an audio ID that it will send to the announcement server. Therefore, if the ACTS Coin Tone Generation Test feature is used, the media servers must be provisioned with segments that play the content shown in the table above.

Charges and credits

Resolution of placeholder phrases ACTS_VAR_CHARGE and ACTS_VAR_CREDIT is handled differently for packet members than for DRAM members. For DRAM members, the CM resolves a monetary amount to a phrase list such as, for example, ACTS_1, ACTS_DOLLAR, ACTS_AND, ACTS_15, ACTS_CENTS, and it sends the DRAM a list of internal phrase IDs corresponding to the pre-defined phrases in the list. Therefore, when DRAM members are used, the CM requires datafill in table DRAMPHRS for all of the pre-defined phrases to which it can resolve monetary placeholders.

For packet members, the CM does not resolve monetary amounts to their constituent phrases, and it does not require datafill in table ANNAUDID of audio IDs for the constituent phrases. Instead, the CM sends the media server a higher-level message specifying that it should play a monetary amount and providing the currency (U.S. dollars) and the amount.

The media server executes the logic to resolve the monetary amount into physical phrases. To do this, it requires that recordings for the constituent phrases it can use for money be placed in audio files with pre-defined names. The pre-defined file names are the same for MS 2000 and UAS, and they are

documented in “Media Server 2000 Series Configuration Management.” Only files for the default language need to be provisioned, as ACTS does not support sending language selectors to the media server.

Time durations

The placeholder phrase ACTS_VAR_PERIOD is also handled differently for packet members than for DRAM members. For DRAM members, the CM breaks down the time duration into a sequence of constituent phrases such as ACTS_3, ACTS_MINUTES, and it sends a list of internal phrase identifiers corresponding to these phrase names to the DRAM. Therefore, the CM requires datafill in table DRAMPHRS for all of the pre-defined phrases to which it can resolve ACTS_VAR_PERIOD.

For packet members, the CM does not resolve time durations to their constituent phrases, and it does not require datafill in table ANNAUDID of audio IDs for the constituent phrases. Instead, the CM sends the media server a higher-level message specifying that it should play a duration and specifying the amount of time.

The media server executes the logic to resolve the duration to a list of physical phrases. To do this, it requires that recordings for the constituent phrases it can use for durations be placed in audio files with pre-defined names. The pre-defined file names are the same for MS 2000 and UAS, and they are documented in “Media Server 2000 Series Configuration Management.” Only files for the default language need to be provisioned, as ACTS does not support sending language selectors to the media server.

Silence

With DRAMs, pauses in the announcement require audio files that contain silence. The phrase name ACTS_PAUSE is typically used for this, and it requires mapping in table DRAMPHRS to an internal phrase number that identifies a recording of silence on the DRAM.

ACTS_PAUSE is not a placeholder phrase name, and if it is used in a phrase list for ACTS, it requires datafill in table ANNAUDID. The CM sends the media server a segment ID the same way it does for most other phrases. However, it is possible to provision the media server in a way that avoids using space to store a recording of silence. Refer to “Media Server 2000 Series Configuration Management” for information about provisioning variable-type segments with provisioned values. A variable segment of type silence could be provisioned and associated with a selector that has a provisioned value that determines the duration of the silence. This would be transparent to the logic in the CM.

11.4 Office/Subnet parameters (OP/SP) (CM & SESM)

No impact.

11.5 Upgrade Considerations

11.5.1 Dump and Restore (CM)

No impact.

11.5.2 Element Management Upgrade

No impact.

11.5.3 Downgrade impact

No impact.

11.6 Data schema (DS) (CM)

11.6.1 New/modified tables

Table 1 New or modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ANNMEMS	CHANGED	UNCHANGED
ANNPHLST	The table is not changed, but its documentation is.	UNCHANGED

11.6.2 Table Database Schema information

11.6.2.1 Name: ANNMEMS

Announcement Members Table

11.6.2.1.1 Functional description

Unchanged.

11.6.2.1.2 Usage sequence and implications (CM Only)

Unchanged.

11.6.2.1.3 Size

Unchanged.

11.6.2.1.4 Fields

Unchanged, but note that for custom announcement members with hardware type UAS, the PHLSTIDX field is ignored. This field is present for all members datafilled with HDWTYPE UAS, but it is consulted only if the announcement CLLI is datafilled as STND in table ANNS.

11.6.2.1.5 Datafill example
Unchanged.

11.6.2.1.6 Table release history update
As of SN09, packet members cannot be datafilled for a custom announcements of type TOPSVR or MDS.

Also, documentation of the meaning of the PHLSTIDX field for custom announcement types with hardware type UAS is clarified. (This is not a functional change.)

11.6.2.1.7 Supplementary information
Packet announcement members (HDWTYPE = UAS) are not supported for custom announcements of type MDS or TOPSVR. If a UAS member is datafilled for an announcement that is datafilled in table ANNS with ANTYPE = MDS or TOPSVR, one of the following warning messages is displayed:

```
Packet members are not supported for ANNTYPE MDS
Packet members are not supported for ANNTYPE TOPSVR
```

11.6.2.1.8 Translation verification and other tools
Unchanged.

11.6.2.2 Name: ANNPHLST
Announcement Phrase List Table

11.6.2.2.1 Functional description
Unchanged.

11.6.2.2.2 Usage sequence and implications (CM Only)
Unchanged.

11.6.2.2.3 Size
Unchanged.

11.6.2.2.4 Fields/OIDs
Unchanged.

11.6.2.2.5 Datafill examples

Mechanized Calling Card Service

Example datafill for MCCS appears below. The example assumes that the CLLI name datafilled in table ANNS for MCCS is MCCSTOPS. It also assumes that you are using the suggested phrase names shown in Table 3 on page 2358, and that you are not defining additional MCCS announcements in table EAMCCSAN or MCCSNBEC.

```
ANNPHKEY         PHSLIST
-----------------------------------------
MCCSTOPS 1       MCCSENG1 $
MCCSTOPS 2       MCCSENG2 $
MCCSTOPS 3       MCCSENG3 $
MCCSTOPS 4       MCCSENG4 $
MCCSTOPS 5       MCCSENG5 $
MCCSTOPS 6       MCCSENG6 $
MCCSTOPS 7       MCCSENG7 $
MCCSTOPS 8       MCCSENG8 $
MCCSTOPS 9       MCCSENG9 $
MCCSTOPS 15      MCCSENG15 $
MCCSTOPS 16      MCCSENG16 $
MCCSTOPS 17      MCCSENG17 $
MCCSTOPS 18      MCCSENG17 $
MCCSTOPS 19      MCCSENG17 $
MCCSTOPS 20      MCCSENG9 $
MCCSTOPS 21      MCCSENG9 $
MCCSTOPS 22      MCCSENG16 $
MCCSTOPS 23      MCCSENG5 $
```

Automatic Coin Toll Service

Example datafill for ACTS appears below. The example assumes that the CLLI name datafilled in table ANNS for ACTS is ACTSTOPS. It also assumes that you are using the suggested phrase names shown in Table 5 on page 2362, and that you are not defining additional ACTS announcements in table SPIDDB,

EAACTSAN, or ACTSNBEC. .

```
ANNPHKEY        PHSLIST
----------------------------------------
ACTSTOPS 1      (ACTS_VAR_CHARGE)(ACTS_PLEASE)(ACTS_PAUSE)
                (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)(ACTS_FOR_FIRST)
                (ACTS_VAR_PERIOD) $
ACTSTOPS 2      (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE) $
ACTSTOPS 3      (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)(ACTS_MORE) $
ACTSTOPS 4      (ACTS_THANK_YOU) $
ACTSTOPS 5      (ACTS_THANK_HAVE)(ACTS_VAR_CREDIT)(ACTS_CR_OVERTIME) $
ACTSTOPS 6      (ACTS_ALERT)(ACTS_VAR_PERIOD)(ACTS_END_SIGNAL) $
ACTSTOPS 7      (ACTS_ALERT)(ACTS_VAR_CHARGE)(ACTS_PLEASE)
                (ACTS_PAUSE)(ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)
                (ACTS_FOR PAST)(ACTS_VAR_PERIOD) $
ACTSTOPS 8      (ACTS_ALERT)(ACTS_VAR_CHARGE)(ACTS_PLEASE)(ACTS_PAUSE)
                (ACTS_YOU_HAVE)(ACTS_VAR_CREDIT)(ACTS_CREDIT)
                (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)
                (ACTS_MORE)(ACTS_FOR_PAST)(ACTS_VAR_PERIOD) $
ACTSTOPS 9      (ACTS_ALERT)(ACTS_CHARGES_ARE)(ACTS_VAR_CHARGE)
                (ACTS_PLUS_TAX)(ACTS_VAR_PERIOD) $
ACTSTOPS 10     (ACTS_ALERT)(ACTS_VAR_PERIOD)(ACTS_HAS_ENDED) $
ACTSTOPS 11     (ACTS_PLS_DEPOSIT)(ACTS_1)(ACTS_VAR_COIN) $
ACTSTOPS 12     (ACTS_PAUSE)(ACTS_ALERT) $
ACTSTOPS 13     (ACTS_THANK_YOU)(ACTS_VAR_COIN)(ACTS_TST_ENDED) $
ACTSTOPS 14     (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE) $
ACTSTOPS 15     (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE) $
ACTSTOPS 16     (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)(ACTS_MORE) $
ACTSTOPS 17     (ACTS_THANK_YOU) $
ACTSTOPS 18     (ACTS_THANK_HAVE)(ACTS_VAR_CREDIT)(ACTS_CR_OVERTIME) $
ACTSTOPS 19     (ACTS_ALERT)(ACTS_CHARGES_ARE)(ACTS_VAR_CHARGE)
                (ACTS_PLUS_TAX)(ACTS_VAR_PERIOD) $
ACTSTOPS 20     (ACTS_ALERT)(ACTS_VAR_CHARGE)(ACTS_PLEASE)(ACTS_PAUSE)
                (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)(ACTS_FOR_NEXT)
                (ACTS_VAR_PERIOD) $
ACTSTOPS 21     (ACTS_ALERT)(ACTS_VAR_CHARGE)(ACTS_PLEASE)(ACTS_PAUSE)
                (ACTS_YOU_HAVE)(ACTS_VAR_CREDIT)(ACTS_CREDIT)
                (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)(ACTS_MORE)
                (ACTS_FOR_NEXT)(ACTS_VAR_PERIOD) $
ACTSTOPS 22     (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE) $
ACTSTOPS 23     (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE) $
```

11.6.2.2.6 Table release history update

The explanations and example datafill for custom announcement types MCCS and ACTS were updated in SN09, to correct errors and to document that these applications can use either DRAM or packet announcement resources.

The information about custom announcement type AOSSVR was removed in SN09. This application was specific to TOPS MP positions, which are no longer supported.

11.6.2.2.7 Supplementary information

Mechanized Calling Card Service

MCCS is a TOPS custom announcement type. Although the DMS250 also supports an MCCS application, that application uses standard announcements. This section applies to TOPS MCCS.

MCCS announcements can be provided by DRAMs or by packet-based media servers in a hybrid solution with IP and ENET fabrics. The Media Server 2010 (MS 2010) and the Universal Audio Server (UAS) are examples of media servers.

For DRAMs, MCCS announcements can take the form of prerecorded phrases on two NT1X76CA double density erasable programmable read-only memory (EPROM) cards. Alternatively, an operating company can record its own DRAM announcements for MCCS. Use the DRAMREC CI to define phrases on a DRAM. All MCCS announcements are single-track.

For packetized MCCS announcements, the operating company provides the recordings and provisions them on the media servers using the Announcement Provisioning Server (APS). After that, tables ANNAUDID, CLLI, ANNS, ANNMEMS, and ANNPHLST must also be datafilled in the CM.

MCCS provides no secondary language support in the CM. An operating company can provide bilingual MCCS announcements by recording the announcements in both languages. For DRAMs, since MCCS announcements are single-track, both languages must be recorded on the same track. For packet-based MCCS announcements, a sequence can be created using the APS.

In addition to basic calling card validation, the MCCS custom announcement type can be used for sequence call prompts and for the TOPS Authorization Code and Account Code Billing features.

MCCS pre-defines custom announcement numbers 1 through 9 and 15 through 23. It reserves 10 through 14 for future development. Through datafill in tables EAMCCSAN and/or MCCSNBEC, the operating company can specify that announcement numbers 24 and higher are to be used to brand the initial "thank-you" acknowledgment for correct card entry.

MCCS does not use any variable, or placeholder, phrase names. Nortel suggests, but does not require, that the operating company use phrase names shown in Table 3 for MCCS announcements. The table shows the pre-defined MCCS announcement numbers, the scenario in which each is used, the suggested phrase name for each (assuming the language is English), and suggested content for each. The table shows the announcement numbers in an order that is logical in terms of call flow, rather than listing them in order by announcement number. The table uses the following abbreviations:

CCV	Calling Card Validation
SEQ	Sequence calling
ACB	Account Code Billing
AUTH	Authorization Code

Table 3: Pre-defined MCCS Announcements with Suggested Content

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List	Suggested Content
17	Initial prompt for CCV and ACB if originating station treatment (OST) from table MCCSOST is TONE. Also used as the initial and retry prompt for AUTH.	MCCSENG17	Alert tone ("bong") for calling card dialing. This is a complex tone consisting of 60 ms DTMF #-tone (941/1477 Hz @ -10 dBm), followed immediately by 940 ms of exponentially decayed dial tone (440/ 350 Hz with time constant of 200 ms initially at -10 dBm)
18	Initial prompt for CCV and ACB if originating station treatment (OST) from table MCCSOST is TONEANN.	MCCSENG17	
1	Re-prompt for CCV and ACB when initial prompt was announcement 18 (OST = TONEANN) and timeout occurred.	MCCSENG1	Please dial your card number or zero for an operator now.
2	Re-prompt for CCV and ACB if caller entered an invalid card number (CCV) or invalid account code (ACB).	MCCSENG2	Please dial your card number again now. The card number you have dialed is not valid.

Table 3: Pre-defined MCCS Announcements with Suggested Content

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List	Suggested Content
19	Re-prompt when timeout occurs after caller has heard announcement 2.	MCCSENG17	
3	Re-prompt when timeout occurs after caller has heard announcement 19.	MCCSENG3	Please dial your card number.
9	Re-prompt when timeout occurs after caller has heard announcement 3.	MCCSENG9	Please hang up and dial zero plus the number you are calling.
4	Sign-off message for CCV when caller has entered too many invalid card numbers.	MCCSENG4	Please hang up and dial zero plus the number you are calling. (pause) The card number you have dialed is not valid.
16	Announcement played when card number (CCV) or account code (ACB) has been successfully validated.	MCCSENG16	Thank you.
The following MCCS announcements are used only for sequence calls.			
5	Prompt when # is entered, initiating a sequence call.	MCCSENG5	You may dial another call now.
23	Re-prompt when timeout occurs after announcement 5.	MCCSENG5	
20	Sign-off message when timeout occurs after announcement 23.	MCCSENG9	
6	Re-prompt when caller enters an incorrect number in response to announcement 5.	MCCSENG6	Please dial the number you are calling again now. The number you have dialed is not correct.
7	Re-prompt when timeout occurs after announcement 6.	MCCSENG7	Please dial the number you are calling.
21	Sign-off announcement when timeout occurs after announcement 7.	MCCSENG9	
8	Sign-off announcement when caller has entered too many incorrect numbers for a sequence call.	MCCSENG8	Please hang up and dial zero plus the number you are calling. The number you have dialed is not correct.

Table 3: Pre-defined MCCS Announcements with Suggested Content

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List	Suggested Content
15	The number dialed is restricted for sequence calling.	MCCSENG15	Please hang up and dial direct. This number cannot be dialed as a sequence call.
22	Announcement played when caller has entered a correct number for a sequence call.	MCCSENG16	
Note: MCCS announcement numbers 10 through 14 are reserved for future development. ***Note:*** MCCS announcement numbers higher than 23 may be used to brand the initial thank-you acknowledgment by carrier or NBEC. The datafill for that is in tables EAMCCSAN and MCCSNBEC.			

Note that for some phrases, Table 3 lists the same phrase name against several different announcement numbers or scenarios. The table shows the suggested content only once for each phrase name. The operating company can provision different phrases for some of the announcements that share the same phrase name in the table above. To do that,

- First record the new announcement on the DRAM(s) or provision it on the media servers.
- Then add datafill to table DRAMPHRS (using the DRAMREC CI) or ANNAUDID (manually) mapping a new phrase name defined by the operating company to the internal ID provisioned on the announcement server.
- Finally, datafill the new phrase in table ANNPHLST against the CLLI used for MCCS and the new MCCS announcement number.

Note also that Table 3 shows a relatively inefficient scheme for using announcement store. It is based on the pre-recorded announcements that Nortel provides for DRAMs. If you do not plan to use these pre-recorded announcements, you may want to break out some of the sub-phrases that appear multiple times into their own phrases. For example, the sub-phrase “Please hang up and dial zero plus” appears in several different phrases. A separate recording could be created for that, and it could be included in the phrase lists for all of the announcements that begin that way.

If packet announcements are used for MCCS, the scheme for phrase names shown is Table 3 can be efficient if the media server is provisioned with audio sequences for the announcements that contain common phrases. The sequence identifier is then the one datafilled in table ANNPHLST.

If both DRAM and packet members are used for MCCS (or for any other custom announcement type), be aware that the two kinds of members share the same tuple in table ANNPHLST.

Automatic Coin Toll Service

ACTS is a TOPS custom announcement type that can be used for coin call automation and also for the TOPS Time and Charges, Non-coin Notification, and TOPS Coin Tone Generation Test features.

ACTS announcements can be provided by DRAMs or by packet-based media servers in a hybrid solution with IP and ENET fabrics. The Media Server 2010 (MS 2010) and the Universal Audio Server (UAS) are examples of media servers.

For DRAMs, ACTS announcements can take the form of prerecorded phrases on circuit pack NT1X76AE. Alternatively, an operating company can record its own DRAM announcements for ACTS. Use the DRAMREC CI to define the phrases on a DRAM. All ACTS announcements are single-track.

For packetized ACTS announcements, the operating company provides the recordings and provisions them on the media servers using the Announcement Provisioning Server (APS). After that, tables ANNAUDID, CLLI, ANNS, ANNMEMS, and ANNPHLST must also be datafilled in the CM.

ACTS provides no secondary language support.

ACTS pre-defines custom announcement numbers 1 through 23. Through datafill in tables SPIDDB, EAACTSAN and/or ACTSNBEC, the operating company can specify that announcement numbers 24 and higher are to be used to customize the initial correct deposit and overdeposit “thank-you” acknowledgments for coin calls by Service Provider ID, interLATA carrier, or Non-Bell Exchange Company.

ACTS defines certain placeholder phrase names that are datafilled in table ANNPHLST but should not be datafilled in either DRAMPHRS or ANNAUDID. The following table shows the ACTS pre-defined placeholder phrase names.

Table 4: ACTS use of placeholder phrases

Placeholder Phrase Name	Meaning
ACTS_VAR_CHARGE	Amount of money due.
ACTS_VAR_CREDIT	Amount of credit from overdeposit.
ACTS_VAR_PERIOD	Time duration for charges or for notification.

Table 4: ACTS use of placeholder phrases

Placeholder Phrase Name	Meaning
ACTS_VAR_COIN	Denomination of coin to be deposited for coin test feature.

In addition to the placeholder phrases, Nortel recommends, but does not require, that the operating company use certain other phrase names for ACTS. These are shown in tables 5 and 6. Those phrase names are added to table DRAMPHRS (using the DRAMREC CI) or ANNAUDID (manually, after provisioning the media servers) before they are datafilled in table ANNPHLST.

The following table shows the pre-defined ACTS announcement numbers, the scenario in which each is used, and the suggested phrase list for each. The table shows the announcement numbers in an order that is logical in terms of call flow, rather than listing them in order by announcement number.

Note: Suggested content for the non-variable phrase names is shown in Table 6.

Table 5: Pre-defined ACTS announcements with suggested phrase lists

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List (PHLIST field of table ANNPHLST)
1	Initial deposit request	(ACTS_VAR_CHARGE) (ACTS_PLEASE) (ACTS_PAUSE) (ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_FOR_FIRST) (ACTS_VAR_PERIOD) $
2	Re-prompt on timeout after announcement 1, no coins entered	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) $
3	Inter-coin prompt - Re-prompt after inter-coin timeout for initial period	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_MORE) $
4	Acknowledgement of correct deposit for initial period	(ACTS_THANK_YOU) $
5	Acknowledgement of overdeposit for initial period	(ACTS_THANK_HAVE) (ACTS_VAR_CREDIT) (ACTS_CR_OVERTIME) $

Table 5: Pre-defined ACTS announcements with suggested phrase lists

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List (PHLIST field of table ANNPHLST)
6	Notification at end of initial period, for post-paid overtime	(ACTS_ALERT) (ACTS_VAR_PERIOD) (ACTS_END_SIGNAL) $
7	Charge due deposit request, post-pay, with no previous overdeposit	(ACTS_ALERT) (ACTS_VAR_CHARGE) (ACTS_PLEASE) (ACTS_PAUSE) (ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_FOR PAST) (ACTS_VAR_PERIOD) $
14	Re-prompt on timeout after announcement 7	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) $
8	Charge due deposit request, post-pay, with previous overdeposit	(ACTS_ALERT) (ACTS_VAR_CHARGE) (ACTS_PLEASE) (ACTS_PAUSE) (ACTS_YOU_HAVE) (ACTS_VAR_CREDIT) (ACTS_CREDIT) (ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_MORE) (ACTS_FOR_PAST) (ACTS_VAR_PERIOD) $
15	Re-prompt on timeout after prompt 8	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) $
20	Charge due deposit request, pre-pay, with no previous overdeposit	(ACTS_ALERT) (ACTS_VAR_CHARGE) (ACTS_PLEASE) (ACTS_PAUSE) (ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_FOR_NEXT) (ACTS_VAR_PERIOD) $
22	Re-prompt on timeout after prompt 20	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) $

Table 5: Pre-defined ACTS announcements with suggested phrase lists

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List (PHLIST field of table ANNPHLST)
21	First overtime charge prompt, pre-pay, with previous overdeposit	(ACTS_ALERT) (ACTS_VAR_CHARGE) (ACTS_PLEASE) (ACTS_PAUSE) (ACTS_YOU_HAVE) (ACTS_VAR_CREDIT) (ACTS_CREDIT) (ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_MORE) (ACTS_FOR_NEXT) (ACTS_VAR_PERIOD) $
23	Re-prompt on timeout after prompt 21	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) $
16	Overtime inter-coin prompt (pre-pay or post-pay)	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_MORE) $
17	Acknowledgement of correct deposit for overtime period (pre-pay or post-pay)	(ACTS_THANK_YOU) $
18	Acknowledgement of overdeposit for overtime period (pre-pay or post-pay)	(ACTS_THANK_HAVE) (ACTS_VAR_CREDIT) (ACTS_CR_OVERTIME) $
9	Time and charges quotation	(ACTS_ALERT) (ACTS_CHARGES_ARE) (ACTS_VAR_CHARGE) (ACTS_PLUS_TAX) (ACTS_VAR_PERIOD) $
19	Repeat time and charges quotation (timeout after announcement 9)	(ACTS_ALERT) (ACTS_CHARGES_ARE) (ACTS_VAR_CHARGE) (ACTS_PLUS_TAX) (ACTS_VAR_PERIOD) $
10	Non-coin, customer-requested notification of time.	(ACTS_ALERT) (ACTS_VAR_PERIOD) (ACTS_HAS_ENDED) $

Table 5: Pre-defined ACTS announcements with suggested phrase lists

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List (PHLIST field of table ANNPHLST)
11	Coin test prompt	(ACTS_PLS_DEPOSIT) (ACTS_1) (ACTS_VAR_COIN)
12	Coin test failure. Also coin test cycle done.	(ACTS_PAUSE) (ACTS_ALERT) $
13	Coin test success	(ACTS_THANK_YOU) (ACTS_VAR_COIN) (ACTS_TST_ENDED) $

You do not have to use the exact phrase lists that are suggested in the table above, but it is important that placeholder phrases be datafilled only for the announcements for which they make sense and are shown in the table. For example, it would be an error to datafill placeholder phrase ACTS_VAR_CREDIT in announcement 1, the initial deposit request.

One reason you might want to define your own phrase names would be to play a different “thank-you” acknowledgment for announcement 4 than for announcement 17. To provision different announcements:

- First record the new announcement on the DRAM(s) or provision it on the media servers.
- Then add datafill to table DRAMPHRS (using the DRAMREC CI) or ANNAUDID (manually) mapping a new phrase name defined by the operating company to the internal ID provisioned on the announcement server.
- Finally, datafill the new phrase in table ANNPHLST against the CLLI used for ACTS and the ACTS announcement number.

The following table shows the suggested content for the phrase names from Table 5. It does not include the placeholder phrase names, for which variable substitution occurs before the audio identifiers are determined. It also does not include the pre-defined phrase names that are substituted for placeholder phrases.

Table 6: Suggested content for ACTS phrases, other than those used for placeholder substitution

Phrase Name	Suggested Phrase Content
ACTS_ALERT	(alerting tone, recording as an announcement)
ACTS_PLEASE	“please”
ACTS_PAUSE	(2 s pause)
ACTS_PLS_DEPOSIT	“Please deposit”
ACTS_FOR_FIRST	“for the first”
ACTS_MORE	“more”
ACTS_THANK_YOU	“Thank you”
ACTS_THANK_HAVE	“Thank you. You have”
ACTS_CR_OVERTIME	“credit toward overtime”
ACTS_END_SIGNAL	“has ended. Please signal when through.”
ACTS_FOR_PAST	“for the past”
ACTS_YOU_HAVE	“You have”
ACTS_CREDIT	“credit”
ACTS_CHARGES_ARE	“The charges are”
ACTS_PLUS_TAX	“plus tax for”
ACTS_HAS_ENDED	“has ended.”
ACTS_1	“one”
ACTS_TST_ENDED	“test has ended.”

Note: The ACTS phrases shown in the tables in this section are not the complete list of phrases that must be present in table DRAMPHRS or ANNAUDID to support ACTS. Tables DRAMPHRS (legacy) and ANNAUDID (packet) must also include certain phrases to support variable substitution. Variable substitution is done differently for packet announcements than for DRAM announcements. Section “Automatic Coin Toll Service” in “DMS-100 Family NA100 Translations Guide” lists all the phrases that must be provisioned on DRAMS if legacy announcements are

used for ACTS, and these include the ones used for variable substitution. If packet announcements are used, refer to “ACTS” on page 2349 of this document.

Auxiliary Operator Service System

The AOSSVR custom announcement type is no longer supported. It was used with TOPS MP positions, which are no longer supported.

11.6.2.2.8 Translation verification and other tools

Unchanged.

11.7 Service Orders (SO) (CM & SESM)

No impact.

11.8 Software optionality control (SOC)

This feature is not controlled by SOC. Note however that some of its prerequisite configuration is SOC controlled. Refer to “Hardware and Software Requirements” on page 2342 for information about the feature’s prerequisites.

11.9 Element Management

No impact.

11.10 User interface changes

No impact.

11.11 OSSGate Interface Changes

No impact.

11.12 Security

No impact.

11.13 Configuration Walkthrough

See “Initial Configuration” on page 2343.

12: Configuration (CN): A00009036

Note: Only the Data Schema section is impacted by this activity.

12.1 Feature Name

Table HOMELRN Option SITE Expansion

12.2 Hardware and Software Requirements - *N/A*

12.3 Initial Configuration - *N/A*

12.4 Office/Subnet parameters (OP/SP) (CM & SESM) - *N/A*

12.5 Upgrade Considerations - *N/A*

12.6 Data schema (DS) (CM, MIBS, RDB)

12.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
HOMELRN	CHANGED	UNCHANGED

12.6.2 Table/MIB/Remote Database Schema information

12.6.2.1 Name: HOMELRN

12.6.2.1.1 Functional description

Table HOMELRN Option SITE is increased to allow 256 SITE names per HOMELRN entry, the previous maximum was 10.

There are no other changes to Table HOMELRN by this activity other than the increased SITE option maximum.

12.6.2.1.2 Usage sequence and implications (CM Only)

No change to current implications

12.6.2.1.3 Size

Table HOMELRN Option SITE maximum limit increases to 256 SITE names per HOMELRN entry.

There is no additional allocation of store to accomodate the increase. The current Option SITE memory allocation is sufficient to handle the increase.

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
HOMELRN	0	4000 - 8000	UNCHANGED by this activity

12.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for <abbreviated name of table.

<conditional information>

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTIONS	Changed	SITE		Option SITE can contain up to 256 site names (increased from 10)

12.6.2.1.5 Datafill example

No change

12.6.2.1.6 Table release history update

SN09 - Increased Numebr of SITEs that can be datafilled in table HOMELRN through option SITE from 10 to 256.

12.6.2.1.7 Supplementary information

None

12.6.2.1.8 Translation verification and other tools

None

12.7 Service Orders (SO) (CM & SESM) - *N/A*

12.8 Software optionality control (SOC) - *N/A*

12.9 Element Management - *N/A*

12.10 User interface changes - *N/A*

12.11 OSSGate Interface Changes - *N/A*

12.12 Security - *N/A*

12.13 Configuration Walkthrough - *N/A*

13: Configuration (CN): A00009078

13.1 Feature Name

ICM Dual CTI

13.2 Hardware and Software Requirements

For DMS-100, at least two EIUs are needed it the customer wants each TCP/IP links to connect to different EIUs.

For CS2Kc, a primary and a backup 3PC card (Ethernet card) is needed.

13.3 Initial Configuration

Subscription to this feature has to be done according to the DS section. SOC for this feature needs to be turned on. EIU needs to be configured as in interface, if the customer wants each TCP/IP links to connect to different EIU's.

13.4 Upgrade Considerations

13.4.1 Dump and Restore (CM)

Al l of the existing TCP/IP linksets with one link will remain the same after a Dump and Restore.

All of the existing OMs for TCP/IP linksets will remain with a slight change of a link number of 0 appearing after the linkset name.

13.4.2 Element Management Upgrade

13.4.3 Downgrade impact

13.5 Data schema (DS) (CM, MIBS, RDB)

13.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SCAICOMS	Changed	NEW

13.5.2 Table/MIB/Remote Database Schema information

13.5.2.1 Name: SCAICOMS

SCAI Communications Table

13.5.2.1.1 Functional description

The operating company uses table SCAICOMS to define the CompuCALL (X.25) and ICM (TCP/IP)links.

Changes will be made to support another TCP/IP link within an existing linkset.

13.5.2.1.2 Usage sequence and implications (CM Only)

To support another TCP/IP link within an existing linkset the following changes have to be made.

The datafill of this table is done in the following order for the TCP/IP linksets.

LINKSET: enter the linkset name.

LNKSEL: TCP

IPADDR: ### ### ### ###

Where # is a digit ranging from 0 to 9. Please note that the space should be present after entering each set of digits.

IPADDR: ### ### ### ###

MULTIMSG: Y/N

OPTION: CONTAUD

AUDIT: N

OPTION: $

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

> Y

Everything above except the entry in bold exists now. A prompt for a second IP address will be provided. If a customer only wants a single IP address, this will be achieved by typing a $ at the prompt for second IP address.

IPADDR: $

Please look at secion 12.4.2.1.5 for the examples

13.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SCAICOMS	0	256 (x.25) + 96 (TCP/IP) = 352	Protected

13.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for table SCAICOMS.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
IPADDR	Changed	Prompt for another IP address will be displayed	### ### ### ###	IP address. If only one IP address is needed the second prompt for IP address should be cancelled by typing in a $.

13.5.2.1.5 Datafill example

The following example shows sample datafill for table SCAICOMS.

LINKSET: TCP_AA

LNKSEL: TCP

IPADDR: 47 150 19 1

IPADDR: 47 102 3 4

MULTIMSG: N

OPTION: CONTAUD

AUDIT: N

OPTION: $

TUPLE TO BE ADDED

TCP_AA TCP (47 150 19 1) (47 102 3 4) N (CONTAUD N) $

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

> Y

Another example for adding just one link.

LINKSET: TCP_BB

LNKSEL: TCP

IPADDR: 47 10 3 2

IPADDR: $

MULTIMSG: N

OPTION: CONTAUD

AUDIT: N

OPTION: $

TUPLE TO BE ADDED

TCP_BB TCP (47 10 3 2) $ N (CONTAUD N) $

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

> Y

13.5.2.1.6 Table release history update

A prompt for another IPADDR field was added.

13.5.2.1.7 Supplementary information

N/A

13.5.2.1.8 Translation verification and other tools

SCAICOMS does not use translation verification tools.

13.6 Software optionality control (SOC)

Order code ICM00081, ICM Dual Link optionalizes the functionality of the

Table 4 SOC

SOC option name:	ICM
SOC option title:	ICM Dual Link
SOC option control type:	STATE
New SOC option?	Yes
SOC option order code	ICM00081
Option defined in DRU:	CCM
Affected products:	LEC00022, LET00022, LLT00022, SN09, ISN09

second TCP/IP link within a linkset.When ICM00081 SOC is in the IDLE state, datafill of the second TCP/IP link will be allowed. But the second attempt to connect to a link within the linkset will fail. Only one connection is allowed at a time.

14: Configuration (CN): A00009085

14.1 Feature Name

ACD & ICM Capacity Expansion

14.2 Hardware and Software Requirements

14.3 Initial Configuration

14.4 Office/Subnet parameters (OP/SP) (CM & SESM)

14.4.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCOPT	MAX_NUMBER _ACD_AGENTS _PER_SWITCH	CHANGED	CM

14.4.2 Parameter information

14.4.2.1 MAX_NUMBER_ACD_AGENTS_PER_SWITCH

Maximum Number of Automatic Call Distribution Agents Per Switch

14.4.2.1.1 Functional description

This is a pre-existing office parameter which specifies the maximum number of ACD agent positions that the operating company can provision in the switch.

The purpose of this parameter will not be changed by this activity.

The range of this parameter will be increased to have a maximum value of 99,999. The ability to assign a new value to this parameter is restricted. A new value can only be assigned by changing the limit of the ACD00101 SOC.

When the SOC usage limit is increased or decreased, the value stored in the office parameter is automatically updated to reflect the new limit.

14.4.2.1.2 Range information

Table 2 Range Information

Minimum	Maximum	Default
0	99,999	0

14.4.2.1.3 Memory requirements

No memory impact.

14.4.2.1.4 Parameter release history update

The maximum value is being increased from 30,000 to 99,999 for SN09.

14.5 Upgrade Considerations

14.5.1 Dump and Restore (CM)

14.5.2 Element Management Upgrade

14.5.3 Downgrade impact

14.6 Data schema (DS) (CM, MIBS, RDB)

14.6.1 New/modified tables, MIBs, or Database Schema

Table 3 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ACDGRP	CHANGED	UNCHANGED
ACDSGRP	CHANGED	UNCHANGED
ACDMISPL	CHANGED	UNCHANGED
ACDLOGIN	CHANGED	UNCHANGED
ACDENLOG	CHANGED	UNCHANGED

14.6.2 Table/MIB/Remote Database Schema information

14.6.2.1 Name: ACDGRP

ACD Group Info.

14.6.2.1.1 Functional description

ACDGRP is an existing table. This table defines ACD groups. Currently, this table can accomodate a maximum of 1,024 tuples. This table will be modified by this activity to accomodate a maximum of 5,000 tuples.

14.6.2.1.2 Usage sequence and implications (CM Only)

Current datafill order is unchanged.

14.6.2.1.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ACDGRP	0	5,000	Protected

14.6.2.1.4 Fields/OIDs

No change is made to the fields table ACDGRP.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

14.6.2.1.5 Datafill example

The following example shows sample datafill for table ACDGRP.

14.6.2.1.6 Table release history update

Table is expanded to accomodate a maximum of 5,000 tuples.

14.6.2.1.7 Supplementary information

N/A

14.6.2.1.8 Translation verification and other tools

ACDGRP does not use translation verification tools.

14.6.2.2 Name: ACDSGRP

ACD Sub-Group Info.

14.6.2.2.1 Functional description

ACDSGRP is an existing table. This table defines ACD sub-groups. Currently, this table allows provisioning of a maximum of 256 sub-groups per ACD group. This table will be modified to allow the provisioning of a maximum of 2,500 sub-groups par ACD group.

14.6.2.2.2 Usage sequence and implications (CM Only)
Current datafill order is unchanged.

14.6.2.2.3 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ACDGRP	0	5,000	Protected

14.6.2.2.4 Fields/OIDs
No change is made to the fields table ACDSGRP.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

14.6.2.2.5 Datafill example
The following example shows sample datafill for table ACDSGRP.

14.6.2.2.6 Table release history update

14.6.2.2.7 Supplementary information
N/A

14.6.2.2.8 Translation verification and other tools
ACDSGRP does not use translation verification tools.

14.6.2.3 Name: ACDMISPL
ACDMIS Pool Info.

14.6.2.3.1 Functional description
ACDMISPL is an existing table. This table defines ACDMIS Pools. The existing field PROTOCOL is modified to add a new value BCS57.

14.6.2.3.2 Usage sequence and implications (CM Only)
Current datafill order is unchanged.

14.6.2.3.3 Size
The size of table ACDMISPL is not impacted by this activity.

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory

14.6.2.3.4 Fields/OIDs

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PROTOCOL	CHANGED	None	BCS24 or BCS25 or BCS26 or BCS27 or BCS29 or BCS30 or BCS31 or BCS32 or BCS33 or BCS34 or BCS35 or BCS42 or BCS43 or **BCS57**	New protocol version BCS57 is added.

14.6.2.3.5 Datafill example
The following example shows sample datafill for table ACDMISPL.

14.6.2.3.6 Table release history update
The PROTOCOL field of the table ACDMISPL is modified to add the new value BCS57.

14.6.2.3.7 Supplementary information
N/A

14.6.2.3.8 Translation verification and other tools
ACDGRP does not use translation verification tools.

14.6.2.4 Name: ACDLOGIN
ACD Login Table.

14.6.2.4.1 Functional description

ACDLOGIN is an existing table. This table maps ACD Login IDs to a corresponding password, if needed. This table also maps Customer groups to the corresponding ACD Login IDs, if requested. This table will be expanded by this activity to accomodate a maximum of 99,999 tuples.

14.6.2.4.2 Usage sequence and implications (CM Only)

Current datafill order is unchanged.

14.6.2.4.3 Size

Table 10 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ACDLOGIN	0	99,999	Memory is allocated dynamically through the use of SEGSTOR in blocks of 512.

14.6.2.4.4 Fields/OIDs

The following table lists the fields for ACDLOGIN.

Table 11 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LOGINID	CHANGED	None	5 digit number between 00001 and 99999	The range of ACD Login ID is expanded to accomodate 99,999 Login IDs.

14.6.2.4.5 Datafill example

The following example shows sample datafill for table ACDLOGIN.

14.6.2.4.6 Table release history update

Table is expanded to accomodate a maximum of 99,999 tuples.

14.6.2.4.7 Supplementary information

N/A

14.6.2.4.8 Translation verification and other tools

ACDLOGIN does not use translation verification tools.

14.6.2.5 Name: ACDENLOG

ACD Enhanced Login Table.

14.6.2.5.1 Functional description

ACDENLOG is an existing table. This table allows multiple customer groups the full range of Login IDs for their ACD agents. This table is indexed by a two part key, made up of the Partition Number (PARTNO) and Login ID (LOGINID). This table will be expanded by this activity to accomodate a maximum of 99,999 tuples per partition.

14.6.2.5.2 Usage sequence and implications (CM Only)

Current datafill order is unchanged.

14.6.2.5.3 Size

Table 12 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ACDENLOG	0	99,999	Memory is allocated dynamically through the use of SEGSTOR in blocks of 512.

14.6.2.5.4 Fields/OIDs

The following table lists the fields for ACDENLOG.

Table 13 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LOGINID	CHANGED	None	5 digit number between 00001 and 99999	The range of Login ID is expanded to accomodate 99,999 Login IDs.

14.6.2.5.5 Datafill example

The following example shows sample datafill for table ACDENLOG.

14.6.2.5.6 Table release history update

Table is expanded to accomodate a maximum of 99,999 tuples per partition.

14.6.2.5.7 Supplementary information

N/A

14.6.2.5.8 Translation verification and other tools

ACDENLOG does not use translation verification tools.

14.7 Service Orders (SO) (CM & SESM)

This activitty does not introduce any new Service Order commands, LCCs, or options.

14.7.1 Service order change details

When the ACD option is added to a line (ADO, NEW, NEWACD commands), or when ACD option data is changed (CHF command), one of the prompts offered by SERVORD is POSID. Currently, any value between 00001 and 30000 is accepted as valid input for the POSID. This activity will change the acceptable value of POSID to be in the range of 00001 to 99999.

14.7.1.1 How service order options are presented

14.7.1.1.1 Description

The range of valid input for the POSID prompt has been modified to be between 00001 and 99999.

14.7.1.1.2 Example

Figure 1 Example of the ADO command in prompt mode

```
SO:
>ado
SONUMBER:   NOW  3 11  6 AM
>
DN_OR_LEN:
>6218000
OPTKEY:
>1
OPTION:
>acd
ACDGRP:
>acdtest1
ACDSGRP:
>0
IDNUM:
>y
POSID:
>99999
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 3 11 6 AM 6218000 ( 1 ACD ACDTEST1 0 Y 99999 ()()) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
```

Figure 2 Example of the ADO command in no-prompt mode

```
SO:
>ado $ 6218000 1 acd acdtest1 0 y 99999 $
```

The NEW, NEWACD, and CHF commands also offer the POSID prompt when used to manipulate ACD data. Examples of these commands are not provided because the effect of this change is identical to the ADO example shown above.

14.7.1.1.3 Option prompts

Table 14 System prompts for POSID

Prompt	Valid input	Description	Areas affected by prompt
POSID	00001 to 99999	ACD agent position ID	Affects SERVORD commands ADO, NEW, NEWACD, and CHF when used to manipulate ACD option data.

14.8 Software optionality control (SOC)

Table 15 SOC

SOC option name:	ACD00101
SOC option title:	ACD Agent Expansion
SOC option control type:	USAGE
New SOC option?	NO
SOC option order code	00037650
Option defined in DRU:	CCM
Affected products:	NA100, SL100
SOC option name:	ACD00104
SOC option title:	Group Increase to 5K
SOC option control type:	STATE
New SOC option?	YES
SOC option order code	00041836
Option defined in DRU:	CCM

Table 15 SOC

Affected products:	NA100, SL100
SOC option name:	ACD00105
SOC option title:	Agents Per Group Exp
SOC option control type:	STATE
New SOC option?	YES
SOC option order code	00041837
Option defined in DRU:	CCM
Affected products:	NA100, SL100
SOC option name:	ACD00106
SOC option title:	Maximum Queued Calls
SOC option control type:	STATE
New SOC option?	YES
SOC option order code	00041838
Option defined in DRU:	CCM
Affected products:	NA100, SL100
SOC option name:	ICM00082
SOC option title:	DNs Per ICM Session
SOC option control type:	STATE
New SOC option?	YES
SOC option order code	00041839
Option defined in DRU:	CCM
Affected products:	NA100, SL100

14.9 Element Management

14.10 OSSGate Interface Changes

N/A

14.11 Security

N/A

14.12 Configuration Walkthrough

N/A

15: Configuration (CN): A00009091

15.1 Feature Name

Equal Access (EA) LPIC Privilege Routing

15.2 Hardware and Software Requirements

Not applicable.

15.3 Initial Configuration

Not applicable.

15.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

15.5 Upgrade Considerations

None.

15.6 Data schema (DS) (CM, MIBS, RDB)

15.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
VEONAME	New	New
XLAPLAN	Changed	New
CXGRP	Changed	New
LPICPXLA	New	New

15.6.2 Table/MIB/Remote Database Schema information

15.6.2.1 Name : VEONAME

Virtual End Office Name

15.6.2.1.1 Functional description

New table VEONAME will contain the list of VEO names. Each VEO name represents a virtual end office that is partitioned on the DMS100/CS2000. The Virtual EO name will be provisioned as a string of up to 16 characters. Table VEONAME can provision upto a maximum of 1000 VEO names including the nil_veo_name as reserved value.

15.6.2.1.2 Usage sequence and implications (CM Only)

When intially configuring the switch, table VEONAME must be provisioned prior to adding option VEONAME in table XLAPLAN, and table CXGRP and adding a new privilege code in table LPICPXLA.

Table control would not allow deletion of a tuple in table VEONAME if it is being used in Table XLAPLAN or Table CXGRP or Table LPICPXLA.

15.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
VEONAME	1	1000	No memory allocation required since the only field in this tuple is of string range data type. The strings are added in data dictionary when a new tuple is added in this table.

15.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for table VEONAME

Table 3 Table field descriptions

Field	New or Changed	Entry	Explanation and action
VEONAME	New	CHAR VECTOR (16)	The table key specifies the Virtual End Office Name.

15.6.2.1.5 Datafill example

The following example shows sample datafill for tableVEONAME.

Table VEONAME:

```
VEONAME
--------------------
ENDOFFICE1
ENDOFFICE2
```

15.6.2.1.6 Table release history update

New table VEONAME is created.

15.6.2.1.7 Supplementary information

None.

15.6.2.1.8 Translation verification and other tools

Not applicable.

15.6.2.2 Name : XLAPLAN

Translation Plan.

15.6.2.2.1 Functional description

Table XLAPLAN contains the translation plans for all the line agents which are datafilled in table LINEATTR. Table LINEATTR contain a field indicating the translation plan for the agent and is key to the table XLAPLAN.

A new options VEONAME is added to table XLAPLAN. This option provides an association between the originating line/trunk agent and Virtual End Office (VEO) . This provides the flexibility to partition the DMS100/CS2000 into multiple virtual end offices. .

15.6.2.2.2 Usage sequence and implications (CM Only)

Table VEONAME must be provisioned prior to adding option VEONAME in table XLAPLAN.

The functionality provided by LPIC Privilege Routing is not provided until option VEONAME is provisioned for the line/trunk agent in table XLAPLAN.

15.6.2.2.3 Size

The size of table XLAPLAN is unchanged.

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory

15.6.2.2.4 Fields/OIDs

The following table lists fields/OIDs for table XLAPLAN

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTION	changed	refinement	VEONAME refinement	adding new option - VEO name

15.6.2.2.5 Datafill example

The following example shows sample datafill for table XLAPLAN.

```
Table XLAPLAN:

XLAPIDX  SCRNCLHSTS  PRTNMZEROMPOS RESINF  OPTIONS  ADMINF
-------------------------------------------------------------------------------------------
613_P621_0  FR01  613   P621  TSPS Y  RESGRP 0 2 VEONAME ENDOFFICE1   $
```

15.6.2.2.6 Table release history update

Option VEONAME is added in table XLAPLAN for LPIC Privilege Rouing Capability.

15.6.2.2.7 Supplementary information

None.

15.6.2.2.8 Translation verification and other tools

Refer to Figure 1 on page 100 for Traver of the call using new option VEONAME in table XLAPLAN.

15.6.2.3 Name : CXGRP

Customer Group Options.

15.6.2.3.1 Functional description

Table CXGRP (Customer Group Options) is required in local or combined local/toll switches to define the options associated with a PX digital trunk. The PX agent tuple in table TRKGRP contains the field for PX Customer Group to index into table CXGRP.

A new option VEONAME is added in Table CXGRP. Option VEONAME provides an association between the originating PX trunk agent and the Virtual End Office (VEO). This provides the flexibility to partition the DMS100/ CS2000 into multiple virtual end offices.

15.6.2.3.2 Usage sequence and implications (CM Only)

Table VEONAME must be provisioned prior to adding option VEONAME in table CXGRP.

The functionality provided by LPIC Privilege Routing is not provided until optionVEONAME is provisioned for the PX trunk agent in table CXGRP.

15.6.2.3.3 Size

The size of table CXGRP is unchanged.

Table 5 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory

15.6.2.3.4 Fields/OIDs

The following table lists fields/OIDs for table CXGRP

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTION	changed	refinement	VEONAME refinement	adding new option - VEO name

15.6.2.3.5 Datafill example

The following example shows sample datafill for CXGRP.

```
Table CXGRP:

CUSTKEY SPB CTD FCTDNTER FCTDNTRA FCTDINT EWATS EWATSI
PXOPTION
-----------------------------------------------------------------------------------------
50 N Y (C544) $ N N N N N (LPIC C541 Y) VEONAME ENDOFFICE2 $
```

15.6.2.3.6 Table release history update

Option VEONAME is added in table CXGRP for LPIC Privilege Rouing Capability.

15.6.2.3.7 Supplementary information

None.

15.6.2.3.8 Translation verification and other tools

For example traver with table CXGRP datafilled, see Figure 2 .

15.6.2.4 Name : LPICPXLA

IntraLATA Primary InterExchange Carrier Privilege Translation

15.6.2.4.1 Functional description

A new table LPICPXLA is implemented to provision a list of NPANXX codes to be excluded from LPIC routing on per VEO basis.

Table LPICPXLA is accessed during call processing for originating agent when table XLAPLAN entry for the agent's pretranslator has option VEONAME assigned and the VEONAME option value is provisioned in table VEONAME amd the SOC, EQA00032 'LPIC Privilege Routing' is turned ON.

15.6.2.4.2 Usage sequence and implications (CM Only)

Table VEONAME must be provisioned prior to adding a new privilege code in table LPICPXLA.

15.6.2.4.3 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LPICPXLA	0	n/a	The table will be using 1 digilator pool (32k-1 digit blocks) for storing NPANXX codes. Max size of this table depeneds upon the digits pattern used for NPANXX codes.

15.6.2.4.4 Fields/OIDs

The following table lists fields/OIDs for table LPICPXLA

Table 7 Table field descriptions

Field	New or Changed	Entry	Explanation and action
PRIVCODE	New	Key1 : VEONM VEO_NAME (String range 0-999) Key2 : DIGITS DIGIT_REGISTER	Key 1 specifies the originating subscriber's Virtual End Office Name. Key 2 specifies NPANXX codes provisioned for each VEONAME.

15.6.2.4.5 Datafill example

The following example shows sample datafill for table LPICPXLA.

Table LPICPXLA:

```
                    PRIVCODE
---------------------------------
ENDOFFICE1     919484
ENDOFFICE2     212782
```

15.6.2.4.6 Table release history update

New table LPICPXLA is created.

15.6.2.4.7 Supplementary information

None.

15.6.2.4.8 Translation verification and other tools

The following example shows the output from Traver when it is used to verify table LPICPXLA and table XLAPLAN.

Figure 1 EQA00032 is ON & LPICPXLA datafilled

```
traver l 5206000 19195282112 b
TABLE LINEATTR
0 1FR NONE NT 0 0 NILSFC 0 NIL NIL 00 619_POT1_0 LPOT_L123_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
619_POT1_0 NSCR 619 POT1 RTE1 Y RES1 0 0 VEONAME VEO2$ $
TABLE RATEAREA
LPOT_L123_0 LPOT NIL L123 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE LENFEAT
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
AIN Orig Attempt TDP: no subscribed trigger.
TABLE STDPRTCT
POT1 ( 1) ( 1) 7
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . 1919 199 N DD 1 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE HNPACONT
619 Y 919 8 ( 114) ( 1) ( 0) ( 0) 1 $
 . SUBTABLE HNPACODE
 . 919 919 FRTE 919
 . SUBTABLE RTEREF
 .  919 N D ISUPIT4DIG 0 N N
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
LNP Info: Called DN is not resident.
LNP Info: HNPA results are used.
TABLE LCASCRCN
619 LPOT ( 29) OPTL N N Y
 . SUBTABLE LCASCRN
 . TUPLE NOT FOUND.  DEFAULT IS NON-LOCAL
TABLE PFXTREAT
OPTL DD N DD UNDT
TABLE LENFEAT
HOST 04 0 00 17 S LPIC LPIC CAR1 Y
TABLE LENFEAT
HOST 04 0 00 17 S PIC PIC CAR2 Y

<continued>
```

```
TABLE LATAXLA
TUPLE NOT FOUND
ASSUMED TO BE DEFAULT INTRALATA, INTRASTATE, STD
TABLE LPICPXLA
VEO1 919528
OPERATING TELCO WILL HANDLE THIS CALL
AIN Info Collected TDP: no subscribed trigger.
AIN Info Analyzed TDP: no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 ISUPIT4DIG              9195282112                ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 ATB

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>
```

Figure 2 PX trunks - EQA00032 is ON & LPICPXLA not datafilled

EXAMPLE of PX trunk datafilled for a different LPIC in table CXGRP:

Note that Table CXGRP does not show up in TRAVER
-- but since it is datafilled with LPIC option and carrier 288, the TRKGRP's choice of 212 is changed to carrier 288 during translations.

The trunk group is also datafilled for VEONAME option, so this call could be routed as a privilege call (non-EA), however, since table LPICPXLA is not datafilled, it is routed as an EA call.

table CXGRP:

```
------------
CUSTKEY SPB CTD FCTDNTER FCTDNTRA FCTDINT EWATS EWATSI PXOPTION
-------------------------------------------------------------------
51 N N N N N N N  ( LPIC 288 Y )  (VEONAME  VEO2 ) $:

 >traver tr CARYPX 5188882060 b
TABLE TRKGRP
CARYPX PX 10 ELO NCRT IC NIL MIDL N P621 PBX1 613 613 LCL NONE TSPS L613 N N 51  <--- CXGRP index
   NIL 6211234 DIALTN N Y 212 Y LATA1  N $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE STDPRTCT
P621 ( 1) ( 0) 1
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . 518 60 N NP 0 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE HNPACONT
613 Y 915 2 ( 74) ( 1) ( 0) ( 0) 2 $
 . SUBTABLE HNPACODE
 . 518 518 FRTE 9
 . SUBTABLE RTEREF
 .   9 T IBNRTE 6
 . . TABLE IBNRTE
 . .   6 N N N N N LLOOPLEAS 0
 . . EXIT TABLE IBNRTE
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
LNP Info: Called DN is not resident.
LNP Info: HNPA results are used.
TABLE LCASCRCN
613 L613 ( 56) OPTL N N Y
 . SUBTABLE LCASCR
 . TUPLE NOT FOUND.  DEFAULT IS NON-LOCAL
...
( con't PX TRUNK traver)-->
```

(con't PX TRUNK traver)-->
...
TABLE PFXTREAT
OPTL NP N DD UNDT
.TABLE PFXTREAT
OPTL NP N DD UNDT
TABLE CLSVSCRC
KEY NOT FOUND
TABLE LATAXLA
TUPLE NOT FOUND
ASSUMED TO BE DEFAULT INTRALATA, INTRASTATE, STD
TABLE LPICPXLA
TUPLE NOT FOUND
TABLE OCCINFO
288 0288 FGC Y Y Y Y N N N Y Y Y Y LONG 0 FGRPC N N N N N N N N Y N N N N N Y
TABLE EASAC
TUPLE NOT FOUND
OVERLAP CARRIER SELECTION (OCS) DOES NOT APPLY - AIN_OFFICE_TRIGGRP DEFINED
TABLE STDPRTCT
P621 (1) (0) 1
. SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO
DOCUMENTATION.
. **1010288 1010288 EA DD 7 P 2881 288 Y OFRT 888 6 20 N**
. SUBTABLE AMAPRT
. KEY NOT FOUND
. DEFAULT VALUE IS: NONE OVRNONE N
. . **TABLE OFRT**
. . 888 CND EA INTNL SK 2
. . S D OGEAATT
. . CND ALWAYS SK 1
. . TS D OGEAATT 0 1 N 6 N
. . EXIT TABLE OFRT
. TABLE STDPRTCT
. ATT1 (1) (0) 5
. . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO
DOCUMENTATION.
. . 5 9 EA DD 0 T NA ATT N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE OFCVAR
+++ TRAVER: SUCCESSFUL CALL TRACE +++
DIGIT TRANSLATION ROUTES

1 OGEAATT 5188882060 ST

+++ TRAVER: SUCCESSFUL CALL TRACE +++

15.7 Service Orders (SO) (CM & SESM)

Not Applicable.

15.8 Software optionality control (SOC)

Table 8 SOC

SOC option name:	VEO LPIC Privilege
SOC option title:	Yes
SOC option control type:	state
New SOC option?	Yes
SOC option order code	EQA00032
Option defined in DRU:	CNA
Affected products:	NA

15.9 Element Management

Not Applicable.

15.10 User interface changes

Not Applicable.

15.11 OSSGate Interface Changes

Not Applicable.

15.12 Security

Not Applicable.

15.13 Configuration Walkthrough

Following are the provisioning steps required in order to use the LPIC Privilege Routing feature:

1. Add the tuples in table VEONAME with valid VEO names.

2. Add the new option VEONAME in table XLAPLAN/CXGRP with valid VEO names from table VEONAME.

3. Add the tuple in table LPICPXLA containing combination of VEO name and NPANXX privilege codes.

4. Turn the SOC EQA00032 to state ON.

Now the switch is configured to use the new LPIC Privilege routing functionality.

To revert back to the existing LPIC privilege routing functionality, turn the SOC EQA00032 to IDLE state

16: Configuration (CN): A00009129

16.1 Feature Name

Controlled Hot Swact

16.2 Hardware and Software Requirements

This feature will require a cPCI SOS image based on CSP22 as well a linux ramdisk based on NCGL8.

16.3 User interface changes

16.3.1 Command: CMREXFUL

16.3.1.1 Command type:

NON-MENU

16.3.1.2 Command target:

3PC

16.3.1.3 Command availability:

RES

16.3.1.4 Command description

This command allows the crafts person to set the day of the full rex. The time of the REX test is still set via the NODEREXCONTROL tuple in table OFCVAR.

16.3.1.5 Command syntax

Table 1 CMREXFUL command parameters and variables

Command	Parameters and variables
CMREXFUL	set {MON,TUE,WED,THU,FRI,SAT,SUN} query
Parameters and variables	Description
set	Set the day of the week that full REX should be scheduled.
query	Displays the current setting for the full REX.

16.3.2 Command: CAPCI

16.3.2.1 Command type:

NON-MENU

16.3.2.2 Command target:

3PC

16.3.2.3 Command availability:

RES

16.3.2.4 Command description

This command allows the crafts person to view the CPU utilization of the call agent blade.

16.3.2.5 Changes to map output

16.3.2.5.1 Sync field change.

Table 2 MAP output from CAPCI command in CSP21

Command: CAPCI
CATMP/HR UTIL ENGCATMP ENGLEVEL SYNC CCOVRLD IDLE 1294680 63% 2032346 BELOW YES OFF NO SCHED FORE MAINT DNC AUXCP OM GTERM BKG NETM SNIP 132% 47% 3% 0% 1% 0% 0% 77% 0% 7%

The sync field will be modified to display one of the following values.

HOT/WARM/NO.

Table 3 MAP output from CAPCI command in CSP22

Command: CAPCI
CATMP/HR UTIL ENGCATMP ENGLEVEL SYNC CCOVRLD IDLE 1294680 63% 2032346 BELOW HOT OFF NO SCHED FORE MAINT DNC AUXCP OM GTERM BKG NETM SNIP 132% 47% 3% 0% 1% 0% 0% 77% 0% 7%

16.3.2.5.2 Sync field transition indicator.

If the sync state of the call agent blade has switched state within the last capci sample period, this transition was indicated by a ‘*’.

Table 4 MAP output from CAPCI command during sync transition in CSP21

Command: CAPCI

```
CATMP/HR UTIL ENGCATMP ENGLEVEL SYNC CCOVRLD IDLE
1294680  63%  2032346    BELOW  *YES     OFF   NO

SCHED  FORE MAINT   DNC AUXCP    OM GTERM   BKG  NETM  SNIP
 132%   47%    3%    0%    1%    0%    0%   77%    0%    7%
```

The transition indication will be changed to one of +/-. A '+' would indicate that the current sync state is higher than the preceding sync state. For example a '+' would be pre-pended on the sync state if the sync state transitioned from NO to WARM. A '-' would indicate that the current sync state is lower than the preceding sync state. For example a '-' would be pre-pended on the sync state if the sync state transitions from HOT to WARM.

Table 5 MAP output from CAPCI command during sync transition from NO to WARM in CSP22.

Command: CAPCI

```
CATMP/HR UTIL ENGCATMP ENGLEVEL SYNC  CCOVRLD IDLE
1294680  63%  2032346    BELOW  +WARM   OFF   NO

SCHED  FORE MAINT   DNC AUXCP    OM GTERM   BKG  NETM  SNIP
 132%   47%    3%    0%    1%    0%    0%   77%    0%    7%
```

16.3.3 Command: SWACT

16.3.3.1 Command type:

MENU

16.3.3.2 Command directory:

CCAMTC;COREMTC;CAMTC

16.3.3.3 Command target:

3PC

16.3.3.4 Command availability:

RES

16.3.3.5 Command description

The command allows the crafts person to switch the unit activity of the call agent.

This feature will modify the warning when the swact command is initiated.

Table 6 Warning message from SWACT command prior to NCGL8/SN09.

Command: SWACT
WARNING: This action will result in a CALL PROCESSING OUTAGE. The SwAct command switches unit activity, followed by an application warm restart. Please confirm ("YES", "Y", "NO", or "N"):

Table 7 Warning message from SWACT command in NCGL8/SN09.

Command: SWACT
WARNING: This action will result in a brief denial of new originations. Existing calls are unaffected. The SwAct command switches unit activity. Please confirm ("YES", "Y", "NO", or "N"):

17: Configuration (CN): A00009189

17.1 Feature Name

SESM Support for 64 Character FQDN

17.2 Hardware and Software Requirements

This feature requires SN09 SESM/Core/GWC loads be installed successfully.

17.3 Initial Configuration

No additional initial configuration step is required by this feature.

17.4 Office/Subnet parameters (OP/SP) (CM & SESM)

None.

17.5 Upgrade Considerations

None.

17.6 Data schema (DS) (CM, MIBS, RDB)

17.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified MIBs and database schema

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MIB		
GWC-GW-MIB	Changed	New
GWC-ENDPOINT-MIB	Changed	New
GWC-EPID-GRP-MIB	Changed	New
GWC-RMGC-MIB	Changed	New
SESM/GWCEM Database Schema		
GWCEM.GATEWAY	Changed	New
GWCEM.GWDOMAIN	New	New
GWCEM.GATEWAYPROFILE	Changed	Old
GWCEM.GWROOTITRANSMIDDLEBOXES	Changed	Old
GWCEM.GLOBALIDS	New	New

Note: 1) For the MIBs in list above, the old table are deprecated from this release onward. 2) The gateway controller will not support the old MIB table.

17.6.2 MIB GWC-GW-MIB

17.6.2.1 Name: gateWayTableV2

.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.legacyCallServer.lcsGateWayController.gwcGwMIB.gateWayTableV2

17.6.2.1.1 Functional description

From SN09,GWC will use the new table gateWayTableV2 to do corresponding SNMP operations.The difference between new table and old table are;1, expand gateWayName size to 64 characters. 2, Add 32 bits gateWayID. 3, Remove useless columns gateWayHeartBeat and gateWayConnset.

17.6.2.1.2 Usage sequence and implications (CM Only)

Not applicable.

17.6.2.1.3 Size

Same as old table.

17.6.2.1.4 Fields/OIDs

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
gateWayID	New		1	
gateWayNameV2	New		2	
gateWayAddressV2	New		3	
gateWayTypeV2	New		4	
gateWayLgrpV2	New		5	
gateWayProtocolV2	New		6	
gateWayProtVersV2	New		7	
gateWayPortV2	New		8	
gateWayProfileV2	New		9	
gateWayAdjacentMiddleBoxIDV2	New		10	
gateWayEntryStatusV2	New		11	

17.6.2.1.5 Datafill example
Not applicable.

17.6.2.1.6 Table release history update
Not applicable.

17.6.2.1.7 Supplementary information
Not applicable.

17.6.2.1.8 Translation verification and other tools
Not applicable.

17.6.3 MIB GWC-ENDPOINT-MIB

17.6.3.1 Name: endPointTableV2
.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.legacyCallServer.lcsGateWayController.gwcEndPointMIB.endPointTableV2

17.6.3.1.1 Functional description
From SN09,GWC will use the new table endPointTableV2 to do corresponding SNMP operations.The difference between new table and old table is epidGWID repalces endPointGW in V2 table.

17.6.3.1.2 Usage sequence and implications (CM Only)

17.6.3.1.3 Size
Same as old table.

17.6.3.1.4 Fields/OIDs

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
epidGWID	New		1	
endPointNameV2	New		2	
endpointTNV2	New		3	
endPointNNV2	New		4	
endPointServStatusV2	New		5	
endPointEntryStatusV2	New		6	

17.6.3.1.5 Datafill example
Not applicable.

17.6.3.1.6 Table release history update
Not applicable.

17.6.3.1.7 Supplementary information
Not applicable.

17.6.3.1.8 Translation verification and other tools
Not applicable.

17.6.4 MIB GWC-EPID-GRP-MIB

17.6.4.1 Name: epidGrpTableV2
.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.legacyCallServer.lcsGateWayController.gwcEpidGrpMIB.epidGrpTableV2

17.6.4.1.1 Functional description
From SN09,GWC will use the new table epidGrpTableV2 to do corresponding SNMP operations.The difference between new table and old table is epidGrpGWID repalces gatewayName in V2 table.

17.6.4.1.2 Usage sequence and implications (CM Only)
Not applicable.

17.6.4.1.3 Size
Same as old table.

17.6.4.1.4 Fields/OIDs

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
epidGrpGWID	New		1	
epidGrpNameV2	New		2	
epidGenerationDescV2	New		3	
nodeNoV2	New		4	
firstTnV2	New		5	
noOfPortsV2	New		6	
v52InterfacesidV2	New		7	
v52LinkidV2	New		8	
v5UALinkidV2	New		9	
priInterfaceidV2	New		10	

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
epidGrpEntryStatusV2	New		11	

17.6.4.1.5 Datafill example
Not applicable.

17.6.4.1.6 Table release history update
Not applicable.

17.6.4.1.7 Supplementary information
Not applicable.

17.6.4.1.8 Translation verification and other tools
Not applicable.

17.6.5 MIB GWC-RMGC-MIB

17.6.5.1 Name: gwToGwcTableV2
.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.legacyCallServer.lcsGateWayController.gwcRmgcDataMIB.gwToGwcTableV2

17.6.5.1.1 Functional description
From SN09,GWC will use the new table gwToGwcTableV2 to do SNMP operations.The difference between new table and old table is gwFQDNV2 is expanded to 64 characters.

17.6.5.1.2 Usage sequence and implications (CM Only)
Not applicable.

17.6.5.1.3 Size
Same as old table.

17.6.5.1.4 Fields/OIDs

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
gwFQDNV2	New		1	
gwcFQDNV2	New		2	
gwEntryStatusV2	New		3	

17.6.5.1.5 Datafill example
Not applicable.

17.6.5.1.6 Table release history update
Not applicable.

17.6.5.1.7 Supplementary information
Not applicable.

17.6.5.1.8 Translation verification and other tools
Not applicable.

17.6.6 Database Schema: GWCEM.GATEWAY

17.6.6.1 Functional description
This table is used to store provisioned gateway entries, 2 fields will be impacted.

17.6.6.2 Fields

Table 2 Modified/Added fields

Field	New/ Changed	Entry	Explanation and action
GATEWAYNAME	Changed	VARCHAR2 (64) NOT NULL	Length will be extended to 64, used to store gateway hostname.
GATEWAYINDEX	New	INTEGER NOT NULL	Gateway index number.

17.6.6.3 Limitations
Field GATEWAYNAME is primary key, so gateway hostname must be completely unique across entire office.

17.6.7 Database Schema: GWCEM.GWDOMAIN

17.6.7.1 Functional description
This new table is used to store provisioned gateway domain name.

17.6.7.2 Fields

Table 3 Fields descriptions

Field	New/ Changed	Entry	Explanation and action
GWCID	New	VARCHAR2 (32) NOT NULL	Indicates which GWC this Gateway Domain Name belongs to. Refer to table “GWCEM.GWCNODE“.
DOMAINNAME	New	VARCHAR2 (64) NOT NULL	Gateway domain name.
DOMAININDEX	New	INTEGER NOT NULL	Gateway domain global index number.

17.6.8 Database Schema: GWCEM.GATEWAYPROFILE

17.6.8.1 Functional description

This table stores all data of gateway profiles, new column will be added into this table.

17.6.8.2 Fields

Table 4 New Field

Field	New/ Changed	Entry	Explanation and action
FQDN_SUPPORTED	New	VARCHAR2 (5)	Indicate whether the default gateway domain name is supported by this profile. Available values are “true” and “false”. String “false” indicates “not support”, string “true” indicates “support”. The default value is “false”.

17.6.9 Database Schema: GWCEM. GWROOTITRANSMIDDLEBOXES

17.6.9.1 Functional description

Expand gatewayname from 32 charaters to 64 characters.

17.6.9.2 Fields

Table 5 New Field

Field	New/ Changed	Entry	Explanation and action
GATEWAYNAME	Changed	VARCHAR2 (64)	To support 64 character FQDN.

17.6.10 Database Schema: GWCEM. GLOBALIDS

17.6.10.1 Functional description

This new added table stores global id of different device.

17.6.10.2 Fields

Table 6 New Field

Field	New/ Changed	Entry	Explanation and action
IDTYPE	New	NUMBER NOT NULL	Indicate 8 bits device type that the GID belongs to.
CALLAGENTID	New	NUMBER NOT NULL	Indicate 8 bits CallAgent ID.
KEY	New	NUMBER NOT NULL	Indicate 16 bits key which is unique on IDTYPE and CALLAGENTID.
GLOBALID	New	NUMBER NOT NULL	Indicate 32 bits GID which is unique accross all device type and call agent id.

17.7 Service Orders (SO) (CM & SESM)

None.

17.8 Software optionality control (SOC)

None.

17.9 Element Management

FQDN support was introduced in SN07/SN08, a “dummy” gateway need to be added which created the suffix or domain name for all the gateways on a GWC. The remaining gateways were provisioned using its unique prefix, or hostname. The domain of the ‘dummy’ gateway then could be appended to the end of all NCS and DNS signaling at call processing time.

In SN09, the procedure of domain name configuration is changed. Customer could set a default gateway domain name when adding GWC node. If provisioned, the default gateway domain name will be applied to all the gateways on this GWC (if the gateway profile supports FQDN). The name which customer filled when associating media gateway will be gateway hostname. The gateway FQDN will be concatenation of gateway hostname and default gateway domain name.

In SN09, if customer does not fill default gateway domain name when adding GWC node. No default gateway domain name will be used, customer can fill in FQDN-liked name when associating media gateway (if the gateway profile supports FQDN). The gateway hostname and FQDN will be the same, as the name user filled.

17.9.1 New/modified GUIs

Table 7 New or modified GUIs

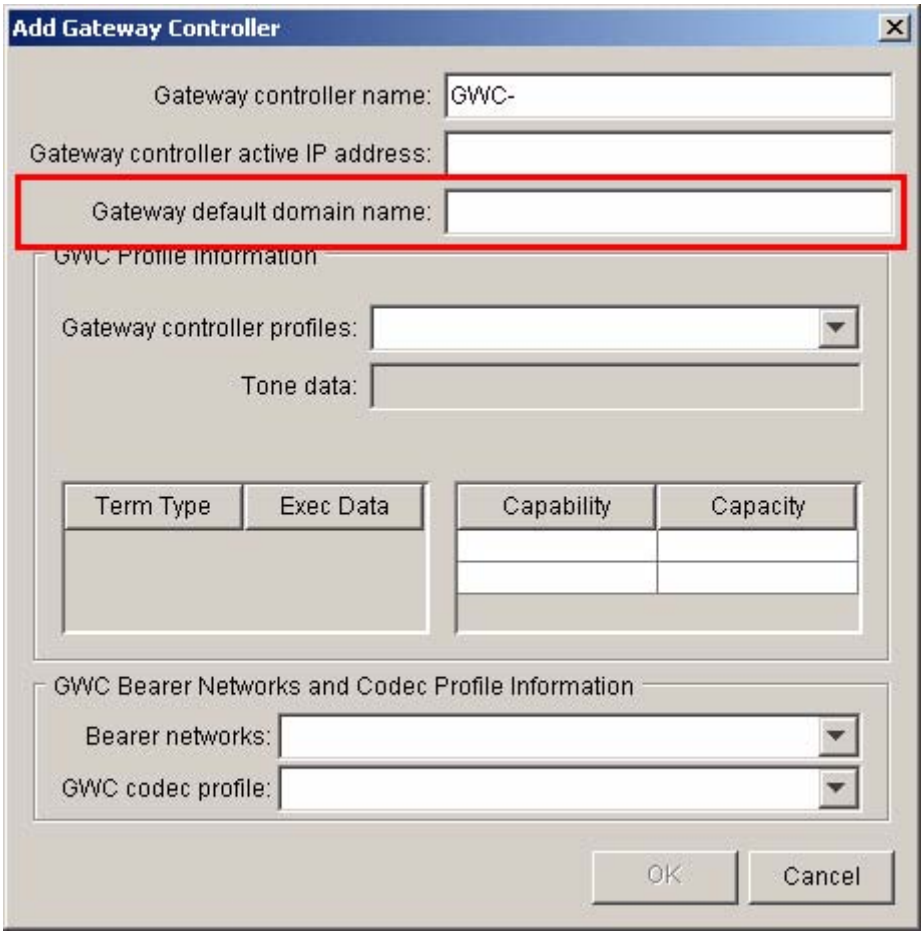
GUI name	NEW, CHANGED, or DELETED
GWCEM	Changed

17.9.2 GUI information

17.9.2.1 GUI name: Add GWC node

This dialog is used to add GWC node by customer. New field “Gateway default domain name” is added in SN09. This field is optional, customer could fill in if default gateway domain name is required. If customer does not fill it when adding GWC node, no default gateway domain name will be set.

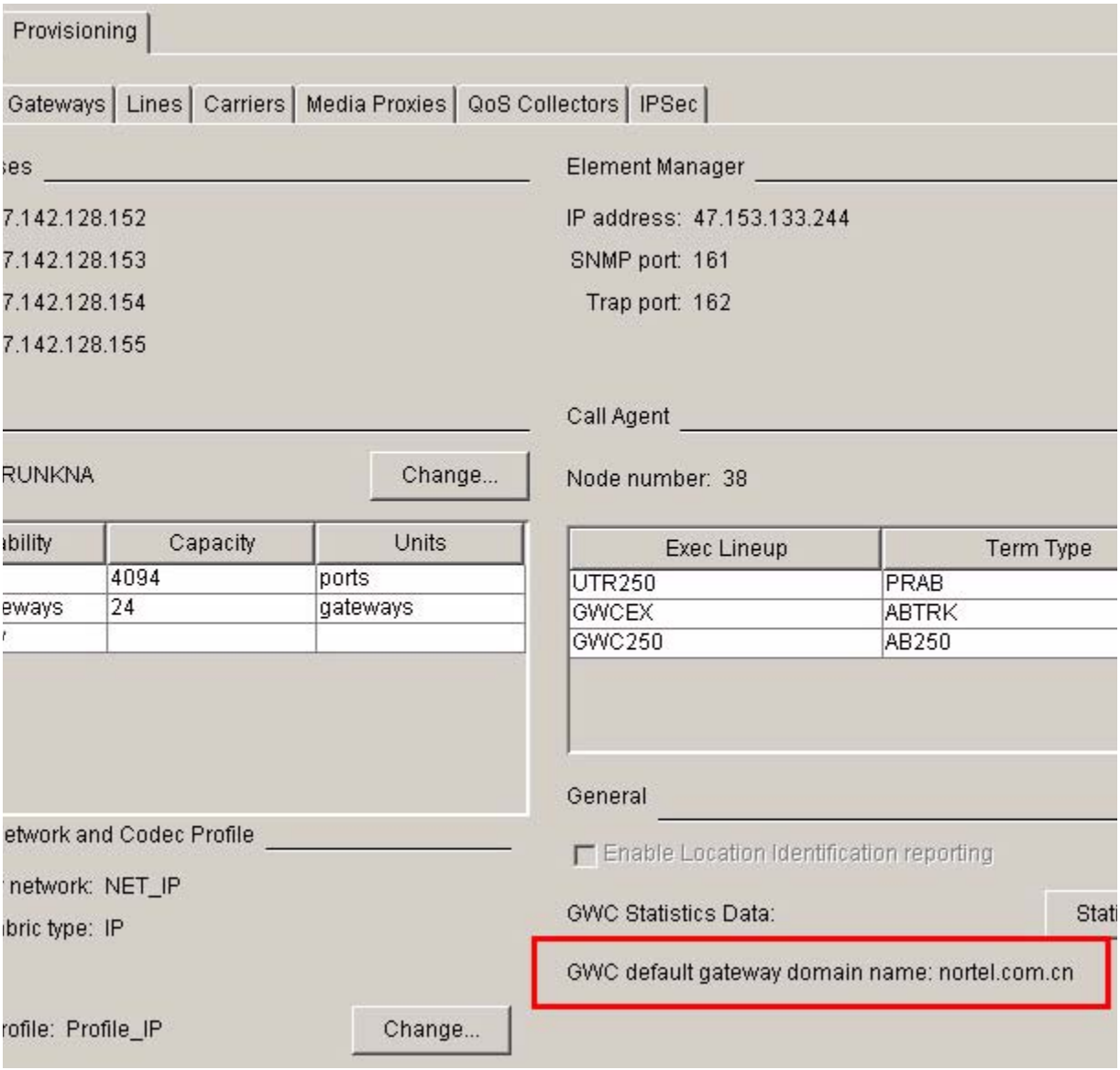
Figure 1 Add GWC node GUI



17.9.2.2 GUI name: GWC provisioning panel

The GWC default gateway domain name will be displayed on right bottom corner of GWC provisioning panel. If no default gateway domain name provisioning on this GWC, it will be displayed as “<Not Configured>”.

Figure 2 GWC provisioning panel GUI



17.9.3 CLUI Interface

None.

17.10 User interface changes

17.10.1 Directory: N/A

17.10.2 Command: QGW

17.10.2.1 Command type: NON-MENU

17.10.2.2 Command target: All

17.10.2.3 Command availability: RES

17.10.2.4 Command description

Table LNENDPT is sorted by LENs and may contain up to 150,000 tuples. Therefore, finding all the LENs & Endpoints for a particular Gateway can be somewhat difficult.The Query Gateway Tool (QGW) is a tool on the CM that can be used to output all the LENs and Endpoints for the specified Gateway in table LNENDPT.

17.10.2.5 Command syntax

Table 8 <CommandName> command parameters and variables

Command	Parameters and variables
QGW	Parms: <GATEWAY> STRING
Parameters and variables	Description
GATEWAY	Displays LENs & Endpoints for the specified Gateway.

17.10.2.6 Qualifications and warnings

None.

17.10.2.7 Responses

17.10.2.7.1 <response>

Table 9 Command outputs with associated meanings and actions

Command
Command: qgw <Gateway name listed in table LNENDPT> Response: ---------- LEN: LG 00 0 00 00 ENDPOINT: aaln/1 LEN: LG 00 0 00 01 ENDPOINT: aaln/2 ---------- **Meaning:** This response means that the specified Gateway has 2 LENs/Endpoints in table LNENDPT and they are displayed in the response. **System or user actions:** No actions required.
Command: help qgw Response: COMMAND: Query Gateway Outputs all the LENs & Endpoints in table LNENDPT associated with the Gateway. Parms: <GATEWAY> STRING Meaning: This response displays help information for QGW. System or user actions: No actions required.
Command: qgw Response: Next par is: <GATEWAY> STRING Enter: <GATEWAY> Meaning: This response is prompting the user for the GATEWAY name. System or user actions: Enter a Gateway name.

Table 9 Command outputs with associated meanings and actions

Command
Command: qgw <Gateway name not listed in table LNENDPT> Response: ERROR - Gateway Name does not exist in table LNENDPT **Meaning:** This response means that the specified Gateway does not exist in table LNENDPT. **System or user actions:** Check to see if the Gateway name is spelled correctly and re-enter command. If still not found, then check for the Gateway existence in SESM.

17.10.2.8 Example

Table 10 Usage examples for QGW command

Description of task:	
Description of task	qgw 'sbv-10.com6.net'
Command: Command response:	---------- LEN: LG 00 0 00 00 ENDPOINT: aaln/1 LEN: LG 00 0 00 01 ENDPOINT: aaln/2 ----------

17.11 OSSGate Interface Changes

17.11.1 XML Command Changes

When user specify a gateway operation, such as assocMG, disAssocMG, changeMG or addGWCtoCS, system will allow user to input either gateway host name only or the full FQDN name.

17.11.1.1 Command XML

17.11.1.1.1 Add GWC command

A new parameter, gwDefaultDomainName, will be added into the Add GWC xml command which is like the following:

Add GWC to CS XML command

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <addGWCtoCS usn="1" version="1.0">
        <Parameters>
          <csUIName>COMPACT6</csUIName>
          <gwcUIName>GWC-10</gwcUIName>
          <profileName>LARGE_LINENA</profileName>
          <gwcActvIp>47.128.142.156</gwcActvIp>
          <gwcSnmpPort>161</gwcSnmpPort>
          <bearerNetworkName>NET_IP</bearerNetworkName>
          <bearerFabricType>IP</bearerFabricType>
          <codecProfileName>Profile_IP</codecProfileName>
          <termType>POTS</termType>
          <termType>KEYSET</termType>
          <execLineup>POTSEX</execLineup>
          <execLineup>KSETEX</execLineup>
          <gwDefaultDomainName>nortel.com.cn</gwDefaultDomainName>
        </Parameters>
      </addGWCtoCS>
    </Methods>
  </Command>
</CommandList>
```

17.11.1.1.2 disAssocMG XML command

Both gateway hostname and gateway full FQDN name are allowed to input when user want to delete the gateway from system.

disAssocMG XML command with full FQDN name

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <disAssocMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>test1.nortel.com.cn</mgUIName>
        </Parameters>
      </disAssocMG>
    </Methods>
  </Command>
</CommandList>
```

disAssocMG XML command with gateway host name

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <disAssocMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>test1</mgUIName>
        </Parameters>
      </disAssocMG>
    </Methods>
  </Command>
</CommandList>
```

17.11.1.1.3 Change MG XML command

Similar with other OSSGate interface, the change gateway interface also changed to support both gateway hostname and full FQDN name.

The xml command is like the following:

Change MG XML command with full FQDN name

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<CommandList >
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
      <Methods>
        <changeMG usn="1" version="1.0">
          <Parameters>
            <mgUIName>test1.nortel.com.cn</mgUIName>
            <reservedTerminations>16</reservedTerminations>
          </Parameters>
      </changeMG>
    </Methods>
  </Command>
</CommandList>
```

Change MG XML command with only hostname

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<CommandList >
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
      <Methods>
        <changeMG usn="1" version="1.0">
          <Parameters>
            <mgUIName>test1</mgUIName>
            <reservedTerminations>16</reservedTerminations>
          </Parameters>
      </changeMG>
    </Methods>
  </Command>
</CommandList>
```

17.11.1.2 Response XML

17.11.1.2.1 QueryGWC response

The gateway domain name that is added with the GWC will be included in the response when user perform a QueryGWC request.

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
 <Response>
 <Interface>cs2kCfgMgrIf</Interface>
  <Methods>
   <queryGWC usn="1" version="1.0">
   <ReturnData>
    <Row>
     <gwcUIList>GWC-10</gwcUIList>
     <gwcIpList>47.142.128.156</gwcIpList>
     <callServerId>COMPACT6</callServerId>
     <nodeName>GWC 10</nodeName>
     <typeList>1</typeList>
     <typeList>6</typeList>
     <typeList>7</typeList>
     <typeList>15</typeList>
     <typeList>16</typeList>
     <xacNodeNumber>27</xacNodeNumber>
     <actvIpAddress>47.142.128.156</actvIpAddress>
     <snmpPort>161</snmpPort>
     <mktTones>NORTHAA</mktTones>
     <termTypes>POTS</termTypes>
     <termTypes>KEYSET</termTypes>
     <pmExecs>POTSEX</pmExecs>
     <pmExecs>KSETEX</pmExecs>
     <capacity>6400</capacity>
     <externalIP>NOT_YET_SUPPORTED</externalIP>
     <externalPort>0</externalPort>
     <bearerNetworkName>NET_IP</bearerNetworkName>
     <bearerFabricType>IP</bearerFabricType>
     <codecProfileName>Profile_IP</codecProfileName>
     <gwDefaultDomainName>nortel.com.cn</gwDefaultDomainName>
    </Row>
    <RC>0</RC>
    <MsgTxt>Query of a Single GWC was successful</MsgTxt>
   </ReturnData>
   </queryGWC>
  </Methods>
 </Response>
</CommandList>
```

17.11.2 Additional OSSGate Changes

None.

17.12 Security

None.

17.13 Configuration Walkthrough

Provisioning/configuring component software and services.

18: Configuration (CN): A00009190

18.1 Feature Name

Universal Carrier Protocol (UCP) C7UPTMR Enhancements

18.2 Hardware and Software Requirements

N/A

18.3 Initial Configuration

N/A

18.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

18.5 Upgrade Considerations

Currently, the XPM patch XIX20, is used to hardcode the ACM timer value to 20 secs for UCS trunks. When the switch is upgraded to SN09 core load, this patch XIX20 will be Obsoleted. New patch, XHW10 for DTC should be applied to support provisionable timers on a per trunk basis for UCP Trunks. When trunks hosted on DTCs are used, this patch will allow the datafilled ISUP timer value to be used during CallP.

After applying the patch perfom the following actions to set the ISUP Timers for ISUP UCP protocol trunks.

- Datafill table C7UPTMR for UCP Potocol with the required timer value.
- Datafill TRKSGRP to change the TMRNAME field to the datafilled C7UPTMR index.

18.5.1 Dump and Restore (CM)

18.5.2 Element Management Upgrade

18.5.3 Downgrade impact

18.6 Data schema (DS) (CM, MIBS, RDB)

18.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
C7UPTMR	CHANGED	NEW

18.6.2 Table/MIB/Remote Database Schema information

18.6.2.1 Name: C7UPTMR

C7UP Timer

18.6.2.1.1 Functional description

Table C7UPTMR provides the ability to provision various ISUP timer values on a per-protocol and direction basis.

18.6.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

18.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
C7UPTMR	0	30	No Change to memory Allocation by this activity

18.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for C7UPTMR.

<conditional information>

Table 3 C7UPTMR Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
TMRKEY	Unchanged	No	Char Vector	
C7UPDIR	Unchanged	No	IC,OG,2W	Trunk Direction

Table 3 C7UPTMR Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PROT	Changed	Yes The Refinement based on PROT and C7UPDIR	Q764, UCS, CCITT, UCP	EXTERNAL_PROTOCOL_TYPE This Field is used specify the ISUP protocol Variant. UCP Protocol is supported by this activity
C7UPDIR = IC area Refinemenrt				
COT	Existing	YES	10 TO 15	Timer Range
RLCSREL	Existing	YES	4 TO 15	
RLCLREL	Existing	YES	60 TO 60	
ICCR	Existing	YES	16 TO 20	
SCCR	Existing	YES	180 TO 300	
RLCSRSC	Existing	YES	4 TO 15	
RLCLRSC	Existing	YES	60 TO 60	
C7UPDIR = OG area Refinemenrt				
TONE	Existing	YES	2 TO 2	
ACM	Existing	YES	20 TO 30	
RLCSREL	Existing	YES	4 TO 15	
RLCLREL	Existing	YES	60 TO 60	
IRETEST	Existing	YES	1 TO 10	
SRETEST	Existing	YES	60 TO 180	
RLCSRSC	Existing	YES	4 TO 15	
RLCLRSC	Existing	YES	60 TO 60	
LPA	Existing	YES	2 TO 2	
C7UPDIR = 2W area Refinemenrt				

Table 3 C7UPTMR Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
COT	Existing	YES	10 TO 15	
TONE	Existing	YES	2 TO 2	
ACM	Existing	YES	20 TO 30	
RLCSREL	Existing	YES	4 TO 15	
RLCLREL	Existing	YES	60 TO 60	
IRETEST	Existing	YES	1 TO 10	
SRETEST	Existing	YES	180 TO 300	
ICCR	Existing	YES	16 TO 20	
SCCR	Existing	YES	180 TO 300	
RLCSRSC	Existing	YES	4 TO 15	
RLCLRSC	Existing	YES	60 TO 60	
LPA	Existing	YES	2 TO 2	

18.6.2.1.5 Datafill example

The following example shows sample datafill for table C7UPTMR

Figure 1 Examples of the C7UPTMR Datafill

```
TABLE C7UPTMR
UCP2W 2W UCP 13 2 30 6 60 10 180 20 200 13 60 2 $
UCPIC IC UCP 13 6 60 20 200 13 60 $
UCPOG OG UCP 2 25 6 60 10 180 13 60 2 $
```

18.6.2.1.6 Table release history update

- UCP ISUP Protocol variant is supported in SN09 for table C7UPTMR, field PROT (External_Protocol_Type).

18.6.2.1.7 Supplementary information

Table TRKSGRP provides the ability to provision C7UPTMR index per trunk subgroup basis in field TMRNAME. The provisioned timers values are used for ISUP Protocol call processing.

18.6.2.1.8 Translation verification and other tools

C7UPTMR does not use translation verification tools.

18.7 Service Orders (SO) (CM & SESM)

N/A

18.8 Software optionality control (SOC)

Table 4 SOC UCSB0001

SOC option name:	UCSB Enhance UCPC7 timer
SOC option title:	Yes
SOC option control type:	Track
New SOC option?	Yes
SOC option order code	UCSB0001
Option defined in DRU:	UCS
Affected products:	SN000009, SNC00009

18.9 Element Management

N/A

18.10 User interface changes

N/A

18.11 OSSGate Interface Changes

N/A

18.12 Security

N/A

18.13 Configuration Walkthrough

N/A

19: Configuration (CN): A00009200

19.1 Feature Name

Packet Trunking Trunk Test: Milli-watt Tone Swap

19.2 Hardware and Software Requirements

For the MWTSwap command to be usable there needs to be a third party test equipment box installed. In SN09 the only supported third party test box that can run MWTSwap is the AudioCodes Media Server (AMS) series products. Once the AMS is installed the office parameter "EXTERNAL_GATEWAY_TEST_LINES" in table OFCVAR should be set to "Y". If this office parameter is set to "N" then it is assumed that the MTM is being used for test equipment and the MWTSwap command will be rejected.

19.3 User interface changes

19.3.1 Directory: MAPCI;MTC;TRKS;TTP;MANUAL

19.3.1.1 Directory description

This MAP level contains the TTP commands for manual trunk test position tests like TGEN, LOSS, etc.

19.3.1.2 Accessing directory: LEVEL MAN

19.3.1.2.1 Access to directory or MAP level and return to CI

To access the MANUAL level of the MAP enter "MAPCI;MTC;TRKS;TTP;LEVEL MAN" at the CI.

To return to the CI level enter "QUIT ALL" or simply "QUIT" to move up to the next higher level (the TTP level in this case).

19.3.2 Command: MWTSwap

19.3.2.1 Command type: Listed MENU and Unlisted MENU

The MWTSwap command is available at the general TTP level command directory as soon as the TTP level is entered. At the TTP level the command is an Unlisted Menu command. The MWTSwap command is also a Listed Menu command at the MANUAL level under the TTP level. Once the MANUAL level is entered the MWTSwap command appears in the menu.

Note: The MWTSwap command visibility at the MANUAL level is conditional on the value of the office parameter EXTERNAL_GATEWAY_TEST_LINES in table OFCVAR. If this office parameter is "Y" (Yes) then the MWTSwap command will be visible in the

menu, and the commands “LOSS” and “TGEN” will be removed from the menu (although will still be Unlisted Commands). When the office parameter is “N” (No) then the MWTSwap command will not be visible in the menu, but will still be an Unlisted command at the MANUAL level.

19.3.2.2 Command target: All

19.3.2.3 Command availability: RES

19.3.2.4 Command description

MWTSwap is a new command implemented as a single command that combines the functionality of the TGEN and LOSS commands. The new command causes a 1004 Hz tone to be generated towards the far-end switch on the posted trunk, while at the same time measuring the loss on an incoming 1004 Hz tone from the far-end switch on the selected trunk. The command should be used in a coordinated fashion with a craftsperson on the far-end switch such that the far-end switch is also generating a 1004 Hz tone at the same time so that a valid loss measurement can be taken by the near-end switch. If no tone detectable on the incoming circuit then the MAP display will indicate this through the text “No Tn” in the results area of the MAP.

The MWTSwap command supports 3 command line parameters, a frequency between 0 and 4000 Hz, a power level between -60 dB and 0 dB (in increments of 1 dB), and a test duration between 1 and 240 seconds. If no command line parameters are present the defaults of 1004Hz, 0 dB, and 60 seconds are used.

Note: Although the frequency range allowed on the command line is between 0 and 4000 Hz, the only supported frequency at this time is 1004 Hz. If any other frequency is given on the command line the command will fail with an appropriate error message.

When the MWTSwap command is entered the MAP is updated to display the frequency of the tone being generated as well as loss measurement information. The loss measurement information is updated on a regular basis (every few seconds) based on data sent from the third party test equipment. The MWTSwap command acts slightly differently from the TGEN and LOSS commands in that it runs for a specified time limit, during which time the user does not have the ability to invoke any other commands. Once the test completes it will return control to the crafts person. The upper limit on the length of the test is 4 minutes (240 seconds), with the default being 60 seconds. The upper limit was considered to be sufficiently long to allow coordination between the near-end and far0end switches in starting the test and long enough to get a stable loss reading on the trunk.

19.3.2.5 Command syntax

Table 1 MWTSwap command parameters and variables

Command	Parameters and variables
MWTSwap	Frequency, Power Level, and Test Duration
MWTSwap	F <Frequency> (0 to 4000) P <Power Level> (-60 to 0) D <Test Duration> (1 to 240)
Parameters and variables	Description
Frequency	Optional parameter. The frequency in Hz of the tone to be generated. Default is 1004 if not present on the command line.
Power Level	Optional Parameter. The power level (in decibels) of the tone to be generated. Default is 0 dB if not present on the command line.
Test Duration	Optional Parameter. The length of the test in seconds, ranging from 1 to 240 seconds. Default duration is 60 seconds if not specified on the command line.

The following is the command syntax as displayed to the user at the MAP:

```
help mwtswap
MWTSWAP-- MILLIWATT TONESWAP - GEN TONE AND MEASURE LOSS
Parms: [<FREQUENCY> {F <Frequency in Hz> {0 TO 4000}}]
       [<POWER LEVEL> {P <Power in dB> {-60 TO 0}}]
       [<TEST DURATION> {D <Duration in seconds> {1 TO 240}}]
```

Note that each of the command line parameters must be prefaced with the appropriate letter to indicate which option is being specified. For example, to specify a frequency of 1004 Hz, a power level of -6 dB and a duration of 120 seconds the command would be as follows:

```
MWTSWAP F 1004 P -6 D 120
```

It is possible to specify as many or as few options as needed on the command line. The only restriction on the optional parameters is that they must appear in the order specified in the syntax specified above. For example, the following command would be invalid and would generate the error shown:

```
MWTSWAP P -6 F 1004 D 30
USING DEFAULT FREQUENCY (1004 HZ)
EITHER incorrect optional parameter(s) OR too many parameters.
```

This is invalid as the frequency option “F” must be the first command line option if it is to be specified. Once the command interpreter sees the power level option “P” it assumes that the frequency will be the default value of 1004

Hz, and the F option is then treated as being an additional unnecessary parameter on the command line.

If no options are specified on the command line then the command will be executed with all the default values. An example of this is:

```
MWTSwap
USING DEFAULT FREQUENCY (1004 HZ)
USING DEFAULT POWER LEVEL (0 DB)
USING DEFAULT DURATION (60 SECS)
```

19.3.2.6 Qualifications and warnings

As noted above, the frequency is restricted to only 1004 Hz tones in SN09. Even though the frequency can be specified on the command line, any entry other than 1004 Hz will be rejected with an appropriate error message as follows:

```
MWTSWAP F 1005
USING DEFAULT POWER LEVEL (0 DB)
USING DEFAULT DURATION (60 SECS)
Action not supported - invalid frequency entered.
Frequency is currently restricted to 1004 Hz for MWTSWAP command.
```

19.3.2.7 Responses

19.3.2.7.1 Responses

Table 2 MAP outputs with associated meanings and actions

Command MWTSwap
"NOT ALLOWED": Error response **Meaning:** This response informs users that this command is not allowed on the posted trunk. This will occur when the office parameter "EXTERNAL_GATEWAY_TEST_LINES" in table OFCVAR is set to "N" and the MWTSwap command is executed. **System or user actions:** Check the value of the office parameter. If it is "N" then the office is not setup to use third party test equipment that supports the MWTSwap command.
"MWTSwap f 4001 Out of range: <Frequency in Hz> {0 TO 4000} Enter: <Frequency in Hz> [<POWER LEVEL>] [<TEST DURATION>]": Error response **Meaning:** The frequency parameter was entered incorrectly on the command line. **System or user actions:** Ensure that a valid frequency is entered on the command line. The allowable range is "0 to 4000".

Table 2 MAP outputs with associated meanings and actions

Command MWTSwap
“MWTSwap f 1005 USING DEFAULT POWER LEVEL (0 DB) USING DEFAULT DURATION (60 SECS) Action not supported - invalid frequency entered. Frequency is currently restricted to 1004 Hz for MWTSWAP command.”: Error response **Meaning:** The frequency parameter was entered incorrectly on the command line. **System or user actions:** Ensure that a valid frequency is entered on the command line. In SN09 the only allowable frequency value is 1004 Hz even though the rage for the parameter is shown as 0 to 400 Hz.
“MWTSwap p 10 USING DEFAULT FREQUENCY (1004 HZ) Out of range: <Power in dB> {-60 TO 0} Enter: <Power in dB> [<TEST DURATION>]”: Error response **Meaning:** The power level parameter was entered incorrectly on the command line. **System or user actions:** Ensure that a valid power level is entered on the command line. The valid range for power level is between -60 and 0 dB in steps of 1 dB.
“MWTSwap d 250 Wrong type: <Power in dB> {-60 TO 0} Enter: <Power in dB> [<TEST DURATION>]”: Error response **Meaning:** The test duration parameter was entered incorrectly on the command line. **System or user actions:** Ensure that a valid test duration is entered on the command line. The valid range for test duration is between 1 and 240 seconds.
“POST A CIRCUIT AND TRY AGAIN”: Error response **Meaning:** The command was entered without a trunk circuit posted at the MAP. **System or user actions:** Ensure that a trunk circuit is posted at the MAP and re-execute the command.
“TESTTRKANN OOS”: Error response **Meaning:** The command was entered while the test trunk announcements are out of service.. **System or user actions:** Post the test trunk announcements at the MAP and take any corrective action required to bring the announcements to an IDL state.

Table 2 MAP outputs with associated meanings and actions

Command MWTSwap
"TEST COMPLETE": Valid response **Meaning:** The test has completed successfully with no errors. **System or user actions:** None.

19.3.2.8 Example

Table 3 Usage examples for MWTSwap command

Description of task:	Generate a 1004 Hz tone at 0 dB for 60 seconds and measure loss on a trunk circuit
Command: MAP response:	Example: MWTSwap Example: USING DEFAULT FREQUENCY (1004 HZ) USING DEFAULT POWER LEVEL (0 DB) USING DEFAULT DURATION (60 SECS) TEST COMPLETE
Description of task:	Generate a 1004 Hz tone at -6 dB for 60 seconds and measure loss on a trunk circuit
Command: MAP response:	Example: MWTSwap P -6 Example: USING DEFAULT FREQUENCY (1004 HZ) USING DEFAULT DURATION (60 SECS) TEST COMPLETE
Description of task:	Generate a 1004 Hz tone at 0 dB for 120 seconds and measure loss on a trunk circuit
Command: MAP response:	Example: MWTSwap D 120 Example: USING DEFAULT FREQUENCY (1004 HZ) USING DEFAULT POWER LEVEL (0 DB) TEST COMPLETE
Description of task:	Generate a 1004 Hz tone at -20 dB for 240 seconds and measure loss on a trunk circuit
Command: MAP response:	Example: MWTSwap P -20 D 240 Example: USING DEFAULT FREQUENCY (1004 HZ) TEST COMPLETE

20: Configuration (CN): A00009207

20.1 Feature Name

DPT Trunk Testing Support

20.2 Hardware and Software Requirements

This activity requires the following:

- SOC option BAS00050 56Kb/sTrk Tst prt must be turned on
- This activity provides interface support for a new Port Identification Number in the Digital ROTL maintenance dial plan. A third party test head is required to use this interface to perform testing on DPT terminals. An example test head is the SAGE Instruments 945RTS test unit.

20.3 Initial Configuration

- SOC option activation
- Third party test head initialization

20.4 Office/Subnet parameters (OP/SP) (CM & SESM)

20.4.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCVAR	DPT_BICC_TEST_NODE	NEW	CM

20.4.2 Parameter information

20.4.2.1 DPT_BICC_TEST_NODE

DPT_BICC_TEST_NODE

20.4.2.1.1 Functional description

This parameter identifies the node to which incoming DPT test calls are moved to

The purpose of this feature is to provide an interface to third party test heads to permit testing of Dynamic Packet Trunks(DPT), if that DPT is hosted by a SPM or MG4K. This interface allows the user to generate a test call over a

desired DPT terminal to a remote switch. Since an incoming DPT call can be terminated on any available DPT node, provisioning of this parameter provides the node information to allow the test call to be terminated to a specified peripheral. This permits the customer to have a known path when conducting a test.

20.4.2.1.2 Provisioning rules

When an incoming DPT call is flagged as a test call from the data in the ISUP IAM message, if the user would like to specify which DPT node they would like to route call to, they can provision this information in this new parameter. The parameter accepts a node type and a node number. Currently, the node type will be limited to SPM and only for an SPM node type that supports DPT terminals.

20.4.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default

20.4.2.1.4 Activation

Enter a PMTYPE type of SPM and a valid node number within the range 0 to 85. If that SPM node exists and supports DPT terminals, then the parameter will be activated. The activation of this office parameter is immediate.

20.4.2.1.5 Dependencies

None.

20.4.2.1.6 Consequences

If the user enters an valid SPM node number but the SPM does not support DPT terminals, the following response will be provided:

‘This node does not have DPT terminals allocated.’

If the user enters a node number out of range, the following response will be provided:

‘Not a valid SPM number.’

20.4.2.1.7 Verification

A DPT group hosted by the SPM node provisioned in the office parameter can be posted at the DPTTRKS level and incoming DPT test calls will show active terminals.

20.4.2.1.8 Memory requirements

No memory impact.

20.4.2.1.9 Parameter release history update

Parameter DPT_BICC_TEST_NODE is new in this release.

20.5 Upgrade Considerations

20.5.1 Dump and Restore (CM)

No impact.

20.5.2 Element Management Upgrade

No impact.

20.5.3 Downgrade impact

No impact.

21: Configuration (CN): A00009218

21.1 Feature Name

MG9K Data Audit Robustness

21.2 Hardware and Software Requirements

This functionality is for MG9000 EM that has SN09 or higher software version.

21.3 Initial Configuration

No changes to the initial configuration.

21.4 Upgrade Impact

21.4.1 Dump and Restore

N/A

21.4.2 12.3.2 Element Management Upgrade

N/A

21.5 Element Management

21.5.1 GUI information

Table 1 New or modified GUIs

GUI name	New, Changed or Deleted
Audit View	Changed
Create Audit View	Deleted
Select VMG frame	New

21.5.1.1 Audit View -- Functional description

In release SN09, the Audit GUI gives the user the ability to run an audit at any time even though a scheduled audit exists for the particular NE. In previous releases the user had to delete an existing scheduled audit in order to run an immediate audit. Additionally, for immediate audits users have the option to specify which sub-system (or VMG) to run the audit on. For example the user might choose to audit just the line circuits in the system, or just a single problem VMG.

21.5.1.2 Audit view - GUI usage and implications

The “Add” and “Remove” buttons no longer exist in the gui. From MG9kEMS software UE9000 MG Element Manager View when the audit view is selected, a list of NEs in the subnet is shown in the NE list. This shows only those NEs that are discovered (and are thus auditable). The user chooses an NE of interest and schedules the audit directly in the properties panel. Two tabs exist, one for scheduled audits, and another for immediate ones.

21.5.1.3 Audit view - GUI size

Not Applicable

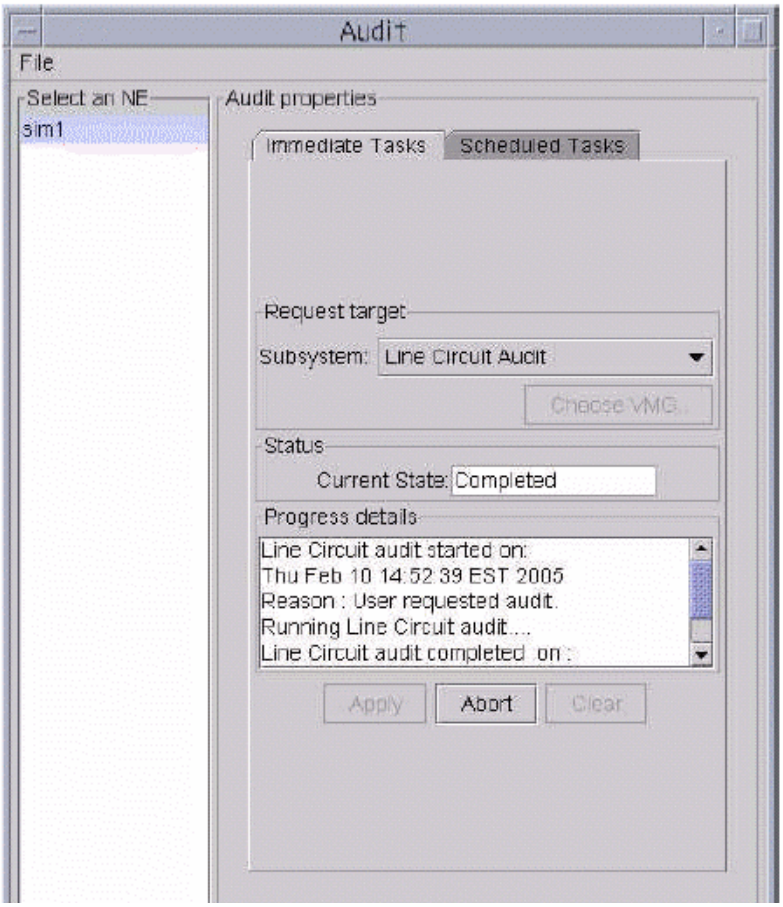
21.5.1.4 Audit view - GUI fields

Subsystem: A drop down menu for selecting a type of audit to run.

21.5.1.5 Audit view - Usage example 1

The following example shows a user selecting and running line circuit audit:

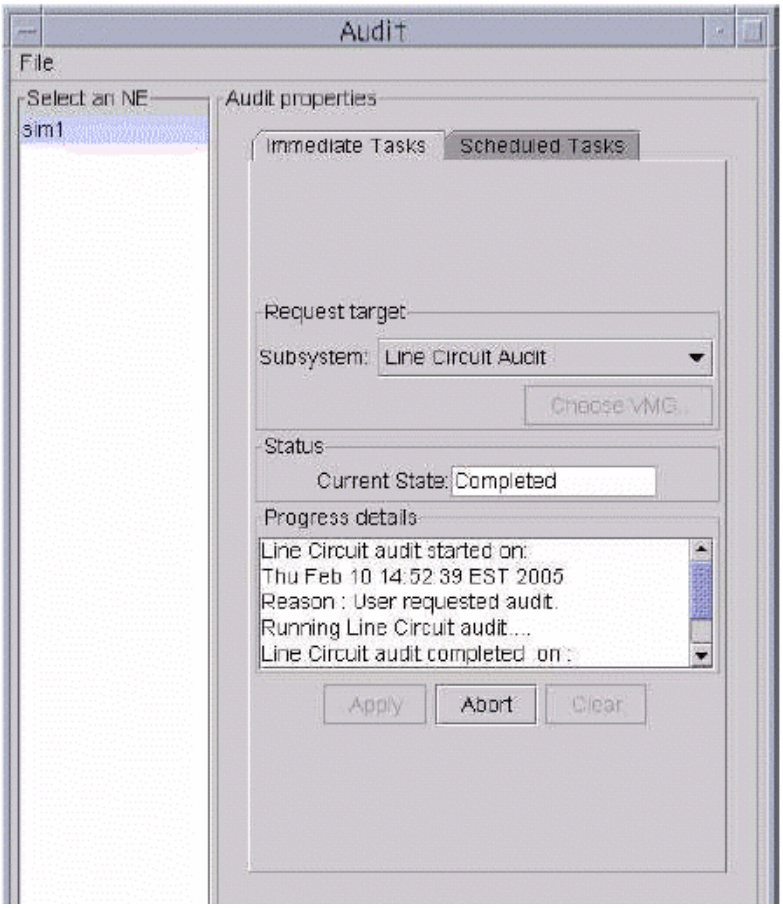
Figure 1 Running an immediate audit



21.5.1.6 Audit view - Usage example 2

The following example shows a user selecting to run a single VMG audit. The user has selected “VMG” from the subsystem drop down menu and clicked on the “Choose VMG” button. Clicking on the “Apply” button on the VMG selection frame will start an audit on the VMG named SLOA011-0-0:

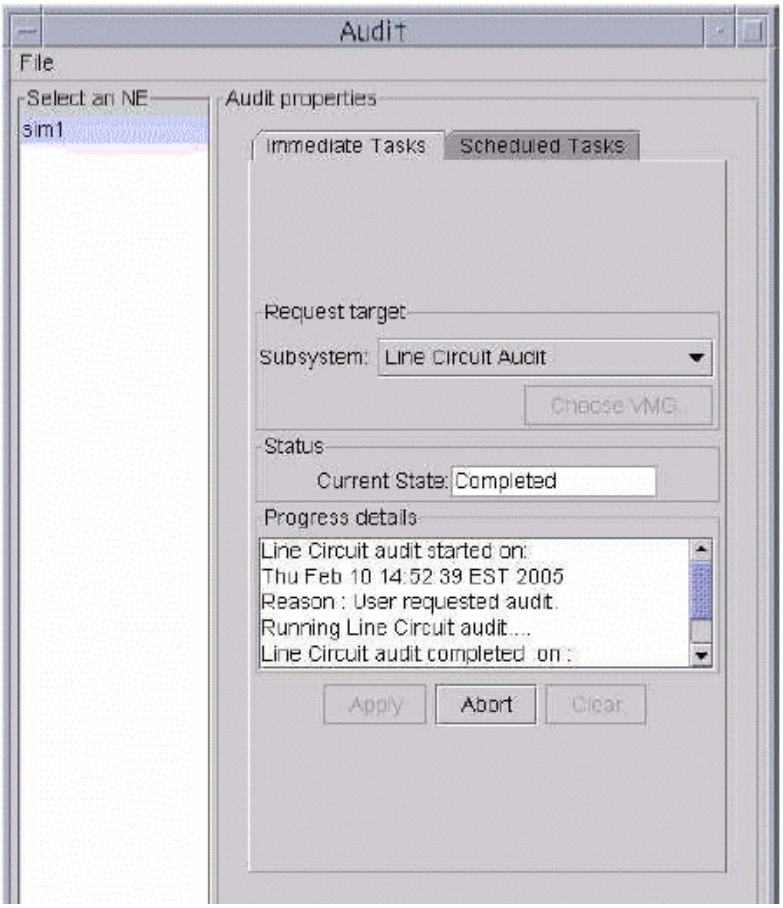
Figure 2 Running a VMG audit



21.5.1.7 Audit view - Usage example 3

The following example shows a user scheduling an audit to run in the future. This audit will run starting at 3:00PM on every Tuesday and Friday of the week, until it is aborted:

Figure 3 Scheduling an audit



22: Configuration (CN): A00009227

22.1 Feature Name

NPM Robustness

22.2 Hardware and Software Requirements

This feature requires an SN09 Network Patch Manager (NPM) and the SN09 SSPFS platform.

22.3 Network Patch Manager Server CLUI

22.3.1 CLUI Interface

The NPM CLUI has been modified to accept patchids and set names in lower case, upper case or a combination of thereof. In addition, several of the NPM CLUI commands have been changed to ensure command naming consistency for commands that provide similar types of functions. Below is a table that maps the old CLUI command to the new command.

Table 1:

Old Command	New Command
getassign	viewassign
ltabs	viewtabs or vtabs
qtask	viewtask or vt
qreps	viewreport all or vr all
qsets	viewset all or vs all
getplan	viewplan or vplan
alarminfo	viewalarm or va
display	viewpatch or vp
addalarm	newalarm or na
newset REPORT	newreport
newset SET	newset

Table 1:

Old Command	New Command
alarm	enablealarm (for the enable portion) disablealarm (for the disable portion) delalarm (for the delete portion) alarmmatches (for the match portion)
sched	modifyplan
updplan	updsched
query	runreport or rr (for executing a report) runset or rs (for executing a set)
getversion	viewversion
getprop	viewprop

In addition a new command: alarmshow has been added. The complete syntax of the new command and well as the changed commands is shown below:

22.3.1.1 The ALARMSHOW Command

The NPM command **alarmshow** is used to toggle the display of alarms as they are raised or cleared. The following syntax is used:

npm ‘alarmshow <ON/OFF>’

where:

npm	is the executable.
alarmshow	is the NPM command.
<ON|OFF>	is the switch to indicate whether to display alarms or not. ON indicates that as alarms are raised or cleared the message will be displayed at the CLUI. OFF indicates that the alarms will not be displayed.

22.3.1.2 The VIEWASSIGN Command

The NPM command **viewassign** is used to view the assign fields applicable for the assign command. The following syntax is used:

npm ‘viewassign’

where:

npm	is the executable.
viewassign	is the NPM command.

22.3.1.3 The VIEWTABS Command

The NPM command **viewtabs** is used to list all reportable tables and field names. The following syntax is used:

npm ‘viewtabs’

where:

npm	is the executable.
viewtabs	is the NPM command.

22.3.1.4 The VIEWTASK Command

The NPM command **viewtask** is used to display the specified task or all defined tasks. The following syntax is used:

npm ‘viewtask <taskname | all>’

where:

npm	is the executable.
viewtask	is the NPM command.
<taskname>	is the name of a specific task to be displayed.
<for all>	will display all tasks.

22.3.1.5 The VIEWREPORT Command

The NPM command **viewreport** is used to display the specified report or all defined reports in the database. The following syntax is used:

npm ‘viewreport <reportname | all>’

where:

npm	is the executable.
viewreport	is the NPM command.
<reportname>	is the name of a specific report to be displayed.
<for all>	will display all reports.

22.3.1.6 The VIEWSET Command

The NPM command **viewset** is used to view the specified set or all defined sets in the database. The following syntax is used:

npm ‘viewset <setname | all>’

where:

npm	is the executable.
viewset	is the NPM command.
<setname>	is the name of a specific set to be displayed.
<for all>	will display all sets.

22.3.1.7 The VIEWPLAN Command

The NPM command **viewplan** is used to view the specified plan or all defined plans in the database. The following syntax is used:

npm 'viewplan <setname | all>'

where:

npm	is the executable.
viewplan	is the NPM command.
<setname>	is the name of a specific plan to be displayed.
<for all>	will display all plans.

22.3.1.8 The VIEWALARM Command

The NPM command **viewalarm** is used to view the specified alarm or all defined alarms in the database. The following syntax is used:

npm 'viewalarm <setname | all>'

where:

npm	is the executable.
viewalarm	is the NPM command.
<setname>	is the name of a specific alarm to be displayed.
<for all>	will display all alarms.

22.3.1.9 The VIEWPATCH Command

The NPM command **viewpatch** is used to view the administrative information associated with a patch. The following syntax is used:

npm 'viewpatch <patchid>'

where:

npm	is the executable.
viewpatch	is the NPM command.
<patchid>	is the patchid to be displayed.

22.3.1.10 The NEWALARM Command

The NPM command **newalarm** is used to define a new alarmable condition. The following syntax is used:

npm ‘newalarm <name> <enable> <alarm> <patchinfo> <“Desc”>’

where:

npm	is the executable.
newalarm	is the NPM command.
<name>	is the name of the alarm being defined.
<enable>	indicates whether to enable (Y) or disable (N) the alarm.
<alarm>	is the severity level of the alarm. Valid values are “NONE”, “MINOR”, “MAJOR”, or “CRITICAL”.
<patchinfo>	is SQL criteria that defines the alarm and should be in the form "PATCH|DEVICE where [criteria]".
<“Desc”>	is a brief description of the alarm.

22.3.1.11 The NEWREPORT Command

The NPM command **newreport** is used to create a report. The following syntax is used:

npm ‘newreport <reportname> <“Description”> <“field1... fieldn [where <Criteria>]”>’

where:

npm	is the executable.
newreport	is the NPM command.
<reportname>	is the name of the report to be created.
<“Description”>	is a short description of the report.
<field1...fieldn	is the name of one or more fields to be included in the report.
where	keyword starting SQL statement
<Criteria>	is the SQL statement that identifies the criteria by which to search the NPM database.

22.3.1.12 The NEWSET Command

The NPM command **newset** is used to create a set definition. The following syntax is used:

npm ‘newset <type> <setname> <“Description”> <[“where <Criteria>”]>’

where:

npm	is the executable.
newset	is the NPM command.
<type>	is either PATCHSET (to create a set that will evaluate patches) or DEVICESET (to create a set that will evaluate devices).
<setname>	is the name of the set to be created.
<“Description”>	is a short description of the report.
where	keyword starting SQL statement
<Criteria>	is the SQL statement that identifies the criteria by which to search the NPM database.

22.3.1.13 The ENABLEALARM Command

The NPM command **enablealarm** is used to enable the specified alarm. The following syntax is used:

npm ‘enablealarm <alarmname>’

where:

npm	is the executable.
enablealarm	is the NPM command.
<alarmname>	is the name of the alarm.

22.3.1.14 The DISABLEALARM Command

The NPM command **disablealarm** is used to disable the specified alarm. The following syntax is used:

npm ‘enablealarm <alarmname>’

where:

npm	is the executable.
disablealarm	is the NPM command.
<alarmname>	is the name of the alarm.

22.3.1.15 The DELALARM Command

The NPM command **delalarm** is used to delete the specified alarm. Only user created alarms can be deleted. The following syntax is used:

npm ‘delalarm <alarmname>’

where:

npm	is the executable.
delalarm	is the NPM command.
<alarmname>	is the name of the alarm to be deleted.

22.3.1.16 The ALARMMATCHES Command

The NPM **alarmmatches** command is used to list either the patches or devices that caused the specified alarm to be raised. The following syntax is used:

npm ‘alarmmatches <alarmname>’

where:

npm	is the executable.
alarmmatches	is the NPM command.
<alarmname>	is the name of the alarm.

22.3.1.17 The MODIFYPLAN Command

The NPM command **modifyplan** is used to modify the scheduled activities of a plan. The modifyplan command may be used to add a specified task or report to a plan or delete a specified task or report from a plan.

Note: The order in which tasks and reports are added to a plan determines the order in which their execution will be requested.

: The following syntax is used

npm ‘modifyplan <plan name> <TASK|REPORT> <Task|Report name> <ADD|DELETE>’

where:

npm	is the executable.
modifyplan	is the NPM command.
<plan name>	is the name of the plan to be modified
<TASK|REPORT>	indicates whether the item being added to or deleted from the given plan is a task or a report.
<Task|Report name>	is the name of the task or report being added to or deleted from the given plan.

	Note: Prompted reports should not be added to plans. At execution time, prompted reports require a user to supply additional input. Plans run without a user being present and cannot provide the required information. The predefined prompted reports include: DEVICE, PATCH, PATCHES_SINCE, and PATCHINFO. Do not add any of these reports or any user defined prompted reports to any plans.
<ADD|DELTE>	indicates whether the specified task or report is to be added to or deleted from the given plan.

22.3.1.18 The UPDSCHED Command

The NPM command **updsched** is used to update the plan schedule in the database. The following syntax is used:

npm ‘updsched <plan name> <freq> <Date Time> <MaxTime> <“Desc”>’

where:

npm	is the executable.
updsched	is the NPM command.
<plan name>	is the name of the plan to be updated
<freq>	is how often the plan should execute. Valid values are “Once”, “Hourly”, “Daily”, “Weekly”, or “Monthly”.
<Date Time>	is the date and time plan is to be executed. Should be in “mm-dd-yy hh:mm” format.
<MaxTime>	is Maximum amount of time to execute plan defined as {No_Limit,15_min, 30_min, 1_Hr, 2_Hr, 4_Hr, 8_Hr, 16_Hr}.
<“Desc”>	is a brief description surrounded by quotes.

22.3.1.19 The RUNREPORT Command

The NPM command **runreport** is used to execute the specified report and display the results. The following syntax is used:

npm ‘runreport <reportname>’

where:

npm	is the executable.

runreport	is the NPM command. “rr”or “q” can be used as a shortcut for “runreport”.
<reportname>	is the name of the report to be executed.

22.3.1.20 The RUNSET Command

The NPM command **runrset** is used to execute the specified set and display the results. The following syntax is used:

npm ‘runset <setname>’

where:

npm	is the executable.
runset	is the NPM command. “rs” or “q” can be used as a shortcut for “runset”.
<setname>	is the name of the set to be executed.

22.3.1.21 The VIEWVERSION Command

The NPM command **viewversion** is used to view the version of the NPM software and database components. The following syntax is used:

npm ‘viewversion’

where:

npm	is the executable.
viewversion	is the NPM command.

22.3.1.22 The VIEWPROP Option

The NPM option **viewprop** is used to list the property value for a specified key or all keys. The following syntax is used:

npm ‘getprop <property_type>’

where:

npm	is the executable.
getprop	is the NPM option.
<property_type>	can be a specific key, or “all” to display all keys.

22.4 Network Patch Manager Reports

Six new system defined reports will be added to the NPM as a result of this feature. NPM CLUI examples follow of the reports to show what fields are in each report.

- DEVICEINFO - lists the devices in the office, the date the devices registered, the loadname in the device and the date the load was discovered in the device.

```
npm>q DEVICEINFO
deviceid,registered,hold,devicebornon,loadname,loaddiscoveredon
NC0S8_1_OC3_0_1_10,TRUE,FALSE,2005-03-17 12:05:12.397,SCOA09AH,2005-03-17 12:
05:57.994
NC0S8_1_OC3_0_1_11,TRUE,FALSE,2005-03-17 12:05:12.417,mdw,2005-03-17 12:05:59.804
NC0S8_1_ITP_0_1_12,TRUE,FALSE,2005-03-17 12:05:12.442,ITPA09AF,2005-03-17 12:
06:00.782
MG9KSERVER_09_wnc0s0mh,TRUE,FALSE,2005-03-17 12:04:20.897,NTMG9KS_9_11_0,2005
```

- LASTAPPLYACTION - A list of the patch, device, status and description of why the apply attempt failed for this patch device relationship.

```
npm>q LASTAPPLYACTION
patchid,deviceid,status,lastactionresults
```

- PFRSSETTINGS - Lists the PFRS Dropbox, PFRS userid and status of if the delete patches is turned on.

```
npm>q PFRSSETTINGS
ftpAddress,ftpUserid,deletePatches
wnc0s0kf,FIELD,FALSE
```

- SYSTEMPLANSETTINGS - Lists all the system plans in the office along with the tasks, enable status, and schedule for each plan.

```
npm>q SYSTEMPLANSETTINGS
name,enabled,status,frequency,extime,maxtime,description,tasks,systemDefined
SYSTEMPLAN,N,IDLE,Daily,2004-01-01 00:00:00.000,No_Limit,NPM System scheduled
 routine activities,[TASK:AUTOAPPLY, TASK:AUTORESTART],TRUE
REPORTCLEANUP,N,IDLE,Daily,2004-01-01 00:00:00.000,No_Limit,Delete reports as
sociated with NPM Plans,[TASK:DELETEREPORTS],TRUE
GETPATCH,N,IDLE,Daily,2004-01-01 23:00:00.000,No_Limit,Patch file retrieval,[
TASK:PFRSGETPATCH],TRUE
GENREPORT,N,IDLE,Daily,2004-01-01 10:00:00.000,No_Limit,PFRS Inform list repo
rt generation,[TASK:PFRSGENREPORT],TRUE
FILEAUDIT,Y,IDLE,Daily,2005-03-18 05:00:00.000,No_Limit,File Audit,[TASK:FILE
AUDIT],TRUE
```

- OFFICEINFOSETTINGS - Lists office information. Currently, only the GWC Auto imaging enabled setting is available in this report.

```
npm>q OFFICEINFO
gwcautoimage
Y
```

- GWCLOADIMAGEREPORT - Lists the imaged load, the patches contained in the load, the time the image was taken and a list of patches available in the office that are not contained in the image.

```
npm>q GWCLOADIMAGEREPORT
loadname,imagedtime,imagedpatchlist,missingpatches
GN090AP,2005-03-17 12:15:31.316,[None],[GWC01GAP, GWC02GAP]
```

All of these reports will be included in the inform report that is generated via the PFRSGENREPORT task in the NPM. The following is an example inform report.

23: Configuration (CN): A00009235

23.1 Feature Name

TLS for SIP

23.2 Hardware and Software Requirements

Nothing required outside of the normal SN09 software load on the appropriate hardware platform.

23.3 Initial Configuration

SN09

23.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

23.5 Upgrade Considerations

If a Session Server is to be placed in a Packet Cable environment, extra steps will be required after the upgrade is complete.

From 07 to 09 upgrade in the case of CA-signed certificate, the customer must execute the procedure “Prepare to validate” which is run on the 07 in order to ensure that cert_mgnt in 09 will be successful if the customer is importing a CA-signed certificate from 07 to 09. This is documented in the NTP. If the certificates are nearing expiry during the upgrade or shortly after the upgrade, the customer is recommended to replace the certificates prior to upgrade in order to avoid downtime once the system is running the 09 load.

From 07 to 09 upgrade in the case of self-signed certificates, the customer will have to generate new certificates.

From 08 to 09 upgrade, running cert_mgnt is not required. If the certificates are nearing expiry during the upgrade or shortly after the upgrade, the customer is recommended to replace the certificates prior to upgrade in order to avoid downtime once the system is running the 09 load.

23.5.1 Dump and Restore (CM)

None.

23.5.2 Element Management Upgrade

None.

23.5.3 Downgrade impact

None.

23.6 Data schema (DS) (CM, MIBS, RDB)

Not applicable.

23.7 Service Orders (SO) (CM & SESM)

Not Applicable.

23.8 Software optionality control (SOC)

Not Applicable.

23.9 Element Management

23.9.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
CS2000 Session Server Tomcat Web Server	Changed

23.9.2 GUI information

23.9.2.1 GUI name: Session Server Tomcat Web Server

This GUI is a CS2000 Session Server-specific management tool.

The changes made to this GUI consist of:

- Additions to the Security configuration parameters web page with new parameters
- Modification of an existing parameter to the security configuration parameters web page.

23.9.2.1.1 Functional description

Changes to the CS2000 Session Server Tomcat Web Server GUI are as follows:

CS2000 Session Server Tomcat Web server security configuration parameters:

Ciphers. This field existed in SN08 and is modified to include new ciphers:

- TLSAllowedCipherSuites

Alarm threshold provisioning. These fields are new:

- AlarmThresholdDroppedConnections - Dropped connections alarm per loop time of 60 seconds
- AlarmThresholdAuthenticationFailure - Certificate Authentication failure alarm - per loop time of 60 seconds
- AlarmThresholdCertExpiryDays - Local certificate expiry alarm in days
- AlarmThresholdLocalCertificatePolicy - remote certificate policy failure alarm per loop time of 60 seconds
- AlarmMinimumDisplayTimeMinutes - Minimum time an alarm should be raised

Secretary options. This field is new:

- ExitOnFailTLSInitialization - Exit application if TLS fails to initialize

Certificate Policy options. These fields are new:

- RequireLocalCertificatePolicy
- RequireauthorityKeyIdentifier
- RequirebasicConstraints
- RequireextKeyUsage
- RequireissuerAltName
- RequirekeyUsage
- RequireprivateKeyUsagePeriod
- RequiresubjectAltName
- RequiresubjectKeyIdentifier

Additions for throttling are:

- ThrottleBurstDurationinSecs
- ThrottleBurstEventThreshold
- ThrottleEnabled
- ThrottleSustainedDurationinSecs
- ThrottleSustainedEventThreshold

Other parameters that are new in SN09 are:

- TlsEnabled

Other parameters that are changed from SN08 to SN09:

- MaxTLSSessions
- SessionCachingEnabled
- SessionCacheSize
- SessionCacheValidDuration

23.9.2.1.2 GUI usage and implications

The purpose of the new configuration parameters is to provide new functionality as well as increased robustness to the security component of the CS2000 Session Server.

23.9.2.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GUI			Not applicable

23.9.2.1.4 GUI fields

The following table lists fields for the CS2000 Session Server Tomcat Web server Security Parameters GUI that have been added or changed.

Table 3 Security Parameters in Tomcat Web Server

Parameter	AlarmThresholdDroppedConnections	Type	Integer
Description	Number of dropped connections - Minor/Major/Critical alarm threshold value within 60 seconds. Related to SIPS600 log and applies to SIPS300 alarm. Note: 0 < Minor threshold < Major Threshold < Critical Threshold < 32767 The value is applied immediately.	Default Value	Minor - 10 Major - 50 Critical - 100
Effect of Change	Changes the threshold for activating alarm for dropped connections in CS2000 Session Server	New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**AlarmThresholdAuthentica-tionFailure**	Type	Integer
Description	Number of certificate authentication failures - Minor Threshold. Related to SIPS 601 log and applies to SIPS301 alarm. Note: 0 < Minor threshold < Major Threshold < Critical Threshold < 32767 The value is applied immediately.	Default Value	Minor - 1 Major - 2 Critical - 5
Effect of Change	Changes the threshold for activating alarm for certificate authentication failures in CS2000 Session Server	New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**AlarmThresholdCertExpiry-Days**	Type	Integer
Description	Number of days until the local certificate expires. Applies to the SIPS302 alarm. Note: Modifying/replacing the local certificate requires a restart of the web services and the SIP application. Note: The SIPS604 log indicates the time and date from when and until when the local certificate is active. Note: This alarm remains raised until the event is no longer observed. Note: 32767 > Critical threshold > Major Threshold > Minor Threshold > 0 The value is applied immedi-ately.	Default Value	Minor - 31 days Major - 15 days Critical - 5 days
Effect of Change	Changes the threshold for acti-vating alarm for local certificate expiry in CS2000 Session Server	New or Changed	New
Adverse Effects			
Counter-ing Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**AlarmThresholdLocalCertificatePolicy**	Type	Integer
Description	Number of certificate policy violations in 60 seconds. Related to the SIPS608 log and applies to the SIPS308 alarm. Note: 0 < Minor threshold < Major Threshold < Critical Threshold < 32767 The value is applied immediately.	Default Value	Minor - 1 Major - 2 Critical - 5
Effect of Change	Changes the threshold for activating alarm for certificate policy violations.	New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**AlarmMinimumDisplay-TimeMinutes**	Type	Integer
Description	The following alarms will remain raised when the event persists. This value indicates the number of minutes that the following alarms should remain raised when the event is no longer continuously observed. AlarmThresholdLocalCertificatePolicy AlarmThresholdAuthenticationFailure AlarmThresholdDroppedConnections The value is applied immediately.	Default Value	60 minutes Minimum value: 1 minute Maximum value: 32767 minutes
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**ExitOnFailTLSInitialization**	Type	Boolean
Description	1) If the key file or certificate file is not present or corrupted, or 2) if the system is running out of memory and having trouble initializing TLS or 3) the certificate does not match the local policy, or 4) the key/certificate do not match, then this value indicates whether to exit the application or continue with the application initialization and attempt to service calls while the issue is resolved. Default is to exit the application because it may indicate issues with system memory or key/certificate files. Because the same key/certificate files are used to run the EM web servers, the recommended value for this parameters is Y. If the value is changed to 'N' (to allow application initialization), then TlsEnabled can be used to initialize TLS. This value is applied only on application restart.	Default Value	Y Recommended Value: Y
Effect of Change		new or changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequireLocalCertificatePolicy**	Type	Boolean
Description	This parameter enables certificate policy checking. For Packet Cable conformance, this must be set to Y. The value is applied immediately.	Default Value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequireauthorityKeyIdentifier**	Type	Boolean
Description	This value ensures whether the authority key identifier is present in the X.509 version 3 certificate extensions. For Packet Cable conformance, this must be set to Y. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequirebasicConstraints**	Type	Boolean
Description	This value ensures whether the basic constraints is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequireextKeyUsage**	Type	Checklist
Description	This value ensures whether the individual key usage settings are present in the X.509 version 3 certificate extensions. Possible values are none of the following, or any combination of the following: serverAuth clientAuth codeSigning emailProtection timeStamping OCSPSigning For Packet Cable conformance, this must be set to (serverAuth and clientAuth). This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	Empty set, See description.
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequireissuerAltName**	Type	Boolean
Description	This value ensures whether the issuer alternative name is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequirekeyUsage**	Type	Checklist
Description	This value ensures whether the key usage settings is present in the X.509 version 3 certificate extensions. Possible values are none of the following, or any combination of the following: digitalSignature nonRepudiation keyEncipherment dataEncipherment keyAgreement keyCertSign cRLSign encipherOnly decipherOnly For Packet Cable conformance, this must be set to (digitalSignature and keyEncipherment). This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	Empty Set, see description
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequireprivateKeyUsagePeriod**	Type	Boolean
Description	This value ensures whether the private key usage field is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequiresubjectAltName**	Type	Boolean
Description	This value ensures whether the subject alternative name is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Parameter	**RequiresubjectKeyIdentifier**	Type	Boolean
Description	This value ensures whether the subject key identifier is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**ThrottleBurstDurationinSecs**	Type	Integer
Description	The maximum number of TLS connections represented by ThrottleBurstEventThreshold that can be serviced in Throttle-BurstDurationinSecs seconds. ThrottleBurstDurationinSecs is recommended to be ThrottleSustainedDurationinSecs divided by 5. This value is applied immediately and requires ThrottleEnabled to be set to “Y” to have effect.	Default Value	1 Minimum 1 Maximum 10
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**ThrottleBurstEventThreshold**	Type	Integer
Description	The maximum of number of TLS connections that can be serviced in ThrottleBurstDurationinSecs seconds. Recommended value 30 This value is applied immediately and requires ThrottleEnabled to be set to “Y” to have effect.	Default Value	30
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Parameter	**ThrottleEnabled**	Type	Boolean
Description	Enables or disables TLS connection throttling Recommended value Y.	Default Value	Y
Effect of Change		New or Changes	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**ThrottleSustainedDurationin-Secs**	Type	Integer
Description	The maximum number of TLS connections represented by ThrottleSustainedEventThresh-old that can be serviced in Throt-tleSustainedDurationinSecs seconds. ThrottleSustainedDurationin-Secs is recommended to be ThrottleBurstDurationinSecs multiplied by 5. This value is applied immedi-ately and requires ThrottleEn-abled to be set to “Y” to have effect.	Default Value	5
Effect of Change		New or Changed	New
Adverse Effects			
Counter-ing Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**ThrottleSustainedEvent-Threshold**	Type	Integer
Description	The maximum of number of TLS connections that can be serviced in ThrottleSustainedDurationin-Secsseconds. Recommended value 100 This value is applied immediately and requires ThrottleEnabled to be set to “Y” to have effect.	Default Value	100
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**TlsEnabled**	Type	Boolean
Description	By default, TlsEnabled is “Y”. If the value is “Y” is cannot be modified. TlsEnabled is “N” in the following case: If ExitOnFailTLSInitialization is set to “N” and TLS fails to initialize. In that case, this boolean can be used to initialize TLS once the issue is resolved.	Default Value	Y
Effect of Change	The value cannot be changed if it is already set to Y. Changing this value from N to Y restarts TLS initialization. The key file and certificate file must be present in order for TLS initialization to be successful. Once successful, look for the SIPS 605 log. If memory allocation for TLS or the SIP application fails, then the SIP application will terminate.	New of Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**MaxTLSSessions**	Type	Integer
Description	The maximum number of TLS Sessions allowed. The default value is set to 256, maximum of 400.	Default value	Default 256, Minimum 10 Maximum 400.
Effect of Change	This is the maximum number of simultaneous TLS connections on the active unit.	New or Changed	Changed maximum value from SN08 to SN09.
Adverse Effects			
Counter-ing Adverse Effects			

Table 4 Cipher Suites

Parameter	**TLSAllowedCipherSuites**	Type	Checklist
Description	The cryptographic ciphers that are supported in the TLS connection. The value is applied immediately. AES128-SHA is the minimum. Any combination of the following is also allowed: AES256-SHA DHE-RSA-AES128-SHA DHE-RSA-AES256-SHA EDH-RSA-DES-CBC3-SHA DES-CBC3-SHA	Default Value	AES128-SHA at a minimum. See description.
Effect of Change	Selecting ciphers other than AES may cause performance degradation.	New or Changed	Changed from SN08
Adverse Effects			
Countering Adverse Effects			

All ciphers listed here support private key sizes of 1024, 1536, and 2048 bits, RSA authentication, and SHA (Secure Hash Algorith) as the HMAC (hashed message authentication code).

Cipher Name: TLS_RSA_WITH_AES_128_CBC_SHA
Short Name: AES128-SHA
Key Agreement: RSA
RSA/DSA Authentication: RSA
Encryption: AES_CBC, 128 bits

Cipher Name: TLS_RSA_WITH_AES_256_CBC_SHA
Short Name: AES256-SHA
Key Agreement: RSA
Encryption: AES_CBC, 256 bits

Cipher Name: TLS_RSA_WITH_3DES_EDE_CBC_SHA
Short Name: DES-CBC3-SHA
Key Agreement: RSA
RSA/DSA Authentication: RSA
Encryption: 3DES_EDE_CBC, 168 bits

Cipher Name: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
Short Name: DHE-RSA-AES128-SHA
Key Agreement: DHE
RSA/DSA Authentication: RSA
Encryption: AES_CBC, 128 bits
DHE Prime Size: 1024

Cipher Name: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
Short Name: DHE-RSA-AES256-SHA
Key Agreement: DHE
RSA/DSA Authentication: RSA
Encryption: AES_CBC, 256 bits
DHE Prime Size: 1024

Cipher Name: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Short Name: EDH-RSA-DES-CBC3-SHA
Key Agreement: DHE
RSA/DSA Authentication: RSA
Encryption: 3DES_EDE_CBC, 168 bits
DHE Prime Size: 1024

Table 5 Session Caching Parameters

Parameter	**SessionCachingEnabled**	Type	Integer
Description	Defines whether session caching is enabled or disabled. Session caching improves performance over TLS connections where traffic is fairly low and over SWACT. It is recommended that all remote servers have TLS session caching functionality enabled. This value now enables or disables client side and server side session caching. Recommended value Y.	Default value	Y
Effect of Change	Turning off session caching does not clear the cache. Items are removed from the server side and client side cache when they are expired. Items may also be removed from the server cache when the server cache is full in order to make room for a new entry.	New or Changed	Changed scope to include client side caching in SN09.
Adverse Effects			
Countering Adverse Effects			

Parameter	**SessionCacheSize**	Type	Integer
Description	Defines the maximum size of the client and server side TLS session cache. Valid values: 10, 100, 1000, 2000, 3200 This recommended value is: (8 x the number of remote sip servers using TLS) <= NEW VALUE. This value should not normally be decreased.	Default value	10
Effect of Change	Increases or decreases the size of the client and server side TLS session cache.	New or Changed	Changed to include new values: 2000, 3200.
Adverse Effects			
Counter-ing Adverse Effects			

Parameter	**SessionCacheValidDuration**	Type	Integer
Description	Defines the length of time a TLS session can be cached. Valid values are 24_Hours, 7_Days, 3_Months. Recommended value: 7_Days	Default value	7_Days
Effect of Change	Changing the values impacts all future TLS sessions, but does not impact entries already in the cache.	New or Changed	Changed to include additional value 3_Months
Adverse Effects			
Countering Adverse Effects			

23.9.2.1.5 Usage example

The following example shows sample datafill or menu selection for the CS2000 Session Server Tomcat Security Parameters Configuration Web Page GUI:

Example:

1. Customer enters the Succession Communication Server 2000 web page.
2. Customer enters the Succession Communication Server 2000 Session Server Manager webpage.
3. Customer clicks on the Provisioning Tab on the Menu Frame
4. Customer clicks on the Security Tab.
5. Customer clicks on the SIP Gateway Tab.
6. Customer clicks on the Security Config Data link, which brings up the Security Configurable Parameters page.
7. All of the parameters listed in See “Security Parameters in Tomcat Web Server” on page 2457. are available.

23.9.2.1.6 GUI release history update

See “Security Parameters in Tomcat Web Server” on page 2457. for parameters that are changed or new in SN09.

23.9.2.1.7 Context sensitive launching information

This GUI is accessed from a series of links starting on the CS2000 Session Server main web page. The normal instructions for launching the CS2000 Session Server Application Web Server can be followed for the new web pages described herein.

23.9.2.1.8 Supplementary information

Not applicable.

23.9.3 CLUI Interface

The Certificate Management Tool has changed slightly from SN08 to SN09.

The tool in its entirety is documented here.

23.9.3.1 Certificate Management Tool (cert_mgnt or cert_mgmt)

The certificate management tool is a customer-visible tool that provides a common interface for provisioning certficates for use by Apache, Tomcat, and the NGSS SIP application.

As of SN08, all three applications use the same certificate.

The certificate management tool is located in /sbin/cert_mgnt or /sbin/cert_mgmt, and is executable only by the root user. Since /sbin is in the path, cert_mgnt can be executed from anywhere.

The certificate management tool provides three functions

- Create a new self-signed certificate for the host
- Create a certificate signing request. The craftsperson would manually send the signing request to the Certificate Authority (CA) where it will be signed.
- Import key and certificate (including CA signed certificate).

The tool makes permissions on private key files and the certificate keystore file to be read/write by the root user.

As described in the SN08 documentation (A00006893), the server.crt contains the local server certificate. The trusted.crt file contains the certificate chain (for CA-signed certificates only) for the local server certificate. Both these files are are read/write by the root user and readable by other users.

Anytime the certificate management tool is run to successful completion, the host must be rebooted, or the three applications that use the certificate must be stopped/ started.

To reboot the host as a root user: at the command prompt: reboot

If rebooting is not appropriate, then stopping/starting each application is necessary.

To stop/start Apache: locate the executable “apachectl” in the directory structure and type: apachectl stop. Once this is successful, type apachectl start

To stop/start Tomcat: local the executable “tomcatd” in the directory structure and type: tomcatd stop. Once this is successful, type tomcatd start.

To stop the NGSS SIP application, the application must be locked and disabled and then enabled and unlocked using the NGSS GUI.

23.9.3.1.1 Certificate Management

Upon installation of the NGSS, the customer can either furnish their own certificates or use the certificate management tool.

If the customer furnishes their own certificates, they will be required to perform their own certificate management.

23.9.3.1.2 Files used by the Certificate Management Tool

The directory /opt/base/share/ssl is the recommended directory to store all certificates, keys, and related files. The cert_mgnt tool performs this automatically.

The tool is run only on 1 host, and the files are not synced/reflected to the other mate host in SN09. Therefore, the files must be manually copied to the other mate host using a secure method such as scp after the tool runs successfully.

server.crt - Only the local server certificate is in this file. In the self-signed certificate option, this file is created automatically by the tool. In the CA-signed option, this file will be provided by the customer, and placed in a temporary directory for import by the tool.

trusted.crt - The certificate chain leading up to the root CA certificate is placed in this file. This file is provided by the customer, and placed in a temporary directory for import by the tool.

server.key - This file contains the private key corresponding to the certificate in server.crt

certificate.keystore - This file contains an encoded version of the server.crt, trusted.crt, and server.key file. This file is created automatically by the tool and is used by Tomcat.

The directory /opt/base/share/ssl should be backed up on a regular basis using a secure method in a physically and logically secure environment. This will help prevent unauthorized access to the private keys.

There are two files (cert_gen.txt and assign_cert.txt) that are placed in the /opt/base/share/ssl directory. These files are used by the tool and should not be removed.

23.9.3.1.3 Certificate and Key revocation

Not applicable.

23.9.3.1.4 Self Signed Certificates

In this case, the craftsperson has chosen to use self-signed certificates.

1. In the case of self-signed certificates, the craftsperson selects option 1 in Figure 1 ”Choose a Certificate Type” on page 2486.
2. In order to proceed, the craftsperson must accept the disclaimer and the notice as indicated in:
   - Figure 2 ”Disclaimer for Self-Signed Certificates (1 of 4)” on page 2487,
   - Figure 3 ”Disclaimer for Self-Signed Certificates (2 of 4)” on page 2487,
   - Figure 4 ”Disclaimer for Self-Signed Certificates (3 of 4)” on page 2488, and
   - Figure 5 ”Disclaimer for Self-Signed Certificates (4 of 4)” on page 2488..

   A customer log is generated logging the user’s acceptance of the disclaimer.

3. Going back at any time will display the previous panel. Selecting proceed will only work if the craftsperson has entered the required information.
4. The craftsperson selects an RSA key size Figure 6 ”Select Key Size” on page 2489. The key size can be 1024/1536/2048 bits. The higher the key size, the stronger the private key. There may be a performance impact to using higher key sizes due to additional encryption requirements.
   - If the key already exists in the /opt/base/share/ssl/ directory, the tool will prompt to reuse it or delete it and recreate a new key.
   - If the craftsperson wishes to reuse the key, the tool will always accept the key’s current size. This is illustrated in Figure 7 ”Key Already Exists” on page 2489
   - If in Figure 7 ”Key Already Exists” on page 2489, the craftsperson select ‘n’ that they do not want to proceed, then the tool prompts for key deletion in Figure 8 ”Remove Existing Key” on page 2490.
   - If in Figure 7 ”Key Already Exists” on page 2489 , the craftsperson select ‘y’ that they do want to proceed, then the tool will reuse the existing key and move on to step 5.
   - If in Figure 8 ”Remove Existing Key” on page 2490, the craftsperson selects ‘n’ that they do want to proceed, the tool will then abort the current operation and return to the top of this step.

- If in Figure 8 ”Remove Existing Key” on page 2490, the craftsperson selects ‘y’ that they do want to proceed, the tool will then make a backup of the existing key to another file in the same directory. A customer log is generated for this case.

5. The user must also select a length of time for which the certificate is valid. This is specified in Figure 9 ”Expiry Days” on page 2490. This is the number of days from the current date for which the certificate is valid.
6. The craftsperson selects a country, state, and city name in Figure 10 ”Country Name” on page 2491, Figure 11 ”State Name” on page 2491, Figure 12 ”Locality Name” on page 2492. These fields are optional. Although they are optional, they help to identify the NGSS to a remote entity.
7. The craftsperson selects an organizational name, and an organizational unit name in Figure 13 ”Organizational Name” on page 2492, and Figure 14 ”Organizational Unit Name” on page 2493. These fields optional. Although they are optional, they help to identify the NGSS to a remote entity.
8. In Figure 15 ”Common Name” on page 2493, the craftsperson identifies the mandatory common name. In the case of the NGSS, this must be the IP address of the active NGSS host. This is used for mutual authentication and is necessary for the correct operation of the NGSS. There is no validation at this stage of the common name.
9. In Figure 16 ”Email Address” on page 2494, the craftsperson identifies the optional email address of the local contact. There is no validation of the email address.
10. Once all the information is entered, the tool displays a summary in Figure 17 ”Summary for Self Signed Certificates” on page 2494. Selecting “proceed” will generate the self signed certificate. The following message will be displayed on success:

```
Exporting certificate/key pair to PKCS#12 keystore
Certificate/key pair has been successfully exported to PKCS#12 format
Changing permissions on key file
Changing permissions on keystore file
```

11. The user must then secure copy the necessary files from the unit where the cert_mgnt was executed to the mate unit.

For example:

```
cd /opt/base/share/ssl
scp * mtc@<mate host IP>:/users/mtc
```

12. The user log into the mate unit and change directory to the location where the certificate files are located. The user can then use the cert_mgnt tool option 3 to import the certificates and commit the files to /opt/base/share/ssl. This is documented in section 23.9.3.1.6 ”Import Certificates and Private Key” on page 2497.

Figure 1 Choose a Certificate Type

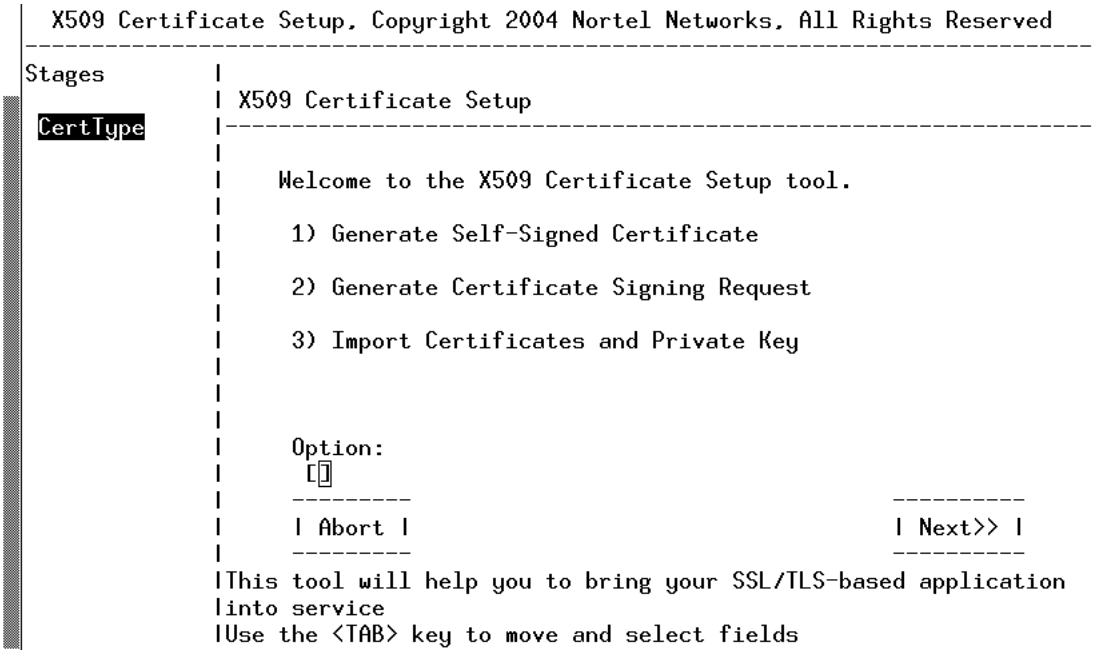


Figure 2 Disclaimer for Self-Signed Certificates (1 of 4)

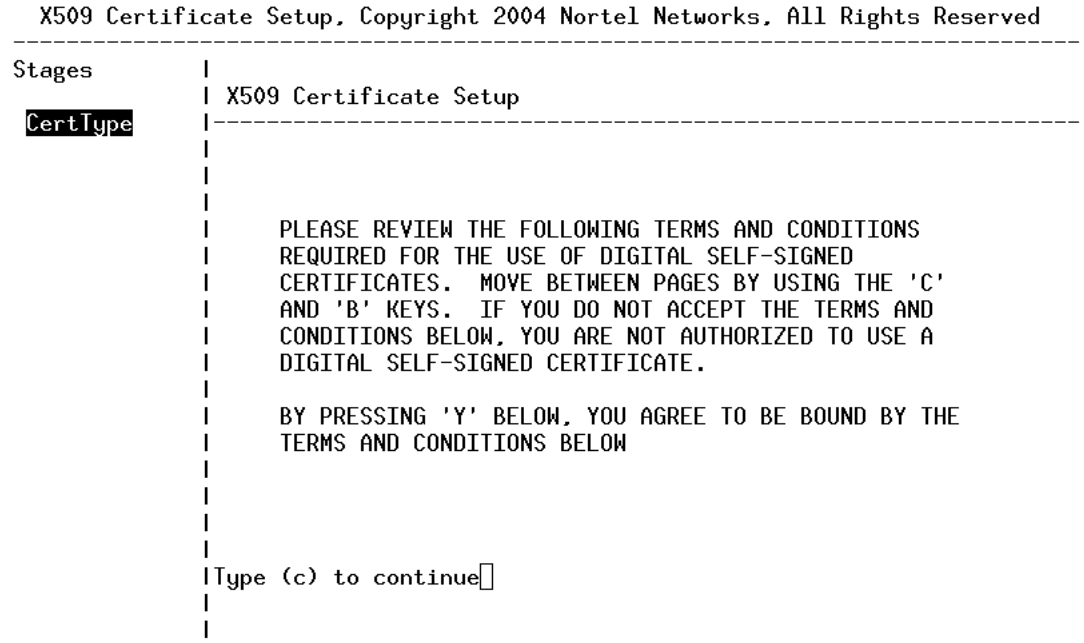


Figure 3 Disclaimer for Self-Signed Certificates (2 of 4)

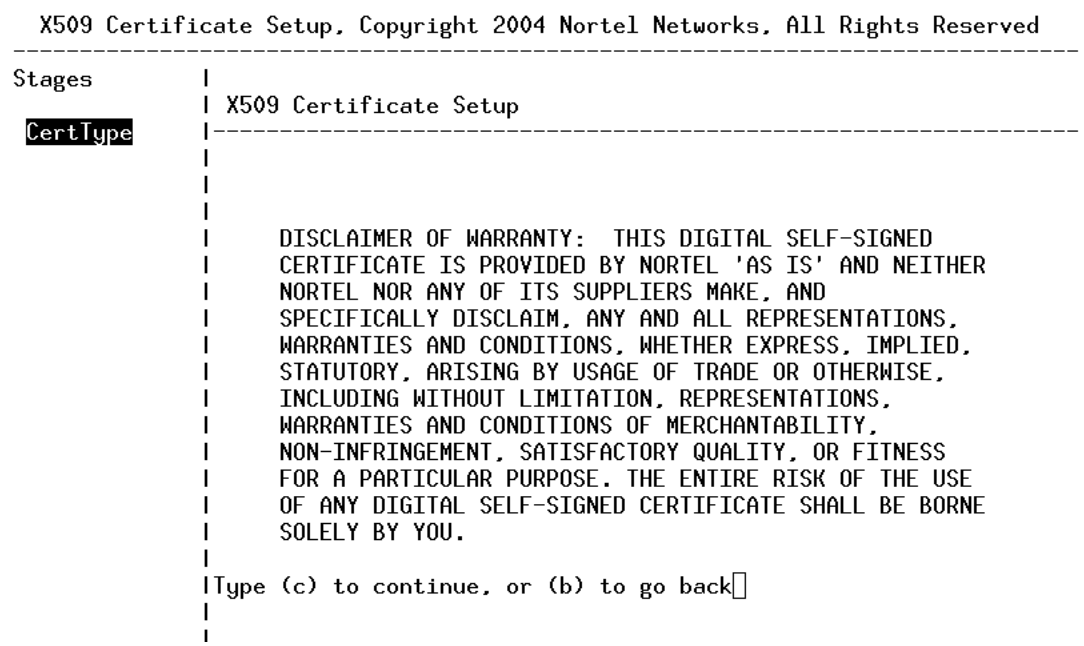


Figure 4 Disclaimer for Self-Signed Certificates (3 of 4)

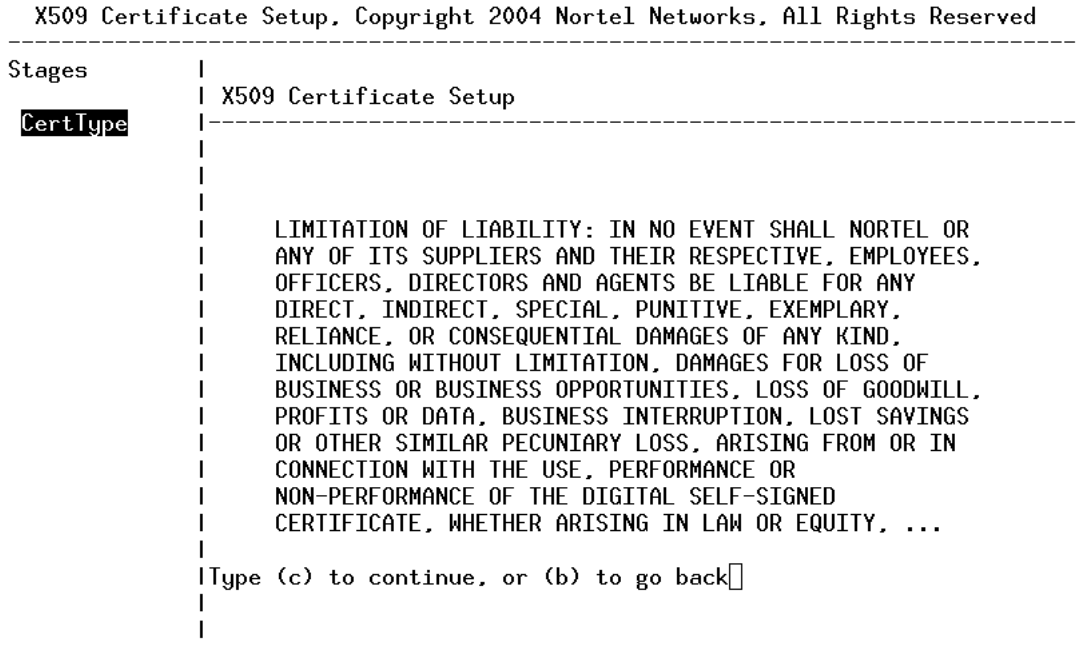


Figure 5 Disclaimer for Self-Signed Certificates (4 of 4)

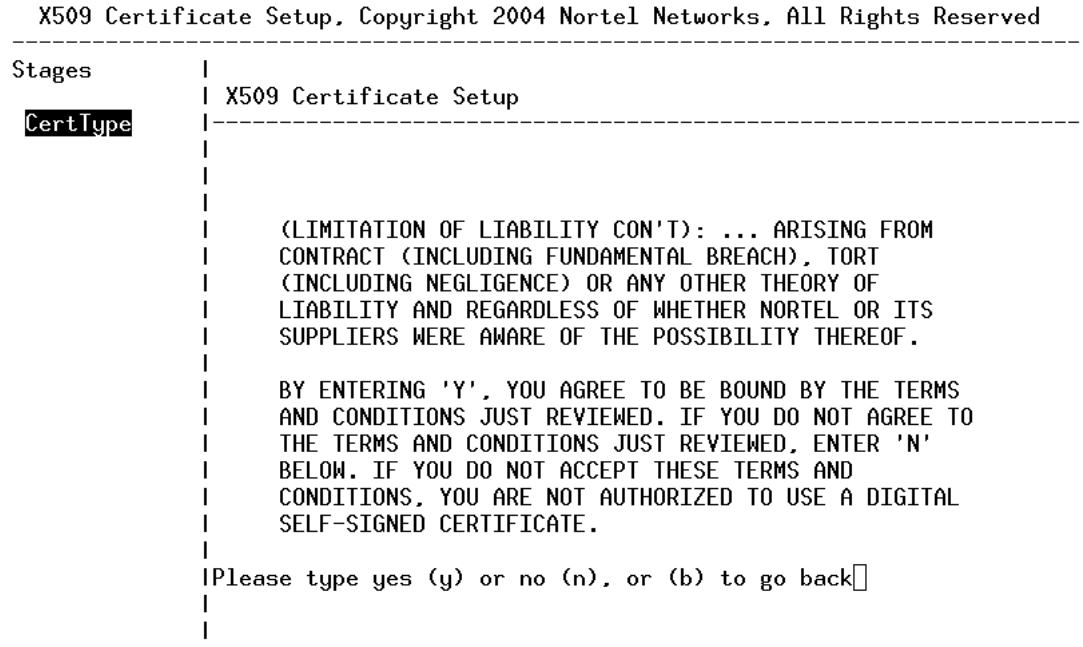


Figure 6 Select Key Size

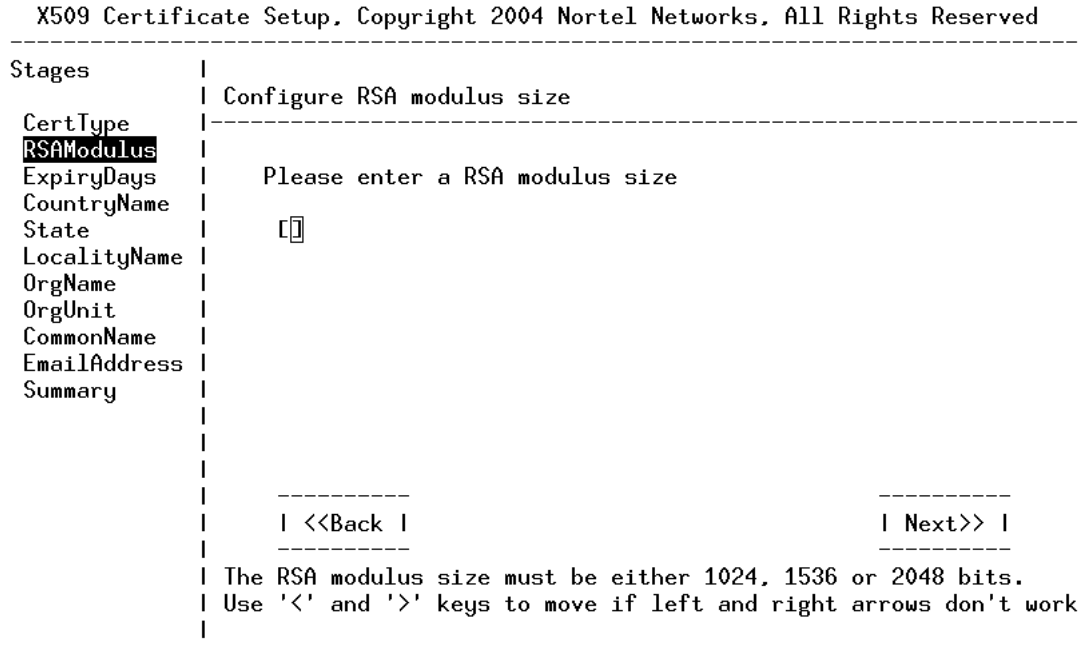


Figure 7 Key Already Exists

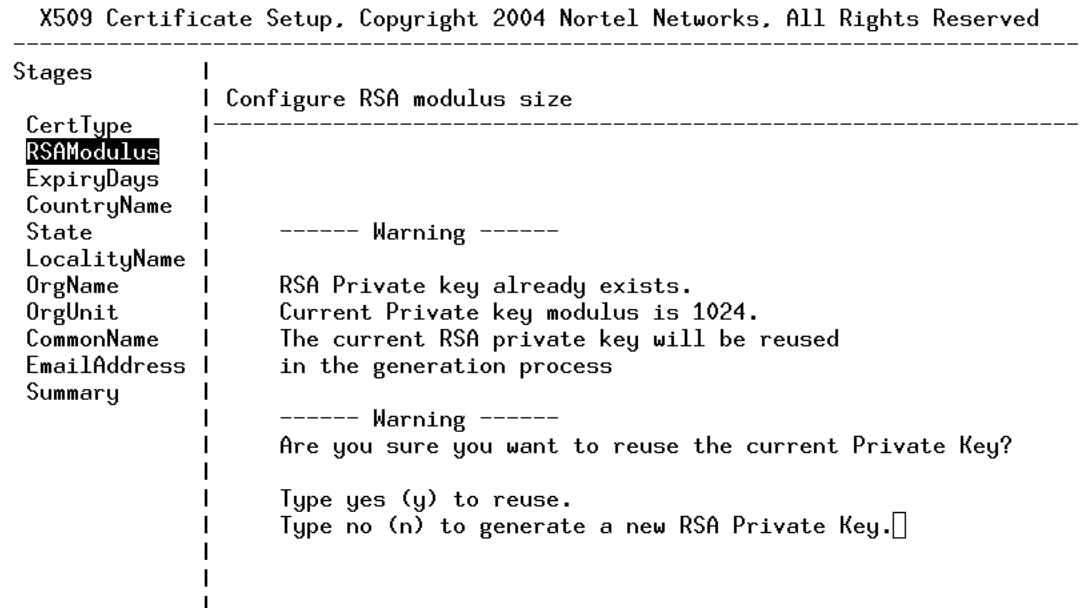


Figure 8 Remove Existing Key

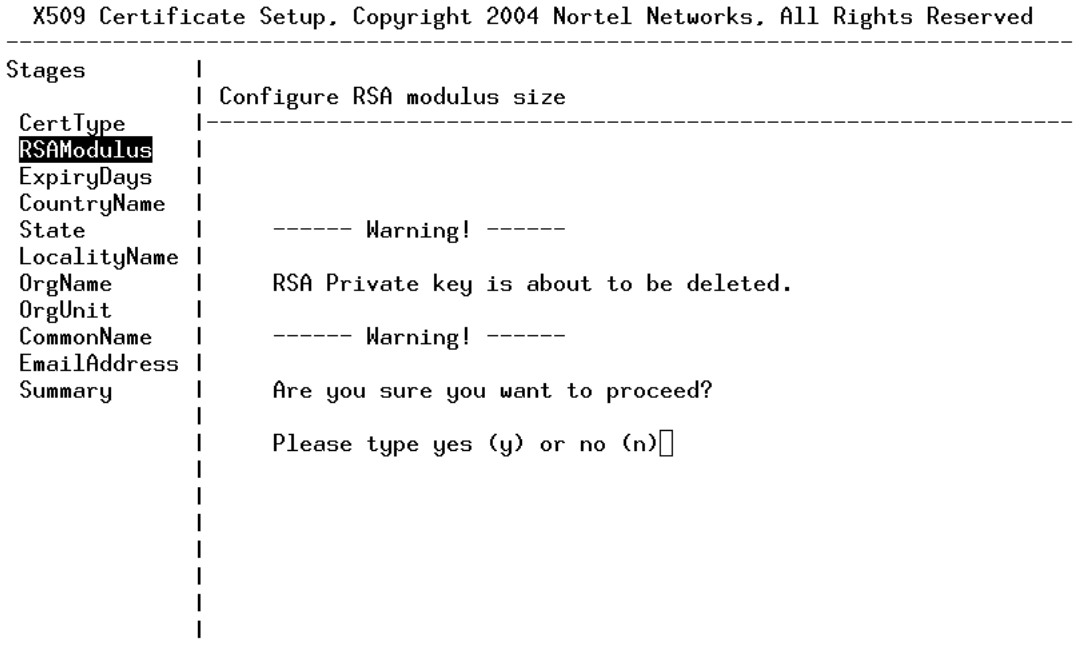


Figure 9 Expiry Days

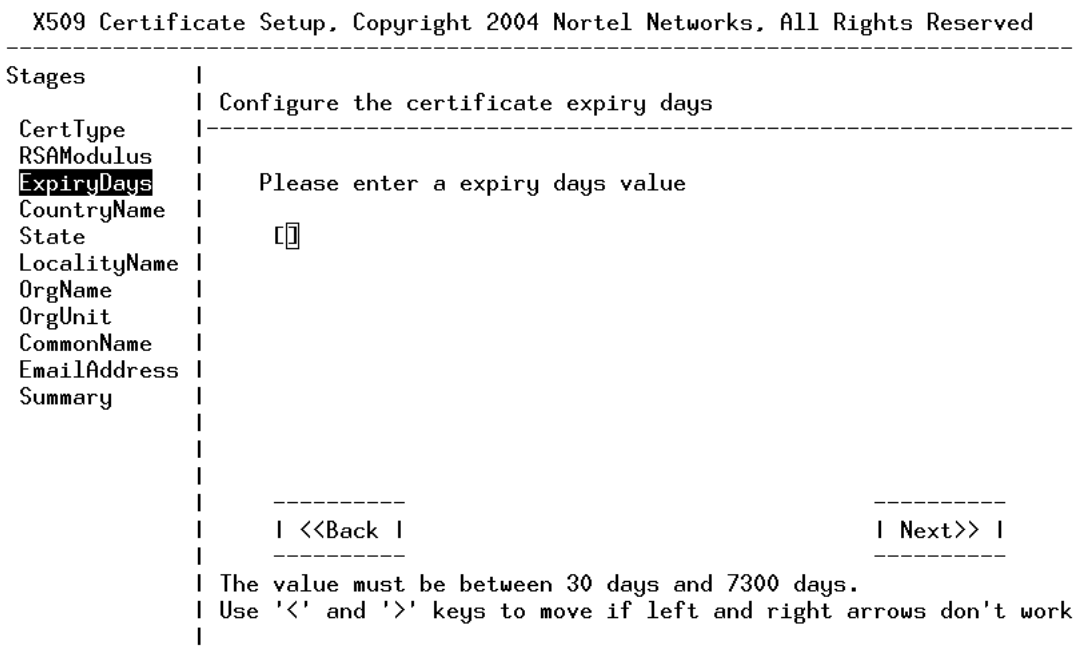


Figure 10 Country Name

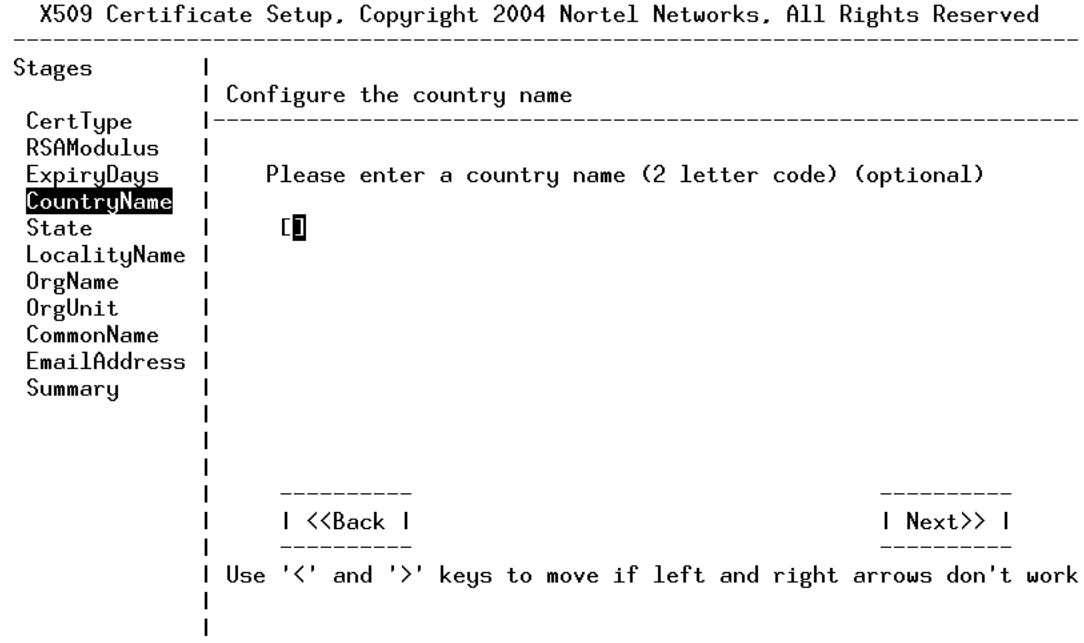


Figure 11 State Name

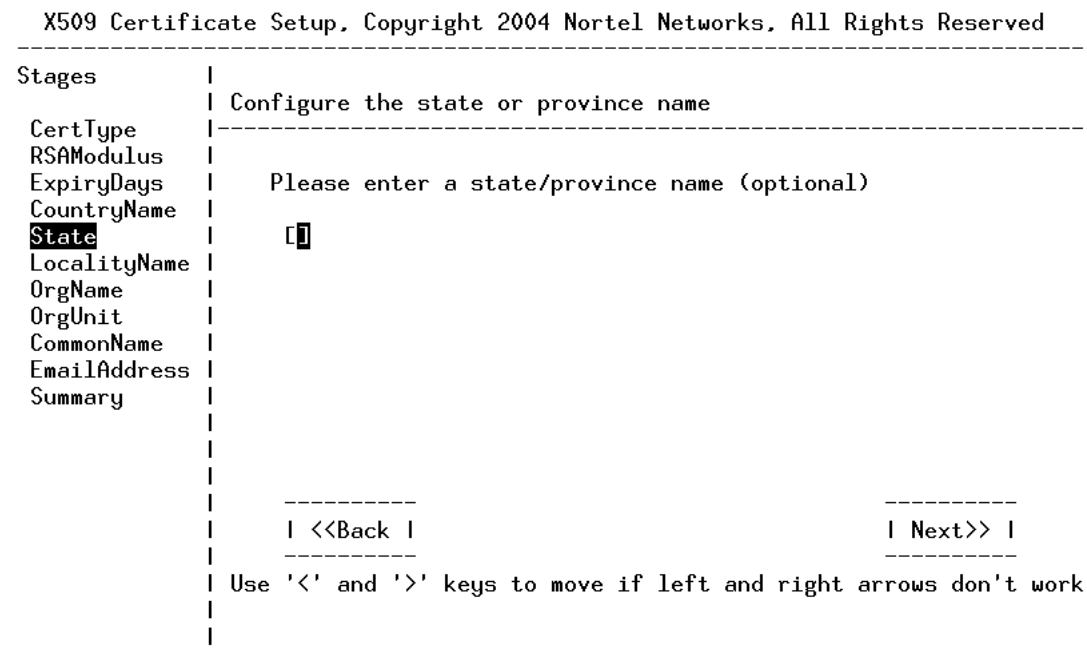


Figure 12 Locality Name

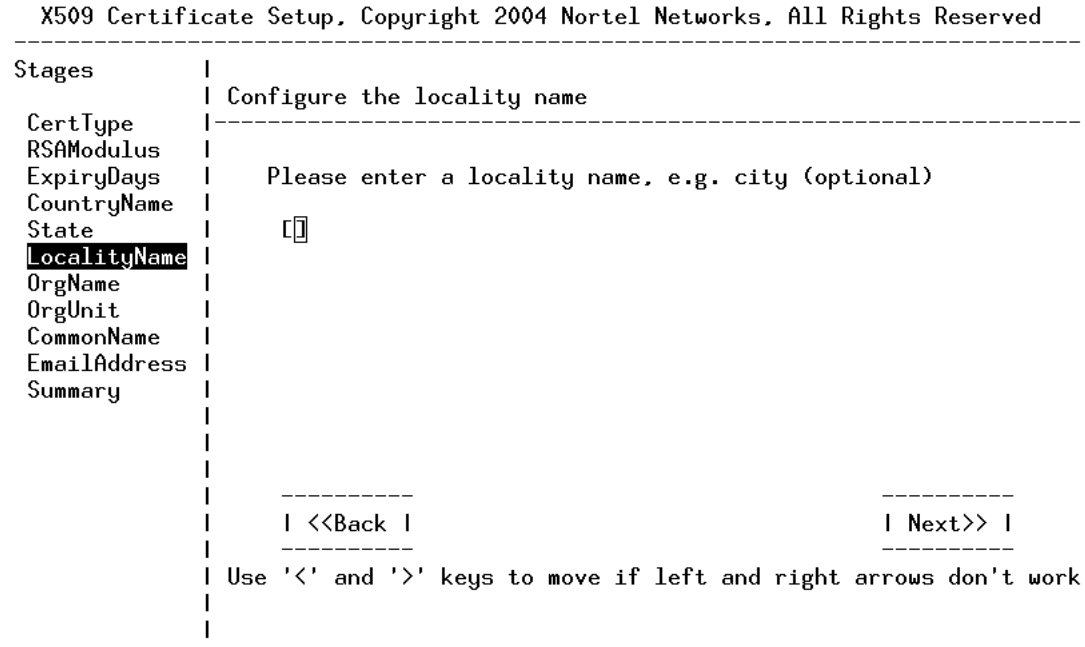


Figure 13 Organizational Name

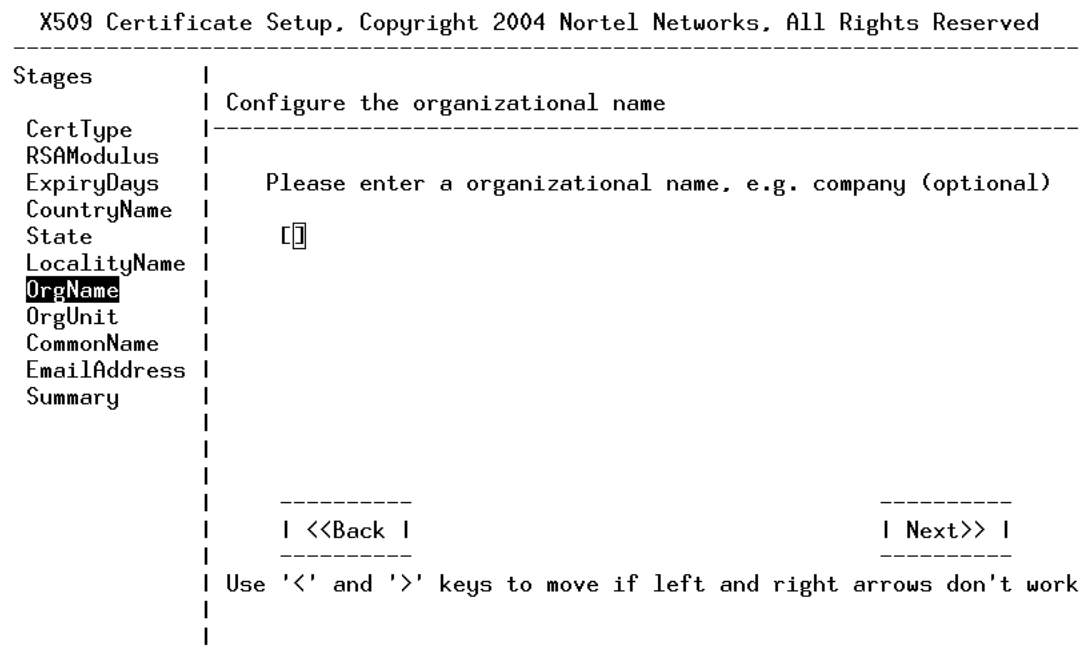


Figure 14 Organizational Unit Name

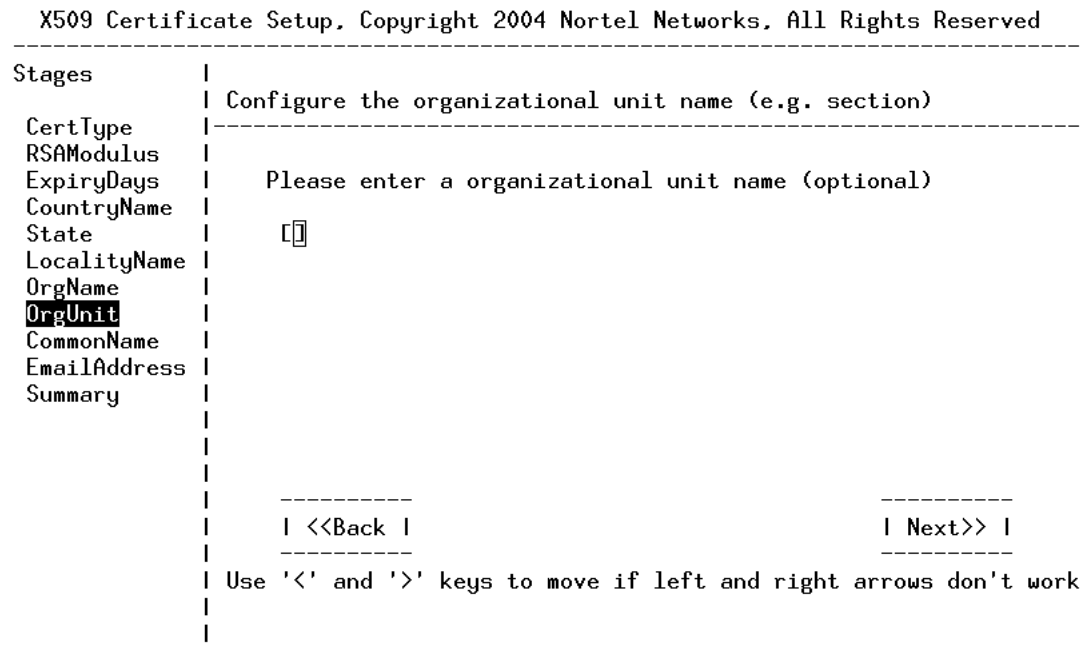


Figure 15 Common Name

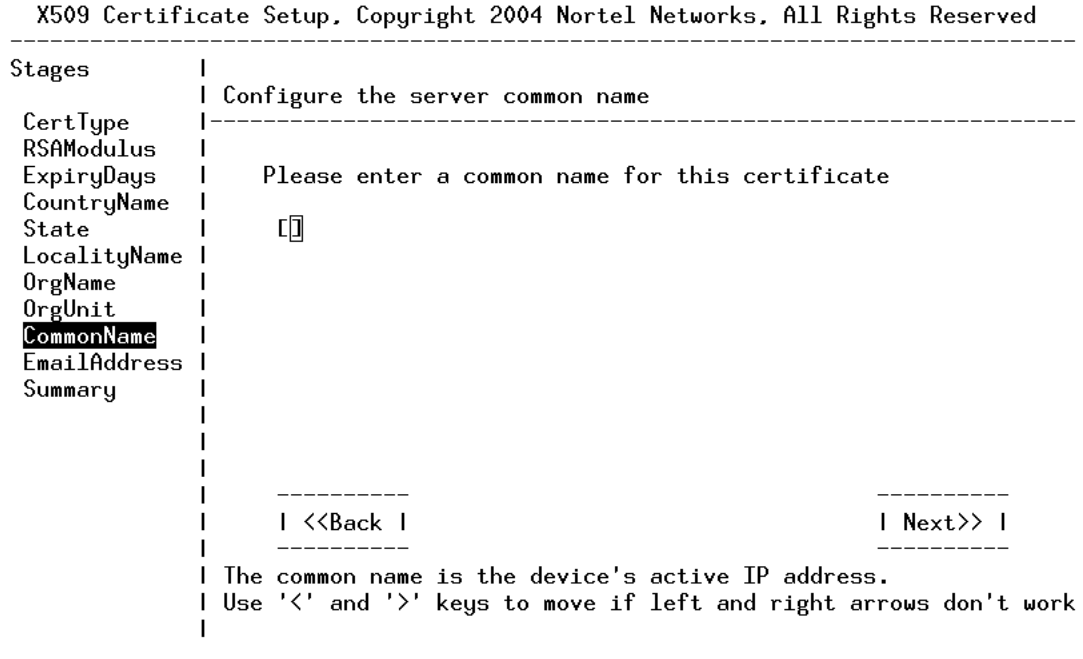


Figure 16 Email Address

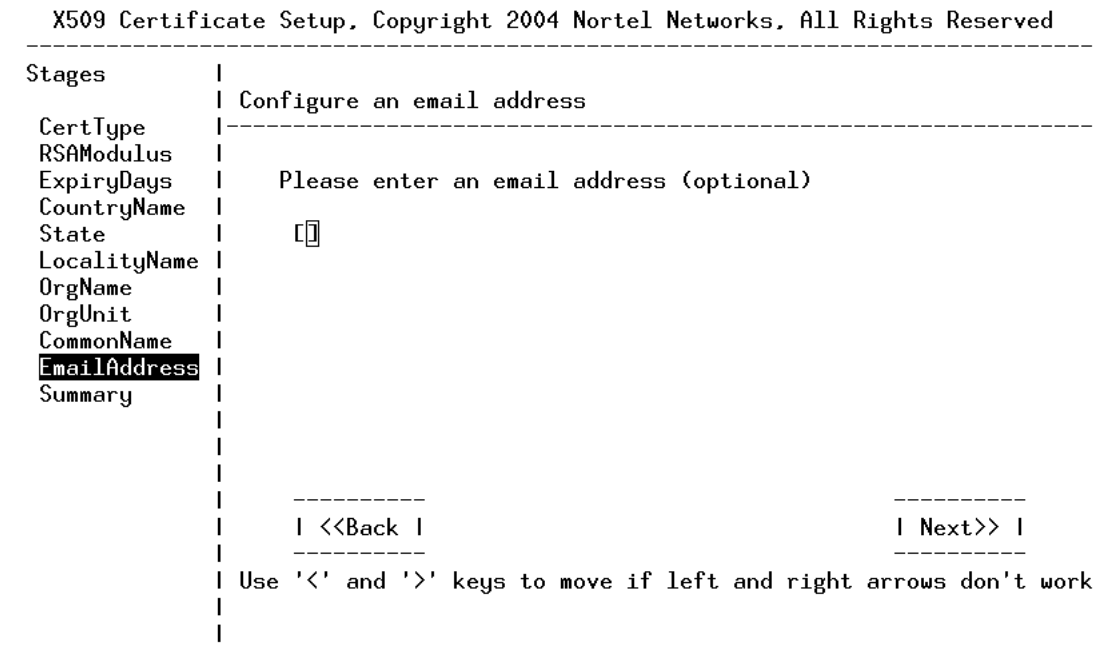
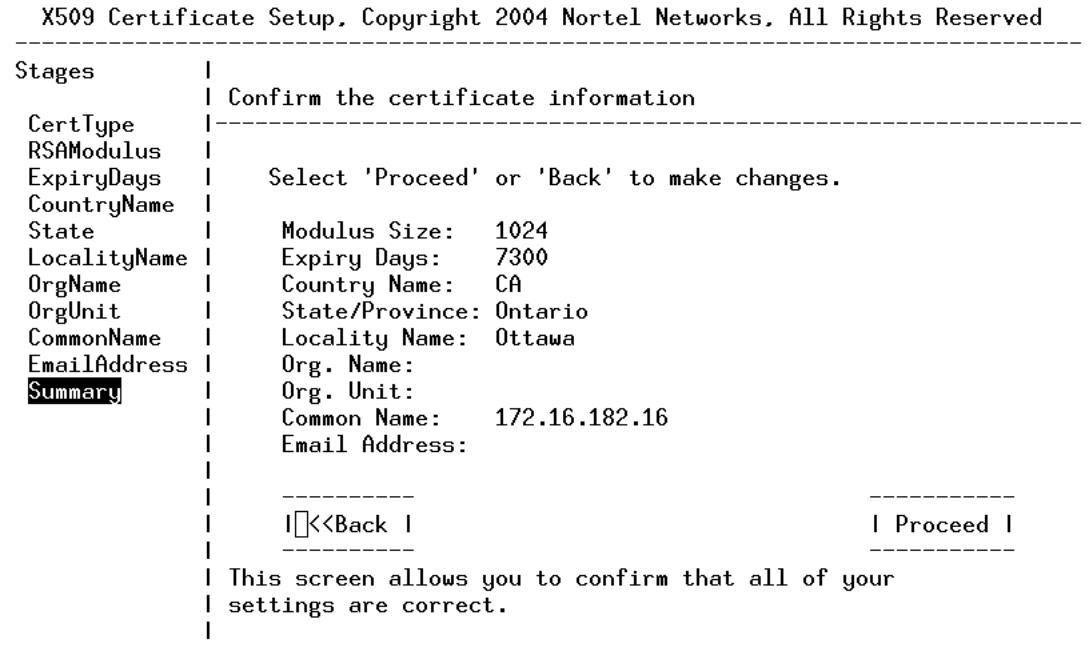


Figure 17 Summary for Self Signed Certificates



23.9.3.1.5 Certificate Signing Request

1. In the case of a certificate signing request, the craftsperson selects option 2 in Figure 1 ”Choose a Certificate Type” on page 2486.
2. Going back at any time will display the previous panel. Selecting proceed will only work if the craftsperson has entered the required information.
3. The craftsperson selects an RSA key size in Figure 6 ”Select Key Size” on page 2489. The key size can be 1024/1536/2048 bits. The higher the key size, the stronger the private key. There may be a performance impact to using higher key sizes due to additional encryption requirements.
   - If the key already exists in the /opt/base/share/ssl/ directory, the tool will prompt to reuse it or delete it and recreate a new key.
   - If the craftsperson wishes to reuse the key, the tool will always accept the key’s current size. This is illustrated in Figure 7 ”Key Already Exists” on page 2489
   - If in Figure 7 ”Key Already Exists” on page 2489, the craftsperson select ‘n’ that they do not want to proceed, then the tool prompts for key deletion in Figure 8 ”Remove Existing Key” on page 2490.
   - If in Figure 7 ”Key Already Exists” on page 2489, the craftsperson select ‘y’ that they do want to proceed, then the tool will reuse the existing key and move on to step 4.
   - If in Figure 8 ”Remove Existing Key” on page 2490, the craftsperson selects ‘n’ that they do want to proceed, the tool will then abort the current operation and return to the top of this step 3.
   - If in Figure 8 ”Remove Existing Key” on page 2490, the craftsperson selects ‘y’ that they do want to proceed, the tool will then make a backup of the existing key to another file in the same directory. A customer log is generated for this case.
4. The craftsperson selects a country, state, and city name in Figure 10 ”Country Name” on page 2491, Figure 11 ”State Name” on page 2491, Figure 12 ”Locality Name” on page 2492. These fields are optional. Although they are optional, they help to identify the NGSS to a remote entity.
5. The craftsperson selects an organizational name, and an organizational unit name in Figure 13 ”Organizational Name” on page 2492, and Figure 14 ”Organizational Unit Name” on page 2493. These fields optional. Although they are optional, they help to identify the NGSS to a remote entity.
6. In Figure 15 ”Common Name” on page 2493, the craftsperson identifies the mandatory common name. In the case of the NGSS, this must be the IP address of the active NGSS host. This is used for mutual authentication and is necessary for the correct operation of the NGSS. There is no validation at this stage of the common name.
7. In Figure 16 ”Email Address” on page 2494, the craftsperson identifies the optional email address of the local contact. There is no validation of the email address.
8. In Figure 18 ”Challenge Password” on page 2496, the tool queries for a challenge password. This password is used by the tool only.

9. Once all the information is entered, the tool displays a summary Figure 19 ”Certificate Signing Request Summary” on page 2497. Selecting “proceed” will generate the self signed certificate. The following message will be displayed on success.
10. Certificate Management:

```
Generating Certificate Signing Request
Generating a RSA Key
RSA private key has been successfully generated
Creating Certificate Signing Request
Certificate Signing Request has been successfully generated
-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----
Changing permissions on key file
Changing permissions on keystore file
```

11. The certificate signing request between the <BEGIN> and <END> delimeters is sent to the Certificate Authority for signing and certificate generation. Once that is done, the certificate authority’s certificate and the signed certificate are used to perform the function in section 23.9.3.1.6 ”Import Certificates and Private Key” on page 2497.

Figure 18 Challenge Password

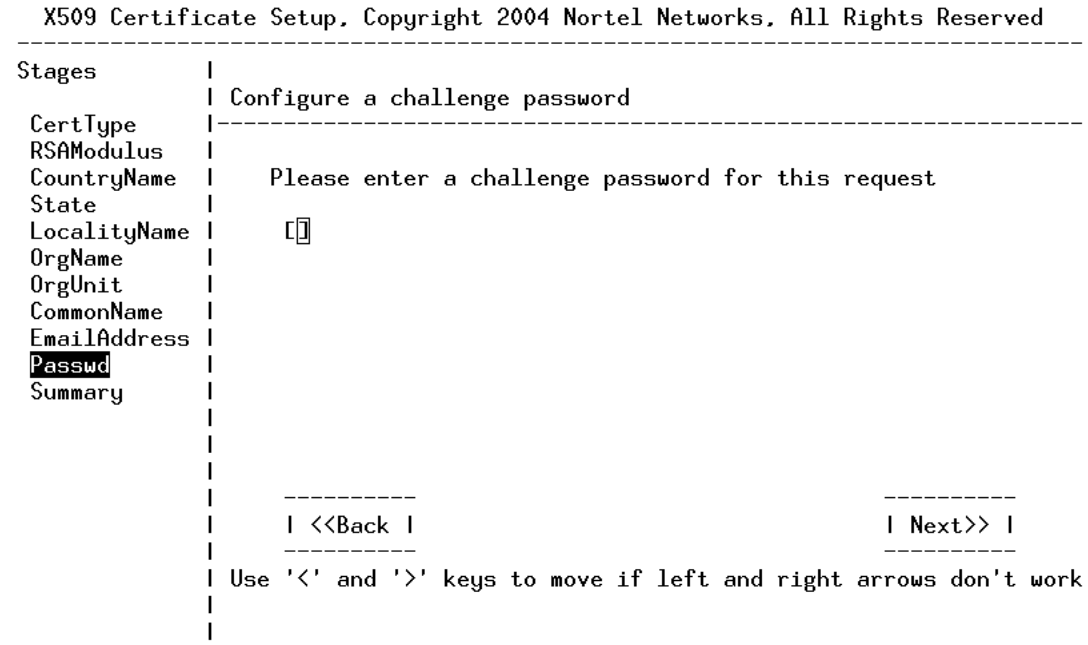
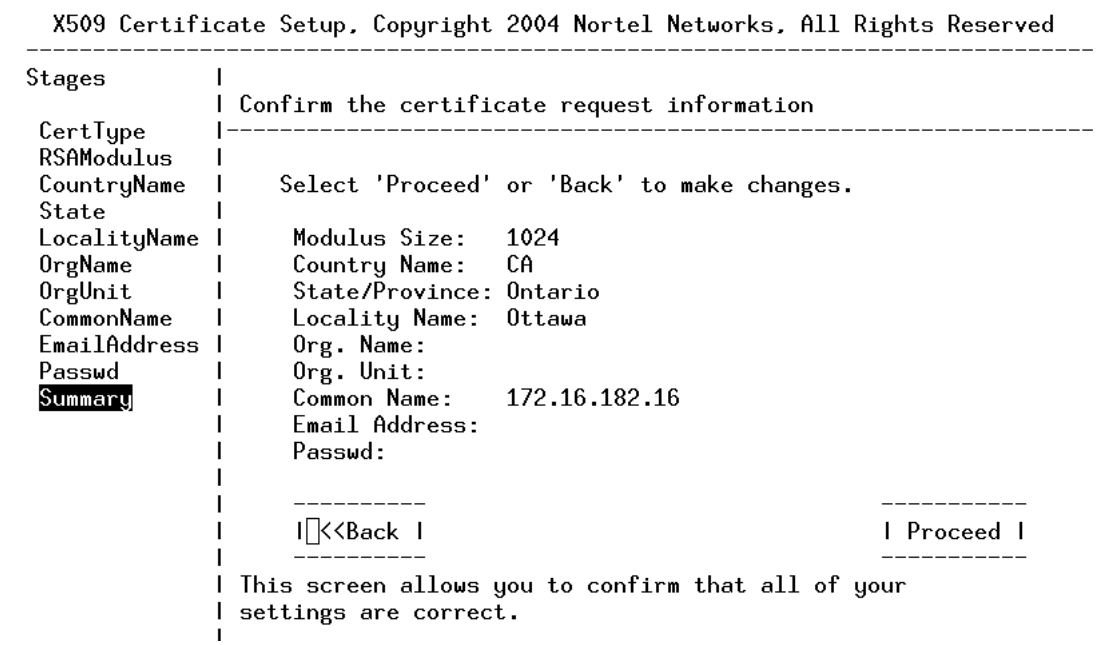


Figure 19 Certificate Signing Request Summary



23.9.3.1.6 Import Certificates and Private Key

It is recommended that this procedure NOT be executed from /opt/base/share/ssl nor is it recommended that the files be copied there prior to the execution of this procedure.

This procedure can be used to:

- Provision the self-signed certificate on the mate unit, and commit the files to /opt/base/share/ssl.
- Provision the CA-signed certificate from the signing request in option 2. The same private key that was generated in option 2 must be available.

1. Provide the CA certificates:
   - If this procedure is being used to provision the self-signed certificate on the mate unit, then, In Figure 20 , the craftsperson supplies the full path and filename where the self-signed certificate can be found. The tool will not proceed unless the file exists.
   - If this procedure is being used to import the CA-signed certificates, then, In Figure 20, the craftsperson supplies the full path and filename where the CA chain certificates can be found. The tool will not proceed unless the file exists.
2. Provide the server CA-signed certificate:

- If this procedure is being used to provision the self-signed certificate on the mate unit, then, In Figure 21 ”Server Certificate - CA signed certificate” on page 2500, the craftsperson supplies the full path and filename where the self-signed certificate can be found. The tool will not proceed unless the file exists.
- If this procedure is being used to import the CA-signed certificates, then, In Figure 21 ”Server Certificate - CA signed certificate” on page 2500, the craftsperson supplies the full path and filename where the CA signed certificate can be found.. The tool will not proceed unless the file exists.

3. Provide the private key. The craftsperson supplies the full path and filename where the private exists in Figure 22 ”Provide the key” on page 2500.
4. Validation. In this step, the tool confirms the user input. By selecting “Proceed”, the tool completes the import in Figure 23 ”Import Summary” on page 2501.
5. If successful, the following messages are displayed (this example is for a self-signed certificate).

```
Provisioning CA Certificate
Verifying certificate/key pair
spawn openssl verify -CAfile server.crt server.crt
server.crt: OK
Certificate validation succeeded
Exporting certificate/key pair to PKCS#12 keystore
Committing trusted certificate to /opt/base/share/ssl
Committing server certificate to /opt/base/share/ssl
Committing private key to /opt/base/share/ssl
Certificate/key pair has been successfully exported to PKCS#12 format
Changing permissions on key file
Changing permissions on keystore file
```

Figure 20 CA Certificate - Trusted certificate

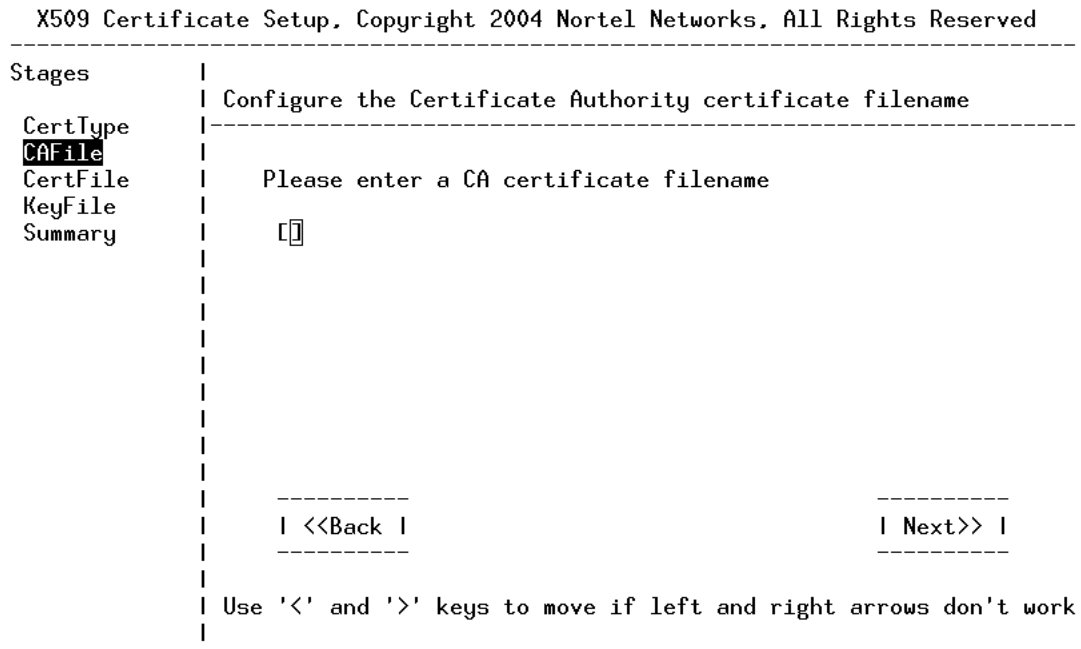


Figure 21 Server Certificate - CA signed certificate

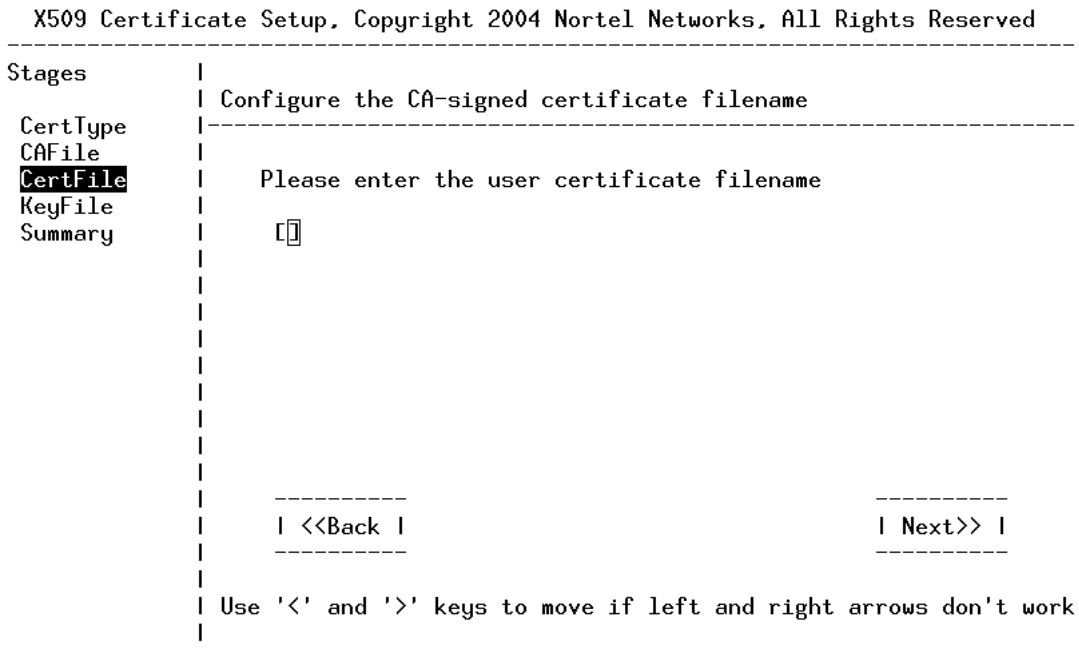


Figure 22 Provide the key

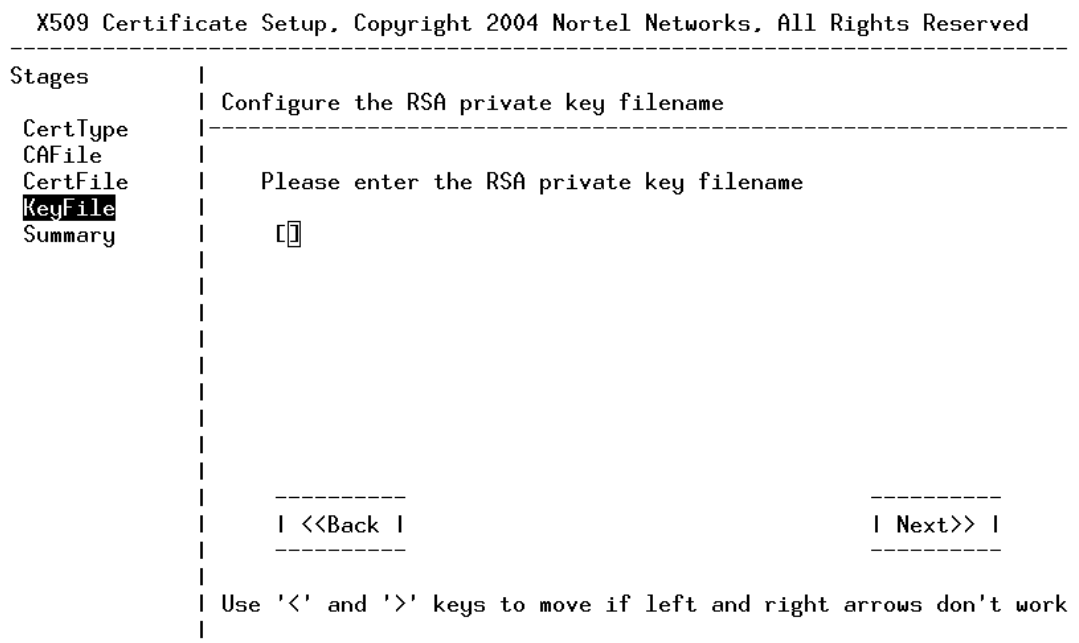
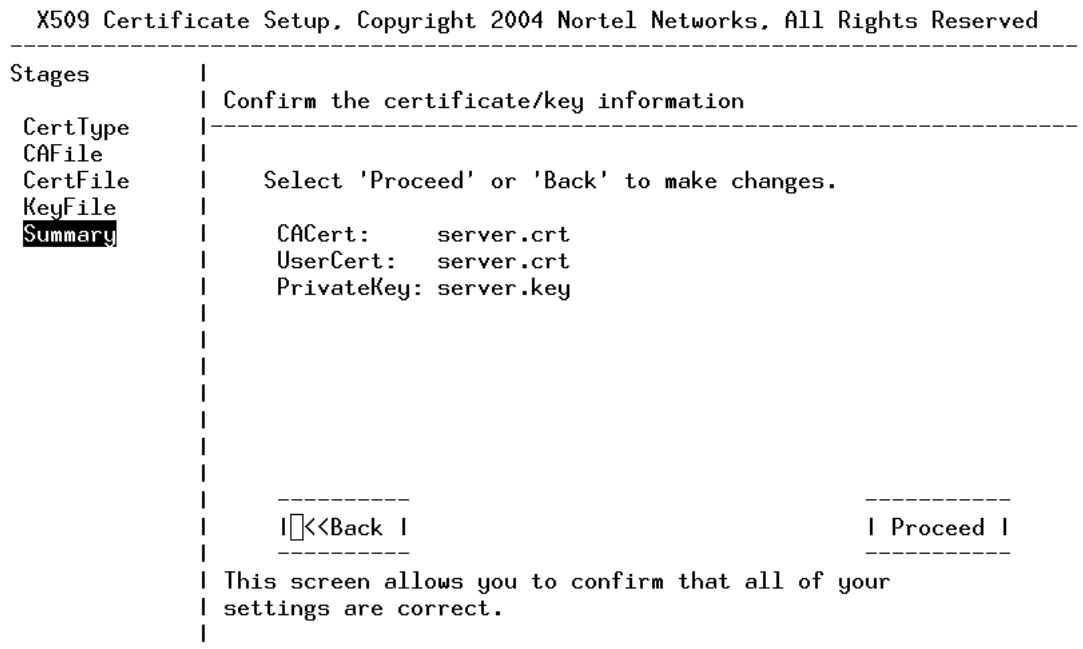


Figure 23 Import Summary



Import Summary shown above assuming a self-signed certificate import from the mate unit.

23.9.3.1.7 After provisioning a new certificate

Once the new certificate/key pair is in place, the Apache, Tomcat, and SIPGWYAPPLN applications must be restarted to ensure they are using the new certificate. This can be handled by rebooting the unit on which the new certificate was provisioned on, or by just stopping and starting the individual applications.

23.10 User interface changes

Not applicable.

23.11 OSSGate Interface Changes

Not applicable.

23.12 Security

23.12.1 Network configuration

Network configurations should not be changed as a result of this feature.

23.12.2 Key management

Key management will be done automatically as part of certificate management procedures. Keys will thus be managed internally by the CS2000 Session Server web server and/or CLI tools. No customer interface dealing with keys will be implemented.

23.12.3 Protocol

This activity is not making changes to protocols that are used to manage security.

23.12.4 Authentication

No change.

23.13 Configuration Walkthrough

See section 23.9 “Element Management” on page 2454.

24: Configuration (CN): A00009280

24.1 Feature Name

MG9K Line Circuit Enhancements

24.2 Hardware and Software Requirements

This functionality is for MG9000 EM that has SN09 or higher software version.

24.3 Initial Configuration

No changes for initial configuration

24.4 Upgrade Considerations

None.

24.5 Element Management

24.5.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
WLC View	CHANGED
GLC View	CHANGED
XDSL View	CHANGED
SAA View	CHANGED
LINE CIRCUIT View	CHANGED
FAULTY CIRCUIT LISTING	NEW

24.5.2 GUI information

24.5.2.1 GUI name: Line Card View (WLC, XDSL,GLC,SAA)

24.5.2.1.1 Functional description

From release SNO9, the line card view would display alarm color indication for the ports. A faulty port would be indicated with magenta color on the line card view. Display of only voice circuit ilogs changes on a XDSL view for faulty ports.

An example of WLC view is shown in Figure 1.

Figure 1 WLC View with faulty and alarm status indications on port ilogs

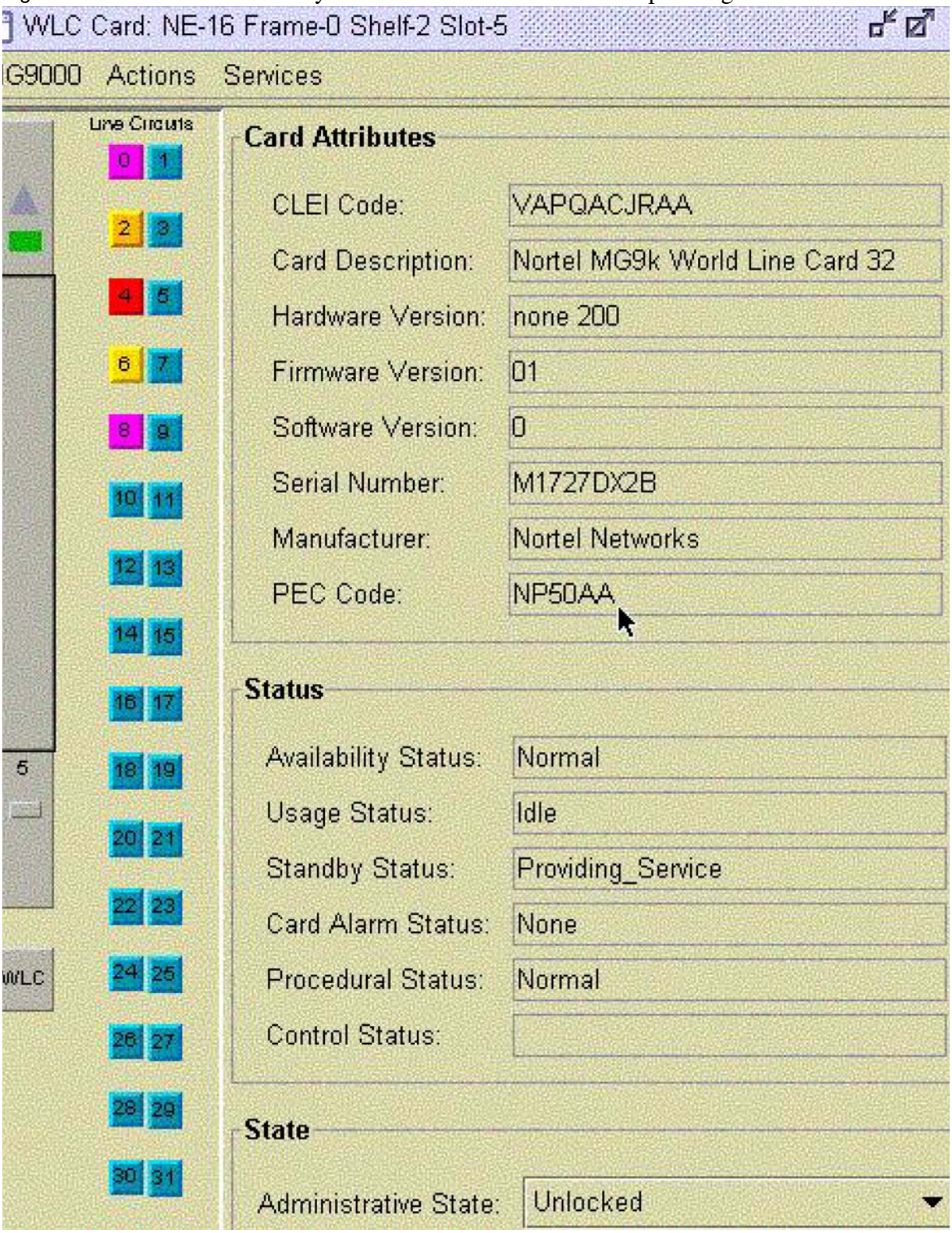


Figure 1 shows the WLC Card view with minor alarm on port 2, critical alarm on port 4, and warning on port 6. Also port 0 and port 8 are manually marked as faulty by the User

24.5.2.1.2 GUI fields

No new GUI fields are added.

Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Circuit Listing	Changed	NA	NA	Line Circuits listed on the WLC card view would be displayed with an appropriate alarm color or fault color. The default color of the port is blue	NA

24.5.2.2 GUI name: Line Circuit View

24.5.2.2.1 Functional description

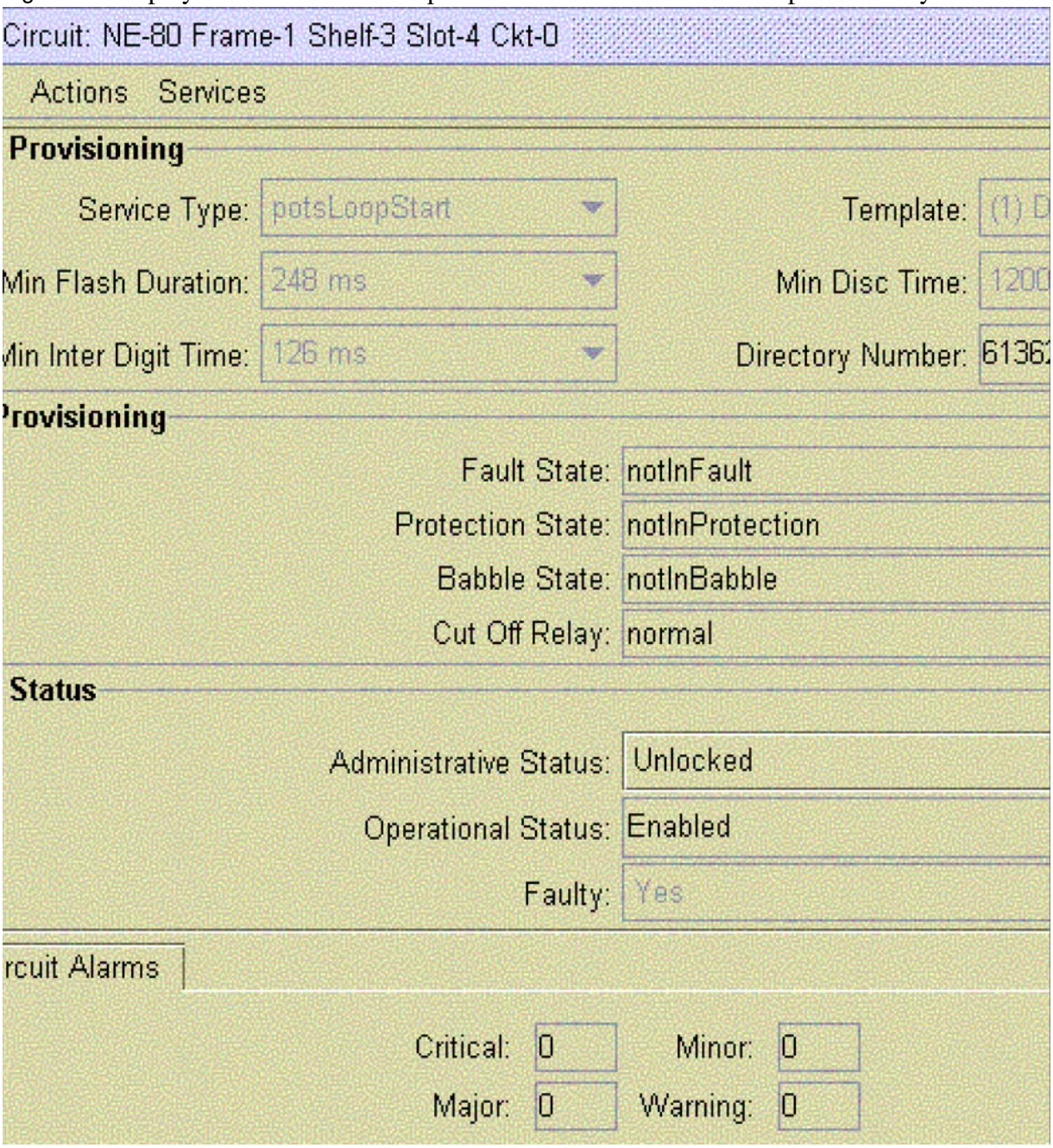
1> From release SNO9, the Line Circuit view would allow the User to mark a port as faulty with a prerequisite that the port should be locked.

The faulty combo box would be available in the 'Circuit Status' section of the Line Circuit View. This combo box would be disabled(greyed out) when the port is unlocked.

2> From release SNO9, the Line Circuit View would display the Directory Number (DN) associated with a termination point (line circuit). This information is displayed in the 'Circuit Provisioning' section of a Line Circuit View.

Figure 2 shows the display of Line Circuit view with associated DN Affected: 6136210202 displayed in Circuit Provisioning section. Also shown is the ability for the User to manullay mark the port as faulty when the port is locked from the Circuit Status section.

Figure 2 Displays associated DN and provision for the User to mark a port as faulty



User can select ‘No’ or ‘Yes’ from the ‘Faulty’ drop down to set the port as faulty or non faulty, accordingly. This dropdown is enabled only when the Administrative Status of the port is locked.

User can unlock the circuit which is marked as faulty. But he is displayed a warning message saying:

"The circuit is marked as faulty; the existing service may be degraded Are you sure?"

By selecting 'OK' option, he can submit the 'unlock' request to the Gateway.

By selecting 'Cancel' option, he would not submit the 'unlock' request to the Gateway.

24.5.2.2.2 GUI fields

24.5.2.3 GUI name: Faulty Circuit Listing View

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Faulty - Combo Box	New	NA	1> No 2> Yes	The Faulty Port Status Combo box and label are displayed in the 'Circuit Status' section of Line Circuit View This field is enabled when the port is locked. By selecting combo item 'No', User removes the faulty bit set for the port By selecting combo item 'Yes', User marks manually a port as faulty.	NA
Directory Number TextBox	New	NA	1>None 2><Associated DN>	The Directory Number label and text box are displayed in the 'Circuit Provisioning' section of the Line Circuit View. This is a read-only field. If any DN is associated with the line circuit then it gets displayed, else the field displays 'None' in the text box.	NA

24.5.2.3.1 Functional description

From release SNO9, the Faulty Circuit Listing view would be added to a new menu item of the Services menu option, on the NE desktop view.

24.5.2.3.2 GUI usage and implications

From the NE desktop view, go to the 'Services' Menu list.

The drop down would list ‘Faulty Circuit Listing’ menu item. Clicking on this menu item would display the ‘Faulty Circuit Listing’ view.

This view would list all the ports manually marked as faulty by the User on an NE along with their location information.

The view would have a timestamp associate with the last refresh and a ‘Refresh’ button. Using ‘Refresh’ button user can view the latest faulty port information.

Figure 3 shows the new ‘Faulty Circuit Listing’ GUI when no faulty ports are available. The text above the table header would display ‘No Faulty circuits found’.

Figure 3 Faulty Circuit Listing GUI with no faulty ports

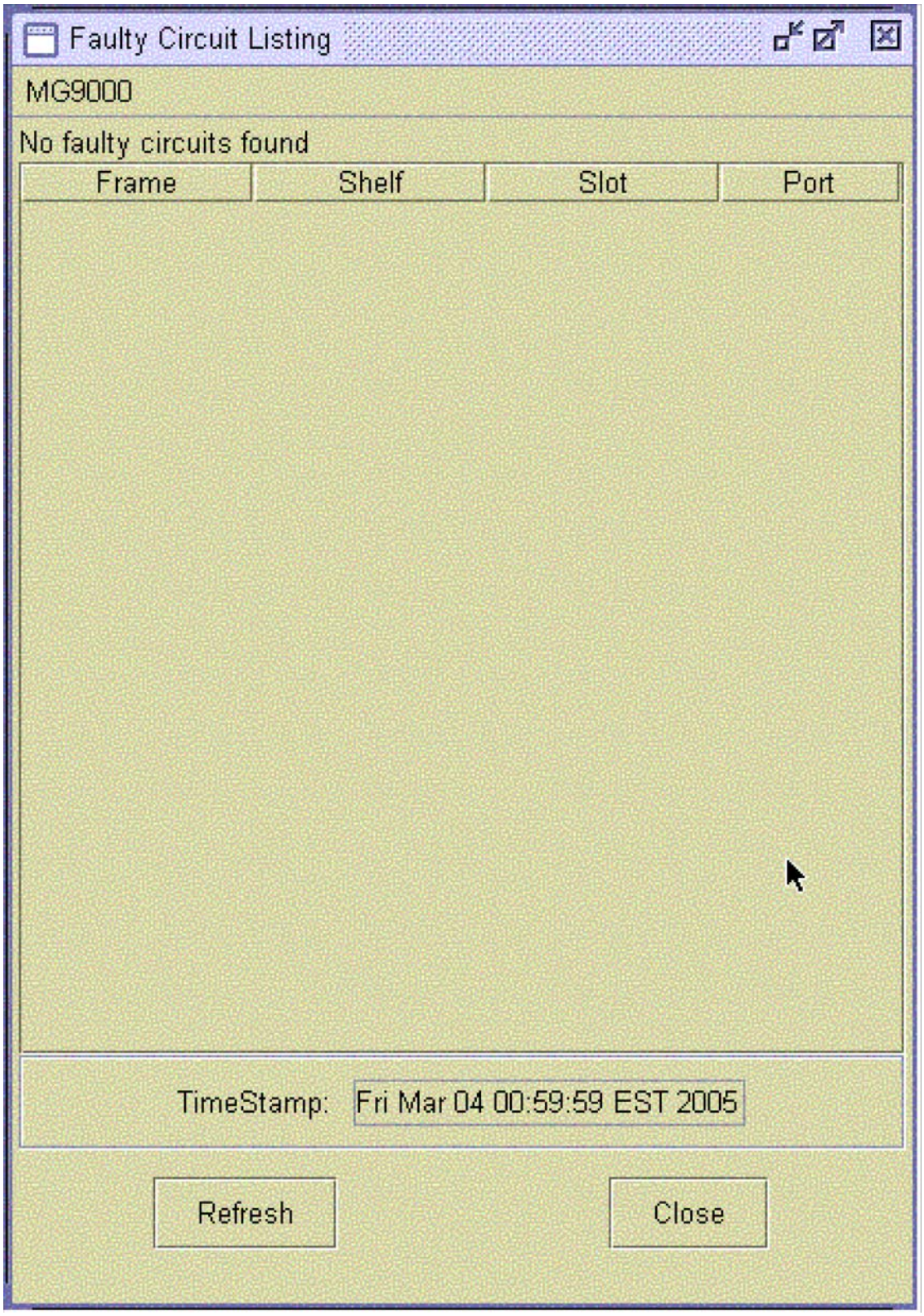
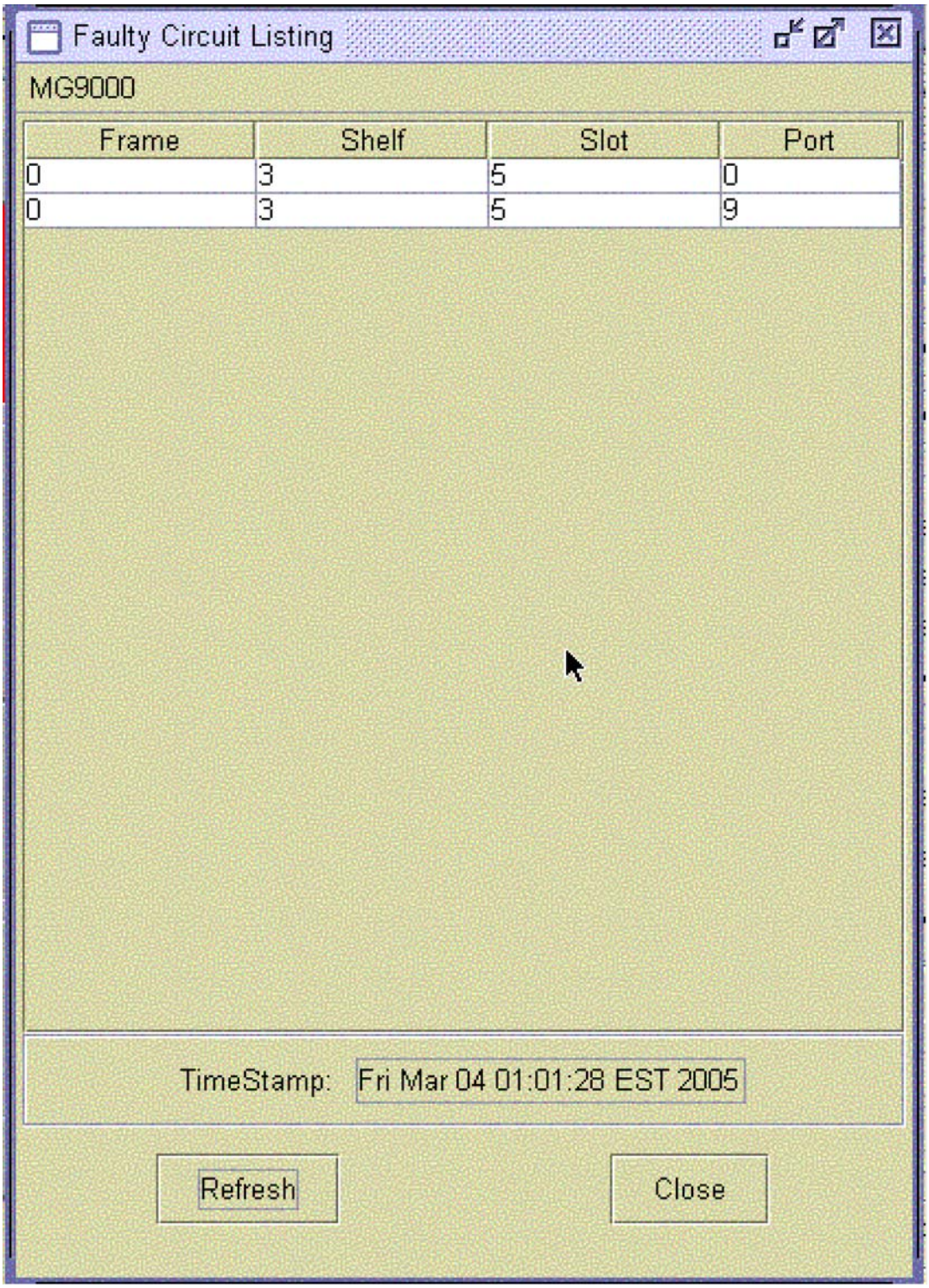


Figure 4 shows the ‘Faulty Circuit Listing’ gui when faulty ports exist. The Time Stamp field indicates the last time when the data was pulled from DB.

Figure 4 Faulty Circuit Listing



24.5.2.3.3 GUI size

24.5.2.3.4 GUI fields

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Faulty Circuit Listing View	1	1	

The following table lists the new fields for the Faulty Circuit Listing View.

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Frame Number	New	NA	NA	The associated frame number of the faulty port	NA
Shelf Number	New	NA	NA	The associated shelf number of the faulty port	NA
Slot Number	New	NA	NA	The associated slot number of the faulty port	NA
Port Number	New	NA	NA	This field speaks about the faulty port number	NA

24.6 Security

NA

25: Configuration (CN): A00009282

25.1 Feature Name

Emergency Stand Alone (ESA) Multiple Level Precedence and Preemption (MLPP) for MG9KEM

25.2 Hardware and Software Requirements

None.

25.3 Initial Configuration

This document assumes that the reader is familiar with Emergency Stand-Alone(ESA). ESA allows intra-nodal calls to complete when the MG is cutoff from thecall server. Prior to SN08 only intra-nodal ESA was supported. With theintroduction of this feature, inter-nodal ESA is now supported as of SN08.Internodal ESA allows groupings of MG nodes into communities of interest(COI). All nodes in a community can communicate with each other during ESA,allowing calls to complete inside the community during ESA.The Passport Virtual Router must be configured before Internodal ESA willfunction. The Passport settings are located on the NE Properties GUI on the EM.Each node in the community must be configured with PVR settings before thecommunity is established.The customer should first determine how the nodes will be grouped together intocommunities. In addition each MG will need to be configured with a new ESAIP address. This IP address should be chosen from an available IP address fromthe call control subnet (the same subnet used for VMG configuration). Nodefault communites are provided so each community must be manuallyconfigured by the customer in order for inter-nodal ESA to function.

The high-level steps for adding a community of interest are as follows:

1) Load the MG9K, MG9KEM, and PVR with required software.

2) Launch the MG9K Element Manager.

3) Select a node to be added to community and configure PVR settings from the

NE Properties screen. Repeat for each node.

4) Select Configure Internodal ESA from the Configuration Menu.

5) Set the ESA IP address of the nodes that are being placed into communities.

6) Create a new community of interest.

7) Add desired nodes to the community of interest.

8) Click Apply button.

9) Repeat for each community of interest.

25.4 Office/Subnet parameters (OP/SP) (CM & SESM)

NA

25.5 Upgrade Considerations

NA

25.6 Data schema (DS) (CM, MIBS, RDB)

NA

25.7 Service Orders (SO) (CM & SESM)

NA

25.8 Software optionality control (SOC)

NA

25.9 Element Management

25.9.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
NE Specific Desktop View	CHANGED
NE specific Internodal ESA View	NEW

25.9.2 GUI information

25.9.2.1 GUI name:NE Specific Desktop View

25.9.2.1.1 Functional description

Internodal ESA NE View: A new GUI is introduced under the submenu option Configuration option of NE Specific Desktop View. On clicking the ‘Internodal ESA’ from the configuration menu of NE Specific Desktop View, Internodal ESA View opens up. This GUI allows the user to ping the Nodes in its COI.

GUI usage and implications

On Clicking the NE from the Subnet view,NE Specific Desktop View is launched.

25.9.2.1.2 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
NE Specific View	1	1	TBD

25.9.2.1.3 GUI fields

The following table lists fields for GUI NE Specific Desktop View that are related to Internodal ESA NE .

GUI field descriptions

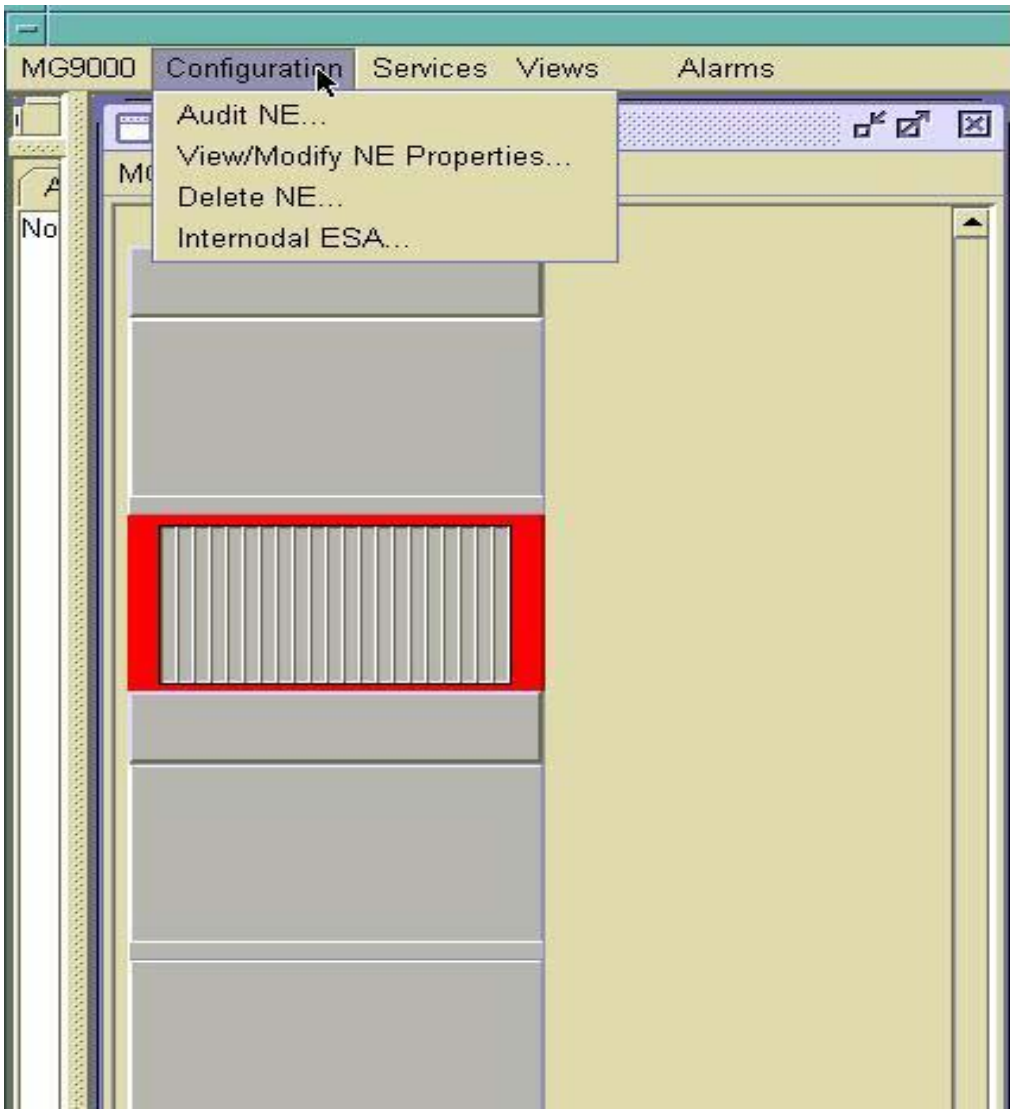
Table 3

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Internodal ESA	New	-	-	On Clicking Internodal ESA NE option of Configuration menu , Internodal ESA NE View is launched	NA

25.9.2.1.4 Usage example

Figure-1 NE Specific Desktop View

Figure-1 Shows the GUI when the Configuration menu item is clicked from NE Specific Desktop View.Menu item “Internodal ESA” is introduced, which when clicked launches Internodal ESA NE GUI.



GUI release history update

None

25.9.2.1.5 Context sensitive launching information
On clicking “Internodal ESA ” of Configuration menu from NE Specific Desktop view, Internodal ESA NE View is launched.

25.9.2.1.6 Supplementary information
None.

25.9.2.2 GUI name:Internodal ESA NE View

25.9.2.2.1 Functional description

Internodal ESA NE View: A new GUI is introduced under the submenu option Configuration option of NE Specific Desktop View. This GUI allows the user to ping the Nodes in its COI.

GUI usage and implications

Apply button has to be pressed .On pressing Apply ,the ping test is performed on to nodes.

25.9.2.2.2 GUI size

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Internodal ESA View	1	1	TBD

25.9.2.2.3 GUI fields

The following table lists fields for GUI Internodal ESA NE View .

GUI field descriptions

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
NE Name	New	-	-	Name of the NE belonging to the COI	-
“Initiate Test” button	New	-	-	On Clicking Apply the ping test is performed, each node in the COI will ping every node in the COI and the user will be given ping status for each nod	MIB name: NORTEL-UEMG-ESA.mib Table name:None Attributes: nnEsaNetworkAuditStatus

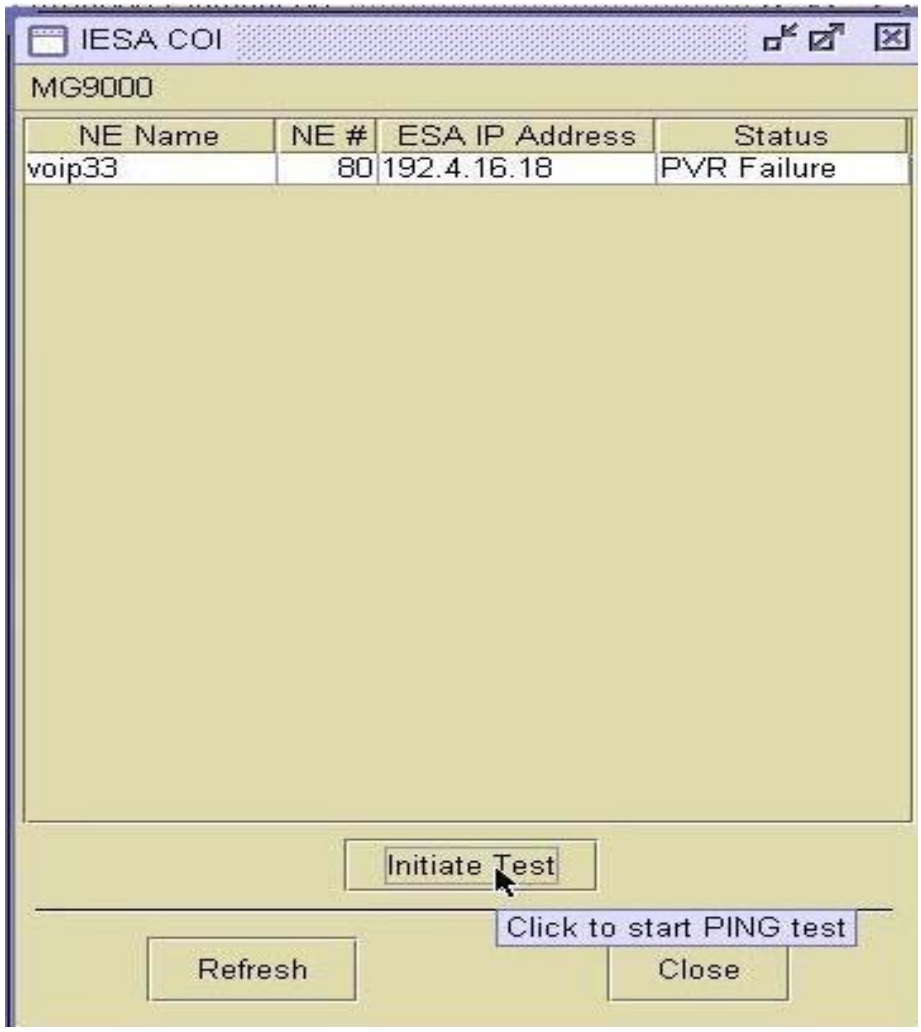
Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
"Refresh" Button	New	-	-	On Clicking Refresh button,the Status is updated	-
“Close” button	New	-	-	On Clicking Close button, GUI is closed	-

25.9.2.2.4 Usage example

Figure-2 Internodal ESA NE View

The following Figure shows the GUI for Internodal ESA NE View



25.9.2.2.5 GUI release history update
A new GUI is introducedInternodal ESA View which allows the user to ping the nodes.

25.9.2.2.6 Context sensitive launching information
On clicking “Internodal ESA NE” of Configuration menu from NE Specific Desktop view, Internodal ESA View is launched. On clicking the “Initiate Test” button of Internodal ESA View, Starts the ping process.

25.9.2.2.7 Supplementary information
None.

25.9.2.2.8 GUI release history update

25.9.2.2.9 Context sensitive launching information

25.9.2.2.10 Supplementary information

None.

25.9.3 CLUI Interface

None

25.10 User interface changes

NA

25.11 OSSGate Interface Changes

None

25.12 Security

NA

25.13 Configuration Walkthrough

Before initial configuration of inter-nodal ESA begins, the MG9K nodes must be configured to support ESA (see feature A00002020 for more details on configuring intra-nodal ESA). The customer should also determine how the nodes will be grouped into communities, i.e. which nodes go into which community of interest. In addition each MG9K that supports inter-nodal ESA will need to be configured with an ESA IP address. This IP address should be chosen from an available IP address from the call control subnet. This is the subnet of IP addresses used for VMG configuration. No default communites are provided so each community must be manually configured by the customer in order for intra-nodal ESA to function.

The high-level steps for adding a community of interest are as follows:

1) Load the MG9K, MG9KEM, and PVR with required software.

2) Launch the MG9K Element Manager.

3) Select a node to be added to community and configure PVR settings from the NE Properties screen. Repeat for each node.

4) Select Configure Internodal ESA from the Configuration Menu.

5) Set the ESA IP address of the nodes that are being placed into communities.

6) Create a new community of interest.

7) Add desired nodes to the community of interest.

8) Click Apply button.

9) Repeat for each community of interest.

When the user presses Apply a status window will display the status of NEs that are being updated. The status window will scroll as NEs are successfully updated or if there are any failures. A configuration alarm will be generated if there are any configuration failures. However, if the user exits the GUI and returns to the GUI, there is no way to determine if there were any previous failures, but the alarm will continue to be displayed in the alarm manager until the configuration is successful. If there is a failure, the user can trigger an audit to re-configure the COI or the user can press the Apply button on the GUI. The Apply button will cause the currently selected COI data to be sent to all affected nodes.

25.14 Element Management

25.14.1 New/modified GUIs

Table 6 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
GW Termination Config Panel	Changed
ESA Config Panel	Changed
ESA Translation List View	Changed
ESA Customer Group List View	Changed

25.14.2 GUI information

25.14.2.1 GW Termination Config Panel

25.14.2.1.1 Functional description

This GUI is being enhanced to display the Line Precedence and Pre-Emptable for the selected Termination. These fields will only be displayed for MLPP, Autovon, switches. The two fields are not to be shown or discussed in the customer documentation due to them being government sensitive.

25.14.2.1.2 GUI usage and implications

This is an existing GUI and there are no changes to the order that the GUIs must be datafilled. The fields added are for display only.

25.14.2.1.3 GUI size

N/A

25.14.2.1.4 GUI fields

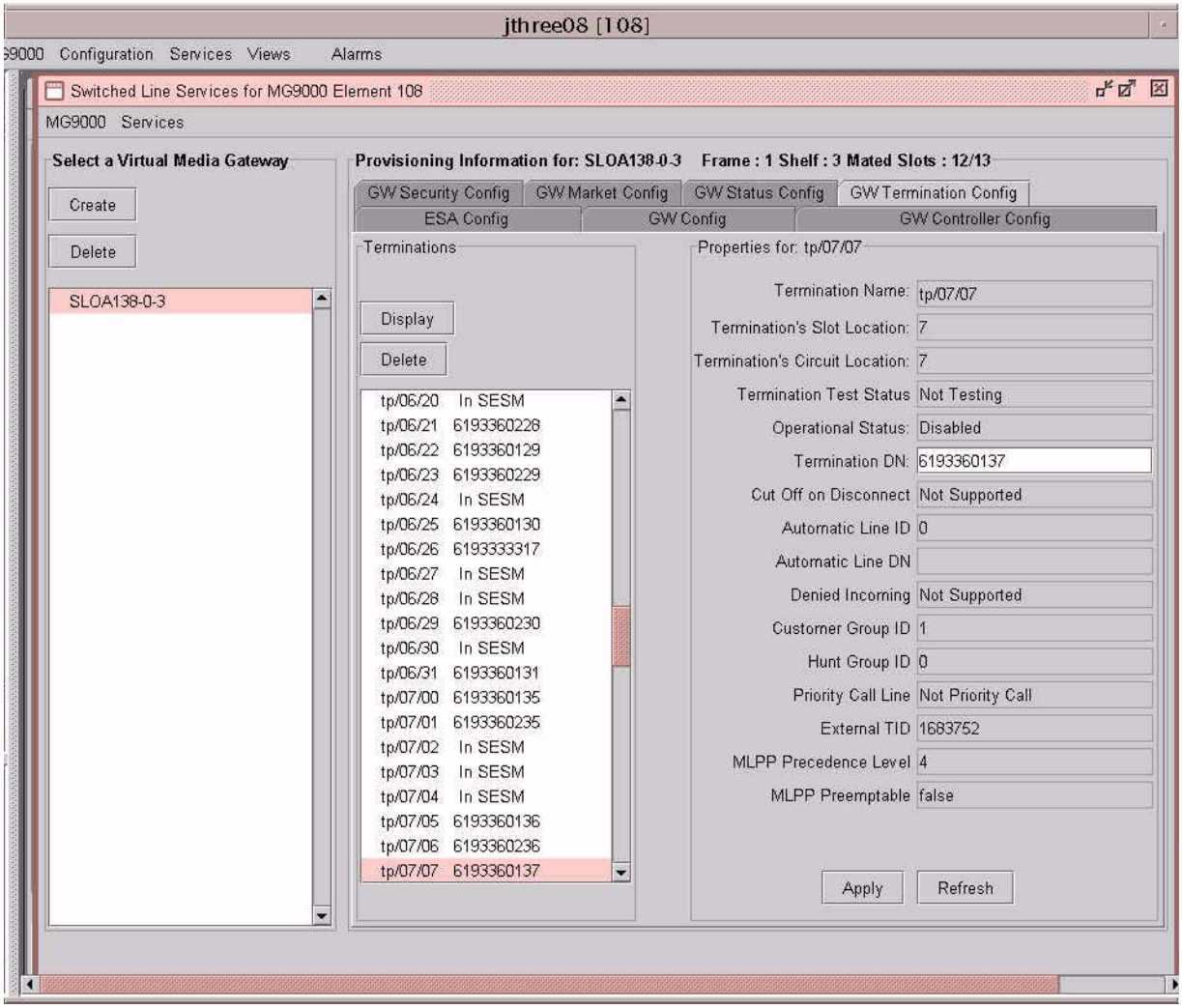
The following table lists the new fields for the GW Termination Config Panel

Table 7 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Pre-Emptable	New	N/A	Read only	Indicates if the termination is pre-emptable.	nnEsaLinesPreEmptable
Precedence Level	New	N/A	Read only	Shows the terminations Precedence Level: FlashOverride = 0 Flash = 1 Immediate = 2 Priority = 3 Routine = 4	nnEsaLinesPrecedenceLevel

25.14.2.1.5 Usage example

The following is an example of the new GW Termination Config Panel:



25.14.2.1.6 GUI release history update

The following new fields were added:

- Precedence Level
- Pre-emptable

25.14.2.1.7 Supplementary information

None

25.14.2.1.8 CLUI Interface

N/A

25.14.2.2 ESA Config Panel

25.14.2.2.1 Functional description

This GUI is being enhanced to remove the reference to the North American market for the “Enhanced” ESA Mode selector. Prior to SN09 Enhanced ESA was only available for the North American Market.

25.14.2.2.2 GUI usage and implications

This is an existing GUI and there are no changes to the order that the GUIs must be datafilled.

25.14.2.2.3 GUI size

N/A

25.14.2.2.4 GUI fields

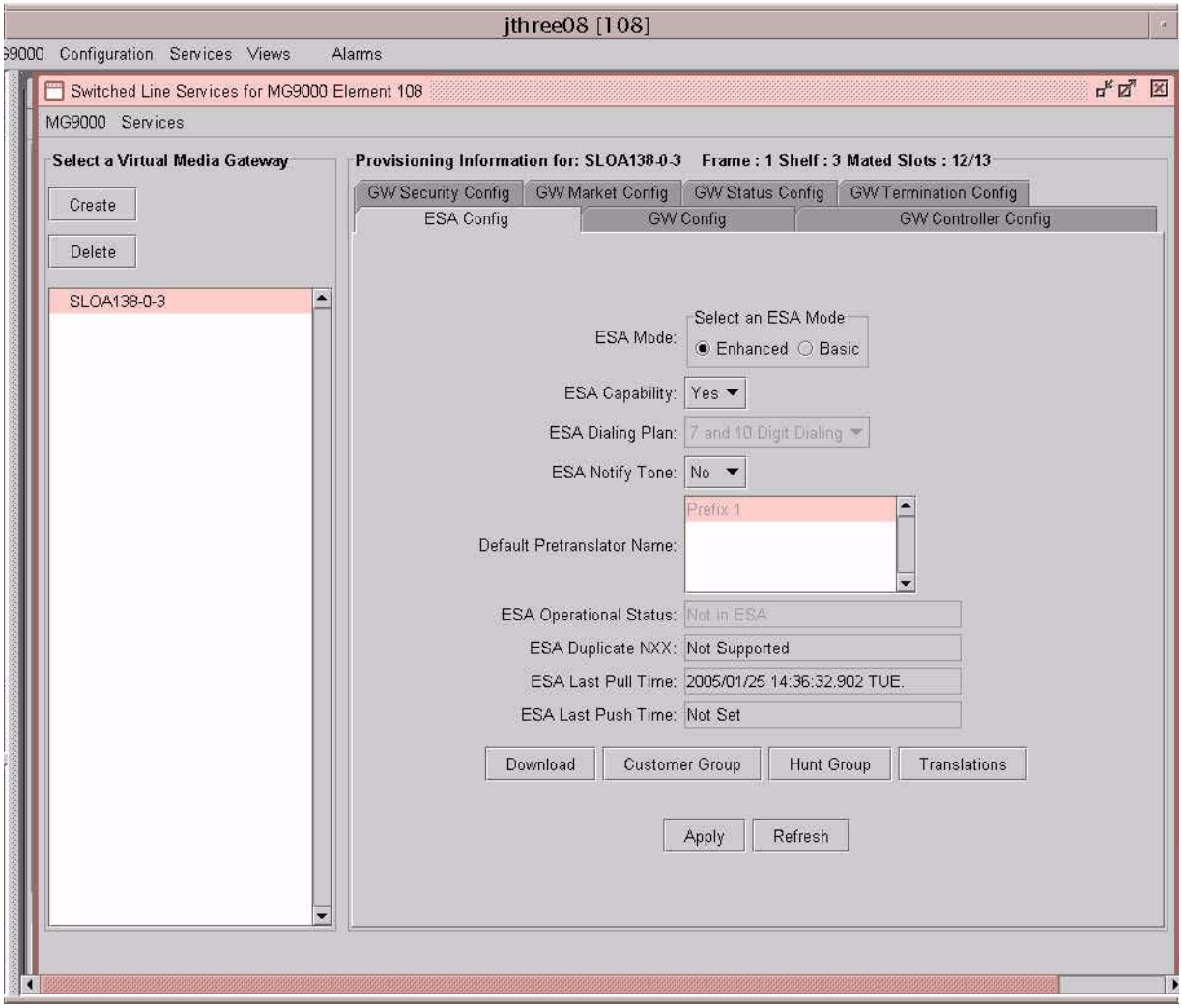
The following table lists the modified fields for the ESA Config Panel

Table 8 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
ESA Mode	Changed	N/A	“Enhanced” or “Basic”	The “Enhanced” will use the ESA data provided by the Core. This will be used by both ABI and ITP VMGs. Enhanced ESA can now be used for both the North American and International markets. The “Basic” will work in the same manner that ESA is configured in SN06 using the MG9000 EM for ITP VMGs but will not be supported for ABI VMGs.	None

25.14.2.2.5 Usage example

The following is an example of the new ESA Config Panel:



25.14.2.2.6 GUI release history update

The following fields were modified:

- ESA Mode entry labels

25.14.2.2.7 Supplementary information

None

25.14.2.2.8 CLUI Interface

N/A

25.14.2.3 ESA Translation List View

25.14.2.3.1 Functional description

This GUI is being enhanced to now indicate the source of the CORE translator that the translation entry came from. Also if the translation entry is of the type DGCOD then the existing Digits field will be split in the middle to separate the To and From digits.

25.14.2.3.2 GUI usage and implications

This is an existing GUI and there are no changes to the order that the GUIs must be datafilled. The fields added are for display only.

25.14.2.3.3 GUI size

N/A

25.14.2.3.4 GUI fields

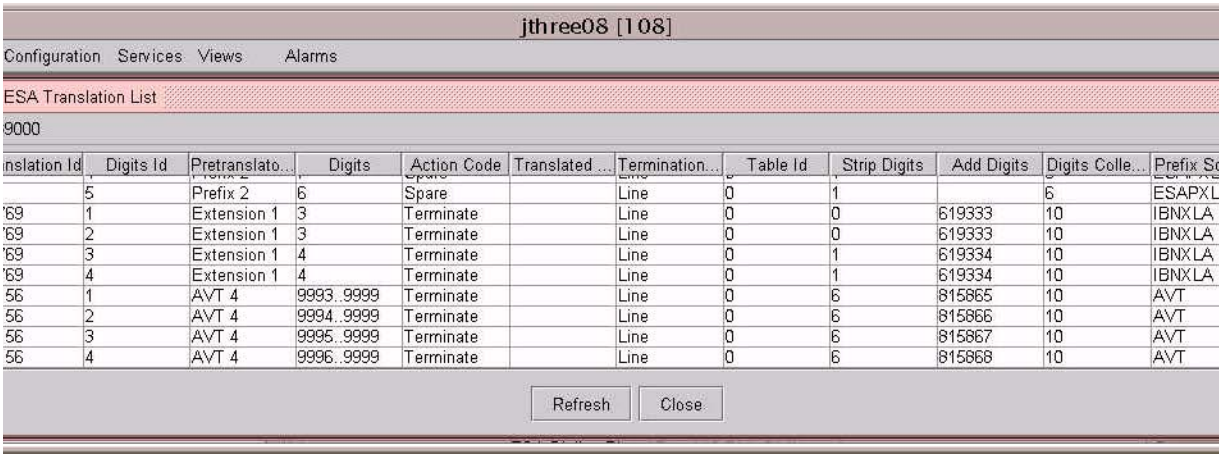
The following table lists the modified fields for the ESA Translation List View

Table 9 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Source	New	N/A	ESAPLXA IBNXLA, ESADGC OD and AVT	Indicates which CORE translator the entry came from.	None
Digits	Changed	N/A	TO..From	For ESADGCOD and AVT translation entries this field will display the To and From digits in the 111..222 format.	nnESAPrefixDigits

25.14.2.3.5 Usage example

The following is an example of the new ESA Translation List View:



25.14.2.3.6 GUI release history update

The following fields were added:

- Source

The following fields were modified:

- Digits

25.14.2.3.7 Supplementary information

None

25.14.2.3.8 CLUI Interface

N/A

25.14.2.4 ESA Customer Group List View

25.14.2.4.1 Functional description

This GUI is being enhanced indicate whether the Extension IDs are actually indexes into the EXTN table or the DGCOD table. This will be performed by modifying the existing “Extension ID” column name to “DGCOD ID” when the indexes are for DGCOD.

This GUI is also being enhanced to display the AVT ID for a customer group. This AVT ID will be displayed in a new column labeled AVT ID.

25.14.2.4.2 GUI usage and implications

This is an existing GUI and there are no changes to the order that the GUIs must be datafilled. The fields added are for display only.

25.14.2.4.3 GUI size

N/A

25.14.2.4.4 GUI fields

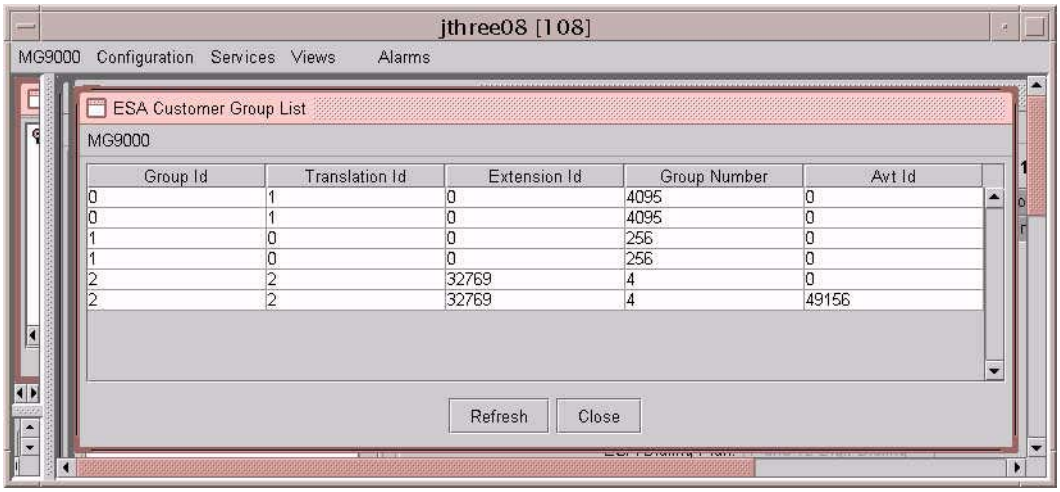
The following table lists the modified fields for the ESA Translation List View

Table 10 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
AVT ID	New	N/A	read only	The customer groups AVT index.	

25.14.2.4.5 Usage example

The following is an example of the new ESA Translation List View:



25.14.2.4.6 GUI release history update

The Extension ID column name will now read DGCOD ID whenever the indexes are for a DGCOD table, international.

For MLPP switches there will be a new column, AVT ID, that will include the customer groups AVT ID.

25.14.2.4.7 Supplementary information

None

25.14.2.4.8 CLUI Interface

N/A

25.15 Command interface changes

N/A

25.16 Security

N/A

25.17 Configuration Walkthrough

N/A

26: Configuration (CN): A00009339

26.1 Feature Name

Packet Cable T.38 Support

26.2 Hardware and Software Requirements

26.3 Initial Configuration

26.4 Office/Subnet parameters (OP/SP) (CM & SESM)

26.5 Upgrade Considerations

26.6 Data schema (DS) (CM, MIBS, RDB)

26.7 Service Orders (SO) (CM & SESM)

26.8 Software optionality control (SOC)

26.9 Element Management

26.9.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
DQoS Configuration on SESM	CHANGED

26.9.2 GUI information

26.9.2.1 GUI name: DSCP of DQoS Configuration

26.9.2.1.1 Functional description

This capability changes the DSfield on DQoS Configuration to DSCP (6-bit binary) and makes it provisionable via “Change DQoS Configuration” GUI.

26.9.2.1.2 GUI usage and implications

A pulldown menu of predefined values (IP Class of Service) for DSCP is provided. User could also provision her own DSCP value that is not in the pulldown menu by keying in a 6-bit binary stream.

26.9.2.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
DSCP	1	30	15kb per GUI

26.9.2.1.4 GUI fields

The following table lists fields for GUI or pull down menu of DSCP.

Table 3 IP Service Class names on DSCP pulldown menu

Field	New or Changed	Entry	Explanation and action	Associated MIB entry
EF	New	101 110	Expedited Forwarding	None
CS0 and DE	New	000 000	Best Effort (Default)	None
CS1	New	001 000	Class of Service 1	None
AF11	New	001 010	Assured Forwarding 11	None
AF12	New	001 100	Assured Forwarding 12	None
AF13	New	001 100	Assured Forwarding 13	None
CS2	New	001 000	Class of Service 2	None
AF21	New	010 010	Assured Forwarding 21	None
AF22	New	010 100	Assured Forwarding 22	None
AF23	New	010 110	Assured Forwarding 23	None
CS3	New	011 000	Class of Service 3	None
AF31	New	011 010	Assured Forwarding 31	None
AF32	New	011 100	Assured Forwarding 32	None
AF33	New	011 110	Assured Forwarding 33	None
CS4	New	100 000	Class of Service 4	None
AF41	New	100 010	Assured Forwarding 41	None
FA42	New	100 100	Assured Forwarding 42	None
FA43	New	100 110	Assured Forwarding 43	None
CS5	New	101 000	Class of Service 5	None

Table 3 IP Service Class names on DSCP pulldown menu

Field	New or Changed	Entry	Explanation and action	Associated MIB entry
CS6	New	110 000	Class of Service 6	None
CS7	New	111 000	Class of Service 7	None

26.9.2.1.5 Usage example

The following example shows sample datafill or menu selection for GUI <abbreviated name of GUI>:

26.9.2.1.6 GUI release history update

26.9.2.1.7 Context sensitive launching information

26.9.2.1.8 Supplementary information

26.9.3 CLUI Interface

26.10 User interface changes

26.11 OSSGate Interface Changes

26.12 Security

26.13 Configuration Walkthrough

27: Configuration (CN): A00009375 & A00009376

27.1 Feature Name

CICM Third-party Corrective Content Patching & CICM Selective Binary Component Patching

27.2 Data schema (DS)/ MIBs

This feature will utilise two areas of the Windows Registry for the storage of information relating to status of installed patches and maintenance releases on this node.

Table 2: MIB entries

MIB name (registry key etc)	Description (including backwards compatibility)
hklm\system\currentcontrolset\services\cxipboot\data\patches	Storage area for patch information
hklm\system\currentcontrolset\services\cxipboot\data\upgrade	Storage area for maintenance release information

27.3 Operating system parameters (OP)

No Operating System Parameters will be changed by this feature, unless of course by the deployment of an OS patch. In which case details of the Operating System Parameters changed will be in the Release Notes of the patch concerned.

27.4 Alarms (AL)

No new alarms will be raised as part of this feature.

27.5 New/modified filesystem directories (FS)

Several new directories will be required for this feature.

Table 5: directories

Directory name	Location	Function
D:\CentrexIP\support\patches	CICM-EM	Location for patch files to be written ready for installation
D:\CentrexIP\support\upgrades	CICM-EM	Location for Maintenance Release files to be written ready for installation
C:\cxipinstall\???????	Node being Patched	Temporary area for unpacking patch and maintenance release data ready for installation

2.5 Command interface (CI)

A Command Line Interface will be provided for use by GNPS to assist in the removal of partially applied patches. However this interface will not be available for use by customers and as such the details of its functionality are beyond the scope of this document.

2.6 Software optionality control (SOC)

This feature is available on all CICM and CICM-EM platforms running SN09 or later.

2.7 Licensing

This feature will utilise MD5 checksums, which require no licensing. No other Third Party licensed software was used in the development of this feature.

2.8 References

A00005987 CxipRestore Tool

28: Configuration (CN): A00009463

28.1 Feature Name

CBM to Support Centralized User Authentication with IEMS

28.2 Hardware and Software Requirements

SN09 CBM standard hardware and software are required.

No new hardware is needed for this feature. However, the software for this feature needs to be installed on the CBM before feature configuration can take place.
For CBM deployment with IEMS centralized security server, IEMS and its hardware and software dependencies need to be available and configured.

28.3 Initial Configuration

- No initial hardware configuration is required for this feature.
- The initial software configuration for this feature is using local security server (i.e. native Solaris security system) for authentication and authorization. No user input is needed for initialization.

28.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable to this feature.

28.5 Upgrade Considerations

28.5.1 Dump and Restore (CM)

Not applicable to this feature.

28.5.2 Element Management Upgrade

No impact to Element Management Upgrade when a CBM is deployed without external security server.

When a CBM is deployed with IEMS centralized security server in SN09, the CBM is changed from using Pre-SN09 local security system to external security server. Both CBM and IEMS server must be upgraded to the same release before CBM can be configured to use IEMS.

In order to migrate to central authentication and authorization, some of the existing local user accounts need to be created on the external security server - IEMS. CBM local user migration can only take place after CBM is changed to IEMS external server configuration.

28.5.3 Downgrade impact

No impact to downgrade if the CBM feature installation is aborted.

28.6 Data schema (DS) (CM, MIBS, RDB)

Not applicable to this feature.

28.7 Service Orders (SO) (CM & SESM)

Not applicable to this feature.

28.8 Software optionality control (SOC)

Not applicable to this feature.

28.9 Element Management

28.9.1 New/modified GUIs

N/A

28.9.2 GUI information

N/A

28.9.3 CLUI Interface

28.9.3.1 Configuring Central security server and SAML on CBM

The SSPFS Command Line Interface (CLI) tool is proposed to be used to configure the CBM with the Central security server (IEMS including SAML). The following are the user interface and options that are available and can be used to do this:

```
wcary03v-unit0(active):/> cli
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select - 2



Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
```

```
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit

select - 13



Security Services Configuration
 1 - Socks Configuration
 2 - IEMS Server Location Configuration
 3 - PAM Configuration

 X - exit

select - 2



IEMS Server Location Configuration
 1 - iems_ip (Configure IEMS Server IP)

 X - exit

select - 1

=== Executing "iems_ip"


Enter IEMS Server IP Address (default: 0.0.0.0):
Enter IEMS Fully Qualified Domain Name(default: no_default):

IEMS IP:         0.0.0.0
IEMS Fully Qualified Domain Name:        no_default

Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
quit

=== "iems_ip" completed successfully
```

```
IEMS Server Location Configuration
 1 - iems_ip (Configure IEMS Server IP)

 X - exit

select - x



Security Services Configuration
 1 - Socks Configuration
 2 - IEMS Server Location Configuration
 3 - PAM Configuration

 X - exit

select - 3



PAM Configuration
 1 - Central Security Client Configuration

 X - exit

select - 1



Central Security Client Configuration
 1 - pam_orig (Use Default PAM Configuration)
 2 - pam_radius (Use Security Server)

 X - exit

select - 1

=== Executing "pam_orig"

pkgparam: ERROR: unable to locate parameter information for "NNswmgmt"
pkgparam: ERROR: unable to locate parameter information for "NNpamradclt"
pkgparam: ERROR: unable to locate parameter information for "NNnsssaml"
ERROR: NNswmgmt package not found

=== 255 was the return code for "pam_orig"



Central Security Client Configuration
```

```
 1 - pam_orig (Use Default PAM Configuration)
 2 - pam_radius (Use Security Server)

 X - exit

select - 2

=== Executing "pam_radius"

pkgparam: ERROR: unable to locate parameter information for "NNswmgmt"
pkgparam: ERROR: unable to locate parameter information for "NNpamradclt"
pkgparam: ERROR: unable to locate parameter information for "NNnsssaml"
ERROR: NNswmgmt package not found

=== 255 was the return code for "pam_radius"



Central Security Client Configuration
 1 - pam_orig (Use Default PAM Configuration)
 2 - pam_radius (Use Security Server)

 X - exit

select - x



PAM Configuration
 1 - Central Security Client Configuration

 X - exit

select - x



Security Services Configuration
 1 - Socks Configuration
 2 - IEMS Server Location Configuration
 3 - PAM Configuration

 X - exit

select - x



Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
```

```
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

 X - exit

select - x



Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select - x
wcary03v-unit0(active):/>
```

Note1: The error messages for 2 of the options that are shown in the above snap-shot, are due to the missing packages for the CBM profiles.

Note2: Pending the results of the negotiation with the SSPFS and CBM architects/designers, there may be a need for additional options for the CLI tool, under the "Security Services Configuration" selections.

28.10 User interface changes

N/A

28.11 OSSGate Interface Changes

N/A

28.12 Security

28.12.1 Network configuration

28.12.2 Key management

28.12.3 Protocol

28.12.4 Authentication

28.13 Configuration Walkthrough

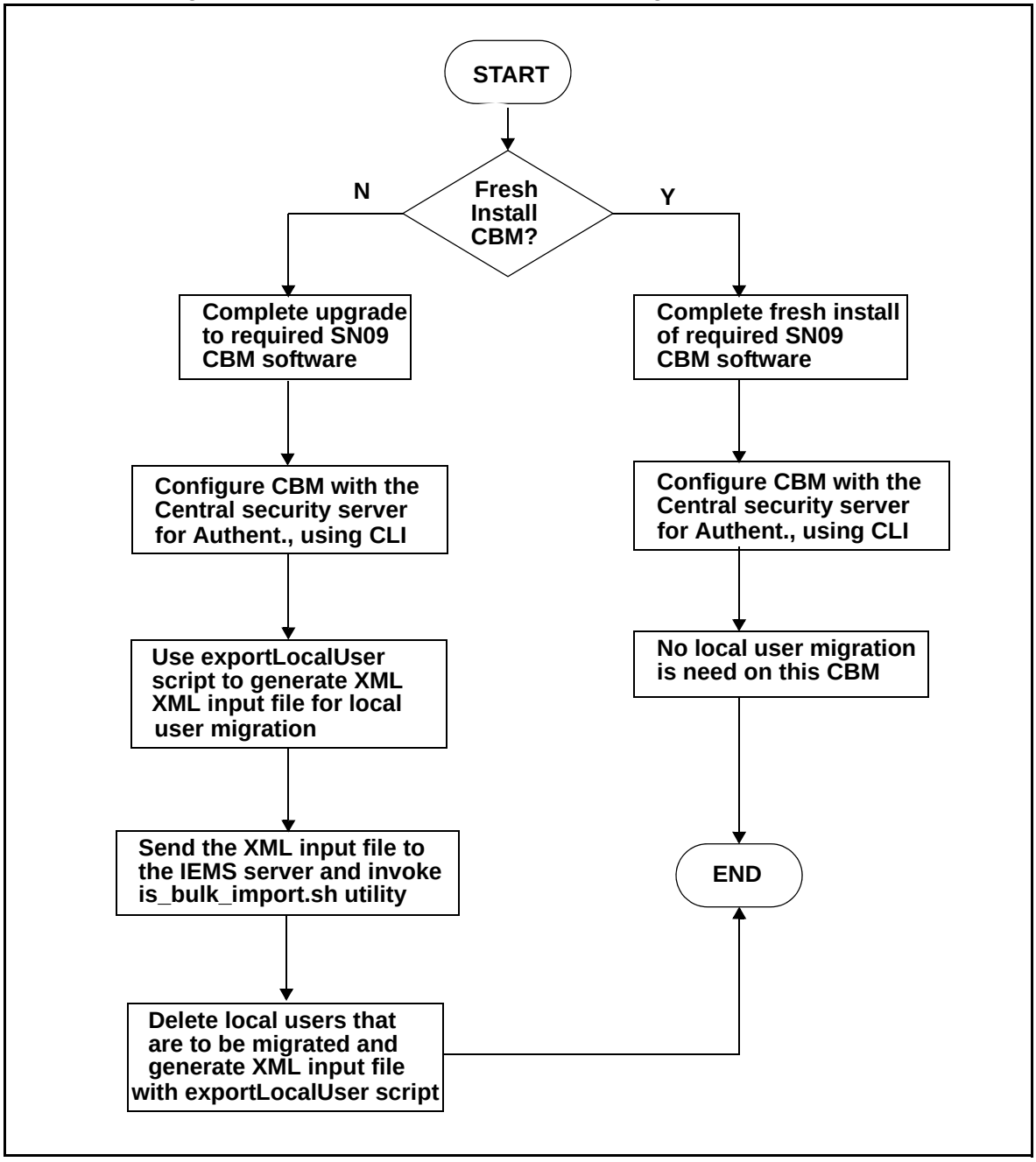
28.13.1 CBM Local User Migration to IEMS

CBM user migration to the IEMS needs to take place when the CBM settings are changed from the local security configuration (i.e. Standalone) to the IEMS central security server configuration.

A new CBM exportLocalUser script is introduced by this feature to generate the XML input file needed by the IEMS's is_bulk_import.sh utility for CBM local user migration.

The following figure shows the steps for CBM local user migration to IEMS:

Figure 1 Flow chart for CBM Local User Migration to IEMS



29: Configuration (CN): A00009470

29.1 Feature Name

SDM to support Security Assertion Markup Language (SAML) NSSwitch client

29.2 Hardware and Software Requirements

SDM standard hardware and software are required.

No new hardware is needed for this feature. However, the software for this feature needs to be installed on an SDM before feature configuration can take place.

For SDM deployment with IEMS centralized security server, IEMS and its hardware and software dependencies need to be available and configured.

29.3 Initial Configuration

- No hardware initial configuration for this feature.
- The initial software configuration for this feature is using local security server (i.e. native AIX security system) for authentication and authorization. No user input is needed for initialization.

29.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable to this feature.

29.5 Upgrade Considerations

29.5.1 Dump and Restore (CM)

Not applicable to this feature.

29.5.2 Element Management Upgrade

No impact to Element Management Upgrade when an SDM is deployed without external security server.

IEMS central server must be upgraded to the same release as SDM before an SDM can be configured to use IEMS as the centralized security server.

Local user migration from SDM to IEMS should not take place during upgrade. It should take place after SDM and IEMS are upgraded to the same software release.

29.5.3 Downgrade impact

No impact to downgrade if the SDM feature installation is aborted.

29.6 Data schema (DS) (CM, MIBS, RDB)

Not applicable to this feature.

29.7 Service Orders (SO) (CM & SESM)

Not applicable to this feature.

29.8 Software optionality control (SOC)

Not applicable to this feature.

29.9 Element Management

29.9.1 CLUI Interface

29.9.1.1 sdmmtc SecuConf

In order to configure SAML client on SDM, SecuConf menu under sdmmtc will be enhanced for SAML client configuration.

The following is the proposed SecuConf screens for selecting SAML for naming service.

```
   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb      .     SysB    .     ISTb    .     Host: wcary2p7
    M              M                            Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: LOCAL
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
 8          4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15
16
17 Help
18 Refresh
 jjsecu1
Time  15:30  >
```

```
   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb      .     SysB    .     ISTb    .     Host: wcary2p7
    M              M                            Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: LOCAL
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
 8          4 Remote Audit Log Destination: -
```

```
 9
10
11
12
13
14
15
16
17 Help
18 Refresh
 jjsecu1
Time  15:31  >change 1


   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
    M                 M                            Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: LOCAL
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
 8          4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15          Change Authentication Naming Service
16          Please choose one of the following available option(s) on the
17 Help      system. More option(s) will be available if the corresponding
18 Refresh   fileset(s) is(are) applied. (1) SAML (2) LOCAL :
 jjsecu1
Time  15:38  >1


   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
    M                 M                            Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: LOCAL
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
 8          4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15
16          Change Authentication Naming Service - SAML
17 Help
18 Refresh   Enter the IP Address of the SAML Server:
 jjsecu1
Time  15:40  >47.1.2.3


   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
```

```
   M              M                          Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: LOCAL
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
 8          4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15
16          Change Authentication Naming Service - SAML
17 Help
18 Refresh   Enter the Fully Qualified Domain Name of the SAML Server:
 jjsecu1
Time  15:43  >iems-server1.nortel.com


   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
    M              M                          Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: LOCAL
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
 8          4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15
16          Change Authentication Naming Service - SAML
17 Help
18 Refresh   Enter the system account password of the SAML Server:
 jjsecu1
Time  15:45  >****[1]


   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
    M              M                          Fault Tolerant
SecuConf
 0 Quit
 2
 3
 4
 5
 6
 7
 8
 9
10
```

[1]Stars may not be shown in future releases.

```
11          Change Authentication Naming Service - SAML
12
13          The SAML Server to be configured:
14             IP address: 47.1.2.3
15             Fully Qualified Domain name: iems-server1.nortel.com
16
17 Help     Do you wish to proceed?
18 Refresh  Please confirm ("YES", "Y", "NO", or "N")
 jjsecu1
Time  15:47  >y


   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
    M                 M                            Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: SAML
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
 8          4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15
16
17 Help
18 Refresh   Change 2 - Command complete.
 jjsecu1
Time  15:48  >
```

The same configuration steps should be used when any of the SAML client configuration values (IP Address, Fully Qualified Domain Name or System account password) need to be changed later.

NOTE: For network amAdmin system account password change, please refer to MFT's Security Services 1.1 Interface Definition Appendix G (IEMS amAdmin password change procedure).

http://knowledgeonline.ca.nortel.com/sws/livelink.exe/3747266/Security_Services_1.1_ID?func=doc.Fetch&nodeid=3747266

When SAML is selected for Authentication Naming Service, IEMS should be used for Authentication PAM Stack. This is the correct combination for using IEMS as the central security server on an SDM.

29.9.2 New command: deleteIEMSLocalEntry

A new command, deleteIEMSLocalEntry, is added so the administrator can clean up the /etc/passwd file after a SN08 SDM with IEMS as the central server is upgraded to SN09 SDM software. This command is not needed when an SDM with IEMS configuration is upgraded from SN09 or newer releases.

The synopsis of the command is:

```
deleteIEMSLocalEntry { "ALL" | user}
```

Where:

ALL will cause all IEMS user entries in /etc/passwd will be deleted

<user> is the UID of the IEMS user that will be deleted

29.9.2.1 Example

The following is the example command line for cleaning up /etc/passwd after an SDM with IEMS configuration is upgraded from SN08 to SN09:

```
deleteIEMSLocalEntry ALL
```

29.9.3 Deleted command: enableIEMSUser

SN08 SDM command, enableIEMSUser for allowing an IEMS user to logon to an SDM will be deleted.

29.9.4 Deleted command: disableIEMSUser

SN08 SDM command, disableIEMSUser to disallow an IEMS user to logon to an SDM will be deleted.

29.10 User interface changes

Not applicable to this feature.

29.11 OSSGate Interface Changes

Not applicable to this feature.

29.12 Security

The feature will enhance user authentication and authorization for SDM.

29.12.1 Network configuration

n/a

29.12.2 Key management

n/a

29.12.3 Protocol

n/a

29.12.4 Authentication

When a SDM is deployed without an external security server, user authentication and authorization will be performed locally on the SDM.

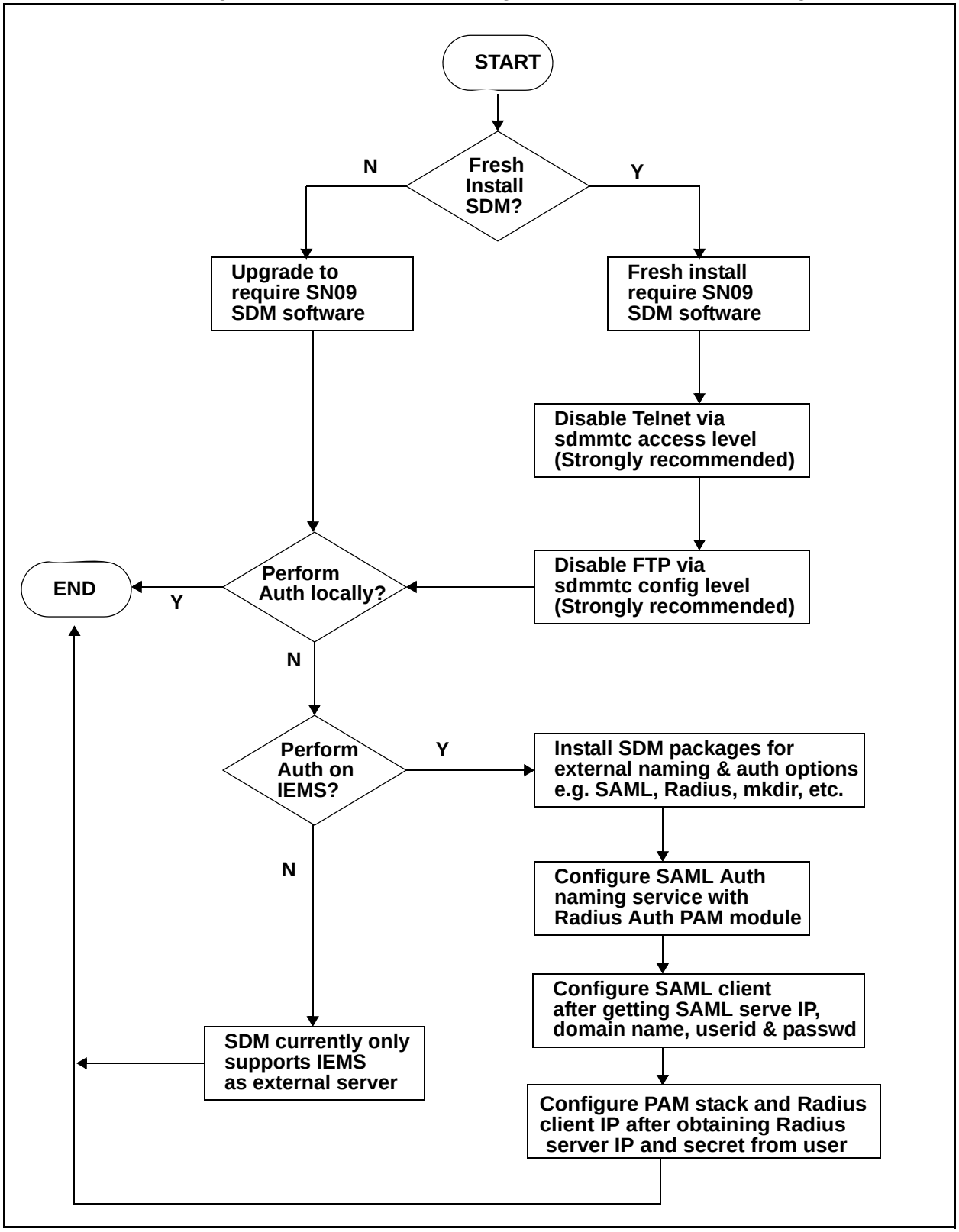
When a SDM is deployed with an external security server like IEMS, user authentication and authorization will be performed through IEMS via Radius protocol.

29.13 Configuration Walkthrough

29.13.1 Security services configuration

The following figure shows the configuration steps for this feature.

Figure 1 Flow chart for Naming Service and PAM Stack configuration



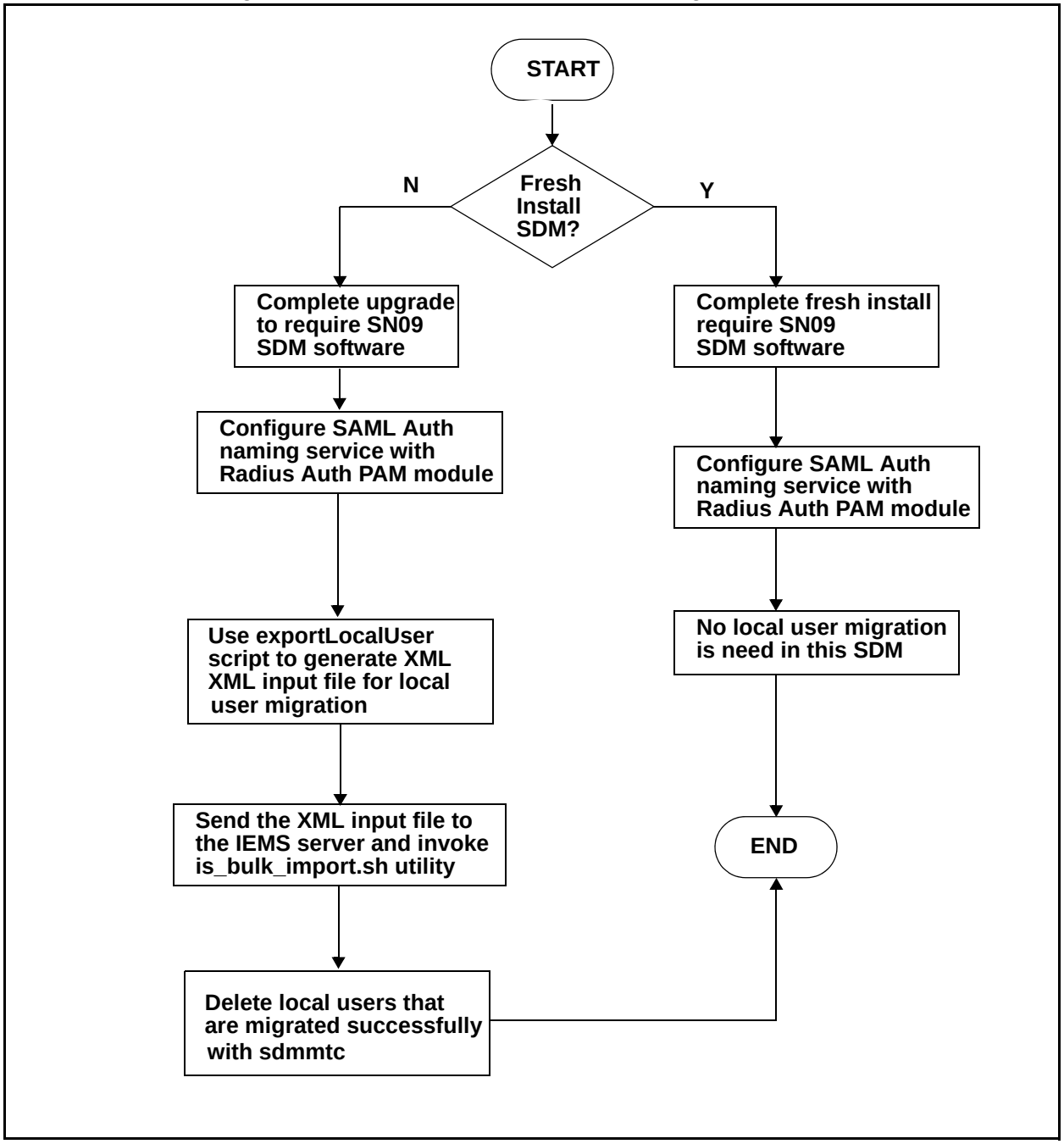
29.13.2 SDM Local User Migration to IEMS

SDM user migration to IEMS needs to take place when an SDM is changed from local security configuration to IEMS central security server configuration.

A new SDM exportLocalUser script is introduced by this feature to generate the XML input file needed by IEMS's is_bulk_import.sh utility for SDM local user migration.

The following figure shows the steps for SDM local user migration to IEMS.

Figure 2 Flow chart for SDM Local User Migration to IEMS



30: Configuration (CN): A00009520

30.1 Feature Name

Trunk blocking tools for MG4K and GWC on SN09

30.2 Hardware and Software Requirements

None

30.3 Initial Configuration

None

30.4 Office/Subnet parameters (OP/SP) (CM & SESM)

None

30.5 Upgrade Considerations

None

30.6 Data schema (DS) (CM, MIBS, RDB)

None

30.7 Service Orders (SO) (CM & SESM)

None

30.8 Software optionality control (SOC)

None

30.9 Element Management

None

30.10 User interface changes

30.10.1 Command: <POST>

30.10.1.1 Command type: <Listed MENU>

30.10.1.2 Command target: <All>

30.10.1.3 Command availability: <RES>

30.10.1.4 Command description

A new post type ‘I’ is added for command POST under MAPCI TTP level. With this post type, users can post the trunks in the existing post set by further criteria.

30.10.1.5 Command syntax

Table 1 <CommandName> command parameters and variables

Command	Parameters and variables
POST	I
Parameters and variables	**Description**
I	Post trunks in existing post set

30.10.1.6 Qualifications and warnings

None

30.10.1.7 Example

- Example 1:

>MAPCI;MTC;TRKS;TTP;POST G TRUNK_EXAMPLE

- Enters the TTP MAP level and create post set for all trunks in group TRUNK_EXAMPLE.

>**POST I D GWC 32**

- Post all trunks that are on GWC 32 in the existing post set(it contains all trunks in group TRUNK_EXAMPLE).

Using the above 2 commands, user gets all the trunks which are in group TRUNK_EXAMPLE and on GWC 32.

- Example 2:

>MAPCI;MTC;TRKS;TTP;POST D GWC 32

- Enters the TTP MAP level and create post set for all trunks on GWC 32.

>**POST I G TRUNK_EXAMPLE**

- Post all trunks that whose CLLI is trunk_example in the existing post set(it contains all trunks GWC 32).

Using the above 2 commands, user gets all the trunks which are in group TRUNK_EXAMPLE and on GWC 32.

30.11 OSSGate Interface Changes

None

30.12 Security

None

30.13 Configuration Walkthrough

None

31: Configuration (CN): A00009532

31.1 Feature Name

Support host to host tunnels for all northbound OSS connections

31.2 Hardware and Software Requirements

SN09 or later software load for the SSPFS server (such as Integrated Element Manager System (IEMS)).

31.3 Initial Configuration

31.3.1 Security

From a high-level here are the steps to enable security for a northbound OSS.

1. Load SSPFS server (such as IEMS) with required SN09 or later software load.
2. Enable security on the OSS to secure the connection to the SSPFS server. Details of this step are beyond the scope of this document as each OSS provisioning mechanism is different.
3. The craftsperson will then use a web browser and connect to the SSPFS server machine's Server Security Manager (SSM). This is done using the item under the EMS Platforms, SSPFS menu at the top, or manually by entering the correct address information in a supported web browser. *Only users with the necessary security privileges can access to SSM . This is done using a separate Succession Login to SSM.*
4. After logging in, the craftsperson will enable security for communications with the OSS IP address.
5. This will complete securing the OSS link.

31.3.1.1 OSS

Details of OSS operation are beyond the scope of this document as each OSS provisioning mechanism is different.

IPSec and IKE configuration parameters that are provisioned on the OSS must match the corresponding IPSec and IKE parameters on the IEMS, provisioned via the Server Security Manager.

31.3.1.2 SSPFS Server System

IPSec and IKE configuration parameters that are provisioned, via the server security manager, must match the corresponding IPSec and IKE parameters on the OSS.

31.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable

31.5 Upgrade Impact

Not applicable

31.6 Data schema (DS) (CM, MIBS, RDB)

Not applicable

31.7 OSS Changes

Not applicable

31.8 External Interface Changes

Not applicable

31.9 Integrated Element Manager System

31.9.1 Security Button

A new security item under the EMS Platforms, SSPFS menu at the top, is now available in IEMS to launch the Server Security Manager. The URL will be http://<SSPFS server ip address>/ipsec/security.html.

31.9.2 Server Security Manager

31.9.2.1 Functional description

This HTML webpage will be used to define security parameters to secure communications into and out from the SSPFS server machine. This includes IEMS to OSS communications.

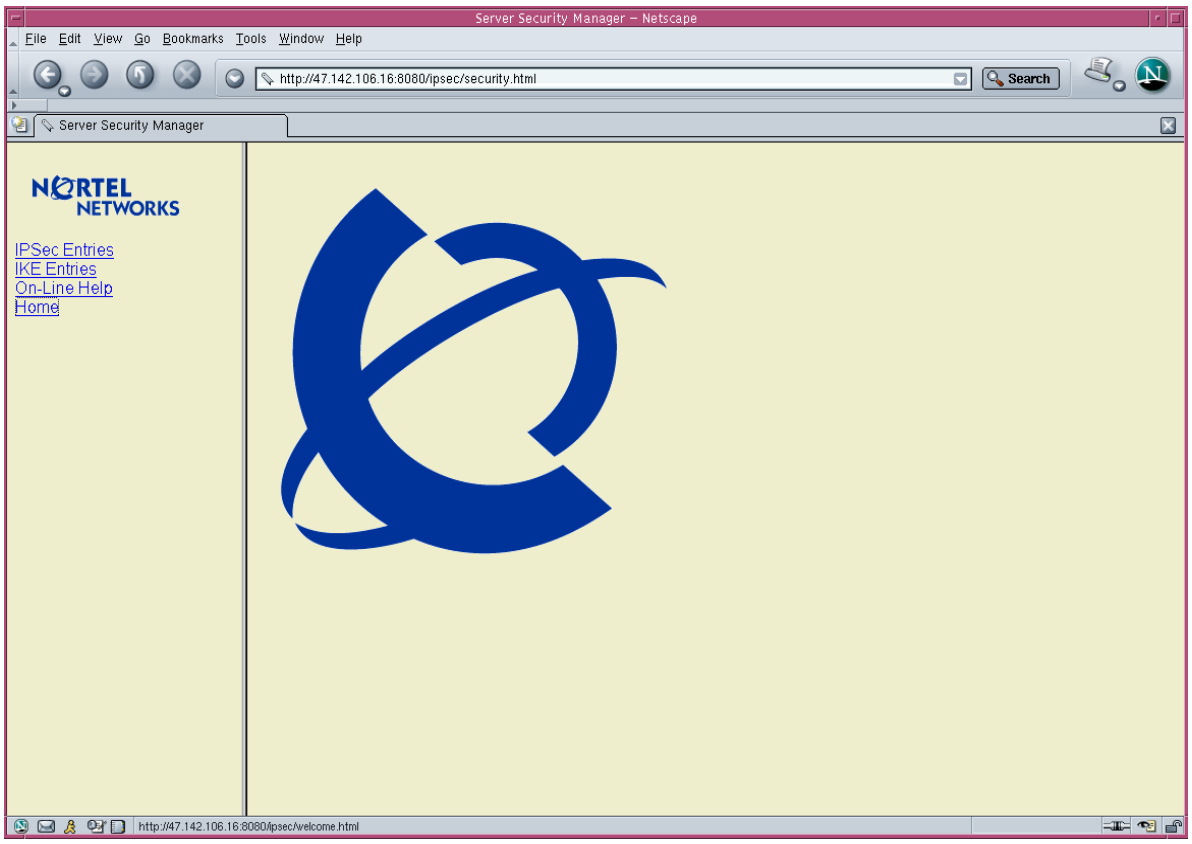
The craftsperson will be presented with two tables representing currently provisioned security parameters. One for IPSec parameters and one for IKE parameters. Options to add and delete entries are available. Adding entries will be performed using HTML forms.

The IPSec Entries page allows retrieval and manipulation of IPSec policies for a host server. Once the policies are configured, all outbound and inbound datagrams are subject to policy checks as they exit and enter the host server. If no entry is found, no policy checks will be made, and all the traffic will pass through unimpeded. Depending upon the match of the policy entry, a specific action will be taken.

The IKE Entries page allows retrieval and manipulation of Internet Key Exchange policies for a host server. Once a policy is configured, the IKE daemon running on the IEMS server can negotiate with a remote host to establish the actual IPSec keys used to secure messages between IEMS and the OSS host.

Note: Only users with the necessary security privileges can access SSM. This is done using a separate Succession Login to SSM.

The following is the first page presented to the craftsperson upon opening the Server Security Manager:



Navigation is performed using the links on the left frame. User input is performed or operation output is displayed in the right frame.

31.9.2.2 GUI usage and implications

Primary usage of this interface in SN09 is to secure the communications channel between SSPFS server application such as IEMS and an OSS.

First, IPSec entries are created using the desired parameters. If the craftsperson has chosen to use the “IPSec” action, the second step is to create a corresponding IKE entry using the desired parameters.

Note: This interface provides for securing all network communications and not just OSS communications. Care must be taken when provisioning or deleting the security parameters, so as not to effect other essential communications, such as telnet, ftp, etc.

31.9.2.3 IPSec fields

The following table lists the security fields for IPSec parameters.

Table 1 IPSec field descriptions

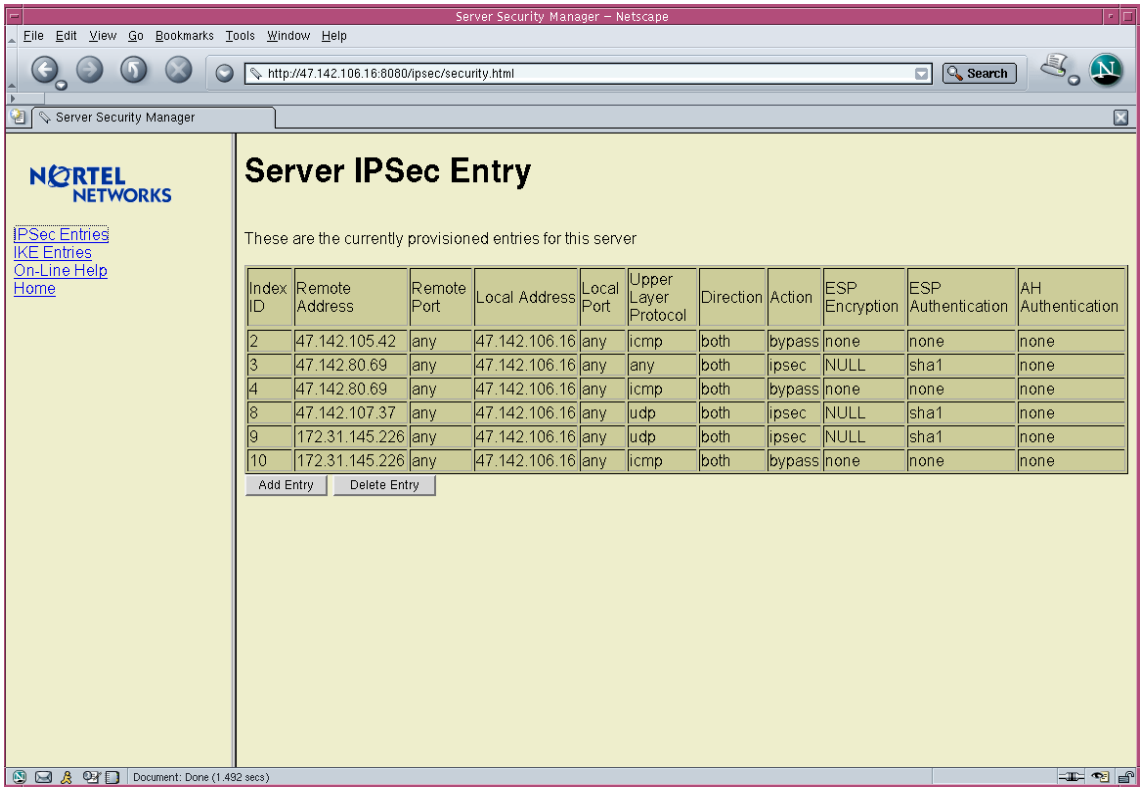
Field	New or Changed	Subfield	Entry	Explanation and action
Index ID	New	No	Integer	Internal index used by the server to track and reference IPSec entries.
Remote Address	New	No	A numeric internet IP address of the form: www.xxx.yyy.zzz	Remote Address means the source address on incoming packets and destination address on outgoing packets.
Remote Port	New	No	1 - 65535, any	IP port of the remote system communicating with this server.
Local Address	New	No	A numeric internet IP address of the form: www.xxx.yyy.zzz	Local Address means the destination address on incoming packets and source address on outgoing packets.
Local Port	New	No	1 - 65535, any	IP port of this server.
Upper Layer Protocol	New	No	any, icmp, tcp, and udp.	Determines which protocol traffic this entry is matched against.
Direction	New	No	in, out, and both.	Determines whether this entry is for inbound or outbound traffic.
Action	New	No	bypass, drop, and ipsec.	Determines the action to take when the traffic pattern is matched.

Table 1 IPSec field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action
ESP Encryption	New	No	none, any, NULL, des, 3des.	Describes the encryption algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to “ipsec”.
ESP Authentication	New	No	none, any, sha1, and md5.	Describes the authentication algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to “ipsec”.
AH Authentication	New	No	none, any, sha1, and md5.	Describes the encryption algorithm that will be used to apply the IPSec AH header on outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to “ipsec”.

31.9.2.4 IPSec provisioned entries example

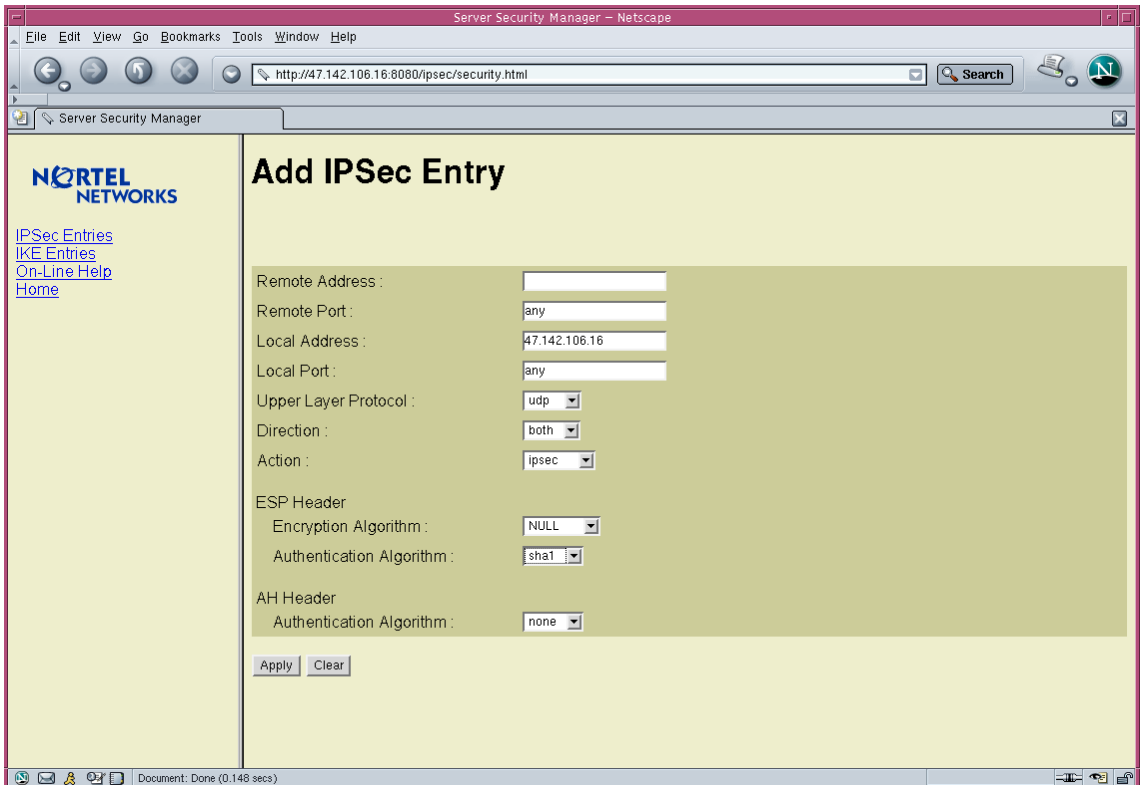
The following example shows a number of IPSec entries for an IEMS server:



Index ID	Remote Address	Remote Port	Local Address	Local Port	Upper Layer Protocol	Direction	Action	ESP Encryption	ESP Authentication	AH Authentication
2	47.142.105.42	any	47.142.106.16	any	icmp	both	bypass	none	none	none
3	47.142.80.69	any	47.142.106.16	any	any	both	ipsec	NULL	sha1	none
4	47.142.80.69	any	47.142.106.16	any	icmp	both	bypass	none	none	none
8	47.142.107.37	any	47.142.106.16	any	udp	both	ipsec	NULL	sha1	none
9	172.31.145.226	any	47.142.106.16	any	udp	both	ipsec	NULL	sha1	none
10	172.31.145.226	any	47.142.106.16	any	icmp	both	bypass	none	none	none

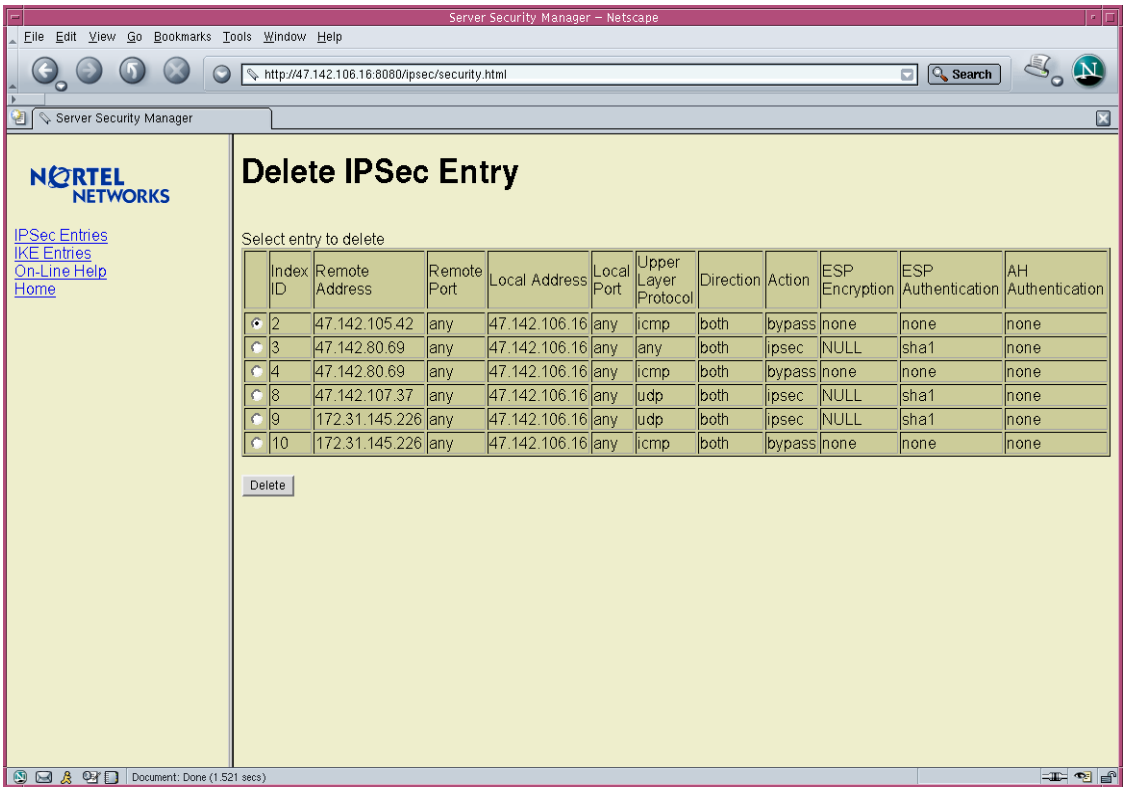
31.9.2.5 IPSec entry form example

The following example shows a form for creating IPSec entries for an IEMS server:



31.9.2.6 IPSec entry deletion example

The following example shows a table for deleting IPSec entries for an IEMS server:



31.9.2.7 Recommended Parameter settings

******This section will need to be verified.******

The following are the recommended parameters to be used when connecting to an OSS

1. Remote Address is the address of the OSS as seen by SSPFS server application, such as IEMS.
2. Remote Port is “any”.
3. Local Address is the address of the SSPFS server as seen by the OSS.
4. Local Port is “any”.
5. Upper Layer Protocol is “any”.
6. Direction is “both”.
7. Action is “ipsec”.
8. ESP Encryption Algorithm is “3des”. (if encryption of data is required)

9 ESP Authentication Algorithm is “sha1”.

10 AH Authentication Algorithm is “none”.

31.9.2.8 IKE fields

The following table lists the security fields for IKE parameters.

Table 2 IKE field descriptions

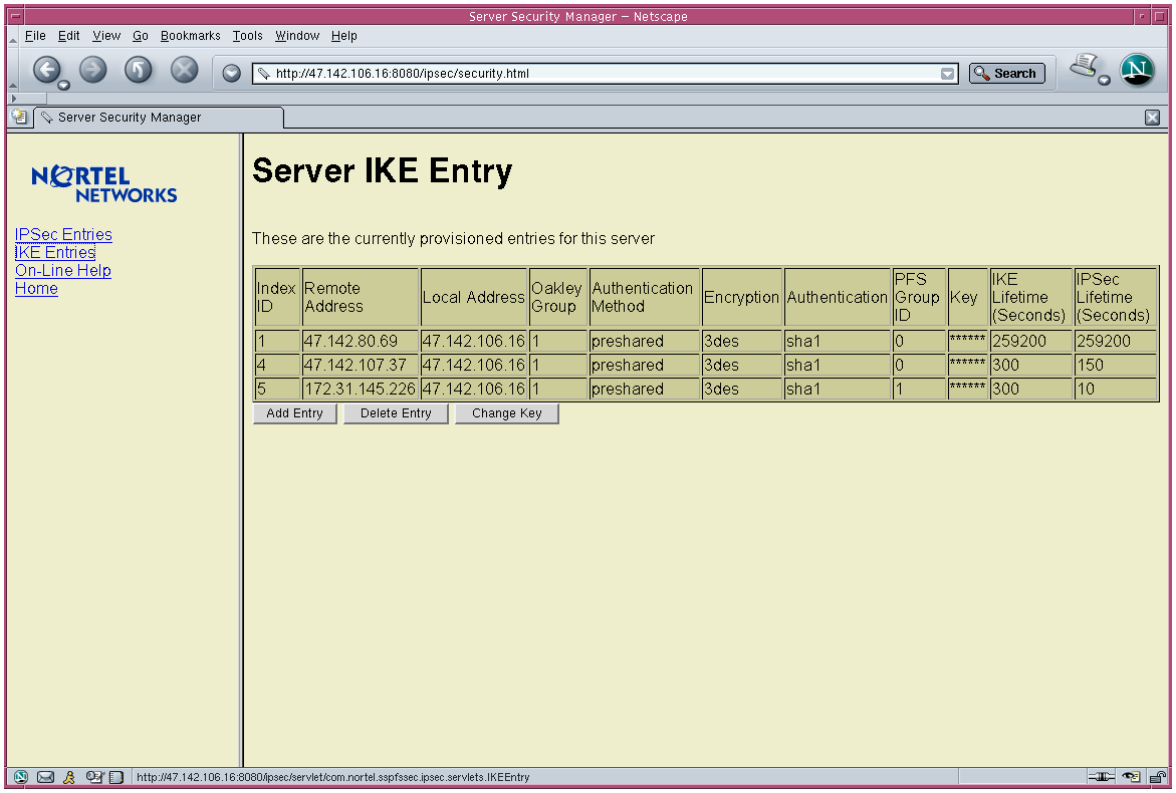
Field	New or Changed	Subfield	Entry	Explanation and action
Index ID	New	No	Integer	Internal index used by the server to track and reference IKE entries.
Remote Address	New	No	A numeric internet IP address of the form: www.xxx.yyy.zzz	IP address of the remote system communicating with this server.
Local Address	New	No	A numeric internet IP address of the form: www.xxx.yyy.zzz	IP address of this server.
Oakley Group	New	No	1 (768-bit), 2 (1024-bit), or 5 (1536-bit).	The Oakley Diffie-Hellman group used for IKE Security Association key derivation.
Authentication Method	New	No	Preshared is the only supported option.	The authentication method used for IKE phase 1.
Encryption	New	No	des and 3des	Specifies the encryption algorithm for a Security Association.
Authentication	New	No	sha1 and md5.	Specifies the authentication algorithm for a Security Association.
PFS Group ID	New	No	0 (do not use Perfect Forward Secrecy for IPsec SAs), 1 (768-bit), 2 (1024-bit), and 5 (1536-bit).	The Oakley Diffie-Hellman group used for IPsec Security Association key derivation.
Key	New	No	20 - 120 character ASCII string	Specifies the preshared key for this Security Association.

Table 2 IKE field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action
IKE Lifetime	New	No	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days.	Specifies the lifetime for a IKE phase 1 Security Association.
IPSec Lifetime	New	No	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days.	Specifies the lifetime for an IPSec Security Association.

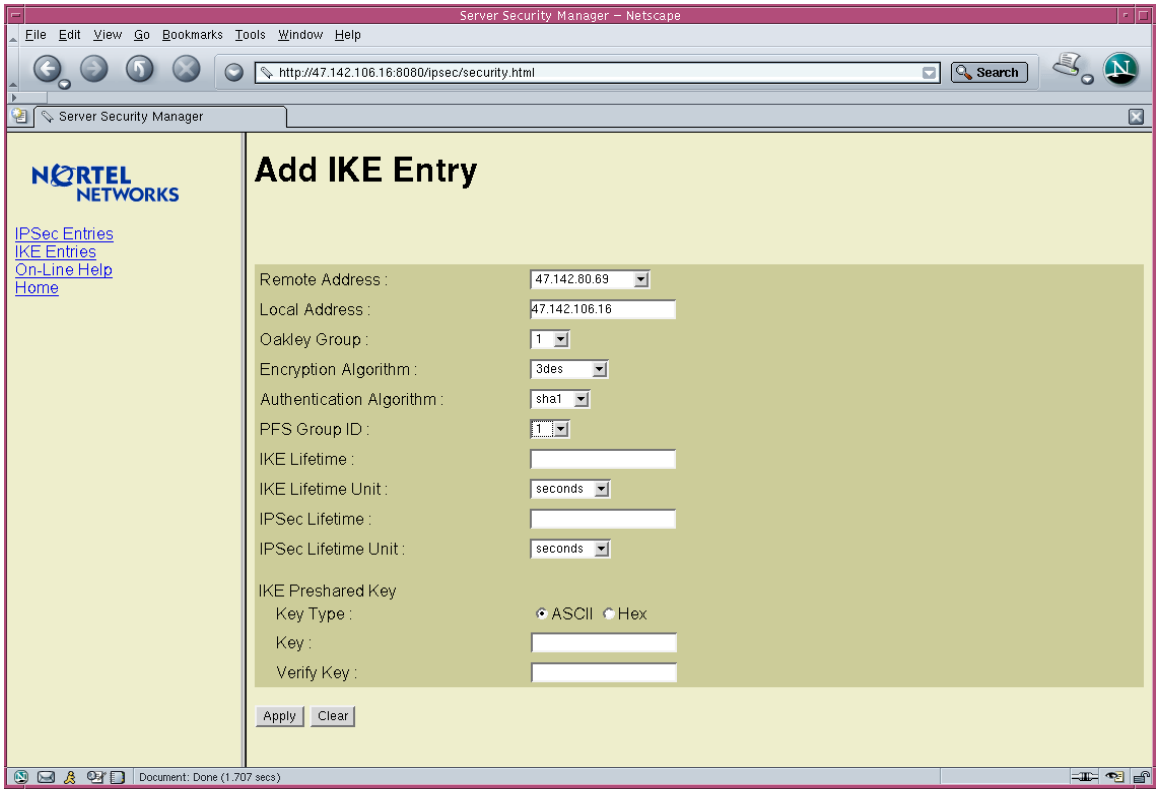
31.9.2.9 IKE provisioned entries example

The following example shows a number of IKE entries for an IEMS server:



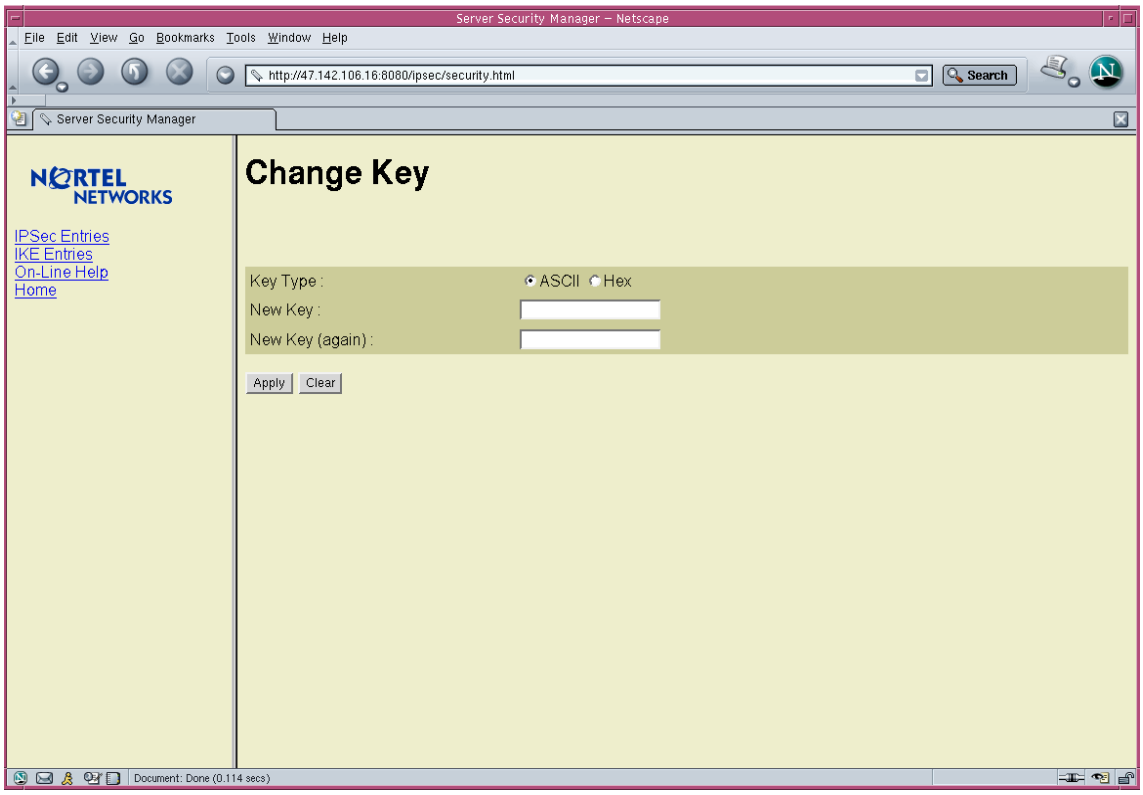
31.9.2.10 IKE entry form example

The following example shows a form for creating IKE entries for an IEMS server:



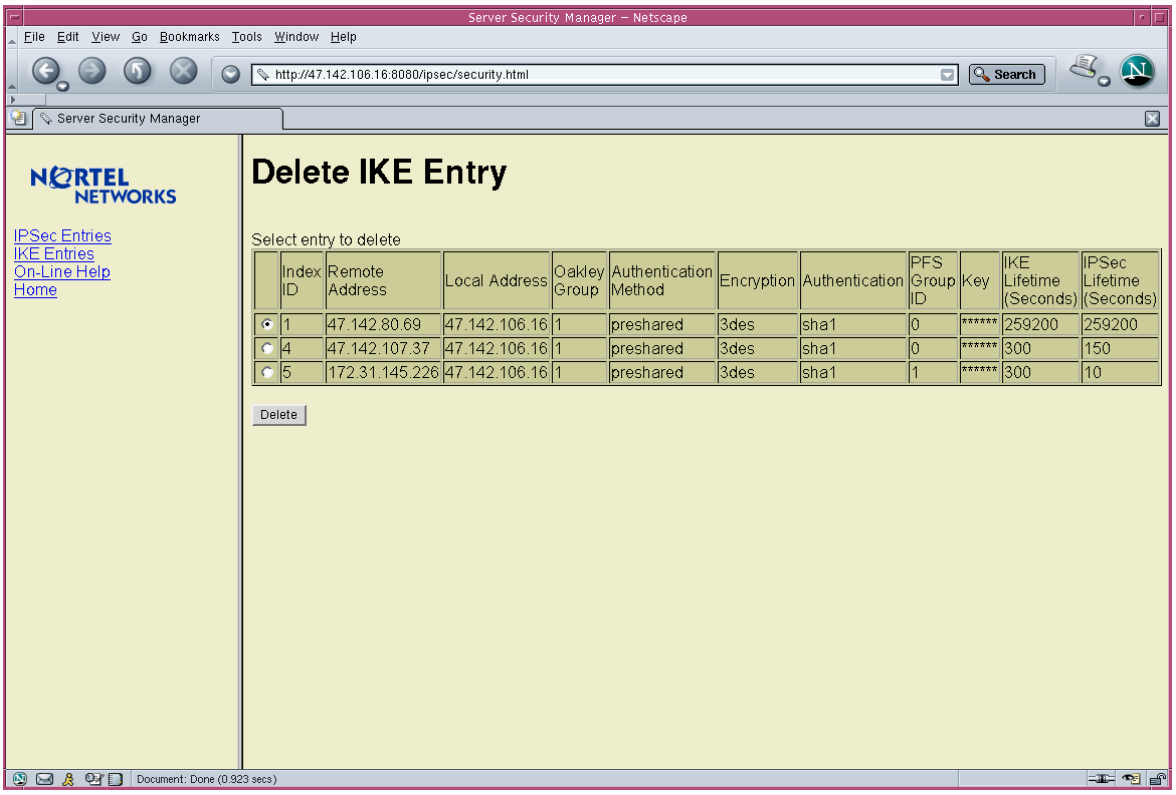
31.9.2.11 IKE change key form example

The following example shows a form for changing an IKE key entry for an IEMS server:



31.9.2.12 IKE entry deletion example

The following example shows a table for deleting IKE entries for an IEMS server:



31.9.2.13 OSS Parameter settings

******This section will need to be verified.******

For each OSS provisioned and requiring IPSec security, one IPSec entry must be created. For each “ipsec” entry there must be a corresponding IKE entry.

The IKE entry must be provisioned as follows:

1. Remote Address is the address of the OSS as seen by SSPFS based application, such as IEMS.
2. Local Address is the address of the OSS as seen by SSPFS based application, such as IEMS.
3. Oakley Group is “1”.
4. Encryption Algorithm is “3des”.
5. Authentication Algorithm is “sha1”.
6. PFS Group ID is “1”.
7. IKE Lifetime is “8”.

8. IKE Lifetime Unit is “hours”.

9. IPSec Lifetime is “8”.

10. IPSec LIfetime Unit is “hours”.

11. Key Type is “ASCII”.

12. Enter the same key that is entered at the OSS. Twice for verification.

31.9.2.14 GUI release history update

The following information was added:

Initial availability.

31.9.2.15 Supplementary information

None

31.9.2.16 CLUI Interface

Not applicable

31.10 Command interface changes

Not applicable

31.11 Security

31.11.1 Network configuration

UDP Port 500 needs to be open on any firewall for IKE.

UDP Port 500 needs to be open on any firewall for IPSec.

31.11.2 Key management

31.11.2.1 IKE Preshared key

The IKE preshared key is input by the user in the Server Security Manager. This key is secured by the use of secure http, if configured, from the browser to the server.

Note: Solaris stores all keys in a hidden system file not accessible by common users but is available to the ROOT user.

31.11.3 Protocol

IPSec is being used on the Solaris machine.

31.11.4 Authentication

A separate Succession Login will be used for Server Security Manager.

31.12 Configuration Walkthrough

31.12.1 OSS Security

From a high-level here are the steps to enable security on the northbound OSS.

1. Load SSPFS server with required SN09 or later software load.
2. Enable security on the OSS to secure the connection to the SSPFS server. Details of this step are beyond the scope of this document as each OSS provisioning mechanism is different.
3. The craftsperson will then use a web browser and connect to the SSPFS server machine's Server Security Manager (SSM). This is done using the item under the EMS Platforms, SSPFS menu at the top, or manually by entering the correct address information in a supported web browser.
4. After logging in, the craftsperson will enable security on communications with the OSS IP address.
5. This will complete securing the OSS link.

32: Configuration (CN): A00009576

32.1 Feature Name

H.323 RASLess Provisioning

The SN09FF RASLess H.323 Provisioning feature provides the ability to explicitly configure H.323 gateways/gatekeepers on the Succession CS2K (Communication Server 2000) with the “RAS-less” functionality.

32.2 Hardware and Software Requirements

This feature is being delivered as part of the Succession release SN09FF.

32.3 Initial Configuration

This activity enables a craftperson to explicitly provision the RAS-less functionality against a H.323 gateway/gatekeeper on the CS2K. The associate media gateway operation processed on the CS2K Management Tools server has been updated with the ability to accept optional device data via the GUI or OSSGate XML interface. The RASLess option is part of the new optional application data. The new optional data, including RASLess, can be queried and viewed via the GUI or XML interface of the CMT (CS2K Management Tools) server.

The CS2K Management Tools server and GWC(s) (Gateway Controllers) must be configured with the SN09FF software.

32.4 Subnet parameters (SESM)

The RAS-less capability is configured during gateway association via the CS2K Management Tools server.

H.225 defines RAS (Registration, Admission and Status) messages and procedures for controlling access to the network. These messages allow H.323 endpoints to discover and register with a H.323 gatekeeper, to provide information about their capabilities and to request the allocation of appropriate amounts of bandwidth. For some applications, H225/H245 signaling should be used between the CS2K and another entity (e.g. softswitch, gatekeeper, or gateway) for setting up calls, but with no RAS messages. This mode of operation is deemed “RAS-less”.

32.4.1 New/modified subnet parameters

Table 1 New RAS-less parameter

Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
RASLess	New	associate media gateway, query media gateway

32.4.2 Parameter information

The optional RASLess boolean configures a H.323 gateway/gatekeeper on the CS2K with the RAS-less capability.

32.4.2.1 RASLess

RASLess

32.4.2.1.1 Functional description

The optional RASless boolean configuration signifies to the CS2K H.323 Gatekeeper application that the respective gateway/gatekeeper will function in a “RAS-less” mode.

32.4.2.1.2 Provisioning rules Range information

Only H.323 gateways/gatekeepers can be configured with the RASLess option.

32.4.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
boolean option (True or False)	boolean option (True or False)	False

32.4.2.1.4 Activation

The parameter is activated once a H.323 gateway/gatekeeper with the RASLess option set to “True” is provisioned.

32.4.2.1.5 Dependencies

There are no table dependencies.

32.4.2.1.6 Consequences

The RASLess option is a boolean.

32.4.2.1.7 Verification

A craftperson can verify that the RASLess option is working if a H.323 gateway/gatekeeper can successfully register without sending RAS messages to a CS2K H.323 gatekeeper.

32.5 Upgrade Considerations

The RASLess functionality was added to the H.323 GWC in the SN08 release. The functionality was configured by setting the gateway's protocol port value to "1720". During an upgrade from SN08/SN09 to SN09FF, all H.323 gateways/gatekeepers with a provisioned port value of "1720" will have the RASLess boolean set to "True".

32.5.1 Element Management Upgrade

If an attempt is made to provision a H.323 gateway/gatekeeper with the RASLess functionality on a pre-SN09FF H.323 GWC, an error message will be generated and presented to the craftperson via the CS2K Management Tools GUI or XML interface.

32.5.2 Downgrade impact

If a downgrade is executed the RASLess option will be deleted from the respective H.323 gateways/gatekeepers.

32.6 Data schema (DS) (CM, MIBS, RDB)

32.6.1 New GWC-APP-DATA-MIB

Table 3 New or modified tables

MIB name	NEW/CHANGED/ or DELETED/
GWC-APP-DATA-MIB	New

32.6.2 Table/MIB/Remote Database Schema information

A new optional GWC-APP-DATA-MIB has been created to convey optional application specific data to the GWC.

32.6.2.1 Name: GWC-APP-DATA-MIB

32.6.2.1.1 Functional description

The new GWC-APP-DATA-MIB is a generic structure to provide the ability of the GWC EM to convey optional application data to the GWC.

32.6.2.1.2 OIDs

The following table lists OIDs for the new GWC-APP-DATA-MIB.

Table 4 OID descriptions

OID	New or Changed	Subfield or refinement	Entry	Explanation and action
appDataGlobalId	New	N/A	GWCDeviceGID	global identifier
appDataTag	New	N/A	Integer	name
appDataValue	New	N/A	String	value
appDataEntryStatus	New	N/A	RowStatus	status column for row entry

32.6.2.1.3 Datafill example

The following example shows sample datafill for table Optional Device Data.

globalID, RASLESS, true

32.7 Element Management

32.7.1 New/modified GUIs and Functionality

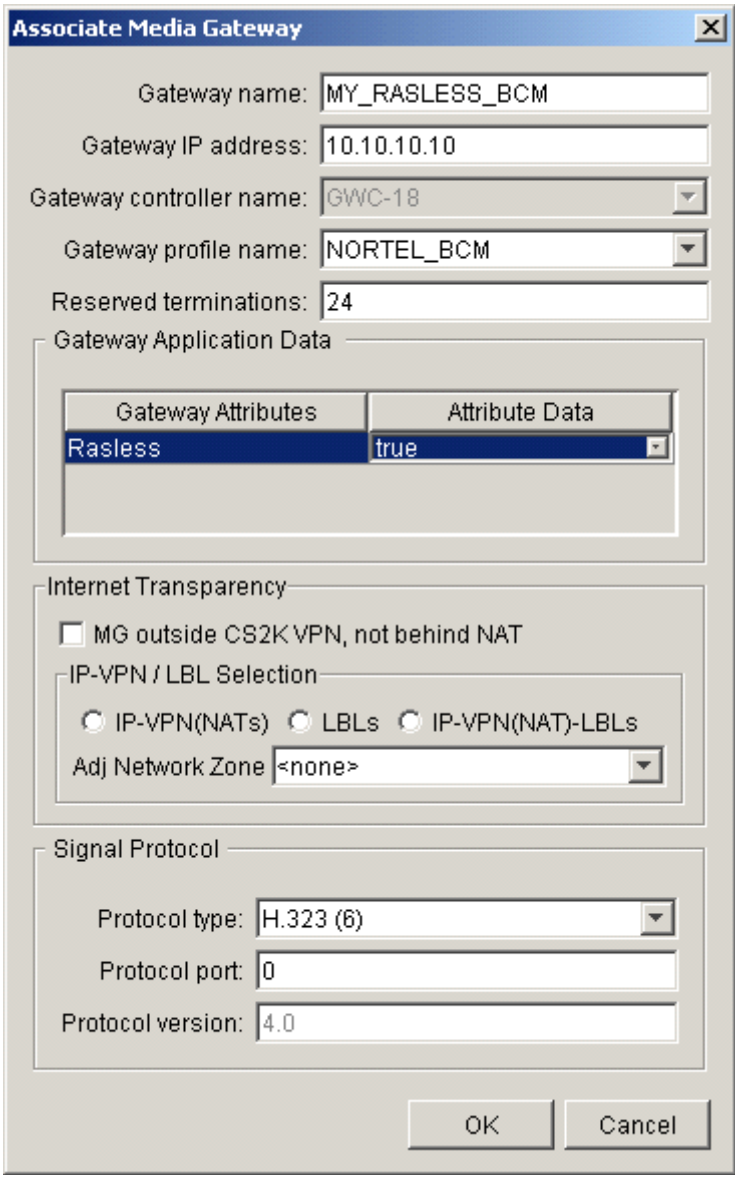
This section describes the changes to GUI of the CS2K Management Tools server affected as a result of this activity.

Table 5 Modified GUI

GUI name	NEW, CHANGED, or DELETED
Associate Media Gateway	Changed by adding optional application data in SN09FF
Details dialog box of the Gateway tab component	Changed by adding optional application data in SN09FF

32.7.2 GUI information

32.7.2.1 GUI name: Associate Media Gateway



Please note that GUI snapshot above displays the RASLess option for a H.323 gateway during an associate gateway operation.

32.7.2.1.1 Functional description

The Associate Media GW dialog box is displayed by using the configuration menu from the main CMT (CS2K Management Tools) GUI or by selecting the "Associate" button from the Gateway panel of a GWC. This dialog box is used to add gateways to the CMT, which in turn populates the respective GWC device. The fields that are available with this dialog have not been updated. An optional data component has been added.

32.7.2.1.2 GUI usage and implications

The associate gateway operation has been updated with the ability to configure the optional RAS-less capability. The RASLess option is displayed as part of the GWC Provisioning Panel of the CMT GUI. The Gateway Tab of the GWC Provisioning Panel has been updated to display the RASLess option.

Once the associate media gateway operation is invoked, the corresponding associate media gateway dialog is launched. To configure the RAS-less functionality, a craftperson must choose a H.323 gateway profile from the "Gateway profile name" pull down menu of the associate media gateway dialog box.

If a H.323 gateway profile is chosen, specific H.323 configuration data options are presented. The new optional data panel has been added to the associate gateway dialog box. The optional "RAS-less" data is presented as part of the new optional data choices. A craftperson can enable the RAS-less capability by setting the option to "true". The default value is "false".

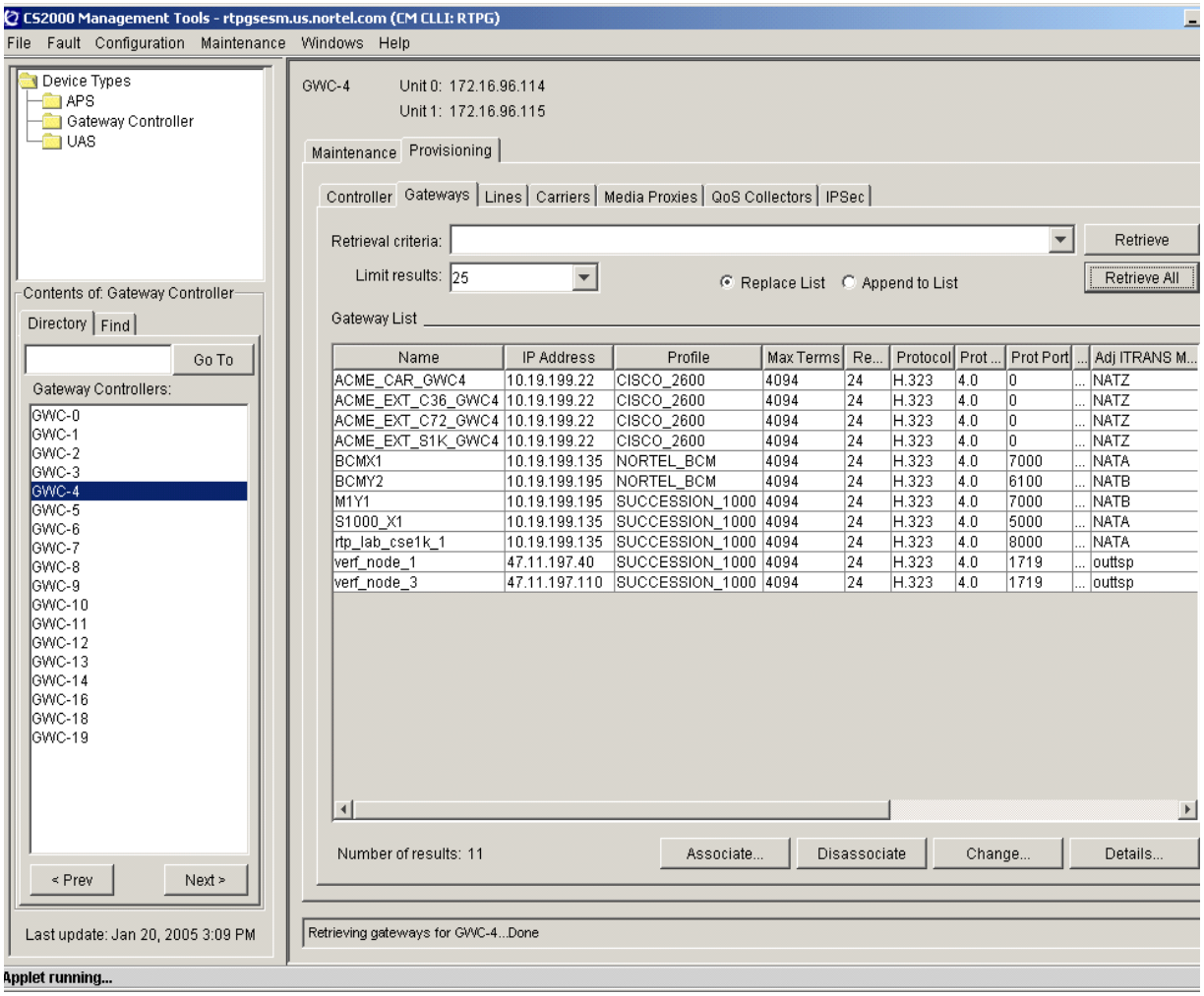
Once all the required data is entered, the "OK" button of the associate media gateway dialog box will be enabled. By clicking on the "OK" button, the GWC EM will process the operation and generate the required SNMP messages. The SNMP messages are sent to the respective GWC. The craftperson will receive a successful or failure response from the GWC EM upon completion of the operation.

The "Details" button of the Gateway tab of the GUI will display the new optional data if supported by the specific gateway profile. A craftperson can click on the Details button to launch a gateway's Details dialog box. The optional gateway data will be displayed for the respective gateway. The RASLess option is listed in the dialog box if the selected gateway is H.323. If there isn't any gateway application data defined for the selected gateway, a dialog box will be launched indicating the respective gateway profile does not have any optional data defined.

The Details button is also used to display the associated "root middleboxes" of a respective gateway. Currently, H.323 gateways do not support root middleboxes.

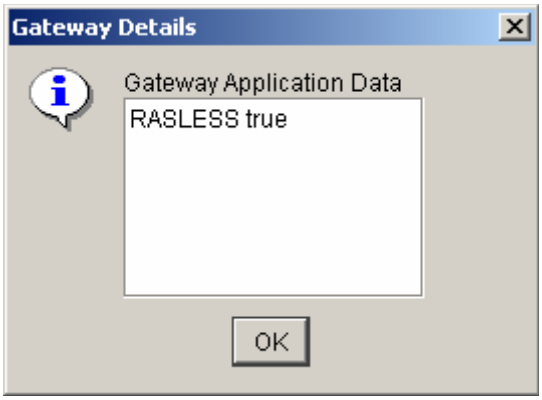
Note: *All current H.323 gateway profiles support the new optional RASLess configuration except for the H323_PROXY gateway profile.*

32.7.2.2 GUI name: Gateway tab of the GWC Provisioning Panel



To display the gateway optional data, a craftperson must click on the “Details” button in the lower right corner of the Gateway tab. The Gateway tab is a component of the GWC Provisioning Panel.

The GUI snapshot below displays the details of a H.323 RAS-less configured gateway.



32.7.2.2.1 Functional description

The “Details” button of the Gateway tab of the GUI will display the new optional data if supported by the specific gateway profile. A craftperson can click on the Details button to launch a gateway’s Details dialog box. The optional gateway data will be displayed for the respective gateway. The RASLess option is listed in the dialog box if the selected gateway is H.323. If there isn’t any gateway application data defined for the selected gateway, a dialog box will be launched indicating the respective gateway profile does not have any optional data defined.

32.8 User interface changes

32.8.1 OSSGate User Interface

This activity modifies support for the operations listed below:

- **associateMG (updated functionality for H.323)**
- **queryMG response (updated functionality for H.323)**

32.8.2 Terminology & Description of New Method Parameters

32.8.2.1 assocMG

The Associate MG command is the OSSGate XML interface used to datafill media gateways. This interface has been modified by adding the optional device data, which includes the RASLess option.

32.8.2.2 queryMG

The Query MG command is the OSSGate XML interface used to retrieve media gateways provisioned on the CS2K. The query interface will return the new RASLess boolean if the query MG operation was invoked against a RAS-less H.323 gateway/gatekeeper.

32.8.3 H.323 Gateway Certificate Changes

H.323 Nortel BCM Certificate changes example

```
<?xml version="1.0" encoding="UTF-8" ?>
<certificate>

 <MaxEndpoints>4094</MaxEndpoints>
 <Category>LARGE</Category>
 <EndpointType>nocarrierTrkGwcNN</EndpointType>
 <GenerateLGRP>true</GenerateLGRP>
 <ResvTermMandatory>true</ResvTermMandatory>
 <ChangeIPAvailable>true</ChangeIPAvailable>
 <DispPhyLocation>false</DispPhyLocation>
 <InventoryType>H.323 Gateway</InventoryType>
 <InventoryRole>Media Gateway</InventoryRole>
 <SupportedProtocol>
  <protocolName>h323</protocolName>
  <version>4.0</version>
 </SupportedProtocol>
 <GWCProfileNumber>61</GWCProfileNumber>
 <EPIDGenDesc>auto1</EPIDGenDesc>
 <ServiceTypeList>H323</ServiceTypeList>
 <ServiceTypeList>ITRANS</ServiceTypeList>
  <CompatibleGWProfileList>NORTEL_BCM</CompatibleGWProfileList>
  <GwAppData name="Rasless" values="false,true" pattern="true|false"/>

 <GatewayNameFormatList>
    <nameFormat formatKey="GATEWAY.H323" enabled="true">
      <delimiters>`</delimiters>
      <maxTokens>1</maxTokens>
      <name>H323 Gateway</name>
      <tokenFormats>
        <tokenFormat tokenKey="GW">
          <pattern><![CDATA[[^"`'<>=]* ]]></pattern>
          <name>Name</name>
        </tokenFormat>
      </tokenFormats>
    </nameFormat>
    <nameFormat formatKey="GATEWAY.ALL" enabled="true">
      <template>gatewayName</template>
      <delimiters>none</delimiters>
      <minLength>1</minLength>
      <maxLength>32</maxLength>
      <name>Generic For All Gateways</name>
      <tokenFormats>
```

Please note that all the existing H.323 certificates except "H323_PROXY" were updated to include the new RASLess option.

32.8.4 XML - Example Commands and Responses

Listed below are syntax examples of the XML commands affected by the H.323 work in this activity. For some cases, new functionality is introduced. For others, new optional tags in reference to H.323 are highlighted. The XML in these examples are formatted for ease of understanding.

32.8.4.1 Command Examples for Associate MG command

The command syntax for assocMG command has changed from prior releases in reference to adding optional data for H.323 gateways. The syntax is listed here as a convenience.

Example format of an **assocMG** command with RASLess

```
<?xml version="1.0" encoding="UTF-8"  ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
    <assocMG usn="1" version="1.0">
        <Parameters>
              <mgUIName>MY_RASLESS_BCM</mgUIName>
              <mgProfileName>NORTEL_BCM</mgProfileName>
              <mgIpAddr>47.142.10.10</mgIpAddr>
              <mgProtocolType>6</mgProtocolType>
              <mgProtocolVersion>4.0</mgProtocolVersion>
              <mgProtocolPort>1720</mgProtocolPort>
              <gwcUIName>GWC-18</gwcUIName>
              <reservedTerminations>24</reservedTerminations>
                <gwAppDataList>
                   <gwAppData>
                      <gwAppTag>Rasless</gwAppTag>
                        <gwAppValue>true</gwAppValue>
                    </gwAppData>
                 </gwAppDataList>
        </Parameters>
    </assocMG>
   </Methods>
  </Command>
</CommandList>
```

32.8.4.2 Command Examples for queryMG command

The command syntax for queryMG command has not changed from prior releases in reference to querying H.323 gateways. The response has changed and now includes the optional data RASLess for H.323 gateways. The syntax is listed here as a convenience.

Example format of a query**MG** command

```
<?xml version="1.0" encoding="UTF-8" ?>
  <CommandList>
    <Command>
      <Interface>cs2kCfgMgrIf</Interface>
      <Methods>
        <queryMG usn="1" version="1.0">
         <Parameters>
           <mgUIName>MY_RASLESS_BCM</mgUIName>
         </Parameters>
        </queryMG>
      </Methods>
   </Command>
</CommandList>
```

Example format of a queryMG response with the RASLess option

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Response><Interface>cs2kCfgMgrIf</Interface>
   <Methods><queryMG usn="1" version="1.0">
    <ReturnData>
     <Row>
      <mgUIList>MY_RASLESS_BCM</mgUIList>
      <mgIpList>47.142.10.10</mgIpList>
      <callServerId>MY_CS2K</callServerId>
      <gwcUIName>GWC-18</gwcUIName>
      <svcTypeList>6</svcTypeList>
      <svcTypeList>5</svcTypeList>
      <nodeName>GWC 18</nodeName>
      <itransMiddleboxName>NOT_SET</itransMiddleboxName>
      <algName>NOT_SET</algName>
      <engrEndPoints>24</engrEndPoints>
      <protType>h323</protType>
      <protVersion>4.0</protVersion>
      <protPort>1720</protPort>
      <profileName>NORTEL_BCM</profileName>
      <maxEngrEndPoints>4094</maxEngrEndPoints>
      <frameNumber>not_set</frameNumber>
      <unitNumber>not_set</unitNumber>
      <frameType>not_set</frameType>
      <floorPos>not_set</floorPos>
      <rowPos>not_set</rowPos>
      <framePos>not_set</framePos>
      <unitPos>not_set</unitPos>
      <gwAppDataList>
        <gwAppData>
          <gwAppTag>RASLESS</gwAppTag>
          <gwAppValue>true</gwAppValue>
        </gwAppData>
      </gwAppDataList>
     </Row><RC>0</RC>
     <MsgTxt>Query of a Single MG was successful</MsgTxt>
    </ReturnData>
   </queryMG>
  </Methods>
 </Response>
</CommandList>
```

32.8.5 XML Schema Listings for affected RASLess H.323 commands

32.8.5.1 Assoc MG

The AssocMG schema has been updated to include the optional application data.

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
            xml:lang="en" >
```

```
 <!--
*****************************************************************************
*************** -->
 <!-- * Define AssocMG Method Parameters -->
 <!--
*****************************************************************************
*************** -->
 <xsd:complexType name="assocMGMethodType">
  <xsd:all>
   <xsd:element name="Parameters" type="assocMGParamsType" />
  </xsd:all>
  <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
 </xsd:complexType>
 <xsd:complexType name="assocMGParamsType">
  <xsd:sequence>
   <xsd:element name="mgUIName" type="NoSpaceNameType" />
   <xsd:element name="mgProfileName" type="NoSpaceNameType" />
   <xsd:element name="mgIpAddr" type="IPAddressType" />
   <xsd:element name="mgProtocolType" type="MGProtocolType" />
   <xsd:element name="mgProtocolVersion" type="xsd:decimal" />
   <xsd:element name="mgProtocolPort" type="xsd:unsignedShort" />
   <xsd:element name="mgSiteName" type="MGSiteNameType" minOccurs="0" />
   <xsd:element name="gwcUIName" type="GWCNameType" minOccurs="0" />
   <xsd:element name="reservedTerminations" type="ReservedTerminationsType" minOccurs="0" />
    <xsd:element name="frameNumber" type="FrameNumberType" minOccurs="0"/>
    <xsd:element name="unitNumber" type="UnitNumberType" minOccurs="0"/>
    <xsd:element name="frameType" type="xsd:string" minOccurs="0"/>
    <xsd:element name="floorPosition"   type="xsd:unsignedShort" minOccurs="0"/>
    <xsd:element name="rowPosition"   type="xsd:string" minOccurs="0"/>
    <xsd:element name="framePosition"   type="xsd:unsignedShort" minOccurs="0"/>
   <xsd:element name="unitPosition"  type="xsd:unsignedShort" minOccurs="0"/>
   <xsd:element name="slotPosition"  type="xsd:unsignedShort" minOccurs="0"/>
   <xsd:choice minOccurs="0">
    <xsd:element name="pepServerName" type="xsd:token" />
    <xsd:element name="algName" type="xsd:token" />
    <xsd:element name="itransMiddleboxName" type="xsd:token" />
    <xsd:element name="rootMiddleboxName1" type="NoSpaceNameType" />
   </xsd:choice>
   <xsd:element name="rootMiddleboxName2" type="NoSpaceNameType" minOccurs="0" />
   <xsd:element name="rootMiddleboxName3" type="NoSpaceNameType" minOccurs="0" />
   <xsd:element name="rootMiddleboxName4" type="NoSpaceNameType" minOccurs="0" />
   <xsd:element name="rootMiddleboxName5" type="NoSpaceNameType" minOccurs="0" />
   <xsd:element name="gwAppDataList" type="GwAppDataListType" minOccurs="0" />
  </xsd:sequence>
 </xsd:complexType>
</xsd:schema>
```

The snbase.xsd was updated with the new GwAppDataListType:

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
            xml:lang="en" >
 <!--
*****************************************************************************
*************** -->
 <!-- ** Global Attribute Groups Used by all schemas  -->
 <!--
*****************************************************************************
*************** -->

 <!-- ********************************************************************** -->
 <!-- * Define Common Usn_Version Attribute Group-->
 <!-- ********************************************************************** -->
 <xsd:attributeGroup name="Usn_VersionAttrbGroup" >
  <xsd:attribute name="usn" type="xsd:integer" use="required" />
  <xsd:attribute name="version" type="xsd:decimal" default="1.0" use="optional" />
```

```
 </xsd:attributeGroup>
 <!--
*********************************************************************************
**************** -->
 <!-- ** Global Complex Types Used by all schemas -->
 <!--
*********************************************************************************
**************** -->
 <!--
*********************************************************************************
**************** -->
 <!-- * Global Simple Types Used or Useable by all schemas follows: -->
 <!--
*********************************************************************************
**************** -->
 <!--
*********************************************************************************
**************** -->
 <!-- * Define No Space Name Type -->
 <!--
*********************************************************************************
**************** -->
 <xsd:simpleType name="NoSpaceNameType">
  <xsd:restriction base="xsd:token">
   <xsd:minLength value="1" />
   <xsd:pattern value="\S{1,32}" />
  </xsd:restriction>
 </xsd:simpleType>
 <!--
*********************************************************************************
**************** -->
 <!-- * Define IPAddressType-->
 <!--
*********************************************************************************
**************** -->
 <xsd:simpleType name="IPAddressType">
  <xsd:restriction base="xsd:string">
   <xsd:pattern value="\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}"/>
  </xsd:restriction>
 </xsd:simpleType>
 <!--
*********************************************************************************
**************** -->
 <!-- * Define MGProtocolType-->
 <!--
*********************************************************************************
**************** -->
 <xsd:simpleType name="MGProtocolType">
  <xsd:restriction base="xsd:integer">
   <xsd:minInclusive value="1" />
   <xsd:maxInclusive value="6" />
   <xsd:pattern value="\d{1}" />
  </xsd:restriction>
 </xsd:simpleType>
 <!--
*********************************************************************************
**************** -->
 <!-- * Define GWCNameType-->
 <!--
*********************************************************************************
**************** -->
 <xsd:simpleType name="GWCNameType">
  <xsd:restriction base="xsd:string">
   <xsd:pattern value="GWC-\d\d?\d?" />
  </xsd:restriction>
 </xsd:simpleType>
```

```
 <!--
*****************************************************************************************
*************** -->
 <!-- * Define ReservedTerminationsType -->
 <!--
*****************************************************************************************
*************** -->
 <xsd:simpleType name="ReservedTerminationsType">
  <xsd:restriction base="xsd:integer">
   <xsd:minInclusive value="0" />
   <xsd:maxInclusive value="6400" />
  </xsd:restriction>
 </xsd:simpleType>
 <!--
*****************************************************************************************
*************** -->
 <!-- * Define IpPortTypeType-->
 <!--
*****************************************************************************************
*************** -->
 <xsd:simpleType name="IpPortType">
  <xsd:restriction base="xsd:integer">
   <xsd:minInclusive value="0" />
   <xsd:maxInclusive value="65535" />
  </xsd:restriction>
 </xsd:simpleType>
 <!--
*****************************************************************************************
*************** -->
 <!-- * Define MGSiteNameType-->
 <!--
*****************************************************************************************
*************** -->
 <xsd:simpleType name="MGSiteNameType">
  <xsd:restriction base="NoSpaceNameType">
   <xsd:maxLength value="4" />
  </xsd:restriction>
 </xsd:simpleType>
 <!-- ********************************************************************************************* --
>
 <!-- * Define GwAppDataType-->
 <!-- ********************************************************************************************* --
>
 <xsd:complexType name="GwAppDataType">
  <xsd:sequence>
   <xsd:element name="gwAppTag"   type="xsd:string"/>
   <xsd:element name="gwAppValue" type="xsd:string"/>
  </xsd:sequence>
 </xsd:complexType>
  <!-- ********************************************************************************************* -
->
 <!-- * Define GwAppDataListType-->
 <!-- ********************************************************************************************* --
>
 <xsd:complexType name="GwAppDataListType">
  <xsd:sequence>
   <xsd:element name="gwAppData" type="GwAppDataType" minOccurs="0"
maxOccurs="20"/>
  </xsd:sequence>
 </xsd:complexType>
</xsd:schema>
```

32.8.5.2 Query MG

No changes have been made to the QueryMG schema. The response for H.323 gateways will include the gateway optional data.

32.9 Limitations and Restrictions

• The optional RAS-less feature can only be provisioned against H.323 gateways/gatekeepers on the CS2K.
• The optional RAS-less feature is not supported with a NAT configuration of N:1. The N:1 NAT configuration is when multiple gateways behind a NAT share the same “NAT’d” IP address and the gateways are uniquely identified by the port value.
• The gateway profile “H323_PROXY” does not support the RAS-less functionality.

32.10 Configuration Walkthrough

32.10.1 Adding a H.323 GW with RASLess option

- SN09FF
  - — Add a H.323 GWC to the system
  - — Associate GW with the GWC including the RASLess option set to “true”
    - Adds GW to GWC
  - — Add a H.323 Carrier
    - Adds EPG to GW

33: Configuration (CN): A00009611

33.1 Feature Name

IEMS Keymile Integration

33.2 UNEM GUI Launch

- Launch UNEM Network browser
- UMUX shelf Configuration GUI

33.2.1 Launch UNEM Network Browser

While adding the UNEM, an additional parameter is provided to specify if the SSH is enabled or not in the device

33.2.2 SSH Enabled

Linux
While launching the UNEM Network browser / UMUX Shelf Configuration a dialog will come up to provide the username/password, IEMS will use the X11 port forwarding and bring up the appropriate GUI.

Windows
While launching the UNEM Network browser/UMUX Shelf Configuration, a dialog box with provision to provide Exceed file path and the login/password using which the appropriate GUI will be brought up.

33.2.3 SSH Disabled

Linux
For solaris clients IEMS will invoke the default Telnet prompt. User has to do the rest manually for invoking the GUI.

Windows
While invoking the UNEM Network Browser / UMUX Shelf Configuration, IEMS client will use the xstart.exe(Exceed tool) to launch the GUI in non-encryption mode.

33.2.4 Launching from the UMUX

The SSH enabled (true/false) value provided for the UNEM while addition will be updated for all the UMUX (NEs). If the SSH is enabled in the UNEM, the launch UMUX shelf configuration from the UMUX devices will try to launch through SSH. If SSH is not enabled in the UNEM device, the launch will fail and the user can subsequently modify the SSH property to disable and proceed with the launch.

33.2.5 Commands used for launch

UNEM Network Browser -- **/usr/local/bin/nocslogin -e ec**

UMUX Shelf Configuration -- **/usr/local/bin/nocslogin -e ne -i**

Windows NON SSH Mode

UNEM Network Browser -- **/usr/local/bin/nocrlogin -e ec -s auto -d**

UMUX Shelf configuration -- **/usr/local/bin/nocrlogin -e ne -i**

33.3 Launching UNEM Browser for UNEM

The UNEM browser for UNEM version 9.0 can be launched from Integrated EMS Java Web Start Client. This procedure describes how to launch the UNEM browser from Integrated EMS Java Web Start Client.

Note: The launching of UNEM Browser works only if the Patch Collection 1 is installed on the UNEM Server.

33.3.1 To launch UNEM browser for UNEM version 9.0, follow these steps:

At Integrated EMS workstation

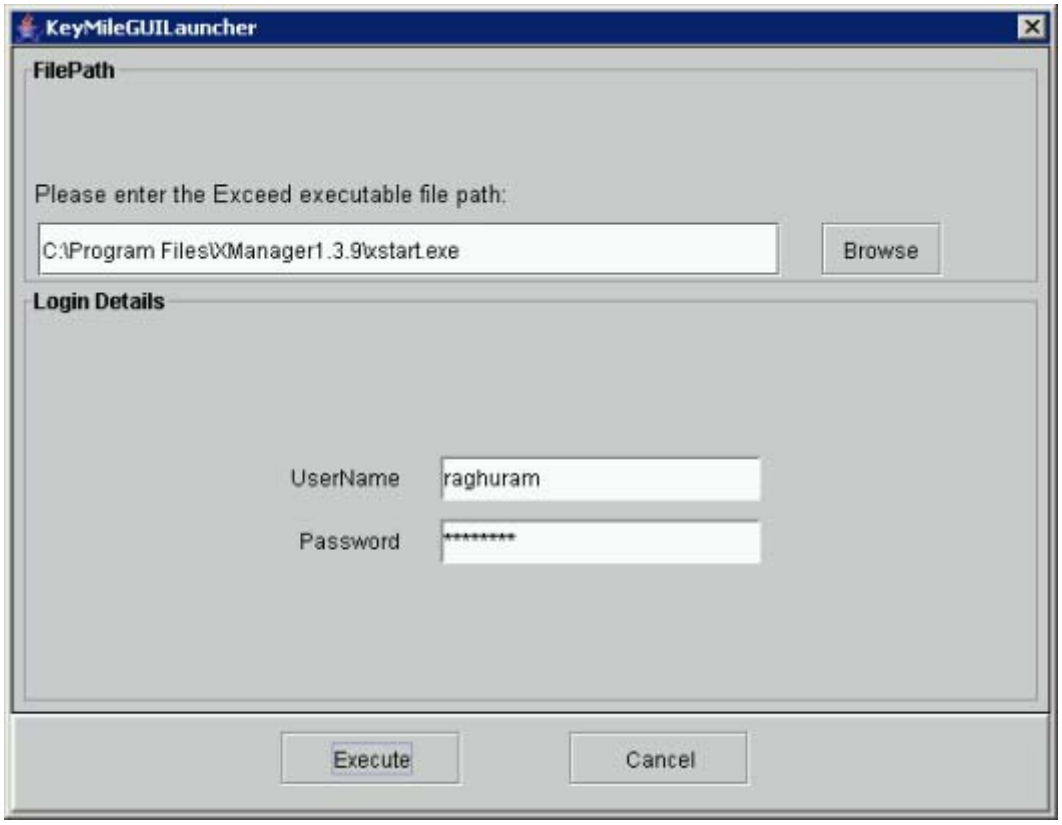
1 Launch the Integrated EMS Java Web Start Client (refer to "Launching the Integrated EMS Java Web Start Client.")

2 Go to the **Element Managers** topology in the Integrated EMS tree.

3 Select an UNEM map symbol.

4 Right-click the map symbol and select the **Launch UNEM Browser** menu item.

The system displays a window similar to the following screen shot for the Integrated EMS Client in Microsoft Windows platform.



5 For Microsoft Windows-based client, click the **Browse** button to select the Exceed application executable file path. This step is not applicable for Solaris-based clients as this field is not present.

Note: For launching the application without SSH, "xstart.exe" must be selected and "exceed.exe" must be selected for launching the application with SSH enabled.

6 Type the user name and password in the respective fields.

7 Click the **Execute** button to execute the specified command.

Note: Integrated EMS saves the location of the script or the executable file and commands in the client system from which the Integrated EMS Java Web Start Client is launched.

33.4 Launching applications for UMUX NEs

The UNEM browser and UMUX Shelf Configuration GUI for UMUX NEs (UMUX 1500, UMUX 1200, and UMUX 900 NEs) version 9.0 can be launched from Integrated EMS Java Web Start Client. This procedure

describes how to launch the UNEM browser from Integrated EMS Java Web Start Client

Note: The launching of UNEM Browser or UMUX Shelf Configuration works only if the Patch Collection 1 is installed on the UNEM Server.

33.4.1 To launch UNEM browser or UMUX Shelf Configuration GUI for UMUX NEs version 9.0, follow these steps:

At Integrated EMS workstation

1 Launch the Integrated EMS Java Web Start Client (refer to "Launching the Integrated EMS Java Web Start Client.")

2 Go to the **Element Managers** topology in the Integrated EMS tree.

3 Select an UMUX NE map symbol.

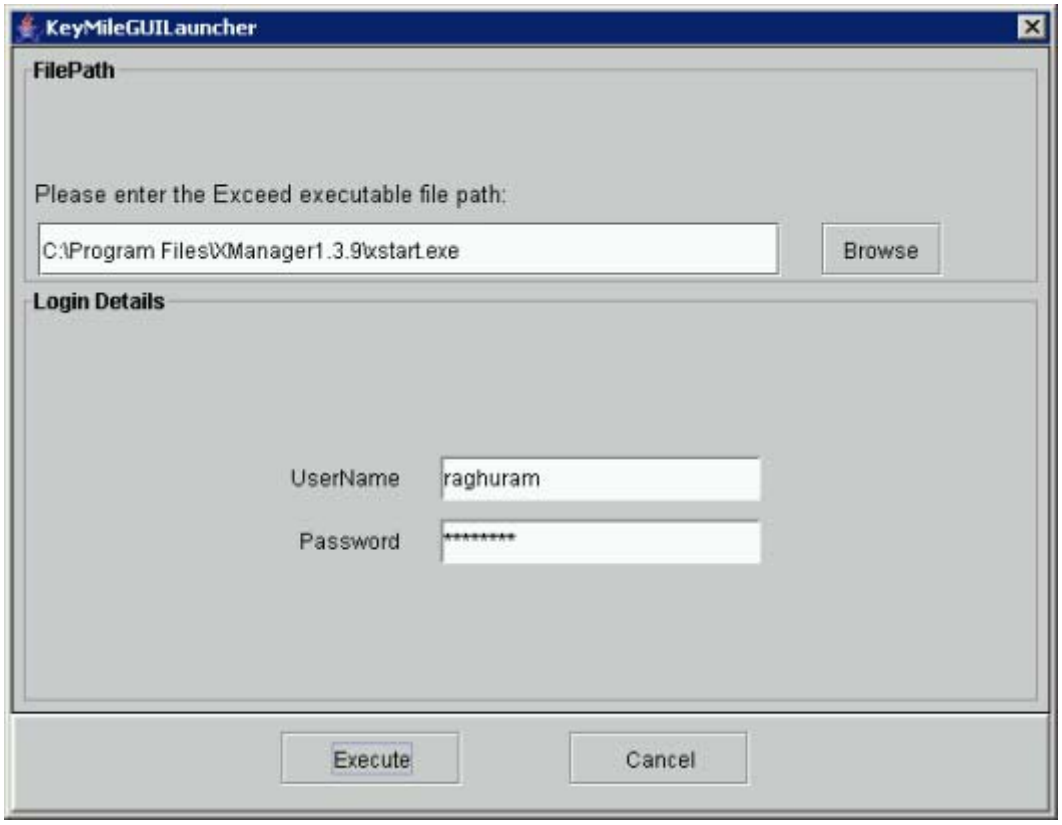
4 Right-click the map symbol and select the **Launch UNEM Browser** menu item.

The system displays a window similar to the following screen shot for the Integrated EMS Client in Microsoft Window platform.

OR

Right-click the map symbol and select the **Launch UMUX Shelf Configuration** menu item.

The system displays a window similar to the following screen shot for the Integrated EMS Client in Microsoft Windows platform.



5 For Microsoft Windows-based client, click the **Browse** button to select the Exceed application executable file path. This step is not applicable for Solaris-based clients as this field is not present.

Note: For launching the application without SSH, "xstart.exe" must be selected and "exceed.exe" must be selected for launching the application with SSH enabled.

6 Type the user name and password in the respective fields.

7 Click the **Execute** button to execute the specified command.

Note: Integrated EMS saves the location of the script or the executable file and commands in the client system from which the Integrated EMS Java Web Start Client is launched.

33.5 Adding a UMUX Network Element Manager (UNEM)

UNEM manages UMUX 1500, UMUX 1200, and UMUX 900 NEs in the UMUX network. The UMUX stands for Universal Multiplexer. When you add an UNEM, these NEs are added as a map symbol under the **Network Elements** topology and **UMUX-1500**, **UMUX-1200**, and **UMUX-900** topology (under **Network Elements** node) respectively. The UNEM is added

as a map symbol in the **Element Managers** topology. Also, the UNEM is added as map symbols in the **EMS-UNEM-Mgr** topology (with added UNEM display name in brackets). This procedure describes how to add the UNEM to the Integrated EMS topology using Integrated EMS Java Web Start Client.

The following list provides the operations available for UNEM in Integrated EMS.

Tasks Supported in Integrated EMS for UNEM

Task in Integrated EMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	Yes	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No

Tasks Supported in Integrated EMS for UNEM

Task in Integrated EMS	Availability	
	Java Web Start Client	Web Client
Other operations		
Launching corresponding applications	Yes	No

33.5.1 To add the UNEM to the topology, follow these steps:

At Integrated EMS workstation

1 Launch the Integrated EMS Java Web Start Client (refer to "Launching Integrated EMS Java Web Start Client").

2 Select the **Tools**-->**Add**-->**EMS/NE** menu command to invoke the **Add EMS/NE** dialog.

3 Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard. For details on these fields, refer to the following table:

Description of fields in Add EMS/NE Wizard

Field	Description
Host Name/IP Address	The field for the host name or IP address of the element manager.
Time Zone	A list box to select the time zone associated with the object.
Display Name	The name that must be displayed in the topology for the map symbol.

4 Select "EMS" from the **Type** list box.

5 Select "UNEM" from the **Device Type** list box.

6 Select the **SSH enabled** field if the SSH is enabled in the UNEM device.

Note: If the SSH enabled field is selected and the UNEM server does not have SSH installed, the launching of UNEM Browser from UNEM and UMUX NEs and launching of UMUX Shelf Configuration fails. For procedure to launch UNEM Browser for UNEM, refer to "Launching UNEM browser for UNEM"

7 Click the **Next** button.

8 In the **Port** field, enter the port value (in which the EMS communicates with Integrated EMS).

9 Enter the community in the **Community** field.

10 Select the SNMP version "v1" from the **Version** list box.

Note: The port value and the SNMP version are dependent on the UNEM configuration that is added.

11 Click the **Next** button.

12 Click the **Finish** button to add the UNEM.

Once the UNEM is added, a message appears in the status bar of the wizard as in the following screen shot:

The UNEM with the specified name is added to the **Element Managers** topology panel. Also, the UNEM is added as map symbols in the topology node named **EMS-UNEM-Mgr** (with the specified display name in brackets).

33.6 Adding UMUX NEs

UNEM manages UMUX 1500, UMUX 1200 and UMUX 900 NEs in the UMUX network. Refer to “Adding a UMUX Network Element Manager (UNEM)” on page 2589 procedure to add a UNEM. When you add an UNEM, these NEs are automatically discovered and added as map symbols under the **Network Elements** topology. Also they are added as map symbols under the **UMUX-1500**, **UMUX-1200**, and **UMUX-900** topology (under **Network Elements** node) respectively.

The following list provides the operations available for UNEM NEs in Integrated EMS.

Tasks Supported in Integrated EMS for UNEM NEs

Task in Integrated EMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	No	No
Managing or unmanaging the object	No	No

Tasks Supported in Integrated EMS for UNEM NEs

Task in Integrated EMS	Availability	
	Java Web Start Client	Web Client
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	No	No
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

33.7 References

IEMS-Keymile_Integration_DID_v2.0.pdf

UMUX (R7) User Guide, LZTBU 320 115 /3

UNEM (R7) User Guide Basic Package, LZTBU 310 106 /2

UNEM (R7) User Guide Networking Package, LZTBU 310 306 /2

34: Configuration (CN): A00009655

34.1 Feature Name

BladeCenter-T RTP Media Portal

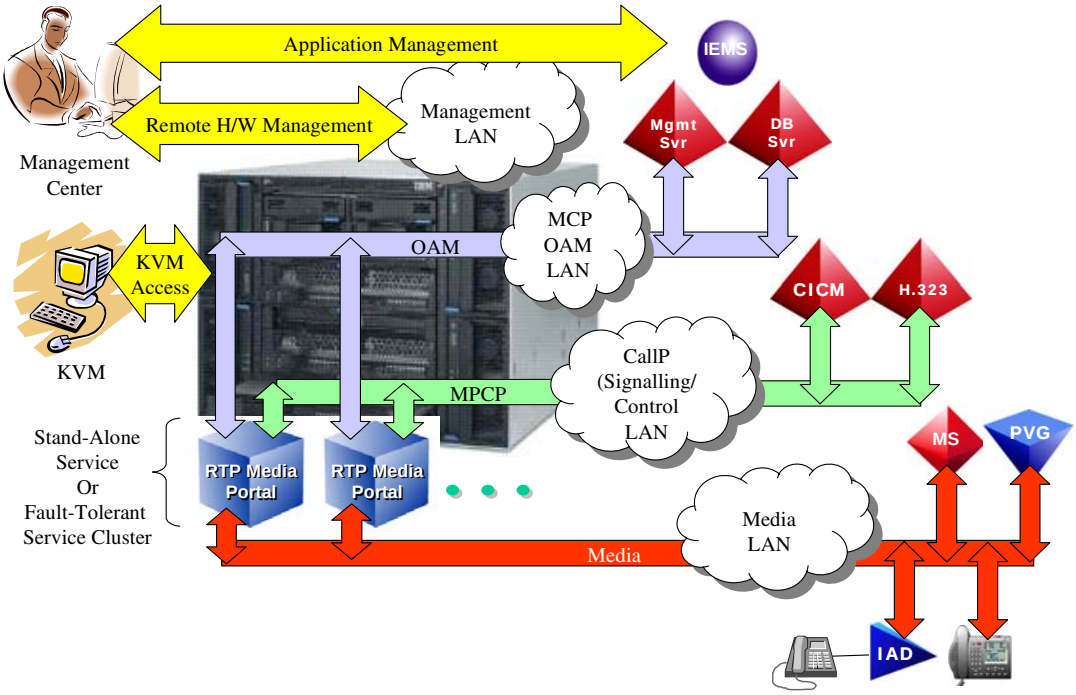
34.2 Overview

The introduction of the BladeCenter-T RTP Media Portal introduces: new hardware components, a new software architecture with new capabilities (Fault Tolerant Service Clusters), and new network connectivity configurables that enable management of the platform and execution of the service (refer to the following figure).

As a result the new BladeCenter-T RTP Media Portal introduces configuration requirements in the following areas:

- Hardware Configuration: (beyond the scope of this document.)
- Network Configuration: describes the network connectivity – this is used to define connectivity of the BladeCenter-T RTP Media Portal into the broader solution (and connections into Service Provider network[s]). The BladeCenter-T RTP MP can connect to a myriad of networks that provide: management access to the hardware components, OAM access to the product, control channel service capabilities, and access to the media streams upon which the service operates. Configuring the BladeCenter-T RTP Media Portal for connection in to a network is executed as part of the initial installation and commissioning procedures – and as part of maintenance/repair activities – that are described in detail in the appropriate methods and procedures.
- Service Configuration: describes the configuration of the stand-alone RTP Media Portal service instance, and the N+1 Fault Tolerant RTP Media Portal service cluster. Service configuration is established and can be easily modified as required to adapt to usage patterns, meet new needs, etc.

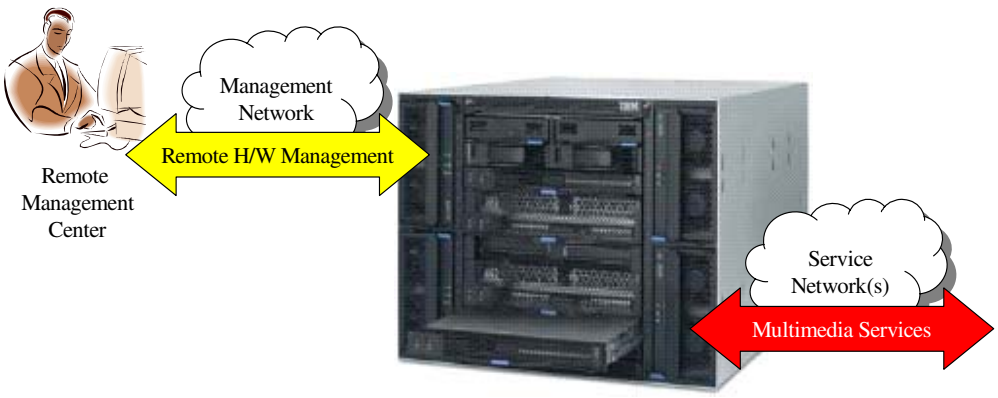
Figure 1 BladeCenter-T RTP Media Portal Configuration Overview



34.3 Network Configuration

The BladeCenter-T RTP Media Portal network configuration is partitioned between two network-spaces: one for management operations (a Management Network), and one for service execution (one or more Service Networks). Refer to the following figure. Certain subcomponents of the BladeCenter-T RTP Media Portal reside in the dedicated Management Network and others reside in the Service Network(s). Subcomponents with presence in the Management Network enable administrative access to the BladeCenter-T platform. Those subcomponents that reside in the Service Network(s) participate in the following aspects of the RTP Media Portal service: Operations/Administration/Maintenance (OAM), service control (MPCP), and execution of media processing functions.

Figure 2 BladeCenter-T RTP Media Portal Network Spaces



The Management Module and the Ethernet Switch Module are configured with IP addresses to provide them presence in the Management Network. The Management Network provides remote administrative and maintenance access to the BladeCenter-T platform.

The Blade Servers are configured with presence (an IP address) in the Service Network(s). The RTP Media Portal service instance that resides on the Blade Servers is also configured with presence in the Service Network(s). This positions both the BladeCenter-T platform and the RTP Media Portal in the service-space – where they can execute the RTP Media Portal service.

This distribution of subcomponents across different network-spaces enables the BladeCenter-T Management Modules reside on a secure management subnet, while the Blade Servers reside on a generally accessible service network in which they can participate in multimedia service delivery. That is, the management functions of the BladeCenter-T chassis are not accessible from outside the Management Network.

The following assumptions apply to the recommended network configuration of this product:

- •The BladeCenter-T Management Module (MM) and Alteon Ethernet Switch Modules (ESMs) must reside on the same subnet. The actual IP addresses and subnet mask are subnet-specific and are outside the scope of this document.
- •The Blade Servers and RTP Media Portal service instances reside on a different subnet from the BladeCenter-T Management Modules. The actual IP addresses and subnet mask for the Blade Servers are subnet-specific and are outside the scope of this document.

- Prior to network configuration of the BladeCenter-T, a sufficient number of IP addresses must be available. The IP address requirements for the various BladeCenter-T subcomponents are listed below):

  Total IPaddrs =

  [(2xIPaddr)] {for Management Module internal/external ports}

  + [(1xIPaddr) x (Number_of_ESM)]

  + (1xIPaddr) {Multicast IPaddr for Fault Tolerant Service Cluster}

  + [(4xIPaddr) x (Number_of_Blade Servers)]

Table 1: BladeCenter-T RTP Media Portal: Overall IP Address Requirements

Network	Subcomponent	IPaddr Requirements	IPaddr Count
Management Network	Management Module (only one set required)	1xIPaddr (external)	3-4
		1xIPaddr (internal)	
	Ethernet Switch Module 1	1xIPaddr (internal)	
	Ethernet Switch Module 2	1xIPaddr (internal)	
Service Network (per Blade Server)	Blade Server (OAM)	1xIPaddr (external)	4-33
(per Service Instance)	MPCP (Control)	1xIPaddr (external)	
	Media1 (Net1)	1xIPaddr (external)	
	Media2 (Net2)	1xIPaddr (external)	
(per Service Cluster)	Fault Tolerant Service Cluster (for Service Clusters only)	1xIPaddr (multicast)	
		Total	**Up to 37 IPaddrs**

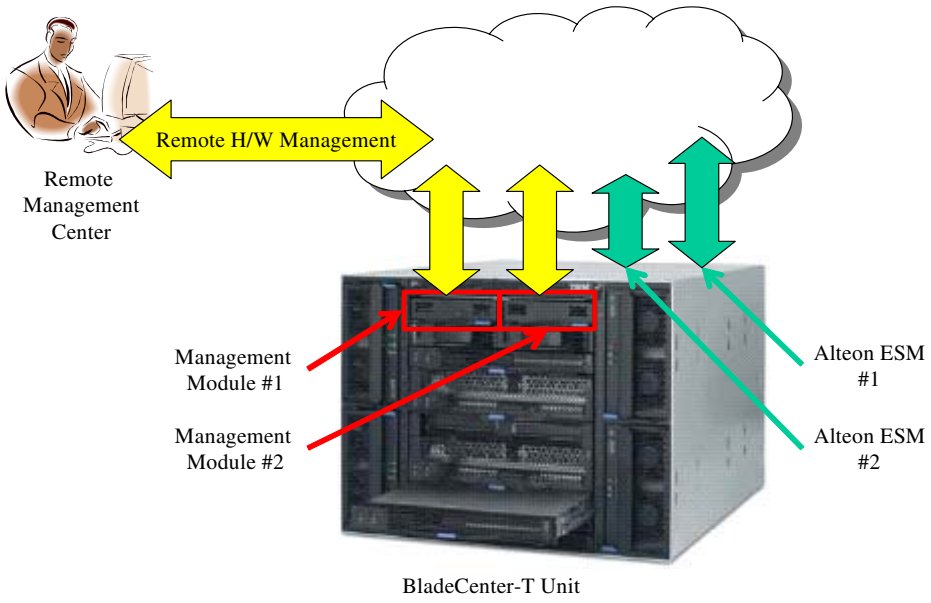
34.3.1 Management Network

34.3.1.1 Overview

The BladeCenter-T RTP Media Portal requires IP Addresses in the Managed Network. In order to provide ubiquitous remote management capabilities, the remote management client IP addresses, the Management Module IP

addresses, and the Alteon ESM management IP addresses all reside in the same subnet. Refer to the following figure.

Figure 3 BladeCenter-T RTP Media Portal: Management Network Overview



The physical relationship of these IP address assignments to the Management Module and the Alteon ESM are represented in the following figure. The actual network topology created by these IP Address assignments is described in the subsequent figure.

Figure 4 Management Network Connections: Physical View (Layer-2 and Layer-3)

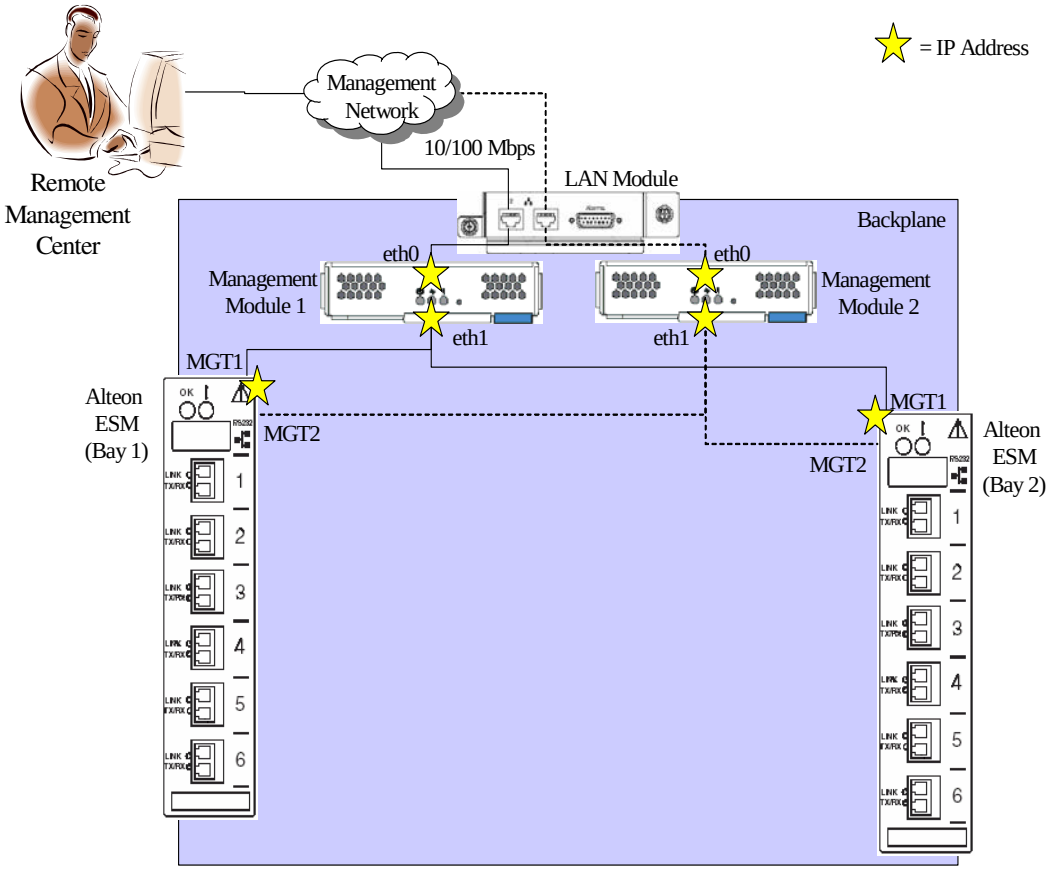
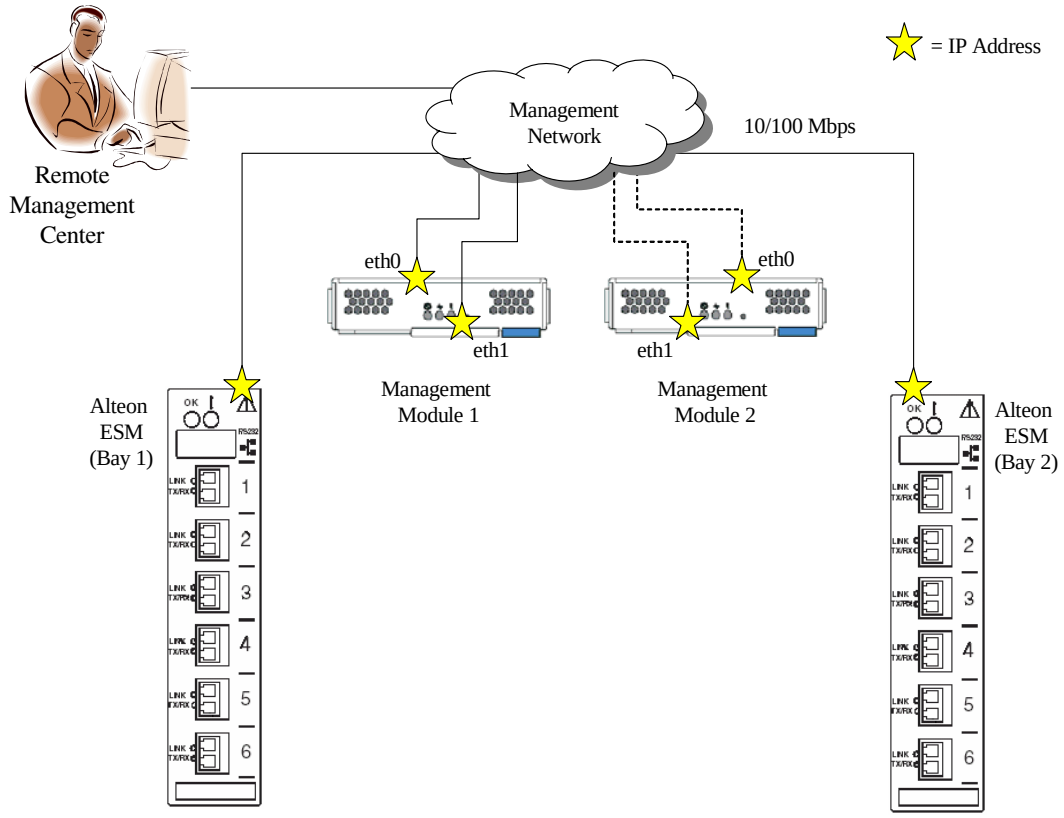


Figure 5 Management Network Connections: Logical View (Layer-3)



34.3.1.2 Configuration of the BCT Management Module

The Management Module provides access to the maintenance and control functions of the IBM BladeCenter-T chassis and its sub-components. Access to these functions is facilitated over the Management Network which connects the remote management center to the Management Modules (via Ethernet connections to the LAN Module which then connect over the back-plane to the Management Modules external interface – eth0).

The LAN Module bridges the external physical Ethernet connection to the Management Network over the backplane to the Management Module (eth0). It is through this path that the Management Module (through eth0), the Alteon Ethernet Switch Modules (accessed through relay between Management Module eth0 and eth1), and other chassis subcomponents can be reached for administrative activities.

There are two new IP Addresses required on the Management Network in order to configure the Management Modules for a given BladeCenter-T (the Management Modules run active/standby so the same settings are shared). These new Management Network IP Addresses overwrite the default factory

settings for each of the Management Modules interfaces (refer to the following table).

Note: It is only necessary to configure the primary Management Module (with IP addresses, etc.); the secondary Management Module does not need to be explicitly configured. In the event that the primary Management Module fails, the secondary Management Module will automatically inherit the settings from the primary Management Module. It is only necessary that both Management Modules be connected to the same network subnet.

Table 2: Management Module: Default IP Addresses.

Interface	Default IP address
eth0	192.168.70.125 / 255.255.255.0
eth1	192.168.70.126 / 255.255.255.0

34.3.1.3 Configuration of the Alteon Ethernet Switch Module (ESM)

The Alteon ESM is configured so that it is only manageable through the BladeCenter-T Management Module. In order to establish this capability the default IP address configured on the Alteon ESM must be overwritten with a valid IP address on the Management Network.

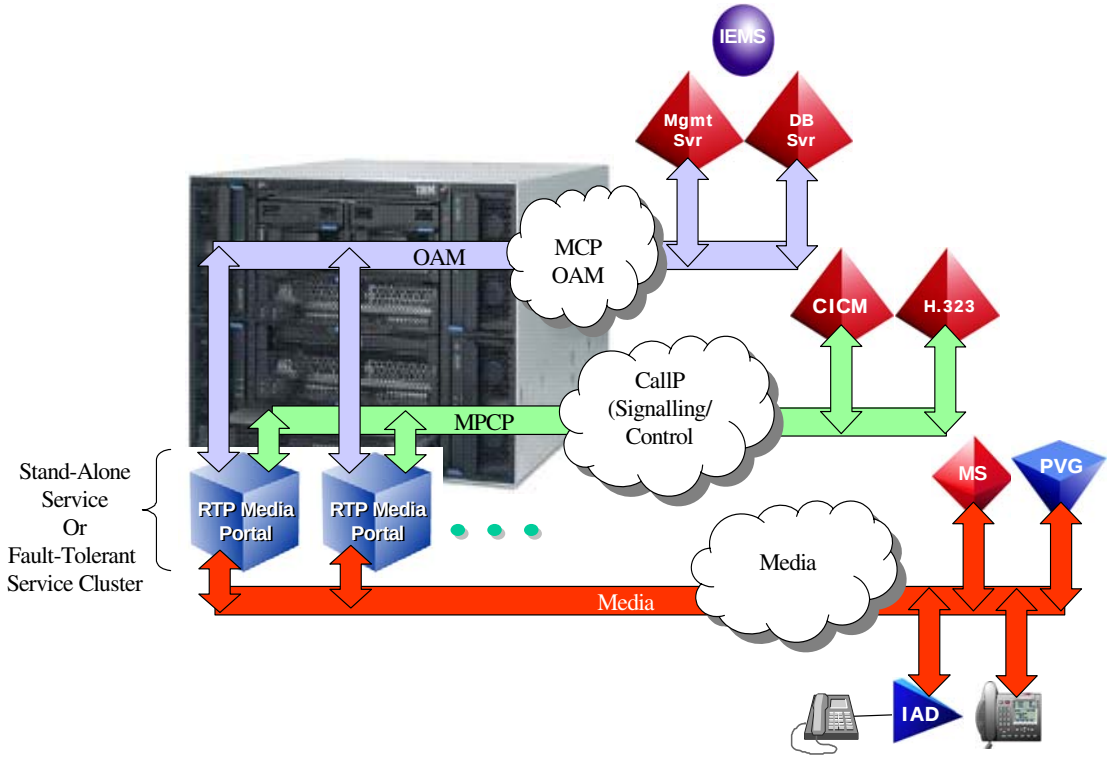
Table 3: Alteon ESM: Default IP Addresses.

Interface	Default IP address
1	10.90.90.91

34.3.2 Service Network

The Service Network is the network-space within which the services are provided and consumed. In fact, this network-space may exist as multiple Service Networks (as depicted in the following figure).
In order to provide the RTP Media Portal service, both the hosting BladeServer and the resident service instance must have presence in the Service Network(s) in order to connect: Service OAM, Service control (MPCP), and Service access (media). Refer to the following figure.

Figure 6 BladeCenter-T RTP Media Portal: Service Network Overview



The physical relationship of these IP address assignments to the Management Module and the Alteon ESM are represented in the following figure. The actual network topology created by these IP Address assignments is described in the subsequent figure.

Figure 7 Service Network Connections: Physical View (Layer-2 and Layer-3)

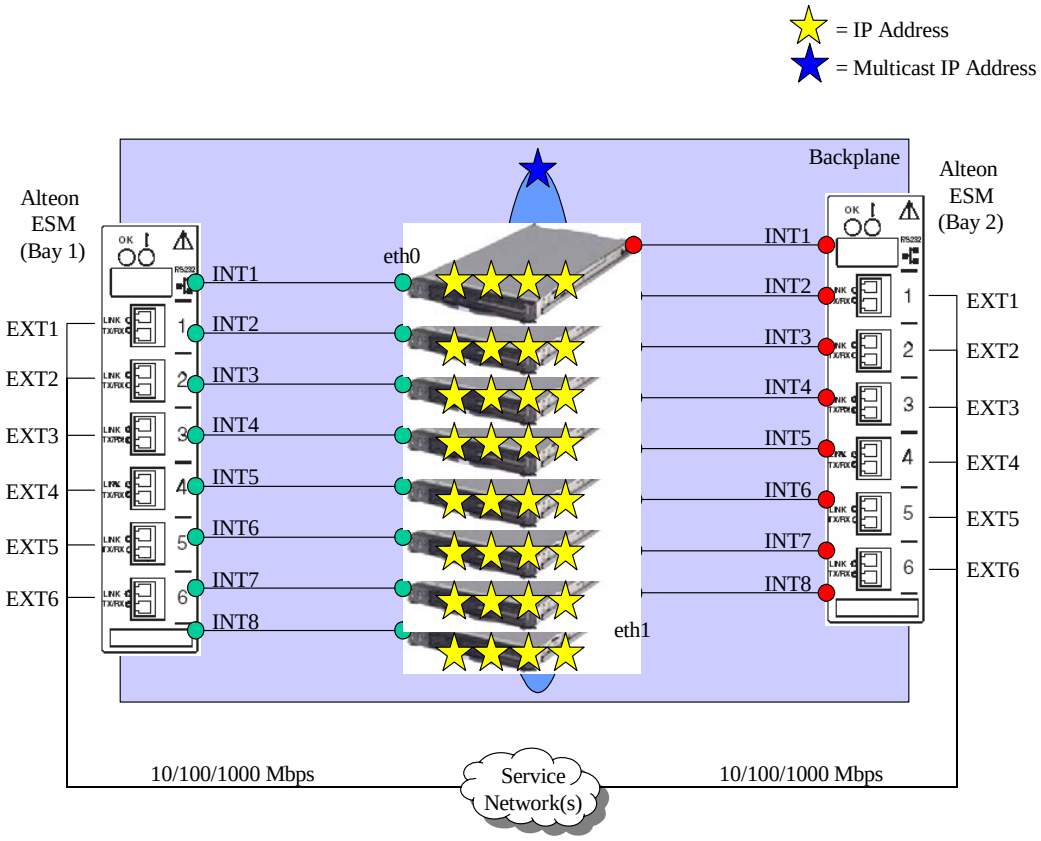
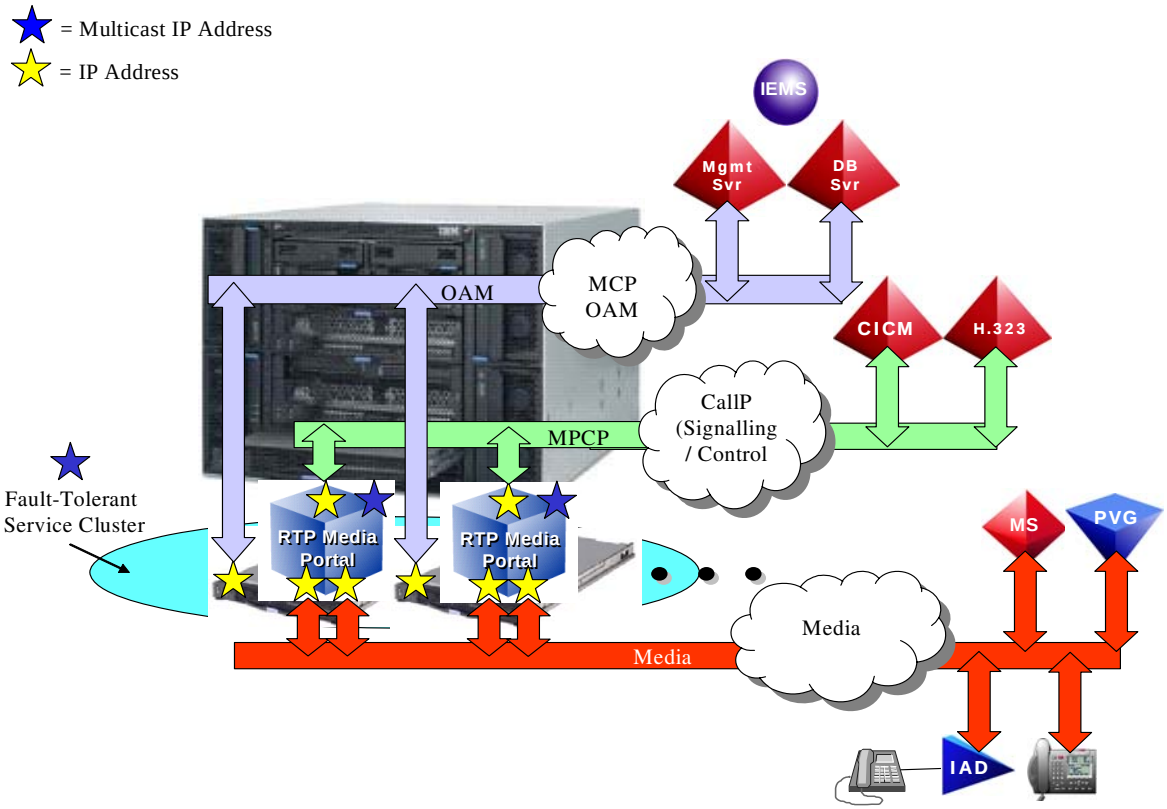


Figure 8 Service Network Connections: Logical View (Layer-3)



34.4 Service Configuration

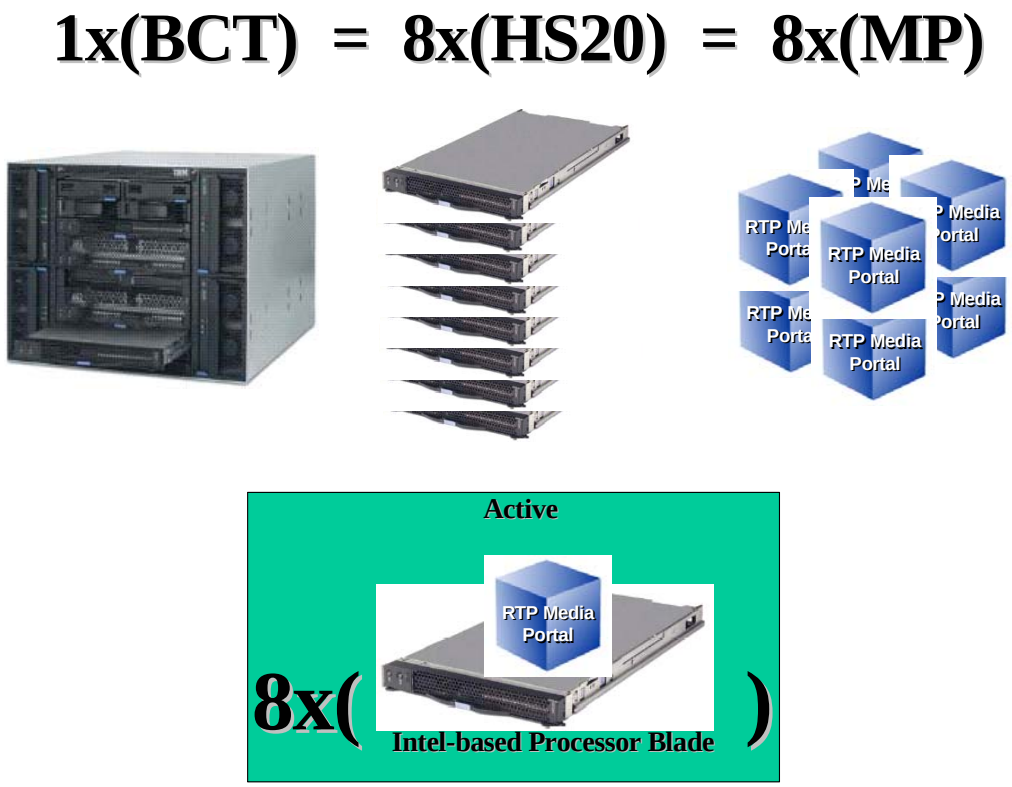
34.4.1 Overview

The introduction of the BladeCenter-T RTP Media Portal represents a major change in how the RTP Media Portal is viewed. The software re-architecture required by the BladeCenter-T RTP Media Portal essentially abstracted the functionality provided by the RTP Media Portal from the underlying platform – effectively establishing the RTP Media Portal as a service that is independent of a fixed relationship with its supporting hardware. Further, the introduction of the N+1 fault tolerance framework adds yet another dimension to the RTP Media Portal. As a result, this feature introduces more than a new hardware platform into the product, it introduces a major new configuration of the RTP Media Portal Service.

The BladeCenter-T RTP Media Portal can be configured to operate as either a collection of independent service instances (“Stand-Alone”), or as an N+1 fault tolerant service cluster (“Clustered”).

When configured as a collection of stand-alone service instances, the BladeCenter-T can support the execution of up to eight (8) independent non-redundant instances of the RTP Media Portal Service (refer to the following figure).

Figure 9 Stand-Alone RTP Media Portal Service Instances (Chassis View)



When configured as a redundant N+1 fault-tolerant service cluster, the BladeCenter-T can support the execution of up to seven (7) active instances of the RTP Media Portal Service and one (1) hot standby instance that is ready to assume the active sessions for any of the active instances (refer to the figure that follows on the next page).

These advances required adaptations to RTP Media Portal configuration to accommodate the new paradigms: RTP Media Portal as a service, and the N+1 fault tolerant RTP Media Portal Service Cluster. Adaptations were performed within the constraints of the capabilities and limitations of the MCP Management System. The resulting changes provide:

- The ability to configure the BladeCenter-T RTP Media Portal as a Stand-Alone Service Instance.

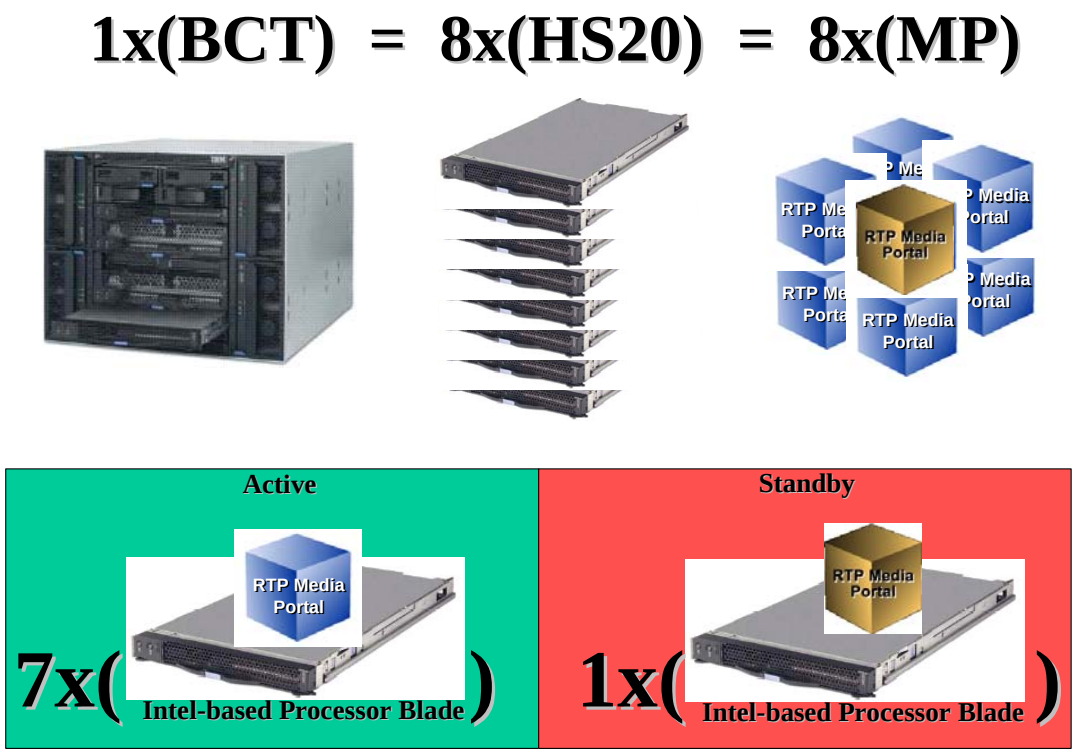
- The ability to configure the BladeCenter-T RTP Media Portal as an N+1 Fault Tolerant Service Cluster.
- The ability to manage the BladeCenter-T RTP Media Portal as a set of distinct network elements (unfortunately there are no Cluster-level management capabilities – management of the Cluster is achieved through the coordinated management of the individual Cluster members).

Fortunately, the configuration adaptations appear as minor changes to the configuration data as presented in the Management Console and so a consistent interface can be be presented for all varieties (the Motorola CPX8216-T introductory platform, and the new IBM BladeCenter-T platform) and configurations (Stand-alone, and Clustered) of the RTP Media Portal. In fact the configuration of the original Motorola CPX8216-T-based RTP Media Portals is unchanged (there is one new configuration parameter added to the RTP Portal Network Element, but for legacy CPX8216-T sites it is left set to its default value of “null”), while the new BladeCenter-T RTP Media Portal utilizes both pre-existing configuration structures (e.g. the RTP Portals Network Element for the conveyance of Engineering Parameters) and the adaptations made to configuration structures (e.g. the new “Clusters” entity in Network Data.

Additionally, both Stand-Alone and Clustered configurations of the BladeCenter-T RTP Media Portal are configured exactly the same – the differentiation being that the Stand-Alone is configured as a “1+0” (1 active instance, and no standby instances) Service Cluster. The real differences between the Stand-Alone and Clustered configurations is in their run-time characteristics and reaction to faults.

All of this is discussed in more detail in the following sections.

Figure 10 N+1 Fault Tolerant RTP Media Portal Service Cluster (Chassis View)



34.5 BladeCenter-T RTP Media Portal Configuration

34.5.1 Overview

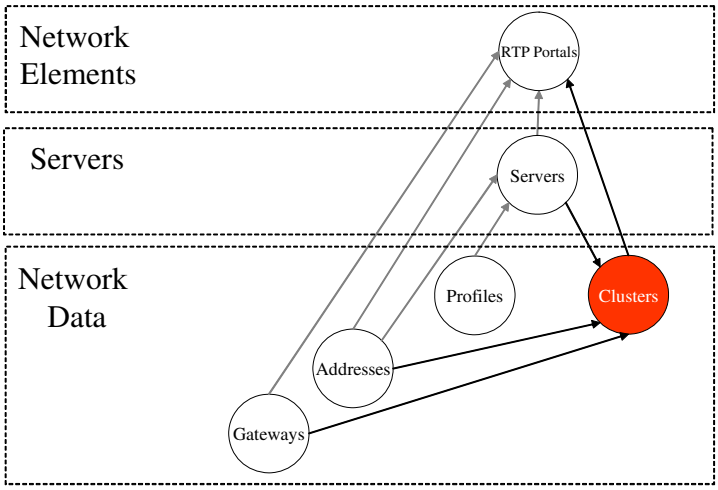
Pre-existing RTP Media Portal configuration structures remain intact for continued support of legacy Motorola CPX8216-T RTP Media Portal deployments. These pre-existing structures consisted of Network Data (specifically “Addresses”, “Gateways”, and “Profiles”), Servers, and Network Elements (where all data constituting an RTP Media Portal was combined together in the RTP Portal Network Element).

The BladeCenter-T RTP Media Portal builds on top of pre-existing configuration structures as follows (refer to the following figure):

- Network Data: the new “Clusters” entity is created in Network Data. The new “Clusters” entity contains all of the information required to configure a RTP Media Portal Service Cluster. As Network Data, “Clusters” is delivered over the MCP OAM Framework to all BladeCenter-T RTP Media Portal nodes.
- Servers: unaffected.
- Network Elements: The “RTP Portal” Network Element is enhanced with the addition of a new field “Cluster” that references a specific entry in the

new Network Data “Clusters” entity. The new “Cluster” field provides the means for identifying an RTP Media Portal’s membership in an N+1 Fault Tolerant Service Cluster.

Figure 11 RTP Media Portal Service: Data Relationahips



The new Network Data “Clusters” entity contains configuration information for RTP Media Portal Service Clusters. This configuration information includes the Common Service Data for the Cluster, the Service Instance Data, and the Fault Tolerant Framework Data (refer to the following table). The Common Service Data is a set of configuration parameters replicated from the RTP Portal Network Element’s “Bladerunner” information. The Service Instance Data defines the parameters that are unique to each active instance of the service. The Fault Tolerance Framework Data defines the parameters that define the Service Cluster.

Table 4: RTP Media Portal Service Cluster: Configuration Data

Data Type	Parameter Name	Parameter Type	Parameter Description
Common Service Data	Cluster Name		Cluster name or id or both - something unique for this cluster. Convention: <Cxx>+<name>
	Default Gateway		Pull-down of available Gateways (from Network Data) that overrides the "Default Gateway" specified in the RTP Portal NE data.
	CallLegs		Overrides "CallLegs" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	CriticalPortUsageAlarmLevel		Overrides "CriticalPortUsageAlarmLevel" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	IdleSessionAuditPeriod		Overrides "IdleSessionAuditPeriod" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	LongCallDuration		Overrides "LongCallDuration" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	LongIdleDuration		Overrides "LongIdleDuration" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	MajorPortUsageAlarmLevel		Overrides "MajorPortUsageAlarmLevel" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	MinorPortUsageAlarmLevel		Overrides "MinorPortUsageAlarmLevel" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	PollTimerDelay		Overrides "PollTimerDelay" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	LongCallDuration		Overrides "LongCallDuration" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	StaticRTPPorts		Overrides "StaticRTPPorts" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	Number of Port		Overrides "Number of Port" parameter present in the RTP Portal NE "Blade" Data.
	Min Port Value		Overrides "Min Port Value" parameter present in the RTP Portal NE "Blade" Data.
	Max Port Value		Overrides "Max Port Value" parameter present in the RTP Portal NE "Blade" Data.
	Session Manager		Pull-down of available Servers (from Servers) that overrides the "Session Manager" Data specified in the RTP Portal NE.*There can be multiple occurrences of this data*
	Discovery Probe Timer Period		Integer field specifying the frequency of the periodic MPCP RSIP to the controlling Call Servers. The value entered into this field overrides the value for the "Discovery Probe timer" field for each instance of "Session Manager" Data specified in the RTP Portal NE.

Fault Tolerance Framework Data	Multicast IPaddr		These two parameters uniquely define this Cluster. They represent the Peering Plane used by this Cluster for the establishment of the reliable messaging framework. The reliable messaging framework is used to carry the election protocol, checkpoint run-time service data to the Standby Service Instance, and to monitor member status.
	Multicast Port		
	Heartbeat Period		Frequency of heartbeat status check.
Service Instance Data	{N}		{implied} The number of instances of "Service Data" implies the value of "N". This correlates exactly to the expected number of servers (which is "N+1").
	Instance Name		Name of this Service Instance. Convention: <Cluster-Name>+<Ixx>+<Instance-Name>
	Controlipaddr		Pull-down of available IPaddrs (from Network Data:Addresses). This parameter provides a unique IPaddr for the RTP Media Portal Service that is different from the platform IPaddr. This is the result of abstracting the RTP Media Portal Service from the platform, and is used for conveyance of MPCP messages.
	ControlNetMask		Defines the Control-plane subnet for this Service Instance
	Net1MediaIP		Pull-down of available IPaddrs (from Network Data:Addresses) that overrides "Net1 Media IP" parameter present in the RTP Portal NE "Blade" Data. This defines one of the two media IPaddrs that establish presence for this service in the Media-Plane.
	Net1NetMask		Overrides "Net1NetMask" parameter present in the RTP Portal NE Config Parm Group "BladeRunner". Defines the Media-plane subnet for this Service Instance.
	Net2MediaIP		Pull-down of available IPaddrs (from Network Data:Addresses) that overrides "Net2 Media IP" parameter present in the RTP Portal NE "Blade" Data. This defines one of the two media IPaddrs that establish presence for this service in the Media-Plane.
	Net2NetMask		Overrides "Net2NetMask" parameter present in the RTP Portal NE Config Parm Group "BladeRunner". Defines the Media-plane subnet for this Service Instance

34.5.2 Procedural Overview

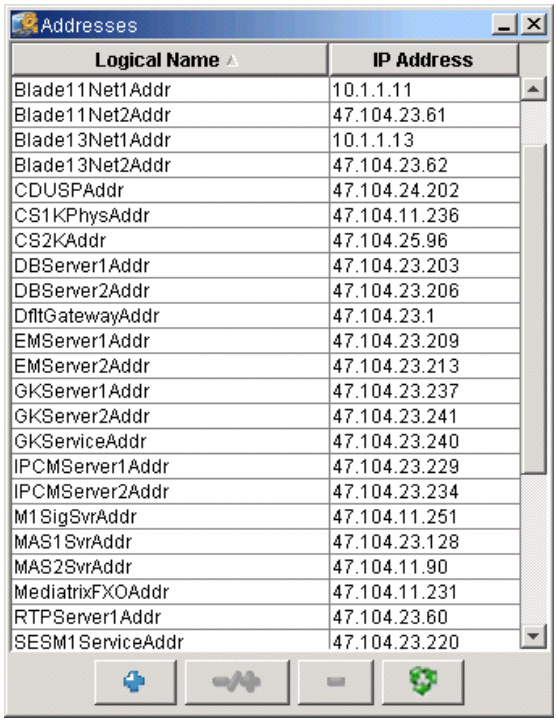
The BladeCenter-T RTP Media Portal is configured using the MCS System Management Console, and is accomplished through the use of the new “Clusters” entity in the Network Data, and a new field in the RTP Portals Network Elements (the new field references an entry in the “Clusters” Network Data to specify cluster membership). Refer to the following figure.

Figure 12 System Management Console: Affected Data Structures

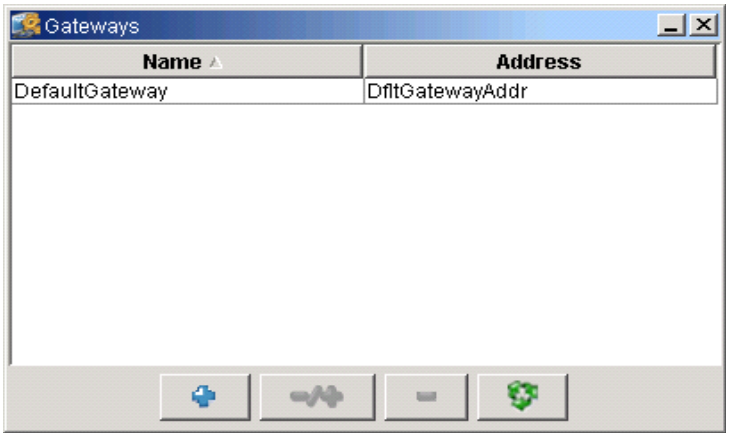
Procedurally, the BladeCenter-T RTP Media Portal is configured in a fashion similar to that used to datafill the CPX8126-T RTP Media Portal – with some additional steps that are necessary to include the creation/population of the new data structures:

Step 1: Datafill Supporting Parameters
At this initial stage all new referenced data must be entered into the system:

- Enter all new IP addresses into Network Data::Addresses.



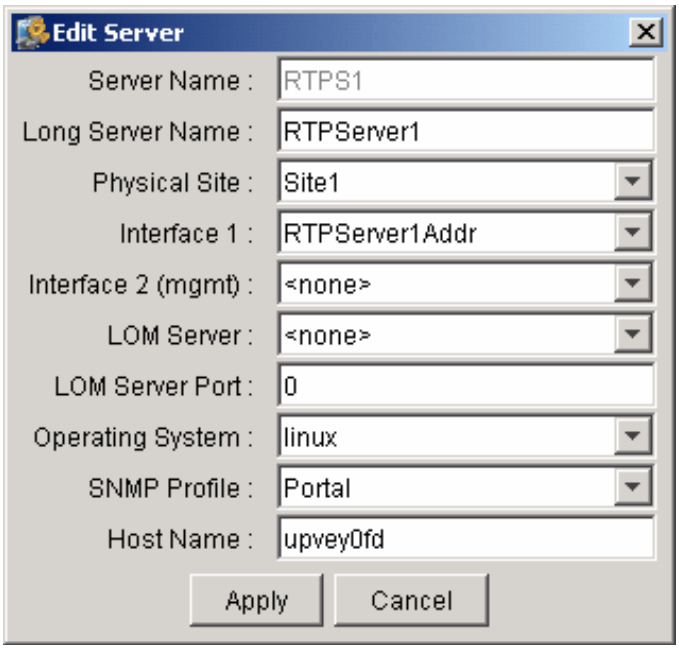
- Enter all new Gateways into Network Data::Gateways.



Note: There are no changes to the structure of this data.

Step 2: Datafill "Servers" Parameters
This stage of configuration creates a logical representation of a Server within which to group together all the data that defines a Server including physical IP address associations (the physical IP address was actually assigned during installation and commissioning):

- Datafill the “Interface1” field (pick-list of datafilled IP “Addresses”) with the intended physical IP address for each Blade Server in the BladeCenter-T chassis. This IP address is the bond0 physical address on the Blade Server – and is also used to represent the Blade Server and the RTP Media Portal Service Instance in the MCS OAM System.

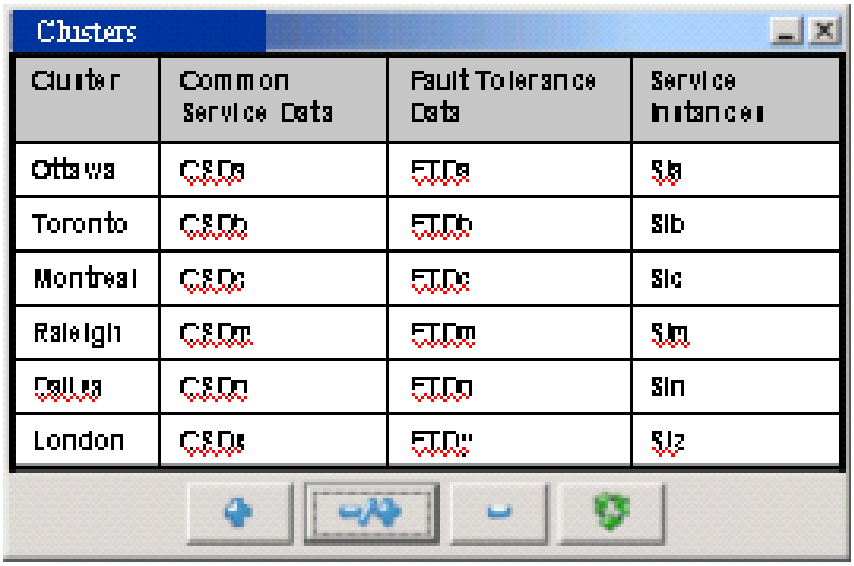


Note: There are no changes to the structure of this data.

Step 3: Datafill “Clusters” Entities
This stage of configuration creates a logical representation of the Service Cluster within which to group together all the data that defines the cluster.

The first step is to create a new Service Cluster:

- Open the “Clusters” window in Network Data, and then click the “+” button to create a new Service Cluster.



Once created the new Service Cluster can be populated with the parameters that uniquely identify this cluster as well as all of the parameters that define the service characteristics for this cluster (refer to the following figure):

- Common Service Data must be supplied that defines the operating parameters of the service instances (all service instances in a cluster run the same service configuration to maintain service consistency):
- Fault Tolerance Framework Data must be supplied to define the characteristics of the channel used for intra-cluster communication between all cluster members.
- Service Instance Data is where each of the RTP Media Portal Service Instances is defined (i.e. the MPCP control IP address, and up to two media IP addresses). There is one entry per Service Instance – this constitutes the “N” in the N+1 Fault Tolerance strategy. Refer to the second figure that follows for sample screenshots of adding a Service Instance.

Figure 13 New Network Data: Clusters

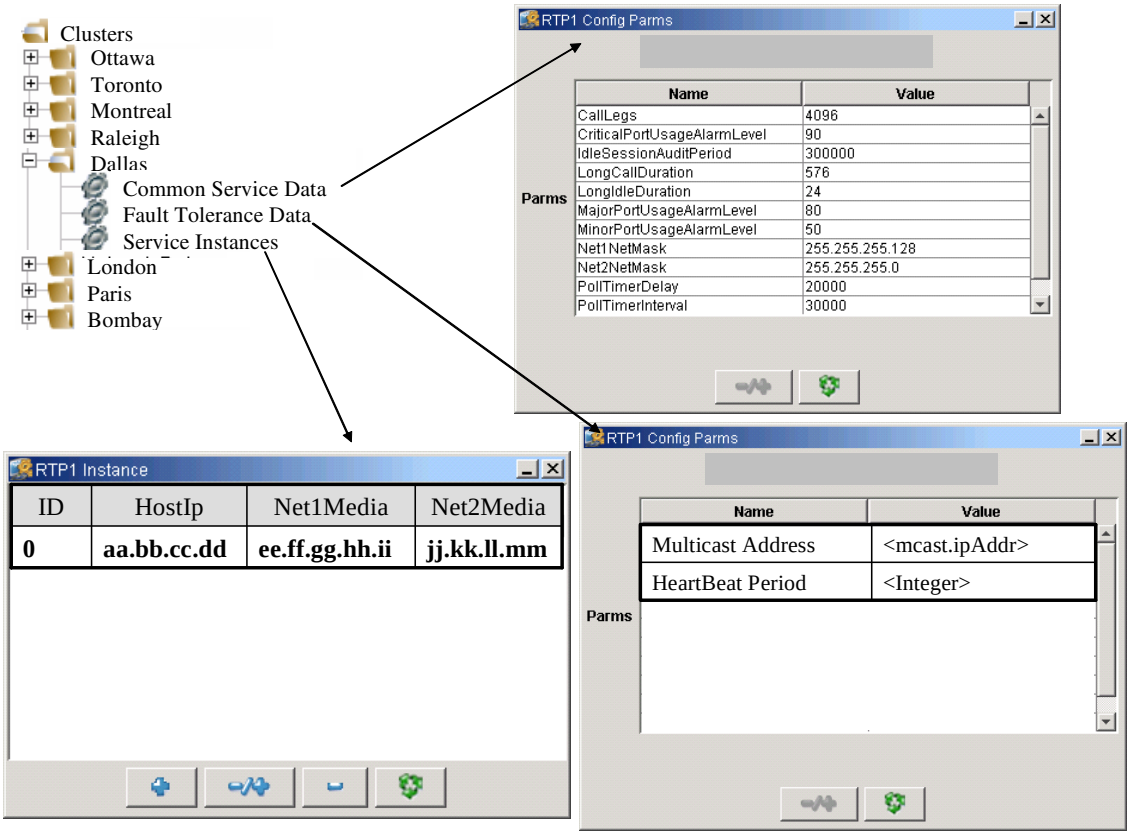
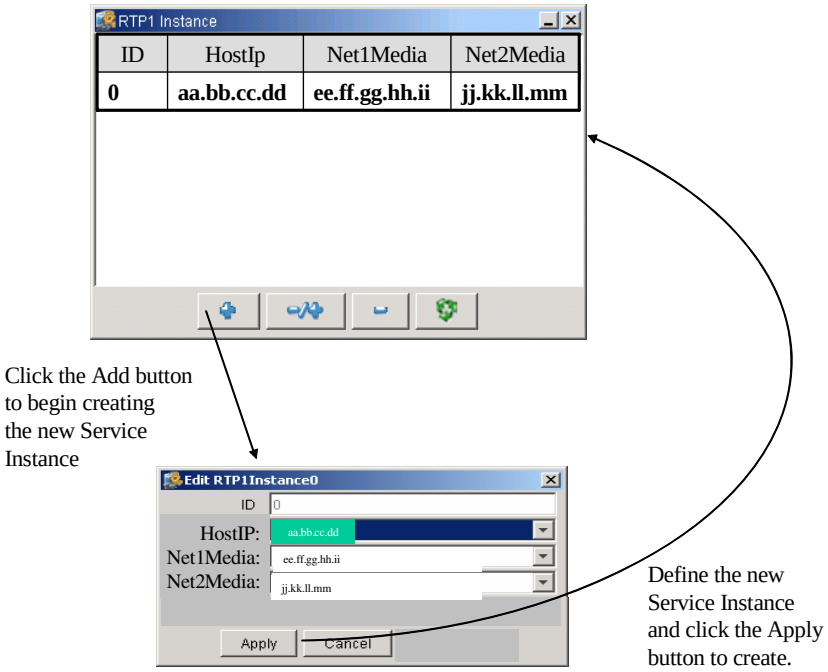


Figure 14 Clusters (Network Data): Adding a Service Instance



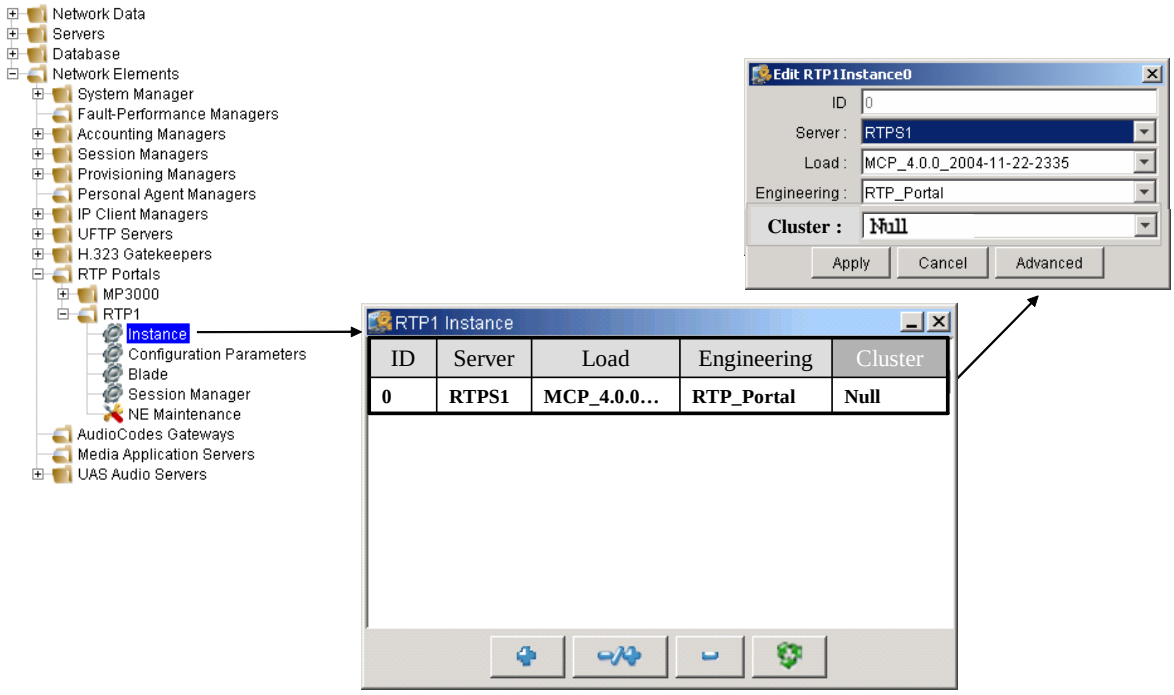
Step 4: Datafill "RTP Portals" Network Elements

As for the CPX8216-T based RTP Media Portal, the RTP Portal Network Element is the most fundamental configuration data structure. The RTP Portal Network Element provides the BladeCenter-T RTP Media Portal with: Engineering parameters, and a point of attachment into the MCS OAM Framework. It is the RTP Portal NE that: enables the deployment of the RTP Media Portal software, provides the channel for telemetry (Logs, Alarms, and Operational Measurements), and enables the maintenance events (Start, Stop, and Kill).

Also, in the context of the BladeCenter-T RTP Media Portal, each RTP Portal Network Element represents one Blade Server. This one-to-one mapping is due to the fact that the RTP Portals NE identifies the target server (through reference to an entry in the "Servers" Configuration Data).

This stage of configuration also provides the opportunity to specify membership in a BladeCenter-T RTP Media Portal Service Cluster through use of the new Cluster field in the RTP Portal NE data. Refer to the following figure.

Figure 15 RTP Portal NE: Specification of Cluster Membership



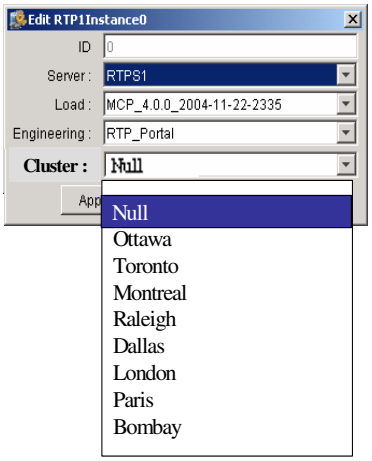
The new RTP Portal NE Cluster field is populated by selecting from a pick list. The pick-list contains an entry for each of the Clusters defined in the Network Data (and a “null” entry). Refer to Figure 62 on page 129. Each Server participating in a Service Cluster (identified within the RTP Portal Network Element data structure) is assigned Cluster membership in this manner – thuereby establishing the “N+1” servers hosting the Cluster.

Cluster membership is only available to the BladeCenter-T RTP Media Portal – the legacy CPX8216-T RTP Media Portal cannot be a member of a Service Cluster and must have “null” selected in the new “Cluster” field that appears in the Instance data of the RTP Portal NE.

Both BladeCenter-T RTP Media Portal configurations (the Stand-alone and the Service Cluster) must be configured as members of a Cluster. In the case of the BladeCenter-T RTP Media Portal Stand-alone, configuration is performed such that a “1+0” (1 Active Service Instance and 0 Standby Service Instances) cluster is created. All Clusters are uniquely defined by the combination of multicast IP Address and multicast port specified in the Fault Tolerance Data in the new “Clusters” Network Data, but what makes the Stand-Alone configuration unique is that there is onle one Service Instance configured.

Note: The legacy CPX8216-T RTP Media Portal will fail to start if it detects Cluster configuration in its datafill.

Figure 16 RTP Portal NE: Cluster Pick-List



35: Configuration (CN): A00009822

35.1 Feature Name

General Security Log When the User Logs Out

35.2 Hardware and Software Requirements

No new hardware dependencies has been introduced by this feature.

35.3 Hardware and Software Requirements

The server piece of this application at this time requires an oracle database server to be in place on the server machine.

35.4 Initial Configuration

SN09 IEMS Central SS software

Oracle

35.5 Memory Requirements

The statistics that follow were taken at a stressed state. The database was populated with 6000 session entries and a CSM Report Client was configured to pull this data every 10 seconds.

RAM Usage: 10 M (1 M with 200 records)

Note: CSMEngineNotifier & CSMEngineReport are servlets. They reside within the Tomcat process and therefore we are not adding in the existing JRE overhead calculations.

Application Code Disk Usage: 2066 K (du -s -k /opt/nortel/CSReport)

Application Data Disk Usage: 0

The CSM design heavily utilized the database for storage retention. We do not keep any custom CSM data in the /data partition.

Application Database Usage:

The CSMDB_TS - with 6000 entries - used 720,896 Bytes.

35.6 Upgrade Considerations

At this time, this feature will not impact upgrades.

35.7 Data schema

A new tablespace called CSM_TS will be added to the oracle database server on the authentication machine to support this feature. In this tablespace will reside two tables, Activity & Version.

35.8 Element Management

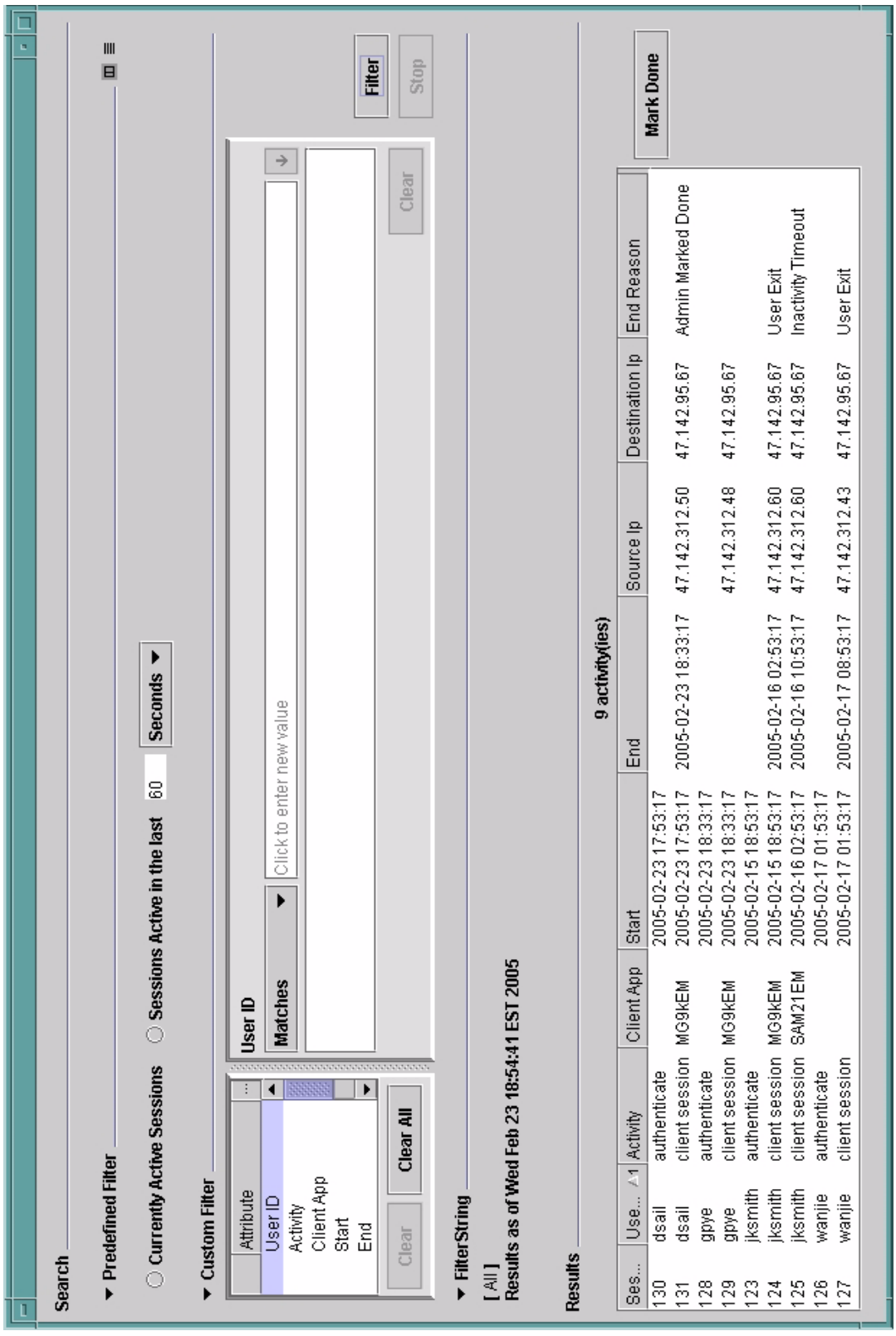
35.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Client Session Monitor	New

35.8.2 GUI information

35.8.2.1 GUI name: Client Session Monitor


Search
Predefined Filter
Currently Active Sessions
Sessions Active in the last
60
Seconds
Custom Filter
Attribute
User ID
Activity
Client App
Start
End
Clear
Clear All
User ID
Matches
Click to enter new value
Clear
Filter
Stop
FilterString
[All]
Results as of Wed Feb 23 18:54:41 EST 2005
Results
9 activity(ies)
Mark Done
Ses...
Use...
Activity
Client App
Start
End
Source Ip
Destination Ip
End Reason
130 dsail authenticate 2005-02-23 17:53:17
131 dsail client session MG9kEM 2005-02-23 17:53:17 2005-02-23 18:33:17 47.142.312.50 47.142.95.67 Admin Marked Done
128 gpye authenticate 2005-02-23 18:33:17
129 gpye client session MG9kEM 2005-02-23 18:33:17 47.142.312.48 47.142.95.67
123 jksmith authenticate 2005-02-15 18:53:17
124 jksmith client session MG9kEM 2005-02-15 18:53:17 2005-02-16 02:53:17 47.142.312.60 47.142.95.67 User Exit
125 jksmith client session SAM21EM 2005-02-16 02:53:17 2005-02-16 10:53:17 47.142.312.60 47.142.95.67 Inactivity Timeout
126 wanjie authenticate 2005-02-17 01:53:17
127 wanjie client session 2005-02-17 01:53:17 2005-02-17 08:53:17 47.142.312.43 47.142.95.67 User Exit

35.8.2.1.1 Functional description

The CSM GUI client provides a report that will give the security user the ability to view the historical client sessions for the users. The report will by default populate with the currently active sessions. However, the user has the ability to configure the display criteria. The report will refresh the displayed contents once every 60 seconds.

The CSM GUI client can be launched via a menu on IEMS or directly accessing the URL (jnlp) for the client. The CSM GUI is hooked into the common LoginServlet code. If a user has an authentication session active, the GUI will be displayed. However, if an authentication session is not active, the user will be prompted for user and password via the common login dialog.

Once logged in the users group levels will be checked - the GUI report can only be viewed by those users which are in the SEC* group. Any user not in that group will not be allowed entry to the report. Also, the ability to mark a client session as ended will only be accessible to those users of the group SECADM.

35.8.2.1.2 GUI usage and implications

This UI will be used to display current client application sessions as well as historical lifetime of client application sessions by user.

When the GUI first is displayed - the report shown will be for all current application sessions. This report will update every 60 seconds to maintain accuracy. The user has the ability to modify the filter (search) criteria for the report. If the users wishes to change a criteria they simply modify the filter parameters and hit the ‘Filter’ button. This will repopulate the list with the data matching the new filter criteria. The criteria the report is generated with - and the time of generation - are clearly displayed in the FilterString area.

In setting the filters, the user may choose either to use a predefined criteria or to create a custom criteria from the available attributes. The two predefined criteria filters available are ‘currently active sessions’ and ‘activity within the last <timeperiod>’.

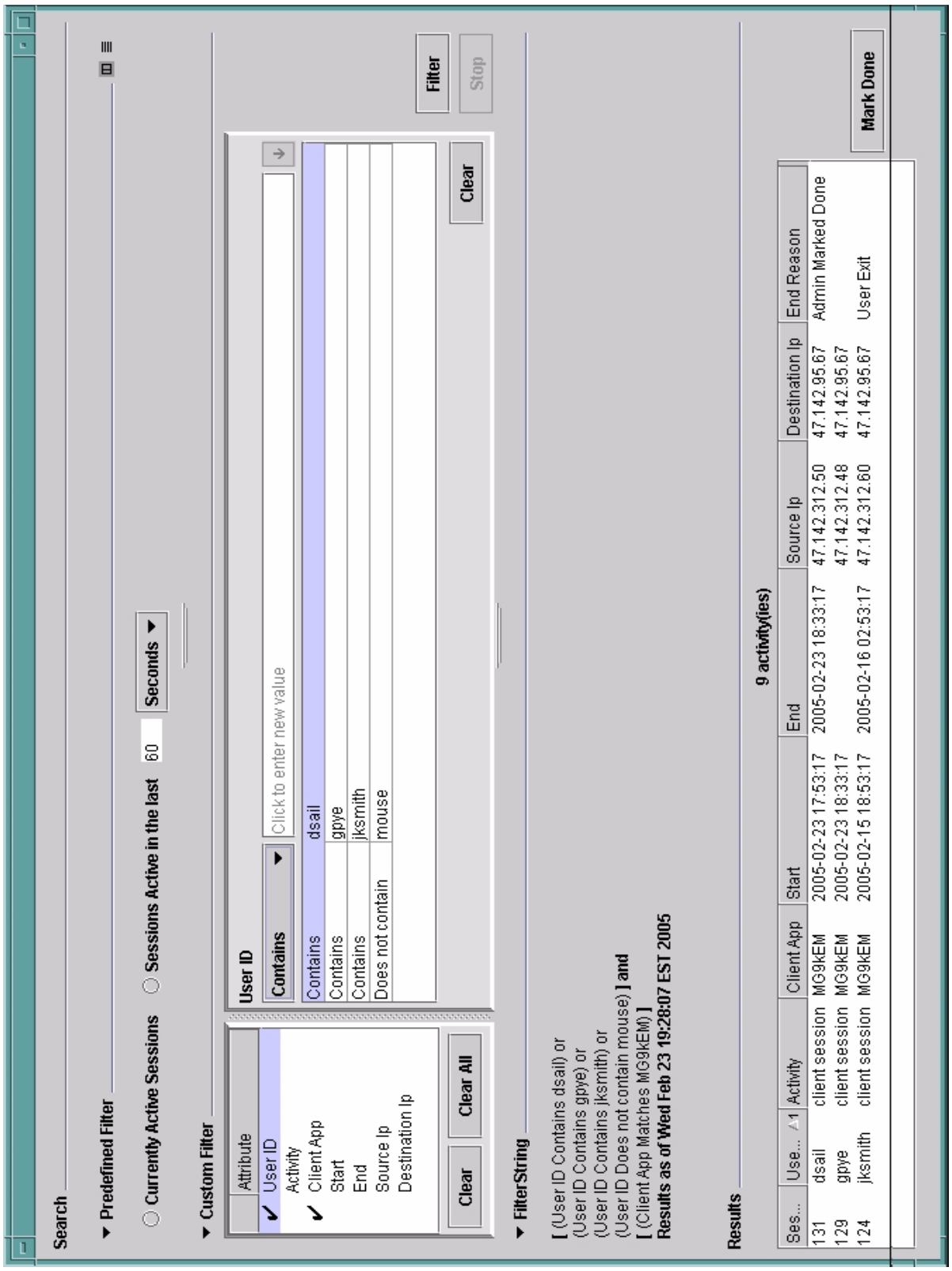
The predefined filter ‘currently active sessions’ will populate the custom filter area with the correct settings to query on active sessions. The user then hits ‘Filter’ and the report will update with this criteria.

The predefined filter ‘activity within....’ allows the user to request the report display all activity that has occurred in an interval prior to the report generation. The user may enter the numeric value for the time interval and the period type from a choice option of “Seconds”,”Minutes”,”Hours”,”Days”. Once the user has selected their settings - they simply hit the “Filter” button and the report will update.

The “Custom Filter” area allows a user to build a custom criteria from the available attributes. For fields which are strings such as UserID, Activity, ClientApp, SourceIp and DestinationIp the criteria that can be used to match on are “Matches”, “Does not match”, “Contains”, “Does not contain”, “Starts with”.

For fields which are dates such as Start Activity and End Activity - the matching criteria are “Matches”, “Does not match”, “Before”, “After”, “Between”. The date requires the date format of YYYY-MM-DD HH:MM:SS. The exception is that the term “Current” can be entered in the field to indicate the current time and the turn “Null” can be entered to indicate the time is not yet set.

Once a user has decided a criteria is correct - they simply need hit “Filter” and the report will populate. The below snapshot shows a report that has criteria matching (and not matching) on user id - as well as Client Activity. The user simply selected the field to query upon - then the match criteria - entered the data in the text field that says “Click to enter new value” and hit return. The criteria is then added to the list of query items for that data element.


Search
Predefined Filter
Currently Active Sessions
Sessions Active in the last
60
Seconds
Custom Filter
Attribute
User ID
Activity
Client App
Start
End
Source Ip
Destination Ip
Clear
Clear All
User ID
Contains
Click to enter new value
Contains
dsail
Contains
gpye
Contains
jksmith
Does not contain
mouse
Clear
Filter
Stop
FilterString
[(User ID Contains dsail) or
(User ID Contains gpye) or
(User ID Contains jksmith) or
(User ID Does not contain mouse)] and
[(Client App Matches MG9kEM)]
Results as of Wed Feb 23 19:28:07 EST 2005
Results
9 activity(ies)
Ses...
Use...
Activity
Client App
Start
End
Source Ip
Destination Ip
End Reason
131 dsail client session MG9kEM 2005-02-23 17:53:17 2005-02-23 18:33:17 47.142.312.50 47.142.95.67 Admin Marked Done
129 gpye client session MG9kEM 2005-02-23 18:33:17 47.142.312.48 47.142.95.67
124 jksmith client session MG9kEM 2005-02-15 18:53:17 2005-02-16 02:53:17 47.142.312.60 47.142.95.67 User Exit
Mark Done

35.8.2.1.3 GUI size

Not Applicable

35.8.2.1.4 GUI fields

The following table lists fields for GUI:

Table 2 GUI field descriptions

Field	New or Changed	Entry	Explanation and action	Associated MIB entry
SessionID	New	String	This is the id that uniquely identifies a client activity session.	Table CSM_TS.Activity.SessionId
UserID	new	String - 8 char length	This is the login id of the user who initiated the session.	Table CSM_TS.Activity.UserId
Activity	new	String	Designates the type of activity - ex. Authentication or Client Session	Table CSM_TS.Activity.ActivityType
Client Application Name	new	String	The name of the client application that session denotes. (not applicable to authentication).	Table CSM_TS.Activity.AppName
Start Date	New	Date (YYYY-MM-DD HH:MM:SS)	This is the time the activity started.	Table CSM_TS.Activity.StartDate
End Date	New	Date (YYYY-MM-DD HH:MM:SS)	This is the time the activity ended. (Not applicable to authentication).	Table CSM_TS.Activity.EndDate
Source Ip	New	String [xxx.xxx.xxx.xxx]	This is the Ip Address of the machine from which the user launched the session. (Not applicable Authentication)	Table CSM_TS.Activity.SourceIp
Destination Ip	New	String [xxx.xxx.xxx.xxx]	This is the Ip of the machine from which the client application is loaded. (ex. MG9kEM Midtier)	Table CSM_TS.Activity.DestinationIp
End Reason	New	String	This is the reason the session ended. Reasons can be User Exited, Inactivity, etc.	Table CSM_TS.Activity.EndReason

35.8.2.1.5 Usage example

The Client Session Monitor will be initially displayed to the user populated with the entries indicating current active client sessions. The user has the ability to modify the report criteria by selecting new criteria and then hitting "Filter". Once "Filter" is hit the data list will repopulate with the results of the new query. The Query that the current data list applies to is displayed in the middle section of the form under "Filter String" and is timestamped with the last time the query was run.

In the case where a client session appears to still be active via the report - but the security user knows the session to no longer be active - the security user can mark that session as completed. The ability to mark a client session as ended will only be accessible to those users of the group SECADM. Marking a session as completed will not cause any actions outside the realm of this report. It will simply update the session activity in the database - it will not force a user off - end their session - etc. If a user is still active and their session is marked completed, when the user truly ends the session - the row will be updated with that actions end time.

The displayed report has the ability to sort by clicking on the column the user wishes to key the sort.

35.8.2.1.6 Context sensitive launching information

There are two methods of launching this client. The first will be from the IEMS security layer via a menu item.

The second will be via a url to the authentication machine. This url will be something along the lines of:

http://<ip>/ClientSessionManager.jnlp

If the user has already authenticated and that authentication session is still active, the CSM GUI will be immediately displayed. If there is not an authentication session currently active - the user will be prompted for their user name and password via the common login utility.

35.9 Security

35.9.1 Network configuration

None

35.9.2 Key management

None

35.9.3 Protocol

This CMS GUI will be a java client which is launched using the JavaWebStart client support software.

The messaging between the CMS GUI and the CMS Server will be via https.

35.9.4 Authentication

Access to the Client Session Monitor is for this feature will require the user to login and authenticate via the common login panel. The user must be a member of the sec* group.

35.10 Configuration Walkthrough

The CSMonitor Audit functionality keeps the session database from growing too large. All client monitor sessions, even after they are closed, are kept in the Client Session Monitor database to provide historical data of logins and logouts. The CSMonitor Audit functionality allows the user to configure when to poll the database for sessions to clean up and allows the criteria for clean up to be specified.The selection of sessions is strictly based on start time and may delete session which have not ended. Therefore, care must be taken to specify criteria so as not to delete any active sessions.

In order to configure the CSMonitor Audit and start the cleanup of sessions from the Client Session Monitor database, the following steps are performed:

1 - login to the IEMS security server as root

2 - enter the cli command

3 - select the Configuration option

4 - select the Succession Element Configuration option

5 - select the CSMCLEANUP Application Configuration option

6 - select the setCleanupTime option

7 - enter the amount of time for the CSMonitor Audit to poll the database for removal of sessions based on the criteria below, sessions are only removed when the CSMonitor wakes up after the time period specified. For example, if 24 hours is specified the CSMonitor Audit wakes up 24 hours from the time CSMonitor Audit is started and queries the database for sessions needing to be removed.

8 - select the setCleanupCriteria option

9 - select criteria for removal from the database. Max sessions per user criteria keeps the sessions based on start time for each user id. Time based criteria keeps sessions based on start time.

10 - if max criteria select above, skip to step 14

for time based criteria, enter the number of hours to keep sessions. For example, it 1 hour then any session started one hour prior to the audit polling are kept. If user x has two session one started at 10:00 and another started at 13:00 and the current time is 13:20 only the session started at 13:00 is maintained in the database. If user y has three sessions, first started at 12:21 and ended at 12:30. Second session started at 13:05 and the third session stared at 13:19. All three session for user y are kept. It is advisable to keep session at least 24 hours. Suggested is 7 days or 168 hours. Maximum is 30 days or 720 hours.

11 - select exit option, until no longer in CLI.

12 - restart CSMonitor_Audit for the changes to take affect (servrestart CSMonitor_Audit)

13 - done with configuration

14 - for max session per user based criteria, enter the maximum number of session to keep for each user. Go to step 11.

36: Configuration (CN): A00009839

36.1 Feature Name

Ability to apply patches during ESUP upgrade

36.2 Hardware and Software Requirements

No new hardware dependencies has been introduced by this feature.

With this feature ESUP will use the NTSimTool package to convert ".patch" files to ".tape" files.

36.3 Initial Configuration

N/A

36.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

36.5 Upgrade Considerations

N/A

36.6 Data schema (DS) (CM, MIBS, RDB)

N/A

36.7 Service Orders (SO) (CM & SESM)

N/A

36.8 Software optionality control (SOC)

N/A

36.9 Element Management

N/A

36.10 User interface changes

This feature brings some changes in user interactions. This feature will intoduce a new screen at the begining just **before** the existing screen where ESUP asks for media type. This new screen will prompt user to enter "upgrade type". The options will be:

1) Upgrade to higher release

2) Patch only upgrade

Following figure shows the new screen:

Figure 1 :New screen prompting user to enter upgrade type

```
================================================================
=
===              Enhanced SDM Upgrade Procedure
===
================================================================
=
===
===  Please select the upgrade type
===     1) Upgrade to higher release
===     2) Patch only upgrade
===
===     type 'abort' to abort the upgrade
================================================================
=

Upgrade Type >
```

If user selects option 1, then the “select media” screen comes next. If user selects option 2, then “select media” is bypassed as patches will always be taken from DISK-media only.

During an upgrade to higher release, ESUP gives user another prompt asking - whether he wants to install patches or not? If the user enters ‘yes’, ESUP prompts the user to enter the location of the patch filesets. These prompts comes **after** the “select media” screen. Following figure explains this scenario:

Figure 2 : New prompt asking for patches location

```
================================================================
===              Enhanced SDM Upgrade Procedure
===
===
================================================================
===
=== The following device has been selected to perform the
upgrade
===
===            Media Type: DISK
===
================================================================
Continue (yes/no) >yes

Please enter the directory location for [CS2E0090 NCL Load]
Enter 'go' to accept the default or 'abort' to abort the
upgrade.
   Directory (default:/swd/sdm/esd/) >go

[01:45:44] Examining load content of /swd/sdm/esd/ .... Com-
pleted.
[01:46:38] Verifying load content of /swd/sdm/esd/ .... Com-
pleted.
Do you want to install patches (yes/no/abort)? yes

Please enter the directory location for [CS2E0090 PATCHES]
Enter 'go' to accept the default or 'abort' to abort the
upgrade.
   Directory (default:/swd/sdm/esd/) >
```

During a patch-only upgrade, ESUP will bypass the “select media” screen. It will directly prompt the user to enter the location of patches. Following screen shows that:

Figure 3 :New prompt asking for patches location in patch-only upgrade

```
================================================================
=
===              Enhanced SDM Upgrade Procedure
===
================================================================
=
===
===  Please select the upgrade type
===     1) Upgrade to higher release
===     2) Patch only upgrade
===
===     type ‘abort’ to abort the upgrade
================================================================
=

Upgrade Type >2

Please enter the directory location for [CS2E0090 PATCHES]
Enter ’go’ to accept the default or ’abort’ to abort the
upgrade.
   Directory (default:/swd/sdm/esd/) >
```

36.11 OSSGate Interface Changes

N/A

36.12 Security

N/A

36.13 Configuration Walkthrough

N/A

37: Configuration (CN): A00009840

37.1 Feature Name

CBM IPSec Northbound Interface

37.2 Hardware and Software Requirements

SN09 or later SSFPS load (with NTIpSec package) for the CBM.

OSS supporting IPSec communication.

37.3 Initial Configuration

37.3.1 Security

Following are the high-level steps to enable security between OSS and the CBM.

- Load the CBM with SN09 or later version of SSPFS
- After logging into the CBM, the craftsperson will then invoke the CLI tool available as part of SSPFS and proceed to the option of configuring the IPSec/IKE parameters with the OSS details.
    - The user should not log from the target OSS machine onto the CBM to perform the IPSec/IKE configuration.
- Enable security on the OSS to secure the connection from OSS to the CBM

37.3.2 OSS

IPSec and IKE configuration parameters which are provisioned on the OSS must match the corresponding parameters on the CBM provisioned through the configuration interface bundled under the CLI tool.

37.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable

37.5 Upgrade Considerations

Not Applicable

37.6 Data schema (DS) (CM, MIBS, RDB)

Not Applicable

37.7 Service Orders (SO) (CM & SESM)

Not Applicable

37.8 Software optionality control (SOC)

Not Applicable

37.9 Element Management

37.9.1 New/modified GUI

Not Applicable

37.9.2 GUI information

Not Applicable

37.9.3 CLUI Interface

This interface is bundled into CLI tool available as part of SSFPS.

This interface will be accessible from “IP configuration” menu entry available in the list of Configuration options. The following figure (Figure 1) indicates the sequence of menu options navigated in reaching the IPSec/IKE configuration interface.

Figure 1 : CLI Menu Options

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select - 2

Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)
19 - backup_config (Backup Configuration)

select - 6

IP Configuration
 1 - config_router (Configure Default Router and Netmask)
 2 - config_data (Configure System Data IP Addresses)
 3 - ipsecike_config (Configure IPSec/IKE Rules)

 X - exit

select - 3

 X - exit
```

37.9.3.1 Functional Description

Figure 2 indicates the screen snapshot when the IPSec/IKE configuration interface menu option is exercised from the list of options displayed in the IP Configuration menu (option 3 as indicated in Figure 1).

Figure 2 : IPSec/IKE Configuration Interface

```
IPSec/IKE Configuration Menu
 1 - IPSec Configuration
 2 - IKE Configuration

 X - Exit

 Select -
```

37.9.3.2 CLUI usage and implications

This activity provides an easy to use IPSec configuration interface on the CBM for configuring IPSec/IKE parameters.

Initially, IPSec entries are created by entering the necessary parameters. If the craftsperson has chosen to use “ipsec” action,the next step would be to create a corresponding IKE entry using the necessary parameters.

37.9.3.3 IPSec configuration interface

The following figure (Figure 3) lists the screen snapshot when IPSec configuration option is chosen from the IPSec/IKE configuration menu initially displayed.

Figure 3 : IPSec Configuration Interface

```
IPSec Configuration Menu
 1  -  Add IPSec entry
 2  -  Delete IPSec entry
 3  -  List All IPSec entries

 X  -  Exit

Select -
```

37.9.3.3.1 IPSec fields

The following table lists the parameters which would accepted by the interface and the valid options for each of these parameters.

Table 1 : IPSec field descriptions

Field	Entry	Explanation and Action
Remote Address	A numeric internet IP address of the form : www.xxx.yyy.zzz	Source address on incoming packets and destination address on outgoing packets
Remote Port	1-65535,all	IP port of the remote system communicating with the server
Local Address[a]	A numeric internet IP address of the form : www.xxx.yyy.zzz	Destination address on incoming packets and source address on outgoing packets
Local Port	1-65535, all	IP Port of this server
Upper Layer Protocol	any, udp,tcp and icmp	Determines which protocol traffic this entry is matched against
Direction	in, out and both	Determines whether this entry is for inbound or outbound traffic
Action	bypass,drop and ipsec	Determines the action to be taken when the traffic pattern is matched
ESP Encryption	none, any, NULL, DES, 3DES	Encryption Algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to “ipsec”

Table 1 : IPSec field descriptions

Field	Entry	Explanation and Action
ESP Authenticaion	none,any, SHA1, MD5	Authentication Algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to “ipsec”
AH Authentication	none,any, SHA1, MD5	Authentication algorithm that will be used to apply the IPSec AH protocol to outbound datagrams and verify it to be present on inbound datagrams, Only valid when action is set to “ipsec”

a. The Local Address would be cluster IP address if the system is a HA configuration. If the system is having a simplex configuration, the local address would be the address of this node.

37.9.3.3.2 IPSec Add Entry Example

The following figure (Figure 4) shows screen snapshot for IPSec Add entry option.

Figure 4 : IPSec adding a new rule

```
Enter the Remote IP Address   : 47.135.214.62
Enter the Remote Port No [1-65535,all] : all
Enter the Local IP Address [47.135.214.127] :
Enter the Local Port No [1-65535,all] : all
Enter the Upper Layer Protocol [any,udp,tcp,icmp] : any
Enter the Direction [in,out,both] : both
Enter the Action [ipsec,drop,bypass] : ipsec
Enter the ESP Header
  Authentication Algorithm [md5,sha1,none,any] : sha1
  Encryption Algorithm [none,NULL,des,3des,aes,blowfish] : 3des
Enter the AH Header
  Authentication Algorithm [md5,sha1,none,any] : md5
```

The following figure (Figure 5) captures the screen snapshot of the confirmation prompt for IPSec add entry screen.

Figure 5 : IPSec add entry confirmation screen

Do you wish to add the following IPSec configuration Information

Remote IP Address : 47.135.214.62
Remote Port No. : all
Local IP Address : 47.135.214.127
Local Port No. : all
Upper Layer Protocol : any
Direction : both
Action : ipsec
ESP Encryption Algorithm : 3des
ESP Authentication Algorithm : sha1
AH Authentication Algorithm : md5

Select [save, edit, abort] -

The following figure (Figure 6) captures the screen snapshot when the values entered for a new IPSec rule through add option is being edited before committing to the database.

Figure 6 : IPSec Add entry - Edit option

```
Press ENTER to continue with the current option

Remote IP Address [47.135.214.62] :
Remote Port No. [all] :
Local IP Address [47.135.214.127] :
Local Port No. [all] :
Upper Layer Protocol [any] :
Direction [both] :
Action [ipsec] :
ESP Encryption Algorithm [3des] :
ESP Authentication Algorithm [sha1] : md5
AH Authentication Algorithm [md5] : sha1

Do you wish to add the following IPSec configuration Information

Remote IP Address              : 47.135.214.62
Remote Port No.                : all
Local IP Address               : 47.135.214.127
Local Port No.                 : all
Upper Layer Protocol           : any
Direction                      : both
Action                         : ipsec
ESP Encryption Algorithm       : 3des
ESP Authentication Algorithm : md5
AH Authentication Algorithm  : sha1

 Select [save, edit, abort] -  save

Configuration successfully completed

For downstream configuration refer to instructions placed
in downstream.ipsec file in /etc/inet/remotesystem/solaris directory
```

37.9.3.3.3 IPSec List Entry Example

The following figure (Figure 7) shows screen snapshot when the list option is exercised.

The rules will be listed in the order in which they are listed in the IPSec configuration file (ipsecinit.conf).

Figure 7 : IPSec List Entry Output

```
--------------------------------------------------------------------------------
indexID      raddr          laddr             lport    rport    dir  status
--------------------------------------------------------------------------------
 1       47.135.214.62  47.135.214.127   all      all      both  up
 2       47.135.214.63  47.135.214.127   all      all      both  down


Enter the indexID of rule to be detailed (x to exit) - 2

Remote IP Address              : 47.135.214.63
Remote Port No.                : all
Local IP Address               : 47.135.214.127
Local Port No.                 : all
Direction                      : both
Action                         : ipsec
ESP Encryption Algorithm       : 3des
ESP Authentication Algorithm : sha1
AH Authentication Algorithm  : sha1

Enter the indexID of rule to be detailed (x to exit) -
```

37.9.3.3.4 IPSec Delete Entry Example

The following figure (Figure 8) shows screen snapshot when the delete option is exercised from IPSec configuration interface.

Figure 8 : IPSec Delete Entry Output

```
-------------------------------------------------------------------------------
indexID     raddr           laddr           lport    rport    dir  status
-------------------------------------------------------------------------------
 1      47.135.214.127  47.135.214.62   all      all      both  up
 2      47.135.214.130  47.135.214.62   all      all      both  down

 Enter the indexID of rule to be deleted (x to exit) - 2

Remote IP Address             : 47.135.214.130
Remote Port No.               : all
Local IP Address              : 47.135.214.62
Local Port No.                : all
Direction                     : both
Action                        : ipsec
ESP Encryption Algorithm      : 3des
ESP Authentication Algorithm : sha1
AH Authentication Algorithm  : sha1

Do you wish to delete the above ipsec rule
Select [Yes, No, Exit(x)] :
```

37.9.3.4 IKE Configuration Interface

The following figure (Figure 9) lists the screen snapshot when IKE configuration option is chosen from the IPSec/IKE configuration menu initially displayed.

Figure 9 : IKE Configuration Interface

```
IKE Configuration Menu
 1  -  Add IKE entry
 2  -  Delete IKE entry
 3  -  List IKE entries
 4  -  Change Preshared key for IKE entry

 X  -  Exit

Select -
```

37.9.3.4.1 IKE Fields

The following table lists the parameters which would accepted by the interface and the valid options for each of these parameters.

Table 2 IKE Field Descriptions

Field	Entry	Explanation and Action
Remote Address	A numeric internet IP address of the form : www.xxx.yyy.zzz	IP Address of the remote system cmmunicating with this server
Local Address	A numeric internet IP address of the form : www.xxx.yyy.zzz	IP Address of this server
Oakley Group	1 (768 bit), 2 (1024 bit) or 5 (1536 bit)	The Oakley Diffie-Hellman group used for IKE Security Association key derivation
Authentication Method	Preshared	Authentication method used for IKE phase 1.
Encryption	DES, 3DES	Specifies the encryption algorithm for a security association
Authentication	SHA1, MD5	Specifies the authentication algorithm for a security association
PFS Group ID	0 (do not use Perfect Forward Secrecy for IPSec SAs), 1(768 bit), 2(1024 bit),5(1536 bit)	Oakley Diffie-Hellman group used for IPSec Security Association key derivation
Preshared Key File	String (file name with full path)	Specifies the file with complete path which would contain the preshared key. This file would contain the preshared key for this Security Association.

Table 2 IKE Field Descriptions

Field	Entry	Explanation and Action
IKE Lifetime	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days	Specifies the lifetime for an IKE phase 1 Security Association
IPSec Lifetime	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days	Specifies the lifetime for an IPSec Security Association

37.9.3.4.2 IKE Add Entry Example

The following figure (Figure 10) shows screen snapshot for IKE Add entry option.

Figure 10 : IKE adding a new rule

```
Enter the Remote IP Address : 47.135.214.62
Enter the Local IP Address [47.135.214.127] :
Enter the Oakley Group [1,2,5] : 2
Enter the Authentication Method [preshared] : preshared
Enter the Encryption Algorithm [des, 3des] : 3des
Enter the Authencation Algorithm [md5, sha1] : sha1
Enter the PFS Group ID [0,1,2,5] : 0
Enter the IKE Lifetime value : 14400
Enter the IKE Lifetime unit [secs,min,hrs] : secs
Enter the IPSec Lifetime Value : 14400
Enter the IPSec Lifetime unit [secs,min,hrs] : secs
Enter the IKE Preshared Key file location (full path) : /tmp/arun1
```

The following figure (Figure 11) captures the screen snapshot of the confirmation prompt for IKE add entry screen.

Figure 11 : IKE add entry confirmation screen

Do you wish to add the following IKE configuration Information

Remote IP Address : 47.135.214.62
Local IP Address : 47.135.214.127
Oakley Group : 2
Authentication Method : preshared
Encryption Algorithm : 3des
Authentication Algorithm : sha1
PFS Group ID : 0
IKE Lifetime : 14400
IKE Lifetime unit : secs
IPSec Lifetime : 14400
IPSec Lifetime unit : secs
IKE preshared key Location : /tmp/arun1

Select [save, edit, abort] - save

Configuration successfully completed

For downstream configuration refer to instructions placed
in downstream.ike file in /etc/inet/remotesystem/solaris directory

The following figure (Figure 12) captures the screen snapshot when the values entered for a new IKE entry through add option is being edited before committing to the database.

Figure 12 : IKE Add entry - Edit option

```
Press ENTER to continue with the current option
Remote IP Address [47.135.214.63] :
Local IP Address [47.135.214.127] :
Oakley Group [2] :
Authentication Method [preshared] :
Encryption Algorithm [3des] :
Authentication Algorithm [sha1] :
PFS Group ID [0] :
IKE Lifetime value [400] :
IKE Lifetime Unit [secs] :
IPSec Lifetime Value [400] : 800
IPSec Lifetime Unit [secs] : secs
IKE Preshared key File location [/tmp/arun1] :

Do you wish to add the following IKE configuration Information

Remote IP Address            : 47.135.214.63
Local IP Address             : 47.135.214.127
Oakley Group                 : 2
Authentication Method        : preshared
Encryption Algorithm         : 3des
Authentication Algorithm     : sha1
PFS Group ID                 : 0
IKE Lifetime                 : 400
IKE Lifetime unit            : secs
IPSec Lifetime               : 800
IPSec Lifetime unit          : secs
IKE preshared key Location   : /tmp/arun1

 Select [save, edit, abort] -  save

Configuration successfully completed

For downstream configuration refer to instructions placed
in downstream.ike file in /etc/inet/remotesystem/solaris directory
```

37.9.3.4.3 IKE List Entry Example

The following figure (Figure 13) shows screen snapshot when the list option is exercised from the IKE configuration interface menu.

Figure 13 : IKE List Entry Output

```
-------------------------------------------------------
 indexID       raddr            laddr
-------------------------------------------------------
  1         47.135.214.62      47.135.214.127
  2         47.135.214.63      47.135.214.127


 Enter the indexID of rule to be detailed (x to exit) - 2

Remote IP Address          : 47.135.214.63
Local IP Address           : 47.135.214.127
Oakley Group               : 2
Authentication Method       : preshared
Encryption Algorithm        : 3des
Authentication Algorithm    : sha1
PFS Group ID               : 0
IKE Lifetime                : 400
IPSec Lifetime              : 800
IKE preshared key           : ********

 Enter the indexID of rule to be detailed (x to exit) -
```

37.9.3.4.4 IKE Delete Entry Example

The following figure (Figure 14) shows screen snapshot when the delete option is exercised from the IKE configuration interface menu.

Figure 14 : IKE Delete Entry Output

```
-------------------------------------------------------
indexID       raddr            laddr
-------------------------------------------------------
 1         47.135.214.62      47.135.214.127
 2         47.135.214.63      47.135.214.127


 Enter the indexID of rule to be deleted (x to exit) - 2

Remote IP Address          : 47.135.214.63
Local IP Address           : 47.135.214.127
Oakley Group               : 2
Authentication Method      : preshared
Encryption Algorithm       : 3des
Authentication Algorithm   : sha1
PFS Group ID               : 0
IKE Lifetime               : 400
IPSec Lifetime             : 800
IKE preshared key          : ********

Do you wish to delete the above ike rule
Select [Yes, No, Exit(x)] :
```

37.9.3.4.5 IKE Change Key Entry Example

The following figure (Figure 15) shows screen snapshot when the change key option is exercised from the IKE configuration interface menu.

Figure 15 : IKE Change Key Output

```
-------------------------------------------------------
indexID       raddr            laddr
-------------------------------------------------------
 1        47.135.214.62      47.135.214.127
 2        47.135.214.63      47.135.214.127

 Enter the indexID of rule whose key is to be changed (x to exit) - 2

Remote IP Address           : 47.135.214.63
Local IP Address            : 47.135.214.127
Oakley Group                : 2
Authentication Method       : preshared
Encryption Algorithm        : 3des
Authentication Algorithm    : sha1
PFS Group ID                : 0
IKE Lifetime                : 400
IPSec Lifetime              : 800
IKE preshared key           : ********
Do you wish to change key for above IKE rule
Select [Yes, No, Exit (x)] - yes


 Enter the preshared key file location (full path) : /tmp/arun2


Do you with to change key to the above
Select [Yes, No, Exit(x)] - yes

Configuration successfully completed

 Enter the indexID of rule whose key is to be changed (x to exit) -
```

37.9.3.5 OSS parameter settings

- The IPSec and IKE specific entries which needs to be configured at the downstream would be put into files (downstream.ipsec & downstream.ike) on the SSPFS box in /etc/inet/remotesystem/solaris directory
- Appropriate instructions would be provided as part of the interface to read from the static files so created, for configuring IPSec on the downstream

- The configuration information for the downstream machine would be limited to Solaris in this release.

Note : This static file contains confidential information (related to preshared key) and should be removed from the machine once its no longer needed.

37.9.3.6 CLUI release history update

Initial Availability

37.9.3.7 Supplementary Information

None

37.10 User interface changes

Not Applicable

37.11 OSSGate Interface Changes

Not Applicable

37.12 Security

37.12.1 Network configuration

None

37.12.2 Key management

Preshared keys would be used for IKE communication.

The IKE preshared key would be entered by the user as part of the IPSec/IKE configuration interface. Solaris stores all keys in a hidden system file not accessible by common users but is available to the root user.

37.12.3 Protocol

IPsec is being used on the solaris machine.

37.12.4 Authentication

Not Applicable

37.13 Configuration Walkthrough

37.13.1 CBM

Following lists the steps which needs to be carried out on the CBM.

The user should not log from target OSS machine onto the CBM to perform the IPSec/IKE configuration.

- Load the CBM with SN09 or later version of SSPFS
- Login as root into the CBM.

- Launch the CLI tool
- Select the IPSec/IKE Configuration option from the list of options listed by the CLI tool (available only as root user).
- In the IPSec/IKE Configuration menu, select the IPSec configuration option to add IPSec rules.
- Using the IKE configuration option in IPSec/IKE Configuration menu, add IKE rules.
- Exit the CLI tool.

37.13.2 OSS

- Make appropriate modifications to the configuration files on the downstream for enabling IPSec communication.

Note : This interface would generate configuration information for configuring IPSec on the downstream (for Sun and Linux boxes). This information would be make available on the CBM in the /tmp directory as static file. The downstream would require to be manually modified to reflect this configuration information.

37.14 Glossary

Term	Description
AH	Authentication Header
CBM	Core and Billing Manager
CLI	Command Line Interface (config tool of SSPFS)
IP	Internet Protocol
IPSec	Internet Protocol Security
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
OSS	Operations Support System
PFS	Perfect Forward Secrecy
SA	Security Association
SSPFS	Succession Server Platform Foundation Software
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

38: Configuration (CN): A00009890

38.1 Feature Name

Provisioning for Media Proxy insertion for SIP lines

38.2 Hardware and Software Requirements

The Session Server :MCS-EM OPI v9.0 or above provisioning interface.
The Session Server :MCS-EM Admin user name and password available to CS2K(SESM) configuration engineer.

38.3 Initial Configuration

See the Session Server(MCSEM) configuration that has been documented under activity A00008522.

As documented by the above acivity the SESM (CS2M) needs to be pre-configured to add connectivity information for the Session Server(MCSEM).

e.g. IP Address, Port, Username and Password for the Session Server(MCSEM).

38.4 Upgrade Considerations

38.4.1 Element Management Upgrade

For CS2M upgrade from versions 6.2 , 7.0 and 8.0 to SN09.

If there has been any IP-VPN(NAT)s provisioned in the CS2M configuration manager, these will need to be synchronised with the Session Server(MCSEM). Before the syncronisation can take place the Call Agent ID is required to be entered. If the Call Agent ID is not already provisioned a prompt will ask the user to enter the Call Agent ID, this should be a number that uniquly qualifies the call agent within the customer domain. e.g. If a carrier has 5 CS2Ks then they should be numbered 1..5 in each CS2K Configuration manager.

The CS2K Audit will attempt to perform a regular synchronisation. If the user wishes to commission this information prior to the scheduled audit, then a manual audit request will synchronise the data to allow correct Media Proxy insertion for SIP lines.

38.4.2 Downgrade impact

None

38.5 Element Management

The CS2M configuration manager :GWCEM has been modified to flow-through IP-VPN (NAT) Zone information to the Session Server(MCSEM). This is only visible to the user if there is an error condition. The error sent to the user may inform them that the Session Server(MCSEM) has failed to add the IP-VPN(NAT) Zone and therefore the current operation has failed.

The CS2K Audit GUIs have been modified to allow the user to audit the Session Server(MCSEM) provisioning data.

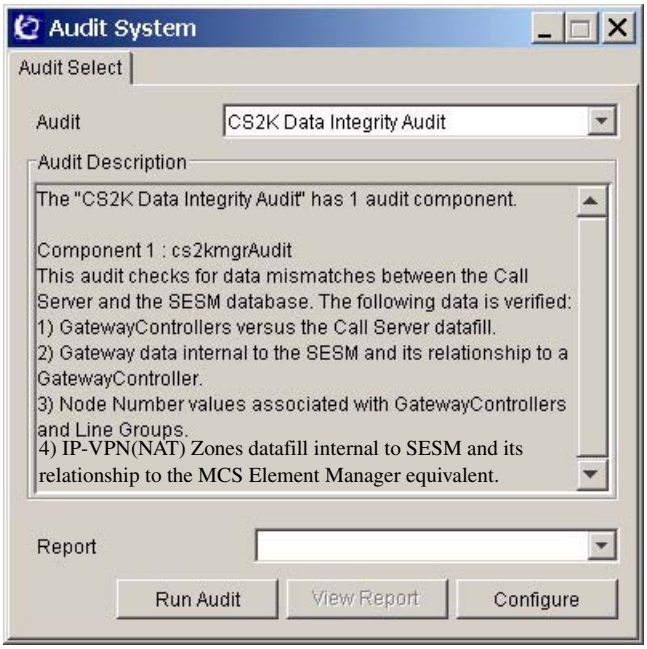
38.5.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Audit System	Changed
CS2K Data Integrity Audit Configuration	New
CS2K Data Integrity Audit Report	Changed

38.5.2 GUI information

38.5.2.1 GUI name: Audit System



38.5.2.1.1 Functional description
Functionality is unchanged, however when selecting the “CS2K Data Integrity Audit” from the pull down selector, the Audit Description text is enhanced to describe the introduction of new audit functionality related to the audit of IP-VPN(NAT) Zones data fill against the Session Server(MCSEM).

38.5.2.1.2 GUI usage and implications
Unchanged.

38.5.2.1.3 GUI size
Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Audit System	0	1	Minimal impact

38.5.2.1.4 GUI fields
Unchanged.

38.5.2.1.5 Usage example
No change in usage.

38.5.2.1.6 GUI release history update

38.5.2.1.7 Context sensitive launching information
None.

38.5.2.1.8 Supplementary information
None.

38.5.2.2 GUI name: CS2K Data Integrity Audit Configuration

38.5.2.2.1 Functional description
This GUI allows the user to selectively run the existing CS2K data integrity audit, the new CS2K SIP Media Proxy Data Integrity Audit or both audit components.

The GUI is accessed from the Audit System GUI upon selecting the “CS2K Data Integrity Audit” and pressing the “Run Audit” button.

38.5.2.2.2 GUI usage and implications

This GUI allows the user to select which sub components of the CS2K data integrity audit to run. This is done by selecting the check boxes for the 2 sub components.

The user is able to restrict the audit run to only those areas of interest. By selecting the “CS2K Call Server Data Integrity Audit” the exisiting audit functionality is exercised whereas by selecting the “CS2K SIP Media Proxy Data Integrity Audit”, the integrity of network zone datafill provisioned jointly at the CS2K and the MCS element manger is exercised.

Where the MCS element manager is not provisioned at the CS2M, the “CS2K SIP Media Proxy Data Integrity Audit” option will be disabled.

By selecting the “Run Audit” button, the required audit components will be run. Where no audit components have been selected, the “Run Audit” button will be disabled.

The “Close” button cancels the run of the audit components and closes the GUI.

38.5.2.2.3 GUI size

Table 3 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
CS2K Audit Config	0	1	Minimal

38.5.2.2.4 GUI fields

The following table lists fields for GUI CS2K Audit Config.

Table 4 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
CS2K Call Server Data Integrity Audit	New	-	check box	Selects if the CS2K Call Server Data Integrity Audit will be executed	-
CS2K SIP Media Proxy Data Integrity Audit	New	-	Check box	Selects if the CS2K Media Proxy Data Integrity Audit should be executed	-

Table 4 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Run Audit	New	-	Button	Run the selected audit sub components	-
Close	New	-	Button	Close the GUI without running the selected audit sub components	-

38.5.2.2.5 Usage example

See Main screen shot for an example of both audit sub components selected.

38.5.2.2.6 GUI release history update

New functionality

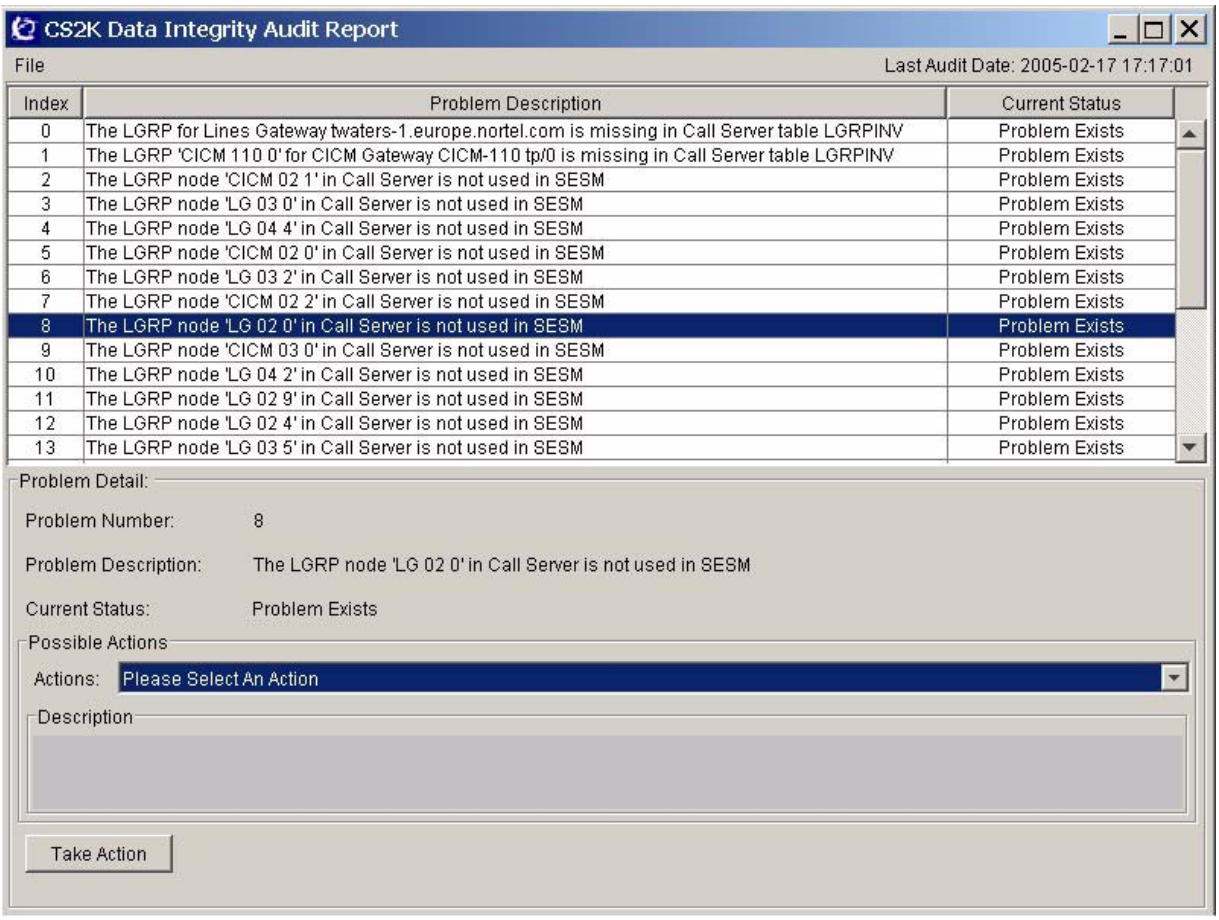
38.5.2.2.7 Context sensitive launching information

None.

38.5.2.2.8 Supplementary information

None.

38.5.2.3 GUI name: CS2K Data Integrity Audit Report



38.5.2.3.1 Functional description

This existing GUI displays problem reports for issues detected during the run of the audit. The functionality of the GUI is completely unchanged, however additional problem types will be detected by the “SIP Media Proxy Data Integrity Audit”. These new problem types will be displayed using the existing mechanism and appropriate Actions will be available via the Actions selector to correct the issues.

38.5.2.3.2 GUI usage and implications

Usage is unchanged.

38.5.2.3.3 GUI size

Table 5 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
CS2K Data Integrity Audit Report	0	1	No change

38.5.2.3.4 GUI fields

GUI fields are unchanged.

38.5.2.3.5 Usage example

Usage is unchanged.

38.5.2.3.6 GUI release history update

GUI unchanged but additional problem report types will be displayed.

38.5.2.3.7 Context sensitive launching information

None.

38.5.2.3.8 Supplementary information

None.

38.6 Configuration Walkthrough

Create a user or use an existing user for the Session Server(MCSEM) provisioning interface(OPI).

Use the CS2M configuration tool to configure the Session Server(MCSEM) connectivity information. See the MCSEM configuration that has been documented under activity A00008522.

If there are IP-VPN(NATs) provisioned already into the CS2M configuration manager, then perform an audit for the Session Server(MCSEM), to ensure the current data is synchronised.

Provision any new IP-VPN(NATs) or Distributed NATs into the CS2M Configuration Manager.

Make Configuration changes to existing gateways Or add new Gateways to the CS2K Configuration Manager to use the IP-VPN(NAT) information.

On the Session Server(MCSEM) provision the SIP Lines to use the routability groups that correspond to the Network Zones that were flowed through by the CS2M.

Calls between GWC controlled lines (IAD,H323,CICM) and MCS controlled SIP lines should now correctly insert Media Proxies when required.

39: Configuration (CN): A000010303

39.1 Feature Name

Map Level Service Control Application Programming Interface

39.2 Hardware and Software Requirements

39.2.1 Hardware requirements

In order to enable this capability for affected subscribers, the following must be present in the provider's network:

- Some Provider Network Server designed to support service queries/ updates via some Web or PC Client based interface.
- SESM/OSSGATE - An application that is used for the provisioning and maintenance of lines, trunks etc. The OSSGATE passes on the command information to the SDM.
- SDM - The SDM is an interface to the core. It takes in the commands given by the SESM and passes them onto the core and also takes the responses from the core and gives it to the SESM.

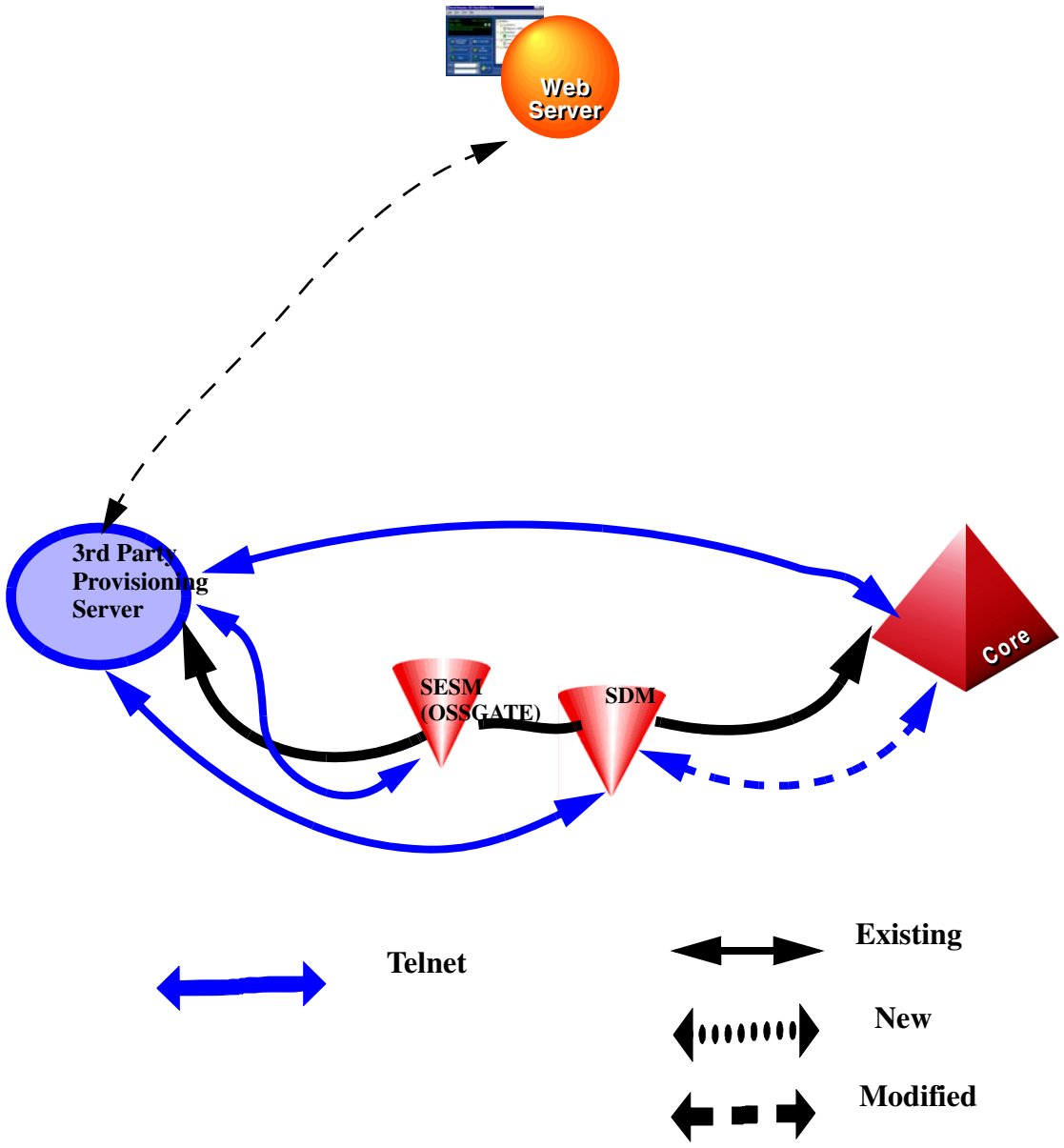
39.2.2 Software requirements

The new SOC SMGT0001 will control the CI interface to Service Management. This SOC will be independent of the AIN TCAP Service Management SOC control. The following table gives the possible supported state of both the SOCs:

Table 1 Supported SOC states

AIN SOC	Service Management SOC	Implication
ON	ON	Both interfaces will be active at the same time.
IDLE	IDLE	Both interfaces will be inactive at the same time.
ON	IDLE	AIN interface to be active and SVCNTRL to be inactive.
IDLE	ON	AIN interfaces to be inactive and SVCNTRL to be active.
ON for some	ON	Some combination of AIN interfaces active and SVCNTRL active.
ON for some	IDLE	Some combination of AIN interfaces active and SVCNTRL inactive.

39.3 Initial Configuration



In the case of CS2K, the commands issued by the end user will be sent via a 3rd party provisioning server to the OSSGATE via telnet. This is then sent to the SDM(Supernode Data Manager or CS2K Manager) which is the interface

to the core for processing. The output will then be sent back and displayed to the end user via the web server. In the case of TDM lines, there is a direct connection between the provisioning server and the core. This architecture can be used both for DMS and CS2K.

39.4 Software optionality control (SOC)

Table 2 SOC

SOC option name:	Service Mgmt-DMSCS2K
SOC option title:	Map Based Service Control
SOC option control type:	State
New SOC option?	Yes
SOC option order code	SMGT0001
Option defined in DRU:	CCM
Affected products:	SNNCSH09

39.5 Command interface changes

39.5.1 Directory: SVCNTRL

The command to enter into this CI tool is

> svcntrl <query/update> <DN> <feature/service> <attribute><attribute parameter>

39.5.1.1 Directory description

On entering command SVCNTRL, the user should enter one of the two options i.e. either query a service or update a service. For Query, the further options will be the DN, the feature/service and the attribute to be queried. For Update, the further options will be the DN, the feature/service and the attribute, and the attribute parameter to be updated.

39.5.1.2 Accessing directory: SVCNTRL

The directory will be a single level directory. The user will be able to enter the commands on a single line.

39.5.1.2.1 Access to directory or MAP level and return to CI

Access to the directory from CI prompt will be available on entering SVCNTRL at the CI level. Enter a Carriage Return to return to the CI prompt.

CI:

>svcntrl <query/update> <DN> <feature> <attribute><attribute parameter>

39.5.2 Command: SVCNTRL

39.5.2.1 Command type: NON- MENU

39.5.2.2 Command target: All

39.5.2.3 Command availability: RES

39.5.2.4 Command description

SVCNTRL is the command issued at CI prompt that is used to both query the status and/or programmed information as well as activate/deactivate and update their corresponding service.

39.5.2.4.1 The Query command

The Query command is used to query the following attributes depending on what the service is:

Table 3 List of supported Query attributes

Enumeration	Return Value	Description
status	active or inactive	Query the status of the corresponding service.
list	list of DNs 10 digits in length with /without priv. ind.	Query all entries in the corresponding service's screening list.
listSize	Positive integer less than 255	Query the number of entries in the corresponding service's screening list.
forwardDN	DN upto 30 digits in length	Query the forwarding DN of the corresponding call diversion service.
delayInterval	Positive integer between 1 and 10	Query the delay Interval(number of rings) of the corresponding service.
scList	List of DNs variable in length up to 30 digits	Query all entries in the corresponding Speed Call list.
all	Some aggregate o f the above	Query all attributes of the corresponding service.

The following table gives the structure of the SVCNTRL query command and how a valid command is to be issued. It also gives the valid option for each of the services. Only one attribute can be queried at a time.

Table 4 Query Command Syntax

Command	Action	DN	Feature	Attribute
SVCNTRL	Query	<10 digit DN>	MWI	Status All
			VMWI	
			AMWI	
			ACRJ	
			ACB	
			AR	
			CSMI	
			CWT	
			LDSA	
			MSB	
			SUPPRESS	
SVCNTRL	Query	<10 digit DN>	DRCW	Status List List Size All
			SCRJ	
			SIMRING	
SVCNTRL	Query	<10 digit DN>	CFU	Status Forward DN All
			CFDA	
			CFB	
SVCNTRL	Query	<10 digit DN>	SCA	Status List List Count All
			SCF	Status List List Count Forward DN All
SVCNTRL	Query	<10 digit DN>	CFDVT	Delay Interval All
SVCNTRL	Query	<10 digit DN>	SCS	Speed Call List All

Some examples of the Query command are:

Syntax to query the status of SCRJ for 6136631001

>svcntrl query 6136631001 scrj status

Status - Service_Active

Syntax to query the SCRJ list for 6136631001

>svcntrl query 6136631001 scrj list

List_Dn -

6136634567;6136678901;61366710021

6136631021; 6136789021;6136779001;

6136772021

Syntax to query SCRJ for 6136631001

>svcntrl query 6136631001 scrj all

Status - Service_Active

List_Size - 7

List_Dn -

6136634567; 6136678901; 61366710021

6136631021; 6136789021; 6136779001

6136772021;

If the DN is not provisioned with the service, then the following error message is displayed:

Syntax to query status of CSMI on 6136671021

>svcntrl query 6136671021 CSMI status

Failure - Unavailable_Resources

39.5.2.4.2 The Update Command

The Update command is used to update the following attributes depending on what the service is:

Table 5 List of supported Update Actions

Enumeration	Description
activate	Activate corresponding service.

Enumeration	Description
deactivate	Deactivate corresponding service.
delayInterval	Set delay interval for corresponding service.This is an integer value between 1 and 10 and represents the no. of rings.
adddn	Add specified DN to corresponding service's screening list.
deletedn	Delete specified DN from corresponding service's screening list.
deleteAlldn	Delete all DNs from corresponding service's screening list.
deleteAllPrivdn	Delete all private DNs from corresponding service's screening list.
setfwdDN	Set forwarding DN for corresponding call diversion service.
clearFwdDN	Clear forwarding DN for corresponding call diversion service.
toggle	Toggle status of the corresponding services.
invoke	Invoke the corresponding service.
changeList	Change a specified speed call cell entry.

The following table gives the structure of the SVCNTRL Update command and how a valid command is to be issued. It gives the valid option for each of the services. Only one attribute can be updated at a time.

Table 6 Update Command Syntax

Command	Action	DN	Feature	Attribute	Attribute parameters

SVCNTRL	Update	<10 digit DN>	MWI	Activate Deactivate	
			VMWI		
			AMWI		
			ACRJ		
			ACB		
			AR		
			CSMI		
			CWT		
			LDSA		
			MSB		
			SUPPRESS		
SVCNTRL	Update	<10 digit DN>	DRCW	Activate Deactivate Adddn Deletedn DeleteAlldn	
			SCRJ		DN <Dn> SpeedCallCode <SCC>
			SIMRING		
SVCNTRL	Update	<10 digit DN>	CFU	Activate Deactivate Setfwddn ClearFwddn	
			CFDA		dn <DN> SpeedCallCode <SCC>
			CFB		
SVCNTRL	Update	<10 digit DN>	SCA	Activate Deactivate Adddn Deletedn DeleteAlldn DeleteAllprivdn	dn <DN> SpeedCallCode <SCC> ICM
			SCF	Activate Deactivate Adddn Deletedn DeleteAlldn DeleteAllprivdn SetFwdDN ClearFwdDN	dn <DN> SpeedCallCode <SCC> ICM
SVCNTRL	Update	<10 digit DN>	CFDVT	Set Delay Interval < 1 to 10>(number of rings)	< 1 to 10> (number of rings)
SVCNTRL	Update	<10 digit DN>	CNDB	Toggle	
			CNAB		

SVCNTRL	Update	<10 digit DN>	COT	Invoke	
			CCW		
SVCNTRL	Update	<10 digit DN>	SCS	Change List	SpeedCallCode <SCC> dn <DN>
			SCL		
			SCU		

Note: For SIMRING, deleteallprivdn and ICM is invalid.

Some examples of the Update command are:

Syntax to activate Call Forward BusyLine on 4164731051

>svcntrl update 4164731051 cfb activate

Success - Service_Activated

Syntax to clear the forward DN on 4164731051

>svcntrl update 4164731051 cfb clearFwdDn

Success - ForwardingDn_Cleared

>svcntrl update 4164731051 cfb setFwdDn dn 4164631001

Success - ForwardingDn_Set

Error conditions:

If we try to activate an already activated service

>svcntrl update 4164731051 cfb activate

Failure - Service_Already_Active

If the user tries deleting a list which is empty, the response would be

>svcntrl update 4164731051 simring deleteallDN

Failure - List_Is_Empty

If the SOC for SPRING (call forward ringing) is not turned on, the response would be

>svcntrl update 4164731051 cfdvt delayInterval 4

Failure - Unavailable_Resources

39.5.2.5 Command syntax

Table 7 Command Syntax

Command	Parameters and variables
SVCNTRL	**input parameters** <query/update> <DN> <feature/service> <attribute> <attribute parameters> **output parameters** A readable sentence depending upon what the return code is

39.5.2.6 Qualifications and warnings

39.5.2.7 Responses

39.5.2.7.1 Error codes for the Query Command

Table 8 Error codes for the Query Command

Return Code	Description
Failure - Invalid_Dn	DN entered is not valid.
Failure - Unavailable_Resources	The service is not subscribed on the DN.
	The feature SOC is idle.
	SLE SOC is idle.
Failure - SOC_Idle	The SVCNTRL SOC is idle.

39.5.2.7.2 Responses for the update command

The following table gives the valid responses for the update command

Table 9 Responses for the Update Command

Response	Meaning
Success - Service_Activated	Successful activation/deactivation of the service.

Response	Meaning
Success - Service_Deactivated_or_Cancelled	Successful deactivation of the service.
Success - AnonymousEntry_Added	Successful addition of a private no to the list of a DN.
Success - PublicEntry_Added	Successful addition of a DN to the list of another DN.
Success - AnonymousEntry_Removed	Successful deletion of a private number from a DNs list.
Success - PublicEntry_Removed	Successful deletion of a DN from a DNs list.
Success - All_Anonymous_Entries_Removed	Successful deletion of all private DNs from the list.
Success - All_Entries_Removed	Successful deletion of all DNs from the list.
Success - ForwardingDn_Set	Successful setting of a FwdDN to another DN.
Success - ForwardingDn_Cleared	Successful clearing of a FwdDN from another DN.
Success - DelayInterval_Updated	Successful updation of delay interval of a DN.
Failure - Service_Already_Active	Not updated because the service is already active on the DN.
Failure - Service_Not_Activated	Gives this response because the service might be inactive and the user is trying to deactivate or in the case of ACB/AR if the feature queue is not present.
Failure -Invalid_Forwarding_Dn	FwdDN not set because the FwdDN did not pass validation.
Failure - List_Is_Empty	When trying to delete a DN from the list of another DN and if the list is empty.
Failure -List_Is_Full	When trying to add a DN to the list of another DN and if the list is full and cannot accommodate more DN's.
Failure - Public_Dn_Already_On_List	If the DN you are trying to add to the list of another DN is already present.
Failure - Anonymous_Dn_Already_On_List	If the private DN you are trying to add to the list of another DN is already present.
Failure - Dn_Not_On_List	If the DN you are trying to delete is not on the list.
Failure - No_Match	When trying to update the delay interval, if the ring control is not programmable ring type.

Response	Meaning
Failure - Unsuccessful_Update	When the update is not successful and for different features and actions, its meaning is different.
	For ACB/AR, activation of the feature is not supported.
	For CFB, if Fixed or Programmable version is not provisioned.
	For CFBL & CFDA, with control N type.
	FOR CFDA if IECFD is provisioned or if CFD Normal is provisioned.
	For Speed Call, if SCU is provisioned.
	For services that use SLE, if SLE datafills are missing in Table CUSTSTN.

39.5.2.7.3 Error codes for the update command

Table 10 Error codes for the Update Command

Return Code	Description
Failure - Invalid_Dn	DN entered is not valid.
Failure - MSRID_Does_Not_Match_User_Profile	For all types of MWT an Msr Id has to be input.This will be validated against Table MSRTAB.If there is a mismatch, then it returns this code.
Failure - Unavailable_Resources	The service is not subscribed on the DN.
	The feature SOC is idle.
	For ACB and AR, checks the validity of the feature and if the feature is not allowed gives this response.
	For ACRJ, COT if universal access is not permitted.
	For CFB, if IECFB is provisioned.
	For CFD, if IECFD is provisioned.
	For CFU, if CFU/CFI/CFF is not provisioned.
	For CNAB & CNDB, if the call is not up.
	FOR MWI, if EMW or CALLOG is assigned to the line.
	The SLE SOC is idle.
	Deactivate MWT when MWT is not active
Failure - SOC_Idle	The SVCNTRLCI SOC is idle.

Table 11 Map outputs with associated meanings and actions

Command
Ex1: If the user tries to update the delay interval of a DN with CFW ring control **>svcntrl** update 4164731051 cfdvt delayInterval 4 **RESPONSE**:>Failure - Unavailable_Resources **Meaning:** Each feature is controlled by a SOC and this SOC needs to be turned on. The above response means that the SOC for SPRING is not turned on. **System or user actions:** For the delay Interval attribute to be update the SOC for SPRING should be turned on. **Ex2:**If the user tries deleting the list of a DN with the SIMRING feature **>svcntrl update 4164731051 simring deleteallDN** **RESPONSE:> Failure - List_Is_Empty** **Meaning:This means that there is no DN present in the list of 4164731051** **System or user actions:** This is not an error scenario, so no action need be taken but the user can query the DN for the list before trying to delete the list.

39.5.2.7.4 Error responses when invalid entries are given

Table 12 Error responses for invalid entries

Return Value	Description
Failure - Invalid_Action	When any other value other than update or query is entered after SVCNTRL.
Failure - Invalid_DNformat	When the DN entered has alpha numeric values or if the DN is not of 10 digit form.
Failure - Unrecognized_Service	When the service entered is invalid.
Failure - Invalid_Attribute	When the attribute entered for that service is invalid.
Failure - Invalid_Attribute_Parameter	When the parameters for the attributes are specified incorrectly. For e.g., if the value of delay interval to be updated is greater than 10.
Failure - Missing_Parameter	When an incomplete command is issued, i.e. if the service, attribute, or any of the parameters are missing.

If the user enters an invalid option then the tool will throw an exception. Rather than prompting the user, the appropriate message will be given and the user

will have to re-enter the command with valid options. The following are the responses for invalid entries.

Ex 1: When the action given is not update/query

>svcntrl updation 6136631001 acrj activate

The response would be:

Failure - Invalid_Action

Ex2: If the DN is invalid

>svcntrl query abc6790123 drcw list

The response would be:

Failure - Invalid_DNformat

Ex3: If the DN entered is not 10 digit

>svcntrl query 6631001 cfb ForwardDN

The response would be:

Failure - Invalid_DNformat

Ex4: If the service is not valid

>svcntrl update 6136671021 cssi activate

The response would be:

Failure - Unrecognized_Service

Ex5: If the attribute is not valid for that service

>svcntrl update 4164671021 cndb FwdDn

The response would be:

Failure - Invalid_Attribute

EX7: If the attribute parameters are invalid

>svcntrl update 4164671001 cfdvt delayInterval 65

The response would be:

Failure - Invalid_Attribute_Parameter

Ex6: If the parameters entered are insufficient

>svcntrl update

The response would be:

Failure - Missing_Parameter

>svcntrl query scs

Failure - Missing_Parameter

39.5.2.8 Example

Table 13 Examples of SVCNTRLCI command

Description of task:	To query the delay Interval on DN 613 663 1001 with CFW ring control.
Command: MAP response:	>**svcntrl query 6136631001 CFDVT delayInterval** **Delay_Interval - 2**
Description of Task:	To set the forward DN for 6136631001 with cfb option
Command: MAP response:	>**svcntrl update 6136631001 cfb setFwdDN dn 6136671001** **Success - ForwardingDN_Set**
Description of Task:	To query the status of CSMI on 6136671021
Command: Map Response:	>**svcntrl query 6136671021 csmi status** **Failure - Unavailable_Resources** (This response is when the service CSMI is not subscribed on the DN)

39.6 OSSGate Interface Changes

39.6.1 XML Command Changes

N/A

39.6.1.1 Command XML

N/A

39.6.1.2 Response XML

N/A

39.6.2 Additional OSSGate Changes

Through this feature, the CI command, SVCNTRL is made accessible through OSSGate. For more information about SVCNTRL See “Command: SVCNTRL” on page 2664.

39.7 Security

39.8 Configuration Walkthrough

The following are the configuration steps for CS2K:

a. Enable SOC SMGT0001 on the core. The SOC needs to be turned on for the query and update commands to function.

b. Enable the SDM telnet session. This is necessary in order to make the interface to the core active.

c. For CS2K, enable the OSSGATE telnet session to enable provisioning.

d. For TDM, there should be a direct telnet connection from the 3rd party provisioning server to the core.

Ensure that telnet is enabled throughout the session.

40: Configuration (CN): A000010742

40.1 Feature Name

GWC EM Enhancements to Support SIREN

40.2 Hardware and Software Requirements

The components modified by this feature, GWC EM and SESM, will be delivered as part of the CS2M load (CS2K Management Tools). CS2M requires the SSPFS (Solaris Software Platform Foundation Software) load as its platform software. The software will interact with GWCs and other necessary components within the Succession and Siren environments.

40.3 Initial Configuration

The CS2M install scripts will be changed to prompt the user if running in Succession or Siren environment. If running in Siren environment, then the SAM21EM software will not be installed.

In order to accommodate various lab set up scenarios, a "lab only" mode will be supported by the SESM configure script. The user will need to enter "-labOnly" as a parameter when invoking the configure script. The SESM configure script will prompt for different information depending on whether running in Succession or Siren environment.

If running in Succession environment and in "lab only" mode, the configure script will prompt the user for the SAM21EM server's IP address and the SAM21EM database password. This is necessary for labs that have the SAM21EM software and the SESM software on different machines.

If running in Siren environment, the configure script will prompt the user for the Siren shelf's IP address and port. This information is required for lab and customer installations.

40.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable

40.5 Upgrade Considerations

40.5.1 Dump and Restore (CM)

None

40.5.2 Element Management Upgrade

The SESM configuration information as to whether it is configured as Siren or Succession should be saved over an upgrade. Upgrade procedures will be the same as the Succession CS2M upgrade procedures.

It should be noted that this feature does not address Succession to Siren migration for SESM/GWC EM.

40.5.3 Downgrade impact

Downgrades are not applicable for the first release.

40.6 Data schema (DS) (CM, MIBS, RDB)

Not applicable

40.7 Service Orders (SO) (CM & SESM)

Not applicable

40.8 Software optionality control (SOC)

Not applicable

40.9 Element Management

The GWCEM/SESM component of the CS2K Management Tools is used to perform configuration and provisioning of GWCs.

40.9.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
GWC EM	Changed

40.9.2 GUI information

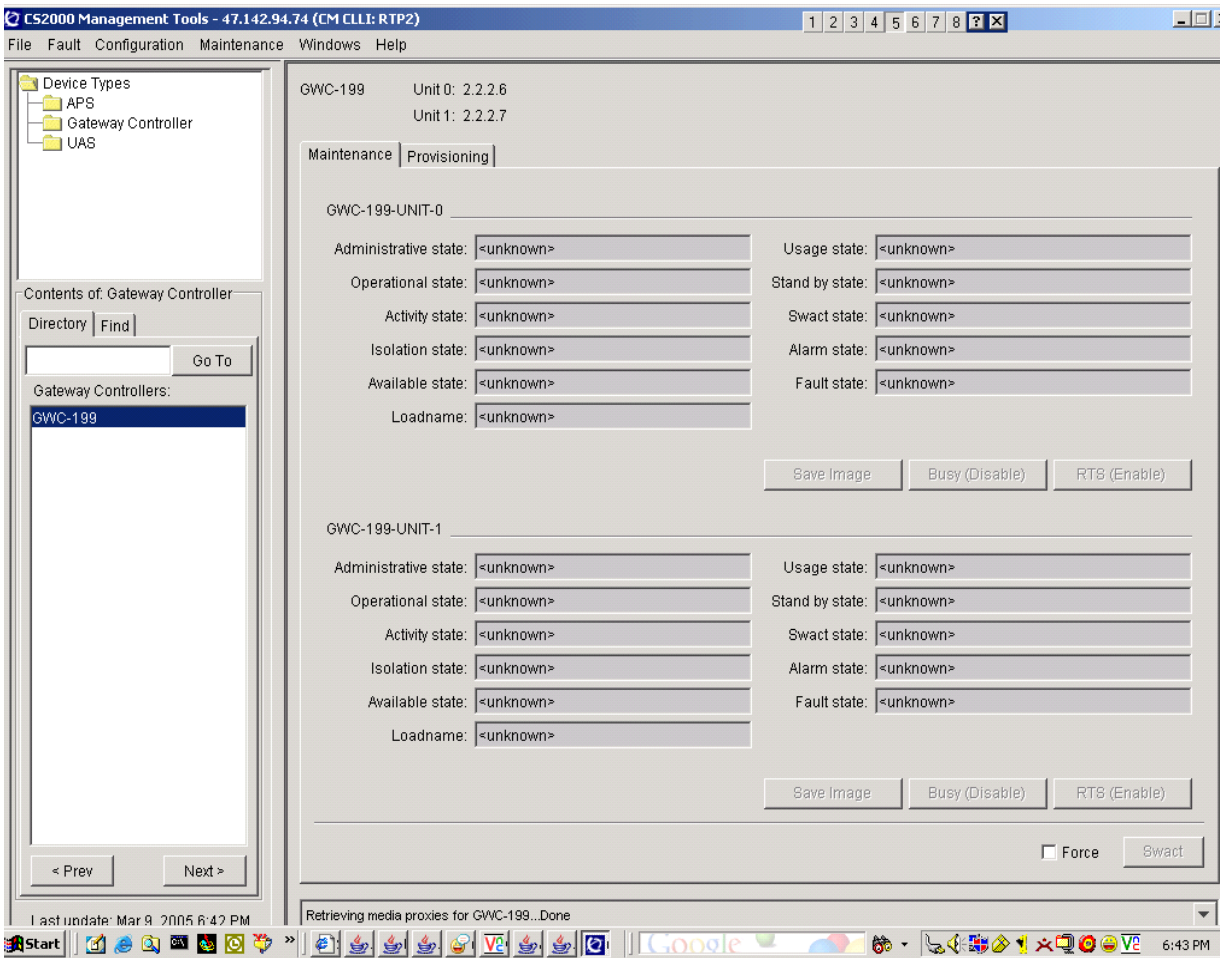
40.9.2.1 GUI name: GWC EM

Gateway Controller Element Manager

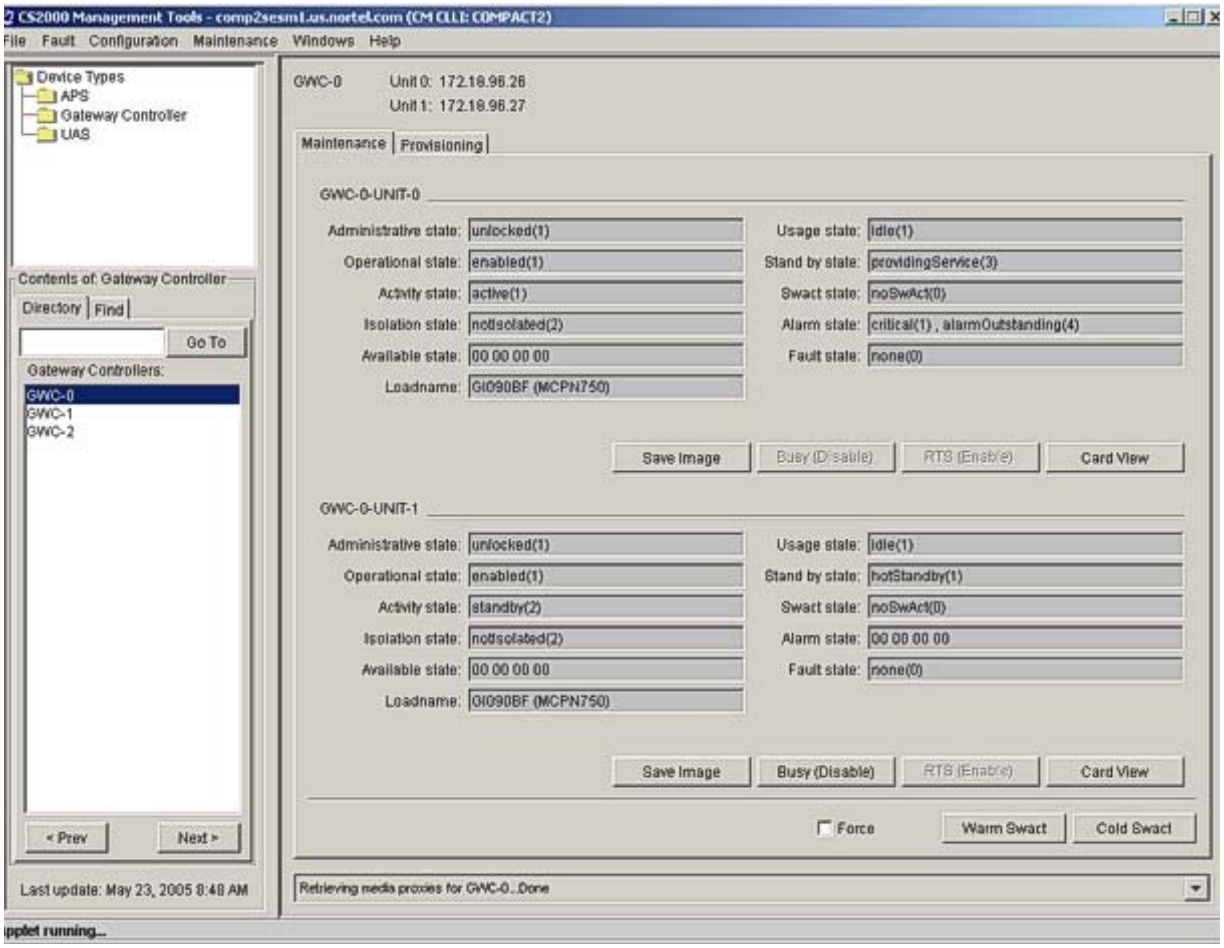
40.9.2.1.1 Functional description

There are two modifications necessary in the GWC EM GUI.

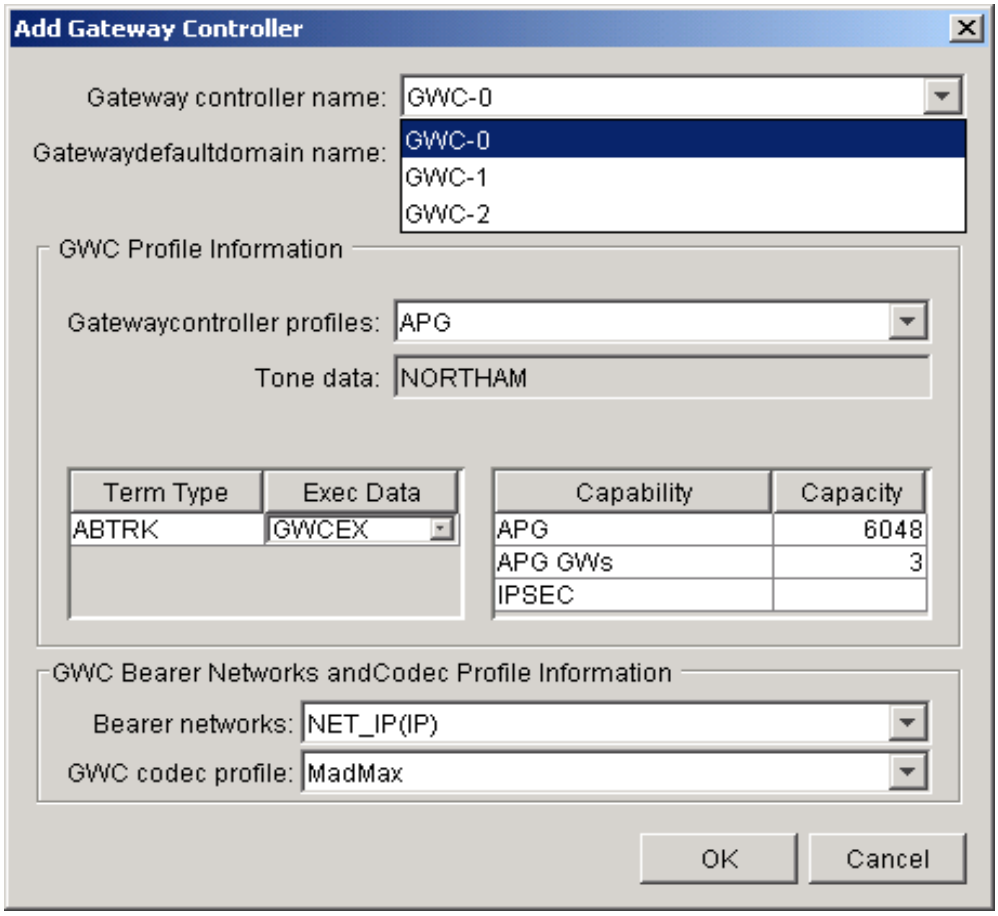
1. In Siren configuration, the ability to bring up the SAM21 card view of the GWC card is removed, and the warm and cold swact buttons are replaced with a single ‘swact’ button. The following picture shows the changes necessary for the Siren platform.



For clarity, it should be noted that for Carrier VoIP installations, the card view button will still be present, and the warm and cold swact buttons are not changed. This is shown below.



2. In both Siren and Succession configurations, the ‘Add GWC’ dialog box will now prompt only for GWC name and not the IP address. The IP addresses will be determined internally by the hardware management software. This picture shows the list of GWC’s displayed to the user. These GWC’s are the Gateway Controllers already provisioned in the Siren Shelf (in case of Siren) or SAM21 (in case of Succession).



40.9.2.1.2 GUI usage and implications

Current datafill order unchanged.

40.9.2.1.3 GUI size

No changes

40.9.2.1.4 GUI fields

Not applicable

40.9.2.1.5 Usage example

See screen examples in section “Functional description” on page 2678.

40.9.2.1.6 GUI release history update

The IP address field is removed from the ‘Add GWC’ dialog.

The ‘Card View’ button is removed in the Siren environment, and the ‘Warm Swact’ and ‘Cold Swact’ buttons are combined into a single ‘Swact’ button.

40.9.2.1.7 Context sensitive launching information

No changes

40.9.2.1.8 Supplementary information

Not applicable

40.10 User interface changes

Not applicable

40.11 OSSGate Interface Changes

40.11.1 XML Command Changes

The Add GWC (addGWCtoCS) operation is modified to make parameter gwcActvIp optional. The IP address will be looked up using the GWC name (gwcUIName). The tag is made optional because we do not want to change the current external OSS interface. If gwcActvIp is provided, it will not be used.

40.11.1.1 Command XML

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
        <Command>
                <Interface>cs2kCfgMgrIf</Interface>
                <Methods>
                        <addGWCtoCS usn="1" version="1.0">
                                <Parameters>
                                        <csUIName>COMPACT6</csUIName>
                                        <gwcUIName>GWC-12</gwcUIName>
                                        <profileName>LARGE_LINENA</profileName>
                                        <gwcSnmpPort>161</gwcSnmpPort>
                                        <msgRouterIp>47.142.128.144</msgRouterIp>
                                        <msgRouterIpPort>4684</msgRouterIpPort>
                                        <bearerNetworkName>NET_IP</bearerNetworkName>
                                        <bearerFabricType>IP</bearerFabricType>
                                        <codecProfileName>Test</codecProfileName>
                                        <termType>POTS</termType>
                                        <termType>KEYSET</termType>
                                        <execLineup>POTSEX</execLineup>
                                        <execLineup>KSETEX</execLineup>
                                </Parameters>
                        </addGWCtoCS>
                </Methods>
        </Command>
</CommandList>
```

40.11.1.2 Response XML

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
        <Response>
                <Interface>cs2kCfgMgrIf</Interface>
                <Methods>
                        <addGWCtoCS usn="1" version="1.0">
                                <RC>0</RC>
                                <MsgTxt>Add GWC operation was successful</MsgTxt>
                        </addGWCtoCS>
                </Methods>
        </Response>
</CommandList>
```

40.11.2 Additional OSSGate Changes

None

40.12 Security

Not applicable

40.13 Configuration Walkthrough

Not applicable

41: Configuration (CN): A000010880

41.1 Feature Name

ABI SMU Support

41.2 Hardware and Software Requirements

N/A

41.3 Initial Configuration

N/A

41.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

41.5 Upgrade Considerations

N/A

41.6 Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
LTCINV	CHANGED	UNCHANGED

41.6.1 Table/MIB/Remote Database Schema information

41.6.1.1 Name: LTCINV

41.6.1.1.1 Line Trunk Controller Inventory Table **Functional description**

Existing Table.

Usage sequence and implications (CM Only) Current datafill order remains unchanged.

SizeTable Size remains unchanged.

41.6.1.1.2 Fields/OIDs

Table LTCINV is changed such that an SMU XPM can now add the optional field, EXTDS512. This optional field was already valid for XPMs which were supported in an ABI configuration (e.g. LTC, LGC, PLGC, SMA2, etc.). This field is used to identify the host gateway, as defined in table GATWYINV.

This changes should have no impact on documentation, other than allowing an SMU entry to have field EXTDS512 as was previously allowed for LTC, LGC, PLGC, SMA2 and SMS).

Table 2 Table LTCINV, field OPTATTR description

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTATTR	changed	n/a	EXTDS512	Now valid to enter EXTDS512 as an value in the OPTATTR field for SMU XPM.

41.6.1.1.3 Datafill example

The following example shows sample datafill for table LTCINV with SMU datafilled as an ABI XPM.

SMU 0 186 SME 1 18 2 E 26 6X02EE ESU13BB (POTS POTSEX) $ (4 30) (4 31)(4 32) (4 33) $ (UTR15) (MSG6X69) (CMR13 CMR10A) $ NORTHAM MX77AA MX77AA 0 UPFWNR04 (**EXTDS512** HOST ABI 10) $ 6X40AC N

41.6.1.1.4 Table release history update

n/a

Supplementary information The changes made to table LTCINV allowing SMU XPMs OPTATTR field to contain the EXTDS512 value are analogous to previous features allowing other XPMs to be supported in an ABI configuration.

41.6.1.1.5 Translation verification and other tools

N/A

41.7 Service Orders (SO) (CM & SESM)

N/A

41.8 Software optionality control (SOC)

N/A

41.9 Element Management

N/A

41.10 User interface changes

N/A

41.11 OSSGate Interface Changes

N/A

41.12 Security

N/A

41.13 Configuration Walkthrough

N/A

42: Configuration (CN): A000011167

42.1 Feature Name

MG9KEM Central Userid and Password Support

42.2 Hardware and Software Requirements

This functionality is for an MG9K Element Manager (EM) that has SN09 or higher software version.

42.3 Initial Configuration

No changes.

42.4 Office/Subnet parameters (OP/SP) (CM & SESM)

The EM (subnet) level userid and password configuration information is in the Element Manager section of this document.

42.5 Upgrade Considerations

42.5.1 Dump and Restore (CM)

NA

42.5.2 Element Management Upgrade

For an upgrade to SN09, the central userid and password will be defaulted to "mg9kadm/mg9kadm". The already-defined NE-level userid and passwords will not be affected by the upgrade and will be used as the second level of authentication as described previously.

42.5.3 Downgrade impact

During a downgrade, the central userid and password will no longer be configured and the NE-level userid and passwords will be the same as they were in the previous release, unless they have been changed by the customer after the upgrade.

42.6 Data schema (DS) (CM, MIBS, RDB)

42.6.1 New/modified tables, MIBs, or Database Schema

The Office Wide Defaults table in the EM Oracle database will have two new rows used to store the EM-level userid and password: "centralid" and centralpw".

42.6.2 Table/MIB/Remote Database Schema information

NA

42.7 Service Orders (SO) (CM & SESM)

NA

42.8 Software optionality control (SOC)

NA

42.9 Element Management

The MG9K Element Manager will be used to define the EM-level userid and password.

42.9.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Subnet View	Changed
Subnet Level User Id and Password	New

42.9.2 GUI information

42.9.2.1 GUI name: Subnet View

42.9.2.1.1 Functional description

This GUI is used to manage EM data that pertains the all the NEs defined for the EM.

42.9.2.1.2 GUI usage and implications

There is no requirement to datafill GUIs in a specific order.

42.9.2.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Subnet View	1	1	NA

42.9.2.1.4 GUI fields

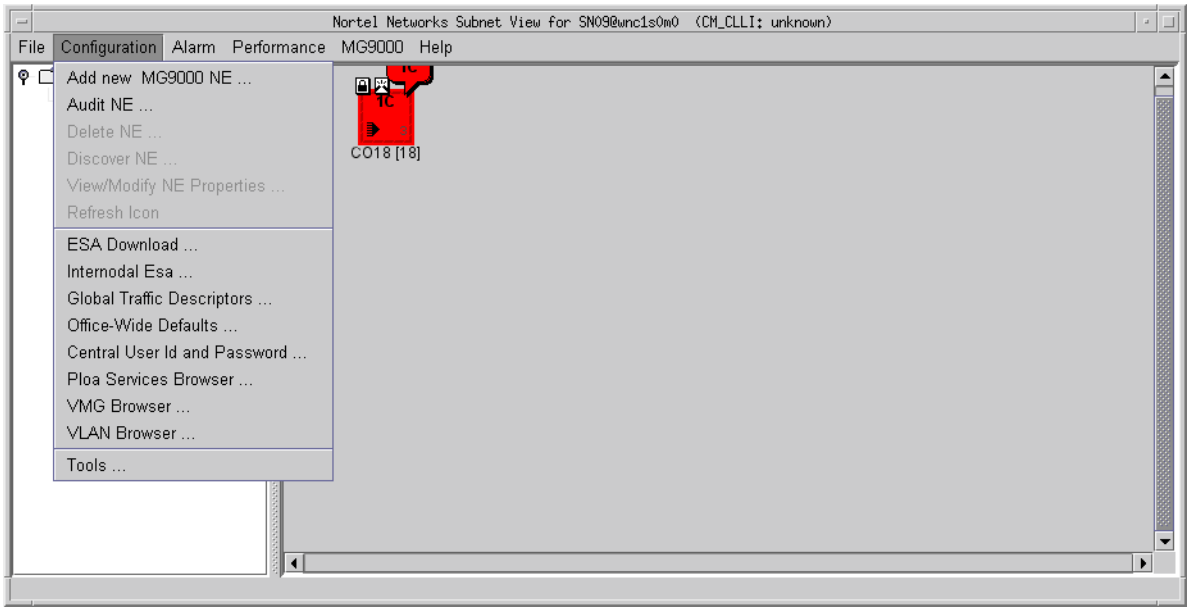
A new entry will be added to the Configuration pull-down menu on the Subnet View GUI. The following table lists fields for the pull-down menu in SubnetView.

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Configuration	Changed	User Id and Password	NA - pull-down menu item	Selection of this item will open the User Id and Password GUI	NA

42.9.2.1.5 Usage example

The following figures show the Configuration level and User Id and Password GUIs.



42.9.2.1.6 GUI release history update

A new menu item, User Id and Password will be added to the pull-down Configuration menu.

Context sensitive launching information

The EM GUI is launched using JavaWebStart. There are no changes to the launching of the GUI.

42.9.2.1.7 Supplementary information

None.

42.9.2.2 GUI name: User Id and Password View

42.9.2.2.1 Functional description

This GUI is used define the subnet-level userid and password.

42.9.2.2.2 GUI usage and implications

There is no requirement to datafill GUIs in a specific order.

42.9.2.2.3 GUI size

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
User Id and Password View	1	1	NA

42.9.2.2.4 GUI fields

The following table lists fields for the User Id and Password GUI. The ability to Apply data, Refresh data, and Close the GUI will also be provided via buttons at the bottom of the GUI.

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
User Id	New	None	NA - pull-down menu	1- 32 characters (must be alphabetic characters or numbers)	NA
Password	New	None	NA - pull-down menu	1- 128 characters The entered data will not be visible to the user.	NA

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Password (Verify)	New	None	NA - pull-down menu	1- 128 characters The entered data will not be visible to the user. This field must match what is entered in the Password field and is used to verify entry of the same password in both fields.	NA

42.9.2.2.5 Usage example

The GUI will contain three new editable fields, User Id, Password, and Password (Verify). When the password is entered, it will not be visible to the user and must be entered twice to confirm that the customer has entered it correctly. The GUI will contain Apply, Refresh, and Close buttons.

42.9.2.2.6 GUI release history update

The new User Id and Password GUI is created.

Context sensitive launching information

The EM GUI is launched using JavaWebStart. There are no changes to the launching of the GUI.

42.9.2.2.7 Supplementary information

When the user configures or changes the userid and/or password, an Information message will be output to indicate that the entered userid and password will be used instead of the NE-level userid and password.

42.9.3 CLUI Interface

NA

42.10 User interface changes

NA

42.11 OSSGate Interface Changes

NA

42.12 Security

This activity provides IEMS/ Radius authentication of the MG9K userid and password. The userid and password will be configured on a per MG9K

Element Manager (EM) basis instead of only on an NE basis. If Radius is not available when the EM communicates with the MG9K, the NE-level userid and password will be used for authentication instead of the EM-level userid and password.

42.12.1 Network configuration

NA

42.12.2 Key management

NA

42.12.3 Protocol

NA

42.12.4 Authentication

The same EM-level userid and password must be entered at the IEMS/Radius server and at the EM GUI.

42.13 Configuration Walkthrough

To allow the IEMS/Radius server to provide central authentication of the MG9K userid and password, the same EM-level userid and password must be entered at the IEMS/Radius server and at the EM GUI. This authentication is required during ESA or OM data transfer to the MG9K.

The following provides additional information and the recommended configuration.

- The NE-level userid is not configurable (mg9kadm) and passwords can be configured on a per-MG9K basis.
    - When customers change the NE-level account password of a MG9K, the corresponding MG9K's password must be updated via the MG9K EM.
    - Based on customers' security policies, the NE-level account passwords can be all different or the same. MG9K EM/MG9K does not ensure that all NE-level account passwords are all different or the same. They are managedly independently of each other by the customers.
- An office-wide central account should be created and managed separately.
    - It is recommended that customers name the account using a different ID (i.e., not 'mg9kadm').
    - The userid and password for this central account should be changed via IEMS (Radius) first and then must be updated via the SN09 MG9K EM to keep it in sync.

- After the MG9K EM is upgraded to SN09, the MG9Ks should be upgraded.
- After all the MG9Ks have been upgraded to SN09, the userid and password defined in Radius for SN08 should be removed.
- Although MG9K does not support authorization in SN09, it is recommended that the SN09 central account be a member of the MGADM group.

43: Configuration (CN): A00011281

43.1 Feature Name

MS2000 IPSec Configuration via IEMS

43.2 Hardware and Software Requirements

SN09 IEMS

SN08 or later MS2000

43.3 Initial Configuration

Standard SN09 IEMS deployment

43.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

43.5 Upgrade Considerations

Not applicable.

43.6 Data schema (DS) (CM, MIBS, RDB)

Not applicable.

43.7 Service Orders (SO) (CM & SESM)

Not applicable.

43.8 Software optionality control (SOC)

Not applicable.

43.9 Element Management

43.9.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
IEMS - MS2000 Node Configuration	Changed

43.9.2 GUI information

43.9.2.1 GUI name: IEMS-MS2000 Node Configuration

43.9.2.1.1 Functional description

This GUI is used to configure the MS2000 node from the IEMS. This feature extends the existing GUI to include configuration of the IPSec and IKE parameters needed to allow for secure messaging between the IEMS and the MS2000 as well as between the MS2000 and the GWC.

43.9.2.1.2 GUI usage and implications

To configure IPSec and IKE parameters and enable them on the device, the following steps must be taken:

- set the IPSec and IKE parameters on the MS2000, including the initial key, via the new IEMS GUI tool.
- set IPSec as enabled on the MS2000 and reset the box
- set the IPSec and IKE parameters, including the initial key, on the SSPFS HTML servlet that currently exists. For documentation on the SSPFS configuration tool, see: http://triweb/ja00/sloa/docs/howto_ipsec/howto_ipsec.html.
- return to the IEMS GUI and set the actual key.
- reset the MS2000
- return to the SSPFS HTML servlet and set the actual key.
- set the IPSec and IKE parameters for the GWC comms on the MS2000
- reset the MS2000

43.9.2.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
MS2000 Config	0	1	N/A

43.9.2.1.4 GUI fields

The following table lists fields for GUI MS2000 Config.

Table 3 IPSec GUI field descriptions

Field	New or Changed	Entry (examples)	Explanation and action	Associated MIB entry
IPSecPolicyRemoteIPAddress	New	47.142.42.135	Destination IP address or a DNS name, this parameter is mandatory.note: if a DNS is given make sure the DNS server is also configured (DNSPriServerIP)	<see field name>
IPSecPolicySrcPort	New	161	Source port. 0 means all ports match.	
IPSecPolicyDstPort	New	9961	Destination port. 0 means all ports match.	
IPSecPolicyProtocol	New	0	Protocol type. 0 - all protocols match; 17- UDP, 6-TCP.	
IPsecPolicyKeyExchangeMethodIndex	New	0-19 (see IKE table; matches with the IKE index)	The Index for the corresponding IKE entry, a few policies may be associated with a single IKE entry	
IPsecPolicyLifeInSec	New	600	Lifetime in seconds for security association derived from this policy.	

IPSecPolicyProposal Encryption_X	New	2	X – stands for the proposal number, up to 4 proposals are allowed [0-3].the valid encryption values are: 0 - NULL (no encryption) 1 - DES 2 - 3DES
IPSecPolicyProposal Authentication_X	New	4	X – stands for the proposal number, up to 4 proposals are allowed [0-3].the valid authentication values are: 2 - SHA1 (SHA1_96)4 - MD5 (MD5_96)
IKEPolicySharedKey	New	020a04090e	The pre-shared key. The key is in text string format. Both peers need to register the same pre-shared key for the authentication process to succeed. The MS2000 will accept any key, however it is recommended that a hex character sequence is used.
IKEPolicyProposalEncryption_X	New	2	X – stands for the proposal number, up to 4 proposals are allowed [0-3].the valid encryption values are: 1 - DES 2 - 3DES
IKEPolicyProposalAuthentication_X	New	4	X – stands for the proposal number, up to 4 proposals are allowed [0-3].the valid authentication values are: 2 - SHA1 (SHA1_96) 4 - MD5 (MD5_96)

IKEPolicyProposalDHGroup_X	New	1	X – stands for the proposal number, up to 4 proposals are allowed [0-3].the valid DH Group values are: 0 - 786 Bit 1 - 1024 Bit
IKEPolicyLifeInSec	New	1200	Lifetime in seconds for security association derived from this policy.

43.9.2.1.5 Usage example

See walkthrough section at the end of this section for examples of using this code.

43.9.2.1.6 GUI release history update

SN08 - MS2000 GUI introduced.

SN09 - Updated to include IPSec configuration mechanism.

43.9.2.1.7 Context sensitive launching information

Launched from the IEMS - right click on the MS2000 node and choose configure MS2000 node option.

43.9.2.1.8 Supplementary information

None

43.9.3 CLUI Interface

Not applicable.

43.10 User interface changes

Not applicable.

43.11 OSSGate Interface Changes

Not applicable.

43.12 Security

Not applicable.

43.13 Configuration Walkthrough

43.13.1 Adding IPSec to the MS2000 node

43.13.1.1 Add IKE and IPSec parameters to the MS2000 for IEMS/ MS2000 secure messaging

1. Launch the MS2000 Config and Maintenance Tool
2. Select the IPSec and IKE Config Tab
3. Select the IKE Configuration Tab
4. Select “Add Entry”
5. Enter the fields for the initial IKE configuration for the MS2000. These values will only be used to establish a temporary secure connection to allow the setting of the actual IKE fields. Essential: these fields should be selected based on the desired IPSec/IKE configuration for the lab. These fields will be needed for later configuration.
6. After all the fields are entered, the Add Entry button should be pressed.
7. Select the IPSec Configuration Tab.
8. Select “Add Entry”.
9. Enter the values for the IPSec temporary configuration. The index chosen for the IKE entry previously should be entered in the Exchange Method field here. Essential: these fields should be selected based on the desired IPSec/IKE configuration for the lab. These fields will be needed for later configuration.
10. Select “Add Entry”.
11. With both the IKE and IPSec tables configured, click the Enable IPSec check box.
12. In the new dialog box that appears, confirm the enabling of IPSec.
13. After receiving the message indicating successful enabling of IPSec, the MS2000 needs to be reset. This is done via the Reset button on the left-hand side of the MS2000 config tool. Reset the MS2000 to enable the new parameters.
14. Once the MS2000 is reset, the IEMS will not be able to talk to the MS2000 until the IEMS server is configured for IPSec with the MS2000 IP. This is done via the configuration GUI at http://(ip address of server)/ipsec/security.html.
15. Adding IPSec support on SSPFS is described in detail in this document: http://iwebrtp.us.nortel.com/spvn/sloa/docs/howto_ipsec/howto_ipsec.html

16 Add the IPSec and then the IKE parameters via the GUI provided. Ensure that the selections made match the selections made during the MS2000 configuration. Do not close this window as it will be used again later.

17 At this point, communications between IEMS and the MS2000 have been secured. Configuration of the actual IPSec/IKE parameters can now begin.

18 Return the IPSec/IKE Configuration tab of the MS2000 Config tool.

19 Select the IKE Configuration tab.

20 Select the row in the table and click “Edit Entry”.

21 In the edit dialog, modify the desired fields. If the parameters previous entered are what is desired for the actual IKE parameters, only the shared key field needs to be modified. Click “Save”.

22 Select the IPSec table if any of the IPSec parameters need to be modified. If so, click “Edit Entry”, modify the values, and click “Save”.

23 At this point, the MS2000 needs to be reset again in order to enable the new preshared key (and any other modified values).

24 The IEMS server IPSec configuration for communications with the MS2000 needs to be modified to support the new parameters and shared key. Return the SSPFS configuration tool and delete the existing entries added earlier. Add new entries to match the new configuration of the MS2000, including the new preshared key.

43.13.1.2 Add IPSec and IKE parameters for MS2000/GWC communications

1 If secure messaging between the MS2000 and IEMS are desired before sending the preshared key to the AMS, complete the steps in section 12.12.1.

2 On the IEMS GUI, launch the MS2000 Config and Maintenance Tool.

3 Select the IPSec and IKE Config Tab.

4 Select the IKE Configuration Tab.

5 Select “Add Entry”.

6 Enter the IKE values needed to communicate with the GWC. These values should match the values provisioned on the GWC when appropriate. Essential: note which index is chosen as this field will be needed for later configuration.

7 After all the fields are entered, the Add Entry button should be pressed.

8 Select the IPSec Configuration Tab.

9 Select “Add Entry”.

10 Enter the IPSec values needed to communicate with the GWC. The index chosen for the IKE entry previously should be entered in the Exchange Method field here.

11 Select “Add Entry”.

12 If IPSec is not currently enabled, enable it following the steps 11 and 12 in section "Adding IPSec to the MS2000 node" .

13 Reset the MS2000 box following step 13 in section "Adding IPSec to the MS2000 node" . The MS2000 will now communicate securely with the GWC.

43.13.2 Disable IPSec on the MS2000

1 On the IEMS GUI, launch the MS2000 Config and Maintenance Tool.

2 Select the IPSec and IKE Config Tab.

3 If the Enable IPSec check box is selected, deselect it to disable IPSec.

4 A dialog will appear to confirm the desire to disable IPSec. Click “Yes”.

5 If desired, the data in the IPSec and IKE configuration tables can be deleted from the MS2000. Select the appropriate tab, select the row and click “Delete Entry”.

6 Reset the MS2000 following step 13 in section "Adding IPSec to the MS2000 node" .

7 Once the MS2000 has reset, if IPSec was previously enabled between the IEMS and MS2000, the IEMS Server must disable IPSec to the MS2000 node in order to communicate.

8 Launch http://(ip address of server)/ipsec/security.html.

9 After logging in, select the entries corresponding to the MS2000 node and delete them. Once they are deleted, the IEMS will again be able to communicate with the MS2000.

43.13.3 Edit the preshared key on the MS2000

1 On the IEMS GUI, launch the MS2000 Config and Maintenance Tool.

2 Select the IPSec and IKE Config Tab.

3 Select the IKE Configuration Tab.

4 Select the row containing the key to update.

5 Click “Edit Entry”.

6 Update the preshared key.

7 Click “Save”.

8 Reset the MS2000 following step 13 in section 12.12.1.

9 Update the IEMS Server or GWC with the preshared key so that the MS2000 can communicate with that device.

44: Configuration (CN): A00011827

44.1 Feature Name

GWC Autonomous SWACT

44.2 Hardware and Software Requirements

The autonomous SWACT activity does not require special hardware.

The autonomous SWACT functionality is available for packetized voice solutions that utilize IP solutions (IP over GigE and AAL5) and ATM solutions (Voice over AAL2) with these products:

- MSC Server 1000
- MSC Server 2000
- CS 2000 (North American and International software loads)
- CS 2000 - Compact (North American and International software loads)

44.3 Initial Configuration

- The initial configuration for GWC autonomous SWACT is disabled for each GWC.

44.4 Upgrade Considerations

44.4.1 Element Management Upgrade

The following upgrades are supported:

- SN07 -> SN09.1
- SN08 -> SN09.1
- SN09 -> SN09.1

44.4.2 Downgrade impact

If a downgrade is needed, then the GWCs go back to the initial GWC autonomous SWACT state of disabled.

44.5 Data schema (DS) (CM, MIBS, RDB)

44.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
GWC Maintenance Controls MIB	NEW	N/A

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
GWC.GWCMTCCONTROLS	NEW	N/A

44.5.2 Table/MIB/Remote Database Schema information

44.5.2.1 Name: GWC-Maintenance-Controls-MIB

44.5.2.1.1 Functional description

The GWC-Maintenance-Controls-MIB contains timers and other maintenance-related controls that are provisioned in CMT and are needed in the GWC.

44.5.2.1.2 Fields/OIDs

The following table lists fields/OIDs for GWC-Maintenance-Controls-MIB:

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
gwcAutoSwactTimer	New		1	The timer represents the time to wait before doing a SWACT, given that the time starts after the following conditions have been met: -All gateways have been taken out-of-service by the GWC due to lost communication. The GWC determines communication has been lost with a gateway after approximately 40 seconds without receiving a message. -The messaging queues have been processed to notify the Core of the state transitions.
gwcAutoSwactAlarmFlag	New		2	This flag is sent down to the GWC to request the clearing of the alarm when the GWC does an autonomous SWACT.

44.5.2.1.3 Table release history update

SN09.1: Initial version of the GWC-Maintenance-Controls-MIB.

44.5.2.1.4 Translation verification and other tools

GWC-Maintenance-Controls-MIB does not use translation verification tools.

44.5.2.2 Name: GWC.GWCMTCCONTROLS

44.5.2.2.1 Functional description

The GWC.GWCMTCCONTROLS table contains timers and other maintenance-related controls that are provisioned in CMT.

44.5.2.2.2 Fields/OIDs

The following table lists fields/OIDs for GWC.GWCMTCCONTROLS

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GWCID	New		VARCHAR2 (32) NOT NULL	The ID of the GWC.
AUTOSWACTTIMER	New		NUMBER	The timer represents the time to wait before doing a SWACT, given that the time starts after the following conditions have been met: -All gateways have been taken out-of-service by the GWC due to lost communication. The GWC determines communication has been lost with a gateway after approximately 40 seconds without receiving a message. -The messaging queues have been processed to notify the Core of the state transitions.

44.5.2.2.3 Datafill example

The following example shows sample datafill for table GWCMTCCONTROLS:

```
GWCID                          AUTOSWACTTIMER

------------------------------- --------------

GWC-2                          40
```

44.5.2.2.4 Table release history update

SN09.1: Initial version of the GWCMTCCONTROLS table.

44.5.2.2.5 Translation verification and other tools

GWCMTCCONTROLS does not use translation verification tools.

44.6 Element Management

44.6.1 New/modified GUIs

Table 4 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Controller Panel	Changed
Change GWC Auto Swact Dialog	NEW

44.6.2 GUI information

44.6.2.1 GUI name: ControllerPanel

The Controller Panel is within the Provisioning Panel.

44.6.2.1.1 Functional description

The Controller Panel contains IP address information, the GWC profile, Bearer Network and Codec Profile information, and other general information for the selected GWC. This GUI is modified to also contain GWC Autonomous SWACT information, as well as an additional Change button to change the state of the control and/or timer and to make a request to the GWC to do a clear of the Swact Alarm.

44.6.2.1.2 GUI usage and implications

The Controller Panel displays and modifies information concerning the GWC. The state of the GWC Autonomous SWACT control and timer (if control is enabled) is displayed on the Controller Panel. The GWC Autonomous SWACT state is initially disabled for all GWCs. If the Change button is selected, the state and/or timer can be changed for the specified GWC.

44.6.2.1.3 GUI size

Table 5 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Controller Panel	No change.	No change.	N/A

44.6.2.1.4 GUI fields

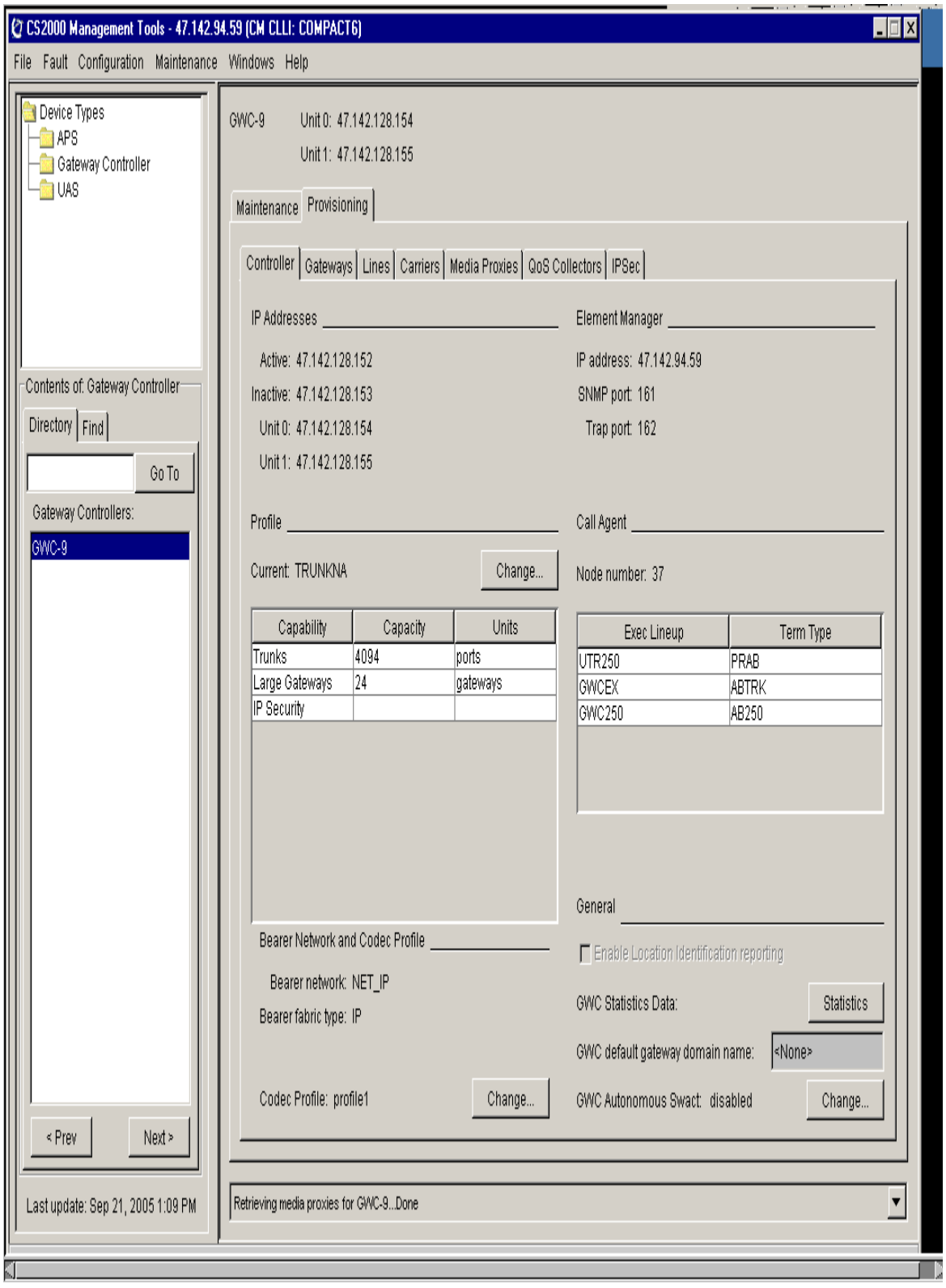
The following table lists new fields for the Controller Panel GUI:

Table 6 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
GWC Auto SWACT	New			A new label, field and button is added to the Controller Panel.	GWC-Maintenance-Controls-MIB

44.6.2.1.5 Usage example

The following example shows a sample GUI for the Controller Panel where GWC Autonomous SWACT is disabled:


CS2000 Management Tools - 47.142.94.59 (CM CLLI: COMPACT6)
File Fault Configuration Maintenance Windows Help
Device Types
APS
Gateway Controller
UAS
Contents of: Gateway Controller
Directory Find
Go To
Gateway Controllers:
GWC-9
< Prev
Next >
Last update: Sep 21, 2005 1:09 PM
GWC-9 Unit 0: 47.142.128.154
Unit 1: 47.142.128.155
Maintenance Provisioning
Controller Gateways Lines Carriers Media Proxies QoS Collectors IPSec
IP Addresses
Active: 47.142.128.152
Inactive: 47.142.128.153
Unit 0: 47.142.128.154
Unit 1: 47.142.128.155
Element Manager
IP address: 47.142.94.59
SNMP port: 161
Trap port: 162
Profile
Current: TRUNKNA
Change...
Call Agent
Node number: 37
Capability Capacity Units
Trunks 4094 ports
Large Gateways 24 gateways
IP Security
Exec Lineup Term Type
UTR250 PRAB
GWCEX ABTRK
GWC250 AB250
General
Bearer Network and Codec Profile
Bearer network: NET_IP
Bearer fabric type: IP
Enable Location Identification reporting
GWC Statistics Data:
Statistics
GWC default gateway domain name:
<None>
Codec Profile: profile1
Change...
GWC Autonomous Swact: disabled
Change...
Retrieving media proxies for GWC-9...Done

44.6.2.1.6 GUI release history update
SN09.1: Modification of Controller Panel for GWC Autonomous SWACT.

44.6.2.1.7 Context sensitive launching information
N/A

44.6.2.1.8 Supplementary information
N/A

44.6.2.2 GUI name: ChangeGWCAutoSwact

44.6.2.2.1 Functional description
The new dialog contains a check box for enabling the control and a timer where the user can enter an integer between 0 and 300 seconds. The timer cannot be filled in if GWC Autonomous SWACT is not enabled.

Three buttons exist on the dialog. The OK button is to process the changes. The Cancel button is to close the dialog without processing changes. After the autonomous SWACT occurs and the customer has identified and fixed the problem on the inactive unit, the Clr Alarm button can be used to make a request to the GWC to clear the alarm that gets generated when the GWC does an autonomous SWACT.

44.6.2.2.2 GUI usage and implications
This dialog appears whenever the GWC Autonomous SWACT button is selected on the Controller Panel. The current status of the control and timer for the selected GWC is displayed.

44.6.2.2.3 GUI size

Table 7 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
ChangeGWC AutoSwact	0	N/A	N/A

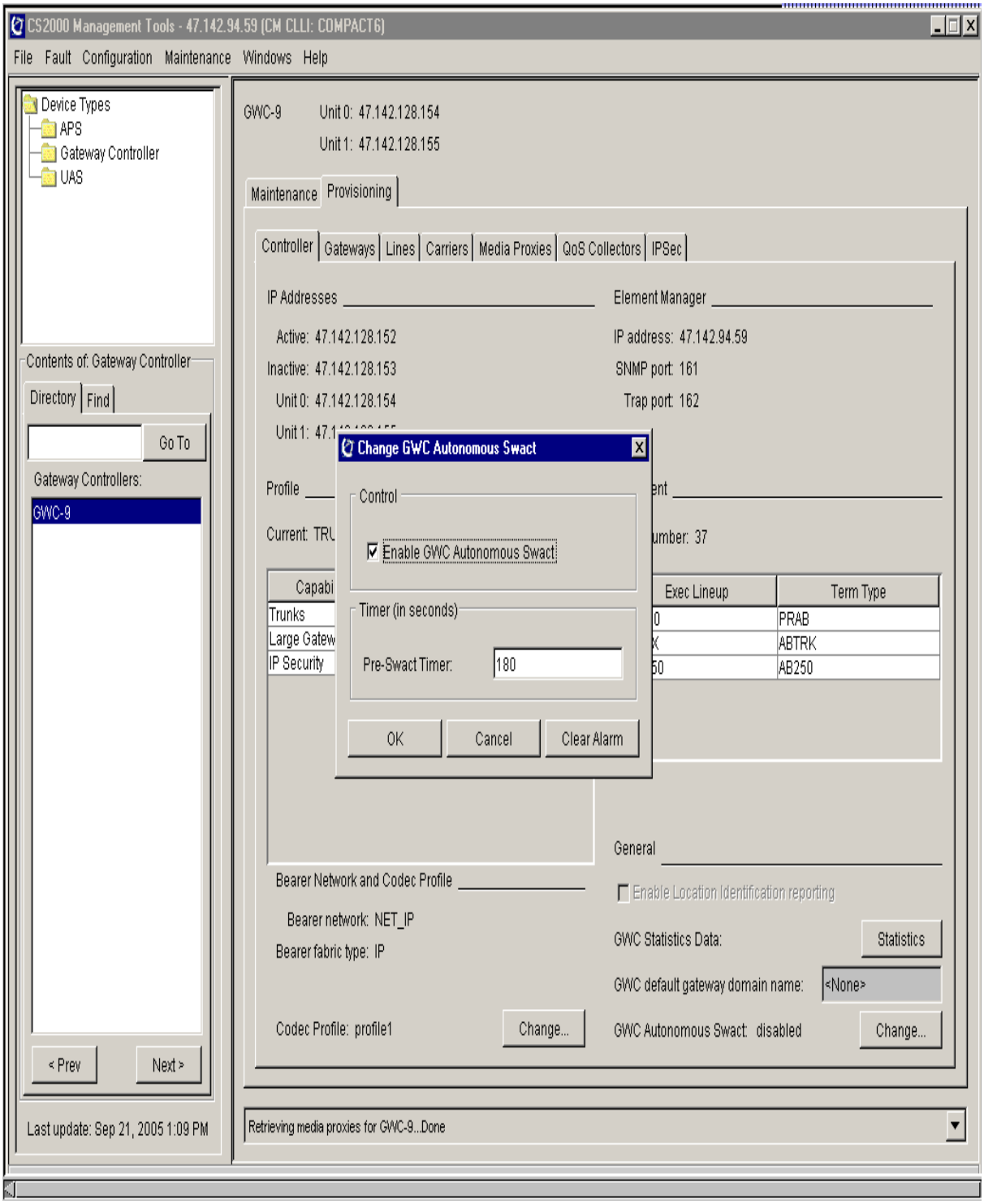
44.6.2.2.4 GUI fields
The following table lists fields for GUI:

Table 8 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Control	New		1	A check box, allowing the user to enable or disable GWC Autonomous SWACT.	GWC-Maintenance-Controls-MIB
Timer	New		2	A label and text box where the user can fill in the pre-Swact timer. The timer is only valid if the control is in the enabled state. The default value for the timer is 180 seconds.	GWC-Maintenance-Controls-MIB

44.6.2.2.5 Usage example

The following example shows a sample dialog for the ChangeGWCAutoSwact GUI:



44.6.2.2.6 GUI release history update

SN09.1: Creation of Change GWC Autonomous Swact dialog.

44.6.2.2.7 Context sensitive launching information

N/A

44.6.2.2.8 Supplementary information

N/A

44.6.3 CLUI Interface

N/A

44.7 Configuration Walkthrough

A change of the GWC Autonomous SWACT information can be made anytime after the GWC has been added.

45: Configuration (CN): A000012001

45.1 Feature Name

IEMS Call Server 2000 SIP Integration

45.2 Hardware and Software Requirements

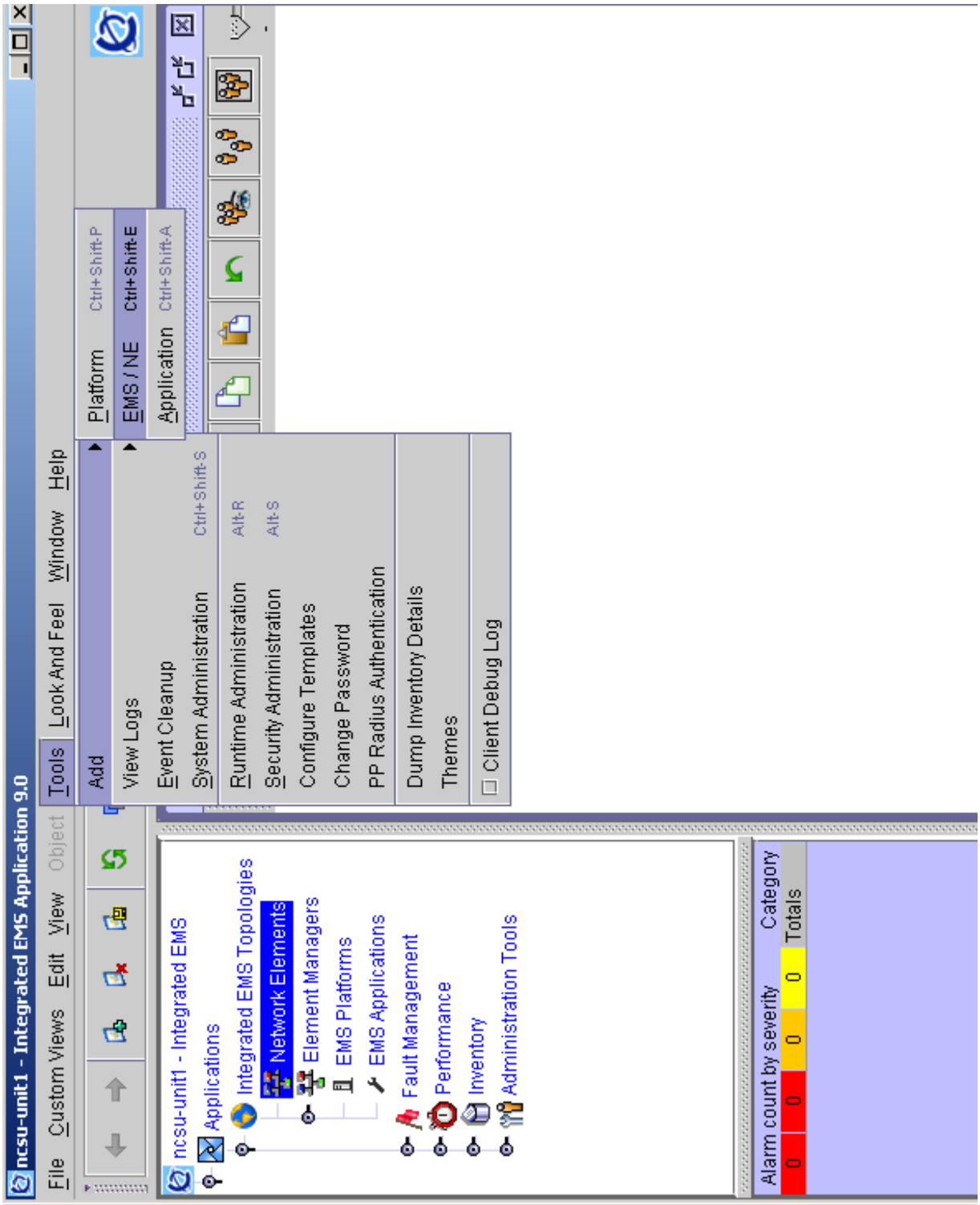
Note: All screen shots captured in this version are draft documents, and this document will be updated when the official versions are complete.

The feature requires IEMS to be installed on SN10 or later SSPFS loads.

45.3 Addition of an SSLines Mgr

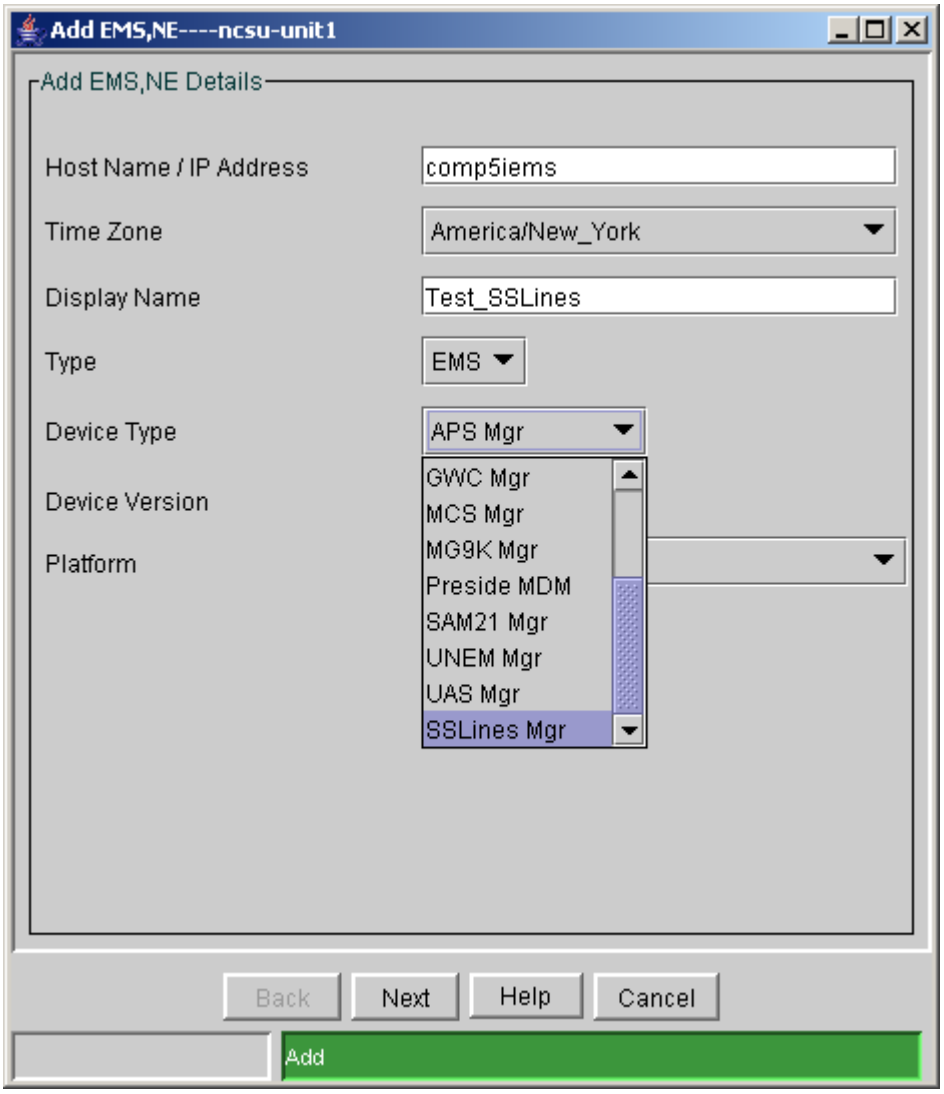
The SSLines configuration is similar to that of the MCS Mgr device in SN08, only shown here is the configuration of the first panel as all the other components are the same.

Figure 1 Getting add panel



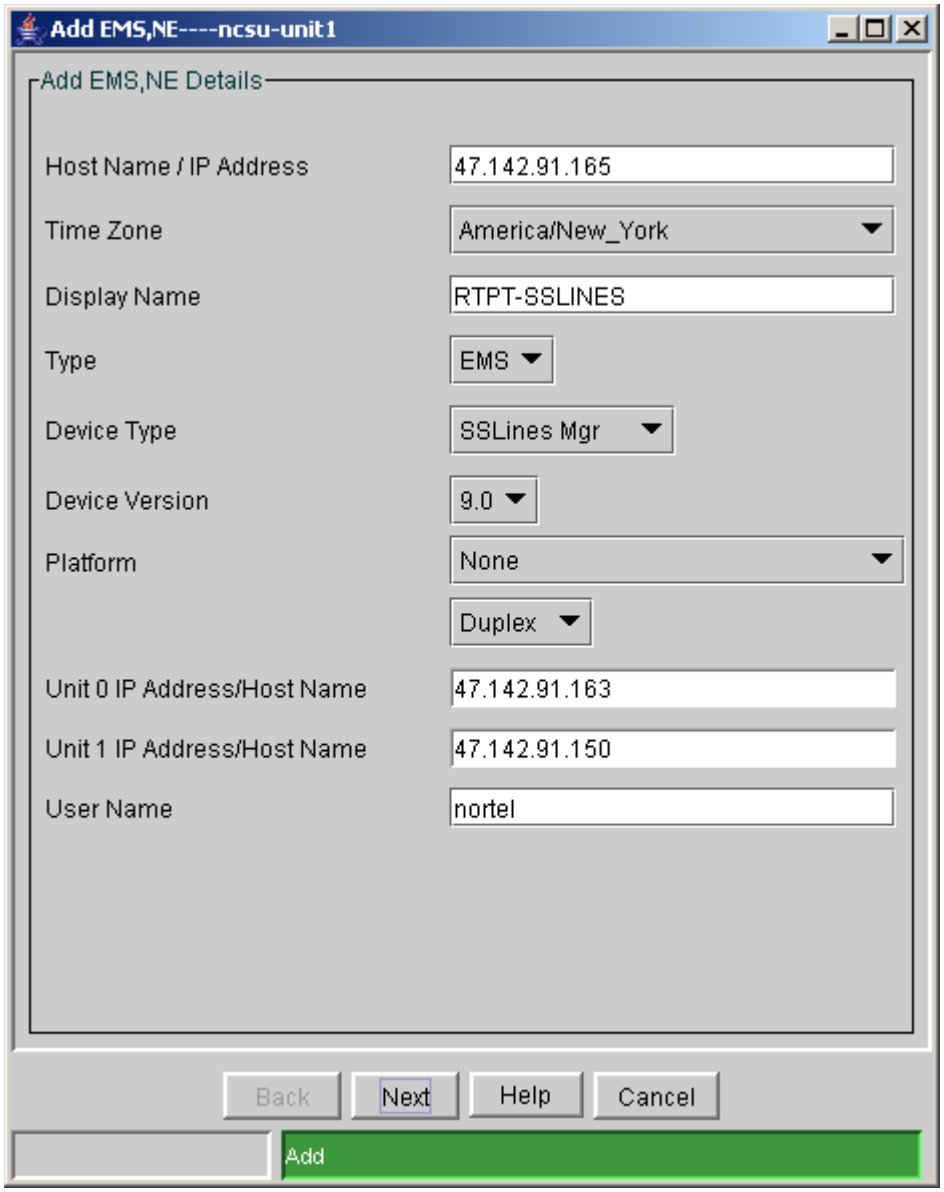
From this add panel, the SSLines option must be chosen.

Figure 2 Selecting SSLines Mgr



After this, the IP addresses for the System Manager platform and username are entered as follows. As shown below, the default is duplex for the SSLines or SIP lines on the Langley hardware.

Figure 3 Setting configuration data.



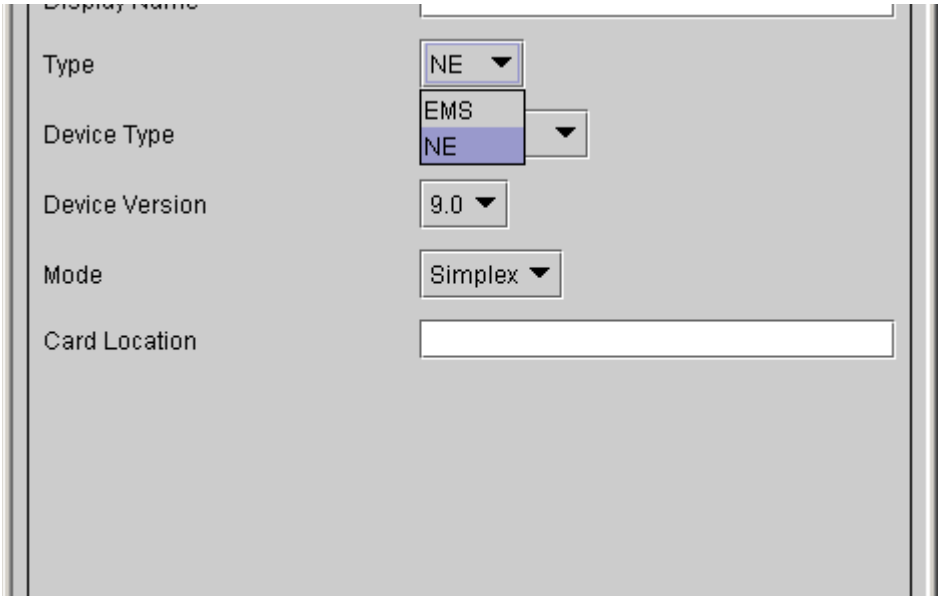
The other configuration screens are configured like the MCS Mgr configuration in SN08. Please see the SN08 documentation for those references.

45.4 Addition of an SSTrunks NE

The SSTrunks is the SN10 rebranded name of the Session Server. Following is a screen shot of the add panel. All SN08 configuration parameters are present in the SN10 version.

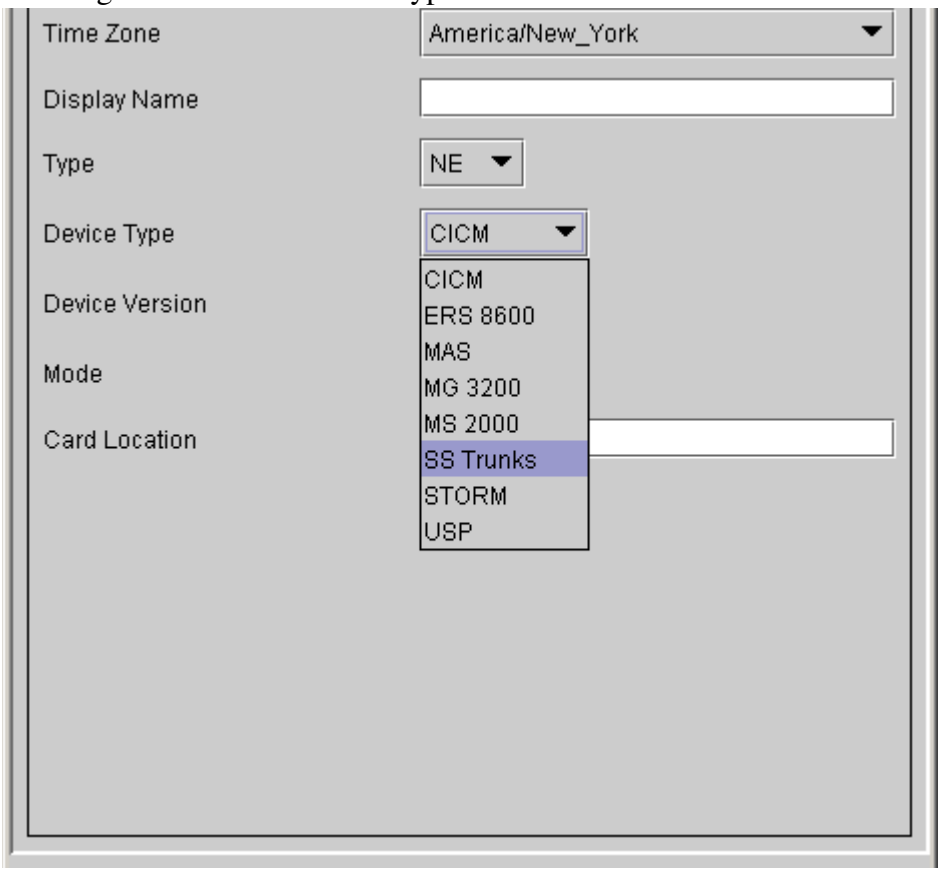
After the add node is selected, select Type as NE

Figure 4 Selecting Type as NE



Then the Device Type of SS Trunks is chosen:

Figure 5 Select Device Type of SS Trunks

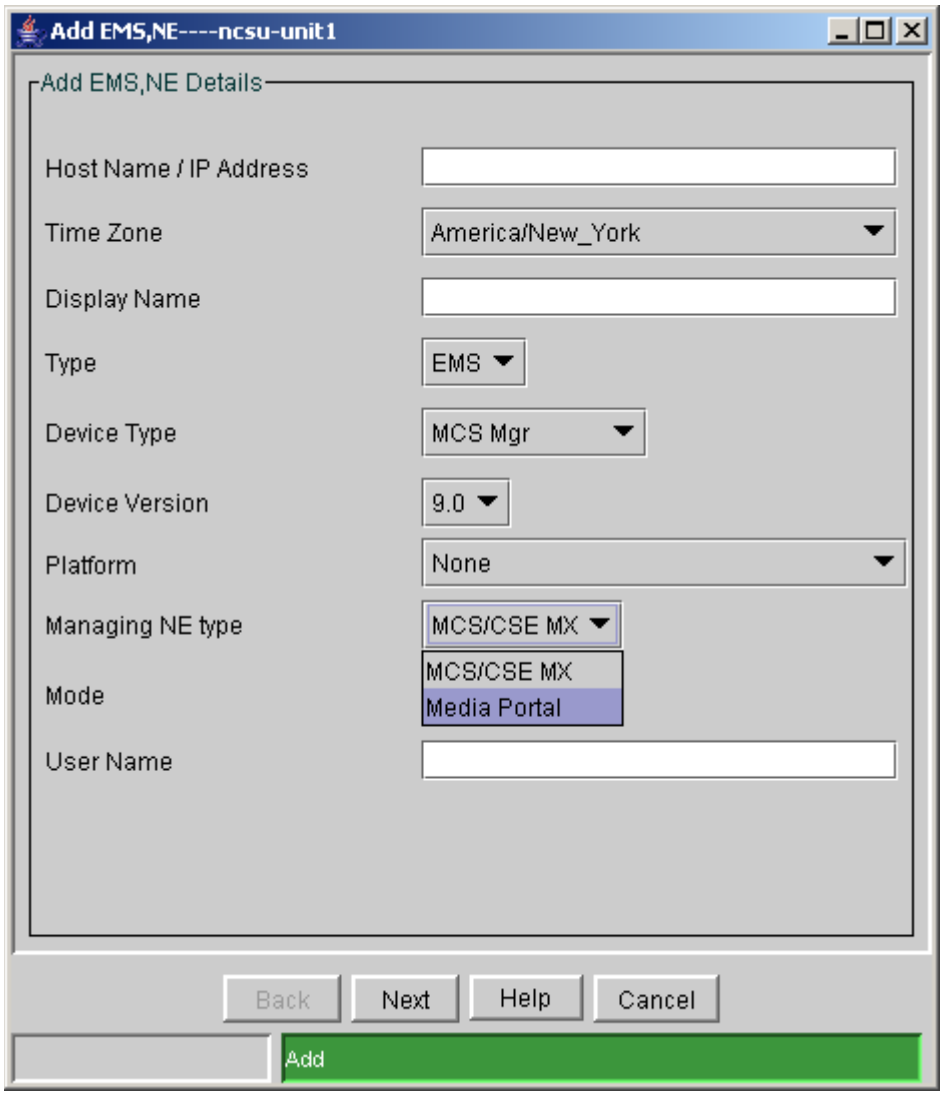


All configuration after the Device Type is chose is the same as SN08, please see the SN08 documentation for details.

45.5 Change of configuration for Media Proxy to Media Portal

The Media Proxy NE type has been changed to Media Portal as shown below.

Figure 6 Addition of MCS with Media Portal as NE



45.6 Configuring Session Managers for SSH launch

There is a requirement to be able to launch SSH directly to the Session Managers. To fulfill this requirement a new option needs to be added to allow the configuration of these Session Managers. This new option will be allowed from the EM in the MAP for SSLines.

Figure 7 Example launch of configure session manager

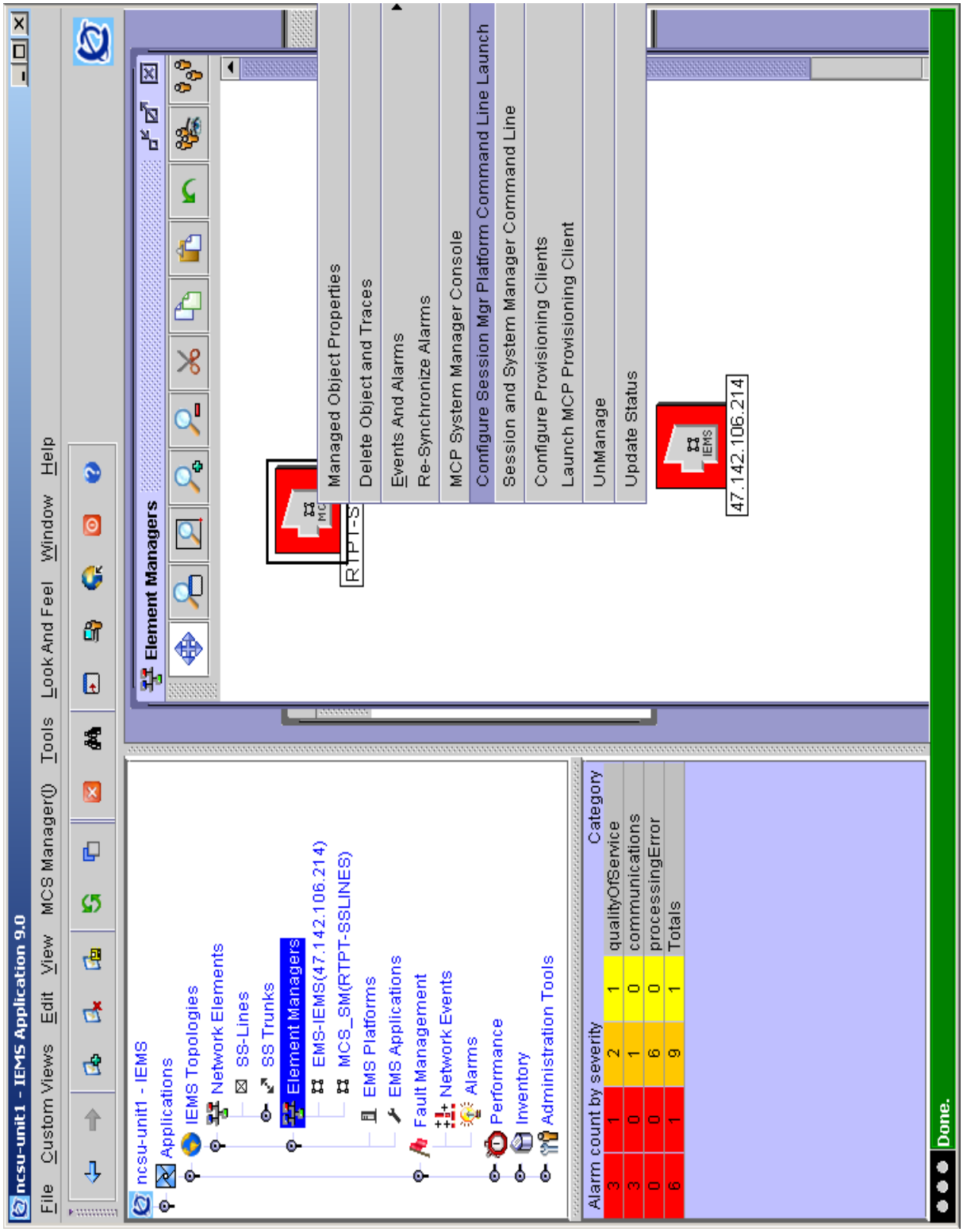


Figure 8 Or from MCS_SM map view

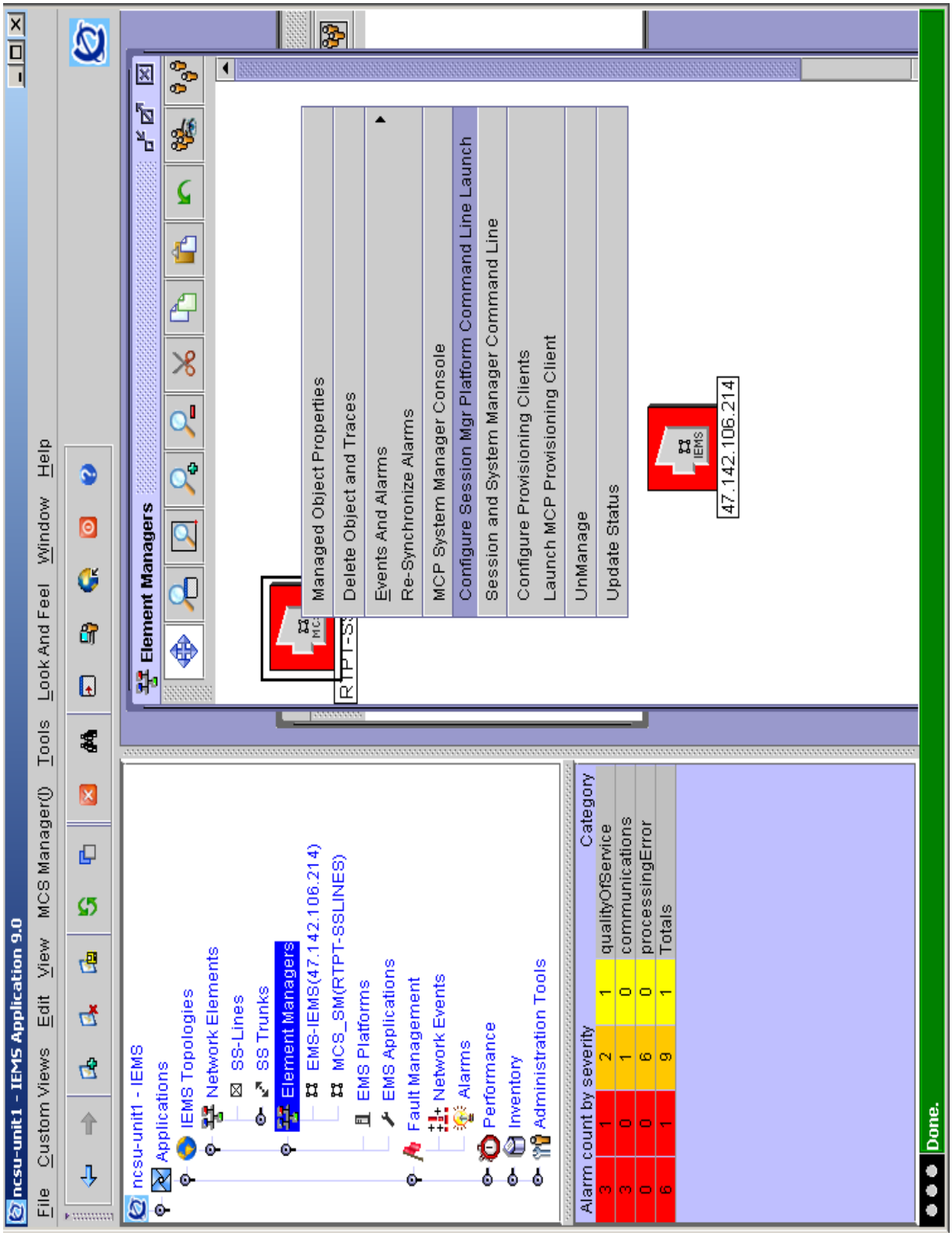
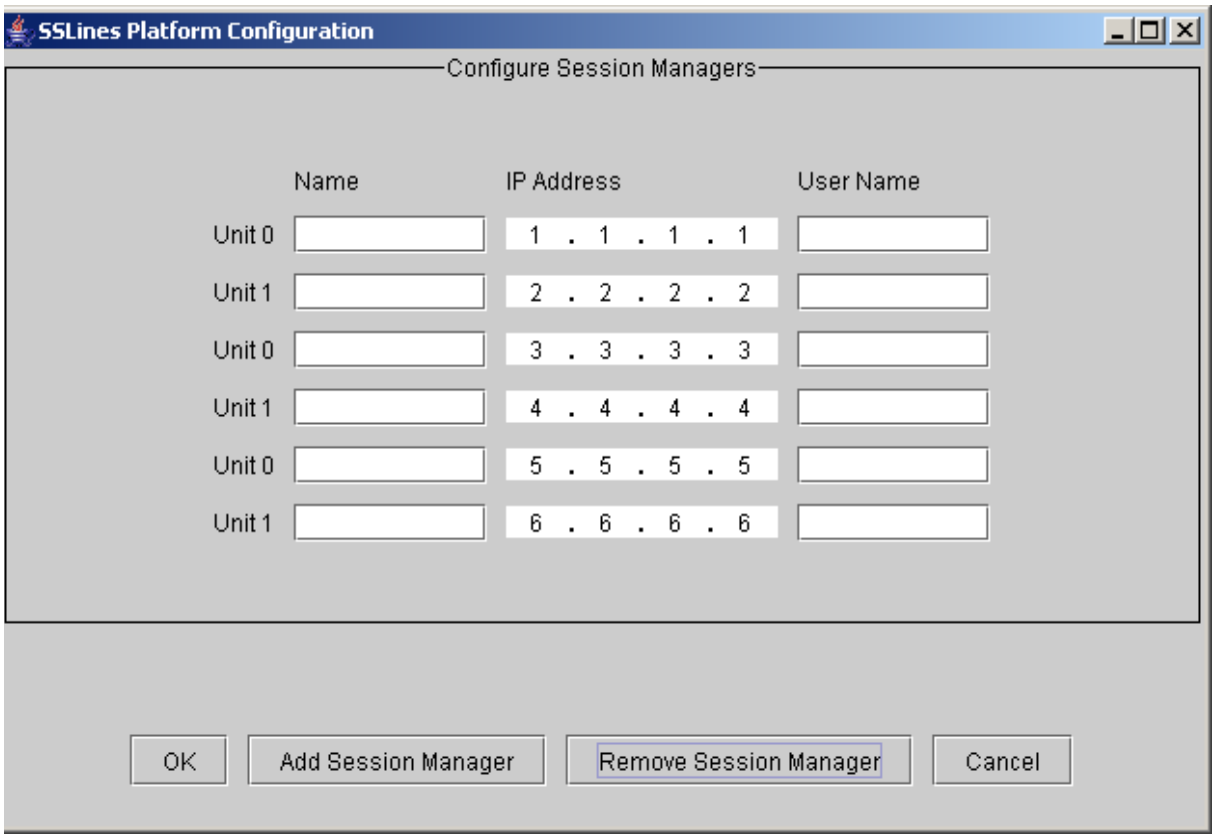


Figure 9 Configuring session managers that can have SSH launched to them



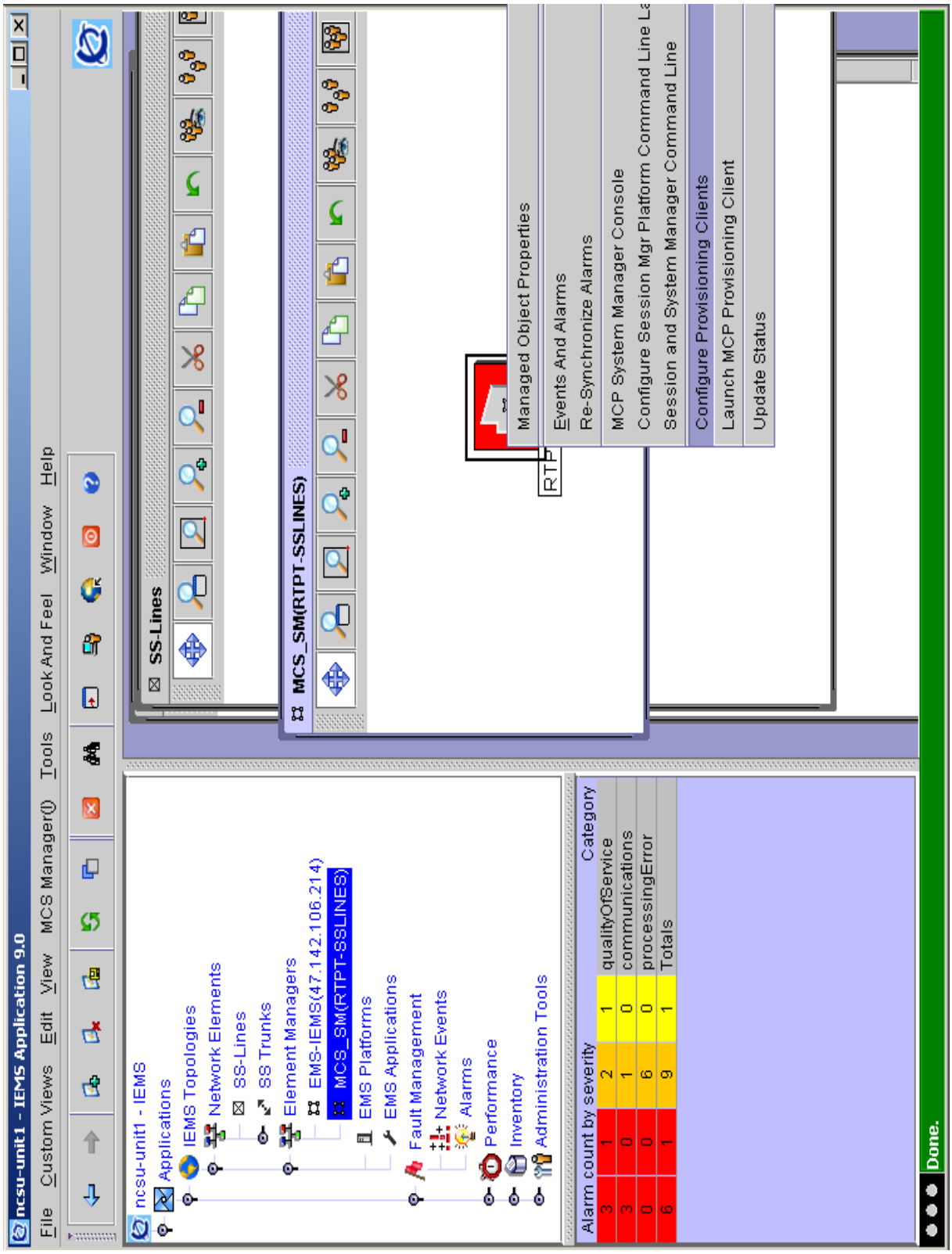
As noticed there can be 3 Session Manager pairs configured. This is a fully configured deployment.

The Add Session Manager and Remove Session Manager adds and removes a pair from the configuration screen. Only the Session Managers that are configured will be configured in the IEMS database.

45.7 Configuring Session Managers for SSH launch

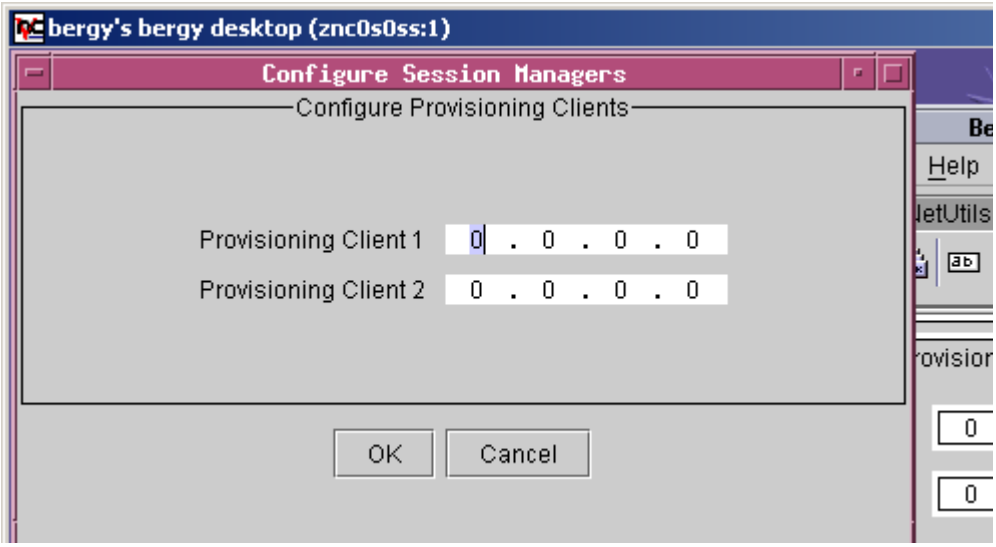
There is a requirement to be able to launch the Provisioning Client wherever they are running on the Sip lines deployment. To fulfill this requirement a new option needs to be added to allow the configuration of the IP addresses of where the provisioing servers are running. This new option will be allowed from the EM in the MAP for SSLines. These are not duplex or clustered.

Figure 10 Example launch of configuring Provisioning Client



The configuration of the provision clients can be done from either the MCS_SM map or from the Element Managers Map. Until the configuration is done, the provisioning clients cannot be launched.

Figure 11 Configuring Provisioning Clients for later launch



After the configuration the following dialog will be displayed.As the dialog indicates the WEBSERVER requires a restart prior to launching the provisioning client.The commands on the sspfs to restart the WEBSERVER is

servrestart WEBSERVER

Figure 12 Restart WEBSERVER dialog

45.8 Configuring the apache proxy using CLI

The apache webserver on the IEMS server machine must be configured to proxy https communication between the SSLines manager and its client and also between the povisioning webservers and the provisioning client. Both will be configured using the SSPFS cli tool.

The proxy configuration must be manually removed when the SSL lines platform is deprovisioned from IEMS.

Provisioning client proxy

An entry is required for each proisioning webserver IP. This the provsioning IP entered in the “SSL Lines Platform Configuration” frame in section 12.5.

Procedure (adding an entry):

1. Login into the IEMS server box as root and invoke the “cli” command:

#cli

Select option 2 (Configuration), then option 2 (Apache Proxy Configurration), then option 1 (add_proxy_conf).

2. Configure the proxy as shown below:

When prompted for the proxy IP address enter the address of the provisioning webserver.

When prompted for the “hostname/tag associated the IP” again enter the address of the provisioning web server.

When propmpted for the optional remote hostname/tag , leave blank and hit “Enter”

When prompted for the port number enter the value “8443”

Answer “Y” when prompted to restart the Apache server.

Repeat the steps above for the other provisioning client IP address.

The session below shows the proxy configuration for provisioning web server at IP address 47.142.23.24:

 # cli

Command Line Interface

1 - View

2 - Configuration

3 - Other

X - exit

select - 2

Configuration

1 - NTP Configuration

2 - Apache Proxy Configuration

3 - DCE Configuration

4 - OAMP Application Configuration

5 - CORBA Configuration

6 - IP Configuration

7 - DNS Configuration

8 - Syslog Configuration

9 - Database Configuration

10 - NFS Configuration

11 - Bootp Configuration

12 - Restricted Shell Configuration

13 - Security Services Configuration

14 - Login Session

15 - Location Configuration

16 - Cluster Configuration

17 - Succession Element Configuration

18 - snmp_poller (SNMP Poller Configuration)

19 - backup_config (Backup Configuration)

X - exit

select - 2

Apache Proxy Configuration

1 - add_proxy_conf (Add an IP to the Apache Proxy Module configuration)

2 - del_proxy_conf (Delete an IP from the Apache Proxy Module configuration)

3 - list_proxy_conf (List the Apache Proxy Module configuration)

X - exit

select - 1

=== Executing "add_proxy_conf"

Enter proxy IP address (X to exit): 47.142.23.24
Enter hostname/tag associated with IP 47.142.23.24: 47.142.23.24
Optional, enter remote hostname/tag associated with IP 47.142.23.24:
Enter port number [443]: 8443
Accept the following values:
IP Address = 47.142.23.24
Hostname = 47.142.23.24
Remote Tag =
Port Num = 8443
!!WARNING!! This will result in WEBSERVER going down (restarting) for a short time
Continue? [Y/N]:Y
Stopping group using servstop
Apache Web Service Stopping
WEBSERVER Stopped

Starting WEBSERVER through servstart
Updated alarm successfully.
Found valid security certificate, starting Web Services with SSL support...
Apache Web Service Starting
WEBSERVER Started

=== "add_proxy_conf" completed successfully

Apache Proxy Configuration
1 - add_proxy_conf (Add an IP to the Apache Proxy Module configuration)

2 - del_proxy_conf (Delete an IP from the Apache Proxy Module configuration)

3 - list_proxy_conf (List the Apache Proxy Module configuration)

X - exit

select - select - (X, 1-3) X

Procedure (removing an entry):

The procedure for removing a proxy entry is virtually identical to the procedure for adding an entry:

1. Login into the IEMS server box as root and invoke the “cli” command:

#cli

Select option 2 (Configuration), then option 2 (Apache Proxy Configurration), then option 1 (del_proxy_conf).

2. Delete the proxy entry by entering the provisioning IP address and port number when prompted.

The example session snippet below shows the IP address 47.142.24.23 being removed from the configuration:

Apache Proxy Configuration:

1 - add_proxy_conf (Add an IP to the Apache Proxy Module configuration)

2 - del_proxy_conf (Delete an IP from the Apache Proxy Module configuration)

3 - list_proxy_conf (List the Apache Proxy Module configuration)

X - exit

select - 2

=== Executing "del_proxy_conf"

Enter proxy IP address (X to exit): 47.142.23.24

Optional, enter remote hostname/tag associated with IP 47.142.23.24:

Enter port number [443]: 8443

Accept the following values:

IP Address = 47.142.23.24

Remote Tag =

Port Num = 8443

!!WARNING!! This will result in WEBSERVER going down (restarting) for a short time

Continue Removal? [Y/N]:

Enter proxy IP address (X to exit): 47.142.23.24

Optional, enter remote hostname/tag associated with IP 47.142.23.24:

Enter port number [443]: 8443

Accept the following values:

IP Address = 47.142.23.24

Remote Tag =

Port Num = 8443

!!WARNING!! This will result in WEBSERVER going down (restarting) for a short time

Continue Removal? [Y/N]:Y

Stopping group using servstop

Apache Web Service Stopping

WEBSERVER Stopped

Starting WEBSERVER through servstart

Alarm exists, updating alarm...

ComponentID: CLASS=SEC;CLASSTYPE=EXPIRED;SUBTYPE=HTTPSCERT;FILE=validcert.ksh

Updated alarm successfully.

Found valid security certificate, starting Web Services with SSL support...

Apache Web Service Starting

WEBSERVER Started

=== "del_proxy_conf" completed successfully

SSLines Management console proxy:

The configuration for the SSLines management console is identical to the provisioning client configuration above except for the port number and IP address used:

- When prompted for proxy IP address, use the address on which the management server resides.
- Use 12121 for the port number.

Below is an example session snippet for configuring proxy for server on IP address 47.142.200.69:

Apache Proxy Configuration

1 - add_proxy_conf (Add an IP to the Apache Proxy Module configuration)

2 - del_proxy_conf (Delete an IP from the Apache Proxy Module configuration)

3 - list_proxy_conf (List the Apache Proxy Module configuration)

X - exit

select - 1

=== Executing "add_proxy_conf"

Enter proxy IP address (X to exit): 47.142.200.69

Enter hostname/tag associated with IP 47.142.200.69: 47.142.200.69

Optional, enter remote hostname/tag associated with IP 47.142.200.69:

Enter port number [443]: 12121

Accept the following values:

IP Address = 47.142.200.69

Hostname = 47.142.200.69

Remote Tag =

Port Num = 12121

!!WARNING!! This will result in WEBSERVER going down (restarting) for a short time

Continue? [Y/N]:Y

46: Configuration (CN): A00012183

46.1 Feature Name

Public Key Manager

46.2 Hardware and Software Requirements

PKManager is bundled as part of the IEMS package. The manager application shares the IEMS platform dependencies.

46.3 Initial Configuration

Initial installation of the PKManager will be performed as part of the IEMS installation. The installation procedure will require changes to allow the PKManager servlet and web clients to be launched securely on initial startup. Currently, the certificate for Apache on SSPFS must be manually installed before secure communications over HTTPS can occur.

The IEMS installation script currently checks for an Apache certificate before allowing installation to proceed. With PKManager, the user now has the option to use their own certificate (from a third party - for example) or to allow the installation script to generate one automatically. The installation will prompt the user to select the certificate *mode* to use for the WebPKProxy (used by Tomcat) certificate: **“Create” or “Managed”**

- If **Managed Mode**, then the user will be prompted to enter the path for the certificate he wants to use. Once entered, new scripts will import the certificate into the PKManager database and install the certificate in the appropriate directory for Tomcats’ use.
- If **Create Mode** is chosen, then the user will be prompted to enter values for Distinguished Name components used in certificate generation. These include the following:

  Common Name, country, region, locality, email address, Organization name, organization unit name, and company.

The installation scripts will then generate a new certificate, add it to the PKManager database for tracking, and install it for Tomcat usage.

The user will have the ability to change these default settings for the distinguished name through the PKGUI. See Section 46.6.2.2 on page 2738 for screen details.

46.4 Upgrade Considerations

46.4.1 Dump and Restore (CM)

N/A

46.4.2 Element Management Upgrade

N/A

46.4.3 Downgrade impact

N/A

46.5 Data schema (DS) (CM, MIBS, RDB)

46.5.1 New/modified tables, MIBs, or Database Schema

New tables used by PKManager -- none

46.6 Element Management

IEMS

This feature integrates the Public Key Manager application with IEMS to provide the following capabilities from the IEMS GUI:

- Add the Public Key Manager as an application to IEMS topology
- View PKManager alarms on IEMS
- Launch the PKManager GUI client from IEMS using single sign-on.

Public Key Manager GUI (PKGUI)

The PKGUI is a web-based user interface that provides a set of user screens for certificate administration and management tasks. On successful login, the user is directed to a home page presenting links to various functions and displaying configuration and state information for the application and its registered clients.

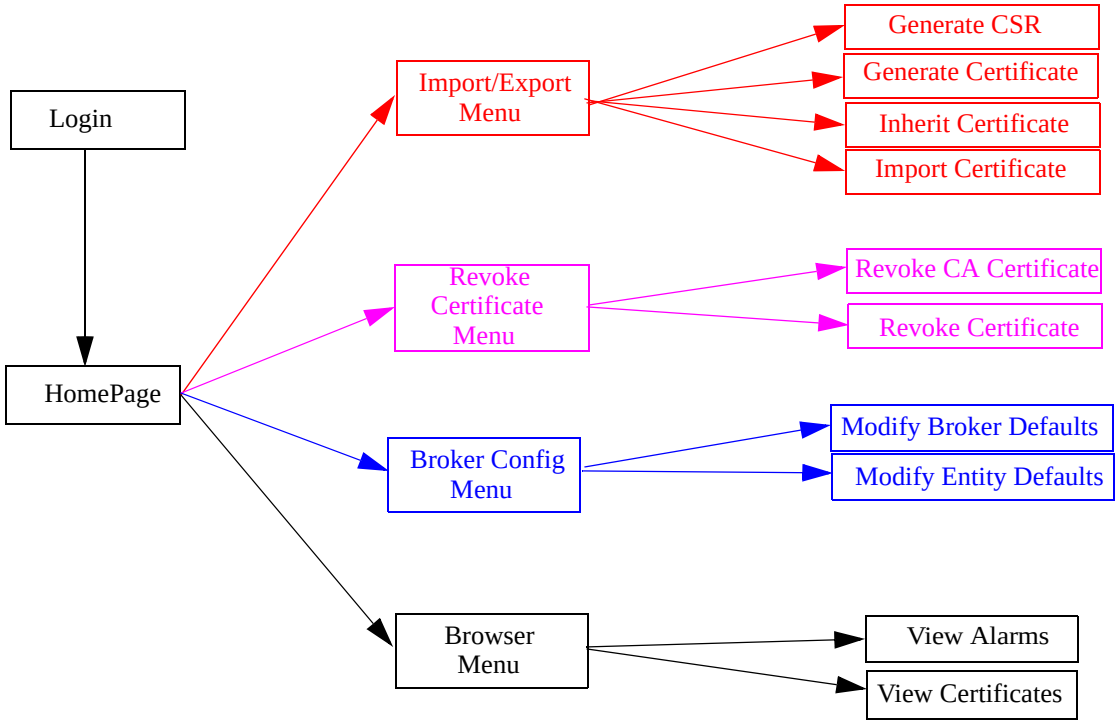
User Authorization Note: This tool restricts access to users belonging to the authorization groups “secadm” and “secro”. All operations in the GUI will check for group membership before allowing access to a given operation. The group “secadm” is used to permit all operations in this tool; while “secro” is used to permit viewing and browsing only. See “PKGUI Auth Groups and Operations Mapping” on page 2764 for mapping details.

46.6.1 New/modified GUIs

Table 1 New GUIs for PKManager Web Application

GUI name	NEW, CHANGED, or DELETED
1. PK Manager Home	NEW
2. Broker Configuration Menu	NEW
3. Import/Export Menu	NEW
4. Revoke Certificate Menu	NEW
5. Browser menu (read-only)	NEW
6. Modify Broker Defaults - Section 46.6.2.1 on page 2736	NEW
7. Configure Entity Defaults -Section 46.6.2.2 on page 2738	NEW
8. Generate CSR for Export -Section 46.6.2.3 on page 2740	NEW
9. Import Certificate for Integrated/NonIntegrated Client - Section 46.6.2.4 on page 2744	NEW
10. Create Integrated/Non-Integrated Certificate for Export - Section 46.6.2.5 on page 2747	NEW
11. Inherit Certificate - Section 46.6.2.6 on page 2750	NEW
12. Revoke Certificate - Section 46.6.2.7 on page 2752	NEW
13. Revoke CA Certificate - Section 46.6.3.1 on page 2754	NEW
14. View Certificates - Section 46.6.4.1 on page 2755	NEW
15. View Certificate Details - Section 46.6.4.2 on page 2757	
16. View Alarms - Section 46.6.4.3 on page 2759	NEW
17. View Alarm Details - Section 46.6.4.4 on page 2761	NEW

PKGUI Screen Flow



46.6.2 GUI information

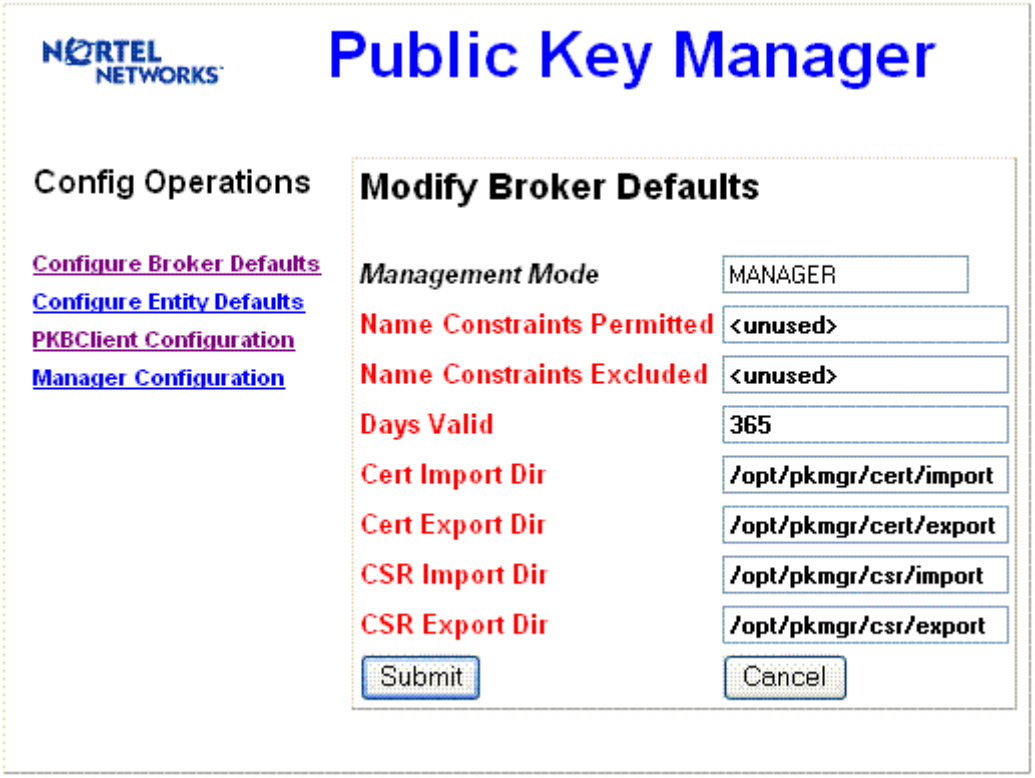
46.6.2.1 GUI name: Modify Broker Defaults

46.6.2.1.1 Functional description

The Modify Broker Defaults screen is accessed from the Broker Configuration link in the menu panel on the left side of the Home page. This menu will be displayed as the top-level or entry screen to the application.

This screen is intended for use during initial setup of the PKBroker application on SSPFS. It provides a simple form that allows the user to set default values for PKBroker parameters used throughout the PKGUI implementation. These defaults are saved in the PKBrokerProfile table on the PKManager server in SSPFS. The default profile name in the table is “NORTEL”.

Modify Broker Defaults Form



Screen Legend:
- User Input Fields
- Derived Values
- Defaults or fixed values

46.6.2.1.2 GUI usage and implications

This GUI is used to change default parameters used by the PKBroker during certificate generation and validation. Most of these parameters will be changed during initial setup and are not likely to be changed.

46.6.2.1.3 GUI fields

The following table lists fields for GUI or pull down menu “Modify Broker Defaults”.

Table 2 PKGUI - Modify Broker Defaults

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Name Constraints Permitted	NEW			This field defines the constraints the user can specify during certificate generation and validation	
Name Constraints Excluded	NEW			This field defines the constraints the PKManager will **not** include in certificate generation and validation	
Days Valid	NEW			Defines the number of days a generated certificate will be valid in the system. The certificate will expire after this period.	
Certificate Import Directory	NEW			Input directory used by PKManager to retrieve certificates for import	
Certificate Export Directory	NEW			Output directory used by PKManager for generated certificates	
CSR Import Directory	NEW			Input directory used by PKManager to retrieve certificates for import	
CSR Export Directory	NEW			Output directory used by PKManager for generated certificates	

46.6.2.1.4 Usage example
See screen shot above.

46.6.2.1.5 GUI release history update

46.6.2.1.6 Context sensitive launching information
This GUI is launched by clicking the “Modify Entity Defaults” link from the “Broker Config Sub-menu”.

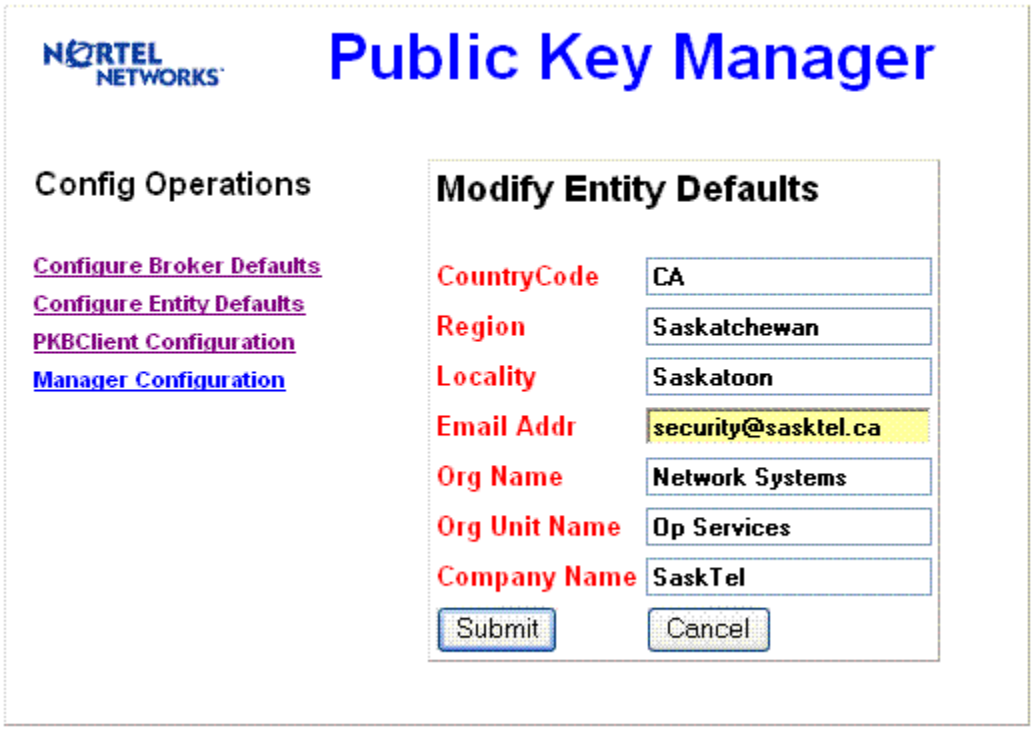
46.6.2.1.7 Supplementary information
NONE

46.6.2.2 GUI name: Modify Entity Defaults

46.6.2.2.1 Functional description
This screen allows the user to change the default Distinguished Name components used by the PKManager to generate certificates and requests.

This screen is intended for use during initial setup of the PKBroker application on SSPFS. It provides a simple form that allows the user to set default values for Distinguished Name parameters used for certificate management and generation. Configure Entity Defaults Form

Entity Defaults screen (prototype)



46.6.2.2.2 GUI usage and implications

This screen is intended for use during initial setup of PKManager - before it is used to generate a managed certificate or CSR. The customer has the option to set these values to their own customer values. These default values should not be changed once they are set.

46.6.2.2.3 GUI fields

The following table lists fields for GUI or pull down menu “Modify Entity Defaults”.

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Country	NEW			2 character country code	
Region	NEW			State/Province/other	
Locality	NEW			City	
Email Address	NEW			email address	
Org Name	NEW			Organization Name	
Org Unit Name	NEW			Organization Unit Name	
Company	NEW			Company Name	

46.6.2.2.4 Usage example

The following example shows sample datafill or menu selection for GUI "Modify Entity Defaults" (also see screenshot above):

- Country: *US*
- Region: *North Carolina*
- Locality: *Raleigh*
- Email Address: *security@nortelnetworks.com*
- Organization Name: *Succession*
- Organization Unit Name: *OAM Security*
- Company Name: *Nortel*

46.6.2.2.5 GUI release history update

46.6.2.2.6 Context sensitive launching information

This GUI is launched by clicking the "Modify Entity Defaults" link from the "Broker Config Sub-menu".

46.6.2.2.7 Supplementary information

NONE

46.6.2.3 GUI name: Generate CSR for Export

46.6.2.3.1 Functional description

This screen will allow the user to generate a certificate request for submission to an external certificate authority. The user is required to manually enter the Entity ID and IP address of the certificate host. The EntityType will be selected from a drop-down menu containing the list of integrated devices to choose from.

Generate CSR for Export (proto)

Screen Legend:

User Input Fields

Derived Values

Defaults or fixed values

46.6.2.3.2 GUI usage and implications

46.6.2.3.3 GUI size

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory

46.6.2.3.4 GUI fields

The following table lists fields for GUI or pull down menu “Generate CSR for Export”.

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
EntityType	NEW		MG9KEM, MG9K, GWCEM, GWC, WebPKProxy	Selector (integrated devices only)	
EntityID	NEW			hostname of entity	
IP Address	NEW			IP address of entity	
Common Name	NEW			**Derived** value == <entityID> <IPAddress>	
Subject Alt Name	NEW			**Derived** value== <IP Address>	
Cert Request				Certificate request output file. Derived value == <entityID>CSR.pem	

Note: All Subject fields in the GUI are read-only and provided by the values set in the “Modify Entity Defaults” screen.

46.6.2.3.5 Usage example

The following example shows sample datafill or menu selection for GUI “Generate CSR for Export”:

The user is required to enter data for the following fields:

- ***Entity Type*** - list of **integrated** device types
- ***EntityID*** - this is a typically a hostname by convention

- ***IP address*** - (e.g.: 47.142.144.127)

The following fields comprise the Subject and are **NOT** configurable by the user from this screen. Values for these fields are loaded from the *EntityDefault* table.

Defaulted Fields (Subject)

Country Code
Region
Locality
Email Address
Organization Name
Organization Unit Name
Company Name

**Note: the above defaults are set during initial setup of the PKBroker and should NOT be changed. This is done through the "Configure Broker Defaults" screen.

Derived Fields:

The following fields are derived from the entered data. They include the following:

Common Name - derived by concatenating the entityID and IP address fields. The combined fields are delimited by the space character.

Example:
entityID = wnc0s0qh.us.nortel.com
IP=47.142.144.127
Common Name = "wnc0s0qh.us.nortel.com 47.142.144.127"

Subject Alternate Name - this field is assigned the IP address entered.

Certificate Request Output file - certificate request output files will always end with the suffix: **"**CSR.pem**".** The suffix is appended to the Entity ID to derive the final file name.

example: EntityID = wnc0s0qh
CSR file = wnc0s0qhCSR.pem

The files are generated to the default target directory: **/opt/pkmgr/csr/export.**

46.6.2.3.6 GUI release history update

46.6.2.3.7 Context sensitive launching information

This GUI is launched by clicking the "Generate CSR for Export" link from the "Import/Export Sub-menu".

46.6.2.3.8 Supplementary information

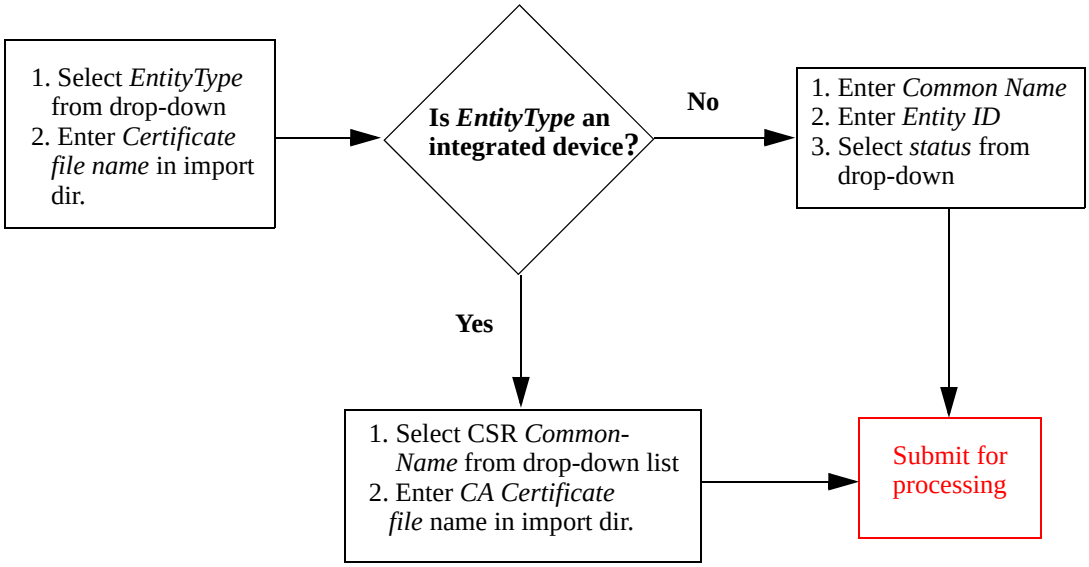
NONE

46.6.2.4 GUI name: Import Certificate

46.6.2.4.1 Functional description

This screen will allow the user to manually import certificates for expiration monitoring for a supported device. Most fields on this screen are common for both **integrated and non-integrated** devices. Certificates to be imported for integrated devices must be matched with a corresponding CSR from the database. In this scenario, a drop-down menu will be displayed to choose from available CSRs in the database. The operation integration "type" will be determined by the EntityType selected by the user and set appropriately in the PKBRequest object passed to the server.

Import Certificate - GUI Datafill Flow



46.6.2.4.2 GUI usage and implications

This screen is launched when selected from the Import/Export menu page.

Main Menu --> Import/Export Menu-->Import Certificate

46.6.2.4.3 GUI fields

The following table lists fields for GUI or pull down menu “Import Certificate”.

Table 6 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Entity Type			MG9KEM, MG9K, GWCEM, GWC, WebPKProxy,SSM	select from drop-down	
Device Certificate file				file name of Device certificate in default import directory	
CSR Common Name				Integrated devices - selected from drop-down NonIntegrated devices - entered manually by user to match import certificate	
CA Certificate file				Integrated EntityType only - file name of CA certificate in default import directory	
EntityID				NonIntegrated devices only - entered manually by user according to import certificate	
Status			Available, Unavailable	NonIntegrated devices only - select from drop-down	

46.6.2.4.4 Usage example

The following example shows sample datafill or menu selection for GUI “Import Certificate”:

User Input Fields

The user is initially presented with a single drop-down menu to select the entity type and a text box for specifying the certificate path on the server.

Common Fields:

- ***Entity Type*** - select from drop-down list
- ***Device Certificate path*** - this field is required for both import types.

When selected, the integration "type" will be determined and the screen will change as follows:

Integrated device fields:

- ***CSR Common Name*** - from drop-down list
- ***CA Certificate path*** - the file path to the CA certificate for the device cert to be imported.

If an integrated device is selected, (for example, GWCEM), then another drop-down menu will be displayed below the first containing the CommonNames of all outstanding CSRs in the database. The user can select from this list and the following fields will be auto-populated from it as read-only text:

- ***Entity ID***

Non-Integrated Device Fields:

If the entity type selected is not integrated, then additional text boxes will appear on the screen prompting the user for the following data fields:

- ***Common Name***
- ***Entity ID***
- ***Status*** - this will be entered as Active or Inactive from a drop-down menu.

Note: The default certificate import directory for all import types is:

/opt/pkmgr/cert/import.

**The user is required to place the certificate there for import.

46.6.2.4.5 GUI release history update

46.6.2.4.6 Context sensitive launching information

This GUI is launched by clicking the "Import CSR" link from the "Import/ Export Sub-menu".

46.6.2.4.7 Supplementary information

NONE
No screenshot available

46.6.2.5 GUI name: Create Certificate for Export

Create Integrated/Non-Integrated Certificate for Export

46.6.2.5.1 Functional description

Integrated and Non-Integrated devices

This screen will allow the user to generate a private key and certificate for use with a supported device. This screen is common for both Integrated and non-integrated devices. The operation integration “type” will be determined by the EntityType selected by the user and set appropriately in the PKBRequest object passed to the server.

46.6.2.5.2 GUI usage and implications

46.6.2.5.3 GUI fields

The following table lists fields or pull down menu.

- ***Entity Type*** - select from drop-down list
- ***EntityID*** - this is a typically a hostname by convention
- ***IP address*** - (e.g.: 47.142.144.127)

Table 7 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
EntityType	NEW		MG9KEM, MG9K, GWCEM, GWC, WebPKProxy	Selector (integrated devices only)	
EntityID	NEW			hostname of entity	
IP Address	NEW			IP address of entity	
Common Name	NEW			**Derived** value == <entityID> <IPAddress>	
Subject Alt Name	NEW			**Derived** value== <IP Address>	
Cert Output file	NEW			Certificate output file. **Derived** value == <entityID>Cert.pem	
Private Key file	NEW			Private Key output file. **Derived** value == <entityID>Key.pem	

User Input Fields

The user is required to enter data for the following fields:

- ***Entity Type*** - select from drop-down list
- ***EntityID*** - this is a typically a hostname by convention
- ***IP address*** - (e.g.: 47.142.144.127)

The following fields comprise the Subject ID and are **NOT** configurable by the user from this screen. Values for these fields are loaded from the *EntityDefault* table.

Defaulted Fields (Subject)

Country Code
Region
Locality
Email Address
Organization Name
Organization Unit Name
Company Name

**Note: the above read-only defaults are set during initial setup of the PKBroker and should NOT be changed. This is done through the "Configure Entity Defaults" screen.

Derived Fields:

The following fields are derived from the entered data. They include the following:

Common Name - derived by concatenating the entityID and IP address fields. The combined fields are delimited by the space character.

Example:
entityID = wnc0s0qh.us.nortel.com
IP=47.142.144.127
Common Name = "wnc0s0qh.us.nortel.com 47.142.144.127"

Subject Alternate Name - this field is assigned the IP address entered.

Certificate Output file - certificate output files will always end with the suffix: **"**Cert.pem**".** The suffix is appended to the Entity ID to derive the final file name.

Private Key Output File - certificate output files will always end with the suffix: **"**Key.pem**".** The suffix is appended to the Entity ID to derive the final file name.

example: EntityID = wnc0s0qh
cert file = wnc0s0qhCert.pem
key file = wnc0s0qhKey.pem

Note: Output files are saved in the export directory specified in the Broker Defaults screen. The default target directory is: **/opt/pkmgr/cert/export.**

46.6.2.5.4 Usage example

The following example shows sample datafill or menu selection for GUI "Create Certificate for Export":

Create Certificate for Export Screen (prototype)

Screen Legend:
User Input Fields

Derived Values
Defaults or fixed values

46.6.2.5.5 GUI release history update

46.6.2.5.6 Context sensitive launching information

This GUI is launched by clicking the “Create Certificate forExport” link from the “Import/Export Sub-menu”.

46.6.2.5.7 Supplementary information

NONE

46.6.2.6 GUI name: Inherit Certificate

46.6.2.6.1 Functional description

This screen is used to manually import a WebPKProxy certificate generated by a commercial or external certificate authority. By doing so the certificate management and monitoring services of the PKManager are obtained. This enables a purchased and the valid certificate to continue to be used.

46.6.2.6.2 GUI usage and implications

46.6.2.6.3 GUI size

Table 8 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory

46.6.2.6.4 GUI fields

The following table lists fields or pull down menu.

Table 9 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Common Name	NEW			Common Name entered to match that of certificate being imported	
Entity ID	NEW			EntityID entered to match that of certificate being imported	

Table 9 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Device Certificate filename	NEW			Device certificate filename	
CA Cert or Cert Chain file name	NEW			CA Certificate file name **OR** Certificate Chain file name	

Note: Import files must be placed in default import directory set in "Configure Broker Defaults" screen. The default certificate import directory for all import types is:

/opt/pkmgr/cert/import.

46.6.2.6.5 Usage example

The following example shows sample datafill or menu selection for GUI "Inherit Certificate":

<no screen shot available>

User Input Fields

The user is presented with a number of text boxes that must be manually populated to match the configuration of the certificate being imported.

- ***Common Name*** - entered manually in text box
- ***Entity ID*** - entered manually in text box
- ***Device Certificate file name***
- ***CA Certificate* or *Certificate Chain file name***

Note: The default certificate import directory for all import types is:

/opt/pkmgr/cert/import.

The user will be required to place the certificate there for import.

46.6.2.6.6 GUI release history update

46.6.2.6.7 Context sensitive launching information

This GUI is launched by clicking the "Inherit Certificate" link from the "Import/Export Sub-menu".

46.6.2.6.8 Supplementary information

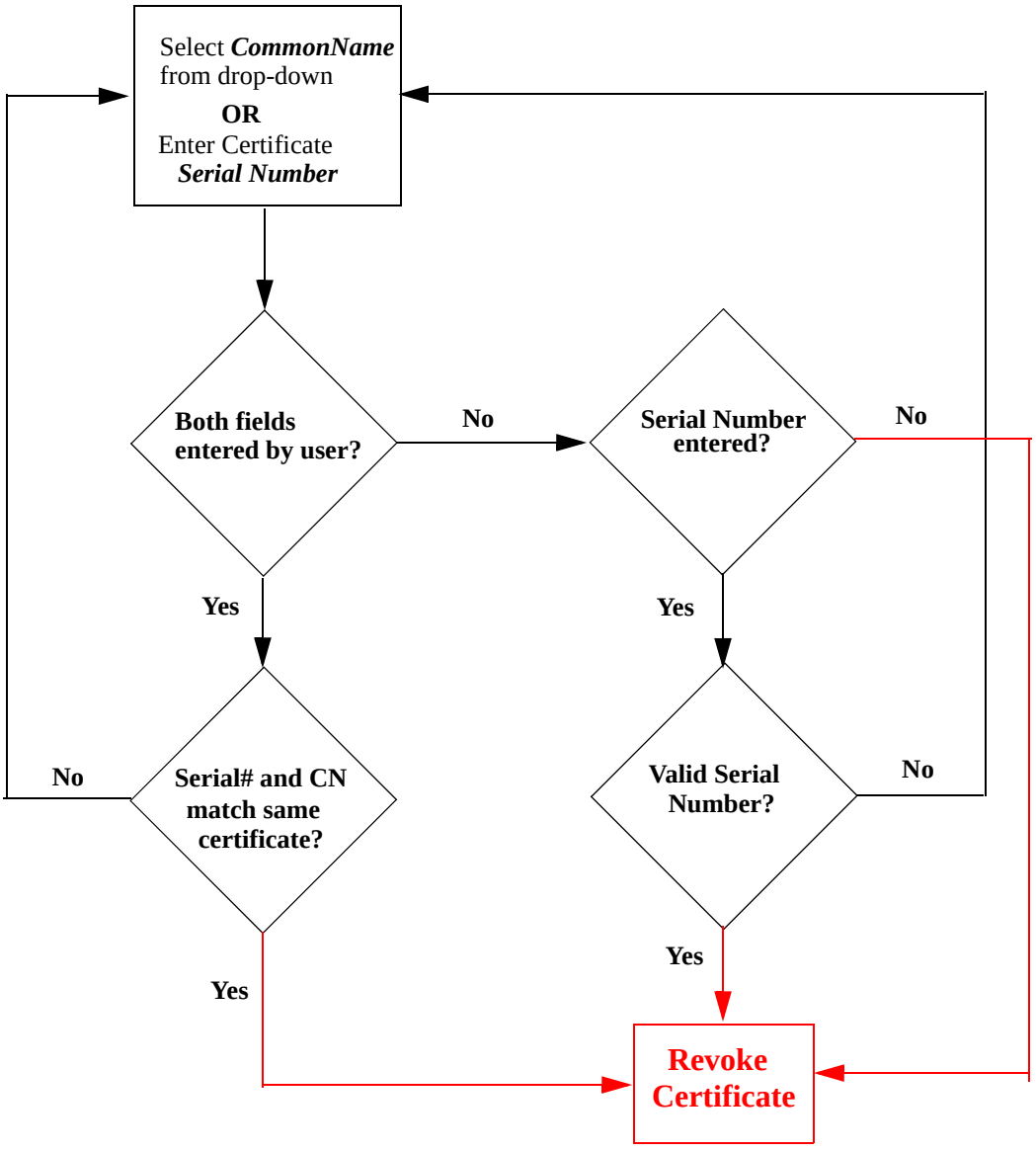
NONE

46.6.2.7 GUI name: Revoke Certificate

46.6.2.7.1 Functional description

This screen will allow the user to manually revoke any certificate that is monitored by the PKManager. ***Integrated device certificates*** that are revoked result in creation and delivery of replacement certificates to their original downstream clients.

Revoke Certificate - GUI Datafill Flow



46.6.2.7.2 GUI usage and implications

46.6.2.7.3 GUI fields

The following table lists fields for GUI or pull down menu “Revoke Certificate”.

Table 10 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Input Type	NEW		Radio Button	activates the input field to use: drop-down or text box	
Common Name	NEW		activated by radio button	Selector - drop-down list of certificate common names is presented for selection	
Serial Number	NEW		activated by radio button selection	User has option to directly enter the serial number of the certificate to revoke	

46.6.2.7.4 Usage example

The following example shows sample datafill or menu selection for GUI “Revoke Certificate”:

<screen-shot not available >

The user can specify a certificate to revoke in one of two ways:

- Select the certificate from a drop-down menu of certificate Common Names
- Enter the Serial Number of the certificate directly

If both fields are datafilled by the user, a check is performed to ensure the serial number entered matches the serial number of the certificate selected by Common Name. If only one field is used (as is the intended use - for convenience), then the certificate information is retrieved for the selected or entered certificate and used to populate the missing data in the other field.

46.6.2.7.5 GUI release history update

46.6.2.7.6 Context sensitive launching information

This GUI is launched by clicking the “Revoke Certificate” link from the “Revoke Certificate Menu”.

46.6.2.7.7 Supplementary information

46.6.3 GUI information

46.6.3.1 GUI name: Revoke CA Certificate

46.6.3.1.1 Functional description

Revoke CA Certificate is used to immediately revoke a CA certificate that is monitored by the PKManager. ***This operation should be used with extreme caution*** as it will cause the PKManager to initiate certificate replacements for **ALL** certificates generated and managed by the PKManager.

This screen will allow the user to select a root CA from a drop-down menu. This selection will be limited to one of the following

Common Names: (static drop-down)

- **PKBRoot**
- **PKBCA**

The initial screen will also display a warning to the user about the potential danger of this operation.

Once a selection has been made and the user submits the form data, an pop-up window will be presented asking the user to confirm the operation should proceed.

Since this operation could take a significant amount of time to run, all other GUI operations that modify data will be blocked. An error message will be displayed in the footer panel during this time for such operations. “View Certificates” and “View Alarms” screens will still be available for use.

*Note: Only users with “**secadm**” group membership will be permitted to run this command.*

User Input Fields

The user is initially presented with a single drop-down menu to select the root CA certificate by Common Name.

- **Common Name** (will be PKBRoot or PKBCA)

Following the application-wide convention, database or system error messages will be added to the request context and displayed in the footer window in red using the <html:errors> tag.

46.6.3.1.2 GUI usage and implications

46.6.3.1.3 GUI fields

The following table lists fields or pull down menu for “Revoke CA Certificate”.

Table 11 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Common Name	NEW		PKBRoot, PKBCA	Common Name Select from drop-down	

46.6.3.1.4 Usage example

The following example shows sample datafill or menu selection:

<no screen-shot available>

The user is initially presented with a single drop-down menu to select the root CA certificate by Common Name.

- **Common Name** (will be PKBRoot or PKBCA)

Following the application-wide convention, database or system error messages will be added to the request context and displayed in the footer window in red using the <html:errors> tag.

46.6.3.1.5 GUI release history update

46.6.3.1.6 Context sensitive launching information

This GUI is launched by clicking the “Revoke Certificate” link from the “Revoke Certificate Menu”.

46.6.3.1.7 Supplementary information

NONE

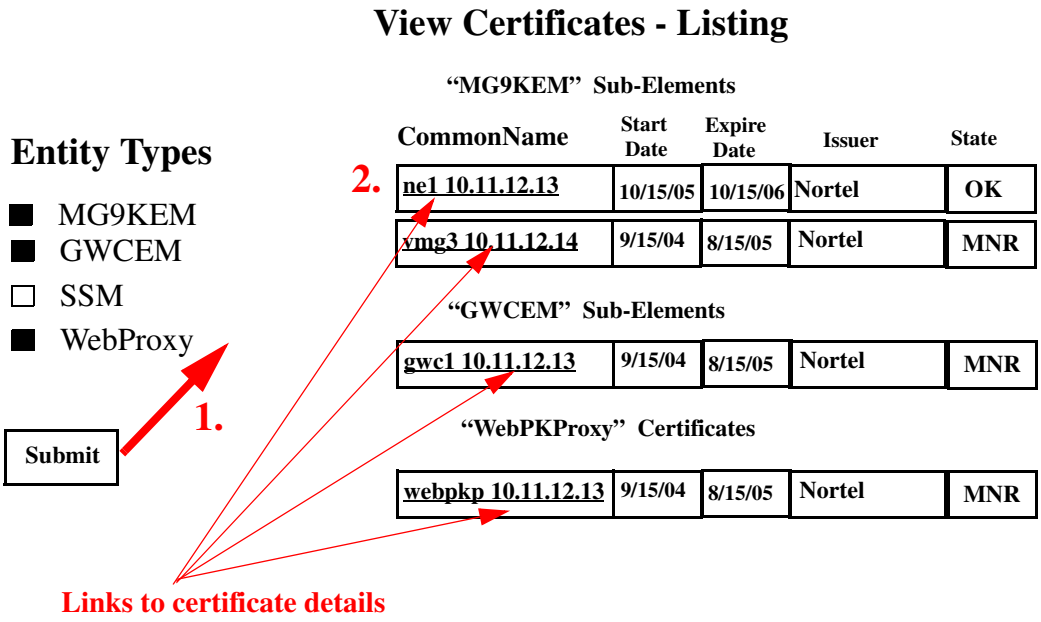
46.6.4 GUI information

46.6.4.1 GUI name: View Certificates

46.6.4.1.1 Functional description

This screen provides the user with the ability to browse certificates according to their entity type (device) hierarchy. The user has the ability to choose one or more entity types from which a database query will be launched to retrieve the associated data. A table of certificate summary information will be displayed. Next to each item listed will be a “View Details” button that will forward the

user to another screen displaying full contents of a specific certificate (see next GUI screen section). Entity types that logically contain sub-components (for example, MG9K contains VMGs), an additional *"List <childEntityType>s"* button will be provided next to the entry to list a summary of the sub-components. When selected, the sub-components summary are listed in the same format as the parent types. Each NE listed for the MG9K, for example, would have a button next to it called "List VMGs".



46.6.4.1.2 GUI usage and implications

Certificate Browser usage

1. User selects entity types to list in the certificate summary and clicks on submit to retrieve data. The representation above illustrates the fields retrieved for display and the strategy used to navigate.

2. The certificates are listed according to their manager types or category - if not managed.

46.6.4.1.3 GUI fields

The following table lists fields or pull down menu.

Table 12 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Common Name	NEW		Display field	Common Name of certificate	
Start Date	NEW		Display field	“Not Before” validity date of certificate	
End Date	NEW		Display field	“Not after” validity date of certificate	
Issuer	NEW		Display field	Name of certificate Issuer	
Status	NEW		Display field - must be one of: ok, maj, mnr	certificate expiration state	

46.6.4.1.4 Usage example

The following example shows sample datafill or menu selection for GUI “View Certificates”:

<screen-shot not available>

46.6.4.1.5 GUI release history update

46.6.4.1.6 Context sensitive launching information

This GUI is launched by clicking the “View Certificates” link from the “Certificate Browser Menu”.

46.6.4.1.7 Supplementary information

NONE

46.6.4.2 GUI name: Certificate Details

46.6.4.2.1 Functional description

This screen displays a form containing a detailed listing of a specified certificate’s fields.

46.6.4.2.2 GUI usage and implications

This screen depends on the “View Certificates” screen in the previous section to specify a certificate to view. It is selected from the listed provided by that screen.

46.6.4.2.3 GUI fields

The following table lists fields or pull down menu.

Table 13 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Issued to			display only	Common Name	
Version			display only	version (3)	
Serial Number			display only	Serial Number	
Issuer			display only	Issuer	
Valid from			display only	start date of certificate validity	
Valid to			display only	expiry date of certificate	
Subject		Common Name, country, region, locality, email, org, org unit, company	display only	display components of subject	
Constraints			display only	as listed as defined in certificate	
Signature Algorithm			display only	md5RSA	

46.6.4.2.4 Usage example

The following example shows sample datafill or menu selection for GUI "View Details":

This screen is launched by clicking the "Common Name" link for a listed certificate in the "View Certificates" screen.

<screen-shot not available>

46.6.4.2.5 GUI release history update

46.6.4.2.6 Context sensitive launching information

This screen is launched from the view certificates screen by right-clicking on a listed certificate link.

46.6.4.2.7 Supplementary information

NONE

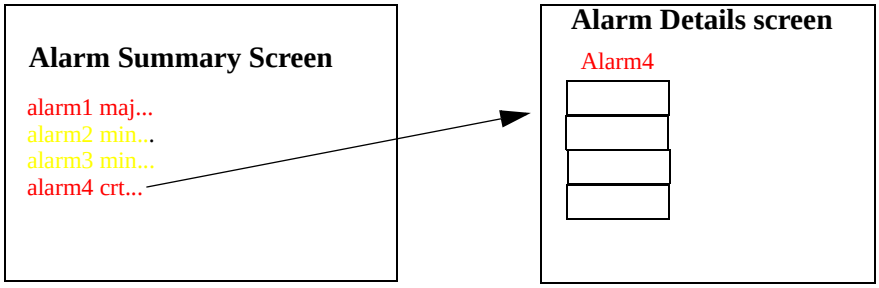
46.6.4.3 GUI name: View Alarms

46.6.4.3.1 Functional description

This screen

This menu selection will display a summary of the current set of active alarms raised by the PKBroker in the main “Body” tile of the display screen. Each alarm listed will be displayed as a hyperlink that will provide full alarm details when clicked. The following tables provide a breakdown of the fields in each.

Alarm Viewer logical screen flow



46.6.4.3.2 GUI usage and implications

This GUI is launched from the “View Alarms” sub-menu of the “Browser Menu”.

46.6.4.3.3 GUI fields

The following table lists fields for GUI or pull down menu “View Alarms”.

Table 14 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
DateTime	NEW		read-only	Date/time of alarm	
LogName	NEW		read-only	Log name as defined in log stream	
Log Number	NEW		read-only	log number as defined in log stream	

Table 14 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Severity	NEW		read-only	Maj, min, info	
Event Label	NEW		read-only	description of fault	

46.6.4.3.4 Usage example

The following example shows sample datafill or menu selection for GUI:

PKManager Alarm Summary table

The following alarms will be used to demonstrate the fields displayed in the summary and detail views.

RTP2 * PKM304 SEP26 18:25:00 0401 TBL PKM First Alarm Forewarning of a Certificate Expiration
Location: PKManager=wnc0s0jd
NotificationID: 20492
State: Raise
Category: Advanced Warning
Cause: First alarm warning of impending X509 certificate expiration
Time: SEP26 18:25:00 2005
Component Id: PKManager
Specific Problem: A certificate will expire soon CN, GWC-2 42.45.123.16
Description: Initial forewarning of an impending certificate expiration

RTP2 ** PKM301 SEP23 18:25:00 0401 TBL PKM Certificate delivery failure
Location: PKManager=wnc0s0jd
NotificationID: 20092
State: Raise
Category: Processing Error
Cause: Failed to deliver an X509 certificate
Time: SEP23 18:25:00 2005
Component Id: PKManager
Specific Problem: Failed to deliver a certificate for CN, GWC-2 42.45.123.16
Description: Attempt deliver a certificate to an application for a device failed.

Table 15 Example Content of Alarm Summary display

DateTime	OfficeID	LogName	LogNum	Severity	EventLabel
SEP23 18:25:00	RTP2	PKM	301	MAJ	Certificate delivery failure
SEP26 18:25:00	RTP2	PKM	304	MIN	First Alarm Forewarning of a Certificate Expiration

Note** - each row will be a hyperlink to display full details described in Section 46.6.4.4 on page 2761. Text color RED for critical and major alarms. Yellow for minor.

46.6.4.3.5 GUI release history update

46.6.4.3.6 Context sensitive launching information

46.6.4.3.7 Supplementary information

46.6.4.4 GUI name: Alarm Details

46.6.4.4.1 Functional description

46.6.4.4.2 GUI usage and implications

46.6.4.4.3 GUI fields

The following table lists fields or pull down menu.

Table 16 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Severity	NEW		read-only	Maj, min, info	
Date Time			read-only	MMMMDD hh:mm:ss	
LogName	NEW		read-only	Log name as defined in log stream	
Log Number	NEW		read-only	log number as defined in log stream	
Sequence Number	NEW		read-only	sequence number	
Event Type	NEW		read-only CBSY', 'EXC ', 'FAIL', 'FLT ', 'INFO', 'INIT', 'LO ', 'MANB', 'OFFL', 'PASS', 'PBSY', 'RTS ', 'SUMM', 'SYSB', '**TBL** ', 'TRAN', 'TRAP', 'UNEQ'.	from NTSTD/SCC2 log header	

Table 16 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Device ID	NEW		read-only value: PKM	device identifier for PKManager	
Event Label	NEW		read-only	description of fault	
Location	NEW		read-only	device location	
Notification ID	NEW		read-only	id of event sent by PKManager	
Category	NEW		read-only	alarm type category	
Cause	NEW		read-only	cause description	
Component ID	NEW		read-only	fault identifier	
Specific Problem	NEW		read-only	problem text with component info	
Description	NEW		read-only	detailed problem text	

46.6.4.4.4 Usage example

The following example shows sample datafill or menu selection for GUI "Alarm Details":

This screen is launched by clicking on an entry in the "Alarm Summary" page. A new screen with the following fields will be displayed

Table 17 Alarm Details Display Contents

Field	Example
Severity	MAJ
LogName	PKM
LogNumber	301
Day Time	SEP23 18:25:00 2005
Sequence Number	20092
EventType	TBL
Device ID	PKM
EventLabel	Certificate delivery failure
Location	PKManager=wnc0s0jd

Table 17 Alarm Details Display Contents

Field	Example
Notification Id	0-65535
Category	Processing error
Cause	Failed to deliver a certificate
Component Id	PKManager
SpecificProblem	Failed to deliver a certificate for CN, GWC-2 42.45.123.16
Description	Attempt deliver a certificate to an application for a device failed

46.6.4.4.5 GUI release history update

46.6.4.4.6 Context sensitive launching information

This screen is launched from the “Alarm Summary” by clicking on one of the summary rows (displayed as a link).

46.6.4.4.7 Supplementary information

NONE

46.6.5 CLUI Interface

NONE

46.7 User interface changes

46.8 OSSGate Interface Changes

46.9 Security

Security

Login

- standard SSPFS-based central security mechanism. Session management handled by common mechanisms. Inactivity timeout and session ID validation for each requested operation

User Authorization and Operations

Table 18 PKGUI Auth Groups and Operations Mapping

	GUI Operation	Auth Group(s) permitted
1.	**Login**	secadm, secro
2.	**Modify Broker Defaults**	secadm
3.	**Configure Entity Defaults**	secadm
4.	**Generate Certificate for Export**	secadm
5.	**Generate Certificate Request**	secadm
6.	**Import Certificate**	secadm
7.	**Revoke Certificate**	secadm
8.	**Revoke CA Certificate**	secadm
9.	**Inherit Certificate**	secadm
10.	**View Certificates**	secadm, secro
11.	**View Alarms**	secadm, secro

46.9.1 Network configuration

46.9.2 Key management

46.9.3 Protocol

46.9.4 Authentication

46.10 PKManager Configuration Walkthrough

1 User invokes IEMS installation script using existing procedure

2 Installation scripts detect if a managed certificate is already installed and prompts the user to enter one of the following selections:

- Use existing managed certificate (this is for IEMS upgrade only). Selecting this option will result in no further user input being needed for certificate management.
- Create a new CertificateL - this will prompt the user to enter values for Distinguished name components (see initial config section)
- Import a new, externally generated certificate - the user will be prompted to enter the path of the certificate to be imported and managed for use.

3 The appropriate conf script is invoked to ensure a certificate is in place before proceeding

4 IEMS installation proceeds as before.

46.11 MG9KEM Configuration

46.11.1 Hardware and Software Requirements

46.11.1.1 MG9kEM

Standard Media Gateway 9000 Element Manager (MG9000 EM) configuration.

46.11.2 Initial Configuration

46.11.2.1 MG9kEM

Standard Media Gateway 9000 Element Manager (MG9000 EM) configuration.

46.11.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

46.11.4 Upgrade Considerations

46.11.4.1 Dump and Restore (CM)

46.11.4.2 Element Management Upgrade

46.11.4.3 Downgrade impact

46.11.4.4 MG9kEM

The new Mg9kEM PKI support capabilities are only supported for Mg9k gateways running SN09.x or newer software loads. If a Mg9k uses PKI for securing its OAMP or CallP channel, it cannot be downgraded to a SN09 or earlier load unless the PKI option is removed.

46.11.5 Data schema (DS) (CM, MIBS, RDB)

N/A

46.11.6 Service Orders (SO) (CM & SESM)

N/A

46.11.7 Software optionality control (SOC)

N/A

46.11.8 Element Management - Mg9kEM

46.11.8.1 New/modified GUIs

Table 19 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
MG9000 Provisioning View	CHANGED
NE Properties View	CHANGED
GW Security Config panel	CHANGED

46.11.8.2 GUI name: MG9000 Provisioning View

46.11.8.2.1 Functional description

This is an existing view. This view is used for the initial commissioning of a NE.

46.11.8.2.2 GUI usage and implications

The MG9000 Provisioning View is updated to include a new “Use Certificate” option. With this new “Use Certificate” option, during the initial NE commissioning, the user can specify whether the NE intends to utilize PKI for securing the OAMP channel.

46.11.8.2.3 GUI fields

Table 20 GUI field descriptions

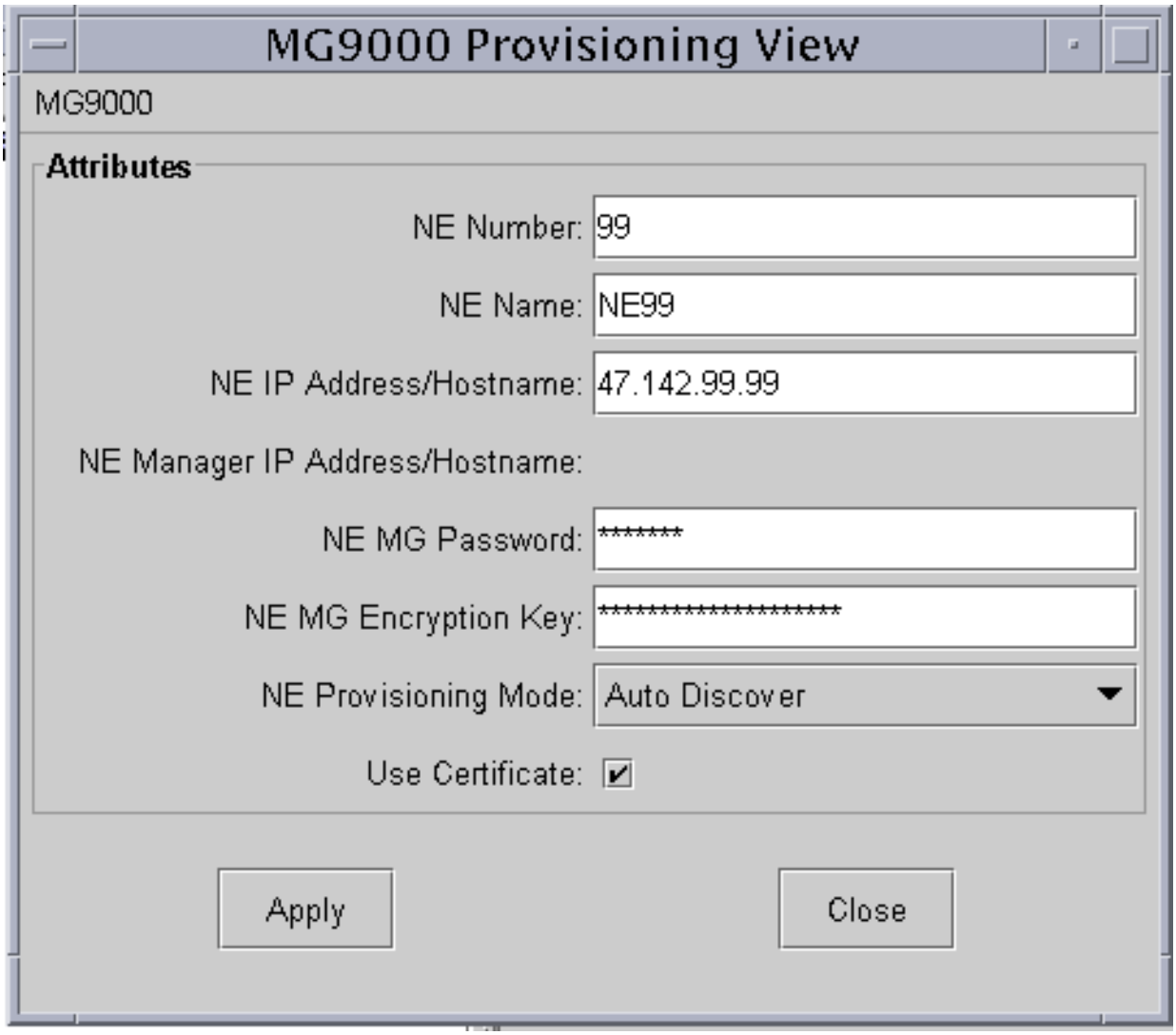
Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Use Certificate	new			whether the NE intents to use PKI for securing its OAMP channel	

46.11.8.2.4 Usage example

To launch the GUI, from the Mg9kEM Subnet GUI, click on the “Configuration” pulldown menu, then select the “Add new MG9000 NE...” from the list. Once the view is displayed, the user may fill in all the parameters for the NE and if PKI is required for securing the OAMP channel between the EM and the NE, the “Use Certificate” check box should be selected.

Note: Before provisioning a NE to use PKI, provisioning steps at the LCI and SSM are required. For details on how to fully provision the NE to use PKI, please refer to the initial commissioning procedures in the Configuration Walkthrough section.

Here is an example of the view:



46.11.8.2.5 GUI release history update

46.11.8.2.6 Context sensitive launching information

This view is accessible from the Mg9kEM Subnet View

46.11.8.2.7 Supplementary information

46.11.8.3 GUI name: Properties View

46.11.8.3.1 Functional description

This is an existing view. This view is used to display or modify NE specific attributes.

46.11.8.3.2 GUI usage and implications

The Properties View is updated to include a new “Use Certificate” option. The user can use this view to view or modify the PKI setting that controls the security for the OAMP channel.

Two additional display fields are added to Properties View:

- Last Pushed Certificate

  This field displays the serial number of the last device certificate that was successfully downloaded to Mg9k.

- Latest Certificate

  This field displays the serial number of the latest device certificate received from the PKBroker.

Normally, if PKI is in use for this NE, these two fields should contain the same serial number. However, if for some reason, the Mg9k does not have the latest certificates available, the two fields would not match. A manual certificate download can be initiated to push the latest certificates to the gateway.

46.11.8.3.3 GUI fields

.

Table 21 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Use Certificate	new			whether the NE intents to use PKI for securing its OAMP channel	
Last Pushed Certificate	new			the serial number of the last device certificate that was successfully downloaded to Mg9k	
Latest Certificate	new			the serial number of the latest device certificate received from the PKBroker	

46.11.8.3.4 Usage example

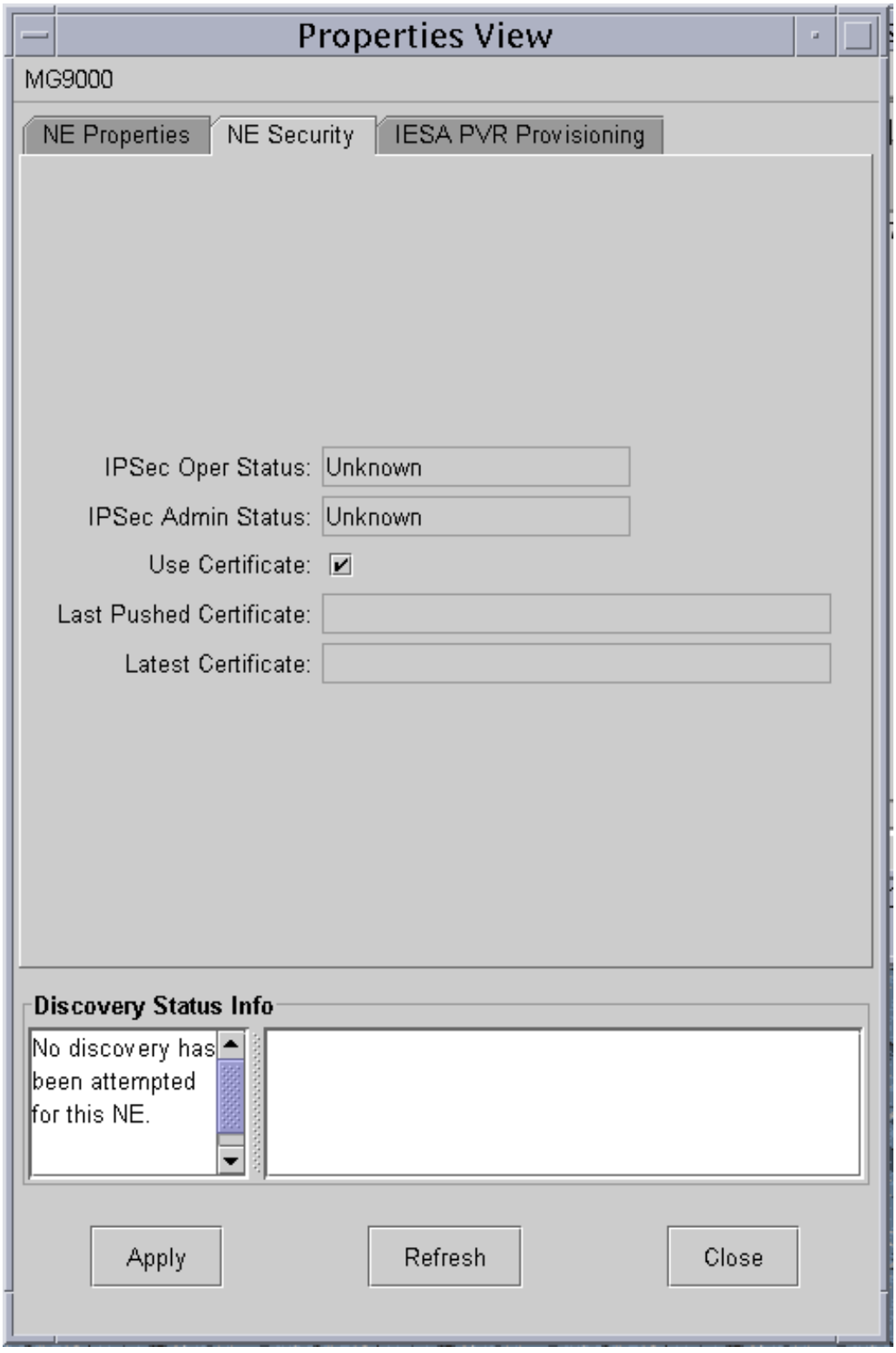
To launch the GUI, select a NE from the Mg9kEM Subnet GUI then click on the “Configuration” pulldown menu, then select the “View/Modify NE

Properties...” from the list. Once the view is displayed, the user may view or change the PKI setting for the NE by selecting the “NE Security” tab and manipulating the “Use Certificate” setting from the GUI.

> **Note:** To avoid unexpected communication loss between the EM and the NE, proper procedures should be followed when modifying the PKI option for the NE. Please refer to the procedures in the Configuration Walkthrough section for more details.

Assuming the “Use Certificate” indicator is already set for the NE, if for some reason, a manual certificate download is required to re-send the certificates to the gateway, the “Apply” button can be use to initiate the certificate download request.

Here is an example of the view:



46.11.8.3.5 GUI release history update

46.11.8.3.6 Context sensitive launching information

This view is accessible from the Mg9kEM Subnet View

46.11.8.3.7 Supplementary information

46.11.8.4 GUI name: GW Security Config panel

46.11.8.4.1 Functional description

This is an existing view. This view is used to configure security information for the call control channel between the Mg9k and the GWC.

46.11.8.4.2 GUI usage and implications

The GW Security Config panel is updated to include a new selector where the user can specify whether the VMG intends to use certificate, preshared key for securing it callp link. When the “Use Certificate” option is specified, the EM will, start the process to retrieve and download the certificates to the gateway. The user can continue with the remaining VMG provisioning steps without waiting for the certificate download to complete. However, the gateway will not enable call processing for this VMG until it has successfully received and processed the VMG certificates from the E

The GW Security panel will also contain a new option to allow the user to explicitly trigger a certificate download request.

Prior to this feature, the GW Security Config panel is an optional panel during VMG provisioning. With this feature, this panel will become a required step during VMG provisioning. When provisioning a new VMG, the GW Security Config panel will be presented as part of the VMG provisioning progression. The user will have to select the type of security the VMG will use.

46.11.8.4.3 GUI fields

Table 22 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Security Infrastructure	new	Certificates or Preshared Key		whether the VMG intends to use PKI or PSK for securing its callp channel	
Last Pushed Certificate	new			the serial number of the last device certificate that was successfully downloaded to Mg9k	

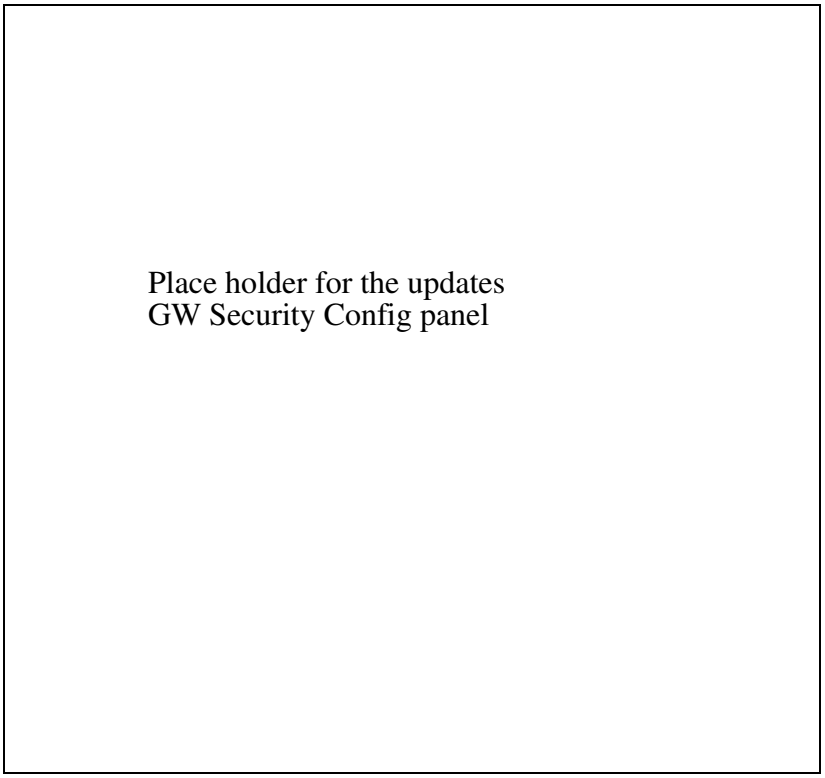
Table 22 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Latest Certificate	new			the serial number of the latest device certificate received from the PKBroker	

46.11.8.4.4 Usage example

More details to come.

Here is an example of the view:



46.11.8.4.5 GUI release history update

46.11.8.4.6 Context sensitive launching information

This view is accessible from the Mg9kEM Switched Line Services View.

46.11.8.4.7 Supplementary information

46.11.9 User interface changes

N/A

46.11.10 OSSGate Interface Changes

N/A

46.11.11 Security

46.11.11.1 MG9kEM

Only users in the “emsrw” or “emsadm” group are authorized to setup or modify the PKI related options for the NE (i.e. OAMP link). This is consistent with other NE specific provisioning actions.

Only users in the “emssprov”, “emsrw” or “emsadm” group are authorized to setup or modify the PKI related options for the VMGs (i.e. Callp links). This is consistent with other VMG specific provisioning actions.

46.11.12 Configuration Walkthrough

46.11.12.1 Mg9kEM - OAMP link with PKI

The following procedures should be followed when provisioning and modifying the security setting for the OAMP channel between the Mg9kEM and the Mg9k.

Overall Assumptions:

1. The certificate for the EM box itself is already installed and working. Setting up PKI for the EM box itself is not covered here.
2. With the exception of the “Initial Commissioning” procedure, all other procedures assume:
   a. Mg9k is fully discovered
   b. Mg9k is at 9.x+ load
   c. OAMP link between the EM and the Mg9k is up and running.
3. Enabling security for the Mg9k is done from the LCI; not from the EM.
4. The following transition scenarios are covered by this document:
   — no security to PKI
   — PSK to PKI
   — PKI to PSK

— PKI to no security

5. The following transition scenarios are part of the existing IPsec functionality and are not covered by this document:

— no security to PSK

— PSK to no security

46.10.12.1.1 Initial commissioning

Assumptions: none

Procedure:

1. At the LCI, commission the Mg9k:
   a. Unlock all cards. Provision Carriers and unlock them
   b. At the DCC IPsec Config screens:
      i. select “Use Certificates” checkbox
      ii. configure remaining IPsec fields
      iii. enable security
   c. Continue the normal commissioning steps:
      i. provision OAMP parameters to give the Mg9k a presence in the network
      ii. user make notes of the fingerprint info for the Mg9k
      iii. at the completion of the provisioning steps, the Mg9k will not initiate a cold start trap to the EM; it will wait for its set of certificate files to be delivered by the EM.
2. At the SSM, add an IPsec policy and IKE entry for the OAMP link to use certificates
3. At the EM, add a new NE for the newly commissioned Mg9k:
   a. User selects the “user certificate option when provisioning the NE, and the EM performs the following checks:
      i. the IKE entry with PKI exists for this NE
      ii. Mg9k is running the 9.x+ load
      iii. Mg9k is present in the network (i.e. fingerprint available)
   b. If all the previous conditions are met, the user is presented with the Mg9k’s fingerprint for verification. Once the fingerprint is verified, the EM:
      i. gets the Mg9k’s certificates from PKManager
      ii. bundles the certificates into a tar file

iii. SFTP the certificate tar file to the Mg9k's active DCC

c. If the conditions are not met or Mg9k fingerprint verification fails, the user will have the option to create the NE without the "Use Certificate" indicator; the EM will not attempt the certificate transfer process in this case. Once the NE is created, the user can modify the NE setting to "Use Certificate" which will in turn perform all the same checks again before initiating the certificate download process.

4. Once the Mg9k receives the certificate bundle, the Mg9k:

a. validates and installs the certificates for use by Windriver IPsec stack

b. once the file is installed, it's sync'd to the mate DCC card

c. after the certificate files are functional, the Mg9k will use them to establish an SA with the EM

d. when this SA is established, a cold start trap is sent

Limitations and restrictions:

1. The IPsec and IKE provisioning is controlled at the SSM. Adding/deleting policies may result in communication loss between the EM and Mg9k.

2. The EM will only display the Mg9k fingerprint at the GUI from user initiated request.

46.10.12.1.2Transitioning from no security to PKI

Assumptions:

1. In SSM, IPsec policy does not exist for this NE

Procedure:

1. At the EM, modify the NE's setting to "Use Certificate". The EM:

a. gets the Mg9k's certificates from PKManager

b. bundles the certificates into a tar file

c. SFTP the certificate tar file to the Mg9k's active DCC

d. informs the user to complete the SSM and LCI steps

2. Once the certificate delivery to the Mg9k is successful, at the SSM, the user will add an IPsec policy and IKE entry for the OAMP link to use certificates

3. At the LCI's DCC IPsec config screens, update the IPsec configuration:

a. select "Use Certificates" checkbox

b. configure remaining IPsec fields

c. enable security

d. the Mg9k will:

i. establish the SA with the EM

ii. send nnIpsecCertifDownload trap to EM

Limitations and restrictions:

1. the communication link between the Mg9k and the EM will be down during the time when the IPsec policy is in affect but the security for the Mg9k is not yet enabled n from the LCI. (i.e. between steps 2 and 3)

46.10.12.1.3 Transitioning from PSK to PKI

Assumptions:

1. The SSM component supports flex policy

2. In SSM, IKE entry with ***PSK*** exists for this NE

Procedure:

1. At the SSM, add an IKE entry for the OAMP link to use certificates. Since the SSM supports flex policy, the OAMP link is not affected.

Note: if IKE entry with PSK did not exist when the IKE/PKI entry is added, the communication between the NE and the EM will go down. This is really a transition from no security to PKI; steps in this section are not applicable in this case.

2. At the EM, modify the NE's setting to "Use Certificate". If the IKE entry with PKI exists for this NE and the communication channel between EM and NE is up, the EM:

a. gets the Mg9k's certificates from PKManager

b. bundles the certificates into a tar file

c. SFTP the certificate tar file to the Mg9k's active DCC

d. sets the DCC's nnIpsecConfigEtnry::nnIpsecConfigAuthenMethod field to "certificate"

e. once the Mg9k receives the certificates, the Mg9k will:

i. reestablish SA using PKI

ii. send nnIpsecCertifDownload trap to EM

3. EM will reply on the nnIpsecCertifDownload trap to indicate the NE is now using PKI. EM will continue to encrypt with PSK until it receives the nnIpsecCertifDownload trap?

4. If IKE entry with PKI does not exist for this NE or the communication channel is down between the EM and the NE, the transition attempt is blocked.

Limitations and restrictions:

46.10.12.1.4Transitioning from PKI to PSK

Assumptions:

1. The SSM component supports flex policy
2. In SSM, IKE entry with ***PKI*** exists for this NE
3. The NE on the EM is set to "Use Certificate"
4. Preshared key on the EM and the NE are both previously provisioned and they match each other

Procedure:

1. At the SSM, add an IKE entry for the OAMP link to use PSK. Since the SSM supports flex policy, the OAMP link is not affected.

   Note: if IKE entry with PKI did not exist when the IKE/PSK entry is added, the communication between the NE and the EM will go down. This is really a transition from no security to PSK; steps in this section are not applicable in this case.
2. At the EM, modify the NE's setting by ***deselecting*** the "Use Certificate" indicator. If the IKE entry with PSK exists for this NE and the communication channel between EM and NE is up, the EM:
   a. sets the DCC's nnIpsecConfigEtnry::nnIpsecConfigAuthenMethod field to "psk". Mg9k should fail the set request if it does not have the preshared key or could not transition to PSK mode
   b. the Mg9k will:
      i. reestablish SA using PSK
      ii. send nnIpsecCertifDownload trap to EM?
3. EM will reply on the nnIpsecCertifDownload trap to indicate the NE is now using PSK. EM will continue to encrypt with PKI until it receives the nnIpsecCertifDownload trap?
4. If IKE entry with PSK does not exist for this NE or the communication channel is down between the EM and the NE, the transition attempt is blocked.

Limitations and restrictions:

1. if there is a preshared key mismatch between the EM and the NE, the keys will need to be manually reconciled from the EM and/or LCI.

46.10.12.1.5 Transitioning from PKI to no security

Assumptions:

1. In SSM, only IKE entry with PKI exists for this NE
2. The NE on the EM is set to “Use Certificate”

Procedure:

1. At the SSM, the user deletes the IPsec policy and IKE/PKI entry for the OAMP link
2. At the LCI’s DCC IPsec config screen, disable security
3. At the EM, modify the NE’s setting by deselecting the “Use Certificate” indicator.
   a. If IKE entry with PKI does not exist for this NE, remove the certificate related data from the EM for this NE
   b. If only the IKE entry with PKI exists for this NE, inform the user complete the SSM and LCI steps first

Limitations and restrictions:

1. the communication link between the Mg9k and the EM will be down during the time when the IPsec policy removed but the security for the Mg9k is not yet disabled from the LCI. (i.e. between steps 1 and 2)

46.10.12.1.6 Disabling IPsec

Assumptions:

Procedure:

1. Remove all IPsec and IKE entries for the NE
2. At the LCI’s DCC IPsec config screen, disable security
3. Although not required, it’s recommended that if the NE at the EM is provisioned to “Use Certificate”, this indicator is removed from the EM.

Limitations and restrictions:

46.10.12.1.6 Certificate Recovery from Comm. Link Down

Assumptions:

1. Communication is down between the EM and the NE and certificate corruption at the Mg9k is suspected
2. The NE on the EM is set to “Use Certificate”

Procedure:

1. User confirms IP connectivity between the EM and the NE (e.g ping)
2. At the EM, user initiates a certificate download from the GUI
3. At the LCI, reconfigure other security related data as needed

Limitations and restrictions:

46.1 MG9K Configuration

46.1.1 Hardware and Software Requirements

46.1.1.1 MG9K

Standard Media Gateway 9000 configuration.

46.1.2 Initial Configuration

46.1.2.1 MG9K

Standard Media Gateway 9000 Element Manager (MG9000 EM) configuration.

46.1.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

46.1.4 Upgrade Considerations

46.1.4.1 Dump and Restore (CM)

46.1.4.2 MG9K Upgrade

46.1.4.3 Downgrade impact

46.1.4.4 MG9K

PKI support is available in SN09.x loads.

46.1.5 Data schema (DS) (CM, MIBS, RDB)

N/A

46.1.6 Service Orders (SO) (CM & SESM)

N/A

46.1.7 Software optionality control (SOC)

N/A

46.1.8 MG9K

46.1.8.1 New/modified GUIs

Table 23 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
IPSec Control	CHANGED

46.1.8.2 GUI name: LCI IPsec Control

The LCI is used to configure and control IP Security on the MG9K's Data Controller Card (DCC).

46.1.8.2.1 Functional description

This is an existing view which allows a user the select the 'Authentication Type' used by IPsec to secure the node's external IP interface.

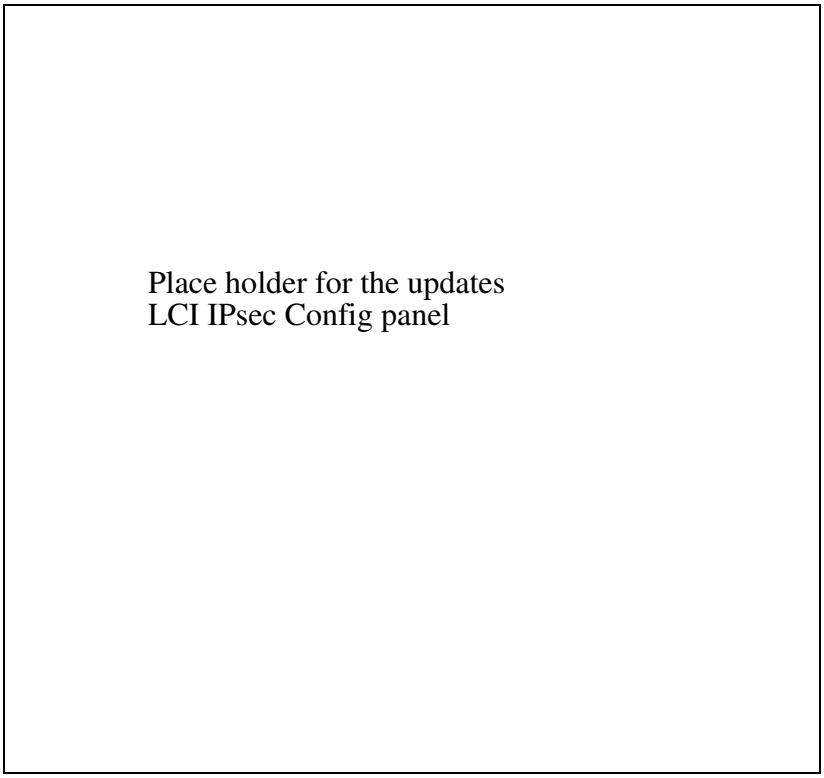
46.1.8.2.2 GUI usage and implications

The IPsec Configuration View is updated to allow the user to select authentication type of pre-shared key or Digital Certificate.

46.1.8.2.3 Usage example

The LCI is used to manage the IPsec options on the DCC card of the MG9K. Optionally, it can be used to also configure and control IP security for VMGs. For the DCC, the LCI is essential to bring a node in service with IP security enabled.

Here is an example of the view:



46.1.8.3 GUI name: LCI OAMP Control Panel

This screen is mainly used to configure the OAMP link's network parameters. It also the user to configure a preshared encryption key. This key is used to encrypt/decrypt sensitive data transferred between the MG9K and its element manager. When digital certificates are used to authenticate the IPsec channels between the MG9K and it manager, a pre-shared key is no longer required as sensitive data can be encrypted with the device certificate.

46.1.8.3.1 Functional description

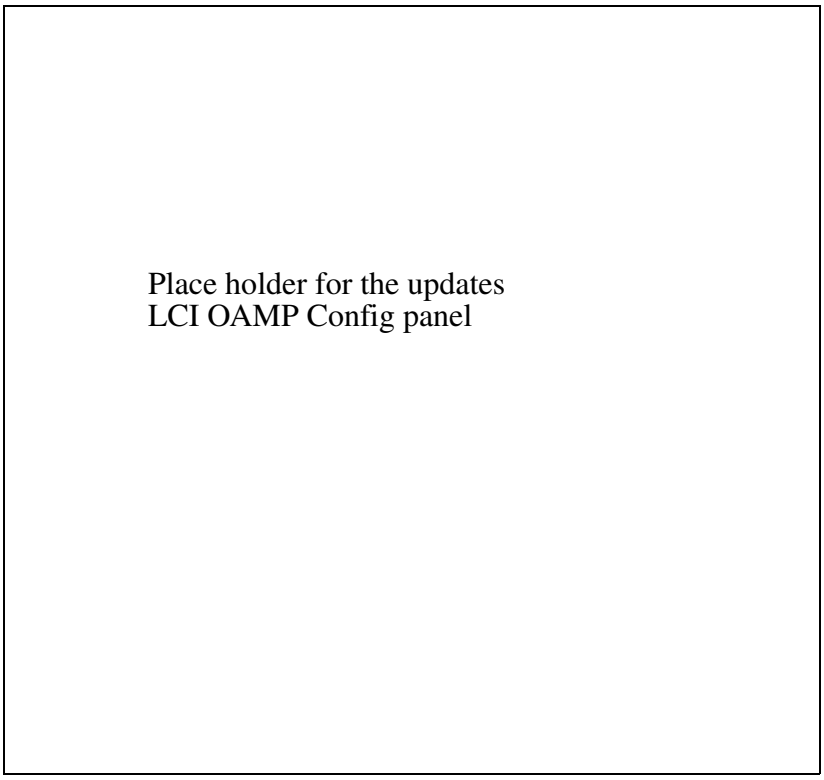
Given that it is a customer preference to authenticate IPsec with digital certificates, the OAMP config screen will no longer enforce the a key to be entered unless there is no authentication type selected.

46.1.8.3.2 GUI usage and implications

If the user chooses to configure the OAMP screen before configuring the IPSec scree, they will be asked to either enter a PSK or go back to the IPsec control screen and configure IPsec.

46.1.8.3.3 Usage example

Here is an example of the view:



46.1.9 OSSGate Interface Changes

N/A

46.1.10 Security

46.1.10.1 MG9K LCI

LCI users are ‘administrative’ users and currently have permissions for node wide changes.

46.1.11 Configuration Walkthrough

See walkthroughs in previous section.

46.2 GWC-EM Configuration

46.2.1 Hardware and Software Requirements

46.2.2 Initial Configuration

46.2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

46.2.4 Upgrade Considerations

46.2.4.1 Dump and Restore (CM)

46.2.4.2 Element Management Upgrade

46.2.4.3 Downgrade impact

When SN09.1 SESM has detected an earlier GWC load, it should only allow provisioning of a single preshared key in the new IKE Authentication dialog. Any SNMP SETs to the older GWC load must use the existing MIB tables, not the new definitions.

46.2.5 Data schema (DS) (CM, MIBS, RDB)

46.2.5.1 New/modified tables, MIBs, or Database Schema

Table 24 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ikepreferenceentry	changed	
connectionpolicyentry	changed	
IKEauthenticationentry	new	
GWC-SPD-MIB	changed	

46.2.6 Table/MIB/Remote Database Schema information

46.2.6.1 Name: MIB GWC-SPD-MIB table ikePreferenceTableV1

46.2.6.1.1 Functional description

This table clones the table ikePreferenceTable and remove the field “ikePrefAuthMethod”

46.2.6.1.2 Usage sequence and implications (CM Only)

N/A

46.2.6.1.3 Size
N/A

46.2.6.1.4 Fields/OIDs
The table oid is .1.3.6.1.4.1.562.28.0.1.4.1.7.1.18.

46.2.6.1.5 Datafill example

46.2.6.1.6 Table release history update
N/A

46.2.6.1.7 Supplementary information
N/A

46.2.6.1.8 Translation verification and other tools
N/A

46.2.6.2 Name: ikepreferenceentry
IKE preference entry

46.2.6.2.1 Functional description
This table stored the ike preference configuration by the customer. It remove the field “ikeprefauthmethod”

46.2.6.2.2 Usage sequence and implications (CM Only)
N/A

46.2.6.2.3 Size
N/A

46.2.6.2.4 Fields/OIDs
It removes the field “ikeprefauthmethod”.

46.2.6.2.5 Datafill example

Column Name	Type	Content
gwcid	VARCHAR2(32) NOT NULL	GWC-2
ikepreferenceid	NUMBER	1
ikeprefciphalg	NUMBER	1
ikeprefhashalg	NUMBER	1
ikeprefpfsgroupid	NUMBER	1

Column Name	Type	Content
ikepreflifetimesec	NUMBER	600
ikepreflifetimekb	NUMBER	0
ikeprefphase1only	NUMBER	0
ikeprefcommit	NUMBER	0
ikeprefcom- pathashid	NUMBER	0
ikeprefcompatalignpayl	NUMBER	0
ikeprefippcp4bytespi	NUMBER	0
ikeprefusecertid	NUMBER	0
ikeprefnocert	NUMBER	0
ikeprefnocertreq	NUMBER	0
ikeprefnoinitcont	NUMBER	0
ikepreferenceidstring	VARCHAR2(255)	IKE-preference

46.2.6.2.6 Table release history update
N/A

46.2.6.2.7 Supplementary information
N/A

46.2.6.2.8 Translation verification and other tools
N/A

46.2.6.3 Name: MIB GWC-SPD-MIB table connectionPolicyTableV1

46.2.6.3.1 Functional description
This table clones the table connectionPolicyTableV1 and remove the field “ipsecConnIkeRemGwId” and “ipsecConnIkePrefListId”. Adds a new field “ipsecConnIkeAuthMethodIdV1”

46.2.6.3.2 Usage sequence and implications (CM Only)
N/A

46.2.6.3.3 Size
N/A

46.2.6.3.4 Fields/OIDs
The table oid is .1.3.6.1.4.1.562.28.0.1.4.1.7.1.19.

46.2.6.3.5 Datafill example

46.2.6.3.6 Table release history update
N/A

46.2.6.3.7 Supplementary information
N/A

46.2.6.3.8 Translation verification and other tools
N/A

46.2.6.4 Name: connectionpolicyentry
Connection Policy entry

46.2.6.4.1 Functional description
This table stored the connection policy configuration by the customer. It remove the field “IPSECCONNIKEREMGWID” and “IPSECCONNIKEPREFLISTID”.

46.2.6.4.2 Usage sequence and implications (CM Only)
N/A

46.2.6.4.3 Size
N/A

46.2.6.4.4 Fields/OIDs
Remove the fields “ipsecconnikeremgwId” and “ipsecconnikepreflistid”. Add a new field “ipsecconnikeauthmethodidV1”

46.2.6.4.5 Datafill example

Column Name	Type	Content
gwcid	VARCHAR2(32) NOT NULL	GWC-2
ipsecconnpolicyid	NUMBER	1
ipsecconntransprotoc	NUMBER	0
ipsecconnlhostport	NUMBER	8999
ipsecconnlhostform	NUMBER	0
ipsecconnlocipsasel	NUMBER	0
ipsecconnlocportsasel	NUMBER	0

Column Name	Type	Content
ipsecconnrmipsasel	NUMBER	0
ipsecconnrmportsasel	NUMBER	0
ipsecconntranprotsasel	NUMBER	0
ipsecconnremgwaddr	VARCHAR2(255)	
ipsecconnpolrhost	VARCHAR2(255)	5.6.7.8
ipsecconnpolprofileid	NUMBER	1
ipsecconnpreflistid	NUMBER	1
ipsecconncertalias	VARCHAR2(255)	
ipsecconnpeercertfile	VARCHAR2(255)	
ipsecconnikeauthmethodidV1	VARCHAR2(255)	

46.2.6.4.6 Table release history update
N/A

46.2.6.4.7 Supplementary information
N/A

46.2.6.4.8 Translation verification and other tools
N/A

46.2.6.5 Name: MIB GWC-SPD-MIB table ikeAuthenticationTable

46.2.6.5.1 Functional description
This table is new table and store the ike authentication method setting.

46.2.6.5.2 Usage sequence and implications (CM Only)
N/A

46.2.6.5.3 Size
N/A

46.2.6.5.4 Fields/OIDs
the table oid is .1.3.6.1.4.1.562.28.0.1.4.1.7.1.20.

46.2.6.5.5 Datafill example

46.2.6.5.6 Table release history update
N/A

46.2.6.5.7 Supplementary information
N/A

46.2.6.5.8 Translation verification and other tools
N/A

46.2.6.6 Name: IKEauthenticationentry
IKE authentication entry

46.2.6.6.1 Functional description
This table stored the ike authentication configuration by the customer. It is a new table.

46.2.6.6.2 Usage sequence and implications (CM Only)
N/A

46.2.6.6.3 Size
N/A

46.2.6.6.4 Fields/OIDs
will be add after the MIB file definition completed.

46.2.6.6.5 Datafill example

Column Name	Type	Content
gwcid	VARCHAR2(32) NOT NULL	
ikeauthenremgwid	VARCHAR2(255)	
ikeauthpreflistid	NUMBER	
ikeauthpki	NUMBER	Disabled (0) or Enabled (1)
ikeAuthPsk1	NUMBER	Disabled (0) or Enabled (1)
ikeAuthPskHexFmt1	NUMBER	False (0), True (1)
ikeAuthPskData1	VARCHAR2(255)	

Column Name	Type	Content
ikeAuthPskTime1	NUMBER	
ikeAuthPsk2	NUMBER	
ikeAuthPskHexFmt2	NUMBER	
ikeAuthPskData2	VARCHAR2(255)	
ikeAuthPskTime2	NUMBER	

46.2.6.6.6 Table release history update
N/A

46.2.6.6.7 Supplementary information
N/A

46.2.6.6.8 Translation verification and other tools
N/A

46.2.7 Service Orders (SO) (CM & SESM)
N/A

46.2.8 Software optionality control (SOC)
N/A

46.2.9 Element Management
GWCEM

46.2.10 New/modified GUIs
Table 25 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
IKE Preference Panel	changed
Add/Change IKE Preference dialog	changed
Connection Policy Panel	changed
Add/Change Connection Policy dialog	changed
IKE Authentication panel	new
Add/Change IKE Authentication dialog	new
IKE certificate panel	new
View IKE certificate dialog	new

46.2.10.1 GUI name: IKE Preference Panel

46.2.10.1.1 Functional description

This panel displays the IKE preference configuration data.

46.2.10.1.2 GUI usage and implications
Provisioning a GWC with IPsen supported, then configure this IPsen configuration.

46.2.10.1.3 GUI size
N/A

46.2.10.1.4 GUI fields
The column “Authentication method” is deleted.

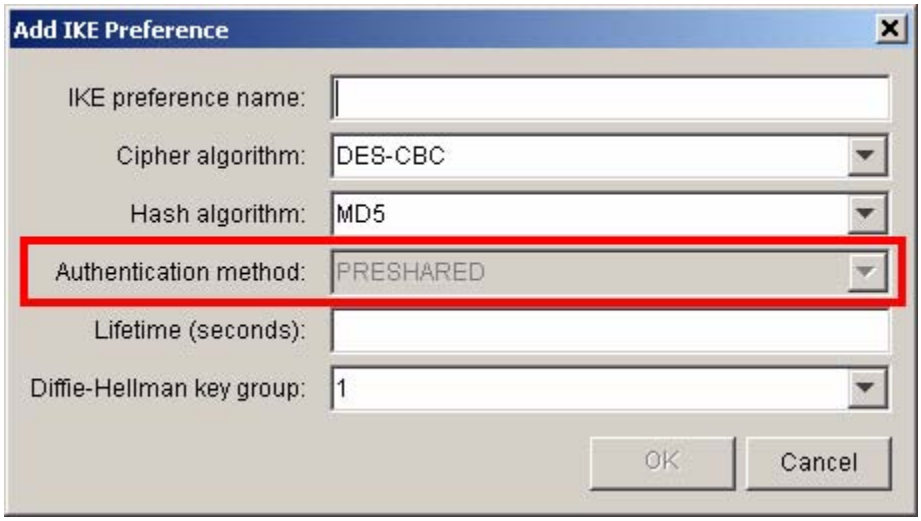
46.2.10.1.5 Usage example
At first, configure a IKE preference, then the configured item will be shown in the panel.

46.2.10.1.6 GUI release history update
N/A

46.2.10.1.7 Context sensitive launching information
N/A

46.2.10.1.8 Supplementary information
N/A

46.2.10.2 GUI name: Add/Change IKE Preference dialog



46.2.10.2.1 Functional description
This dialog show the IKE preference configuration parameter list and used to configure these parameters.

46.2.10.2.2 GUI usage and implications
Provisioning a GWC with IPsen supported, then configure IKE preference.

46.2.10.2.3 GUI size
N/A

46.2.10.2.4 GUI fields
The parameter “Authentication method” is deleted.

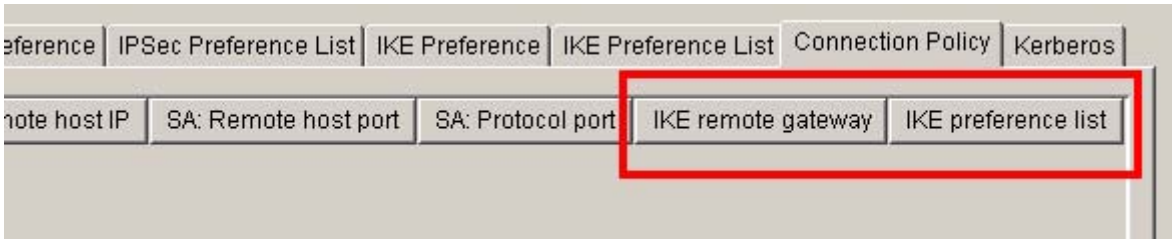
46.2.10.2.5 Usage example
In IKE preference panel, click “Add/Change” button, the dialog will be shown. You can configure /change a IKE preference.

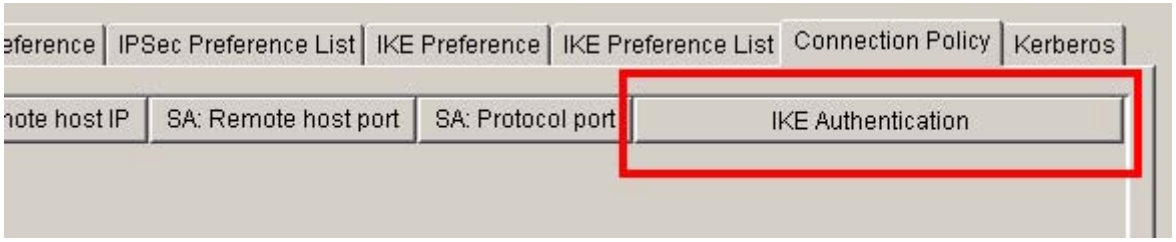
46.2.10.2.6 GUI release history update
N/A

46.2.10.2.7 Context sensitive launching information
N/A

46.2.10.2.8 Supplementary information
N/A

46.2.10.3 GUI name: Connection Policy Panel





46.2.10.3.1 Functional description
This panel display the connection policy configuration data.

46.2.10.3.2 GUI usage and implications
Provisioning a GWC with IPsen supported, then click the IPsen tab and click this panel.

46.2.10.3.3 GUI size
N/A

46.2.10.3.4 GUI fields
The column “IKE remote gateway” and “IKE preference list” is deleted and add a new column “IKE Authentication”.

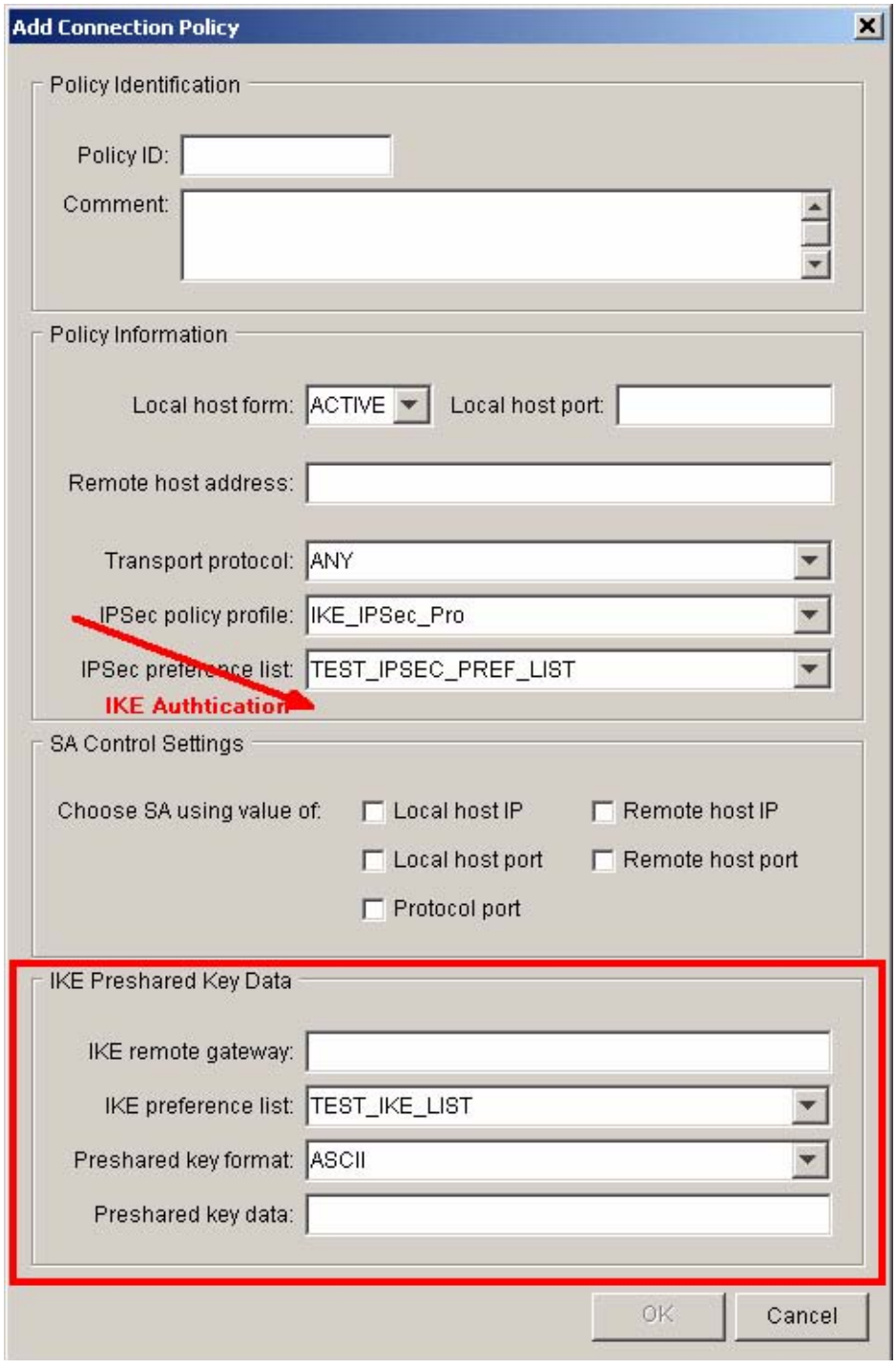
46.2.10.3.5 Usage example
At first, configure a connection policy, then the configured item will be shown in the panel.

46.2.10.3.6 GUI release history update
N/A

46.2.10.3.7 Context sensitive launching information
N/A

46.2.10.3.8 Supplementary information
N/A

46.2.10.4 GUI name: Add/Change Connection Policy Dialog



46.2.10.4.1 Functional description

This dialog show the connection policy configuration parameter list and used to configure these parameters.

46.2.10.4.2 GUI usage and implications
Provisioning a GWC with IPsen supported, then configure connection policy.

46.2.10.4.3 GUI size
N/A

46.2.10.4.4 GUI fields
The area “IKE Preshared Key Data” will be removed from Add/Change Connection Policy Dialog box. Additional, a new drop down selector “IKE Authentication” will be added into this dialog box.

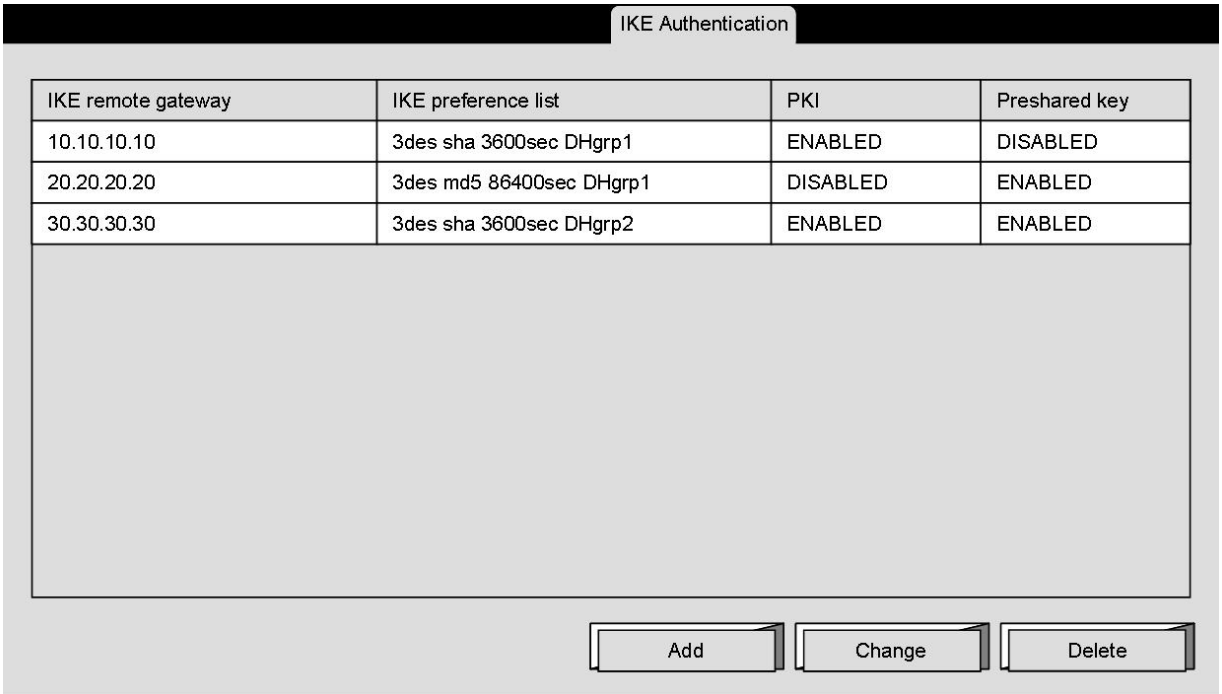
46.2.10.4.5 Usage example
In connection policy panel, click “Add/Change” button, the dialog will be shown. You can configure /change a connection policy.

46.2.10.4.6 GUI release history update
N/A

46.2.10.4.7 Context sensitive launching information
N/A

46.2.10.4.8 Supplementary information
N/A

46.2.10.5 GUI name: IKE Authentication Panel



46.2.10.5.1 Functional description
This panel display the IKE authentication configuration data.

46.2.10.5.2 GUI usage and implications
Provisioning a GWC with IPsen supported, then configure this IPsen configuration.

46.2.10.5.3 GUI size
N/A

46.2.10.5.4 GUI fields
This panel will include 4 columns:

- IKE remove gateway column contains an IPV4 address.
- IKE preference list column contains an index into the “IKE Preference List” panel.
- PKI column displays either ENABLED or DISABLED.
- Preshared-Key column displays either ENABLED or DISABLED

and 3 buttons:

- Add
- Change
- Delete.

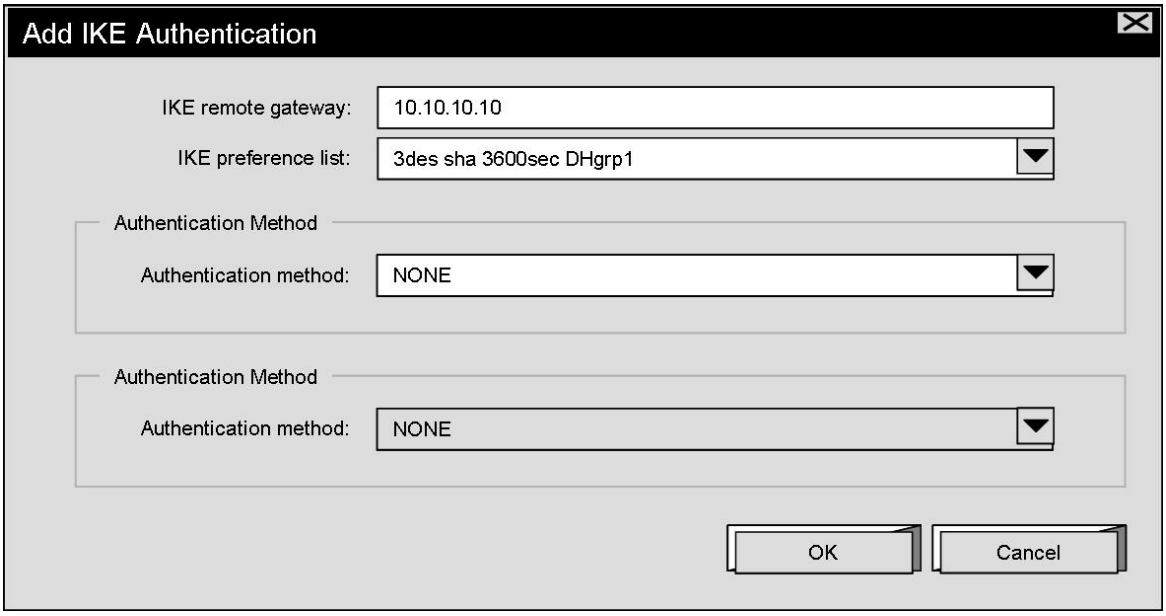
46.2.10.5.5 Usage example
At first, configure a IKE Authentication, then the configured item will be shown in the panel.

46.2.10.5.6 GUI release history update
N/A

46.2.10.5.7 Context sensitive launching information
N/A

46.2.10.5.8 Supplementary information
N/A

46.2.10.6 GUI name: Add/Change IKE Authentication dialog



46.2.10.6.1 Functional description

This dialog show the IKE authentication configuration parameter list and is used to configure these parameters.

46.2.10.6.2 GUI usage and implications

Provisioning a GWC with IPsen supported, then configure IKE authentication.

46.2.10.6.3 GUI size

N/A

46.2.10.6.4 GUI fields

This dialog will include 4 field:

- IKE remove gateway.
- IKE preference list cl.
- PKI.
- Preshared-Key.

46.2.10.6.5 Usage example

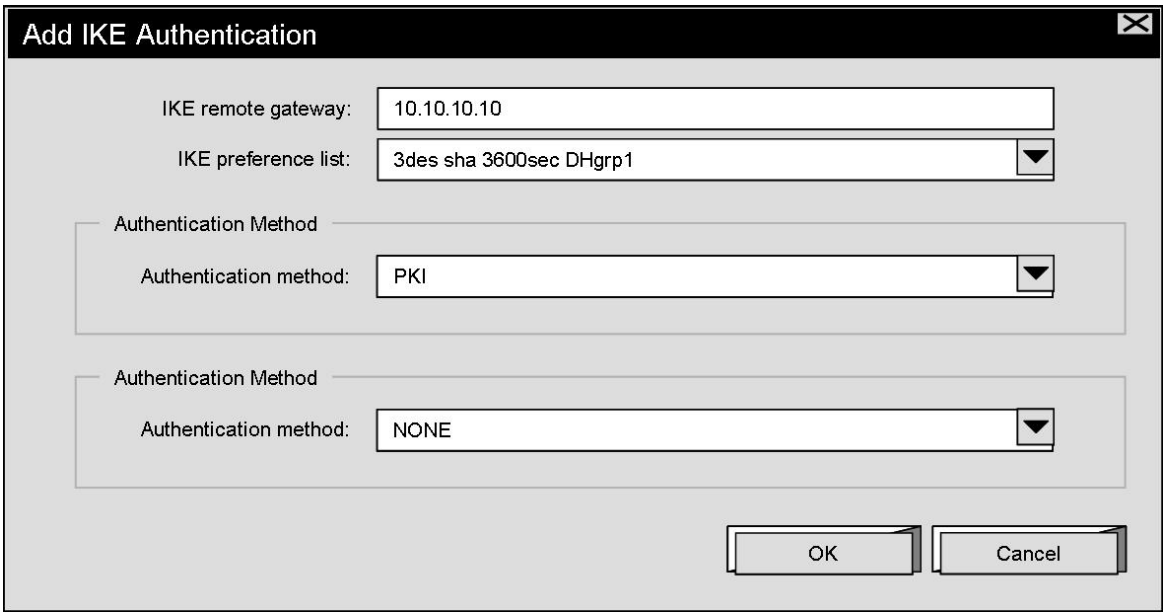
In IKE authentication panel, when the “Add” button is clicked, the “Add IKE Authentication” dialog box will appears, which includes following fields:

- IKE remove gateway column contains an IPV4 address.
- IKE preference list column contains an index into the “IKE Preference List” panel.

- Authentication Method field is a drop down selector, available values consisting of “None”, “PRESHARED” and “PKI”.
- Please note that the second Authentication Method only becomes editable after the first Authentication Method is datafilled. They have the same available values.
- In SN10, at most one PKI and at most one PRESHARED can be selected in the same IKE Authentication item. E.g. you can select only “PKI”, or only “PRESHARED” as authentication method. Also you can select both “PKI” and “PRESHARED” as authentication methods. But you cannot select two “PKI” or two “PRESHARED”.

If you select PKI as authentication method, just simply save it by clicking “OK” button.

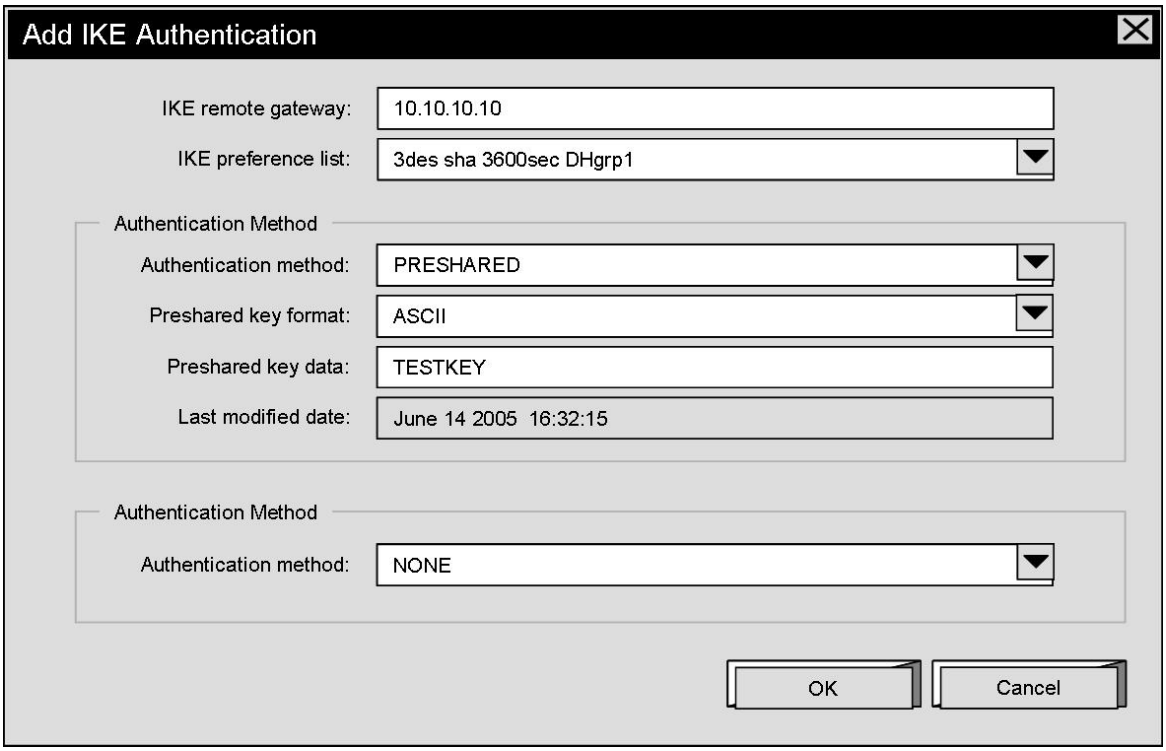
Figure 1 Add IKE Authentication - PKI method



If you select “PRESHARED” as authentication method, three more fields will appear on the dialog box:

- Preshared key format field is a drop down selected, only be shown when “PRESHARED” is selected as authentication method. Available values consisting of “ASCII” and “HEX”.
- Preshared key data is a text field, only be shown when “PRESHARED” is selected as authentication method.
- Last modified data is a non editable text field, only be shown when “PRESHARED” is selected as authentication method. SESM will display current time in this field.

Add IKE Authentication - Preshared method

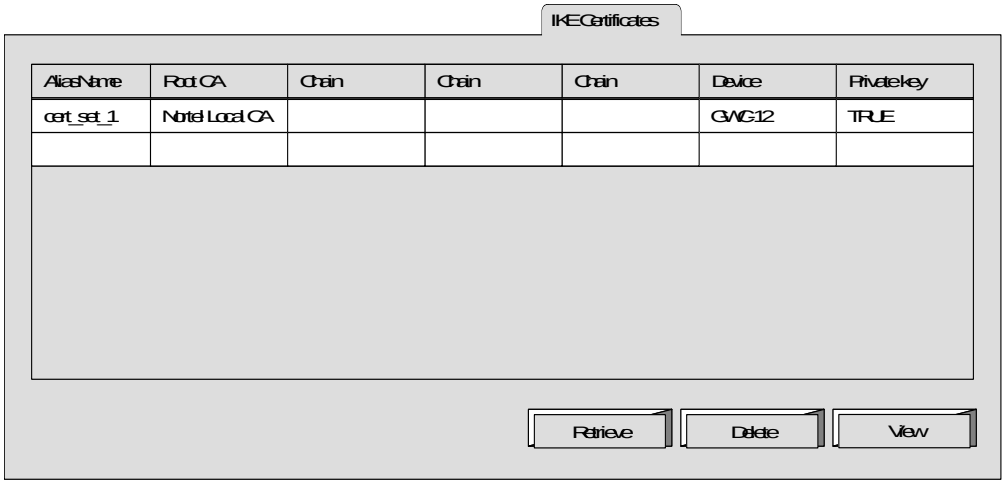


46.2.10.6.6 GUI release history update
N/A

46.2.10.6.7 Context sensitive launching information
N/A

46.2.10.6.8 Supplementary information
N/A

46.2.10.7 GUI name: PKI Certificate Panel



46.2.10.7.1 Functional description
This panel display the entire chain (root, intermediate, device certs + private key) in a single row with one piece of info (maybe subject name) on each certificate.

46.2.10.7.2 GUI usage and implications
Provisioning a GWC with IPsen supported, then view this panel.

46.2.10.7.3 GUI size
N/A

46.2.10.7.4 GUI fields
TBD.

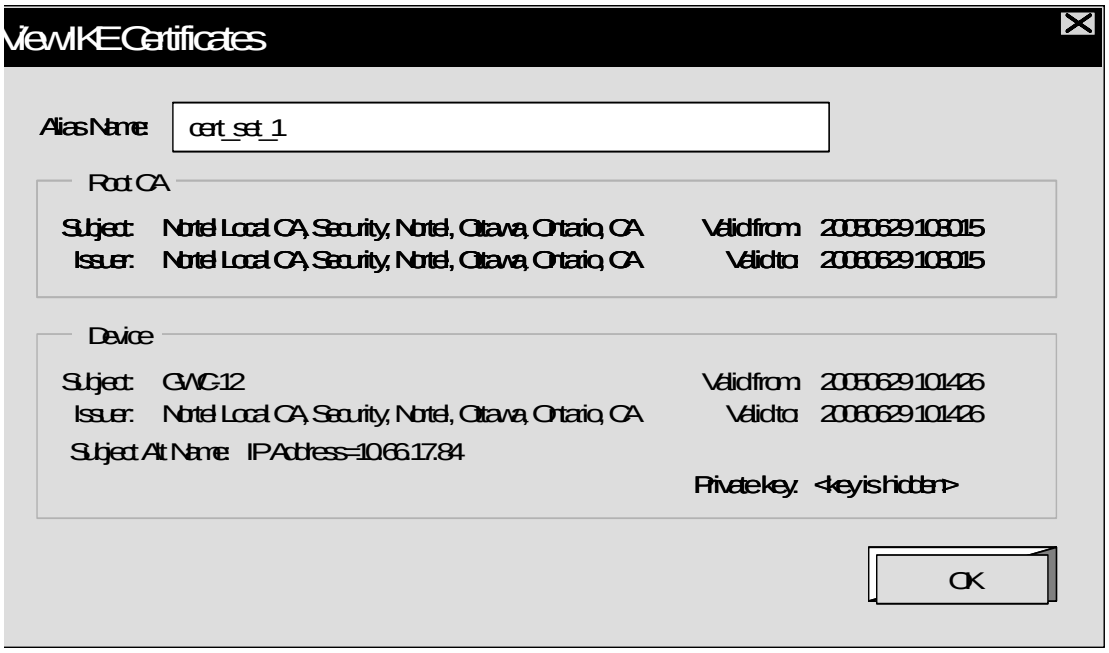
46.2.10.7.5 Usage example
At first, provision a GWC with IPsec supported, then the panel display the entire chain (root, intermediate, device certs + private key) in a single row with one piece of info (maybe subject name) on each cert.

46.2.10.7.6 GUI release history update
N/A

46.2.10.7.7 Context sensitive launching information
N/A

46.2.10.7.8 Supplementary information
N/A

46.2.10.8 GUI name: IKE Preference Panel



46.2.10.8.1 Functional description
This dialog display the entire chain with more info.

46.2.10.8.2 GUI usage and implications
Provisioning a GWC with IPsen supported, then view the entire chain with more info.

46.2.10.8.3 GUI size
N/A

46.2.10.8.4 GUI fields
TBD.

46.2.10.8.5 Usage example
In IKE certificate panel, click “view” button, the dialog will be shown. You can view the entire chain with more info.

46.2.10.8.6 GUI release history update
N/A

46.2.10.8.7 Context sensitive launching information
N/A

46.2.10.8.8 Supplementary information
N/A

46.2.11 User interface changes

N/A

46.2.12 OSSGate Interface Changes

N/A

46.2.13 Security

46.2.14 Configuration Walkthrough

The following transition scenarios are covered by this document:

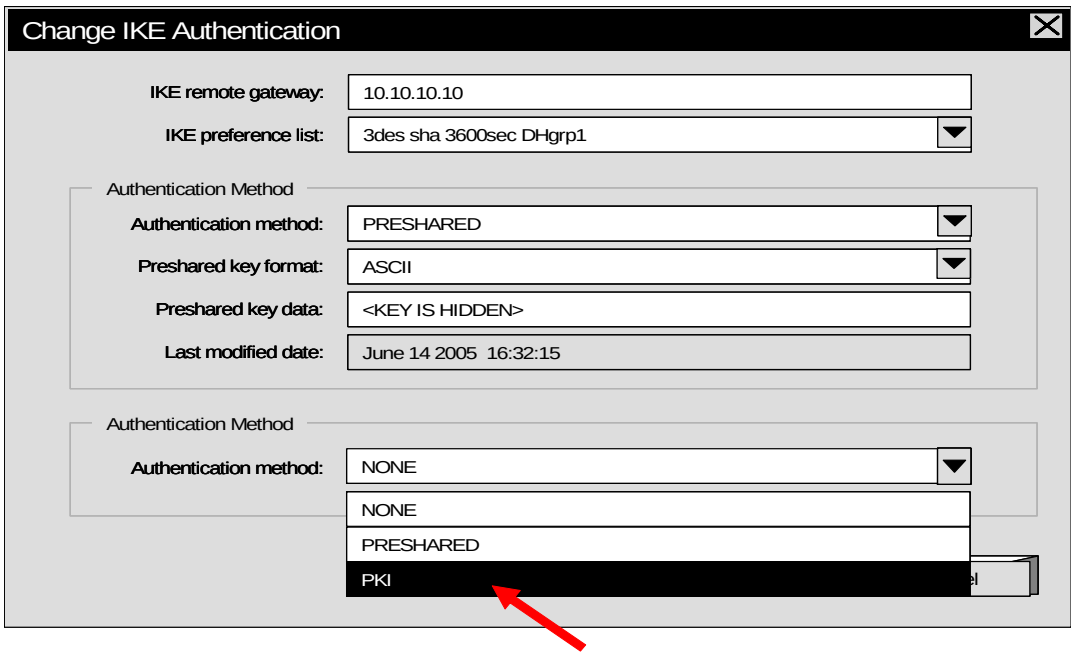
1. PSK to PKI

2. PKI to PSK

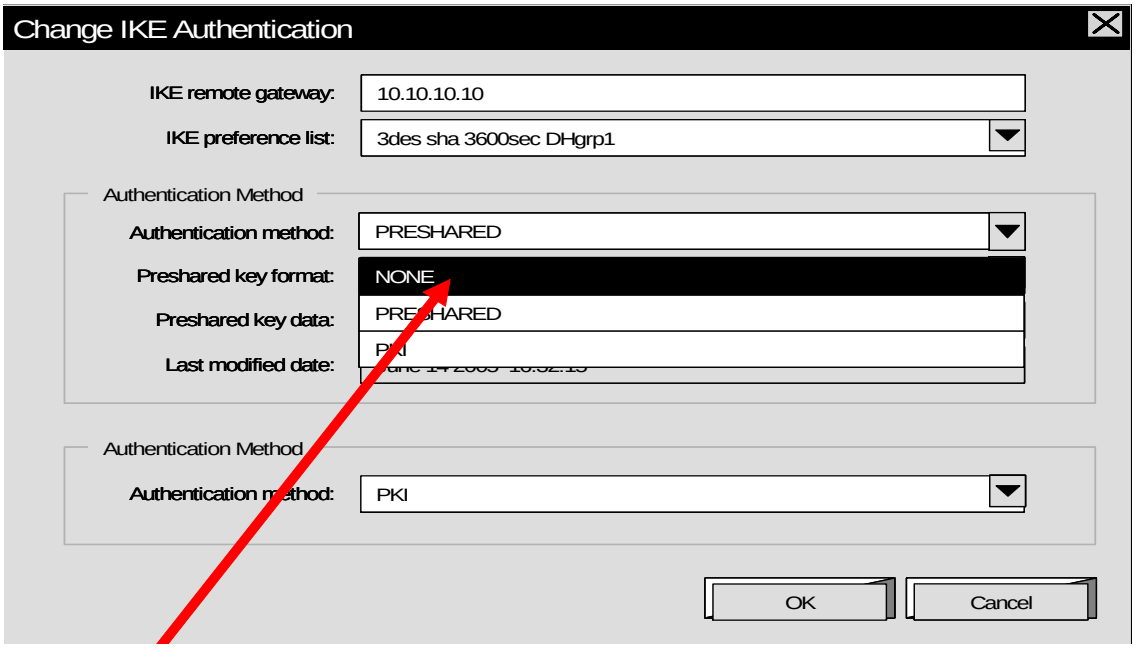
46.2.14.1 Transition from PSK to PKI

1. In IKE authentication panel, select “Change” button.

In the IKE authentication change dialog, set the second Authentication Method to PKI: (PSK -to- PSK + PKI)



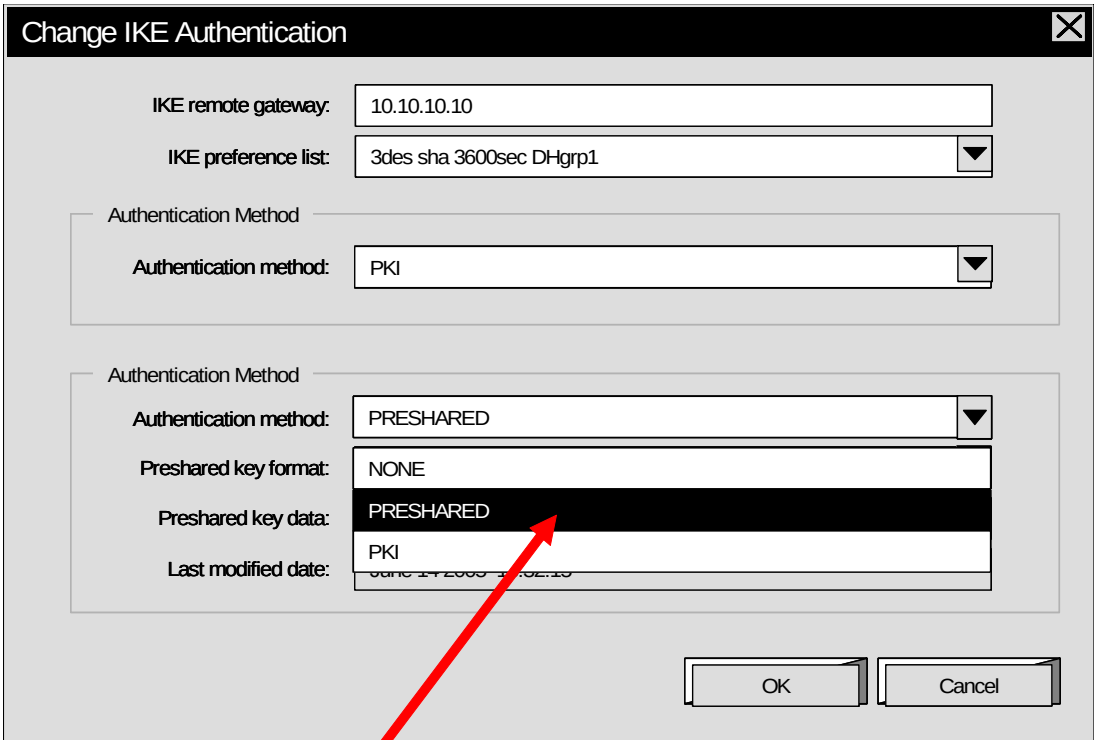
2. After the GWC use the PKI as its new profile, the customer will delete the PSK from the IKE authentication setting: (PSK+PKI - to - PKI)



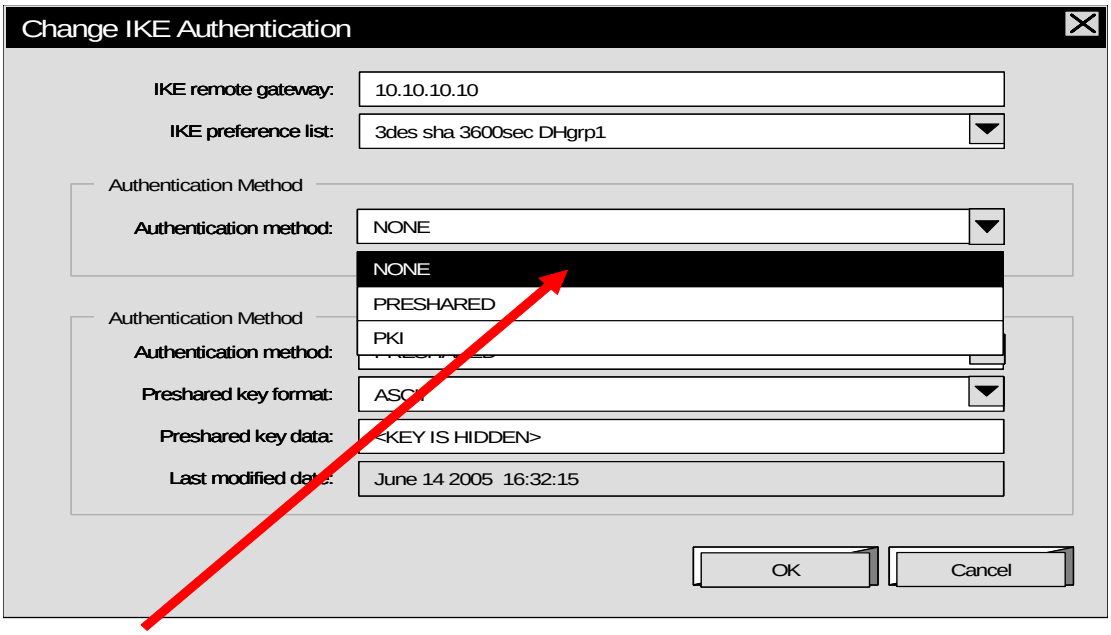
46.2.14.2 Transition from PKI to PSK

1. In IKE authentication panel, select “Change” button.

In the IKE authentication change dialog, set the second Authentication Method to PSK: (PKI -to- PKI + PSK)



2. After the GWC use the PSK as its new profile, the customer will delete the PKI from the IKE authentication setting: (PKI+PSK - to - PSK)



46.3 Configuration - SSM Certificate Handling

46.3.1 Hardware and Software Requirements

SN09.1 or later software load for SSPFS and the MG9K Element manager.

46.3.2 Initial Configuration

46.3.2.1 SSPFS Certificate

From a high-level, here are the steps to install the certificate “chain” on the SSPFS Machine from PKBroker.

1. Load IEMS with the required SN09.1 or later software.
2. Load both SSPFS and MG9000 Element Manager with required SN09.1 or later software.
3. For installing the certificate(s) on the SSPFS machine, thru PKBroker, the craftsperson will perform a certificate signing request from X. This is done by X. Behind scenes, PKBroker sends request to SSM on the SSPFS Machine. SSM generates a certificate signing request and forwards the CSR to PKBroker and the certificate is returned along with all supporting certificates. These certificates are installed in Solaris.
4. To verify the installation of certificates, the craftsperson will press the display all certificates button from the Certificate page.

46.3.2.2 IKE Entry with certificates

IPSec and IKE configuration parameters that are provisioned, via the Server Security Manager (SSM), must match the corresponding IPSec and IKE parameters on the MG9000, provisioned via the LCI and MG9000 Element Manager.

From a high-level here are the steps to enable security on the OAM&P links.

1. Load both MG9000 and MG9000 Element Manager with required software.
2. When commissioning the MG9000,the craftsperson will enable security using certificates for that network element using the Node Provisioning view of the Element Manager.
3. The craftsperson will then use a web browser and connect to the MG9000 Element Manager server machine. (SSM) After logging in, the craftsperson will enable security by creating IPSec and IKE entries using the MG9000 IP address. When provisioning the IKE entry the craftperson will elect to use certificates instead of pre-shared key.
4. Cold start from MG9000 or manual discovery from Element Manager.
5. This will complete securing the OAM&P link.

46.3.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable

46.3.4 Upgrade Impact

46.3.4.1 Server Security Manager

For SN07 or earlier to SN09.1 upgrades, there are no impacts as IPSec was not available.

For SN08 or SN09 to SN09.1 upgrades, an SSPFS backup and restore will be necessary to move IPSec configuration forward to SN09.1. No data conversion will be necessary.

46.3.5 Data schema (DS) (CM, MIBS, RDB)

New Mib for the OAM&P provisioning of IPSec: TBD

New Mib for the VMG provisioning of IPSec: TBD

46.3.6 OSS Changes

None

46.3.7 External Interface Changes

None.

46.3.8 Server Security Manager

46.3.8.1 GUI name: Server Security Manager

Server Security Manager

46.3.8.1.1 Functional description

This HTML webpage is used to define security parameters to secure communications into and out from the SSPFS Machine. This includes MG9000 Element Manager to MG9000 OAM&P communications.

The craftsperson will be presented with two tables representing currently provisioned security parameters. One for IPSec parameters and one for IKE parameters. Options to add and delete entries are available. Adding entries will be performed using HTML forms.

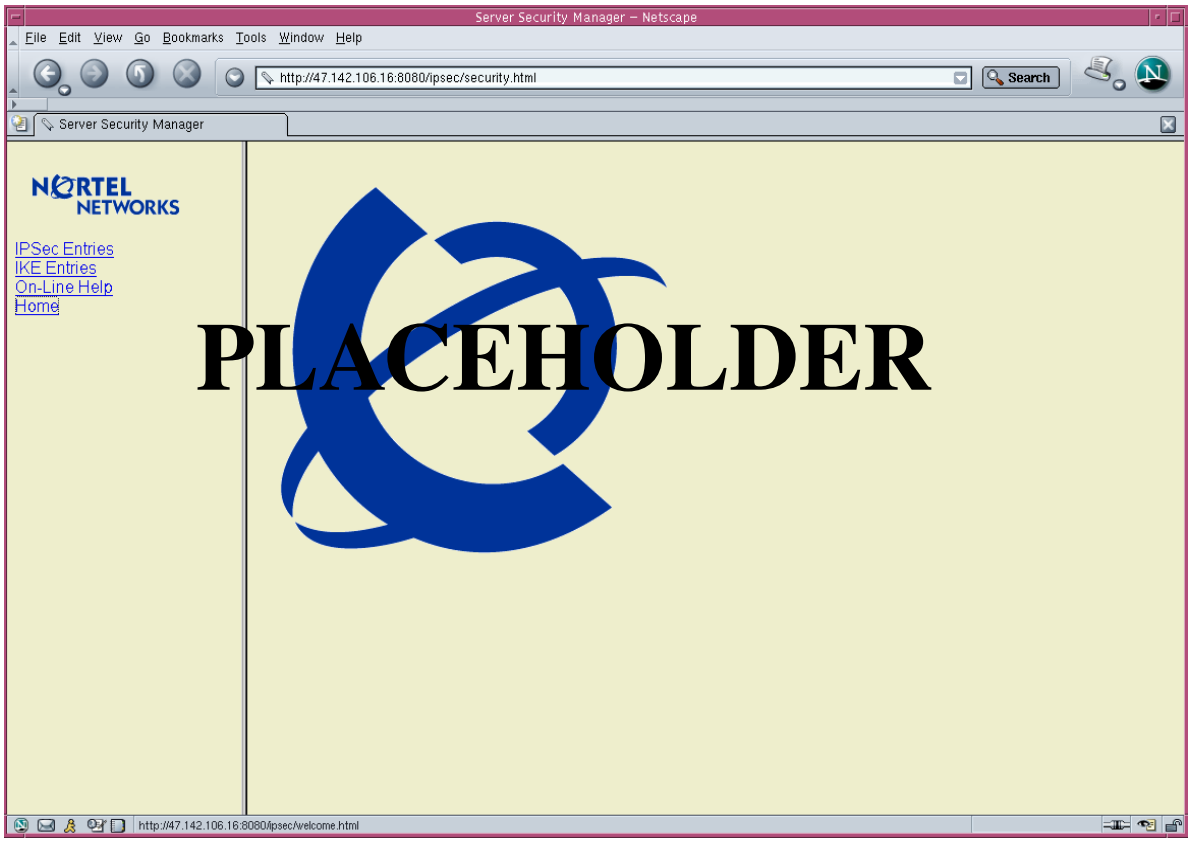
The IPSec Entries page allows retrieval and manipulation of IPSec policies for a host server. Once the policies are configured, all outbound and inbound datagrams are subject to policy checks as they exit and enter the host server. If no entry is found, no policy checks will be completed, and all the traffic will pass through. Depending upon the match of the policy entry, a specific action will be taken.

The IKE Entries page allows retrieval and manipulation of Internet Key Exchange policies for a host server. Once a policy is configured, the IKE daemon running on the host server discovers a remote host's public encryption key. The local system can then encrypt messages destined for the remote host whose public key it has discovered.

A new "Transforms" button will be available from the IKE Entries page to allow the craftperson to enter and view multiple transforms per IKE entry. For example, one transform could support a preshared key and another could support certificates.

A new "Certificates" link will be available on the navigation bar on the left. This will access the SSPFS Machine's certificates. Options to perform certificate signing requests to the CA authority and to delete certificates will be found.

The following is the first page presented to the craftsperson upon opening the Security Interface:



Navigation is perform using the links on the left frame. User input is performed or operation output is displayed in the right frame.

46.3.8.1.2 GUI usage and implications

First, IPSec entries are created using the desired parameters. If the craftsperson has chosen to use the “IPSec” action, the second step is to create a corresponding IKE entry using the desired parameters.

This interface provides for securing all network communications and not just Element Manager communications. Care must be taken when provisioning or deleting the security parameters, so as not to effect other essential communications, such as telnet, ftp, etc.

46.3.8.1.3 IPSec Entry

No changes are planned.

46.3.8.1.4 IKE Entry

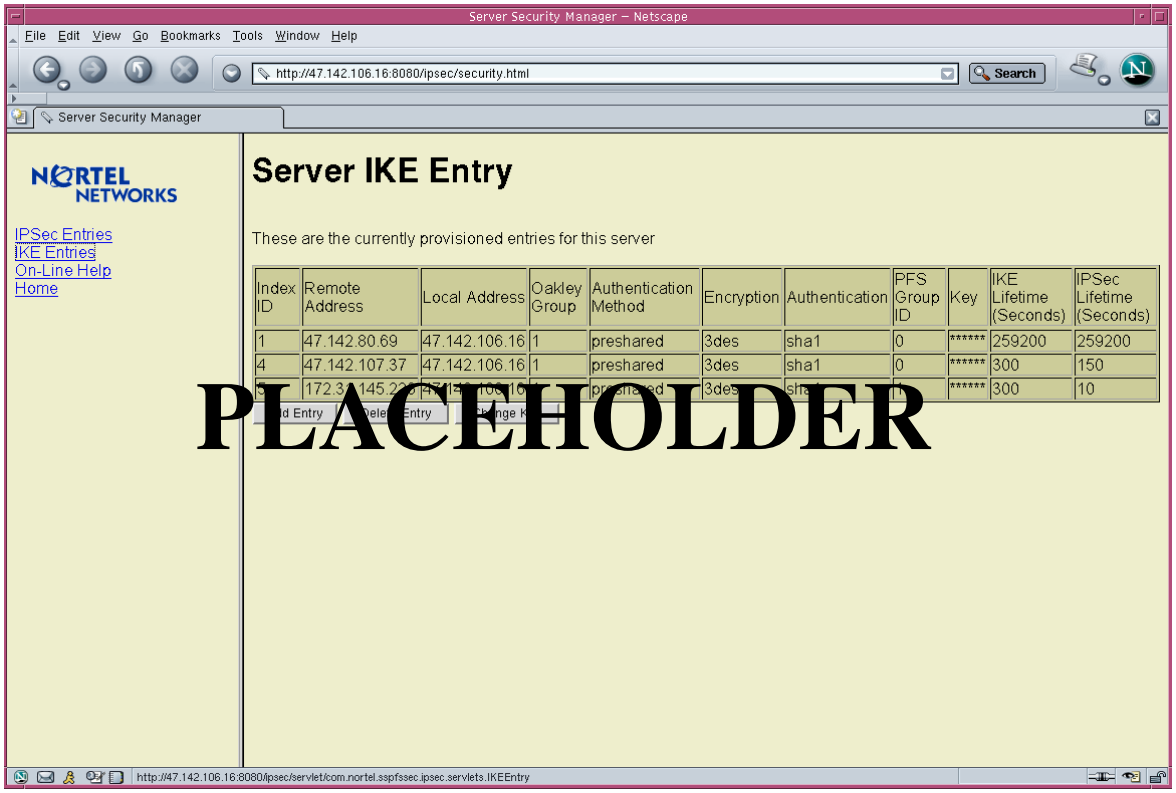
The following table lists the security fields for IKE parameters.

Table 26 IPSec field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action
Index ID	No	No	Integer	Internal index used by the server to track and reference IKE entries.
Remote Address	No	No	A numeric internet IP address of the form: www.xxx.yyy.zzz	IP address of the remote system communicating with this server.
Local Address	No	No	A numeric internet IP address of the form: www.xxx.yyy.zzz	IP address of this server.
Type	New	No	Preshared Key or Certificate	Selects the type of security negotiation and authentication to use.
Oakley Group	No	No	1 (768-bit), 2 (1024-bit), or 5 (1536-bit).	The Oakley Diffie-Hellman group used for IKE Security Association key derivation.
Authentication Method	No	No	Preshared is the only supported option.	The authentication method used for IKE phase 1.
Encryption	No	No	des, 3des, and blowfish.	Specifies the encryption algorithm for a Security Association.
Authentication	No	No	sha1 and md5.	Specifies the authentication algorithm for a Security Association.
PFS Group ID	No	No	0 (do not use Perfect Forward Secrecy for IPsec SAs), 1 (768-bit), 2 (1024-bit), and 5 (1536-bit).	The Oakley Diffie-Hellman group used for IPsec Security Association key derivation.
Key	No	No	16 - 120 character ASCII string	Specifies the preshared key for this Security Association.
IKE Lifetime	No	No	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days.	Specifies the lifetime for a IKE phase 1 Security Association.
IPSec Lifetime	No	No	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days.	Specifies the lifetime for an IPSec Security Association.

46.3.8.1.5 IKE provisioned entries example

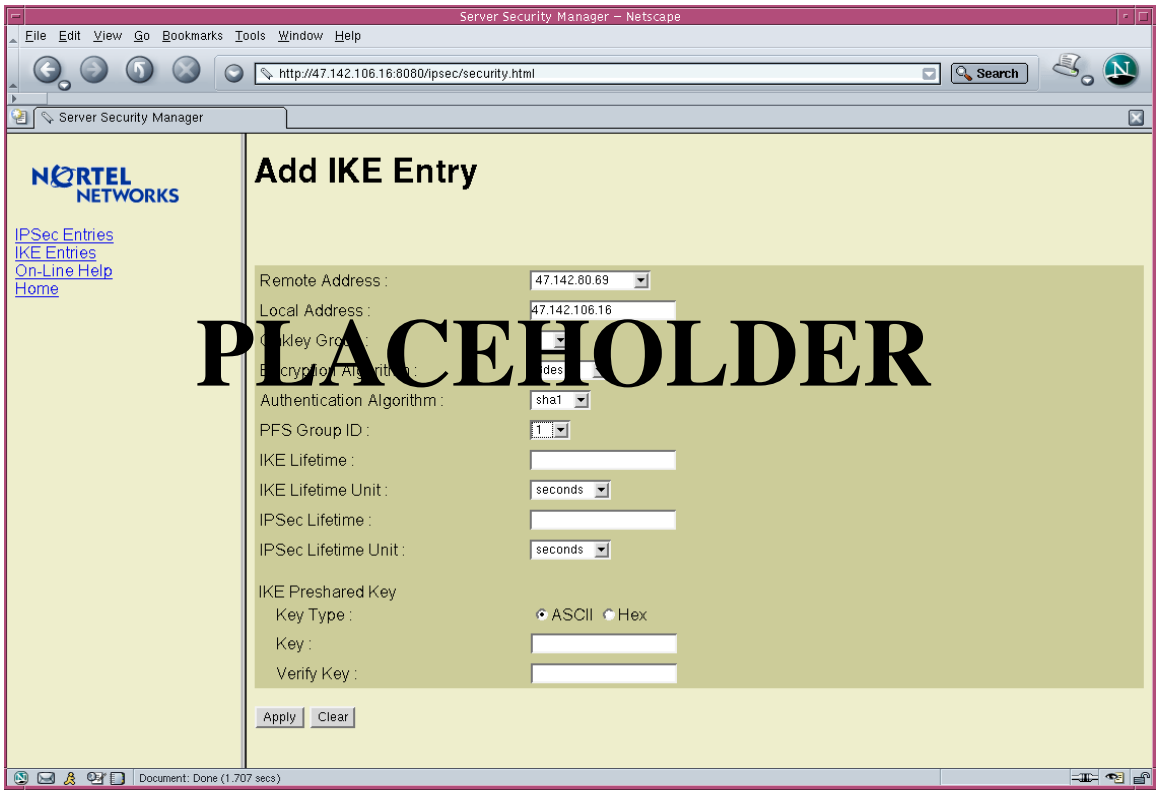
The following example shows a number of IKE entries for an SSPFS server:



PLACEHOLDER

46.3.8.1.6 IKE entry form example

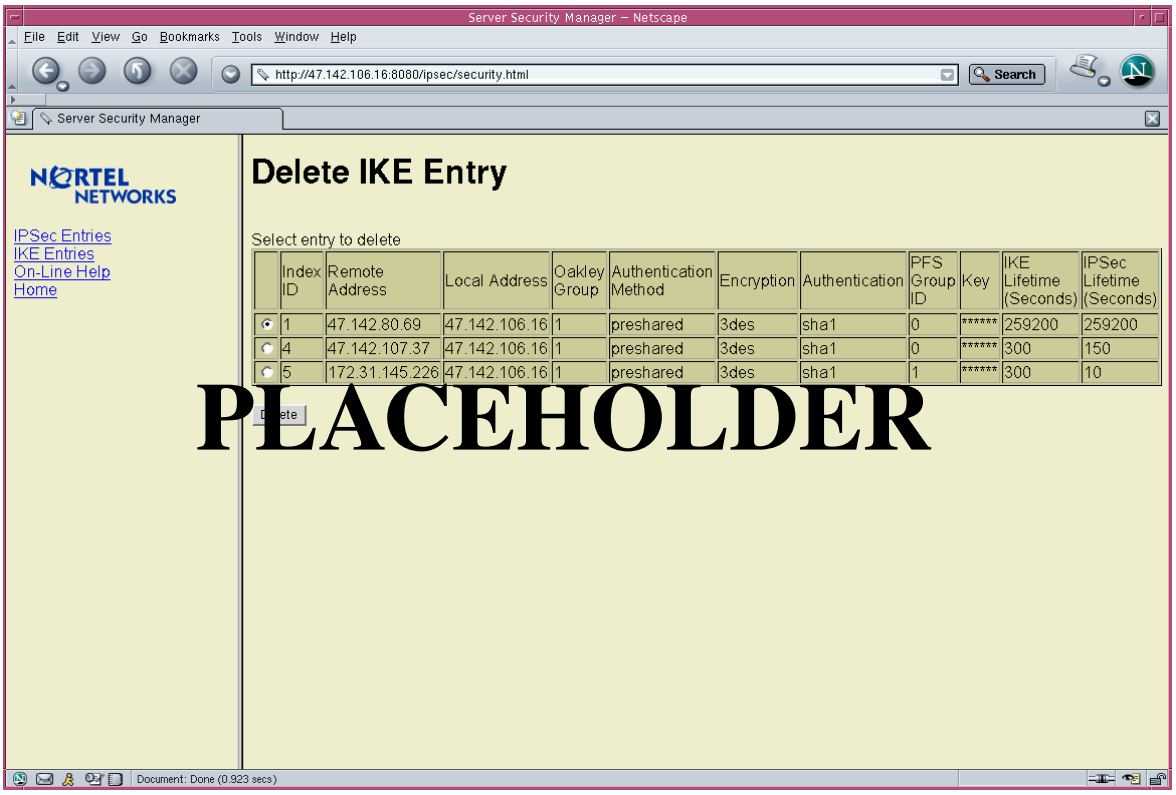
The following example shows a form for creating IKE entries for an SSPFS server:



PLACEHOLDER

46.3.8.1.7 IKE entry deletion example

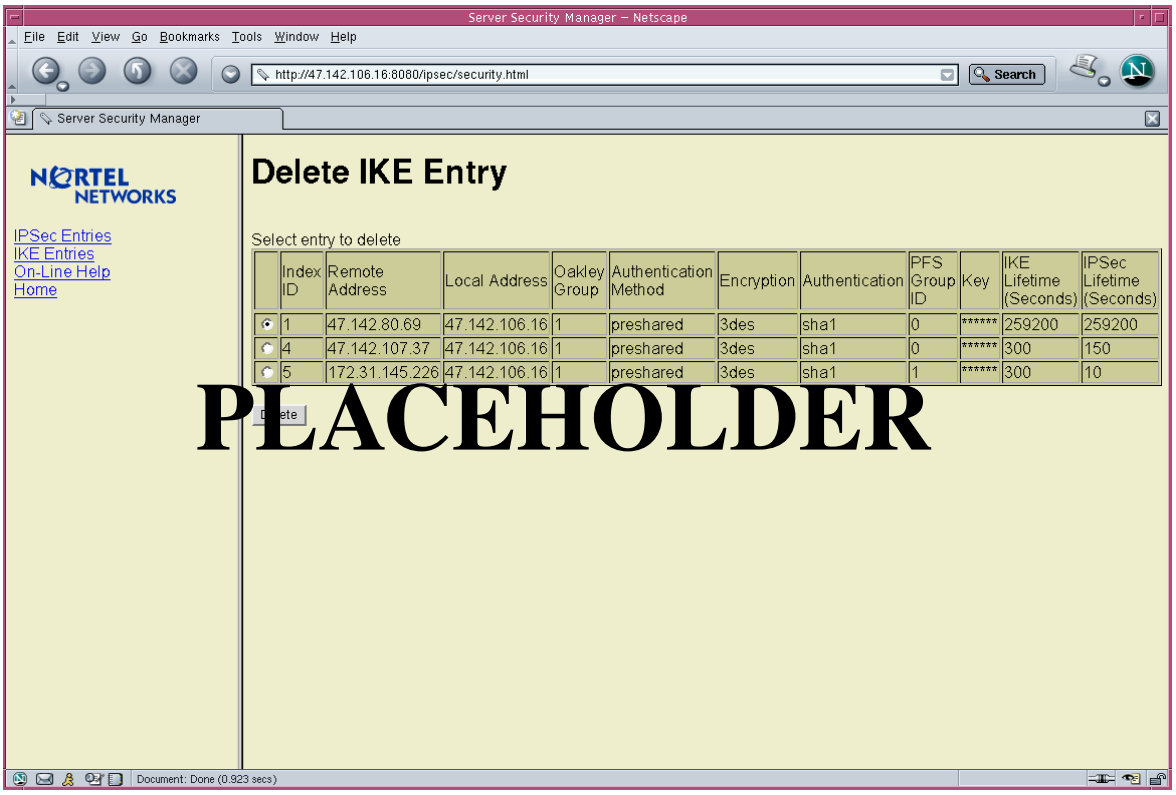
The following example shows a table for deleting IKE entries for an SSPFS server:



PLACEHOLDER

46.3.8.1.8 IKE entry adding transform example

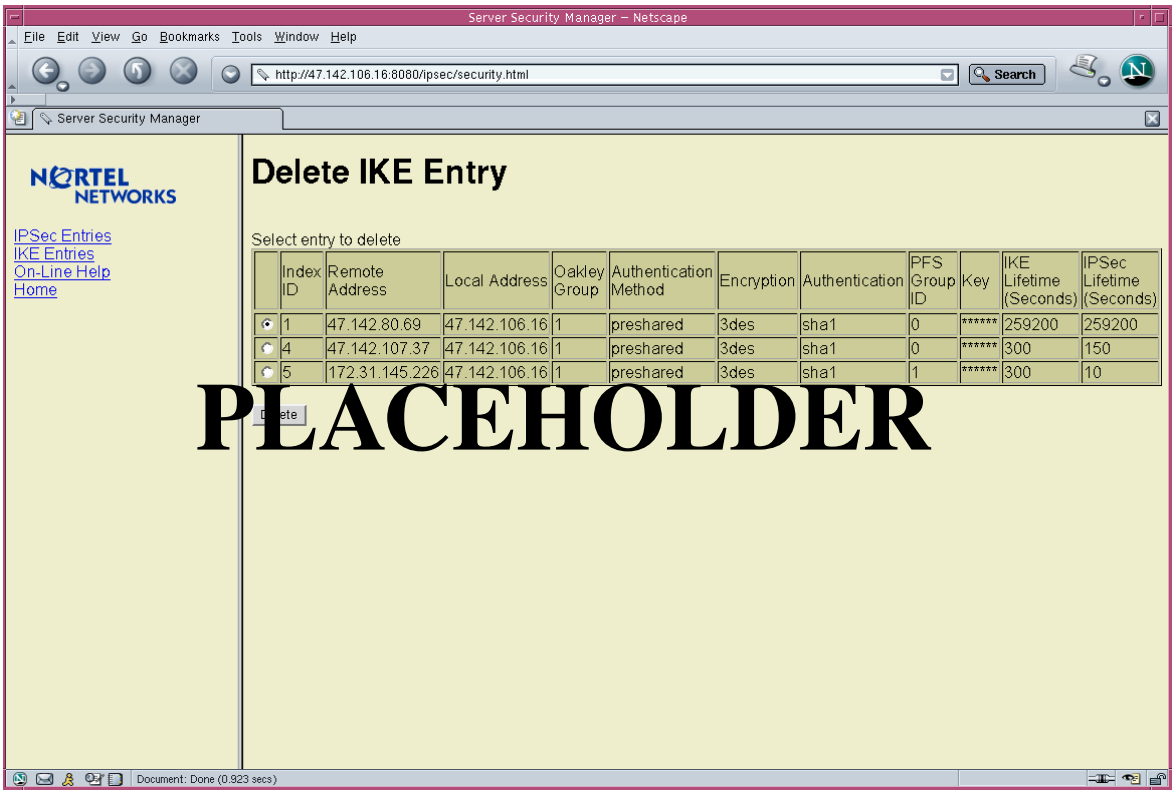
The following example shows a form for adding a transform to from IKE entry for an SSPFS server:



PLACEHOLDER

46.3.8.1.9 IKE entry view with transform example

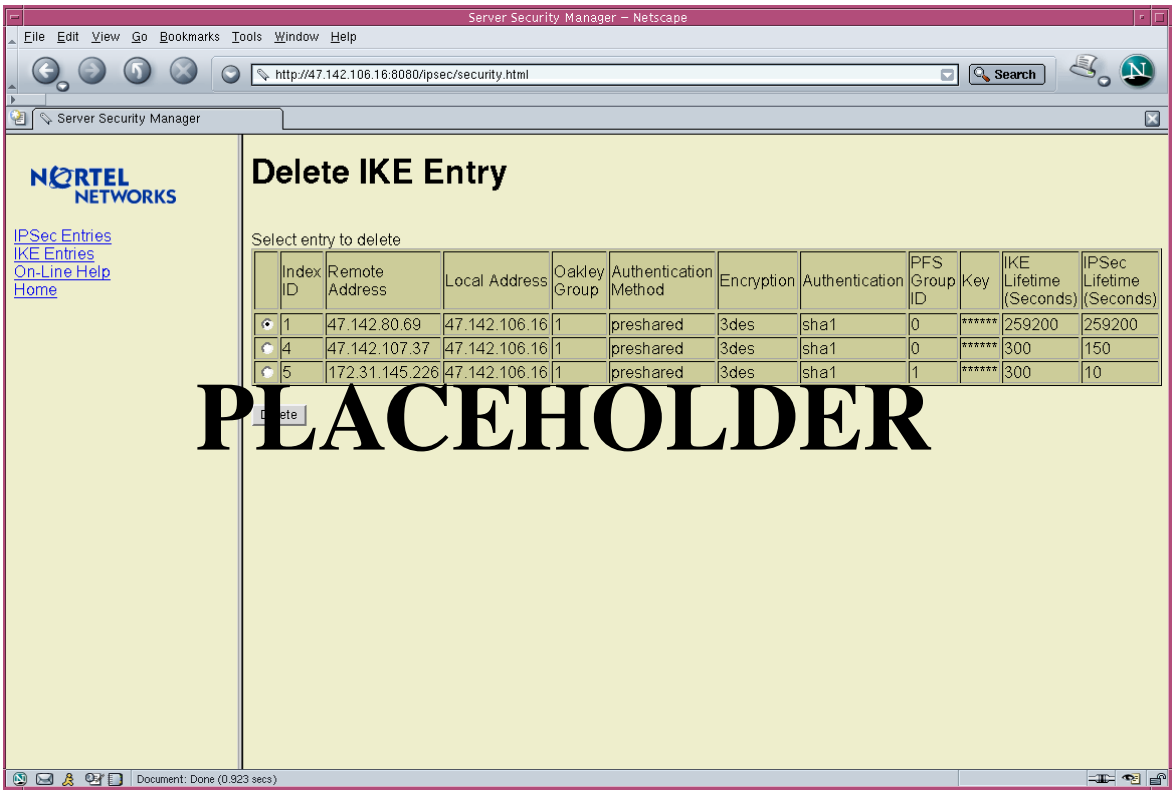
The following example shows a form detailing all transform information for an IKE entry for an SSPFS server:



PLACEHOLDER

46.3.8.1.10 IKE entry delete transform example

The following example shows a form for deleting a transform from IKE entry for an SSPFS server:



PLACEHOLDER

46.3.8.1.11 MG9000 Parameter settings

For each MG9000 provisioned and requires IP security, two IPSec entries must be created, one bypass for “ping” and another for “ipsec”. For each “ipsec” entry there must be a corresponding IKE entry.

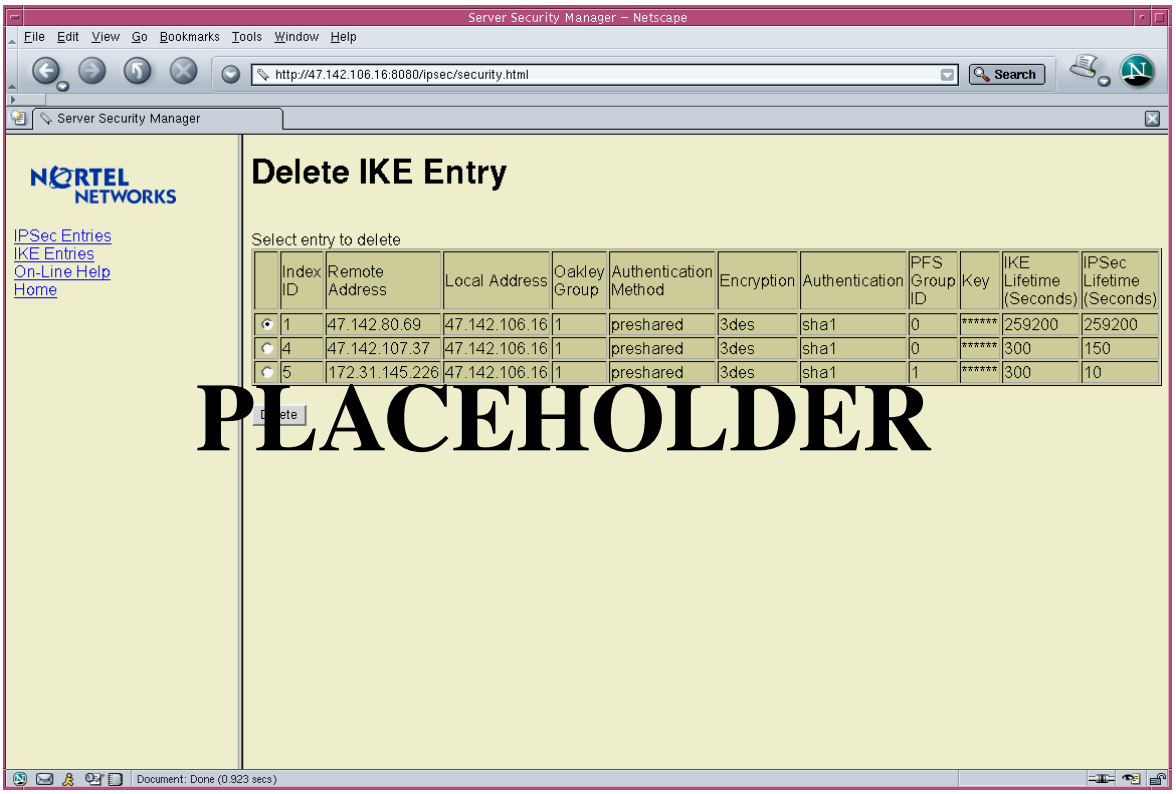
The IKE entry must be provisioned as follows:

1. Remote Address is the address of the MG9000 as seen by the Element Manager.
2. Local Address is the address of the Element Manager as seen by the MG9000.
3. Type is “Certificate”
4. Oakley Group is “1”.
5. Encryption Algorithm is “3des”.
6. Authentication Algorithm is “sha1”.
7. PFS Group ID is “1”.

8. IKE Lifetime is “8”.
9. IKE Lifetime Unit is “hours”.
10. IPSec Lifetime is “8”.
11. IPSec LIfetime Unit is “hours”.

46.3.8.1.12 Certificate Commands example

The following example shows the certificate commands available for an SSPFS server:



PLACEHOLDER

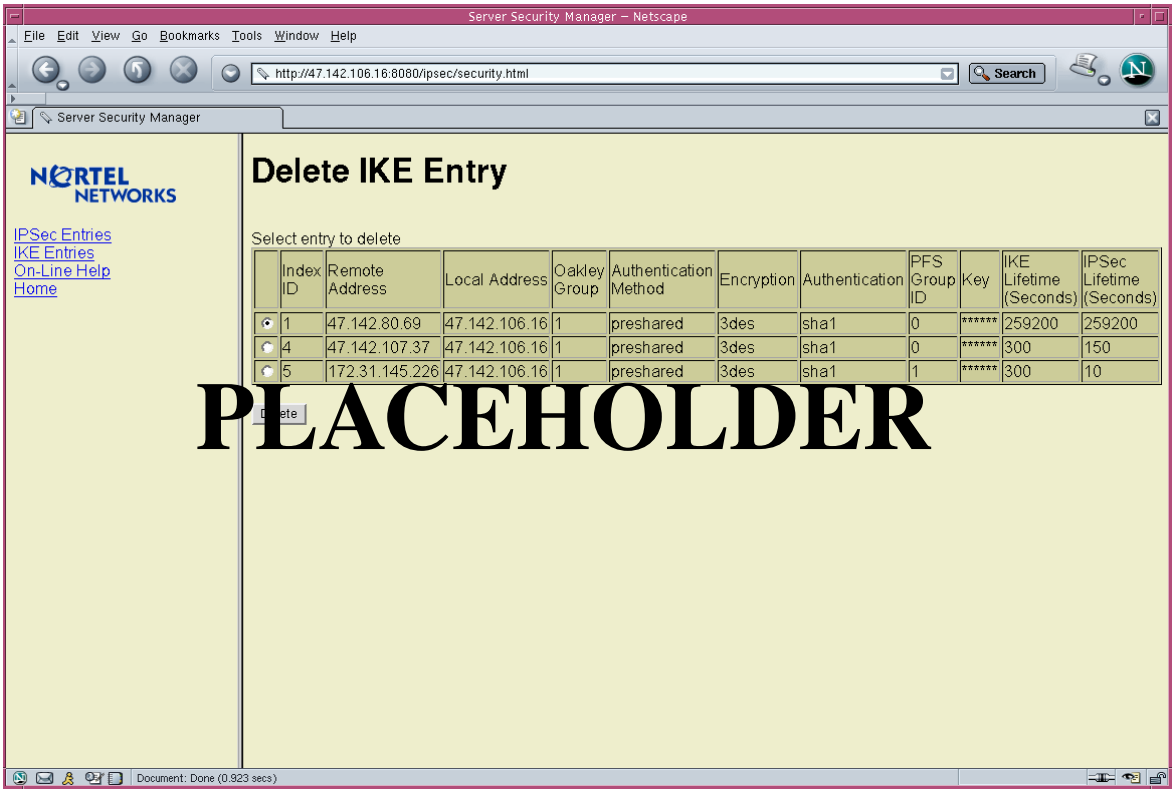
46.3.8.1.13 Certificate command page

The commands are as follows:

1. Certificate Signing Request - generate a certificate signing request.
2. Clear All - remove all certificates from the machine.
3. Display All - display all certificates currently provisioned.

46.3.8.1.14 Display All certificate example

The following example shows the Display All certificate page:



PLACEHOLDER

46.3.8.1.15 Display All certificate page

This page will display all the certificates currently provisioned on the SSPFS machine.

46.3.8.1.16 GUI release history update

The following information was added:

1. Type field to select Preshared Key or Certificate to IKE entry form and IKE table.
2. New pages for IKE transforms. Add, delete and view transforms.
3. New pages for certificates. Certificate Signing Request, Clear All and Display All.

46.3.8.1.17 Supplementary information

None

46.3.8.1.18 CLUI Interface

Not applicable

46.3.9 Command interface changes

Add, Delete and show IKE Entry transforms.

Certificate signing request command line option.

46.3.10 Security

46.3.10.1 Network configuration

No changes to the network are necessary to support the IPSec implementation.

46.3.10.2 Key management

46.3.10.2.1 SSPFS IKE Preshared key

The SSPFS IKE preshared key input by the user in the SSPFS Security Servlet. This key is secured by the use of secure http, if configured, from the browser to the server. Solaris stores all keys in a hidden system file not accessible by common users but is available to the ROOT user.

46.3.10.2.2 SSPFS Certificate Public/Private key

For the SSPFS Certificate Public/Private keys, Solaris stores all keys in a hidden system file not accessible by common users but is available to the ROOT user.

46.3.10.3 Protocol

IPSec is being used on the Solaris machine.

46.3.10.4 Authentication

Succession login will still be used for SSPFS Security Servlet.

46.3.11 Configuration Walkthrough

46.3.11.1 SSM Certificate Installation (Initial Commissioning)

From a high-level, here are the steps to install the certificate “chain” on the SSPFS Machine from SSM running on the SSPFS Machine.

1. Load IEMS with the required SN09.1 or later software.
2. Load both SSPFS and MG9000 Element Manager with required SN09.1 or later software.
3. For installing the certificate(s) on the SSPFS machine, thru the SSM Servlet, the craftsperson will perform a certificate signing request from the Certificate page. This is done by pressing the Cert Signing Request button. Behind scenes, the certificate is forwarded for signing and returned along with all supporting certificates. These certificates are installed in Solaris.
4. To verify the installation of certificates, the craftsperson will press the display all certificates button from the Certificate page.

46.3.11.2 SSM Certificate Installation (PKBroker)

From a high-level, here are the steps to install the certificate "chain" on the SSPFS Machine from PKBroker.

1. Load IEMS with the required SN09.1 or later software.
2. Load both SSPFS and MG9000 Element Manager with required SN09.1 or later software.
3. For installing the certificate(s) on the SSPFS machine, thru PKBroker, the craftsperson will perform a certificate signing request from X. This is done by X. Behind scenes, PKBroker sends request to SSM on the SSPFS machine. SSM generates a certificate signing request and forwards the CSR to PKBroker and the certificate is returned along with all supporting certificates. These certificates are installed in Solaris.
4. To verify the installation of certificates, the craftsperson will press the display all certificates button from the Certificate page.

46.3.11.3 SSM Certificate Removal

From a high-level, here are the steps to remove the certificate "chain" on the SSPFS Machine.

1. Load both SSPFS and MG9000 Element Manager with required software.
2. For removing the certificate(s) from the SSPFS machine, thru the SSM Servlet, the craftsperson will perform a delete all certificates from the Certificate page. This is done by pressing the Clear Certificates button. Behind scenes, the certificates are removed.
3. To verify the deletion of certificates, the craftsperson will press the display all certificates button from the Certificate page.

47: Configuration (CN): A00012198

47.1 Feature Name

GLC12 Coin Card Support from EM

47.2 Hardware and Software Requirements

The MG9000 and MG9000 software load which supports GLC12 card should be available.

47.3 Initial Configuration

The GLC12 card should be present on the MG9000.

47.4 Office/Subnet parameters (OP/SP) (CM & SESM)

NA

47.5 Upgrade Considerations

Since this card is supported in SN09.1 release, upgrade and downgrade scenarios have to be taken care.

No special care to be taken for EM upgrade/downgrade.The normal upgrade procedure will be followed for upgrading the EM to SN09.1. If SN09.1 EM is managing a node which has a GLC12 card, it would be displayed as GLC12 as against SAA12 in previous releases.

When a SN09.1 EM managing a SN09.1 MG9000 (with a GLC12 card) has to be downgraded to SN09, the MG9000 has to be downgraded (with proper patches for GLC12) prior to downgrading the EM. In SN09 EM the GLC12 card would be displayed as SAA12 card. The functionality is same when SN09.1 EM is downloaded SN08. In SN07EM, the GLC12 card will not be discovered.

47.6 Data schema (DS) (CM, MIBS, RDB)

NA

47.7 Service Orders (SO) (CM & SESM)

NA

47.8 Software optionality control (SOC)

NA

47.9 Element Management

There are no new views added for this feature. The card view will display the GLC12 card details and when the user double clicks on the port, the Line circuit view will open as shown in the following figures,

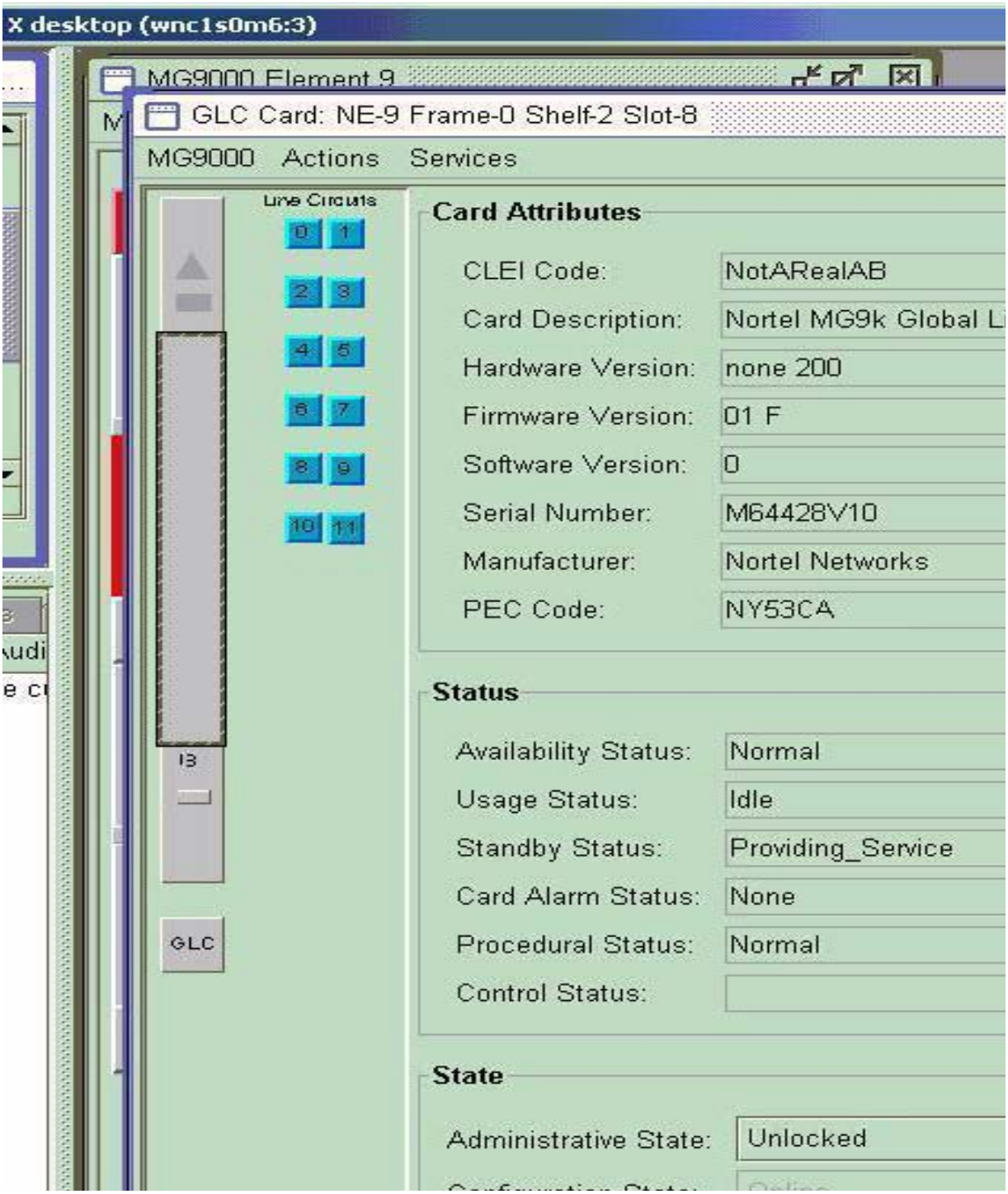


Figure 1: GLC12 Card View

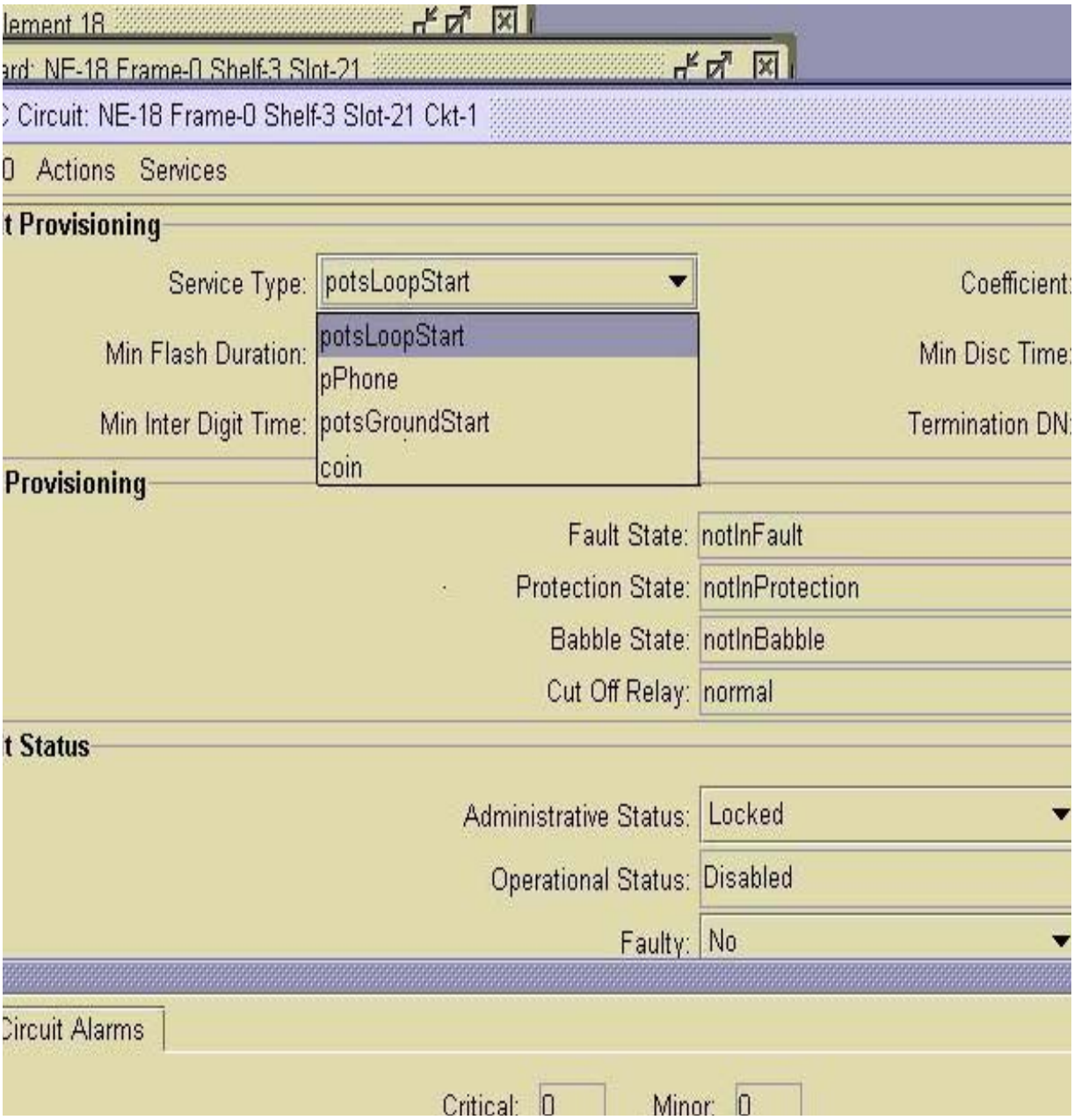


Figure 2: GLC12 Circuit View

The GLC12 line circuit will support pPhone, potsGroundStart, potsLoopStart and coin service types. The SAA12 can be replaced with a GLC12(and vice versa) without deprovisioning the card. When the card is replaced, if the circuit

view and circuit listing views will be closed if they are open. When the user opens the views again, the GLC information will be displayed in these views. When a SAA12 card is replaced with a GLC12 card, in the card view the actions submenu will be added. This actions submenu will have ‘Coefficient Table Manager’ entry. Clicking on which ‘Line Coefficient Table ‘will be opened.The circuit listing view which can be opened from Services submenu will display coefficient with other details.

When a GLC12 card will be replaced with a SAA12 card, the actions submenu will be removed and the circuit listing view will not display coefficient details with other existing details.

The audit will correct if there is a mismatch in the PEC code types, the proper card types would be decided depending on the PEC code and the same would be updated in the EM

Line Coefficient Download:

With this design, the EM is limiting the market the user can select for VMGs which in turn will limit the line coefficients on the GW.

A combobox ‘NE Market’ has been added to Add New MG9000 view. The user has to select the market from the market list while adding the NE. By default the market in the officewide defaults will be selected. The user can modify the market and apply the market to NE. The same market has to be selected for the VMGs which will be created.

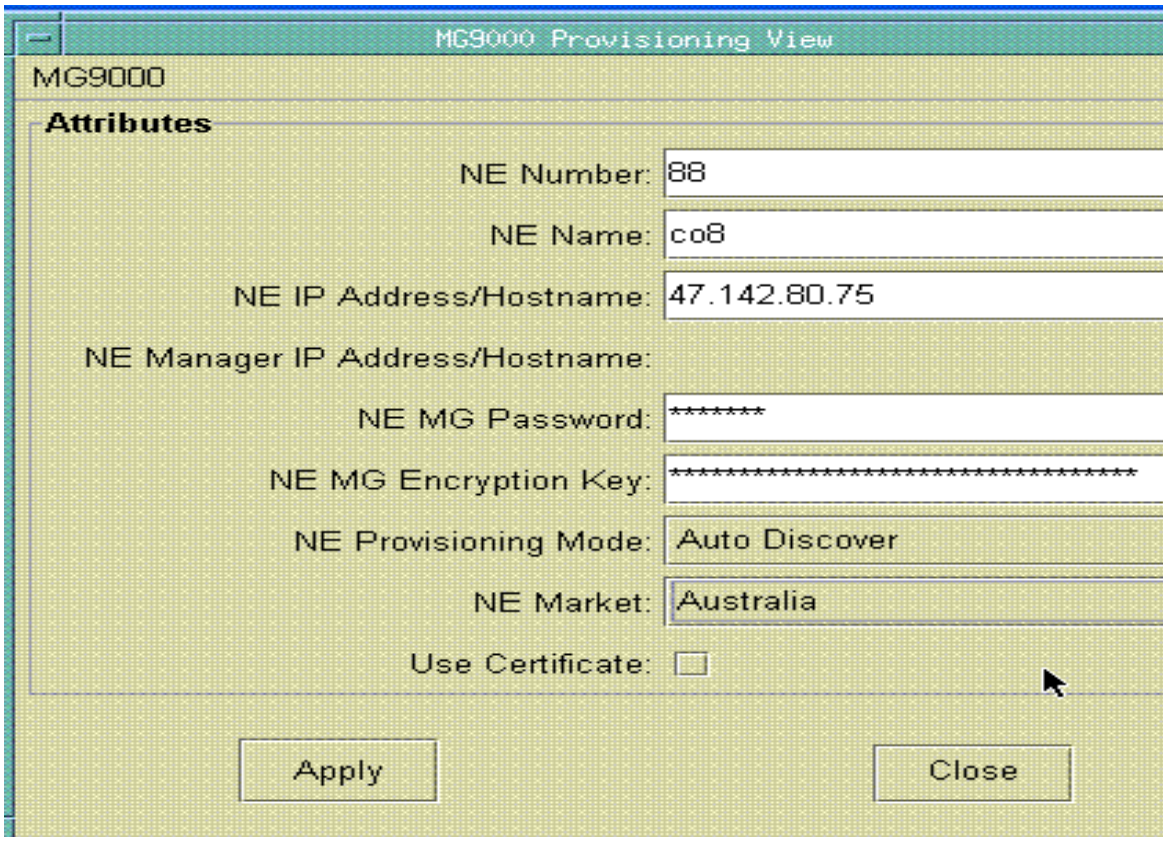


Figure 3: Add New MG9000 View

The market set for the NE can be viewed from 'Add/Modify NE Properties View'. This market's coefficients will be downloaded onto the GW during LineCoefficient audit.

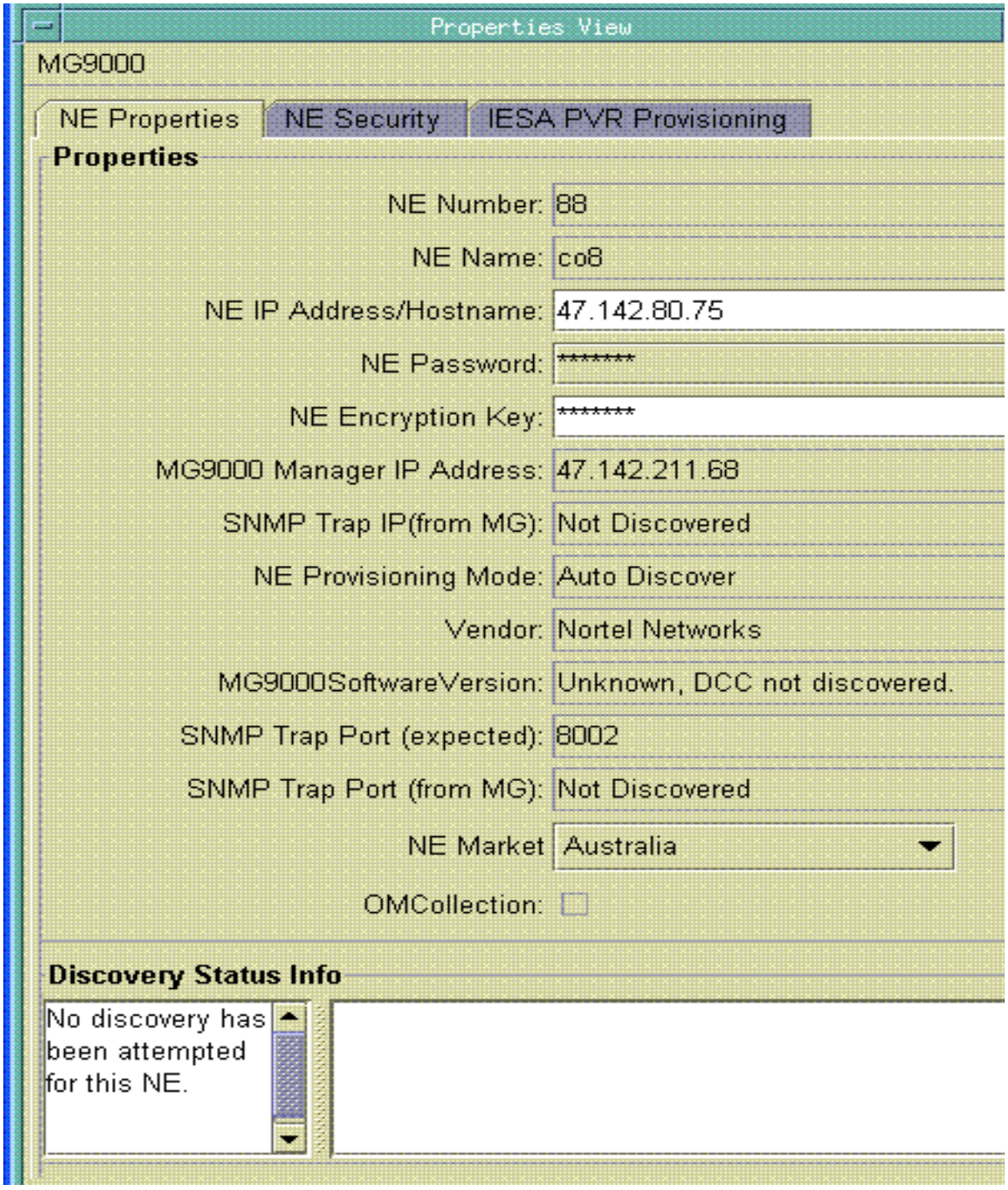


Figure 4: Add/Modify NE Properties View

Once the VMGs are created, the market can be modified only if the new market selected belongs to the same country code as that of the set market. If the user tries to select a market which does not belong to the same country code, an error message will be displayed to the user. If there are no VMGs the market can be modified to any other market (different country code) and the line coefficient audit will run which will push those coefficients onto the GW.

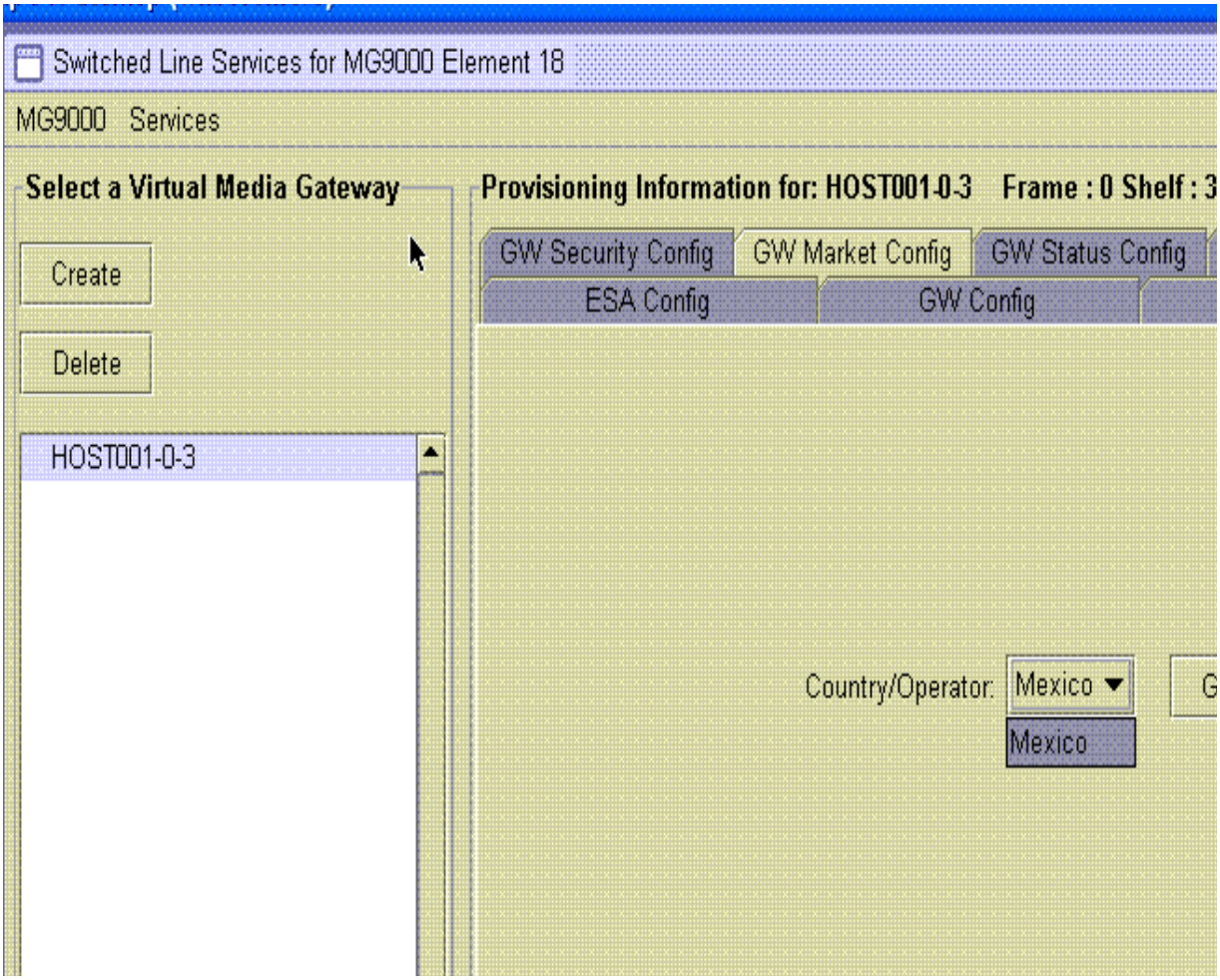


Figure 5: Get market for VMG.

Once the market is set for the NE, the VMGs created will have to use the same NE market. In SwitchLineServices View in the getMarket() tab in the VMG displays only the market set for that NE. But if a VMG already exists (before setting the NE's market, this can happen during upgrade scenarios) which has a different market, then both VMG market and the NE market will be displayed. The user will be able to change the market to NE market.

47.10 User interface changes

NA

47.11 OSSGate Interface Changes

None

47.12 Security

47.12.1 Network configuration

NA

47.12.2 Key management

NA

47.12.3 Protocol

NA

47.12.4 Authentication

NA

47.13 Configuration Walkthrough

None

48: Configuration (CN): A00012199

48.1 Feature Name

MG9K EM CPR Robustness

48.2 Hardware and Software Requirements

There is no specific hardware required for this feature.

48.3 Initial Configuration

The browser path should be defined in operating system environment where EM client is running.

48.4 Office/Subnet parameters (OP/SP) (CM & SESM)

NA

48.5 Upgrade Considerations

NA

48.6 Data schema (DS) (CM, MIBS, RDB)

48.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
NORTEL-UEMG-NODE-MIB	Changed	Unchanged

48.6.2 Table/MIB/Remote Database Schema information

48.6.2.1 Name: NORTEL-UEMG-NODE-MIB

48.6.2.2 Functional description

Two scalar MIB variables will be added in this MIB for LCI launch functionality. One MIB variable will store slot 10 out of band IP and another MIB variable will store slot 11 out of band IP. One additional MIB will be introduced for clear persist and discover functionality.

48.6.2.3 Usage sequence and implications (CM Only)

None

48.6.2.4 Size

NA

48.6.2.5 Fields/OIDs

The following table lists fields/OIDs added in NORTEL-UEMG-NODE-MIB.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
slot 10 outofbandIP	New	NA	This MIB will hold Slot 10 ethernet DCC IP.	When craftperson wants to launch LCI out of band thorough slot 10, this IP will be required to form the URL. For e.g. if this IP is 47.142.80.80 the URL for launching browser will be “https:// 47.142.80.80”.
slot 11 outofbandIP	New	NA	This MIB will hold Slot 11 ethernet DCC IP.	When craftperson wants to launch LCI out of band thorough slot 11, this IP will be required to form the URL. For e.g. if this IP is 47.142.80.81 the URL for launching browser will be “https:// 47.142.80.81”.
norNodeClear PersistOp	New	NA	Off	This MIB once set from EM would trigger clear persist and discover functionality on MG9K.

48.6.2.6 Datafill example

None

48.6.2.7 Table release history update

NA.

48.6.2.8 Supplementary information

These MIBs will be supported for all the types of DCC cards.

48.6.2.9 Translation verification and other tools

None

48.7 Service Orders (SO) (CM & SESM)

NA

48.8 Software optionality control (SOC)

NA

48.9 Element Management

48.9.1 New/modified GUIs

Table 3 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
NE Discovery View	Changed

48.9.2 GUI information

48.9.2.1 GUI name: NE Discovery View

48.9.2.2 Functional description

The NE Discovery View will now show one more button for “Clear persist and discover” functionality.

Impact on existing functionality of NE Discovery View:

This new button will be shown for all the NEs. When user clicks this button for GW version less than SN091, an appropriate information message will be shown for not supporting this feature. This field cannot be grayed out for lower release NEs because this feature needs to be supported for undiscovered NEs also and EM will not have GW version information for undiscovered NEs.

48.9.2.3 GUI usage and implications

None

48.9.2.4 GUI size

Table 4 New or modified GUIs

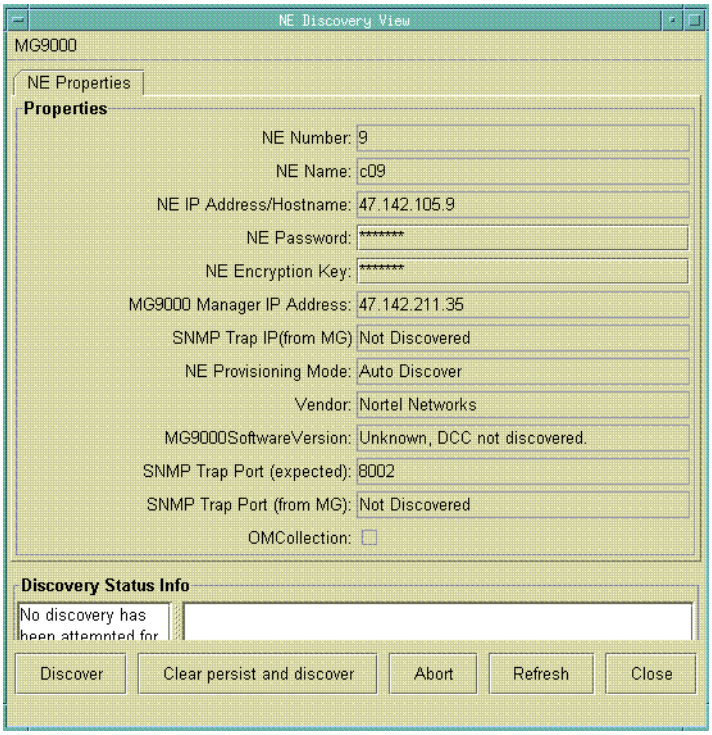
Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
NE Discovery View	1	Number Of NEs in subnet	TBD

48.9.2.5 GUI fields

As discussed before NE Discovery view will have one more button next to “Discover” button.

48.9.2.6 Usage example

The following example shows the NE Discovery View on EM GUI.



48.9.2.7 Context sensitive launching information

None

48.9.2.8 Supplementary information

None.

48.9.2.9 GUI name: Subnet Configuration Menu

48.9.2.10 Functional description

LCI session will be invoked through a new submenu in configuration menu of subnet view.

48.9.2.11 GUI usage and implications

None

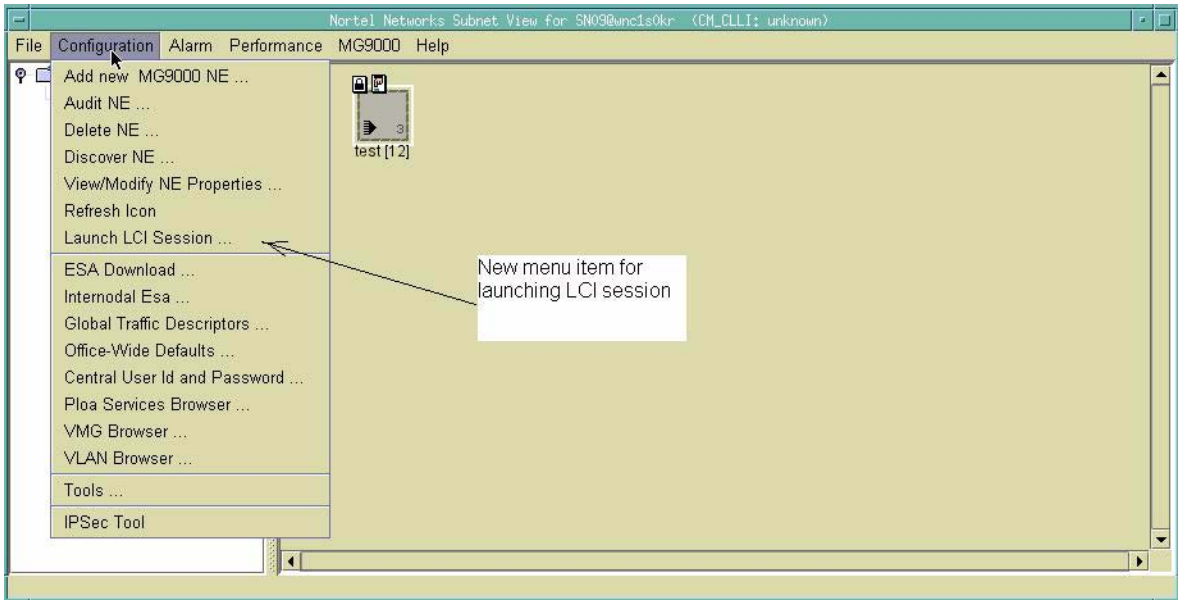
48.9.2.12 GUI size

Table 5 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Configuration menu	1	1	TBD

48.9.2.13 GUI fields

The new menu item will look like as shown below.



48.9.2.14 Usage example

The example above shows the new menu item details.

48.9.2.15 Context sensitive launching information

None

48.9.2.16 Supplementary information

None.

48.9.2.17 GUI name: Launch LCI View

48.9.2.18 Functional description

After clicking on “Launch LCI Session”, a new view will be invoked for launching LCI. This view will give user option of connecting to LCI either inband or out of band. The inband invocation will be successful only if proper

network routing is done. The details are given functional description document on the inband IP and network routing. Out of band invocation can be done either through slot 10 or slot 11.

48.9.2.19 GUI usage and implications

None

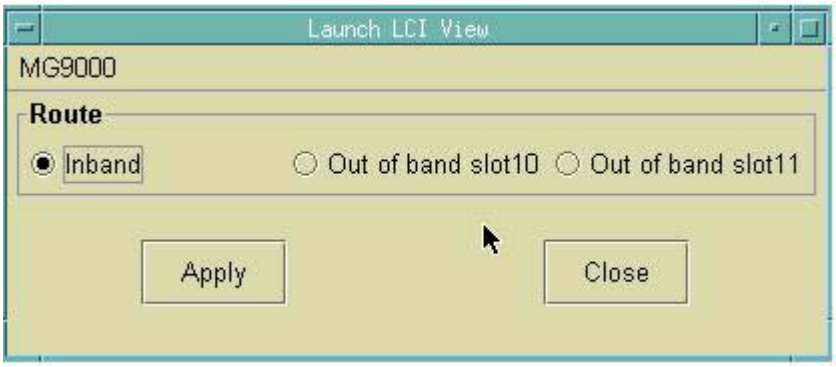
48.9.2.20 GUI size

Table 6 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Launch LCI View	1	1	TBD

48.9.2.21 GUI fields

The new view will look like as shown below.



48.9.2.22 Usage example

The example above shows the new menu item details.

48.9.2.23 Context sensitive launching information

None

48.9.2.24 Supplementary information

None.

48.9.3 CLUI Interface

NA

48.10 User interface changes

NA

48.11 OSSGate Interface Changes

None

48.12 Security

48.12.1 Network configuration

NA

48.12.2 Key management

NA

48.12.3 Protocol

NA

48.12.4 Authentication

The clear persist and discover functionality will be allowed for EM users with admin privileges for e.g. users with emsadm and higher permissions.

Launching LCI session is also supported only for admin users.

48.13 Configuration Walkthrough

None

49: Configuration (CN): A00012215

49.1 Feature Name

Global Line Card Field Programmable Gate Array

49.2 Hardware and Software Requirements

The NTNY53BA GLC card can replace any NTNY53AB or NTNY53AA card. The NTNY53BA GLC card provides all the supported capabilities of the NTNY53AB GLC card. The ITP cards must be at a release that allow the GLC card to be downloadable.

49.3 Initial Configuration

Lock and offline an existing NTNY53AB GLC card. Replace with the NTNY53BA GLC card. Online and unlock the NTNY53BA card. Select the GLC card and examine the FPGA configuration load to determine if the card needs to be downloaded and enter the information to download a new FPGA configuration load if needed.

49.4 Office/Subnet parameters (OP/SP) (CM & SESM)

None

49.5 Upgrade Considerations

49.5.1 Dump and Restore (CM)

None

49.5.2 Element Management Upgrade

Once the GLC, WLCor SAA hardware is replaced with a GLC NTNY53BA or NTNY53CA PEC code, any changes to the FPGA configuration load can be made via software downloading a new FPGA configuration load onto the GLC card. Normally, the FPGA configuration load for a GLC card is not changed. Only under rare circumstances would the FPGA configuration load be changed. Therefore, normal release to release upgrades do not include downloading GLCs.

The process for upgrade would be to upgrade the entire office utilizing the mg9kuptool upgrade CLUI tool. Once the entire office is upgraded, the customer should examine the FPGA configuration load on the GLC cards and make sure there is not a new release of the GLC configuration load. If there is a new release of the configuration load, the upgrade GUI from the frame view can be utilized to download multiple GLCs per PEC code. If only one GLC needs the new FPGA configuration load, for example to soak the new configuration load prior to releasing to all GLC cards, the software download manager should be selected from the card view for the chosen GLC card.

No alarms are output in the event two GLC cards with the same PEC code have different FPGA configuration loads.

49.5.3 Downgrade impact

If the ITP card is downgraded to a release that does not support downloading of GLC cards, any NTNY53BA and any NTNY53CA GLC cards can be attempted to download the FPGA however, since the ITP card does not support the software download of the FPGA, an error from the ITP is output. The customer is not prevented from attempting to download the FPGA as long as the correct GLC hardware is still in place.

49.6 Data schema (DS) (CM, MIBS, RDB)

norLineVineticReload 1.3.6.1.4.1.562.38.6.8.18

The norLineMib is changed to add in a new nnUemgLineTestTypes. This new test type tests to see if the circuit controller associated with this circuit needs to be reloaded. If no reload is necessary the test is completed. If the circuit controller needs to be reloaded, the controller for the 4 associated circuits is reloaded.

49.7 Service Orders (SO) (CM & SESM)

None

49.8 Software optionality control (SOC)

None

49.9 Element Management

49.9.1 New/modified GUIs

GUI name	NEW, CHANGED, or DELETED
GLC card View	Changed
GLC diagnostic View	Changed
Upgrade View from Frame View	Changed

49.9.1.1 GUI name: GLCC

GLC Card View

49.9.1.1.1 Functional description

The GLC Card View is modified to allow a new action of software downloading to occur. The software download manager menu item allows the configuration load of the FPGA on the GLC card to be software downloaded from the SDM/CBM. This prevents a hardware retrofit of the GLC card in the unlikely event the FPGA configuration load needs to change once the card is in the field. Also the GLC Card View is modified to show the FPGA

configuration load on the GLC card. Showing the FPGA configuration load allows the customer to visibly see what configuration load is currently on the hardware and allows the customer to determine if a new load needs to be downloaded to the FPGA.

49.9.1.1.2 GUI usage and implications

The floating IP must be assigned prior to using the GLC software downloading action. Also, the GLC card must be locked before the software downloading can take place. The software download manager invokes the existing software download GUI used to software download MTA and XDSL cards. The customer would have to input the file name including the directory path, IP address of the SDM/CBM, the user name on the SDM/CBM used to upgrade/ software download loads, and the server password to the SDM/CBM just as they do today for MTA and XDSL cards.

49.9.1.1.3 GUI size

49.9.1.1.4 GUI fields

Table 1 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GLCC	0 if no GLCs assigned in the office	one per GLC card in the office(14 per shelf for master shelf and 18 per shelf for each subtending shelf)	no increase in memory

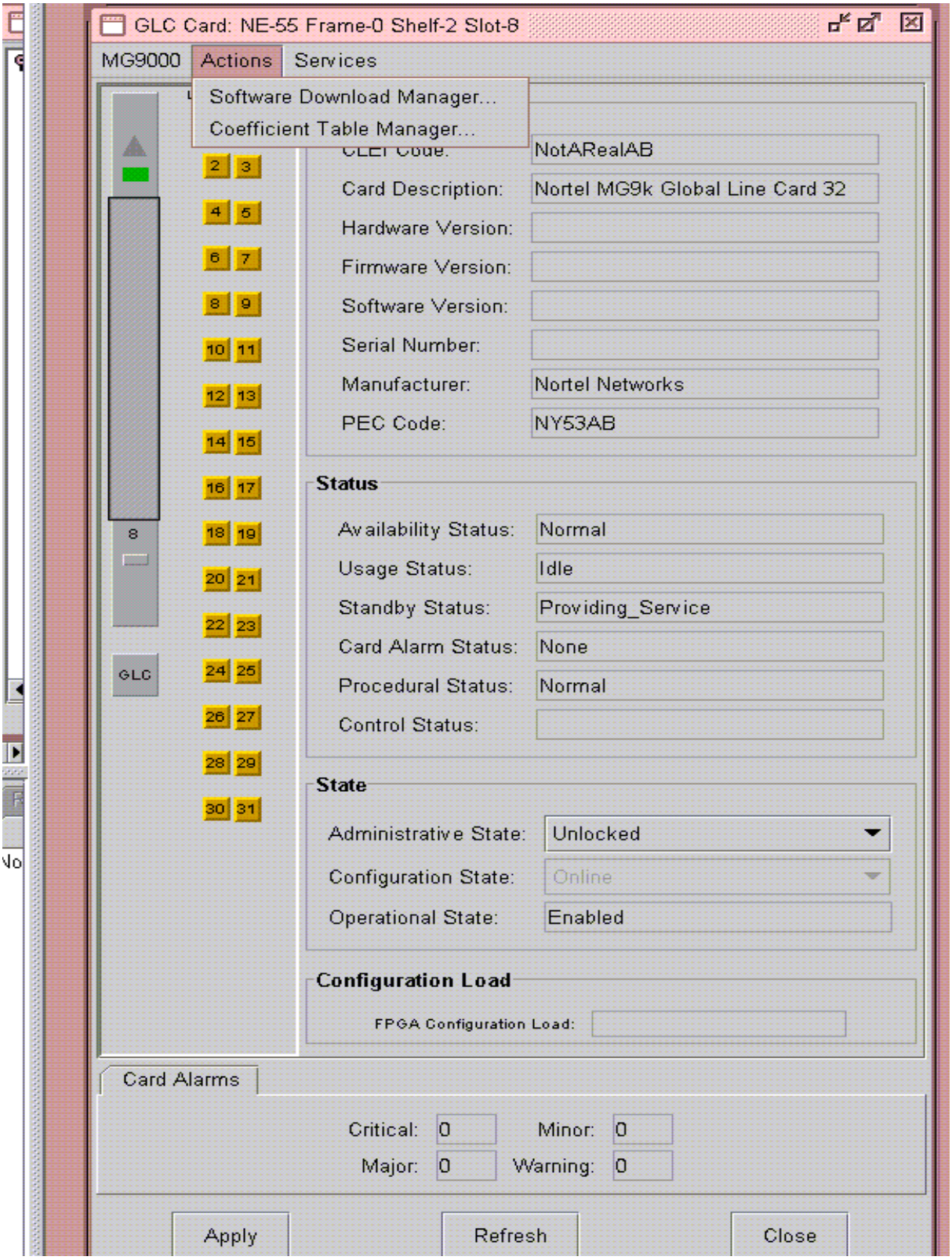
The following table lists fields for GUI GLCC.

Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Actions Menu	Changed	Software Download Manager	none	Added new Software Download Manager menu selection for GLC cards. This brings up the existing software download GUI view.	None for new menu option, existing NorNodeSWLoadEntry for software download GUI view.
FGPA Configura-tion Load	New	None	none	Displays the current FPGA load on the GLC card	norNodeSWLoadCurrentLoadName

49.9.1.1.5 Usage example

The following example shows the software download manager menu selection and the Configuration load name area for GUI GWCC.


GLC Card: NE-55 Frame-0 Shelf-2 Slot-8
MG9000
Actions
Services
Software Download Manager...
Coefficient Table Manager...
NotARealAB
Card Description:
Nortel MG9k Global Line Card 32
Hardware Version:
Firmware Version:
Software Version:
Serial Number:
Manufacturer:
Nortel Networks
PEC Code:
NY53AB
Status
Availability Status:
Normal
Usage Status:
Idle
Standby Status:
Providing_Service
Card Alarm Status:
None
Procedural Status:
Normal
Control Status:
State
Administrative State:
Unlocked
Configuration State:
Online
Operational State:
Enabled
Configuration Load
FPGA Configuration Load:
Card Alarms
Critical:
0
Minor:
0
Major:
0
Warning:
0
Apply
Refresh
Close
GLC

49.9.1.1.6 GUI release history update

Add Software Download Manager menu under the action menu for GLC card views. Add new area, configuration Load, to display the FPGA configuration load to the user.

49.9.1.1.7 Context sensitive launching information

In order to allow the user to select the software download, the user must have read write privileges. The software download manager and configuration Load are only visible to GLCs which have a PEC code of NTNY53BA or above. The software download manager and configuration load do not appear on NTNY53AA or NTNY53AB GLC cards.

49.9.1.1.8 Supplementary information

None

49.9.1.2 GUI name: GLCD

GLC Circuit Diagnostic View

49.9.1.2.1 Functional description

In order to perform the new diagnostic test, Circuit Controller Diagnostic, the GLC Line Circuit View for a particular circuit is opened from the GLC Card View. The Circuit Controller diagnostic is designed to determine if the circuit controller needs to be reloaded, and reload if necessary as determined by the gateway. The Actions menu from the GLC circuit View is selected. Maintenance menu is selected. Diagnostic menu is selected and inside the Diagnostic View, a new Diagnostic type is added for checking to see if a circuit controller requires reloading. The new diagnostic type is Circuit Controller Diagnostic.

49.9.1.2.2 GUI usage and implications

This new circuit controller diagnostic could be used if all four circuits of a circuit controller were in the operational disabled state and there were no other readily apparent reason for the 4 circuits to have an issue. The GLC card GUI indicates which 4 circuits are in a circuit controller group by alternating between dark blue and light blue. The first 4 GLC circuits are in one circuit controller group. Circuits 4 - 7 are in the next circuit controller group, and so on. So if a group of 4 circuits have no dialtone and there is no other apparent cause, run the circuit controller diagnostic or perform a lock-forced unlock if it appears to be an entire card.

49.9.1.2.3 GUI size

The GLC Circuit View and Diagnostic View are existing GUIs. Adding in a new selectable diagnostic type does not add any memory to the GUI.

49.9.1.2.4 GUI fields

The following table lists fields for GLCD

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Diagnostic Type	Changed	Controller Diagnostic	None	Selecting the new Controller diagnostics determines if the controller for this line circuit and the other 3 line circuits on this controller needs to be reloaded and reloads if appropriate	norLineVineticReload

49.9.1.2.5 Usage example

The following example shows menu selection for GLCD GUI to invoke the controller diagnostic:

49.9.1.2.6 GUI release history update

Add a new diagnostic type for circuit controller diagnostic for GLC Circuits. All GLCs, NTNY53AA/AB/BA/CA, are able to perform the circuit controller diagnostic. This diagnostic tests the circuit controller to determine if this single circuit controller needs to be reloaded.

49.9.1.2.7 Context sensitive launching information

In order to allow the new diagnostic, circuit controller diagnostic, to be selected the user must have maintenance privileges. The circuit controller diagnostic is available to any GLC PEC code including NTNY53AA and NTNY53AB.

49.9.1.2.8 Supplementary information

None

49.9.1.3 GUI name: UPGF

Upgrade View from the Frame View

49.9.1.3.1 Functional description

In order to provide the customer with the ability to software download all GLCs of a certain PEC code, the Upgrade Wizard invoked from the upgrade view for multiple cards is changed to add in the GLC-32 BA and GLC-12 CA check boxes to indicate software download of the FPGA is required for these GLC PEC codes.

49.9.1.3.2 GUI usage and implications

The customer selects the frame view. From the frame view, the customer selects the Actions pull down menu and selects Software Upgrade, the user then selects the Configure button from the upgrade view. The upgrade wizard opens and the user selects complete upgrade (GLC FPGAs can not be prep downloaded) and clicks on the Next button. The Card Type Selection portion of the upgrade wizard is shown and the user selects GLC-12 CA Cards and may optionally chose to select GLC-32 BA Cards. The software upgrade order would be GLC-32 BA cards, GLC-12 CA cards, XDSL cards, MTA cards, DS1 cards, ABI cards, ITP cards, ITX cards, and then Supercore cards. Downgrading order would be the opposite starting with Supercore cards and ending with GLC-32 BA cards.

49.9.1.3.3 GUI size

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
UGPF	0	1 per NE	no increase

49.9.1.3.4 GUI fields

The following table lists new or modified fields for the Upgrade Wizard invoked from the UpgradeView >

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
GLC-32 BA Cards	New	None	N/A	Check this box to software download all GLC-32 BA cards in the office	N/A
GLC-12 CA Cards	New	None	N/A	Check this box to software download all GLC-12 CA cards in the office	N/A

49.9.1.3.5 Usage example

The following example shows the addition of the GLC-32 BA and GLC-12 CA cards to the upgrade wizard.:

49.9.1.3.6 GUI release history update

Add GLC cards to the upgrade wizard only when opened from the frame view. Since there are separate FPGA loads for each GLC PEC code, the different PEC codes for the GLCs may be selected.

49.9.1.3.7 Context sensitive launching information

In order to view the upgrade wizard and see the GLC cards, the user must have administration privileges. Also, the GLC selection boxes only appear if the customer has those GLC PEC codes in the office. For example, if the customer only has NTNY53AB cards in the system, no GLC cards are shown in the upgrade wizard. If the customer has only NTNY53BA GLC cards in the office then only the GLC-32 BA Cards selection box would appear. Only GLCs with PEC codes above NTNY53BAare shown in the upgrade wizard.

49.9.1.3.8 Supplementary information

None

49.9.2 CLUI Interface

Not applicable

49.10 User interface changes

None

49.11 OSSGate Interface Changes

None

49.12 Security

No changes

49.13 Configuration Walkthrough

Replace GLC or WLC card with the NTNY53BA version of the GLC hardware. The ITP must be running with a software load capable of allowing the software download to the FPGA on the GLC card.

Once the NTNY53BA or NTNY53CA version of the GLC is resident in the system, the FPGA for those GLCs can be attempted to be software downloaded. First, select a GLC card and open the GLC card view. Examine the FGPA configuration load to determine if the FPGA has the correct load. If the FPGA does not have the correct load, verify the GLC Administrative State is locked. Lock the card if the administrative state is unlocked. Select the action menu, select the software download manager item. A new software download view is opened. Enter the File Path (the directory path and FPGA load name on the SDM/CBM), Server IP (IP address of the SDM/CBM where the loads reside), Server userName (user name on the SDM/CBM used to software download or upgrade loads), Server password (password on the SDM/CBM used to software download). Select Download button. Once the download has completed, unlock the GLC card.

50: Configuration (CN): A00012223, A00012217, A00012225

50.1 Feature Name

SESM Support for SIP Lines, Part 2

50.2 Hardware and Software Requirements

This feature requires the 905-240 GWC card, pec code NTRX51DL. It also requires that the CM, GWC SESM and MCS gateways are on a SN09 drop 2 load for all documented functionality to be available (otherwise the SN09 functionality is the default).

50.3 Initial Configuration

50.3.1 SESM-CS2K Prov Mgr EM Server Configuration

```
SESM-CS2KSS configuration


OPI - Provisioning Manager Interface configuration

Enter OPI transport protocol to EM server ( http/https - default: https)
 [1] - http
 [2] - https
 [x] - exit

select - 2

 Enter the IP address / Name of the primary CS2KSS prov server (default:
47.142.91.164) : 47.142.91.164
 Enter the primary CS2KSS prov server https port (default is 8443): 8443


 Enter the IP address / Name of the secondary  CS2KSS prov server (default:
47.142.91.164) : 47.142.91.164
 Enter the secondary CS2KSS EM server https port (default is 8443): 8443


 Enter the OPI administrator user name (default: admin): admin

 Enter the OPI administrator password:
 Re-enter the OPI administrator password:

OMI - Provisioning Manager Interface configuration

Enter OMI transport protocol to EM server ( http/https - default: https)
 [1] - http
 [2] - https
 [x] - exit

select - 2

 Enter the IP address / Name of the primary CS2KSS mtc server (default:
47.142.91.164) : 47.142.91.164
 Enter the primary CS2KSS mtc server https port (default is 12121): 12121
```

```
 Enter the IP address / Name of the secondary  CS2KSS mtc server (default:
47.142.91.164) : 47.142.91.164
 Enter the secondary CS2KSS mtc server https port (default is 12121): 12121


 Enter the OMI administrator user name (default: admin): admin

 Enter the OMI administrator password:
 Re-enter the OMI administrator password:


OPI - Provisioning Manager configuration

Transport protocol to EM server                   :   https://
Primary CS2KSS Provisioning Manager IP / Name     :   47.142.91.164
Primary CS2KSS Provisioning Manager port          :   8443
Secondary CS2KSS Provisioning Manager IP / Name   :   47.142.91.164
Secondary CS2KSS Provisioning Manager port        :   8443
The administrator user name                       :   admin


OMI - Maintenance Manager configuration

Transport protocol to Maintenance Manager         :   https://
Primary CS2KSS Maintenance Manager IP / Name      :   47.142.91.164
Primary CS2KSS Maintenance Manager port           :   12121
Secondary CS2KSS Maintenance Manager IP / Name    :   47.142.91.164
Secondary CS2KSS Maintenance Manager port         :   12121
The administrator user name                       :   admin

Is the information correct? (y or n) :y
```

The configuration tool will prompt the user to enter the following for the OMI link information:

- Transport protocol to SS-EM server (https).
- IP address / host name of primary SS-EM server
- IP address / host name of secondary SS-EM server. Some configurations may not include a secondary SS EM server. If so, configure the same information provided for the primary server (by default this should be the case).
- HTTPS communication port to SS EM server (12121).
- SS-EM Provisioning Manager administrator user name
- SS-EM Provisioning Manager administrator password

The OPI version information is not required anymore since it is dynamically determined when the OPI and OMI links come into service.

The IP address and port will be used to generate the SS-EM Provisioning Manager URL which in turn will be added to sesm.properties file.

As part of the configuration, the IP address will be validated for format, range and reachability. Other user entered data will be validated for format, range, values etc.

The user name will be added to sesm.properties as clear text.

The password will be stored separately and accessible only to the root user.

All configuration information (url, username, etc.) except password can be displayed by using the SESM "/opt/nortel/NTsesm/admin/bin/configure" tool.

50.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

50.5 Upgrade Considerations

Initial support for Session Server SIP lines gateways was delivered in SN09. This feature will extend that support in various areas (provisioning, audits, and maintenance) and will therefore be required to implement a backwards compatibility mechanism in order to allow interactions with older Session Server element manager loads which do not support the new functionality.

50.5.1 Dump and Restore (CM)

Not Applicable.

50.5.2 Element Management Upgrade

Upgrading the SESM from SN09 to SN09 drop 2 loads while the Session Server remains on SN09 level software can be done without the need for manual interactions. The backwards compatibility logic within SESM should be able to query any existing Session Server element managers for its load version and implement the backwards compatible interface accordingly.

Some new configuration will be required for the SESM application following either the upgrade of the Session Server or the upgrade of the SESM in order to allow SESM connections to the maintenance system on the Session Server element manager. These new connections are necessary to enable SN09 drop 2 maintenance, audit and provisioning capabilities following system upgrade.

50.5.3 Downgrade impact

No impact - works as per current process.

50.6 Data schema (DS) (CM, MIBS, RDB)

N/A

50.7 Service Orders (SO) (CM & SESM)

No new service orders are created under this activity, however a new suboption for the SIP_DATA option is defined which can be used in NEW/CHF/EST/ ADD commands applicable to SIP lines hosted off of Session ServerVMGs.

All listed may also be used via the Bulk Provisioning Tool.

50.7.1 Service order change details

LCC and options
A new SIP_DATA suboption is introduced by this feature. The SIP_DATA suboption SIP_SUBDOMAIN, like the existing suboptions, is not presented to XACore SERVORD (it is removed from the command prior to XACore SERVORD command processing).

50.7.1.1 Option Format:

SIP_DATA sub-options-and-values $

where

sub-options = SIP_CLIENT_TYPE, SIP_URI, SIP_PASSWD, SIP_PACKAGE, SIP_LOCATION, ***SIP_SUBDOMAIN***

The SIP_DATA option and sub-option tags and values may be entered in either lower or upper case transparently.

> ***Note:*** sub-option values have external case restrictions. See "50.7.1.4 Usage/Format Validation and Rules" on page 2846.

50.7.1.2 Sub-option value formats:

SIP_SUBDOMAIN option value format = {token_string_value}

50.7.1.3 SIP_DATA Sub-option and Value Examples:

"SIP_DATA SIP_PACKAGE test package SIP_URI someone@nortel.com **SIP_SUBDOMAIN rtp.nortel.com** SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD test1password $"

50.7.1.4 Usage/Format Validation and Rules

OSSGate/SERVORD+ SIP_DATA SIP_SUBDOMAIN validation will be limited. The Session Server element manager will be responsible for validating the actual value contents.

When the SIP_SUBDOMAIN suboption is specified in provisioning commands (e.g. NEW, EST, etc.), subsequent queries (e.g. QLEN/QDN/etc.) will include a SIP_SUBDOMAIN data in output.

Queries showing SIP_URI information will always include the domain (not sub-domain) information formatted as <user>@<domain>. If a subdomain

value is used in the SIP_URI suboption (<user>@<subdomain>) in provisioning commands, subsequent queries will show the SIP_URI with the domain, <user>@<domain>.

Prior to delivery of this feature content, if the customer has more than 35000 lines (> 1 Session Server for lines) the SIP_URI suboption in the command must include the subdomain. Subsequent queries will not display information about subdomains.

The use of Directory Number in the SIP_URI value (e.g. 2145209999@nortel.com) is discouraged. CDN commands which modify the DN assigned to the user will ***not*** automatically update the SIP_URI.

50.7.1.4.1 Rules Enforced for SIP_DATA by OSSGate/SERVORD+

Breaking these rules causes immediate command failure/rejection by OSSGate/SERVORD+:

- One or more sub-options are REQUIRED when the SIP_DATA option is specified.
- Sub-option tags are reserved words and may not be used as values for other sub-options or for any non-related types (e.g. CM customer group, gateway names, etc.). For example, “SIP_PASSWORD sip_password” is an invalid option and value pair. “sip_password” may not be used as the value specified for the SIP_PASSWORD sub-option. “sip_password” may not be used as a part or whole value for any other sub-option (e.g. “SIP_LOCATION sip_passwd” will be rejected).
- The SIP_DATA terminator, “$”, is a reserved token and may not be used as a value of any SIP_DATA sub-option. If a sub-option is present in the SIP_DATA options list, then it must have a valid value other than “$”.
- The tag-value pair relationship for the options/sub-options will be enforced from a simple format perspective. All sub-options must have associated values. The overall SIP_DATA option must be terminated by a “$”.
- Multiple/extraneous SIP_DATA options or sub-options found in a single NEW/CHF/EST/ADD command, will result in rejection of the command by OSSGate/SERVORD+. This limits the number of SIP LENs/endpoint which can be included in EST/ADD group commands to **ONE**.
- SIP_URI must be of the format user@domain. The domain information is parsed from the URI value. A missing domain (e.g. missing @ delimiter or domain information) will cause immediate command failure. An invalid domain name specified will be rejected by the Session Server Provisioning Manager.
- SIP_LOCATION must be included in the SIP_DATA option when the command issued results in the creation of a new user on the Session Server.

- SIP_SUBDOMAIN is an optional suboption and if not present, the domain parsed from the URI is used when creating the user on the Session Server element manager

50.7.1.4.2 Rules NOT Explicitly Enforced for SIP Data by OSSGate/SERVORD+

These rules are not explicitly enforced by OSSGate/SERVORD+. Breaking these rules may cause command failures or other unintended consequences:

- SIP_DATA and the associated sub-option tags are reserved words and may not be used as values for any non-related types (e.g. CM customer group, gateway names, etc.). Use of the reserved keywords in this manner may cause unexpected problems when attempting to use OSSGate/SERVORD+ for provisioning ANY type of line.
- CHF commands affecting SIP_DATA on SIP lines requires that gateway/termination names (or associated LEN) be used in the command instead of DN. Use of DN will result in the command being processed only by the CM, which is undesirable when SIP_DATA is present in the command.
- ADO and DEO commands for SIP lines affecting MDN data requires that gateway/termination names (or associated LEN) be used in the command instead of DN (e.g. “ADO $ <DN or LEN> <OPTIONS>”). Use of DN will result in the command being processed only by the Core/CM, which will result in group data misalignment between the Core/CM and the SS-EM.
- Use of the SIP_DATA option is not supported in commands which do not affect SIP lines or in commands which are not supported for flowthrough **for** SIP lines. Use of the SIP_DATA option in these commands may cause unintended command failures.
- The SIP_DATA option may fall anywhere in the command string except as the first token (which is reserved for the command name), however it is ***highly recommended*** that the SIP_DATA option be placed in the normal option field range of the command.
- The values assigned to sub-options SIP_CLIENT_TYPE, SIP_PACKAGE, and SIP_LOCATION are ***case sensitive***. **When commissioning these associated values on the Session Server Provisioning Manager, you MUST use the case which will be sent from the OSS (some OSS support only upper case, some lower case, and yet others mixed case).** Failure to commission these values in the Session Server Provisioning Manager using the case text supported by the OSS will result in command failures at OSSGate/SERVORD+.
- SIP_URI is normalized to lower case by the Session Server Provisioning Manager when received from OSSGate/SERVORD+. Caseless comparisons are performed by the Session Server Provisioning Manager when determining if a URI entered at OSSGate is already in use (e.g. “Slynch@Nortel.com” is considered identical to “slynch@nortel.com” from the Session Server Provisioning Manager’s perspective). Only the

normalized/lower-case URI is stored by the Session Server Provisioning Manager (e.g. “USERname1@Domain1.net” received from OSSGate/ SERVORD+ would be stored as “username1@domain1.net” in the Session Server Provisioning Manager).

50.7.1.5 Data Mapping Example

In the following command,

LEN: MSM1 00 0 00 00

is mapped to

VMG: TestMSMVMG.1

termination/endpoint: MSM1/000/0/0000

OSSGate command:

```
NEW $ 9195200500 IBN PRADEFAULT 0 0 LATA1 0 MSM1 00 0 00 00 DPL
Y 10 SIP_DATA SIP_PACKAGE test package SIP_PASSWD test1Password
SIP_URI someone@somecompany.com SIP_CLIENT_TYPE SIP Line
SIP_LOCATION Nortel Networks.RTP SIP_SUBDOMAIN
local.somecompany.com $ MDN SCA Y Y TONE N $
```

XACore SERVORD command derived from OSSGate command:

```
NEW $ 9195200500 IBN PRADEFAULT 0 0 LATA1 0 MSM1 00
0 00 00 DPL Y 10 MDN SCA Y Y TONE N $
```

Data sent to SS-EM:

VMG: TestMSMVMG.1

termination: MSM1/000/0/0000

Domain: somecompany.com

Subdomain: local.somecompany.com

User: someone

Password: test1Password

firstName: SIPLineUser (default value)

lastName: SIPLineUser (default value)

Package: test package

locale: English (default value)

timezone: Eastern Standard Time (default value)

clientType: sip line

DN: 9195200500

location: nortel networks.rtp

status: ACTIVE (default value)

group type: MDN

group name: 9195200500

50.7.2 New commands

Not Applicable.

50.7.3 Line equipment format changes

50.7.3.1 LEN

No LEN format changes are introduced by this feature. Typical LEN format for SS LENs:

SITE FFF G TT tt

SITE = SITE name

FFF = frame number, 0-511

G = group number, 0-9

TT tt = terminal, 00 00 - 10 23

50.7.3.2 Media gateway endpoint format

No gateway/endpoint format changes are introduced by this feature. Typical SS VMG and endpoint formats:

VMG = 64 character free-form string (e.g. TestSSVMG.1)

endpoint/termination = SITE/FFF/G/TTtt

where SITE, FFF, G, and TTtt value are as specified in the SS LEN format with the following conversion padding rules:

- The LEN's individual TT tt values will always be zero-padded to 2 digits when converted to an endpoint/termination name (e.g. TT tt value "2 7" would be converted to an endpoint/termination TTtt value of "0207").
- The LEN's FFF value will always be zero-padded to 3 digits (e.g. FFF value "6" would be converted to endpoint/termination FFF value "006").

50.8 Software optionality control (SOC)

50.9 Element Management

SESM

50.9.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Line Data Audit	**CHANGED**

50.9.2 GUI information

50.9.2.1 GUI Name: Line Data Audit

In this feature, the line audit will also audit the data in Session Server EM. The audit GUI look and feel does not change, except that few checks are added to warn the user of system load. Also the audit output file (both valid and problem files) will have extra information pertaining to the Session Server audit.

50.9.2.1.1 Functional description

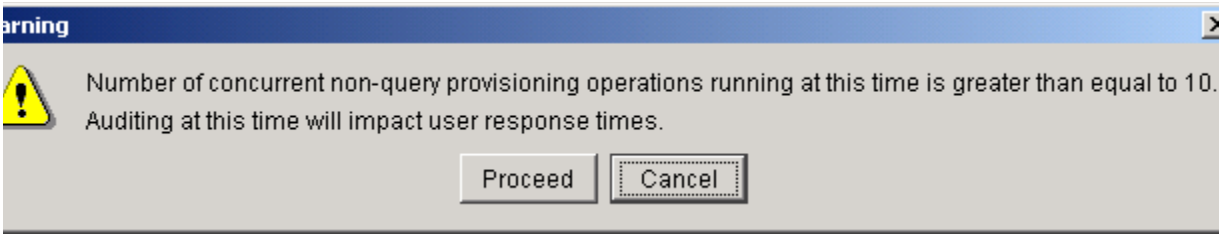
Warning Dialogues in Audit GUI:

One of the requirement in this feature is to avoid running (at least warn) line audit when the system is loaded, as the audit might impact more important provisioning activities. In this feature, the manual line audit will check for the system load and warn the user if its not an appropriate time to run audit.

If any of the three checks is true, then the server will return 'not ready' with details to the GUI, which in turn will pop a dialogue box to warn user of system load and gives him a chance to decide if he wants to run the audit at a later time, since running audit has the potential to slow down the system impacting higher priority provisioning activities.

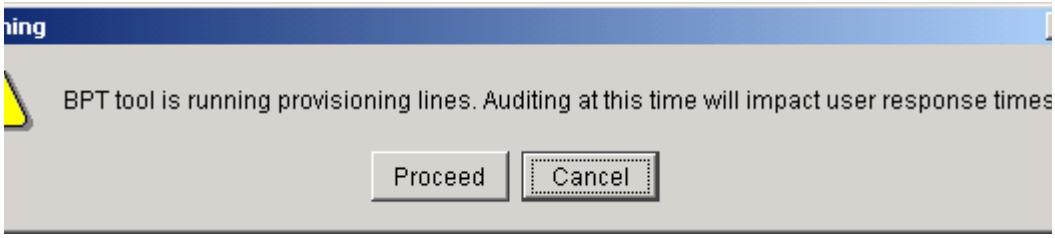
First check done by the server is to see if there are 10 or more concurrent non-read-only operations in progress. If yes, the audit server returns 'not ready' with details to the GUI. Shown below is example dialogue box.

Figure 1 Warning if 10 or more non-query type line provisioning in progress



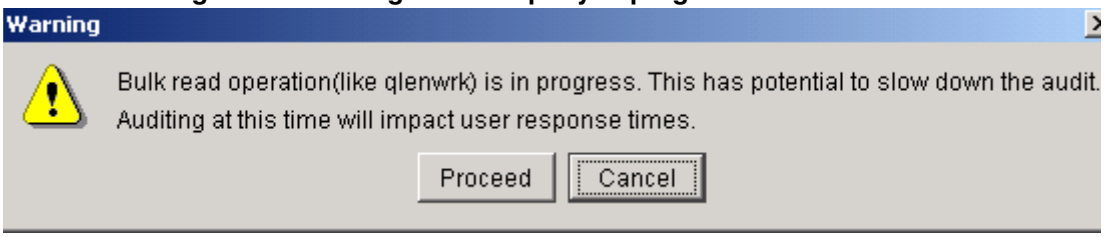
The second check is to see whether BPT tool is running a lines batch operation. If yes, the server returns ‘not ready’ with details to GUI. Shown below is example dialogue box in this condition.

Figure 2 Warning if BPT tool is running, provisioning lines



The third check is to see whether any bulk query operation (like qlenwrk,qdnwrk etc) is already in progress. If yes, the server will return ‘not ready’ to the GUI. Shown below is example dialogue box in this scenario.

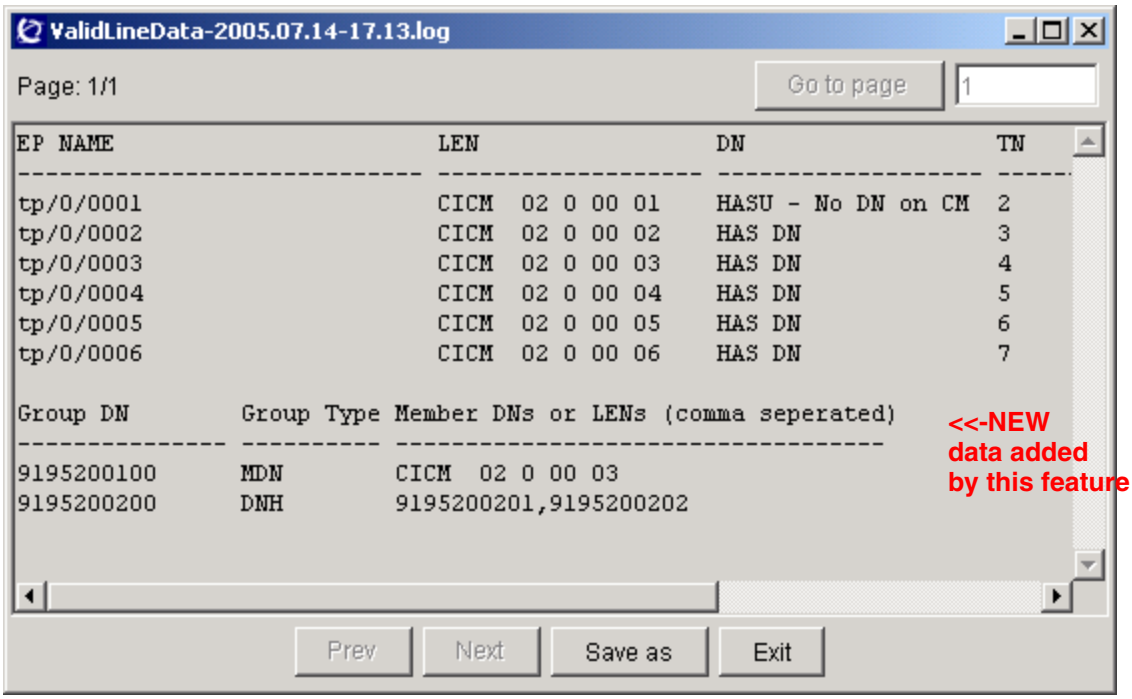
Figure 3 Warning if a bulk query in progress before line audit starts



Line Data Audit Valid Data output:
After the line data audit finishes, the ValidLineData.log file will have additional information obtained by auditing the Session Server EM.

The endpoints in GWCEM will be compared with SS EM, the group DN and its member DN information will be compared with the core and the DN to len mapping will also be compared with the core.

In the first screen shot is shown, valid data w.r.t the Session server will be at bottom. In the following screen shot, the group DN and its type and the member DNs are printed on screen, which is new audit data added by this feature if SIP MGs are provisioned.



50.9.2.2 Line Data Audit Problem Data output:

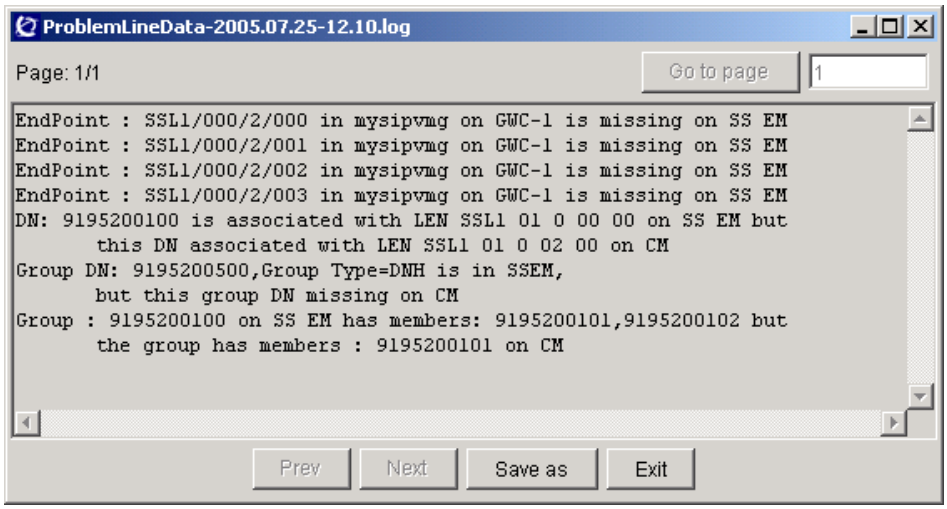
Shown below is screen shot of problem line data results. The problems could be in following areas

1. Endpoint exists in GWCEM, but not in Session server EM

2. DN associated with endpointId (len) in SS EM, while that same DN maps to different LEN on core

3. group DN in SS EM but that group information is missing in core

4. member DN/LENs in SS EM belonging to a group do not match the member list in that group on core.



50.9.2.3 GUI usage and implications

50.9.2.3.1 GUI size

Not applicable.

50.9.2.3.2 GUI fields

Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

50.9.2.3.3 Usage example

50.9.2.3.4 GUI release history update

50.9.2.3.5 Context sensitive launching information

Not impacted, no changes

50.9.2.3.6 Supplementary information

None

50.9.2.4 CLUI Interface

Warning in BPT on Audit Running:

A check is introduced in BPT tool where it determines if Line Audit is currently running. If yes, BPT tool will warn the user that line audit is in

progress and gives the user a chance to run the lines batch later, as the throughput of the Lines batch could be slower due to line audit running.

Screen shot from BPT tool when lines batch is started if line audit is in progress.

***** W A R N I N G *****

Line Audit is currently in progress.

This lines batch may run slower and may also invalidate audit results

Do you still want to proceed with lines batch? <y/n>:

The above warning tells the user that line audit is in progress and perhaps the lines batch should be run after the audit is finished.

50.9.3 LMM CLUI

To access the LMM CLUI telnet to OSSGate, enter ^B, “mode MTC”. Once in the MTC level, “LMM” is entered for access to the LMM CLUI.

```
>
? mode MTC

Mode is MTC.
```

The CMCLLI command is used to return the SDM IP and CMCLLI name:

```
>CMCLLI
      SDM IP = 47.142.134.124
      CM CLLI = RTP2



>LMM
      report <-v>
      report <-l> <report name>
      report <-gen> <GWC Options>

      post <-d, -l, -gw, -u, -r, -set, -display, -count>

      bsy <-d, -l, -gw, -set> [inb]
      rts <-d, -l, -gw, -set>
      tst <-d, -l, -gw, -u, -set>
      FRLS <-d, -l>

      qdn <dn>
      qlen <len>
      qsip <dn, len>

      help

      quit
```

The commands (i.e. report, bsy) can be entered in either upper or lower case. The options (i.e. -d, -l) must be entered in lower case. The parms can be entered in either case but in the case of the GW name, should be in the proper case.

50.9.3.1 REPORT Commands

The REPORT commands are used with the GW in Trouble reports. Using the commands, the user has the ability to list, view and delete any of the reports. The GENERATE or GEN is used to run the process to create a report.

Command format:

```
report <-l>
report <-v> <REPORT NAME>
report <-gen> <GWC List | all>
```

Command usage:

To obtain a list of reports currently available

```
>report -l
The following reports are available:
Report-2005-08-10-22-06-14
```

To view a specific report

```
>report -v Report-2005-08-10-22-06-14
GW Name   Results for GWC-0
t1124ent.us.nortel.com   GW DISABLED

GW Name   Results for GWC-10
test4   GW DISABLED
```

To request a new GW in Trouble report for GWC 1

```
report -gen 1
```

To request a new GW in Trouble report for GWC 1, 2 and 3

```
report -gen 1, 2, 3
```

or

```
report -gen 1-3
```

or

```
report -gen 1, 2-3
```

To request a new GW in Trouble report for all valid (small and large line) GWCs

```
report -gen all
```

50.9.3.2 MTC Commands

This set of commands is used to perform operations on either one or a set of lines.

Command format:

```
post -d <DN> [verbose]
post -l <LEN> [verbose]
```

```
post -gw <GW/VMG> [verbose]
post -u <URI> [verbose]
post -r <Domain name> [verbose]
post -display [verbose]
post -count

bsy -d <DN> [inb]
bsy -l <LEN> [inb]
bsy -gw <GW or VMG> [inb]
bsy -set [inb]

rts -d <DN>
rts -l <LEN>
rts -gw <GW/VMG>
rts -set

tst -d <DN>
tst -l <LEN>
tst -gw <GW/VMG Name>
tst -u <URI>
tst -set

frls -d <DN>
frls -l <LEN>
```

50.9.3.2.1 REPORT Commands

The REPORT commands are used with the GW in Trouble reports. Using the commands, the user has the ability to list and view any of the reports. The -gen is used to run the process to create a report.

Command format:

```
report <-l>
report <-v> <REPORT NAME>
report <-gen> <GWC List | all>
```

Command usage:

To obtain a list of reports currently available

```
>report -l
The following reports are available:
Report-2005-11-14-12-12-01
```

To view a specific report

```
>report -v Report-2005-11-14-12-12-01
GWC-14  Number of GWs out of service = 1

R7A20204.rtp7.net status = GW DISABLED

GWC-13  Number of GWs out of service = 11


To request a new GW in Trouble report for GWC 1
report -gen 1
```

To request a new GW in Trouble report for GWC 1, 2, 3 and 4

```
report -gen 1, 2, 3, 4
```

or

```
report -gen 1-4
```

or

```
report -gen 1, 2-4
```

To request a new GW in Trouble report for all valid (small and large line) GWCs

```
report -gen all
```

50.9.3.2.2 POST

The POST command can be used to generate a set of lines and be used for maintenance (BSY, etc.) actions.

The POST command will list the contents of the post set to the screen using a “brief” format. The information listed will be dn, len, uri, clientIp, gwc, lcc, cm line state, scc line state and MCS line state (if a SIP Line).

The VERBOSE option includes included the above and adds the following, GW/VMG name, GW ipaddress, GW type, endpointName, domain/ subdomain.

To post by DN (SIP Line)

```
>post -d 7550505
DN         = 6137550505
LEN        = SS 00 0 00 05
LCC        = IBN
GWC NAME   = GWC-5
GW NAME    = rtp7ssa
EPT NAME   = SS/000/0/0005
GW EPT ST  = ON-HOOK
CM EPT ST  = IDL
SIP URI    = user5@rtp7ssa.com
CLIENT IP  =
SS EPT ST  =


Number of endpoints returned = 1
```

To post by DN, non SIP Line

> post -d 6210010

```
DN         = 6136210010
LEN        = UAIP 00 1 00 00
LCC        = IBN
GWC NAME   = GWC-14
GW NAME    = rtp7-1104b.us.nortel.com
EPT NAME   = aaln/1
GW EPT ST  = ON-HOOK
CM EPT ST  = IDL


Number of endpoints returned = 1
```

To post by LEN:

```
      > post -l ss 0 0 0 5
DN         = 6137550505
LEN        = SS 00 0 00 05
LCC        = IBN
GWC NAME   = GWC-5
GW NAME    = rtp7ssa
EPT NAME   = SS/000/0/0005
GW EPT ST  = ON-HOOK
CM EPT ST  = INB
SIP URI    = user5@rtp7ssa.com
CLIENT IP  =
SS EPT ST  =
```

To post by GW:

Note: Since the minimum VMG size for SIP is 1023 endpoints, posting by vmg may take a long time (approx 5 mins per LGRP) and will produce a huge output.

```
      > post -gw rtp7-1104b.us.nortel.com
DN         = 6136210010
LEN        = UAIP 00 1 00 00
LCC        = IBN
GWC NAME   = GWC-14
GW NAME    = rtp7-1104b.us.nortel.com
EPT NAME   = aaln/1
GW EPT ST  = ON-HOOK
CM EPT ST  =

DN         = 6136210011
LEN        = UAIP 00 1 00 01
LCC        = IBN
GWC NAME   = GWC-14
GW NAME    = rtp7-1104b.us.nortel.com
EPT NAME   = aaln/2
GW EPT ST  = ON-HOOK
CM EPT ST  =

DN         = 6136210012
LEN        = UAIP 00 1 00 02
LCC        = RES
GWC NAME   = GWC-14
GW NAME    = rtp7-1104b.us.nortel.com
EPT NAME   = aaln/3
GW EPT ST  = ON-HOOK
CM EPT ST  =

DN         = 6136210013
LEN        = UAIP 00 1 00 03
LCC        = RES
GWC NAME   = GWC-14
GW NAME    = rtp7-1104b.us.nortel.com
EPT NAME   = aaln/4
GW EPT ST  = ON-HOOK
CM EPT ST  =
```

To post by URI:

```
      > post -u user5@rtp7ssa.com
DN         = 6137550505
LEN        = SS 00 0 00 05
LCC        = IBN
GWC NAME   = GWC-5
GW NAME    = rtp7ssa
EPT NAME   = SS/000/0/0005
GW EPT ST  = ON-HOOK
CM EPT ST  =
SIP URI    = user5@rtp7ssa.com
CLIENT IP  =
SS EPT ST  =
```

To post Registered users by domain. This command will return the users that have registered their clients with their provisioned domains.

Note: This command may take a long time and will produce a huge output.

```
      > post -r rtp7ssa.com
DN         = 6137550505
LEN        = SS 00 0 00 05
LCC        = IBN
GWC NAME   = GWC-5
GW NAME    = rtp7ssa
EPT NAME   = SS/000/0/0005
GW EPT ST  =
CM EPT ST  =
SIP URI    = user5@rtp7ssa.com
CLIENT IP  =
SS EPT ST  =

DN         = 6137550510
LEN        = SS 00 0 00 10
LCC        = IBN
GWC NAME   = GWC-5
GW NAME    = rtp7ssa
EPT NAME   = SS/000/0/0010
GW EPT ST  =
CM EPT ST  =
SIP URI    = user10@rtp7ssa.com
CLIENT IP  =
SS EPT ST  =


Number of endpoints returned = 2
```

To display the contents of the post se using the verbose option:

```
      >  post -display verbose
DN         = 6137550505
LEN        = SS 00 0 00 05
LCC        = IBN
GWC NAME   = GWC-5
GW NAME    = rtp7ssa
EPT NAME   = SS/000/0/0005
GW EPT ST  = ON-HOOK
CM EPT ST  = IDL
SIP URI    = user5@rtp7ssa.com
CLIENT IP  =
SS EPT ST  =
```

```
Node Num  = 213
Term Num  = 6
GWC IP    = 47.142.92.172
GW IP     = 47.142.91.154
GW TYPE   =
```

To display the number of entries in the post set:

```
>post -count
Post set size = 104
```

50.9.3.2.3 BSY

The BSY commands informs the CM to perform the requested action. A response message indicates the success or failure of the command. These messages are generated by the CM.

To Maintenance/Manual Busy a line by DN:

```
> bsy -d 7550505
DN = 7550505
CM RETURN CODE = CM_OK
```

To Maintenance/Manual Busy a line by LEN:

```
>  bsy -l ss 0 0 0 5
LEN = ss 0 0 0 5
CM RETURN CODE = CM_OK
```

To Maintenance/Manual Busy all lines on a GW:

```
> bsy -gw rtp7-1104b.us.nortel.com
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

To Busy by the posted set:

```
> bsy -set
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

The BSY INB operation performs two operations; first is a BSY then upon success, performs the INB operation. If the line is already in the BSY state then only the INB operation is performed.

If the line is IDL

```
      >  bsy -d 7550505 inb
DN = 7550505
CM RETURN CODE = CM_OK
DN = 7550505
CM RETURN CODE = CM_OK
```

If the line is BSY

```
> bsy -d 7550505 inb
DN = 7550505
CM RETURN CODE = CM_ALRDY_IN_REQ_STATE
DN = 7550505
CM RETURN CODE = CM_OK
```

50.9.3.2.4 RTS

To return-to-service a line by DN:

```
      > rts -d 7550505
DN =  7550505
CM RETURN CODE = CM_OK
```

To return-to-service a line by LEN:

```
      >  rts -l ss 0 0 0 5
LEN = ss 0 0 0 5
CM RETURN CODE = CM_OK
```

To return-to-service all lines on a GW:

```
      > rts -gw rtp7-1104b.us.nortel.com
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

To Busy by the posted set:

```
      > rts -set
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

50.9.3.2.5 TST

The TST performs a diag (where possible) depending upon the GW's ability to perform diagnostics on endpoints. Only GCP and MGCP GWs support the TST command.

To test by DN (SIP):

```
> tst -d 7550505

DN = 6137550505
LINE_STATE = PASSED
ENDPOINT_STATE = UNKNOWN
CLIENT = user5@47.142.166.65
TEST RESULT = PASSED
```

To test by DN (MGCP line):

```
> tst -d 6210010

DN = 6136210010
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
```

To test using the LEN (SIP)

```
      > tst -l ss 0 0 0 5

DN = 6137550505
LINE_STATE = PASSED
ENDPOINT_STATE = UNKNOWN
CLIENT = user5@47.142.166.65
TEST RESULT = PASSED
```

To test using the URI

```
      > tst -u user5@rtp7ssa.com

URI = user5@rtp7ssa.com
LINE_STATE = PASSED
ENDPOINT_STATE = UNKNOWN
CLIENT = user5@47.142.166.65
TEST RESULT = PASSED
```

To test by GW (or VMG).

Note: Testing by VMG may take a long time and produce a large amount of information.

MGCP based GW:

```
> tst -gw rtp7-1104b.us.nortel.com

DN = 6136210010
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
DN = 6136210011
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
DN = 6136210012
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
DN = 6136210013
LINE_STATE = ON-HOOK
```

```
ENDPOINT_STATE = OK
```

SIP GW

```
> tst -gw rtp7ssa

DN = 6137550500
LINE_STATE = FAILED
ENDPOINT_STATE = UNKNOWN
ERROR = Test Executed

DN = 6137550501
LINE_STATE = FAILED
ENDPOINT_STATE = UNKNOWN
ERROR = Test Executed
```

50.9.3.3 QUERY Commands

The query commands are used to perform various existing queries. These queries are the same as those from Servord.

Command format:

```
qdn <DN>
qlen <LEN>
qsip <DN, LEN>
```

Command usage:

To Query a DN

```
QDN 7201000
------------------------------------------------------------------------------
DN:     7201000
TYPE: SINGLE PARTY LINE
SNPA: 619   SIG: DT    LNATTIDX: N/A
LINE EQUIPMENT NUMBER:     SS    00 2 00 00
END POINT: rtp2sesm1  SS/000/2/0000
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:            BNR     SUBGRP: 0  NCOS: 0
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: N
PM NODE NUMBER     :    142
PM TERMINAL NUMBER :    1
OPTIONS:
CWT DGT DPL Y 10
OFFICE OPTIONS:
SRA

END POINT DATA:
SIP_CLIENT_TYPE: ont
SIP_EP_NAME: SS/000/2/0000
SIP_VMG_NAME: rtp2sesm1
SIP_DN: 6197201000
SIP_LOCATION: rtp2
SIP_PACKAGE: basic
SIP_URI: user0@rtp2.com
------------------------------------------------------------------------------
```

To query by LEN

```
> qlen SS 0 2 0 0
------------------------------------------------------------------------------
LEN:     SS    00 2 00 00
END POINT: rtp2sesm1  SS/000/2/0000
TYPE: SINGLE PARTY LINE
SNPA: 619
DIRECTORY NUMBER:     7201000
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:            BNR     SUBGRP: 0  NCOS: 0
SIGNALLING TYPE:  DIGITONE
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: N
PM NODE NUMBER     :    142
PM TERMINAL NUMBER :    1
OPTIONS:
CWT DGT DPL Y 10
OFFICE OPTIONS:
SRA
END POINT DATA:
SIP_CLIENT_TYPE: ont
SIP_EP_NAME: SS/000/2/0000
SIP_VMG_NAME: rtp2sesm1
SIP_DN: 6197201000
SIP_LOCATION: rtp2
SIP_PACKAGE: basic
SIP_URI: user0@rtp2.com
------------------------------------------------------------------------------
```

To query using the QSIP command. The parm can be either a DN or LEN.

```
> qsip 7550505
SS    00 0 00 05
SS/00/0/0005
------------------------------------------------------------------------------
SIP USER DATA
=============
SIP URI: user5@rtp7ssa.com
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: Y
NUMBER OF CONTACTS: 1
CONTACTS: user5@47.142.166.65
SERVICE PACKAGE:
basic_package
SERVICES:
ALCLNT N IM SIPLN ADVSCR 3 3 N CLNTCO N N N N ADHOC 4 ADDRBK 50 PRES 10 Y
20 Y VIDEO N N NWLOG 50 50

SIP LINE DATA
=============
ENDPT ID: SS/000/0/0005
VMG: rtp7ssa
ZONE ID(s):
CLIENT TYPE: ONT
STATIC CLIENT: Y

SIP CALL DATA
=============
ACTIVE CALL APPEARANCES:
  NODENO   TERMNO
NUMBER OF ACTIVE SESSIONS IN CS2000 SESSION SERVER: 0
------------------------------------------------------------------------------
>
```

50.9.3.4 MISC Commands

To quit from the LMM level - the user will remain in the MTC mode.

```
QUIT
```

50.9.3.5 Command Parsing

Multiple commands can be input on the same line - they must be separated by a ";". Up to 4 lens, dns or uris can be specified with the POST, BSY, TST and RTS commands. Due to the potential volume of output, only one GW or VMG can be specified.

The commands are not case sensitive, but the parameters may be, i.e. GW name will be case sensitive.

51: Configuration (CN): A00012526

51.1 Feature Name

TDM Call Recording Feature

51.2 Hardware and Software Requirements

There is no specific hardware requirement for this feature. The basic ICM software package as well as the software for the SN10 feature A00012527 are needed to use this feature.

51.3 Initial Configuration

The subscription to this feature has to be done according to the DS section below.

51.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

51.5 Upgrade Considerations

51.5.1 Dump and Restore (CM)

No new tables are being added for this feature.

51.5.2 Element Management Upgrade

N/A

51.5.3 Downgrade impact

None.

51.6 Data schema (DS) (CM, MIBS, RDB)

51.6.1 New/modified tables, MIBs, or Database Schema

The following table describes changed table information.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SCAISSRV	Changed	Unchanged

51.6.2 Table/MIB/Remote Database Schema information

51.6.2.1 Name: SCAISSRV

Switch Computer Application Interface Subservices table.

51.6.2.1.1 Functional description

Table SCAISSRV is used to enter default tuples for each SCAI message category as well as to add customizable category. This allows the customer to subscribe to these categories using Table SCAIPROF.

51.6.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

51.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SCAISSRV	0	511	Protected

51.6.2.1.4 Fields/OIDs

The following table lists fields for table SCAISSRV.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
TRNKINFO	New	Subfield	Y/N	trunk information

A new default tuple CTXEVENT19$ under category CTXEVENT will be created with the optional parameter TRNKINFO of the function CALLOFFR set to Y.
A new default tuple RESEVENT19$ under category RESEVENT will be created with the optional parameter TRNKINFO of the function CALLOFFR set to Y.

A new default tuple ACDEVENT19$ under category ACDEVENT will be created with the optional parameter TRNKINFO of the function CALLQUED and CALLOFFR set to Y.

```
TABLE SCAISSRV
 SUBSERV SPROFILE
 ------------------------------------------------
CTXEVENT19$ CTXEVENT (SETOFFHK Y Y Y)
(CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
(CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLREL Y Y Y Y)
(CALLNAME Y Y Y Y Y) $
```

RESEVENT19$ RESEVENT (SETOFFHK Y Y)

```
 (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLREL Y Y Y)
 (CALLNAME Y Y Y Y Y) $


 ACDEVENT19$ ACDEVENT (CALLQUED Y Y Y Y Y Y Y Y Y Y Y)
 (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLREL Y Y Y Y Y Y) (AGTLGDIN Y Y Y) (AGTLGDOUT Y Y)
 (AGTREADY Y Y)
 (AGTNREADY Y Y N) (LOBEVENT Y Y Y) (EMKEVENT Y Y Y Y Y Y)
(AGT SETACT Y Y N)
$
```

51.6.2.1.5 Datafill example

The following example shows sample datafill for table SCAISSRV.

1. EXAMPLE

TABLE: SCAISSRV

>add TRKTUP1

MACHINES NOT IN SYNC - DMOS NOT ALLOWED

JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED

ENTER Y TO CONTINUE PROCESSING OR N TO QUIT

>y

CATEGORY:

>CTXEVENT

FUNCTION:

>CALLOFFR

> NCALLID: Y

> CALLLNGNO:Y

> CALLNGNAME: Y

CHARGENO: Y

CALLTYPE: Y

ORIGDN: Y

ORIGNAME: Y

PREVAPPL:Y

HOSTCALD: Y

DEVICEID: Y

FWDPARTY: Y

TRNKINFO: Y

FUNCTION:

>$

>$

TUPLE TO BE ADDED:

TRKTUP1

CTXEVENT (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y **Y**) $

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

>y

2. EXAMPLE

>add TRKTUP2

MACHINES NOT IN SYNC - DMOS NOT ALLOWED

JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED

ENTER Y TO CONTINUE PROCESSING OR N TO QUIT

> y

CATEGORY:

>ACDEVENT

FUNCTION:

>CALLOFFR

>NETCALLID: Y

>ACDDN: y

>CALLNGNO: Y

>CHARGENO: Y

>CALLTYPE: Y

>ORIGDN: Y

>PREVAPPL: N

>HOSTCALD: Y

>ACDGROUP: Y

>DEVICEID: Y

>FWDPARTY: Y

>CPADIGS: Y

>**TRNKINFO: Y**

FUNCTION:

>CALLQUED

>NCALLID: Y

>ACDDN: Y

>CALLNGNO: Y

>CHARGENO: Y

>CALLTYPE: Y

>ORIGDN: Y

>PREVAPPL: Y

>HOSTCALD: Y

>ACDGROUP: Y

>FWDPARTY: Y

>CPADIGS: Y

> **TRNKINFO: Y**

>FUNCTION:

>$

TUPLE TO BE ADDED:

TRKTUP2

ACDEVENT (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y **Y**) (CALLQUED

Y Y Y Y Y Y Y Y Y Y Y Y **Y**) $

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

>y

51.6.2.1.6 Table release history update

A new field TRNKINFO is added under function CALLOFFR for categories RESEVENT, CTXEVENT and ACDEVENT, under function CALLQUED for category ACDEVENT.

This feature will be released in SN10. An activatable patch will also be available in SN09.

51.6.2.1.7 Supplementary information

N/A

51.6.2.1.8 Translation verification and other tools.

SCAISSRV does not use translation verification tools.

51.7 Service Orders (SO) (CM & SESM)

N/A

51.8 Software optionality control (SOC)

This feature will have a state controlled SOC. With the SOC turned on, the new parameter added to indicate the trunk information will be sent in the two existing messages, dv_call_queued_U and dv_call_offered_U messages,

provided the new parameter is subscribed for these messages and the call is coming in from a trunk. For nodal calls, no trunk information will be provided, the new parameter will not show in the message.

With the SOC turned off, even if the new parameter for the two messages have been subscribed to, the new parameter will not be sent along with the messages.

Table 4 SOC

SOC option name:	ICM Call Recording
SOC option title:	Yes
SOC option control type:	State
New SOC option?	Yes
SOC option order code	ICM00085
Option defined in DRU:	CCM
Affected products:	LEC00023, LET 00023, LLT00023 SN10, ISN10, SE09, SE10

52: Configuration (CN): A00012527

52.1 Feature Name

Provisioning of CS2K trunks on GW and Carrier basis

52.2 Hardware and Software Requirements

Software Requirements:

- SN09 drop 2 Succession Core load or later

52.3 Initial Configuration

N/A

52.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

52.5 Upgrade Considerations

52.5.1 Dump and Restore (CM)

Table GATWYINV and GWEPCARR will use the existing data transfer "TabXfr" mechanism available to all Table Control tables to preserve their data during an upgrade.

52.5.2 Element Management Upgrade

N/A

52.6 Data schema (DS) (CM, MIBS, RDB)

52.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
GATWYINV	CHANGED	UNCHANGED
GWEPCARR	NEW	NEW

52.6.2 Table GATWYINV Database Schema information

52.6.2.1 Name: GATWYINV

Long Table Name: GATeWaY INVentory

52.6.2.1.1 Functional description

Table GATWYINV holds the gateway related information. It currently allows only ABI GWs which are provisioned in parallel in the CM and SESM. The modification shall allow support for PVG and GW gateways.

As the gateway physical location and element manager information is not significant for GW and PVG gateway types, the tuple options ELMGR and GTWYLOC are not allowed for these gateway types.

GATWYINV Table needs to be datafilled prior to datafilling table GWEPCARR.

52.6.2.1.2 Usage sequence and implications (CM Only)

No change to datafill order. The sequence is as follows:

1. Table SERVRINV - GWC datafill

2. Table GATWYINV - GW datafill

52.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
GATWYINV	0	32767	Memory is automatically allocated in increments with block size of 2K.

52.6.2.1.4 Fields/OIDs

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GTWYPRFL	Changed	Refined to support for 2 new profiles	PVGPRF	PVG gateway profile
			GWPRF	Generic Gateway (GW) profile

52.6.2.1.5 Datafill example

Figure 1 Sample GATWYINV Tuples with PVG and GW profiles

```
GTWY   PMNO  GTWYPRFL   GTWYNAME  GTWYADDR  GTWYCSPM   GTWYOPTS
--------- ---------- ---------- ---------- ---------- ---------- ----------

  PVG     5          PVGPRF     pvg5.myco.com  (99 9 9 5) $       HOST GWC 15     $

  GW      1          GWPRF      gw1.myco.com   (99 9 9 6) $       HOST GWC 15     $
```

Figure 2 Prompting sequence and Range values for GATWYINV

```
TABLE GATWYINV
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
GTWYPMNO:
TYPE OF GTWYPMNO IS GTWY_TC_KEY_T
TYPE IS GTWY_TC_KEY_T MULTIPLE WITH
      GTWY_TYPE    {NLGW,ABI,CICM,GW,MG9K,PVG,MS,SESS}
     GTWY_NO      {0 TO 1023}
GTWYPMNO:
>PVG 5
GTWYPRFL:
TYPE OF GTWYPRFL IS GTWY_PROFILE_TYPE
TYPE IS GTWY_PROFILE_TYPE {NILPROFILE,GWPRF,MG9KITP,MG9KABI,
                           CICMPRF,MSUAS,PVGPRF,ST3PPRF,
                           LT3PPRF,SL3PPRF,LL3PPRF,CALIXC7,
                           SSL1PRF}
GTWYPRFL:
PVGPRF
GTWYNAME:
TYPE IS GTWY_NAME_VECTOR VECTOR OF UP TO 32 CHAR'S
>PVG5.myco.com'
GTWYADDR:
192 21 165 70
GTWYCSPM:
 HOST GWC 3
GTWYOPTN:
 >$
TUPLE TO BE ADDED:
PVG 5 PVGPRF   PVG5.myco.com (192 21 165 70) $ HOST GWC 3 $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
  .>y
TUPLE ADDED
```

Deletion of Tuple from table GATWYINV is not allowed, if that tuple is referenced in Table GWEPCARR.

Figure 3 GATWYINV Tuple deletion

TABLE GATWYINV:
>pos GW 1
GW 1 GWPRF gw1.myco.com (99 9 9 6) $ HOST GWC 3 $
>del
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
Error: Table GWEPCARR still references this Gateway.!
Action: Remove all references to this Gateway before deleting.
TUPLE TO BE DELETED:GW 1 GWPRF gw1.myco.com (99 9 9 6) $ HOST GWC 3 $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>n
DMO REJECTEDWARNING: CURRENTLY NOT POSITIONED

52.6.2.1.6 Table release history update

SN09 drop 2 Feature A00012527: Available in the Core with the SN09 drop 2 or later release.
Modified field: GTWYPRFL to support for PVG and GW profiles.

52.6.2.1.7 Supplementary information

N/A

52.6.2.1.8 Translation verification and other tools

Table GATWYINV does not impact translations. Therefore TABAUDIT is the tool used to verify the contents of table GATWYINV.

Figure 4 Sample tabaudit output for Verifying Table GATWYINV datafill

```
>tabaudit
TABAUDIT:
>include gatwyinv
>execute
------------------------------------------------------------------------------
|                                                                            |
|            TABAUDIT STATUS                                                 |
|                                                                            |
------------------------------------------------------------------------------
The following tables are included:       table GATWYINV (95)

The following tables are excluded:
From table VERSIONS (0)                  to table SERVRINV (94).
From table LTCINV (96)                   to table INWATNPA (1449).
Please confirm ("YES", "Y", "NO", or "N"):
>y
Creating TABAUDIT summaryfile: SUMMARY$TTY0 on SFDEV.
Starting DMS data verification ...
Table GATWYINV: New table control.
Completed tuple checking.
SUMMARY: Tbl GATWYINV: tuples checked 0, passed 0, failed 0.
Data verification is completed.
```

52.6.3 Table GWEPCARR Database Schema information

52.6.3.1 Name: GWEPCARR

Long Table Name: GateWay End Point CARRier

52.6.3.1.1 Functional description

New table GWEPCARR shall hold the mapping from GW and carrier number to the TID range used by trunks on the carrier. The key to table GWEPCARR is the GW type and number and the carrier number. The number of channels on a carrier is restricted to 24 for North America and 31 for International. The table will also hold the carrier name information.

Only Add and Delete operations will be supported on table GWEPCARR.

Datafilling table GWEPCARR with a gateway, that does not exist in table GATWYINV, is not allowed.

52.6.3.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

1. Table GATWYINV - Gateway datafill.

2. Table GWEPCARR - New Table, Gateway and carrier datafill.

52.6.3.1.3 Fields/OIDs

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Valid entries	Explanation and action
GWCARR	New	GW_TYPE	{NLGW,ABI,CICM,GW,MG9K,PVG,MS,SESS}	{GW, PVG}	This is the type of the gateway as defined on the Core. The valid values are PVG and GW.
		GW_NUM	{0 - 1023}	{0-1023}	This is the unique external number of the gateway.
		CARRIER_NUM	{0 - 168}	{1-168}	This is the carrier over which the trunk is configured. Valid Values are in the range {1 - 168}
HOST	New	HOST_TYPE	{GWC}	{GWC}	This is a valid pm type of the cside host xpm.
		HOST_NO	{0 - 255}	{0 - 255}	The unique external number of the cside host Gateway Controller.
START	New	GW_CARR_TERM_NUM_TC	{1 - 4094}	{1 - 4094}	This gives the starting terminal number on a particular carrier.
CARRSIZE	New	GTWY_CARRIER_SIZE_TC	{0 - 31}	{24, 31}	This is 24 for North America and 31 for International loads.
CARRNAME	New	CARR_NAME_VECTOR	Up to 32 Char's	Up to 32 Char's	Carrier Name as given in the SESM

52.6.3.1.4 Datafill example

Figure 5 Sample GWEPCARR tuples

```
TABLE GWEPCARR:
GWCARR  HOST  START CARRSIZE  CARRNAME
--------------------------------------------------------------------------
 PVG 1 2  GWC 3   25        24      sts/13/0/3/vt15/1/1/1
 GW  1 1  GWC 3    1        24      sts/13/0/3/vt15/1/1/1
```

Figure 6 Prompting sequence and Range values for GWEPCARR

```
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
GWCARR:
TYPE OF GWCARR IS GWEPCARR_KEY_T

TYPE IS GWEPCARR_KEY_T MULTIPLE WITH
      GW_TYPE       {NLGW,ABI,CICM,GW,MG9K,PVG,MS,SESS}
      GW_NUM        {0 TO 1023}
      CARRIER_NUM    {0 TO 168}GWCARR:
GWCARR:
 >ms 0 0
HOST:
TYPE OF HOST IS GW_CARR_HOST_NODE
TYPE IS GW_CARR_HOST_NODE MULTIPLE WITH
      HOST_TYPE        {GWC}
      HOST_NO          {0 TO 255}
HOST:
 >gwc 0
START:
TYPE OF START IS GW_CARR_TERM_NUM_TC
TYPE IS GW_CARR_TERM_NUM_TC {1 TO 4094}
START:
 >1
CARRSIZE:
TYPE OF CARRSIZE IS GTWY_CARRIER_SIZE_TC
TYPE IS GTWY_CARRIER_SIZE_TC {0 TO 31}
CARRSIZE:
>32
CARRNAME:
 TYPE OF CARRNAME IS CARR_NAME_VECTOR
TYPE IS CARR_NAME_VECTOR VECTOR OF UP TO 32 CHAR'S
CARRNAME:
 >'sts/13/0/3/vt15/1/1/1'
TUPLE TO BE ADDED:
MS 0  0  GWC 0  1 32  sts/13/0/3/vt15/1/1/1(2)

Gateway type must be either PVG or GW

Carrier Number must be in the range 1 to 168

Carrier size must be 24 or 31 channels

 Gateway does not exist in table GATWYINV
PVG 5 1 GWC 3 1 24 sts/13/0/3/vt15/1/1/1
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
 .>y
 TUPLE ADDED
```

52.6.3.1.5 Table release history update

Release SN09 drop 2, feature A00012527: Initial release of this new table GWEPCARR.

52.6.3.1.6 Supplementary information

N/A

52.6.3.1.7 Translation verification and other tools

Table GWEPCARR does not impact translations. TABAUDIT tool is not supported as Update operation is not allowed for GWEPCARR table.

52.7 Software optionality control (SOC)

N/A

52.8 Element Management

Telco should continue to provision SESM as before.

52.9 User interface changes

The most basic improvement to OA&M made possible using carrier information in the CM is in the TTP.The CktLoc command is not currently supported for GWC trunks. This component shall support GWC for CktLoc and shall allow display of carrier information for the trunk member currently being posted.

52.9.1 MAPCI, TTP Level, CktLOc Command changes

Figure 7 Existing TTP Display with Modified CktLoc Command

```
XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
AMDI      .     DLOG E    .      1 SPM     .    SYSB     57C..     .     SDM
  M                              *C*             CR C    *C*             M
TTP
 0 QUIT      POST     1  DELQ            BSYQ         DIG
 2 Post_     TTP  6-0000
 3 SEIZE     CKT TYPE     PM NO.          COM LANG STA S R  DOT TE  RESULT
 4           2W S7 S7 GWC  15    12       TEST   0 INB
 5 BSY                                                    R
 6 RTS
 7 TST
 8
 9 CktInfo
10 CktLoc
11 Hold      CktLoc
12 NEXT      GW         Ckt  Chnl
13 RLS       PVG   57   1      1
14 Ckt_
15 TrnslVf_  GW Name
16 StkSdr_   PVGRTP1023
17 Pads      Endpoint Name
18 Level_      STS/13/0/3/VT15/1/1/1/1
  ADMIN
Time  15:59  >
```

To access the CktLoc from the CI environment, enter:

>MAPCI;MTC;TRKS;TTP;

>Post g <Trunk>

>CktLoc

If the TID to carrier mapping is not present (Gateway and carrier entry not in GWEPCARR Table), then the following error message will be displayed.

Figure 8 Error Message for CktLoc if gw and carrier Info not present in GWEPCARR

```
XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
AMDI      .     DLOG E    .       1 SPM     .    SYSB     57C..     .     SDM
  M                              *C*             CR C    *C*              M
TTP
 0 QUIT      POST     1  DELQ            BSYQ         DIG
 2 Post_     TTP  6-0000
 3 SEIZE     CKT TYPE     PM NO.          COM LANG STA S R  DOT TE  RESULT
 4           2W S7 S7 GWC   7    12       TEST   0 INB
 5 BSY                                                  R
 6 RTS
 7 TST
 8
 9 CktInfo
10 CktLoc
11 Hold      CktLoc
12 NEXT      CARRIER INFO NOT PRESENT IN TABLE GWEPCARR
13 RLS
14 Ckt_
15 TrnslVf_
16 StkSdr_
17 Pads
18 Level_
  ADMIN
Time  15:59  >
```

52.10 OSSGate Interface Changes

N/A

52.11 Security

N/A

52.12 Configuration Walkthrough

The craftsperson has to manually look into the SESM datafill and then provision tables GATWYINV and GWEPCARR in core.

Given below are the SESM data and the corresponding core datafills that needs to be done.

Figure 9 Gateway information in SESM

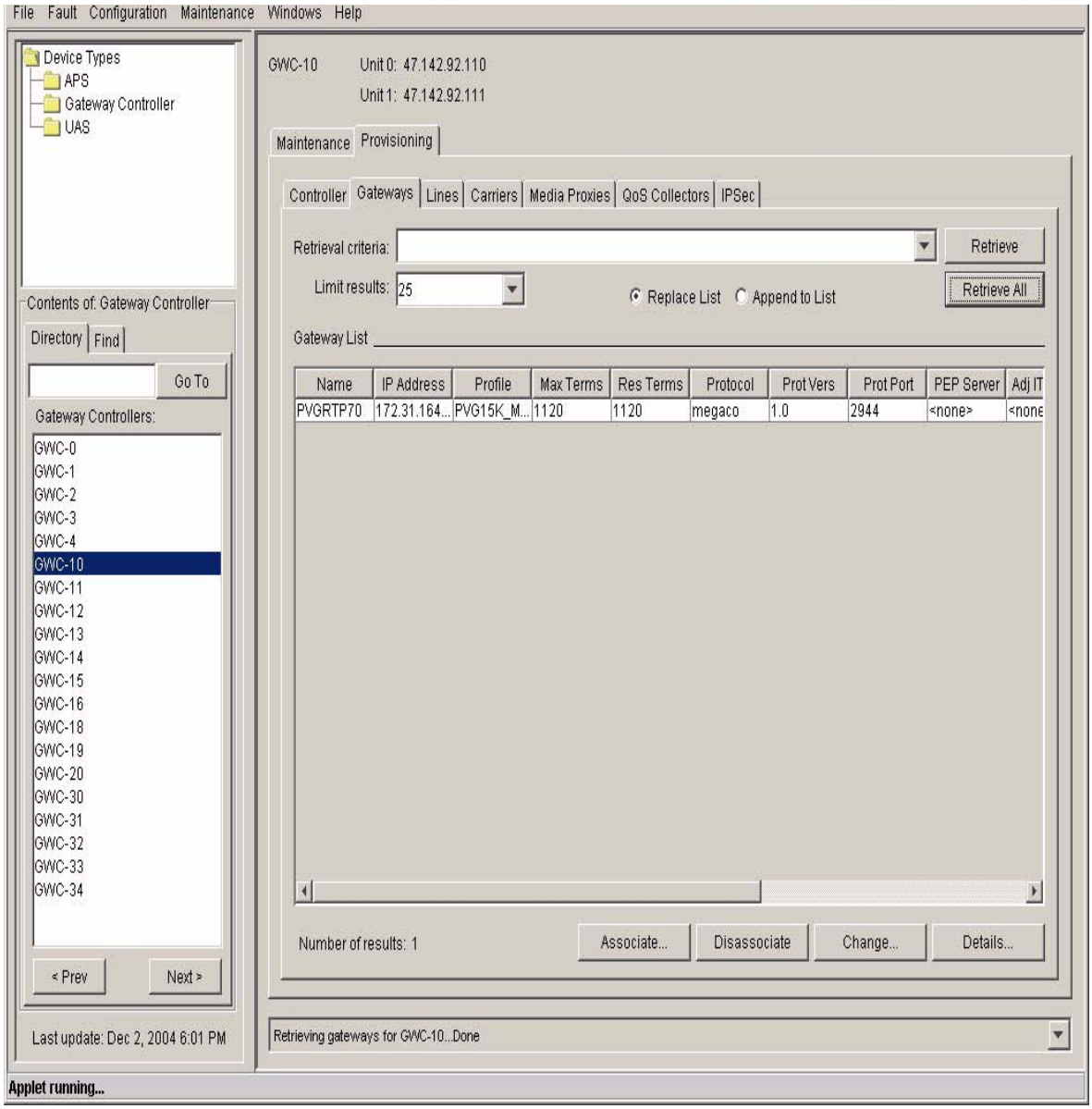


Figure 10 Table GATWYINV - Sample tuple

```
GTWY   PMNO  GTWYPRFL  GTWYNAME  GTWYADDR  GTWYCSPM  GTWYOPTS
-------- ---------- ---------- ---------- ---------- ---------- ----------
  PVG     5         PVGPRF      PVGRTP70    (172 31 164 1) $       HOST GWC 10     $
```

Figure 11 Carrier information in SESM

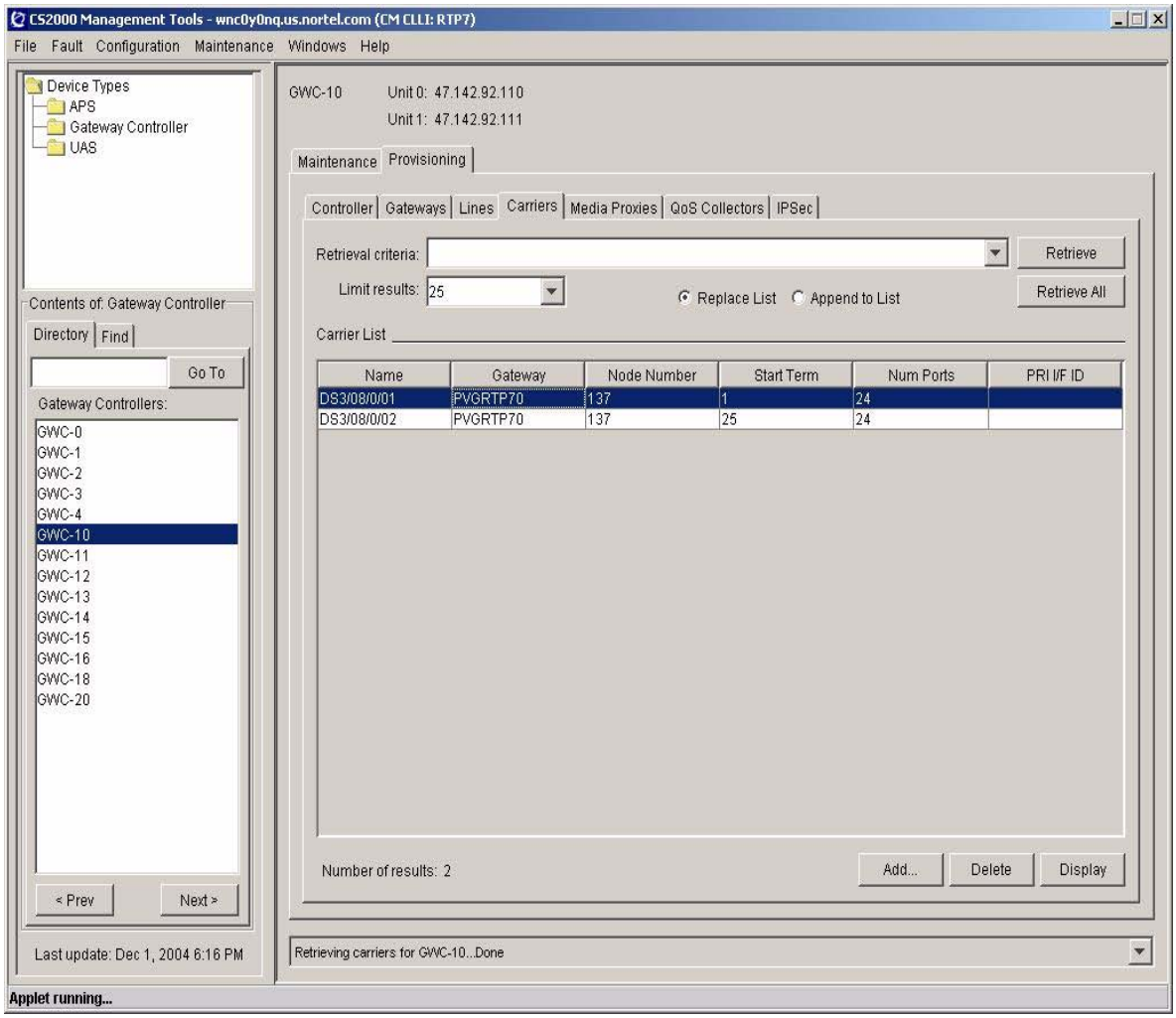


Figure 12 Table GWEPCARR - sample tuples

```
TABLE GWEPCARR:
GWCARR          HOST          START       CARRSIZE    CARRNAME
---------------------------------------------------------------------------------------
PVG 1 1         GWC 10        1             24          DS3/08/0/02
```

53: Configuration (CN): A00012570

53.1 Feature Name

Disabling Non-secure Network Services in SSPFS

53.2 Hardware and Software Requirements

Any SSPFS supported platform running SN09.1+ release.

53.3 Initial Configuration

The initial configuration is done via SSPFS CDs. Upon completion of the SSPFS fresh install, this feature will disable: ftp, tftp, telnet, snmp and nfs.

53.4 Office / Subnet parameters (OP/SP) (CM & SESM)

No new office parameters introduced by this feature.

53.4.1 New/modified office/subnet parameters

Not applicable.

53.4.2 Parameter information

Not applicable.

53.5 Upgrade Impact

Upon system upgrade from one release to the other, the state of non-secure services is preserved. The disabling of such services has to be performed via cli after the upgrade.

53.5.1 Dump and Restore (CM)

Not applicable.

53.5.2 Element Management Upgrade

Not applicable.

53.5.3 Downgrade impact

Since the non-secure service state are not altered on upgrade, there is no impact on downgrade.

53.6 Data schema (DS) (CM, MIBS, RDB)

53.6.1 New/modified tables MIBs or Database Schema

Not applicable.

53.6.2 Table/MIB/Remote Database Schema information

Not applicable.

53.7 Service Orders (SO) (CM & SESM)

Not applicable.

53.8 Software optionality control (SOC)

Not applicable.

53.9 Element Management

Not applicable.

53.9.1 New/modified GUIs

Not applicable.

53.9.2 GUI information

Not applicable.

53.9.3 CLUI Interface

As identified before, new sub-menu items will be introduced into the "**Security Services Configuration**" layer within the configuration panel for SSPFS cli configuration tool.

53.10 User interface changes

53.10.1 Directory: <directory name/MAP level>

For pictorial representation of the menu level, please refer to the diagram in figure 2.

The top level CLUI is invoked via the command cli. The result is listed below:

```
# cli
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select –
```

To get to the configuration level, the operator is requested to enter 2. The resulting menu is prompted to the operator:

```
Configuration
1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Remote Backup Configuration
```

```
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
 X - exit

select –
```

Option 14 above will be extended. Here is the new menu generated when the operator selects option 14:

```
Security Services Configuration
1 - Socks Configuration
 2 - IEMS Server Location Configuration
 3 - PAM Configuration
 4 - Common Inet Services (ftp, tftp, telnet, snmp and nfs)
 5 - Tools Inet Services (time, daytime)
 6 - Other Inet Services
 7 - proftpd User Configuration
 8 - query_registry (Query Network Services Package Registration)
 X - exit

select -
```

Upon selection of any of the new sub-menus 4-6, the operator will get the following commands menu:

```
Common Services Configuration (ftp, tftp, telnet, snmp and nfs)
 1 - query_common_inetd (Services State Query )
 2 – enable_common_inetd (Enable a service registered in inetd.conf)
 3 - disable_common_inetd (Disable a service registered in inetd.conf)

 X - exit

select -
```

Here is an example of the result of a query state for the Common Network Services:

```
Common Services State
0. telnet       Enabled
1.    ftp       Disabled
2.   tftp       Enabled
3.   snmp       Disabled
4.    nfs       Disabled
```

Here is an example of the disable Service command:

```
Enable Common Service
1. tftp /usr/sbin/in.tftpd
2. telnet       /usr/sbin/in.telnetd
```

```
Select service number to disable: 1
The selected services was tftp  /usr/sbin/in.tftpd
Configuration file updated.
Operating system deamon refreshed.
Oparation completed.
```

Upon the selection of proftpd User Configuration, the operator will receive the following options:

```
1 - query_proftpd_users (Query users defined in proftpd)
 2 - add_proftpd_user  (Add a user to proftpd)
 3 - add_dflt_GWC_anonymous_user (Restore the GWC anonymous user )
 4 - del_proftpd_user (Delete a given user from proftpd)
 5 – query_user_registry (Query the packages registered for ftp users)
```

53.10.2 Command: <command command name>

Not applicable.

53.10.2.1 Qualifications and warnings

Not applicable.

53.10.2.2 Responses

Not applicable.

53.10.2.3 Example

Not applicable.

53.11 Security

The security implications of this feature are that on a fresh install of the SSPFS software, the default state of the non-secure services such as ftp, tftp, snmp, telnet and nfs will be preserved. A configuration tool is provide to root user group to be able to manually disable these services to increase the security profile of the target platform.

53.11.1 Network Configuration

Not applicable.

53.11.2 Key Management

Not applicable.

53.11.3 Protocol

Not applicable.

53.11.4 Authentication

Not applicable.

53.12 Configuration Walkthrough

The section walks through minor changes in the platform initial installation, upgrade, patching and power cycle/failover.

On system installation, a minor change is performed to the sspfs post-install script resulting into the disabling non-necessary services such as RPC not used in any sspfs product offering.

On system upgrade, the setting of non-secure services is maintained throughout the upgrade. Once the system is re-clone/back in sync, then the non-secure services can be disabled manually via cli.

For system patching via NPM, the preferred option is to use sftp. Therefore the deactivation of non-secure services should have no impact to the patchability of the platform.

For power-cycle or failover of a node in the cluster, there is a small window of time when the control files are being synchronized and the inetd services is being re-initialized. Since this script functionality is typically done once after upgrade, it is acceptable to re-run the configuration if a power-cycle or failover occurred during the configuration changes.

54: Configuration (CN): A00012889

54.1 Feature Name

Passphrase Protected Keys for SSH

54.2 Hardware and Software Requirements

- OpenSSH installed on SDM/CBM.
- SBA and OMDD applications are installed and InSv.

54.3 Initial Configuration

- Configure and activate a SBA stream.
- No initial configuration of OMDD is required.

54.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

54.5 Upgrade Impact

N/A

54.6 Data schema (DS) (CM, MIBS, RDB)

N/A

54.7 Service Orders (SO) (CM & SESM)

N/A

54.8 Element Management

N/A

54.9 Command interface changes

N/A

54.10 Security

54.10.1 Secure Data Transfer to OSS with Public Key Authentication

This feature enhances the existing secure outbound file transfer functionality by introducing the key-based (public key) authentication.

The key-based authentication mechanism is provided as an additional option for the user. Hence, the user can select to use either the password-based or the key-based authentication while adding and changing the secure file transfer schedules in the SBA (billmtc) or OMDD (omui) user interface programs.

54.10.2 Passphrase protection.

The passphrase is stored in the Private Data Manager in an encrypted format.

54.11 Configuration Walkthrough

54.11.1 Host key acceptance for downstream OSS

The initial host key acceptance of the downstream processor should be done manually before it can use the SSH protocol to transfer file from SDM/CBM. Figure 1 shows an example how to accept a host key manually.

Figure 1 Host key acceptance

54.11.2 SBA specific configuration

SBA secure outbound file transfer can be configured by adding or changing an existing schedule tuple after the user has done a host key acceptance.The “sendfile” command can be used to validate if OSS is ready for key-based authentication. Text in bold indicates changes in SBA UI.

Figure 2 shows an example on how a user can configure secure outbound file transfer using password-based authentication.

Figure 3 shows an example on how a user can configure secure outbound file transfer using key-based authentication.

Figure 4 shows an example of how to append the public key to .ssh/ authorized_keys file of the user on the remote system running with OpenSSH server.

Figure 5 and Figure 6 shows an example of how a user can modify the existing schedule tuple configuration.

Figure 7 and Figure 8 shows an example of how a user can delete the schedule tuple.

Figure 2 Prompts for schedule add (*Password based authentication*).

```
Valid streams are {'OCC'}.
Press Enter to accept 'OCC'.
Enter Stream:

Valid file format types are {'DIRP'}.
Press Enter to accept 'DIRP'.
Enter File_Format_Type:

Destination can have between 1 and 15 alphanumeric characters.
Enter Destination: OSS

Valid protocols are {'FTPW', 'RFTPW' 'SFTPW', 'KSFTPW'}.
Press Enter to accept 'FTPW'.
Enter Protocol: SFTPW

WARNING: File Transfer to this destination will fail if OpenSSH is not installed
Please install OpenSSH if it is not already installed.

Primary destination must follow IP address format (i.e. N.N.N.N
where N indicates a number between 0 and 255).
Enter Primary_Destination: 47.135.213.53

Primary port can be 22 or between 1025 and 65535.
Press Enter to accept '22'.
Enter Primary_Port:

Alternate destination must follow IP address format (i.e. N.N.N.N
where N indicates a number between 0 and 255).
Enter Alternate_Destination: 47.135.213.53

Alternate port can be 22 or between 1025 and 65535.
Press Enter to accept '22'.
Enter Alternate_Port:

... (con't on next figure)
```

```
Start time is in time of day format (hh:mm) where hh is hours between 0
and 23 and mm is minutes between 0 and 59.
Enter Start_Time: 00:00

Stop time is in time of day format (hh:mm) where hh is hours between 0
and 23 and mm is minutes between 0 and 59.
Enter Stop_Time: 23:00

Interval can be between 5 and 1440 minutes.
Press Enter to accept '120'.
Enter Interval:

Remote storage directory can have between 1 and 255 characters.
Enter Remote_Storage_Directory: /billing

Remote login can have between 1 and 20 characters.
Enter Remote_Login: test

Remote password can have between 1 and 20 characters.
Enter Remote_Password: ******
Re-enter Remote_Password: ******

Maximum retries can be between 0 and 10.
Press Enter to accept '3'.
Enter Maximum_Retries:

Retry wait time can be between 1 and 60 seconds.
Press Enter to accept '1'.
Enter Retry_Wait_Time:

File extension can have between 0 and 3 characters.
Enter 'Blank' for no file extension.
Press Enter to accept 'Blank'.
Enter File_Extension:

... (con't on next figure)
```

```
Field separator can have 1 character.
Press Enter to accept '.'.
Enter Field_Separator:

WARNING: Billing files associated with this tuple will not
transfer downstream when Active is set to No.

Valid active values are {'No', 'n', 'Yes', 'y'}.
Press Enter to accept 'No'.
Enter Active: y



Stream                  : 'OCC'
File_Format_Type        : 'DIRP'
Destination             : 'OSS'
Protocol                : 'SFTPW'
Primary_Destination     : '47.135.213.53'
Primary_Port            : '22'
Alternate_Destination   : '47.135.213.53'
Alternate_Port          : '22'
Start_Time              : '00:00'
Stop_Time               : '23:00'
Interval                : '120'
Remote_Storage_Directory: '/billing'
Remote_Login            : 'test'
Remote_Password         : '******'
Maximum_Retries         : '3'
Retry_Wait_Time         : '1'
File_Extension          : ''
Field_Separator         : '.'
Active                  : 'Yes'

Valid actions are {'Save', 'Edit', 'Abort'}.
Press Enter to accept 'Edit'.
Enter Action: save

Schedule tuple added.
```

Figure 3 Prompts for schedule add (Key based).

Valid streams are {'OCC'}.
Press Enter to accept 'OCC'.
Enter Stream:

Valid file format types are {'DIRP'}.
Press Enter to accept 'DIRP'.
Enter File_Format_Type:

Destination can have between 1 and 15 alphanumeric characters.
Enter Destination: OSS

Valid protocols are {'FTPW', 'RFTPW' 'SFTPW', **'KSFPW'**}.
Press Enter to accept 'FTPW'.
Enter Protocol: **KSFTPW**

WARNING: File Transfer to this destination will fail if OpenSSH is not installed
Please install OpenSSH if it is not already installed.

Primary destination must follow IP address format (i.e. N.N.N.N
where N indicates a number between 0 and 255).
Enter Primary_Destination: 47.135.213.53

Primary port can be 22 or between 1025 and 65535.
Press Enter to accept '22'.
Enter Primary_Port:

... (con't on next figure)

```
Alternate destination must follow IP address format (i.e. N.N.N.N
where N indicates a number between 0 and 255).
Enter Alternate_Destination: 47.135.213.53

Alternate port can be 22 or between 1025 and 65535.
Press Enter to accept '22'.

Start time is in time of day format (hh:mm) where hh is hours between 0
and 23 and mm is minutes between 0 and 59.
Enter Start_Time: 00:00

Stop time is in time of day format (hh:mm) where hh is hours between 0
and 23 and mm is minutes between 0 and 59.
Enter Stop_Time: 23:00

Interval can be between 5 and 1440 minutes.
Press Enter to accept '120'.
Enter Interval:

Remote storage directory can have between 1 and 255 characters.
Enter Remote_Storage_Directory: /billing

Remote login can have between 1 and 20 characters.
Enter Remote_Login: test

Maximum retries can be between 0 and 10.
Press Enter to accept '3'.
Enter Maximum_Retries:

Retry wait time can be between 1 and 60 seconds.
Press Enter to accept '1'.
Enter Retry_Wait_Time:

File extension can have between 0 and 3 characters.
Enter 'Blank' for no file extension.
Press Enter to accept 'Blank'.
Enter File_Extension:
```

WARNING: Billing files associated with this tuple will not
transfer downstream when Active is set to No.

Valid active values are {'No', 'n', 'Yes', 'y'}.
Press Enter to accept 'No'.
Enter Active: Y

Stream : 'OCC'
File_Format_Type : 'DIRP'
Destination : 'OSS'
Protocol : '**KSFTPW**'
Primary_Destination : '47.135.213.53'
Primary_Port : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port : '22'
Start_Time : '00:00'
Stop_Time : '23:00'
Interval : '120'
Remote_Storage_Directory: '/billing'
Remote_Login : 'test'
Maximum_Retries : '3'
Retry_Wait_Time : '1'
File_Extension : ''
Field_Separator : '.'
Active : 'Yes'

Valid actions are {'Save', 'Edit', 'Abort'}.
Press Enter to accept 'Edit'.
Enter Action: save

Schedule tuple added.

The public key on the CBM is stored at :
/cbmdata/users/maint/.ssh/sba:occ:dirp:oss_rsa.pub

Please append this public key to the user's authorization file on the destination machine.

Press Return to Continue...

Figure 4 Appending public key to authorized_keys file of the user on the downstream machine

On SDM/CBM

```
> login: root
> root's Password: xxxx
> cd ~maint/.ssh
> ssh root@47.135.214.66 'cat >> .ssh/authorized_keys' < id_rsa.pub
> Password:
>
```

Figure 5 Prompts for schedule change (From password to key-based).

```
Valid streams are {'AMA', 'OCC'}.
Press Enter to accept 'AMA'.
Enter Stream: OCC

Valid file format types are {'DIRP'}.
Press Enter to accept 'DIRP'.
Enter File_Format_Type:

Valid destinations are {'OSS', }.
Press Enter to accept 'OSS'.
Enter Destination:


Stream                : 'OCC'
File_Format_Type      : 'DIRP'
Destination           : 'OSS'
Protocol              : 'SFTPW'
Primary_Destination   : '47.135.213.53'
Primary_Port          : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port        : '22'
Start_Time            : '00:00'
Stop_Time             : '23:00'
Interval              : '120'
Remote_Storage_Directory: '/billing'
Remote_Login          : 'test'
Remote_Password       : '******'
Maximum_Retries       : '3'
Retry_Wait_Time       : '1'
File_Extension        : ''
Field_Separator       : '.'
Active                : 'Yes'

Enter the field name to be changed.  Stream, File_Format_Type
 and Destination cannot be changed.
Enter 'All' to be prompted for all field names.
Press Enter to accept 'All'.
Enter Field_Name: Protocol

Valid protocols are {'FTPW', 'RFTPW', 'SFTPW', 'KSFTPW'}.
Press Enter to accept 'SFTPW'.
Enter Protocol: KSFTPW
```

WARNING: File Transfer to this destination will fail if OpenSSH is not installed
Please install OpenSSH if it is not already installed.

Primary port can be 22 or between 1025 and 65535.
Press Enter to accept '22'.
Enter Primary_Port:

Alternate port can be 22 or between 1025 and 65535.
Press Enter to accept '22'.
Enter Alternate_Port:

Stream : 'OCC'
File_Format_Type : 'DIRP'
Destination : 'OSS'
Protocol : 'KSFTPW'
Primary_Destination : '47.135.213.53'
Primary_Port : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port : '22'
Start_Time : '00:00'
Stop_Time : '23:00'
Interval : '120'
Remote_Storage_Directory: '/billing'
Remote_Login : 'test'
Maximum_Retries : '3'
Retry_Wait_Time : '1'
File_Extension : ''
Field_Separator : '.'
Active : 'Yes'

Valid actions are {'Save', 'Edit', 'Abort'}.
Press Enter to accept 'Edit'.
Enter Action: Save

Schedule tuple changed.

The public key on the CBM is stored at :
/cbmdata/users/maint/.ssh/sba:occ:dirp:oss_rsa.pub

Please append this public key to the user's authorization file on the destination machine.

Press Return to Continue...

Figure 6 Prompts for schedule change (From Key-based to Password).

```
Valid streams are {'AMA', 'OCC'}.
Press Enter to accept 'AMA'.
Enter Stream: OCC

Valid file format types are {'DIRP'}.
Press Enter to accept 'DIRP'.
Enter File_Format_Type:

Valid destinations are {'OSS', }.
Press Enter to accept 'OSS'.
Enter Destination:


Stream                : 'OCC'
File_Format_Type      : 'DIRP'
Destination           : 'OSS'
Protocol              : 'KSFTPW'
Primary_Destination   : '47.135.213.53'
Primary_Port          : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port        : '22'
Start_Time            : '00:00'
Stop_Time             : '23:00'
Interval              : '120'
Remote_Storage_Directory: '/billing'
Remote_Login          : 'test'
Maximum_Retries       : '3'
Retry_Wait_Time       : '1'
File_Extension        : ''
Field_Separator       : '.'
Active                : 'Yes'

Enter the field name to be changed.  Stream, File_Format_Type
 and Destination cannot be changed.
Enter 'All' to be prompted for all field names.
Press Enter to accept 'All'.
Enter Field_Name: Protocol

Valid protocols are {'FTPW', 'RFTPW', 'SFTPW', 'KSFTPW'}.
Press Enter to accept 'KFTPW'.
Enter Protocol: SFTPW
```

```
WARNING: File Transfer to this destination will fail if OpenSSH is not installed
Please install OpenSSH if it is not already installed.

Primary port can be 22 or between 1025 and 65535.
Press Enter to accept '22'.
Enter Primary_Port:

Alternate port can be 22 or between 1025 and 65535.
Press Enter to accept '22'.
Enter Alternate_Port:

Remote password can have between 1 and 20 characters.
Enter Remote_Password: ******
Re-enter Remote_Password: ******

Stream                : 'OCC'
File_Format_Type      : 'DIRP'
Destination           : 'OSS'
Protocol              : 'SFTPW'
Primary_Destination   : '47.135.213.53'
Primary_Port          : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port        : '22'
Start_Time            : '00:00'
Stop_Time             : '23:00'
Interval              : '120'
Remote_Storage_Directory: '/billing'
Remote_Login          : 'test'
Remote_Password       : '******'
Maximum_Retries       : '3'
Retry_Wait_Time       : '1'
File_Extension        : ''
Field_Separator       : '.'
Active                : 'Yes'

Valid actions are {'Save', 'Edit', 'Abort'}.
Press Enter to accept 'Edit'.
Enter Action: Save

Schedule tuple changed.

Press Return to Continue...
```

Figure 7 Prompts for schedule delete (password-based).

```
Stream                : 'OCC'
File_Format_Type      : 'DIRP'
Destination           : 'OSS'
Protocol              : 'SFTPW'
Primary_Destination   : '47.135.213.53'
Primary_Port          : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port        : '22'
Start_Time            : '00:00'
Stop_Time             : '23:00'
Interval              : '120'
Remote_Storage_Directory: '/billing'
Remote_Login          : 'test'
Remote_Password       : '******'
Maximum_Retries       : '3'
Retry_Wait_Time       : '1'
File_Extension        : ''
Field_Separator       : '.'
Active                : 'Yes'

Valid responses are {'Yes', 'No', 'Abort'}.
Press Enter to accept 'No'.
Delete this tuple? yes

1 schedule tuple(s) deleted.

Press Return to Continue...
```

Figure 8 Prompts for schedule delete (key-based)

```
Stream                : 'OCC'
File_Format_Type      : 'DIRP'
Destination           : 'OSS'
Protocol              : 'KSFTPW'
Primary_Destination   : '47.135.213.53'
Primary_Port          : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port        : '22'
Start_Time            : '00:00'
Stop_Time             : '23:00'
Interval              : '120'
Remote_Storage_Directory: '/billing'
Remote_Login          : 'test'
Maximum_Retries       : '3'
Retry_Wait_Time       : '1'
File_Extension        : ''
Field_Separator       : '.'
Active                : 'Yes'

Valid responses are {'Yes', 'No', 'Abort'}.
Press Enter to accept 'No'.
Delete this tuple? yes

1 schedule tuple(s) deleted.


Press Return to Continue...
```

54.11.3 OMDD specific configuration

This activity modifies the Add, List and Modify File Transfer Destination menus of OMUI. The “Add File Transfer Destination” menu in OMUI enables the user to configure a destination where OMDD can transfer OM reports. The “Modify File Transfer Destination” menu enables the user to modify an already configured file transfer destination.

When the file transfer destination is added or modified, user will be asked to select the type of user authentication, in addition to the already existing parameters. The choices for the type of user authentication will be “Password” and “Key”.

If the user chooses “Key”, a message will be displayed informing the user to dump the contents of the public key file into the authorization file of the destination machine.

Figure 9 shows an example configuration of file transfer destination using Password-based authentication.

Figure 10 shows an example configuration of file transfer destination using Key-based authentication.

The same changes are made in the “Modify File Transfer Destination” menu also.

Figure 11 shows the list of names of the file transfer destinations that are currently configured.

The text in bold indicate the changes to the OMDD UI.

Figure 9 OMUI File Transfer Destination menu (password-based)

```
    Add File Transfer Destination

File Transfer Destination name > ftd1
Destination IP Address > 47.135.214.61
Type of File Transfer: Standard/Secure > Secure
Type of Autentication: Password/Key > Password
Destination Port [22] >
Destination Login > user1
Destination Password >
WARNING: File Transfer to this destination will fail if OpenSSH is not installed.
Please install OpenSSH if it is not already installed.
 Add File Transfer Destination(Y/N)? Y

Please wait....

ftd1: the request was successful.

Press Enter for File Transfer Destination menu.
```

Figure 10 OMUI File Transfer Destination menu (key-based)

Add File Transfer Destination

File Transfer Destination name > ftd1
Destination IP Address > 47.135.214.61
Type of File Transfer: Standard/Secure > Secure
Type of Autentication: Password/Key > Key
Destination Port [22] >
Destination Login > user1
WARNING: File Transfer to this destination will fail if OpenSSH is not installed.
Please install OpenSSH if it is not already installed.
Add File Transfer Destination(Y/N)? Y

Please wait....

ftd1: the request was successful.

The public key on the CBM is stored at :
/cbmdata/users/maint/.ssh/OMDD:ftd1_rsa.pub

Please append this public key to the user's authorization file on the destination machine.

Press Enter for File Transfer Destination menu.

Figure 11 List File Transfer Destination

List of File Transfer Destinations

FTD name	IP Address	Transfer type	Port	Login name
ftd1	47.135.214.6	**Secure-Password**	22	User1
ftd2	47.135.214.6	**Secure-Key**	22	User2

1. List File Transfer Destination Usage.
2. Return to File Transfer Destination menu.

Select Option >

Performance Management List (PFs)

Introduction

This chapter describes impacts to performance management, such as operational measurements and performance measurements, for the features planned for this release. Only those features with performance-management impacts are listed.

Featid	Title
A00007544.AB06	NCAS Link and SIP NMS Support based on RFC 3842
A00007547.AB12	SIP Lines Core Call Processing Support
A00009515.AA14	Out-of-Band Interop with MCS
A00009777	IEMS Mediant 2000 Integration
A00009893.AA12	Session Server Call Processing Overload
A00012109.AA17	Session Server Shared Library Replacement (SLR) Patching

1: Performance (PF): A00007544

1.1 Feature Name

NCAS Link and SIP NMS Support based on RFC 3842

1.2 Performance management strategy

The Operational Measurements will be pegged to generate the performance history. The details of performance management will be than developed as per engineering rules.

1.3 Performance management tools and utilities

The OMSHOW command and EADAS will be used for the OM display and OM transfer to remote system.

1.4 Performance Measurements (PM), Operational Measurements (OM), and stats

This feature does not have any specific PM. However, this feature introduces new OM groups in the DMS/CS2K Core and in the Session Server (NGSS).

1.4.1 PM, OM, and stats format

The OM in the NGSS and CORE follow the previously defined OM strategy and framework. The new group and appropriate fields are added. An existing OM group INSCTP is also pegged whenever necessary. The following are the details of the new OM groups and fields in the NGSS and DMS/CS2K Core.

1.4.1.1 OM Group NMSNCAS (NGSS)

The New OM group called NCAS_LINK is introduced to keep a record of the state changes of the NCAS Link and the number of messages sent and received over the NCAS link

This OM group accurately tracks the messages send and received on the NCAS link between CS2K Core and Session Server. The OM pegging will provide

information on the message traffic between CS2K Core and Session Server.It will also have a count of the number of times the NCAS Link has gone down and come up

1.4.1.2 Release history update

Added new in this release.

1.4.1.3 Registers

The following table gives an overview of the registers associated with the NCAS_LINK OM group.

Table 1 OM Registers in the NMSNCAS OM Group

OM field	Description
NUM_LINK_UP	Number of times the NCAS Link is brought up
NUM_LINK_DOWN	Number of times the link goes down
NUM_MSG_SENT	Number of messages sent over the NCAS Link
NUM_MSG_RCVD	Number of times a response is received over the NCAS Link
NUM_MSG_SEND_FAIL	Number of times the message send fails
NUM_MSG_RCV_FAIL	Number of times the message receive fails.

The following figure will be updated during coding.

OM group registers displayed are as follows:

Figure 1 OM Group Display

<regName> <regName> <regName> <regName>

1.4.1.4 Group Structure

OM group provides one tuple for each NCAS selector datafilled in Table MSGRTE.
Key field: <KField><description> TBA

Info field: <IField><description> TBA

1.4.1.5 Associated OM groups

None

1.4.1.6 Associated functional groups

The following functional groups are associated with OM group: None

1.4.1.7 Associated functionality codes

Not Applicable

1.4.1.8 OM group registers logic flow chart

TBA

1.4.2 Register NUM_LINK_UP

1.4.2.1 Register description

This register represents how many times the NCAS Link has been brought up.

1.4.2.2 Register release history update

New in this release

1.4.2.3 Associated registers

1.4.2.4 Associated logs

TBA

1.4.3 Register NUM_LINK_DOWN

1.4.3.1 Register description

This register represents how many times the NCAS Link has gone down.

1.4.3.2 Register release history update

New in this release

1.4.3.3 Associated registers

1.4.3.4 Associated Logs

1.4.4 Register NUM_MSG_SENT

1.4.4.1 Register description

This register represents how many times the a message is successfully sent over the NCAS Link.

1.4.4.2 Register release history update
New in this release

1.4.4.3 Associated registers
None

1.4.4.4 Associated logs
None

1.4.5 Register NUM_MSG_RCVD

1.4.5.1 Register description
This register represents how many times responses are successfully received over the NCAS Link .

1.4.5.2 Register release history update
New in this release

1.4.5.3 Associated registers
None.

1.4.5.4 Associated logs
None.

1.4.6 Register NUM_MSG_SEND_FAIL

1.4.6.1 Register description
This register represents how many times the message sent over the NCAS Link has failed

1.4.6.2 Register release history update
New in this release

1.4.6.3 Associated registers
None.

1.4.6.4 Associated logs
None

1.4.7 Register NUM_MSG_RCV_FAIL

1.4.7.1 Register description
This register represents how many times the a message receive over an NCAS Link has failed.

1.4.7.2 Register release history update
New in this release

1.4.7.3 Associated registers

None.

1.4.7.4 Associated logs

None

1.4.8 Performance File (CSV, SSV, XML) Format

The NGSS performance file format is used.

1.4.9 OM Group NMSNCAS (For CS2K Core only)

1.4.9.1 OM description

The New OM group called NMSNCAS is introduced to keep a record of the NMS messages sent and received by the CS2K Core over NCAS link.This OM group accurately tracks the messages sent and received on the NCAS link between CS2K Core and Session Server. The OM pegging will provide information on the message traffic between CS2K Core and Session Server.

1.4.9.2 Release history update

Added new in this release.

1.4.9.3 Registers

The following table gives an overview of the registers associated with the NMSNCAS OM group.

Table 2 OM Registers in the NMSNCAS OM Group

OM field	Description
SCTPNMSS	NMS TCAP messages sent successfully over SCTP
SCTPNMSR	NMS TCAP messages received successfully over SCTP
SCTPREJS	NMS REJ messages sent successfully over SCTP
SCTPREJR	NMS REJ messages receievd successfully over SCTP

The following figure will be updated during coding.

OM group registers display on the MAP terminal as follows:

Figure 2 OM Group Display

1.4.9.4 Group structure

OM group provides one tuple for each NCAS selector datafilled in Table MSGRTE.

Key field: <KField><description> TBA

Info field: <IField><description> TBA

1.4.9.5 Associated OM groups

None.

1.4.9.6 Associated functional groups

None

1.4.9.7 Associated functionality codes

Not Applicable

1.4.9.8 OM group registers logic flow chart

1.4.10 Register SCTPNMSS (applies only to DMS)

1.4.10.1 Register description

This register represents how many NMS TCAP messages are sent to SCTP in half hour time period. This will provide information of performance needs for the NCAS link.

1.4.10.2 Register release history update

New in this release

1.4.10.3 Associated registers

None.

1.4.10.4 Associated logs

NMSS115.

1.4.11 Register SCTPNMSR (applies only to DMS)

1.4.11.1 Register description

This register represents how many NMS TCAP messages are received from SCTP in half hour time period.This will provide information of performance needs for the NCAS link.

1.4.11.2 Register release history update

New in this release

1.4.11.3 Associated registers

None.

1.4.11.4 Associated logs

NMSS116

1.4.12 Register SCTPREJS (applies only to DMS)

1.4.12.1 Register description

This register represents how many NMS REJECT messages are sent to SCTP in half hour time period.

1.4.12.2 Register release history update

New in this release.

1.4.12.3 Associated registers

None

1.4.12.4 Associated logs

NMSS117

1.4.13 Register SCTPREJR (applies only to DMS)

1.4.13.1 Register description

This register represents how many NMS REJECT messages are received from SCTP in half hour time period.

1.4.13.2 Register release history update

New in this release.

1.4.13.3 Associated registers

None

1.4.13.4 Associated logs

NMS118

1.4.14 OM Group INSCTP (For CS2K Core only)

This is an existing OM Group defined for AIN Transports. The OMs pegged for this OM Group are as follows:

- **MSGOUT:** Pegs Outgoing IN messages using SCTP
- **MSGIN:** Pegs Incoming IN messages using SCTP
- **SDFAIL:** Pegs IN messages using SCTP for which send failed
- **DATAERR:** Pegs IN messaageswhich encounted errors at application data
- **MSG2BIG:** Pegs IN messages which failed due to message length
- **BMSOPFAIL:** Peg instances when buffer errors are encountered while sending IN messages over SCTP
- **DATARCVD:** Pegs for incoming IN message decoding
- **NOTREADY:** Pegs when SCTP layer indicates that it is not ready to process the message.

Please refer to A00004500 for further information.

2: Performance (PF): A00007547

2.1 Feature Name

SIP Lines Core Call Processing Support

2.2 Performance management strategy

2.3 Performance management tools and utilities

2.4 Performance Measurements (PM), Operational Measurements (OM), and stats

New OM group DPLOM.

Registers:

- DPLFNVA
- DPLFBAL
- DPLFREB
- DPLRLOS
- DPLRCAL
- DPLUSE
- DPLFRE
- DPLNOA
- DPLNOD

2.4.1 PM, OM, and stats format

2.4.2 Performance File (CSV, SSV, XML) Format

2.4.3 OM Group template (applies only to DMS)

2.4.3.1 OM description

OM Group DPLOM - Dynamic Packet Line OM

2.4.3.2 Release history update

Creation of new group DPLOM

2.4.3.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 1 OM Group Display

DPLFNVA	DPLFBAL	DPLFREB	DPLRLOS
DPLCAL	DPLUSE	DPLUSE2	DPLFRE
DPLFRE2	DPLNOA	DPLNOA2	DPLNOD
DPLNOD2			

2.4.3.4 Group structure

OM group provides 1 tuple for the CS2K.

Key field: None

Info field: None

2.4.3.5 Associated OM groups

<None>

2.4.3.6 Associated functional groups

The following functional groups are associated with OM group: <None>

2.4.3.7 Associated functionality codes

Not applicable

2.4.3.8 OM group registers logic flow chart

2.4.4 Register DPLFNVA

2.4.4.1 Register description

Register DPLFNVA

Dynamic Packet Line Failed Allocation due to No VIDs Available.

DPLFNVA is a peg register. It records the number of times that a call failed to allocate a VID from the DPL VID resource because the free list was empty

2.4.4.2 Register release history update

Initial creation

2.4.4.3 Associated registers

<None>

2.4.4.4 Associated logs

<None>

2.4.5 Register DPLFBAL

2.4.5.1 Register description

Register DPLFBAL

Dynamic Packet Line Failed Allocation due to Queue Balancing

DPLFBAL is a peg register. It records the number of times that a call failed to allocate a VID from the DPL VID resource because the free list was being balanced

2.4.5.2 Register release history update

Initial creation

2.4.5.3 Associated registers

<None>

2.4.5.4 Associated logs

<None>

2.4.6 Register DPLFREB

2.4.6.1 Register description

Register DPLFREB

Dynamic Packet Line Failed Dealocation due to Queue Rebuilding.

DPLFREB is a peg register. It records the number of times that a call failed to return a VID to the DPL VID resource because the free list was being rebuilt.

2.4.6.2 Register release history update

Initial creation

2.4.6.3 Associated registers

<None>

2.4.6.4 Associated logs

<None>

2.4.7 Register DPLRLOS

2.4.7.1 Register description

Register DPLRLOS

Dynamic Packet Line Recover Lost

DPLRLOS is a peg register. It records the number of VIDs that were recovered and put back on the resource pool free list when a call failed to return a VID to the DPL VID resource pool free list because the free list was being rebuilt.

2.4.7.2 Register release history update
Initial creation

2.4.7.3 Associated registers
<None>

2.4.7.4 Associated logs
<None>

2.4.8 Register DPLRCAL

2.4.8.1 Register description
Register DPLRCAL

Dynamic Packet Line Recover Call VID.

DPLRCAL is a peg register. It records the number of VIDs that were recovered and put back on the resource pool free list when a call failed to return a VID to the DPL VID resource pool free list because the call terminated abnormally.

2.4.8.2 Register release history update
Initial creation

2.4.8.3 Associated registers
<None>

2.4.8.4 Associated logs
<None>

2.4.9 Register DPLUSE

2.4.9.1 Register description
Register DPLUSE

Dynamic Packet Line Usage.

DPLUSE is a usage register. The scan rate is slow: 100s. It records the number of VIDs allocated from the DPL VID resource pool.

2.4.9.2 Register release history update
Initial creation

2.4.9.3 Associated registers
<None>

2.4.9.4 Associated logs
<None>

2.4.10 Register DPLFRE

2.4.10.1 Register description
Register DPLFRE

Dynamic Packet Line Free.

DPLFRE is a usage register.The scan rate is slow: 100s. It records the size of the DPL VID resource pool free list.

2.4.10.2 Register release history update
Initial creation

2.4.10.3 Associated registers
<None>

2.4.10.4 Associated logs
<None>

2.4.11 Register DPLNOA

2.4.11.1 Register description
Register DPLNOA

Dynamic Packet Line Number Of Allocations.

DPLNOA is a peg register. It records the number of times that a call successful allocations from the DPL VID resource pool

2.4.11.2 Register release history update
Initial creation

2.4.11.3 Associated registers
<None>

2.4.11.4 Associated logs
<None>

2.4.12 Register DPLNOD

2.4.12.1 Register description

Register DPLNOD

Dynamic Packet Line Number Of Deallocations.

DPLNOD is a peg register. It records the number of times that a call successfully returned a VID to the DPL VID resource pool

2.4.12.2 Register release history update

Initial creation

2.4.12.3 Associated registers

<None>

2.4.12.4 Associated logs

<None>

3: Performance (PF): A00009515

3.1 Feature Name

Out-of-Band Interop with MCS

3.2 Performance management strategy

The Operational Measurements will be pegged to generate the performance history. The details of performance management will be then developed as per engineering rules.

3.3 Performance management tools and utilities

The OMSHOW command and EADAS will be used for the OM display and OM transfer to remote system.

3.4 Performance Measurements (PM), Operational Measurements (OM), and stats

This feature does not have any specific PM. However, this feature introduces new OM groups in the Session Server (NGSS).

Following two new groups are added under this activity:

- SIPGW_OOB OM Group
- SIPGW_NCAS OM Group

3.4.1 PM, OM, and stats format

The OM in the Session Server follows the previously defined OM strategy and framework. Two new groups and appropriate fields are added. See section 14.3.3. for details on the OM groups and their registers.

3.4.2 Performance File (CSV, SSV, XML) Format

The Session Server performance file format is used.

3.5 SIPGW_OOB OM Group

3.5.1 SIPGW_OOB OM description

The New OM group called SIPGW_OOB is introduced to keep a record of the Out-of-Band related SIP messages sent and received between the Session Server and the MCS.

3.5.2 Release history update

Added new in this Release

3.5.3 Registers

The following table gives an overview of the registers associated with the SIPGW_OOB OM group.

Table 1 OM Registers in the SIPGW_OOB OM Group

OM field	Description
REFER_RECEIVED	OBB REFER REceived
REFER_ACCEPTED	OOB REFER Accepted - 202 Accepted sent
REFER_REJECTED	OOB REFER Rejected
NOTIFY_200OK	NOTIFY Sent following receipt of CLOSE msg
NOTIFY_PROCEEDING	Proceeding NOTIFY sent
NOTIFY_TERMINATE	Final NOTIFY sent
NOTIFY_REPORT_FAIL	NOTIFY sent indicating failure.

OM group registers display on the MAP terminal as follows:

Figure 1 OM Group Display

<regName> <regName> <regName> <regName>

3.5.4 Group structure

3.5.5 Associated OM groups

SIPGW_NCAS OM Group - See section 14.5 for detailed description

3.5.6 Associated functional groups

None

3.5.7 Associated functionality codes

None

3.5.8 OM group registers logic flow chart

Figure 2 Successful OOB REFER Scenario

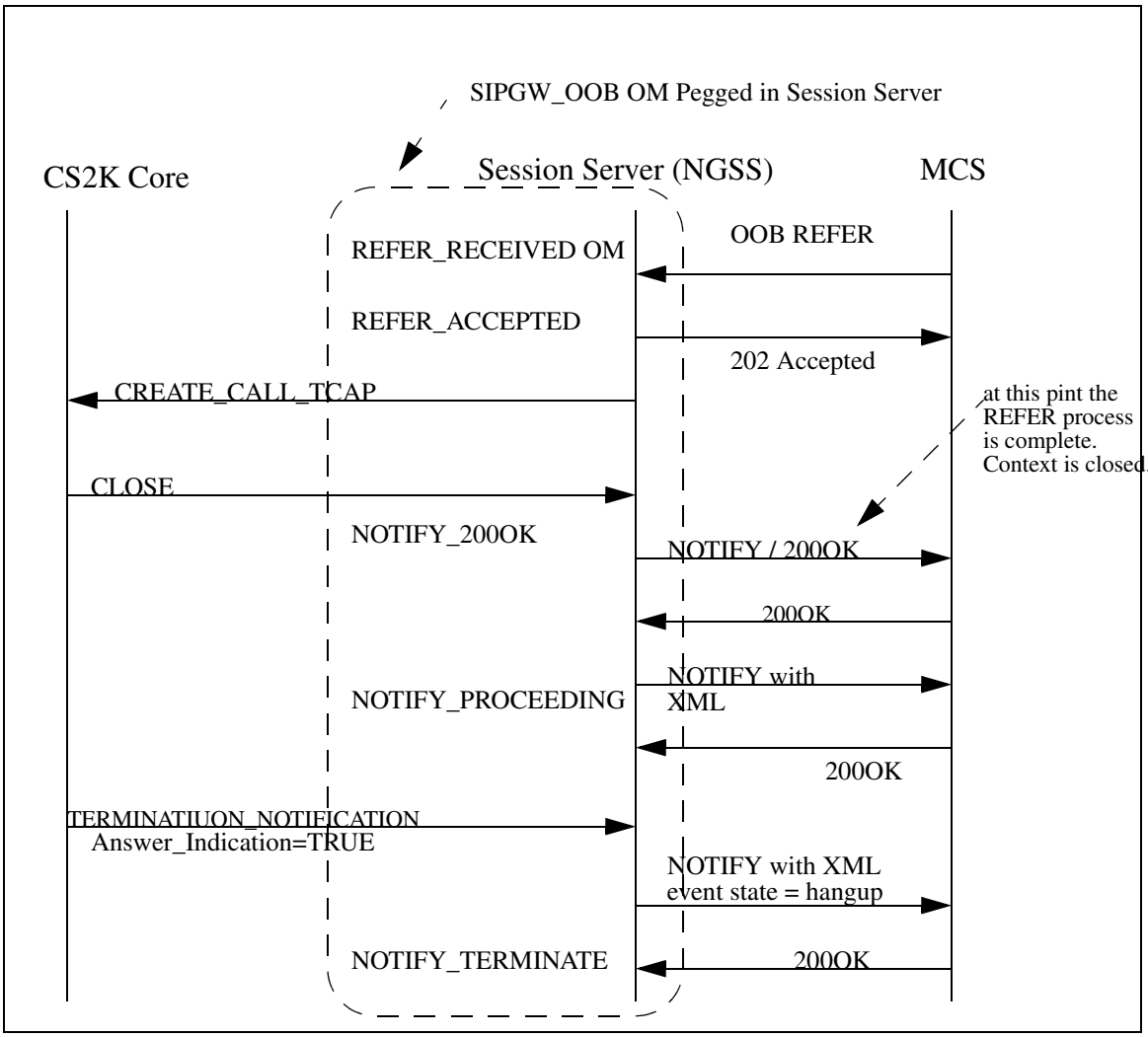


Figure 3 Failure OOB REFER Scenario

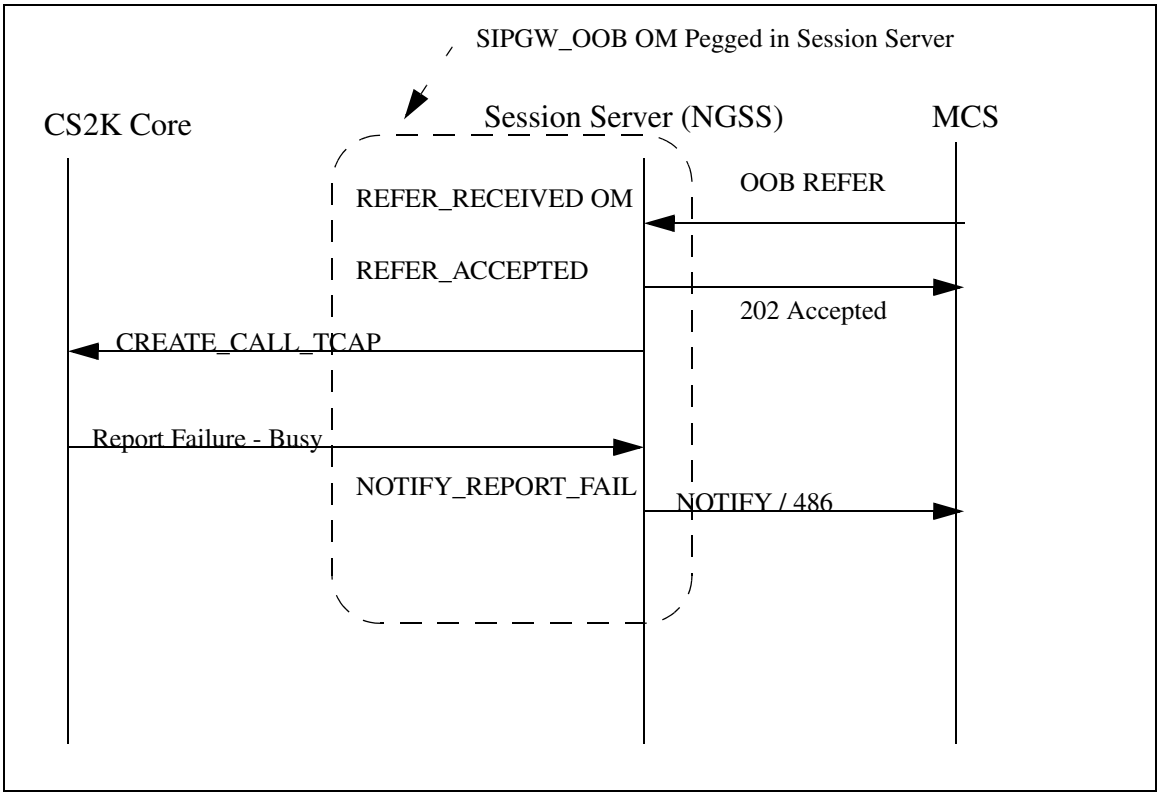
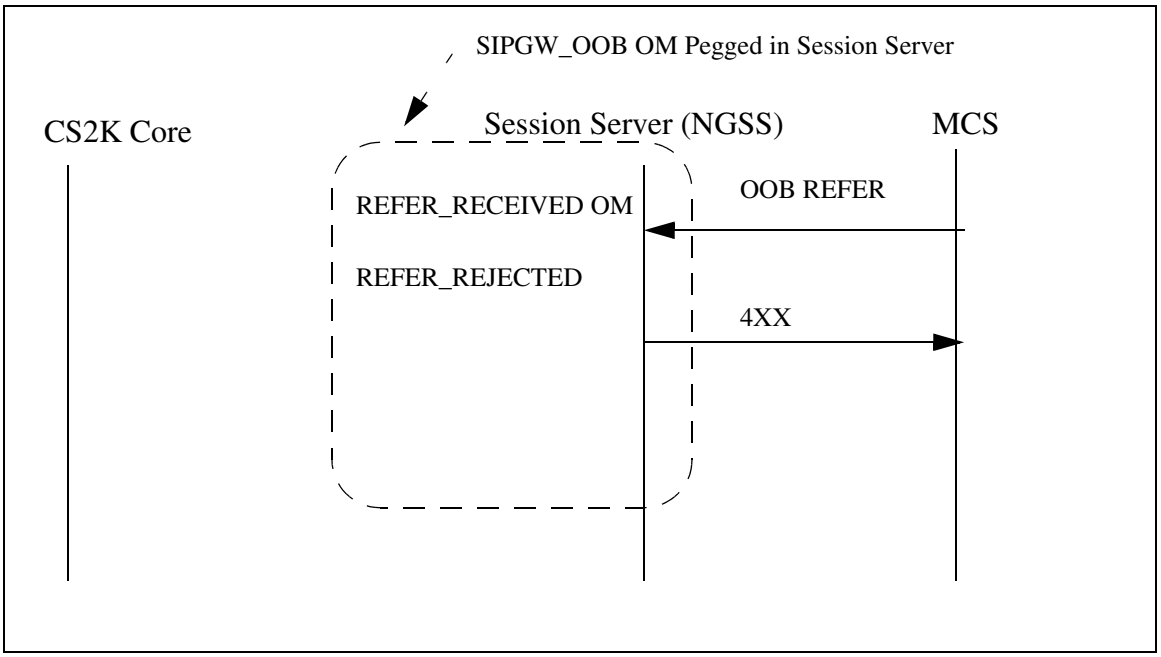


Figure 4 Failure OOB REFER Scenario



3.5.9 Register REFER_RECEIVED

3.5.9.1 Register description

This register is pegged every time the Session Server receives an Out-of-Band REFER request from the MCS.

3.5.9.2 Register release history update

New in this release

3.5.9.3 Associated registers

REFER_ACCEPTED, REFER_REJECTED

3.5.9.4 Associated logs

None

3.5.10 Register REFER_ACCEPTED

3.5.10.1 Register description

This register is pegged every time the Session Server validates an Out-of-Band REFER request and requests a Create_Call TCAP to be sent to the core.

3.5.10.2 Register release history update

New in this release

3.5.10.3 Associated registers

REFER_RECEIVED, CREATE_CALL_SENT (SIPGW_NCAS group),

3.5.10.4 Associated logs

None

3.5.11 Register REFER_REJECTED

3.5.11.1 Register description

This register is pegged every time the Session Server is unable to validate the OOB REFER request.

3.5.11.2 Register release history update

New in this release

3.5.11.3 Associated registers

REFER_RECEIVED

3.5.11.4 Associated logs

None

3.5.12 Register NOTIFY_200OK

3.5.12.1 Register description

This register is pegged every time the Session Server receives a CLOSE TCAP message from the core and a NOTIFY/200OK request is sent to the MCS

3.5.12.2 Register release history update

New in this release

3.5.12.3 Associated registers

CLOSE_RECEIVED (SIPGW_NCAS group)

3.5.12.4 Associated logs

None

3.5.13 Register NOTIFY_PROCEEDING

3.5.13.1 Register description

This register is pegged every time the Session Server sends a NOTIFY/ Proceeding msg to the MCS.

3.5.13.2 Register release history update

New in this release

3.5.13.3 Associated registers

CLOSE_RECEIVED (SIPGW_NCAS group)

3.5.13.4 Associated logs

None

3.5.14 Register NOTIFY_TERMINATE

3.5.14.1 Register description

This register is pegged every time the Session Server sends a NOTIFY msg indicating that the Call has ended.

3.5.14.2 Register release history update

New in this release

3.5.14.3 Associated registers

TERM_NOTIFY_RECEIVED (SIPGW_NCAS group)

3.5.14.4 Associated logs

None

3.5.15 Register NOTIFY_REPORT_FAIL

3.5.15.1 Register description

This register is pegged every time the Session Server sends a NOTIFY msg indicating a failure in Create_Call Completion

3.5.15.2 Register release history update

New in this release

3.5.15.3 Associated registers

FAILURE_RECEIVED (SIPGW_NCAS group)

3.5.15.4 Associated logs

None

3.6 SIPGW_NCAS OM Group

3.6.1 SIPGW_NCAS OM description

The New OM group called SIPGW_NCAS is introduced to keep a record of the Out-of-Band related TCAP messages sent and received between the Session Server and the CS2K. TCAP messages are sent over and SCPLite NCAS link

3.6.2 Release history update

Added new in this Release

3.6.3 Registers

The following table gives an overview of the registers associated with the SIPGW_NCAS OM group.

Table 2 OM Registers in the SIPGW_OOB OM Group

OM field	Description
CREATE_CALL_SENT	CREATE_CALL Request Sent
CREATE_CALL_FAIL	CREATE_CALL Request failed
CLOSE_RECEIVED	CLOSE Msg Received
TERM_NOTIFY_RECEIVED	CLOSE Msg Received

OM group registers display on the MAP terminal as follows:

Figure 5 OM Group Display

<regName> <regName> <regName> <regName>

3.6.4 Group structure

3.6.4.1 Associated OM groups

SIPGW_OOB OM Group - See section 14.4 for detailed description

3.6.4.2 Associated functional groups

None

3.6.4.3 Associated functionality codes

None

3.6.4.4 OM group registers logic flow chart

Figure 6 Successful OOB REFER Scenario

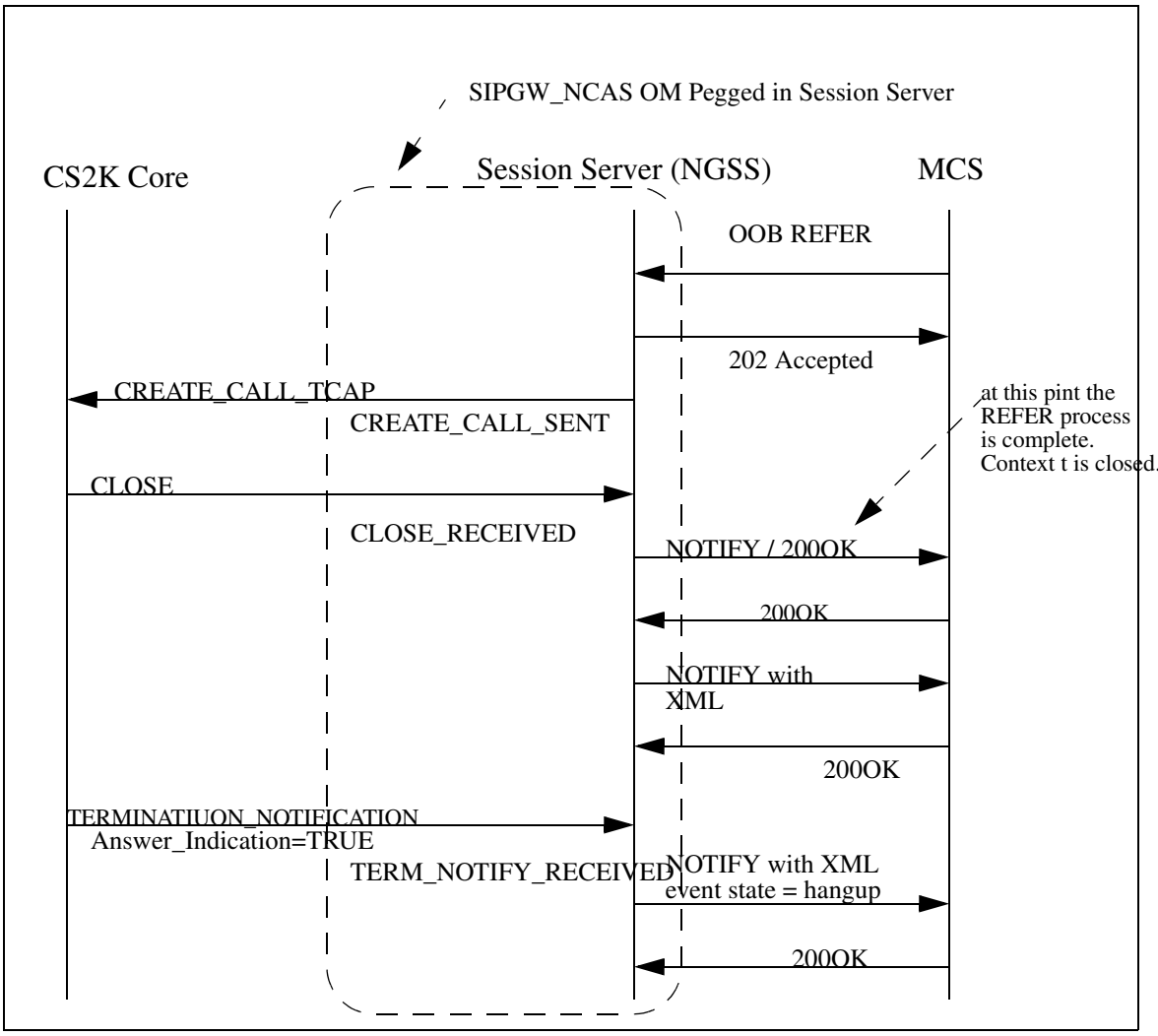
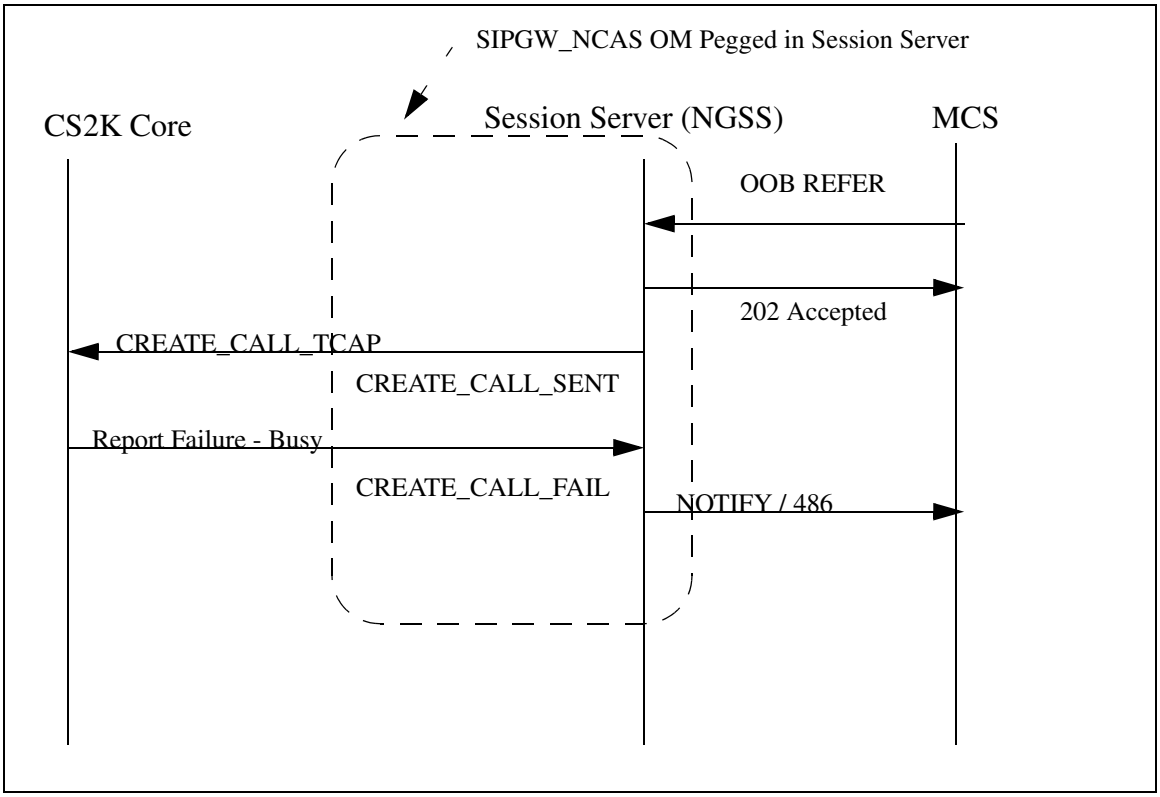


Figure 7 Failure OOB REFER Scenario



3.6.5 Register CREATE_CALL_SENT

3.6.5.1 Register description

This register is pegged every time a Create_Call is sent to the core over the NCAS link.

3.6.5.2 Register release history update

New in this release

3.6.5.3 Associated registers

REFER_RECEIVED, REFER_ACCEPETD (SIPGW_OOB Group)

3.6.5.4 Associated logs

None

3.6.6 Register CREATE_CALL_FAIL

3.6.6.1 Register description

This register is pegged every time a Create_Call request fails to complete

3.6.6.2 Register release history update

New in this release

3.6.6.3 Associated registers

NOTIFY_REPORT_FAIL (SIPGW_OOB Group)

3.6.6.4 Associated logs

None

3.6.7 Register CLOSE_RECEIVED

3.6.7.1 Register description

This register is pegged every time the Session Server receives a CLOSE msg in response to the Create_Call request

3.6.7.2 Register release history update

New in this release

3.6.7.3 Associated registers

NOTIFY_200OK, NOTIFY_PROCEEDING (SIPGW_OOB Group)

3.6.7.4 Associated logs

None

3.6.8 Register TERM_NOTIFY_RECEIVED

3.6.8.1 Register description

This register is pegged every time the Session Server receives a Terminate_Notification msg from the core

3.6.8.2 Register release history update

New in this release

3.6.8.3 Associated registers

NOTIFY_TERMINATE (SIPGW_OOB Group)

3.6.8.4 Associated logs

None

4: Performance (PF): A00009777

4.1 Feature Name

IEMS Mediant 2000 Integration

4.2 Performance management strategy

IEMS will collect the Performance metrics from the MG 3200 as it is being done for the MS2000 via SNMP. The below mentioned PMs from the acPerfMediaGateway MIB will be included for data collection for MG 3200 device.

The OIDs for which data collection would be done are :

PM Name	OID
Call Processing Performance Management	
acPerfCpNumDupsForCompletedTransactions	1.3.6.1.4.1.5003.10.1.1.1
acPerfCpNumDupsForOutstandingTransactions	1.3.6.1.4.1.5003.10.1.1.2
acPerfCpMessageSendSuccesses	1.3.6.1.4.1.5003.10.1.1.3
acPerfCpMessageSendErrors	1.3.6.1.4.1.5003.10.1.1.4
acPerfCpMessageReceiveSuccesses	1.3.6.1.4.1.5003.10.1.1.5
acPerfCpMessageReceiveErrors	1.3.6.1.4.1.5003.10.1.1.6
acPerfCpProtocolSyntaxErrors	1.3.6.1.4.1.5003.10.1.1.7
acPerfCpMessageRetransmissions	1.3.6.1.4.1.5003.10.1.1.8
acPerfCpMessageMaxRetransmissionsExceeded	1.3.6.1.4.1.5003.10.1.1.9
acPerfCpMessagesFromUntrustedSources	1.3.6.1.4.1.5003.10.1.1.10
RTP Performance Measurements	
acPerfRtpSenderPackets	1.3.6.1.4.1.5003.10.1.2.1
acPerfRtpSenderOctets	1.3.6.1.4.1.5003.10.1.2.2
acPerfRtpReceiverPackets	1.3.6.1.4.1.5003.10.1.2.3
acPerfRtpReceiverOctets	1.3.6.1.4.1.5003.10.1.2.4
acPerfRtpRcvrLostPackets	1.3.6.1.4.1.5003.10.1.2.5
acPerfRtpFailedDueToLackOfResources	1.3.6.1.4.1.5003.10.1.2.6
acPerfRtpSimplexInSessionsTotal	1.3.6.1.4.1.5003.10.1.2.7
acPerfRtpSimplexInSessionsCurrent	1.3.6.1.4.1.5003.10.1.2.8
acPerfRtpSimplexOutSessionsTotal	1.3.6.1.4.1.5003.10.1.2.9

acPerfRtpSimplexOutSessionsCurrent	1.3.6.1.4.1.5003.10.1.2.10
acPerfRtpDuplexSessionsTotal	1.3.6.1.4.1.5003.10.1.2.11
acPerfRtpDuplexSessionsCurrent	1.3.6.1.4.1.5003.10.1.2.12
System Performance Measurements	
acPerfSystemPacketEndpoints	1.3.6.1.4.1.5003.10.1.3.1
acPerfSystemPacketEndpointsInUse	1.3.6.1.4.1.5003.10.1.3.2

A new XML file template containing the above OIDs will be created for the performance collection of MG 3200 and all the necessary changes to include this in collection and report jobs will be done in the IEMS.

MG 3200 Integration A00009777 - DID Document

5: Performance (PF): A00009893

5.1 Feature Name

Session Server Call Processing Overload

5.2 Performance management strategy

OM group SIPGW_OVERLOAD is added to the Session Server to provide statistics related to the resourses that are monitored to determine whether the SIP Gateway application is in overload.

5.3 Performance Measurements (PM), Operational Measurements (OM), and stats

5.3.1 PM, OM, and stats format

Component: SIPGW_OVERLOAD

Performance measurement name: CPU_OCCUPANCY

Performance measurement description: The value calculated for the amount of time the CPU spent performing work as a percentage to its total running time over the last sampling period.

History: created in SN09

Performance Value Range: 0 - 100

Collection Interval: /opt/apps/etc/sipAppEnvVars (numSamples x interval)

OSS delivery (and interface) or Local only: Local

OSS Collection Interval: N/A

Element Manager Screen Name: N/A

File Name: /opt/apps/ngsspm/stdhist/ NGSS.STD_OMs.QoS.<year>.<month>.<day>_<time>_EDT.csv

Memory Usage: 4 Bytes

Component: SIPGW_OVERLOAD

Performance measurement name: CPU_OCCUPANCY_HWM

Performance measurement description: The maximum value calculated for the amount of time the CPU spent performing work as a percentage to its total running time over a 30 minute period. Reset to 0 every 30 minutes.

History: created in SN09

Performance Value Range: 0 - 100

Collection Interval: /opt/apps/etc/sipAppEnvVars (numSamples x interval)

OSS delivery (and interface) or Local only: Local

OSS Collection Interval: N/A

Element Manager Screen Name: N/A

File Name: /opt/apps/ngsspm/stdhist/ NGSS.STD_OMs.QoS.<year>.<month>.<day>_<time>_EDT.csv

Memory Usage: 4 bytes

Component: SIPGW_OVERLOAD

Performance measurement name: GCP_QUEUE_SIZE

Performance measurement description: The size of the GCP queue at the time the last sample was collected.

History: created in SN09

Performance Value Range: 0 - 4,294,967,296

Collection Interval: /opt/apps/etc/sipAppEnvVars (numSamples x interval)

OSS delivery (and interface) or Local only: Local

OSS Collection Interval: N/A

Element Manager Screen Name: N/A

File Name: /opt/apps/ngsspm/stdhist/ NGSS.STD_OMs.QoS.<year>.<month>.<day>_<time>_EDT.csv

Memory Usage: 4 bytes

Component: SIPGW_OVERLOAD

Performance measurement name: GCP_QUEUE_SIZE_HWM

Performance measurement description: The maximum sampled size of the GCP queue over a 30 minute period. Reset to 0 every 30 minutes.

History: created in SN09

Performance Value Range: 0 - 4,294,967,296

Collection Interval: /opt/apps/etc/sipAppEnvVars (numSamples x interval)

OSS delivery (and interface) or Local only: Local

OSS Collection Interval: N/A

Element Manager Screen Name: N/A

File Name: /opt/apps/ngsspm/stdhist/
NGSS.STD_OMs.QoS.<year>.<month>.<day>_<time>_EDT.csv

Memory Usage: 4 bytes

Component: SIPGW_OVERLOAD

Performance measurement name: SIP_QUEUE_SIZE

Performance measurement description: The size of the SIP queue at the time the last sample was collected.

History: created in SN09

Performance Value Range: 0 - 4,294,967,296

Collection Interval: /opt/apps/etc/sipAppEnvVars (numSamples x interval)

OSS delivery (and interface) or Local only: Local

OSS Collection Interval: N/A

Element Manager Screen Name: N/A

File Name: /opt/apps/ngsspm/stdhist/
NGSS.STD_OMs.QoS.<year>.<month>.<day>_<time>_EDT.csv

Memory Usage: 4 bytes

Component: SIPGW_OVERLOAD

Performance measurement name: SIP_QUEUE_SIZE_HWM

Performance measurement description: The maximum sampled size of the SIP queue over a 30 minute period. Reset to 0 every 30 minutes.

History: created in SN09

Performance Value Range: 0 - 4,294,967,296

Collection Interval: /opt/apps/etc/sipAppEnvVars (numSamples x interval)

OSS delivery (and interface) or Local only: Local

OSS Collection Interval: N/A

Element Manager Screen Name: N/A

File Name: /opt/apps/ngsspm/stdhist/
NGSS.STD_OMs.QoS.<year>.<month>.<day>_<time>_EDT.csv

Memory Usage: 4 bytes

5.3.2 Performance File (CSV, SSV, XML) Format

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime,Realiability
SIPGW_OVERLOAD,PeriodBased,15,unknown,Valid
Labels=Begin
TupleKey,KeyName
Key,KeyName
Reg1Name,Reg2Name,Reg3Name,Reg4Name
CPU_OCCUPANCY,CPU_OCCUPANCY_HWM,GCP_QUEUE_SIZE,GCP_QUEUE_SIZE_HWM
Reg5Name,Reg6Name
SIP_QUEUE_SIZE,SIP_QUEUE_SIZE_HWM
Labels=End
RowOfValues=Begin
RowOfValues=End
Table=End
```

6: Performance (PF): A00012109

6.1 Feature Name

Session Server Shared Library Replacement (SLR) Patching

6.2 Performance management strategy

Unchanged

6.3 Performance management tools and utilities

Unchanged

6.4 Performance Measurements (PM), Operational Measurements (OM), and stats

This activity adds five spare registers to each of the NGSS SIPGW OM groups listed below:

- SIPGW_CALLP
- SIPGW_SERVICES
- SIPGW_MISC
- SIPGW_TLS
- SIPGW_OVERLOAD
- SIPGW_OOB
- SIPGW_NCAS

In addition, the following three spare OM groups are added by this feature:

- SIPGW_SPARE1
- SIPGW_SPARE2
- SIPGW_SPARE3

The spare OM registers and spare OM groups introduced by this activity are reserved for future use.

6.4.1 PM, OM, and stats format

6.4.1.1 SIPGW_CALLP spare OMs

The following table lists the spare registers added to the SIPGW_CALLP OM group.

Table 1 OM Group: SIPGW_CALLP

Register Name	Description
SIPGW_CALLP_SPARE_1	reserved for future use
SIPGW_CALLP_SPARE_2	reserved for future use
SIPGW_CALLP_SPARE_3	reserved for future use
SIPGW_CALLP_SPARE_4	reserved for future use
SIPGW_CALLP_SPARE_5	reserved for future use

6.4.1.2 SIPGW_SERVICES spare OMs

The following table lists the spare registers added to the SIPGW_SERVICES OM group.

Table 2 OM Group: SIPGW_SERVICES

Register Name	Description
SIPGW_SERVICES_SPARE_1	reserved for future use
SIPGW_SERVICES_SPARE_2	reserved for future use
SIPGW_SERVICES_SPARE_3	reserved for future use
SIPGW_SERVICES_SPARE_4	reserved for future use
SIPGW_SERVICES_SPARE_5	reserved for future use

6.4.1.3 SIPGW_MISC spare OMs

The following table lists the spare registers added to the SIPGW_MISC OM group.

Table 3 OM Group: SIPGW_MISC

Register Name	Description
SIPGW_MISC_SPARE_1	reserved for future use
SIPGW_MISC_SPARE_2	reserved for future use
SIPGW_MISC_SPARE_3	reserved for future use
SIPGW_MISC_SPARE_4	reserved for future use
SIPGW_MISC_SPARE_5	reserved for future use

6.4.1.4 SIPGW_TLS spare OMs

The following table lists the spare registers added to the SIPGW_TLS OM group.

Table 4 OM Group: SIPGW_TLS

Register Name	Description
SIPGW_TLS_SPARE_1	reserved for future use

Register Name	Description
SIPGW_TLS_SPARE_2	reserved for future use
SIPGW_TLS_SPARE_3	reserved for future use
SIPGW_TLS_SPARE_4	reserved for future use
SIPGW_TLS_SPARE_5	reserved for future use

6.4.1.5 SIPGW_OVERLOAD spare OMs

The following table lists the spare registers added to the SIPGW_OVERLOAD OM group.

Table 5 OM Group: SIPGW_OVERLOAD

Register Name	Description
SIPGW_OVERLOAD_SPARE_1	reserved for future use
SIPGW_OVERLOAD_SPARE_2	reserved for future use
SIPGW_OVERLOAD_SPARE_3	reserved for future use
SIPGW_OVERLOAD_SPARE_4	reserved for future use
SIPGW_OVERLOAD_SPARE_5	reserved for future use

6.4.1.6 SIPGW_OOB spare OMs

The following table lists the spare registers added to the SIPGW_OOB OM group.

Table 6 OM Group: SIPGW_OOB

Register Name	Description
SIPGW_OOB_SPARE_1	reserved for future use
SIPGW_OOB_SPARE_2	reserved for future use
SIPGW_OOB_SPARE_3	reserved for future use
SIPGW_OOB_SPARE_4	reserved for future use
SIPGW_OOB_SPARE_5	reserved for future use

6.4.1.7 SIPGW_NCAS spare OMs

The following table lists the spare registers added to the SIPGW_NCAS OM group.

Table 7 OM Group: SIPGW_NCAS

Register Name	Description
SIPGW_NCAS_SPARE_1	reserved for future use
SIPGW_NCAS_SPARE_2	reserved for future use
SIPGW_NCAS_SPARE_3	reserved for future use

Register Name	Description
SIPGW_NCAS_SPARE_4	reserved for future use
SIPGW_NCAS_SPARE_5	reserved for future use

6.4.1.8 SIPGW_SPARE1 spare OMs

The following table lists the registers added to the new SIPGW_SPARE1 OM group.

Table 8 OM Group: SIPGW_SPARE1

Register Name	Description
SIPGW_SPARE1_REG_1	reserved for future use
SIPGW_SPARE1_REG_2	reserved for future use
SIPGW_SPARE1_REG_3	reserved for future use
SIPGW_SPARE1_REG_4	reserved for future use
SIPGW_SPARE1_REG_5	reserved for future use
SIPGW_SPARE1_REG_6	reserved for future use
SIPGW_SPARE1_REG_7	reserved for future use
SIPGW_SPARE1_REG_8	reserved for future use
SIPGW_SPARE1_REG_9	reserved for future use
SIPGW_SPARE1_REG_10	reserved for future use

6.4.1.9 SIPGW_SPARE2 spare OMs

The following table lists the registers added to the new SIPGW_SPARE2 OM group.

Table 9 OM Group: SIPGW_SPARE2

Register Name	Description
SIPGW_SPARE2_REG_1	reserved for future use
SIPGW_SPARE2_REG_2	reserved for future use
SIPGW_SPARE2_REG_3	reserved for future use
SIPGW_SPARE2_REG_4	reserved for future use
SIPGW_SPARE2_REG_5	reserved for future use
SIPGW_SPARE2_REG_6	reserved for future use
SIPGW_SPARE2_REG_7	reserved for future use
SIPGW_SPARE2_REG_8	reserved for future use
SIPGW_SPARE2_REG_9	reserved for future use
SIPGW_SPARE2_REG_10	reserved for future use

6.4.1.10 SIPGW_SPARE3 spare OMs

The following table lists the registers added to the new SIPGW_SPARE3 OM group.

Table 10 OM Group: SIPGW_SPARE3

Register Name	Description
SIPGW_SPARE3_REG_1	reserved for future use
SIPGW_SPARE3_REG_2	reserved for future use
SIPGW_SPARE3_REG_3	reserved for future use
SIPGW_SPARE3_REG_4	reserved for future use
SIPGW_SPARE3_REG_5	reserved for future use
SIPGW_SPARE3_REG_6	reserved for future use
SIPGW_SPARE3_REG_7	reserved for future use
SIPGW_SPARE3_REG_8	reserved for future use
SIPGW_SPARE3_REG_9	reserved for future use
SIPGW_SPARE3_REG_10	reserved for future use

6.4.2 Performance File (CSV, SSV, XML) Format

Unchanged

6.4.3 OM Group template (applies only to DMS)

N/A

Table of Contents

RelDoc Introduction, International 3
(I)SN09FF Feature Subset Cross Reference Tables: International Features 9
Feature to Functional Group Cross Reference 9
Functional Group to Feature Impacts Cross Reference 11
Functional Descriptions List (FNs) 15
. . Functional Description (FN): A00009037 19
. . Functional Description (FN): A00006664 55
. . Functional Description (FN): A00006665 72
. . Functional Description (FN): A00007289 82
. . Functional Description (FN): A00008429 85
. . Functional Description (FN): A00008477 105
. . Functional Description (FN): A00008479 111
. . Functional Description (FN): A00008484 117
. . Functional Description (FN): A00008556 166
. . Functional Description (FN): A00008721 195
. . Functional Description (FN): A00009024 208
. . Functional Description (FN): A00009037 210
. . Functional Description (FN): A00009039 218
. . Functional Description (FN): A00009097 291
. . Functional Description (FN): A00009120 300
. . Functional Description (FN): A00009143 307
. . Functional Description (FN): A00009145 333
. . Functional Description (FN): A00009158 344
. . Functional Description (FN): A00009165 372
. . Functional Description (FN): A00009216 374
. . Functional Description (FN): A00009228 385
. . Functional Description (FN): A00009245 395
. . Functional Description (FN): A00009282 403
. . Functional Description (FN): A00009297 405
. . Functional Description (FN): A0009321 477
. . Functional Description (FN): A0009322 483
. . Functional Description (FN): A00009446 493
. . Functional Description (FN): A00009489 518
. . Functional Description (FN): A00010168 526
. . Functional Description (FN): A00011363 534
. . Functional Description (FN): A00012291 551
. . Functional Description (FN): A00012349 553
. . Functional Description (FN): A00012477 557
. . Functional Description (FN): A00012509 560
. . Functional Description (FN): A00012510 565
. . Functional Description (FN): A00012511 571
. . Functional Description (FN): A00012847 575

. . Functional Description (FN): A00013275 581
. . Functional Description (FN): A00013286 600
Fault Management List (FMs) 603
. . Fault Management (FM): A00006663 605
. . Fault Management (FM): A00008556 607
. . Fault Management (FM): A00009120 611
. . Fault Management (FM): A00009245 616
. . Fault Management (FM): A00009282 624
Configuration Management List (CNs) 629
. . Configuration (CN): A00006664 631
. . Configuration (CN): A00007289 649
. . Configuration (CN): A00008429 650
. . Configuration (CN): A00008477 659
. . Configuration (CN): A00008484 666
. . Configuration (CN): A00008556 669
. . Configuration (CN): A00009037 690
. . Configuration (CN): A00009145 695
. . Configuration (CN): A00009216 699
. . Configuration (CN): A00009282 701
. . Configuration (CN): A00009321 707
. . Configuration (CN): A00009322 726
. . Configuration (CN): A00009489 734
. . Configuration (CN): A00013275 740

RelDoc Introduction, International

TDM and Carrier VoIP SOFTWARE

PRODUCT COMPUTING MODULE LOAD RELEASE DOCUMENT

(PCL) Release Document

ATTENTION International Customers: Use both parts

The features in this section of the document are specific and exclusive to the International market. Any features that apply to both the North American and International markets are located in the North American section of this document.

This release document is supplied for each Software Stream for the International load. This release document provides software feature information pertinent to the new software load.

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

The release document consists of the following sections:

FEATURE CONTENT
This section provides information concerning TDM and Carrier VoIP system features associated with software releases. Due to process conflicts, information on PVG and MDM features is limited. Each office configuration is customized to meet Telco/Carrier requirements. The following subsections include information necessary to determine that system software changes have occurred since the last software release.

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

CROSS REFERENCE TABLES

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

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

- Functional Descriptions (FN) -summarizes the functions of the feature
- Fault Management (FM)) --indicates major additions/changes to the LOGs and Alarms.
- Configuration (CN) may include information on the following:
  - — Data Schema (DS) -indicates major additions/changes to the Data Schema table
  - — Service Orders (SO) -indicates major additions/changes to the Service Orders
  - — User Interface (UI) - indicates major additions/changes to the User Interface
- Accounting (ACC)
  - — Automatic Message Accounting (AM) -indicates major additions/ changes to the AMA
- Performance (PF) -- indicates major additions/changes to Operational Measurements (OMs) and/or Performance Measurements.

How To Use the Feature Content Section

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

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

A functional group is made up of several features.

- Table 1: Feature to Functional Group Cross Reference

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

- Table 2: Functional Group to Feature Impacts Cross Reference

  These tables list all documentation listed in the feature content section. As stated above, the documentation is sorted first by feature functional group,

and then by featid within the functional group. This table indicates which sections are included (for example, FM, CN, PF, or ACC) in the release document.

Publication history-International

October 2006

(I)SN09U is an extension of the (I)SN09 software release and supersedes both (I)SN09 and (I)SN09FF for CVoIP applications. (I)SN09 continues to be supported for TDM-only applications. The (I)SN09U software release incorporates all capabilities of (I)SN09, (I)SN09FF, and additional corrective content delivered as part of Nortel's (I)SN09 software robustness program. (I)SN09, (I)SN09FF, and (I)SN09U are valid terms for use within the (I)SN09U software release.

Version 01.04 re-release of Standard for (I)SN09U, combining content from SN09 and SN09FF.

May 2006

Version 01.03 re-release of Standard for (I)SN09FF due to CR changes in the North American section of the document.

April 2006

Version 01.02 Standard release for (I)SN09FF. The following features have been added for the Standard version:

- A00009297, QoSR: Support of AAL2
- A00012291, MG15K Call-waiting Tone Support & Additional International Tones
- A00012847, CS2K DPNSS Message Waiting Indicator for UMS
- A00013286, Core Flex Large Line GWC Prof (Phase 1)

December 2005

Version 01.01 Preliminary release for (I)SN09FF.

(I)SN09U Feature Subset Cross Reference Tables: International Features

Feature to Functional Group Cross Reference

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

> ***Note:*** Features available in Nortel's FMDOC library show a version/issue number (i.e., AA05, etc.), while the features obtained from other sources do not have a version/issue number.

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

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of Base/TL, CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00006663.AB02	DDRM Alarms and Audits	WT22
A00006664.AB05	DDRM Line Testing	WT22
A00006665.AB06	DDRM ESA Support	WT22
A00007289.AA06	RT Selector Enhancement for Metering	WT22
A00008429.AA09	Ring Back When Free (RBWF) Enhancements	WT22
A00008477.AA10	Increase size of table MSGRTE	WT22
A00008479.AA05	IP Correlation ID Enhancement	WT22
A00008484.AA07	IN Terminating Trigger Feature Interactions	WT22
A00008556.AA35	SIP Lines Core OAMP support	WT22
A00008721.AA09	DUAL RCO2 Development	WT22, XPM22

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of Base/TL, CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00009024.AA22	ETSI BRI (Basic Rate Interface) on Succession - PhaseI	WT22, GC09
A00009037.AA06	CORE - Enhanced ESA for International MG9000	WT22
A00009039.AA09	International MG9000 Line Test Support	WT22
A00009097	IUP ACI Handling Enhancement	WT22
A00009120.AA17	Multi-Time Zone Enhancments	WT22
A00009143.AA11	FTUP & SPIROU NAOC to VN4/VN6/ETSI PRI & H323 AOC Interworking	GC09
A00009145.AA10	Record Feature Usage	WT22
A00009158.AA04	M3UA over SCTP from Core to USP	Core22
A00009165.AA03	USP - Offline Routesets without Alarms	Core22, USP11
A00009216.AA10	JI-ISUP to Base ETSI ISUP V2 Mapping Enhancement	WT22
A00009228.AA07	International Trunk Interception in CS2K	WT22
A00009245.AA12	Succession Test Trunks: T904 Support	WT22
A00009282	MG9KEM - International ESA and MLPP Support	MG9KEM09
A00009297	QoSR: Support of AAL2	GC09
A00009321.AA15	NMC Code Blocking	WT22
A00009322.AA16	Call Lock and Do Not Disturb Enhancements	WT22
A00009373	Vodafone Portugal 3G Video Features (Interworking)	MCS09
A00009446.AA01	M2UA/SCTP Protocol for PVG SS7 backhaul support	USP11
A00009489.AA11	CHT: Call Waiting Enhancement	WT22
A00010168.AA06	H.323 support for COnnected Line Presentation/ COn-nected Line Restriction (COLP/COLR)	GC09

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
Note: Core is comprised of Base/TL, CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00011363.AA03	International H.323 2CLI (Calling Line Identity) Support	WT22, GC09
A00012291	MG15K Call-waiting Tone Support & Additional International Tones	PVG09.1
A00012349.AA10	U3WC Support For SIP Lines	WT23
A00012477.AA09	Session Initiation Protocol (SIP) Services - Call Completion to Busy Subscriber (CCBS)	WT23
A00012509.AA11	SIP Services Wake up Call Reminder	WT23
A00012510.AA15	SIP Services: Malicious Call Trace	WT23
A00012511.AA10	SIP Services: Payment Ceiling Advice (PCA)	WT23
A00012847.AA06	CS2K DPNSS Message Waiting Indicator for UMS	WT23
A00013275	C&W: CS2M support for variable sized LGRP	CS2M09.1
A00013286.AA12	Core Flex Large Line GWC Prof (Ph1)	Core23

Functional Group to Feature Impacts Cross Reference

Table 2 is organized alphabetically by functional group. Within each group, the features are listed numerically. If a Feature belongs to more than one group, it appears in each group to which it belongs. The table also indicates which sections are included for a given feature (for example, FN, FM, CN, PF, or ACC) in the release document.

Table 2 Functional Group to Feature Impacts Cross Reference

Functional Group (Stream and release)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
Core22	A00009158.AA04	Y				
Core22, USP11	A00009165.AA03	Y				
Core23	A00013286.AA12	Y				

Functional Group (Stream and release)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
CS2M09.1	A00013275	Y				
GC09	A00009143.AA11	Y				
GC09	A00009297	Y				
GC09	A00010168.AA06	Y				
MCS09	A00009373	Y				
MG9KEM09	A00009282	Y	Y	Y		
PVG09.1	A00012291	Y				
WT22	A00006663.AB02	Y	Y			
WT22	A00006664.AB05	Y		Y		
WT22	A00006665.AB06	Y				
WT22	A00007289.AA06	Y		Y		
WT22	A00008429.AA09	Y		Y		
WT22	A00008477.AA10	Y		Y		
WT22	A00008479.AA05	Y				
WT22	A00008484.AA07	Y		Y		
WT22	A00008556.AA35	Y	Y	Y		
WT22, XPM22	A00008721.AA09	Y				
WT22, GC09	A00009024.AA22	Y				
WT22	A00009037.AA06	Y		Y		
WT22	A00009039.AA09	Y				
WT22	A00009097	Y				
WT22	A00009120.AA17	Y	Y	Y		
WT22	A00009145.AA10	Y		Y		
WT22	A00009216.AA10	Y		Y		
WT22	A00009228.AA07	Y				

Functional Group (Stream and release)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
WT22	A00009245.AA12	Y				
WT22	A00009321.AA15	Y		Y		
WT22	A00009322.AA16	Y		Y		
WT22	A00009489.AA11	Y		Y		
WT22, GC09	A00011363.AA03	Y				
WT23	A00012349.AA10	Y				
WT23	A00012477.AA09	Y				
WT23	A00012509.AA11	Y				
WT23	A00012510.AA15	Y				
WT23	A00012511.AA10	Y				
WT23	A00012847.AA06	Y				

Functional Descriptions (FN)

Introduction

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

Featid	Title
A00006663.AB02	DDRM Alarms and Audits
A00006664.AB05	DDRM Line Testing
A00006665.AB06	DDRM ESA Support
A00007289.AA06	RT Selector Enhancement for Metering
A00008429.AA09	Ring Back When Free (RBWF) Enhancements
A00008477.AA10	Increase size of table MSGRTE
A00008479.AA05	IP Correlation ID Enhancement
A00008484.AA07	IN Terminating Trigger Feature Interactions
A00008556.AA35	SIP Lines Core OAMP support
A00008721.AA09	DUAL RCO2 Development
A00009024.AA22	ETSI BRI (Basic Rate Interface) on Succession - PhaseI
A00009037.AA06	CORE - Enhanced ESA for International MG9000
A00009039.AA09	International MG9000 Line Test Support
A00009097	IUP ACI Handling Enhancement
A00009120.AA17	Multi-Time Zone Enhancments

A00009143.AA11	FTUP & SPIROU NAOC to VN4/VN6/ETSI PRI & H323 AOC Interworking
A00009145.AA10	Record Feature Usage
A00009158.AA04	M3UA over SCTP from Core to USP
A00009165.AA03	USP - Offline Routesets without Alarms
A00009216.AA10	JI-ISUP to Base ETSI ISUP V2 Mapping Enhancement
A00009228.AA07	International Trunk Interception in CS2K
A00009245.AA12	Succession Test Trunks: T904 Support
A00009282	MG9KEM - International ESA and MLPP Support
A00009297	QoSR: Support of AAL2
A00009321.AA15	NMC Code Blocking
A00009322.AA16	Call Lock and Do Not Disturb Enhancements
A00009373	Vodafone Portugal 3G Video Features (Interworking)
A00009446.AA01	M2UA/SCTP Protocol for PVG SS7 backhaul support
A00009489.AA11	CHT: Call Waiting Enhancement
A00010168.AA06	H.323 support for COnnected Line Presentation/COnnected Line Restriction (COLP/COLR)
A00011363.AA03	International H.323 2CLI (Calling Line Identity) Support
A00012291	MG15K Call-waiting Tone Support & Additional International Tones
A00012349.AA10	U3WC Support For SIP Lines
A00012477.AA09	Session Initiation Protocol (SIP) Services - Call Completion to Busy Subscriber (CCBS)
A00012509.AA11	SIP Services Wake up Call Reminder
A00012510.AA14	SIP Services: Malicious Call Trace
A00012511.AA09	SIP Services: Payment Ceiling Advice (PCA)

A00012847.AA06	CS2K DPNSS Message Waiting Indicator for UMS
A00013275	C&W: CS2M support for variable sized LGRP
A00013286.AA12	Core Flex Large Line GWC Prof (Phase 1)
A00013457	Message Waiting Indication using SIP VM/UM based on RFC 3842 (*FN located in the North American chapter*)

1: Functional Description (FN): A00009037

1.1 Feature name and Feature ID

A00006663 - DDRM ALARMS AND AUDITS

1.1.1 INTRODUCTION

DDRM (DMS Dicle Remote Module) project provides remote LCM node facility to DRX-4 rural exchanges in Turk Telecom network.

This activity handles two components : Alarms and OM & LOGS

- **Component 1. Alarm**

DDRM is capable of detecting and reporting faults for almost all hardware cards. This feature enables to follow up those alarms via OM, LOGs & MAPCI and allows the craftperson to specify the faulty cards remotely. Alarm severity are positioned properly on MAPCI and activate proper processes in DDRM Maintenance SW. Node Status is set to SBSY or ISTB and/or related line states are set to lockout state till the recovery messages are received by DDRM in brief.

Solicited Queries of configurationare made by basic DMS MTC process.

*** RTS:** In test phase all DDRM Alarms are cleared except LC Alarm to refresh permanent alarm conditions in case of any missing recovery messages: **this cleanup is done if only both units are out of service**

Then status of cards datafilled at LCMINV is requested by DMS during test phase. DDRM bundles those status in one ack. response message (implemented ISN08 Activity A00006661). DDRM rescan the alarm conditions and reports all card faulty once it gains the activity.

*** TEST PM:** This clears all DDRM Alarms except LC Alarms on DMS if both unit states are out of service. DDRM reports the mismatch on the configured / datafilled cards at LCMINV in reply. DDRM is expected to produce the current alarm messages if alarm condition remains after INSV state by means of unsolicited messages.

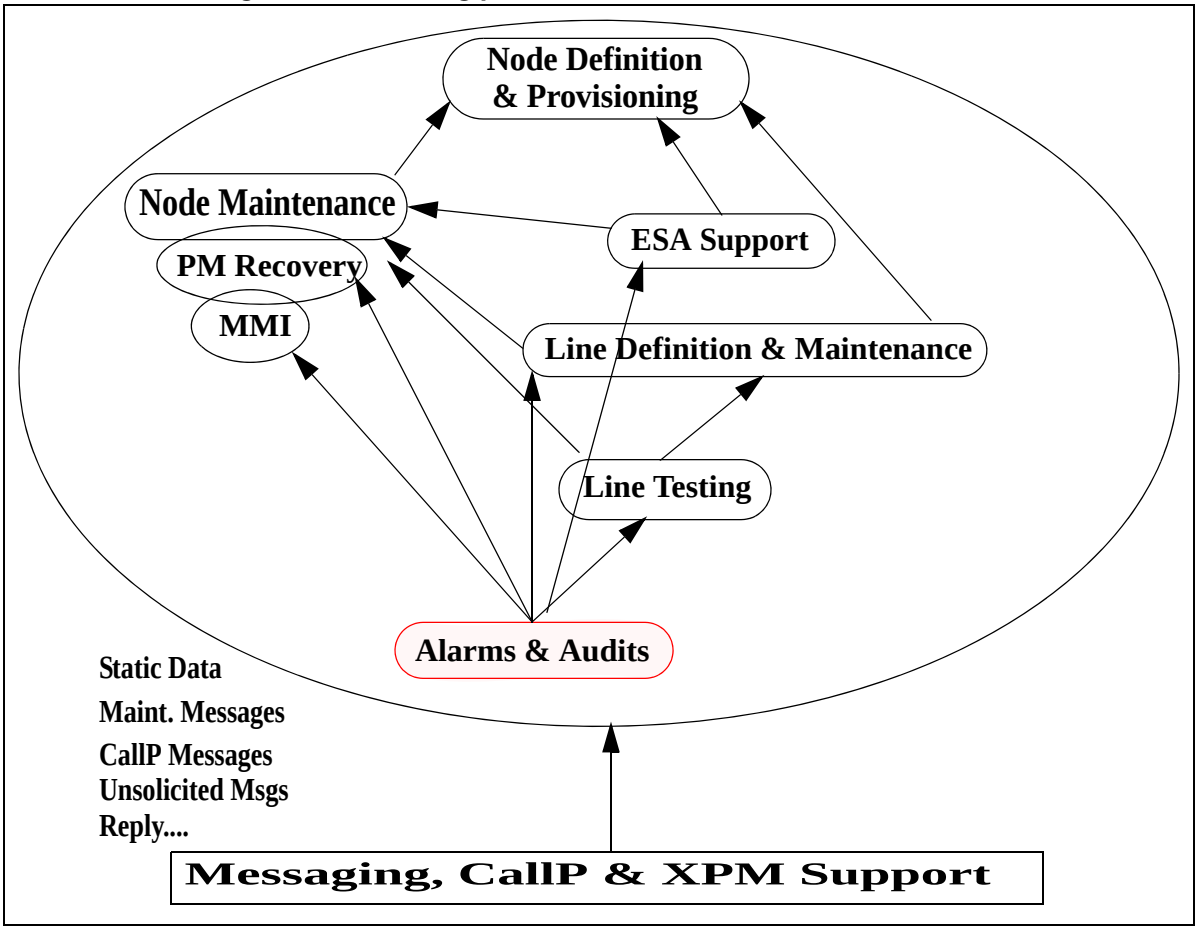
*** AUDIT**: Existing RLCM Node and Line Audits continue to work for DDRM. For babbling faults, DMS Babbling Audit and recovery may commence diagnostic tests for recovery of the alarms if Babbling is reported: DDRM is not capable of reporting babblings on the line at ISN09 but DMS is ready to accept. As such babbling is not testable.

DMS doesn't limit to send existing audits, queries and maintenance messages for DDRM: DDRM is expected to ignore those messages as they are not useless for DDRM.

- **Component 2. OM**

This component aims changes to resuse the existing OM of RLCMs for new RLCM variant - DDRM. Figure 1 on page 20 shows the big picture view and how this part of the project fits in the overall project:

Figure 1 DDRM big picture view



1.1.2 ALARM - GENERIC BEHAVIOUR

The following alarms are reported by DDRM node to DMS:

- Module Alarm
- Card Configuration Alarm
- POC Alarm
- Ring Alarm
- -48v Alarm
- ETM /TBK Alarm

DDRM reports the mismatches during RTS if the configuration data sent by DMS according to the datafill at LCMINV doesn't match the real configuration on DDRM shelfs. Mismatches are registered as an alarm and be monitored by executing Query Fault for posted at MAPCI:MTC:PM Level.

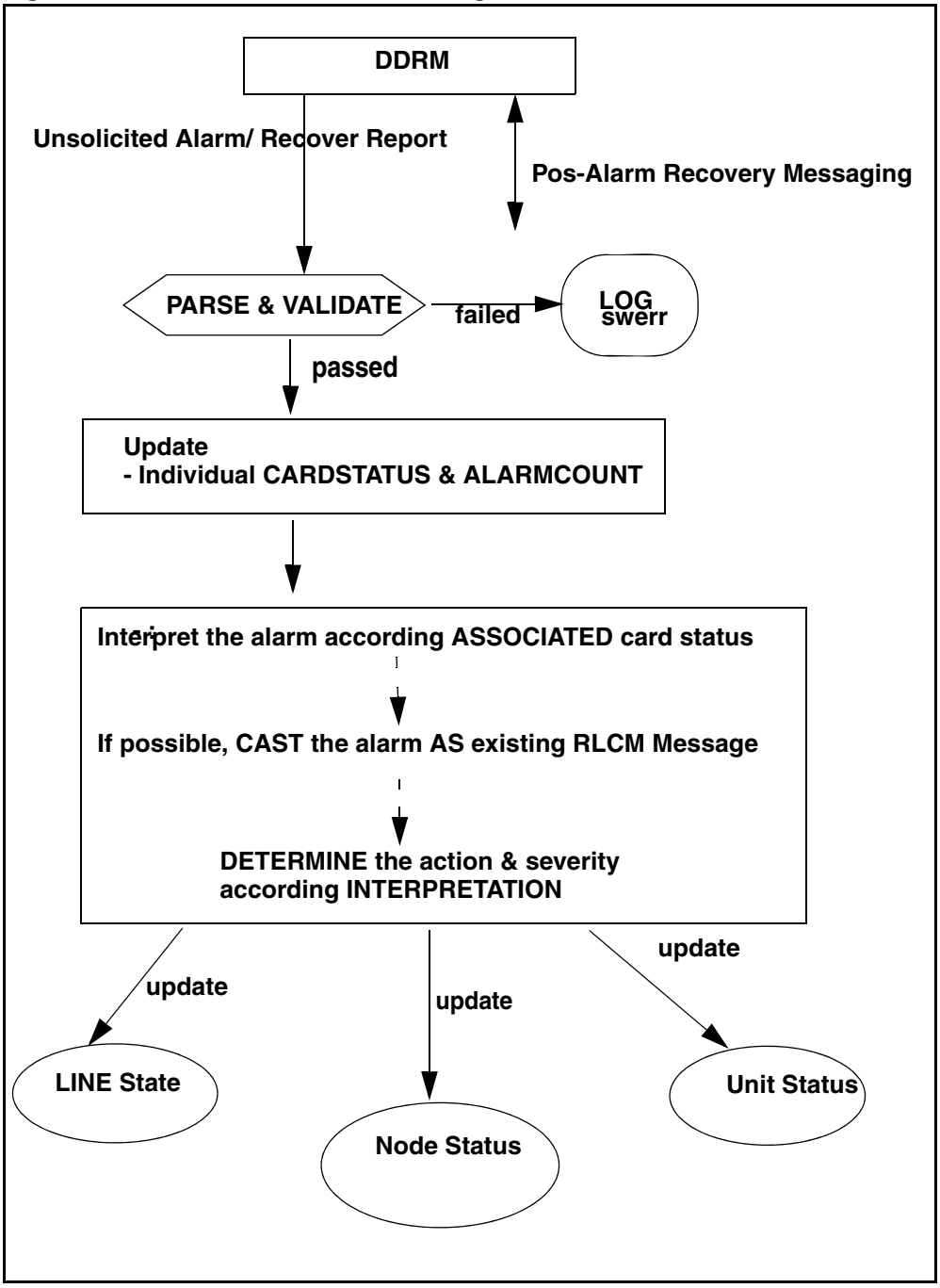
When the reasons occurred on DDRM for those alarms the modified DMS-X / LCM messages are sent to DMS. After the reception of this indication, DMS takes the related actions like changing the state of DDRM and / or changing the state of lines and managing the call processing related facilities etc.

When the reasons which cause the alarms are recovered DDRM sends the modified DMS-X / LCM messages to DMS. After that DMS takes the related actions and the service facilities of DDRM node and it's subscribers continue as expected.

DMS-X/LCM messages conveys the faulty card address as the subject of recovery or alarmed condition.

DMS accept those messages if node state is INSV or ISTB status: **any reports are ignored by DMS for status except of INSV or ISTB status.**

Figure 2 Alarm - Generic Behavior Diagram



1.1.3 Additional Queries By DMS

RTS and TEST PM queries GNS, MXC, UTR, LTT-TMS, D's if those are datafilled at LCMINVproperly (ISN08 MTC Activity).

ISN09 DDRM enables to reports all of alarms once it gains the activity.

RTS failes if bundle ack message includes the alarms which causes a SBSY condition on Node Status. status for these cards: This messaging is done by Test Sub-routine of RTS process, which is also called during TEST PM command.

All alarms are cleared during Test Phase of TST./RTS/or SBSY->RTS transition if node status is not ISTB/INSV.

Other queries are relevant with Node Audit and Line Diagnostics: those audits may enable DDRM to rescan the alarms and report unsolicited (not expected as reply against audit/recover messages) if the need is raised.

1.1.4 Alarm Conditions and Severity Map

Table on page 24 gives the problem reasons which cause alarms, their severity class, the state of DDRM after reception of the alarm and the existence of a recovery message for them, as described at DMS_DDRM Spec. Document at FMDOC.

Any individual module alarm does not reveal a problem associated with single or both units of DDRM. For example an MXC controls the LCs on its shelf and each shelf contains odd and even subdrawers (equivalent 4xLC = 1 Subdrawer of an standard LCM), where RLCM even drawers are controlled by unit0 whilst odds are under control of unit1. So an individual MXC cannot indicate a single unit problem.

When a alarm occurs for DDRM node it is shown on DMS MAP level. For the display of alarms on DMS MAP level see section.

Table 1: Alarm - Severity

Card problems & subscriber alarms on DDRM	Alarm severity Class			Modified DMS-X/ LCM report message (From DDRM)	DDRM state	Modified DMS-X/ LCM Recovery message (From DDRM)	Remarks
Card problems on DDRM	**Critical**	**Major**	**Minor**				
Last GNS Card (single and double plane)	+			+	SYSB	+	
One GNS Card (double plane)		+		+	ISTB	+	Both units of DDRM is INSV.
One DTC card (for 2 DTC configuration)		+		+ [1]	ISTB	-	The DDRM unit which is connected to the DTC card with problem is in SYSB state and DDRM is in take-over mode. The other unit is in INSV and DDRM state is ISTB. Any clean-up is not expected on SYSB unit because DDRM is ISTB state. The existing calls which are connected through this DTC should be released by DDRM / DMS. If there is no problem with E1 links then they are taken from the service.

Table 1: Alarm - Severity

Card problems & subscriber alarms on DDRM	Alarm severity Class			Modified DMS-X/ LCM report message (From DDRM)	DDRM state	Modified DMS-X/ LCM Recovery message (From DDRM)	Remarks
Card problems on DDRM	Critical	Major	Minor				
Last DTC card	+			+ [2]	CBSY/ SYSB	NA	The alarm report message is expected if there is at least one E1 available.
One MXC card		+		+	ISTB	+	The subscribers on the same shelf with this MXC card are not given any service facilities and their state are set to LO. DDRM state is ISTB. LTT / TMS, UTR, POC & RG cards on the same shelf are assumed as out of service even if there are no alarm messages specific for these cards. If LTT / TMS cards are on the same shelf then MTA tests are affected for all subscribers
Last MXC card	+			+	SYSB	+	

Table 1: Alarm - Severity

Card problems & subscriber alarms on DDRM	Alarm severity Class			Modified DMS-X/ LCM report message (From DDRM)	DDRM state	Modified DMS-X/ LCM Recovery message (From DDRM)	Remarks
Card problems on DDRM	Critical	Major	Minor				
One UTR card			+	+	ISTB	+	
Last UTR card		+		+	ISTB	+	
LTT - TMS card		+		+	ISTB	+	The messages are received separately for each card.

Table 1: Alarm - Severity

Card problems & subscriber alarms on DDRM	Alarm severity Class			Modified DMS-X/ LCM report message (From DDRM)	DDRM state	Modified DMS-X/ LCM Recovery message (From DDRM)	Remarks
Card problems on DDRM	Critical	Major	Minor				
One POC card			+[3]	+	ISTB	+	The POC card alarm can not be provided from DDRM for standby POC card. **So when a problem occurs on the standby POC card** the alarm severity class is based on MXC and GNS cards. But for any reason a POC alarm about the standby card is received but any other alarm message e.g. like MXC on this shelf is not received standby POC alarm is seen on DMS MAP but subscribers are expected to continue their service facilities as before this alarm. If there is not any Critical alarm reason then DDRM state is ISTB.

Table 1: Alarm - Severity

Card problems & subscriber alarms on DDRM	Alarm severity Class			Modified DMS-X/ LCM report message (From DDRM)	DDRM state	Modified DMS-X/ LCM Recovery message (From DDRM)	Remarks
Card problems on DDRM	Critical	Major	Minor				
Last POC card	+			NA	SYSB	NA	When a problem on last POC card occurs E1 links are went down and the problem can not be reported.*DDRM node is restarted*. If this alarm is received because of any reason but not any other alarm condition (e.g about DTC,MXC & GNS) occurs then POC alarm is received by DMS but subscribers are expected to continue their service facilities as before this alarm.
One -48V input			+	+	ISTB	+	

Table 1: Alarm - Severity

Card problems & subscriber alarms on DDRM	Alarm severity Class			Modified DMS-X/ LCM report message (From DDRM)	DDRM state	Modified DMS-X/ LCM Recovery message (From DDRM)	Remarks
Card problems on DDRM	**Critical**	**Major**	**Minor**				
2nd -48v	+			NA	SYSB	NA	When the 2nd -48v problem occurs E1 links are went down and the 2nd 48v problem can not be reported. If this alarm is received because of any reason but not any other alarm condition (e.g about DTC,MXC & GNS) occurs then -48v alarm is received by DMS but subscribers are expected to continue their service facilities as before this alarm.
Ringing generator on one POC card			+	+	ISTB	+	
Ringing generator on standbyPOC card		+		+	ISTB	+	
Last ringing generator on POC card	+			+	ISTB	+	
Subscriber alarms on DDRM [4]							

Table 1: Alarm - Severity

Card problems & subscriber alarms on DDRM	Alarm severity Class			Modified DMS-X/ LCM report message (From DDRM)	DDRM state	Modified DMS-X/ LCM Recovery message (From DDRM)	Remarks
Card problems on DDRM	Critical	Major	Minor				
Line is defined but there is no H/W				+	Not affected	+	
Line is defined but there is wrong card				+	Not affected	+	
Hazard / Babbling				+	Not affected	+	

Table 1: Alarm - Severity

Card problems & subscriber alarms on DDRM	Alarm severity Class			Modified DMS-X/ LCM report message (From DDRM)	DDRM state	Modified DMS-X/ LCM Recovery message (From DDRM)	Remarks
Card problems on DDRM	Critical	Major	Minor				
ETM card		+		+	ISTB	+	If there is no ETM option datafill on DMS then DDRM does not send this alarm even if ETM module exists and / or it has a problem. If there is ETM option datafill on DMS but there is no ETM module on DDRM or there is a problem with it then ETM alarm is sent by DDRM. In this case test facilities are not supported for DDRM. The test attempts are failed and a proper prompt is given on DMS.
TBK card			+	+	ISTB	+	The message is received separately for each TBK card including the status of all TBK cards.

Note 1: If the DTC alarm message is received and there is no E1 link problem between this DTC card and DMS the alarm report message is expected from both units. The existing calls which are connected by this DTC card are released **by DDRM / DMS.** The related E1 links are taken from the service for not to assign a speech channel through them.

Note 2: The alarm report message is expected for the last available DTC card if there is at least one available E1 link.

Note 3: It is a Critical alarm for a single plane configuration.

Note 4: Subscriber alarm is expected for the cases; a- during the initializing phase b-RTS DRWR command c-TST DRWR command d-card out. The alarm severity class of the defined conditions for DDRM subscribers are based on the existing threshold value criteria on DMS as office based.

1.1.5 Module Alarm: GNS

If the CPUs can not be communicated on DDRM node, DMS is informed via the modified DMS-X / LCM message which is sent from DDRM. The CPUs can be on MXC, DTC and GNS cards of a DDRM node. The effect of the alarm changes based on the card type of CPU.
These type of problems are recovered on DDRM node itself.

DDRM is expected to drop the calls which are controlled with GNS in alarmed condition.

If the problem is with one of GNS card then DDRM node is out of order unless there is no standby of GNS card. If there is a standby GNS (double plane configuration) then the service facilities are given to the related modules over the standby GNS. The priority of the alarm is identified based on the message is for the last available GNS or not.

For "double plane" configuration;

- If modified DMS-X / LCM message is received for one of GNS card it means **a Major PM** alarm for DMS. A major alarm indication is seen on DMS and the state of DDRM node is changed to **ISTB** while both units are in INSV. The service facilities of DDRM subscribers are not effected. When the problem with GNS card is recovered then DDRM sends a new defined DMS-X / LCM message to DMS. If there is not another alarm or problem, "Major PM" alarm indication is cleared on DMS MAP and the state of DDRM node is changed to INSV again.
- If the 2nd of modified DMS-X / LCM message is received for the remaining GNS card it means a **Critical PM** alarm for DMS. A critical alarm indication is seen on DMS and the state of DDRM node is changed as **SYSB** on DMS. DDRM node stays in SYSB state until a message about the recovery of at least one GNS card is received. The existing procedures

on DMS for a critical PM alarm on a remote node is valid (call processing stops, state changes of DDRM node and its' subscribers etc). If at least one of GNS card problem is recovered DDRM sends a new defined DMS-X / LCM message to DMS. After that if there is not another alarm or problem, the state of DDRM is returned to ISTB from SYSB. If the problem with the 2nd GNS card is also recovered then the state of DDRM is changed to INSV from ISTB . Call processing and other service facilities continue as expected.

For "single plane" configuration if the modified DMS-X / LCM message is received for the problem on GNS card it means a **Critical PM** alarm for DMS. A critical alarm indication is seen on DMS and the state of DDRM node is changed as **SYSB** on DMS. DDRM node stays in SYSB state until a message about the recovery of the GNS card is received. The existing procedures on DMS for a critical PM alarm on a remote node is valid (call processing stops, state changes of DDRM node and its' subscribers etc)

When the problem is recovered then DDRM sends a new defined DMS-X / LCM message to DMS. If there is not another alarm or problem, **Critical PM** alarm indication is cleared on DMS MAP and the state of DDRM node is changed to INSV again.

The details of this alarm is queried via "QueryPM FLT" command on PM level.

1.1.6 Module Alarm : MXC

If there is a problem with MXC card then the subscribers which are on the same shelf with this MXC are not given any service. It means a **Major PM** alarm for DMS. DMS changes the state of DDRM node to **ISTB**.

*A*ll lines (LMB) , UTR , LTT, TMS , POC and RG cards on the shelf are out of service along the period of alarmed condition. The service facilities for the subscribers which are controlled by MXC cards on other shelves continue without any interruption.

MXC Alarms raise LC alarms on the shelf of the alarmed MXC and all datafilled lines on the shelf goes to LO until recovery of MXC alarms.

For all card alarms are displayed as MXC Alarmed once Query LC command is executed. All application that utilize utr ,ltt-tms functions are expected to check MXC alarms first : if MXC is alarmed, the application assume that other cards relevant with the shelf of MXC alarmed are out of service.

If MXC alarm is recovered , all LC alarms of the cards that equipped on the shelf of MXC are cleared at DMS, all equipped/datafilled lines goes to IDLE. Other card status are returned to the status that is set prior to MXC Alarm. And DDRM is expected to reports the alarms after rescan is done once MXC recovers on DDRM. (LTT/TMS, UTR, POC and RG) .

The modified DMS-X / LCM message is seperately received for each MXC card problem and DDRM state is ISTB. If all MXC cards on a DDRM node have problem then all subscribers are effected and it means a **Critical PM** alarm for DMS. The state of DDRM node is changed as SYSB on DMS. The existing behaviors of DMS will be kept for line states.

When the problem with the MXC card is recovered DDRM sends the modified DMS-X / LCM message to DMS. This message is seperately sent for each MXC card. After that if there is not another alarm or problem the line states of subscribers are changed automatically and the service facilities of subscribers which are controlled by this MXC are started. The state of DDRM node stays in ISTB until the problems for all MXC cards are recovered in case that no another ISTB reasons exist.

The details of this alarm is queried via "QueryPM FLT" command on PM level. All cards are displayed as MXC Alarm or the current alarms are masked with MXC Alarm when DDRM reports MXC Alarm exception message. Upon receiving Recover Message, masks on the current alarms disappeared and previous alarm are displayed if no recover message is received regarding to the previous alarm.

1.1.7 DTC Problems

1.1.7.1 DTC Hardware and Setup Configuration on DDRM

The sharing of E1 link indexes according to 2 DTC card and 4 E1 link configuration on DDRM :

- **The E1 links with 0th and 2nd indexes** are connected to DTC 0 and they are assumed as Unit 0. The 1st channel of E1 primary link (with 0th index) is the messaging channel.
- **The E1 links with 1st and 3th indexes** are connected to DTC 1 and they are assumed as Unit 1. The 1st channel of E1 primary link (with 1th index) is the messaging channel.

The number of message channels for DDRM are based on DTC card configuration as defined below;

- **2 DTC card with 2 / 1 E1 links -** Each DTC has one message channel and each DTC card means a unit of DDRM node
- **1 DTC with 2 E1 links -** This DTC card has two message channels and each E1 means a unit of DDRM node
- **1 DTC with 1 E1 link -** This DTC card has one message channel and only one unit of DDRM is in-service. This means that DDRM node is in takeover mode.

At least one DTC is expected on DDRM side. If one of two messaging channels are full then takeover occurs and the subscribers on this unit are given their service facilities over the other units' message channel. If the speech channels of a unit is full other unit's speech channels are used. But its' message channel is in-service and DMS sends the messages over the available 2 message channels.

See Table 2 on page 36 for the number of E1 link and message channels based on the relation between DMS datafill and DDRM configuration.

Table 2: DDRM units based on the DTC & E1 datafill on DMS and DDRM configuration Table 1

DMS datafill	DDRM config	DDRM Unit 0	DDRM Unit 1	Remarks
DTC 0 : 2 E1 DTC 1 : 2 E1	DTC 0 : 2 E1 DTC 1 : 2 E1	INSV (One message channel & 2 E1 link)	INSV (One message channel & 2 E1 link)	
DTC 0 : 1 E1 DTC 1 : 2 E1	DTC 0 : 1 E1 DTC 1 : 2 E1	INSV (One message channel & 1 E1 link)	INSV (one message channel & 2 E1 link)	
DTC 0 : 1E1 DTC 1 : 1 E1	DTC 0 : 1E1 DTC 1 : 1 E1	INSV (one message channel & 1 E1 link)	INSV(one message channel & 1 E1 link)	
DTC 0 : 2 E1 DTC 1 : 1 E1	DTC 0 : 2 E1 DTC 1 : 1 E1	INSV (one message channel & 2 E1 link)	INSV (one message channel & 1 E1 link)	
DTC 0 : 2 E1 DTC 1 : -	DTC 0 : 2 E1 DTC 1 : -	INSV (one message channel & 1 E1 link)	INSV (one message channel & 1 E1 link	
DTC 0 : - DTC 1 : 2 E1	DTC 0 : - DTC 1 : 2 E1	INSV (one message channel & 1 E1 link)	INSV (one message channel & 1 E1 link	
DTC 0 : 1 E1 DTC 1 : -	DTC 0 : 1 E1 DTC 1 : -	INSV (one message channel & 1 E1 link)	MANB / CBSY	
DTC 0 : - DTC 1 : 1 E1	DTC 0 : - DTC 1 : 1 E1	MANB / CBSY	INSV (one message channel & 1 E1 link	
DTC 0 : 2 E1 DTC 1 : 2 E1	DTC 0 : 1 E1 DTC 1 : 1 E1	ISTB (One message channel & 1 E1 link	ISTB (One message channel & 1 E1 link)	DDRM does not send an E1 alarm for DTC 0 & DTC 1.
DTC 0 : 2 E1 DTC 1 : 2 E1	DTC 0 : 1 E1 DTC 1 : 2 E1	ISTB (One message channel & 1 E1 link)	INSV (One message channel & 2 E1 link)	DDRM does not send an E1 alarm for DTC 0.

Table 1

DMS datafill	DDRM config	DDRM Unit 0	DDRM Unit 1	Remarks
DTC 0 : 2 E1 DTC 1 : 2 E1	DTC 0 : 2E1 DTC 1 : 1E1	INSV (one message channel & 2 E1 link)	ISTB (One message channel & 1 E1)	DDRM does not send an E1 alarm for DTC 1.
DTC 0 : 2 E1 DTC 1 : -	DTC 0 : 2 E1 DTC 1 : 2 E1 / 1 E1/ -	INSV (one message channel & 1 E1 link)	INSV (one message channel & 1 E1 link	Both E1 links should be connected to DTC 0. DTC 1 is not configured on DDRM.
DTC 0 : 2 E1 DTC 1 : -	DTC 0 : 1 E1 DTC 1 : 2 E1 / 1 E1/ -	ISTB (one E1 is available & 1 E1 link)	MANB / CBSY	E1 link should be connected to DTC 0. DDRM does not send an E1 alarm for DTC 0. DTC 1 is not configured on DDRM.
DTC 0 : 1 E1 DTC 1 : -	DTC 0 : 2 E1 DTC 1 : 2 E1 / 1 E1 / -	ISTB (one mesage channel & 1 E1 link)	MANB / CBSY	DTC 1 is not configured on DDRM.
DTC 0 : - DTC 1 : 2 E1	DTC 0 : 2 E1 / 1 E1 / - DTC 1 : 2 E1	INSV(One message channel & 1 E1 link)	INSV (one message channel & 1 E1 link	Both E1 links should be connected to DTC 1. DTC 0 is not configured on DDRM.
DTC 0 : - DTC 1 : 2 E1	DTC 0 : 2 E1 / 1 E1 / - DTC 1 : 1 E1	MANB / CBSY	ISTB (one message channel & 1 E1 link)	E1 link should be connected to DTC 1. DDRM does not send an E1 alarm for DTC 1. DTC 0 is not configured on DDRM.
DTC 0 : - DTC 1 : 1 E1	DTC 0 : 2 E1 / 1 E1 DTC 1 : 2 E1	MANB / CYSB	ISTB (one message channel & 1 E1 link	E1 link should be connected to DTC 1. DTC 0 is not configured on DDRM.

Table 1

DMS datafill	DDRM config	DDRM Unit 0	DDRM Unit 1	Remarks
DTC 0 : - DTC 1 : -	**Not allowed configuration on DMS**			

ISN09 Table Control SW is enhanced and new optional keys are defined to configure DTC cards. New tuple will be in following format :

DTC0/1_values can be 0, 1, 2 as corresponding to SINGLE, DOUBLE, NONE in order.

DDRM needs two messaging channels at least. LCMINV allows user to datafill C-side ports of DDRM connected to PLGC and forced to datafill the first two ports. Those two ports are indicated as Messaging E1 and carry the messaging channel for units , seperately. E1-0 for unit0 , E1-1 for unit1.

At least one DTC must be datafilled otherwise add/change fails in datafill on LCMINV.

When DTC0=0/2 (Single/None) and DTC1=2/0 (None/Single,) Table Control SW produces a warning ('UNIT-.... CANNOT BE INSV/ISTB') & ('UNIT-.. TAKEOVER') accordingly.

New enhancements allows user to define DTC Number and Channel Configuration as shown below :

Table 3: LCMINV DTC vs Channel Configuration

DTC0	DTC1	DTC0 1th E1	DTC0 2nd E1	DTC1 1th E1	DTC1 2nd E1
DOUBLE	-	M	M	-	-
-	DOUBLE	-	-	M	M
DOUBLE	DOUBLE	M	S	M	S
DOUBLE	SINGLE	M	S	M	-
SINGLE	DOUBLE	M	-	M	S
SINGLE	SINGLE	M	-	M	-

Table 3: LCMINV DTC vs Channel Configuration

DTC0	DTC1	DTC0 1th E1	DTC0 2nd E1	DTC1 1th E1	DTC1 2nd E1
SINGLE	-	M	-	-	-
-	SINGLE	-	-	M	-

SINGLE : it present capacity covering 1 message channel and 29+30= 59 Speech Channels on the DTC (with HDLC)

DOUBLE: It presents the capacity covering 2 Message Channels and 29+29 Speech Channels on the 2xE1 DTC (with HDLC)

M : Messaging Channel

S: Speech Channel

DDRM has configured the channels according to the above table during RTS. If no DTC card exists on the slot phsically against the configuration, no alarm is needed to fail the RTS for unit : it is expected that DMS cannot communicate with DDRM and RTS cannot start for this specific unit.

RTS fails for the unit for which DTC Mismatch is reported. RTS logs the fail reason for related DTC.

1.1.7.1 DTC Alarm Handling

DTC Unsolcited Exception Reports cause to log the alarm and display via QueryPM FLT on DMS. Each DTC Alarm causes to down the relevant unit according to the datafill in LCMINV. Recovery message causes to cleanup the alarm : closed E1s are opened within the system recovery started by DMS.

An special (rare) exceptional condition may occur when any DTC loss the connection with other module cards : in this case DDRM is expected to close the M+S Channels of unit which the DTC is alarmed and associated with for that reason. DDRM needs to know this condition and doesnt produce virtual module alarms. DMS needs to close this link so this can be achieved to stop the carrier maintenance on this E1 so DMS disconnects the existing calls in TakeOver mode. If other DTC detects this special condition on the DTC and sent the DTC alarm , DMS will drop the unit and takeover is realized.

For the configurations with 2 DTC cards if there is a problem with one of DTC card the service facilities for DDRM node and its' subscribers are given through the remaining DTC card. It means a **Major PM** alarm for DMS. The related unit of DDRM is set to CBSY / SYSB and the state of DDRM node is changed to **ISTB**. When the problem is recovered the recovery alarm message is sent from DDRM through the available DTC card. If there is not another alarm or problem the state of DDRM node is changed to INSV again.

In case the alarm message is received for the 2nd or for the last available DTC card this means a **Critical PM** alarm for DMS. The state of DDRM node is changed to CBSY / SYSB. If it is allowed on DMS and at least one UTR card is available, ESA-mode is entered on DDRM node.The recovery alarm message is not expected for the first DTC availability. In this case the general DMS-X/ LCM messaging is expected during E1 link alignment as in the existing structure and ESA-Exit procedure is performed. But for the 2nd DTC availability the recovery message is sent through the DTC card which is given into the service previously. If there is not other alarm or problem the critical alarm indication on DMS MAP is cleared. The state of DDRM node is changed to INS.

When DTC card alarm is received and if there is no E1 link problem between this DTC card and DMS the existing calls which are already established through this DTC card are released by DMS / DDRM. Also the related E1 links are taken from the service for not to assign a speech channel.
The details of this alarm is queried via "QueryPM FLT" command on PM level.

1.1.8 Card configuration Alarms

In generic this type of alarm is reported for the problems on peripheral cards of a DDRM node. LC, LTT-TMS and UTR cards are used as peripheral cards. These type of problems are recovered on DDRM node itself.

This message identifies the shelf and slot number and it means a **Major PM** alarm for DMS. A major alarm indication is seen on DMS and the state of DDRM node is changed to **ISTB**. The service facilities of DDRM subscribers are not effected except MTA test facilities.

When the problem with the LTT -TMS cards is recovered then DDRM sends the modified DMS-X / LCM message to DMS. If there is not another alarm or problem, the alarm indication on DMS MAP is cleared and the state of DDRM node is changed to INSV. After that MTA test facilities can be run again for DDRM subscribers.

The details of this alarm is queried via "QueryPM FLT" command on PM level. MTA tests which require LTT-TMS in are effected.

If the UTR cards on DDRM are not on the same slots which are configured on DMS DDRM sends the modified DMS-X / LCM message. This message identifies the shelf and slot number of UTR Card and it means a **Minor PM** alarm for DMS. A minor alarm indication is seen on DMS and the state of DDRM node is changed to **ISTB**. The service facilities of DDRM subscribers are not effected. This modified DMS-X / LCM message is seperately received for each UTR card.

When the message is received for the last remaining UTR card then the services which are given in ESA-mode are effected. It means a **Major PM** alarm for DMS. A major alarm indication is seen on DMS MAP and the state of DDRM node is changed to ISTB.

When the problem with UTR card is recovered then DDRM sends the modified DMS-X / LCM message to DMS. If there is not another alarm or problem, the indication on DMS MAP is cleared and the state of DDRM node is changed to INSV.
MXC recovery also cleanup the LTT , TMS, UTR and LC alarms if those cards are placed on the shelf of MXC.

The details of this alarm is queried via "QueryPM FLT" command on PM level.

LC Card faults :

The card configuration of DDRM node is sent from DMS during the initializing phase. Based on this information DDRM knows the occurance of the below cases and informs DMS via a modified DMS-X / LCM message for both conditions;

- The line is defined but there is no H/W on LC slot (**etc: card-out**)
- The line is defined but there is a wrong card on LC slot (eg. UTR or LTT / TMS)

The LC Message has not include any information of above conditions. DMS treat this alarm message as Missing Card Alarm Exception in DMS and MCARD RLCM Line Fault Alarm is raised. Existing RLCM Missing Card Alarm thresholds are kept.

When this message is received from DDRM the states of related lines will be set as LO on DMS
This alarm is also sent;

- during the initializing
- at the end of RTS drwr
- at the end of TST DRWR
- when the card is out of the LC slot

This message identifies the shelf and slot number of LC for 8 ports. When this message is received from DDRM node it causes LO for the lines on the LC of the message.

As an unexpected case if the line states can not be set to LMB because of any reason after the reception of this message from DDRM then the incoming call attempt to this subscriber is ended with **"Ring Failure"** message by remote node as response to **"Ring Request"**. Also DMS Line Audits follows the status of Line.

The details of this alarm is queried via "QueryPM FLT" command on PM level.

Upon receiption of LC Recovery message LO Lines returns to IDLE and ready for new calls.

1.1.9 POC alarm

This alarm indicates that the DC voltage level failure on POC card.

The modified DMS-X / LCM message is sent from DDRM and this message identifies shelf number of the POC card. When this message is received it means that there is no standby of +/-5v, +/-12v and -48v between two shelves. It is a Minor PM alarm for DMS. A Minor PM alarm indication is seen on DMS and the state of DDRM node is changed to ISTB.

Generally shelf 1 - shelf 2 and shelf 3 - shelf 4 have standby facility for each other.

This alarm is not service efective and service facilities are not impacted for DDRM node and its's subscribers unless the standby POC card has a problem.

If both POC cards are alarmed, then the subscribers which are on the same shelves with POC cards are not given any service facilities. In this case DDRM does not send standby POC alarm but sends a Module alarm for MXC cards on the same shelves. If both POC alarms are received for one unit, it means that one of those cards has virtual alarm since POC Alarm circuit can be broken for any reason.

If GNS cards are on the same shelves with these POC cards which have the problem then Module Alarm for GNS cards are received as well. Alarm severity class for MXC and GNS cards are valid.

If POC alarm for standby POC card is received because of any reason but not any other alarm condition (e.g about DTC,MXC & GNS) occurs then POC alarm is received by DMS but subscribers are expected to continue their service facilities as before this alarm. In this case craftperson is required to check the circuits before deciding to take the alarmed POCs off.

If the problem occurs on the last available POC card then the modified DMS-X / LCM message can not be reported because E1 links go down. It means a Critical PM alarm for DMS and DDRM state is SYSB.

These type of problems are recovered on DDRM node itself. When the problem is recovered DDRM sends the modified DMS-X / LCM message to DMS if there is not another alarm or problem. The alarm indication on DMS MAP level is cleared .For the modified message format of these alarm and their recovery message see Appendix chapter of DMS_DDRM.

If a MXC recovery message for the alarmed MXC card which is on the same shelf with POC card is received then POC card alarm is reseted on DMS. In case the continuity of POC card alarm DDRM sends this alarm to DMS again.

1.1.10 - 48 v alarm

There are two -48v input of DDRM node and they have standby facility for each other. This alarm indicates that there is a problem with one of -48v inputs and its' standby facility does not exist.

DDRM sends the modified DMS-X / LCM message and it means a Minor PM alarm for DMS. A Minor PM alarm indication is seen on DMS and the state of DDRM node is changed to ISTB.

This alarm is not service effective and service facilities are not impacted for DDRM node and its's subscribers unless the standby -48v input has a problem.

If both cards are reported as alarmed, the modified DMS-X/LCM message can not be reported because E1 links go down and a Critical PM alarm is seen on DMS. The state of DDRM node is changed to SYSB on DMS MAP level.
If -48v input alarm for standby is received because of any reason but not any other alarm condition (e.g about DTC,MXC & GNS) occurs then this alarm is received by DMS but subscribers are expected to continue their service facilities as before this alarm. DMS will clear the alarm when standby 48V alarm recovery message is sent by DDRM while node status is ISTB/INSV.

These type of problems are recovered on DDRM node itself. When the problem with one of -48v input is recovered DDRM sends the modified DMS-X / LCM message to DMS.If there is not another alarm or problem the alarm indication on DMS MAP level is cleared and the state of DDRM is changed to INSV.

The recovery message is not expected from DDRM for the 2nd -48v input problem in case of all E1s are down since SBSY Test Phase clear all the alarms and node will have INSV if all 48V alarm conditions are remove. Generally, DDRM is expected to rescan the alarms after it gains the activity with RTS.

MXC recovery cleanup the 48V alarms.

1.1.11 Ring alarm

POC cards on DDRM node provide Ringing as well. POC cards on shelf 1-shelf 2 and shelf 3 -shelf 4 have standby facility for each other. If there is a problem with a Ring Generator of these POC cards then the alarm is generated. DDRM sends the modified DMS-X / LCM message and it means a **Minor PM** alarm for DMS. A **Minor PM** alarm indication is seen on DMS and the state of DDRM node is changed to ISTB.

This alarm is not service effective and service facilities are not impacted for DDRM node and it's subscribers unless the standby card has a Ringing generator problem. If then a 2nd Ring alarm is received from DDRM and it means a **Major PM** alarm for DMS. DDRM state is ISTB at this condition and ***continue to give service to the lines even if terminations are without ring.***

In this case the subscribers which are on the same shelf are not given Ringing facility. There is not a direct relation with Ringing Generator problem and MXC, GNS alarms.
If all Riging Generators have problem for ringing application then it means a **Critical PM** alarm for DMS.

These type of problems are recovered on DDRM node itself. When the problem is recovered DDRM sends the modified DMS-X / LCM message to DMS. The alarm indication on DMS MAP level is cleared (If there is not another alarm or problem).
The details of this alarm is queried via "QueryPM FLT" command on PM level.

1.1.12 ETM / TBK Alarms

For the problems with ETM card and for its recovery the modified DMS-X / LCM messages are sent from DDRM.

If there is ETM option datafill on DMS but there is no ETM module on DDRM or there is a problem with it then ETM alarm is sent by DDRM. When this alarm message is received it means a **Major PM** alarm for DMS. A Major alarm indication is seen on DMS and the state of DDRM node is changed to ISTB. The test facilities are not supported for DDRM. If a test is attempted on DMS a proper prompt is given on DMS.

If there is no ETM option datafill on DMS then DDRM does not send this alarm even if ETM module exists and / or it has problem.

When the problem with ETM is recovered then DDRM sends the modified DMS-X / LCM message to DMS. If there is no another alarm or problem the alarm indication on DMS MAP is cleared and the state of DDRM node is changed to INSV. After that MTA test facilities can run again for DDRM subscribers.

The details of this alarm is queried via "QueryPM FLT” command on PM level.

If a TBK card is not on the slot or there is a problem with a TBK card then modified DMS-X / LCM message is received from DDRM. This message identifies TBK card number and it means a **Minor PM** alarm for DMS. A Minor alarm indication is seen on DMS and the state of DDRM node is changed to ISTB. This modified DMS-X / LCM message is seperately received for each TBK card. If a test is attempted on DMS then a failure prompt is given with a proper and existing reason on DMS. If a test is attempted a failure prompt with a proper and existing reason is given on DMS.

The service facilities of DDRM subscribers are not effected except MTA test facilities.The line test facilities are not supported for the related line cards.

When the problem with TBK card is recovered then DDRM sends the modified DMS-X / LCM message to DMS. If there is no another alarm or problem the alarm indication on DMS MAP is cleared and the state of DDRM

node is changed to INSV. After that MTA test facilities can run again for DDRM subscribers.

The details of this alarm is queried via “QueryPM TBK” command on PM level.

1.1.13 Hazard Alarms

If an overvoltage problem occurs on a subscriber with overvoltage option of DDRM then DMS is informed **via modified LCM Line Message .**When this message is received from DDRM the states of related lines will be set as HZD on DMS and existing Hazard DMS MTC is triggered. HZD condition is cleared after Modified Hazard DDRM Unsolicited message is received.

Also Hazard condition on DDRM lines with the overvoltage option is expected to be reported via an alarm message by DDRM node unless ETM option is used. If ETM option is used then HAzard alarm is sent for all line types by DDRM. In the existing structure of DMS severity of Hazard alarm is office-based not PM based and the alarm severity class is defined with threshold values as office based.

1.1.14 Severity on Display

The following existing LCM display is valid also for DDRM.

Table 1 Critical DDRM Alarm Display on DMS MAP

Alarm Display	CM	MS	IOD	Net	PM	CCS	Lns	Trks
	.	.	.	.	**nLCM** *C*	.	.	.
Indications on Display	“n” indicates the number of LCMs with alarms. “*C*” shows the alarm class “critical”.							

Major DDRM Alarm Display on DMS MAP

Alarm Display	CM	MS	IOD	Net	PM	CCS	Lns	Trks
	.	.	.	.	nLCM *M*	.	.	.
Indications on Display	“n” indicates the number of LCMs with alarms. “*M*” shows the alarm class “major”.							

Line Alarm Display on DMS MAP

Alarm Display	CM	MS	IOD	Net	PM	CCS	Lns	Trks
	.	.	.	.	.	.	MCard *M*	.
Indications on Display	"*M*" shows the alarm class "major".The number of alarm conditions reaches or exceeds the major class threshold.							

Hazard Line Alarm Display on DMS MAP

Alarm Display	CM	MS	IOD	Net	PM	CCS	Lns	Trks
	.	.	.	.	.	.	HZD *M*	.
Indications on Display	"*M*" shows the alarm class "major".The number of alarm conditions reaches or exceeds the major class threshold.							

1.1.15 Existing Line alarms on DMS

The existing line alarms on DMS are valid for DDRM subscribers as well. See Table 4 on page 47.

Table 4: Supported DDRM Line Alarms

Alarm Status Code	DDRM Action	Description	Remarks
DF	No.	Two or more line circuits have SDIAG, DIAG, NDIAG, FAC, MSET, MCARD, IMIN, IMAJ, UCARD, or QDIAG type alarms that are in the same class.	
FAC	YES	The relevant facility of DIAG tests are out of service this is reported in DIAG tests : etc subscriber loop tests	
DIAG	Yes.	The threshold of line circuits that have failed the extended diagnostic has been reached or exceeded.	Raised as a result of DDRM Line Diagnostic Tests

Alarm Status Code	DDRM Action	Description	Remarks
HZD	Yes	Indicates that a line hazard such as leakage resistance or foreign line voltage has been detected on a card. It also indicates that the cut-off relay has been operated to isolate the line card.	Unsolicited Message from DDRM trigger this alarm or Raised as a result of DDRM Line Diagnostic Tests
IMAJ	Yes	The threshold of line circuits that have reported ICMO at the major rate has been reached or exceeded. ICMO (incoming message overload) is the state where LTC or LGC is receiving too many messages from line card.	This is part of results of DDRM Line Diagnostics (ltp:diag) DMS follows up these errors via Babbler Audits. If DDRM reports balling via Babbling DDRM Alarm, this is raised.
IMIN	Yes	The threshold of line circuits that have reported ICMO at the minor rate has been reached or exceeded.	This is part of results of DDRM Line Diagnostics (ltp:diag)
MCARD	Yes	The threshold of line circuits that have reported missing line cards has been reached or exceeded.	This is part of results of DDRM Line Diagnostics (ltp:diag). This is also raised by LC Alarm Message.
MSET	Yes	The threshold of line circuits that have reported missing sets has been reached or exceeded.	Raised as a result of DDRM Line Diagnostic/ Tests
PSDF	No	On or more line circuits have reported a PSPD type alarm, and one or more line circuits have reported SDIAG, DIAG, NDIAG, FAC, MSET, MCARD, IMIN, IMAJ, UCARD, or QDIAG type alarms, where all alarm types (including the PSPD type) are in the same class.	

Alarm Status Code	DDRM Action	Description	Remarks
PSPD	No	The threshold of lines with a permanent signal condition has been reached or exceeded. The cause may be either partial dialing of a digit sequence or an off-hook condition with no digits dialed.	This is triggrered with LO trunks - related to callp on PLGC
QDIAG	No	The threshold of line circuits that are in the shower queue has been reached or exceeded.	
CMIN	No	The threshold of line circuits that have reported CP errors at the minor rate has been reached or exceeded.	
CMAJ	No	The threshold of line circuits that have reported CP errors at the major rate has been reached or exceeded.	

1.1.16 The other existing RLCM specific alarms which are not used for DDRM

The existing RLCM specific alarms which are not used for DDRM are listed below;

- RMM Minor
- ESA Minor
- ESA Critical
- EXT FSP RLCE frame Major

1.1.17 LOGs

Except LC Alarms (LC Configuration, Hazard, Babbling) each DDRM Exception Report are logged with PM179: PM179 Log format has the following information:

- Message Type (recovered or alarmed)
- Card Type
- Shelf

- Slot
- If alarm is LC, HW Status Value (note that this field is valid for Babbling and Hazard for ISN09. Online, Missing and Wrong Card may be printed, however it has no meaning.) is printed as second line.

1.1.18 ALARM EXCEPTIONS

- Unexpected values in the fields of exception reports cause PM116 Logs will be produced. SW Swerrs are produced to debug the unexpected value or range. In those cases message is ignored and not registered as alarm or recovered. Printing of PM116 matches the existing behavior of DMS against the RLCM exception reports.
- Any other problems in handling messages (etc exhaust resource due to excessive messages) causes PM116 again.
- After validation, RECOVER reports are accepted if only previous alarm status is TRIGGERED otherwise the message is ignored.No swerr is printed.PM116 is logged.
- After validation, TRIGGER message are received for a card which is already marked as ALARMed, this message is ignored. No Swerr is printed. PM116 is logged.

1.1.19 DDRM OM

This component refers a standard enhancements to pre-existing defined LCM OM definition. There is no requirement to have new OM types.

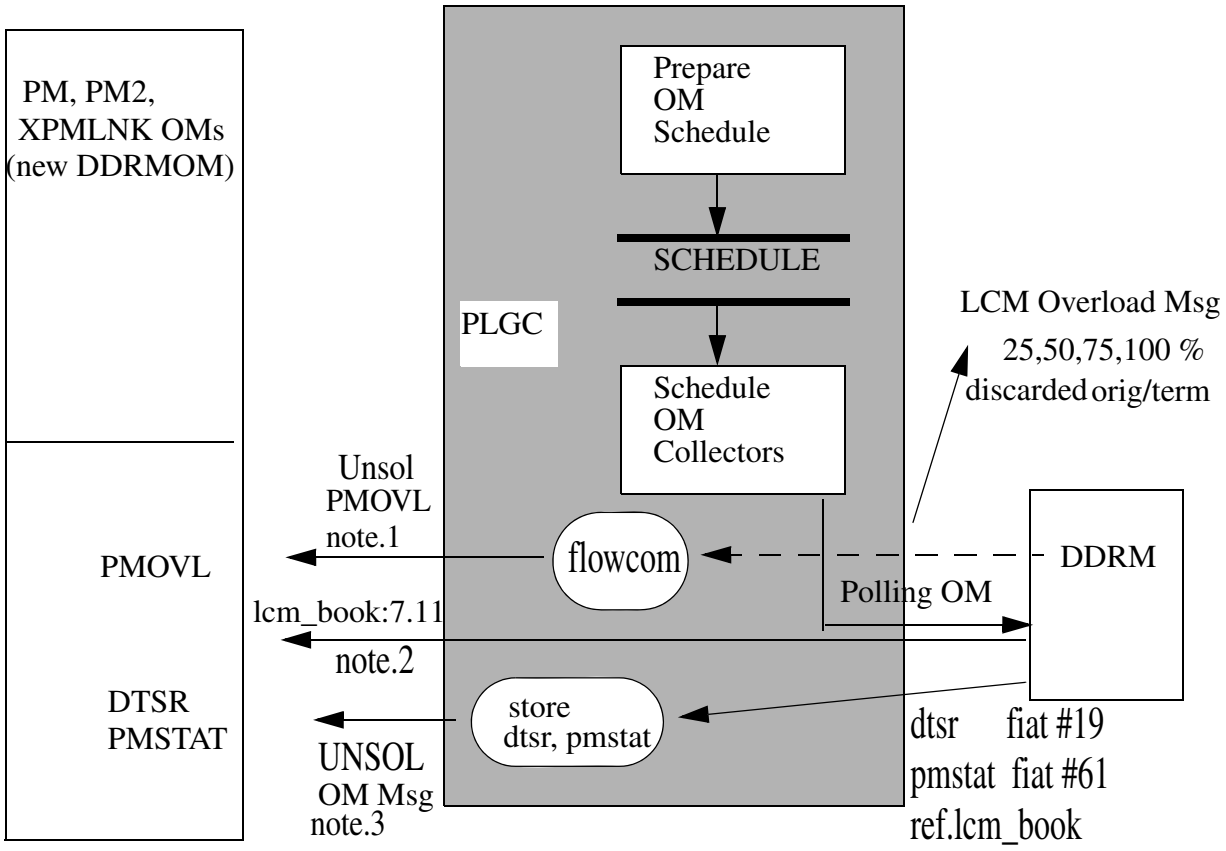
All exception alarms are pegged as PM OMs in the same way RLCM Alarms are received.

Existing DTSR and PMSTAT, PMOVL OM handling is given the following figure.

Among those OMs, Host PLGC sends regular query messages to collect the total calls for a period and delay-dial istatistics from DDRM: remote is expected to calculate the dial delays with the help of timestamps of call-origination previously sent by host to DDRM in a message. For complete description, please refer to NTP and DMS_DDRM references. DDRM doesn’t provide those delays, so DTSRs are invalid for DDRM.

DMS is ready to produce DDRM PMOVL OMs in case DDRM simulate or actually get an extion for an overload condition as it produces the relevant messages as defined for RLCMs. DMS existing handling is kept but those OM formats are changed to cover new PM type.

Figure 3 OM Design MAP



Note.1--- Per denied originitaion and terminations XPMOVL

Note2--- This unsolicited message is sent to the XPM from the LCM to indicate that the LCM is being overloaded with call originations, terminations, etc. and thus not processing all DMSX messages that are being sent to it due to a lack of call processing resources.

Note3. (DTSR : Dial Tone Statistic Request Fiat #19) & (PMSTAT: Processor Occupancy Status LCM messages (LCM_BOOK fiat: mf_pmstat_re #61)) is handled if DDRM provides or need those messages.

1.2 Hardware Requirements or Dependencies

Figure 2 Logical view of DMS host and DDRM node

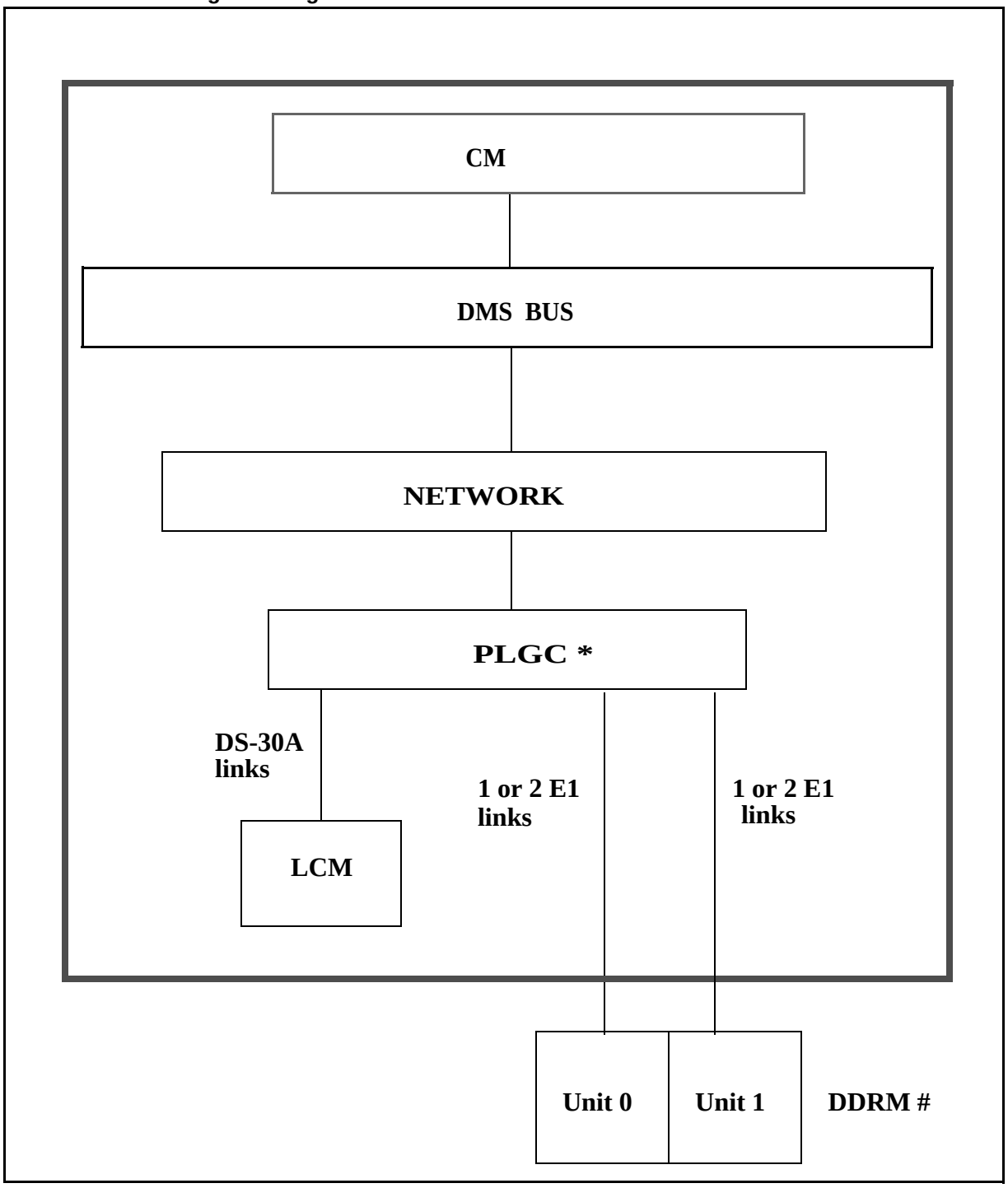
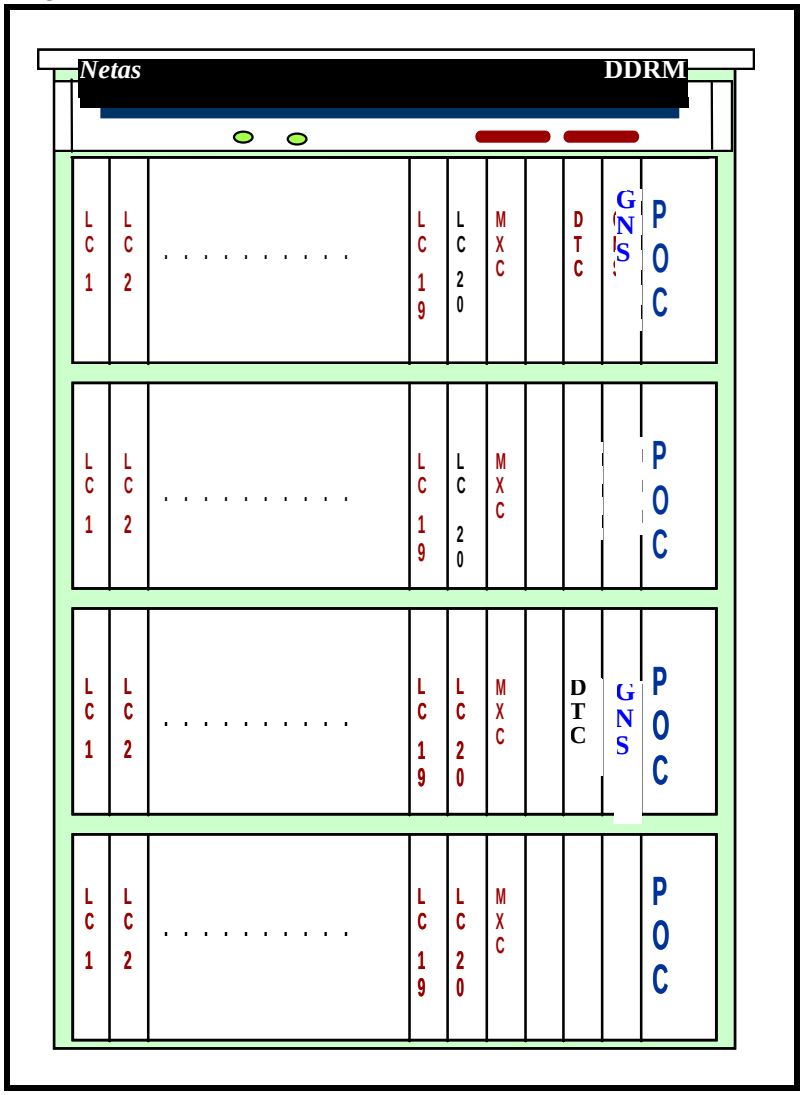


Figure 2 DDRM with one cabinet



1.1 Software Requirements or Dependencies

This feature needs DDRM Hardware and DDRM SW which works at least with single E1 links at worst case. Two-links configuration are needed for recovery phase since DMS doesn't change single UNIT of DDRM.

- A00006660 - for DDRM TABLE CONTROL and resources for ALARM

- A00006661 -for DDRM Maintenance RTS to query alarms.
- A00006662 - for Definition & Maintenance - Line Audits.
- A00006666 - for XPM support and Callp to handle alarms during INSV

1.2 Limitations and restrictions

- DMS Existing Audits or no new Audit/Recovery does not detect or recover the long-term alarmed condition. CraftPerson can refresh DDRM DMS alarms by RTS or TEST if both units are out of service when the alarms remains long-term because of any missing recovery message from DDRM.

1.3 Interactions

This activity impact TEST and ESA Activities which are being implemented at ISN09: tests for allowable cards are exhibited if any LC alarm.

1.4 Glossary

Term	Description
DDRM	DMS Dicle Remote Module
DRX-4	Dicle Rural Exchange-4
DTC	Digital Trunk Card
ESA	Emergency Stand Alone
GNS	Group Network Switching
LC	Line Card
LCM	Line Concentrating Module
LTT	Line and Trunk Test Simulator
MTA	Metallic Test Access
MXC	Module Switching Controller
POC	Power Converter Card
RLCM	Remote Line Concentrating Module
TMS	Test Measurement and Signalling
ETM	External Test Module
TBK	Test Connection Card

2: Functional Description (FN): A00006664

2.1 Feature name and Feature ID

A00006664 - DDRM Line Testing

DDRM (DMS Dicle Remote Module) project as a whole provides a platform which supports DDRM node as a remote line module of DMS like an RLCM (Remote Line Concentrating Module).

This feature is responsible of support the LTP level test commands of the posted DDRM subscriber lines on a regular MMP switch for ISN09 stream.

2.2 Description

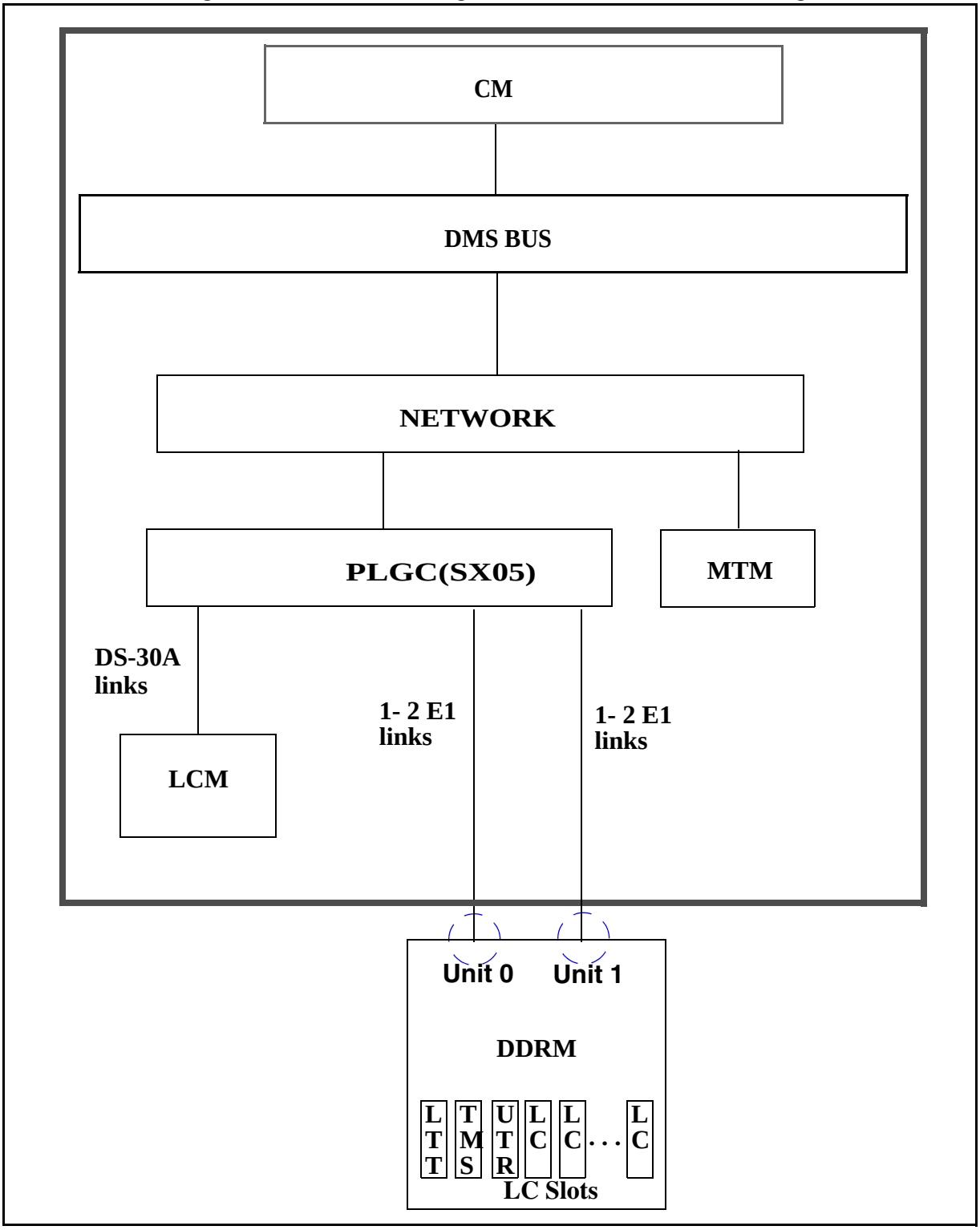
This feature provides support in DMS-MMP product for line testing available in DDRM. The main purpose of this feature is to create an interface between DMS and DDRM through E1 (PCM30) links to execute supported LTP and ALT level test commands for the posted DDRM subscriber lines.

Line test functions are accessed through the LTP (Line Test Position) level of MAPCI, facilitate the basic measurements and monitoring capabilities necessary to maintain DDRM subscriber lines from the DMS. DDRM is triggered to perform these functions by suitable DMSX messages via PCM30 interface.

Related metallic test measurements are performed by the LTT and TMS cards configured in DDRM node instead of RMM (Remote Maintenance Module) of RLCM (Remote Line Concentrating Module). Those are driven by DDRM software. The main responsibility of this feature is to form an interface between the DMS and DDRM node (i.e. requesting test proper test commands supported by DDRM, and receiving the results and interpreting them on DMS).

Functional configuration view is given in Figure 1, on page 56

Figure 1 Functional Configuration view of DDRM line testing



2.2.1 Supported DDRM Line Tests

DDRM line tests which are issued commands on LTP MAP level in DMS are applicable for only testable line card types. For other DDRM line card types, the command is prompted like that:

‘Command is not valid on this type of DDRM line.’

The test items supported by DDRM lines are listed in Table 1, on page 57.

Table 1 The line types and the supported DDRM test items by them

Test Item	DRBLCN	DRMLCN	DRBLCP	DRDLCP	DRMLCP
Line Manual Busy	+	+	+	+	+
Return to service	+	+	+	+	+
Forced Release & Manuel Busy	+	+	+	+	+
Digit Test from subscriber	+	+	+	+	+
Line Test (LNTST)				+	+
DC Voltage				+	+
AC foreign voltage				+	+
Loop resistance test				+	+
Continuity (Capacitance test)				+	+
LTA-Line Test Access	+	+	+	+	+
Tone sending to subscriber	+	+	+	+	+
Ring voltage application/test				+	+
Line return loss	+	+	+	+	+
Weighted circuit noise	+	+	+	+	+
RlsConn-Release connection	+	+	+	+	+
Onhook balance network test(BAL)	+	+	+	+	+
Onhook/Offhook balance network test(BALNET)	+	+	+	+	+
Talk Line Test Access	+	+	+	+	+
Monitor Line Test Access	+	+	+	+	+
Line Card Diagnostic					

Test Item	DRBLCN	DRMLCN	DRBLCP	DRDLCP	DRMLCP
Loop Detector Test				+	+
Metering pulse level / frequency					+
Automatic Line Test					
ALTBAL	+	+	+	+	+
ALTDIAG				+	+
ALTLIT				+	+

DRBLCN: Basic Line Card

DRMLCN: Basic Line card with metering

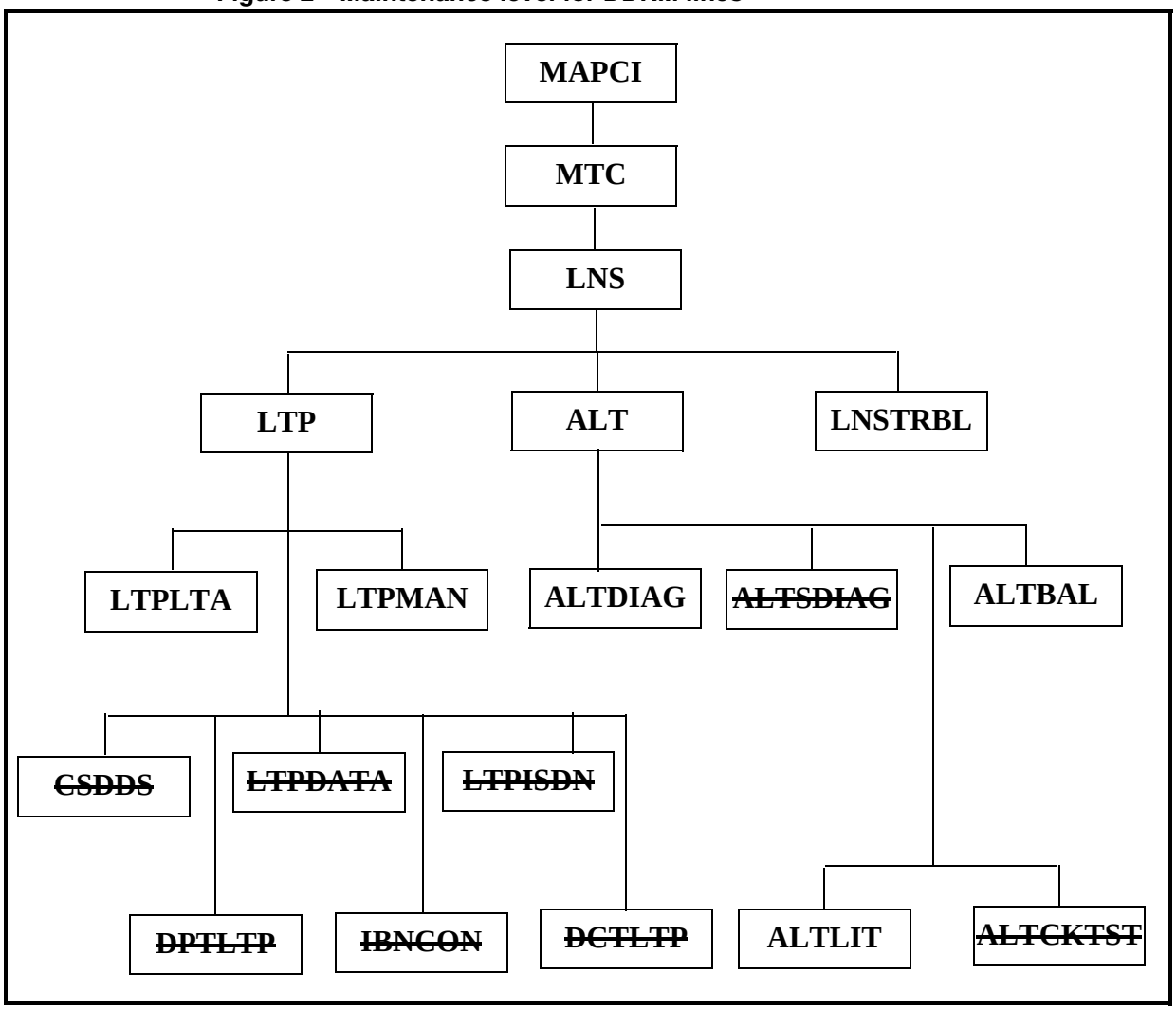
DRBLCP: Basic Line card with protection

DRDLCP: Basic Line card with test and over voltage

DRMLCP: Basic Line card with metering, test and over voltage

In DMS100-MMP product, the supported MAPCI;MTC;LNS levels are shown in Figure 2 on page 59. The levels and sublevels in strikethrough are not supported for DDRM subscriber lines.

Figure 2 Maintenance level for DDRM lines



The supported line tests for DDRM subscriber lines listed in Table 1, on page 57 are located in MAPCI;MTC;LNS;LTP and MAPCI;MTC;LNS;ALT levels.

2.2.1.1 Line Test Position (LTP) Level

Figure 3, on page 60 shows the supported LTP MAP level commands. Supported line tests listed in Figure 3, on page 44 are shown in **bold**.

Figure 3 Supported LTP level Commands (in bold)

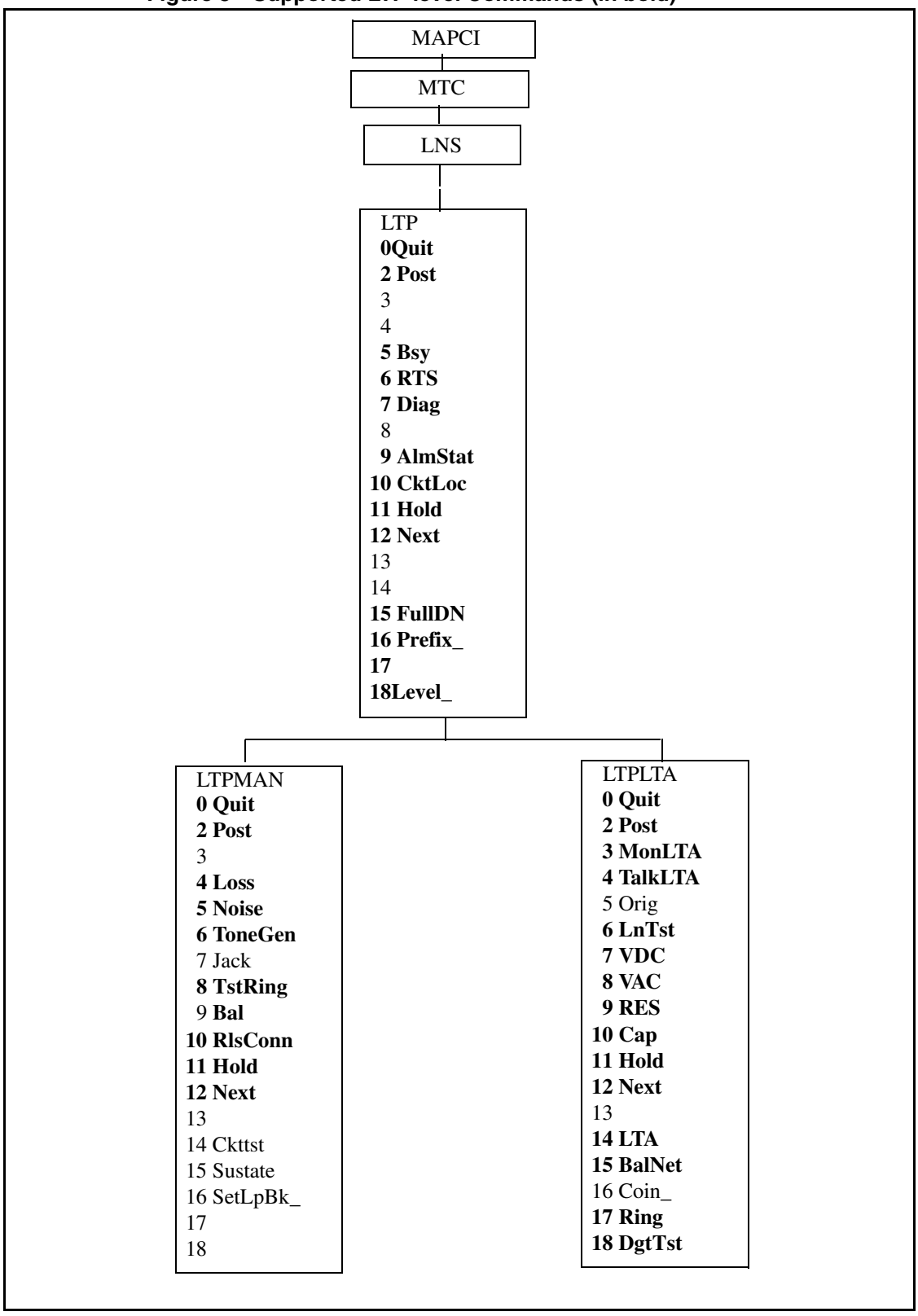


Table 2 A brief description of Supported LTP level commands for DDRM lines

Menu Item	Command	Function	Remarks
LTP 0	Quit	Return to the LNS level.	See Note 3 See Note 9
LTP 2	Post	Posts a line or set of lines to the LTP.	See Note 3 See Note 9
LTP 5	Bsy	Changes the state of the line in the control position, or optionally the complete set of posted lines, from IDL to MB.	See Note 1 See Note 9
LTP 6	RTS	The RTS command changes the state of the line in the control position, or optionally the complete set of posted lines, from MB to IDL.	See Note 1 See Note 9
LTP 7	Diag	Diagnose the posted line. The loop detector test checks the ability of a DDRM line circuit to recognize an off-hook condition on a loop-start line. Supervision circuity responses are checked by DMS-100 switch for the correct status changes. The metering test tests DDRM line cards for the presence and suitability of the signal provided by the metering tone card.	See Note 5 See Note 8
LTP 9	AlmStat	Query or set the lines (LNS) alarm thresholds.	See Note 3 See Note 9
LTP 10	CktLoc	Physical location of posted line card.	See Note 3 See Note 9
LTP 11	Hold	Moves the line in the control position to a spare hold position, and the next line from the posted set, if any, to the control position.	See Note2 See Note 3 See Note 9
LTP 12	Next	Moves the line in a specified HOLD position to the control position, or replaces the line in the control position with the next line in the posted set. Replaces, saves or drops the replaced line.	See Note 2 See Note 3 See Note 9
LTP 15	FullDN	Display full national number.	See Note 3 See Note 9
LTP 16	Prefix_	Set/Clear DN Prefix.	See Note 3 See Note 9
LTP 18	Level_	Used to enter the various LTP levels.	See Note 3
Nonmenu Command	FRLS	This command is not visible at the LTP level. The FRLS command forcibly disconnects a line circuit from test equipment or any other circuit and changes its state to MB.	See Note 9

Menu Item	Command	Function	Remarks
LTPMAN 4	Loss	The LOSS command measures the insertion loss of a test tone sent from the subscriber end of a loop to the switch.	See Note 9
LTPMAN 5	Noise	The NOISE command measures the C-message weighted circuit noise on a subscriber loop.	See Note 9
LTPMAN 6	ToneGen	The TONEGEN command transmits a tone on a subscriber loop.	See Note 6
LTPMAN 8	TstRing	The TSTRING command tests the ringing relay in the line card for proper functioning.	See Note 8 See Note 9
LTPMAN 9	BAL	BAL command performs an on-hook balance network test on a subscriber loop. The command optionally updates the balance network value and loss pad value in the line circuit according to the test results.	See Note 9
LTPMAN 10	RlsConn	The RLSCONN command releases test equipment that is connected to line.	See Note 8 See Note 9
LTPLTA 3	MonLTA	The TALKLTA command connects a monitor circuit to a subscriber line.	See Note 9
LTPLTA 4	TalkLTA	The TALKLTA command connects a talk circuit to a subscriber line.	See Note 7
LTPLTA 6	LnTst	The LNTST command performs resistance, capacitance, and voltage tests on a line.	See Note 8 See Note 9
LTPLTA 7	VDC	The VDC command performs a dc voltage measurement on a subscriber loop.	See Note 8
LTPLTA 8	VAC	The VAC command performs an ac voltage measurement on a subscriber loop.	See Note 8
LTPLTA 9	Res	The RES command performs resistance measurements on a subscriber loop.	See Note 8
LTPLTA 10	Cap	The CAP command performs a capacitance measurement on a subscriber loop.	See Note 8
LTPLTA 14	LTA	Used with RLS parameter to release monitor connections to CPB lines.	See Note 8 See Note 9
LTPLTA 15	BALNET	The BALNET command performes a balance network test on a subscriber loop that is in either the onhook or ofhook mode.	See Note 9
LTPLTA 17	Ring	The RING command will send the appropriate signalling to the DDRM which will cause ringing to be sent to the subscriber.	See Note 5
LTPLTA 18	DgtTst	The DGTTST command tests the DIGITONE pad or dial on the subscriber station.	See Note 5 See Note 8

Menu Item	Command	Function	Remarks
Note 1: The BSY, RTS commands work as hidden commands from the subtending LTP levels, and operate the same as in the root LTP level. ***Note 2:*** The Hold and Next command on the subtending LTP levels operate the same as in the root LTP level. ***Note 3:*** The existing functionality remains for this command as respect of DDRM lines ***Note 4:*** Other LTP level menu commands aren't supported by DDRM lines. Other LTP nonmenu commands aren't supported by DDRM lines as well. ***Note 5:*** No optional parameter is supported for DDRM lines. ***Note 6:*** The metallic option for ToneGen is not supported for DDRM lines. ***Note 7:*** The battery option for TalkLTA is not supported for DDRM lines. ***Note 8:*** This command uses LTT/TMS test cards. ***Note 9:*** No parameter change has been done for this command.			

The diagnostic subtests for DDRM lines differs from the other POTS line types. The following subtests are supported by DDRM lines:

- loop detector test
- Metering test (only metering lines)

Other commands which are unsupported for posted DDRM lines are prompted on MAP like that:

'**Command is not valid on a DDRM line.**'

2.2.1.2 Automatic Line Testing (ALT) Level

Figure 4, on page 64 shows the supported ALT MAP level commands. Supported line tests listed in Figure 2, on page 59 are shown in **bold**. Other sublevels apart from ALTLIT, ALTBAL and ALTDIAG are not supported for DDRM lines.

For ALT tests test results are categorized as follows for RLCM and LCM lines; PASS, FAIL, N/A and TOTAL, the sum of PASS + FAIL+ N/A . When a LIT test is run for a DDRM line, either PASS, FAIL or N/A is incremented. In case of a failure caused by incompatible line card types N/A is incremented, in all other failure scenarios FAIL is incremented.

Figure 4 Supported ALT level Commands (in bold)

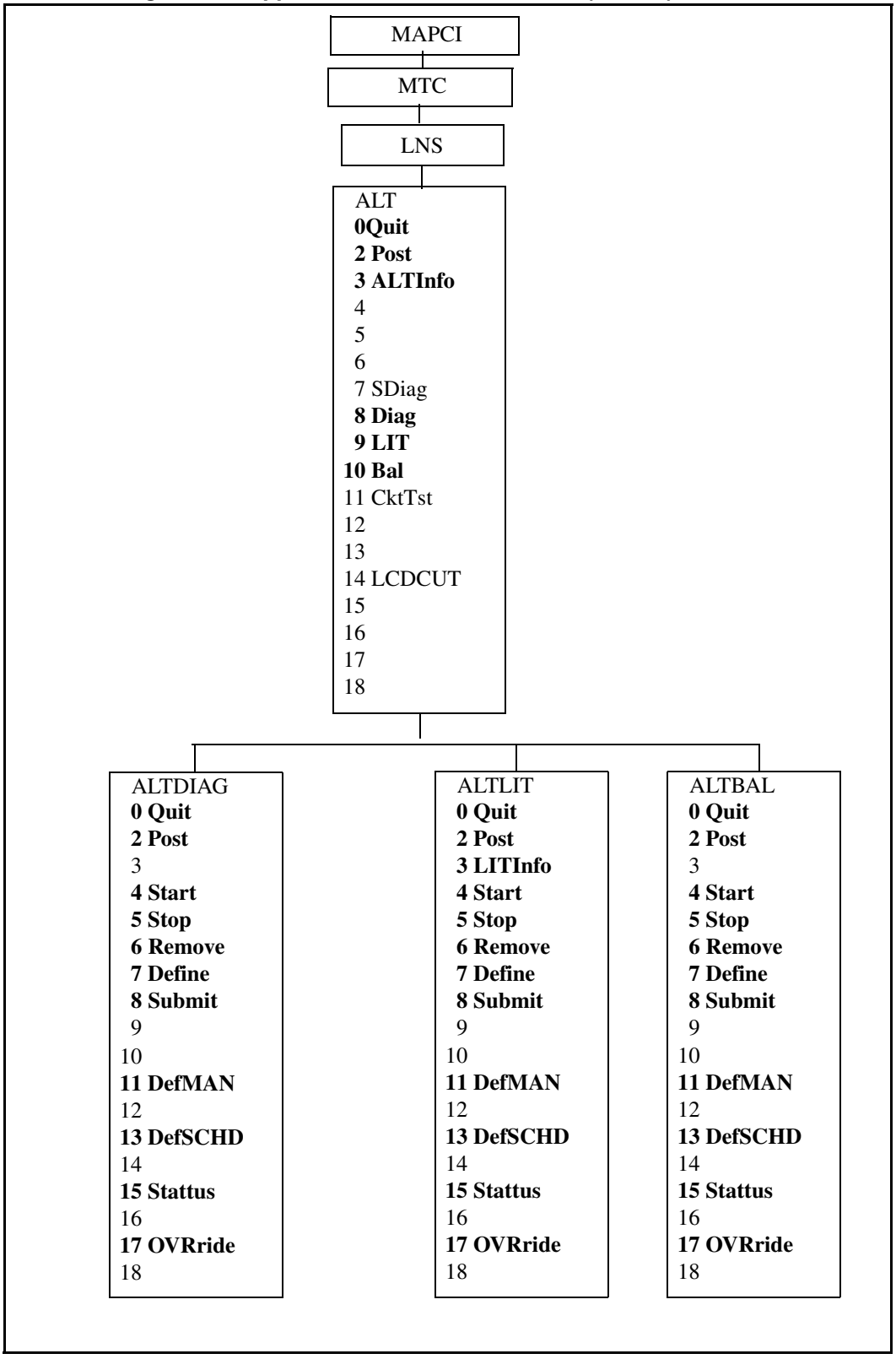


Table 3 A brief description of ALT level commands for DDRM lines

Menu Item	Command	Function	Remarks
ALT 0	Quit	The QUIT command causes the system to leave the current level and return to a higher level of the MAP.	See Note 1
ALT 2	Post	The POST command posts the scheduled ALT TESTID that is stored in memory (in Table ALTSCHED)	See Note 1
ALT 3	ALTInfo	The ALTINFO command checks test data stored in memory (Table ALTSCHED)	See Note 1
ALT 8	Diag	The DIAG command accesses the DIAG sublevel of ALT. If a TESTID is not entered as a parameter, a new TESTID must be defined with the DEFSCHD or DEFMAN command.	See Note 2
ALT 9	LIT	The LIT command accesses the LIT sublevel of ALT. If a TESTID is not entered as a parameter, a new TESTID must be defined with the DEFSCHD or DEFMAN command.	See Note 1
ALT 10	BAL	BAL command performs an on-hook balance network test on a subscriber loop. The command optionally updates the balance network value and loss pad value in the line circuit according to the test results.	See Note 1
ALTLIT 3	LITInfo	The LITINFO command displays the system default values for the LIT parameters.	See Note 1
ALTDIAG/ ALTBAL/ ALTLIT 4	Start	The START command sets the posted scheduled ALT test in a state such that it is ready to run at the next scheduled time.	See Note 1
ALTDIAG/ ALTBAL/ ALTLIT 5	Stop	The STOP command stops a test and changes the status of the TESTID.	See Note 1
ALTDIAG/ ALTBAL/ ALTLIT 6	Remove	The REMOVE command removes the data associated with the posted TESTID from memory (table ALTSCHED). If the TESTID is for a scheduled test, the system prompts for a YES or NO confirmation.	See Note 1
ALTDIAG/ ALTBAL/ ALTLIT 7	Define	The DEFINE command defines test data for the specified TESTID.	See Note 1
ALTDIAG/ ALTBAL/ ALTLIT 8	Submit	The SUBMIT command submits the defined test data for the posted TESTID into memory (table ALTSCHED).	See Note 1

Menu Item	Command	Function	Remarks
ALTDIAG/ ALTBAL/ ALTLIT 11	DefMAN	The DEFMAN command is used to assign a TESTID to the test that corresponds to the current ALT sublevel. For example, the DEFMAN command entered at the LIT level of MAP device number 7, will be assigned a TESTID of MANUAL07.	See Note 1
ALTDIAG/ ALTBAL/ ALTLIT 13	DefSCHD	The DEFSCHD command is used to assign a TESTID to the scheduled test that corresponds to the current ALT sublevel.	See Note 1
ALTDIAG/ ALTBAL/ ALTLIT 15	Stattus	The STATUS command checks the status of the posted TESTID.	See Note 1
ALTDIAG/ ALTBAL/ ALTLIT 17	OVRride	The OVRRIDE command overrides a scheduled test so that testing will not start until a specified day and time has passed.	See Note 1
Note 1: There is no change for this item. ***Note 2:*** DIAG test suits are changed for DDRM lines.			

2.2.2 Testing Procedures

DDRM line tests are categorized in 3 subset. Only Far-End Measurements require the involvement of the LTT and TMS cards. In other words measurements will be performed at DDRM. Other measurements are performed by DMS.

2.2.2.1 Near-End Measurements (LOSS, NOISE, TONEGEN)

These include the test commands which use the DMS-MTM testing facilities in LTPMAN sublevel. The result of the measurement resides till the craftperson releases the test.

Procedure for Near End Measurements

- Post DDRM line from the LTPMAN level.
- Perform the command. Observe the measurement on the MAP.
- Invoke RlsConn when complete to release test facilities.

2.2.2.2 Far-End Measurements (LNTST, VAC, VDC, RES, CAP, ALTLIT, TstRing)

Some tests require Metallic Test Access (MTA) provided by DDRM node. The LTP test commands are requested by LTP MAP level and DDRM performs them by using its LTT and TMS cards.

Procedure for Far End Measurements

- Post DDRM line from the LTPLTA level / for TstRing from LTPMAN level.
- Perform the command. Observe the measurements on the MAP.
- Invoke LTP RLS when complete to release test facilities (TstRing doesn't need manual release operation).

2.2.2.3 Line Monitoring (MonLTA, TalkLTA, Ring and DgtTst)

The LTPLTA commands MonLTA and TalkLTA establishes monitor and talk connections to DDRM subscriber lines in the MB and CPB state. If the line is in the MB state, a direct network connection between the headset and line is made. If the line is CPB, a connection between the line under test, the connected circuit, and the headset is set up through a 3-port conference circuit, and the line will enter the CPD state (DMS network connections to establish monitor/talk connections are used because of nonexistence of MONTALK card in DDRM).

The Ring command applies ringing current to a subscriber loop that has a monitor connection established. This enables the craftsperson at the switch monitoring a MB line to alert the subscriber or craftsperson in the field to go off-hook, allowing line quality to be monitored.

Procedure for DDRM line monitoring

1. Post DDRM line from LTPLTA level. If line is IDL, perform BSY command to place the line in the MB (Maintenance Busy) state.
2. Invoke MonLTA/TalkLTA command.
3. If line is CPB, connections through the 3-port circuit are made and line is monitored via the HSET. If line is MB, a network connection to the HSET is established, and the Ring command may now be entered to alert subscriber or craftsperson in the field.
4. To release connections, enter LTA RLS. The RTS command may be used for lines that are in the MB state.

   Note: DgtTst could not be invoked unless the talk connection is established. It may use DDRM testing facilities to detect digit tones.

New LTP level prompts are given in Table 4, on page 67 for DDRM lines.

Table 4 New Prompts for LTP level Test Commands for DDRM lines

No	Prompt	Description	LTP level Test Commands
1	"Command is not valid on a DDRM line."	The test command is not supported for DDRM lines.	All apart from Table 2.

Table 4 New Prompts for LTP level Test Commands for DDRM lines

No	Prompt	Description	LTP level Test Commands
2	“Command is not valid on this type of DDRM line.”	When the command is performed for unsupported line card (The test command may be supported for line card types with metering or over voltage).	LCO, Diag, TstRing, RlsConn, LnTst, VDC, VAC, Res, Cap, LTA, DgtTst
3	“Line state INVALID, must be MB or CPB”	The line state should be MB or CPB when establishing monitor or talk connection.	MonLTA, TalkLTA
4	“Conference circuit not available”	The conference circuit could not be established for monitor or talk connection.	MonLTA, TalkLTA
5	“Test could not be executed because LTT and/or TMS is not in a proper state. “	LTT/TMS test cards are not available for testing.	LCO, Diag, , RlsConn, LnTst, VDC, VAC, Res, Cap, LTA, DgtTst

2.1 Hardware Requirements or Dependencies

2.1.1 DDRM Line Cards (DRBLCN, DRMLCN, DRBLCP, DRDLCP and DRMLCP)

DDRM line tests are performed on the DDRM specific line cards as shown in Figure 1, on page 57 .

2.1.2 DDRM Test Cards (LTT, TMS and UTR)

In order to perform line test commands for DDRM lines; LTT, TMS and UTR cards should be plugged in DDRM LC slots. VDC, VAC, RES, CAP, LNTST, TstRing, LIT and DgtTst require these cards.

2.1.3 HSET Circuit (NT5X30)

The HSET trunk referenced for DDRM line monitoring is provided by the standard 5X30 101 Communications Test Line Circuit Card. TalkLTA, Ring and DgtTst commands need HSET circuit.

2.1.4 TTT Circuit (NT2X96)

The TTT trunk referenced for DDRM lines is provided by the standard 2X96 Circuit Card. ToneGen, Loss and Noise commands need TTT circuit.

2.1.5 TTU Circuit (NT2X47)

The TTU trunk referenced for DDRM lines is provided by the standard 2X47 Circuit Card. Diag command needs TTU circuit.

2.2 Software Requirements or Dependencies

This feature depends on the following features:

- AT.00006664 DDRM Node Definition and Provisioning
- AT.00006661 DDRM Node Maintenance
- AT.00006662 DDRM Line Definition and Line Maintenance
- AT.00006663 DDRM Alarms and Audits
- AT.00006666 DDRM XPM Support and Monitoring

2.3 Limitations and restrictions

- LTP MAP level support of diagnostic tests is supported by this feature. The subtests are implemented by AT.00006662.
- The state should be set to MB or CPB before establishing monitor or talk connection.
- LCO command is not allowed to the DDRM lines. Because of the fact that DDRM hardware does not support this requirement.
- For DRDLCP and DRMLCP type of DDRM lines, when VAC/VDC/CAP/RES test is applied with continuous parameter " **Continuous parameter is restricted for DDRM line.** " prompt is returned.
- Continuous parameter of diag test is not supported for DDRM lines.
- LTA command has three parameters. Namely IN, OUT, RLS. The expected behaviour in DMS is as follows; By LTA IN command mesaurements are done both on Line Card and on subscriber loop. By LTA OUT Line Card is isolated and mesaurements are done on subscriber loop. By LTA RLS the connections for tests are released. Due to the fact that DDRM is capable of performing tests only on subscriber loop, when LTA IN is performed " **LTA IN is not valid for DDRM lines, mesaurements can be done for LTA OUT only.** " prompt is returned.
- For LCM and RLCM lines 5 types of ALT subtests are available: ALTDIAG, ALTSDIAG, ALTBAL, ALTLIT, ALTCKTST. For DDRM lines ALTSDIAG is not supported because DDRM lines do not have two distinct DIAG sets. Other ALT subtests are available.
- When the LTT and/or TMS cards are not in a proper state for the tests which require the exsistence of LTT and TMS cards, " **Test could not be executed because LTT and/or TMS is not in a proper state.** " is returned.

- During the TSTRING test, ring will not be applied to the DDRM subscriber.

2.4 Interactions

2.4.1 AT.00006662 DDRM Lines Maintenance

The subtests of diagnostic are implemented by this feature.

2.4.2 AT.00006661 DDRM DDRM Node Maintenance

Existence of DDRM test cards in DDRM LC slots.

2.4.3 AT.00006663 DDRM Alarms and Audits

Existence of DDRM test cards in DDRM LC slots.

2.5 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface __X__

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

2.6 Glossary

Term	Description
DMS	Digital Multiplex Switch
MMP	Multi Market Product
XPM	Extended Peripheral Module
CM	Central Module
RLCM	Remote Line Concentrating Module
RMM	Remote Maintenance Module
DDRM	DMS Dicle Remote Module
MTM	Maintenance Trunk Module
MAPCI	MAP Command Interpreter
LTP	Line Test Position
LTPLTA	LTP Line Test Access
LTPMAN	LTP Manual
LTT	Line and Trunk Test simulator
TMS	Test Measurement and Signaling

2.7 Recommended Reading/References

a. DMS_DDRM DDRM (DMS Dicle Remote Module) Spec Document
b. A00006638 DMS - DDRM HLD
c. A00006664 DDRM Node Definition and Provisioning
d. A00006661 DDRM Node Maintenance
e. A00006662 DDRM Lines Inventory
f. A00006663 DDRM Alarms and Audits
g. A00006665 DDRM ESA Support
h. A00006666 DDRM XPM Support and Monitoring
i. AR1625 GPP Line Maintenance Phase 2

3: Functional Description (FN): A00006665

3.1 Feature name and Feature ID

A00006665 - DDRM ESA Support

3.2 Description

DDRM (DMS Dicle Remote Module), is a rural area exchange developed for Turkey Market. Because of DDRM deployment on the field, it is requested to maintain and administer DDRM related operations over DMS switches. By this way the benefits of DDRM in Turkey market will be enhanced and the demands from the customer to reuse these switches as remote modules will be satisfied.

The Emergency Stand Alone feature (ESA) allows lines attached to the same remote peripheral (DDRM) to establish calls within the remote peripheral, when the remote peripheral is disconnected from its host peripheral (PLGC).

DDRM is not equipped with a special card supporting the ESA option. The ESA software runs on the DDRM main processor.

When operating in the ESA mode, DDRM offers limited services to subscribers. Only basic line-to-line calls (for both DP and DTMF lines) are supported. Subscriber features and AMA call recording are not supported in ESA. In normal operation of DDRM UTR on PLGC is used in order to receive tones. UTRD on DDRM is needed on DDRM in ESA mode in order to support tones so if UTRD is not datafilled in LCMINV table, ESA datafill will be prevented in LCMINV. If UTRD is not existing on the DDRM although it is datafilled, alarm will be raised by the ddrm alarms and audits component. If DDRM is in ESA mode, DDRM itself will take all the actions.

When connection of E1 links between DMS and DDRM is lost for any reason DDRM enters ESA-mode if ESA related datafill is appropriate on DMS. DDRM node continues intra-remote calls in ESA-mode based on the information received from DMS with static data download.The other facilities like inter-exchange calls, supplementary services, metering and billing are not supported in ESA mode. In the existing structure of DMS; " ESA module is defined, loaded and maintained from DMS. The loading and maintenance processes are not valid any more for DDRM node. For definition process only indication of ESA and UTRD configuration is set in the inventory table where DDRM node is defined. " A dedicated channel, channel 3 of primary link is used for ESA messaging between ESA processor and host XPM, PLGC. But because of the system restrictions on DDRM channel 3 is not used any more for ESA messaging. Instead DMS-X message channel, channel 1 is used.

3.2.1 Feature Synopsis

With A00006665 DDRM ESA Support activity, the following ESA functional components are covered:

- LCMINV table control component
- DDRM ESA Entry/Exit Component.
- DDRM ESA Static Data Component
- DDRM ESA Inservice Troubles Component

Basic Differences of DDRM ESA component from RLCM ESA component could be summarized as fallows:

1) DDRM doesn't have ESA processor.

2) DDRM doesn't use channel 3 as messaging channel, instead it does use channel 1.

3) Unlike RLCM case, in DDRM case DMS doesn't download EXECS information since DDRM is supporting ESA on main processor.

4) DDRM doesn't need some tables, for ESA mode of operation, which are downloaded during static data download these are hunt group table, automatic line index table, prefix tables.

5)DDRM supplies tones by using UTRD in ESA mode, tones are supplied by tone & clock card in RLCM in ESA mode.

6) There is no need for XESAINV table in DDRM datafill on DMS since this table supports RLCM peripheral ESA processor related information.

7)For definition process only indication of ESA and UTRD configuration is set in the inventory table where DDRM node is defined.

8)UTR configuration - one LC slot on each shelf is generally used for UTR card and each shelf supports 152 subscribers. So 608 subscribers are supported for 4 shelf. It is not possible that one UTR card can serve all subscribers of a DDRM node during ESA mode. The subscribers which do not have UTR card on their shelves can not given their service facilities in ESA mode. But one UTR card is enough for line test facilites. In that case 632 subscribers aredefined for a DDRM node with 4 shelves.

3.2.2 ESA related configuration on DMS and LCMINV Table Control Changes

In the LCMINV table where DDRM node is defined there is a field which indicates ESA mode is supported or not. If the indication of ESA is Y then the related information for ESA is downloaded as static data from DMS to DDRM for basic intra-remote calls on DDRM. If the indication of ESA is N then ESA mode is not allowed on DDRM and the static data is not downloaded to DDRM. If ESA indication is changed from N to Y BSY/RTS of the RLCM is needed in order to download ESA data. XESAINV table is not needed for DDRM since it is used for ESA processor configuration in RLCM.

DMS will inform DDRM, if ESA equipment is available in the existing structure. if at least one UTRD and its datafil exists, DDRM will be ready to enter ESA mode after BSY/RTS operation. If ESA indication is N for DDRM this information is sent via a DMSX message in BSY/RTS time.

3.2.2.1 ESA related office parameters -

"LCM-ESA_ENTRY_BADCSIDE" and "RLCM_ESAENTRY_BADLINK" are used for DDRM ESA configuration. They are used to decide about ESA entry, DDRM processor will wait for defined threshold times for BADCSIDE and BADLINK conditions specified by these two parameters.

RLCM_ESA_NOTIFY_TONE is an office paramater and controls whether the subscriber hears a distinctive dial-tone burst during ESA mode. When this parameter is set to Y then ESA specific tone is expected to be applied by DDRM. Its frequency will be a multiple of 450 Hz. ESA mode is expected to be in control on DDRM side if a UTRD related alarm is received from DDRM and ESA related datafill on DMS as in the expected way.

If the ESA related configuration and datafill is appropriate for ESA, ESA field in table LCMINV is set to Y, then static data for ESA mode is downloaded in BSY/RTS time. It is expected that DDRM should route the calls based on these information and based on line states which are previously downloaded. Office parameter "RLCM_ESASDUPD_HOUR" is used to set the start time to download ESA static data to all remotes on host site. For nightly audit to run RLCM_ESASDUPD_BOOL should be set to Y in table OFCENG and the ESA field in table LCMINV for the specific DDRM should be set to Y.

The downloaded static data over DMS-X signalling channel, channel 1 are; " DN for each defined subscribers of DDRM node " Translation tables " Tones - Dial tone, Ring Back tone, Congestion tone, Busy tone. Howler tone will be applied by DDRM itself. TNs are sent for each defined subscribers of DDRM

node and sending of them are not based on ESA mode. They are sent as a step of line definition process.

3.2.3 ESA Entry

ESA mode is expected to be triggered automatically when the regular checks on communication links (monitoring the message channel to DMS, Monitoring E1 reception status etc) reveal a problem. In the existing structure of DMS there are two reasons to enter ESA mode; Badlink and Badcside. It should be noted that Badlink check is not specific for ESA. It is a generic control method to check E1 links (e.g E1 frame alignment) between host and remote. But Badcside is specific for ESA mode and a message is sent from remote site if the ESA mode indication is Y during DDRM definition on DMS. Badlink - The fault condition of unusable communication links triggers badlink. The communication links between remote node andDMSbecome unusable. The possible reasons for this fault condition are ; The links are severed between remote and the host The Peripheral side (P-side) message link (DS-1 card) of LTC is pulled out or DTC card on DDRM is pulled out.

The "RLCM_ESAENTRY_BADLINK" office parameter on remote site determines the desired delay timer between the failure of the C-side message link and the entry of ESA mode. The default value is 30 seconds and the value range is between 30 and 1000 second with 10 second intervals. If ESA-mode is entered because of Badlink problem then the existing behaviors of DMS for the state of remote nodes will be kept. Badcside this is for monitoring message channel to DMS. Remote node checks to the host site periodically by means of looparound message in order to decide on ESA enterance. Upon receiving the host looparound message, the remote side knows that remote - CC communication is possible. When a failure is detected remote node waits for a delay before entering ESA-mode which is identified with an office parameter "LCM-ESA_ENTRY_BADCSIDE". Its default value is 15 minute and the range is between 1 minute and 60 minutes with 1 minute intervals.

3.2.4 ESA Exit

When the failure reasons which trigger ESA mode entry are recovered DMS requires exit from DDRM then DDRM node performs ESA exit operations. The active calls which are already set up in ESA mode are dropped after exiting ESA. This process is called as "cold exit". Warm exit is not supported by DDRM. There are two possible types to exit from ESA; System Exit and Manual Exit.

"RLCM_XPMESAEXIT" timeout value is used to decide System / Manual Exit procedures. Its default value is 0 and the value range is between 0 and 1000 with 10 second intervals.

System exit is an automatic exit from ESA-mode which is invoked by the host site without craftsperson interference. System exit is invoked if "RLCM_XPMESAEXIT" timeout value has a value except 0. DDRM will RTS automatically and return to normal mode of operation from from ESA mode and active calls which are established in ESA mode will be dropped.

Manual exit is a procedure which is initiated by the craftsperson. Manual exit is invoked if "RLCM_XPMESAEXIT" timeout value is 0(default value). Manual exit allows the craftsperson to view the number of calls on the remote site before RTSing the unit. This feature allows the craftsperson to delay the ESA exit if there are a large number of calls currently active. When E1 links are down DDRM state is seen as Cbsy until they are up again. If E1 link is started to be restored then the state of DDRM is returned to Sysb. If nothing is done by craftsperson, it will stay in SysB situation. But If BSY / RTS of DDRM is applied by the craftperson, DDRM will return to service.

After the ESA exit procedure, ESA processor on remote node sends operational measurements(OM), peg counts and the reason for ESA-mode entry back to DMS. These messages are "ESA Operational Measurements Reply to CC" and "ESA peg Counts Reply to CC". All of these information appears in PM171 log on DMS.

Table 5: The fields in PM171 log on DMS

FIELD	DESCRIPTION
ESA ENTER REASON	Enter Reason Description
VALUE	ESA Enter reason ID
ORIG_ATT_TOTAL ORIG_ATT	total origination attempts (Received Dial Tone)
ORIG_BLK (CHNL_BLK) (CHNL_BLK)	resources unavailable for origination Channel Blocked count in dialling state
ORIG_ABND	Dialling number or hung up before finish-ing diallig
DIAL_ERR	Error in DP or DT dialling
ORIG_SB (LINK_SB)	Originating facility goes system busy
XLA_ERR	Translation error of the dialling number

Table 5: The fields in PM171 log on DMS

FIELD	DESCRIPTION
DIALLED_NUM_INV	The dialled number was not on the same RLCM or a timeout occured while dialling (took too long time to dial number
IA_TERM_ATT_TOTAL (TERM_ATT)	Termination attempt for intra-switched calls
IA_TERM_CUS (TERM_SUC)	termination successed for intra-switched (Number of calls asnwered)
IA_TERM_BLK (TERM_BLK)	intra-switched calls blocked due to lack of resources
IA_TERM_BSY	Intra-switched calls whose terminations were non-idle (busy,system busy, abond-ened etc)
IA_TERM_SB	Intra-switched calls whose terminations went system busy while processing the call (usually because of ring faults)
IA_TERM_NO_ANS	Intra-switched calls where there was no answer
RING_TMO	Ringing timeout
COIN_FLT	Coin faults or failures
RING_BLK	Ring blocake in ringing state
TEST_REG	Test register failure in ringing state
CON_FAIL	Continuinty test fail while ringing
PRE_TRIP	Ringing fault message count in talking state
NO_IPC	No Inter peripheral Connection (IPC) buffer available
PREFIX USAGE	Usage counts for up to 16 entries in the POTS Prefix table. If no POTS prefix entry has been defined then this field is black

There is another statistics called as "DTSR statistics request". This is not specific for ESA mode. The number of calls that has over 3 seconds delay before given dial tone in each class is requested by DMS. The remote site sends "DTSR statistics Request Response" to DMS by means of a DMSX message.

3.2.5 DDRM ESA Static Data Download Subcomponent

DDRM ESA static data includes:

1. ESA tables
   - node table
   - terminal type table
   - digit collection table
   - multi-ring table
2. ESA translation tables

The ESA translation table download sequence is:

- translation data collection
- translation data download

ESA translation tables required by the DDRM are:

- Line terminal data table
- Extension header table
- Extension table
- Digit translation tables (EFG and ABCD tables)
- Tone table
- Office parameter table

DDRM ESA data downloading is triggered by:

- a successful DDRM RTS
- a DDRM ESA nightly audit

3.2.6 DDRM Node Maintenance Component

This component consists of fallowing subcomponents:

1. DDRM RTS sequence — This component invokes DDRM ESA Exit during DDRM RTS (both *manual* and *system*).

2. DDRM SYSRTS sequence —
   The LCM SYSRTS sequence is activated during the C-side host RTS. This invokes the LCM RTS sequence.
3. DDRM ESA Static Data request handling — This handles maintenance requests submitted for the DDRM ESA Static Data download.
4. DDRM Nightly Audit request handling —
   This supplies the interface between DDRM Nightly Audit and the existing LCM maintenance processes.

3.2.7 ESA Inservice Troubles

If the Static Data is not updated for the DDRM ESA or a problem occurs during Static Data download, the status of DDRM is changed to the appropriate ISTB.

LCM ISTB types do not now have a value which indicates Static Data problems. This is because LCM peripherals software do not contain Static Data tables. RLCM ESA is a separate node, and its ESA Static Data ISTB is only displayed in the ESA PM level.

The ISTB reasons will include:

- Static Data mismatch with CC
- Invalid ESA translation data

3.3 Hardware Requirements or Dependencies

UTRD which receives tones in ESA mode, is needed in order to enter ESA mode.

3.4 Software Requirements or Dependencies

For successful deployment of this activity following activities are required:

- A00006660 - DDRM Node Definition and Provisioning

  ESA is defined by node definition made in LCMINV table. CM checks ESA field information and UTRD datafill and existence.. When ESA field is changed nightly audit needs to be triggered which will download ESA data If necessary.

- A00006661 - DDRM Node Maintenance

  ESA data will be downloaded by by sucesfull RTS and by nightly audit. These are triggered by node maintenance..

- A00006663 - DDRM Alarms and Audits

If UTRDis non-existent on DDRM major alarm will be raised. ESA enterence will be prevented by checking alarm status..

- A00006666 - DDRM XPM Support and Monitoring

  DDRM ESA related messages will pass through XPM.

Also:

- DDRM node, internal software

  CM part o f ESA needs proper reply messages from DDRM internal software in order to function. Also, call processing in ESA mode will be handled by DDRM ESA software.

3.5 Limitations and restrictions

DDRM ESA will not be triggered if UTRD is non-existent. Also UTRD datafill is needed in order to datafill ESA field in LCMINV table. Automatic line index, hunt group and prefix tables are not downloaded in static data since they are not needed.

3.6 Interactions

a. A00006660 DDRM NODE DEFINITION AND PROVISIONING
b. A00006666 DDRM XPM SUPPORT AND MONITORING
c. A00006661 DDRM NODE MAINTENANCE
d. A00006663 DDRM ALARMS and AUDITS

3.7 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

3.8 Glossary

Term	Description
DDRM	DMS Dicle Remote Module
DRX-4	Dicle Rural Exchange-4
ESA	Emergency Stand Alone
LCM	Line Concentrating Module
RLCM	Remote Line Concentrating Module
UTRD	Universal Tone Receiver for DDRM

3.9 Recommended Reading/References

e. DMS_DDRM DDRM (DMS Dicle Remote Module) Spec Document
f. A00006638 DMS - DDRM HLD
g. A00006664 DDRM Node Definition and Provisioning
h. A00006661 DDRM Node Maintenance
i. A00006662 DDRM Lines Inventory
j. A00006663 DDRM Alarms and Audits
k. A00006665 DDRM ESA Support
l. A00006666 DDRM XPM Support and Monitoring

4: Functional Description (FN): A00007289

4.1 Feature name and Feature ID

A00007289 - RT Selector Enhancement for Metering

4.2 Description

4.2.1 Purpose

The purpose of this feature is to optionally remove the incompatability of metering behavior between DMS-100I and DMS-100 MMP systems, when RT selector is used in XXRTE routing tables.

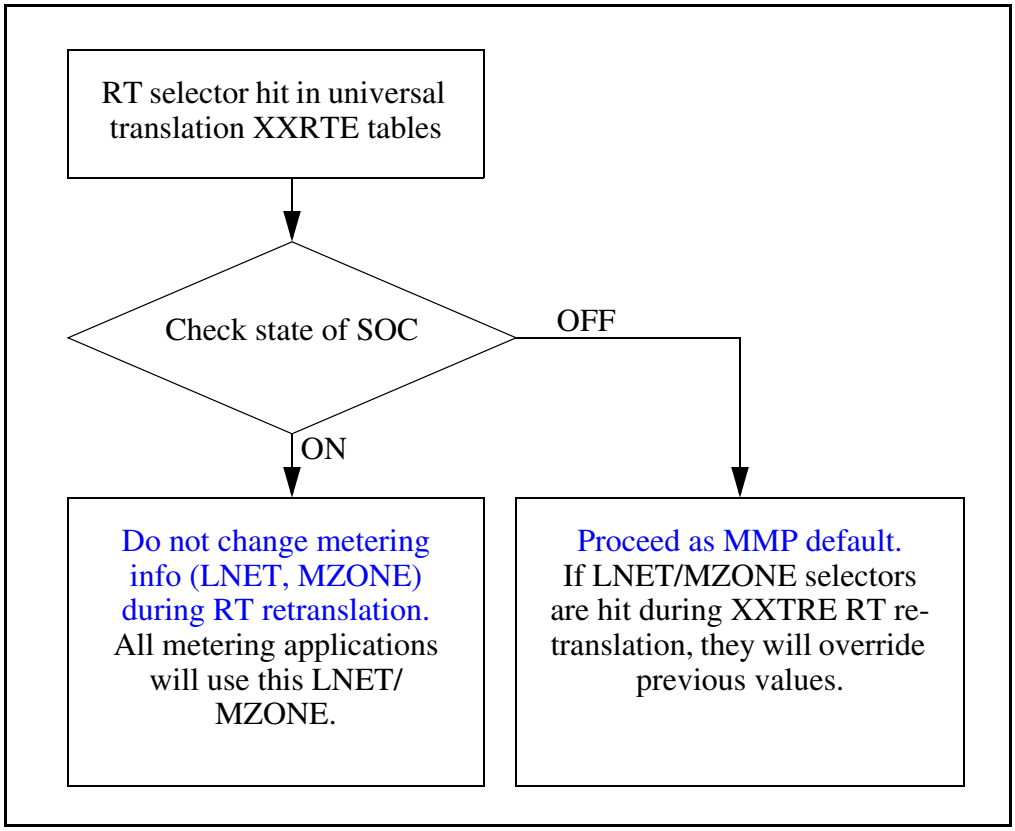
4.2.2 Introduction

The RT selector in XXRTE tables causes a re-translation to take place with new digits, which are supplied as parameters to the selector. During the translation of these new digits, it is likely that LNET/MZONE values different than those encountered before RT was hit will be encountered. Default MMP behavior is that the new LNET/MZONE will overwrite the previous ones, so that at the end of translation, the values that are last hit (i.e. the ones hit within retranslation) will be used for metering. On the other hand, DMS-100I product does not let re-translation overwrite LNET/MZONE, so at the end of the translation, the values which are hit before RT will be the ones which will be used for metering.

This activity implements a SOC optionality (METR0018). If the SOC state is ON and the translation is in XXRTE RT-based retranslation, DMS-100 MMP product will preserve LNET and MZONE during the retranslation, in the same way as DMS-100I.

4.2.3 Behavioral Diagram

Table 1 Feature flowchart



4.3 Hardware Requirements or Dependencies

This feature is meant to be used in DMS-100 MMP offices of Turk Telekom.

4.4 Software Requirements or Dependencies

This feature will work on DMS-100 MMP products, provided that the SOC is set to ON.

This feature may optionally be used in DMS-100 MMP markets that use metering.

4.5 Interactions

The effect of this feature is limited to metering behavior of RT selector in XXRTE routing tables. Other RT selectors (for example, RT selector in OFRT

table), or other selectors which cause re-translation (like GRX and IBNRT) are not effected.

Only the metering behavior of XXRTE RT selector is affected.

Metering is affected such that RT re-translation of XXRTE tables do not override LNET/MZONE.

Any application that uses/reads LNET/MZONE after/during translations will be indirectly effected (if translations use XXTRE-RT, and the SOC state is ON).

There are no changes in TRAVER behavior.

4.6 Applicable customer facing sections

Table 2 Customer facing sections

Fault Management	**N/A**
Logs	N/A
Alarms	N/A
Configuration	
Data Schema (SOC)	X

2.1 Glossary

Term	**Description**
XXRTE	The routing tables of Universal Translation, i.e PXRTE, FARTE, etc.
DMS-100I	The DMS-100 International product.
DMS-100 MMP	The DMS-100 Multi-Market product, the product in which this feature will be in use.
LNET	Logical Network - A parameter used in metering.
MZONE	Metering Zone (or Destination Zone) - A parameter used in metering.

5: Functional Description (FN): A00008429

5.1 Feature name and Feature ID

A00008429 - Ring Back When Free (RBWF) Enhancements

5.2 Description

5.2.1 Introduction

Throughout this document,

- RBWF is used as a general term for RAG flavors which are Nodal RAG and BTUP Call Back When Free (CBWF) for this activity.
- The subscriber that invokes the RBWF service is known as the RAGOR. The subscriber that was busy when a call was made to it, resulting in the RBWF service being invoked against it, is known as the RAGEE.

This activity enhances the Nodal RAG (Ring Again) and BTUP Call Back When Free (CBWF) flavours of existing RAG Service (based on two new SOCs introduced by this activity).

This activity is implemented in ISN09 release and any functionality introduced by this activity is only available in INTL TDM loads.

In the “Background Information” section existing RAG functionality is summarized, and in the “Functional Overview” section RBWF enhancements introduced by this activity are explained.

5.2.2 Background Information

The RAG feature allows a RAGOR to set a Ring Again request against a RAGEE, if the RAGEE is busy, and be recalled when the RAGEE becomes idle. Once the RAGEE becomes free then the RAGOR is automatically rung back. Once the RAGOR picks up the ringing call then the RAGEE is rung and the call continues as a normal call.

The activation and deactivation of RAG feature is as follows:

1. The RAGOR encounters a busy signal. The RAGOR activates the RAG feature (either by single digit activation mechanism, or by dialling RAG feature code after FLASH). The RAGOR goes on-hook.
2. When the RAGEE becomes idle, the RAGOR receives a special ring back tone.
3. The RAGOR goes off-hook. The switch places the call, and the call continues as a normal call. The system deactivates the RAG feature.

Interrogation functionality of RAG service does not exist before this activity.

After a specified amount of time, RAG automatically reactivates if the RAGOR does not answer the ring back. To cancel a RAG request, the RAGOR can go off-hook and dial the RAG feature code.

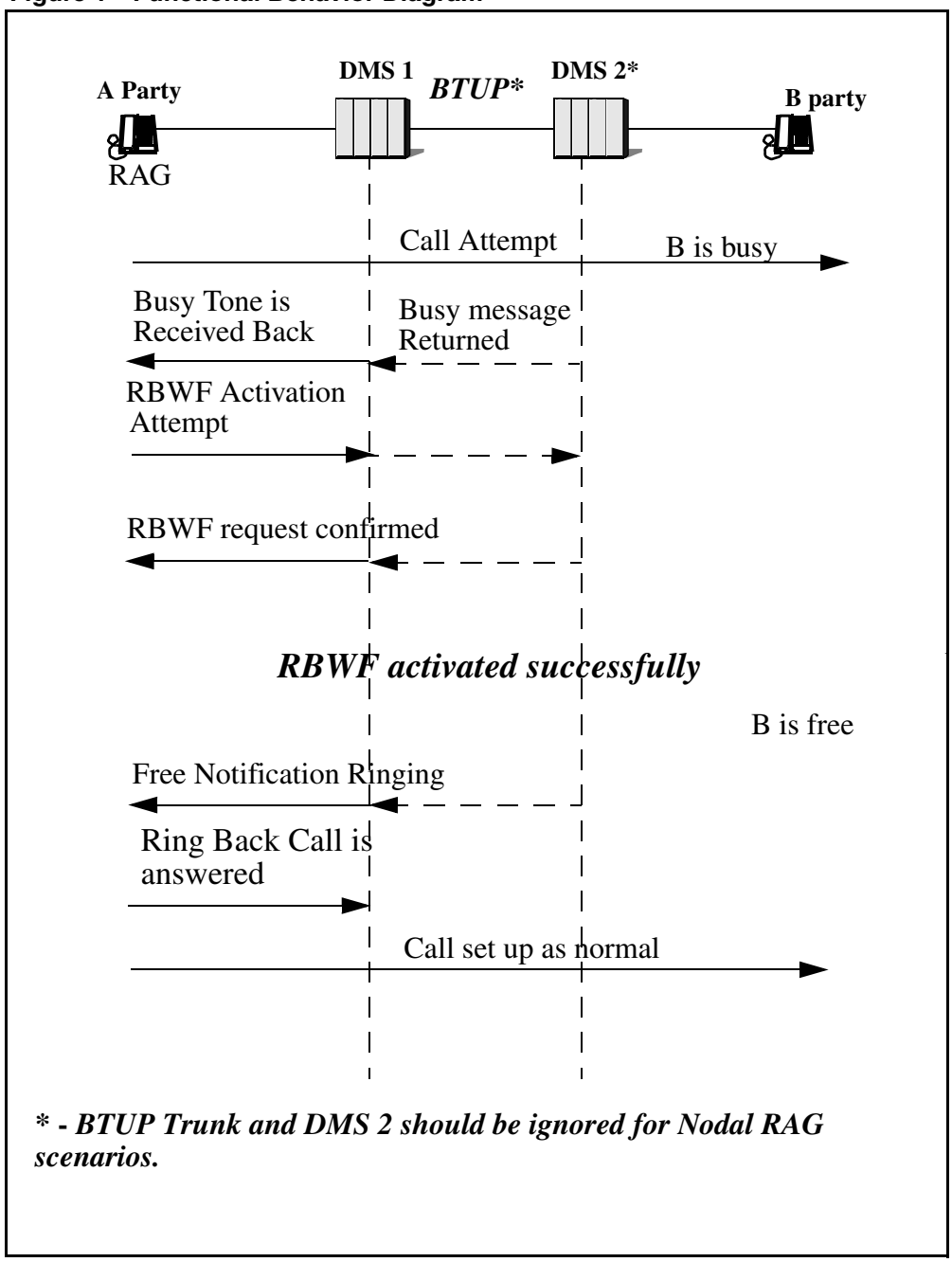
Ring Again Cancellation Timer deactivates the RAG requests when the busy party remains off-hook for a specified amount of time.This timer is datafilled in table CUSTSTN, with RAGCANTO field of RAGTIM option for nodal RAG (0, 2 TO 30 mins), and in table CUSTNTWK, with ORIGDUR (5 TO 180 mins) and TERMDUR (5 TO 185 mins) fields of NTWRAG option for BTUP CBWF.

Only one RBWF request can be active for RAGOR. If RAGOR attempts to activate a new RBWF request, when there already exists an active RBWF request, new RBWF request overwrites the existing one.

For Nodal RAG, RBWF activation is not allowed for inter-group calls, if INTRAGRP=N.

Following figure shows the activation and call setup sequence for RBWF services.

Figure 1 Functional Behavior Diagram



Please refer to related NTPs and the references given at the end of the document, for further information on existing Nodal RAG and BTUP CBWF functionality.

5.2.3 Functional Overview

This feature provides the following functionalities/enhancements to RBWF Services:

- Number of RBWF requests that can be activated by a RAGOR is increased from 1 to N, which is datafillable up to 6.
- Cancellation command results in cancellation of all active RBWF requests cancelled.
- Interrogation functionality is newly introduced by his activity, and interrogation results in announcement of all active RBWF requests of the RAGOR.
- Individual datafillable dialling sequences for RBWF deactivation, and interrogation are provided.
- Billing for nodal RBWF calls is supported.
- Nodal RBWF functionality is improved so that RBWF can work between different customer groups, regardless of the INTRAGRP flag.
- Range of existing Ring Again Cancellation Timer for Nodal RBWF calls is extended from 30 to 185 mins. This timer allows the end user to set a limitation how long each nodal ring again request can remain active at the switch. This limit is set on a customer group basis (RAGCANTO field of RAGTIM tuple in table CUSTSTN). Please note that this timer is individually started for each RBWF request, and expiry of this timer for a RBWF request causes deactivation of that request only.

RBWF enhancements implemented by this activity are controlled with two new SOC options, so that existing functionality is not affected when these SOCs are IDLE. Two new SOC options introduced by this activity are SVBI Multiple RBWF and SVBI RBWF Enh. Please refer to Section “Providing Optionality for RBWF Enhancements”.

Please note that multiple RBWF functionality is designed considering that only Nodal RAG and BTUP CBWF flavours of RBWF are used in the switch. It is strongly recommended that SVBI0037 SVBI Multiple RBWF SOC should not be turned ON in the switches where other flavours of RBWF (i.e. DPNSS, TCAP CBWF, CCBS etc) are being used. Turning this SOC ON might cause unexpected behaviour if RBWF flavours other than nodal RAG and BTUP CBWF are being used.

In addition, some new options in tables ISERVOPT and AMAOPTS are introduced in order to control the functionality. All of these options are discussed in next sections.

Please note that this activity does not change the call topology and BTUP signalling of existing RBWF services.

5.2.3.1 Providing Optionality for RBWF Enhancements

Main functionalities of this activity are controlled by two new SOC options, SVBI Multiple RBWF and SVBI RBWF Enh. Both of these SOCs are state SOCs, which can be either in SOC_ON or SOC_IDLE state.

SVBI Multiple RBWF SOC controls the following:

- Allowing N RBWF request to be activated by the RAGOR.
- Rejecting N+1th request.

Table 1 SVBI0037 Multiple RBWF SOC

SOC Group	SVBI
SOC Option Name	SVBI0037
SOC Option Title	Multiple RBWF
SOC Option Control Type	State
New SOC Option?	Yes
Option defined in DRU	WT22
Affected Products	DMS100 - MMP

If SVBI0037 Multiple RBWF SOC is turned OFF when RAGOR has more than one active RBWF requests, these requests are completed normally after SOC is turned OFF. If RAGOR attempts to activate a new request after SVBI0037 SOC is turned OFF, new RBWF request overwrites the first RBWF request activated before.

SVBI RBWF Enh SOC controls the following:

- Allowing nodal RBWF between different customer groups via ignoring INTRAGRP flag.
- Billing of nodal RBWF usage.
- Deactivation and interrogation functionalities with new dialling sequences.

  Note: If only SVBI RBWF Enh SOC is ON, then there should be at most one RBWF request to announce or cancel - however if there are more than one (because the SVBI Multiple RBWF SOC was on when they were activated) then all requests are announced / cancelled.

Table 2 SVBI0036 RBWF Enh SOC

SOC Group	SVBI
SOC Option Name	SVBI0036
SOC Option Title	RBWF Enh
SOC Option Control Type	State

Table 2 SVBI0036 RBWF Enh SOC

New SOC Option?	Yes
Option defined in DRU	WT22
Affected Products	DMS100 - MMP

Please note that datafilling of any option, which is introduced by this activity, is allowed even if these SOCs are IDLE. But new functionalities are only available when related SOC(s) is ON.

5.2.3.2 RBWF Activation, Interrogation and Cancellation Through Translation Tables

In the existing implementation, if single digit activation mechanism is not used, RBWF services are activated and deactivated via using the same dialling sequence (ex. *37#), datafilled in translation tables.

Figure 2 Existing Datafill for RAG act and deact access codes

```
TABLE IBNXLA
KEY                      RESULT
----------------------------------------
FTRSTAR  37      FEAT N N RAG
```

This activity provides different dialling sequences for RBWF activation and deactivation, and also introduces RBWF Interrogation functionality in INTL TDM product. In order to provide this, two new IBN_LOG_FEATURES “RAGD” and “RAGINT” are introduced to be used in table IBNXLA.

Access codes for RBWF act, deact and interrogation are datafillable in table IBNXLA, and following figure shows a datafill example for using *37# for activation, #37# for deactivation and *#37# for interrogation of RBWF.

Figure 3 New datafills for RBWF act, deact and interrogation access codes

```
TABLE IBNXLA
KEY                      RESULT
----------------------------------------
FTRSTAR  37      FEAT N N RAG
FTROCT   37      FEAT N N RAGD
FTRSTAR  C37     FEAT N N RAGINT
```

RAGINT and RAGD are datafillable in table IBNXLA, even if RBWF Enh SOC is IDLE. But please note that, NACK tone is given if subscriber attempts to use deact/interrogation with these dialling sequences, when RBWF Enh SOC is IDLE.

Behavior of the RBWF service during RBWF act, deact and interrogation are explained in the following flowcharts:

Figure 4 Flow Chart for RBWF Activation

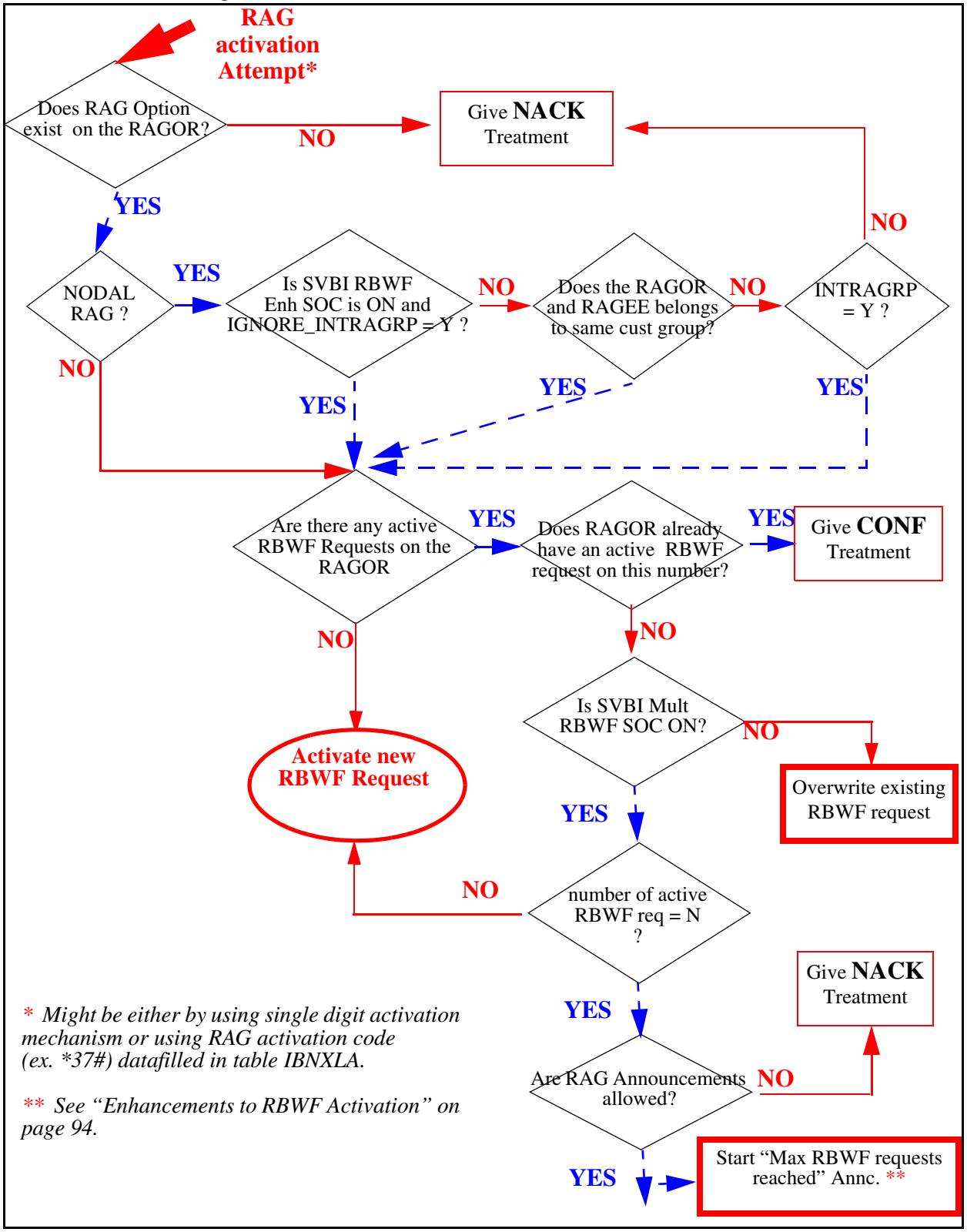


Figure 5 Flow Chart for RBWF Deactivation

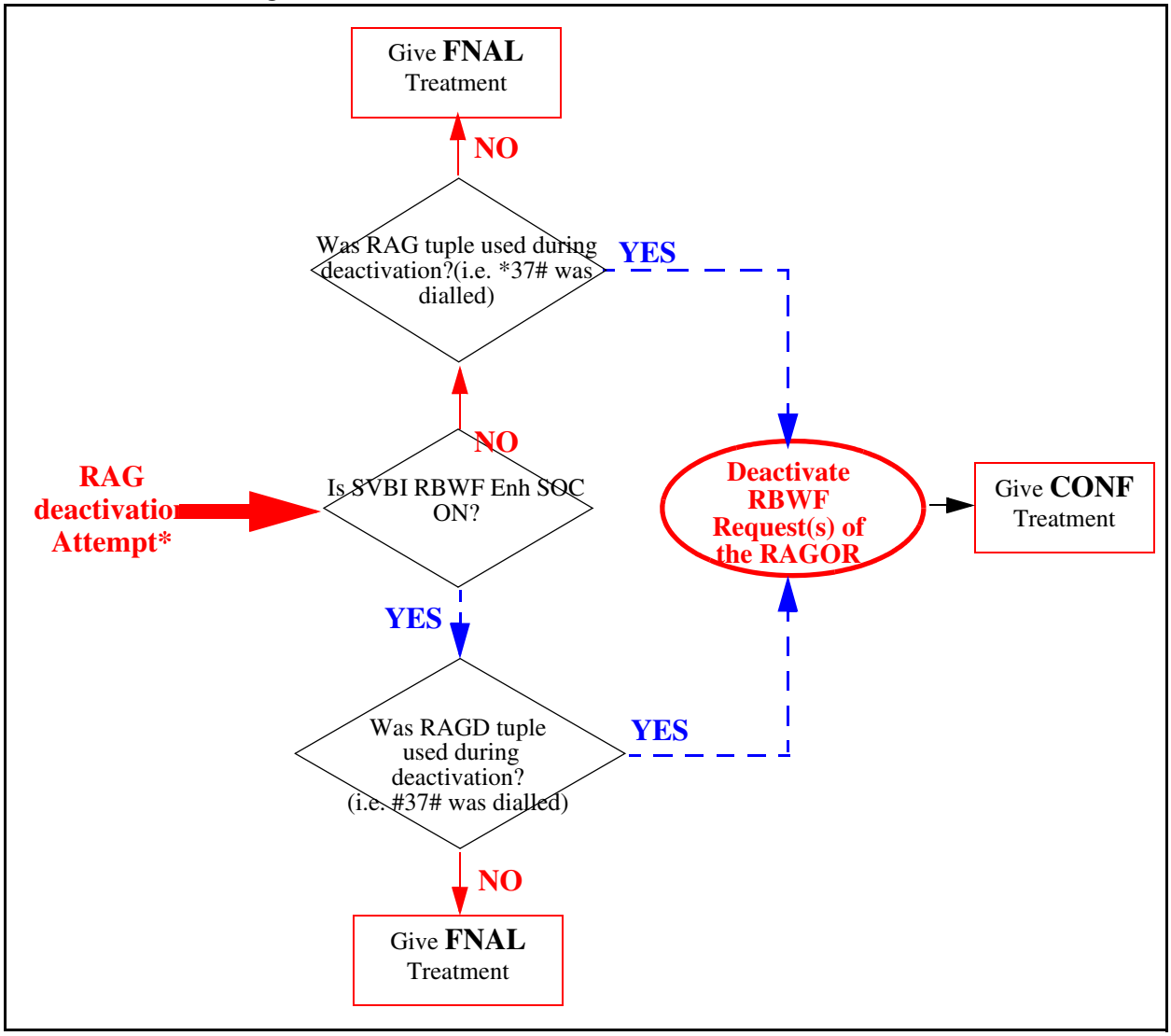
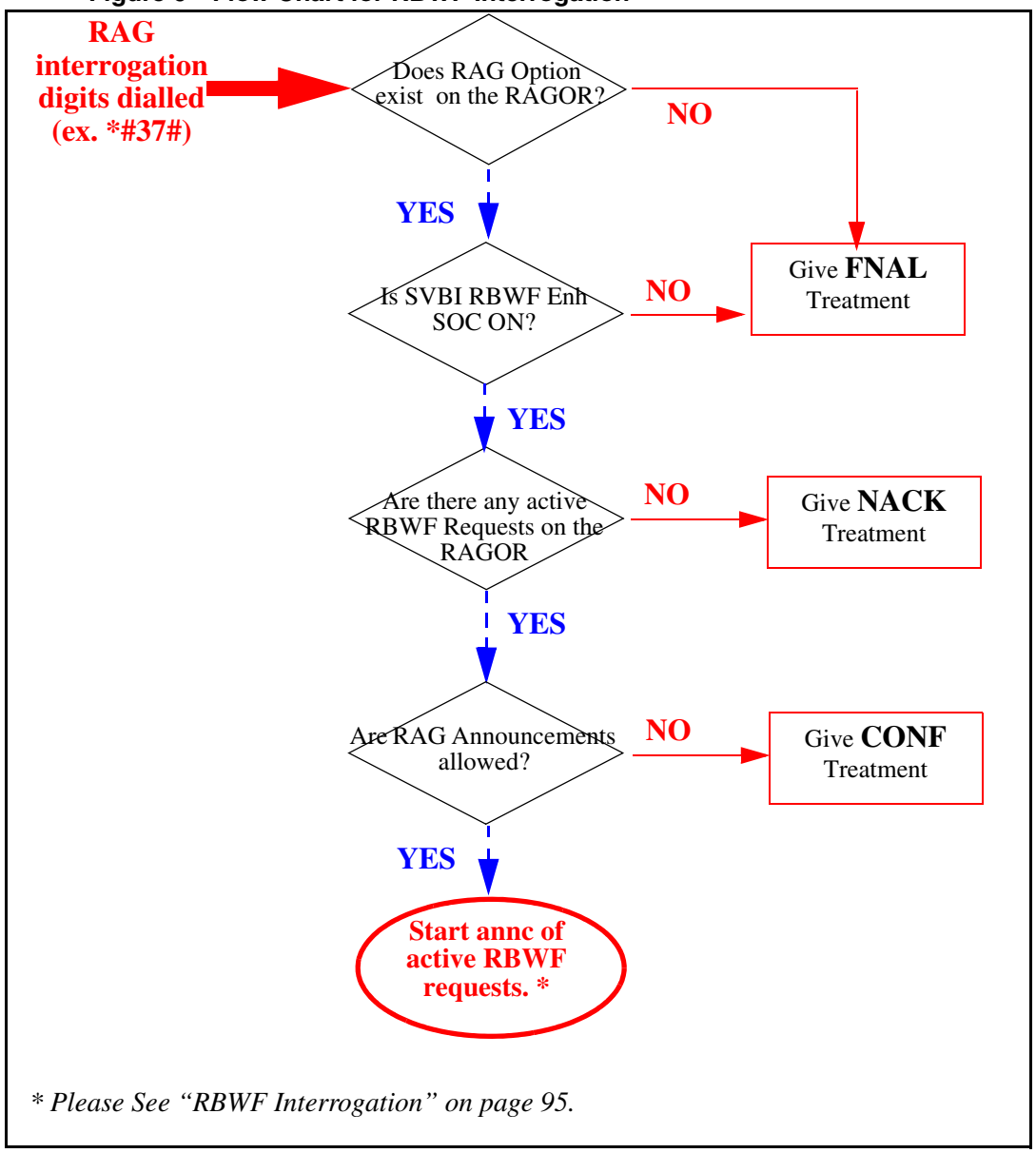


Figure 6 Flow Chart for RBWF Interrogation



** Please See "RBWF Interrogation" on page 95.*

5.2.3.3 RBWF Activation and Cancellation on EBS Lines

In the existing implementation, RAG key on EBS sets is used for both activation and cancellation. If it is hit any time when there is an active RBWF request, RBWF cancellation is performed. Hitting RAG key when there are no RBWF requests is considered as RBWF activation.

This behaviour is changed by this activity, since hitting RAG key for activating a new RBWF request (when there already exists one), should be taken as RAG activation, not cancellation.

If SVBI0037 Multiple RBWF SOC is ON,

- **hitting RAG key when RAGOR is not involved in a call (ON-HOOK), is considered as RAG cancellation attempt.**
- **hitting RAG key, when a busy destination is encountered, is considered RAG activation attempt.**

Please note that existing behaviour is not changed if SVBI0037 Multiple RBWF SOC is IDLE.

5.2.3.4 Enhancements to RBWF Activation

In current implementation of RBWF, any RAGOR can have only one active RBWF request at a time. By this activity, a RAGOR can have N active RBWF requests, where N is datafillable in table ISERVOPT. If SVBI Multiple RBWF SOC is IDLE, RAGOR can have only one active RBWF request as it is now.

5.2.3.4.1 New Service Option for Multiple RBWF Requests

A new option RBWFENH is defined in table ISERVOPT. This option has two subfields: MAX_RBWF_REQ and IGNORE_INTRAGRP.
MAX_RBWF_REQ determines the maximum number of RBWF requests that can be activated by a RAGOR simultaneously. It takes values between 1 and 6. Its default value is 5, if not datafilled.

Please note that if SVBI Multiple RBWF SOC is IDLE, only one RBWF request is allowed as it is now, even if MAX_RBWF_REQ is different than one. If user attempts to datafill MAX_RBWF_REQ with a value greater than 1 when SVBI Multiple RBWF SOC is IDLE, a warning msg is displayed, however datafill is allowed.

Figure 7 Datafill Sample for MAX_RBWF_REQ in table ISERVOPT

```
TABLE: ISERVOPT

 RBWFENH             RBWFENH 5 Y
```

5.2.3.4.2 Increasing Number of RBWF Requests up to N

In the existing implementation, only one active RBWF request is allowed for a RAGOR.By this activity number of RBWF requests allowed for a RAGOR is increased up to N.

- *Ragging on the same number twice:*

In the existing implementation of NODAL RAG, if RAGOR attempts to rag on the same number again, just CONF tone is given without resetting the existing RBWF request (i.e. timers are not reset) . This behavior is not modified by this

activity. If current RAGEE number is one of the active RBWF requests of the RAGOR, just CONF tone is given.

In the existing implementation of BTUP CBWF, active RBWF request is cancelled when user attempts to activate a new one, even if incoming request is for the same number. This behavior is changed by this activity, as to be consistent with NODAL RAG implementation.

- *Ragging on a new number:*

In the existing implementation, if any other number is requested, active RBWF request is cancelled and new request is accepted.

By this activity, if SVBI Multiple RBWF SOC is ON, active RBWF requests are not cancelled, instead a new RBWF request is activated. If max number of RBWF requests were already reached, new request is rejected with an announcement.

5.2.3.4.3 Rejection of N+1th RBWF request

If max number of RBWF requests allowed are reached, new RBWF request of the RAGOR should be rejected if SVBI Multiple RBWF SOC is ON. If RAG announcements are allowed (datafilled in ANNC_CONF field of RAG tuple in ISERVOPT), new request is rejected with an announcement, otherwise NACK tone is given. Following is a rejection announce sample:

Figure 8 RBWF Request Rejection Announcement sample

```
"The maximum number of ringback requests are registered
against your line.No further ringback requests can be
accepted at the moment"
```

5.2.3.5 Enhancements to RBWF Deactivation

When the RAGOR attempts to cancel his/her RAG requests, via dialling the cancellation digits, all of the active RAG requests of this RAGOR are cancelled.

5.2.3.6 RBWF Interrogation

Interrogation functionality of RBWF is being introduced by this activity. If all criterias in the interrogation flowchart are met (i.e. SVBI Mult RBWF SOC is ON, RAG Annc allowed, etc), successful interrogation results in announcement of all active RBWF Requests. Provided announcement is like the following:

Figure 9 Interrogation Announcement sample for an agent having 3 active RBWF requests

```
"Telephone Number 01483 8207308 is waiting for ringback.
 Telephone Number 436 7854 is waiting for ringback.
 Telephone Number 436 7945 is waiting for ringback."
```

5.2.3.7 RBWF Announcements

RBWF announcements are custom announcements that consist of a number of simple phrases, in English, datafilled in table ANNPHLST (See Appendix for sample announcement datafill). Each simple phrase has a corresponding recording on the EDRAM card.

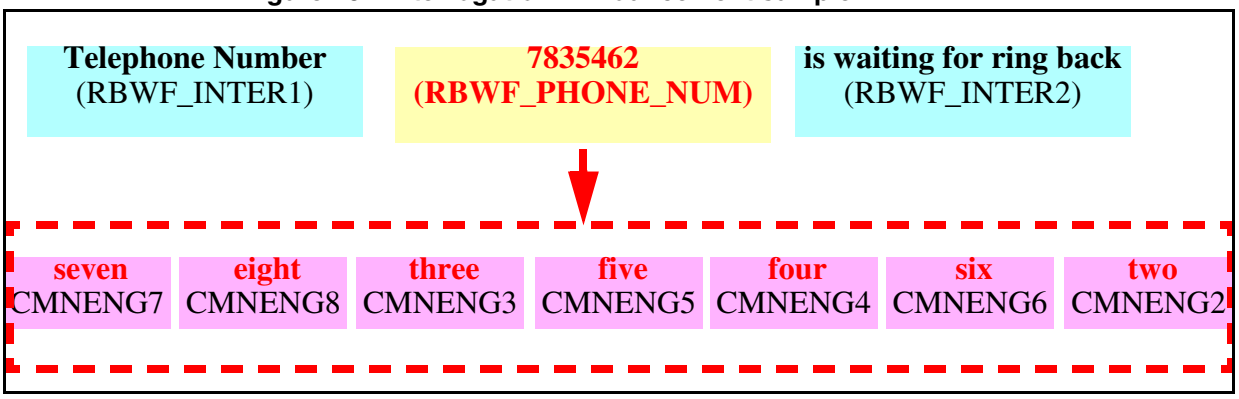
- *RBWF Interrogation Announcement*

RBWF interrogation announcement is provided as a result of successful RBWF interrogation, and includes the RAGEE telephone numbers which were activated by the RAGOR requesting the interrogation.

There are two simple phrases introduced for RBWF interrogation announcement, which are RBWF_INTER1 and RBWF_INTER2. RBWF_PHONE_NUM is a compound phrase, which corresponds to the RAGEE number. RBWF_PHONE_NUM does not have a constant recording on EDRAM, and its components (i.e. combination of simple phrases) are determined at run time according to the digits of the RAGEE number.

Tuple datafilled in ANNPHLST is repeated for “number of existing RBWF requests of RAGOR” times. Please note that announcement given stricly depends on datafill sequence.

Figure 10 Interrogation Announcement sample

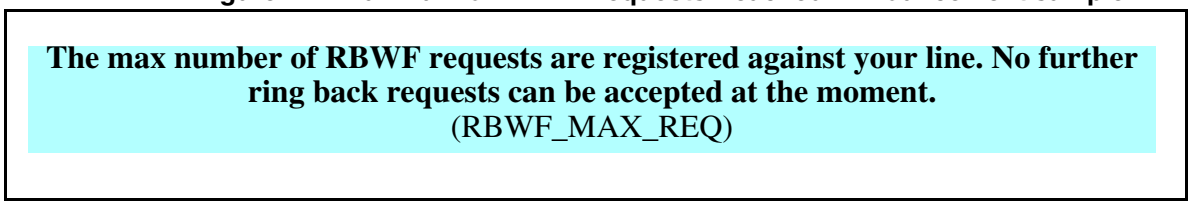


- *Max Num of RBWF Requests Reached Announcement*

This announcement is given when RAGOR attempts to initiate a new RBWF request, and RAGOR already has N active requests (N - Max Num of RBWF allowed).

There are one simple phrase introduced for RBWF request rejection announcement, which is RBWF_MAX_REQ.

Figure 11 Max Num of RBWF Requests Reached Announcement sample



Following is the list of phrases which are introduced by this activity.

Table 3 List of English Phrases introduced

Phrase Name	Recording
RBWF_INTER1	Telephone Number
RBWF_INTER2	is waiting for ring back
RBWF_PHONE_NUM	Compound Phrase - RBWF request number
RBWF_MAX_REQ	The max number of RBWF requests are registered against your line. No further ring back requests can be accepted at the moment.

For the announcement of telephone number, existing basic English phrases for digits 0 to 9 should also be recorded properly, which are the phrases CMNENG0 to CMNENG9.

Table 4 List of English Digits Phrases CMNENG0 to CMNENG9

Phrase Name	Recording
CMNENG0	Zero
CMNENG1	One
CMNENG2	Two
CMNENG3	Three
CMNENG4	Four
CMNENG5	Five
CMNENG6	Six
CMNENG7	Seven
CMNENG8	Eight
CMNENG9	Nine

Please see Appendix for sample datafill of RBWF Announcements.

5.2.3.8 Billing of Nodal RBWF Calls

Billing of BTUP CBWF calls was already implemented by an activity “AJ4955- BTUP CBWF Billing”. Billing of BTUP CBWF calls are controlled by BTUP_CBWF_BILL option in table AMAOPTS. If it is ON, service feature ID field of AMA record is marked with value “029”. Please note that 029 is a reserved value for RAG feature.

Billing of nodal RBWF calls are implemented by this activity in the same manner, via marking the Service Feature ID field with value 029. This functionality is controlled with SVBI RBWF Enh SOC and a new option, “NODAL_RAG_BILL” in table AMAOPTS.

Both SVBI RBWF Enh SOC and NODAL_RAG_BILL option must be ON in order to enable billing of Nodal RBWF calls.

Figure 12 Sample Datafill For NODAL_RAG_BILL option in Table AMAOPTS

```
TABLE AMAOPTS
OPTION                SCHEDULE
-----------------------------
NODAL_RAG_BILL        ON
```

Usage of Nodal RAG is reported in AMA record in the following scenarios:

1. RAGOR ignores ring back call
2. RAGOR answers ring back call and disconnects immediately before or after the RAGEE is rung.
3. Ringing is applied to the RAGEE and RAGEE does not answer.
4. A complete call setup occurs between RAGOR and the RAGEE, and call is disconnected by either party after the conversation ends.

Please note that for cases 2 to 4 service feature ID field of AMA record is marked with value “029”, if all criterias are met for generating AMA record (i.e. datafills, translations, SOC options for billing etc). But For case 1, AMA record is generated at any condition, independent of billing datafills.

Figure 13 AMA Record Sample for an Answered RBWF call

HEX ID:	AA	
STRUCTURE CODE:	40510C	
CALL CODE:	006C	STATION PAID [1]
SENSOR TYPE:	036C	DMS 100F
SENSOR ID:	0754019C	(FROM OFFICE PARM)[2]
REC OFFICE TYPE:	036C	DMS 100F
REC OFFICE ID:	0754019C	
DATE:	80204C	DECEMBER 03, 2004
TIMING IND:		
TIMING GUARD FLAG	0	UNUSED
SHORT CLD PARTY OFF-HOOK IND	0	SHORT CLD PARTY OFF-HOOK
LONG DUR/SERV PTY CAPABILITY IND	0	UNUSED
UNUSED	0	
UNUSED	0C	
STUDY IND:		
STUDY TYPE A	0	UNUSED
STUDY TYPE B	0	UNUSED
STUDY TYPE C	0	UNUSED
TEST CALL IND	0	UNUSED
UNUSED	0	
ORIG/TERM NANP NUM IND	0	UNUSED
OPERATOR SERV IND	0C	UNUSED
CLD PTY OFF-HK:	**0C**	**CLD OFF-HOOK DETECTED**
SERVICE OBSERVED:	0C	NONE
OPER ACTION:	0C	ANI, CUSTOMER DIALED CALL
SERVICE FEATURE:	**029C**	
SIG DIGITS NEXT FIELD:	010C	
ORIG OPEN DIGITS 1:	00007835462C	
ORIG OPEN DIGITS 2:	FFFFFFFFFF	
ORIGINATING CHARGE INFO:	FFFF	
DOMESTIC/INTL INDICATOR:	1C	DOMESTIC
SIG DIGITS NEXT FIELD:	010C	
TERM OPEN DIGITS 1:	00007835478C	
TERM OPEN DIGITS 2:	FFFFFFFFFF	
CONNECT TIME:	1439387C	14:39:38.7
ELAPSED TIME:	000000019C	000000:01.9
MODULE CODE:	042C	CALL RECORD SEQUENCE NUM
CALL RECORD SEQUENCE NUMBER:	0000011C	
MODULE CODE:	000C	FINAL MODULE

[2]As datafilled in OFFICE_ID_ON_AMA_TAPE in OFCENG

5.2.3.9 Ignoring INTRAGRP flag for Nodal RBWF Calls

In the existing RBWF Service, Nodal RBWF between different customer groups does not work when INTRAGRP is N. By this activity RBWF Service functions independent of INTRAGRP flag.

Allowing Nodal RBWF to work between different customer groups even when INTRAGRP flag is N, is controlled with SVBI RBWF Enh SOC and IGNORE_INTRAGRP field of RBWFENH tuple in ISERVOPT.

Default value of IGNORE_INTRAGRP is Y if RBWFENH tuple is not datafilled in table ISERVOPT.

Both SVBI RBWF Enh SOC and IGNORE_INTRAGRP field of RBWFENH tuple in ISERVOPT must be Y, in order to allow Nodal RBWF to work between different customer groups regardless of INTRAGRP flag.

Figure 14 Sample Datafill For RAG tuple in table ISERVOPT

```
SOPTSKEY                                                SOPTSVAR
--------------------------------------------------------------
RBWFENH                                              RBWFENH 5 Y
>
```

5.2.3.10 Increasing Cancellation Timer for Nodal RBWF Calls

Ring again cancellation timer allows the end user to set a limit on how long a nodal or network ring again request can remain active. This value is datafillable through tables CUSTSTN for nodal RAG and CUSTNTWK for network RAG.

Currently range of nodal RAG Cancellation timer (RAGCANTO field of RAGTIM tuple) is 2 to 30, or 0 and range of network RAG Cancellation timer is 5 to 180 mins for ORIGDUR and 5 TO 185 mins for TERMDUR (fields of NTWKRAG option).

The range for RAG Cancellation Timer is extended up to 185 by this activity, so that it includes the value 45.

This functionality is not controlled by any of the SOCs or any other option.

Figure 15 Sample Datafill For RAGTIM tuple in table CUSTSTN

```
TABLE CUSTSTN
CUSTNAME     OPTNAME                                        OPTION
-------------------------------------------------------------------
CUSTRAG      RAGTIM                                  RAGTIM 8  45
```

5.3 Hardware Requirements or Dependencies

This feature uses the Enhanced Digital Recorded Announcement Machine (EDRAM) to provide the announcement as a result of successful RBWF interrogation. Simple phrases needed for RBWF announcements can be loaded into EDRAM as voice files.

5.4 Software Requirements or Dependencies

Are the same as the ones required by Nodal RAG and BTUP CBWF.

5.5 Limitations and restrictions

This activity is tested and supported for INTL TDM loads only.

All limitations and restrictions that apply to Nodal RAG and BTUP CBWF Services also applies to this activity.

5.6 Interactions

Billing Interaction

When this feature is enabled, the option UNANS_LOCAL in table AMAOPTS is overridden which controls the reporting of unanswered AMA records having Service Feature field because it is necessary to report the BTUP CBWF usage when Ragee or Ragor do not answer.

This feature interacts with AMAREQD option in table CUSTSMDR (feature AJ4226 - The option that controls the generation of AMA management reporting), in the following way:

If the translations do not provide billing trigger and feature AJ4226 (AMA Time To Answer) is active then management reported record for answered/ unanswered BTUP-CBWF calls will have the SERVICE FEATURE field marked with 029C. If neither translations nor AMAREQD trigger an AMA record then this feature does not produce an AMA record.

Other Interactions:

All interactions that appy to Nodal RAG and BTUP CBWF are also valid for this activity.

5.7 Glossary

AMA	Automatic Message Accounting
BTUP	British Telecom National User Part
CBWF	Call Back When Free
CONF	Confirmation
NACK	Negative Acknowledgement
NRAG	Network Ring Again
OM	Operational Measurement
PLM	Product Line Management
RAG	Ring Again
RBWF	Ring Back When Free
SVBI	Service Base International

5.8 Recommended Reading/References

a. AG4664 - CBWF using BTUP NEEDs
b. AE0440 - DPNSS CBWF
c. AE0328 - DPNSS CBWF Call Processing
d. AJ04955 - BTUP CBWF Usage Billing
e. A59017799 - RBWF Activation Consistency
f. AJ5518 - Single Digit Activation of RBWF

APPENDIX: Datafill for RBWF Announcements

This appendix describes changed datafill required for RBWF announcements on an EDRAM card. For complete information, refer to *NTP-297-1001-527 Digital Recorded Announcement Machine DRAM and EDRAM Guide*.

Table CLLI

This table is used to define new CLLIs for two announcement groups. Field TRKGRSIZE defines the total number of members in each group.

Figure 16 Table CLLI

```
TABLE CLLI
CLLI   ADNUM TRKGRSIZ                              ADMININF
-------------------------------------------------------
RBWFANN   800        4                          MULTIPLE_RBWF
```

Table ANNS

This table assigns the CLLI name defined in table CLLI to an announcement type. Field CLLI contains the CLLI name. For RBWF service, field ANTYPE must be datafilled with RBWF. Announcement is repeated for number of times defined by MAXCYC field.

Figure 17 Table ANNS

```
TABLE ANNS
CLLI  ANNARCH TRAFSNO   CYTIME MAXCYC                    DATA
-----------------------------------------------------------
RBWFANN    ALL      1       1     1       RBWF    25       1
```

Table ANNMEMS

This table contains the assignments for each announcement member in the announcement group defined in table ANNS. Each tuple here corresponds to one trunk member in its group at MAP TTP level. For custom announcement such as RBWF, hardware type must be DRAM, only one track can be datafilled in field TRACKLIST and the track number must be 0.

Figure 18 Table ANNMEMS

```
TABLE ANNMEMS
ANNMEM      HDWTYPE           CARD
-----------------------------------------------------------
RBWFANN 1   DRAM              DRA   0        DTM    0 14 $
```

Table ANNPHLST

Each tuple in this table defines one custom announcement. For RBWF Announcements, RBWFANN tuple with index 1 corresponds to Max RBWF Requests Reached, and RBWFANN tuple with index 2 corresponds to RBWF Interrogation announcements.

Figure 19 Table ANNPHLST

```
ANNPHKEY          PHSLIST
-------------------------------------------------------
RBWFANN 1         RBWF_MAX_REQ $
RBWFANN 2         RBWF_INTER1 RBWF_PHONE_NUM RBWF_INTER2 $
```

Please note that announcement provided strictly depends on the datafill of this table. Phrases are announced in the order they are datafilled in this table.

6: Functional Description (FN): A00008477

6.1 Feature name and Feature ID

A00008477 - Increase size of table MSGRTE

6.2 Description

This feature provides the expansion of the MSGRTE table size upto 100,000 tuples by adding a new table MSGRTE2.

6.2.1 Table MSGRTE2

New table MSGRTE2 is used for routing and processing of facility messages of some protocols (e.g. PRA, DPNSS, etc.) in a manner identical to that performed by the existing table MSGRTE (Please refer to FN section of AD1315 for more details about the functional model of the table MSGRTE). The selection of which table will be active is achieved by the SOC XLAS0057 as described in the section 2.2.3..

New table MSGRTE2 has the same format as the table MSGRTE, and shares the same functionality provided by the MSGRTE table. The difference, and hence the need for a new table, is that the new table supports upto 100,000 entries while the existing table has a limit of 32K-1 digilator blocks.

Table MSGRTE2 is indexed by a three field key consisting of the Network identifier (NETID), and two digit strings (FROMDIGS and TODIGS). The data in the table is a list of routes made up of one to four route elements. Each element consists of one Message Route Selector (MSGRTSEL) such as LOCAL, PRA, SS7 and DPNSS. Each selector has its own special refinement. A sample of new table MSGRTE2 is shown below in Figure 1:

Figure 1 Sample Datafill of Table MSGRTE2

```
TABLE: MSGRTE2
MSGRTKEY
MSGRTRES
-----------------------------------------------------
PUBLIC 12345 12345 ( SS7 ANSIAB_ROUTES 4 0 NEWNET NEWPUB) $
```

6.2.2 Structure of Table MSGRTE2

The structure of table MSGRTE2 is shown in Table 1.

Table 6 Structure of Table MSGRTE2

Field	Subfield or Refinement	Range of Values	Description
MSGRTKEY			*Message Route Key* This is the key to table MSGRTE2 and consists of subfields NETID and DIGRANGE.
	NETID	String up to 32 characters	*Network Identifier* Network name datafilled in table NETNAMES
	DIGRANGE		*Digit Range* This field consists of subfields FROMDIGS and TODIGS.
	FROMDIGS	Alphanumeric (vector up to 10 characters, 0 to 9, A to F)	*From Digits* Digit string for the lower bound of the digit range to which the route list applies
	TODIGS	Alphanumeric (vector up to 10 characters, 0 to 9, A to F)	*To Digits* Digit string for the upper bound of the digit range to which the route list applies
MSGRTRES			*Message Route Result.* The list of routes used to transmit messages. Up to four routes can be datafilled.
	MSGRTSEL	DPNSS, LOCAL, PRA or SS7	*Message Route Selector* • DPNSS if TCAP NRAG messages are sent over DPNSS virtual trunks. • LOCAL if the message terminates on this switch. • PRA if the message is routed out on a specified PRA-D channel. • SS7 if a the message is routed over a specific SS7 route set.

Each Message Route Selector such as DPNSS, LOCAL, PRA and SS7 has its own special refinement.

6.2.2.1 MSGRTSEL = LOCAL

If the entry for field MSGRTSEL is LOCAL, the refinement is as followed.

Table 7 Structure of LOCAL refinement

Field	Subfield or Refinement	Range of Values	Description
	DELDIGS	0 to 15	*Delete Digits* Number of deleted digits from the destination address
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix Digits* Digit string prefixed to the destination address

6.2.2.2 MSGRTSEL = DPNSS

If the entry for field MSGRTSEL is DPNSS, the refinement is as followed.

Table 8 Structure of DPNSS refinement

Field	Subfield or Refinement	Range of Values	Description
	ISUPTRK	Alphanumeric (up to 16 characters)	*ISUP Trunk CLLI Name*
	DELDIGS	0 to 15	*Delete digits*
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix digits*
	OPTIONS	NEWNET	*DPNSS Option*
	NETNAME	String up to 32 characters	*Network Identifier* Network name datafilled in table NETNAMES

6.2.2.3 MSGRTSEL = PRA

If the entry for field MSGRTSEL is PRA, the refinement is as followed.

Table 9 Structure of PRA refinement

Field	Subfield or Refinement	Range of Values	Description
	TRKCLLI	Alphanumeric (up to 16 characters)	*Trunk Common Language Location Identifier* Trunk CLLI name
	DELDIGS	0 to 15	*Delete Digits*
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix Digits*
	OPTIONS	NEWNET or NEWTOR	*PRA Options* • NEWNET for a new network and datafill subfield NETNAME. • NEWTOR for a new type of route and datafill subfield TYPEOFRT.
	NETNAME	String up to 32 characters	*Network Identifier* Network name datafilled in table NETNAMES
	TYPEOFRT	PUB or PVT	*Type of Route* • PUB for a public route. • PVT for a private route.

6.2.2.4 MSGRTSEL = SS7

If the entry for field MSGRTSEL is SS7, the refinement is as followed.

Table 5 Structure of SS7 refinement

Field	Subfield or Refinement	Range of Values	Description
	DPC	Alphanumeric (up to 16 characters)	*Destination Point Code*
	DELDIGS	0 to 15	*Delete Digits*
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix Digits*
	OPTIONS	NEWNET	*SS7 Option*
	NETNAME	String up to 32 characters	*Network Identifier* datafilled in table NETNAMES

6.2.3 Activation of the Feature

Activation of the feature is controlled by SOC XLAS0057.

MSGRTE and MSGRTE2 tables are not effective at the same time - both tables could be datafilled but only one of them will be in effect. The selection of which table will be used is achieved through the SOC option XLAS0057. When the state of the SOC option is ON, MSGRTE table will be disabled and call processing will begin to use the new table MSGRTE2. When the SOC option is IDLE, MSGRTE2 table will be disabled and the MSGRTE table will be in effect.

When the state of the SOC is changed, a warning message will be displayed to inform the user about which table is in use. When the state of the SOC option is changed to ON, following warning message will be displayed ‘Table MSGRTE will not be effective, instead MSGRTE2 table will be used.’. When the state of the SOC is changed to IDLE following message will be displayed ‘Table MSGRTE2 will not be effective, instead MSGRTE table will be used

Datafill changes can be made independently to either MSGRTE or to MSGRTE2, the system does not keep these tables syncronised. When making a change (e.g. add, delete, update) to the inactive table (as defined by status of SOC XLAS0057) then a warning message will be displayed. The warning message will not be displayed for other operations that does not cause a change (pos, list, etc.) in the table.

6.3 Hardware Requirements or Dependencies

Not Applicable.

6.4 Software Requirements or Dependencies

Not Applicable.

6.5 Limitations and restrictions

Not Applicable.

6.6 Interactions

Not Applicable.

6.7 Applicable customer facing sections

Fault Management	
Logs	N/A
Alarms	N/A
Configuration	
Data Schema	X
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Software Optionality Control	X
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

6.8 Glossary

Term	Description
PRA	Primary Rate Access
SS7	Signaling System No7
DPNSS	Digital Private Network Signaling System
TCAP	Transaction Capabilities Application Part
NRAG	Network Ring Again

7: Functional Description (FN): A00008479

7.1 Feature name and Feature ID

A00008479 - IP Correlation ID Enhancement

7.2 Description

7.2.1 Feature Description

This document describes the feature for carrying the correlation ID from SSP to IP over Base ETSI ISUP V2 for several IN triggering agents.

SCP sends the correlation ID to SSP in ETC message and the correlation ID is carried by the UUI (user to user information) parameter from SSP to external IP in IAM message over Base ETSI ISUP V2.

Sending of correlation ID is required for the following interworkings:

IN Triggering Agent	Call routed to External IP over
BTUP V2/V2+	ETSI ISUP V2
ETSI ISUP V1/V2 BASE	ETSI ISUP V2
Spanish ISUP V1/V2	ETSI ISUP V2
FTUP (SSUTR2)	ETSI ISUP V2
UK ISUP	ETSI ISUP V2
Italian ISUP	ETSI ISUP V2
Belgium ISUP	ETSI ISUP V2
Portugal ISUP	ETSI ISUP V2
ETSI PRI	ETSI ISUP V2
Spanish PRI	ETSI ISUP V2
Italian PRI	ETSI ISUP V2
French PRI VN4	ETSI ISUP V2
DPNSS/DASS2	ETSI ISUP V2
POTs Lines (LCME, GPP CAS and V5.2)	ETSI ISUP V2

IN Triggering Agent	Call routed to External IP over
EBS (P-Phone) Lines	ETSI ISUP V2
ETSI BRI Lines (Direct and V5.2)	ETSI ISUP V2

This is available in ISN09 release.

This feature focuses on BASE ETSI ISUP V2. It may work for other variants of ETSI ISUP V2, but this activity (design and test) focuses on Base ETSI ISUP V2 only.

7.2.2 Desired Behavior

Figure 1 Functional Behavior of the Feature

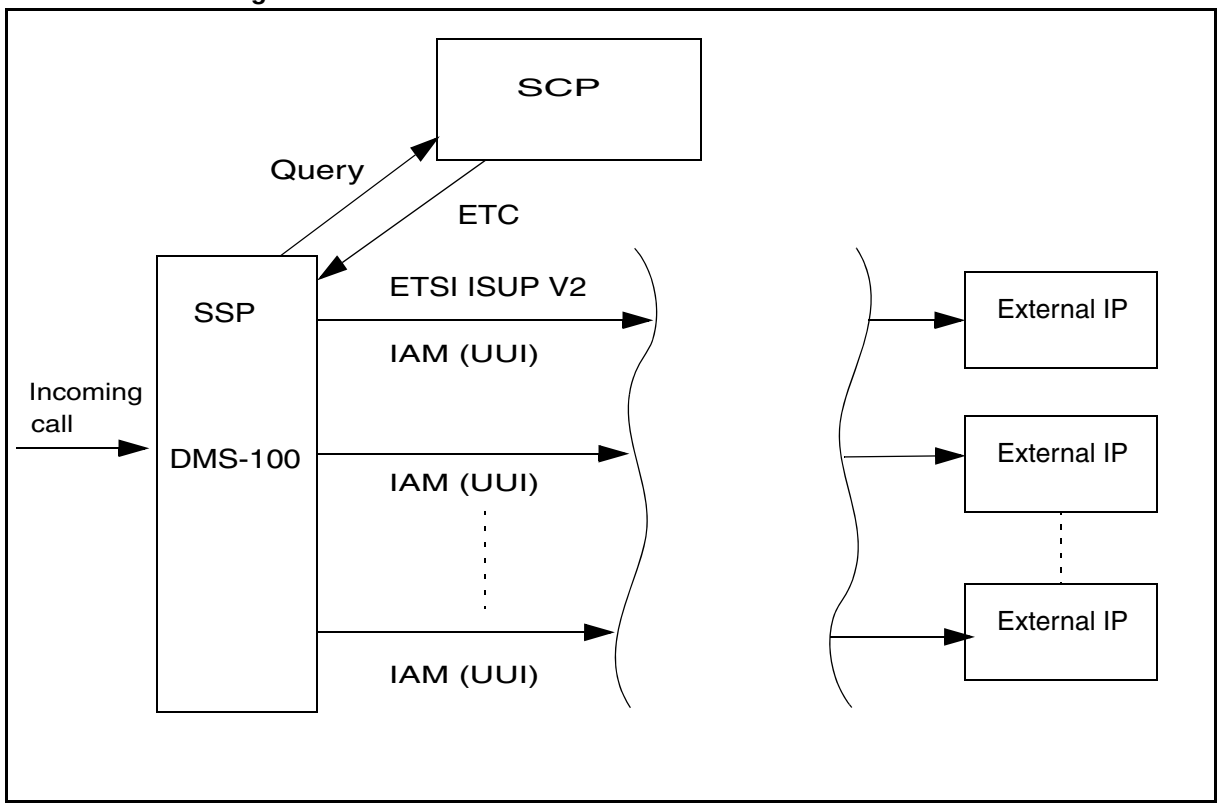


Figure 1 illustrate desired behavior of the activity. SCP sends the correlation ID to SSP in ETC message and the correlation ID is carried by the UUI (user to user information) parameter from SSP towards external IP in IAM message over Base ETSI ISUP V2.

The DMS as SSP allows receipt of correlation ID in ETC message from SCP in 2 ways:

a. embedded in the assistingSSPIPRouting address parameter

b. in a separate correlationID parameter

For this feature, the second way(b) is accepted. SSP receives the correlation ID in ETC message in a separate correlationID parameter from SCP. This is only mechanism the design supports.

Also, there are 3 mechanisms to pass the correlation ID from SSP to IP:

1) In User to User Information (UUI)

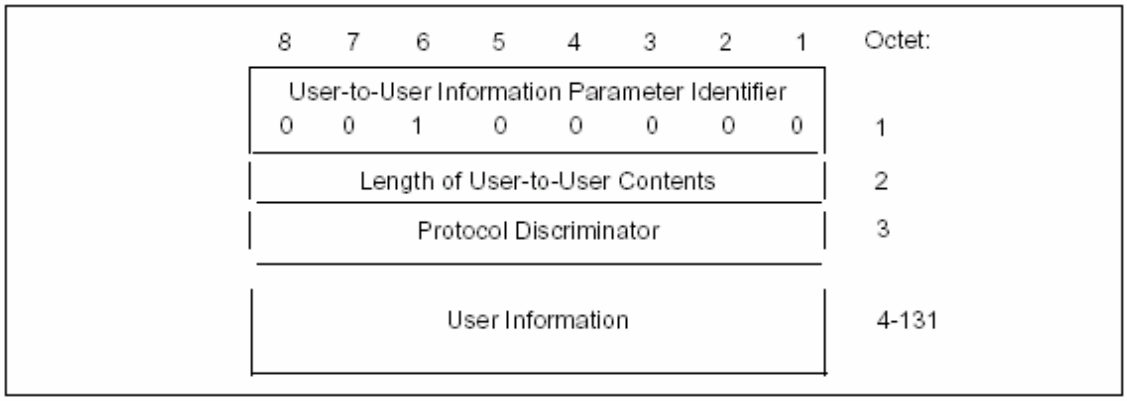
2) As a suffix to the Called Party Address (CDPN) used to route the call to the IP

3) In IAM message as a seperate optional parameter (If the "CORRELATIONID_TRANSPORT IN_CRID" is datafilled in the SERVINFO table , the correlation ID is carried in IAM message as a seperate optional parameter. This is implemented in the avtivity A00007793 in ISN08 stream. For more information ,refer to A00007793.)

For this feature, it is passed in the UUI (1). This is only mechanism the design supports. The "CORRELATIONID_TRANSPORT IN_CRID" should not be datafilled in the SERVINFO table for carring it in the User to User Information (UUI).

Figure 2 shows the UUI parameter format on ETSI ISUP V2.

Figure 2 UUI on ETSI ISUP V2



The format of the correlation ID received in the ETC message is described by the following figures. (Figure 3, Table 1, Table 2, Table 3)

Figure 3 The Format of the Correlation ID

```
EstablishTemporaryConnectionArg ::= SEQUENCE {
    assistingSSPIPRoutingAddress[0]   AssistingSSPIPRoutingAddress,
    correlationID[1]                  CorrelationID  OPTIONAL,
    legID     [2]                     LegID  OPTIONAL,
    scfID     [3]                     ScfID  OPTIONAL,
    extensions[4]                     SEQUENCE SIZE(1..numOfExtensions) OF
                                      ExtensionField   OPTIONAL,
-- ...
    }

CorrelationID:= Digits

Digits::= OCTET STRING (SIZE (minDigitsLength .. maxDigitsLength ))
```

Table 1 Generic Digits Format

Octet	8	7	6	5	4	3	2	1
1	Encoding scheme			Type of digits				
2	Digits							
…								
n	Digits							

Table 2 Encoding Scheme

Value	Meaning	May be sent by ITU IN SSP (P&C digResp)	May be received by ITU IN SSP (ETC corrID, PA/P&C VarPtno.)	May be received and sent by ITU IN SSP (RRBE/ERB)
000	BCD even (even number of digits)	✔	✔	
001	BCD odd (odd number of digits)	✔	✔	
010	IA5 character (ASCII)			✔
011	Binary coded			
110 to 111	Spare			

Table 3 Type of Digits

Value	Meaning	May be sent by ITU IN SSP (P&C digResp, ERB MC info)	May be received by ITU IN SSP (ETC corrID, PA/P&C VarPt no, RRBE MC info)
00000	Reserved for account code	✔	✔
00001	Reserved for authorisation code		✔
00010	Reserved for private networking travelling class mark		✔
00011	Reserved for business communication group identity		✔
00100 to 01111	Spare for international use		✔
10000 to 11110	Spare for national use		✔
1111111	Reserved for extension		✔

7.3 Hardware Requirements or Dependencies

None

7.4 Software Requirements or Dependencies

None

7.5 Limitations and restrictions

- This feature focuses on BASE ETSI ISUP V2. It may work for other variants of ETSI ISUP V2, but this activity (design and test) focuses on Base ETSI ISUP V2 only.
- For this feature, SSP receives the correlation ID in ETC message in a separate correlationID parameter from SCP. This is only mechanism the design supports.
- Correlation ID is carried from SSP to external IP in the UUI parameter. For this feature, this is only mechanism the design supports.
- The UUI parameter delivered by the IN triggering agent is replaced by the UUI parameter with the correlation ID received from the ETC message.

7.6 Interactions

None

7.7 Applicable customer facing sections

Fault Management

Logs __N/A___

Alarms __N/A___

Configuration

Data Schema __N/A___

User Interface __N/A___

Element Management __N/A___

Security __N/A___

Service Order __N/A___

Office Parameters __N/A___

Accounting (includes AMA billing) __N/A___

Performance (includes operational measurements) __N/A___

7.8 Glossary

TERM	Explanations
IAM	Initial Address Message
ISUP	ISDN User Part
ETSI	European Telecommunications Standards Institute
SCP	Service Control Point
SSP	Service Switching Point
UUI	User to User Information
IP	Intelligent Peripheral
IN	Intelligent Network
ETC	Establish Temporary Connection

7.1 Recommended Reading/References

1. ITU Intelligent Networks DMS-100 Service Switching Point Version: INSYSGDE.AA03

2. ITU-T Recommendation Q.763

8: Functional Description (FN): A00008484

8.1 Feature name and Feature ID

A00008484 - IN Terminating Trigger Feature Interactions

8.2 Description

8.2.1 Introduction

The CustomNet product has remained largely unchanged for a number of years. Users are demanding the enhanced services provided on various VoIP platforms without wanting to change from their existing CustomNet service.

The whole project provides the vehicle to enhance CustomNet so the user can retain existing functionality whilst adding new functionality from various application server platforms to provide features such as:

- Presence
- Instant Messaging
- Document sharing/collaboration
- Click to Call
- Find-me/Follow-me

Most enhanced features to be delivered from the application servers can be mapped into one of three call models:

- Call Notification (supports Presence, Call Logs, etc)

This model involves informing the application servers that the user is involved in a call and with whom. It is applied on all originating calls and is the default model for terminating calls.

- Call Routing (supports Find-me/Follow-me, Call Screening, etc)

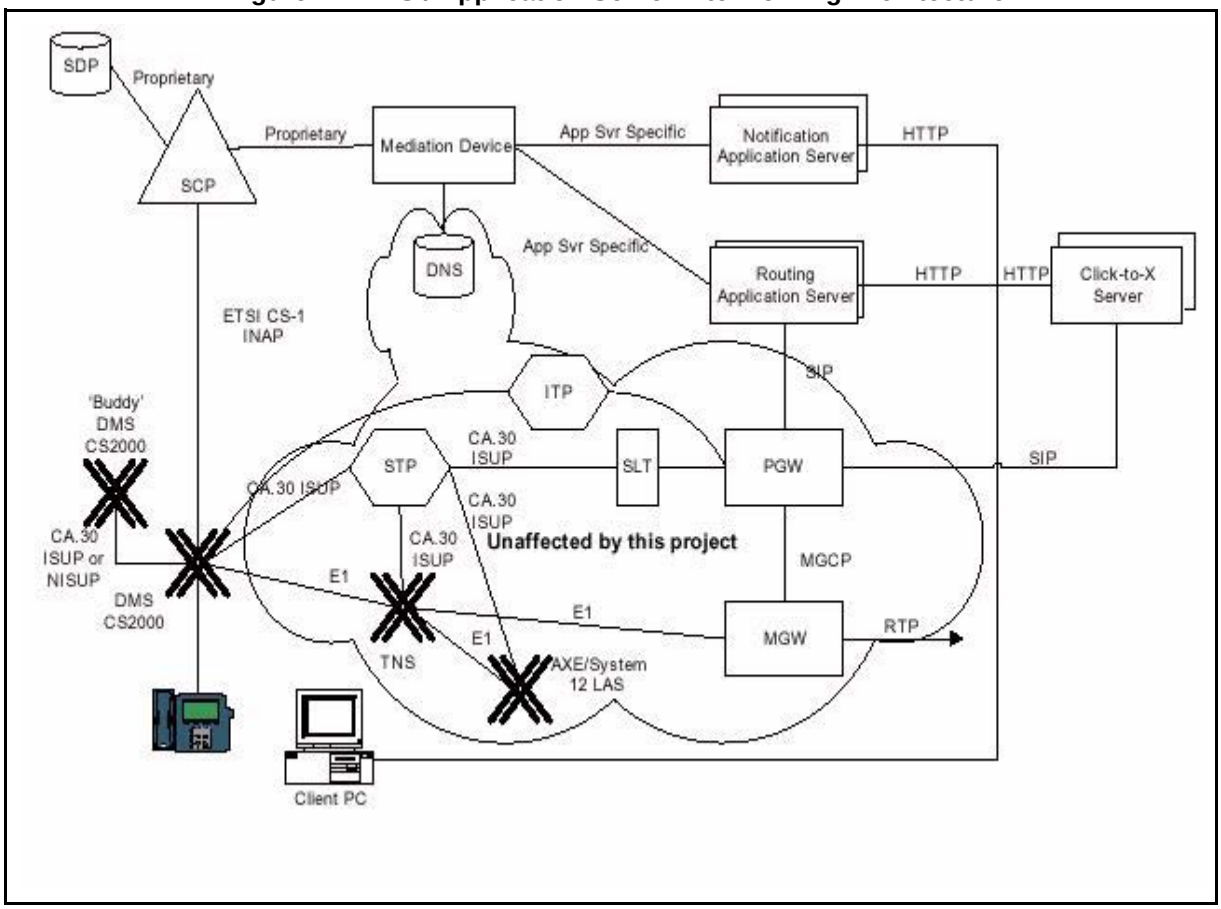
This model is only applicable for incoming calls and even then, only for a certain set of services under a limited set of conditions. The routing information must be either a single destination or a sequence (e.g. forwarding on busy or no answer).

- Click-to-X (supports Click-to-call, some forms of conferencing, etc)

Where an application server must initiate calls then this model applies.

The architecture, as seen in figure “DMS / Application Server Interworking Architecture” on page 118, consists of several elements that essentially convert events in the DMS/CS2000 switch captured through traditional IN triggers (TDP-3, originating EDPs, TDP-12, terminating EDPs) and convert them to messages for interworking with the application servers.

Figure 1 DMS / Application Server Interworking Architecture



These call models however, do not support many low-level line based features which are best supported from the access exchange which implies a co-existence between IN and non-IN features (which are listed in table “Feature list” on page 118) which is the subject of this part of the whole project.

Table 1 Feature list

Feature Name
Account Codes

Feature Name
Additional Directory Number
Authorisation Codes
Automatic Call Back (RAG)
Automatic Dial (AUD)
Busy Verification
Call Barring (Network Class Of Service)
Call Forward All Calls (CFI)
Call Forward Busy - Block Internal (CBI)
Call Forward Busy (CFB)
Call Forward Extensions
Call Forward No Answer (CFD)
Call Hold
Call Park (PRK)
Call Pick Up Group (CPU)
Calling Name Delivery
Calling Name Display
Calling Number Delivery
Calling Number Display
Camp-On (MBSCAMP)
Class Of Service Restrictions
Conference 6 (CNF C06)
Date & Time
Direct Call Park (DCPK)
Direct Station Select/Busy Lamp Field (BLF)
Directed Call Pick Up (DCPU)
Display Queued Calls

Feature Name
Do Not Disturb
Flexible Console Alerting
Intercom Group (GIC)
Key Short Hunt (KSH)
Last Number Redial (LNR)
Last Number Redial from Set (LNRA)
Multiple Appearance Of Directory Numbers (MDN)
Music on Hold (KSMOH)
Permanent Hold (HLD) Including Music on Hold
Speed Call Long (SCL)
Speed Call Short (SCS)
Transfer, Hold & 3 way Conference (CXR)

8.2.2 Interaction Model

Since non-IN features listed may involve multi-leg calls (i.e. CXR) it is best to describe the interactions based on the scenarios where calls are a combination of basic call and IN call.

8.2.2.1 Basic Call

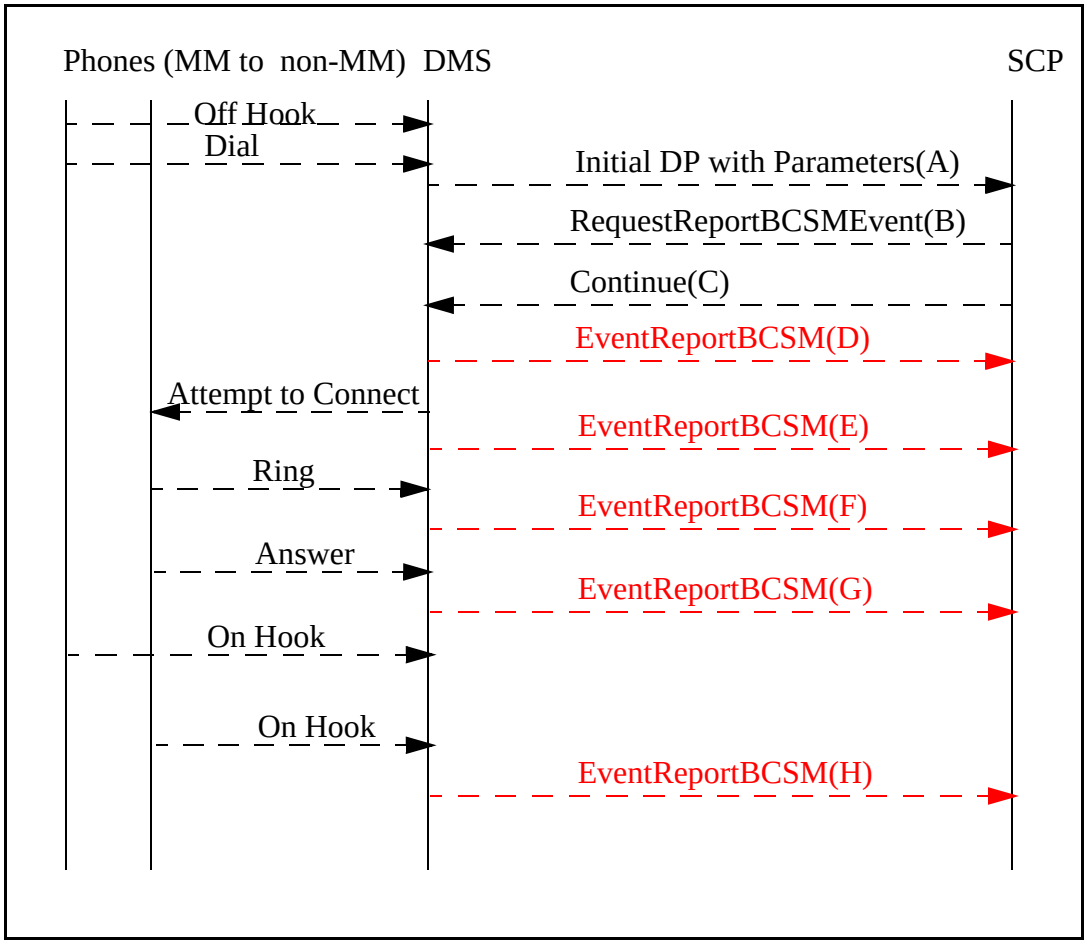
Neither TDP-3 nor TDP-12 triggering occurs.

8.2.2.2 IN Call

Multiple IN dialogs (i.e. TDP-3 and TDP-12 together) for a single call at the same time are not supported. An IN call may be thought as one of the followings:

8.2.2.2.1 MM to non-MM

In this case TDP-3 triggering occurs.



(A) Initial DP with Parameters:

The parameters sent to the SCP are SERVKEY, CLI, CDPA, EVENT_TYPE, OCN, RDN and RD_INFO.

EVENT_TYPE in this scenario is INFOANAL which means TDP-3. OCN, RDN and RD_INFO is to be used for call forward cases.

(B) RequestReportBCSMEvent:

The originating BCSM events armed by the SCP are EDP-4(N), EDP-5(N), EDP-6(N), EDP-7(N), EDP-9(N, for port1 and port 2) and EDP-10(N). Since the only functions of interest for originating calls are those associated with the Call Notification model, Notify and Continue EDPs are used for Presence, Call Logs, etc.

(C) Continue

Since the only functions of interest for originating calls are those associated with the Call Notification model, Continue is sent for Presence, Call Logs, etc.

(D) EventReportBCSM:

At this point EDP-4(Route Select Failure) or EDP-10(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended.

(E) EventReportBCSM:

At this point EDP-5(Busy) or EDP-10(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended.

(F) EventReportBCSM:

At this point EDP-6(No Answer) or EDP-10(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended.

(G) EventReportBCSM:

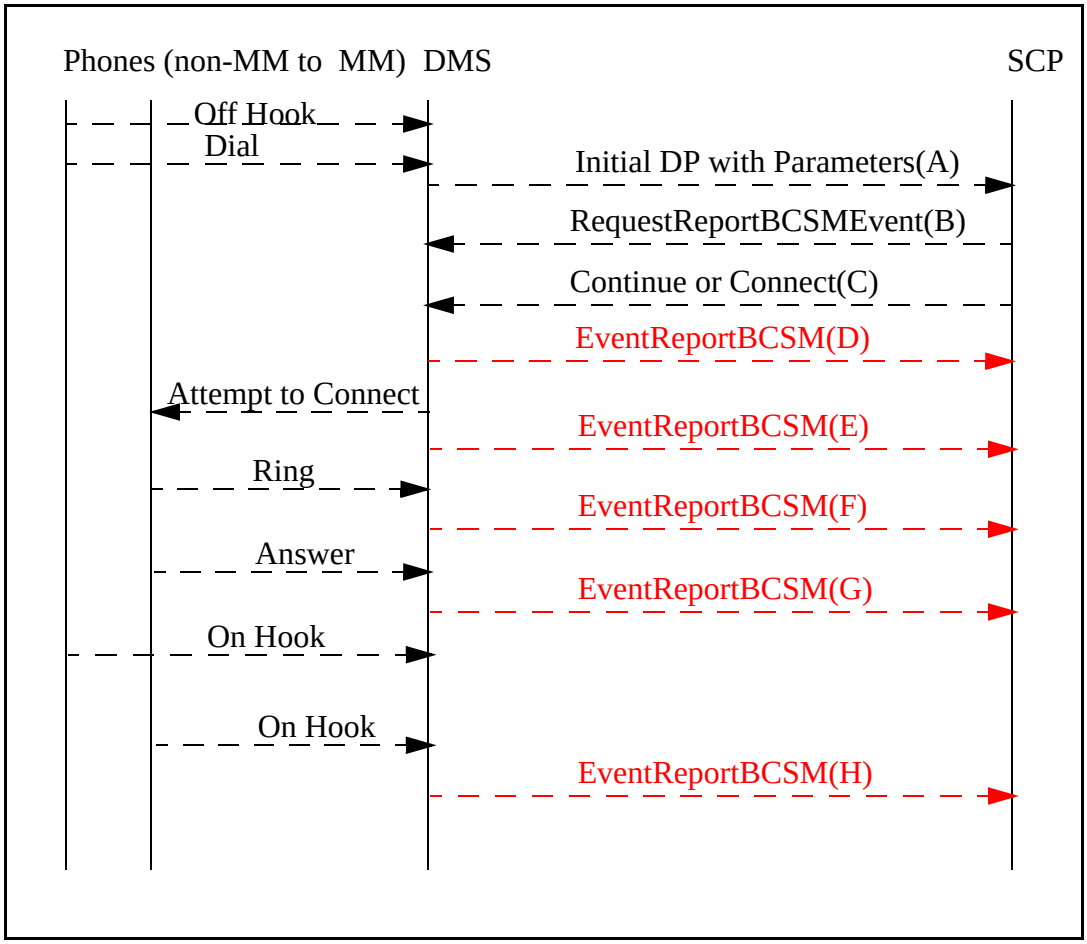
At this point call is answered and EDP-7(Answer) is encountered. EventReportBCSM is sent to SCP to notify that the call has been answered.

(H) EventReportBCSM:

At this point either the calling party or the called party on hooked and EDP-9(Disconnect) is encountered. EventReportBCSM is sent to SCP to notify that the call has been ended by the calling party(EventReportBCSMEvent for port 1) or the called party(EventReportBCSMEvent for port 2).

8.2.2.2.2 Non-MM to MM

In this case TDP-12 triggering occurs.



(A) Initial DP with Parameters:

The parameters sent to the SCP are SERVKEY, CLI, CDPA, EVENT_TYPE, OCN, RDN and RD_INFO.
EVENT_TYPE in this scenario is TERMATT which means TDP-12.
OCN, RDN and RD_INFO is to be used for call forward cases.

(B) RequestReportBCSMEvent:

If Connect is to be sent after RequestReportBCSMEvent then the originating BCSM events armed by the SCP are EDP-4(N), EDP-5(R, N), EDP-6(R, N), EDP-7(N), EDP-9(N, for port1 and port 2) and EDP-10(N). If Continue is to be sent after RequestReportBCSMEvent then the terminating BCSM events armed by the SCP are EDP-13(R, N), EDP-14(R, N), EDP-15(N), EDP-17(N, for port1 and port 2) and EDP-18(N). Terminating calls make use of both the Call Notification and Call Routing models and in order to requery Interrupted EDPs are used for busy and no answer cases along with Nofify and Continue EDPs.

(C) Continue or Connect

Terminating calls make use of both the Call Notification and Call Routing models and there are 3 possibilities for Call Routing model(Call Notification is similar to that used for originating calls except for the use of TDP-12 and terminating EDPs) as follows:

After querying the AS;

- if the destination number is that of the terminating MM user itself then the SCP issues a Continue message.
- if the destination number is not that of terminating MM user itself then the SCP issues a Connect message to connect the call directly.
- if the call is to be routed through AS then the SCP issues a Connect message with the AS as the destination number.

(D) EventReportBCSM:

At this point EDP-4(Route Select Failure) or (EDP-10, EDP-18)(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended.

(E) EventReportBCSM:

At this point (EDP-5, EDP-13)(Busy) or (EDP-10, EDP-18)(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended. For busy cases if the EDP is interrupted then requery is also possible.

(F) EventReportBCSM:

At this point (EDP-6, EDP-14)(No Answer) or (EDP-10, EDP-18)(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended. For no answer cases if the EDP is interrupted then requery is also possible.

(G) EventReportBCSM:

At this point call is answered and (EDP-7, EDP-15)(Answer) is encountered. EventReportBCSM is sent to SCP to notify that the call has been answered.

(H) EventReportBCSM:

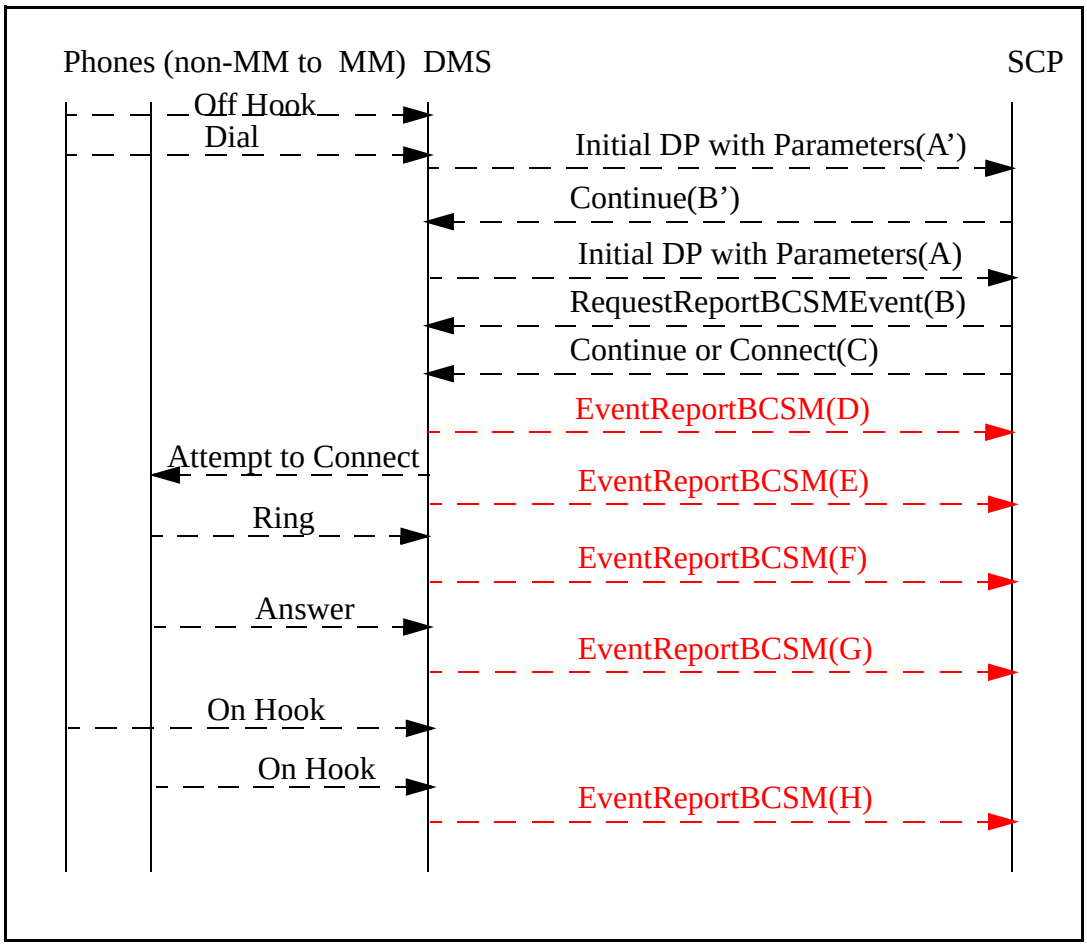
At this point either the calling party or the called party on hooked and (EDP-9, EDP-17)(Disconnect) is encountered. EventReportBCSM is sent to SCP to notify that the call has been ended by the calling

party(EventReportBCSMEvent for port 1) or the called party(EventReportBCSMEvent for port 2).

8.2.2.2.3 MM to MM

This case involves both the TDP-3 triggering and the TDP-12 triggering but since two open IN dialogs can not co-exist a workaround is proposed as follows:

After TDP-3 triggering, the SCP, by the help of the SDP, checks the calling and called parties for whether both are multimedia users in the same switch or not. If so (it is in this case) then SCP will not arm EDPs (this lets TDP-12 triggering) and the multimedia session will be provided by TDP-12 and terminating EDPs.



(A') Initial DP with Parameters:

The parameters sent to the SCP are SERVKEY, CLI, CDPA, EVENT_TYPE, OCN, RDN and RD_INFO.

EVENT_TYPE in this scenario is INFOANAL which means TDP-3.
OCN, RDN and RD_INFO is to be used for call forward cases.

(B') Continue

Since at this point, the SCP, by the help of the SDP, determines that the calling and called parties both are multimedia users in the same switch and the only functions of interest for originating calls are those associated with the Call Notification model, Continue is sent for Presence, Call Logs, etc without sending RequestReportBCSMEvent.

(A) Initial DP with Parameters:

The parameters sent to the SCP are SERVKEY, CLI, CDPA, EVENT_TYPE, OCN, RDN and RD_INFO.
EVENT_TYPE in this scenario is TERMATT which means TDP-12.
OCN, RDN and RD_INFO is to be used for call forward cases.

(B) RequestReportBCSMEvent:

If Connect is to be sent after RequestReportBCSMEvent then the originating BCSM events armed by the SCP are EDP-4(N), EDP-5(R, N), EDP-6(R, N), EDP-7(N), EDP-9(N, for port1 and port 2) and EDP-10(N). If Continue is to be sent after RequestReportBCSMEvent then the terminating BCSM events armed by the SCP are EDP-13(R, N), EDP-14(R, N), EDP-15(N), EDP-17(N, for port1 and port 2) and EDP-18(N). Terminating calls make use of both the Call Notification and Call Routing models and in order to requery Interrupted EDPs are used for busy and no answer cases along with Nofify and Continue EDPs.

(C) Continue or Connect

Terminating calls make use of both the Call Notification and Call Routing models and there are 3 possibilities for Call Routing model(Call Notification is similar to that used for originating calls except for the use of TDP-12 and terminating EDPs) as follows:

After querying the AS;

- if the destination number is that of the terminating MM user itself then the SCP issues a Continue message.
- if the destination number is not that of terminating MM user itself then the SCP issues a Connect message to connect the call directly.
- if the call is to be routed through AS then the SCP issues a Connect message with the AS as the destination number.

(D) EventReportBCSM:

At this point EDP-4(Route Select Failure) or (EDP-10, EDP-18)(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended.

(E) EventReportBCSM:

At this point (EDP-5, EDP-13)(Busy) or (EDP-10, EDP-18)(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended. For busy cases if the EDP is interrupted then requery is also possible.

(F) EventReportBCSM:

At this point (EDP-6, EDP-14)(No Answer) or (EDP-10, EDP-18)(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended. For no answer cases if the EDP is interrupted then requery is also possible.

(G) EventReportBCSM:

At this point call is answered and (EDP-7, EDP-15)(Answer) is encountered. EventReportBCSM is sent to SCP to notify that the call has been answered.

(H) EventReportBCSM:

At this point either the calling party or the called party on hooked and (EDP-9, EDP-17)(Disconnect) is encountered. EventReportBCSM is sent to SCP to notify that the call has been ended by the calling party(EventReportBCSMEvent for port 1) or the called party(EventReportBCSMEvent for port 2).

As seen from the figure above, MM to MM case may be summarized in terms of the MM to non-MM and non-MM to MM cases as follows:

- MM to non-MM case (TDP-3 triggering occurs however no RequestReportBCSMEvent is sent).
- non-MM to MM case (TDP-12 triggering occurs).

8.2.3 Feature Interactions

8.2.3.1 Account Codes

No impact.

8.2.3.2 Additional Directory Number

No impact.

8.2.3.3 Authorisation Codes

No impact.

8.2.3.4 Automatic Call Back (RAG)

A off-hooks and dials B(busy) which results in the following IN call.

IN Call	
A	B(busy)

ERB(s) reported: Busy
Remaining EDP(s): If reported ERB is R then EDPs armed for port 1 remain. If reported ERB is N then no EDPs remain.

If B is busy, (EDP-5(N), EDP-13(N)) is encountered and Busy EventReportBCSM is sent to SCP to notify that the call has ended and A hears busy tone. A activates RAG and on-hooks. When B on-hooks, A rings and after A off-hooks B is called automatically as if A dials B again which results in the following IN call.

IN Call	
A	B

This is the same as a normal IN call from A to B although it is a RAG generated call.

Limitation / Restriction:

If EDP-5(R) or EDP-13(R) is used then Busy ERB is reported but the caller does not hear busy tone (since the SSP waits instructions from the SCP, like connecting to a new destination) and can not use the RAG feature. However after Busy ERB is reported, if a Continue or EDP-5(N) or EDP-13(N) followed by a Continue or a Connect to a busy destination or EDP-5(N) or EDP-13(N) followed by a Connect to a busy destination is sent then it is still possible to invoke RAG. For Connect scenarios to another busy destination RAG is activated for the second call.

8.2.3.5 Automatic Dial (AUD)

No impact.

8.2.3.6 Busy Verification

This is an MSAC related feature and IN interaction with MSAC is not supported.

8.2.3.7 Call Barring (Network Class Of Service)

No impact.

8.2.3.8 Call Forward All Calls (CFI)

There are three possible scenarios as follows:

(a) Both the original and the forwarded calls are IN calls.

A off-hooks and dials B which results in the following IN call.

IN Call(1)	
A	B

This is a normal IN call although B does not ring. The call is treated as if A called another party if forwarded call does not produce a new IN trigger.

If B has CFI to C, then B does not ring and call is immediately transferred to C and if this transfer produces a new IN dialog then the first IN dialog is aborted except a TDP-12 does not abort a previous TDP-3.

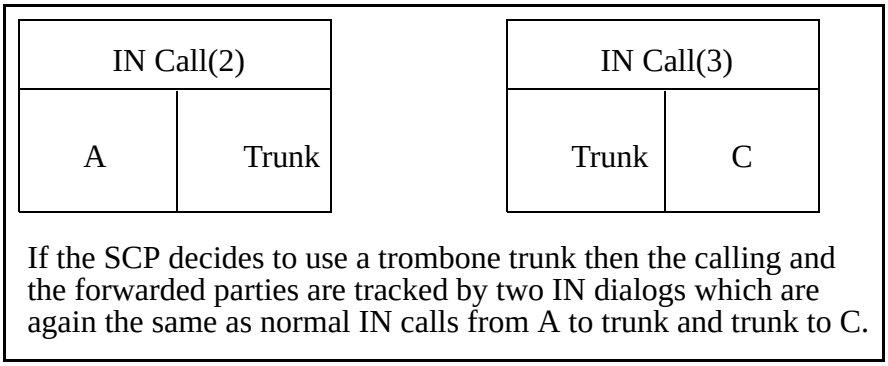
For this new IN dialog there are call forwarding parameters present.

If trombone trunking is not used:

IN Call(2)	
A	C

The forwarded call produced a new IN trigger which aborts the previous one (only TDP-3 aborts a previous dialog). This is the same as a normal IN call from A to C.

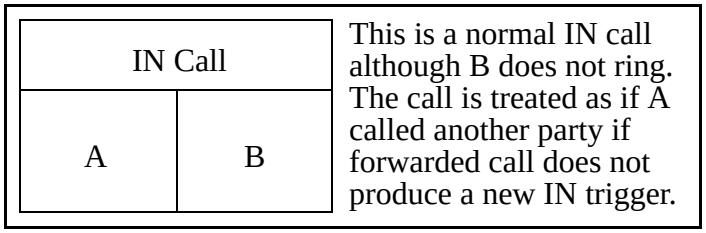
If trombone trunking is used:



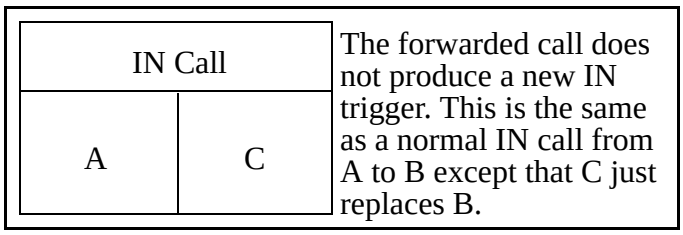
If the SCP decides to use a trombone trunk then the calling and the forwarded parties are tracked by two IN dialogs which are again the same as normal IN calls from A to trunk and trunk to C.

(b) The original call is an IN call but the forwarded call is not.

A off-hooks and dials B which results in the following IN call.



If B has CFI to C, then B does not ring and call is immediately transferred to C and if this transfer does not produce a new IN dialog then the first IN dialog is used.

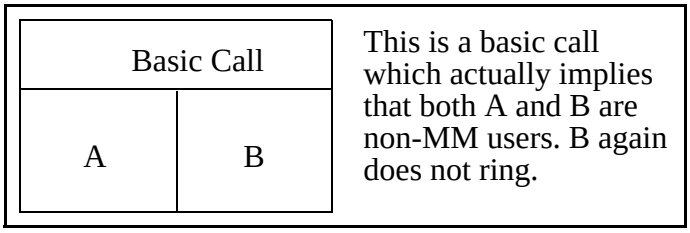


Limitation / Restriction:

SCP does not understand that C has replaced B.

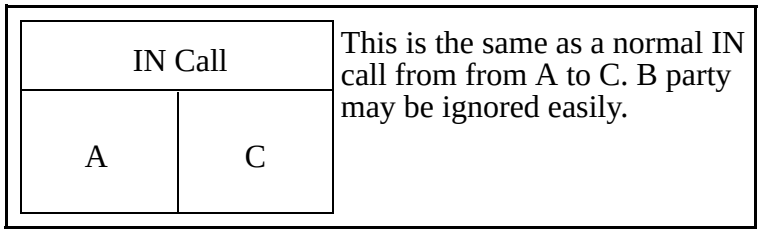
(c) The original call is not an IN call but the forwarded call is.

A off-hooks and dials B which results in the following basic call.



If B has CFI to C then B does not ring and call is immediately transferred to C and if this transfer produces an IN dialog then this IN dialog is used.

For this IN dialog there are call forwarding parameters present.



8.2.3.9 Call Forward Busy - Block Internal (CBI)

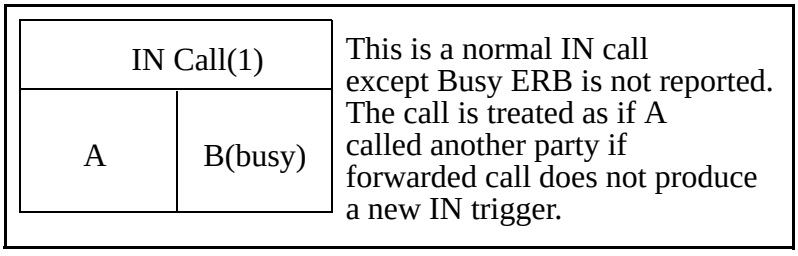
This is the same as the CFB case except that internal calls are blocked and are not forwarded. In other words, if the call is external then it is treated as CFBcase and if the call is internal it is treated as an IN call to a busy party.

8.2.3.10 Call Forward Busy (CFB)

There are three possible scenarios as follows (A, B or C may be trunks):

(a) Both the original and the forwarded calls are IN calls.

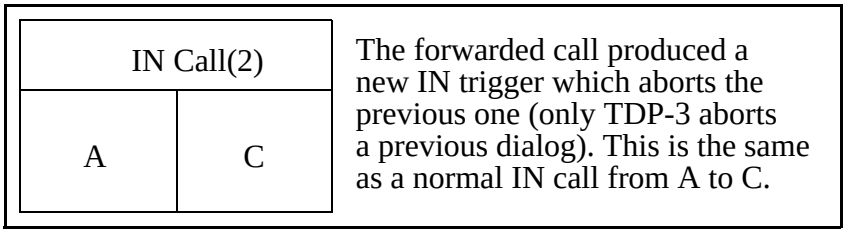
A off-hooks and dials B(busy) which results in the following IN call.



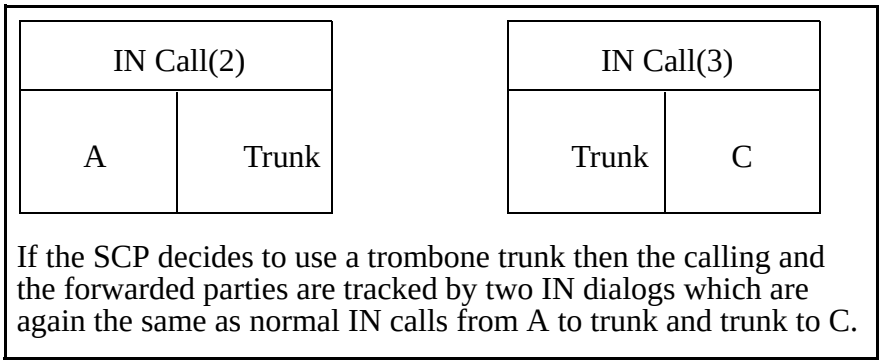
If B has CFB to C and B is busy then call is immediately transferred to C without hitting (EDP-5, EDP-13)(Busy) and if this transfer produces a new IN dialog then the first IN dialog is aborted except a TDP-12 does not abort a previous TDP-3.

For this new IN dialog there are call forwarding parameters present.

If trombone trunking is not used:

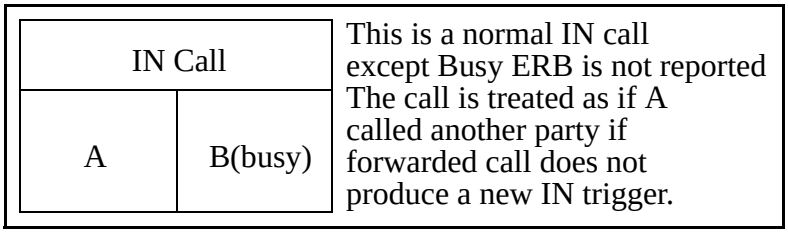


If trombone trunking is used:

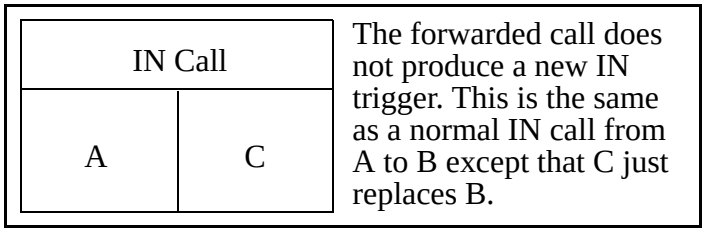


(b) The original call is an IN call but the forwarded call is not.

A off-hooks and dials B(busy) which results in the following IN call.



If B has CFB to C and B is busy then call is immediately transferred to C without hitting (EDP-5, EDP-13)(Busy) and if this transfer does not produce a new IN dialog then the first IN dialog is used. (EDP-5, EDP-13)(Busy) is still valid.

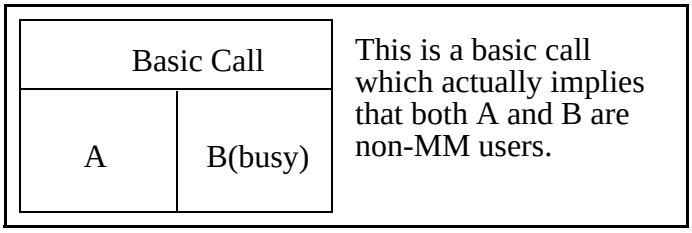


Limitation / Restriction:

SCP does not understand that C has replaced B.

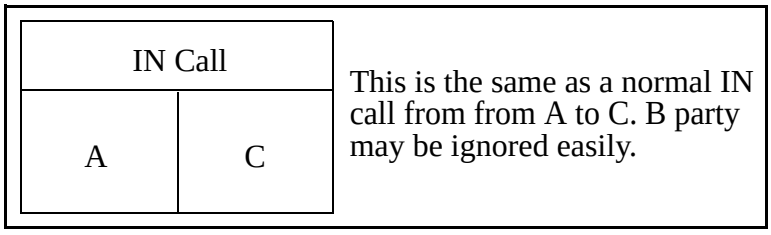
(c) The original call is not an IN call but the forwarded call is.

A off-hooks and dials B(busy) which results in the following basic call.



If B has CFB to C and B is busy then call is immediately transferred to C and if this transfer produces an IN dialog then this IN dialog is used.

For this IN dialog there are call forwarding parameters present.



8.2.3.11 Call Forward Enhancements

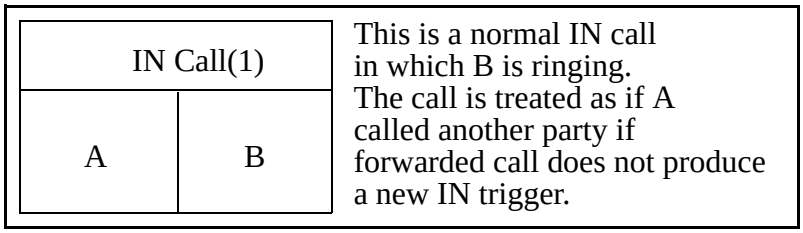
This is similar to other call forward cases as it enhances them. For the description of this feature please see Appendix section at the end of this document.

8.2.3.12 Call Forward No Answer (CFD)

There are three possible scenarios as follows (A, B or C may be trunks):

(a) Both the original and the forwarded calls are IN calls.

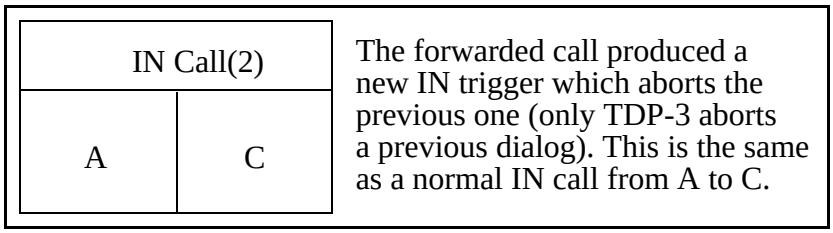
A off-hooks and dials B which results in the following IN call.



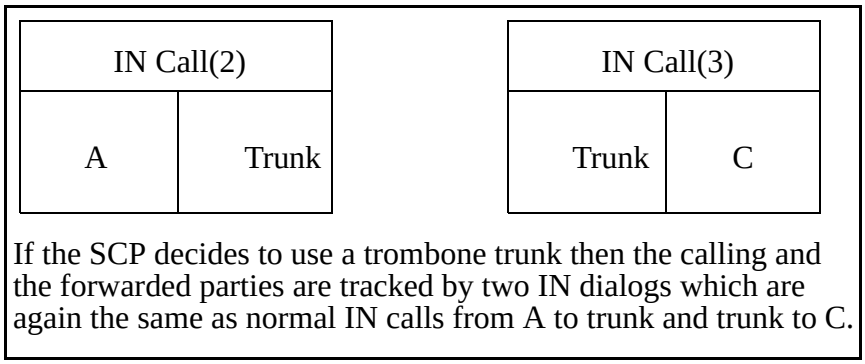
If B has CFD to C and B does not answer then call is transferred to C if EDP-6 timer > CFD timer and if this transfer produces a new IN dialog then the first IN dialog is aborted except a TDP-12 does not abort a previous TDP-3. If EDP-6 timer < CFD timer then EDP-6 has precedence and call forwarding will not occur. EDP-6 timer = CFD timer case is not supported.

For this new IN dialog there are call forwarding parameters present.

If trombone trunking is not used:

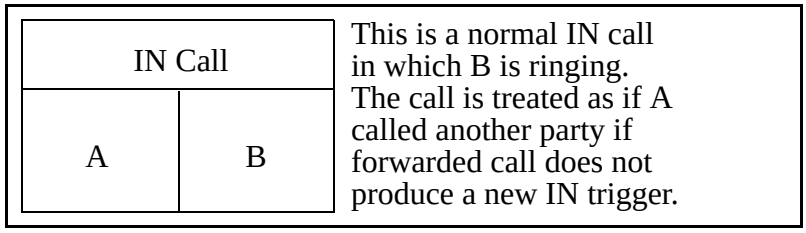


If trombone trunking is used:

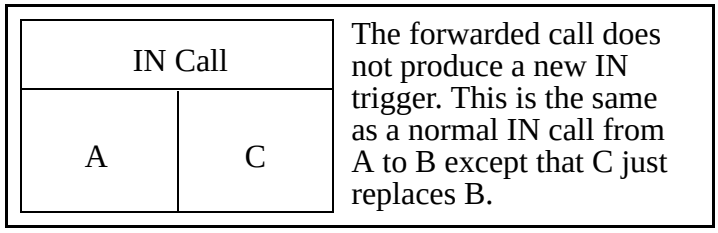


(b) The original call is an IN call but the forwarded call is not.

A off-hooks and dials B which results in the following IN call.



If B has CFD to C and B does not answer then call is transferred to C if EDP-6 timer > CFD timer and if this transfer does not produce a new IN dialog then the first IN dialog is used. EDP-6 is still valid. If EDP-6 timer < CFD timer then EDP-6 has precedence and call forwarding will not occur. EDP-6 timer = CFD timer case is not supported.

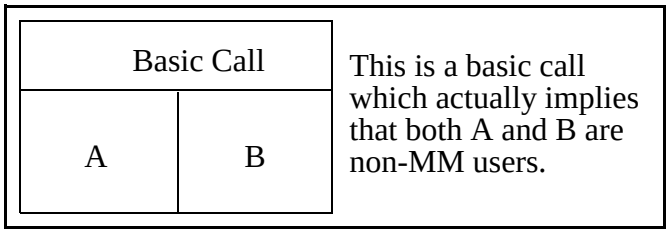


Limitation / Restriction:

SCP does not understand that C has replaced B.

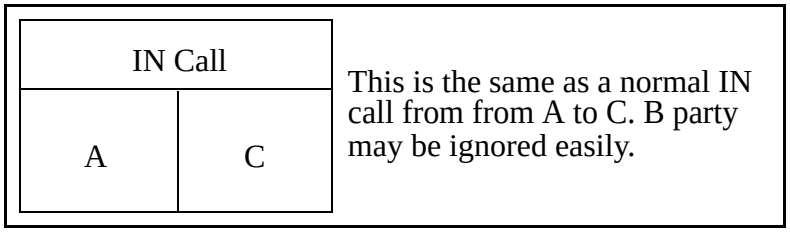
(c) The original call is not an IN call but the forwarded call is.

A off-hooks and dials B which results in the following basic call.



If B has CFD to C and C does not answer then call is immediately transferred to C and if this transfer produces an IN dialog then this IN dialog is used.

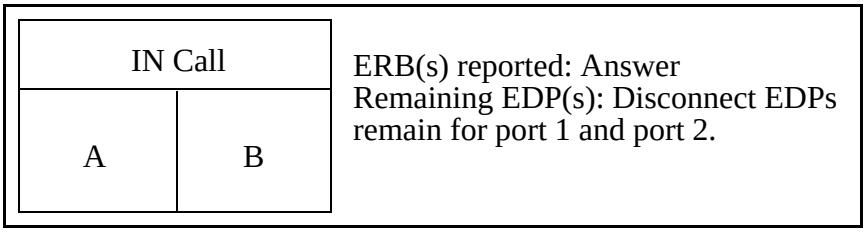
For this IN dialog there are call forwarding parameters present.



8.2.3.13 Call Hold

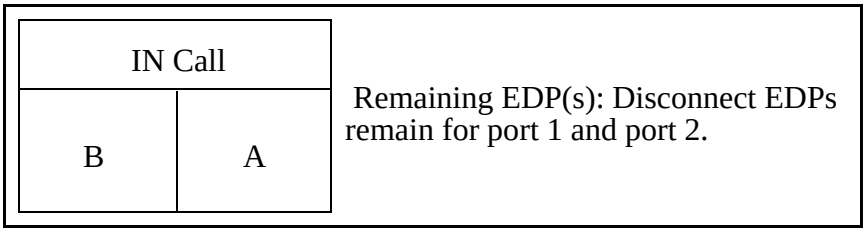
(a) The calling party activates CHD.

A and B are talking in an IN call as follows:



A activates CHD and B is on hold. If A reactivates CHD, it returns back to the original call above.

If A on-hooks the controller is migrated to port 2 if it is not already on port 2 as follows and A is rering by B and A answers. This answer does not produce a new Answer ERB since it has already been reported.



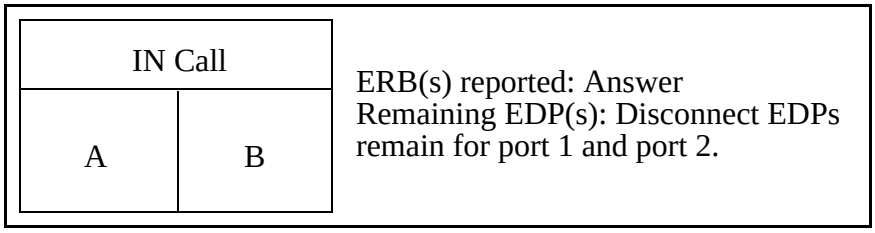
After this point if A on-hooks a Disconnect ERB is reported for port 2 and if B on-hooks a Disconnect ERB is reported for port 1.

If A does not answer the rering until timeout then a Disconnect ERB is reported for port 2.

While on hold if B on-hooks a Disconnect ERB is reported for port 1.

(b) The called party activates CHD.

A and B are talking in an IN call as follows:



B activates CHD and A is on hold. If B reactivates CHD, it returns back to the original call above.

If B on-hooks, the controller is not migrated to port 2 as it is already on port 2 and B is rering by A and B answers. This answer does not produce a new Answer ERB since it has already been reported.

After this point if A on-hooks a Disconnect ERB is reported for port 1 and if B on-hooks a Disconnect ERB is reported for port 2.

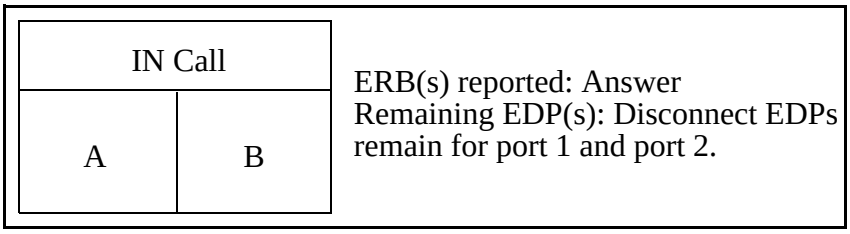
If B does not answer the rering until timeout then a Disconnect ERB is reported for port 2.

While on hold if A on-hooks a Disconnect ERB is reported for port 1.

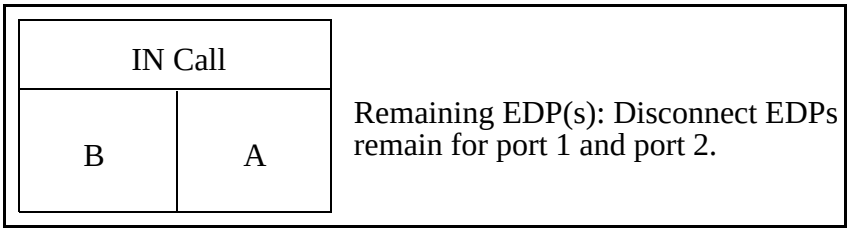
8.2.3.14 Call Park (PRK)

(a) The calling party activates PRK.

A and B are talking in an IN call as follows:



A activates PRK and B is parked. The parkee is migrated to port 1 if it is not already on port 1 as follows.



A reactivates PRK and retrieves B and after this point if A on-hooks a Disconnect ERB is reported for port 2 and if B on-hooks a Disconnect ERB is reported for port 1.

While parked if B on-hooks a Disconnect ERB is reported for port 1.

(b) The called party activates PRK.

A and B are talking in an IN call as follows:

IN Call		ERB(s) reported: Answer Remaining EDP(s): Disconnect EDPs remain for port 1 and port 2.
A	B	

B activates PRK and A is parked. The parkee is not migrated to port 1 as it is already on port 1. B activates PRK and retrieves A and after this point if A on-hooks a Disconnect ERB is reported for port 1 and if B on-hooks a Disconnect ERB is reported for port 2.

While parked if A on-hooks a Disconnect ERB is reported for port 1.

8.2.3.15 Call Pick Up Group (CPU)

A dials B which results in the following IN call.

IN Call		This is a normal IN call in which B is ringing.
A	B	

Before B answers and EDP-6 timer expires, C activates CPU and an Answer ERB is reported. After this point if A on-hooks a Disconnect ERB is reported for port 1 and if C on-hooks a Disconnect ERB is reported for port 2.

IN Call		This is the same as a normal IN call from A to B except that C just replaces B.
A	C	

Limitation / Restriction:

SCP does not understand that C has replaced B.

8.2.3.16 Calling Name Delivery

No impact.

8.2.3.17 Calling Name Display

No impact.

8.2.3.18 Calling Number Delivery

No impact.

8.2.3.19 Calling Number Display

No impact.

8.2.3.20 Camp-On (MBSCAMP)

(a) Both the call to be camped on and the call that camps on are IN calls.

A and B are talking in an IN call as follows:

IN Call(1)	
A	B

ERB(s) reported: Answer
Remaining EDP(s): Disconnect EDPs remain for port 1 and port 2.

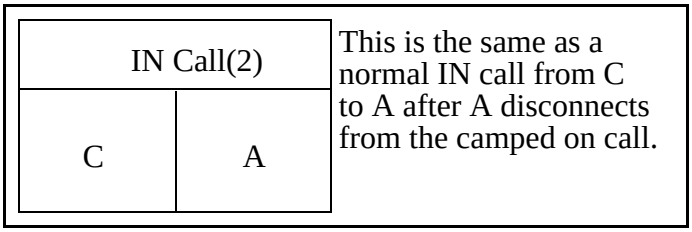
C has MBSCAMP and dials A and hears audible ringback tone instead of busy tone. A hears a special tone. Busy and No Answer ERBs are not reported.

IN Call(2)	
C	A

This is the same as a normal IN call from C to A except that Busy and No Answer ERBs are not reported and C hears ringback tone instead of busy tone.

If B on-hooks a Disconnect ERB is reported for port 2 from the first IN dialog. A on-hooks and rings. When A answers an Answer ERB is reported from the second IN dialog.

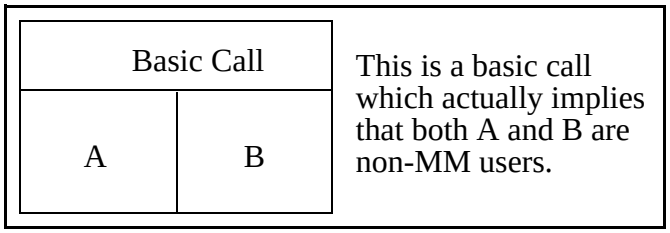
If A on-hooks a Disconnect ERB is reported for port 1 from the first IN dialog. A rings. When A answers an Answer ERB is reported from the second IN dialog.



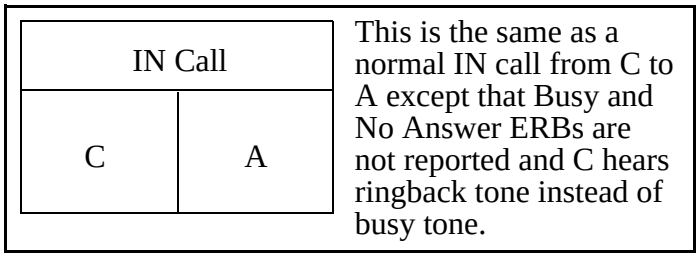
After this point if A on-hooks a Disconnect ERB is reported for port 2 and if C on-hooks a Disconnect ERB is reported for port 1.

(b) The call to be camped on is a basic call and the call that camps on is an IN call.

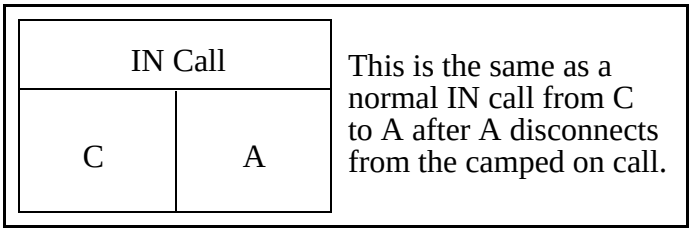
A and B are talking in a basic call as follows:



C has MBSCAMP and dials A and hears audible ringback tone instead of busy tone. A hears a special tone. Busy and No Answer ERBs are not reported.



A on-hooks. A rings. When A answers an Answer ERB is reported.



After this point if A on-hooks a Disconnect ERB is reported for port 2 and if C on-hooks a Disconnect ERB is reported for port 1.

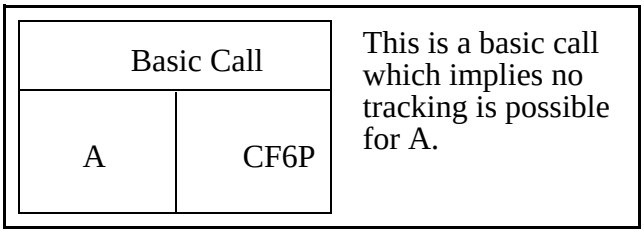
8.2.3.21 Class Of Service Restrictions

No impact.

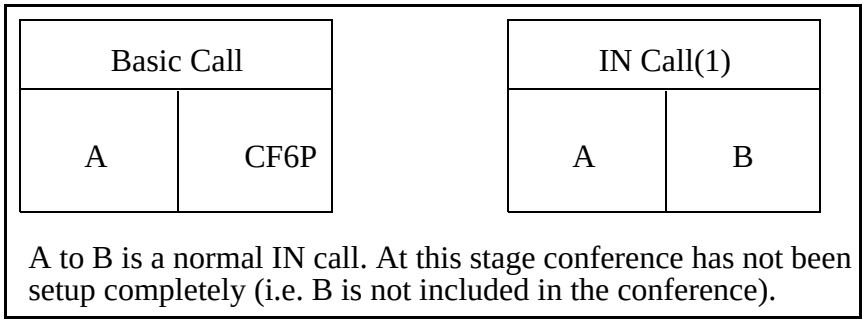
8.2.3.22 Conference 6 (CNF C06)

(a) The party which starts the conference directly activates CNF C06 without being active in a call.

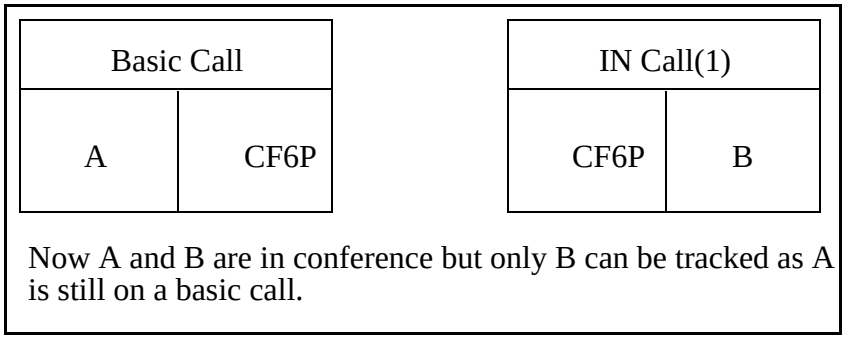
A off-hooks and activates CNF C06 which results in the following basic call:



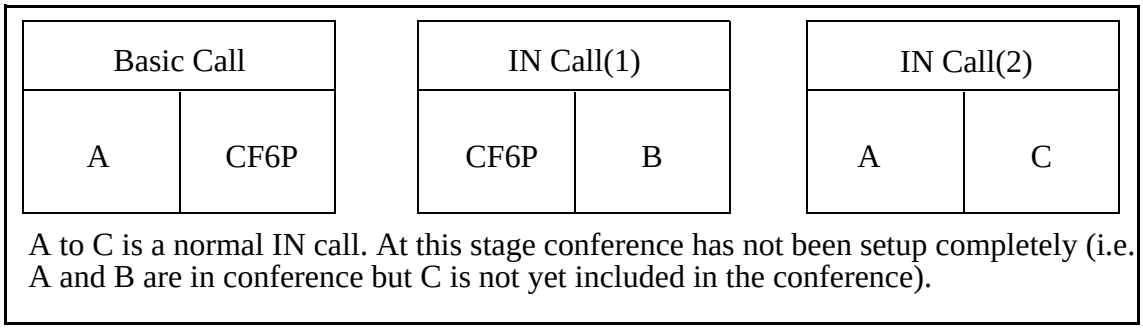
A flashes and dials B which results in the following topology:



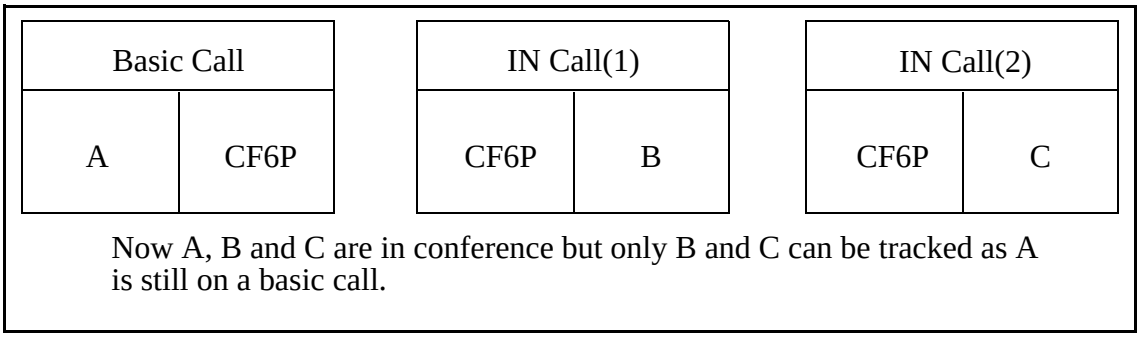
A activates CNF C06 which actually sets up the conference as follows:



A flashes and dials C which results in the following topology. This case is similar to the case above where A flashes and dials B.

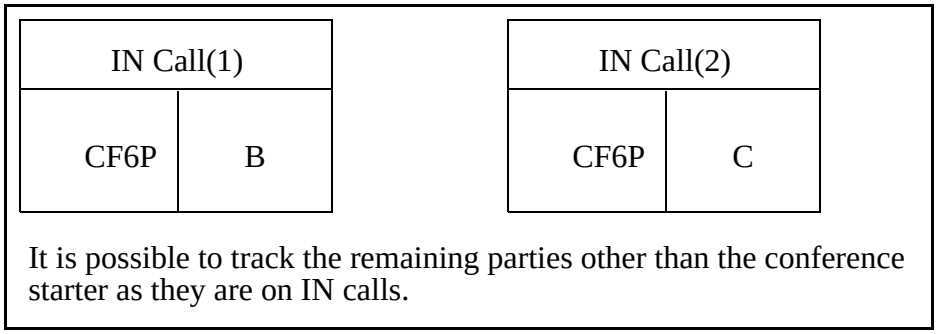


A activates CNF C06 which actually sets up the conference for all parties (i.e. C is included to the conference).



D, E and F can attend the conference in the same way.

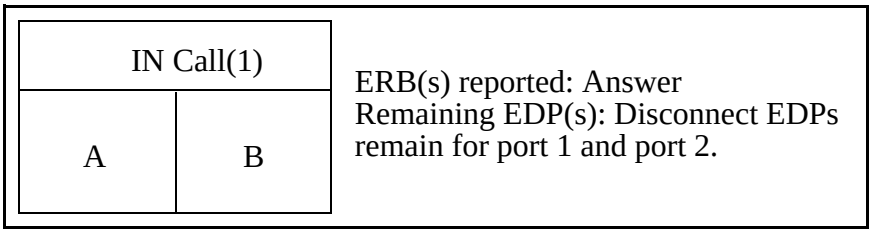
If A on-hooks no indication is sent to SCP since A is on a basic call. The remaining parties stay in conference.



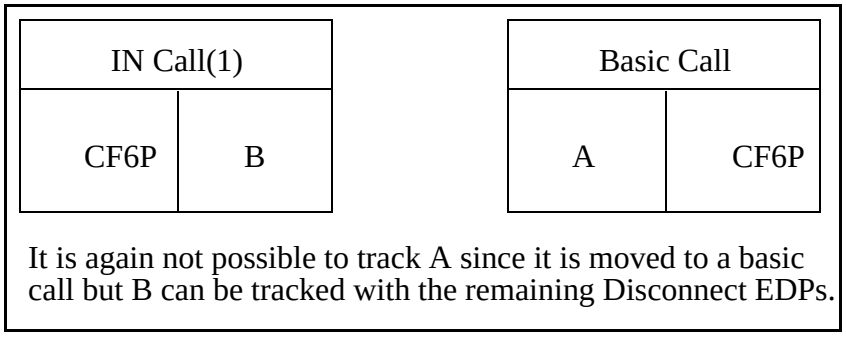
If B, C, D, E or F on-hooks a Disconnect ERB is reported for port 2.

(b) The party which starts the conference is already active in an IN call.

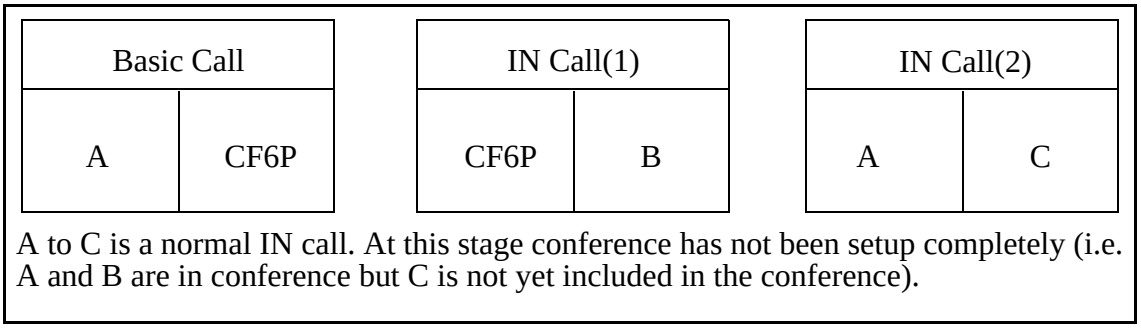
A and B are talking in an IN Call as follows:



A activates CNF C06 which immediately sets up the conference.

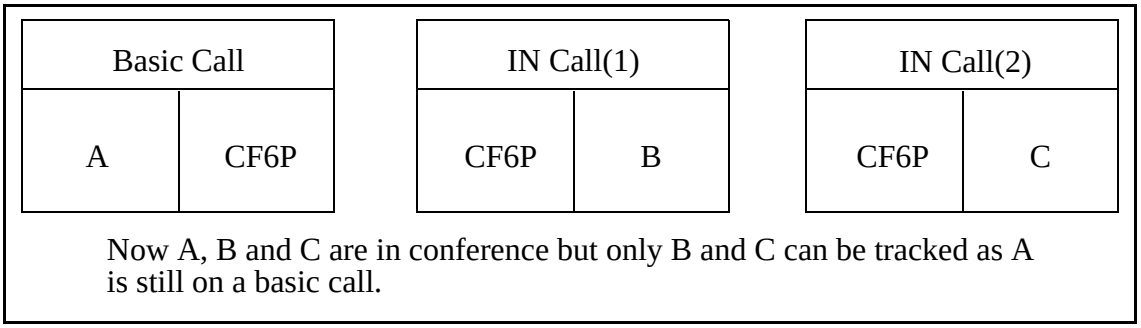


A flashes and dials C which results in the following topology. This case is similar to the case in (a) where A flashes and dials C.



A to C is a normal IN call. At this stage conference has not been setup completely (i.e. A and B are in conference but C is not yet included in the conference).

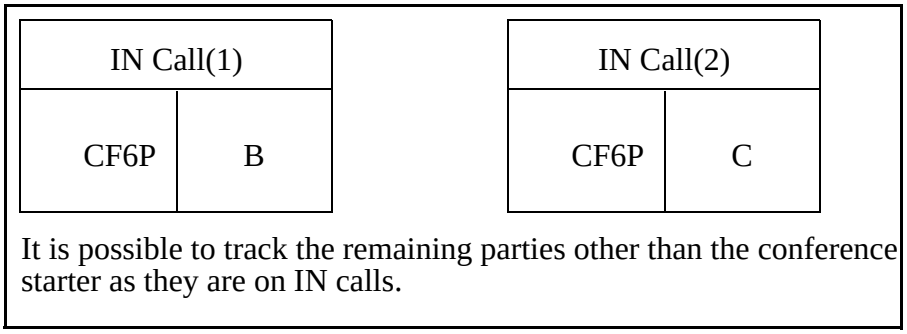
A activates CNF C06 which actually sets up the conference for all parties (i.e. C is included to the conference).



Now A, B and C are in conference but only B and C can be tracked as A is still on a basic call.

D, E and F can attend the conference in the same way.

If A on-hooks no indication is sent to SCP since A is on a basic call. The remaining parties stay in conference.



It is possible to track the remaining parties other than the conference starter as they are on IN calls.

If B, C, D, E or F on-hooks a Disconnect ERB is reported for port 2.

Limitation / Restriction:

Since the party starting the conference resides on a basic call its state is not tracked correctly. The application servers see that the party invoked multiple calls but they do not understand that whether it on-hooked or not. However it

is possible for application servers to understand whether other parties on-hooked or not. In scenarios where only 2 parties remain after the conference starter on-hooks, a Disconnect ERB is reported for port 1 for on-hooks of the remaining parties.

8.2.3.23 Console Queues

This is an MSAC related feature and IN interaction with MSAC is not supported.

8.2.3.24 Cut Through Dialling

This is an MSAC related feature and IN interaction with MSAC is not supported.

8.2.3.25 Date & Time

No impact.

8.2.3.26 Direct (ICM)

Not supported. The architecture of this feature is very different and does not pass through normal translators or terminators and hence TDP-3 and TDP-12 triggering is not possible. For the description of this feature please see Appendix section at the end of this document.

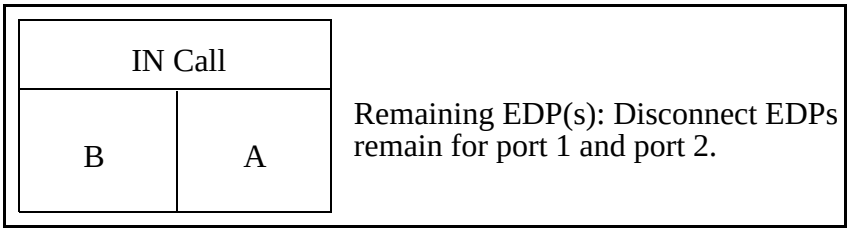
8.2.3.27 Direct Call Park (DCPK)

(a) The calling party activates DCPK.

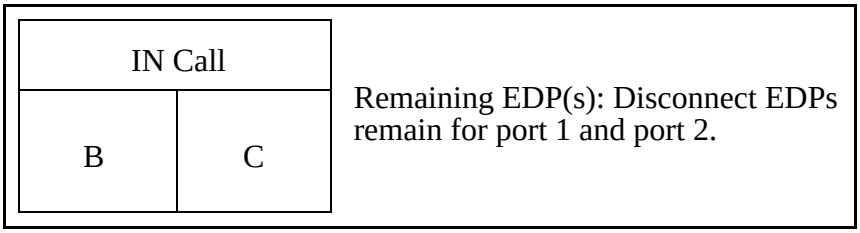
A and B are talking in an IN call as follows:

IN Call		
A	B	ERB(s) reported: Answer Remaining EDP(s): Disconnect EDPs remain for port 1 and port 2.

A activates DCPK and B is parked against C. The parkee is migrated to port 1 if it is not already on port 1 as follows.



C activates DCPK and retrieves B.

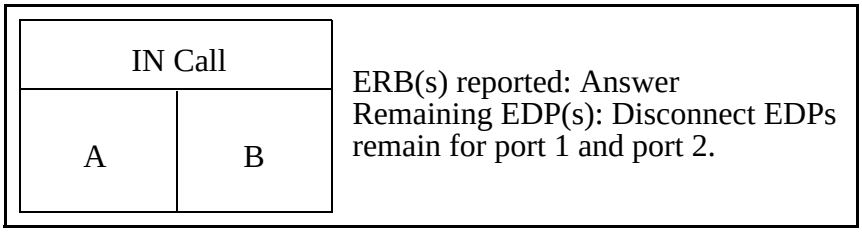


After this point if C on-hooks a Disconnect ERB is reported for port 2 and if B on-hooks a Disconnect ERB is reported for port 1.

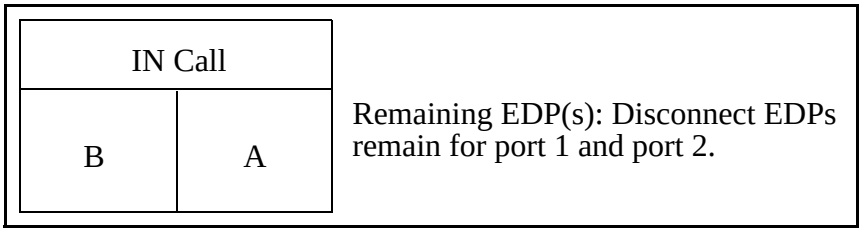
While parked if B on-hooks a Disconnect ERB is reported for port 1.

(b) The called party activates DCPK.

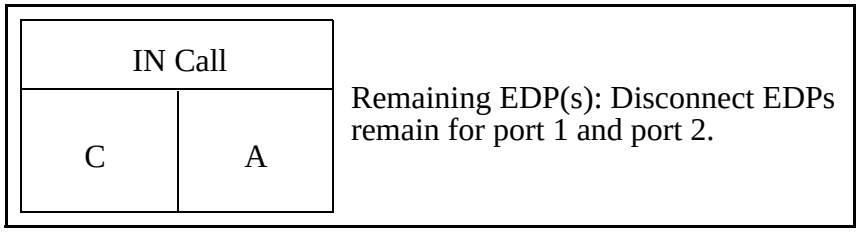
A and B are talking in an IN call as follows:



B activates DCPK and A is parked against C. The parkee is migrated to port 2 this time.



C activates DCPK and retrieves A.



After this point if A on-hooks a Disconnect ERB is reported for port 1 and if C on-hooks a Disconnect ERB is reported for port 2.

While parked if A on-hooks a Disconnect ERB is reported for port 1.

Limitation / Restriction:

SCP does not understand that C has replaced B.

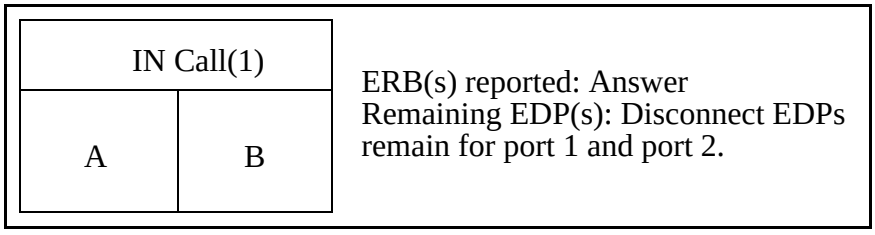
8.2.3.28 Direct Station Select/Busy Lamp Field (BLF)

For the description of this feature please see Appendix section at the end of this document.

This feature does not pass through normal translators and hence TDP-3 is not supported for BLF originated calls.

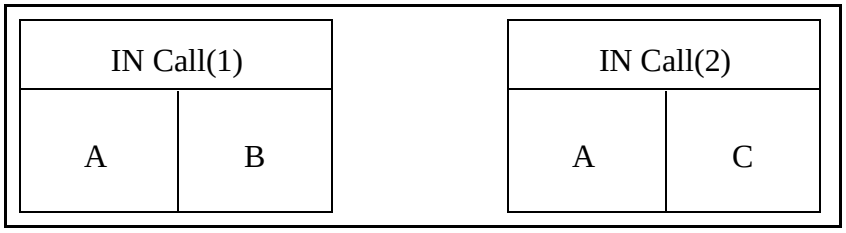
(a) BLF is used for call transfer.

A and B are talking in an IN call as follows:

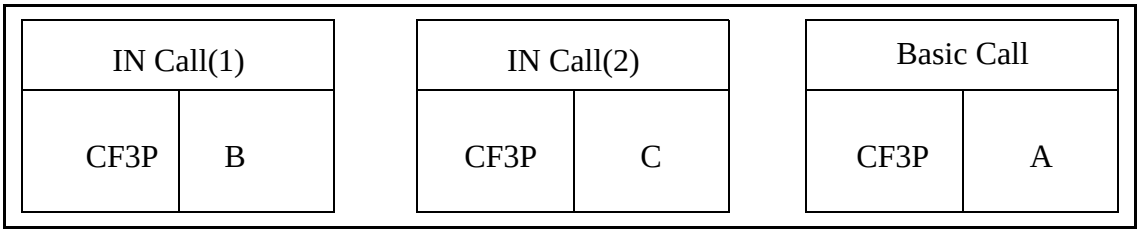


A has BLF for C and can see the status of C (i.e. when C is busy the lamp is on).

A hits Conf/Transfer key and then hits BLF key and C is dialled automatically. After this, it is similar to a CXR case.

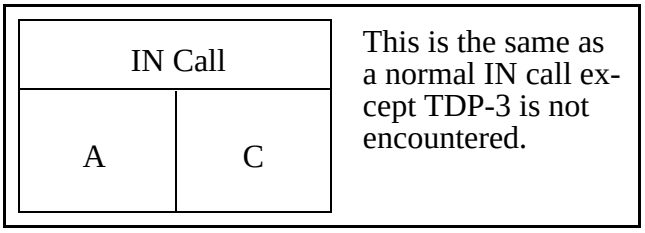


B hits Conf/Transfer key again.



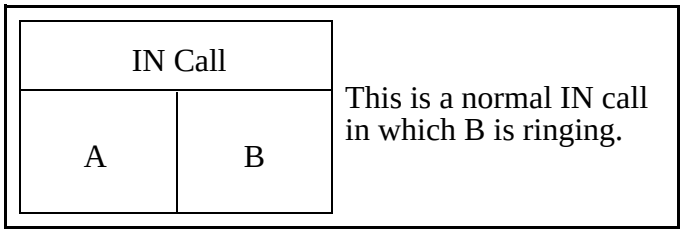
(b) BLF is used to for direct call.

A off-hooks and hits BLF key and C is dialled automatically.

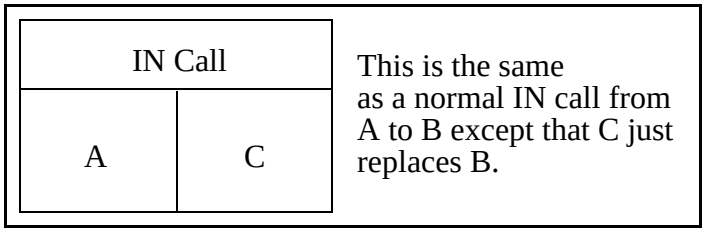


8.2.3.29 Directed Call Pickup (DCPU)

A dials B which results in the following IN call:



Before B answers and EDP-6 timer expires, C activates DCPU and an Answer ERB is reported.



After this point if A on-hooks a Disconnect ERB is reported for port 1 and if C on-hooks a Disconnect ERB is reported for port 2.

Limitation / Restriction:

SCP does not understand that C has replaced B.

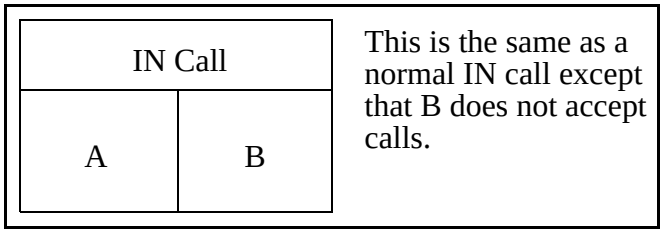
8.2.3.30 Display Queued Calls

No impact.

8.2.3.31 Do Not Disturb

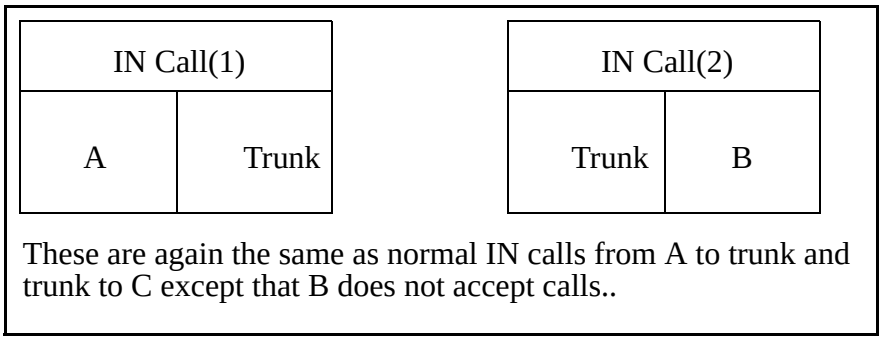
(a) Line to line call.

A dials B which results in the following IN call.



Call is not allowed to terminate and the IN dialog reports Busy ERB.

(b) Trunk to line call.



Call is not allowed to terminate and the second IN dialog reports Busy ERB. Also for the first IN dialog Busy ERB is reported to notify that the call has ended with the cause value privateNetworkServingRemoteUser.

8.2.3.32 Extend Calls

This is an MSAC related feature and IN interaction with MSAC is not supported.

8.2.3.33 Flexible Console Alerting

No impact.

8.2.3.34 Intercom Group (GIC)

Not supported. The architecture of this feature is very different and does not pass through normal translators or terminators and hence TDP-3 and TDP-12 triggering is not possible. For the description of this feature please see Appendix section at the end of this document.

8.2.3.35 Key Short Hunt (KSH)

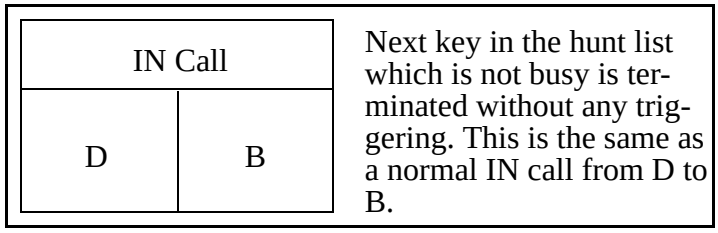
For the description of this feature please see Appendix section at the end of this document.

A(key 1), B(key 2) and C(key 3) are keys of the business set and A and B are TDP-12 triggering datafilled. A is busy. D dials A which results in the following IN call.

IN Call	
D	A

This is a normal IN call except Busy ERB is not reported. Next key in the hunt list will be tried.

Busy ERB is not reported and B rings without TDP-12 triggering and when B answers Answer ERB is reported. After this point if D on-hooks a Disconnect ERB is reported for port 1 and if B on-hooks a Disconnect ERB is reported for port 2.



Limitation / Restriction:

SCP does not understand that C has replaced B.

8.2.3.36 Last Number Redial (LNR)

No impact.

8.2.3.37 Last Number Redial from Set (LNRA)

No impact.

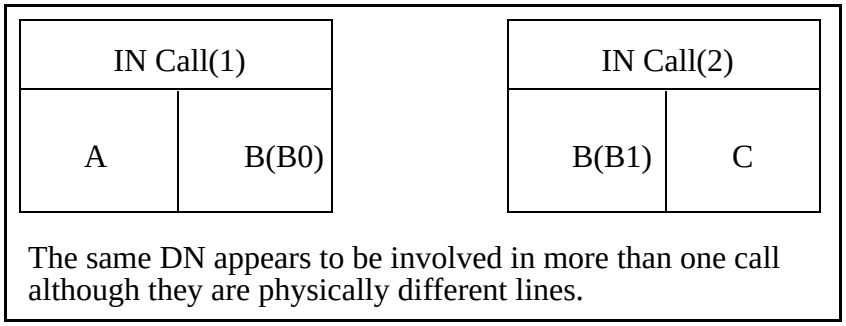
8.2.3.38 Multiple Appearance Of Directory Numbers (MDN)

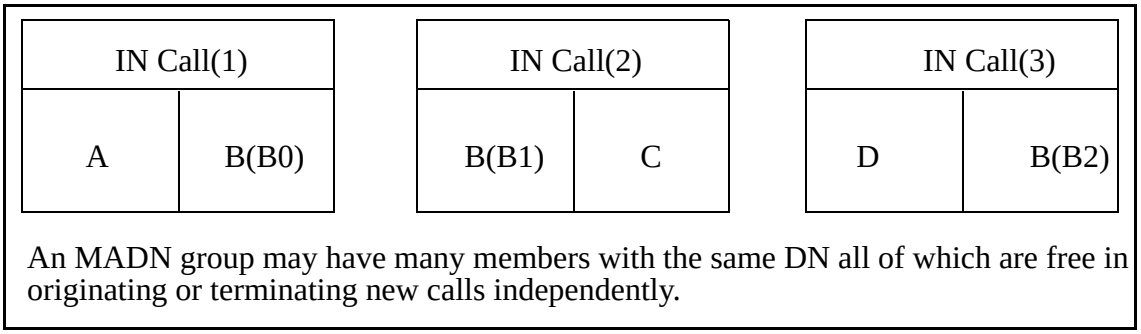
(a) SCA (Single Call Arrangement)

No impact.

(b) MCA (Multiple Call Arrangement)

All the MADN members have the same DN but when one of them is active others can also originate or can be terminated to as IN calls.



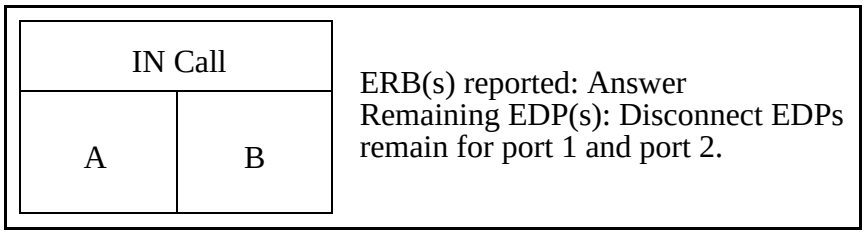


An MADN group may have many members with the same DN all of which are free in originating or terminating new calls independently.

8.2.3.39 Music on Hold (KSMOH)

(a) The calling party activates KSMOH.

A and B are talking in an IN call as follows:

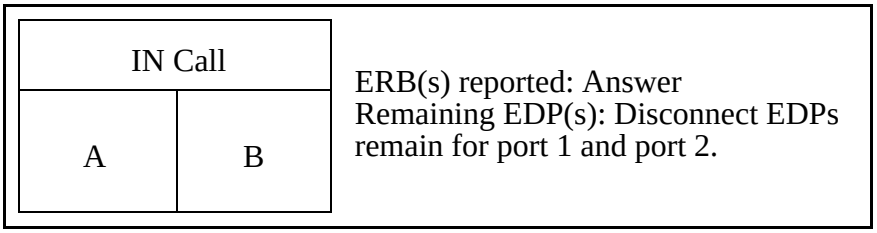


A activates KSMOH and B is on hold. A can retrieve B by pressing the DN key associated with the held call. After this point if A on-hooks a Disconnect ERB is reported for port 1 and if B on-hooks a Disconnect ERB is reported for port 2.

While on hold if B on-hooks a Disconnect ERB is reported for port 2.

(b) The called party activates KSMOH.

A and B are talking in an IN call as follows:



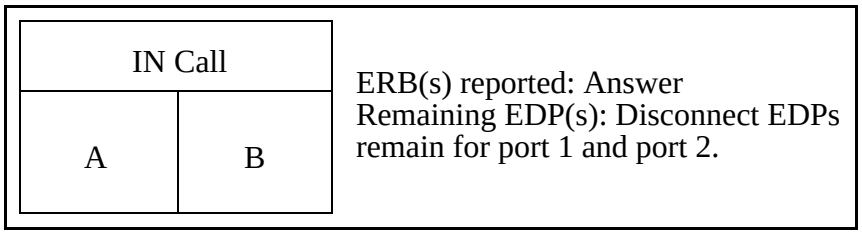
B activates KSMOH and A is on hold. B can retrieve A by pressing the DN key associated with the held call. After this point if A on-hooks a Disconnect ERB is reported for port 1 and if B on-hooks a Disconnect ERB is reported for port 2.

While on hold if A on-hooks a Disconnect ERB is reported for port 1.

8.2.3.40 Permanent Hold (HLD) Including Music on Hold

(a) The calling party activates HLD.

A and B are talking in an IN call as follows:

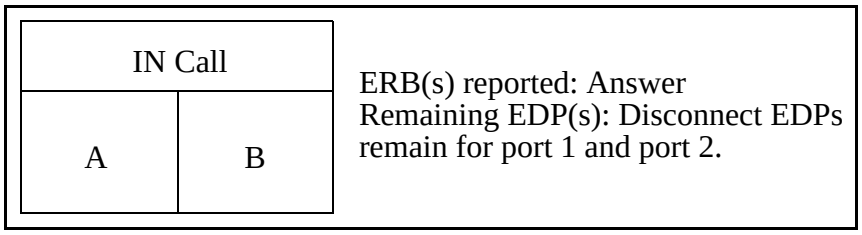


A activates HLD and on-hooks and B is on permanent hold. A off-hooks and retrieves B and after this point if B on-hooks a Disconnect ERB is reported for port 2 and if A on-hooks a Disconnect ERB is reported for port 1.

While on permanent hold if B on-hooks a Disconnect ERB is reported for port 1.

(b) The called party activates HLD.

A and B are talking in an IN call as follows:



B activates HLD and on-hooks and A is on permanent hold. B off-hooks and retrieves A and after this point if B on-hooks a Disconnect ERB is reported for port 2 and if A on-hooks a Disconnect ERB is reported for port 1.

While on permanent hold if A on-hooks a Disconnect ERB is reported for port 1.

8.2.3.41 Speed Call Long (SCL)

No impact.

8.2.3.42 Speed Call Short (SCS)

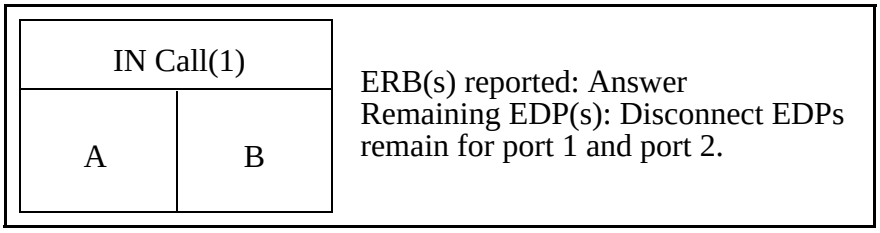
No impact.

8.2.3.43 Transfer, Hold & 3 way Conference (CXR)

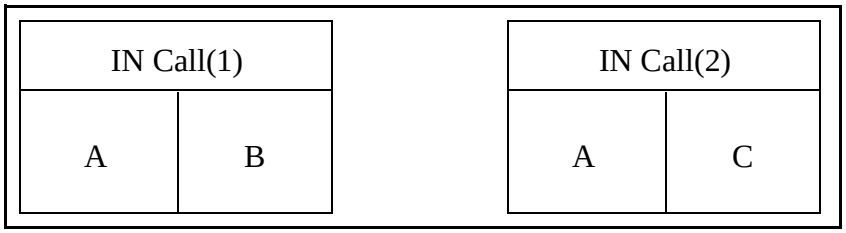
There are six scenarios as follows:

(a) Both the first call and the second call are IN calls and the calling party activates CXR.

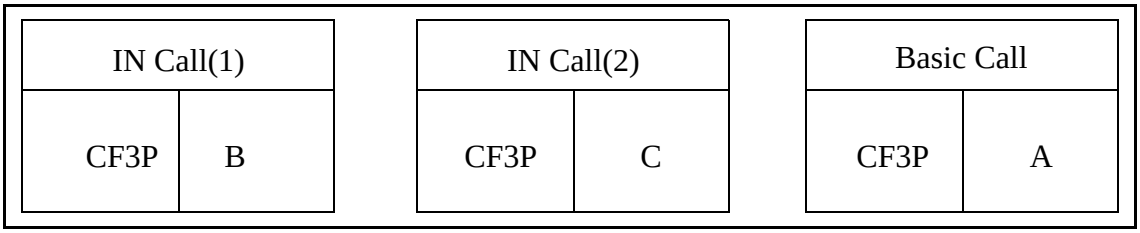
State 1



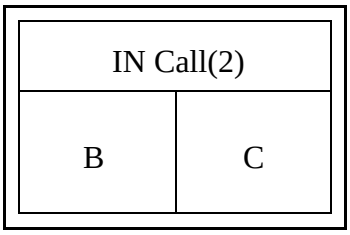
State 2



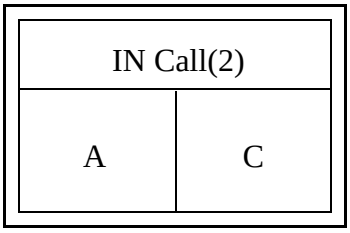
State 3



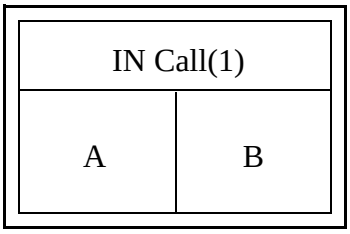
IN Call(1) -> EDP(9), EDP(17) for port 1: A on-hooked. Call was at State 2 or State 3.



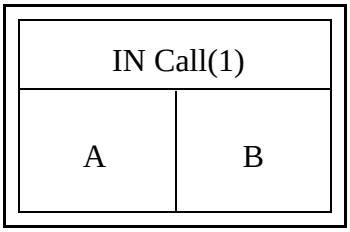
IN Call(1) -> EDP(9), EDP(17): B on-hooked. Call was at State 2 or State 3.



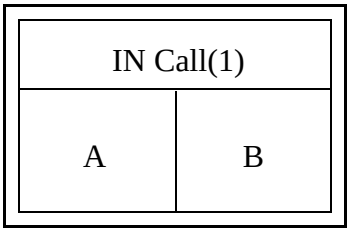
IN Call(2) -> EDP(4), EDP(5), EDP(6), EDP(13), EDP(14): Second call failed. Call was at State 2.



IN Call(2) -> EDP(9), EDP(17): C on-hooked. Call was at State 2 or State 3.

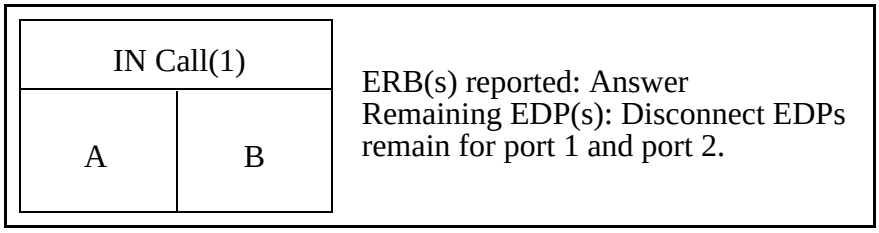


IN Call(2) -> EDP(9), EDP(17) for port 1: A flashed a second time during conference. Call was at State 3.

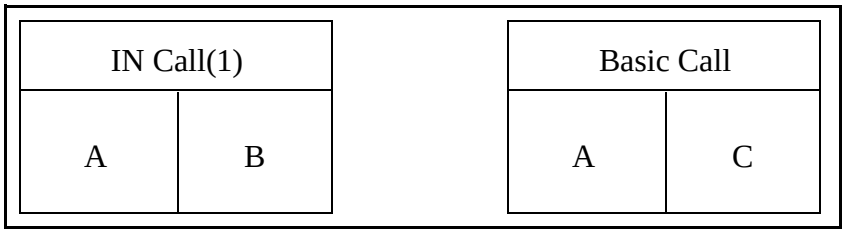


(b) The first call is an IN call, the second call is a basic call and the calling party activates CXR.

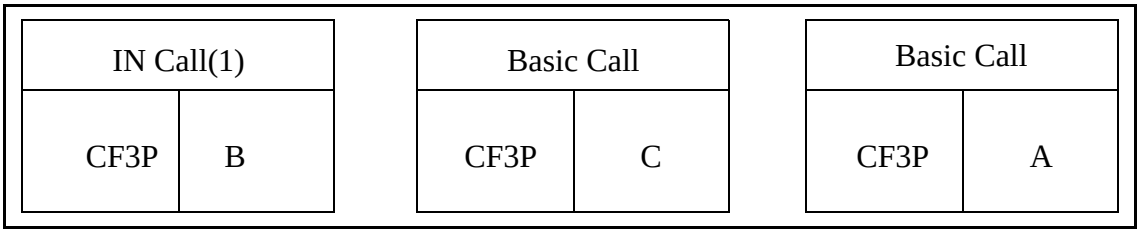
State 1



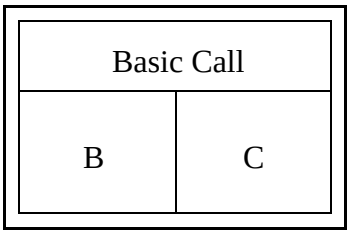
State 2



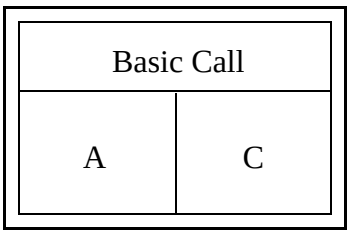
State 3



IN Call(1) -> EDP(9), EDP(17) for port 1: A on-hooked. Call was at State 2 or State 3.

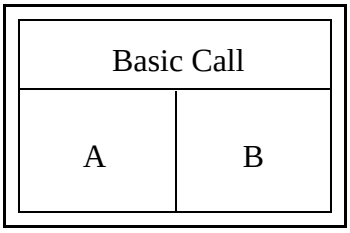


IN Call(1) -> EDP(9), EDP(17): B on-hooked. Call was at State 2 or State 3.

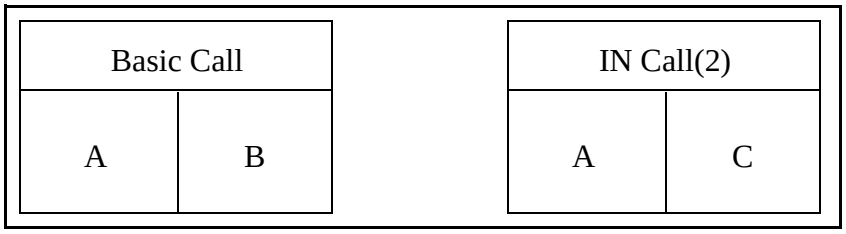


(c) The first call is a basic call, the second call is an IN call and the calling party activates CXR.

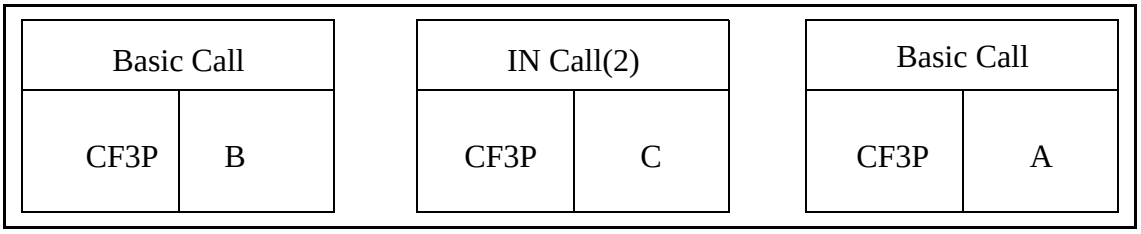
State 1



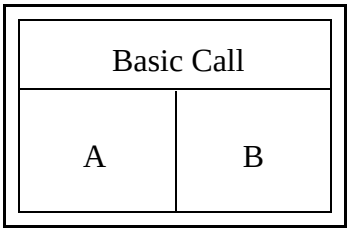
State 2



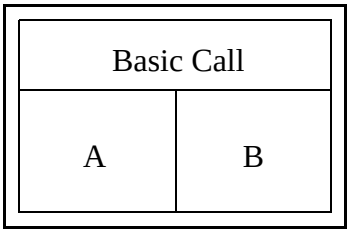
State 3



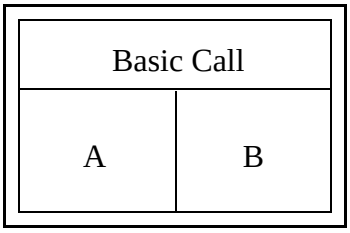
IN Call(2) -> EDP(4), EDP(5), EDP(6), EDP(13), EDP(14): Second call failed. Call was at State 2.



IN Call(2) -> EDP(9), EDP(17): C on-hooked. Call was at State 2 or State 3.

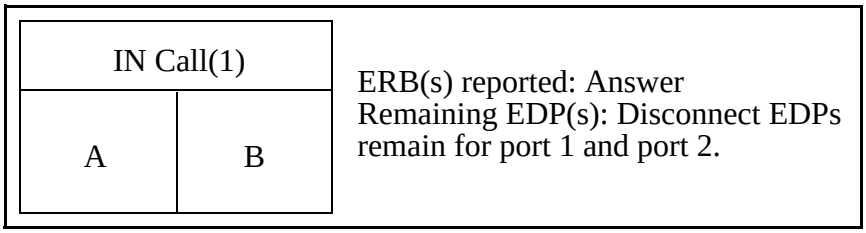


IN Call(2) -> EDP(9), EDP(17) for port 1: A flashed a second time during conference. Call was at State 3.

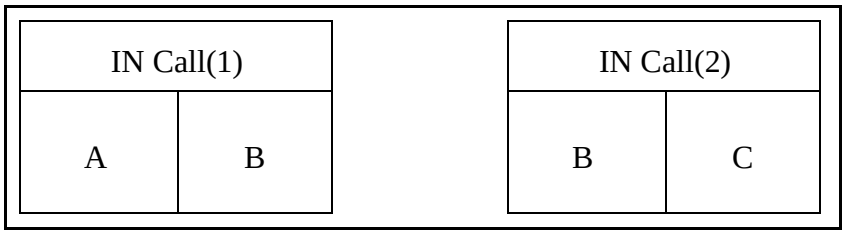


(d) Both the first call and the second call are IN calls and the called party activates CXR.

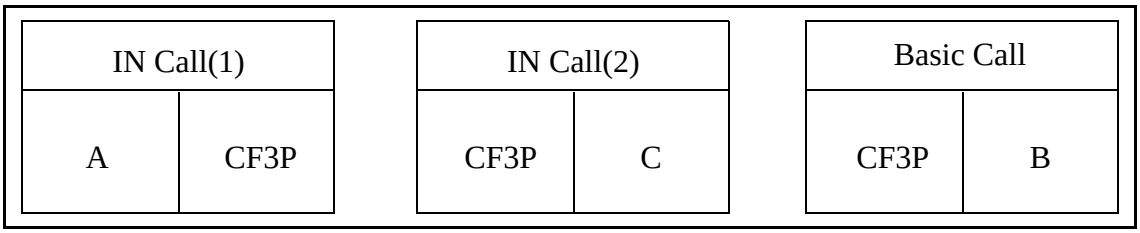
State 1



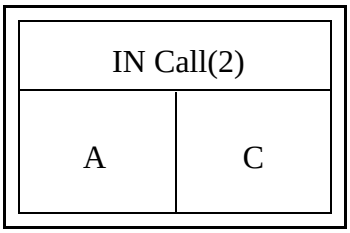
State 2



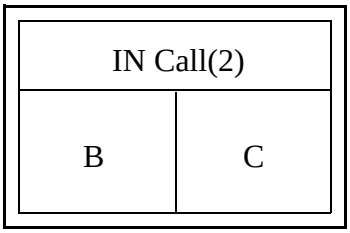
State 3



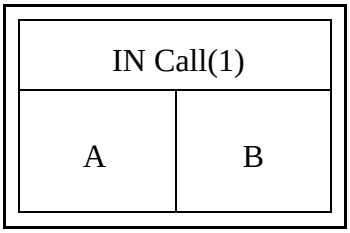
IN Call(1) -> EDP(9), EDP(17) for port 1: B on-hooked. Call was at State 2 or State 3.



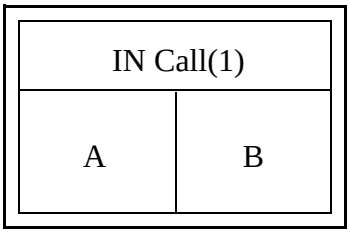
IN Call(1) -> EDP(9), EDP(17): A on-hooked. Call was at State 2 or State 3.



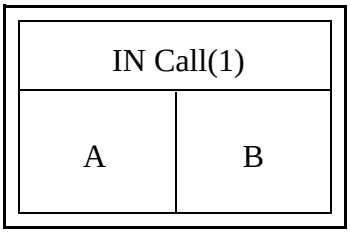
IN Call(2) -> EDP(4), EDP(5), EDP(6), EDP(13), EDP(14): Second call failed. Call was at State 2.



IN Call(2) -> EDP(9), EDP(17): C on-hooked. Call was at State 2 or State 3.

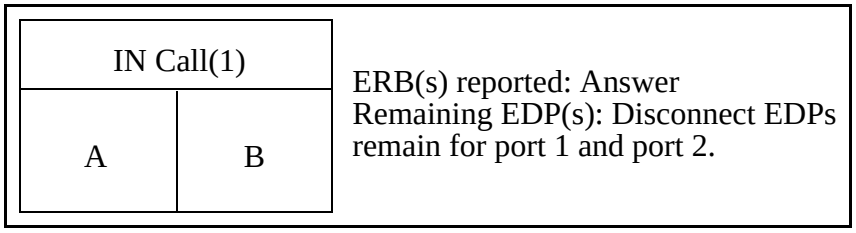


IN Call(2) -> EDP(9), EDP(17) for port 1: B flashed a second time during conference. Call was at State 3.

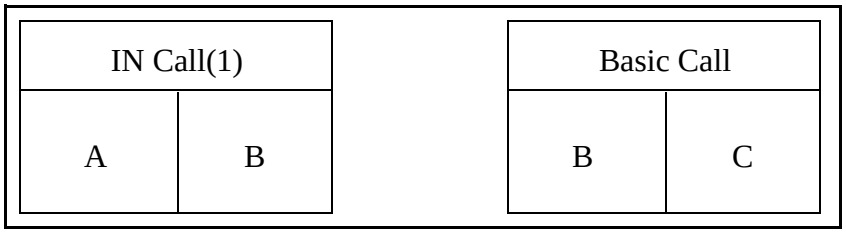


(e) The first call is an IN call, the second call is a basic call and the called party activates CXR.

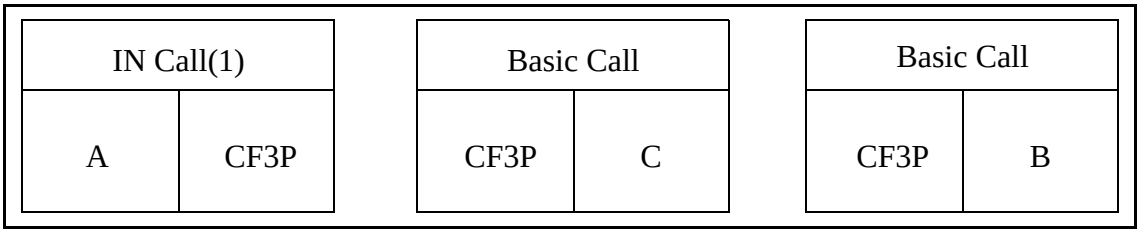
State 1



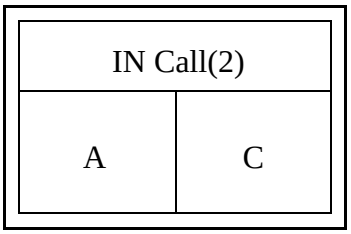
State 2



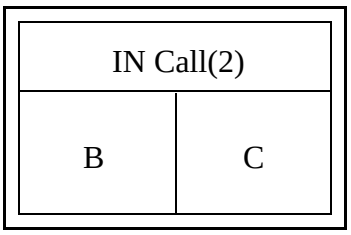
State 3



IN Call(1) -> EDP(9), EDP(17) for port 1: B on-hooked. Call was at State 2 or State 3.

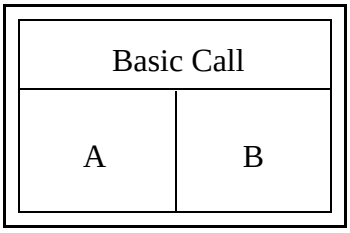


IN Call(1) -> EDP(9), EDP(17): A on-hooked. Call was at State 2 or State 3.

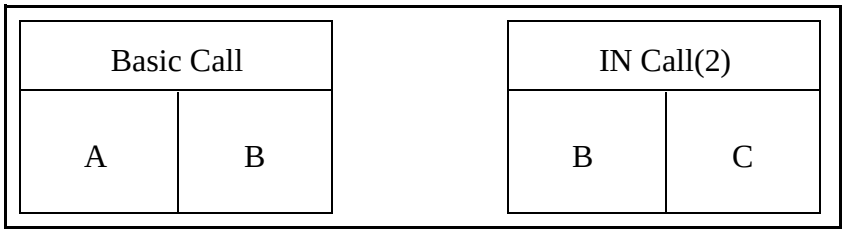


(f) The first call is a basic call, the second call is an IN call and the called party activates CXR.

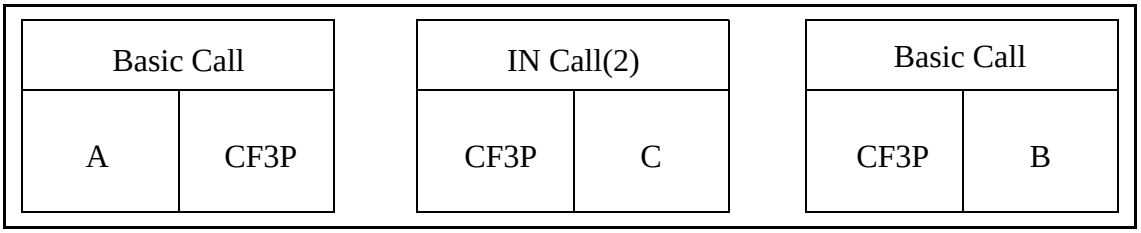
State 1



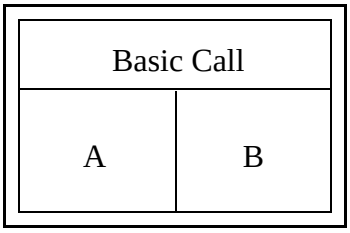
State 2



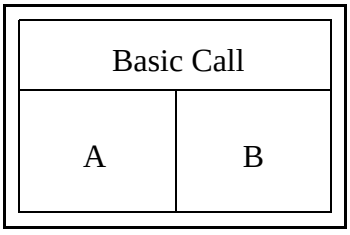
State 3



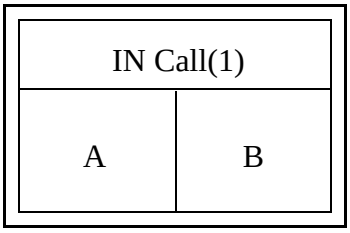
IN Call(2) -> EDP(4), EDP(5), EDP(6), EDP(13), EDP(14): Second call failed. Call was at State 2.



IN Call(2) -> EDP(9), EDP(17): C on-hooked. Call was at State 2 or State 3.



IN Call(2) -> EDP(9), EDP(17) for port 1: B flashed a second time during conference. Call was at State 3.



Limitation / Restriction:

In scenarios where there is only one IN dialog parties can not be tracked correctly.

8.2.4 Optionality

A new SERVINFO option CONV_DESK is defined which can be datafilled on a per service basis. In order for the IN triggers to behave as described above this option should be datafilled.

8.3 Hardware Requirements or Dependencies

Not applicable.

8.4 Software Requirements or Dependencies

Not applicable.

8.5 Limitations and restrictions

Limitations and restrictions are specified for each feature.

As a general limitation / restriction:

- In scenarios where IN dialog is aborted multimedia session ends.
- Only Connect, Continue, EDP-4(N), EDP-5(N), EDP-6(N), EDP-7(N), EDP-9(N), EDP-10(N), EDP-13(R, N), EDP-14(R, N), EDP-15(N), EDP-17(N), EDP-18(N) should be used.
- IN specific billing (i.e. FCI operation, SERVINFO options) is not supported.

8.6 Interactions

This is already the subject of this document.

8.7 References/Recommended Reading

A00008464 - Terminating EDPs support.

8.8 Glossary

Term	Description
EDP	Event Detection Point
IN	Intelligent Networks
MSAC	Meridian Services Attendant Console

8.9 Appendix

8.9.1 Call Forward Enhancements

The IBN Call Forward Enhancements allows for the addition of multiple Call Forwarding and personal call screening options to a customer group. These enhancements are for customer groups only. The system cannot assign these enhancements to separate lines.

This option can allow multiple Call Forwarding for other Call Forwarding features like CFU, CFI, CFB, CFD.

The personal call screening option allows the system to transfer forwarded calls back to a base station. The system forwards the calls even if Call Forwarding is active. This option can allow personal call screening for Call Forwarding features like CFU, CFI, CFB, and CFD.

Other options in this package also include customer group transparency, ring splash for CFI and denied call forwarding.

8.9.2 Direct (ICM)

The MBS Intercom allows an end user to press the Intercom (ICM) key to terminate on a selected Meridian business set (MBS).

If directory numbers (DN) are not active on the terminating MBS, audible ringing occurs and the ICM key of the terminator flashes. The terminator can press the ICM key to answer or wait 2 s. When the terminator waits 2 s, an automatic connection occurs.

If busy DNs are on the terminating MBS, a buzzing tone occurs. The system does not make an automatic connection. Press the ICM key to answer the call. The system places the active calls on automatic hold.

You can answer the intercom call on the loudspeaker or through the handset. The entry of both sets can occur to originate or answer an intercom call on the ICM key.

8.9.3 Direct Station Select/Busy Lamp Field (BLF)

Direct Station Select/Busy Lamp Field for MBS provides the following capabilities:

- Busy lamp field (BLF) enables a Meridian business set (MBS) end user to determine if a directory number (DN) is idle or busy by monitoring the state of the lamp next to the assigned feature key. This lamp is on when the DN is busy or off when the DN is idle.
- Direct station select (DSS) enables the end user of the monitoring set to press the specified feature key to dial the monitored DN directly.

Direct Station Selection/Busy Lamp Field for MBS can be used for direct calling or transferring calls, as described in the following paragraphs.

Direct calling by an MBS end user:

While calling a monitored DN, an MBS end user notes that the lamp light associated with the DN is not lit. He or she presses a DN key and then the BLF key associated with the DN.

Transferring calls:

The procedure to transfer a call or establish a three-way call using the BLF key is the same procedure as if the monitored DN was dialed directly.

8.9.4 Intercom Group (GIC)

The MBS Group Intercom (GIC) allows an end user to terminate on a member of a selected group using abbreviated dialing. An intercom group can have a maximum size of 10 members, 1000 members, or 10 000 members. End users in a 10 member group dial a single digit, 0 to 9, to reach others members in their group. End users in a 100 member group dial a two digit number, 00 to 99. In a 1000 member group, end users dial a three digit code, 100 to 999. In a 10 000 member group, end users dial a four digit code, 0000 to 9999. A Meridian business set (MBS) can have members of several different GIC groups. A separate feature key must represent each group.

The DMS-100 switch accommodates a maximum of 4095 GIC groups. You can assign each GIC group to one large customer group. You can assign each GIC group to many customer groups.

8.9.5 Key Short Hunt (KSH)

This feature provides the capability for incoming calls to search a set of DN appearances on a business set for an idle DN to terminate.

KSH is a subset feature and must be assigned to key 1 if feature KSH is required. Either all DNs of the business set or a subset of DNs can be specified in the hunt list.

Hunting of an idle DN starts from the dialed DN, then goes up the keys of the business set as defined in the keylist. This hunt is not circular and stops once an idle DN is found or the hunt list following the dialed DN is exhausted. If the hunt list is exhausted without finding an idle DN, then an optional overflow DN or route is terminated.

The keylist can only contain standard DNs or multiple appearance DNs (MADN), but not intercom (ICM), group intercom (GIC), or private business line (PBL) DNs. A given DN cannot appear in more than one short hunt group or any other type of hunt group: multiline hunt (MLH), distributed line hunt (DLH), or directory number hunt (DNH). Any MADN member in the hunt keylist must be the primary member of that MADN group.

9: Functional Description (FN): A00008556

9.1 Feature name and Feature ID

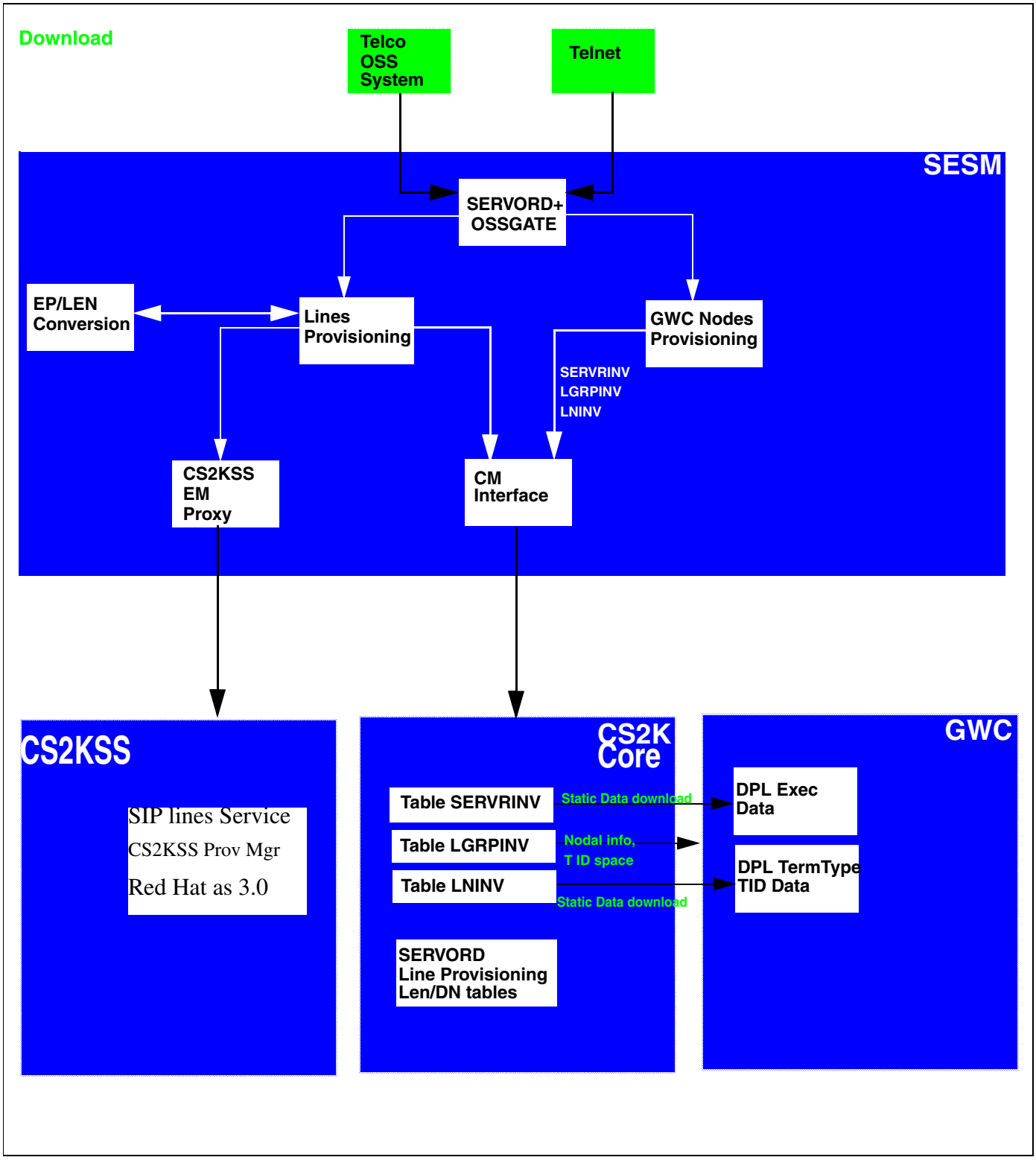
A00008556 - SIP Lines Core OAMP support

9.2 Description

The provisioning of DPL agents affects three major network components, the CS2K core, GWC, and CS2K Session Server(CS2KSS). Each of these components have their own specific provisioning requirements and each are provisioned via the appropriate application within SESM. The relationships between these components and SESM are shown in Figure 1 DPL Provisioning Component Overview below.

Refer A00008522 FN for SESM provisioning instructions.

Figure 1 DPL Provisioning Component Overview



This activity focuses on the CORE OAMP(Operation, Administration, Maintenance & Provisioning) portion of the overall SIP feature. The components in this activity are as follows:

- GWC Provisioning.
- CS2KSS-GWC Association.
- DPL Lines Provisioning.
- Journal File.
- NCAS Link Provisioning.
- Core Maintenance support.
- Tool support
- SOC support (Refer the CN section).
- NCAS Link Logs (Refer the FM section).

9.2.1 GWC provisioning:

The GWC is commissioned through the SESM. The core stores information about this commissioned GWC in the table SERVRINV. The SIP feature deals with supporting new type of agent called dynamic packet line on the GWC.

- A new term_type DPL_TERM and a new exec_lineup called DPLEX are defined for supporting the DPL agents on the GWC. The new definitions DPL_TERM and DPLEX are passed onto the core along with the GWC information when the GWC is commissioned.

- On the core side, the table SERVRINV is enhanced so that it can accept these new definitions. When the GWC is commissioned, a tuple similar to the below one is expected to be datafilled in the table SERVRINV automatically:

Table SERVRINV:

SRVRNAME SRVRADDR ***SRVREXEC*** *SRVRTONE BEARNETS SRVROPTS*
GWC 0 IP 45 46 47 48 ***(DPL_TERM DPLEX)*** *$ NORTHAA (NET_IP Y)$ $*

This table is supposed to be provisioned via SESM and not manually. The field in bold is updated to support a new entry DPL_TERM DPLEX.

9.2.2 CS2KSS-GWC Association:

Currently, a gateway controller can be associated with a maximum of 6 gateways (LGRP nodes) in CS2KSS. After the GWC is commissioned, a logical association is created in the core between the GWC and the gateways in the CS2KSS.

- The table LGRPINV stores the information about the LGRP node and the GWC which it is associated with. After the GWC information is provisioned in the table SERVRINV, the LGRP node information for corresponding LGRP nodes are datafilled in the table LGRPINV. The table LGRPINV is enhanced so that a new lgrp_type 'SSDPL' is supported. This new lgrp_type signifies that this LGRP node is associated with DPL lines.

- Currently, each LGRP node can support 1023 lines and this size will not change as a part of this feature. The information on these lines for each of the LGRP node is stored in the table LNINV. Table LNINV does not require any enhancements to support this functionality.

- A tuple with following structure is expected after the table LGRPINV is provisioned:

Table LGRPINV:

LGRP_NO	*SRVR_NAME*	***GRPTYPE***	*LGRPOPTS*
LG 1 1	*GWC 5*	***SSDPL***	*$*

This table will be provisioned via SESM and is not supposed to be datafilled manually. As shown above, a new lgrp_type 'SSDPL' is supported now for table LGRPINV.

When 1 LGRP is provisioned, corresponding 1023 lines subtending from that lgrp will be datafilled in table LNINV. As a part of this feature, the table LNINV is enhanced so that it can support only RDTLSG(North American market) and GWLPOT(International Market) cardcode for SSDPL lgrp_type. Also, the restriction has been applied to the cardcodes valid for the other lgrp_types. A sample tuple:

Table LNINV:

LEN	*CARDCODE*	*PADGRP*	*STATUS*	*GND*	*BNV*	*MNO*	*CARDINFO*
CS2KSS 1 1 10 13	RDTLSG	PKLNL	HASU	N	NL	Y	NIL

As a part of this feature the following valid cardcodes apply for different lgrp_types:

LGRP_TYPE	List of Valid Cardcodes
SSDPL	RDTLSG, GWLPOT
S	RDTLSG, RDTCON, GWLPOT, RDTEBS,GWLEBS
M	RDTEBS, GWLEBS
C	RDTLSG, RDTCON, GWLPOT
LL_3RDPTY	RDTLSG, RDTCON, GWLPOT, RDTEBS, GWLEBS
CALIX_C7	RDTLSG, RDTCON, GWLPOT, RDTEBS, GWLEBS

The table LNINV will be provisioned via SESM and is not supposed to be datafilled manually.

9.2.3 DPL Lines Provisioning:

The DPL line is differentiated from other lines by adding DPL option on that line. The table IBNFEAT is enhanced to support a new data_feature DPL. The DPL option can be added only to IBN/RES lines. Also, SERVORD+ is enhanced for accepting new DPL related options and should be used for datafilling the DPL option.

9.2.3.1 The new DPL option

As a part of supporting new DPL option, table IBNFEAT, LCCOPT and OPTOPT are enhanced.

- The table IBNFEAT have been enhanced to support the DPL data_feature. The DPL line option will have a SIP sub option. The SIP sub option of DPL will itself have a sub option of MAX_NUM_CALLS(10).
- The table control editor commands, ADD,DEL and CHA are disabled for the DPL option in table IBNFEAT much in the same manner of the PDO option.

Table IBNFEAT:

LEN DNNO DF FEATURE DATA
LG 01 1 00 14 0 ***DPL DPL Y 10***

This table will be provisioned via SESM.

- DPL option can only be added via Servord and not Table Control.

- The options incompatible with the DPL option can be datafilled in the table OPTOPT. A sample tuple:

Table OPTOPT:

DPL (BC) (CSDO) (EOF) (FIG) (FTS) (LDTPSAP) (LNPTST) (MAN) (MPB) (NDC) (NOH) (VOWDN) $

You can add options in this tuple which you want to make incompatible with option DPL. This is just a sample tuple. To see the list of supported options with DPL, please refer the interactions section of FN.

- The LCC's supporting the DPL option can be modified through the table LCCOPT. Currently, only IBN and RES lines support the DPL option. Sample tuples are as belows for IBN and RES LCC's.

Table LCCOPT:

RES (ACB) (ACRJ) (ADSI) (ADSL) (AIN) (AINDENY) (AINDN) (AMATEST) (AMSG) **(DPL)**

IBN (ACB) (ACD) (ACDNR) (ACRJ) (ADSI) (AIN) (AINDN) (ALI) (AMATEST) (AMSG) **(DPL)**

9.2.3.2 SERVORD+ Enhancements:

SERVORD+ Enhancements have been made so that it will now accept three new options related to SIP lines provisioning: DPL, SIP_PASSWORD and SIP_DATA. DPL will be seen in the core whereas the options SIP_PASSWORD and SIP_DATA will be send to the CS2KSS.

- When provisioning a SIP line all three of the options described above must be present in the SERVORD+ NEW command.
- The above options can not be added later via ADO.
- ADO and DEO of options that are compatible with DPL will be permitted. But ADO/DEO can not be used with the DPL line option.
- Only NEW, OUT and CHF will support the DPL line option. It is possible to add a DPL compatible option that does not require the DPL option in the command (such as ADO PIC). CHF can be used to

manipulate the MAX_NUM_CALLS value subfield of the DPL option. The line must not be in the CPB or call processing busy state or the change will be rejected. CHG can be used to change all but the LCC (line class code).

- DGT option is required. It will be automatically added if not present.
- Long SERVORD+ commands are supported by allowing commands to be continued on a second line by using a + sign.
- The SIP URI change will be reflected in the CS2KSS and not in the core.
- E.g. of the SERVORD+ command:

Servord+ NEW Command:

NEW $ 6212500 IBN BNR 0 0 613 NILLATA 0 LG 000 0 10 13 DPL Y 3 SIP_PASSWORD xx SIP_DATA bobby mb1

9.2.3.3 Journal File:

The Journal File (JF) subarea provides a facility for preserving Data Modification Orders (DMO) on tape so that data tables can be restored if the switch should fail. The Journal File is an optional feature of the DMS switch which preserves DMO on magnetic tape. If a switch failure occurs that requires a reload, this magnetic tape is loaded back into the machine and switch data is restored to its condition at the time of switch failure.

9.2.4 NCAS Link Provisioning:

The core communicates directly with the CS2KSS Provisioning Server through NCAS links. The CS2KSS Provisioning Server can return both static and dynamic call data stored in CS2KSS back to the core via the NCAS link

The NCAS link is going to be an instance of SCTP. The table IPAPPL provides SCTP instance for various connections in DMS. This table is enhanced to support a new application called SIPMTC (just like AIN, SMDI etc). The core can now communicate with CS2KSSs using this SCTP instance.

Table IPAPPL:

InstKey	*InstName*	*Transport*	*IPDevice*	*IPaddrs*	*port*	*optlist*
1	*a*	*sctp*	*hiop*	*198 202 188 221*	*4982*	*(application **sipmtc**)*
						(setprime 1)

The NCAS link association is going to be used for the new QSIP command.

The SIPMTC application is supported over HIOP only.

The multihoming functionality is not supported in SIPMTC application.

The port number allocated for SIPMTC application is 4982.

Multiple instances for SIPMTC are not allowed i.e. in table IPAPPL, there can be only one instance datafilled for SIPMTC.

9.2.5 Core Maintenance Activities:

On the core side, maintenance actions can be performed on the DPL lines. The maintenance operations will keep the core, gwc and cs2kss informed about each other's activities.

9.2.5.1 MAP Commands and Line State Propagation:

The DPL line can be posted on mapci; lns; ltp level.

- The line states for DPL lines on the Core include: IDL, LMB, MB, INB, CPB, CPD, SB. After the line is posted, operations like BSY, RTS, FRLS, HOLD, NEXT can be performed on the posted line. When these operations are performed, the state change of the lines is propagated to the GWC which in turn notifies CS2KSS.
- There are plans to support DIAG in the second phase of this feature, but they will not be supported in the current release. When DIAG is run on the core side, a message will be displayed: "This command is not valid for posted line.".
- At the map level, the base DPL tid will be posted. If there is any call active, then the information posted for base DPL tid will depend upon the number of call appearances active. If there is only call appearance active, then the linking information for that call appearance will be posted. However, for more than one call appearance, the linking information will not be displayed for all the call appearances. The maintenance operations on specific call appearances will be supported in later release.
- The DPL line can be posted at all the sub-levels of the LTP level: LTPLTA, IBNCON, LTPMAN, LTPDATA, LTPISDN, DCTLTP, DTPLTP. But no maintenance operations can be performed on posted DPL lines at any of these sub-levels.
- For the BSY command, the CS2KSS will be notified that this DPL client is not available for call processing. If there are no call appearances active, then the base TID will be put into MB state and no calls can be associated with this DPL agent. If there are any call appearances active, then the base TID will be put into CPD state. When all the calls are taken down, the base dpl TID will move from CPD to MB state. New calls cannot be originated/terminated on the DPL line that has been busied. The line has to be RTSed back for new calls to be originated/terminated.

- A FRLS on a DPL agent will clear all active calls for the line. If there are no active calls then the base TID, then the tid will be put to MB state. If there are active calls, a FRLS will terminate all the sessions. However, FRLS on a particular session will be supported in a later release.
- On RTS operation, the line will be put into IDL state. This operation cannot be performed when the calls are active on a DPL line.
- The maintenance operations BSY/RTS/FRLS at the MAP level are applicable for all the multiple call appearances. The Mtc operations are applied to all the VIDs.
- The HOLD command puts the posted DPL line in the hold position.
- The NEXT command moves the line in a specified HOLD position to the control position, or replaces the line in the control position with the line in a specified hold position. The NEXT command does not list the next provisioned DPL VID.
- The LGRP node can be posted at the PM level but maintenance operations cannot be performed on the entire LGRP. Thus, the state changes because of maintenance operations are propagated upwards to the core through the GWC.

Note: The maintenance operations are not supported for the SSDPL lgrp.

- When the BSY LGRP command is given for the SSDPL lgrp, the following error message is displayed:

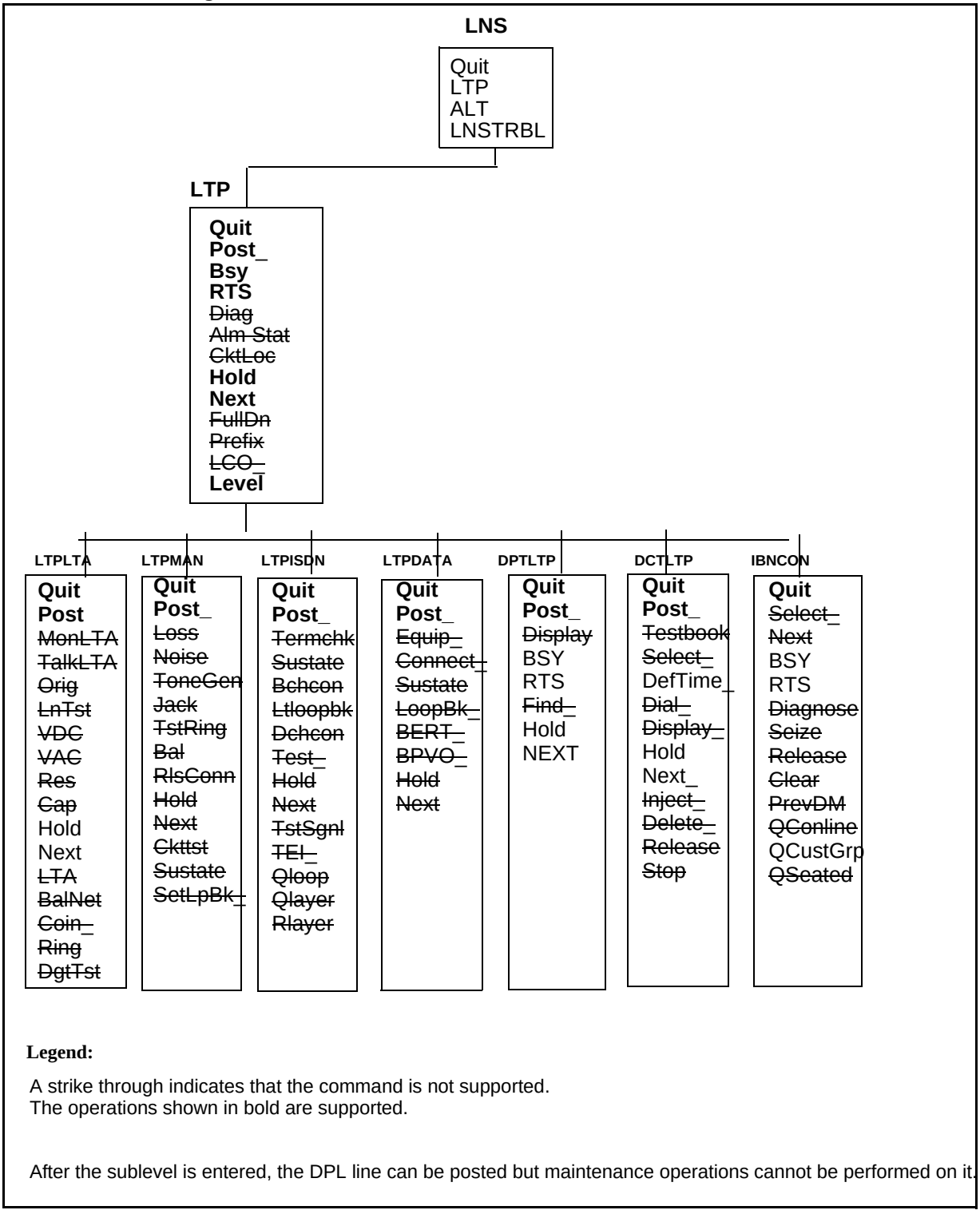
BSY COMMAND IS NOT SUPPORTED FOR THIS TYPE OF LGRP NODE.

- When the RTS command is given for the SSDPL lgrp, the following error message is given:

RTS CAN ONLY GO FROM MANB STATE.

Figure 2 Map Level below shows the MAP levels and operations which are supported and blocked for DPL lines.

Figure 2 MAP level



Legend:

A strike through indicates that the command is not supported.
The operations shown in bold are supported.

After the sublevel is entered, the DPL line can be posted but maintenance operations cannot be performed on it.

At the **LTPLTA** level, the error messages that will be seen for the unsupported maintenace commands are:

MonLTA, TalkLTA, Orig, LnTst, VDC, VAC: **This command is not valid for posted line.**
BalNet: **This command is not valid for Call Server LGRP lines.**
Coin, Ring, DgtTst: **No talk connection to posted line**

At the **LTPMAN** level, the error messages that will be seen for the unsupported maintenance commands are:

Loss, Noise, Tonegen, Jack, RlsConn : **This command is not valid for the posted line.**
Tstring: **To test the ringing function for Call Server LGRP lines, please run the DIAG command.**
Bal: **This command is not valid for Call Server LGRP lines.**
Ckttst: **CKTTST command is not valid on POTS/COIN lines.**
Sustate: **SUSTATE command is not valid on POTS/COIN lines.**
SetLpBk_ : **SETLPBK command is not valid on POTS/COIN lines.**

At the **LTPISDN** level, the error messages that will be seen for the unsupported maintenance commands are:

TERMCHK: **TERMCHK command is not valid on POTS/COIN lines.**
Sustate: **SUSTATE command is not valid on POTS/COIN lines.**
BchCon: **BCHCON command is not valid on POTS/COIN lines.**
LTLOOPBK: **LTLOOPBK command is not valid on POTS/COIN lines.**
DCHCON: **DCHCON command is not valid on POTS/COIN lines.**
TEST: **TEST command is not valid on POTS/COIN lines.**
TSTSGNL: **TSTSGNL command is not valid on POTS/COIN lines.**
TEI: **TEI command is not valid on POTS/COIN lines.**
QLOOP: **QLOOP command is not valid on POTS/COIN lines.**
QLAYER: **QLAYER command is not valid on POTS/COIN lines.**
RLAYER: **RLAYER command is not valid on POTS/COIN lines.**

At the **LTPDATA** level,

Equip, Loopbk_, BERT_, : **This command is not valid for Call Server LGRP lines.**
Connect: **CONNECT command is not valid on POTS/COIN lines.**
Sustate: **SUSTATE command is not valid on POTS/COIN lines.**
BPVO: **BPVO command is not valid on POTS/COIN lines.**

At the **DPTLTP** level,

Find_ : **CLLI entered is not of a DPT trunk**
Display: **DN not involved in a call**

At the **DCTLTP** level,

Testbook: **No testbook is active.**
Select: **SELECT command not executed. No testbook is active.**
Dial: **DIAL command not executed. No testbook is active.**
Display: **DISPLAY command not executed. No testbook is active.**
Inject: **INJECT command not executed. No testbook is active.**
Delete: **DELETE command not executed. No testbook is active.**
Release: **RELEASE command not executed. No testbook is active.**
Stop: **STOP command not executed. No testbook is active.**

At the **IBNCON** level,

Select: **That line is not associated with a console.**
Next, Diagnose, Seize, Release, Clear, PrevDm, Qconline, Qseated: **Console not selected.**

9.2.5.2 Restart and Swact Recovery:

It is desired that when Core, GWC and CS2KSS undergo restart/swact, each of the component's view of line states are in sync.

When the core undergoes restart/swact it notifies the GWC about the type of restart/swact. The GWC performs the necessary operations and also notifies the CS2KSS regarding this. The heartbeat mechanism is used to notify each other of their availability.

When the core undergoes restarts/swacts, a message is sent to GWC about the type of restart/swact. The GWC has to take action upon the type of restart/ swact that occurred.

Core Recovery:
The stable calls are the ones in the talking state. The unstable calls imply the ones not in the talking state.

- For core warm restart, GWC clears all unstable calls.
- For core cold restart, GWC clear all stable and unstable calls.
- For core warm SWACT, GWC clear unstable calls.
- For core cold SWACT, GWC clears all stable and unstable calls.
- For core reload restart, BSY GWC Node. When core recovers, RTS the GWC node.
- After the core restart is completed, a message is sent to the GWC that the core is in 'Running' state. If the GWC was BSYed, it will be RTSed. The core sends a SST320 message to RTS all the lines of an LGRP.

- If the CS2KSS is OOS before the restart, lines are put into LMB state. The availability of CS2KSS is tracked by the GWC by the heartbeat mechanism.
- Even if the line was manually BSYed before restart, the line is RTSed to IDL state after restart is over.
- When the core recovers, the endpoints appear as SB until the recovery process is complete, then they transition to IDL. However, the transition state SB cannot be tracked because by the time core recovers completely and we can post the line at the mapci level, the line would have been RTSed to IDL state.

GWC Recovery:

- When the GWC is busy, the state of the GWC in the core side will be ManB. If the GWC is OOS, the state of the GWC in the core would be SysB. When the GWC is not InSv, the LGRP will be in SysB state.
- When GWC goes down, a message is sent to the core to put the line in LMB state.
- When GWC recovers, message is sent to the core to put the line into IDL state. But since the connection between the GWC and CS2KSS is lost, the lines will be put into LMB state. When the discovery message from CS2KSS to GWC is sent, the lines of the corresponding lgrp are out into IDL state.

CS2KSS Recovery:

The maintenance operations are not supported on CS2KSS in this release. The line states are depedent upon whether CS2KSS is up or not.

- CS2KSS gateway is not provisioned on the GWC side.
  If the gateway is not provisioned on the GWC side, the lgrp state is SYSB the lines will be in INB state.

- CS2KSS gateway is provisioned but the gateway is OOS
  When the gateway is OOS, the lgrp is in SYSB state and the lines are in the LMB state. Only when the DISCOVERY message is sent to the GWC from the CS2KSS, the lines are put to IDL state.

9.2.6 Tools:

9.2.6.1 QSIP:

QSIP is a new query command at the CI level. It has been introduced as a part of
this activity. QSIP would query the SIP Line data for a particular SIP Line.

The QSIP command will display the information in the table below.

Table 10: QSIP Response FIelds

QSIP Field	Format/Value	Description
SIP URI	<user>@<domain>	The SIP URI that corresponds to the the DN in the QSIP query.
Account Status	ACTIVE/INACTIVE	The status of the subscriber's account. If the account is active, the subscriber is allowed to make calls. If the account is inactive, the subscriber is not allowed to make calls.
Registration State	Y/N	Indication if the subscriber is registered/logged-into a SIP client.
Allow Post Busy Termination	Y/N	This field suggests that the line is allowed to have termination even if it in busy in another call if value is set to Y.
Number of Contacts	<integer>	The number of unique registered destinations where the subscriber is logged into.
Contacts	List of <user>@<ip address>:<port>	Displays no more than 3 contacts. A SIP contact is IP address the subscriber registered from.
Service Package	<string>	Name of the Service Package the subscriber has on the Session Server.
Services	<string>	List of services and service data in the Service Package.

Table 10: QSIP Response FIelds

QSIP Field	Format/Value	Description
Endpt ID	<SITE>/<FFF>/<G>/<TTtt>	SITE = 1-4 Alphanumeric characters. Corresponds to provisioned SITE name in the XACore. FFF = 000-511 Corresponds to the frame number used in the logical group name in the XACore. G = 0-9 Corresponds to the group number used in the logical group name in the XACore. TTtt= 0000-1022 Corresponds to the circuit numbers (upper and lower) in the LENs defined against the logical group in the XACore.
Virtual Media Gateway	<string>	Name of Virtual Media Gateway.
Zone ID List	List of <integer>	Displays no more than 3 zone ids. The zone id allows the software to determine a media portal insersion is required or not.
Client Type	<string>	The type of client this subscriber is associated with (for example, ONT). Client Types can be defined in the Session Server ProvClient.
Static Client	Y/N	This field is set to "Y" meaning this is a wireline or fix client. The value "N" is for the future usage.
Node number and Terminal number of the VIDs of all the Active Call Appearances	List of <node> <terminal>	Lists the endpoints involved in SIP sessions.

Table 10: QSIP Response FIelds

QSIP Field	Format/Value	Description
Number of Active Sessions in CS2000 Session Server	<integer>	The number of active SIP voice sessions this subscriber is involved in at the point in time whenthe QSIP query is issued.

The QSIP command will launch a Query message to the CS2000 Session Server over the NCAS link. The CS2000 Session Server will launch a Response to the Core over the NCAS link. Upon receiving the Response from the CS2000 Session Server, the Core QSIP command will display the above SIP Lines information.

The response for the QSIP query sent is expected to arrive within a specific time
interval. The default QSIP response time interval is 15 seconds. However, the timeout can be set from 1 to 30 seconds. If any value greater than 30 or lesser than 1 is given as the timeout value, the timeout value will be set to the default timeout value of 15. Timeout is an optional parameter in the QSIP command.

The QSIP command will only display the CS2000 Session Server services that are ENABLED. There could be services provisioned on the SIP line which are DISABLED which would not be shown. However, the QSIP will display the Service Package Name which would help if it is known which services are in a particular Service Package.

If a SIP line has contacts, only the URIs of the first three contacts will be shown.

If a SIP line has more than 3 middle box ids, only 3 middle box ids will be displayed.

If QSIP cannot display the SIP data from the CS2000 Session Server a message will be printed as follows:

SIP DATA CANNOT BE DISPLAYED DUE TO <REASON>

Where <REASON> could be one of the following

- RESPONSE TIMEOUT FROM CS2000 SESSION SERVER
- BAD MESSAGE RECEIVED FROM CS2000 SESSION SERVER
- QSIP SEND REQUEST FAILURE
- The QSIP Application Error String from the QSIPReportError message received from CS2000 Session Serve

If the response from the CS2000 Session Server does not have any data for all the parameters then the following message is displayed:

- SIP DATA CANNOT BE DISPLAYED BECAUSE NO DATA RECEIVED FROM CS2000 SESSON

If the CS2000 Session Server responds with partial data , before the SIP data portion of the QSIP display begins there will be a message:
"PARTIAL DATA RECEIVED FROM THE CS2000 SESSION SERVER."
Then, the QSIP will display whatever data it can and leave the other fields blank.

If the total number of parameters, including main parameters and their sub-parameters, received in the response message from CS2000 Session Server is greater then 19 then it would be considered as an error scenarior and the following message would be displayed:

SIP DATA CANNOT BE DISPLAYED DUE TO BAD MESSAGE RECEIVED FROM CS2000 SESSION SERVER

The Allow Post Busy Termination and Node numbers and Terminal numbers of the VIDs active on the call are displayed only if some data is received in the response message from the CS2000 Session Server.

QSIP will work for all the LENs that work fine with QLEN. However, to get data the LEN should correspond to a SIP Line.

If QSIP is used with a non-SIP DN then the following message will be displayed:
QSIP SHOULD BE GIVEN FOR SIP LINES ONLY

If a non-existent DN is specified for QSIP then the following message will be displayed:
INVALID DN SPECIFIED FOR THE QSIP COMMAND

If a non-existent LEN is specified for QSIP then the following message will be displayed:
INVALID LEN SPECIFIED FOR THE QSIP COMMAND

The QSIP command’s CI format is shown below:

```
>q qsip
DISPLAY SIP LINE INFORMATION
     COMMAND FORMAT: QSIP <DR_LEN_TYPE>
      PARMS: [<TIMEOUT> {1 TO 30}]
```

- Example for QSIP (DN as a parameter)

```
> qsip 6138675309
SIP USER DATA
=============
SIP URI: 6138675309@NORTELNETWORKS.COM
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: N
NUMBER OF CONTACTS: 12
CONTACTS: 6138675309@4.3.2.1:5060 6138675309@4.3.2.1:5061
6138675309@1.2.3.4:5062
SERVICE PACKAGE:
DEFAULT_PKG
SERVICES:
ADHOC 4 ADDRBK 50 VMAIL

SIP LINE DATA
=============
ENDPT ID: PHX/003/0/1000
VMG: VMG.1
ZONE ID(s): 1234 1234 3456
CLIENT TYPE: ONT
STATIC CLIENT: N

SIP CALL DATA
=============
ACTIVE CALL APPEARANCES:
  NODENO   TERMNO
NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12
--------------------------------------------------------------------------------
```

- Example #2 for QSIP (LEN as a parameter)

```
> qsip 6138675309
SIP USER DATA
=============
SIP URI: 6138675309@NORTELNETWORKS.COM
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: N
NUMBER OF CONTACTS: 12
CONTACTS: 6138675309@4.3.2.1:5060 6138675309@4.3.2.1:5061
6138675309@1.2.3.4:5062
SERVICE PACKAGE:
DEFAULT_PKG
```

SERVICES:
ADHOC 4 ADDRBK 50 VMAIL

SIP LINE DATA
==========
ENDPT ID: PHX/003/0/1000
VMG: vmg
ZONE ID(s): 1234 1234 3456
CLIENT TYPE: ONT
STATIC CLIENT: N

SIP CALL DATA
==========
ACTIVE CALL APPEARANCES:
NODENO TERMNO
NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12

9.2.6.2 QDN/QLEN/DISPCALL/PMIST/CALLTRAK:

The QDN, QLEN, DISPCALL, PMIST, and CALLTRAK tools will be supported for DPL Lines, and they will retain their same functionality and same command interfaces. There will be no impact to these tools by this activity. However, tools like CALLTRAK are tid-based, and thus when tracing on a DPL line with multiple active calls, trace data for ALL of the active calls with be captured.

9.2.6.3 DISPCALL:

DISPCALL is a tool which is used to capture the call data associated with the agent.The agent can be selected to capture the call information using following commands.They are SAVETID and SAVELEN.

The parameter for SAVETID is node number and terminal number.And parameter for SAVELEN is LEN of the agent. For DPL lines a new optional parameter KEY has been added along with the existing parameter for both SAVETID and SAVELEN.The KEY parameter holds the key value of the call appearance.The key values can be obtained form the tool DPLTEST.

IF the agent is selected with out key value for DPL lines, the tool checks for number of call appearance associated with the selected TID or LEN. IF there is only one call appearance associated with the TID/LEN then it gives the information associated with that call. IF there are multiple call appearances, then it displays the message saying multiple calls associated with this call,please enter the key value.

9.2.6.4 CALLTRAK:

CALLTRAK tool is used to capture the IO messages and procedure traces for the agent selected. For DPL lines, Since all the VIDS are allocated dynamically, and deallocated by the time the call complete, there would not be any vids associated with the agent by the time logs are displayed using the display command. So the log may not show the exact agent information.

For DPL lines, the hook has been added in the calltrak,so that it will store only the base TID in the call data and also capture all the information associated with that TID. Since only the base TID is stored in the call data, the calltrak log will not show the KEY information in the IO message for DPL lines.

Ex:

```
INCOMING  14:48:20.116  NODE TYPE= LGRP_NODE
SCP_X_ALERTING_MSG

NN= 00B5  TN= 002F  MSGTAG= 00  ROUTE= 0080  ERROR=
00  LENGTH= 0C

AGENT= SS   00 0 00 46    DN 6136215046

6D 02 00 00
```

9.2.7 Information regarding the Network Services / Signalling Interworking:

The following tables illustrate the network services/signalling interworking information.

Table 11: Client Services

Call Forward (local)
Call Return (local)
Call Waiting
Call Waiting Disable
Caller ID
Do Not Disturb (local)
Hold
3-Way Call
Call Transfer

Table 12: Country Specific services

Austria - Carrier Pre-Selection (via TNS parameter)
Belgium LNP (OR, ACQ)
Belgium TOPS
Belgium Lawful Intercept
Belgium 8 / 9 Digit Dialplan
France ETSI V.23 CLASS
France Backward Charging via Tax Message
Germany Network AOC
Germany Carrier Pre-Selection
Germany Carrier Pre-Selection
Germany TNS Routing
Germany Lawful Intercept
Germany Call Compl Busy Sub
Germany QSIG
Germany LNP
Germany Variable Dial Plan
Israel Backward Charging for Intnl Calls
Israel Voice Mail
Netherlands LNP (OR, ACQ)
UK LNP (OR and ACQ)
UK Carrier Pre Selection
UK Bellcore CLASS

UK Automatic Recall
UK MSAC
UK CDR Billing
UK ACD / Compucall
UK Network ACD
UK DPNSS Feature Transparency
Mexico TOPS
Mexico CLASS
Mexico Trunk Offer
Australia Lawful Intercept
Australia ACD / Compucall
Australia Network ACD
Australia CLASS
Australia TOPS
Australia TR533 (IN variant)
Australia LNP (ACQ)
Australia E800
Australia Carrier Pre-selection
Australia Centrex IP

Table 13: Agent Interworking

Agent Interworking Test - French BRI
Agent Interworking Test - Israel Res Lines (MMP15 only)
Agent Interworking Test - UK DASS 2

Agent Interworking Test - Mexico Fixed Wireless Access
Agent Interworking Test - Australia MFT
Agent Interworking Test - Australia TS13

Table 14: Signalling Interworking

Signalling Interworking test - ETSI ISUP V1
Signalling Interworking test - ETSI ISUP V2
Signalling Interworking test - IBN7
Signalling Interworking test - H.323
Signalling Interworking test - QSIG
Signalling Interworking test - ETSI PRI
Signalling Interworking test - V5.2
Signalling Interworking Test - Austria ISUP
Signalling Interworking Test - Belgium ISUP(migrating to ETSI V2)
Signalling Interworking Test - France, SSUTR2
Signalling Interworking Test - France, SPIROU
Signalling Interworking Test - France, SSURN

Signalling Interworking Test - German ISUP
Signalling Interworking Test - Israel ISUP
Signalling Interworking Test - Israel PRI
Signalling Interworking Test - Israel FDCP R2
Signalling Interworking Test - Netherlands ETSI ISUP V2
Signalling Interworking Test - Netherlands Dutch PRI
Signalling Interworking Test - Norway ISUP
Signalling Interworking Test - Spain ISUP V1
Signalling Interworking Test - Spain PRI
Signalling Interworking Test - Swiss ETSI ISUP V2
Signalling Interworking Test - Swiss PRI
Signalling Interworking Test - UK IUP
Signalling Interworking Test - UK ISUP
Signalling Interworking Test - UK IBN7 Backbone
Signalling Interworking Test - Mexico ISUP
Signalling Interworking Test - Mexico Telmex ISUP
Signalling Interworking Test - Mexican R2

Signalling Interworking Test - Australia IE ISUP
Signalling Interworking Test - Australia I-ISUP
Signalling Interworking Test - Australia ATUP
Signalling Interworking Test - Australia AISUP
Signalling Interworking Test - Australia IBN7 Backbone
Signalling Interworking Test - Australia RLT
Signalling Interworking Test - Australia TS14
Signalling Interworking Test - NZ ISUP
Signalling Interworking Test - Newzealnd R2

Table 15: PMA Based

Last Number Redial
Anonymous Call Rejection
IBN CFU/CFB/CFD intra-group / intergroup screening
IBN Do Not Disturb
Subscriber Activated Call Blocking - International Line Restriction for interna tional deployment
IBN Call Forward Program-ming - No call forward inter-rogation option may be desired in some markets.
Call screening override

Speed Dial programming

Table 16: Network based

Message Waiting
Station Message Detail Recording
Special Billing - CDR
Suspended Service
Terminating DN Billing
Tollfree Services
Multi-Switch Business Group (MBG) i/w
Interop with other Succession endpoints (PVG, MG9K, legacy lines via IW SPM IP, etc.)
Direct Inward Dial
Direct Outward Dial
E911 termination
IN - no digit collection
Lawful Intercept
Free Number Terminating
Customer groups with mix of Unistim, SIP, IBN lines
Subscriber Line Usage
Operator Number Identification
PIC
Dial Plan Management
Virtual Private Network (VPN)

INWATS / OUTWATS - Free-phone number Intl.
VFG
Local Number Portability
Carrier Pre-Selection (provi-sioned and prefix dialing)
Simple MEETME and PRE-SET Conference
Carrier Toll Denial - International calls - Inter-Lata - Intra-Lata
NCOS restrictions
NCOS Time of Day routing
Denied Termination
Denied Origination

9.2.8 International ICAF (Document : A00009771)

For international AIN the EDP2 and EDP8 are not tested for this release SN09 , since there these EDPs require digit collection.

9.3 Hardware Requirements or Dependencies

None.

9.4 Software Requirements or Dependencies

The CORE OAMP functionality has dependencies associated with some of the other components in the overall SIP lines feature:

- SESM
- CS2KSS
- GWC
- OSSGATE
- NCAS Link

9.4.1 SESM:

SESM EM needs the enhancements in table LGRPINV for bulk provisioning and line provisioning.

9.4.2 CS2KSS:

- QSIP core client is dependent on the CS2KSS API for QSIP query.
- SCPLITE APIs should be present to support the QSIP messaging.
- The CS2KSS profile team has to provide an API to get the Registration status and the SIP URI information
- The CS2KSS callp should provide an API to give the Active sessions for a SIP Line
- The CS2KSS will need to know the syntax of the QSIP messages it will receive from and send to the Core.

9.4.3 GWC

- GWC EM requires table SERVRINV enhancements to support the new term type DPL and a new exec lineup DPLEX.
- The state changes due to the operations BSY, RTS, FRLS, HOLD, NEXT performed on SIP lines in core should be propagated to the GWC.
- When the CS2KSS or GWC are taken down, the same should be notified to the core.
- Audit messages will be sent between the CORE & GWC and the message protocol from both the parties should be understood by each other.
- Carcodes for the DPL lines are restricted to RDTLSG for the North American market whereas it is restricted to GWLPOT for the International market.

9.4.4 OSSGATE:

- It needs the IBNFEAT and servord enhancements for line provisioning and other servord+ line commands like DEO, ADO etc.

9.4.5 NCAS Link:

- It should be available for the QSIP query to take place.

9.5 Limitations and restrictions

- Since the CLTG command is applicable only to POTS and RES lines, the CLTG Servord command applies to only RES DPL lines. CHG NCOS will have to be used for providing the functionality to IBN DPL lines. The CLTG and CHG will be done via SESM.

9.6 Interactions

None.

9.7 Glossary

Term	Description
CS2K	Communication Server 2000
CPD	Call Processing Deloaded
CB	Connection Broker
DEL	Deloaded
GWC	Gateway Controller
INB	Installation Busy
LMB	Line Module Busy
LCC	Line Class Code
NCAS	Non Call Associated Signalling
NEQ	Not Unequipped
OSSGATE	Operation Support System Gate
OAMP	Operation, Administration, Maintenance & Provisioning
CS2KSS	Communication Server 2000 Session Server
SESM	Succession Element and Sub-Element Manager
SB	System Busy
SERVORD	Service Order
SOC	Software Optionality Control
SCTP	Stream Control Transmission Protocol

10: Functional Description (FN): A00008721

10.1 Feature name and Feature ID

A00008721 - DUAL RCO2 Development

10.2 Description

10.2.1 Introduction

This activity introduces the DUAL Remote Switching Center Offshore (RCO2) concept into the Digital Multiplex Systems (DMS) International Market.

10.2.2 Basic DUAL RCO2 Terminology

In order to clearly explain the DUAL RCO2 concept first of all some keywords should be defined.

Interlinks: The PSide E1 links connecting the two RCO2s in a Dual pair

Spouse: The other RCO2 in the Dual pair (as opposed to "mate" which refers to the other unit of the same RCO2)

Master: The RCO2 listed first in table IRLNKINV -the one which performs the channel allocation for Interswitched calls, etc.

Slave: The RCO2 that is not the Master

Emergency Stand Alone (ESA): The state in which the RCO2s' ability to perform basic Call Processing (CallP) continues even when they are isolated from the Computing Module (CM). While in ESA, the RCO2 will perform only the most basic services, but it allows "communities of interest" served by the same RCO2 (or Dual RCO2) to maintain their ability to call within themselves even when cut off from the rest of the office for any reason.

Dual Emergency Stand Alone or Dual ESA (DESA): When both Spouses are separately in ESA mode and Interlink messaging is functioning, allowing calls to Interswitch; DESA Entry is attempted whenever ESA Entry occurs and conditions are right (e.g. the Spouse is already in ESA, as verified by an Interlink message exchange).

Forced ESA (FESA): An option that causes ESA Entry on one RCO2 to force immediate ESA Entry on the Spouse RCO2 so as to allow DESA to occur.

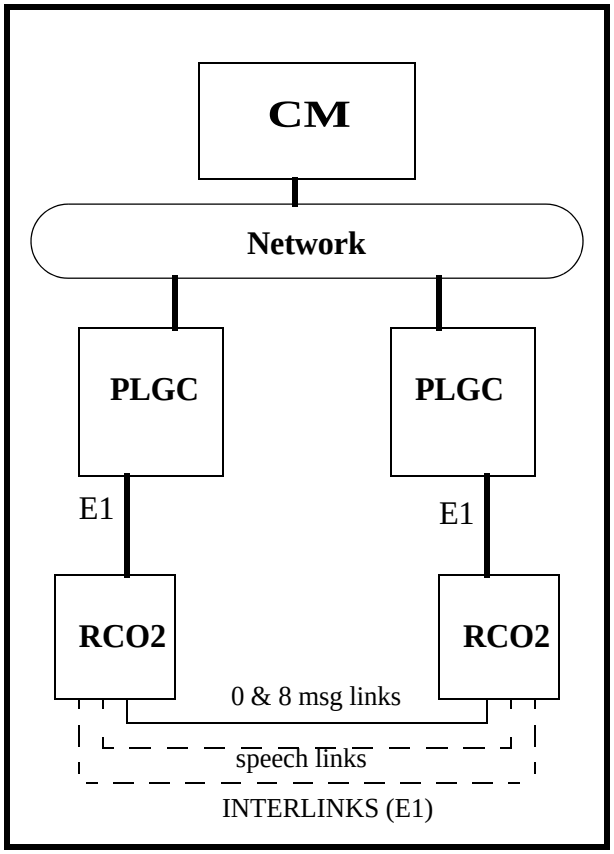
10.2.3 A General Dual RCO2 Description

A Dual RCO2 consists of two collocated RCO2 peripherals connected together by two or more P-side PCM30 links. When communication with the host (CC) is possible, interswitching occurs within the Dual RCO2 after CC call control determines that the call originating on an RCO2 can terminate on that RCO2's spouse. (The spouse RCO2 in a Dual RCO2 configuration is the RCO2 connected by interlinks to the particular RCO2 under discussion).

When communication with the CC is not possible, an RCO2 enters the ESA state. Once the RCO2 is in the ESA state, the ESA CC module handles the call processing functions previously handled by the CC. For an RCO2 which is in ESA, all calls that can be intraswitched are intraswitched. When DESA mode is achieved that coverage is expanded to incude calls that can interswitch as well.

Please refer to Figure 1 for an overview of the DUAL RCO2 interlinks.

Figure 1 Dual RCO2 Interlink Overview



10.2.4 Dual RCO2 Basics

A Dual RCO2 is made up of two collocated RCO2s connected via PSide Interlinks. There is a minimum of two Interlinks required as there must be two messaging Interlinks (no more, no less), with any additional Interlinks all considered speech Interlinks. All System maintenance for Interlinks is driven by the RCO2s, with CM providing MAP updates and the human interface (i.e. manual actions).

A Dual RCO2 consists of a Master RCO2 (the first one listed in table IRLNKINV) and a Slave RCO2. The Master makes the decisions about channel allocation and Interlink Maintenance, etc., and the Slave acts on them (this prevents contention). Each RCO2 spouse has a node table entry for the other spouse, but not for the International Line Controlling Module (ILCMs), etc., that hang off the other spouse (no need to message directly to them or their terminals). Though for Interswitching to work in DESA mode, both RCO2s receive Dialling Number (DN) info for the both RCO2s as part of ESA Data.

10.2.5 IRLNKINV Table

```
Table IRLNKINV:
RCCNAME INTERRCC IRLNKTAB ESAFORCE
-----------------------------------
REM1 RCO2 7 REM1 RCO2 8 (0 0) (8 8) (1 1) (9 9) $ Y
REM1 RCO2 8 REM1 RCO2 7 (0 0) (8 8) (1 1) (9 9) $ Y
```

Figure 2 Table IRLNKINV

Table IRLNKINV's tuples consist of;
an RCO2 name (REM1 RCO2 7), interlinked RCO2's name (REM1 RCO2 8), the interlinks and the FESA option boolean.

The first RCO2 datafilled (RCO2 7) becomes the master while the following one (RCO2 8) becomes the slave in a dual pair.

A maximum number of 14 interlinks can be datafilled between two RCO2s. Another important point about the interlinks is that interlinks 0 and 8 are reserved for messaging and must come first in the table while the other 12 are used as speech interlinks.

Please refer to Figure 3 for a table IRLNKINV datafill example.

10.2.5.1 FESA Mode

The ESAFORCE option boolean enables the FESA mode if set to Y. FESA mode is initiated when ESA Entry on one RCO2 forces immediate ESA Entry on the Spouse RCO2 so as to allow DESA to occur (note: Interswitched calls cannot survive Warm ESA Entry unless FESA is enabled).

10.2.6 IRLINK Map Screen

After posting the RCO2 by entering the mapci;mtc;pm level, a new command option, IRLINK, is introduced. The IRLINK command enables the management of interlinks by providing commands like;

BSY: used for busying an interlink
TST: used for running maintenance (out-of-service, in-service) tests on an interlink
RTS: used for bringing an interlink into service
INTERSW: used for enabling/disabling inter-switching
QUERYIR: used for querying the current status of an interlink. This command opens a new map interface where the interlinks alarm status can be monitored.

10.2.7 HUNT Groups

This activity supports MLH (Multi Line Hunt Group), DLH (Distributed Line Hunt Group) and DNH (Directory Number Hunt group) when the pilot DN (Directory Number) is located on the spouse RCC. Just like in single ESA DLH is treated as MLH and no circular hunting is allowed on DNH during dual ESA mode.

10.2.8 Logs, Alarms, and OMs

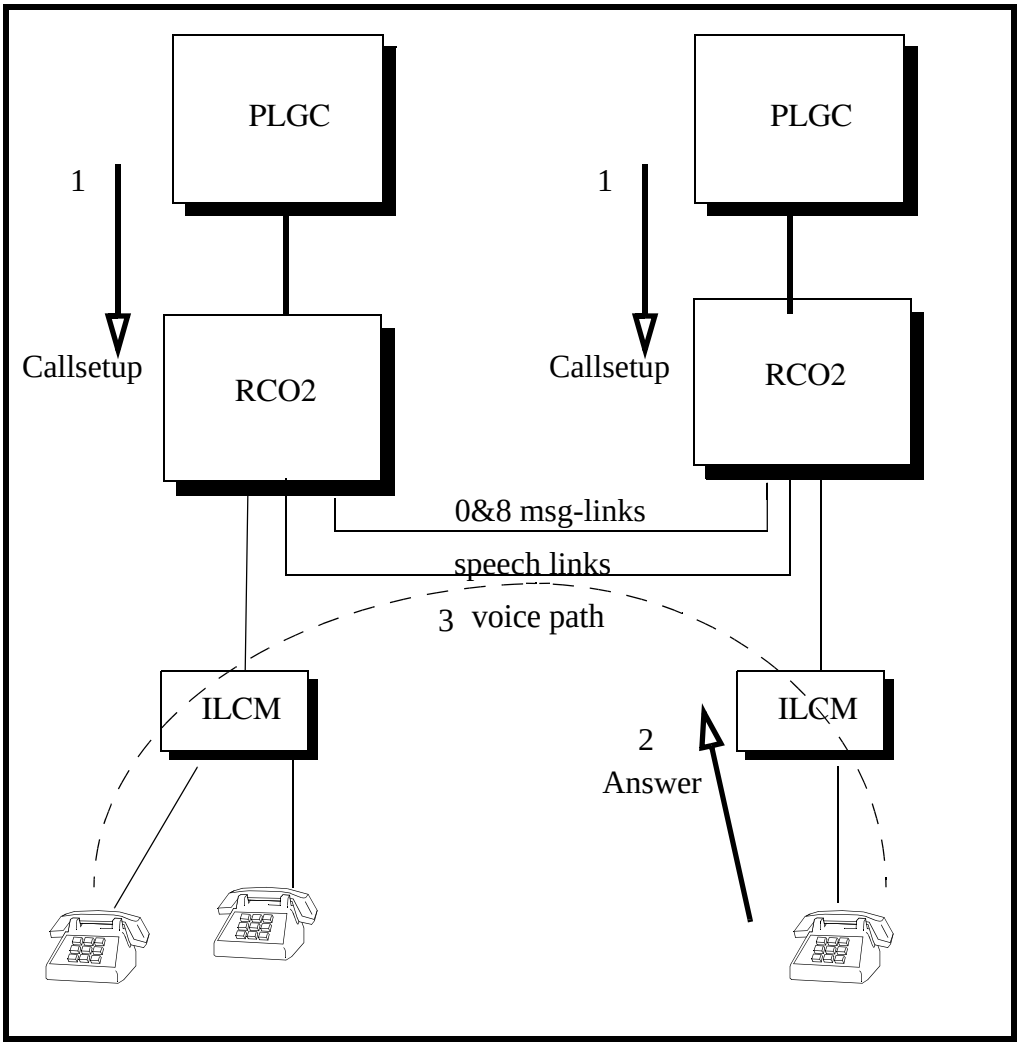
Existing PCM30 logs, alarms and OMs are valid for Dual RCO2 interlinks.

10.2.9 Some Basic Call Setup Scenarios

Some basic call setup scenarios are shown in Figures 4 to 7.

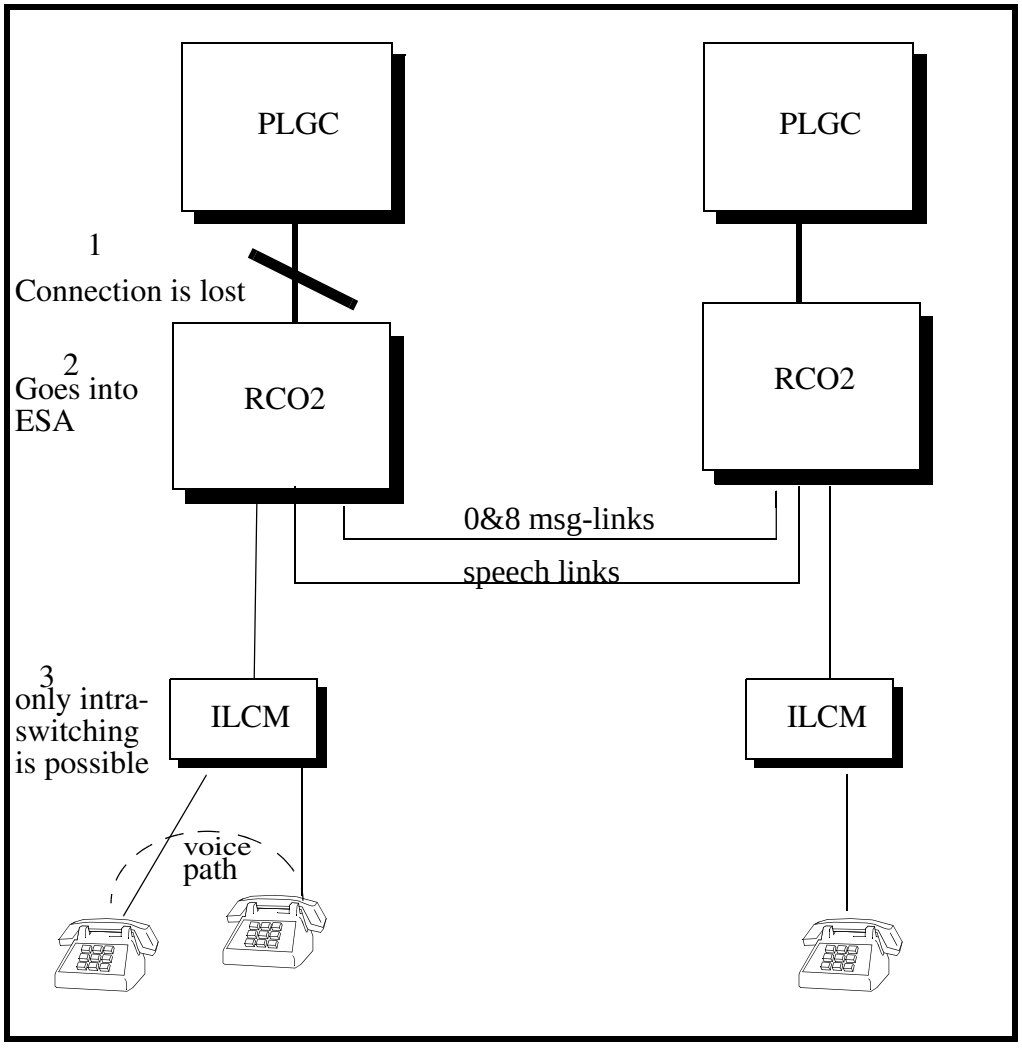
10.2.9.1 Inter- switching in Normal Mode

Figure 3 Normal Mode Inter- switched Call



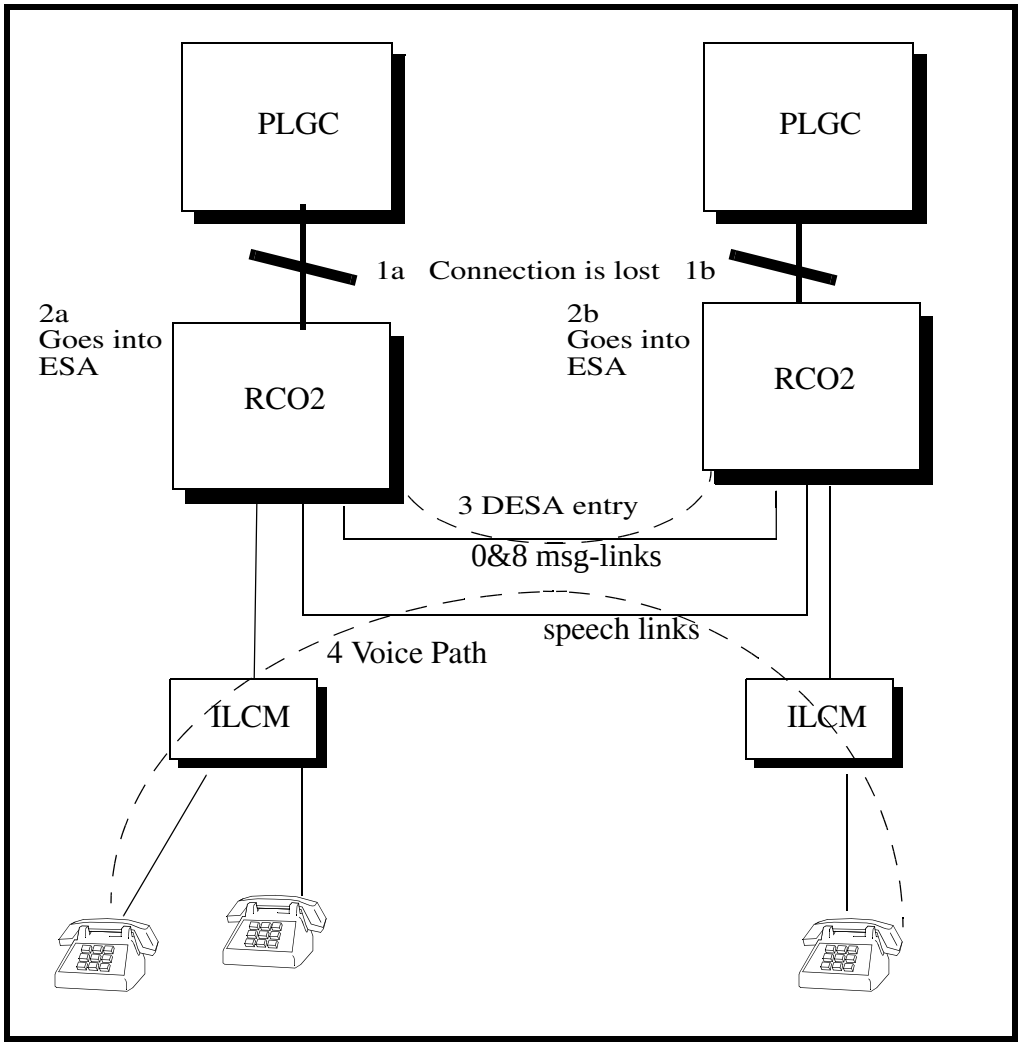
10.2.9.2 Intra- switching in ESA Mode

Figure 4 ESA Mode Intra- switched Call



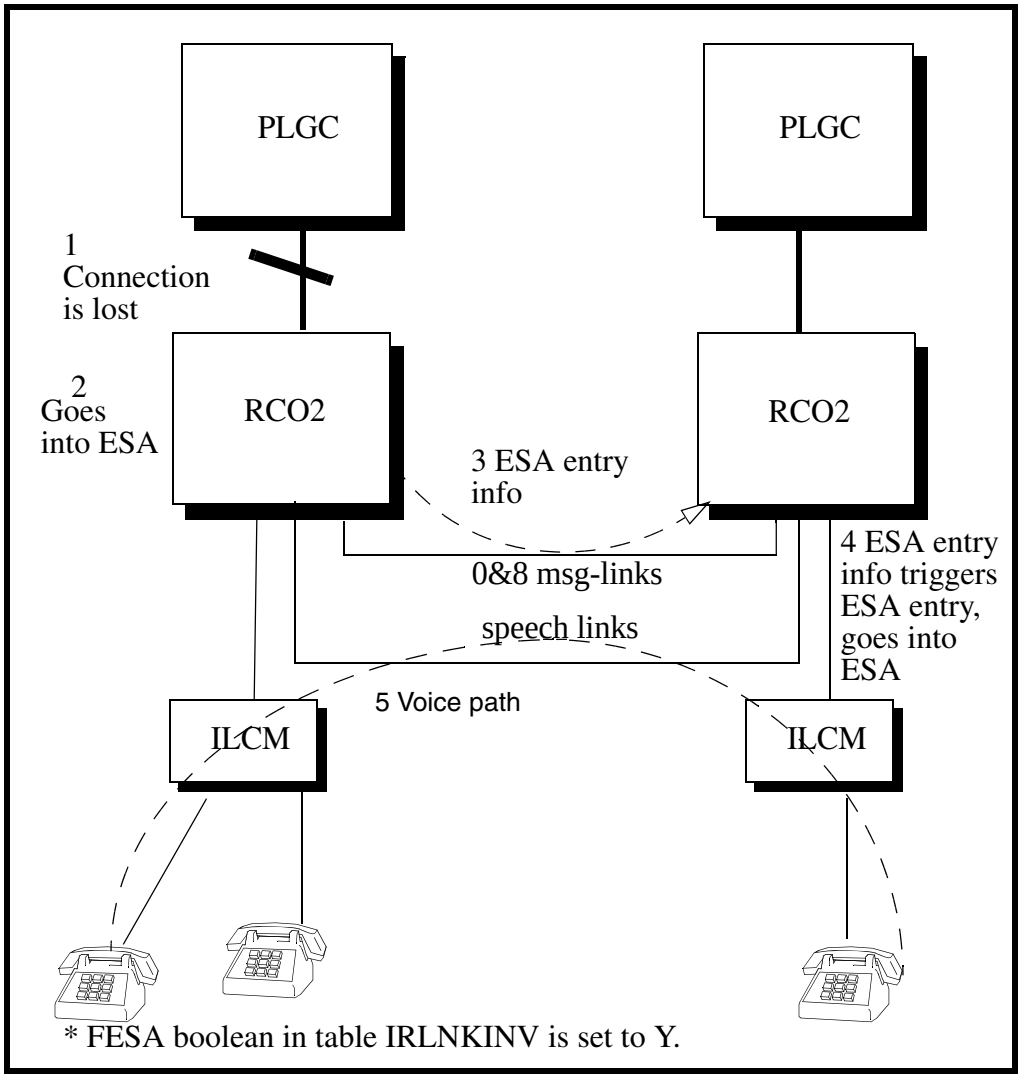
10.2.9.3 Inter-Switching in Dual ESA Mode

Figure 5 Dual ESA Mode Inter- switched Call



10.2.9.4 Inter- switching in Forced ESA Mode

Figure 6 Forced ESA Mode Inter- switched Call



10.2.10 Morocco Line cards

Morocco line cards NT6X93DA and NT6X94DA are supported for

- stand alone RCO2
- ILCM and LCME subtending from stand alone RCO2
- Dual RCO2
- ILCM and LCME subtending from Dual RCO2

Example of Table LNINV:
LEN CARDCODE PADGRP STATUS GND BNV MNO CARDINFO

REM1 07 0 00 01 **6X93DA** NPDGP HASU N NL N NIL

10.3 RCO2 ESA Office Parameters

RSC_ESA_NOTIFY_TONE: This parameter associates with the Distinctive Tone Burst for Emergency Operation feature. This parameter allows short bursts of tone preceeding standard dial tone to remote switching terminal. This tone indicates that emergency operation is in effect to users that have gone to off-hook.

This parameter is in table OFCENG and should be set to "**NO**" if no distinctive tone is required.

10.4 RCO2 ESA Translation Changes

When line translations are changed, the associated changes should be reflected to ESA callp in the RCO2. The impacted RCO2s should be posted at the "MAPCI;MTC;PM" level and "LOADPM PM CC ESADATA" command should be invoked to download the translation tuples into RCO2.

10.5 Hardware Requirements or Dependencies

Needs to be two RCO2 shelves and each of them have to be connected to different a PLGC.
Moroccan line cards NT6X93DA and NT6X94DA are supported in Extended Line Concentrating Module (LCME) as well.
Datafill example of a Dual RCO2 is given below.

Table RCCINV:
RCCNAME ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC LOAD EXECTAB CSPM CSLNKTAB ESA INTRASW ADDLMSGL OPTCARD TONESET PROCPEC E2LOAD EXTINFO OPTATTR

REM1 RCO2 8 101 CRSC 0 6 1 A 4 MX85AA WRI21AM (POTS POTSEX) (KEYSET KSETEX) (RMM_TERM RSMEX) (ESALINES ESAEX) $ PLGC 7 (0) (NILPORT) (3) $ Y Y N (UTR6) (RAM6X69) $ UK100 AX74AA AX74AA UPFWNV03 N $

REM1 RCO2 7 102 CRSC 0 6 1 A 4 MX85AA WRI21AM (POTS POTSEX) (KEYSET KSETEX) (RMM_TERM RSMEX) (ESALINES ESAEX) $

PLGC 1 (4) (5) (6) (7) $ Y Y N (UTR6) (RAM6X69) $ UK100 AX74AA AX74AA UPFWNV03 N $

Table RCCPSINV:
RCCNAME PSLNKTAB

REM1 RCO2 7 (0 NILTYPE) (1 NILTYPE) (2 NILTYPE) (3 NILTYPE) (4 NILTYPE) (5 NILTYPE) (6 NILTYPE) (7 NILTYPE) (8 NILTYPE) (9 NILTYPE) (10 NILTYPE) (11 NILTYPE) (12 NILTYPE) (13 NILTYPE) (14 NILTYPE) (15 NILTYPE) (16 NILTYPE) (17 NILTYPE) (18 NILTYPE) (19 NILTYPE) (20 NILTYPE) (21 NILTYPE) (22 DS30A) (23 DS30A) (24 DS30A) (25 DS30A) (26 DS30A) (27 DS30A) (28 DS30A) (29 DS30A) (30 DS30A) (31 DS30A) (32 NILTYPE) (33 NILTYPE) (34 NILTYPE) (35 DS30A) (36 DS30A) (37 DS30A) (38 DS30A) (39 DS30A) (40 DS30A) (41 NILTYPE) (42 NILTYPE) (43 NILTYPE) (44 NILTYPE) (45 NILTYPE) (46 DS30A) (47 DS30A) (48 NILTYPE) (49 NILTYPE) (50 NILTYPE) (51 NILTYPE) (52 DS30A) (53 DS30A) $

REM1 RCO2 8 (0 NILTYPE) (1 NILTYPE) (2 NILTYPE) (3 NILTYPE) (4 NILTYPE) (5 NILTYPE) (6 NILTYPE) (7 NILTYPE) (8 NILTYPE) (9 NILTYPE) (10 NILTYPE) (11 NILTYPE) (12 NILTYPE) (13 NILTYPE) (14 NILTYPE) (15 NILTYPE) (16 NILTYPE) (17 NILTYPE) (18 NILTYPE) (19 NILTYPE) (20 NILTYPE) (21 NILTYPE) (22 DS30A) (23 DS30A) (24 DS30A) (25 DS30A) (26 DS30A) (27 DS30A) (28 DS30A) (29 DS30A) (30 DS30A) (31 DS30A) (32 DS30A) (33 DS30A) (34 DS30A) (35 DS30A) (36 DS30A) (37 DS30A) (38 DS30A) (39 DS30A) (40 DS30A) (41 DS30A) (42 DS30A) (43 NILTYPE) (44 NILTYPE) (45 NILTYPE) (46 NILTYPE) (47 NILTYPE) (48 NILTYPE) (49 NILTYPE) (50 NILTYPE) (51 NILTYPE) (52 NILTYPE) (53 NILTYPE) $

Table IRLNKINV:
RCCNAME INTERRCC IRLNKTAB ESAFORCE

REM1 RCO2 7 REM1 RCO2 8 (0 0) (8 8) (1 1) (9 9) $ Y
REM1 RCO2 8 REM1 RCO2 7 (0 0) (8 8) (1 1) (9 9) $ Y
BOTTOM

10.6 Software Requirements or Dependencies

Dual RCO2 feature works with WRI22 & ISN09 front-end software. If a feature bridging to ISN06 or ISN07 is requested, then WRI21AM should be used.

10.7 Limitations and restrictions

10.7.1 Limitations

This feature works only when a Dual RCO2 is equipped.

A host link channel is required for the setup of inter- switched calls.

One physical interlink channel is required for an inter-switched call.

10.7.2 Assumptions

Both RCO2s reside under the same Central Control (CC).

CC will attempt to interswitch only when interlinks are in service.

10.7.3 Exceptions

If there are no resources for interswitching the call, then the call is switched using host link channels.

10.7.4 Restrictions

The maximum number of DNs available for a Dual RCO2 is now limited to 12800. (2 RCO2s x 1 DN per line x 6400 lines/RCO2)

This feature is only designed to support interswitching of simple POTS calls. No translation types not supported by Feature BF0614, ESA Translations, are supported.

In addition, translations for calls terminating on trunks located on the spouse RCO2 are not supported. Neither are hunt group services, automatic lines terminating on the spouse RCO2, nor IBN extensions for terminations on the spouse RCO2.

The RCO2 interlinks cannot be displayed at the CARRIER level nor can they be displayed by the TRNSL command when an RCO2 is posted at the MAP.

The type of information displayed at the CARRIER level for peripheral-side links can be viewed for interlinks at the IRLINK level via the QUERYIR command. The QUERYIR display is not dynamically updated.

For IBN, BRI, Coin and EBS lines, only basic calls (no services supported) can be established.

When a hunt group is split across the two RCCs in a dual configuration the hunting for an idle member starts with the lines in the RCC where the

call is originated from. This alters the operation of DNH. If the dialed DN is located on the spouse RCC, seizure will first be attempted on lines on the originating RCC.

There can be a maximum of 400 hunt groups on two RCCs in dual configuration in ESA mode if at the most 200 mutually exclusive hunt groups are configured on each RCC. If hunt groups are split across the two RCCs the maximum number of hunt groups is reduced by the number of hunt groups split across RCCs.

The huntgroup members should be distrinuted on both spouses if the pilot DN is assigned in any of the spouse.

The maximun number of hunt group members is 4000 on each RCC.This number is reduced by the number of split hunt groups when configured in dual ESA.

10.8 Interactions

N/A

10.9 Glossary

Term	Description
Interlinks	The PSide E1 links connecting the two RCO2s in a Dual pair
Spouse	The other RCO2 in the Dual pair (as opposed to "mate" which refers to the other unit of the same RCO2)
Master	The RCO2 listed first in table IRLNKINV - the one which performs the channel allocation for Interswitched calls, etc.
Slave	The RCO2 that is not the Master
DESA	Dual Emergency Stand Alone or Dual ESA - when both Spouses are separately in ESA mode and Interlink messaging is functioning, allowing calls to Interswitch; DESA Entry is attempted whenever ESA Entry occurs and conditions are right (e.g. the Spouse is already in ESA, as verified by an Interlink message exchange)

Term	Description
FESA	Forced ESA - an option that causes ESA Entry on one RCO2 to force immediate ESA Entry on the Spouse RCO2 so as to allow DESA to occur (note: Interswitched calls cannot survive Warm ESA Entry unless FESA is enabled)
RCO2	Remote Switching Center Offshore
ILCM	International Line Concentrating Module
CSM	Channel Supervision Message
PLGC	PCM30 Line Group Controller
LCME	Extended Line Concentrating Module
CM	Computing Module

10.10 References

AF0551- Interlink Maintenance

AF0565 - ESA Call Control

AF0952 - PP ESA Maintenance

AF1008 - ESA Call Control II

11: Functional Description (FN): A00009024

11.1 Feature name and Feature ID

A00009024 - ETSI BRI (Basic Rate Interface) on Succession - Phase I

11.2 Description

This feature implements the H.248 BRI on CS2K with a 3rd party gateway named Keymile. The design is based on the SN08 development which was a prep feature, A00007788.

This feature is also a prep activity and only point-to-point BRI is supported with limited set of BRI features (CLIP, CLIR, COLP, COLR, and DDI). This development is not suitable for deployment. It is not be productized nor have OAM&P support, but serve as an interim step towards full functionality to be completed in SN10.

The provisioning is performed from SESM. For BRI support on SESM, another activity (A00009521) is being developed.

Trial development is limited to PtoP. Specifically, only TEI=0 is supported. Keymile MG shall use TEI=0 only in IUA Message Headers.

H.248 is unaware of D-channels, i.e. no H.248 TerminationID for D-channels.

11.3 Hardware Requirements or Dependencies

N/A

11.4 Software Requirements or Dependencies

N/A

11.5 Limitations and restrictions

BRI point to point functionality is prepared for stable trial of basic call and service capability:

- No support for call survival in the following situations:
  - Core restart warm
  - Core warm swact
  - Core Mtc swact
  - GWC warm swact
  - Keymile GW fail-over
- There is no support for traffic
- No capacity testing
- Provisioning

- •Maximum 1024 BRI lines can be datafilled per GWC. This limitation is handled by SESM.
- •Each BRI gateway can have only 511 lines datafilled. For such gateway with >511 lines, multiple virtual LGRP should be employed. This limitation is handled by SESM.
- •Provisioning performed by PMDEBUG “gwcd regte”, or MIB browser (in case of no BRI-compatible SESM support) is get lost on unit initialization and all Core and GWC provisioning is required to be removed and re-performed.

•Max 250 loops are supported per GW, since each BRI loop is using 1 stream, and each GW is using 1 association, and we can have max 250 streams per association currently.
•Only following agent interworkings are supported:
- •BRI <--> Keymile POTS
- •BRI <--> PVG - ISUP

•Service Interworking
- •No services other than CLIP, CLIR, COLP, COLR, and DDI will be supported.
- •Other services supported by POTS and ISUP agent is not supported for BRI interworking

•No billing or metering support
•No NPI
•limited engineering rules
•limited solution documentation
•Limited OAM&P support (provisioning, SESM, et al)
•Full point to point BRI support is not provided
•BRI Point to MultiPoint support is not provided (DMS-100 Implementation of ETSI ISDN Basic Rate Interface at the S/T Reference Point).
•Specification Enhancements are not provided to include BRI multiple TEI support in: Layer 2, IUA/SCTP, H.248
•Layer 1 and 2 deactivation is not provided
•Full audit support is excluded.

11.6 Interactions

This feature is based on SN08 prep activity, A00007788

For the BRI support on SESM, another activity is being designed, A00009521

The trial functionality will be validated under A00009493.

11.7 Glossary

Term	Description

12: Functional Description (FN): A00009037

12.1 Feature name and Feature ID

A00009037 - CORE - Enhanced ESA for International MG9000

12.2 Description

This activity allows the download of information necessary to support International Emergency Stand Alone (ESA) call processing across all native (non ABI) and ABI lines served by a single MG9000 for intra and internodal ESA.

The download takes place from the CS2000 core to an MG9000 element manager. The data is generated by the core at 6:00 AM (configurable) and stored in a file called ESA_SYSTEM_SD$XML on a device specified by existing OFCENG parameter ESA_GWDATA_DEVICE. It is then downloaded by the MG9000 EM through the SDM.

This activity is CS2000 data collection activity of Intl ESA support on MG9k. So, this FN covers only data collection part on CS2k. This activity can be broken into three parts:

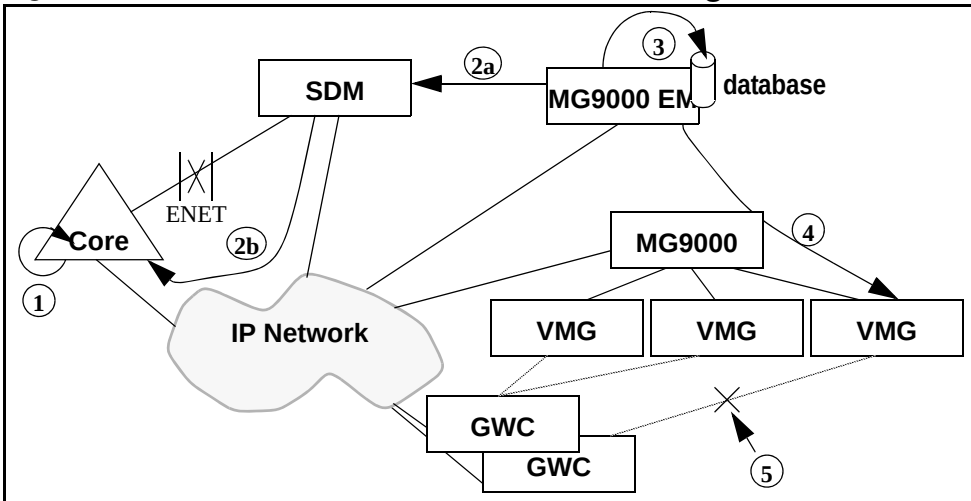
- Intl ESA Data Collection Trigger
- Intl ESA Data Format
- Intl ESA Table

12.2.1 Background Information

ESA functionality is already provided for North American dialing plan which supports 10 digit national and 7 digit subscriber numbers. However, in international markets, subscriber numbers are based on ITU-T E.164 recommendations.

Data transmission and entering ESA mode of MG9k will be same as Basic/NA ESA modes. Please see **A00002020** and **A00002380** activities FNs for more information about ESA data transmission and entering ESA mode.

Figure 1 MG9000 ESA Functional Behavior Diagram



1 Core generates ESA data file(s) at configurable time every day

2 MG9000 EM initiates ftp through SDM

3 MG9000 EM extracts data for each VMG and saves in Oracle database

4 MG9000 EM audits and updates VMG data using XML

5 VMG(s) enter ESA when communication with GWC is lost

12.2.2 Desired Behavior

In international markets, dialling plan may vary each market regardless of actual DN definition on CS2000 core. For example, DN may be defined as 10 digits (3 digits SNPA + 3 digits OFC code + 4 digits STN number) but dialling plan only use 9 digits.

To support international dialling plan, new Intl ESA table is introduced with this activity. This new table contains customer group information and the digit analysis data that applies to specified types of calls. If new table does not contain digit analysis data, default tuple is used in this new table.

New table entries are explained in following sections.

12.2.3 Project Details

This activity (A00009037- CORE - ENHANCED ESA FOR INTERNATIONAL MG9000) is one of three activities to enhance ESA for the MG9000 in the SN09 time frame. The activity addresses the core code and will be sourced into the SN09 stream.

The other features are

- “A00009021 - Enhanced ESA for International MG9000”
- “A00009282 - MG9KEM - INTERNATION ESA AND MLPP SUPPORT”

MG9000 ESA is supported by series of activities. Therefore, please also see Core portion of following activities:

- A00002020 - ESA Translation download
- A00002380 - MG9k ABI ESA

12.3 Intl ESA Data Collection Trigger

ESA data will be built by the core every 24 hours at 6:00 AM if existing office parameter in OFCENG table (ESA_GWDATAUPD_BOOL) is set or as the result of exiting manual CI command (ESACOLL under ESATOOLS directory). Changes to CS2000 line data will not be reflected in the MG9000 until the data has been

- built by the core
- downloaded by the MG9000 Element Manager (EM)
- downloaded to the MG9000

Data collection trigger time is also controlled by existing office parameter ESA_GWDATAUPD_HOUR in OFCENG table.

12.4 Intl ESA Data Format

This activity uses XML file format to store international data. XML file name would be ESA_SYSTEM_SD$XML and stored device name would be datafilled by using existing office parameter ESA_GWDATA_DEVICE. Default value for this office parameter is SFDEV. But, the maximum size of SFDEV is 5 million bytes so a disk device must be available for large offices.

Please refer to ESADATA document of activity A00002020 “ESA Translation download” to see collected ESA tables and ESA information from code and their XML formats.

But, please note that EXTN index in table IBNXLA is not collected if ESADGCOD table is not empty.

12.5 Intl ESA Table

This activity introduces new ESA table (ESADGCOD) for international markets to support international dialling plan on VMGs.

This new table contains customer group information and the digit analysis data that applies to specified types of calls. Following is an example tuple datafill for new table ESADGCOD.

Figure 2 Tuple examples for new table ESADGCOD

TABLE ESADGCOD

KEY			NUMDGTS	ADDIGS	STRIP
IBN_ESA_DEFAULT*	00	50	7	216	0
IBN_ESA_DEFAULT*	51	70	4	216783	1
IBN_ESA_DEFAULT*	71	99	10	$	0
CUST783	0000	0920	8	$	1
CUST783	10	19	8	442	2
CUST783	4	4	4	212442	0
CUST783	5	5	7	$	0
PTTPUB	00	08	8	$	1
PTTPUB	1	9	4	102216	0

* IBN_ESA_DEFAULT is used for customer groups which are not datafilled ESADGCOD table or it is used if related customer group does not have FROM-TOD digits range for dialled digits.

Table 1 Field explanations of new table ESADGCOD

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
KEY	NEW	DGNAME	alphanumeric (up to 16 chars)	Character entries can be entered up to 16 Chars. But, only “IBN_ESA_DEFAULT ” and customer group names (datafilled in CUSTENG table) can be accepted.
		FROMD	up to eight digits(0 to 9, B, or C)	From digits.
		TOD	up to eight digits(0 to 9, B, or C)	To Digits
NUMDGTS	NEW	N/A.	Number {0 to 15}	NUMDGTS:Number of digits to collect (including prefix digits).
ADDIGS	NEW	N/A.	up to fifteen digits (0 to 9, B or C)	ADDIGS: The digits stream which will be added to collected digits.
STRIP	NEW	N/A.	Number {0 to 15}	STRIP: Number of digits to be removed from collected digits.

Use of IBN_ESA_DEFAULT tuple may have following advantages:

- If switch has same dialling plan for all customer groups only IBN_ESA_DEFAULT tuple may be provisioned.
- If only a few customer groups have different dialling plan, only different dialling plans may have datafill in ESADGCOD table. The rest of the customer groups may still use IBN_ESA_DEFAULT datafill.

Figure 3 Tuple examples for table ESAPXLA

```
TABLE ESAPXLA
PXLAKEY RESULT
--------------
ESAXLA   LGRP   VMG 2 0    911   L LGRP 02 0 00 08 N 0
ESAXLA   LGRP   VMG 3 0    911   L LGRP 03 0 00 10 N 0
ESAXLA   LGRP   VMG 2 0    0911   L LGRP 02 0 00 15 N 0
```

Following table shows the dialling examples according to datafills in figure 2 (Table ESADGCOD) and figure 4 (Table ESAPXLA).

Table 2 Dialling examples and results using ESADGCODE table

Dialled Number	Used Tuple in ESADGCOD/ ESAPXLA	Result	Originating Line CUSTGRP
0550 - XXX	IBN_ESA_DEFAULT 00 - 50	216 - 0550 - XXX (Default tuple match)	CUST783
12 - XXXXXX	CUST783 10 - 19	442 - XXXXXX	CUST783
2 - XXXXXX	IBN_ESA_DEFAULT 00 - 50	216 - 2 - XXXXXX (Since CUST783 does not have FROMD - TOD for prefix 2. DEFAULT tuple is used.)	CUST783
3 - XXXXX	IBN_ESA_DEFAULT 00 - 50	Treatment (reorder). (since collected number of digits is not equal to NUMDGTS in DEFAULT tuple.)	CUST783
4 - XXX	CUST783 4 - 4	212442 - 4 - XXX	CUST783
5 - XXXXXX	CUST783 5 - 5	5 - XXXXXX	CUST783
911	ESAXLA 911	DN of LGRP 00 0 00 08 if originating DN is in VMG 2 DN of LGRP 01 0 00 10 if originating DN is in VMG 3	CUST783
0911	ESAXLA 0911	DN of LGRP 04 0 00 15 if originating DN is in VMG 2.	CUST783

12.5.1 Limitations and restrictions

- IBN_ESA_DEFAULT name should not be used in table CUSTENG. If it is used as customer group name, no default entry would be downloaded to MG9000.
- ESAPXLA table has priority over ESADGCOD table. So, if there is overlaps prefixes in tables ESAPXLA and ESADGCOD, ESAPXLA tuple is used.
- Maximum allowable tuple count in table ESADGCOD is 3000 (independent from customer group datafills)

12.6 Hardware Requirements or Dependencies

Since each VMG will include ESADGCOD data separately, XML file size may be greater that 5 million word (10 million bytes). Therefore a disk device must be available for large offices.

12.7 Software Requirements or Dependencies

All Software requirements and dependencies of activities A00002020 and A00002380 are also valid for this activity.

12.8 Limitations and restrictions

All Limitations and restrictions of activities A00002020 and A00002380 are also valid for this activity.

- EXTN table which stores EXTN information in table IBNXLA is not collected if ESADGCOD table is not EMPTY.
- ESADGCOD is supported for the lines which has Customer group information.

12.9 Interactions

The MG9000 EM downloads the ESA data file from the core daily. The time for this download should be set so the data has been freshly built. The default values in the core and MG9000 EM are set to ensure the data is downloaded soon after being built.

12.10 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema __X___

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

12.11 Glossary

Term	Description
ABI	Access Bridging Interface
CS2000	Call Server 2000
EIOP	Ethernet Input/Output Packlet
EM	Element Manager
ESA	Emergency Stand Alone
MG9000	Media Gateway 9000
SDM	SuperNode Data Manager
VMG	Virtual Media Gateway

13: Functional Description (FN): A00009039

13.1 Feature name and Feature ID

A00009039 “International MG9000 Line Test Support”

13.2 Description

MG9000 Line Testing for International Markets is handled by two activities during ISN09 time frame:

a. A00009038 - MG9000 Line Test Support Framework

b. A00009039 - International MG9000 Line Test Support

A00009038 is responsible of providing messaging interface for the supported line test commands between LGRP and GWC.

And this feature, A00009039, provides support for MG9K Line Testing for International markets.

Line Testing and troubleshooting are done using Maintenance and Administration Position (MAP) user interface at the levels under LNS MAP level. The LNS MAP level contains the lines test position (LTP) menu commands, the automatic line testing (ALT) menu commands and the lines service trouble (LNSTRBL) commands. Messaging needed to perform these functions are handled by the AI messaging interface which is provided by activity A00009038.

Prior to this feature, only a few MAP commands, such as BSY, RTS, and FRLS, were supported for MG9K lines in International Markets.

As the primary component of this feature, support of No Test Trunk (NTT) is provided. And majority MAP commands under the LTP, ALT and LNSTRBL level for Succession MG9000 **POTS** and **EBS** lines are provided, ShowerQ support and Subscriber Premise Test support are also provided for these types of Succession lines.

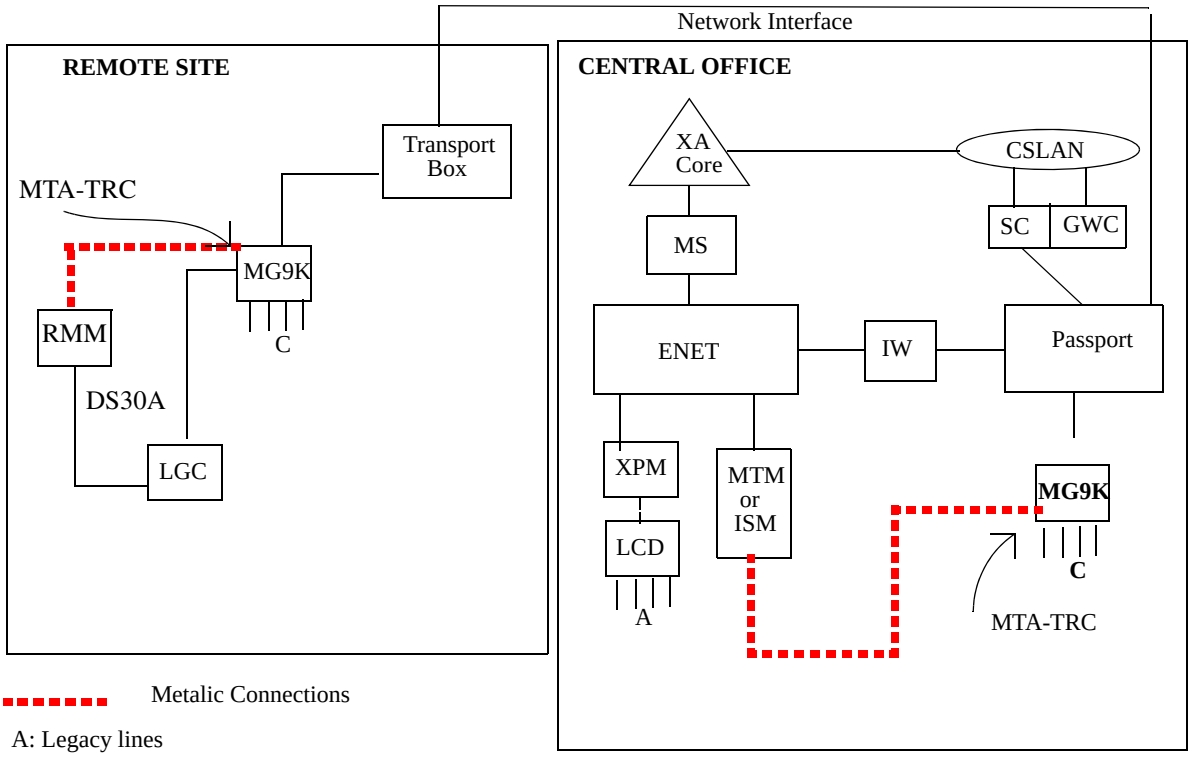
Note: Please note that Line Tests are supported already for CNA market and A00009039 will use this model as a reference.

13.2.1 Overview of Line Maintenance Commands

The following figure is a physical representation of the line types supported in this activity. With this activity, line test support is provided for only native MG9000 lines, with GWLPOTS and GWLEBS card codes. **This activity supports MAP-based line testing. MAP-based line testing uses the legacy**

DMS MTM/ISM hardware or RMM hardware for remote sites and software along with the MG 9000 Line Test System to perform MG 9000 line testing from the Maintenance and Administration Position (MAP) terminal. As shown in the Figure 1, MG9K native lines in the central office are tested by using MTM/ISM hardware. MG9K native lines in the remote side are tested by using RMM hardware.

Figure 1 Line Test Configuration for MG9000 native lines.



A: Legacy lines
C: Native MG9K lines, which include POTS, GND, , EBS types of terminals.
B
****: This solution can be used when MG9K in remote site does not have ABI interface.Normally, RMM is used with LGC connected to the MG9K with ABI interface in Remote site.**

Also, DMS legacy lines located in Peripheral Module (PLGC) can be connected to the MG9K over ABI interface. These lines are known as ABI lines. The Figure illustrates MAP-based line test configuration for ABI lines in detail.

ABI lines are tested using MTM/ISM hardware in the Central office.ABI lines in the remote site are tested using RMM hardware. The testing of ABI lines are already supported. ABI line test support is a test-only issue for this activity. To test ABI lines, Core sends the MAP based line test request to the Gateway Control (GWC). GWC encapsulates this test request into H.248 package and sends the gateway of MG9K. MG9K receives the MAP based line test request from H.248 package and then send it to the LGC. After testing, test results are sent to Core with same route.

Figure 2 Line Test Configuration for MG9K ABI lines

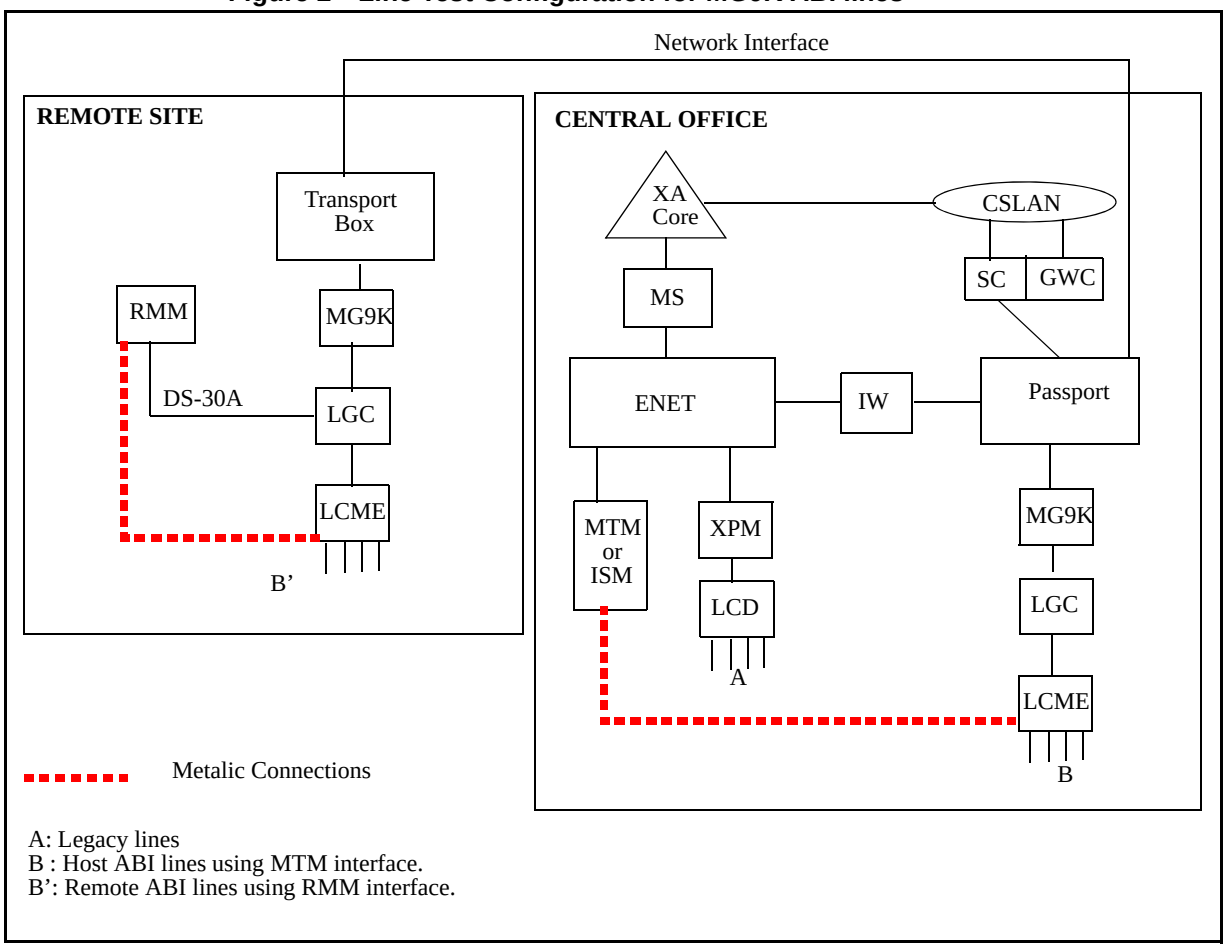
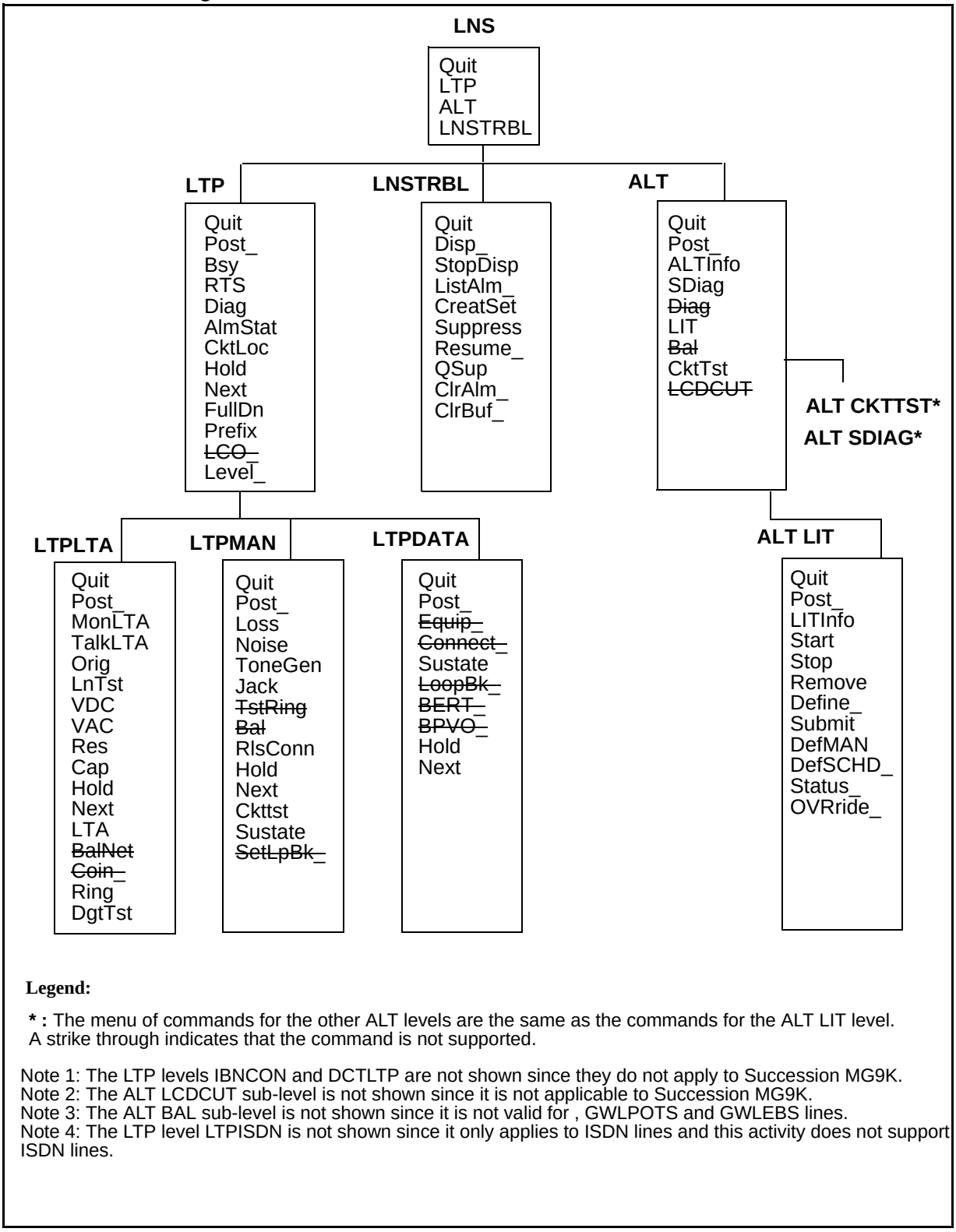


Figure 3 contains a list of the line maintenance commands shown at their respective levels. Most commands are supported for native MG9000 lines. These unsupported commands are indicated by a strike through. Check the legend for additional clarification.

Figure 3 Line Maintenance Commands



Legend:

*** :** The menu of commands for the other ALT levels are the same as the commands for the ALT LIT level.
A strike through indicates that the command is not supported.

Note 1: The LTP levels IBNCON and DCTLTP are not shown since they do not apply to Succession MG9K.
Note 2: The ALT LCDCUT sub-level is not shown since it is not applicable to Succession MG9K.
Note 3: The ALT BAL sub-level is not shown since it is not valid for , GWLPOTS and GWLEBS lines.
Note 4: The LTP level LTPISDN is not shown since it only applies to ISDN lines and this activity does not support ISDN lines.

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

13.2.2 LTP Menu Commands

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

- **Quit**: The QUIT command is used to leave the current level and return to a higher level.
- **Post**: Posts a line or set of lines to the LTP.
- **Bsy**: The BSY command changes the state of the line in the control position, or optionally all lines that are posted, to a specific state.
- **RTS**: The RTS command changes the state of the line in the control position, or optionally the complete set of posted lines, from MB to IDL.
- **Diag**: The DIAG command performs an extended diagnostic on a line in the control position that is in the MB or IDL state, and displays the results on the LTP screen.
- **AlmStat**: The ALMSTAT command triggers the alarm system of the LNS subsystem and displays the status of alarms in the full switch by type of alarm, when used without parameters. The command is used with parameters to display all or selected alarms at specified units in the host or remote sites, or to change the thresholds of the alarm classes in the full switch.
- **CktLoc**: The CKTLOC command locates and identifies the circuit card used for the line circuit in the control position, and displays circuit characteristics.
- **Hold**: The HOLD command moves the line in the control position to a spare hold position, and the next line from the posted set, if any, to the control position.
- **Next**: The NEXT command moves the line in a specified HOLD position to the control position, or replaces the line in the control position with the line in a specified hold position; and exchanges, saves, or drops the replaced line from LTP control.
- **FullDn**: The FULLDN command displays the full National Number.
- **Prefix**: The PREFIX command clears the LTP of prefix digits. Optionally it sets or changes prefix digits.
- **Level_**: The Level command gives the user access to the sublevels LTPLTA, LTPMAN, LTPDATA, IBNCON, and DCTLTP at the MAP.

13.2.2.1 LTPLTA Menu Commands

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

- **Quit**: The QUIT command is used at the LTPLTA sublevel in the same way as it is described at the LTP level.
- **Post_**: The POST command is used in the LTPLTA sublevel in the same way as it is described at the LTP level.
- **MonLTA**: The MONLTA command connects a headset circuit to the MG9000 line in the control position for listening purposes.
- **TalkLTA**: The TALKLTA command connects a talk circuit to a subscriber on a MG9000 line, and optionally connects a talk battery so that the tester can converse with the subscriber when the CO relay is operated.
- **Orig**: The ORIG command configures the loop side of a line circuit in either the off-hook mode or the on-hook mode, or alternates between modes.

  Note: LnTst: The LNTST command performs resistance, capacitance, and voltage tests on a MG9000 line.

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

  User Action: Measure the AC DC TIP and AC DC RING voltages using the VDC command.
- **VDC**: The VDC command performs a dc voltage measurement on a subscriber loop.
- **VAC**: The VAC command performs an ac voltage measurement on a subscriber loop.
- **RES**: The RES command performs resistance measurements on a subscriber loop.
- **CAP**: The CAP command performs a capacitance measurement on a subscriber loop.
- **Hold**: The HOLD command is used at the LTPLTA sublevel in the same way that it is described at the LTP level.
- **Next**: The NEXT command is used at the LTPLTA sublevel in the same way that it is described at the LTP level.
- **LTA**: The LTA command connects the LTA to a line card, or releases the LTA from a line card.
- **Ring**: The RING command places ringing voltage on the loop of a MG9000 line.
- **DgtTst**: The DGTTST command tests the DIGITONE pad or dial on the subscriber station.

13.2.2.2 LTPMAN Menu Commands

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

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

13.2.2.3 LTPDATA Menu Commands

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

- **Quit_**: The QUIT command is used at the LTPDATA sublevel in the same way as it is described in the LTP level.
- **Post_**: The POST command is used at the LTPDATA sublevel in the same way as it is described in the LTP level.
- **Sustate**: The SUSTATE command reports on the loop status of the subscriber data line.

- **Hold**: The HOLD command is used at the LTPDATA level in the same way as it is described in the LTP level.
- **Next**: The NEXT command is used at the LTPDATA sublevel in the same way as it is described in the LTP level.

13.2.3 LNSTRBL Menu Commands

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

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

13.2.4 ALT Menu Commands

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

- **Quit**: The QUIT command causes the system to leave the current level and return to a higher level of the MAP.
- **Post_**: The POST command posts the scheduled ALT TESTID that is stored in memory (in Table ALTSCHED)
- **ALTInfo**: The ALTINFO command checks test data stored in memory (Table ALTSCHED)

- **SDiag**: The SDIAG command accesses the SDIAG sublevel of ALT. If a TESTID is not entered as a parameter, a new TESTID must be defined with the DEFSCHD or DEFMAN command.
- **LIT**: The LIT command accesses the LIT sublevel of ALT. If a TESTID is not entered as a parameter, a new TESTID must be defined with the DEFSCHD or DEFMAN command.
- **CktTst**: The CKTTST command accesses the CKTTST sublevel of ALT. If a TESTID is not entered as a parameter, a new TESTID must be defined with the DEFSCHD or DEFMAN command.

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

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

MG9000 linecard types of GWLPOTS and GWLEBS are only supported by ALT.

13.2.4.1 ALT Sublevel Commands

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

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

- **DefMAN**: The DEFMAN command is used to assign a TESTID to the test that corresponds to the current ALT sublevel. For example, the DEFMAN command entered at the LIT level of MAP device number 7, will be assigned a TESTID of MANUAL07.
- **DefSCHD_**: The DEFSCHD command is used to assign a TESTID to the scheduled test that corresponds to the current ALT sublevel.
- **Status_**: The STATUS command checks the status of the posted TESTID.
- **OVRride_**: The OVERRIDE command overrides a scheduled test so that testing will not start until a specified day and time has passed.

13.2.5 ShowerQ

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

MG9000 linecard types of GWLPOTS and GWLEBS are supported by the ShowerQ.

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

13.2.6 Subscriber Premise Tests

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

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

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

POTS

- DP or DTMF Digits
- Flash Key or Flash Hook
- RLS Key or Onhook

- Talk Key or Offhook
- Set Ringer

PPhone

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

The result for circuit test are shown by LED displays 1, 2 and 8 turning on. The number of messages is not displayed also. The test can be exited during circuit test by pressing the “Hold” key.

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

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

13.2.6.1 Note on Digit Maps

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

When the user dials a three digit access code to initiate a subscriber premise test, it may not match the standard digits maps used with MG9000 lines. The MG9000 has a 10 second timeout and will report collected digits to the CS2000 even if the dialed digits do not match an applied digit map.

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

13.2.7 Line Diagnostics

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

Table 17: CS2000 Line Diagnostics

Test	CS2000 lines (TDM)	MG9K Lines
Provisioning Data	Note 1	x
Missing Card Test	x	Note 2
Trans Hybrid Loss	x	x
Attenuation Pad	x	x
Weighted and Notch Noise	x	x
Flux Cancellation / Echo Return	x	Note 3
Offhook Detection	x	x
Onhook Detection	x	x
Ringing	x	x
Ground Start	x	x
PPhone Provisioning Audit	x	x
Battery Feed	x	Note 4
Talk Battery	X	Note 4
Cutoff Relay	x	Note 4
Test Access Relay	x	Note 4
Facility Check	x	Note 4

X - denotes tests that are supported

1. H.248 gateways have provisioning that must match the provisioning in the CS2000 to provide service. HOST lines do not have remote provisioning data and the provisioning data test is not required.

2. The MG9000 does not support a missing card tests. MG9000 lines can affect the CS2000 line state. If the linecard is missing or disabled, the CS2000 line state will be set to SB to indicate that the line is in a trouble condition.

3. The MG9000 has echo cancellers for all line types; therefore, a echo return test is not performed at this time.
4. MG9000 line diagnostics do not include facility and linecard relay tests.

13.3 Configuration Requirements

13.3.1 Hardware Requirements

13.3.1.1 CS2000 Hardware

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

13.3.1.1.1 Trunk Modules

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

If test hardware is RMM, the following items should be provided:

- A DS30A card has been inserted into the host peripheral (LTC, LGC,RLCM or RC02) in the appropriate slot
- The host XPM and the RMM are connected via a DS30A cable
- The software for this activity is installed in the XACore
- The required LGC load (if the RMM is connected to an LGC) is installed in the XPM.

13.3.1.1.2 Test Circuits

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

- NT4X45AA EDTU (or NT1x90/NT2x96 TTT, NT2x47/NT2x56 TTU, NT4x23 DTU)
- NT4X97AA/4X98BA/BB MTU
- NT2X90AD MONTALK Circuit
- NT5X30AA 101 Communication Test Line (HSET)
- NT1X54AA Jack Ended Trunk (JACK)
- NT2X90AD INC/OC Test Trunk (Analog Test Trunk Interface)
- NTFX44: ILTA (Improved Loop Test Accessory) is provisionable in ISM shelf and is designed to be used with some external test units.

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

- NT2X57 SD Card

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

13.3.1.1.3 MTA Matrix

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

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

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

- NT3X09BA 8x8 Matrix Card

The trunk modules also contain the MTA matrix cards.

13.3.1.1.4 Horizontal Connectivity

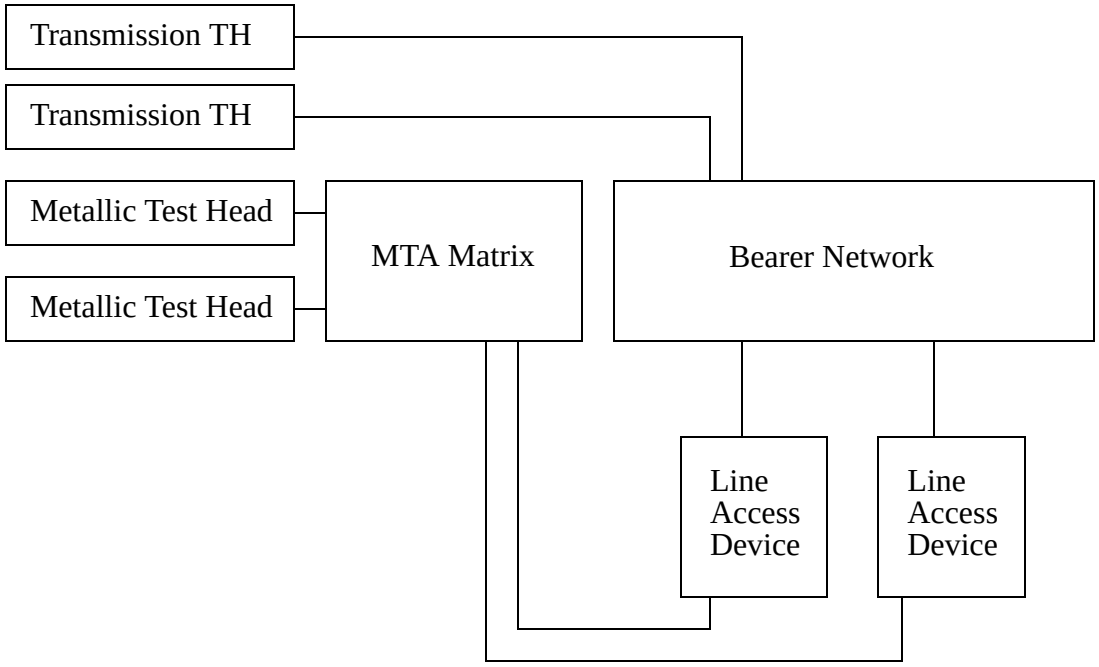
As noted above, the metallic test heads must be wired to the horizontal leads on the MTA matrix.

13.3.1.1.5 Vertical Connectivity

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

13.3.1.1.6 Test Configuration Diagram

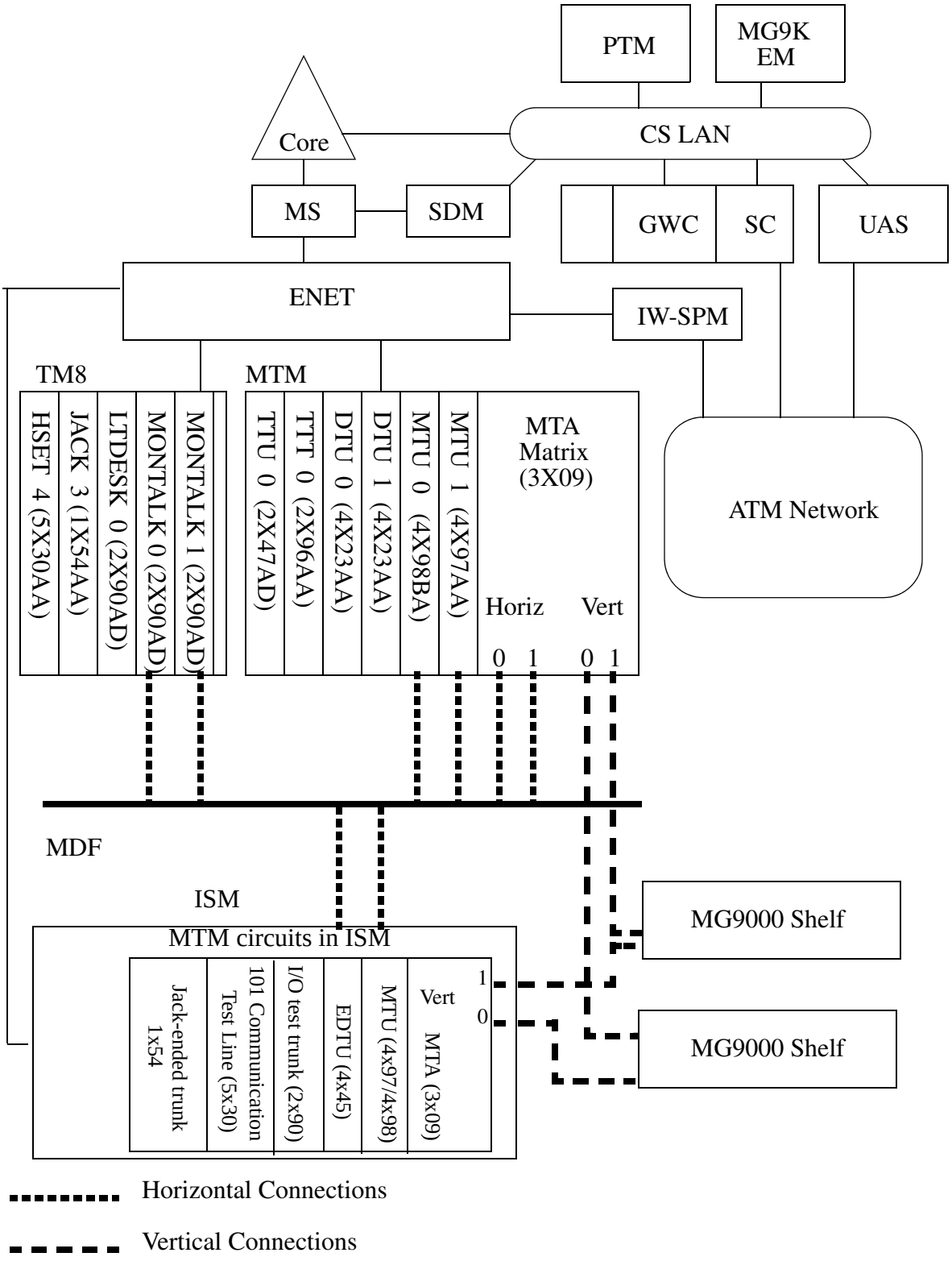
The following diagrams illustrate the hardware configuration required to support CS2000 based line testing for MG9000 lines.



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

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

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


PTM
MG9K EM
Core
CS LAN
MS
SDM
GWC
SC
UAS
ENET
IW-SPM
TM8
MTM
HSET 4 (5X30AA)
JACK 3 (1X54AA)
LTDESK 0 (2X90AD)
MONTALK 0 (2X90AD)
MONTALK 1 (2X90AD)
TTU 0 (2X47AD)
TTT 0 (2X96AA)
DTU 0 (4X23AA)
DTU 1 (4X23AA)
MTU 0 (4X98BA)
MTU 1 (4X97AA)
MTA Matrix (3X09)
Horiz
Vert
0 1 0 1
ATM Network
MDF
ISM
MTM circuits in ISM
Jack-ended trunk 1x54
101 Communication Test Line (5x30)
I/O test trunk (2x90)
EDTU (4x45)
MTU (4x97/4x98)
Vert MTA (3x09)
1
0
MG9000 Shelf
MG9000 Shelf
Horizontal Connections
Vertical Connections

13.3.1.2 MG9000 Hardware

The MG9000 requires the following hardware to support the MG9K line test content provided by activities A00009038 and A00009039:

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

13.3.2 Software Requirements

There are 5 types of equipment/connectivity datafilled required to support the CS2000 line test functionality provided by activity A00009039.

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

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

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

13.3.2.1 Trunk Module Provisioning

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

13.3.2.2 Test Head and Supporting Hardware Provisioning

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

13.3.2.3 MTA Matrix Provisioning

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

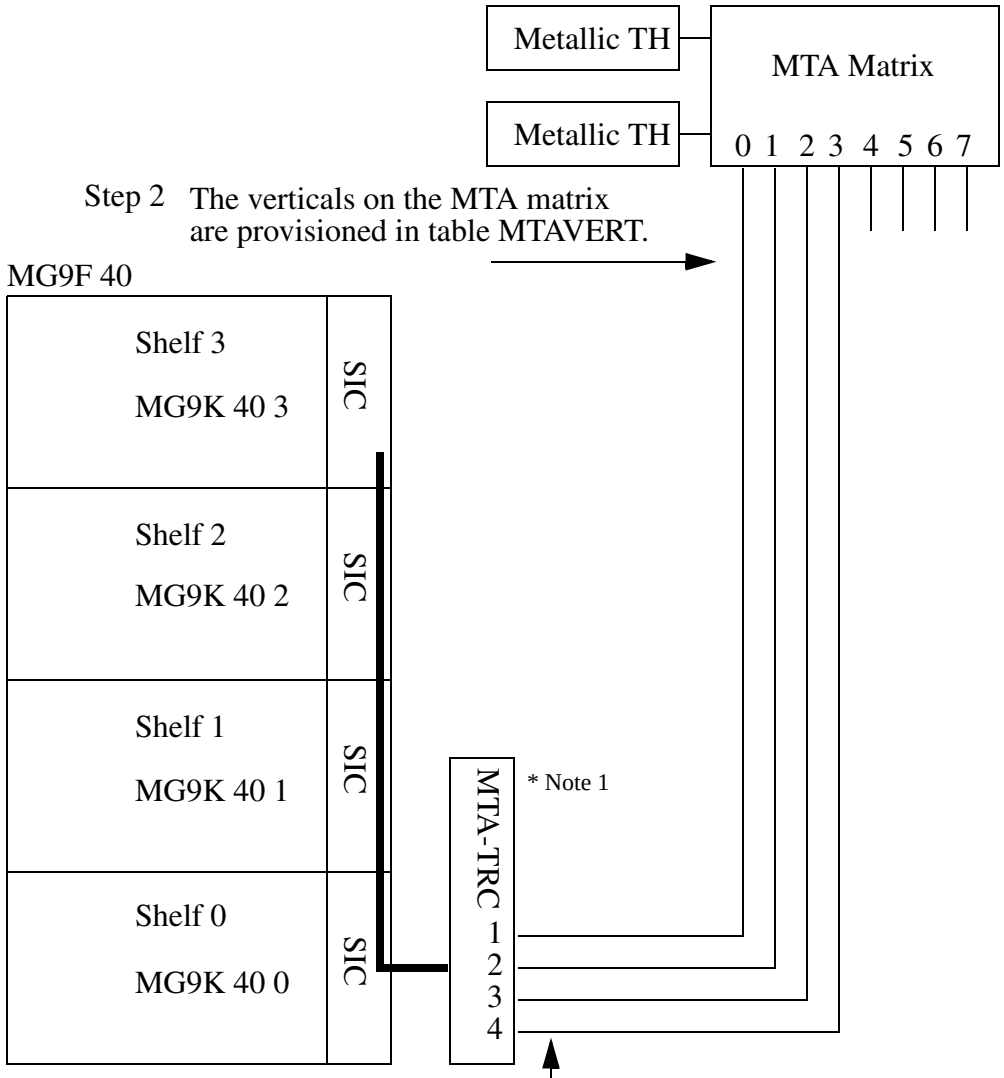
13.3.2.4 Horizontal Connectivity Provisioning

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

13.3.2.5 Vertical Connectivity Provisioning

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

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



*Note 1: In single-shelf MG9Ks, the MTA-TRC card will be located in Slot 9. For multi-self and multi frame MG9Ks, it will be located in a subtended shelf. In frames with master shelves MTA-TRC card will be located in Slot 2 of first subtended shelf. In adjacent frames without master shelves, the MTA-TRC card will be located in slot 2 of shelf 0.

Step1 The metallic test access points on the MG9000 are provisioned in table LGRPINV with a designation of the attached vertical on the MTA matrix.

Table LGRPINV

```
MG9K 40 0  GWC 0  S  MTSTAPT  MG9K  (0  1) $
MG9K 40 1  GWC 0  S  MTSTAPT  MG9K  (1  2) $
MG9K 40 2  GWC 0  S  MTSTAPT  MG9K  (2  3) $
MG9K 40 3  GWC 0  S  MTSTAPT  MG9K  (3  4) $
```

Table MTAVERT

```
0  G  (O  MG9K  40  0) $
1  G  (O  MG9K  40  1) $
2  G  (O  MG9K  40  2) $
3  G  (O  MG9K  40  3) $
```

Vertical Metallic Test Access Point

Provisioning Rules for MG9000 Verticals

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

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

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

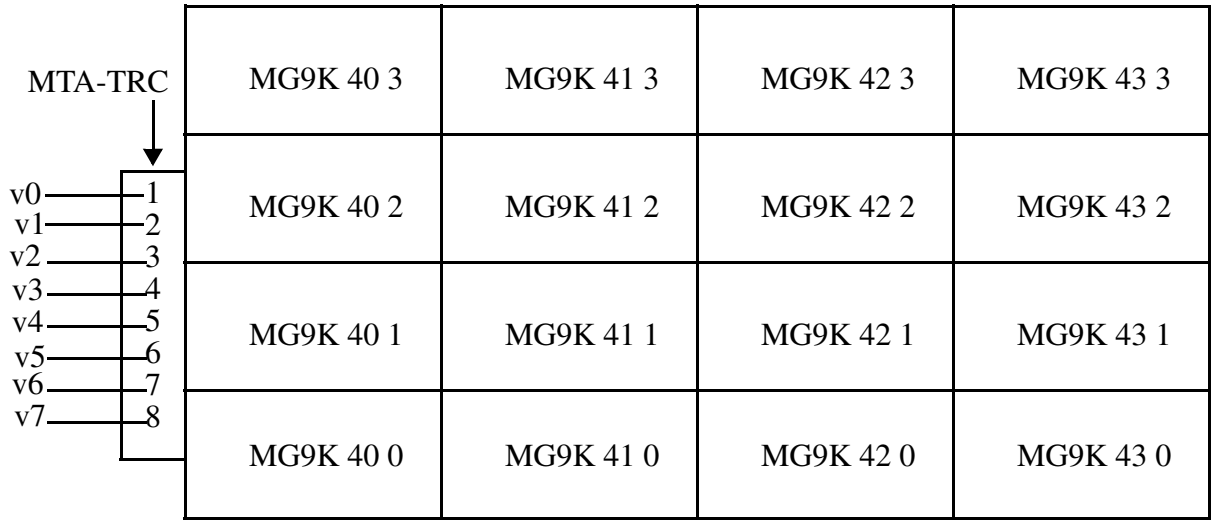
b. As an MG9000 grows beyond 8 shelves, the metallic test access points and verticals used on shelves 0-7 should be reused on shelves 8-15 in sequential fashion.

Example 1: All 8 metallic test access points assigned to verticals.
The following shows example provisioning for table LGRPINV and MTAVERT for a 16 shelf MG9000. In the example given, the MG9000 node is in the MG9K site and it occupies frame 40 41 42 and 43. This example shows all 8 metallic test access points wired to verticals on the MTA matrix.

TABLE: LGRPINV

```
GRPNO SRVRNAME GRPTYPE  LGRPOPTS
------------------------------------------------------------------------
MG9K 40 0  GWC 0  S (MTSTAPT MG9K (0 1) $ ) $
MG9K 40 1  GWC 0  S (MTSTAPT MG9K (1 2) $ ) $
MG9K 40 2  GWC 0  S (MTSTAPT MG9K (2 3) $ ) $
MG9K 40 3  GWC 0  S (MTSTAPT MG9K (3 4) $ ) $
MG9K 41 0  GWC 0  S (MTSTAPT MG9K (4 5) $ ) $
MG9K 41 1  GWC 0  S (MTSTAPT MG9K (5 6) $ ) $
MG9K 41 2  GWC 0  S (MTSTAPT MG9K (6 7) $ ) $
MG9K 41 3  GWC 0  S (MTSTAPT MG9K (7 8) $ ) $
```

```
MG9K 42 0  GWC 1  S (MTSTAPT MG9K (0 1) $ ) $
MG9K 42 1  GWC 1  S (MTSTAPT MG9K (1 2) $ ) $
MG9K 42 2  GWC 1  S (MTSTAPT MG9K (2 3) $ ) $
MG9K  42  3  GWC  1  S (MTSTAPT MG9K (3 4) $ ) $

MG9K 43 0  GWC 1  S (MTSTAPT MG9K (4 5) $ ) $
MG9K 43 1  GWC 1  S (MTSTAPT MG9K (5 6) $ ) $
MG9K 43 2  GWC 1  S (MTSTAPT MG9K (6 7) $ ) $
MG9K  43 3  GWC   1  S (MTSTAPT MG9K (7 8) $ ) $

TABLE: MTAVERT

VERT VERTCONN
------------------------
0  G  ( O MG9K 40 0 ) (O MG9K 42 0) $
1  G  ( O MG9K 40 1 ) (O MG9K 42 1) $
2  G  ( O MG9K 40 2 ) (O MG9K 42 2) $
3  G  ( O MG9K 40 3 ) (O MG9K 42 3) $
4  G  ( O MG9K 41 0 ) (O MG9K 43 0) $
5  G  ( O MG9K 41 1 ) (O MG9K 43 1) $
6  G  ( O MG9K 41 2 ) (O MG9K 43 2) $
7  G  ( O MG9K 41 3 ) (O MG9K 43 3) $
```



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

Example 2: Two metallic test access points reserved for wideband testing
The following shows example provisioning for table LGRPINV and MTAVERT for a 16 shelf MG9000. In the example given, the MG9000 node

is in the MG9K site and it occupies frame 40 41 42 and 43. This example shows only 6 metallic test access points wired to verticals on the MTA matrix.

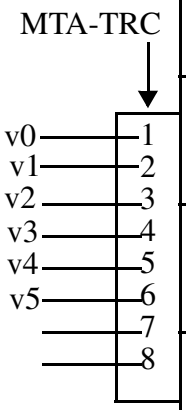
TABLE: LGRPINV

```
GRPNO SRVRNAME GRPTYPE  LGRPOPTS
-------------------------------------------------------------------------
MG9K 40 0  GWC 0  S (MTSTAPT MG9K (0 1) $ ) $
MG9K 40 1  GWC 0  S (MTSTAPT MG9K (1 2) $ ) $
MG9K 40 2  GWC 0  S (MTSTAPT MG9K (2 3) $ ) $
MG9K 40 3  GWC 0  S (MTSTAPT MG9K (3 4) $ ) $
MG9K 41 0  GWC 0  S (MTSTAPT MG9K (4 5) $ ) $
MG9K 41 1  GWC 0  S (MTSTAPT MG9K (5 6) $ ) $
MG9K 41 2  GWC 0  S (MTSTAPT MG9K (0 1) $ ) $
MG9K 41 3  GWC 0  S (MTSTAPT MG9K (1 2) $ ) $
MG9K 42 0  GWC 1  S (MTSTAPT MG9K (2 3) $ ) $
MG9K 42 1  GWC 1  S (MTSTAPT MG9K (3 4) $ ) $
MG9K 42 2  GWC 1  S (MTSTAPT MG9K (4 5) $ ) $
MG9K 42 3  GWC 1  S (MTSTAPT MG9K (5 6) $ ) $
MG9K 43 0  GWC 1  S (MTSTAPT MG9K (0 1) $ ) $
MG9K 43 1  GWC 1  S (MTSTAPT MG9K (1 2) $ ) $
MG9K 43 2  GWC 1  S (MTSTAPT MG9K (2 3) $ ) $
MG9K 43 3  GWC 1  S (MTSTAPT MG9K (3 4) $ ) $
```

TABLE: MTAVERT

```
VERT VERTCONN
-----------------------
0  G  ( O MG9K 40 0 ) (O MG9K 41 2) (O MG9K 43 0)$
1  G  ( O MG9K 40 1 ) (O MG9K 41 3) (O MG9K 43 1)$
2  G  ( O MG9K 40 2 ) (O MG9K 42 0) (O MG9K 43 2)$
3  G  ( O MG9K 40 3 ) (O MG9K 42 1) (O MG9K 43 3)$
4  G  ( O MG9K 41 0 ) (O MG9K 42 2) $
5  G  ( O MG9K 41 1 ) (O MG9K 42 3) $
```

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



MG9K 40 3	MG9K 41 3	MG9K 42 3	MG9K 43 3
MG9K 40 2	MG9K 41 2	MG9K 42 2	MG9K 43 2
MG9K 40 1	MG9K 41 1	MG9K 42 1	MG9K 43 1
MG9K 40 0	MG9K 41 0	MG9K 42 0	MG9K 43 0

13.3.2.6 Provisioning Example

13.3.2.6.1 Trunk Module Provisioning

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

Note: all tables are shown in packeted format.

TABLE: TMINV

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

TM8 0 TME 0 18 1 D 28 0 32 0 0 2X52AG BTMKA02 TM8EX SHELF
MTM 0 TME 0 52 1 D 28 0 32 5 0 2X58CB MTMKA02 MTMEX SHELF
MTM 0 **CISM** 0 5 0 B 3 0 11 2 0 **FX42AA** MTMKA02 MTMEX SHELF

13.3.2.6.2 Test Head and Supporting Hardware Provisioning

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

- NT4X45AA EDTU (or NT1x90/NT2x96 TTT, NT2x47/NT2x56 TTU, NT4x23 DTU)

- NT4X97/NT4X98 MTU
- NT2X90AD MONTALK Circuit
- NT5X30AA 101 Communication Test Line (HSET)
- NT1X54AA Jack Ended Trunk (JACK)
- NT2X90AD INC/OC Test Trunk (Analog Test Trunk Interface)

TABLE: TRKGRP

GRPKEY GRPTYP TRAFSNO PADGRP NCCLS GRPINFO

TTU MAINT 0 NPDGP NCRT 2X47BA
TTT MAINT 0 NPDGP NCIT 2X96BA
DTU MAINT 0 NPDGP NCRT 4X23AA
MTU MAINT 0 NPDGP NCRT 4X97AA
MONTALK MAINT 0 NPDGP NCRT 2X90AD
HSET MAINT 0 NPDGP NCRT 5X30AA
JACK MAINT 0 NPDGP NCRT 1X54AA
LTDESK TD 0 NPDGP NCOT NIL MIDL IC NPRT NSCR 613 613 LCL N N BASIC N

TABLE: TRKMEM

CLLI EXTRKNM SGRP MEMVAR

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

13.3.2.6.3 MTA Matrix Provisioning

After the test heads and supporting circuits are provisioned, the MTA (Metallic Test Access) matrix is provisioned for the CS2000. The MTA matrix is provisioned through table MTAMDRVE. This example shows an MTA matrix with a single MTA matrix card. The CS2000 supports an MTA matrix that is significantly larger. The MTA matrix for a CS2000 is created by linking together multiple MTA cards in both the vertical and horizontal directions.

TABLE: MTAMDRVE

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

13.3.2.6.4 Horizontal Connectivity Provisioning

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

TABLE: MTAHORIZ

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

13.3.2.6.5 Vertical Connectivity Provisioning

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

The following example shows two separate LGRPs. For MG9K 77 1, the entry in LGRPINV associates vertical 0 with metallic test access point 1 on the gateway. For MG9K 40 2, the entry in LGRPINV associates vertical 1 with metallic test access point 1 on the gateway.

TABLE: LGRPINV

```
GRPNO SRVRNAME GRPTYPE  LGRPOPTS
-------------------------------------------------------------------------
MG9K  77 1  GWC   5   S (MTSTAPT MG9K ( 0 1) $)$
MG9K   40 2   GWC    5   S  (MTSTAPT MG9K ( 1 1) $)$
```

TABLE: MTAVERT

```
VERT VERTCONN
-------------
0 G (O MG9K 77 1 ) $
1 G (O  MG9K  40 2 ) $
```

13.4 Line States

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

13.4.1 CS2000 Line States

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

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

– a LTP operator has entered an instruction

During this state tests can be conducted.

- LMB (Line module busy)
  - — Call processing cannot take place because the LGRP that represent the MG9000 shelf for the posted line is out of service.
- LO (Lock-out)
  - — The line has been removed from service by the CS2000, preventing call processing. Manual action is required to change the state.
- MB (Maintenance busy)
  - — The line has been removed from service by maintenance personnel or by the CS2000. Call processing cannot take place.
- NEQ (Not equipped)
  - — The LEN has not been datafilled. Call processing cannot take place.
- PLO (PSPD lock-out)
  - — This is a particular variety of the state LO. The line has been removed from service by the CS2000 because of a PSPD condition. Call processing cannot take place until the condition no longer exists and the CS2000 restores the line state to IDL.
- SB
  - — The line has been removed from service by the CS2000. There are a range of error conditions that can cause an MG9000 line to be set to the SB state in the CS2000. If the CS2000 can set the line to the SB state if it detects an error condition for the line. The CS2000 can also set the line to the SB state if it receive an indication from the GWC that the line is not capable of providing service. This could represent a data error in the GWC or MG9000, or it could represent a fault condition for the line at the MG9000 such as an overcurrent protection condition. For lines in the SB state, the craftsperson should check the state of the circuit at the MG9000 EM.
- *SZ*
  - — *Future line state*
  - — *Not used for MG9000 lines.*

13.4.2 MG9000 Line States

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

13.4.2.1 Line Circuit

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

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

13.4.2.2 H.248 Line Termination

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

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

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

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

- Operational Status
  - The operational status shows the current service state of the H.248 line termination. The values can be enabled, disabled and test.
    - Enabled indicates that the H.248 line termination is in the working state and providing service.
    - Disabled indicates that the H.248 line termination is not in the working state and is not providing service.
    - Test indicates that the line is currently under test.
- Termination Test Status
  - For terminations that are under test, the termination test status provides additional information. The value can be Not Testing, Testing via Call Server, Testing via EM.
    - Not Testing indicates that the line is not currently under test.
    - Testing via Call Server indicates that the line is currently under test from the Call Server.
    - Testing via EM indicates that the line is currently under test from the MG9000 Element Manger.

13.5 Line Options Support

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

- No Double Connect (NDC)

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

- No Hazard Test (NHT)

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

- No Line Insulation Test (NLT)

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

13.6 Diagnostic Users Guide

13.6.1 Diagnostic Results

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

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

13.6.1.1 Line Log

The MG9000 line diagnostic uses the following existing logs:

The LINE100 log indicates a line diagnostic has passed.

```
RTP206BH ***+LINE100 MAR21 08:06:49 3600 PASS LN_DIAG
        MG9K 05 0 02 21    DN 6195200000
        DIAGNOSTIC RESULT   Card Diagnostic OK
        ACTION REQUIRED  None
        CARD TYPE  GWLPOTS
```

The LINE101 indicates that a line diagnostic has failed.

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    MG9K 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test failed:  Single-party ringing
    ACTION REQUIRED    Replace card
    CARD TYPE   GWLPOTS
```

13.6.1.2 Alarm Flags

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

- D - Long diagnostic has failed
- S - Short diagnostic has failed

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

13.6.2 Line State Supported for the Line Diagnostics

13.6.2.1 For LTP Diags

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

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

13.6.2.2 ALT SDIAG

ALT SDIAG will test lines in the following states:

- INB
- MB
- IDL

13.6.2.3 ShowerQ

The ShowerQ tests lines in the following states:

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

13.6.3 Diagnostic Results

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

13.6.3.1 Diagnostic Passed

Display / Log

RTP206BH ***+LINE100 MAR21 08:06:49 3600 PASS LN_DIAG
MG9K 05 0 02 21 DN 6195200000
DIAGNOSTIC RESULT Card Diagnostic OK
ACTION REQUIRED None
CARD TYPE GWLPOTS

Description

- The line tested is functioning correctly.

Alarm

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

Users Action

- No user action is required.

13.6.3.2 CS2000 Software Errors

Display / Log

RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL LN_DIAG
MG9K 05 0 02 21 DN 6195200000
DIAGNOSTIC RESULT Call server software error
ACTION REQUIRED Check Logs
CARD TYPE GWLEBS

Description

- A CS2000 software error has occurred.

Alarm

- The line failure flag is not affected.

Users Action

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

13.6.3.3 GWC Processing Errors

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    MG9K 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   GWC processing error
    ACTION REQUIRED   Chk GWC logs
    CARD TYPE   GWLPOTS
```

Description

- A gateway controller software error has occurred.

Alarm

- The line failure flag is not affected.

Users Action

- Capture the GWC logs and try the test again.

13.6.3.4 GWC Provisioning Faults Detected

13.6.3.4.1 Missing Node Data

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    MG9K 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Node data missing in GWC
    ACTION REQUIRED   Chk GWC data
    CARD TYPE   GWLPOTS
```

Description

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

Alarm

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

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

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

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

Users Action

- Check the node provisioning data for the GWC.

13.6.3.4.2 Missing Line Data

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    MG9K 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Line data missing in GWC
    ACTION REQUIRED   Chk GWC data
    CARD TYPE   GWLPOTS
```

Description

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

Alarm

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

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

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

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

Users Action

- Check the line provisioning data in the GWC.

13.6.3.5 Node State Faults Detected in the GWC

Display / Log

RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL LN_DIAG
MG9K 05 0 02 21 DN 6195200000
DIAGNOSTIC RESULT Gateway is out of service in GWC
ACTION REQUIRED Chk GW state
CARD TYPE GWLPOTS

Description.

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

Alarm

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

Users Action

- The user should check the line state in the CS2000. If the line state is not LMB and this diagnostic error persists, the user should attempt to correct the MG9000 shelf state mismatch between the CS2000 and the Gateway Controller.

13.6.3.6 Line Termination is Out of Service in the GWC

Display / Log

RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL LN_DIAG
MG9K 05 0 02 21 DN 6195200000
DIAGNOSTIC RESULT Line out of service in GWC
ACTION REQUIRED Chk ln state
CARD TYPE GWLPOTS

Description

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

Alarm

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

Users Action

- The user should check the state of the line circuit at the MG9000 element manager to ensure that the line circuit is in the enabled state.

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

13.6.3.7 Gateway Controller to Gateway Messaging Error

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    MG9K 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   No response from gateway
    ACTION REQUIRED   Try again
    CARD TYPE   GWLPOTS
```

Description

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

Alarm

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

Users Action

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

13.6.3.8 Gateway Processing Error

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    MG9K 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Gateway processing error
    ACTION REQUIRED   Chk GW logs
    CARD TYPE   GWLPOTS
```

Description

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

Alarm

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

Users Action

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

13.6.3.9 Gateway Test Resources Unavailable

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    MG9K 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test resources unavailable at gateway
    ACTION REQUIRED   Chk Gateway
    CARD TYPE   GWLPOTS
```

Description

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

Alarm

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

Users Action

- The user should check the state of the line test hardware at the gateway. For the MG9000, the users should check the state of the MTA-TRC pack and the SIC cards. Those cards provide the line test functions within the MG9000.

13.6.3.10 Gateway Test Resource Busy

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    MG9K 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test resources busy at gateway
    ACTION REQUIRED   Try Again
    CARD TYPE   GWLPOTS
```

Description

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

Alarm

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

Users Action

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

13.6.3.11 Line Provisioning Mismatch in the Gateway

Display / Log

RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL LN_DIAG
MG9K 05 0 02 21 DN 6195200000
DIAGNOSTIC RESULT Line data mismatch in gateway
ACTION REQUIRED Chk GW data
CARD TYPE GWLPOTS

Description

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

Alarm

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

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

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

Users Action

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

13.6.3.12 Line Provisioning Missing in the Gateway

Display / Log

RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL LN_DIAG
MG9K 05 0 02 21 DN 6195200000
DIAGNOSTIC RESULT Line data missing in gateway
ACTION REQUIRED Chk GW data
CARD TYPE GWLPOTS

Description

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

Alarm

- The line failure flag for the line is set to D to indicate that the linecard diagnostic has failed. Lines marked with the D failure flag have been

identified by the CS2000 as lines that are not capable of providing service and required user maintenance.

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

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

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

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

Users Action

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

13.6.3.13 Line Card Diagnostic Failures

13.6.3.13.1 Offhook Detection Failure

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    MG9K 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test failed:  Off-hook
    ACTION REQUIRED    Replace card
    CARD TYPE   GWLPOTS
```

Description

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

Alarm

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

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

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

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

Users Action

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

13.6.3.13.2 Onhook Detection Failure

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    MG9K 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test failed:  On-hook
    ACTION REQUIRED    Replace card
    CARD TYPE   GWLPOTS
```

Description

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

Alarm

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

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

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

Users Action

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

13.6.3.13.3 Single Party Ringing Failure

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    MG9K 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Test failed:  Single-party ringing
    ACTION REQUIRED    Replace card
    CARD TYPE   GWLPOTS
```

Description

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

Alarm

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

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

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

Users Action

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

13.6.3.13.4 Transhybrid Loss Failure

Display / Log

```
RTPU07BC ***+LINE101 OCT26 09:40:48 6900 FAIL LN_DIAG
    MG9K 05 0 02 21    DN 2145201001
    DIAGNOSTIC RESULT  -11.6-10.7  0.6  1.4 THL Test
    ACTION REQUIRED  Replace Card
    CARD TYPE  GWLPOTS
```

Description

- The transhybrid loss test passes a series of tones through a linecard in both directions to verify that the linecard will encode and decode speech correctly for voice frequencies. This test also verifies the hybrid circuit in the linecard is not defective. The transhybrid loss tests uses the following frequencies: 304, 704, 1504 and 4305 Hz. The above display/log indicates that the transhybrid loss test has failed. The measured transhybrid loss at each test frequency is displayed in the diagnostic failure log.
- The transhybrid loss test will fail if too much loss or gain is detected when the tones are passed through the line under test. Different linecard have different transmission characteristics. The following shows the ranges that are considered a test pass for the MG9000 linecards.

POTS-32 and 8x8 DSL

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

SAA-12

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

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

Alarm

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

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

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

User Action

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

User Notes

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

13.6.3.13.5 Continuity Failure

Display / Log

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAIL  LN_DIAG
    MG9K 05 0 02 21              DN   6195200000
    DIAGNOSTIC RESULT   Bearer continuity not detected
    ACTION REQUIRED   Try Again
    CARD TYPE   GWLPOTS
```

Description

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

Alarm

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

Users Action

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

13.6.3.13.6 Weighted or Notched Noise Failure

Display / Log

```
RTPU07BC ***+LINE101 OCT26 09:50:13 6200 FAIL LN_DIAG
      MG9K 00 0 00 14    DN 2145201001
      DIAGNOSTIC RESULT  Noise Level 44.1DB Notch Noise
      ACTION REQUIRED  Replace Card
      CARD TYPE  GWLPOTS

RTPU07BC ***+LINE101 OCT26 09:53:55 7100 FAIL LN_DIAG
      MG9K 00 0 00 14    DN 2145201001
      DIAGNOSTIC RESULT  Noise Level  36.5DB Weight Noise
```

ACTION REQUIRED Replace Card
CARD TYPE GWLPOTS

Description

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

  Notched Noise must be less than 42.0 dB

  Weighted Noise must be less than 30.0 dB

Alarm

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

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

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

User Action

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

13.6.3.13.7 Linecard Pads Failure

Display / Log

RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
MG9K 00 0 00 14 DN 2145201001
DIAGNOSTIC RESULT -.7 -2.2 -.4 -.4 Pad 1DB Test
ACTION REQUIRED Replace Card
CARD TYPE GWLPOTS

Description

- Indicates that linecard pad test failed. The CS2000 supports per call gain control, referred to as padding. This linecard pad test will verify that the CS2000 can adjust the pads in an MG9000 linecard. The linecard pad test measures the gain applied by a linecard when a 1, 3, 5, and 7 dB pad are applied to the line under test. The linecard pad test verifies that the correct gain in applied at 304, 704, 1504 and 4305 Hz.

- The example log given shows a diagnostic that failed the 1dB pad test. The diagnostic will allow a 1 dB variance from the requested gain. In the example given, the 704 Hz frequency had a loss of -2.2 dB when a -1.0 dB pad was requested.

Alarm

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

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

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

User Action

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

13.6.3.13.8 Linecard Messaging Failure

Display / Log

```
RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
     MG9K 00 0 00 14    DN 2145201001
     DIAGNOSTIC RESULT  No Signalling to Card 5/10
     ACTION REQUIRED  Replace Card
     CARD TYPE  GWLEBS
```

Description

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

Alarm

- The line failure flag for the line is set to L to indicate that the linecard diagnostic has failed the OPCODE signaling test to the linecard itself.

Lines marked with the L failure flag have been identified by the CS2000 as lines that are not capable of providing service and required user maintenance.

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

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

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

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

User Action

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

13.6.3.13.9 Mainset Messaging Failure

Display / Log

```
RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
    MG9K 00 0 00 14    DN 2145201001
    DIAGNOSTIC RESULT  No Signalling to Set 5/10
    ACTION REQUIRED  Chk Card&Set
    CARD TYPE  GWLEBS
```

Description

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

Alarm

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

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

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

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

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

User Action

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

13.6.3.13.10 Addon / Extension Provisioning Mismatch

Display / Log

```
RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
     MG9K 00 0 00 14    DN 2145201001
     DIAGNOSTIC RESULT  Ext. Not Responding
     ACTION REQUIRED   Sustate
     CARD TYPE  GWLEBS

RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
     MG9K 00 0 00 14    DN 2145201001
     DIAGNOSTIC RESULT  Addon Not Responding
     ACTION REQUIRED   Sustate
     CARD TYPE  GWLEBS

RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
     MG9K 00 0 00 14    DN 2145201001
     DIAGNOSTIC RESULT  Ext. Not Datafilled
     ACTION REQUIRED   Sustate
     CARD TYPE  GWLEBS

RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG
     MG9K 00 0 00 14    DN 2145201001
     DIAGNOSTIC RESULT  Addon Not Datafilled
     ACTION REQUIRED   Sustate
     CARD TYPE  GWLEBS
```

Description

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

Alarm

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

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

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

User Action

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

13.6.4 Multicircuit Linecards

13.6.4.1 Managing Faulty Circuits

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

The diagnostic failure flag can be cleared by replacing the linecard and reexecuting the diagnostic. When the diagnostic passes, the CS2000 will

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

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

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

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

13.7 Routine Maintenance

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

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

This section provides some specific recommendations for MG9000 lines.

13.7.1 Subscriber Service

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

13.7.2 Facility Tests

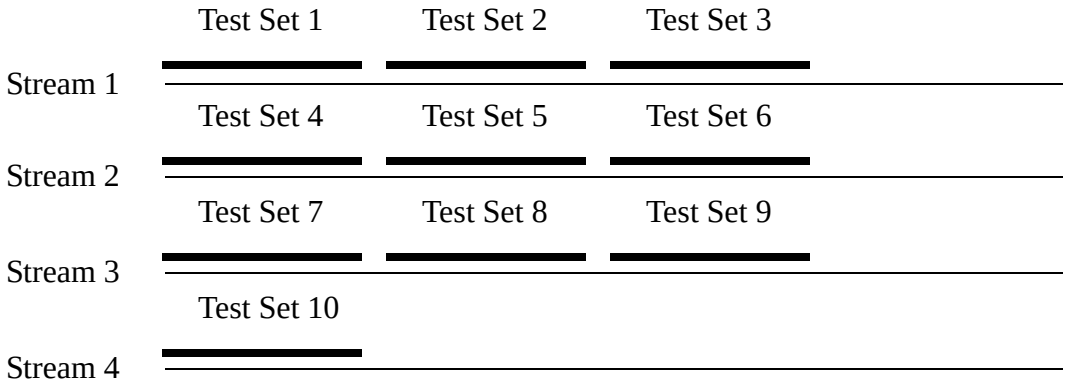
ALT LIT or a loop testing system should be scheduled to routinely test subscriber loops.

13.7.3 ALT Provisioning Recommendations for MG9000 Lines

13.7.3.0.1 MG90000 Tests Sets

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

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



ALT SDIAG

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

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

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

The following example illustrates the issue:

- A craftsperson requests ALT to perform diagnostics for all the MG9000 lines in a single frame.
- Each MG9000 shelf is represented in the core as an LGRP. As stated above, each node in the CS2000 is assigned to a unique test set. Therefore, each MG9000 shelf will be assigned to a unique test set.
- As the linecard diagnostic only requires a TTU in the CS2000, ALT will attempt to create 4 test streams, one for each test set, and assign a TTU to each stream.
- ALT will then assign each test set, one for each shelf, to the 4 test streams.
- Once the test sets are assigned to test streams, ALT will begin processing the ALT test streams in parallel. This will create a scenario where ALT is attempting linecard diagnostic on all 4 shelves in a MG9000 frame concurrently. As the MG9000 can only support 2 simultaneous linecard diagnostics, there will be resources contention in the MG9000. Two of the ALT test streams will execute correctly, and two of the ALT test streams will fail due to unavailable resources at the MG9000.

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

ALT LIT

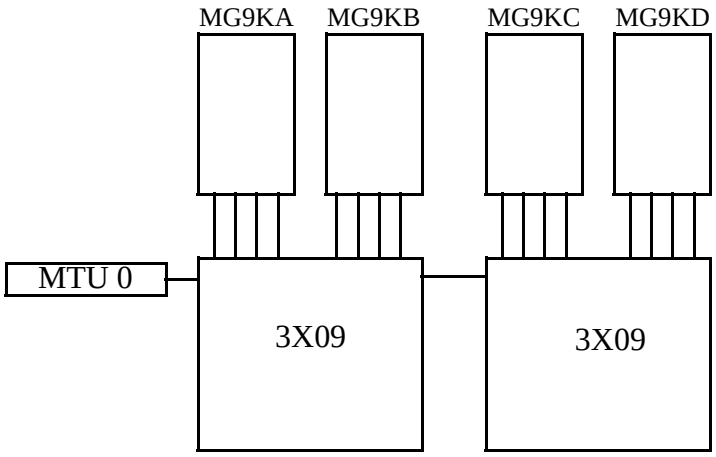
ALT LIT requires an MTU to test the subscriber’s loop. ALT uses the “dedicated” MTUs in the switch. There are two test configuration options which are supported for MG9000 lines. If the customer uses the WTA (Wideband Test Access) panel, there will be a single dedicated MTU for a pair of 3X09s. If the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

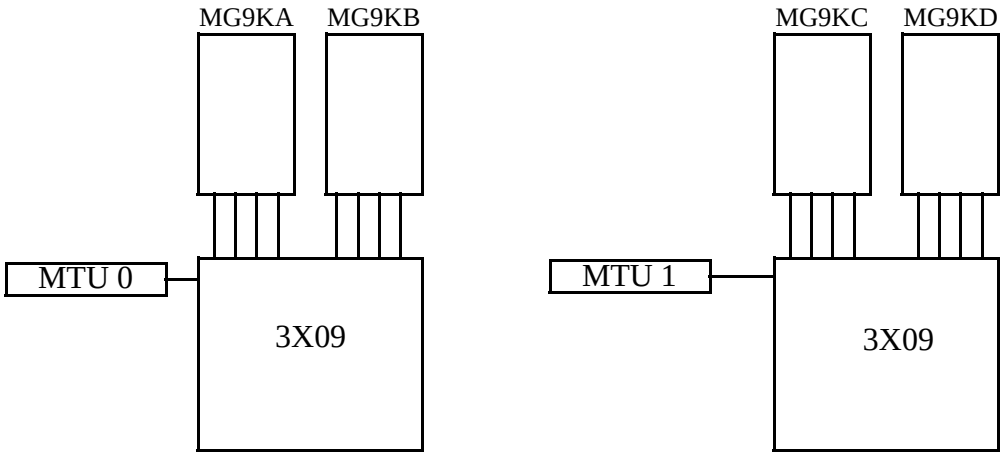
As documented in the engineering rules, a MG9000 node should not span across multiple 3X09 circuit packs. Therefore, in either configuration shown, a given MG9000 can only use one possible dedicated MTU for performing ALT LIT tests.

When ALT LIT creates its test streams, it will create a test stream for each MTU in the switch that has the ALT option set to Y. As ALT LIT is assigning

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

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





ALT CKTTST

ALT CKTTST performs messaging to the MG9000 to check the ability to loopback PPhone messages at the linecard or phone set. For the MG9000, each shelf is represented as a node in the core. Each MG9000 LGRP will be considered a single test set. There is no test equipment required to perform a CKTTST, therefore, ALT can create a unique test stream for each test set up to the maximum number of ALT test streams allowed.

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

13.8 Trouble Shooting

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

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

This section provides some specific recommendations for MG9000 lines.

13.8.1 No Dial Tone

- Determine if the problem is outside plant. Use a loop testing system such as Access Care to perform a detailed loop test.

- If the fault is outside plant, dispatch outside plant personnel.
- If the fault is not outside plant, post the line at the CS2000 and check the CS2000 line state.
- If the line is an manually busy state, stop trouble shooting.
- If the line is in the SB state, that can indicated that the CS2000 has taken the line to the SB state, or it could indicated that the Gateway has taken the line to the SB state.
  - The user can attempt to BSY and RTS the line. If the line returns to the IDL state, verify that dial tone is restored.
  - If the line remains SB, check the line at the MG9000 EM. Check the line circuit for faults. The line circuit must be in the enabled state before the CS2000 line state will return to IDL. If there is a circuit fault at the MG9000, resolve the MG9000 circuit fault. Once resolved and the line circuit is restored to the enabled state, verify that the line has returned to the IDL state in the CS2000. Verify that dial tone is restored.
- If the CS2000 line state is IDL and there is not dial tone, execute the DIAG command on the line. The DIAG command will verify the line provisioning date in the CS2000, GWC and the MG9000. Once the provisioning data is verified, the DIAG will request the MG9000 to execute the embedded circuit diagnostics. This will execute the following tests:
  - Offhook detection
  - Onhook detection
  - Ringing
  - For PPhone lines, OPCODE signaling is verified instead of analog signaling.
- If the line diagnostic fails, resolve the issue reported in the diagnostic.
- If the line diagnostic passes check for dial tone at T/R pair coming off the face place on the linecard. If dial tone does not exist and the line diagnostic passes for the line, escalate to the next level of support. The TALKLTA and ORIG commands can be used to remotely pull dial tone from the T/R of the linecard.

13.8.2 Poor Speech Quality

- Determine if the problem is outside plant. Use a loop testing system such as Access Care to perform a detailed loop test.
- If the fault is outside plant, dispatch outside plant personnel.
- Post the line at the CS2000 MAP position and execute the DIAG command. This will verify the transmission characteristics of the line.

- If the DIAG fails, move the subscriber to a different circuit.
- If the DIAG passes, the TONGEN, LOSS and NOISE commands can be used to perform manual transmission tests on the subscribers linecard and loop.
- If the problem can not be isolated, escalate to the next level of support.

13.8.3 Line Does Not Ring

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

- If the line diagnostic passes check for ringing voltage at T/R pair coming off the face place on the linecard. If ringing voltage does not exist and the line diagnostic passes for the line, escalate to the next level of support.

13.8.4 Call Not Completed Correctly

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

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

13.8.5 PPhone Lines Not Functioning Correctly

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

— Onhook detection (analog lines)

— Ringing (analog lines)

— OPCODE signaling (for PPhone lines)

— Transhybrid Loss (for analog lines)

— Weighed and Notched Noise (for analog lines)

— Padding (for analog lines)

The line diagnostic on a PPhone line will verify the provisioning in the CS2000 matches the set hardware, and it will verify the signaling between the CS2000, the linecard and the PPhone set.

- The Station Ringer test can be executed on site to verify the PPhone set itself.
- If the issue can not be isolated, escalate to the next level of support.

13.9 Logs

13.9.1 Existing Logs Applicable to CS2000 Line Test

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

13.9.2 Modified Logs

13.9.2.1 ALT SDIAG

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

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

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

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

13.10 OMs

13.10.1 Line Troubles

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

13.10.2 Equipment Troubles

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

13.11 Alarms

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

13.11.1 ALMSTAT QUERY

The following shows sample output of an almstat query.

```
                OFFICE LINE FAILURE TOTALS

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

              OFFICE LINE TOTALS
```

```
Number of working lines (total)    in this office is : 1400
Number of working DTMF lines       in this office is : 960
Number of working dial pulse lines in this office is : 3
Number of working EBSs (total)     in this office is : 327
Number of working PSET terminals   in this office is : 1
Number of working M5312 terminals  in this office is : 193
Number of working M5212 terminals  in this office is : 1
Number of working M5316 terminals  in this office is : 132
Number of working Data Units       in this office is : 0
Number of working ISDN loops       in this office is : 110
Number of working BCLID Data Links in this office is : 0

             OFFICE DIAL TONE DELAY (DTSR) INFORMATION

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

Dial Tone Delay Counts And Percentages

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

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

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

13.11.2 ALMSTAT SET

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

13.12 User Error Responses

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

13.12.1 Line State Errors

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

Failed to determine the termination state

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

Failed to put the termination in the test state

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

The line is an ESA call

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

The line is out of service at the gateway

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

13.12.2 Line Test Provisioning Errors

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

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

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

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

Vertical is not datafilled in MTAVERT
Test cannot be performed

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

13.13 Tools

13.13.1 NFF

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

```
No Fault Diagnostic (NFF) utility.

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

Valid commands are:

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

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

13.13.1.1 NFF Results for an MG9000 line

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

```
>mapci nodisp;mtc;lns;ltp;post l ud17 5 3 2 0
MAPCI:
MTC:
LNS:
LTP:
>nff start sfdev diag1
>diag
RTD ***+LINE100 OCT30 08:52:43 1200 PASS LN_DIAG
        UD17 05 3 02 00    DN 6136211701
        DIAGNOSTIC RESULT  Card Diagnostic OK
        ACTION REQUIRED  None
        CARD TYPE  GWLPOTS
>nff stop
NFF stopped
>nff print
No fault found diagnostic result
-
```

```
Diagnostic intermediate result for LEN: UD17 05 3 02 00 on
   OCT-30 08:52:33
Transhybrid loss test result:
                 304    704   1504   3204    Hz
     Max          10     15     15     10    db*10
     Actual      -22    -16    -15    -18    db*10
     Min         -50    -45    -45    -50    db*10
-
Test pads in line card result:
                 304    704   1504   3204    Hz
     1 db pad:   -10    -10    -10    -10    db*10
     3 db pad:   -30    -30    -30    -30    db*10
     7 db pad:   -70    -70    -70    -70    db*10
     0 db pad:     0      0      0      0    db*10
-
     Noise test result:  56   db*10 noise level
-
     Noise test result:  282   db*10 noise level
```

13.13.2 LGLTT

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

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

13.14 Restart Behavior

All CS2000 line test activities are terminated by element restarts.

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

action at the CORE, the line test will remain in the test state until that action is complete.

- After a Gateway restart, any line test in progress is aborted and a failure message is displayed at the MAP.

13.15 Limitations and restrictions

- The CS2000 line test functionality is only supported for MG9000 lines.
- The CS2000 line test functionality is only supported for MG9000 lines when using the following cardcodes: GWLPOT and GWLEBS.

13.16 Interactions

Not applicable.

13.17 Applicable customer facing sections

Fault Management

Logs	__N/A_
Alarms	__N/A_

Configuration

Data Schema	__N/A_
User Interface	__X__
Element Management	__N/A_
Security	__N/A_
Service Order	__N/A_
Office Parameters	__N/A_

Accounting (includes AMA billing)	__N/A_
Performance (includes operational measurements)	__N/A_

13.18 References

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

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

NTP 50041.08 DMS-100/200 Hardware Planning Guide

A00009038 - MG9K Line Test Support Framework

A00001888 - MAP Based Line Tests for MG9000 (CNA)

DCSLNMTC, PLS FMDOC, “DMS Call Server Line Mtce”.

AF7815, PLS DOC, “ICB LINE MAINTENANCE”.

AN1722, PLS DOC, “SCEPTER: MTA AND ISDN DECOUPLING”.

13.19 Glossary

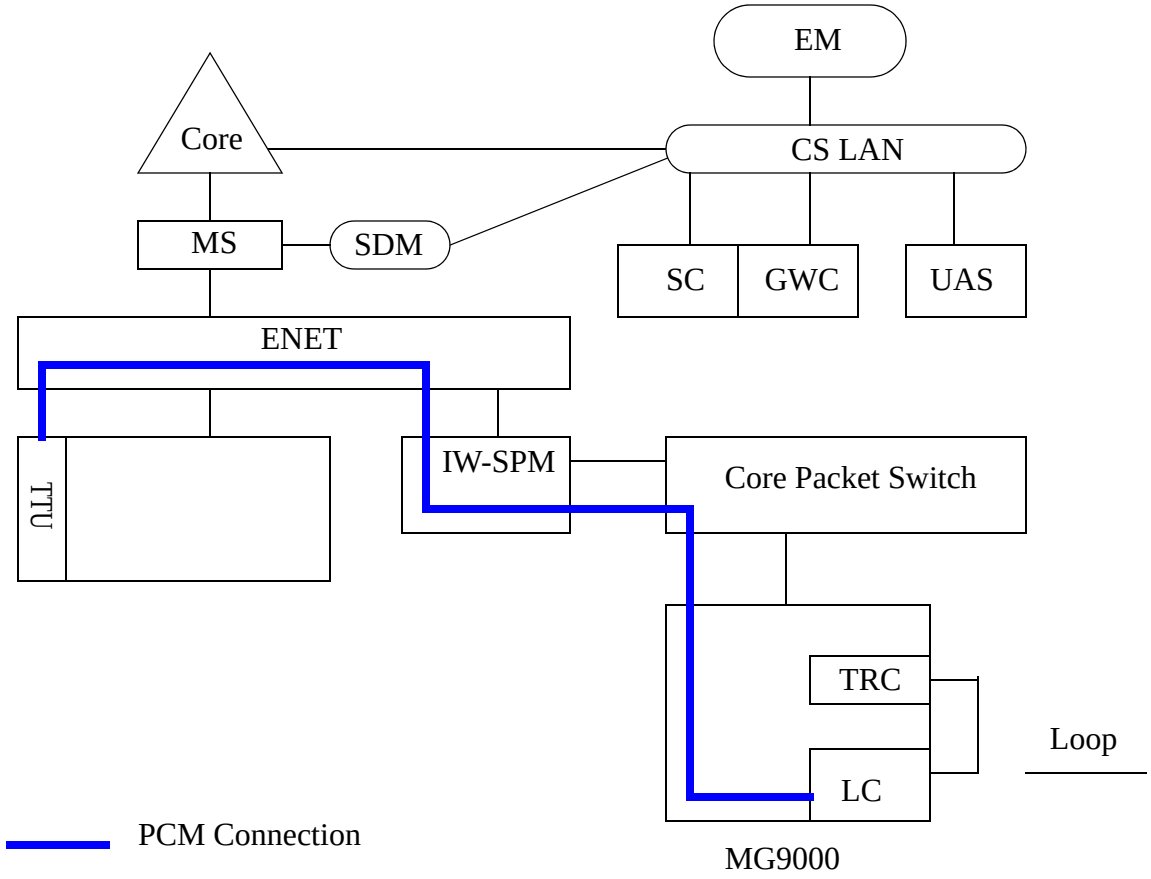
Term	Description
ABI	Access Bridge Interface
ALT	Automatic Line Test
EBS	Electronic Business Set
EDTU	Enhanced Digital Test Unit
LNSTRBL	Lines Service Trouble
LTP	Lines Test Position
LTU	Line Test Unit
MAP	Maintenance and Administration Position
MBS	Meridian Business Set
MTM	Maintenance Trunk Module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

Appendix 1: Test Configuration Diagrams

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

DIAG

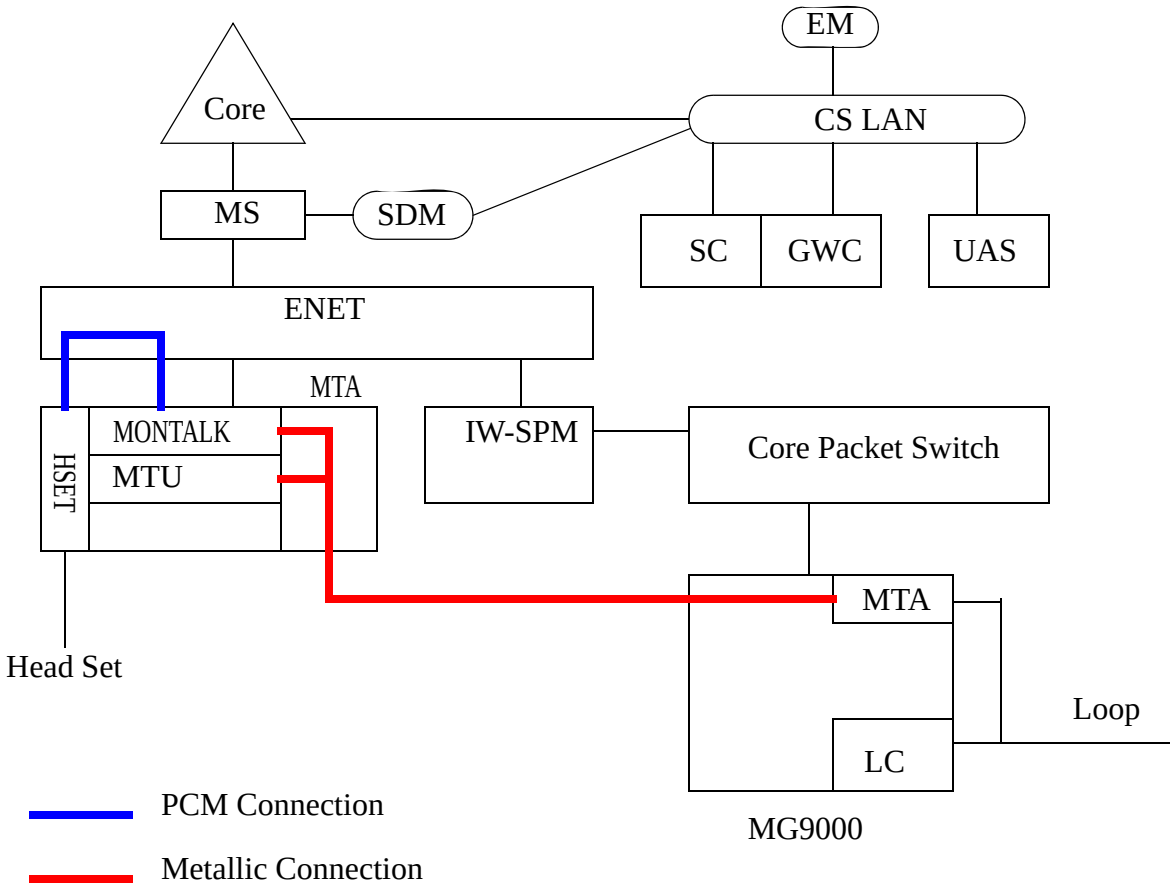
For POTS lines, a TTU located in an ISM/MTM shelf is used during the linecard diagnostic.



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

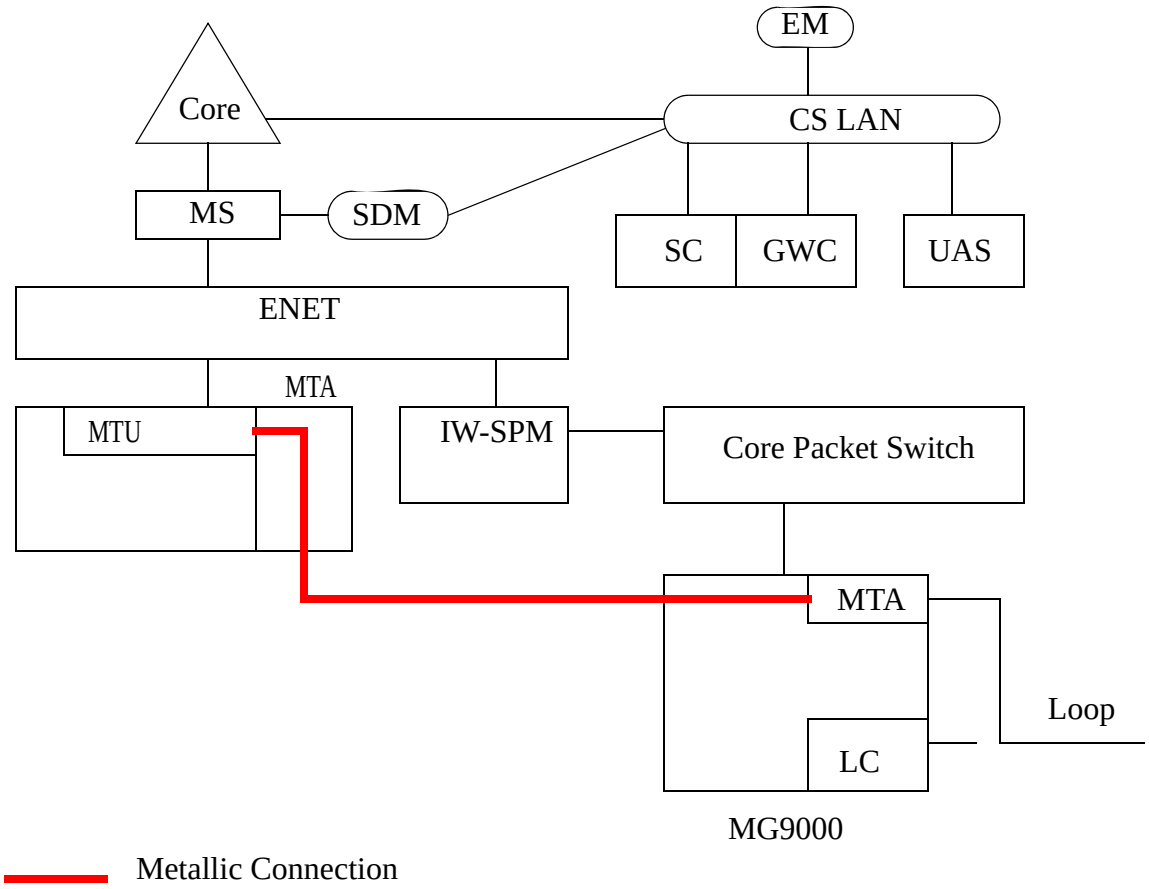
MONLTA, TALKLTA, ORIG, RING, DGTTST

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



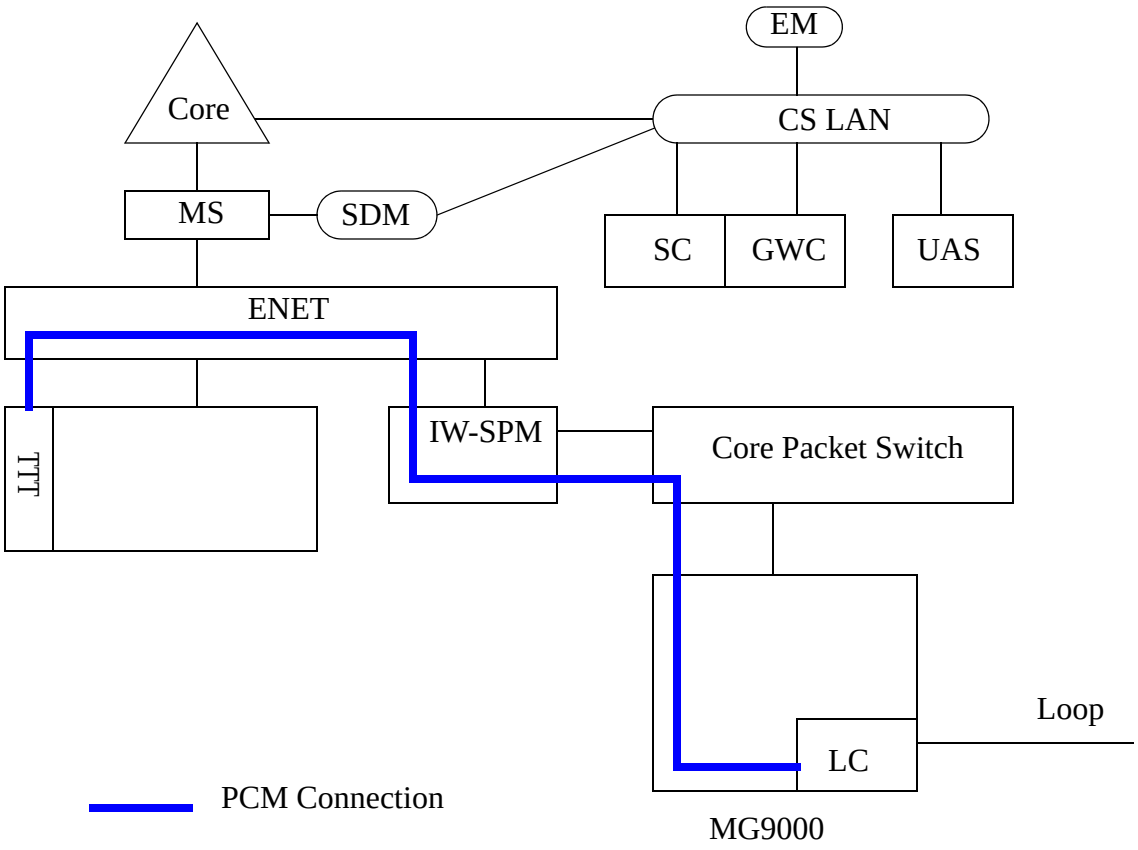
LNTST, VDC, VAC, RES, CAP, LTA

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



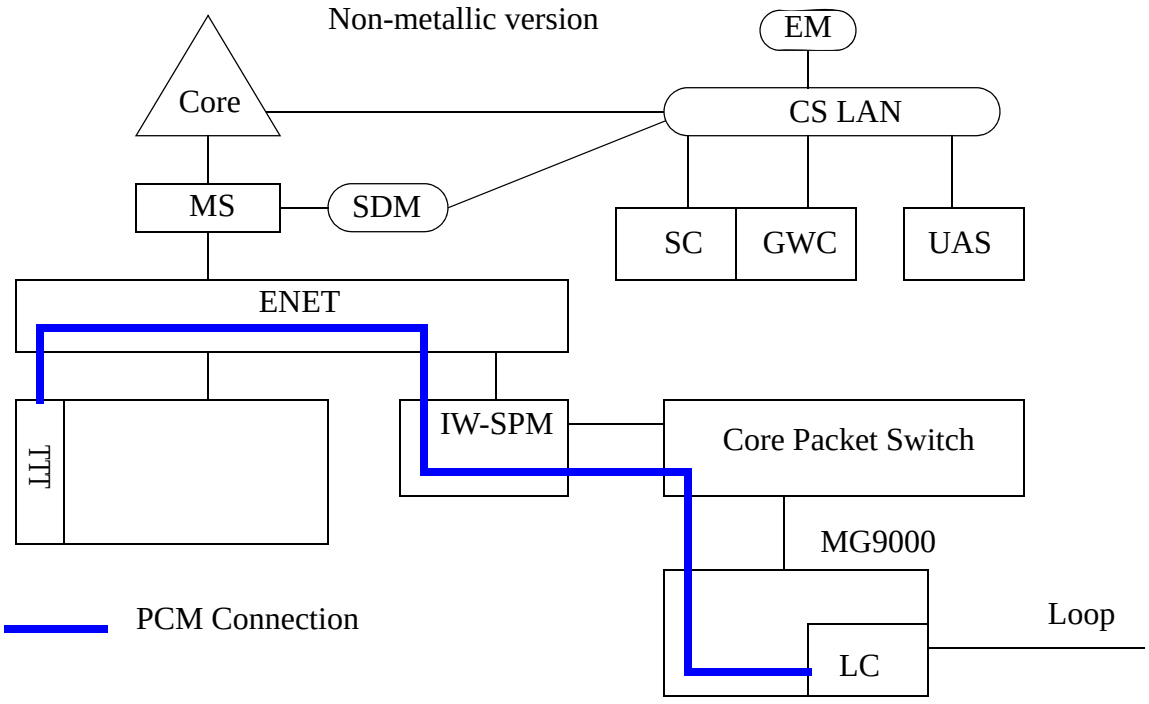
LOSS, NOISE

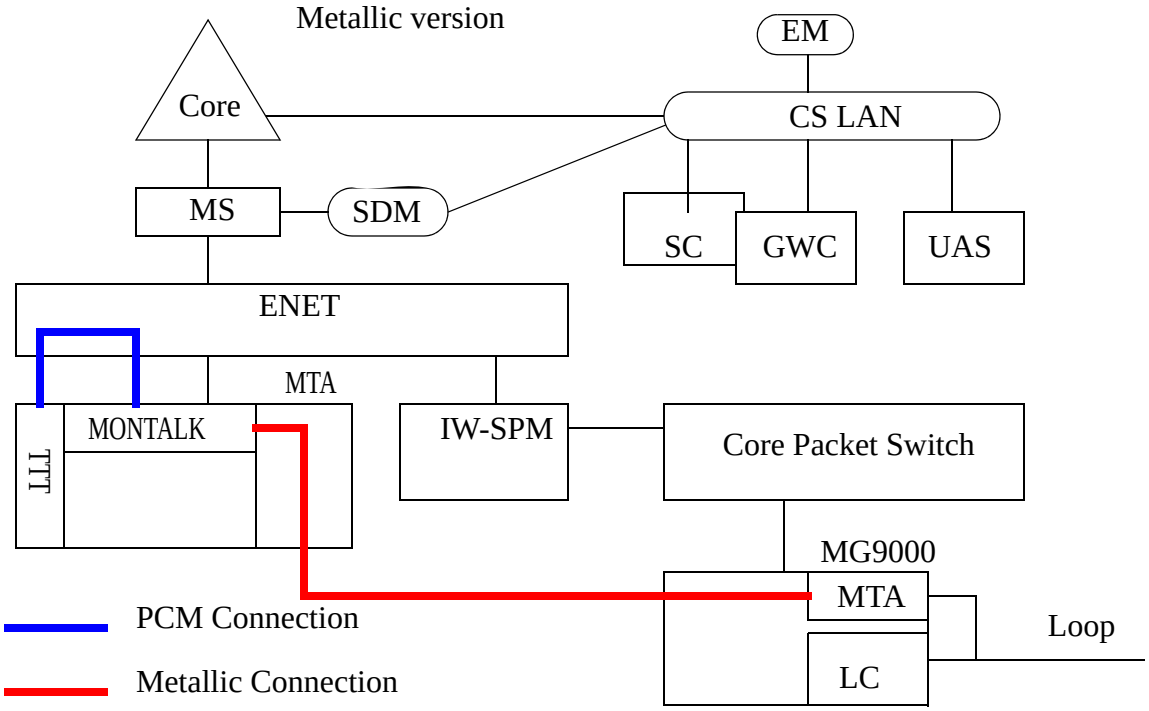
The following diagram shows the configuration used when the above listed commands are performed on an MG9000 line.



TONEGEN

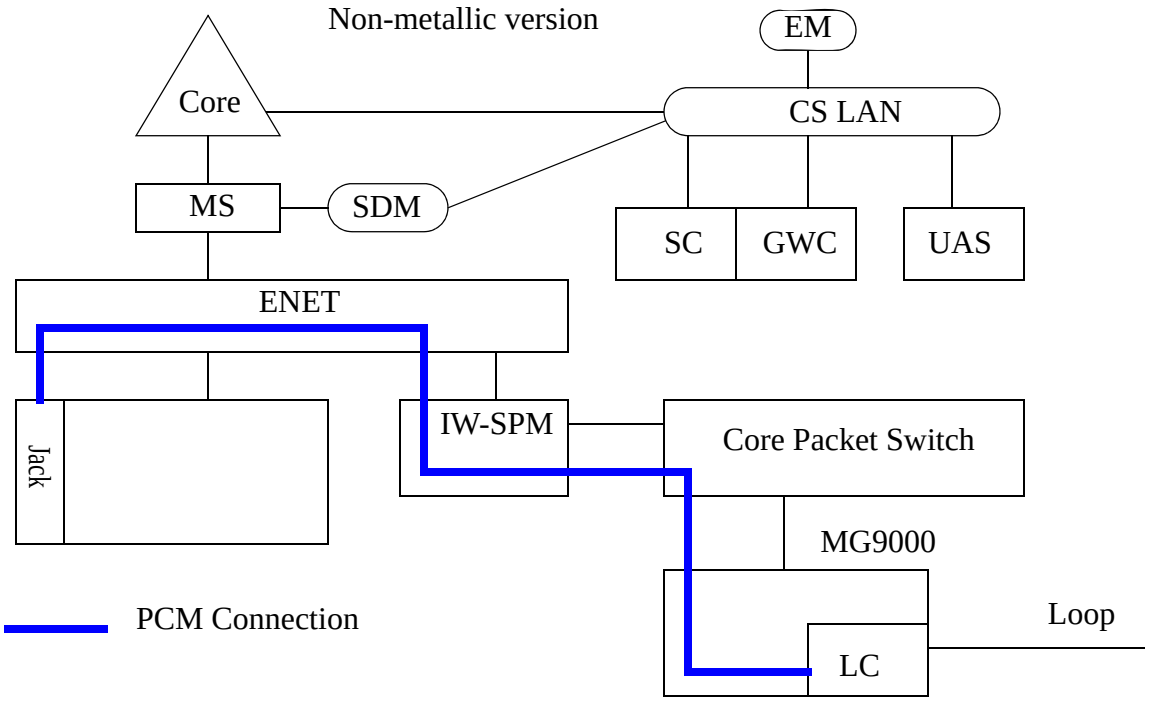
There are two versions of the TONEGEN command, the metallic and non-metallic version.

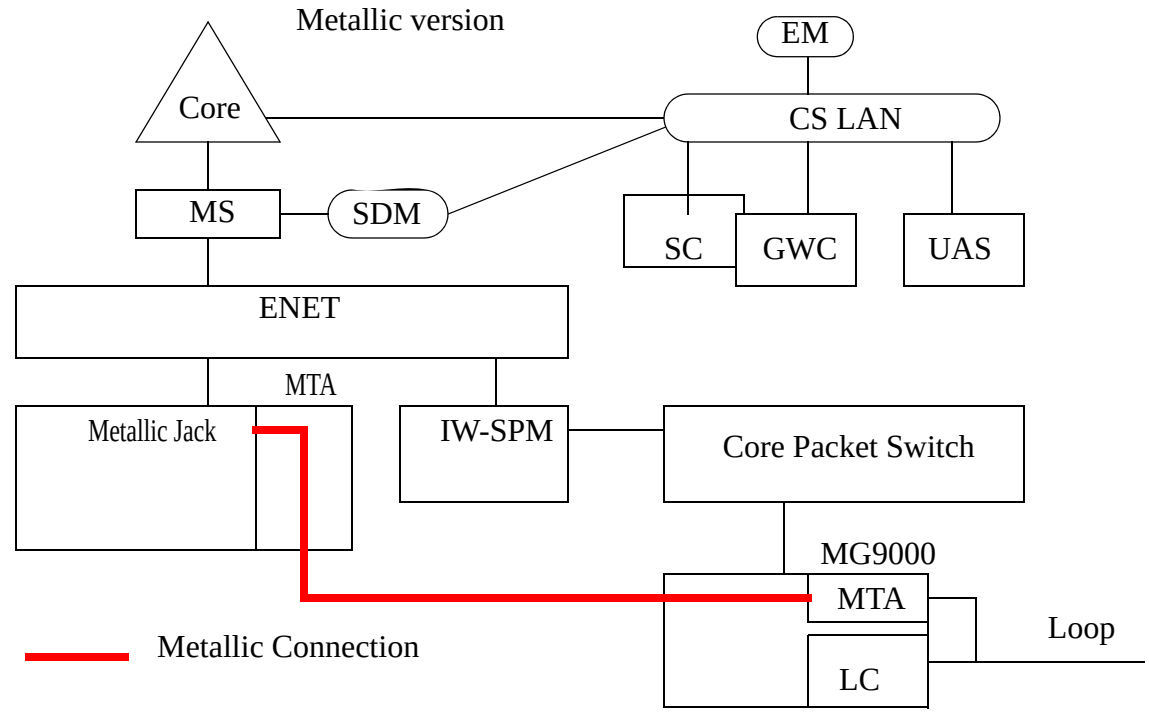




JACK

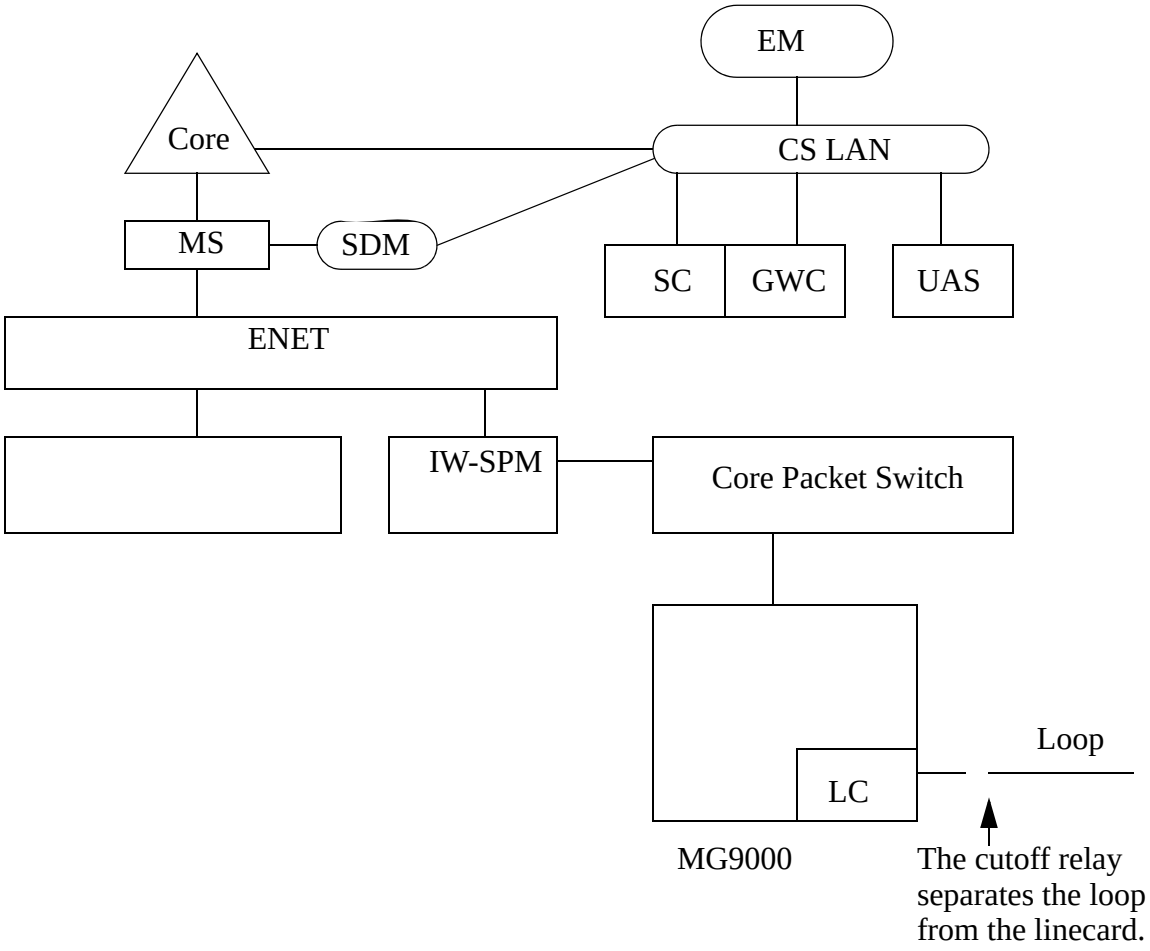
There are two versions of the JACK command, the metallic and non-metallic version





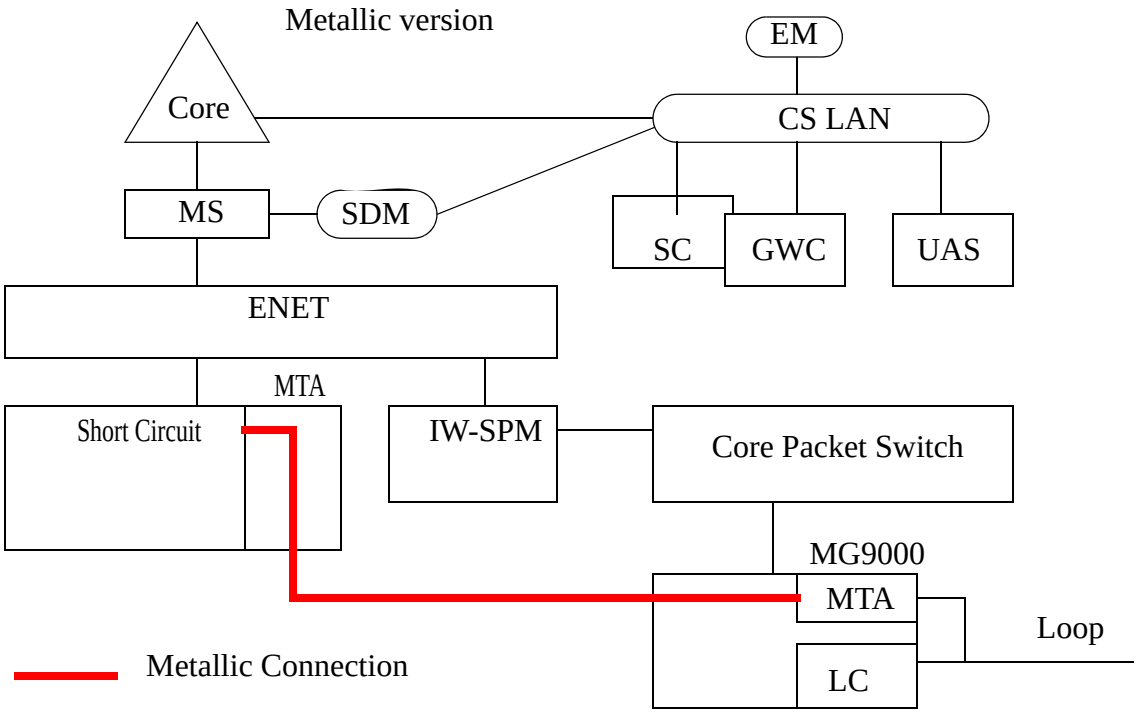
SSMAN

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



DSCKT

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



ALT SDIAG

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

ALT LIT

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

ShowerQ

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

14: Functional Description (FN): A00009097

14.1 Feature name and Feature ID

A00009097 - IUP ACI Handling Enhancement

14.2 Description

14.2.1 Feature description

This activity will provide below functionality for supported incoming BTUP calls:

The handling of ACI request for FCLI (IRC 1 and ICC 0; please refer to "APPENDIX A" on page 296 for IRC/ ICC values) sent to the previous node, is enhanced for scenarios where the requested FCLI data is not received.

When ACI request for FCLI is sent to the previous node, if FCLI data is not received as

- CFN message is received as response [Section 2.2.1.1 "Confusion message is received" on page 292],
- timer T14 expired as no ACI response is received [Section 2.2.1.2 "Timer T14 expired" on page 293],
- ACI with PCLI (ICC 3, IRC 0) or null ACI (ICC 0, IRC 0) [1] ,
- invalid ACI [2] (ICC reserved value) or
- ACI with unpermitted ICC values for FCLI request [3] is received as response,

the call will be allowed to proceed (BTUP protocol on incoming side will always let the call continue) unless prevented by terminating protocol/service/ feature or for billing/screening purposes as FCLI is essential.

Before the introduction of this feature, value of CBI in incoming BTUP IAM/ IFAM affected the call failure/proceeding for receipt of CFN or T14 expiry as response to ACI request for FCLI (eg. for BTUP-PRI/DPNSS calls, call failed if CBI was Y and call proceeded if CBI was N) [Reference 2 sections

[1]Please refer to APPENDIX B."1. ACI response with PCLI or Null ACI is received" on page 297.
[2]Please refer to APPENDIX B."2. Invalid ACI is received" on page 298.
[3]Please refer to APPENDIX B."3. ACI response with unpermitted ICC values for FCLI request, is received" on page 299.
For above items,, incoming BTUP side lets the call to continue unless prevented by terminating protocol/ service. This functionality already exists and no change will be done.

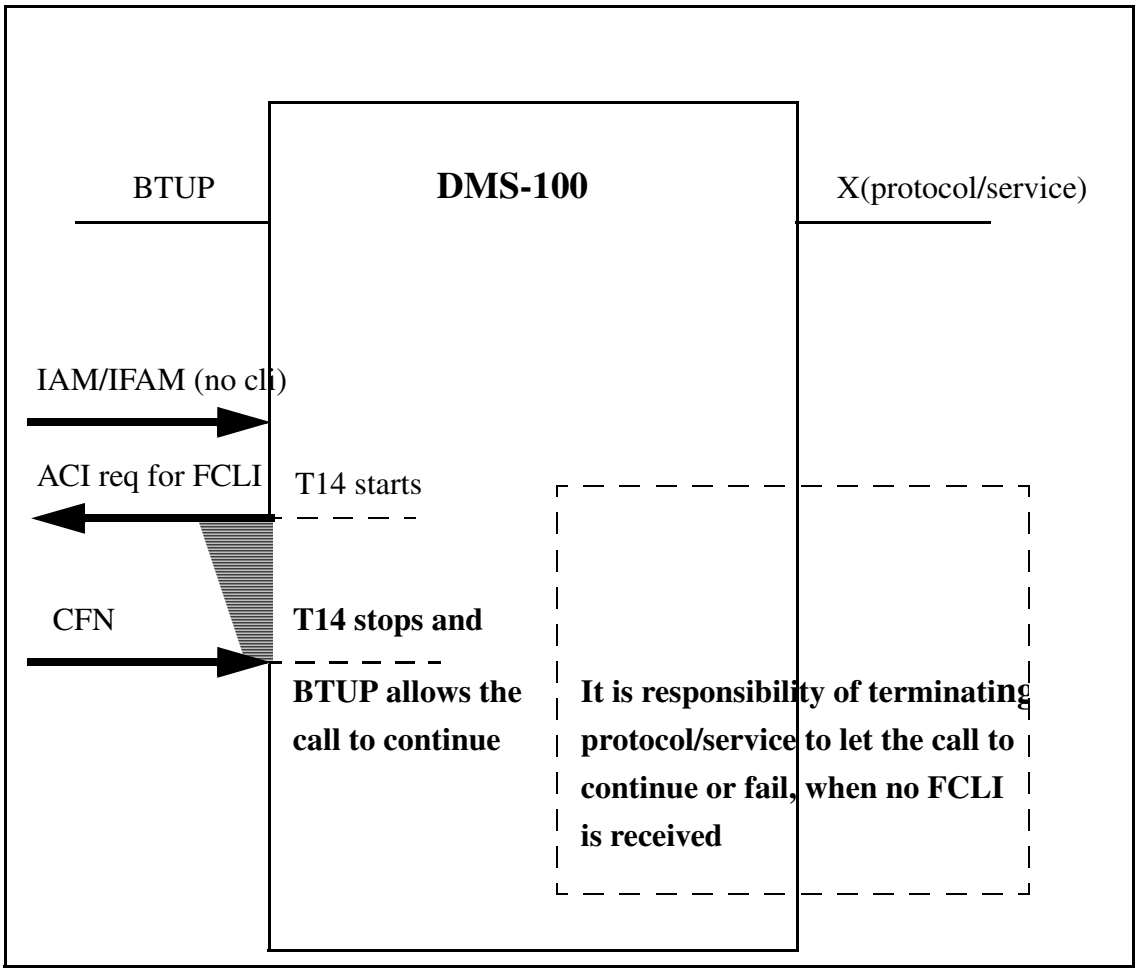
3.2.2.5.60 and 3.2.2.5.70 Nortel Notes] . New implementation will work for all CBI values and call proceeding/failure will not depend on the value of CBI in incoming BTUP IAM/IFAM.

Each of the above scenarios are explained under subsections below and in Appendix B.

14.2.1.1 Confusion message is received

When ACI request for FCLI is sent to the previous node, if CFN message is received as response, call will proceed without FCLI unless prevented by terminating protocol/service.

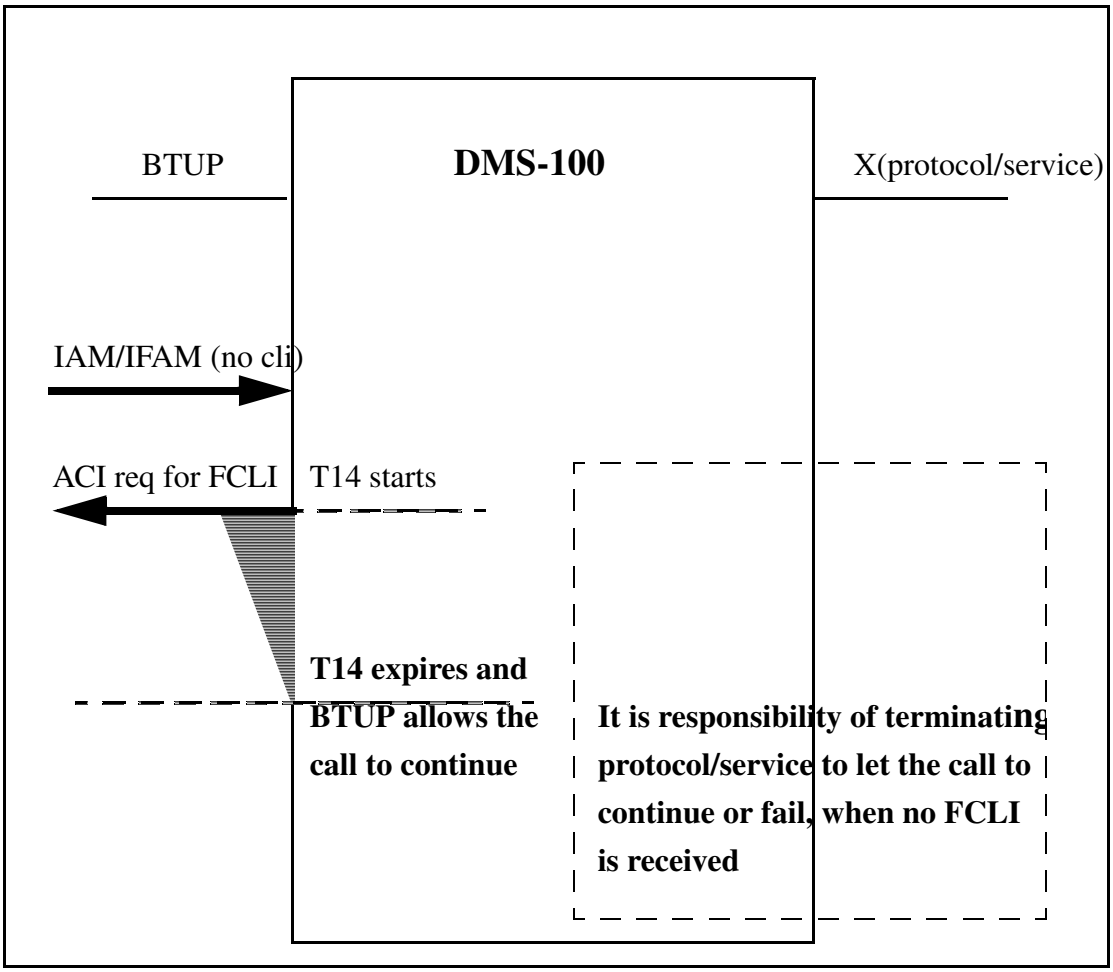
Figure 1 Call is allowed to continue on BTUP side, if CFN is received as response to ACI request for FCLI.



14.2.1.2 Timer T14 expired

When ACI request for FCLI is sent to the previous node, if T14 expired as FCLI data is not received , call will proceed without FCLI unless prevented by terminating protocol/service.

Figure 2 Call is allowed to continue on BTUP side, if T14 expired as ACI response with FCLI is not received.



14.3 Hardware Requirements or Dependencies

None.

14.4 Software Requirements or Dependencies

None

14.5 Limitations and restrictions

If FCLI is not received, the billing records will not contain FCLI under orig open digits parameter.

It's the responsibility of the terminating protocol/service to decide on whether to allow the call to continue or fail, if FCLI is not received. This is not in the scope of this activity.

14.6 Interactions

By the introduction of this feature, the calls will continue without FCLI for the given scenarios. The existing behaviour for supported incoming BTUP to X (protocol/service) calls without FCLI, will not be changed.

References for some of the X protocols/services (for BTUP-X interworking scenarios) which are planned to be tested, are given in section 2.8 Recommended Reading/References.

14.7 Glossary

Term	Explanation
ACI	Additional Call Information
BTUP	British Telephony User Part
CBI	Calling line Blocking Indicator
CFN	Confusion
FCLI	Full Calling Line Identity
ICC	Information Contained Code
IRC	Information Requested Code
IUP	Interconnect User Part

LDLI	Last Diverting Line Identity
PCLI	Partial Calling Line Identity
PN	Presentation Number
RCGLI	Request CallinG Line Identity
SASUI	Send Additional Set-Up Information
SHP	Service Handling Protocol
SIM	isdn composite Service Information Message
T14	Timer 14 in table c7uptmr; runs when waiting for additional info response message

14.8 Recommended Reading/References

1. PNO-ISC SPEC #006

2. IUP Compliance ISN07 and ISN07 (TDM) Implementations Version:PRE 1.0 , Date:16 April 2004

3. AE1010 BTUP CLI HANDLING

4. AJ5284 BTUP PRESENTATION CLI

5. AE1122 BTUP V2+ CLI, CP

PROTOCOLS

6. AE0472 BTUP - IBN LINES INTERWORKING(1)

7. AE0569 BTUP - IBN LINES INTERWORKING(2)

8. AE1594 ETSI BRI to BTUP Interworking

9. AJ4398 ETSI ISUP INTERWORKING WITH BTUP

10. AE0737 BTUP - DPNSS INTERWORKING

11. AG4661 CLI interworking for BTUP to DPNSS

12. AG5046 ETSI PRI/BTUP CLI Handling

13. AE1231 ETSI PRI I/W TO BTUP WITH OVERLAP

14. AE0961 INTL PRI - INTERWORKING TO BTUP

15. AE1544 ETSI INAP CALLP

SERVICES

16. AJ5351 Calling Line Identification (CLI) Screening Via Translations Enhancements
17. AU2513 CLI Screening via Translations
18. AU2804 CLI based VPN access
19. AJ5349 Calling Line Identity (CLI) Screening via Translations - Protocol Support
20. AF2879 CLASS: Anonymous Caller Rejection
21. AE0817 BT7 MALICIOUS CALL INTERWORKING (CC)
22. AE0901 BT7 Emergency Calls
23. AE1008 BT7 Operator Override

APPENDIX A

Below are the possible values for information contained/requested parameter in BTUP ACI message (as given in PNO-ISC spec ##006):

00000000 [0]No information

00000001 [1]Full Calling Line Identity

00000010 [2]Full Called Line Identity

00000011 [3]Partial Calling Line Identity

00000100 [4]Partial Called Line Identity

00000101 [5]Full Calling Line Identity with Calling Subscriber's Basic Service Marks

00000110 [6]Full Called Line Identity with Called Subscriber's Basic Service Marks

00000111 [7]Called Subscriber's Basic Service Marks

00001000 [8]Calling Subscriber's Originating Facility Marks

00001001 [9]Called Subscriber's Terminating Facility Marks

00001010 [10]see 0

00001011 [11]Last Diverting Line Identity

00001100 [12]Presentation Number Line Identification

00001101 [13] to 11111111 [255] reserved

APPENDIX B

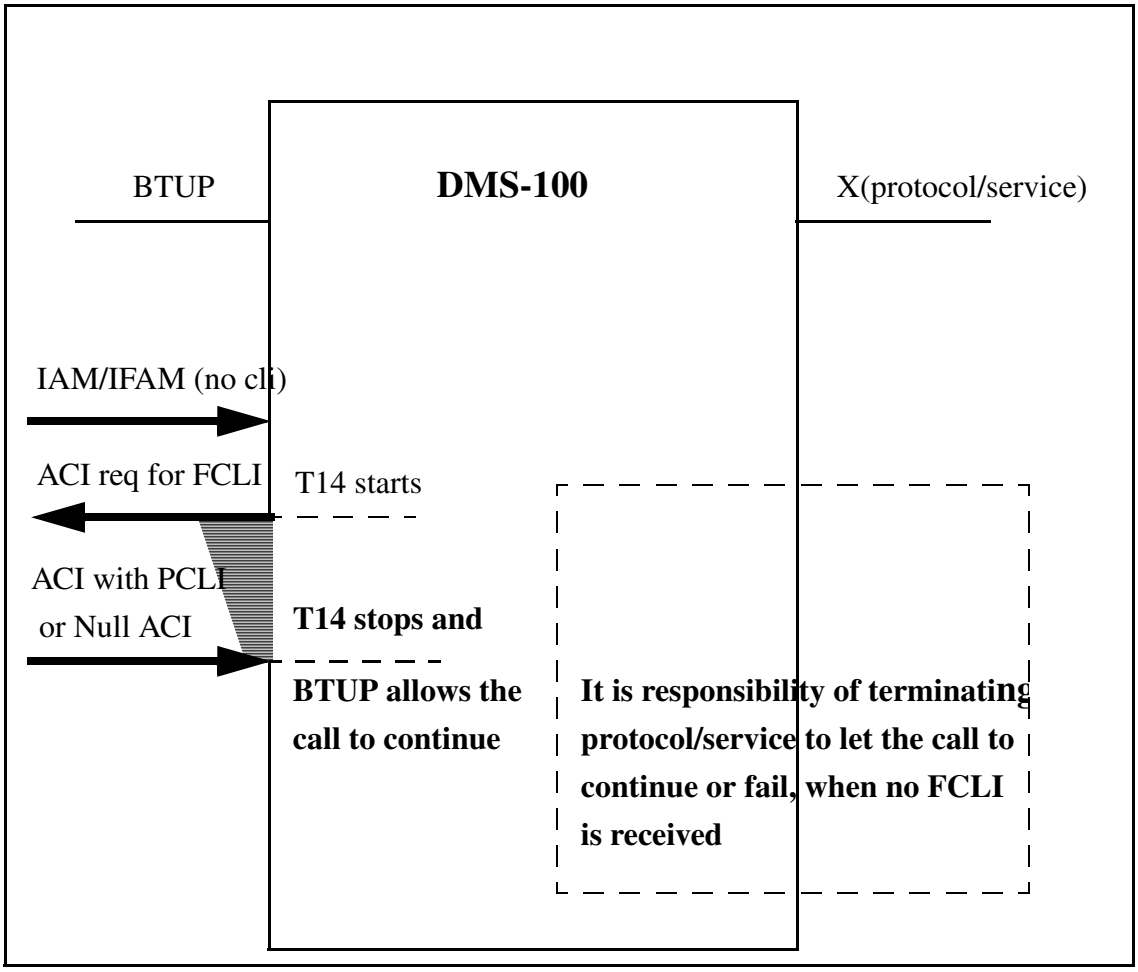
The existing behaviour for some scenarios, is provided below as background for this feature. The functionality will remain unchanged for these scenarios.

1. ACI response with PCLI or Null ACI is received

When ACI with FCLI is sent to the previous node, if ACI response with PCLI or Null ACI is received, T14 stops. Call proceeds/fails depending on the terminating protocol/service.

This is the existing behaviour, no change will be done.

Figure 3 Call is allowed to continue on BTUP side, if ACI response with PCLI or Null ACI is received as response to ACI request for FCLI.

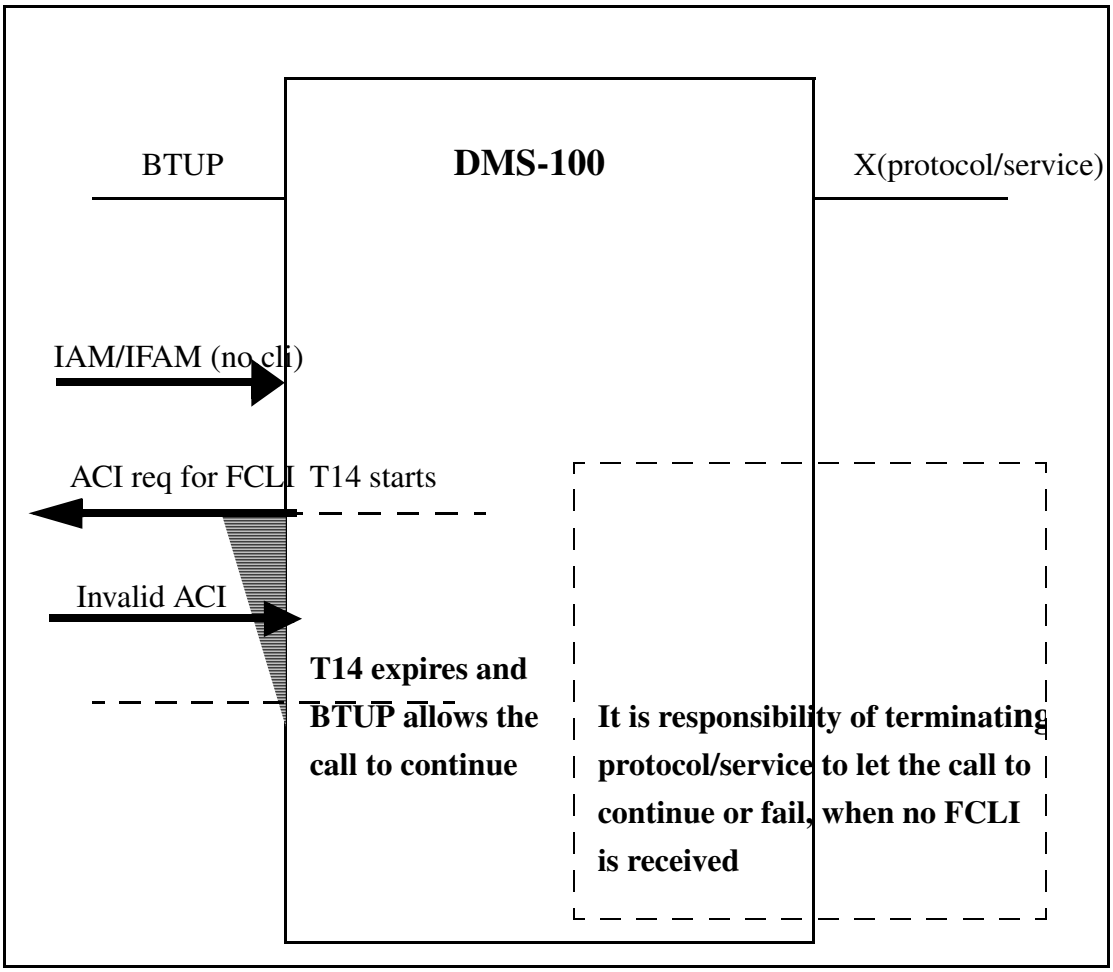


2. Invalid ACI is received

When ACI with FCLI is sent to the previous node, if invalid ACI (ICC reserved value) is received as response, timer T14 doesn't stop. When T14 expires, call proceeds without FCLI unless prevented by terminating protocol/service. So, response is ignored as per Reference 1/2 section 3.2.2.5.50 .

This is the existing behaviour, no change will be done.

Figure 4 Call is allowed to continue on BTUP side, if T14 expired as invalid ACI is received as response to ACI request for FCLI.



3. ACI response with unpermitted ICC values for FCLI request, is received

According Reference 1/ 2 Section 4.3.2, when ACI request for FCLI is sent backward, an ACI response with ICC 0, 1 or 3 is expected. Thus, unpermitted ICC values for ACI response are 2, 4-9, 11 and 12 . For these scenarios, T14 stops and call continues accordingly (same behaviour as given in Figure 3).

15: Functional Description (FN): A00009120

15.1 Feature name and Feature ID

A0009120 Multi-Time Zone Enhancments

15.2 Description

In order to support networks that span Multiple Time Zones (MTZ) features in the Succession/CS2K products must be enhanced. Feature A59038784 introduced a framework to support MTZ and DST (Daylight Savings Times) for subscriber visible services. This feature extends this functionality to the following:

1. Time of Day (TOD) Routing
2. Selected Malicious Call Trace (MCT/MCH) Logs LINE 125 & 126, MCT 103 &105

Currently with the TDM based MMP/DMS products, a callserver is allocated within each time zone. However, with the introduction of Succession/CS2K products, the callserver and the line gateways aren't bound by this limitation and can be located in different time zones. This means that line features/logs/ billing that use or display the local time must be able to modify the callserver time based on the time zone they are located in.

Activity A59038784 introduced a framework for multiple time zones and DST (Daylight Savings Time) for subscriber visible services, supporting IBN and RES lines. The activity introduced a line option, MTZ, which when assigned to a subscriber line provides an index into table MULTITM. Table MULTITM contains information as to the time difference based on the time zone and DST data.

Activity A00005734, Multiple time zone option for KSET lines expanded the functionaility to KSET lines with the M5216 Line Class Code. This allows for the support of CICM lines together with those on the MG9K.

Line features/logs are all currently based on the switch/callserver time, this feature uses the framework to obtain offsets from the switch time and hence the ability to calculate local time for Time of Day (TOD) Routing and select Malicious Call Trace logs. A separate activity will extend this functionality to billing.

There is no Software Optionality Control (SOC) for this activity.

The MTZ framework provides support for core based IBN, RES and M5216 KSET lines, this activity has the same limitation. However, it is assumed that this confers support for succession access lines CICM, MG9K, IADs, MTA and MG9K ABI together with SIP lines.

This activitiy is broken down into the following design components:

15.2.1 TOD Routing:

The desired behavior of the TOD Routing support with MTZ will be able to do TOD routing when MTZ exsists. This will allow a call to route based on the Time of Day even if multiple time zones and DST are present. When TOD routing occurs, a time is scheduled when to route the call. This feature will check if MTZ exists, convert the time given by the user on the individual line from the timezone they are in, into the CM clock time. The call will then be scheduled to route based on that converted time. If MTZ does not exsist, the TOD routing behavior before this feature will occur.

The TOD system is based on datafill of five tables, DAYTYPES, TODHEAD, DAYOWEEK, DAYOYEAR and TIMEODAY.

Table 1:

Table Name	Function
DAYTYPES	Defines the DAYTYPES(such as weekday, weekend, midweek etc) to be used by the other tables
TODHEAD	Defines the name (TODNAME) and the DAYTYPE for the TOD system entry.
DAYOWEEK	This table is used to map the day of the week into a DAYTYPE.
DAYOYEAR	This table is used to map the specified day of year into the DAYTYPE. This overrides the entry in DAYOWEEK based on the TODNAME.
TIMEODAY	The first four tables exist only to allow you to get to the TIMEODAY table. This table defines the actual result for the time, DAYTYPE and TODNAME.

To achieve TOD Routing, datafill of TOD routing must be done in one of the routing tables IBNRT(X), OFR(X), RTEREF of HNPACONT or FNPACONT

Table 2: TOD Route Datafill in routing tables IBNRTE, OFRT,RTEREF

Table Fields	Definition	Datafill
RTE	Route Ref Index	{0-1023}
IBNRTESEL/ RTESEL	Route Selector	CND (Condtitinal Route)
CNDSEL	Conditional Selector	TOD (Time of Day)
TODNAME	TOD Name Datafilled in the TODHEAD table	TOD Name
TIMES	ibn_time_range (results of TOD system will be resolved into this type)	{0 -15}
RTETYPE	CND_RTE_TYPE	{ST,T,SK}
{RTEREF, TABNAME -index, , SKIPNUM}	Route Ref Index Routing Table Name Number of Routes to skip	{0-1023} {Routing tables} {0-7}
INDEX	Route ref index	{0-1023}

Table 3: Example of TOD route datafill:

Table IBNRTE/OFRT

RTE: 1005

IBNRTESEL: CND

CNDSEL: TOD

TODNAME: CGATOD
TIMES: 1

RTETYPE: T

TABNAME: OFRT

INDEX: 100

```
>list
 RTE                                          RTELIST

                                            OPTIONS

------------------------------------------------------------------------

1005          (  CND      TOD   CGATOD          2  T     OFRT  100)$$
```

15.2.2 MCT Logs

There are a number of MCT logs supported by the CS2K both in the North American and International market, however, not all of these logs need to be modified for multiple time zones. The following logs have been identified by the customer as requiring support for MTZ:

LINE125
LINE126
MCT103
MCT105

For each of these logs a new field, LOCAL TIME, will be added, this field will display the local time for that subscriber line based on the switch time modified by the value in table MUTITM if assigned to that line. This feature doesn't impact when or where these logs are output.

The log report format for LINE125 is as follows:

LINE125 mmmdd hh:mm:ss ssdd INFO TRACE_ON_MALICIOUS_CALL_INI...

len DN dn INCOMING TRUNK = CKT trkid

CALLID = callid

CALLING NUMBER = dn

SOURCE = source

LOCAL TIME = <Time>

An example of log report LINE125 follows:

LINE125 APR01 12:00:00 2112 INFO TRACE_ON_MALICIOUS_CALL_INITIATED

HOST 00 0 19 20 DN 2557811999

INCOMING TRUNK = CKT ICCAMA 15

CALLID = 123456

CALLING NUMBER = 2149975015

SOURCE = CALLING NUMBER

LOCAL TIME = 10:00:00

The format for log report LINE126 is as follows:

LINE126 mmmdd hh:mm:ss ssdd INFO TRACE_ON_MALICIOUS_CALL_ INITIATED

len DN dn

CALLING LINE = LEN len DN dn onitxt

CALLID = callid

LOCAL TIME = <Time>

An example of log report LINE126 follows.

LINE126 APR01 12:00:00 2112 INFO TRACE_ON_MALICIOUS_CALL_INITIATED

HOST 00 0 19 20 DN 2557811999

CALLING LINE = LEN HOST 05 1 15 16 DN 7812001

CALLID = 123456

LOCAL TIME = 10:00:00

The log report format for MCT 103 is as follows:

MCT103 mmmdd hh:mm:ss ssdd INFO TRACE_ONMALICIOUS_CALL_ACTIVATED

CALLING_PARTY : <cli> <originating agent>

CALLED_PARTY : <full number><terminating agent>

CALLING_PARTY_CATEGORY : <cpc>

LOCAL TIME = <Time>

An example of log report MCT 103 follows:

MCT103 APR01 12:00:00 2112 INFO TRACE_ON_MALICIOUS_CALL_ACTIVATED

CALLING_PARTY : CKT ICATUPTRUNK 1

CALLED_PARTY : 2762345 LEN HOST 00 0 01 10

CALING_PARTY_CATEGORY : 16

LOCAL TIME = 10:00:00

The log report format for MCT 105 is as follows:

MCT105 mmmdd hh:mm:ss ssdd INFO TRACE_ONMALICIOUS_CALL_ACTIVATED

CALLING_PARTY : <full number> CKT <originating agent>

CALLED_PARTY : <full number> CKT <terminating agent>

LOCAL TIME = <Time>

An example of log report MCT 105 follows:

MCT105 APR01 12:00:00 2112 INFO TRACE_ON_MALICIOUS_CALL_ACTIVATED

CALLING_PARTY : 9717718745 CKT ICATUPTRUNK 1

CALLED_PARTY : 2762345 CKT ICATUPTRUNK 12

LOCAL TIME = 10:00:00

15.3 Hardware Requirements or Dependencies

N/A

15.4 Software Requirements or Dependencies

SN09

15.5 Limitations and restrictions

The limitations and restrictions specified in activity A59038784 are also applicable to this activity.

In addition the following limitations and restrictions apply:

- Multitime Zone enhancments will not be supported if the MTZ option is not on the subscriber’s line.
- The feature is only supported on IBN/RES and M5216 KSET sets.
- MTZ is only supported by the LINE125, LINE126, MCT103 and MCT105 logs.
- The new field ‘LOCAL TIME’ will be present in all LINE125, LINE126, MCT103 and MCT105 logs irrespective of whether the subscriber is in a different time zone than the callserver. In these cases the local time will be the same as the switch time.

15.6 Interactions

This feature interacts with the existing features Multi-Time Zone, A59038784 and .A00005734, Multiple time zone option for KSET lines.

15.7 Glossary

Term	Description
CICM	Centrex IP Client Manager
CLF	Call LIne Indentification withFlash
CLI	Calling Line Identity
CM	Computing Module
CPC	Calling Party Category
CNDSEL	Conditional Selector
DMS	Digital Multiplex Switch
DST	Daylight Savings Time
IAD	Integrated Access Device
IBNRTESEL	IBN Route Selector
MCH	Malicious Call Hold
MCT	Malicious Call Trace
MTA	MultiMedia Terminal Adaptor
MTZ	Multi-Time Zone Enhancment
RTESEL	Route Selector
SIP	Session Initiation Protocol
TOD	Time Of Day

16: Functional Description (FN): A00009143

16.1 Feature name and Feature ID

A00009143: FTUP & SPIROU NAOC to VN4/VN6/ETSI PRI & H323 AOC Interworking

16.2 Description

16.2.1 Summary

This activity extends the functionality implemented in SN08 with A00006730 - French NAOC on Succession CS2K. Please refer to Figure 7, "French NAOC Support on the originating exchange" and Figure 11, "French NAOC Support on the transit exchange" for further details of this extension. The current activity implements the components for the French market by using ***FTUP(SSUTR2)*** and ***SPIROU*** as interconnect protocol between different exchanges.

This activity also extends the functionality implemented in SN08 with A00005822 - AOC Support over H323 which provides a solution to deliver AOC services to the originating agents connected to the CS2K over H323. Please refer to Figure 12, "Nodal AOC Support on the Originating Exchange" for further details of this extension. The current activity implements the AOC support over PVG for VN4 and VN6 PRI originating agents.

The supported items as an extension to activity A00006730 - French NAOC on Succession CS2K are:

- Charge message interworking to ISDN originators on the originating exchange.
  - — reception and validation of ITX charge messages.
  - — generation of Advice of Charge (AOC) messages to ***VN4 PRI*** and ***VN6 PRI*** originating agents from backwards charges received in either ***FTUP(SSUTR2)*** or ***SPIROU*** ITX charge messages (French NAOC).
  - — generation of Advice of Charge (AOC) messages to ***ETSI PRI*** and ***H.323*** originating agents from backwards charges received in ***FTUP(SSUTR2)*** ITX charge messages.
  - — error scenarios and their responses.
- Optional ITX charge recording to AMA for ***FTUP(SSUTR2)*** or ***SPIROU*** agents.

- Tandeming ITX and TXA messages between ***FTUP(SSUTR2) <-> FTUP(SSUTR2), FTUP(SSUTR2) <-> SPIROU, SPIROU <-> FTUP(SSUTR2)*** trunks at the transit exchange.

  Note: Transit of ITX/TXA messages from SPIROU to SPIROU is supported with activity A00006730-French NAOC on Succession CS2K.

- AOC using functional protocol for ***ETSI PRI*** and ***H.323*** originating agents.
- AOC using keypad protocol for ***VN4 PRI*** and ***VN6 PRI*** originating agents.

The supported items as an extension to activity A00005822 - AOC Support over H323 are:

- Nodal AOC (combined CDP and CGP scenario) support over PVG for ***VN4 PRI*** and ***VN6 PRI*** originating agents on CS2K.

  Note: A00005822 addresses two AOC Services: ***AOC-D*** and ***AOC-E***. These are also supported by this activity.

The verification items in the scope of French NAOC on CS2K are:

- Acknowledging the reception of ITX messages received over ***FTUP(SSUTR2)*** via TXA messages for ***VN4 PRI, VN6 PRI***, ***ETSI PRI, H.323*** originating agents.
- Acknowledging the reception of ITX messages received over ***SPIROU*** via TXA messages for ***VN4 PRI, VN6 PRI*** originating agents.
- French NAOC feature interaction support with the 2CLI feature.
- French NAOC feature interaction support with the Number Portability feature.
- Processing ITX/TXA charge messages received over SIP-T (FTUP) or SIP-T (SPIROU).

The verification items in the scope of Nodal AOC on CS2K are:

- Nodal AOC support for H323 to FTUP(SSUTR2) and H323 to SPIROU interworkings.
- Nodal AOC support for ETSI PRI to FTUP(SSUTR2) and ETSI PRI to SPIROU interworkings.

16.2.2 Background information

Network **A**dvice **O**f **C**harge (NAOC) implements the tariffing of calls in a deregulated telecom market. It can operate

- in a **single carrier environment**, where tariffs are sent between different nodes within the same carrier's network.

- in a **multiple carrier environment**,
  - — where tariffs have to be exchanged between different network operators.
  - — where all the tariffs are available on the originating local exchange and there is no need to receive and process tariffs between different operators.

If the originating exchange does not know the tariff to be applied, it has to receive the tariff information over the network from an other exchange.

From the point of view of the **NAOC** service there are two different types of nodes involved in the tariffing of a call in a multiple carrier environment:

1. **CDP** - The main function of the **Charge Determination Point** is to determine which tariff should be applied. The CDP is located in the network of the carrier chosen by carrier selection.

   The tariff information is either sent in an charge message over the network (CDP and CGP on the different exchanges) or passed internally to the CGP interface (CDP and CGP on the same exchange).

2. **CGP** - The **Charge Generation Point** is an exchange where the received charging information is converted into a format that is delivered to the subscriber.

   The CGP is located in the Originating Local Exchange (OLE) that receives the charging information from the **CDP** and routes this information to an originator who has subscribed the **AOC** service.

Operators can be classified in 3 categories from an NAOC point of view.

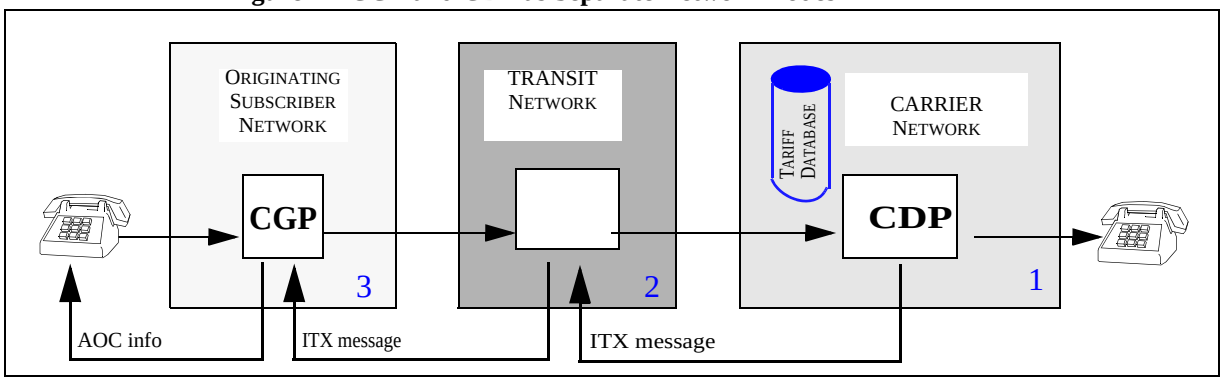
3. ***indirect access operators*** (carrier operators) responsible to generate charge messages (ITX messages) and to feed them in backward direction into another operator's network.
4. ***transit operators*** responsible for receiving the charging messages and tandeming them in backward direction.
5. ***originating operators*** responsible for receiving the charging message on an originating local exchange (OLE), converting them into AOC information and applying them to the supported originating agents.

Based on these types of network nodes, there are two scenarios which have been considered for **NAOC**:

- **CDP** and **CGP** are located in different networks, so that the **CDP** has to send the tariff information over the network boundaries to the **CGP**. Please refer to Figure 1, "CGP and CDP as Separate Network Nodes". This

scenario is dressed by the current activity as an extension to activity A00006730.

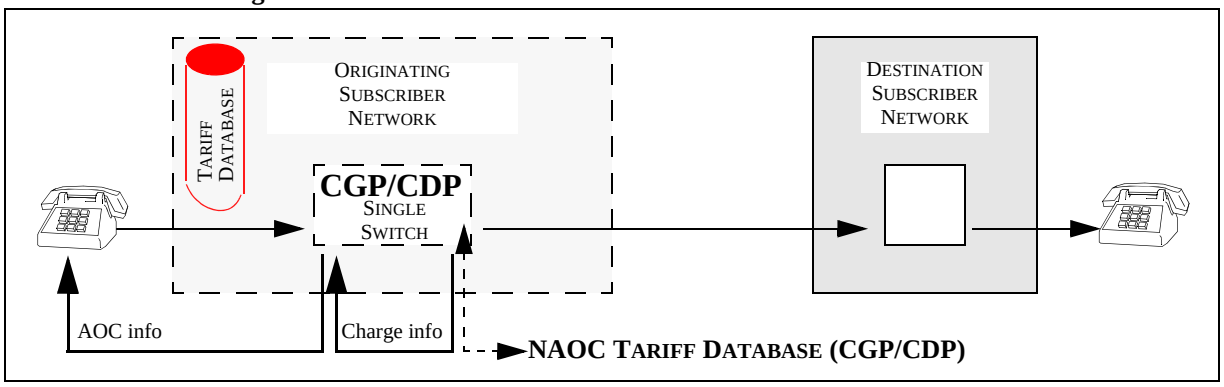
Figure 1 CGP and CDP as Separate Network Nodes



Note: ***ITX message generation*** (CDP functionality) is not supported by this activity while ITX message reception and transit are supported.

- **CDP** and **CGP** are located on the same exchange (**combined CGP/CDP scenario**). Tariff information is retrieved internally from the local tariff database and can be pulsed out to the subscriber. Please refer to Figure 2, "Combined CGP and CDP". This scenario is addressed by the current activity as an extension to activity A00005822.

Figure 2 Combined CGP and CDP



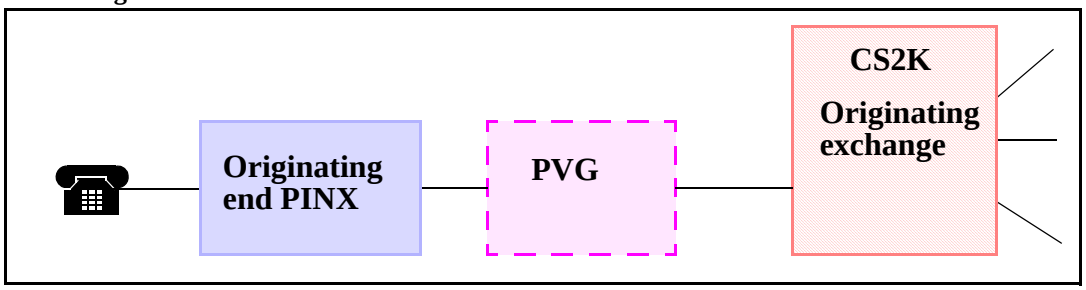
Advice **O**f **C**harge (**AOC**) gives the CS2K Call Server the ability to send network incurred charges to the ISDN subscriber within call control or facility messages.

The AOC service is delivered in three flavors:

AOC-S	Advice Of Charge at call Setup
AOC-D	Advice Of Charge During the call
AOC-E	Advice Of Charge at the End of the call

This activity addresses two AOC services: ***AOC-D*** and ***AOC-E*** like in A00005822. These services are deployed for originating agents connected to the CS2K over PVG. Please refer to Figure 3, "AOC over PVG". For the AOC calculation, the CS2K node has to be configured to determine and apply the tariffs (nodal configuration or combined CGP/CDP).

Figure 3 AOC over PVG



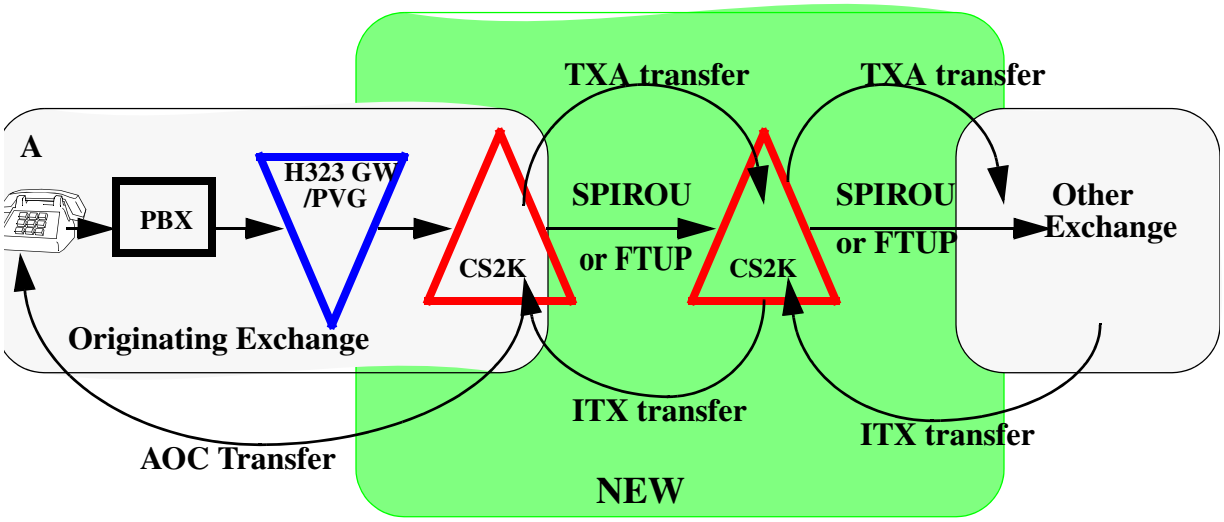
16.2.3 Feature description

'French NAOC' allows service provider to receive charging information over the signalling system during the call and hence to control the billing for the call.

FTUP(SSUTR2) & SPIROU supports the capabilities in the charging service, using nationally defined messages ITX (Charge Unit) and TXA (Charging Acknowledgement). Please refer to Figure 4, "New functionality does bridging between AOC and FTUP/SPIROU NAOC" for further details.

- The following applications are supported on the CS2K for FTUP(SSUTR2) & SPIROU agents in the scope of **French NAOC** support:
  - — ***Charge message interworking to ISDN originators*** on the originating exchange. Please refer to Section 16.2.3.1.
  - — ***Charge message billing***: Allows an alternate operator to receive ITX messages and use them to bill the calls. Please refer to Section 16.2.3.2.
  - — ***Charge message tandeming*** between ***FTUP(SSUTR2) <-> FTUP(SSUTR2), FTUP(SSUTR2) <-> SPIROU, SPIROU <-> FTUP(SSUTR2)*** trunks on the transit exchange. Please refer to Section 16.2.3.3.
  - — AOC using ***functional protocol*** for ***ETSI PRI*** and ***H.323*** originating agents. Please refer to Section 16.2.3.4.
  - — AOC using ***keypad protocol*** for ***VN4 PRI*** and ***VN6 PRI*** originating agents. Please refer to Section 16.2.3.5.
- Verifications for **French NAOC** support (listed in Section 16.2.1) provided by this activity can be found in Section 16.2.3.6.

Figure 4 New functionality does bridging between AOC and FTUP/SPIROU NAOC



- '**Nodal AOC**' (combined CDP and CGP) described in Figure 2, "Combined CGP and CDP" is supported for ***VN4 PRI*** and ***VN6 PRI*** originating agents over PVG gateway on CS2K. Please refer to Section 16.2.3.7 for further details.

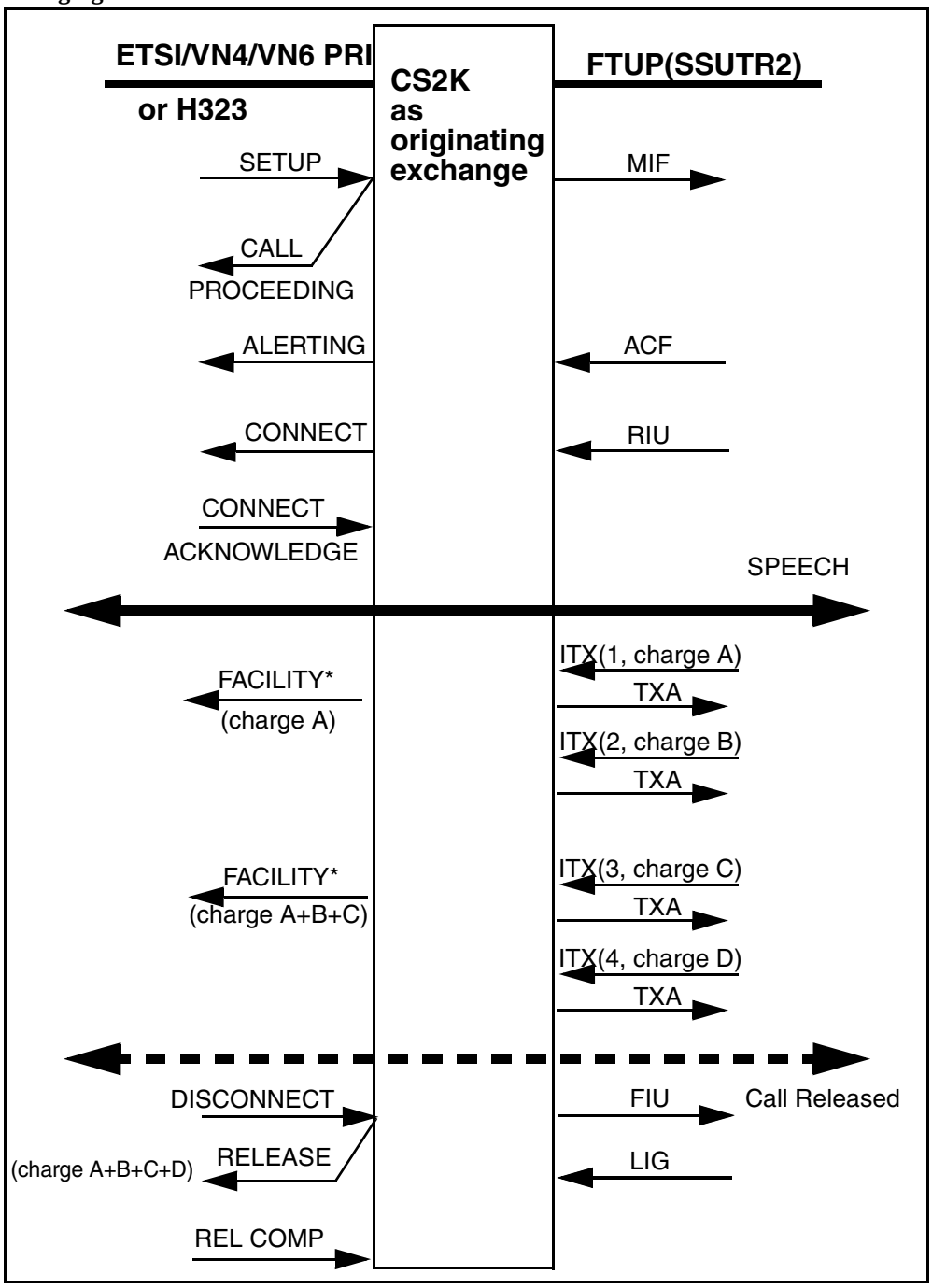
16.2.3.1 Charge message interworking to ISDN originators for French NAOC Support

Allows an alternate operator to present charge information from ITX messages received over FTUP(SSUTR2) or SPIROU trunks to ISDN users using the Advice of Charge (AOC) service. The supported functionalities are:

- reception and validation of ITX messages.
- generation of Advice of Charge (AOC) messages to ***VN4 PRI*** and ***VN6 PRI*** originating agents from Backwards charges received in either ***FTUP(SSUTR2)*** or ***SPIROU*** ITX messages (French NAOC).
- generation of Advice of Charge (AOC) messages to ***ETSI PRI*** and ***H.323*** originating agents from Backwards charges received in ***FTUP(SSUTR2)*** ITX messages.
- error scenarios and their responses. For more information see "ANNEX B: Handling receipt of ITX messages" on page 329.

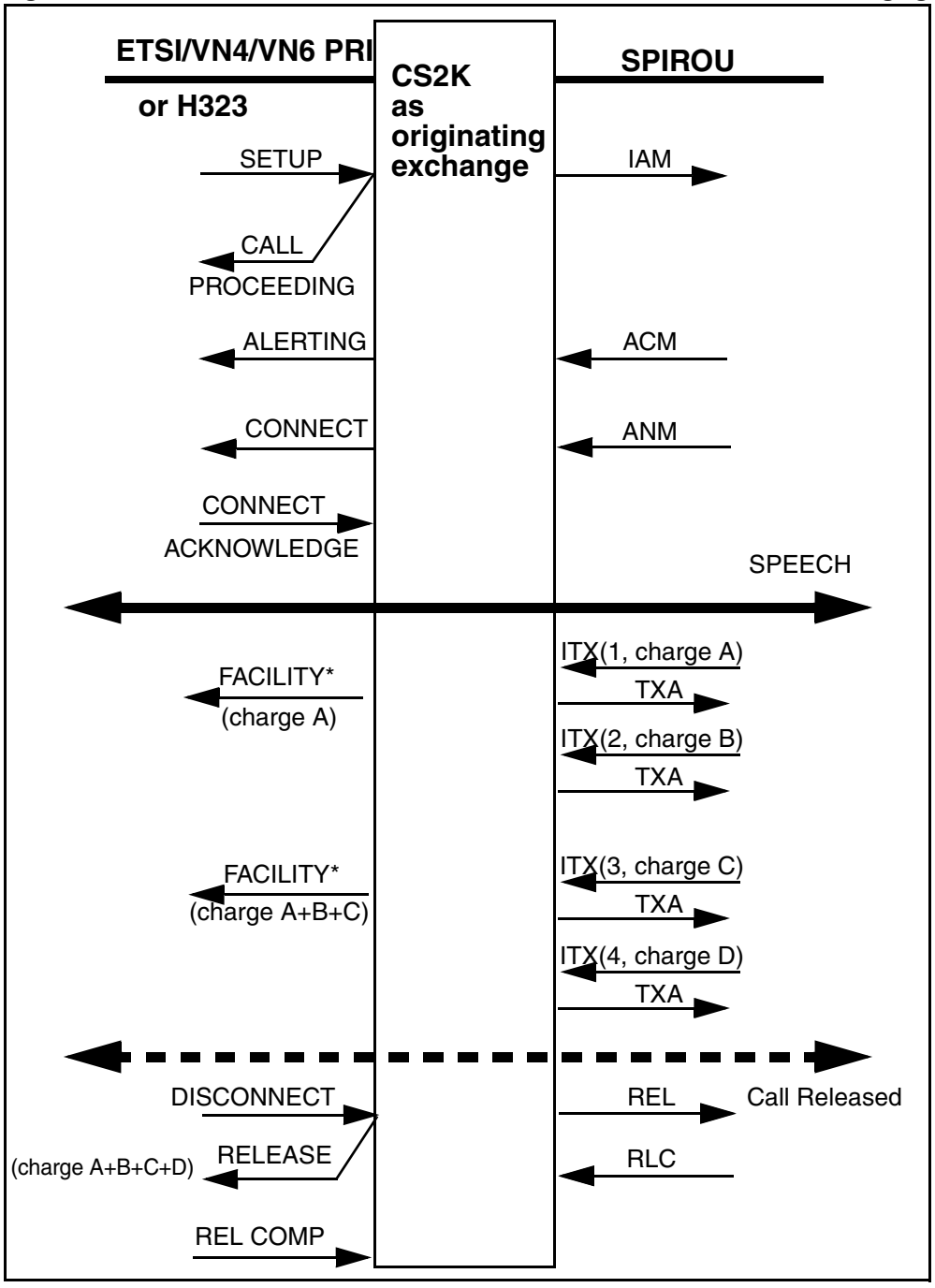
Figure 5, "ETSI/VN4/VN6 PRI or H323 to FTUP(SSUTR2) AOC-D with Backwards Charging" and Figure 6, "ETSI/VN4/VN6 PRI or H323 to SPIROU AOC-D with Backwards Charging" show the messaging for AOC-D where CS2K is an originating exchange.

Figure 5 ETSI/VN4/VN6 PRI or H323 to FTUP(SSUTR2) AOC-D with Backwards Charging



*: For VN4/VN6 PRI originating agents, INFO messages are used instead of FACILITY messages.

Figure 6 ETSI/VN4/VN6 PRI or H323 to SPIROU AOC-D with Backwards Charging



*: For VN4/VN6 PRI originating agents, INFO messages are used instead of FACILITY messages.

Figure 7, "French NAOC Support on the originating exchange" indicates all supported interworkings for each of the relevant originators, in the French market context. French NAOC is only applicable to SSUTR2(FTUP) and SPIROU trunks hence this feature is only applicable to the interworkings marked blue, other supported interworkings where French NAOC is not applicable are marked yellow. The interworkings with SIP-T trunks are tested for verification. “X” indicates the interworkings where French NAOC and interworkings are being supported with this feature.

Figure 7 French NAOC Support on the originating exchange

Platform	Originator	Terminating agents								
		H323 agents	IBN lines	ETSI PRI	QSIG (95)	ETSI ISUP V1	ETSI ISUP V2/V2+	SIP-T (FTUP and SPIROU)	SSUTR2 (FTUP)	SPIROU
CS2K	H323	N/A						X	X	X[a]
	ETSI PRI over PVG	N/A						X	X	X[a]
CS2K	VN4 PRI over PVG	N/A						X	X	X
	VN6 PRI over PVG	N/A						X	X	X

a. Already implemented in SN08 with A00006730
X: Supported with this activity(A00009143)

16.2.3.2 Charge message billing in French NAOC Support

This capability includes presentation of the charging information in AMA billing record if the outgoing SPIROU or FTUP(SSUTR2) trunk is datafilled as supporting the French NAOC Service (option TELETAXE in table TRKOPTS). Please refer to AU3283 for required billing datafill.

The CS2K may optionally store the number of charge units from ITX messages and produce an AMA record with the total number of charge units received. This capability exists both in originating and transit exchange.

16.2.3.3 Charge message tandeming for French NAOC Support

This capability includes transit of ITX messages (FTUP(SSUTR2) to SPIROU, SPIROU to FTUP(SSUTR2), FTUP(SSUTR2) to FTUP(SSUTR2)). Please refer to Figure 8, Figure 9 and Figure 10 for further details.

Note: Transit of ITX messages from SPIROU to SPIROU is supported with activity A00006730-French NAOC on Succession CS2K.

For transit calls, the CS2K normally transits the ITX and TXA messages unchanged. That is, it passes on the ITX message without sending a TXA in reply. The TXA acknowledgement is sent by the originating switch and the CS2K transits the TXA message when received. No checking of the ITX or TXA message contents are performed.

Figure 8 CS2K as interconnect exchange between SPIROU and FTUP(SSUTR2) trunks

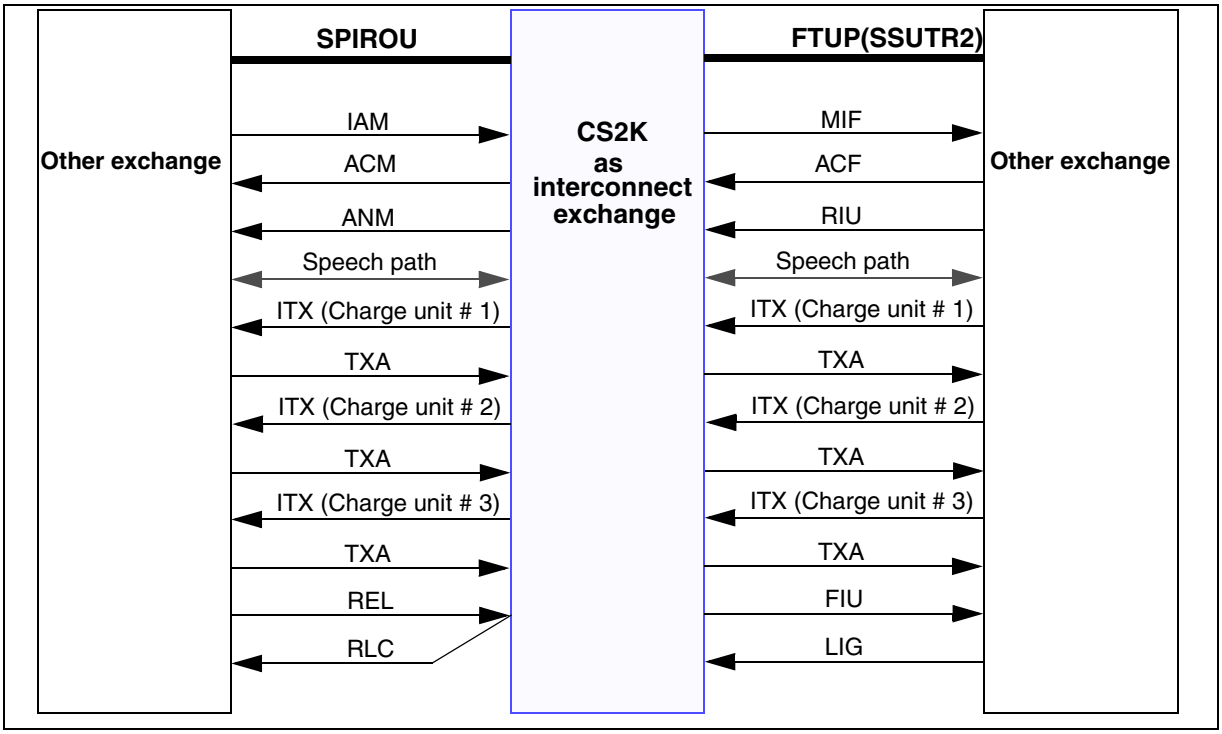


Figure 9 CS2K as interconnect exchange between FTUP(SSUTR2) and SPIROU trunks

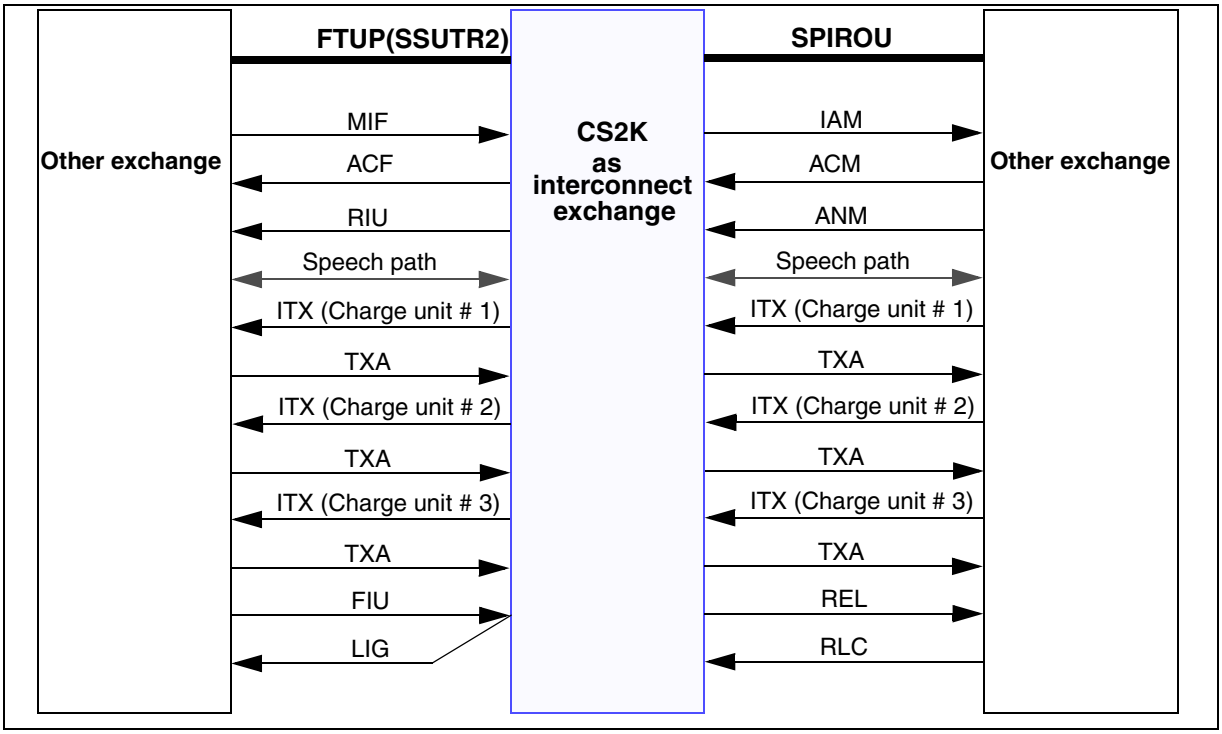


Figure 10 CS2K as interconnect exchange between FTUP(SSUTR2) and FTUP(SSUTR2) trunks

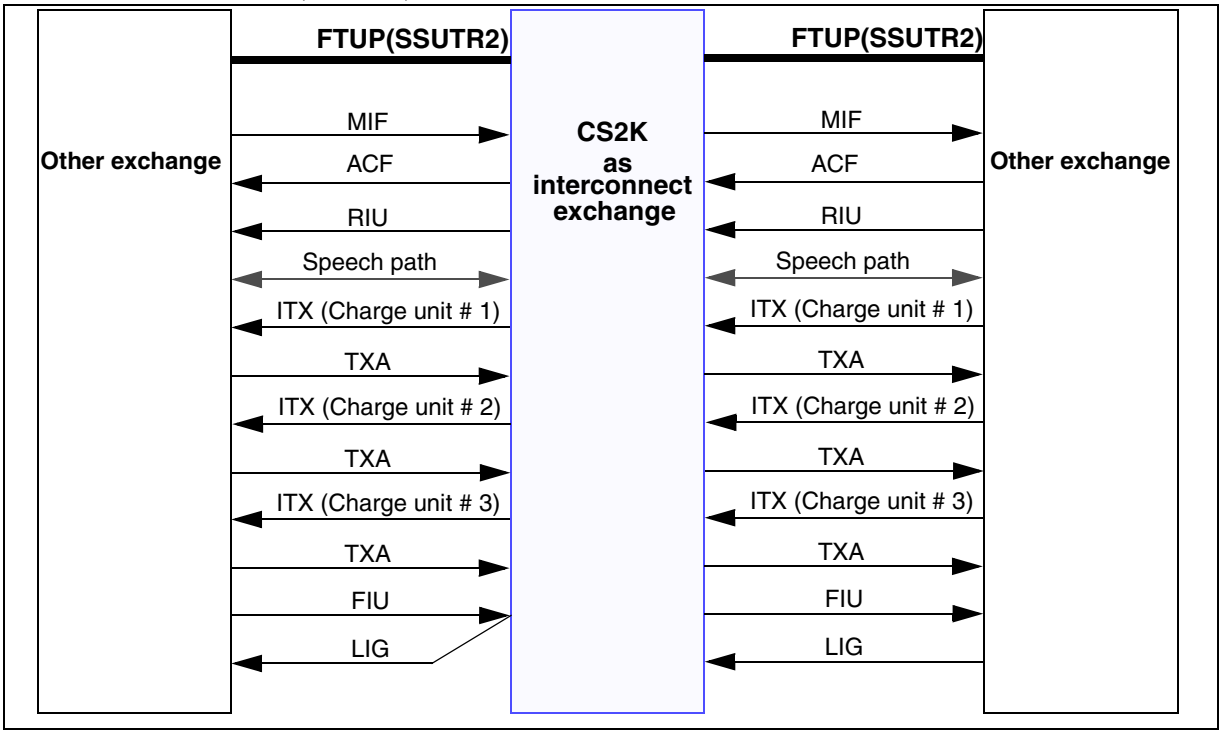


Figure 11, "French NAOC Support on the transit exchange" indicates all supported interworkings for each of the relevant originators, in the French market context. French NAOC is only applicable to SSUTR2(FTUP) and SPIROU trunks hence this feature is only applicable to the interworkings marked blue, other supported interworkings where French NAOC is not applicable are marked yellow. The interworkings with SIP-T trunks are tested for verification. “X” indicates the interworkings where French NAOC and interworkings are being supported with this feature.

Figure 11 French NAOC Support on the transit exchange

Platform	Originator	Terminating agents								
		H323 agents	IBN lines	ETSI PRI	QSIG (95)	ETSI ISUP V1	ETSI ISUP V2/V2+	SIP-T (FTUP and SPIROU)	SSUTR2 (FTUP)	SPIROU
CS2K	SPIROU	N/A						X	X	X[a]
CS2K	SSUTR2 (FTUP)	N/A						X	X	X

a. Already implemented in SN08 with A00006730
X: Supported with this activity(A00009143)

16.2.3.4 Functional Protocol

AOC using functional protocol is supported for the following agents on the originating exchange:

— ETSI PRI

— H323

16.2.3.5 Keypad Protocol

AOC using keypad protocol is supported for the following agents on the originating exchange:

— VN4 PRI

— VN6 PRI

16.2.3.6 Verification for French NAOC Support

The following are verified in this activity:

— French NAOC supports acknowledging the reception of ITX messages received over ***FTUP(SSUTR2)*** via TXA messages for ***VN4 PRI, VN6 PRI***, ***ETSI PRI*** and ***H.323*** originating agents.

— French NAOC supports acknowledging the reception of ITX messages received over ***SPIROU*** via TXA messages for ***VN4 PRI*** and ***VN6 PRI*** originating agents.

— French NAOC feature interaction support with the 2CLI feature.

— French NAOC feature interaction support with the Number Portability feature.

— French NAOC supports by adding processing ITX charge messages received over SIP-T (FTUP) or SIP-T (SPIROU) via TXA messages for the following agents:

— VN4/VN6/ETSI PRI

— H323

16.2.3.7 Nodal AOC Support

A brief overview of the supported agent interworkings is given below. The combinations of supported interworkings are listed in Figure 12, "Nodal AOC Support on the Originating Exchange". Only the agents marked blue and with “X” are being supported. Agents marked yellow and with “V” is verified with this activity.

Figure 12 Nodal AOC Support on the Originating Exchange

Platform	Originator	Terminating agents								
		H323 agents	IBN lines	ETSI PRI	QSIG (95)	ETSI ISUP V1	ETSI ISUP V2/V2+	SIP-T(FTUP and SPIROU)	SSURN2 (FTUP)	SPIROU
CS2K	H323	X[a]							V	
CS2K	ETSI PRI over PVG	X[b]								
CS2K	VN4 PRI over PVG	X								
CS2K	VN6 PRI over PVG	X								

a. Already implemented in SN08 with A00005822
b. Already implemented with A59020791
X: Supported with this activity
V: Verified with this activity

16.3 Hardware Requirements or Dependencies

N/A

16.4 Software Requirements or Dependencies

This activity does not require any additional SOC. The following features are required to be activated by SOC for the originating exchange:

— ***NETK0024*** Network AOC Tariff

— ***NETK0019*** Network AOC

— ***NSUP0020*** NAOC/PCA Supp Svcs

— ***PBXT0011*** ETSI PRI Info

— ***PBXT0018*** QSIG AOC

— ***SULN0011*** AOC on ETSI BRI

16.5 Limitations and restrictions

The current activity does not introduce any new limitations or restrictions except VN4/VN6 restrictions explained in Section 16.5.4.

The restrictions and limitations valid for this activity have been introduced by the previous activities. Please refer to restrictions of these activities AF7344 [35], A59024423 [36], A590038835 [37], A59020791 [33], A00005822 [25], A00006730 [42] about other related restrictions and limitations.

16.5.1 Generic Limitations:

- AOC-S (AOC at call setup) is not supported.
- Provisioning of AOC can only be per trunk group and per GWC. AOC request is always on a per call basis.
- Only connection-oriented charging information is transmitted to the user (charges for supplementary services are not included).
- The calculation of the charging rate time interval can produce a result which is not an exact multiple of 100 ms. The result is therefore rounded up to the next 0.1 sec multiple.
- Interactions with supplementary services other than those specified in the AOC standards will not be handled.
- any ‘aocComplete’ request at Call Transfer will be rejected with a ReturnError APDU with error code ‘supplementaryServiceInteractionNotAllowed’.
- any ‘aocDivChargeReq’ will be ignored but not passed along towards the terminator.

- A conversion factor change does not affect calls in progress; it only affects calls established after the change.
- The design is based on the assumption that AOC will never be delivered by another Call Server located from the Call Server towards the terminating party. Therefore, AOC charge requests can not be passed through the Call Server. Incoming Facility Information Elements (from the terminating side) with operations '***aocInterim***', '***aocFinal***' or '***aocRate***' will be discarded by the GWC and therefore not pass through the CS2000.
- AOC charge requests arriving at the CS2000 after CONNECT are always rejected by the CS2000. This means: no AOC service will be provided for any charge requests received after CONNECT.
- According to the AOC specification it does not make sense to send more than one AOC APDU per message. If an incoming message or Facility IE contains more AOC InvokePDUs, only the first APDU per message is considered. The remaining APDUs are passed through towards the terminating party.
- If an AOC charge request is received in a FACILITY message during the overlap sending phase and before enough digits were received to route, the following situation may lead to failure to provide the service: the reception of the remaining digits necessary to find a route takes longer than 15 seconds. The reason is timer T1 >= 15 seconds running in the originating PINX, waiting for a reply to the request. This timer may time out, because CS2000 can send the reply only when it found the route. As a result, the PINX will report '***notAvailable***' to the user and ignore the AOC information received from CS2000.
- Table ***TRKOPTS***, AOC option, AOCREL = Yes datafill does not have an effect in the following situations (calls are not released):
  - — no AOC service is provisioned, but a request is received. The request is replied with '***notAvailable***' and the call continues. No CS2000 log is generated.
  - — QSIG AOC is provisioned with protocol type KEYPAD or with charging type CHARGING (units). These situations will not even lead to '***notAvailable***' replies, they will lead to GWC Swerrs and CS2000 PM189 logs, and no AOC information being sent out.
- The content of the Interpretation APDU in the AOC requests is not checked by CS2000. But the actions taken (which would depend on it) are always according to the AOC standard.

16.5.2 H323 limitations

- Sending of AOC charge information as currency units is not supported for H.323 trunks yet.

- AOC on H.323 is only supported for bearer calls. AOC on H.323 for non-bearer calls is not supported. Facility IEs with AOC operations for these calls are transparently passed through the CS2K.
- In case no system resources are available in the GWC, a FACILITY message with a Facility IE coded “chargeNotAvailable” is sent towards the originating H.323 gateway.
- Race condition: If a call has AOC-D activated, the originating H.323 gateway might receive a FACILITY message after it sent out a ‘getFinalCharge’ request. This message should not cause an erroneous charge display because it will be received before the RELEASE COMPLETE message with the final charge.
- Basic Service discounts are not supported on H.323 because there is no formal definition of Basic Service for H.323, even though Bearer Capability and High Layer Compatibility are both defined. This means that table AOCBSDSC will not be used by AOC on H.323.
- For calls routed to tones or announcements the charge provided is either ‘freeOfCharge’ or totally missing (which should cause the originating H.323 gateway to report ‘notAvailable’ to the end user).
- A dummy sourceEntityAddress = 0 will be coded in the NFE of outpulsed Facility IEs, because PINX are not supported by QSIG GF.

16.5.3 GWC limitations

- The feature is supported over GWC Warm Swacts. No errors are expected for Swacts with both units InSv. If the inactive unit is RTS’ed and then a Swact happens, there can be errors for the calls that were in talking state at RTS.
- When changes are done in the table ***SERVRINV***, these are not dynamically reported the GWC. After adding the AOC option, the GWC has to be double swacted in order for the changes to take effect
- The SESM interface for table ***SERVRINV*** does not support the AOC option. This option has to be manually added to the table SERVRINV.

16.5.4 VN4/VN6 limitations

- While datafilling table TRKOPTS for VN4/VN6 PRI trunks, only PROTOCOL = KEYPAD datafill is functional. Functional protocol is not supported for these trunk agents.

16.5.5 CM switch activity restrictions

The stable teletaxe service calls remain in the answered state after a CM warm swact or a CM no restart swact (NRS). But a warm/no restart swact will affect the total charge units populated in the billing records.

As the charge units are stored in the history data block (HDB) and since HDB information is not transferred from the active side to the inactive side during the CM swact, the charge units accumulated before the swact will be lost. Hence the billing records generated after the swact will **not** contain the correct charge unit information.

16.5.6 GWC switch activity restrictions

The CS2K is unable to support services over an extended peripheral module (GWC) swact (warm/cold). Given the requirements of the SSUTR2 specification referred to in the ART SPIROU specification (document reference) for backwards Advice of Charge (AOC) handling of error conditions, the following actions occur after GWC swact on an answered call with AOC.

16.5.6.1 Outgoing trunk

The call remains in answered state after an GWC swact has occurred. The inactive unit is not synchronized with the Sequence Number and Last Charge Delta as each ITX message is received. Following an GWC swact, the subsequent received ITX message is **not** verified according to the SSUTR2 specification referred to in the ART SPIROU specification (document reference [40]. Sequence Number and Last Charge Delta are updated **from this ITX message** to provide validation of **further** consecutive ITX messages. Therefore verification of the first ITX message after an GWC swact is ignored. Each following ITX message is verified again.

16.5.6.2 Transit exchange

Transiting of ITX and TXA messages is unaffected by an GWC swact.

16.6 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

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

Accounting (includes AMA billing)_____

Performance (includes operational measurements)_____

16.7 Glossary

Term	Description
AOC	Advice of Charge
CDP	Charge Determination Point
CGP	Charge Generation Point
CS	Carrier Selection
CS2000	Communication Server 2000
CS2K	Communication Server 2000
ETSI	European Telecommunication Standard Institute
IAM	Initial Address Message
IBN	Integrated Business Network
IP	Internet Protocol
ISUP	Integrated Services Digital Network User Part
MMP	Multi Market Platform
NAOC	Network Advice of Charge
PCA	Payment Ceiling Advice
PVG	Passport Voice Gateway
PRI	Primary Rate Interface
SIP	Session Initiation Protocol
SIP-T	Session Initiation Protocol - Telephony
SNP	Service Number Portability
FTUP	French TUP
TUP	Telephone User Part
ITX	Internet Telephony Extender
TXA	Telephone Exchange Acknowledgement
TDM	Time Division Multiplex
OLE	Originating Local Exchange
AMA	Automatic Message Accounting
SPIROU	Signalisation Pour 1’Interconnexion des Rexeaux Ouverts
SSUTR2	Sous System Utilisateur T Reseaux 2

16.8 References

REF #	Description of Reference
[1]	*ETS 300 178 - ISDN; Advice of Charge: charging information at call set-up time supplementary service, Service description, October1992*
[2]	*ETS 300 179 - ISDN; Advice of Charge: charging information during the call supplementary service, Service description, October1992*
[3]	*ETS 300 180 - ISDN; Advice of Charge: charging information at the end of the call supplementary service, Service description, October 1992*
[4]	*ETS 300 182 - ISDN; Advice of Charge supplementary service, DSS-1 protocol, April 1993*
[5]	*ITU-T H.225.0 - Call signalling protocols and media stream packetization for packet-based multimedia communication systems (2000)*
[6]	*ITU-T Q.931 - ISDN user-network interface layer 3 specification for basic call control*
[7]	*ITU-T Q.932 - Generic procedures for the control of ISDN supplementary services*
[8]	*ISO/IEC 11572 / ECMA-142 and ISO/IEC 11574 / ECMA-143 - QSIG Basic Call*
[9]	*ISO/IEC 11582 / ECMA-165 - QSIG Generic functional protocol*
[10]	*ISO/IEC 15049 / ECMA-211 - QSIG Advice of Charge - Specification, Functional Model and Information Flows*
[11]	*ISO/IEC 15050 / ECMA-212 - QSIG Advice of Charge - Interexchange Signalling*
[12]	*ITU-T X.680 Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation (1997)*
[13]	*ITU-T X.681 Information technology - Abstract Syntax Notation One (ASN.1): Information object specification (1997)*
[14]	*ITU-T X.682 Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification (1997)*
[15]	*ITU-T X.683 Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications (1997)*
[16]	*ITU-T X.690 Information technology - ASN.1 encoding rules - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) (1997)*

[17] *ITU-T X.880 Information technology - Remote Operations: Concepts, model and notation (1994)*

[18] *ITU-T X.881 Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) service definition (1994)*

[19] *ITU-T X.882 Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) protocol specification (1994)*

[20] *NDAOCHLD - German ETSI AOC HLD; PLS FMDOC*

[21] *AN1950 - ETSI PRI ADVICE OF CHARGE (WT part); PLS DOC*

[22] *AN1946 - ETSI PRI ADVICE OF CHARGE (XPM part); PLS DOC*

[23] *AE1089 - GLOBAL PRI - PROTOCOL VARIANT CONTROL; PLS DOC*

[24] *AU2537 - PRI REARCH PHASE 1B; PLS DOC*

[25] *A00005822 - AOC over H.323; PLS FMDOC*

[26] *ELO001 - Euro ISDN Advice of Charge SIM; PLS FMDOC*

[27] *ND0035 - AOC for NLOs SIM; PLS FMDOC*

[29] *A59039734 - Eurotrunks Enhancements III (Propagation); PLS FMDOC*

[29] *AJ4901 - ETSI AOC PRI Variants XPM Detailed Design document; PLS DOC*

[30] *AJ4903 - ETSI AOC PRI Variants SHR Detailed Design document; PLS DOC*

[31] *AJ4904 - ETSI AOC PRI Variants CCM Detailed Design document; PLS DOC*

[32] *AJ4905 - ETSI AOC PRI Variants WT Detailed Design document; PLS DOC*

[33] *A59020791 - Support of AOC for ETSI PRI on CS2000; PLS FMDOC*

[34] *A59031474 - NAOC XPM cleanup; PLS FMDOC*

[35] *AF7344 - QSIG Advice Of Charge; PLS DOC*

[36] *A59024423 - QSIG on CS2000; PLS FMDOC*

[37] *A59038835 - QSIG on CS2000 Completion; PLS FMDOC*

[38] *A00002638 - Software Metering Support for Billing; PLS FMDOC*

[39] *A00002625 - Full Line HW Metering / Billing Compliance; PLS FMDOC*

[40] *SPIROU 1998-00n, Edition 1.0.*

[41] *S00002638 - NAOC Metering Framework description; PLS FMDOC*

[42] *A00006730 - French NAOC on Succession CS2K*

[43] *A59020791 - Support of AOC for ETSI PRI on CS2K*

Figure 13 Overview of the NAOC and PCA development

Type	Stream	ACTID	Description of Reference
N A O C	**MMP12**	**59007987**	*ETSI ISUP - Network AOC (CDP+CGP)*, Issue AA25, PLS FMDOC module: *network_aoc_etsi_isup.*
		59008229	*ETSI ISUP - Network AOC Tariff And Time Of Day Switchover (CDP)*, Issue AA67, PLS FMDOC module: *naoc_etsi_isup_tariff_db_tco.*
		59007780	*Network AOC CGP Function*, Issue AA18, PLS FMDOC module: *A59007780.*
	MMP13	**59012308**	*ETSI ISUP Network AOC - analog enhancement,* Issue AA15, PLS FMDOC module *A59012308 (TDM only)*
		59012315	*ETSI ISUP Network AOC - V5.2 enhancement,* Issue AA02, PLS FMDOC module *A59012315*
		59013775	*Network AOC: Integrated CGP and CDP,* Issue AA27, PLS FMDOC module: *A59013775.*
	ISNH03	**59032878**	*NAOC on PRI,* Issue AA05, PLS FMDOC module: *A59032878.*
P C A	**SN04**	**59034497**	*Payment ceiling for Succession Intl. Cable IP,* Issue AA32, PLS FMDOC module: *A59034497.*
	SN05	**59039121**	*NAOC and PCA Feature Interworkings with 3WC, CFx, CXR and HOLD,* Issue AA30, PLS FMDOC module: *A59039121.*
NAOC	**SN06**	**89007454**	*NAOC German Regulatory Enhancements,* Issue AA17, PLS FMDOC module: *A89007454.*
PCA		**89007461**	*Payment Ceiling Regulatory Enhancements,* Issue AA40, PLS FMDOC module: *A89007461.*

NAOC	**SN06.2**	**A00001927**	*Line Hardware Metering,* Issue AA03, PLS FMDOC module: *A00001927.*
		A00002938	*Full Line HW Metering / Billing Compliance*, Issue AA12, PLS FMDOC, module: *A00002625.*
	SN07	**A00002625**	*Full Line HW Metering / Billing Compliance*, Issue AA12, PLS FMDOC, module: *A00002625.*
		A00002637	*NAOC Trunk Metering Enhancements,* Issue AA02, PLS FMDOC module: *A00002637.*
		A00002909	Telekom ISUP (T-ISUP), *Issue AA24, PLS FMDOC module A00002909*
		A00004933	*Indian ISUP Charging, Issue AA02, PLS FMDOC module A00004933*
PCA		**A00002638**	*PCA SW Metering Billing Compliance, Issue AA14, PLS FMDOC module A00002638*
NAOC & PCA		**S00002638**	Software Metering support for Billing, *Issue AA02, PLS FMDOC module S00002638*
NAOC	**SN08**	**A00005822**	AOC over H.323, *Issue AA08, PLS FMDOC module A00005822*
		A00006708	Metering on Israeli ISUP for IDDD calls, *Issue AA10, PLS FMDOC module A00006708*
		A00006730	*French NAOC on Succession CS2K*

Annex A: ITX and TXA Message Formats

SPIROU backward charging messages and parameters are shown in table 1 and 2.

Table 1 ITX message format

Parameter	Type	Value	Length (octets)
Message type	F	#E1	1
Charge unit number	F	Number of charge units	1
Message number	F	Message sequence number	1
End of optional parameters	O	All zeros	1

Table 2 TXA message format

Parameter	Type	Value	Length (octets)
Message type	F	#E2	1
End of optional parameters	O	All zeros	1

FTUP(SSUTR2) backward charging messages and parameters are shown in table 3 and 4.

Table 3 ITX message format

Parameter	Type	Value	Length (octets)
Message header code	F	#40	1
Call charge allocation domain	F	Number of charge units	1
Message number	F	Message sequence number	1

Table 4 TXA message format

Parameter	Type	Value	Length (octets)
Message header code	F	#80	1

ANNEX B: Handling receipt of ITX messages

16.1 CS2K as an originating exchange

This summarizes how ITX messages are handled by the CS2K when it is the originating exchange.

- The first ITX message received for a call must have its message number set to 1.
- The originating CS2K responds with a TXA message to indicate success within 10 seconds after receiving the ITX message.
- The CS2K takes the number of charge units from the Charge unit number parameter and stores it for that call.

- The exchange which has generated the ITX message waits for 15-20 seconds for the TXA acknowledgement. If no TXA is received within that time, it resends the ITX message. If no TXA is received within 60 seconds of the second ITX message, the call is released.
- Subsequent ITX messages must have the message number incremented (up to 255, when it will start from 1 again). If correct, the number of charge units is added to the total for that call and a TXA message is sent in response.
- If the Message number and Charge unit number in an ITX message are identical to those in the previous one, a TXA message is returned and the message is ignored.
- Receipt of ITX messages may continue until the call is released. The arrival rate of ITX messages may vary.
- Once the call is released, an AMA call record will optionally be produced with the total number of charge units received, depending on billing datafill.

16.2 Error handling

When an error occurs during receipt of ITX messages, a billing record is still produced for the call, otherwise this information is lost (and fraud could result). The AMA record will contain an indication that the call was released due to abnormal signalling.

ITX errors are handled as shown in Table 1.

Table 1 Error handling (CS2K as originating exchange)

Error	Action
An ITX is received before both the ACM/ACF and the ANM/RIU.	A reset is implemented on the circuit involved and the call attempt is automatically repeated on another circuit
An ITX is received after the ACM-ACF but before the ANM/RIU.	The ITX is ignored and a PM 189 log is generated.
An ITX is the first ITX received for a call but its Message number is not 1.	The CS2K releases the call and a C7UP 102 log is produced, indicating that the call was released due to abnormal signalling conditions.
An ITX is not the first ITX received for a call, and its Message number is not: • the same as the number of the immediately preceding ITX, or • consecutive to the number of the immediately preceding ITX	

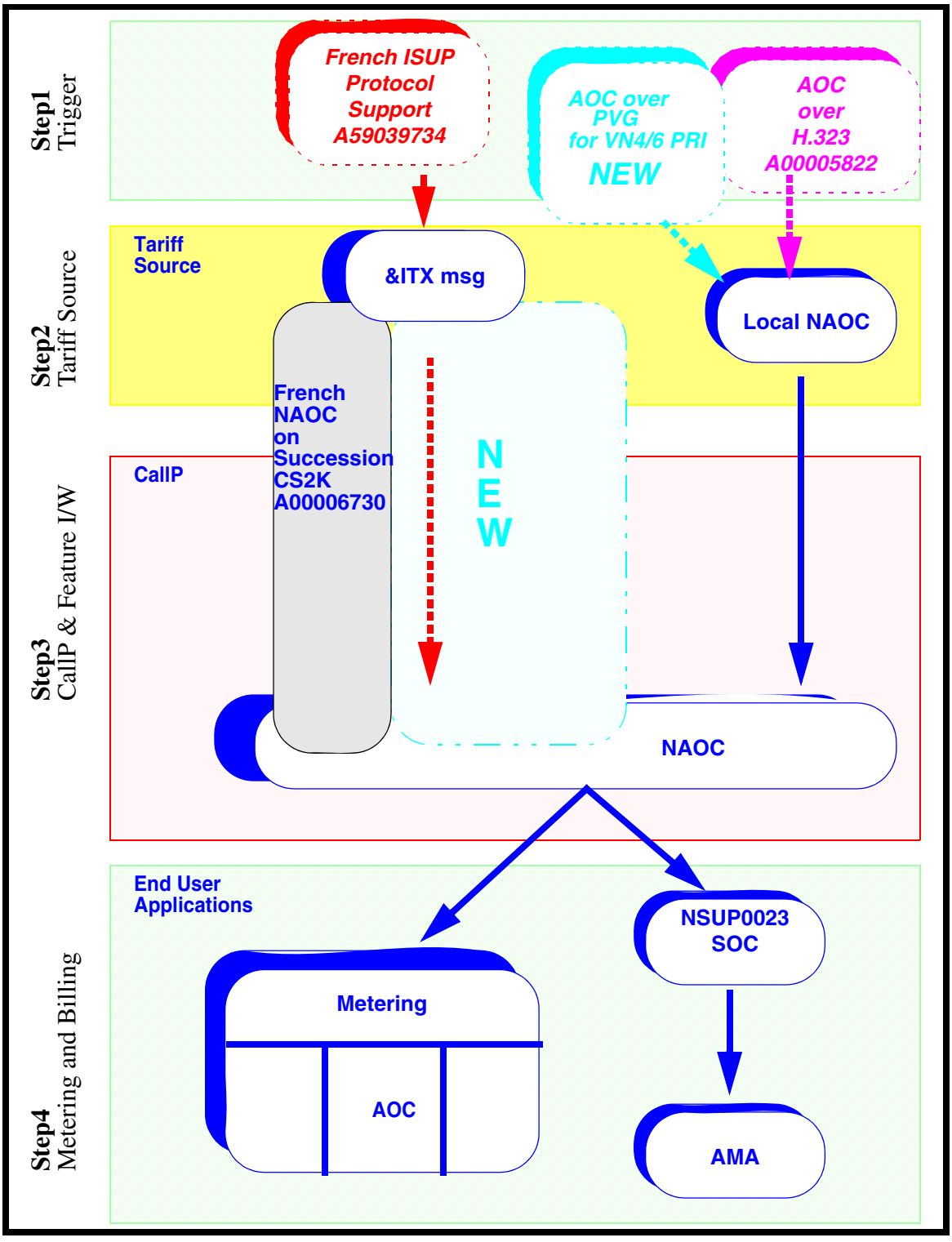
ANNEX C: Current content

The current functionality bridges between the existing features:

- French ISUP support provided on the CS2K by a CSA activity on top of A59013177 and 59034822
- AOC over H.323 (A00005822)
- NAOC metering framework on CS2K (A89007454, 59032878)
- French NAOC on Succession CS2K (A00006730)

See the following Figure 1, "How the new content interacts with existing French NAOC and Nodal AOC feature" for further details.

Figure 1 How the new content interacts with existing French NAOC and Nodal AOC feature



17: Functional Description (FN): A00009145

17.1 Feature name and Feature ID

A00009145: Record Feature Usage

17.2 Description

The purpose of this activity is to provide detailed information about the subscriber action of a service usage at the billing records.

With this activity, developed in ISN09 (MMP22) release, DMS - MMP is capable to give detailed information about the subscriber feature actions as a billing record. By using these billing records, Telco's can charge their customers for their feature usage, if desired.

Feature usage indication is provided for ***Call Lock (ILR), Call Waiting (ICWT), Abbreviated Dialing (SCL), CLIR (SUPPRESS + CNDB), AUL, Do not Disturb (CDND), Directory Number Hunting (DNH)***, and ***Call Wake Up (IWUC)*** upon subscriber actions which are ***activation, deactivation, interrogation,*** and ***customer usage***, where applicable. Crafts person operations via SERVORD are not supported.

This activity is implemented only for IBN lines and provides recording of the feature usage depending on the state of a new AMAOPTS option, which is created by this activity. When this option is ON, a new AMA record is generated and MC611 is appended to this AMA record to indicate the subscriber actions.

When the AMAOPTS option is set to ON and one of the requested features (*) is activated, deactivated, interrogated, or used by the end user, a separate billing record is generated immediately to indicate that user action. This billing record provides the following information within the described fields as below:

- **Feature Subscriber DN:** Stored in the Originating Open Digits 1 field of the Structure Code.
- **Date:** Stored in the Date field of the Structure Code
- **Time:** Stored in the Connect Time field of the Structure Code.
- **Feature Code:** Stored in the Service Identifier field of the module code MC611 context ID 80024
- **Action Type:** Stored in the Service Event field of the module code MC611 context ID 80024.

Note: * stands for the requested set of features which consists of Call Lock (ILR), Call Waiting (ICWT), Abbreviated Dialing (SCL), CLIR (SUPPRESS + CNDB), AUL, Do not Disturb (CDND), Directory Number Hunting (DNH), and Call Wake Up (IWUC).

Feature Subscriber DN represents the IBN line agent which uses the feature actions.

Date is the date at which the feature action is initiated.

Time is the time when the feature action is initiated.

Feature Code is used to represent each feature in the requested set by a feature ID uniquely.

Action Type is used to represent the feature action types which are usage, interrogation, subscriber activation, and subscriber deactivation.

The feature actions; activation, deactivation, interrogation, and usage are not applicable for all of the features in the requested set. A detailed description about which action applies to which feature is given in Table 1 - Feature Requirement List.

Table 1: Feature Requirement List

Feature Name	Feature Option	Act/Deact Billing	Interr. Billing	Feature Usage Billing	For Release
1) Abbreviated Dialing	IBN SCL	Y	Not requested	Y	ISN09
2) Call Waiting	CEPT ICWT	Not requested	Not requested	Y	ISN09
3) Hot Line	IBN AUL	Not requested	Not requested	Y	ISN09
4) Three Way Calling	CEPT I3WC	Not requested	Not requested	Y	Further Releases
5) Call Forwarding Immediately	CEPT CFU	Y	Not requested	Y	Further Releases
6) Call Forwarding on Busy	CEPT CFB	Y	Not requested	Y	Further Releases
7) Call Forwarding on No Answer	CEPT CFD	Y	Not requested	Y	Further Releases
8) Do Not Disturb	CEPT CDND	Y	Not requested	Y	ISN09

Table 1: Feature Requirement List

Feature Name	Feature Option	Act/Deact Billing	Interr. Billing	Feature Usage Billing	For Release
9) Call Wake Up	CEPT IWUC	Y	Not requested	Not requested	ISN09
10) Multiple Line Hunting	IBN DNH	Not requested	Not requested	Y	ISN09
11) Call Lock	CEPT ILR	Y	Not requested	Y	ISN09
12)CLIR/CNDBO	IBN SUPPRESS + CNDBO+CND	Not requested	Not requested	Y	Further Releases
Centrex Features					
CLIR	IBN SUPPRESS + CNDB	Not requested	Not requested	Y	ISN09
Call Transfer (CXR)	IBN CXR	Not requested	Not requested	Y	Further Releases
Call Hold Send the Music	IBN CHD	Not requested	Not requested	Y	Further Releases

17.2.1 Background

17.2.1.1 Existing AMA Record and MC611 Components Used in This Feature

In the existing billing framework, an AMA record consists of a base Structure Code and optional Module Codes containing specific information relevant to the call. If any information is necessary in addition to that contained in a base structure, this information is appended to the base structure in the form of module codes. (For detailed information about Structure Codes and Module Codes please refer to the NTP documents 297-1001-830 and 297-9051-800.)

In this implementation, feature actions are recorded in the form of AMA billing records. The Feature Subscriber DN, Date, and Time info related to the feature action are stored in the base structure of the record. Whereas, Feature Code and Action Type are stored in MC611 with CCI_80024 and this module code is appended to the structure code. The fields of MC611 with CCI_80024 and an example structure code can be seen in Table 2 and Table 3.

Table 2: Structure Code 00514

Information	Number of BCD Characters
Record Descriptor Word	8
Hexadecimal Identifier	2
Structure Code	6
Call Type Code	4
Sensor Type	4
Sensor Identification	8
Recording Office Type	4
Recording Office Identification	8
Date	6
Timing Indicator	6
Study Indicator	8
Called Party Off-Hook	2
Service Observed, traffic sampled	2
Operator Action	2
Service Feature	4
Connect Time	8
Elapsed Time	10
Significant Digits in Next Field	4
Originating Open Digits 1	12
Originating Open Digits 2	10
Originating Charge Information	4
Domestic/International Indicator	4
Significant Digits in Next Field	4
Ext terminating open digits 1	12
Ext terminating open digits 2	10
Completion Indicator	4
Module Code	

Table 3: MC611 with CCI_80024

BCD character	Meaning
1 - 12	Service Identifier Up to 6 EBCDIC characters
13 - 14	Service Event 00 = Unidentified 01 = Provisioning of service to line 02 = Removal of service from line 03 = Administration Programming 04 = Subscriber Programming 05 = Interrogation of Service 06 = Usage of service 07 = Subscriber Activation of Service 08 = Administration Activation of Service 09 = Subscriber Deactivation of Service 10 = Administration Deactivation of Service
15	Not used
16	Sign (hex C)

MC611 with context identifier 80024 is the SUSB context and it is already used in MMP to provide Subscriber Usage Sensitive Billing. For instance, when the SOC option RBIL0005 and the SUSP option in Table AMAOPTS are ON, a billing record with MC611 is generated upon end user's activation of the SACB feature. SOC RBIL0005 must be ON to be able to use SUSB billing.

In this activity, a new AMAOPTS option named MC611_FOR_RFU (where RFU stands for **R**ecord **F**eature **U**sage) is created to control the recording of feature actions. Subscribers' feature actions are recorded only if the MC611_FOR_RFU option is set to ON. A brand new billing record is generated after the feature action is initiated. The Feature Subscriber DN, Date, and Time info are put in the Originating Open Digits 1, Date, and Connect Time fields of this record, respectively. After that, module code MC611 with CCI_80024 is generated. Feature Code and Action Type are put in the Service Identifier and Service Event fields of the MC611 and it is appended to the just created Structure Code.

In Figure 1, an example billing record with MC611 can be seen, which is created for the usage of the AUL.

Figure 1 Example view of the record taken with the CALLDUMP FULL command

```
>calldump ama full

*
HEX ID:                    AA
STRUCTURE CODE:                40514C
CALL CODE:                   006C      STATION PAID
SENSOR TYPE:                 036C      DMS 100F
SENSOR ID:                  0000000C
REC OFFICE TYPE:             036C      DMS 100F
REC OFFICE ID:              0000000C
DATE:                      50317C    MARCH 17, 2005
TIMING IND:
   TIMING GUARD FLAG           0       UNUSED
   SHORT CLD PARTY OFF-HOOK IND   0       UNUSED
   LONG DUR/SERV PTY CAPABILITY IND 0       UNUSED
   UNUSED                   0
   UNUSED                   0C
STUDY IND:
   STUDY TYPE A             0       UNUSED
   STUDY TYPE B             2       NETWORK COMPLETION
   STUDY TYPE C             0       UNUSED
   TEST CALL IND            0       UNUSED
   UNUSED                   0
   ORIG/TERM NANP NUM IND       0       UNUSED
   OPERATOR SERV IND          0C      UNUSED
CLD PTY OFF-HK:              0C      CLD OFF-HOOK DETECTED
SERVICE OBSERVED:            0C      NONE
OPER ACTION:                 0C      ANI, CUSTOMER DIALED CALL
SERVICE FEATURE:            000C     OTHER
SIG DIGITS NEXT FIELD:       010C
ORIG OPEN DIGITS 1:          01027835406C
ORIG OPEN DIGITS 2:         FFFFFFFFFF
ORIGINATING CHARGE INFO:     FFFF
DOMESTIC/INTL INDICATOR:     9C      UNKNOWN
SIG DIGITS NEXT FIELD:       000C
EXT TERM OPEN DIGITS 1:      000000000000000C
EXT TERM OPEN DIGITS 2:      FFFFFFFFFFFFFFFF
CONNECT TIME:               1105378C   11:05:37.8
ELAPSED TIME:              000000000C 000000:00.0
COMPLETION INDICATOR:        001C     COMPLETED: ANSWERED
MODULE CODE:                611C     GENERIC MOD: ONE DGT STR FMT
GENERIC CONTEXT ID:
   PARSE RULES              80024    UNKNOWN
   SIGNIFICANT DIGITS        00C     NIL
GENERIC DIGIT STRING ONE:       81A493000000060C
MODULE CODE:                000C     FINAL MODULE
```

In this figure, Generic Digit String One is interpreted as below:

81A493000000060C

- First twelve characters serve as the Service Identifier
  "81" = a, "A4" = u, "93" = l ---> AUL
- The remaining six characters of the first twelve are represented with zeroes, since there are only three letters in the feature acronym.
- The next two characters, "06", represent the service event, which is usage here.

Generic Digit Strings for the features included in the requested set can be seen in Table 4.

Table 4: Generic Digit Strings

Feature	Service Identifier
AUL	81A493000000**XX**C
CDND	838495840000**XX**C
CNDB	839584820000**XX**C
DNH	849588000000**XX**C
ICWT	8983A6A30000**XX**C
ILR	899399000000**XX**C
IWUC	89A6A4830000**XX**C
SCL	A28393000000**XX**C
SUPPRESS	A2A497979985**XX**C

Note: The XX in the Digit String can be 1- 04 for Subscriber Programming, 2- 05 for interrogation, 3- 06 for usage, 4- 07 for Subscriber Activation, 5- 09 for Subscriber Deactivation as shown in Table 3.

17.2.2 Provisioning for Feature Recording

17.2.2.1 Office Wide Parameters:

1. To enable feature recording, the AMAOPTS option MC611_FOR_RFU, created by this activity to make feature recording optional, is set to ON.
2. To disable feature recording, MC611_FOR_RFU is set to OFF.

Figure 2 Provisioning of the new AMAOPTS option MC611_FOR_RFU

```
> Table AMAOPTS

OPTION SCHEDULE
---------------
MC611_FOR_RFU ON
>
```

17.2.2.2 Software Optionality Control

No new Software Optionality Control is created by this activity.

This activity implements a SUSB like recording of feature actions. SUSB can be summarized as DMS's ability to create a billing record per use of a feature action. The features can be billed based on activation, programming, deactivation, or usage. Module code 611 is appended to some of the structure codes during pay per use billing. It uses the context identifier 80024 which has been approved by Bellcore. The existing SOC option RBIL0005 - Subscriber Usage Sensitive Billing must be ON to generate SUSB records.

17.3 Hardware Requirements or Dependencies

No new customer hardware requirements or dependencies are introduced in this feature.

17.4 Software Requirements or Dependencies

This feature uses the existing AMA/Billing framework and the existing components of this framework.

17.5 Limitations and Restrictions

- This activity is implemented for the requested set of features described in Section 2.2 only. Subscriber actions that are not compatible with these features are not supported.
- The functionality provided by this activity applies to IBN lines only.
- Crafts person actions via SERVORD are not recorded. A feature action is recorded only if it is initiated by the subscriber.
- A feature action is recorded only if it is applicable to the related feature. Applicability of actions to features can be seen in Table 1.
- In order to record a feature action in a billing record:
  - — all the datafill described in Section 2.2.2 must be performed

— the feature must be contained in the required set of features

- All limitations which apply to features in the existing implementation (e.g. feature compatibility, precedence, etc.) apply to this activity, as well.
- All features are activated/deactivated/programmed according to CEPT rules (for non CEPT features CEPTONCENTREX is datafilled in Table ISERVOPT).
- Subscriber feature actions are not recorded if the related feature is not assigned to the line or if it is not a default feature (i.e. trying to activate/ deactivate/use a feature even if it does not exist on the line)
- A subscriber feature action is recorded only if it results in success:
  - — If a feature subscriber wants to activate a feature which is not compatible with one or more features already assigned to the line and that is why the activation action is not successfully ended, this action is not recorded.
  - — If a feature subscriber tries to activate an already active feature or deactivate an already inactive feature, this action is not recorded.
- ICWT usage is recorded only if the ICWT subscriber puts in hold or disconnects the active agent and accepts the new calling agent after he gets the ICWT tone.
- The pilot DN is written into the Originating Open Digits1 for DNH usage.
- SUPPRESS usage is recorded only if the SUPPRESS_DN field is ‘Y’ (SUPPRESS_DN is given through SERVORD action during feature assignment and can be checked via QDN command).
  - — If the state of SUPPRESS is toggled using CNDB (i.e. SUPPRESS_DN becomes ‘N’) for a specific call, CNDB usage is recorded as feature action. SUPPRESS usage is not recorded for that case.
  - — If SUPPRESS is not assigned to the line or SUPPRESS_DN field is set to ‘N’ and CNDB is used for a specific call, CNDB usage is recorded as feature action.

17.6 Interactions

- If a user originated feature action is perceived, this action is recorded in a billing record.
- AMA in MMP is based on Bellcore AMA Format. This feature uses the existing AMA/Billing framework components with no change in their existing structures to realize customer’s requirements. So, there is no effect on the existing AMA subsystem in the MMP load.

17.7 Applicable customer facing sections

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

17.8 Glossary

Term	Description
AMA	Automatic Message Accounting
AUL	Automatic Line
CCI	Call Code Index
CDND	CEPT Do not Disturb
CEPT	Conference of European Posts and Telecommunications Administration
CLIR	Calling Line Identification Restriction
CNDB	Calling Number Delivery Blocking
DIRP	Device Independent Recording Package
DMS	Digital Multiplex System
DNH	Directory Number Hunting
FPE	Feature Processing Environment
ICWT	International Call Waiting
ILR	International Line Restriction
IWUC	International Wake Up Call

Term	Description
MCI	Module Code Index
MMP	Multi Market Product
SCI	Structure Code Index
SCL	Speed Calling Long
SOC	Software Optionality Control
Telco	Telecom Company

17.9 Recommended Reading/References

a. NTP 297-9051-800 ‘DMS100 MMP AMA Reference Guide’

b. NTP 297-1001-830 ‘Bellcore Format Automatic Message Accounting Message Guide’

c. NTP 297-9051-855 Office Parameters Volume 1 0f 3 (OFCENG)

d. 297-9051-351 Data Schema Reference Manual Volume 8 0f 12

18: Functional Description (FN): A00009158

18.1 Feature name and Feature ID

A00009158: M3UA over SCTP from Core to USP

18.2 Description

This activity implements M3UA RFC and SCTP RFC on CS2K core, supporting the following M3UA path type to USP.

- M3UA RFC over SCTP RFC client
- M3UA RFC over SCTP RFC server

This activity introduced changes on CS2K core but makes no changes to GWC platform.

This activity is based on the following specification on M3UA and RFC.

- RFC3332 Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA), September 2002
- M3UA Implementor's Guide, V7, February, 2004
- RFC2960 Stream Control Transmission Protocol, October 2000
- Stream Control Transmission Protocol (SCTP) Implementer's Guide, V12, October 15, 2004

Basically, without special mention, RFC2960 in this doc refers to the SCTP RFC2960 and SCTP Implementer’s Guide V12. RFC3332 in this doc refers to the M3UA RFC3332 and M3UA Implementor's Guide V7.

18.3 Support SCTP RFC on CS2K core

Activity A59023997 and A00003649 has implemented SCTP V5 [reference 6] on CS2K core. This activity will enhance the SCTP implementation based on SCTP RFC2960 [reference 3] and SCTP Implementer’s Guide V12 [reference 4].

18.3.1 SCTP chunk common header

In RFC2960, SCTP chunk common header is same as in SCTP V5. No change is introduced in this activity. Please refer to the following table for SCTP chunk common header format.

Table 5 SCTP chunk Common Header Format

Parameter	Type	Length(Octet)
Source Port Number	Mandatory	2
Destination Port Number	Mandatory	2
Verification Tag	Mandatory	4
Checksum	Mandatory	4

18.3.2 SCTP RFC chunks

This activity changes the following existing chunks to comply SCTP RFC version, please refer to section 2.3.3 for more details.

- SACK
- ABORT
- ERROR

This activity also adds a new chunk SHUTDOWN COMPLETE according to specification in RFC2960.

Other chunks are unchanged.

Table 1 shows the SCTP chunks supported by CS2K core. New and changed chunks are marked in BOLD.

Table 6 SCTP RFC chunks Supported by CS2K core

chunk Type	Value	chunk Explanation
DATA	0x0000	Payload Data
INIT	0x0001	Initiation
INIT ACK	0x0002	Initiation Acknowledgement
SACK	**0x0003**	**Selective Acknowledgement**
HEARTBEAT	0x0004	Heartbeat Request

Table 6 SCTP RFC chunks Supported by CS2K core

chunk Type	Value	chunk Explanation
HEARTBEAT ACK	0x0005	Heartbeat Acknowledgement
ABORT	**0x0006**	**Abort**
SHUTDOWN	0x0007	Shutdown Association
SHUTDOWN ACK	0x0008	Shutdown Acknowledgement
ERROR	**0x0009**	**Operation Error**
COOKIE ECHO	0x000A	State Cookie
COOKIE ACK	0x000B	Cookie Acknowledgement
SHUTDOWN COMPLETE	**0x000C**	**Shutdown Complete**

18.3.3 New and changed chunks

18.3.3.1 Selective Acknowledgement (SACK)

The chunk format of SACK is changed as below. Changed field is in BOLD.

Parameter	Type	Length(Octet)
Chunk Type	Mandatory	1
Chunk Flag	Mandatory	1
Chunk Length	Mandatory	2
Cumulative TSN Ack	Mandatory	4
Advertised Receiver Win-dow Credit	Mandatory	4
Number of Gap Ack Blocks	Mandatory	2
Number of Duplicate TSNs	**Mandatory**	**2**
Gap Ack Block #1 - #N	Mandatory	n*4
Duplicate TSN 1-N	**Mandatory**	**n*4**

Two fields are introduced to this activity:

Number of Duplicate TSNs(16 bits): This field contains the number of duplicate TSNs the endpoint has received.

Duplicate TSN(32 bits): Every time a duplicate TSN is received before sending the SACK, it is added to the list of duplicates and appended to the end of the SACK. That is to say, if it is received n times(n>=1) before sending the SACK, it will be appended n-1 times. if it is received n times(n>=1) after sending the SACK for the TSN, it will be appended to SACK for current TSN n timers. The duplicate count is re-initialized to zero after sending each SACK.

18.3.3.2 Abort Association (ABORT)

The format of ABORT chunk is changed as below.

Parameter	Type	Length(Octet)
Chunk Type	Mandatory	1
Chunk Flag	**Mandatory**	**reserved (7 bits)** **T bit (1 bit)**
Chunk Length	Mandatory	2
zero or more Error Causes	Mandatory	4

When an endpoint is to close the association, ABORT chunk is sent with error causes.

The T bit is set to 0 if the sender filled in the Verification Tag expected by the peer. If the Verification Tag is reflected the T bit MUST be set to 1. Reflecting means that the sent Verification Tag is the same as the received one.

Please refer to section 2.3.3.3 for supported error codes on CS2K core.

18.3.3.3 Operation Error (ERROR)

An endpoint sends this chunk to its peer endpoint to notify it of certain error conditions. It contains one or more error causes. An Operation Error is not considered fatal in and of itself, but may be used with an ABORT chunk to report a fatal condition.

The below table shows the Cause Codes used in ERROR chunk, newly introduced Cause Codes are show in BOLD.

Cause Code	Cause	parameter of the Cause-specific Information	Description
1	Invalid Stream Identifier	Stream Identifier(16 bits) reserved (16 bits)	
2	Missing Mandatory Parameter	Number of missing parameters(32 bits) missing parameter type(16 bit)	
3	Stale Cookie Error	Measure of Staleness(32 bits)	
4	Out of Resource	None	
5	**Unresolvable Address**	**Unresolvable Address(32 bits)**	**Contains: complete Type, Length and Value of the address parameter. Indicates: the sender is not able to resolve the specified address parameter(e.g ,invalid transport address)**
6	**Unrecognized Chunk Type**	**Unrecognized Chunk(32 bits)**	**Contains: complete with Chunk Type, Chunk Flags and Chunk Length Indicates: the receiver does not understand the chunk (didn’t defined)and the upper bits of the 'Chunk Type' are set to 01 or 11**
7	**Invalid Mandatory Parameter**	**None**	**Indicates: one of the mandatory parameters is set to a invalid value**
8	**Unrecognized Parameters**	**Unrecognized Parameters(32 bits)**	**Contains: contains unrecognized parameters copied from the INIT ACK chunk complete with TLV Indicates: returned to the originator of the INIT ACK chunk if the receiver does not recognize one or more Optional TLV parameters in the INITACK chunk.**

9	**No User Data**	**TSN value (32 bits)**	**Contains: the TSN of the DATA chunk received with no user data field** **Indicates: returned to the originator of a DATA chunk if a received DATA chunk has no user data**
10	**Cookie Received While Shutting Down**	**None**	**Indicates: A COOKIE ECHO was received while the endpoint was in SHUTDOWN-ACK-SENT state**
11	**Restart of an association with new addresses**	**New Address TLVs**	**Indicates: An INIT was received on an existing association. But the INIT added addresses to the association that were previously NOT part of the association. The New addresses are listed in the erro code.**
12	**User Initiated Abort**	**Upper Layer Abort Reason**	**Indicates: Upper Layer Abort Reason**
13	**Protocol Violation**	**Additional Information**	

18.3.3.4 Shutdown Complete (SHUTDOWN COMPLETE)

SHUTDOWN COMPLETE chunk is required to sent on reception of SHUTDOWN ACK at the completion of the shutdown process in SCTP RFC version. This activity introduced this new chunk type and supports related shutdown procedures.

The chunk format of new chunk SHUTDOWN COMPLETE is as below:

Parameter	Type	Length(Octet)
Chunk Type	**Mandatory**	**2**
Chunk Flag	**Mandatory**	**Reserved(7 bits)** **T bit (1 bit)**
Chunk Length	Mandatory	2

The T bit is set to 0 if the sender filled in the Verification Tag expected by the peer. If the Verification Tag is reflected the T bit MUST be set to 1. Reflecting means that the sent Verification Tag is the same as the received one.

18.3.4 Enhanced SCTP procedures

18.3.4.1 Normal Establishment of an Association

Association establishment procedures are modified to in RFC2960 section 5.1 comparing to SCTP v5. This activity enhances the existing SCTP implementation based on the specification in RFC2960 section 5.1.

18.3.4.2 Handle Duplicate or unexpected INIT, INIT ACK, COOKIE ECHO, and COOKIE ACK

New procedures are introduced to handle duplicate or unexpected INIT, INIT ACK, COOKIE ECHO, and COOKIE ACK in RFC2960 section 5.2. This activity enhances the existing SCTP implementation based on the specification in RFC2960 section 5.2.

The following scenarios are handled in this activity.

- Handle Duplicate INIT in COOKIE-WAIT or COOKIE-ECHOED States
- Unexpected INIT in States Other than CLOSED, COOKIE-ECHOED, COOKIE-WAIT and SHUTDOWN-ACK-SENT
- Unexpected INIT ACK
- Handle a COOKIE ECHO when a TCB exists
- Handle Duplicate COOKIE ACK

18.3.4.3 Path Verification

RFC2960 section 5.4 Path verification procedure is introduced to ensure all the address presented by the peer are in the fact belonging to the peer in SCTP implementor’s guide V12. This activity enhances the existing SCTP implementation based on RFC2960 section 5.4.

18.3.4.4 User Data Transfer

User data transfer procedures are modified to enhance user data transfer reliability in RFC2960 section 6 comparing to SCTP V5. This activity enhances the existing SCTP implementation based on RFC2960 section 6.

18.3.4.5 Congestion Control

Congestion control procedures are modified in RFC2960 section 7 comparing to SCTP v5. This activity enhances the existing SCTP implementation based on RFC2960 section 7.

18.3.4.6 Fault Management

Fault management procedures are modified in RFC2960 section 8 comparing to SCTP v5. This activity enhances the existing SCTP implementation based on RFC2960 section 8.

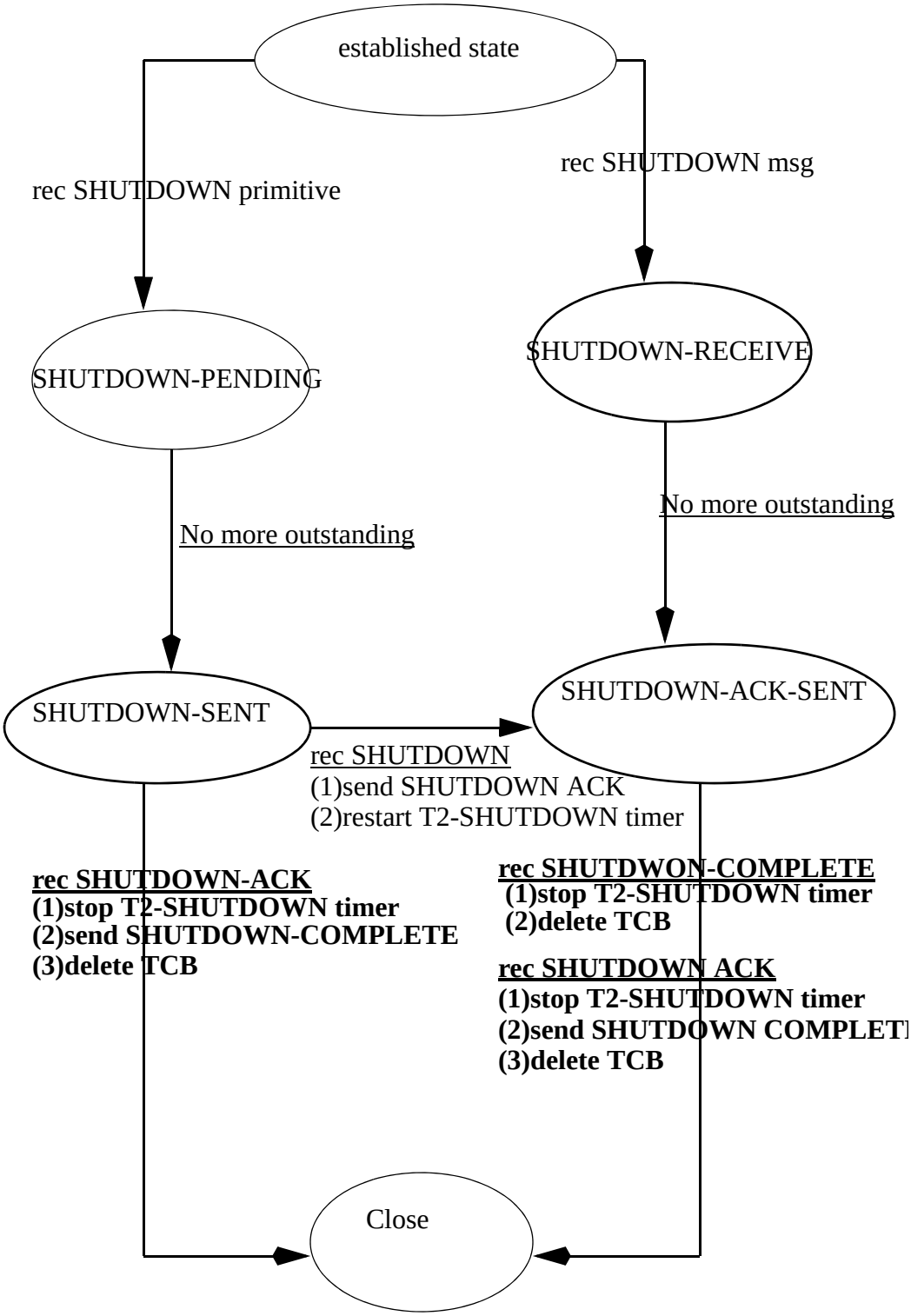
18.3.4.7 Abort of an Association

Association abort procedures are modified in RFC2960 section 9.1 comparing to SCTp V5. This activity enhances the existing SCTP implementation based on RFC2960 section 9.1.

18.3.4.8 Shutdown of an Association

SCTP RFC version has introduced new procedures to the termination of association (RFC2960 section 9.2). Please refer to figure 1 for the new procedure supported on CS2K core. The changes are marked in BOLD.

Figure 1 SCTP state diagram: termination of association


established state
rec SHUTDOWN primitive
rec SHUTDOWN msg
SHUTDOWN-PENDING
SHUTDOWN-RECEIVE
No more outstanding
No more outstanding
SHUTDOWN-SENT
SHUTDOWN-ACK-SENT
rec SHUTDOWN
(1)send SHUTDOWN ACK
(2)restart T2-SHUTDOWN timer
rec SHUTDOWN-ACK
(1)stop T2-SHUTDOWN timer
(2)send SHUTDOWN-COMPLETE
(3)delete TCB
rec SHUTDWON-COMPLETE
(1)stop T2-SHUTDOWN timer
(2)delete TCB
rec SHUTDOWN ACK
(1)stop T2-SHUTDOWN timer
(2)send SHUTDOWN COMPLETE
(3)delete TCB
Close

18.4 Support M3UA RFC on CS2K core

18.4.1 M3UA paths datafill

A new field PROTOCOL is added to table USPPATHS, to allow user to select the protocol of the path. The new field will have following 3 values:

- M3UA_V2_UDP - M3UA V2 over UDP
- M3UA_RFC_SCTP_CLIENT - M3UA RFC over SCTP CLIENT
- M3UA_RFC_SCTP_SERVER - M3UA RFC over SCTP SERVER

Normally, paths in the same pathset **SHOULD** be the same type. Warning message is displayed if customer try to datafill different path type in the pathset. But in-service cutover from M3UA V2 paths to M3UA RFC paths in one pathset is supported and Opposite cutover from M3UA RFC paths to M3UA V2 paths is not supported.

Please refer to section 2.4.11 and 2.4.12 for cutover and rollback procedures for M3UA V2 pathset to M3UA SCTP pathset.

The total message rate of all M3UA RFC paths over SCTP **SHOULD** be less than the max message rate that SCTP on core can support. Currently the max message rate that SCTP can support is 4500 msg/sec. Please refer to sction 2.4.10 and activity A00003649 “SCTP (Stream Control Transmission Protocol) Enhancements on XA-Core” for more detail.

One pathset on the CS2K core is configured as an ASP. IPSP configuration is not supported.

Please refer to figure 2 for datafill example of paths to USP.

Figure 2 Datafill example of M3UA paths to USP on CS2K core

Datafill for path to USP (M3UA V2 over UDP)
table usppaths
PATHNAME SRCPORT DESTIP DESTPORT PATHSEL **PATHPROT**
---
pathset_to_usp 0 4697 192 168 10 42 2905 0 **M3UA_V2_UDP**

Datafill for path to USP (M3UA RFC over SCTP client)
table usppaths
PATHNAME SRCPORT DESTIP DESTPORT PATHSEL **PATHPROT**
---
pathset_to_usp 0 4697 192 168 10 42 2905 0 **M3UA_RFC_SCTP_CLIENT**

Datafill for path to USP (M3UA RFC over SCTP server)
table pathset
PATHNAME SRCPORT DESTIP DESTPORT PATHSEL **PATHPROT**
---
pathset_to_usp 0 4697 192 168 10 42 2905 0 **M3UA_RFC_SCTP_SERVER**

As M3UA V2 path, the valid port number for M3UA RFC path is from 4697-4700 and 4710- 4721.

18.4.2 RFC M3UA message common header

Table 7: RFC M3UA message common header format

Field	Length (byte)	Description
Version	1 byte	it is set to 0x01, indicating M3UA release 1.0
Reserved	1 byte	it is set to 0x00
Message Group	1 byte	Refer to 2.4.3
Message Type	1 byte	Refer to 2.4.3
Message Length	4 byte	The Message Length defines the length of the message in octets, including the Common Header.

If version is not “0x01”, an ERROR message with error code “0x0001” is sent to USP.

18.4.3 RFC M3UA messages

"Table 4 M3UA RFC messages supported by CS2K" represents the set of messages that are required by M3UA RFC.

Table 8: RFC M3UA messages supported by CS2K

Message	Message Class and message type	Description
ERROR	0x0000	Error
NTFY	0x0001	Notify
DATA	0x0101	Payload data
DUNA	0x0201	Destination Unavailable
DAVA	0x0202	Destination Available
DAUD	0x0203	Destination State Audit
SCON	0x0204	Signalling Congestion
DUPU	0x0205	Destination User Part Unavailable
DRST	0x0206	Destination Restricted
ASPUP	0x0301	ASP Up
ASPDN	0x0302	ASP Down
ASPUP ACK	0x0304	ASP Up Acknowledgement
ASPDN ACK	0x0305	ASP Down Acknowledgement
ASPAC	0x0401	ASP Active
ASPIA	0x0402	ASP Inactive
ASPAC ACK	0x0403	ASP Active Acknowledgement
ASPIA ACK	0x0404	ASP Inactive Acknowledgement

If unsupported message class is received, ERROR message with error code 0x0003 is sent to USP.

If unsupported message type is received, ERROR message with error code 0x0004 is sent to USP.

Note: Since M3UA RFC is transported over SCTP, Heartbeat and Heartbeat ACK messages are not supported. SCTP has its own heartbeat mechanism to

detect loss of transport associations, Thus heartbeat procedure is not required when M3UA is transported over SCTP.

18.4.4 RFC M3UA Parameters

"Table 5 M3UA RFC parameters supported by CS2K" represents the set of parameters that are required by RFC M3UA.

Table 9: RFC M3UA parameters supported by CS2K

Parameter	Parameter Id	Description
Traffic Mode Type	0x000b	Supported in ASP ACTIVE
Error Code	0x000c	Supported in ERROR
Status	0x000d	Supported in SCON
Affected Point Code	0x0012	Supported in DAVA, DUNA, DAUD, DRST, DUPU
Network Appearance	0x0200	Supported in SSNM messages and DATA message.
User/Cause	0x0204	Supported in DUPU
Congestion Indications	0x0205	Supported in SCON
Protocol Data	0x0210	Supported in DATA

When an optional parameter is received and not supported, the message is processed but the optional parameter is discarded silently.

18.4.5 RFC M3UA message format

18.4.5.1 ASPSM messages

No optional parameter is supported in the following messages.

ASP UP

ASP DOWN

ASP UP ACK

ASP DOWN ACK

18.4.5.2 ASPTM messages

The message format of ASP ACTIVE is as below:

Parameter	Type	Length (byte)
Traffic Mode Type	Optional	Tag(2 bytes) Length(2 bytes) Traffic Mode Type (4 bytes) 0x0001 - Override

If unsupported traffic mode type is received, ERROR message is sent to peer.

No optional message is supported in the following message.

ASP INACTIVE

ASP ACTIVE ACK

ASP INACTIVE ACK

18.4.5.3 SSNM messages

Message format for DAVA, DUNV, DRST and DAUD is as below.

Parameter	Type	Fields
Network Appearance	Optional	Tag(2 bytes) Length(2 bytes) Value(4 bytes)
Affected Point Code	Mandatory	Tag(2 bytes) Length(2 bytes) Mask 1 (1 bytes) Affected PC 1 (3 bytes) ..... Mask n (1 bytes) Affected PC n (3 bytes)

Message format for SCON is as below:

Parameter	Type	Fields
Network Appearance	Optional	Tag(2 bytes) Length(2 bytes) Value(4 bytes)

Affected Point Code	Mandatory	Tag(2 bytes) Length(2 bytes) Mask 1 (1 byte) Affected PC 1 (3 bytes) ..... Mask n (1 byte) Affected PC n (3 bytes)
Congestion Indications	Optional	Tag (2 bytes) Length (2 bytes) Reserved (3 bytes) Cong Level (1 byte)

Message format for DUPU is as below.

Parameter	Type	Fields
Network Appearance	Optional	Tag(2 bytes) Length(2 bytes) Value(4 bytes)
Affected Point Code	Mandatory	Tag(2 bytes) Length(2 bytes) Mask 1 (1 byte) Affected PC 1 (3 bytes) ..... Mask n (1 byte) Affected PC n (3 bytes)
User/Cause	Mandatory	Tag (2 bytes) Length (2 bytes) Cause (2 bytes) User (2 bytes)

18.4.5.4 DATA message

Message format for DATA is as below.

Parameter	Type	Fields
Network Appearance	Optional	Tag(2 bytes) Length(2 bytes) Value(4 bytes)

Protocol Data	Mandatory	Tag(2 bytes) Length(2 bytes) Protocol Data (variable length)

18.4.5.5 Error Message

Message format for Error is as below.

Parameter	Type	Fields
Error Code	Mandatory	Tag (2 bytes) Length (2 bytes) Error code (4 bytes)

Error Code supported by CS2K is as below.

Error Code	Description
0x01	Invalid Version
0x03	Unsupported Message Class
0x04	Unsupported Message Type
0x06	Unexpected Message
0x09	Invalid Stream Identifier
0x11	Invalid Parameter Value
0x12	Parameter Field Error
0x13	Unexpected Parameter
0x16	Missing Parameter

18.4.5.6 Notify Message

The Notify message used to provide an autonomous indication of M3UA events in USP to the CS2K.

Message format for Notify message is as below.

Parameter	Type	Fields

Status	Mandatory	Tag (4 bytes) Length (4 bytes) Status Type and Status Information (8 bytes) 0x0101 - Application Server State Change, inactive 0x0102 - Application Server State Change, active 0x0103 - Application Server State Change, pending

Notify message with unsupported status type and status information received is discarded silently.

18.4.6 RFC M3UA procedures

This activity implements the M3UA layer procedures based on the RFC3332 section 4.3, 4.5, 4.6.

18.4.6.1 Activate USP paths

Users can activate USP paths via ACT command in MAPCI CCS7 directory. If the path is the first activated path in the pathset, ASP UP and ASP ACTIVE procedure is started. The path is set to INSV after receive NTFY (AS ACTIVE) from USP. If the path is not the first activated path in the pathset, ASP UP and ASP ACTIVE procedure is not started. The path is set to INSV after SCTP association is established.

Please refer to figure 3, 4 for the message flow of activating USP path in pathset over SCTP.

Figure 3 Activate first path in the pathset when both paths are OFFL

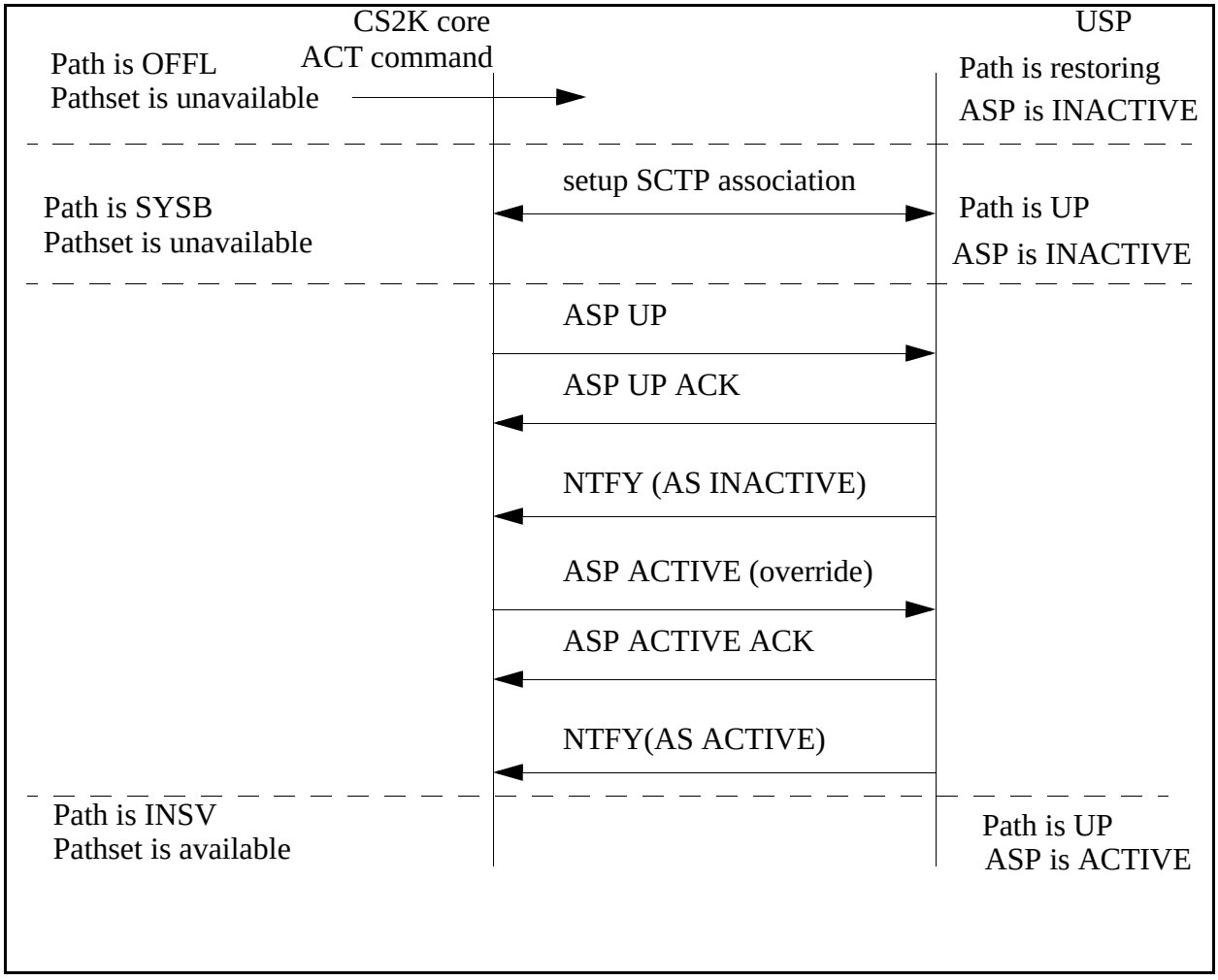
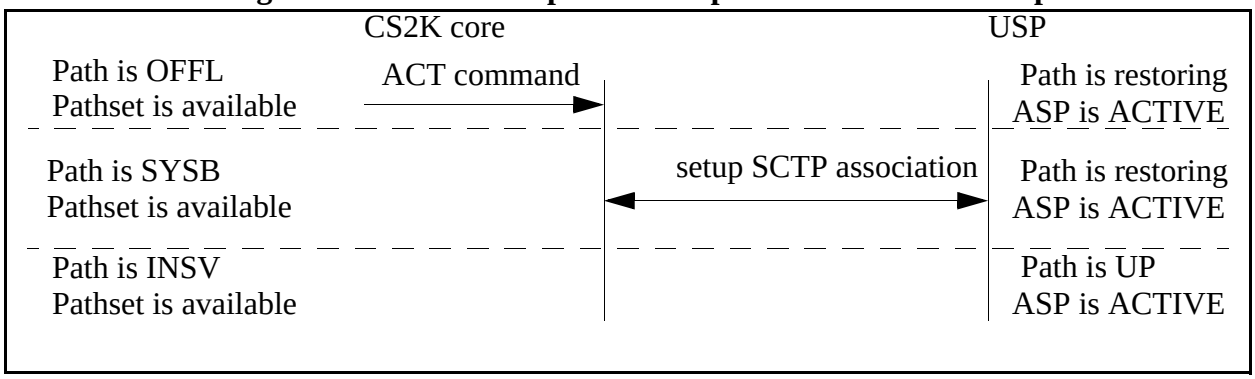


Figure 4 Activate other paths in the pathset when one of the paths is INSV



18.4.6.2 Deactivate M3UA path

Users can deactivate USP paths via DEACT command in MAPCI CCS7 directory. The path is set to OFFL when it is deactivated.

- Deactivate the last INSV path in the pathset

If the path is the last INSV path in the pathset, ASP INACTIVE and ASP DOWN procedure is started. and then the SCTP association is taken down.

After the path is deactivated, there is no more INSV path available. No more outgoing and incoming traffic is allowed immediately. ASPIA and ASPDN is sent to peer to update the ASP status.

In this case, the traffic received from peer ULP before ASPIA is received are discarded because no more outgoing and incoming traffic is allowed after the pathset is down.

- Deactivate INSV path (not the last INSV path in the pathset)

If the path is not the last INSV path in the pathset, ASP INACTIVE and ASP DOWN procedure is not started. SCTP association is taken down immediately.

After the path is deactivated, the path can not send outgoing traffic any more. SCTP SHUTDOWN chunk is sent to peer to take down the SCTP association.On reception of the SHUTDOWN chunk in the peer side, the traffic received from peer ULP before SHUTDOWN arrived are still sent out to the Core. To avoid traffic lost, the path will accept these incoming traffic and report to ULP.

- Deactivate SYSB path

If the path is in SYSB, if SCTP association is established, send SHUTDOWN to shutdown the association, otherwise, send ABORT to abort establishing SCTP association.

Please refer to figure 5, 6, 7, 8 for the message flow of deactivating USP path in pathset over SCTP.

Figure 5 Deactivate a path in pathset if it is not last INSV path

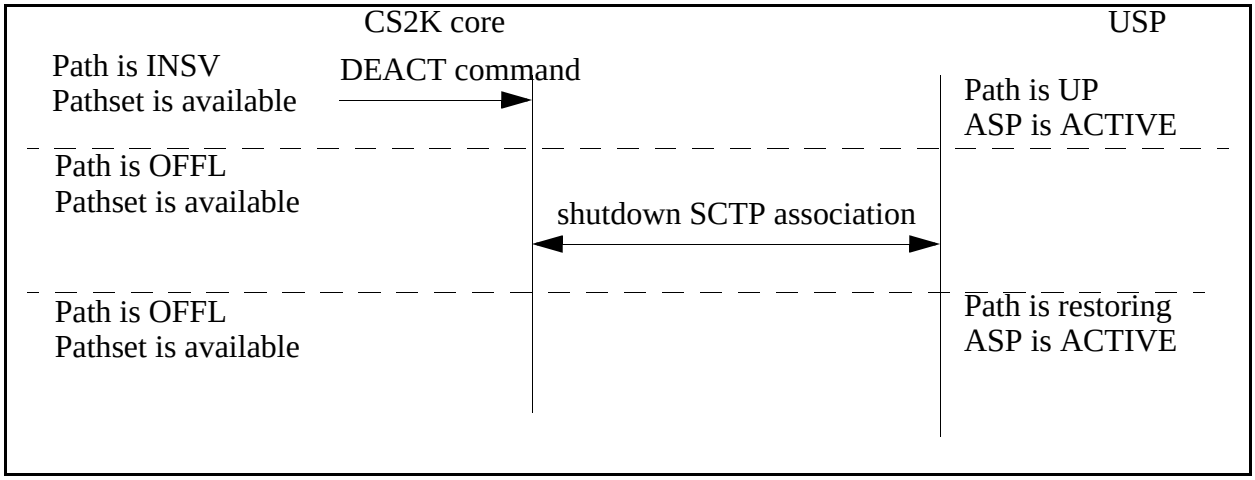


Figure 6 Deactive the last INSV path in the pathset

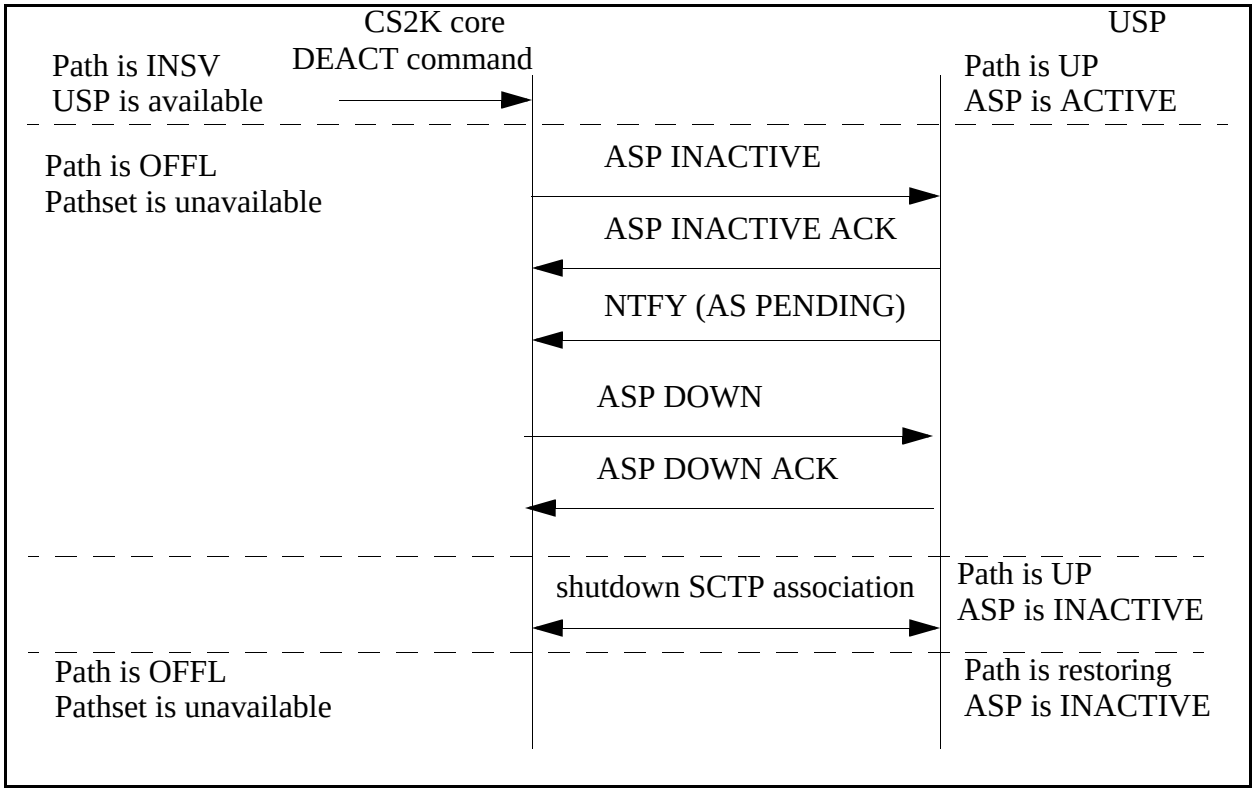


Figure 7 Deactivate a SYSB path if SCTP association is established

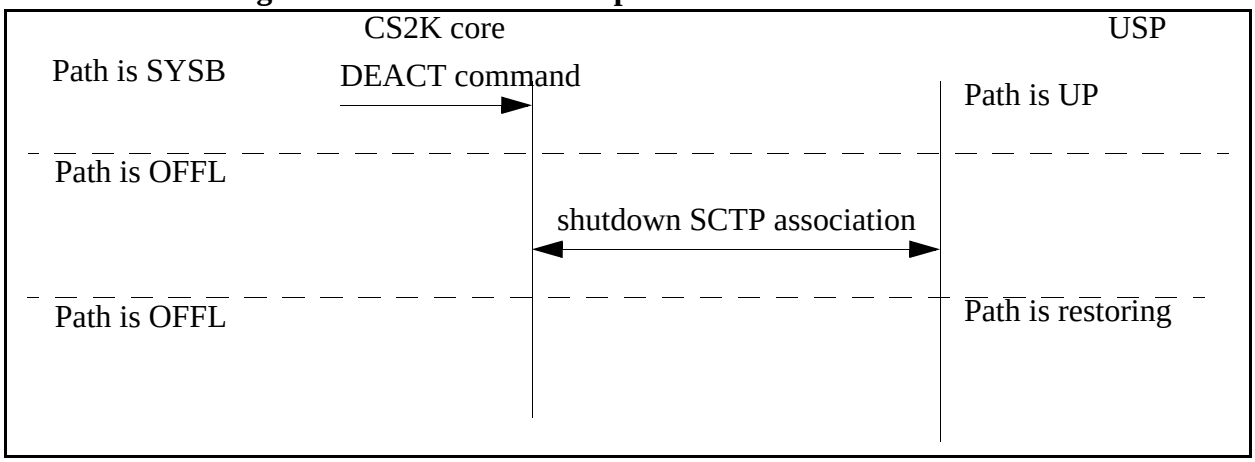
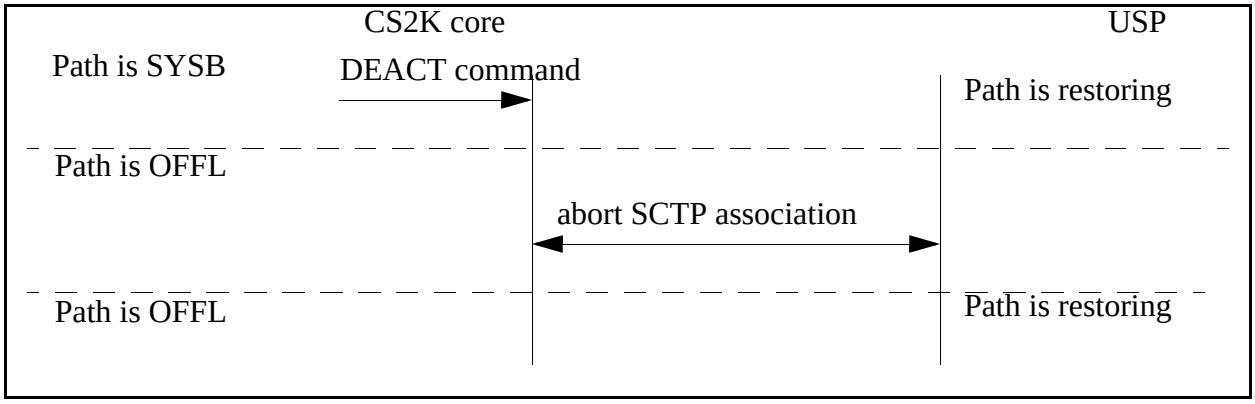


Figure 8 Deactivate a SYSB path if SCTP association is not established



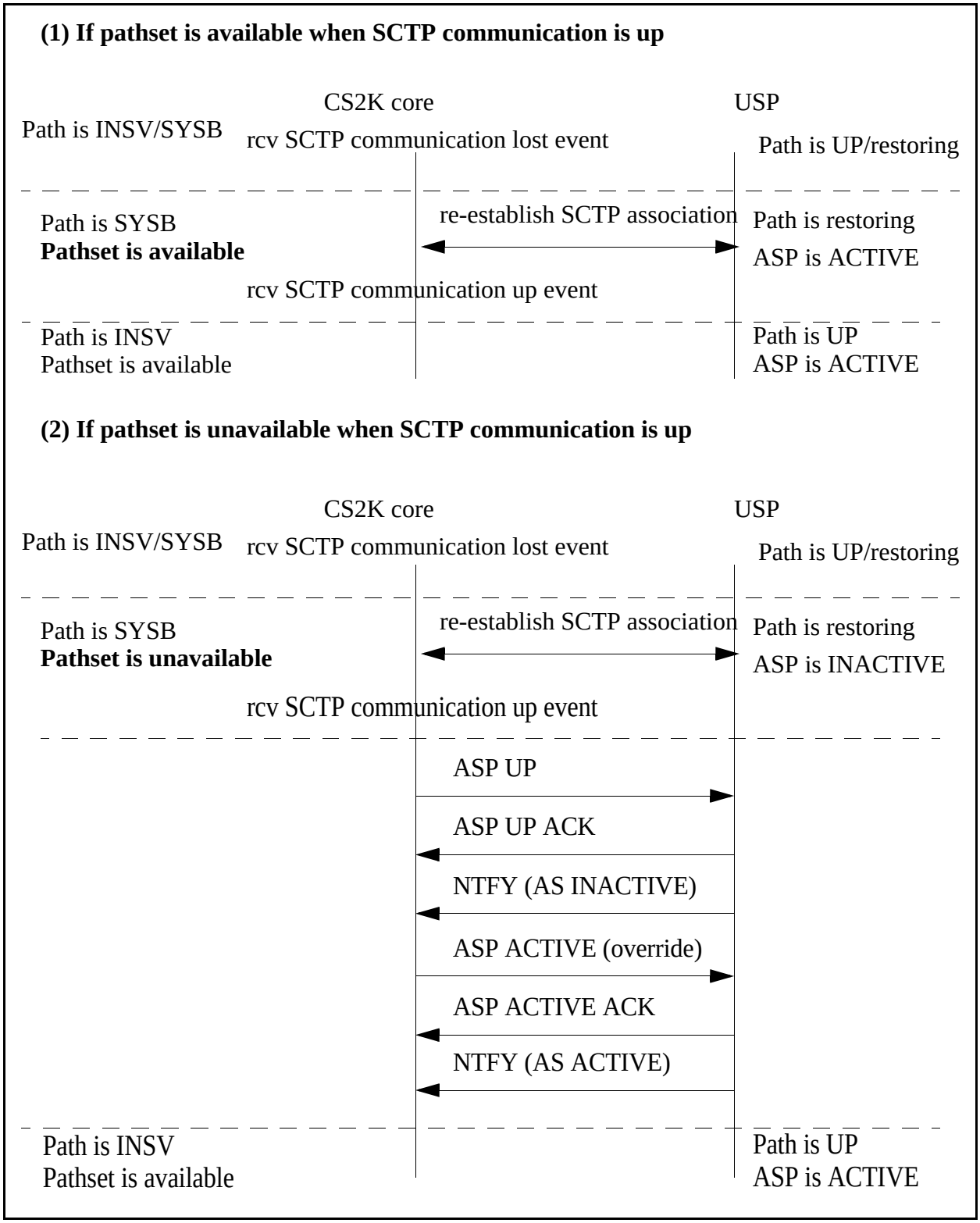
18.4.6.3 SCTP communication lost recovery

On reception of SCTP communication lost notify, M3UA management shall request the SCTP transport layer to re-establish the SCTP association.

If the pathset is unavailable when the SCTP communication is up, ASP UP and ASP ACTIVE procedure is started, otherwise, set the path to INSV.

Please refer to figure 9 for message flow of SCTP communication lost recovery.

Figure 9 Path Recover procedure when SCTP communication lost



18.4.6.4 SCTP congestion handling

Receiving SCTP STATUS CHANGE notification with congestion enter indication from one path in the pathset indicates that other paths in the pathset have the same situation because the paths are load sharing.

On reception of first path congestion indication, the pathset is regarded as congestion, M3UA layer notify the routeset management to update the status of the routeset related with pathset. The routeset status is updated as if received a SCON from USP. When all of the paths are out of congestion, the routeset management is notified. The routeset status related with the pathset is updated as if received a DAVA from USP.

18.4.6.5 SCTP stream mapping

M3UA RFC supports 2 outgoing SCTP streams.

- M3UA DATA message is sent over SCTP stream 1.
- ASPSM, MGMT messages are sent over SCTP stream 0.
- SSNM, ASPTM, BEAT ACK are sent over SCTP stream 0.

If the remote peer can not support 2 incoming streams, M3UA should take down the association.

18.4.6.6 Notify handling procedure

When receiving a Notify message reflecting a change in the AS state from USP, the CS2K core updates the local USP status and restart the ASP UP procedure if necessary. Please refer to the table below for Notify handling on CS2K core.

Table 10: Notify handling

Notify message	Status of paths	Action
AS ACTIVE	At least one path is INSV	No furthur action is taken.
AS ACTIVE	No path is INSV	Set the non OFFL paths to SYSB and start path activation procedure and sent out ASP UP message.
AS INACTIVE	In all cases	Set the non OFFL paths to SYSB and start path activation procedure and sent out ASP UP message.

Table 10: Notify handling

Notify message	Status of paths	Action
AS PENDING	In all cases	Set the non OFFL paths to SYSB and start the path activation procedure and sent out ASP UP message

18.4.6.7 SSNM message handling procedure

DAUD is sent to USP periodly to audit the status of routesets. When the CS2K core receives DAVA, DUNA, SCON, application level is notified.

When the CS2K core receives DRST, application level is notified as if DAVA is received.

Please refer to activity A00009165-Offline Routesets w/o Alarms for more information on SSNM handling when the routeset is not activated on USP and Core.

18.4.7 M3UA RFC message extension

The PROVISIONING messages and MSC_UPDATE messages, which used as M3UA V2 extension on CS2K core to support communication between CS2K core and USP, will be used unchanged as M3UA RFC extension on CS2K core to support communication between core and USP.

18.4.8 Peg OM for M3UA RFC

The existing M3UA OMs are supported for M3UA RFC.

- TXMSG
- RXMSG
- LOSTMSG

M3UA RFC and M3UA V2 use the same OM counters.

18.4.9 M3UA timers for M3UA RFC

- ASPUP timer

When the status of pathset is changed from SYSB to INSV, ASPUP is sent to USP. ASPUP is resent to USP every 2s utill ASPUP ACK is received from USP.

- ASPAC timer

After received ASPUP ACK from USP, ASPAC is sent to USP. ASPAC is resent every 2s utill ASPAC ACK is received from USP.

- ASPIA timer

When the status of pathset is changed from INSV to SYSB or OFFL, ASPIA is sent to USP. ASPIA is sent for only once. If ASPIA ACK is not received from USP, the ASPIA is not sent again. ASPDN is sent out after ASPIA timer timeout.

- ASPDN timer

After received ASPIA ACK from USP or ASPIA timer timeout, ASPDN is sent to USP. ASPDN is sent for only once. If ASPDN ACK is not received from USP, the ASPDN is not sent again. SCTP association is taken down after ASPDN timer timeout.

18.4.10 Max message rate supported

The message rate that one M3UA RFC path can support is up to 1500 msg/sec.

The total message rate of all M3UA RFC paths over SCTP **SHOULD** be less than the max message rate that SCTP on core can support. Currently the max message rate that SCTP can support is 4500 msg/sec. Please refer to activity A00003649 “SCTP (Stream Control Transmission Protocol) Enhancements on XA-Core” for more detail.

18.4.11 Cutover from M3UA V2 pathset to M3UA SCTP pathset

This cutover procedure is used to change the in-service M3UA V2 pathset to M3UA SCTP pathset. This cutover MUST be done with low traffic.

1. Make sure at least **two** paths are provisioned in the M3UA V2 pathset. All of the paths are INSV.

2. Deactivate one of the M3UA_V2_UDP path in the pathset. The status of the path is OFFL now.

3. Change the pathprot from M3UA_V2_UDP to M3UA_RFC_SCTP_*. The pathprot M3UA_RFC_SCTP_* could be M3UA_RFC_SCTP_CLIENT or M3UA_RFC_SCTP_SERVER.

4. Activate the path in MAPCI. Verify the status of the path is INSV now and traffic are sent to the path.

5. Soak for some time. The time depends on customer’s decision.

6. Repeat step 2-5 for other M3UA_V2_UDP paths in the pathset.

Note: it is not recommended provisioning different type paths in one pathset. The cutover status should be regarded as a transient status. During cutover,

there is no traffic change over between paths, which will cause traffic lost when the path is being deactivated.

18.4.12 Rollback from M3UA SCTP pathset to M3UA V2 pathset

This rollback procedure is used to restore the paths to M3UA_V2_UDP paths in case any problem during cutover.

1. Deactivate one of the M3UA_RFC_SCTP_* path in the pathset. The status of the path is OFFL now.

2. Change the pathprot from M3UA_RFC_SCTP_* to M3UA_V2_UDP. The pathprot M3UA_RFC_SCTP_* could be M3UA_RFC_SCTP_CLIENT or M3UA_RFC_SCTP_SERVER.

3. Activate the path in MAPCI. Verify the status of the path is INSV now and traffic are sent to the path.

4. Repeat step 1-3 for other M3UA_RFC_SCTP_* paths in the pathset.

Note: it is not recommended provisioning different type paths in one pathset. The cutover status should be regarded as a transient status. During cutover, there is no traffic change over between paths, which will cause traffic lost when one path is being deactivated.

18.5 Hardware Requirements or Dependencies

NA

18.6 Software Requirements or Dependencies

NA

18.7 Limitations and restrictions

1. This activity implements a basic functionality of M3UA RFC on CS2K core. Only those functionalities mentioned in this document are commited by this activity.

2. This activity doesn’t support dynamic register procedure (RFC3332 section 4.4) on CS2K core.

3. There is no changes introduced in the Core swact mechanism for SCTP and M3UA connections. The existing behavior is expected during SWACT after this activity.

4. There is no changes introduced into the path load sharing mechanism. The existing behavior is expected after this activity.

5. When the path is datafilled as SCTP server, the port used to listen for INIT chunk is not 2905, it can be from 4697-4700 to 4710-4721.

6. It is not recommended provisioning different type paths in one pathset. The cutover status should be regarded as a transient status.

7. There is no traffic change over between paths, which will cause traffic lost when one path is being deactivated.

8. SCTP CRC32 checksum is not supported in Core. Adler checksum should be used to establish SCTP association.

18.8 Interactions

NA

18.9 Glossary

Term	Description
ASPSM	ASP State Maintenance
ASPTM	ASP Traffic Maintenance
M3UA	Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) -User Adaptation Layer
OOTB	Out of Blue
SCTP	Stream Control Transmission Protocol
SCTP v5	SCTP version5
SG	Signaling Gateway
SSNM	SS7 Signalling Network Management
TCB	Transmission Control Block
TCP	Transmission Control Protocol
TLV	Type-Length-Value Coding Format
TSN	Transmission Sequence Number
UDP	User Datagram Protocol

18.10 Reference

1. RFC3332 Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) -User Adaptation Layer (M3UA), September 2002

2. M3UA Implementor's Guide, V7, February, 2004

3. RFC2960 Stream Control Transmission Protocol, October 2000

4. Stream Control Transmission Protocol (SCTP) Implementer's Guide, V12, October 15, 2004

5. <draft-ietf-sigtran-m3ua-02.txt> SS7 MTP3-User Adaptation Layer (M3UA)

6. <draft-ietf-sigtran-sctp-05.txt> Simple Control Transmission Protocol

7. A00009164- USP Supports Multiple CS 2000s

8. A00009159- USP Mated Pair Supporting Mult CS2000s (PREP)

9. A00009165- USP - Offline Routesets w/o Alarms

19: Functional Description (FN): A00009165

19.1 Feature name and Feature ID

A00009165: USP - Offline Routesets without Alarms

19.2 Description

Before this feature, if customer datafills new SS7 routesets in USP which acts as Signal Gateway, but does not wish to, or cannot for some reason, bring them into service immediately, CORE shows alarms for those routesets. The critical alarms caused by it masks other legitimate alarms, resulting in a signaling outage being overlooked.

This type of behavior is very typical for operator craftspersons. In large corporations, the addition of SS7 routesets can be a multi-company activity, where schedules have to be coordinated and resources have to be used as they become available.

The purpose of this feature is to eliminate this kind of alarms found on XA-CORE switch, and provide an OFFLINE state for routeset in CORE.

19.2.1 Set the routeset to offline when it is provisioned from USP

Before this feature, when the routeset is provisioned from USP, its state is set to system busy, then an alarm is generated.

In this feature, the state is set to offline when the routeset is just provisioned from USP.

19.2.2 Enable the operation to offline a routeset in CORE

When CORE receives a DUNA from SG for a routeset, the routeset state is set to SYSB, and an alarm is generated for it. But sometimes, operator wants to offline the routeset and would not expect any alarms on it.

In this feature, when the routeset is seen SYSB (system busy) in CORE , if operator thinks it should be in offline state, the routeset can be offline manually in CORE so that the additional alarm is cleared. This operation can not be done while the routeset is in-service in CORE.

When routeset is in offline state, it can be turn into man-busy state by the command BSY from craftsperson. When DUNA/DAVA/SCON message are received while the corresponding routeset is in offline or man-busy state, these message are discarded.

When RTS command is run for a routeset by craftsperson, routeset state is set to SYSB, and send out a DAUD to USP to get the correct state..

19.2.3 Routeset related with ASM can be deleted at USP only when it is at OFFL state in CORE.

If the routeset is not at OFFL state at CORE, the request to delete it will be rejected by CORE, and the corresponding information will be given.

19.3 Hardware Requirements or Dependencies

N/A.

19.4 Software Requirements or Dependencies

N/A.

19.5 Limitations and restrictions

Need operator to take more action to offline the routeset in CORE, and the additional alarm will exists before the action.

19.6 Interactions

19.7 Glossary

Term	Description
DAVA	Destination Available
DUNA	Destination Unavailable

20: Functional Description (FN): A00009216

20.1 Feature name and Feature ID

A00009216: JI-ISUP to Base ETSI ISUP V2 Mapping Enhancement

20.2 Description

This activity provides an optionality to pass some ISUP parameters unchanged for the JI-ISUP to Base ETSI ISUP V2 interworking. Followings are the parameters to be mapped unchanged:

- Nature of Address (NOA) in Calling Party Number
- ISUP Preference Indicator in Forward Call Indicator
- Calling Party Category value ‘calling subscriber with priority’

This feature is optional with a new controlled SOC option. When the state of this SOC option is ON, feature becomes active, otherwise system behaves as it was before this functionality.

This feature will be available in TDM offices in ISN09 and later releases on DMS100 MMP.

20.3 Current Behavior

20.3.1 NOA of Calling Party Number

In current behavior, Nature of Address of the Calling Party Number is always set to NATL without checking the received value for JI-ISUP to Base ETSI V2 ISUP interworking. Please refer to “Table 1 Current NOA Mapping - JI-ISUP to Base ETSI ISUP V2 i/w” on page 375. for current mapping of the NOA.

Table 1 Current NOA Mapping - JI-ISUP to Base ETSI ISUP V2 i/w

JI-ISUP IAM			dir	Base ETSI ISUP V2 IAM		
Parameter	**Field**	**Field Value**		**Field Value**	**Field**	**Parameter**
Calling Party Number	Nature of Address Indicator	0000000 - spare	⇒	0000011 - All values are mapped to National	Nature of Address Indicator	Calling Party Number
		0000001 - Subscriber number				
		0000010 - Reserved for national use				
		0000011 - National number				
		0000100 - International number				
		0000101 - 1101111 spare				
		1110000 - 1111101 reserved for national use				
		1111110 - peculiar number of network				
		1111111				

Note : The values in shaded cells are the values that are not supported by the JI-ISUP protocol.

20.3.2 ISUP Preference Indicator in Forward Call Indicator

The current behavior of mapping ISUP Preference Indicator for JI-ISUP to Base ETSI V2 ISUP interworking is as follows:

1. If there are any supplementary services in the received IAM (ATP, UUI, CLIP) then set the outgoing ISUP Preference Indicator to 'ISUP Preferred All The Way'.
2. If the condition in item 1 is not met, and the BC received in the TMR/USI combination is set to Speech or 3_1_kHz_Audio, then set the outgoing ISUP Preference Indicator to 'ISUP Not Required All The Way'.
3. If the conditions in item 1 and item 2 are not met, then set the outgoing ISUP Preference Indicator to 'ISUP Preferred All The Way'.

If the received ISUP Preference Indicator value is 'Spare', the Protocol_Error treatment is set and call goes to treatment.

Please refer to "Table 2 Current ISUP PI Mapping - JI-ISUP to Base ETSI ISUP V2 i/w" on page 376. for current mapping of the PI.

Table 2 Current ISUP PI Mapping - JI-ISUP to Base ETSI ISUP V2 i/w

JI-ISUP IAM			dir	Base ETSI ISUP V2 IAM		
Parameter	**Field**	**Field Value**		**Field Value**	**Field**	**Parameter**
Forward Call Indicator	ISDN User Part Preference Indicator	00 - ISDN user part preferred all the way	⇒	Please refer to “Table 3 ISUP Preference Indicator Parameter Coding” on page 376.	ISDN User Part Preference Indicator	Forward Call Indicator
		01 - ISDN user part not required all the way				
		10 - ISDN user part required all the way				
		11 - Spare				

Note : The values in shaded cells are the values that are not supported by the JI-ISUP protocol.

Table 3 ISUP Preference Indicator Parameter Coding

Information Field	**JI-ISUP V.2-->**	**--> ETSI v2**	**JI-ISUP V.2-->**	**--> ETSI v2**
Supplementary Service	**None (No UUI, ATP or CLIP present in the IAM)**		**Any (UUI, ATP and/or CLIP present in the IAM)**	
(Applies to messages: IAM)	**Bits**	**Bits**	**Bits**	**Bits**
ISUP Preferred	HG	HG	HG	HG
For Bearer Service = Speech	00	01	00	00
For Bearer Service = 3.1kHz Aud.	00	01	00	00
For Bearer Service = 64k Unres.	00	00	00	00
For Bearer Service = Other	00	00	00	00
ISUP Not Required All The Way	HG	HG	HG	HG
For Bearer Service = Speech	01	01	01	00
For Bearer Service = 3.1kHz Aud.	01	01	01	00
For Bearer Service = 64k Unres.	01	00	01	00
For Bearer Service = Other	01	00	01	00
ISUP Required All The Way	HG	HG	HG	HG
For Bearer Service = Speech	10	01	10	00
For Bearer Service = 3.1kHz Aud.	10	01	10	00
For Bearer Service = 64k Unres.	10	00	10	00
For Bearer Service = Other	10	00	10	00
Spare	HG	HG	HG	HG
For Bearer Service = Speech	11	01	11	00
For Bearer Service = 3.1kHz Aud.	11	01	11	00
For Bearer Service = 64k Unres.	11	00	11	00
For Bearer Service = Other	11	00	11	00

20.3.3 ISUP Calling Party Category

In existing behavior, Calling Party Category value ‘calling subscriber with priority’ is mapped as CPC Unknown for JI-ISUP to Base ETSI ISUP V2 interworking. Please refer to “Table 4 Current CPC Mapping - JI-ISUP to Base ETSI ISUP V2 i/w” on page 377. for current mapping of Calling Party Category.

Table 4 Current CPC Mapping - JI-ISUP to Base ETSI ISUP V2 i/w

JI-ISUP IAM			dir	Base ETSI ISUP V2 IAM		
Parameter	**Field**	**Field Value**		**Field Value**	**Field**	**Parameter**
Calling Party Category		00000000 - calling party’s category unknown 00000001 - spare 00000010 - spare 00000011- spare 00000100 - spare 00000101 - spare 00000110 - By mutual agreement 00000111 - By mutual agreement 00001000 - By mutual agreement	⇒	00000000 - CPC Unknown	Calling Party Category	
		00001001 - national operator desk		00000000 - CPC Unknown		
		00001010 - ordinary calling subscriber		00001010 - ordinary calling subscriber		
		00001011 - calling subscriber with priority		00000000 - CPC Unknown		
		00001100 - data call		00000000 - CPC Unknown		
		00001101 - test call		00001101 - test call		
		00001111 - payphone		00001111 - payphone		
		00010000 - 11110000 spare		00000000 - CPC Unknown		
		11110001 - 11111110 reserved for national use		00000000 - CPC Unknown		
		11111111 - spare		00000000 - CPC Unknown		

Note : The values in shaded cells are the values that are not supported by the JI-ISUP protocol.

20.4 Desired Behavior

20.4.1 Activation of the feature

Activation of the functionality is controlled by the new SOC option NETK00XX-”NETK Jpn I ISUP Parm Enh”.

NETK Jpn I ISUP Parm Enh is a controlled SOC and it has two states, ON and IDLE. Default state of *NETK Jpn I ISUP Parm Enh* is IDLE. When its state is ON, this feature becomes functional.

Table 5 SOC for Activation of Feature

SOC group:	NETK
SOC option name:	NETK Jpn I ISUP Parm Enh
SOC option title:	NETK Jpn I ISUP Parm Enh
SOC option control type:	state
New SOC option?	Yes
SOC option order code	NETK0087
Option defined in DRU:	WT22
Affected products:	ISN09

20.4.2 NOA of Calling Party Number

This activity provides an optionality to pass the value of NOA in calling party number as unchanged to the Base ETSI ISUP V2 for the JI-ISUP to Base ETSI ISUP V2 interworking. In order to achieve this, the implementation will be made optional by new created SOC option.

The NOA values used in JI-ISUP are

- NATL (0000011)
- INTL (0000100)
- Peculiar Number (1111110)

Peculiar Number is a national use value and it is not supported in ETSI ISUP.

After the state of the new SOC option is changed to ON, and if the received NOA value is NATL or INTL, then received value is transparently passed to the Base ETSI ISUP V2. If the received value is Peculiar Number or any other value, then outgoing NOA of Calling Party Number is set to NATL.

If the state of the new SOC option is IDLE, then by default, the current behavior will be kept as described in Please refer to Section “20.3.1 NOA of Calling Party Number” on page 374..

Table 6 Desired NOA Mapping - JI-ISUP to Base ETSI ISUP V2 i/w

JI-ISUP IAM			dir	Base ETSI ISUP V2 IAM		
Parameter	**Field**	**Field Value**		**Field Value**	**Field**	**Parameter**
Calling Party Number	Nature of Address Indicator	0000000 - spare	⇒	0000011 - National number	Nature of Address Indicator	Calling Party Number
		0000001 - Subscriber number		0000011 - National number		
		0000010 - Reserved for national use		0000011 - National number		
		0000011 - National number		0000011 - National number		
		0000100 - International number		0000100 - International number		
		0000101 - 1101111 spare		0000011 - National number		
		1110000 - 1111101 reserved for national use		0000011 - National number		
		1111110 - peculiar number of network		0000011 - National number		
		1111111		0000011 - National number		

Note : The values in shaded cells are the values that are not supported by the JI-ISUP protocol.

20.4.3 ISUP Preference Indicator of Forward Call Indicator

The existing behavior is modified not to send the call to the treatment when the received ISUP preference indicator value is 11-Spare. If received ISUP preference indicator value is ‘11-spare’, it is mapped as in “Table 3 ISUP Preference Indicator Parameter Coding” on page 376 for JI-ISUP to Base ETSI V2 ISUP interworking:

1. If there are any supplementary services in the received IAM (ATP, UUI, CLIP) then set the outgoing ISUP Preference Indicator to 'ISUP Preferred All The Way'.
2. If the condition in item 1 is not met, and the BC received in the TMR/USI combination is set to Speech or 3_1_kHz_Audio, then set the outgoing ISUP Preference Indicator to 'ISUP Not Required All The Way'.
3. If the conditions in item 1 and item 2 are not met, then set the outgoing ISUP Preference Indicator to 'ISUP Preferred All The Way'.

This changing on the current behavior is in effect when the new created SOC option state is IDLE.

Also with this activity, the received ISUP Preference Indicator is tranparently passed to the Base ETSI ISUP V2 for the JI-ISUP to Base ETSI ISUP V2 interworking. This behavior is optional. In order to achieve this, the implementation will be made via new created SOC option.

The ISUP Preference Indicator values used in JI-ISUP are

- ISUP Preferred All The Way (00)
- ISUP Not Required All The Way (01)
- ISUP Required All The Way (10)

If the received ISUP Preference Indicator value is one of the above, and the state of the new SOC option is ON, then received value is passed unchanged for JI-ISUP to Base ETSI ISUP V2 interworking. If the received value is 'spare (11)', then it is mapped as '00-ISUP Preferred All The Way' when the new SOC option state is ON.

Table 7 Desired ISUP PI Mapping - JI-ISUP to Base ETSI ISUP V2 i/w

JI-ISUP IAM			dir	Base ETSI ISUP V2 IAM		
Parameter	**Field**	**Field Value**		**Field Value**	**Field**	**Parameter**
Forward Call Indicator	ISDN User Part Preference Indicator	00 - ISDN user part preferred all the way	⇒	00 - ISDN user part preferred all the way	ISDN User Part Preference Indicator	Forward Call Indicator
		01 - ISDN user part not required all the way		01 - ISDN user part not required all the way		
		10 - ISDN user part required all the way		10 - ISDN user part required all the way		
		11 - Spare		00 - ISDN user part preferred all the way		

Note : The values in shaded cells are the values that are not supported by the JI-ISUP protocol.

If the state of this SOC option is IDLE, then by default, the current behavior will be kept as described in Please refer to Section “20.3.2 ISUP Preference Indicator in Forward Call Indicator” on page 375. except the received ISUP Preference Indicator value is ‘11-spare’.

20.4.4 ISUP Calling Party Category

This activity also provides an optionality to transparently pass the calling party category value ’Calling subscriber with priority’ to the Base ETSI ISUP V2 for the JI-ISUP to Base ETSI ISUP V2 interworking. In order to achieve this, the implementation will be made optional via new created SOC option.

If the state of this SOC option is not ON, then by default the current behavior will be kept as described in Please refer to Section “20.3.3 ISUP Calling Party Category” on page 377..

After the state of the SOC option is changed to ON, CPC value ’Calling subscriber with priority (00001011)’ will be passed as received from the JI-ISUP side for the JI-ISUP to Base ETSI ISUP V2 interworking.

Table 8 Desired CPC Mapping - JI-ISUP to ETSI ISUP V2 i/w

JI-ISUP IAM			dir	ETSI ISUP V2 IAM		
Parameter	**Field**	**Field Value**		**Field Value**	**Field**	**Parameter**
Calling Party Category		00000000 - calling party's category unknown 00000001 - spare 00000010 - spare 00000011- spare 00000100 - spare 00000101 - spare 00000110 - By mutual agreement 00000111 - By mutual agreement 00001000 - By mutual agreement	⇒	00000000 - CPC Unknown	Calling Party Category	
		00001001 - national operator desk		00000000 - CPC Unknown		
		00001010 - ordinary calling subscriber		00001010 - ordinary calling subscriber		
		00001011 - calling subscriber with priority		00001011 - calling subscriber with priority		
		00001100 - data call		00000000 - CPC Unknown		
		00001101 - test call		00001101 - test call		
		00001111 - payphone		00001111 - payphone		
		00010000 - 11110000 spare		00000000 - CPC Unknown		
		11110001 - 11111110 reserved for national use		00000000 - CPC Unknown		
		11111111 - spare		00000000 - CPC Unknown		

Note : The values in shaded cells are the values that are not supported by the JI-ISUP protocol.

20.5 Hardware Requirements or Dependencies

None

20.6 Software Requirements or Dependencies

To make this new feature functional, new controlled SOC option NETK0087 is used. Since the SOC state will be IDLE after ONP completed, it must be changed to ON manually to make the feature functional.

20.7 Limitations and restrictions

None

20.8 Interactions

This feature is affective in the senarious below:

1. call forwarding (when the received call over JI-ISUP is forwarded to another agent over Base ETSI ISUP V2)
2. Carrier Name Notification (CNN) feature

automatically without making any extra implementation.

The NOA value of the outgoing IAM message can be changed with the datafills and features below:

3. EDITCLI option in table TRKSGRP
4. Serving Country Code (SCC) feature

With this activity, those are still be active on the outgoing Base ETSI ISUP V2 trunk without making any new implementation.

20.9 Glossary

Term	Description
ATP	Access Transport Parameter
BC	Bearer Capability
CLIP	Calling Line Identification Presentation
CPC	Calling Party Category
DMS	Digital Multiplex System
IAM	Initial Address Message
MMP	Multi Market Product
NOA	Nature Of Address
ONP	One Night Process
PI	Preference Indicator
SOC	Software Optionality Control
TMR	Transmission Medium Requirement
USI	User Service Information

Term	Description
UUI	User to User Information

20.10 Recommended Reading/References

a. SIM Specification: Japan Interconnect ISUP DMS/CS2000 Implementation: Interworking Specification

b. ITU-T Recommendation Q763 : Signalling System No.7 - ISDN User Part Formats and Codes

c. A59034248 - Japon Interconnect ISUP Carrier Name Notification for Carrier Designation

d. A59023331 - Serving Country Code

21: Functional Description (FN): A00009228

21.1 Feature name and Feature ID

A00009228: LI - International Trunk Interception in Cs2k

21.2 Description

The Intl'LI feature today provides interception of ETSI ISUP V1/V2 trunk on the DMS platform. This capabilty was never migrated to the CS2K.

New markets, Israel and Russia are being entered in which the DMS did not operated in the past. The main requirement is to support the trunk interception in succession market. Base ETSI ISUP V1/V2, national variants (Israel and Russian ISUP) both SIP and TDM based will be supported by this feature in CS2K.

This feature provides the following LI capabilities for the Succession solution:

- Provide interception of incoming trunk calls over ETSI ISUP V1 and V2 with national Calling Party numbers
- Provide interception of outgoing trunk calls over ETSI ISUP V1 and V2 with national and international Called Party numbers.
- Provide incoming and outgoing trunk interception capability for Israeli and Russian ETSI ISUP variants
- Provide interception capability of trunks connected to PVG, M2000, SIP VRDN and NGSS
- Suppor both CDR and IRI call data delivery options using X.25 and TCP/IP delivery for ETSI V1/V2 trunks, Israeli ISUP, Russian ISUP and trunks connected to PVG, M2000, SIP VRDN and NGSS.
- Provide Stereo and Mono Mode delivery of CallContent for the surveillance of ETSI V1/V2 trunks, Israeli ISUP, Russian ISUP and trunks connected to PVG, M2000, SIP VRDN and NGSS.
- Support New CCC Variant R-ISUP as a valid CCC option.

21.2.1 Provisiong of Trunk Interception Monitoring order

Provsioning for **TRK** in DNBDORD for succession market does not need the munch password activiation.

The example for the Help command is given below. The options related to TRK surveillances are highlited in bold.

>help add

```
ADD DNBDORD ENTRIES
Parms: <group_id> STRING
     <cdc_tgtdn> {NO,
                YES}
     <x25_dn> STRING
     <line_parm> {IBN <DN> STRING,
                PRI <CLLI> STRING
                  <VARIANT> {ETSIPRI,
                        QSIGPRI,
                        AUSTPRI}
                  <DN> STRING,
                BRI <LTGRP> STRING
                  <LTNUM> {0 TO 1022}
                  <DN> STRING,
                MFT <DN> STRING,
                VA <MAXCCC> {4 TO 255}
                  <DN> STRING,
                HNT <LEN> {LEN < > STRING
                        < > STRING
                        < > STRING
                        < > STRING
                        < > STRING}
                  <DN> STRING,
TRK <TRIGGER> {CLI <MAXCCC> {4 TO 255}
                <VARIANT> {incoming_natl}
                <DN> STRING,
                CDN <MAXCCC> {4 TO 255}
                <VARIANT> {outgoing_natl,
                        outgoing_intl}
<ref_no> STRING
     <cccreq> {NO,
              YES <idn> STRING
                <ccc_cug> {NO,
                        YES}
<ccc_name> STRING
                <ccc_sys> STRING
                <ccc_billno> STRING
                <ccc_cgsa> {TGTDN,
                        REFNO,
                        NONE}
                <san_req> {NO,
                        YES <san> STRING}}
```

21.2.1.1 International trunk Target and number formats

For provisioning the new INTL TRK agent type check the following information.:

- whether the requested number is an international number, if not, provisioning of the TRK target is rejected.

(note : the above check just checks that the number entered is a international number. It does not validate the provisioned international number. The operator datafills the correct outgoing CDN.)

- whether the requested number is between 4 digits to 18 digits, if not, provisioning of the TRK target is rejected.

To provision and trigger on an international CDN TRK target order
1) check international_access_code (IAC) in OFCENG; let's assume this is '**00**'
2) check national_country_code (NCC) in OFCENG; let's assume this is '49'

If you want to get a successful LI Intl_CDN TRK trigger your mon order DN must look like the following 'template' DN:
00431234567891

The 00 must be identical to the IAC of the specific switch , and the 43 must not be identical to the NCC of the specific switch, else the called number is not being classified a real international number by the LI application. Any other value for the bold digits unequal the NCC=49 will make it as well.

The 1234 is in the above example the SNPA; and the 567891 the local DN.

The following called number **translations results** will provide a trigger:

- 00431234567891, NOA (NatureOfAddress)=unknown, NPI(NumberingPlanIndicator)=don't care
- 431234567891, NOA=international, NPI=don't care

If the routing table is not manipulated for the outpulsed CDN in any Routing table, the LI trigger will happen if, and only if, the result of a TRAVER will show either of the 2 above trigger digit strings.
But note, that if TRAVER shows 431234567891, it must be ensured that the outpulsed NOA is INTERNATIONAL.

Example without CCC's:

```
DNBDORDER:
>add STPO0 YES 1720140405 TRK CDN 4 outgoing_intl 00437545968924 5651999 NO

Add MON ORDER:
ORD STA   GRPID    CDCTDN X25DN       ACC CLLI/LTID/LEN/MAXCCC/DN
    REFNO     CCCREQ IDN              CUGOAE CCCNAME  CCCSYS
    BILLNO  CCCCGSA   SANREQ    SAN


--------------------------------------------------------------------------------
    DEACT STPO0    YES    1720140405  TRK   4 00431234567891
    5651999   NO
```

ACC - Type of the agent to be monitored

MAXCCC - Maximum number of CCC pairs that can be allocated for monitoring. Based on the operators datafill the number of CCC pairs will be set.

DN - This is the DN is the digits that are matched for interception.

Example with CCC's:

```
DNBDORDER3
>add STPO0 YES 1720140405 TRK 4 00431234567891 5651999 YES 0033401234 NO STEPINTL
PX 112233  NONE NO

Add MON ORDER:
ORD STA   GRPID    CDCTDN X25DN       ACC CLLI/LTID/LEN/MAXCCC/DN
    REFNO     CCCREQ IDN              CUGOAE CCCNAME  CCCSYS
    BILLNO  CCCCGSA   SANREQ    SAN


--------------------------------------------------------------------------------
    DEACT STPO0    YES    1720140405  TRK      4 00431234567891
    5651999   YES    0033401234        NO      STEPINTL PX
    112233  NONE      NO
```

21.2.1.1.1 International number formats

The numbers in the following table show an example of a DN identified as an international number. In this example, the displayed IAC of the DN is 41 in table OFCENG.

Table 11: International DN formats

DN	NPI	Type of Number
41888212345	E.164	international
0041888212345	E.164	unknown

21.2.1.2 Interception of International trunk target monitoring

Whenever an outgoing called number over ETSI ISUP has a matching pattern in DNBDORD and if the surveillance is active for this provisioned outgoing CDN, then CDC/IRI records are generated for this monitored call.

The call content of this call is sent by a pair of CC links. The list below give the sequence of the records.

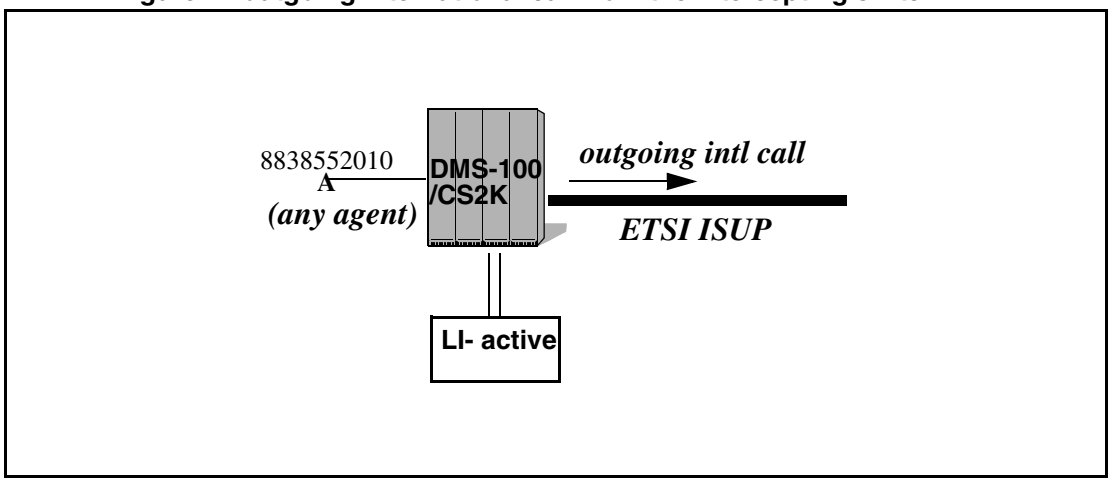
- When the trunk is allocated a BEGIN record is generated and a pair of CC links is setup and connected for this call.
- If the terminator of the call answers then a CONTINUE record is sent.
- When the call is released, an END record is generated and the CC links are also released.

- If the trunk allocation fails then a REPORT record is generated. In this case no CC links are setup.

The address of the target facility is the outgoing CDN which is obtained in the ISUP message. Based on the dialling (enbloc or overlap) the target facility will have the complete number or the part of the number.

The calling number is the address of the correspondent.

Figure 1 outgoing international call from the intercepting switch



In the figure above, A's number is 8838552010. A dials `00431234567891`. The provisioned target `00431234567891`. With respect to this particular scenario the target facility is `00431234567891`and the CDN is `00431234567891`. The other party address is 8838552010.

The target address provisioned can be a complete CDN or a partial address of the complete CDN. for eg,

— complete CDN provisioned : `00431234567891`

— partial CDN provisioned : `00431234`

For the working knowledge refer to "International Lawful Intercept Product and Technology Fundamentals" NN10194-113

21.2.1.3 National trunk Target and number formats

This section describes how LI triggering affects the numbering format for national calls.

21.2.1.3.1 Normalized national number format

The LI triggering for national CLI and CDN monitoring orders is based on a normalized national DN.

The following table shows an example of how a normalized national DN is formatted.

Table 12: Normalized National DN format

DN	NPI	Type Of Number
07545968168	E.164	unknown

Only national CLI and CDN trunk monitoring orders using the above DN format can be datafilled in the DNBDORD level of the LI provisioning interface on the CM. The National access code in table OFCENG (NAC) is the leading 0.

21.2.1.3.2 National number formats

The numbers in the following table shown an example of DNs identified as national numbers that map to their equivalent normalized national DN listed in the previous table. For mapping of the National DN in Table3 to normalized DN format refer to figure 2 and 3.

Table 13: National DN formats

DN	NPI	Type of Nunber
07545968168[1]	E.164	unknown
7545968168	E.164	national
497545968168[2]	E.164	international

1.Leading digit is “0” = NAC (normalized national format)

2.Leading digits are “4” and “9” = international access code (IAC) for Germany. This IAC identifies this number as a national number for the German market i.e National Country code in table OFCENG.

21.2.1.3.3 National CDN/CLI trigger functionality Depending on the selected trigger variant, this trigger is activated when the DNs from the ETSI ISUP V2 IAMs or SAMs match the monitoring order. The DN that is

provisioned in the DNBDORD level can be a complete national number (including the national access code 0) or a partial address of the complete number. (Partial address support applies to the left-most aligned digits only.)

21.2.1.4 Incoming national CLI trigger

The following figure shows how a CPN received in an ETSI ISUP V2 IAM activates CLI monitoring when the equivalent normalized national number matches the target address provisioned in the DNBDORD level, and the monitoring order is active for that address

Example without CCC's:

```
DNBDORDER:
>add STPO0 YES 1720140405 TRK CLI 4 incoming_natl 07545968168 5651999 NO

Add MON ORDER:
ORD STA   GRPID    CDCTDN X25DN       ACC CLLI/LTID/LEN/MAXCCC/DN
    REFNO     CCCREQ IDN              CUGOAE CCCNAME  CCCSYS
    BILLNO  CCCCGSA   SANREQ    SAN


--------------------------------------------------------------------------------
    DEACT STPO0    YES    1720140405  TRK   4   07545968168 5651999 NO
```

..

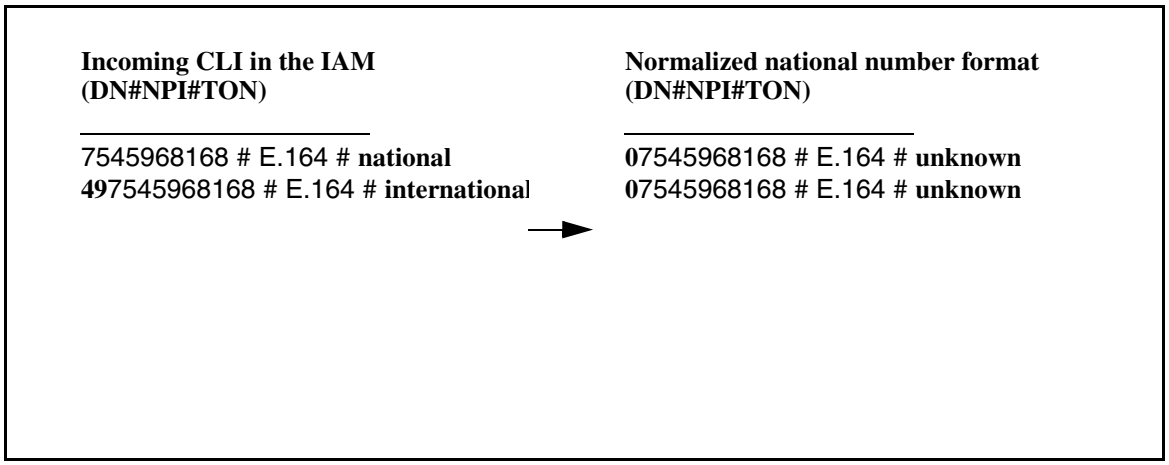


Figure 1 Supported Incoming national DN format

21.2.1.5 Outgoing national CDN trigger

The following figure shows how a CDN sent in an ETSI ISUP V2 IAM or SAM activates CDN monitoring when the equivalent normalized national number matches the target address provisioned in the DNBDORD level, and

the monitoring order is active for that address.

Example without CCC's:

```
DNBDORDER:
>add STPO0 YES 1720140405 TRK CDN 4 outgoing_natl 07545968168 5651999 NO

Add MON ORDER:
ORD STA   GRPID    CDCTDN X25DN       ACC CLLI/LTID/LEN/MAXCCC/DN
    REFNO     CCCREQ IDN              CUGOAE CCCNAME  CCCSYS
    BILLNO  CCCCGSA   SANREQ    SAN


--------------------------------------------------------------------------------
    DEACT STPO0    YES    1720140405  TRK   4    07545968168 5651999 NO
```

Figure 2 Supported outgoing national CDN number format

Outgoing national CDN in the IAM/SAM (DN#NPI#TON)		Normalized national number format (DN#NPI#TON)
07545968168 # E.164 # **unknown**		**0**7545968168 # E.164 # **unknown**
7545968168 # E.164 # **national**	→	**0**7545968168 # E.164 # **unknown**
497545968168 # E.164 # **international**		**0**7545968168 # E.164 # **unknown**

21.2.2 List of features Supported by Trunk Targets

The following list includes the features that the CDN/CLI trunk trigger service supports for national CLI and CDN trunk triggers:

- ETSI Call Forwardingx (x=all Call Forwarding features)
- ETSI Calling Line Identification Presentation (CLIP)
- ETSI Connected Line Identification Presentation (COLP)
- ETSI Hold
- ETSI Call Waiting (CW)
- ETSI Three-Party (3PTY) Conference Call
- International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) MLPP

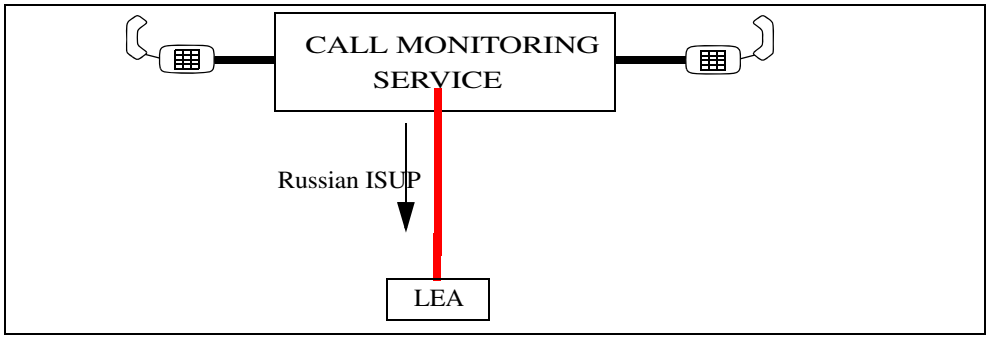
21.2.3 DNBD provisioning capacity

For capacity ty information refer to feature A00009229.

21.2.4 Russian ISUP as CCC link

The interface to the LEA, that is, to the transit network, is implemented using the ETSI ISUP baseline protocol. A detailed description of the parameters passed in the IAM, REL, RLC and CON ISUP messages can be found in the FN of feature AN1940. This activity enables configuring of Russian ISUP, which is a variant of ETSI ISUP, as Call Content Interface.

Figure 3 CCC over Russian ISUP specific variant



21.3 Hardware Requirements or Dependencies

NA

21.4 Software Requirements or Dependencies

NA

21.5 Limitations and restrictions

21.6 Interactions

NA

21.7 Applicable customer facing sections

Fault Management

Logs	NA
Alarms	NA

Configuration

Data Schema	NA

User Interface	NA
Element Management	NA
Security	NA
Service Order	NA
Office Parameters	NA
Accounting (includes AMA billing)	NA
Performance (includes operational measurements)	NA

21.8 Glossary

Term	Description
CCC	Call Contect Channel
CDN	Called Number
CLI	Calling Party Number
LI	Lawful Interception
PVG	Passport Voice Gateway
SIP	Session Initiation Protocol
VRDN	Virtual Router Distribution Node
NGSS	Next Generation Session Server
IAC	International access code
NCC	National Country code
NOA	Nature of Address
NPI	Number Presentation Indication
IAM	Initial Address Message
SAM	Subsequent Address Message
REL	Release message
RLC	Release complete message

22: Functional Description (FN): A00009245

22.1 Feature name and Feature ID

A00009245: Succession Test Trunks: T904 Support

22.2 Description

This activity provides the capability to conduct the Israeli ISUP T904 line trunk test over Gateway TDM trunks in the Succession Packet Trunking IP product. This project is being designed for the IP Greenfield solution for the Telrad market. However, there should be little difference from this design's perspective if the external fabric is IP or AAL2. The AAL1 solution is not being considered at this time. This activity utilizes the capabilities of the Audio Controller (AC) and the Audiocodes Media Server IP (AMS 2010) for performing the tests. Performing the T904 test using the Audio Server (UAS) is not addressed. This document focuses on expanding the CS2K/CS2Kc (core) and Audio Controller (AC) to support T904 TLT. The proposed changes for the AMS 2010, while mentioned for reference purposes, are not addressed in this document.

> ***Note:*** Hybrid offices will continue to use the legacy test equipment via Interworking Bridges (IW's) to get the T904 line trunk test functionality. This activity specifically addresses the T904 TLT for the IP solution in which the legacy equipment is not available.

Currently, the main test hardware for trunk maintenance requests resides in the Integrated Service Module Equipment or ISME. The ISME is specifically designed to accommodate a variety of test and service hardware which can perform frequency and level measurements on specific trunks.

Test Line Tests or TLTs are used to test trunk connections to other adjacent switching offices, both local and toll. TLTs are run under the control of the originating office, often without human intervention at the terminating office, and can be used to test both the originating and terminating ends of trunk.

There are three T900 series tests for Israeli trunks. Only the T904 test is addressed by this activity.

T901 Communications Test (R2/PIE and ISUP trunks)

In this test the ORIG switch establishes communication with the TERM switch, receives ***answer msg*** *and releases the trunk.*

T902 Transmissions Test (R2 trunks)

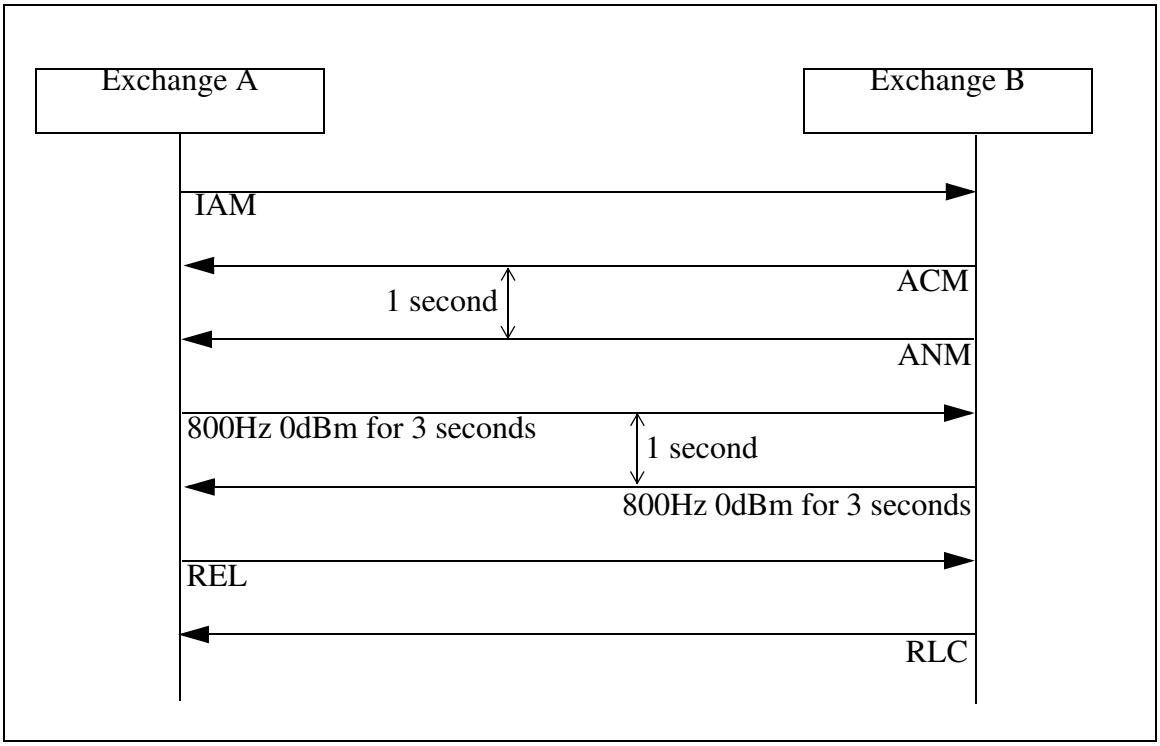
*In this test the ORIG switch establishes communication with the TERM switch, receives **answer msg**, receives **800 Hz tone**, analyses it and releases the circuit.*

T904 Two-way Transmitting Test (R2/PIE and ISUP trunks)

*In this test, the ORIG switch establishes communication with the TERM switch, gets **answer msg**, and sends **800Hz tone** to the TERM switch. The TERM switch analyses the received tone and then sends **800 Hz tone**, which is tested in the ORIG switch. Once the ORIG switch has analyzed the tone, it releases the circuit.*

Note: This test will be supported on Israeli ISUP trunks only, as R2/PIE trunk types are not supported on the existing set of trunk gateways.

Figure 1 T904 Message Sequence



22.2.1 T904 Termination Feature Description

The following steps are performed in the terminating switch after test request is received:

- Seizure of the incoming trunk as a response to receiving the IAM from the originating switch. The IAM should have the following field settings:

— Called Party Address consists of DXF, where “X” is a one-digit number between 0 and 9 that is defined by the administrator.

— Calling Party Category is set to “Test Call”.

— Transmission Medium Requirements is set to “3.1 KHz audio.”

— Nature of Address is set to “Test Line, Test Code.”

— Calling Party Address is not included.

Note: The packet connection between the AMS and the trunk gateway shall use Clear Channel Data.

- Performance of the test protocol. This involves connecting to the AMS to detect the incoming 800Hz at 0 dB tone and to generate the appropriate response tone based on the analysis of the incoming tone:

Table 14: T904 Response Tones

Incoming tone analysis	Response Tone
Tone is within specified range.	800 Hz @ 0dB for 3 seconds.
Tone is determined to be unsteady, out of range or the loss is too high. (-65 DB is max loss.)	Silence @0 dB for 6 seconds.
Tone is determined to have a gain considered too high. (35 DB is max gain.)	Busy tone @0 dB for 11 seconds.

- Release of the trunk (in normal case caused by originator).

22.2.2 T904 Origination Feature Description

The T904 test can be triggered in two ways from the originating switch:

- MAPCI TTP Level Initiation

  The tested trunk is posted on the level mapci;mtc;trks;ttp using command tst. Communication with the far end is done by outpulsing the determined digits. The digits are defined in the table TSTLCONT, subtable TLNOS. The digits are sent automatically and are responsible to activate the test on the far end.

  Sample datafill can be found in Originator Configuration in the CN section.

- MACPCI ATT Level Initiation

  T904 can also be operated from the ATT level as any other test line test.

The following steps are performed on the originating switch:

- Seizure of the outgoing trunk.
- Reserve the AMS test resource.
- Establish connection to the far end.
- Activation of tone to be checked by far end.
- Analysis of the far-end response and appropriate action.
- Release of the trunk.
  - — Execution from TTP MAP level: return trunk to pre-test state
  - — Execution from ATT MAP level:
    - – Success: return trunk to the pre-test state
    - – Failure: take trunk out of service according to the ATT sequence
- Output proper log message
  - — Execution from TTP MAP level: TSTK94X where X is:
    - – 0: Test Success
    - – 1: Communication establishment failure
    - – 2: Tone transmit & receive failure
    - – 3: Tone analysis failure on terminating side
    - – 4: Tone analysis failure on originating side
  - — Execution from the ATT MAP level:
    - – Generate ATT120 log upon test success

Table 15: Test Actions and Test Results according to Trunk States

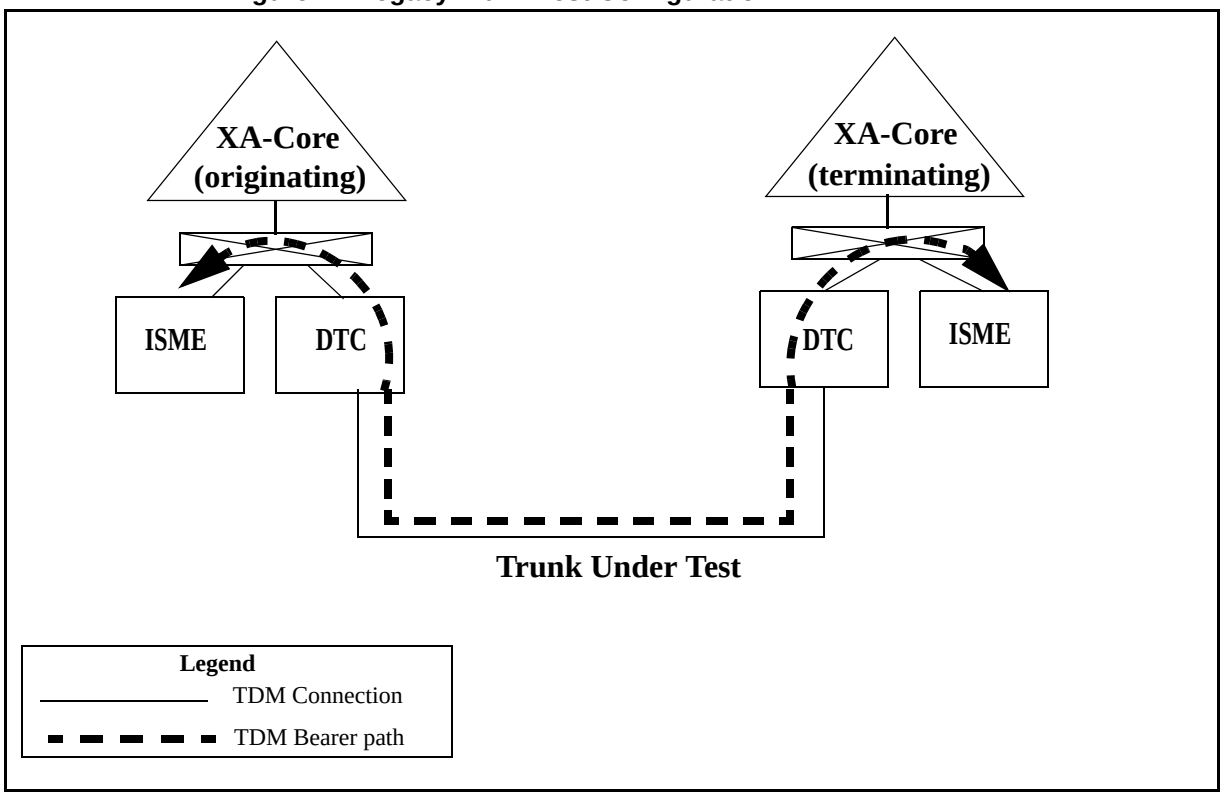
Trunk State	Action	Result
IDL, MB, SZD, INB	Trunk is seized and checked.	PASS or FAIL (According to check result.)
LO, CFL, RMB		FAIL
CPB, CPD, NEQ	Trunk is not seized.	Not checked

22.3 Configuration Overview

22.3.1 Legacy DMS Test Trunk Configuration

In a conventional DMS configuration the Test Line Tests were executed using special hardware connected to the ENET. A request is originated by the user either via a MAP interface or the Automatic Test Trunk system. Connections are created between the Trunk Under Test and the appropriate originating or terminating trunk testing hardware resident on a local ISME. Once completed the test results would be displayed to the user at the MAP or via logs (TSTK940-TSTK944, ATT120).

Figure 2 Legacy Trunk Test Configuration

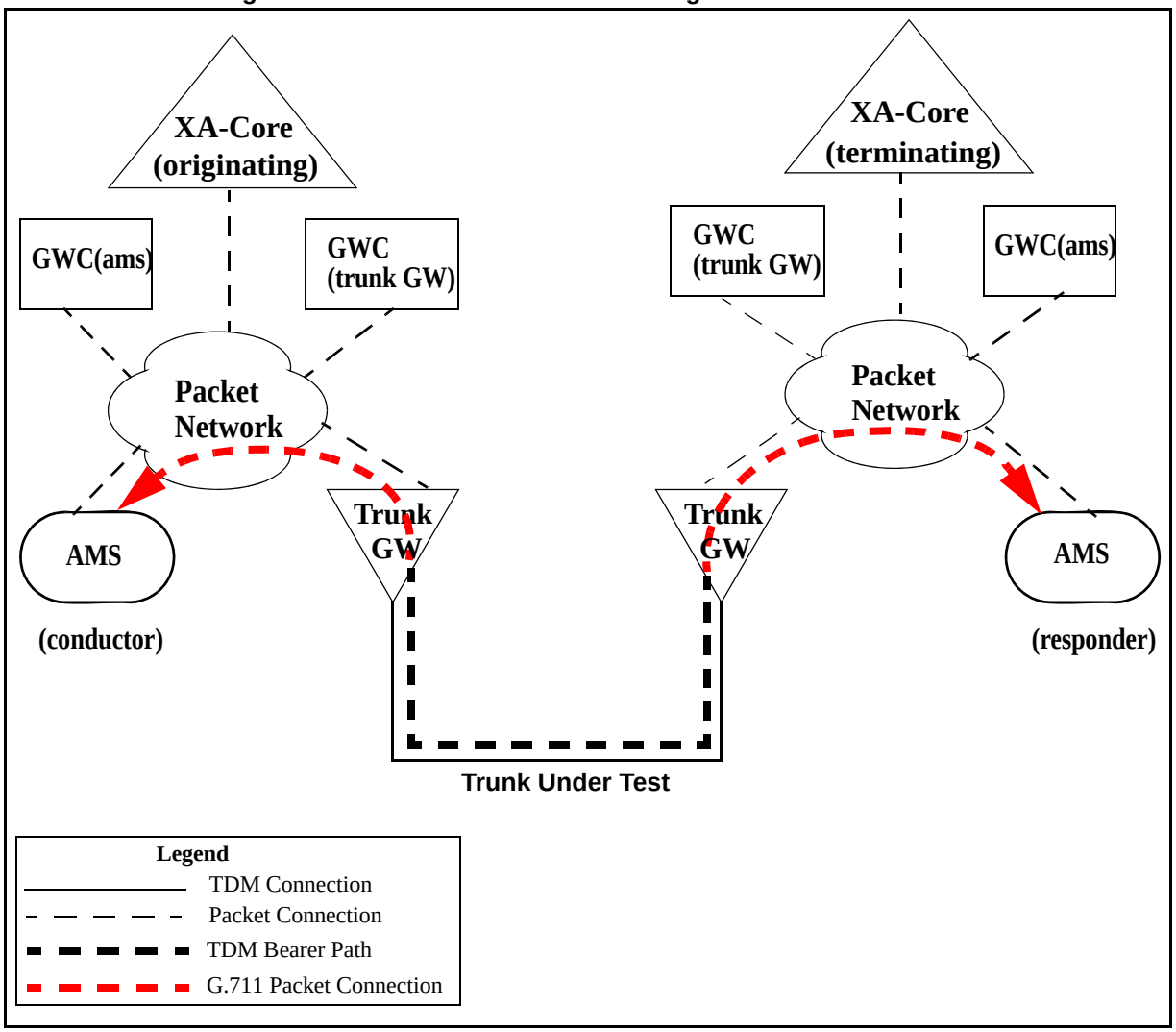


22.3.2 Packet Test Trunk Configuration

The implementation of this feature offers a new method of conducting Test Line Tests via the Audiocodes Media Server IP (AMS 2010). This configuration has the capability of operating without the need for an ENET or ISME. A user can request a test, in the same fashion as a conventional DMS, either via a MAP interface or the Automatic Test Trunk system.

Connections are established between the AMS and the GW TDM Trunk Under Test. Once completed the test results are displayed to the user at the MAP or via logs consistent with the results today on a conventional DMS.

Figure 3 UAS/SAGE Test Trunk Configuration



22.4 Hardware Requirements or Dependencies

For IP: Audiocodes Media Server IP (AMS 2010)

For AAL2: Audiocodes Media Server ATM (AMS 2020)

22.5 Software Requirements or Dependencies

Core: SN09 load or greater

GWC: GC090 load or greater

Provisioning: See “Configuration Walkthrough” in the CN section on page 130.

22.6 Fault Management

Five logs exist for legacy T904 when the test is executed from the TTP MAP level. They are:

- TSTK940: Test Success
- TSTK941: Communication establishment failure
- TSTK942: Tone transmit and receive failure
- TSTK943: Tone analysis failure on the terminating side.
- TSTK944: Tone analysis failure on the originating side.

The TSTK940 log remains unchanged from legacy. The TSTK941, TSTK942, TSTK943 and TSTK944 logs are reused for succession but may contain new fault reasons. See section FM for new error reasons that get displayed for existing TSTK941, TSTK942, TSTK943 and TSTK944 logs.

ATT120 information log referenced in NTP 297-2301-8401 DMS-300 Logs Reference Manual, Volume 1 of 4 is not available.

22.7 Limitations and restrictions

- PIE/R2 trunk types are not currently planned under this activity.
- T900 and T902 TLT tests are not covered under this activity.
- AAL2 testing is not covered under this activity.

22.8 Interactions

Not applicable.

22.9 Glossary

Term	Definition
AC	Audio Controller
AMS 2010	Audiocodes Media Server IP
AMS 2020	Audiocodes Media Server ATM
CLLI	Common Language Location Identifier
GWC	Gateway Controller

Term	Definition
ISME	Integrated Services Module Equipment
IW or IW-SPM	InterWorking SPM
MCMP	Multi-Class Multi-Link PPP
MTM	Maintenance Trunk Module
PLM	PCM Level Meter Card
TDM	Time Division Multiplex
TLT	Test line test
TST	Test Signal Generator card
TTP	Trunk Test Position
TTT	Transmission Trunk Testing

23: Functional Description (FN): A00009282

23.1 Feature name and Feature ID

A00009282: Emergency Stand Alone (ESA) International Support for MG9KEM

23.2 Description

SN08 Introduced Internodal ESA for North American (NA) Markets. This feature provided a Community of Interest (COI) for MG9000 nodes to communicate if unable to communicate with the GWC.

For SN09, this feature is to be expanded to include International markets. COI provisioning will be provided as is used for North America. This feature also removes the restriction that Enhanced ESA be only associated with North America.

International ESA allows the download of information necessary to support International Emergency Stand Alone (ESA) call processing across all native (non ABI) and ABI lines served by a single MG9000 for intra and internodal ESA.

23.3 Hardware Requirements or Dependencies

None

23.4 Software Requirements or Dependencies

This ESA activity on the MG9K is dependent upon two additional activities for successful completion and will be integrated together under an ICAF.

23.5 Limitations and restrictions

- The ESA data from the core will be autonomously downloaded to the MG9000 only once every 24 hours.
- ESA data can be manually downloaded from the core and sent to individual VMGs.
- The MG9000 EM will not allow the modification of any ESA data retrieved from the core.

23.6 Interactions

None

23.7 Glossary

Term	Description
ATM	Asynchronous Transfer Mode
EM	Element Manager (MG9K)
ESA	Emergency Stand Alone
ITP	Integrated Telephony Processor
MEGACO	Media Gateway Control
MG9K	Media Gateway 9000
POTS	Plain Old Telephone Service
SIP	Session Initiation Protocol
TID	Terminal Identifier
VMG	Virtual Media Gateway

24: Functional Description (FN): A00009297

24.1 Feature name and Feature ID

A00009297: QoSR: Support of AAL2

> ***Note:*** The following Functional Description includes both the original QoS feature 89007819 and the updates related to A00009297, QoSR: Support of AAL2.

24.2 Description

This document covers the QoS Collector Application functionality supported in SN09.1 time frame.

In Voice over IP/VoATM networks, Quality of Service (QoS) can be adversely affected by the components in the network. Unlike TDM networks where the voice quality is consistent for all calls, VoIP/VoATM networks can experience different voice quality on all calls.

The common parameters that make up voice quality are:

- Packets sent
- Packets received
- Packet loss
- Octets sent
- Octets received
- Inter-arrival latency
- Jitter

All gateways beginning SN06 VoIP solutions report these statistics via end-of-call reporting mechanisms specific to the protocol used for MGC - VMG communication.

Beginning SN09.1, QCA will collect QoS Reporting statistics from ATM AAL2 Gateways too. The statistics collected are;

- Packets-sent (aal2/ps - H248 representation)
- Packets-Received (aal2/pr - H248 representation)
- Total Packets lost (aal2/tpl - H248 representation)
- Jitter (aal2/jit - H248 representation)

It is the purpose of this activity to design a method for reporting these QoS parameters on a per call basis for the purposes of;

- Network engineering
- Trend analysis
- Trouble-shooting network problems
- SLA validation

This is accomplished by implementing a reporting mechanism that will allow QoS reports (as IPDR records) to be delivered to a customer provided OSS for processing. In order to achieve SLA validation, QoS reports are correlated to appropriate billing records so that the QoS of billed calls can be determined.

QoS Reporting is applicable for more than just VoIP networks. It can be used in hybrid networks as well. From SN06 time frame to SN09 time frame QoS Reporting was limited to pure IP networks which consist only of GWC driven GWs.

Support for SPM peripherals and hybrid networks will be accomplished in a later release.

Beginning SN09.1 time frame QoS Reporting is extended to ATM AAL2 fabric which consists of GWC driven GWs (which support reporting of End of Call QoS statistics)

The proposed architecture for QoS Reporting beginning SN06 consists of the following components;

1. QoS Correlation ID and billing
2. QoS Reporting Application (on GWC)
3. Provisioning
4. QoS Report collection
5. QoS Report processing

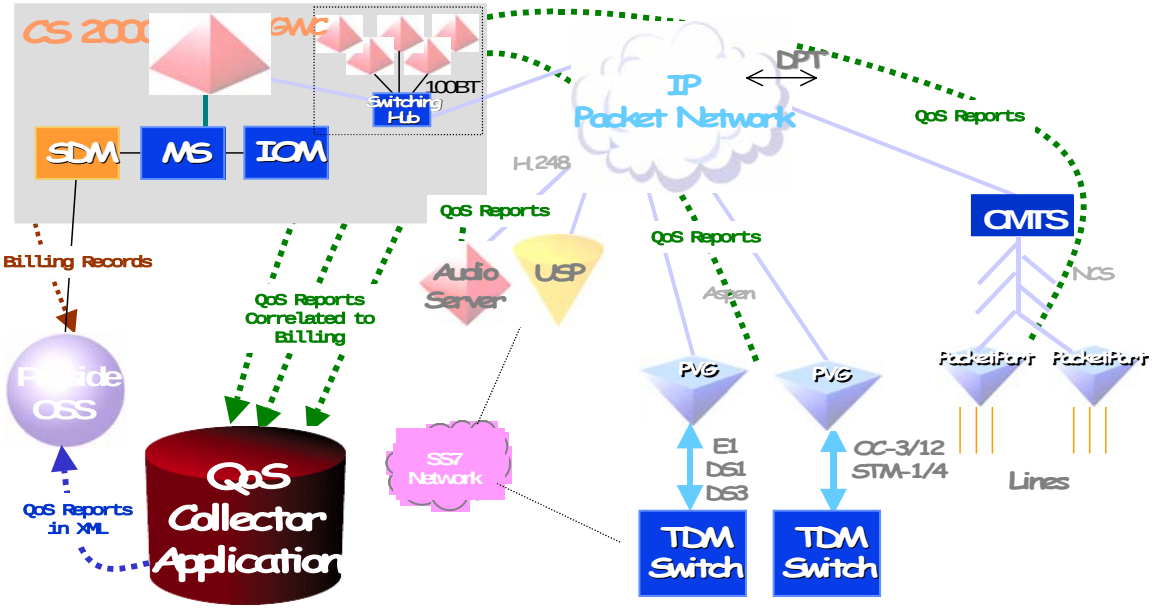
This activity implements component 4. QoS Report collection, the QoS Collector Application (QCA)

24.2.1 System behavior

All QoS (IPDR) records are stored on a QoS Collector Application (QCA) host. The QCA will receive binary QoS records from the GWCs, converts these to QCA IPDR records and stores them in a file. The QCA IPDR records can be obtained by the OSS for processing.

The configuration of this proposal is shown in Figure 1, "QoS Reporting in a VoIP/VoATM Network"

Figure 1 QoS Reporting in a VoIP/VoATM Network



24.2.2 Configuration

The configuration details for the QoS Collector Application are provided by a properties files. The properties file is located at /opt/nortel/qca/properties/qca.properties and can be configured by the user.

The QCA properties are given in Table 1, “QCA properties,” on page 407 and an example QCA properties file is given in Figure 2, "Example of the QCA properties file".

Table 1 QCA properties

Name	Description	Units	Range	default
portNumber[3]	the port number the QCA accepts connections on	N/A	20000 to 20004	20000
MaxFileSize	maximum size of an output file	MBytes	1 to 100	5
MaxFileTime	interval output file is open	minutes	1 to 240	15
RetainFileTime	how long the output files should be retained	days	1 to 30	5
recycleToD	the hour in the day the directories will be recycled	hour	0 to 23	0

Table 1 QCA properties

Name	Description	Units	Range	default
fileExt	the output file extension	N/A	String	xml
nodeName	the node name to be used in the output files	N/A	String	QCA
closedFileCompression[1]	whether the file should be compressed when closed and moved to today	boolean	true or false	true
oldFileCompression[1,2]	whether the files should be compressed at the first directory recycle	boolean	true or false	true

Notes:

1. File compression may be required as there is limited disk space for QCA IPDR record storage.
2. If *closedFileCompression* is true the value of the *oldFileCompression* property is negated as the files will have already been compressed.
3. A range of port numbers is provided for flexibility. The main use is for upgrade purposes, where two QCA instance may be running on a single host. Multiple QCAs, and therefore port numbers, should not be used to segregate QCA traffic.
4. Starting SN09FF the default value of MaxFileSize used in qca.properties file is 5 MB. This change is to improve QCA performance especially on Large Offices where the traffic rate could be as high as 2M BHCA. CR fix for Q01225163 adds this change.

The qca.properties file is read when the QCA is started, therefore the QCA must be stopped and restarted for changes in the qca.properties to be picked up.

When the qca.proprties file is read the contents is validated. If any of the properties are not present or invalid, the default value is automatically used. A warning customer log is generated to indicate that the default value is being used.

An example customer log warning:

```
Oct 11 12:00:02 wmdhs0j8 main:0001 QCA201 WARNING init label:
RetainFileTime property in properties/qca.properties is out of
range. QCA is starting with default retain file time of 5 days
```

Figure 2 Example of the QCA properties file

```
# QCA Properties file
# The QCA will have to be restarted for changes in the properties
# file to be reflected in the application's operation

# The maximum size of a file, in MBytes, before it is closed
# Range is 1 to 100. Default is 1.
  MaxFileSize=1

# The maximum time, in minutes, a file can be open before
# it is closed
# Range is 1 to 240. Default is 15.
  MaxFileTime=15

# Hour of the day that the directory structure is recycled
# Range 0 (12:00 AM) to 23 (11:00 PM). Default is 0 (12:00 AM).
# Do NOT specify minutes.
  recycleToD=0

# port number to start application on.
# Range is 20000 to 20004. Default is 20000.
  portNumber=20000

# How long, in days, the files are kept before deleting
# VERY IMPORTANT: Depending on the call volume and the number of
# days for file retention it could be possible to exhaust all
# available disk space, therefore the value of this property
# should be considered in great depth.If QCA is started with
# the value of this property less than the number of today
# directories for a given port the older directories will be
# deleted.
# Range 1 to 30. Default is 5.
  RetainFileTime=5

# File Extension used in the QCA output file name.
# Default is xml.
  fileExt=xml

# Node name to be used in the QCA output file name.
# Default is QCA.
  nodeName=QCA

# true or false value indicating whether the output file
# should be compressed when closed. Default is true.
  closedFileCompression=true

# true or false value indicating whether the file should be
# compressed at the first directory recycle
# Note: If closedFileCompression is true the value of the
# oldFileCompression property is negated as the files will have
```

24.2.3 Starting QCA

The `qca_server` script is used to start the QCA. The user should log in as root to execute this script.

When the `qca_server` script is run the following warning is displayed:

```
Attempting to register QCA as Qca with PMFADM.
```

If a QCA instance has not already been started with `qca_server` the following message is displayed:

```
Registration as Qca was ok. QCA started.
```

If a QCA instance has already been started with `qca_server` the following message is displayed:

```
pmfadm: Request "Qca" already queued
Could not register QCA as Qca with PMFADM, this suggests a QCA
instance is already running.
```

When the QCA is started the following steps are performed:

- the QCA is registered with PMFADM (processes monitor facility administration).
- This is a Solaris utility that monitors register processes and restarts the process if no longer running.
- configuration details (qca.properties file) are read
- If any of the properties information is not present or is invalid the default value is used and a customer log is generated to indicate this. It is at this point the user can stop the QCA if using default values is not acceptable.
- the QCA attempts to open a server socket on the specified port.
- If the specified port is in use the QCA can not be started.
- a file management process is started
- If the QCA output directory is not available when the QCA is started the directories are created.
- If a file exists in the active output directory, this indicates that QCA did not stop gracefully, the QCA will attempt to complete the file and move it to the today directory.
- the QCA waits for connections from clients (GWCs and SPMs) on the port number specified in the qca.properties.

24.2.4 Stopping QCA

The `stop_qca` script is used to stop the QCA. The user should log in as root to execute this script.

When the `stop_qca` script is run the following warning is displayed:

```
Are you sure you want to stop the QCA? Have you checked the port
number in qca.properties? [ no or yes ]
```

If the port number in qca.properties has been checked and is correctly specified for the QCA to be stopped, this should be validated against the QCA datafill in PTM, then **yes** should be entered, otherwise **no** should be entered and the port number checked.

If a QCA instance was started by `qca_server` the following message will be displayed:

```
Attempting to unregister QCA as Qca from PMFADM.
Attempting to stop local QCA on port : 20001
QCA stopped successfully.
```

If a QCA was not was started by `qca_server` the following message will be displayed:

```
Attempting to unregister QCA as Qca from PMFADM.
pmfadm: "Qca" No such <nametag> registered

QCA not registered with PMFADM as Qca, so stop_qca aborted.
```

If the above message is seen the `query_qca` script should be used to determine if a QCA instance is running on the host.

When the QCA is stopped the following steps are performed, in order:

- the QCA is unregistered with PMFADM
- the QCA stops accepting connections from clients
- the connection to the client(s) is closed
- the IPDR / XML structure in the output file is closed
- the output file is closed and moved to the today directory

Note: to avoid alarms being generated by all the GWCs sending QoS records to the QCA when the QCA is stopped the QCA details must be removed from PTM first. Please refer to activity 89007781 - QoS Reporting: Provisioning for QoS Reporting provisioning details.

24.2.5 Client (GWC) connection to QCA

When the QoS reporting mechanism is started on a client (GWC) it will connect to the QCA as specified in PTM, e.g. IP Address and port.

When a connection is established the QCA waits to received data from the client (GWC).

24.2.6 Client (GWC) Connection heart beat

The TCP/IP connection between the client and QCA will be automatically closed if it is not used for more than 2 hours. To ensure the connection is not closed in this circumstance, the client will send a ‘heart beat’ message after 2 hours of inactivity.

The QCA simply receives the client ‘heart beat’, and does not generate a QCA IPDR record.

24.2.7 QCA File Management

The active output file is in the active directory. When a file is closed it is moved to the today directory.

24.2.7.1 Initialization

When the QCA is started the following file management steps are performed:

- the output directories are created if they do not already exist.
- any files in the active output directory are validated, ensuring that the last IPDR is complete and that the file structure is closed. Once the file is complete it is moved to the today output directory.
- all ‘today’ directories older than the file retention period are deleted. This can occur if the qca.properties is change such that file retention period is reduced.
- a new file is created using the naming convention given below. If the file name already exists the new file will have the number 0 added before the file extension, if this exists, the number 1 will be used, then 2 and so on.

24.2.7.2 Output directory

The directory used for the current QCA output is:

/data/qca/”port number”/output/active

Note: In SN07, QCA registers with the ‘servman’[1] on the SSPFS machine. Depending on your selection of `RetainFileTime` property in qca.properties file and your calculation of Disk consumption depending on Call traffic at your CO, proper disk partition size of /data/qca should be requested during SSPFS installation. For calculation on how much disk space should be allocated, refer to section 2.2.7.5.

Where “port number” is the port number that is specified in qca.properties and that the QCA accepts connections on. This allows the output of two QCAs running on the same host to be distinguished.

24.2.7.3 File names

The QCA will use the following file naming convention:

<Node Type>.<Node Name>.<ReportName>.Year.Mon.Date_HR.MN_<TZ>.<File Ext>

For example:

QCA.Telco_Switch_35.QoS.2002.04.11_02.45_EDT.xml

[1]servman is the application service manager on the SSPFS platform starting SN06.2. servman manages registration and deregistration of all client applications running on the SSPFS machine whether it is simplex or clustered.

Where each of the elements is described as:

<NodeType> - A Nortel defined string identifying the product origination. Always “QCA”.

<Node Name> - This name should MATCH the name of the node that is used in faults, in configuration (FQDN), in accounting and in GUIs. This value is configurable as property nodeName in qca.properties.

<Report Name> - The name of the script/filter/report that is used to create this file. There may be 1 or more report names in operation for a given NE simultaneously. Each report type must be identified in the filename. Always “QoS”

<**Year.Mon.Date_HR.MN_**> - This field when present in the active directory refers to the time when the file was opened or created in the active directory. The same field when present in today directories refers to the time the file was closed i.e the time when the files are closed and recycled to the today directories.

<TZ> - This is the Time Zone of the NE the Performance data is being collected from. This can be an off set from UMT or GMT.

<File Ext> - The file extension specified in qca.properties or the default xml.

24.2.7.4 Output file rotation (closure)

QCA file management provides file rotation (closure) based on file size and time the file has been open, on a ‘which ever comes first’ basis. Theses values are MaxFileSize and MaxFileTime, respectively, in qca.properties.

24.2.7.5 Output file compression

Due to the size of each QCA IPDR record (maximum about 840 bytes) the required disk space to store several days of QCA output files could be very large.

The required disk space storage requirement calculation is a follows:

Assuming:

- BHCA = 550K
- Calls per day = 10 x BHCA = 5.5 M
- QoS records per day = 2 x Calls per day = 11 M
- Record size = 840-bytes
- Compression ratio = 88% (achieved in testing)

Per day disk space required = 11 M x 840 = 8.6 GBytes

When using compression = 8.6 GBytes * 0.12 = 1 GByte

It can be seen that file compression offers a major saving is disk space requirements. And with out compression the disk space in the /data/qca partition would be quickly exhausted.

The file compression is controlled by two properties, closedFileCompression and oldFileCompression.

closedFileCompression controls whether the active file should be compressed when it is closed and moved to the today directory.

oldFileCompression controls whether the retained files should be compressed when the output directories are recycled. When oldFileCompression is enabled, the files in the today-n directories will be checked, and compressed if required, every time directory recycling occurs.

24.2.7.6 Output file retention

The file management of the QCA follows that implemented for the SN05 feature SNMP Performance Measurement Poller (59039902). The output directory structures will contain a *number* of directories, for the current active file, today's closed files and the last *number-1* days closed files.

The clean-up mechanism is described by two parameters:

- 'retain file duration' (RetainFileTime) - how long (in days) should the files be retained on the local disk.
- 'recycle time of day' (recycleToD) - the hour of the day that the today directories are recycled.

Both are parameters specified in the qca.properties file read when the QCA is started.

At a predefined time (recycleToD in qca.properties, default is 12:00 AM), the output directories will be recycled.

The today-n directories are not created when the QCA is started but when the output files are recycled.

When the today directory reaches the maximum file retention period the information is discarded.

E.g.Output file structure if *number* were 30:

/data/qca/"port number"/output/active

/data/qca/"port number"/output/today

/data/qca/"port number"/output/today-1

/data/qca/”port number”/output/today-2

.

/data/qca/”port number”/output/today-28

/data/qca/”port number”/output/today-29

Note: if the QCA is stopped and restarted with a new ‘retain file duration’, that is less than the previous ‘retain file duration’ the QCA operated with, any existing today directories older than the new ‘retain file duration’ will be deleted.

The value for the ‘retain file duration’ should be considered carefully as the operation of the QCA and other applications may be impacted if there is no free disk space because it is used to store QCA output files.

In arriving at a value for the ‘retain file duration’ the following should be considered:

- the BHCA and total number of calls per day.
- total disk space available for file retention
- whether file compression is used.

A similar calculation to that in section 2.2.7.5 ‘Output file compression’ should be used to determine the require ‘per day’ disk space requirements and there fore the ‘retain file duration’, e.g.:

$$\text{‘retain file duration’} = \frac{\text{available disk space in MBytes}}{\text{required MBytes/day}}$$

Suppose the /data/QCA partition size is 8GBytes. Using the assumptions in section 2.2.7.5 ‘Output file compression’ and the above calculation the maximum ‘retain file duration’ value is:

$$\frac{\text{8000 MBytes}}{\text{1000 MBytes}} = \text{8days}$$

However, you may request a higher partition size of /data/qca during SSPFS installation as per the calculation shown in section 2.2.7.5.

24.2.7.7 Retaining modified qca.properties over an Upgrade

Note: Applicable only if values of parameters in qca.properties have been modified (different than default), and the same are required to be maintained over QCA upgrade.

When QCA is installed, qca.properties at /opt/nortel/qca/properties contains default values of various parameters (For example portNumber = 20000, and

retainFileTime = 5). If customers are using other than default values of parameters in qca.properties file, and are planning for upgrade of QCA, following procedure needs to be followed to retain these customized values after upgrade, without having to stop/re-start QCA:

1. Before proceeding with upgrade, change the qca.properties on the inactive side of the cluster as required. (for example, portNumber = 20001, retainFileTime = 5)
2. State of QCA on the inactive side of the cluster: NOT RUNNING
3. Perform the upgrade. (The procedure will involve swacting of the cluster).
4. After the upgrade is complete, the newly active unit of the cluster will have the qca.properties of the previous inactive unit. This way we can expect the modified qca.properties to be maintained over an upgrade, without having to stop/re-start QCA.
5. If the above procedure is not followed, default values of parameters will remain in qca.properties.

For example, consider the present qca.properties have the values for portNumber and retainFileTime to be 20001 and 1 respectively. (It is 20000 and 5 respectively by default). If this qca.properties is to be maintained over an upgrade, the qca.properties of the inactive unit of the cluster has to be updated with these values, before performing the upgrade.

Problem scenario (Before Upgrade):

Active unit	Inactive unit (qca.properties not modified)
(SN08)	(SN09)
portNumber: 20001	portNumber: 20000
RetainFileTime=1	RetainFileTime=5
State: QCA running	QCA Not running

Problem scenario (After Upgrade):

Active unit	Inactive unit
(SN09)	(SN08)

portNumber: 20000 portNumber: 20001

RetainFileTime=5 RetainFileTime=1

State: QCA Running QCA Not running

As seen in above problem scenario, qca.properties will not be maintained over an upgrade if qca.properties not modified in the inactive unit of the cluster.

Solution (Before Upgrade):

Active unit Inactive unit (qca.properties modified)

--- ---

(SN08) (SN09)

portNumber: 20001 portNumber: 20001

RetainFileTime=1 RetainFileTime=1

State: QCA running QCA Not running

Solution (After Upgrade):

Active unit Inactive unit

--- ---

(SN09) (SN08)

portNumber: 20001 portNumber: 20001

RetainFileTime=1 RetainFileTime=1

State: QCA Running QCA Not running

(No records lost)

As seen above, updating qca.properties of inactive unit of the cluster will result in maintaining modified qca.properties over an upgrade.

24.2.7.8 Reporting disk space issues

As the QCA operates, disk space in /data/qca is used for the active file and to retain closed files. If the disk space in /data/qca becomes exhausted this would

effect the operation of the QCA. The QCA uses customer logs to report disk space issues before all the space is used to reduce the possibility of completely filling the partition.

Every time the QCA creates a new file it will attempt check the available disk space, in the unlikely event that available space is not determinable the QCA will write a debug log to a file.

The QCA determines the number of free bytes available in the /data/qca partition and compares this with 3 boundary values; 1 GByte, 500 MBytes and 100 MBytes.

1 GByte boundary

If the available disk space is greater than 1 GByte then no further action is taken. However, if the available disk space is less than 1Gb and more than 500Mb, a minor customer log/alarm is generated.

If some disk space is made available in the /data/qca partition, after a customer alarm was raised, to make the available disk space great than 1GByte, the QCA raises a clear customer log for the minor alarm when the next new file is created.

However, if no action is taken and the available space still lies with between 1 GByte and 500 MBytes when the next file is created, the QCA will generate another minor customer log/alarm.

500 MByte boundary

If the available disk space is less than 500 MBytes and more than 100 MBytes, a major customer log/alarm is generated

If the available disk space goes above 500 MBytes, but below 1 GByte, the QCA raises a clear customer log for the major customer log/alarm when the next new file is created.

If the available disk space goes above 1 GByte the QCA raises clear customer logs for both the major and minor customer logs/alarms when the next new file is created.

However, if no action is taken and the available space still lies with between 500 MBytes and 100 MBytes when the next file is created, the QCA will generate another major customer log/alarm.

100 MByte boundary

If the available disk space is less than 100 MBytes a critical customer log/ alarm is generated

If the available disk space goes above 100 MBytes, but below 500 MBytes, the QCA raises a clear customer log for the critical customer log/alarm when the next new file is created.

If the available disk space goes above 500 MBytes, but below 1 GByte, the QCA raises clear customer logs for both the critical and major customer logs/ alarms when the next new file is created.

If the available disk space goes above 1 GByte, the QCA raises clear customer logs for the critical, major and minor customer logs/alarms when the next new file is created.

However, if no action is taken and the disk space is completely exhausted the QCA will generate a critical customer log/alarm and the QCA will be stopped.

In the scenario where write access is prevented the application will raise a critical customer log/alarm and the QCA will be stopped.

24.2.8 Growing the Size of /data/qca

See Appendix C for the Procedure to grow the size of Partition /data/qca.

24.2.9 QoS record processing

At the end of every call the client reports the QoS statistics to the QCA in a binary QoS record. The QCA validates the record, ensuring the record sequence number, version and length are correct. The QCA then converts the record to an IPDR form. The QCA IPDR record is then written to a file.

Until SN07 the QoS record had only 1 version (size 132 Bytes). In SN08 the QoS Record message version is 2 (size 136 Bytes).

Beginning SN09 the QoS record has version 3 (size 180 = 136 Bytes + 10 Bytes Timestamp - 2 byte filler inVersion 2 + 32 Bytes (GWName is changed to 64 Bytes as compared to 32 Bytes prior to SN09) + 4 byte filler for Version 3.)

Beginning SN09.1 the QCA supports version 4 and version 5 QoS binary Records that come from patched SN07 and SN08 GWCs respectively.

24.2.9.1 Binary QoS record format

The QoS record sent from the client (GWC) is a binary message. A description of the binary QoS record fields is shown in the following table.

Table 2 Binary QoS record fields (version 1 SN07)

Name	Description	Range
MT (MGC Type)	The type of client (MGC) the QoS record was generated by	0 - GWC 1 - SPM

Name	Description	Range
Msg Type	Message type	0 - QoS record 1 - heart beat
Sequence number	Record sequence number	0 to 16777215
RT (Report Type)	Report Type	0 - local 1 - remote
ver (version)	The QoS record version	0 to 15
MGC number	The number of the client (MGC) the QoS record was generated by	0 to 255
Msg length	The length of the message (including header)	0 to 255 (should be 130)
Gateway port number	The port number on the Gateway used in the call	0 to 65535
Gateway IP Address	The IP Address of the Gateway used in the call	4-bytes
Gateway FQDN	Consists of two separate fields; the Gateway name (32 Bytes) and End Point (32 Bytes).	64-bytes
Switch CLLI	The CLLI of the CS2K the client is subtended to	16-bytes
Correlation ID	The correlation id that can be used to correlate the QoS record to an AMA record	10-bytes
Packets Sent	The total number of packets transmitted	0 to 4294967294
Packets Received	The total number of packets received	0 to 4294967294
Octets Sent	The total number of payload octets transmitted	0 to 4294967294
Octets Received	The total number of payload octets received	0 to 4294967294
Packets Lost	The total number of packets lost	0 to 4294967294
Jitter	Estimate of packet interarrival time (milliseconds)	0 to 65534
Latency	Estimate of network latency (milliseconds)	0 to 65534

Table 3 Binary QoS record fields (version 2 SN08)

Name	Description	Range
MT (MGC Type)	The type of client (MGC) the QoS record was generated by	0 - GWC 1 - SPM
Msg Type	Message type	0 - QoS record 1 - heart beat
Sequence number	Record sequence number	0 to 16777215
RT (Report Type)	Report Type	0 - local 1 - remote
ver (version)	The QoS record version	0 to 15
MGC number	The number of the client (MGC) the QoS record was generated by	0 to 255
Msg length	The length of the message (including header)	0 to 255 (should be 130)
Gateway port number	The port number on the Gateway used in the call	0 to 65535
Gateway IP Address	The IP Address of the Gateway used in the call	4-bytes
Gateway FQDN	Consists of two separate fields; (the Gateway name and end point)	64-bytes
Switch CLLI	The CLLI of the CS2K the client is subtended to	16-bytes
Correlation ID	The correlation id that can be used to correlate the QoS record to an AMA record	10-bytes
Packets Sent	The total number of packets transmitted	0 to 4294967294
Packets Received	The total number of packets received	0 to 4294967294
Octets Sent	The total number of payload octets transmitted	0 to 4294967294
Octets Received	The total number of payload octets received	0 to 4294967294
Packets Lost	The total number of packets lost	0 to 4294967294
Jitter	Estimate of packet interarrival time (milliseconds)	**0 to** 4294967294
Latency	Estimate of network latency (milliseconds)	**0 to** 4294967294

Table 4 Binary QoS record fields (version 3 SN09)

Name	Description	Range
MT (MGC Type)	The type of client (MGC) the QoS record was generated by	0 - GWC 1 - SPM
Msg Type	Message type	0 - QoS record 1 - heart beat
Sequence number	Record sequence number	0 to 16777215
RT (Report Type)	Report Type	0 - local 1 - remote
ver (version)	The QoS record version	0 to 15
MGC number	The number of the client (MGC) the QoS record was generated by	0 to 255
Msg length	The length of the message (including header)	0 to 255 (should be 130)
Gateway port number	The port number on the Gateway used in the call	0 to 65535
Gateway IP Address	The IP Address of the Gateway used in the call	4-bytes
Gateway FQDN - GW Name	**Consists of two separate fields; (the Gateway name**	**64-bytes**
Gateway FQDN Endpoint	**End point**	**32-bytes**
Switch CLLI	The CLLI of the CS2K the client is subtended to	16-bytes
Correlation ID	The correlation id that can be used to correlate the QoS record to an AMA record	10-bytes
Packets Sent	The total number of packets transmitted	0 to 4294967294
Packets Received	The total number of packets received	0 to 4294967294
Octets Sent	The total number of payload octets transmitted	0 to 4294967294
Octets Received	The total number of payload octets received	0 to 4294967294

Name	Description	Range
Packets Lost	The total number of packets lost	0 to 4294967294
Jitter	Estimate of packet interarrival time (milliseconds)	0 to 4294967294
Latency	Estimate of network latency (milliseconds)	0 to 4294967294
StartTimeStamp*	Call Start Timestamp	5 -bytes.
EndTimeStamp*	End Time Timestamp	5 -bytes.

*Start and End timestamp addressed in the following section.

24.3 Timestamp (Call Start Time and Call End Time)

24.3.1 DISCLAIMER:

- QoS records contain performance measurement data only and they are never intended to be used as a source for billing information.
- Call durations for billing/revenue generation purposes have to be based on the time data in the billing records, such as AMA and CDR records, and not QoS records.

24.3.2 Timestamp Support

Timestamp support (Call Start Time and Call End Time) for QoS IPDR records are supported beginning SN09. This activity is tracked under A0009297 and provides support to display correct call start time and call end time in the QoS IPDR XML records.

All QoS (IPDR) records are stored on a QoS Collector Application (QCA) host. The QCA receives binary QoS records from the MGCs, converts these to QCA IPDR records and stores them in a file. The QCA IPDR records can be obtained by the OSS for processing

Prior to SN09, the timestamp parameter (Call Start time and Call End time) was hardcoded to a default value 1970-01-01T00:00:00.000Z and thus the QoS record output in the XML file show this default value for all calls irrespective of the actual call start time and call end time for the particular call and does not depict the correct value.

GWC sends end of call statistics to active QCA servers. Timestamps (Call Start and Call End Timestamp) are IPDR parameters that would be displayed on a QoS Report along with other IPDR parameters such as timezone, call completion code, hostname, subscriberID, unique Call ID, IP Address, port

number, sequence number and End of Call QoS Statistics such as average packet latency, inbound byte count, outbound byte count, inbound packet count, outbound packet count, packet lost and packet delay.

24.3.2.1 Timestamp Format

Timestamp (Call Start Time and Call End TIme) are in ISO 8601 format. The format is shown below:

YYYY:MM:DD:HH:MM:SS:MS Where,

YYYY - Year

MM - Month

DD -Day

HH - Hour

MM - Minute

SS - Second

MS - Millisecond

This timestamp is included in the QoS Binary message and this in turn is parsed by the QCA to extract the Call Start Time and Call End Time. QCA IPDr records show these extracted timestamp.

The timestamp used for the QoS Binary records and QoS IPDR XML records (Call Start Time and Call End Time) will be in Universal coordinated time (UTC) previously known as Greenwich Mean Time (GMT). Time represented as UTC will be universal and will not have to worry about Daylight saving time.

GMT is World Time and the basis of every world time zone which sets the time of day and is at the centre of the time zone map. Call Start Time and Call End Time use UTC time format and these timestamp will be represented in QCA XML reports.

> ***Note:*** Since Timestamps are in UTC time format they do not support Day Light Saving time. Hence the Time value in the start and End time might be off by 1 hour compared to the time in billing records during the period between 1st April to 31st October every year.

24.3.2.2 Call Start Time and Call End Time

Call Start TimeStamp (STS) and End TimeStamp (ETS) will be depicted in the QCA Xml records. An example of the timestamp is given below:

<StartTime>2005-01-01T14:52:57.000Z</StartTime>

<EndTime>2005-01-01T14:59:01.000Z</EndTime>

24.3.3 QCA IPDR record format

The output of the QCA is a single stream (file) of IPDR Version 3.1-A.0.2 compliant records.

24.3.3.1 QCA IPDR elements

The IPDR elements used in the QoS output format are shown in the following table.

Table 5 QCA IPDR tags

QoS Field Tag	Type	Range
StartTime	dateTime	ISO 8601 format.
EndTime	dateTime	ISO 8601 format.
timeZoneOffset	integer	Time offset, in minutes, of local time zone referenced to GMT.
callCompletionCode	String	Final call completion code for billing use.
originalDestinationId	String	Called-party (designation) number
hostName	String	0 to 22 characters
subscriberId	**String**	**0 to 65 characters (version 1 and 2)**
		0 to 97 characters (version 3)
uniqueCallId	String	20 hexadecimal digits
ipAddress	String	7 to 15 numerical characters
portNumber	String	0 to 2147483647
seqNum	integer	0 to 16777215
averagePacketLatency	integer	0 to 65536 (version 1)
		0 to 2147483647 (version 2 and 3)
inboundByteCount	integer	0 to 2147483647
outboundByteCount	integer	0 to 2147483647
inboundPacketCount	integer	0 to 2147483647
outboundPacketCount	integer	0 to 2147483647
inboundLostPacketCount	integer	0 to 2147483647
packetDelayVariation	integer	0 to 65536 (version 1)
		0 to 2147483647 (version 2 and 3)

An example QCA IPDR record (for IP/AAL2 fabric):

```
<IPDR>
<StartTime>2005-10-05T15:30:09Z</StartTime>*
<EndTime>2005-10-05T15:32:12Z</EndTime>
<timeZoneOffset>0</timeZoneOffset>
<callCompletionCode>CC</callCompletionCode>
<originalDestinationId></originalDestinationId>
<hostName>GWC3@COMITIP</hostName>
<subscriberId>aaln/1@ttp018.mgsite-2.b4sky.ott</subscriberId>
<uniqueCallId>43c01738000f13e30d05</uniqueCallId>
<ipAddress>10.0.15.1</ipAddress>
<portNumber>2427</portNumber>
<seqNum>18</seqNum>
<averagePacketLatency>0</averagePacketLatency>
<inboundByteCount>41538</inboundByteCount>
<outboundByteCount>0</outboundByteCount>
<inboundPacketCount>301</inboundPacketCount>
<outboundPacketCount>0</outboundPacketCount>
<inboundLostPacketCount>0</inboundLostPacketCount>
<packetDelayVariation>0</packetDelayVariation>
</IPDR>

* Note: Starting SN09, the value of the timestamp in the IPDR
records will show the actual value and not the defaulted value
of 1970-01-01T00:00:00.000Z. This is tracked under the activity
A00009297 and is addressed in section <2.3>
```

An example QCA IPDR record (for AAL2 fabric):

```
<IPDR>
<StartTime>2005-10-05T15:30:09Z</StartTime>*
<EndTime>2005-10-05T15:32:12Z</EndTime>
<timeZoneOffset>0</timeZoneOffset>
<callCompletionCode>CC</callCompletionCode>
<originalDestinationId></originalDestinationId>
<hostName>GWC3@COMITIP</hostName>
<subscriberId>aaln/1@ttp018.mgsite-2.b4sky.ott</subscriberId>
<uniqueCallId>43c01738000f13e30d05</uniqueCallId>
<ipAddress>10.0.15.1</ipAddress>
<portNumber>2427</portNumber>
<seqNum>18</seqNum>
<averagePacketLatency>0</averagePacketLatency>
<inboundByteCount>41538</inboundByteCount>
<outboundByteCount>0</outboundByteCount>
<inboundPacketCount>301</inboundPacketCount>
<outboundPacketCount>0</outboundPacketCount>
<inboundLostPacketCount>0</inboundLostPacketCount>
<packetDelayVariation>0</packetDelayVariation>
</IPDR>

* Note: Starting SN09, the value of the timestamp in the IPDR
records will show the actual value and not the defaulted value
of 1970-01-01T00:00:00.000Z. This is tracked under the activity
A00009297 and is addressed in the Timestamp section.
```

The maximum size of a QCA IPDR record is around 840 characters, this equates to 840-bytes (using UTF-8 encoding).

Not all of the QoS statistics are provided by all media gateways, e.g. the UAS does not support the Jitter and Latency statistics, therefore if the received binary QoS record does not contain a valid value for any of the QoS statistics the element will not be included in the output QCA IPDR record.

24.3.3.2 QCA IPDR element values

Refer to the following table.

Table 6 Mapping of input binary QoS Record fields to output QCA IPDR record elements

Output QCA IPDR elements	Input Binary QoS field	Comment
StartTime	Call Start Time	A00009297 feature: Starting SN09, QoS IPDR records will show correct timestamp (Call start Time) and not the Hardcoded value used: 1970-01-01T00:00:00.000Z earlier.
EndTime	Call End Time	A00009297 feature: Starting SN09, QoS IPDR records will show correct timestamp (Call End Time) and not the Hardcoded value used: 1970-01-01T00:00:00.000Z earlier.
timeZoneOffset	N/AN/A	Not applicable. Hardcoded value used: 0
callCompletionCode	N/A	Not applicable. Hardcoded value used: CC (call completed normally)
originalDestinationId	N/A	Not applicable. Empty String
subscriberId	Concatenation of Endpoint and Gateway Name (from Gateway FQDN)	<EndPoint>@<GW Name>
hostName	Concatenation of MT (MGC Type), MGC Number and Switch CLLI	<MGC Type><MGC Number>@<Switch CLLI>
uniqueCallId	Correlation Id	
ipAddr	Gateway IP Address	standard 4-part format
portNumber	Gateway Port Number	
seqNum	Sequence number	
averagePacketLatency	Latency	Element not present in IPDR if the received binary QoS record value is
inboundByteCount	Octets Received	
outboundByteCount	Octets Sent	

Table 6 Mapping of input binary QoS Record fields to output QCA IPDR record elements

Output QCA IPDR elements	Input Binary QoS field	Comment
inboundPacketCount	Packets Received	less than 0, indicating that the GW did not support the statistic.
outboundPacketCount	Packets Sent	
inboundLostPacketCount	Packet Loss	
packetDelayVariation	Jitter	

Starting SN09.1 - aal2/ps, aal2/pr, aal2/pl, aal2/jit AAL2 parameters (A00009297 feature) are also reflected in QoS Records using inboundPacketCount, outboundPacketCount, inboundLostPacketCount, packetDelayVariation respectively.

The following elements are ‘required’ IPDR elements so have been included in the QCA output for IPDR compliancy.

- StartTime
- EndTime
- timeZoneOffset
- CallCompletionCode
- originalDestinationId

24.3.3.3 QCA IPDR file format

The output of the QCA is a file with format conforming to the IPDR structure. The first line in the file is the header, providing details about the XML version and encoding. The next line is the ‘open’ IPDR tag which gives information about the version of QCA and indicates the start of records. The last line in the file is the ‘close’ IPDR tag which indicates the end of the file.

Refer to the following figure for an example QoS XML file format.

Figure 3 QCA IPDR file format

Line no.	Line	Description
1	`<?xml version="1.0" encoding="UTF-8" ?>`	File header

Figure 3 QCA IPDR file format

2	<IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" IPDRRecorderInfo ="qca.nortelnetworks.com" xsi:schemaLocation="http://www.ipdr.org/namespaces/ ipdr VoIP3.1-A.0.2.xsd" version="3.1-A.0.2">	IPDRDoc is the file open tag
3	<IPDR>	Start of record
	.	
	.	
	.	
	.	
	.	
n-1	</IPDR>	End of record
n	</IPDRDoc>	/IPDRDoc is the file close tag

The IPDRDoc tag gives information about the IPDR format used and the device that generated the IPDR file, e.g.

IPDRRecorderInfo = “qca.nortelnetworks.com”

24.4 Detecting Events and Errors

In the situation that the QCA detects an event (e.g. client closes the connection) or an error (e.g. out of sequence record), a customer log is generated and an error IPDR record is written to the output file.

The error IPDR record is generated so that the OSS does not require two interfaces to the QCA host, one to retrieve IPDR records and one to monitor events and errors. All the relevant information to the QCA output processing is provided in the single output stream.

The error IPDR record is compliant to the IPDR specification, i.e. contains all of the required IPDR elements, some of which will contain default or empty values.

Multiple errors

This is only applicable to unsupported QoS record version and unsupported QoS record length errors.

The QCA allows up to 9 consecutive unsupported QoS record version and up to 9 consecutive unsupported QoS record length errors. When the 10th consecutive error is detected a customer log is generated to indicate this and the connection is being closed.

If a client sends a QoS record with valid length or version before sending 10 unsupported QoS record version or 10 unsupported QoS record length records, a customer log is generated to indicate that the alarm condition has been cleared.

Table 7 QCA Error and Event actions

Error/Event	QCA Action
out of sequence record	customer log generated error IPDR record generated binary QoS record processed
unsupported QoS record version (less than 10 consecutive records)	customer log generated error IPDR record generated binary QoS record discarded
unsupported QoS record version (10th consecutive records)	customer log generated error IPDR record generated binary QoS record discarded connection closed
unsupported QoS record length (less than 10 consecutive records)	customer log generated error IPDR record generated binary QoS record discarded
unsupported QoS record length (10th consecutive records)	customer log generated error IPDR record generated binary QoS record discarded connection closed
unknown message type	customer log generated error IPDR record generated binary QoS record discarded connection closed
unable to read binary QoS record header	customer log generated error IPDR record generated binary QoS record discarded connection closed

Table 7 QCA Error and Event actions

Error/Event	QCA Action
unable to process binary QoS record body	customer log generated
	error IPDR record generated
	binary QoS record discarded
connection closed (not by QCA)[a]	customer log generated
	error IPDR record generated
	connection closed (from QCA end)
QCA stopped	customer log generated
	error IPDR record generated
QCA started	error IPDR record generated
New GWC Connection	customer log generated
	error IPDR record generated

a. Note: This includes the ‘GWC Swact’ scenario.

Note: please refer to Appendix A for more details of the customer logs generated by the QCA.

24.4.1 QCA Error IPDR record

Depending on the type of error, different information can be used in the error IPDR record.

For example, if a message with an ‘unknown message type’ is received the whole message is unreliable so only the connection information can be used. Whereas, if an ‘out of sequence’ record is received the message format is valid so information from the connection and record header can be used.

Default values are used in the QCA error IPDR record for the following required IPDR elements:

- callCompletionCode - CC
- originalDestinationId - empty string
- subscriberId - empty string
- uniqueCallId - empty string

Depending on the type of error or event the following QCA error IPDR record elements may contain information:

- hostName - MGC Id, if the MGC Id is not available it is an empty string and the Node name (the value of the nodeName property in the qca.properties file). Below are some examples.

  - GWC3@CS2K_LAB (if MGC Id is available)
  - CS2K_LAB (if MGC Id is an empty string)
- seqNum - the sequence number of the QoS record with the error, the sequence number is not available it is 0

The following QCA error IPDR record elements are always used to convey information:

- ipAddress
- portNumber
- proprietaryErrorCode

The values for each element in the error IPDR record, other than the default elements, are given in the following table.

Table 8 Error IPDR record elements

Error/Event	Element	Value
Unexpected Record Sequence Number	hostname	MGC Id, Node name
	seqNum	record sequence number
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	0 (plus previous valid record sequence number, e.g. previous sequence number = 1638, proprietaryErrorCode = 01638)
Record Lost: Unsupported Version	hostname	MGC Id, Node name
	seqNum	record sequence number
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	1
Record Lost: Unsupported Record Length	hostname	MGC Id, Node name
	seqNum	record sequence number
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	2

Table 8 Error IPDR record elements

Error/Event	Element	Value
Connection closed: Unrecognized Message Type	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	3
Connection closed: Error while processing QoS record header	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	4
Record Lost: Error while processing binary QoS data	hostname	MGC Id, Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	5
Connection closed	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	6
QCA Stopped	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	7
QCA Started	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection

Table 8 Error IPDR record elements

Error/Event	Element	Value
	portNumber	Port number of connection
	proprietaryErrorCode	8
New GWC Connection[a]	hostname	MGC Id, Node name
	seqNum	record sequence number
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	9

a. These records will be produced for every new connection from the GWCs.

24.4.1.1 Error IPDR record format

Examples for each of the QCA IPDR error records:

Unexpected Record Sequence Number

```
<IPDR>
   <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
   <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
   <timeZoneOffset>0</timeZoneOffset>
   <callCompletionCode>CC</callCompletionCode>
   <originalDestinationId></originalDestinationId>
   <hostName>GWC99@CS2K_LAB</hostName>
   <subscriberId></subscriberId>
   <uniqueCallId></uniqueCallId>
   <ipAddress>47.96.0.243</ipAddress>
   <portNumber>37559</portNumber>
   <seqNum>4</seqNum>
   <proprietaryErrorCode>02</proprietaryErrorCode>
</IPDR>
```

Record Lost: Unsupported Version

```
<IPDR>
   <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
   <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
   <timeZoneOffset>0</timeZoneOffset>
   <callCompletionCode>CC</callCompletionCode>
   <originalDestinationId></originalDestinationId>
   <hostName>GWC99@CS2K_LAB</hostName>
   <subscriberId></subscriberId>
   <uniqueCallId></uniqueCallId>
   <ipAddress>47.96.0.243</ipAddress>
   <portNumber>37665</portNumber>
   <seqNum>2</seqNum>
   <proprietaryErrorCode>1</proprietaryErrorCode>
</IPDR>
```

Record Lost: Unsupported Record Length

```
<IPDR>
   <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
   <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
   <timeZoneOffset>0</timeZoneOffset>
   <callCompletionCode>CC</callCompletionCode>
   <originalDestinationId></originalDestinationId>
   <hostName>GWC99@CS2K_LAB</hostName>
   <subscriberId></subscriberId>
   <uniqueCallId></uniqueCallId>
   <ipAddress>47.96.0.243</ipAddress>
   <portNumber>37676</portNumber>
   <seqNum>2</seqNum>
   <proprietaryErrorCode>2</proprietaryErrorCode>
</IPDR>
```

Connection closed: Unrecognized Message Type

```
<IPDR>
   <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
   <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
   <timeZoneOffset>0</timeZoneOffset>
   <callCompletionCode>CC</callCompletionCode>
   <originalDestinationId></originalDestinationId>
   <hostName>CS2K_LAB</hostName>
   <subscriberId></subscriberId>
   <uniqueCallId></uniqueCallId>
   <ipAddress>47.96.0.243</ipAddress>
   <portNumber>37642</portNumber>
   <seqNum>0</seqNum>
   <proprietaryErrorCode>3</proprietaryErrorCode>
</IPDR>
```

Connection closed: Error while processing QoS record header

```
<IPDR>
   <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
   <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
   <timeZoneOffset>0</timeZoneOffset>
   <callCompletionCode>CC</callCompletionCode>
   <originalDestinationId></originalDestinationId>
   <hostName>CS2K_LAB</hostName>
   <subscriberId></subscriberId>
   <uniqueCallId></uniqueCallId>
   <ipAddress>47.96.0.243</ipAddress>
   <portNumber>37642</portNumber>
   <seqNum>0</seqNum>
   <proprietaryErrorCode>4</proprietaryErrorCode>
</IPDR>
```

Record Lost: Error while processing binary QoS data

```
<IPDR>
   <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
   <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
   <timeZoneOffset>0</timeZoneOffset>
   <callCompletionCode>CC</callCompletionCode>
   <originalDestinationId></originalDestinationId>
   <hostName>GWC99@CS2K_LAB</hostName>
   <subscriberId></subscriberId>
   <uniqueCallId></uniqueCallId>
```

```
  <ipAddress>47.96.0.243</ipAddress>
  <portNumber>37676</portNumber>
  <seqNum>2</seqNum>
  <proprietaryErrorCode>5</proprietaryErrorCode>
</IPDR>
```

Connection closed

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>47.96.0.243</ipAddress>
  <portNumber>37676</portNumber>
  <seqNum>0</seqNum>
  <proprietaryErrorCode>6</proprietaryErrorCode>
</IPDR>
```

QCA Stopped

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>0.0.0.0</ipAddress>
  <portNumber>20000</portNumber>
  <seqNum>0</seqNum>
  <proprietaryErrorCode>7</proprietaryErrorCode>
</IPDR>
```

QCA Started

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>0.0.0.0</ipAddress>
  <portNumber>20000</portNumber>
  <seqNum>0</seqNum>
  <proprietaryErrorCode>8</proprietaryErrorCode>
</IPDR>
```

New GWC Connection

```
<IPDR>
   <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
   <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
   <timeZoneOffset>0</timeZoneOffset>
   <callCompletionCode>CC</callCompletionCode>
   <originalDestinationId></originalDestinationId>
   <hostName>GWC77@CS2K_LAB</hostName>
   <subscriberId></subscriberId>
   <uniqueCallId></uniqueCallId>
   <ipAddress>47.96.0.243</ipAddress>
   <portNumber>37559</portNumber>
   <seqNum>567</seqNum>
   <proprietaryErrorCode>9</proprietaryErrorCode>
</IPDR>
* Note: Starting SN09, the value of the timestamp in the IPDR
records will show the actual value and not the defaulted value of
1970-01-01T00:00:00.000Z. This is tracked under the activity
A00009297 and is addressed in section <4.0.0.1>
```

24.4.2 Streaming to OSS

Real-Time streaming of the QCA IPDR record stream to the OSS is provided via the streamQoS utility. It should be used as follows:

1. Connect to the machine on which QCA is running, e.g. via telnet
2. Change directory to the QCA home directory, e.g. /opt/nortel/qca/
3. Start the logging to file of the window.
4. Type streamQoS to start the stream
5. The streaming utility is stopped by closing the connection

24.4.3 Display tool

A tool to display QCA IPDR records in an output QCA file is provided. There are three outputs from the tool:

- display all the QCA IPDR Records in the file
- display all the QCA IPDR Records for a particular Subscriber Id in the file
- display all the QCA IPDR Records for a particular MGC in the file

The command must have at least one argument, the file name.The command is able to handle the compressed and also uncompressed QCA output files.

To display only the records for a particular Subscriber Id, the Subscriber Id must be provided to the utility.

To display only the records for a particular MGC, the following information is necessary:

- MGC type (GWC or SPM), *mgcType* or *mt* field in QCA IPDR record
- MGC number (0 to 255), *mgcNumber* or *num* in QCA IPDR record

Displaying all QCA IPDR records in a file:

```
displayQoS <file name>
```

Displaying all QCA IPDR record from a particular client in a file:

```
displayQoS <file name> <Subscriber Id>
```

Displaying all QCA IPDR record from a particular client in a file:

```
displayQoS <file name> <MGC type> <MGC number>
```

If the file can not be found an error is displayed.

The first argument is always the file name. If only two arguments are provided the second argument is taken as the Subscriber Id. If more than two arguments are provided they are taken as the MGC type and MGC number.

Example displayQoS output:

```
Displaying QoS Records for GWC 80 from file:
GWC.Telco_Switch_35.QoS.2002.04.11_02.45_EDT.xml

Record:
Start Time*    = 1970-01-01T00:00:00.000Z
End Time*      = 1970-01-01T00:00:00.000Z
TimeZone Offset  = 0
Call Comp Code   = CC
Orig Dest Id     =
Host name        = GWC171@3911296719576333
Subscriber id    = 709615575170887 78@4995546324
Correlation Id   = 14714216668188184186
IP Address       = 96.143.185.15
Port Number      = 35187
Sequence Number  = 9
Latency          = 19685
Octets Received  = 1894381033
Octets Sent      = 1785294279
Packets Received = 648495757
Packets Sent     = 286520160
Packets Lost     = 922391632
Jitter           = 14826

Record:
Start Time*    = 1970-01-01T00:00:00.000Z
End Time*      = 1970-01-01T00:00:00.000Z
TimeZone Offset  = 0
Call Comp Code   = CC
Orig Dest Id     =
Host name        = GWC99@CS2K_LAB
Subscriber id    =
Correlation Id   =
IP Address       = 47.96.0.243
Port Number      = 37559
Sequence Number  = 4
Previous seq num = 2
Error Code       = 0 (Unexpected Record Sequence Number)


End of XML QoS File.
```

Example displayQoS output (for call over AAL2 fabric):

```
Displaying QoS Records for GWC 80 from file
GWC.Telco_Switch_35.QoS.2002.04.11_02.45_EDT.xml

Record:
Start Time*    = 1970-01-01T00:00:00.000Z
End Time*      = 1970-01-01T00:00:00.000Z
TimeZone Offset  = 0
Call Comp Code   = CC
Orig Dest Id     =
Host name        = GWC171@3911296719576333
Subscriber id    = 7096155751708778@4995546324
Correlation Id   = 14714216668188184186
IP Address . . . = 96.143.185.15
Port Number      = 35187
Sequence Number  = 9
Latency          = 19685
Octets Received  = 1894381033
Octets Sent      = 1785294279

Packets Received = 648495757
Packets Sent     = 286520160
Packets Lost     = 922391632
Jitter           = 14826

Record:
Start Time*    = 1970-01-01T00:00:00.000Z
End Time*      = 1970-01-01T00:00:00.000Z
TimeZone Offset  = 0
Call Comp Code   = CC
Orig Dest Id     =
Host name        = GWC99@CS2K_LAB
Subscriber id    =
Correlation Id   =
IP Address       = 47.96.0.243
Port Number      = 37559
Sequence Number  = 4
Previous seq num = 2
Error Code       = 0 (Unexpected Record Sequence Number)


End of XML QoS File.


* Note: Starting SN09, the value of the timestamp in the IPDR
records will show the actual value and not the defaulted value of
1970-01-01T00:00:00.000Z. This is tracked under the activity
A00009297 and is addressed in section <2.3>
```

Note: when displaying error IPDR records, the displayQoS utility adds a textual description to the error code value.

Note: when displaying Unexpected Record Sequence Number error IPDR records, the displayQoS utility extracts the previous sequence number value from the proprietryErrorCode and displays it as a separate field, Previous seq num.

24.4.4 Installation

The QCA application (NTQCA.pkg) is available in the CS2M[1] software package. Below are the steps to install the QCA

- Insert the CD with the CS2M load and log onto the SESM server as root. Then change the directory to the bin directory on the CD.

```
cd /cdrom/cdrom0/bin
```

- To start the install process, enter the following command.

```
./appl_mgr.ksh
```

Note: Select option 1 to install all the application along with QCA.

Below are the steps when QCA needs to be installed on a SSPFS machine which does not run the CS2M load.

- FTP the NTQCA.pkg onto the SSPFS machine. Log in as root.
- Install the new QCA software using: pkgadd -d NTQCA.pkg

Below are the steps to follow to uninstall the QCA package.

- Connect to the host where the QCA is running.
- Log in as root.
- Stop the QCA server: stop_qca.
- Uninstall the original QCA package: pkgrm NTQCA.

24.4.5 Upgrades

As of SN06.2, the QCA is a patchable component. The patchability mechanism conflicts with the in-service upgrade mechanism. So the support for in-service upgrade of QCA on a single SSPFS machine is removed. Please see section 2.2.15 for more details.

The QCA software upgrades are performed using the install scripts provided with QCA as part of the new software release. Software upgrades of QCA must be coordinated with the OSS to avoid loss of data. The OSS would be redirected to an alternative QCA instance while the primary QCA is being updated. Once the primary instance is updated, the OSS can be redirected back to the primary instance and the other instances can be updated.

24.4.6 QCA customer logs

In addition to QCA Error IPDR Records the QCA raises alarms and events via the customer logging stream.

[1]CS2M (CS 2000 Management Components) refers to a NCL software package used on the CS 2000 management tools server. This package includes SESM, NPM, SAM21EM, QCA.

The QCA uses the logging API introduced by activity 89008996 “Log Reporting and Storage Mechanism for Managed Elements”.

Figure 4 Sample customer log message generated by QCA

```
Oct 11 12:00:02 wmdhs0j8 main:0001 QCA201 WARNING init wmdhs0j8
RetainFileTime property in properties/qca.properties is out of
range. QCA is starting with default retain file time of 5 days
```

The QCA customer logs contain the following fields

- Report name
- Report Number
- Priority
- Event Type
- Device ID
- Message

All the QCA customer logs contain the following information:

- Report name = “QCA”
- Device ID = QCA host name

See Appendix A - QCA Customer Logs for a summary of QCA customer logs and the contents of the other fields in the logs.

The QCA also generates debug logs to report software errors.

24.4.7 Patchability

In SN06.2, the activity A00003229 provides the functionality of making the QCA a patchable OAM device. The Network Patch Manager is responsible for administering individual fixes to QCA. Patches for the QCA will be in the same format and have the same naming convention of OAM patches such as NPM, SAM21EM, etc

When a QCA patch (containing modified Java-based classes) is delivered to a customer site, the patch is applied and then the QCA application is required to be stopped and then restarted by the NPM for the patch to be ‘enabled’. The restart enables a new Java Virtual Machine to be started that picks up the patched/modified Java classes. This procedure also applies to removal of QCA patches. For a QCA patch to be truly removed, the patch is removed and then a restart must be performed via the NPM on the application.

The QCA application must be inservice to perform any maintenance operations such as application, removal, or restart. In addition, the QCA application must be inservice for an audit to succeed. Because QCA is monitored or polled by an external system (OSS) for performance data or SLA agreements, it is important that any changes to QCA be coordinated to avoid loss of data or duplication of data. The OSS should be moved from monitoring the primary instance of QCA to an alternative QCA instance while the primary QCA is being updated via the restart request initiated by NPM. Once the primary instance is updated, the OSS should be redirected back to the primary instance and the other instances can be updated.

Since QCA is an OAM software application, it will be registered in the NPM database upon system start-up and initialization, and it will appear as a device with the device name QCA_<node_name>, where node_name is the name of the SSPFS machine where the QCA is running. Reports and queries at the NPM Graphical User Interface (GUI) and NPM Command Line User Interface (CLUI) will show the QCA as a device.

In SN06.2, the support for in-service QCA upgrade (on a single SSPFS machine) is removed to enable QCA patchability. Hence, the scripts to start and stop the second instance of QCA (qca_server2 and stop_qca2) will be obsoleted in this release.

The following sections briefly give information about applying/removing patches to/from QCA.

24.4.7.1 Applying patch to QCA

The following steps are a recommended procedure in applying QCA patches to a QCA application.

- QCA patch files are delivered to a customer site to the SSPFS machine containing the NPM server via RPS/PFRS or by manual action.
- QCA patches are introduced to the NPM database via the NPM CLUI with the ‘getpatch’ command.
- QCA patches are applied to the QCA application via the NPM apply command at the NPM GUI or NPM CLUI.

After all the QCA patches are applied, a restart command from the NPM GUI or NPM CLUI is invoked on the QCA application to enable or activate the patches.

> ***Note:*** A restart consists of stopping the QCA application and then starting the application. It is important that any maintenance activities associated with the QCA should be completed or stopped before the restart from the NPM GUI or CLUI is invoked. Also, the OSS should be directed from the primary instance of QCA to an alternative instance prior to the restart. The NPM restart will result in current active file being moved into the *today*

directory and a new active file will be opened. The whole of this operation will take around **60 seconds**, during this period any QoS records sent from GWC to QCA will be lost.

Also, a NPM restart will result in following logs.

1. NPM 620: Initiated restart on device,<qca_devicename>.
2. GWC 312: QCA connection failure, indicating that GWC is having communication problems with QCA.
3. NPM 620: A restart initiated by the NPM on device <qca_devicename> has completed.
4. QCA 322: New GWC Connection, indicating that QCA has come up after the restart, and is accepting connections.
5. GWC 399: Clear event for GWC312, indicating that previous 'Raise' event is cleared.

Note: It is important to note the NPM database could show patches to be applied to an OAM device, but the patch is not actually enabled or performing its task to address the original problem. It is only after a restart is performed from the NPM GUI or CLUI on the OAM device that the patch is enabled.

- After the restart is performed on the QCA an NPM audit needs to be executed to update OAM patch enabled statuses in the NPM database. The audit can be performed manually from the NPM GUI or CLUI or it will be done automatically on the device approximately 20-25 minutes after the restart has been completed.

24.4.7.2 Removing Patch from QCA

The following steps are a recommended procedure in removing QCA patches from QCA.

- QCA patches are removed via the NPM remove command at the NPM GUI or NPM CLUI.
- After all QCA patches are removed, a restart command from the NPM GUI or NPM CLUI is invoked on the QCA to disable the patches.

Note: A restart consists of stopping the QCA application and then starting the QCA application. It is important that any maintenance activities associated with QCA should be completed or stopped before the restart from the NPM GUI or CLUI is invoked. Also, the OSS should be directed from the primary instance of QCA to an alternative instance prior to the restart. The NPM restart will result in current active file being moved into the *today* directory and a new active file will be opened. The whole of this operation will take around **60 seconds**, during this period any QoS records sent from GWC to QCA will be lost.

Also, a NPM restart will result in following logs.

1. NPM 620: Initiated restart on device,<qca_devicename>
2. GWC 312: QCA connection failure, indicating that GWC is having communication problems with QCA.
3. NPM 620: A restart initiated by the NPM on device <qca_devicename> has completed.
4. QCA 322: New GWC Connection, indicating that QCA has come up after the restart, and is accepting connections.
5. GWC 399: Clear event for GWC312, indicating that previous 'Raise' event is cleared.

Note: It is important to note the NPM database could show patches to be removed from an OAM device, but the patch is still enabled or performing its task to address the original problem. It is only after a restart is performed from the NPM GUI or CLUI on the OAM device that the patch is disabled.

- After the restart is performed on the QCA, an NPM audit needs to be executed to update QCA patch enabled statuses in the NPM database. The audit can be performed manually from the NPM GUI or CLUI or it will be done automatically on the device approximately 20-25 minutes after the restart has been completed.

24.4.7.3 AutoApply

QCA patches can be automatically applied if the end user has the automated process scheduled to run. Refer to the NPM online help for more information on this automated process.

24.4.7.4 Restart and AutoRestart Restrictions

Due to the implications to the OSS, restrictions are placed on the NPM restart command for QCA devices. The following restrictions are enforced by the NPM:

- QCA devices are not included in the set of OAM devices that can be auto-restarted, nor can a QCA restart be included in any plans scheduled at a designated time. Only a manual restart of a QCA device is supported.
- Only one QCA at a time can be restarted. The multitasking ability of NPM is not utilized for QCA.

A warning will be displayed to the user by the NPM CLUI or GUI explaining the implications of restarting QCA. The user will be forced to choose whether to continue with the restart command or to cancel.

24.4.8 QCA Software Management

The QCA application is designed to allow multiple copies to run in the network to provide increased levels of reliability. Additional copies of the QCA

application should be installed on different servers and assigned in the GWC EM. Two instances of QCA can not be installed on the two halves of the same high availability cluster; they must be on separate servers. Because QCA is monitored or polled by an external system (OSS) for performance data or SLA agreements, it is important that any changes to QCA be coordinated with the OSS to avoid loss of data or duplication of data. These changes include starting or stopping the application, applying corrective content, or applying upgrades. The OSS must be able to move from monitoring one instance of QCA to another during patching or upgrades or any activity that interrupts the QCA application. The OSS can either be manually redirected to another instance of QCA or programmed to automatically redirect on command.

24.5 Hardware Requirements or Dependencies

The QCA application has the following requirements:

- SUN Netra T1400

440Mhz UltraSPARCC IIi with QFE card, 4MB Cache, 512MB RAM, 2x18.2GB Disk Running SUN Solaris 8 Oracle DB 8.1.6 Enterprise and Java Virtual Machine.

Note: The QCA can run on the same SUN Netra T1400 that SESM and other network management tools are running on.

24.6 Software Requirements or Dependencies

- SSPFS 3d party software suite Version 06.

24.7 Limitations and restrictions

24.7.1 Upgrades

To ensure that the QCA support the version of QoS record used in the network, the QCA must be upgraded before the QoS reporting clients are upgraded.

Note: For a major release upgrade, where the SSPFS software is upgraded before the QCA, a QCA running on a separate host is required to ensure no loss of QoS records.

Note: For a QCA maintenance release upgrade or when applying patches, a QCA running on a separate host is required to ensure no loss of QoS records.

Note: Corrective content is applied and managed by the Network Patch Manager (NPM) in SN06.2. Because of the need to coordinate QCA changes like patching with the external OSS, QCA patches are manually applied and activated. This allows the OSS to be redirected to an alternative QCA instance while the primary QCA is being updated. Once

the primary instance is updated, the OSS can be redirected back to the primary instance and the other instances can be updated.

24.8 Interactions

- Syslog daemon server

24.9 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

24.10 Glossary

Term	Description
ATM	Asynchronous Transfer Mode
CLLI	Common Language Location Identifier
CLUI	Command Line User Interface
CMTS	Cable Modem Terminal System
DPT	Dynamic Packet Trunk
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
GW	Gateway
GWC	Gateway Controller
IP	Internet Protocol

Term	Description
IOM	Input/Output Module
OC	Optical Carrier
OSS	Operations Support System
MGC	Media Gateway Controller
MS	Message Switch
NCS	Network Control System
NE	Network Element
NPM	Network Patch Manager
OL	Octets Lost
OR	Octets Received
OS	Octets Lost
PFRS	Patch File Receipt System
PL	Packets Lost
PR	Packets Received
PL	Packets Sent
PSE	Patching Server Element
PVG	Passport Voice Gateway
QCA	QoS Collector Application
QoS	Quality of Service
RPS	Regional Patch Selector
SDM	SuperNode Data Manager
SESM	Succession Element and Subelement Manager
SLA	Service Level Agreement
SPM	Spectrum Peripheral Module
STM	Synchronous Transfer Mode
USP	Universal Signalling Processor
UTF	Universal Text Format
VMG	Virtual Media Gateway
VoIP	Voice over IP

Term	Description
XML	eXtensible Markup Language

24.11 References.

1. Activity 89007790 - QoS Reporting: Correlation ID and billing
2. Activity 89007749 - QoS Reporting: GWC QoS Reporting Application and Connection Management
3. Activity 89007781 - QoS Reporting: Provisioning
4. Activity 59039902 - SNMP Performance Measurement Poller
5. Activity 89008996 - Log Reporting and Storage Mechanism for Managed Elements
6. Activity 00009297 - QoSR Support of AAL2 and Timestamp.
7. Activity 00009189 - CS2M support for 64 Character Gateway name.

Appendix A - QCA Customer logs

Table 1 Service summary (initialization) warning logs

Event / Error	Report Number	Priority	Event Type	Description	QCA Action	Customer Action
Qca.properties not available at QCA start-up.	201	Warning	INIT	Properties file (properties/ qca.properties) not available. QCA is starting with default settings.	Default used	None
portNumber property not in properties/ qca.properties at QCA start-up.	201	Warning	INIT	portNumber property not in properties/qca.properties. QCA is starting with default port number of 20000	Default used	None
portNumber property in properties/qca.properties not in range at QCA start-up.	201	Warning	INIT	portNumber property in properties/qca.properties not in range. QCA is starting with default port number of 20000	Default used	None
portNumber property in properties/qca.properties not a number at QCA start-up.	201	Warning	INIT	portNumber property in properties/qca.properties could not be used. QCA is starting with default port number of 20000	Default used	None
MaxFileSize property not in properties/ qca.properties.	201	Warning	INIT	MaxFileSize property not in properties/qca.properties. QCA is starting with default maximum file size of 1 MByte	Default used	None

Table 1 Service summary (initialization) warning logs

Event / Error	Report Number	Priority	Event Type	Description	QCA Action	Customer Action
MaxFileSize property in properties/qca.properties not in range.	201	Warning	INIT	MaxFileSize property in properties/qca.properties not in range. QCA is starting with default maximum file size of 1 MByte	Default used	None
MaxFileSize property in properties/qca.properties not a number.	201	Warning	INIT	MaxFileSize property in properties/qca.properties could not be used. QCA is starting with default maximum file size of 1 MByte	Default used	None
MaxFileTime property not in properties/ qca.properties.	201	Warning	INIT	MaxFileTime property not in properties/qca.properties. QCA is starting with default maximum file time of 15 minutes	Default used	None
MaxFileTime property in properties/qca.properties not in range.	201	Warning	INIT	MaxFileTime property in properties/qca.properties not in range. QCA is starting with default maximum file time of 15 minutes	Default used	None
MaxFileTime property in properties/qca.properties not a number.	201	Warning	INIT	MaxFileTime property in properties/qca.properties could not be used. QCA is starting with default maximum file time of 15 minutes	Default used	None
RetainFileTime property not in properties/ qca.properties.	201	Warning	INIT	RetainFileTime property not in properties/qca.properties. QCA is starting with default retain file time of 5 days	Default used	None
RetainFileTime property in properties/ qca.properties not in range.	201	Warning	INIT	RetainFileTime property in properties/qca.properties not in range. QCA is starting with default retain file time of 5 days	Default used	None
RetainFileTime property in properties/ qca.properties not a number.	201	Warning	INIT	RetainFileTime property in properties/qca.properties could not be used. QCA is starting with default retain file time of 5 days	Default used	None
recycleToD property not in properties/ qca.properties.	201	Warning	INIT	recycleToD property not in properties/qca.properties. QCA is starting with default recycle hour of day of 0	Default used	None
recycleToD property in properties/qca.properties not in range.	201	Warning	INIT	recycleToD property in properties/qca.properties not in range. QCA is starting with default recycle hour of day of 0	Default used	None

Table 1 Service summary (initialization) warning logs

Event / Error	Report Number	Priority	Event Type	Description	QCA Action	Customer Action
recycleToD property in properties/qca.properties not a number.	201	Warning	INIT	recycleToD property in properties/qca.properties could not be used. QCA is starting with default recycle hour of day of 0	Default used	None
fileExt property not in properties/qca.properties.	201	Warning	INIT	fileExt property not in properties/qca.properties. QCA is starting with default file extension of xml	Default used	None
oldFileCompression property not in properties/ qca.properties.	201	Warning	INIT	oldFileCompression property not in properties/qca.properties. QCA is starting with default value of true	Default used	None
oldFileCompression property in properties/ qca.properties not true or false.	201	Warning	INIT	oldFileCompression property in properties/qca.properties could not be used. QCA is starting with default value of true	Default used	None
closedFileCompression property not in properties/ qca.properties.	201	Warning	INIT	closedFileCompression property not in properties/ qca.properties. QCA is starting with default value of true	Default used	None
closedFileCompression property in properties/ qca.properties not true or false.	201	Warning	INIT	closedFileCompression property in properties/ qca.properties could not be used. QCA is starting with default value of true	Default used	None
nodeName property not in properties/ qca.properties.	201	Warning	INIT	nodeName property not in properties/qca.properties. QCA is starting with default value of QCA	Default used	None
old file retention directory (today-x) is being removed.	202	None	INIT	File Recovery: removing closed file retention directory: *directory* as it is older than *x* days.	Directory removed	None
File found in active directory when QCA started.	202	None	INIT	File Recovery: file *file name* found in active directory. This could indicate that the QCA failed. Please check debug logs.	File completed (if necessary) and moved to today directory.	Check debug logs.

To comply with X.733, the structure of the logs will also contain following attributes. The logs are differentiated from each other by Specific Problem and Description attributes.

- Location : QCA Host Name
- Category : Appropriate category from X.733 list of available categories.
- Cause : Appropriate category from X.733 list of available cause-values.
- Time : Time at which log was generated.
- ComponentID : File /Directory path, GWC name (components causing generation of log)
- SpecificProblem : Text giving details of the specific-problem
- Description : Text describing the problem and/or giving more information.

Table 2 Trouble logs

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
File handler or server socket could not be started.	300	None	FAIL	QCA not started: Could not open server socket: +*reason* or QCA not started: Could not create File Handler: +*reason*	QCA not started	Rectify problem and re-start QCA.
Out of sequence QoS record received.	302	None	FLT	Out of Sequence QoS Record received. '*MGC Type MGC number*': sequence number = '*record sequence number*' previous sequence number = '*last record sequence number*'	XML Error record generated.	None
Problem processing binary QoS record.	302	None	FLT	Problem processing binary QoS record: Sequence number = '*record sequence number*' Relevant MGC is mentioned in *Component ID* attribute of the log.	XML Error record generated. XML QoS Record not written to file.	None

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
QoS Record received with Unsupported Length. (Notification Id: 9)	301	Minor	FLT	Location: <hostName> Notification ID: 9 State: Raise Category:Processing Error Cause: Corrupt Data. Time:<time> Component Id: 'MGCType MGCNum' Specific Problem: The QCA has received records with < numberOfLengthErrors> length errors from the source. Description: If 10 (or more) records with unsupported length are received consecutively, Major fault log is generated and the connection is closed.	XML Error record generated. XML QoS Record not written to file.	Investigate why client is sent QoS Record with Unsupported Length
10 sequential QoS Records received with Unsupported Length.	301	Major	FLT	Location: <hostName> Notification ID: 9 State: Raise Category:Processing Error Cause: Version mismatch. Time:<time> Component Id: 'MGCType MGCNum' Specific Problem: 10 unsupported length records received. The connection to the client will be closed	Connection to client closed	Investigate why client is repeatedly sending Unsupported Length QoS records
QoS Record received with Unsupported Version. (Notification Id: 57)	301	Minor	FLT	Location: <hostName> Notification ID:57 State: Raise Category:Processing Error Cause: Version mismatch. Time:<time> Component Id: 'MGCType MGCNum' Specific Problem: The QCA has received records with <NumberOfVersionErrors> version errors from the source. Description: If 10 (or more) records with unsupported version are received consecutively, Major fault log is generated and the connection is closed.	XML Error record generated. XML QoS Record not written to file.	Investigate why client is sent QoS Record with Unsupported Version
10 sequential QoS Records received with Unsupported Version.	301	Major	FLT	Location: <hostName> Notification ID: 57 State: Raise Category:Processing Error Cause: Version mismatch. Time:<time>Component Id: 'MGCType MGCNum' Specific Problem: 10 unsupported version records received. The connection to the client will be closed.	Connection to client closed	Investigate why client is repeatedly sending Unsupported Length QoS records

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
The binary QoS Record header could not be processed.	305	None	FLT	Connection closed: Error while processing QoS record header: Client at, IP Address '*client IP Address*'. Local Port '*local port number*' closed connection.	Connection to client closed	Investigate why client is sent QoS Record with faulty header
Disk space shortage, local disk requires more free space. Disk Space is below 100Mb.	310	Critical	TBL	Location: <hostName> Notification ID: 49 State: Raise Category:Processing Error Cause: StorageCapacityproblem. Time:<time>Component Id: / data/qca Specific Problem: checkDiskSpace() has shown that there is less than 104857600 bytes available on the local disk. More Space is required immediately.	None	More space must be created.
Disk Space is starting to run seriously low. This means that the available space is below 500Mb.	310	Major	TBL	Location: <hostName> Notification ID: 49 State: Raise Category:Processing Error Cause: StorageCapacityProblem. Time:<time>Component Id: / data/qca. Specific Problem:Less than 524288000 bytes available on the local disk.Critical alarm will be raised if disk space continues to drop.	None	More space must be created.
Disk space is below the minimum threshold. Initially set at 1Gb.	310	Minor	TBL	Location: <hostName> Notification ID: 49 State: Raise Category:Processing Error Cause: StorageCapacityProblem. Time:<time>Component Id: / data/qca. Specific Problem: Less than 1073741824 bytes available on the local disk. Major alarm will be raised if the disk space continues to drop.	None	More space must be created.
A request to get a new file name has failed, there are either 10000 files with the same name or the new file can not be created.	315	Warning	FLT	Unable to get an unused file name for <fileName> Please check the output directory.	file null.xml used	Output directories need to be checked.

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
The QCA has failed to write the footer information to the active file whilst attempting to close. The active file might have been compressed without the footer information.	315	Warning	FLT	Cannot write the FOOTER to the active file. This file is corrupted FileName = <fileName>.	None	Check the file and confirm that all XML tags have been closed.
The active file did not exist when trying to write to it. Attempt to get new file then failed. Further failures will result in the QCA being shutdown.	315	None	FLT	Active file <fileName> has been removed. Data may have been lost. Creating new file, and attempting to write record again. Failure to do so will result in shutdown of the QCA	Attempts to create a new output file	File IO problems, if problem is resolved the Major alarm will be withdrawn.
Attempting to write data to file, the active file does not exist. Try to get new file. This has failed. Sleep The thread and try and get new file again.This also failed. No file to write to, QCA will shutdown.	315	None	FAIL	Could not get new file to write records. File <fileName> is corrupted or removed. QCA shutting down.	QCA is stopped.	check: disk space and write permissions. If all is well try starting QCA again.
The XML writer and the file all seem well, unfortunately the file cannot be accessed at in either the first or second attempt, serious problem with file IO. QCA will shutdown.	315	None	FAIL	Could not write to the activefile. Active file exists but cannot write records to it. Reason unknown. QCA shutting down	QCA is stopped.	check: disk space and write permissions. If all is well try starting QCA again.

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
The QCA has encountered inconsistent errors when building the directory structure for old files, old files may have been deleted and directory locked. The error should never appear, as it is the last resort.	315	None	FAIL	Cannot create directories under *output* directory. Cannot write records. QCA shutting down	QCA is stopped.	Check: directory structure, active and old files.
Attempt to rename the active file from the active directory to the today directory has failed. Serious error, but no loss of data immediately. Files can be moved by hand if required.	315	None	FLT	Could not rename active file <fileName> to file <newFileName>. Please check write permissions for the output directory	Closed file remains in active directory.	Check the directories exist and all the write permissions.
Could not create new active file. Data is being lost.QCA must shut down.	315	None	FAIL	Could not get new file for writing. Critical Error: <reason>. QCA shutting down.	QCA is stopped.	Check the active directory for old files and permissions.
Attempt to compress an old active file has failed.	315	None	FLT	Could not compress file: <fileName>. File compression failed.	None	Check the active directory for old files and permissions.
Failed to rename directories on the Recycle_day proc. This is where all files are moved along a level and the last gets deleted.	315	None	FLT	Could not rename director from <dirName> to <newDirName>. Check disk space and permissions.	None	Check disk space and permissions.
New GWC connection received.	322	None	INFO	New GWC COnnection: '*MGC Type MGC number*': sequence number = '*record sequence number*'	XML Error record generated	

Table 3 Information and alarm clear logs

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
Connection closed.	305	None	INFO	Connection closed. Client at, IP Address '*client IP Address*'. Local Port '*local port number*' closed connection.	Connection to client closed	None
Client has stopped sending records with unsupported length (clear for QCA 301 Notification Id: 9)	399	None	INFO	Location: <Hostname> Notification Id: 9 State: Alarm Cleared Time: <time>	None	None
Client has stopped sending records with unsupported version (clear for QCA 301 Notification Id: 57)	399	None	INFO	Location: <Hostname> Notification Id: 57 State: Alarm Cleared Time: <time>	None	None
Critical disk space issue cleared (clear for 310 Critical Alarm)	399	None	INFO	Location: <Hostname> Notification Id: 49 State: Alarm Cleared Time: <time>	None	None
Major disk space issue cleared (clear for 310 Major Alarm)	399	None	INFO	Location: <Hostname> Notification Id: 49 State: Alarm Cleared Time: <time>	None	None
Minor disk space issue cleared (clear for 310 Minor Alarm)	399	None	INFO	Location: <Hostname> Notification Id: 49 State: Alarm Cleared Time: <time>	None	None

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
QCA cannot be stopped	203	None	INIT	Location: <Hostname> Category: PROCESSINGERROR Cause: CONFIGERROR Time: ComponenetID: SpecificProblem: QCA not running on specified port: Description: Cannot stop QCA Action: Use query_qca command to determine the port QCA is running on. Make sure it matches with portNumber in qca.properties file."	Connection to client closed	None

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
QCA cannot be stopped	203	None	INIT	Location: <Hostname> Category: PROCESSINGERROR Cause: CONFIGERROR Time: ComponenetID: SpecificProblem: Missing qca.properties file. Description: Could not read properties. QCA cannot be stopped.Action:Restore qca.properties file.	None	None
QCA cannot be stopped	203	None	INIT	**Location**: <Hostname> **Category**: PROCESSINGERROR **Cause**: CONFIGERROR Time: **ComponenetID**: **SpecificProblem**: Attribute portNumber missing from qca.properties while trying to stop QCA.**Description**: Cannot determine QCA port number to stop QCA. **Action**: Add portNumber information to qca.properties file.	None	None
QCA cannot be stopped	203	None	INIT	**Location**: <Hostname> **Category**: PROCESSINGERROR **Cause**: CONFIGERROR Time: **ComponenetID**: **SpecificProblem**: Incorrect portNumber specified in qca.properties**. Description**: Cannot determine QCA port number to stop QCA **Action:** Use query_qca command to determine the port QCA is running on. Make sure it matches with portNumber in qca.properties file.	None	None
QCA cannot be stopped	203	None	INIT	**Location**: <Hostname> **Category**: PROCESSINGERROR **Cause**: CONFIGERROR Time: **ComponenetID**: **SpecificProblem**: Out of range portNumber specified in qca.properties.**Description**: Cannot determine QCA port number to stop QCA. **Action**: Use query_qca command to determine the port QCA is running on. Make sure it matches with portNumber in qca.properties file.	None	None
Connection closed.	305	None	ERROR	**Location**: <Hostname> **Category**: COMMUNICATIONS **Cause**: COMMSUBFAIL **Time**: **SpecificProblem**:. MSGTYPEERROR **Description**: Client at, IP Address: closed connection.	None	None
Connection closed.	305	None	INFO	**Location**: <Hostname> **Category**: COMMUNICATIONS **Cause**: COMMSUBFAIL **Time**: **SpecificProblem**: CONNECTIONCLOSED **Description**: Client at, IP Address: closed connection.	None	None

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
Connection closed.	305	None	ERROR	**Location**: <Hostname> **Category**: COMMUNICATIONS **Cause**: COMMSUBFAIL **Time**: **SpecificProblem**: HEADERERROR.**Description**: Client at, IP Address: closed connection	None	None
Connection closed.	305	None	INFO	**Location**: <Hostname> **Category**: COMMUNICATIONS **Cause**: COMMSUBFAIL **Time**: **SpecificProblem**: CONNECTIONCLOSED.**Description**: Client at, IP Address: closed connection	None	None
Connection closed.	305	None	INFO	**Location**: <Hostname> **Category**: COMMUNICATIONS **Cause**: COMMSUBFAIL **Time**: **SpecificProblem**: nCONNECTIONCLOSED **Description**: Client at, IP Address: closed connection	None	None

Appendix B- QCA Customer log Sample Exact Format

Log Report 201:

Table 1 201 Message

Report Number	Message
201	May 27 16:41:45 rtpysesm1 QCA: _V2_~I=rtpysesm1~H=rtpysesm1~A=QCA~S=0000~~ QCA201 WARNING INIT rtpysesm1 ^M Location: rtpysesm1^M Category: processingError^M Cause: configurationOrCustomizationError^M Time: May 27 16:41:45 2005^M ComponentID: /opt/nortel/qca/properties/qca.properties^M SpecificProblem: Missing qca.properties file.^M Description: Could not read properties. QCA is starting with default settings.^M

Log Report 202:

Table 2 202 Message

Report Number	Message
202	Aug 19 22:22:02 wnc0s0qu QCA: _V2_~I=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0000~~ QCA202 NONE INIT wnc0s0qu ^M Location: wnc0s0qu^M Category: processingError^M Cause: fileError^M Time: Aug 19 22:22:02 2004^M ComponentID: /data/qca/20000/output/active/^M SpecificProblem: Old file(s) present in active directory.^M Description: Moving old file: QCA.QCA.QoS.2004.08.19_22.19_EDT.xml, found in active directory. This could indicate that QCA failed.^M

Log Report 203

Table 3 203 Message

Report Number	Message
203	May 30 22:55:50 india1sesm QCA_STOP: _V2_~I=india1sesm~H=india1sesm~A=QCA_STOP~S=0000~~ QCA203 NONE INIT india1sesm ^M Location: india1sesm^M Category: processingError^M Cause: configurationOrCustomizationError^M Time: May 30 22:55:50 2005^M ComponentID: /opt/nortel/qca/properties/qca.properties^M SpecificProblem: Missing qca.properties file.^M Description: Could not read properties. QCA cannot be stopped.^M Action: Restore qca.properties file.^M

Log Report 300

Table 4 300 Message

Report Number	Message
300	May 31 04:22:08 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0002~~ QCA300 NONE FAIL india1sesm ^M Location: india1sesm^M Category: processingError^M Cause: communicationsSubsystemFailure^M Time: May 31 04:22:08 2005^Ml ComponentID: GWC-99^M SpecificProblem: Socket creation error.^M Description: QCA not started:^M

Log Report 302

Table 5 302 Message

Report Number	Message
302	May 31 04:22:08 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0002~~ QCA302 NONE FLT india1sesm ^M Location: india1sesm^M Category: processingError^M Cause: informationOutOfSequence^M Time: May 31 04:22:08 2005^M ComponentID: GWC-99^M SpecificProblem: Unexpected Record Sequence Number^M Description: Out of sequence QoS record received. Sequence Number = 1670001 Previous sequence number = 0^M

Log Report 305

Table 6 305 Message

Report Number	Message
305	Aug 19 22:18:34 wnc0s0qu QCA: _V2_~I=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0121~~ QCA305 NONE INFO wnc0s0qu ^M Location: wnc0s0qu^M Category: communications^M Cause: communicationsSubsystemFailure^M Time: Aug 19 22:18:34 2004^M SpecificProblem: Connection closed^M Description: Client at, IP Address: kiran-1.ca.nortel.com. Port: 2512 closed connection.^M

Log Report 310

Table 7 310 Message

Report Number	Message
310	May 30 22:52:45 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0000~~ QCA310 CRIT TBL india1sesm ^M Location: india1sesm^M NotificationID: 49^M State: Raise^M Category: Processing Error^M Cause: storageCapacityProblem^M Time: May 30 22:52:44 2005ComponentID: /data/qca/^M SpecificProblem: checkDiskSpace() has shown that there is less than ^M 104857600 bytes available on the local disk.^M Description: More Disk space is required immedietly.^M

Log Report 315

Table 8 315 Message

Report Number	Message
315	Aug 19 22:15:43 wnc0s0qu QCA: _V2_~I=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0001~~ QCA315 NONE FLT wnc0s0qu ^M Location: wnc0s0qu^M Category: processingError^M Cause: fileError^M Time: Aug 19 22:15:43 2004^M ComponentID:/data/qca/20000/output/active//data/qca/20000/output/active/QCA.QCA.QoS.2004.08.19_22.12_EDT.xml^M SpecificProblem: Active file: /data/qca/20000/output/active/QCA.QCA.QoS.2004.08.19_22.12_EDT.xmlhas been removed/deleted.^M Description: Data may have been lost. Creating new file, and attempting to write records again. Failure to do so will result in QCA shutdown.^M

Log Report 322

Table 9 322 Message

Report Number	Message
322	Aug 19 22:15:43 wnc0s0qu QCA: _V2_~I=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0004~~ QCA322 NONE INFO wnc0s0qu ^M Location: wnc0s0qu^M Category: communications^M Time: Aug 19 22:15:43 2004^M ComponentID: GWC-17^M SpecificProblem: New GWC connection^MDescription: New connection from GWC-17. Sequence Number = 1^M

Log Report 399

Table 10 399 Message

Report Number	Message
399	Aug 18 06:49:08 wnc0s0qu QCA: _V2_~I=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0087~~ QCA399 NONE INFO wnc0s0qu ^M Location: wnc0s0qu^M NotificationID: 49^M State: Cleared^M Time: Aug 18 06:49:08 2004^M

*** NOTE: (There are no changes in Alarms as a result of feature A00008338)

1> There are 3 different Types of Alarms uniquely identified by the Notification ID

a> Notification ID: 9

Event: Client is sending Records with unsupported Length.

Raise Severity (Major or Minor)

Raise Customer Log Report Number: QCA 301

Clear Severity: (None)

Clear Customer Log Report Number: QCA 399.

b> Notification ID: 57

Event: Client is sending Records with unsupported Version.

Raise Severity (Major or Minor)

Raise Customer Log Report Number: QCA 301

Clear Severity: (None)

Clear Customer Log Report Number: QCA 399.

c> Notification ID: 49

Event: Critical/Major/Minor Disk Space issue.

Raise Severity (Critical, Major or Minor)

Raise Customer Log Report Number: QCA 310.

Clear Severity: (None)

Clear Customer Log Report Number: QCA 399.

Example of Raise/Clear Alarms:

Table 11 301 Message- Raise

Report Number	Message
301	May 31 07:37:20 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0001~~ QCA301 MINOR FLT india1sesm ^M Location: india1sesm^M NotificationID: 9^M State: Raise^M Category:Processing Error^M Cause: corruptData^M Time: May 31 07:37:20 2005^M ^M ComponentID: GWC99^M SpecificProblem: The QCA has received records with 1 length errors from the source.^M Description: If 10 (or more) records with unsupported length^M are received consecutively, Major fault log is generated^M and the connection is closed.^M

Table 12 399 Message- Clear

Report Number	Message
399	May 31 07:39:47 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0001~~ QCA399 NONE INFO india1sesm ^M Location: india1sesm^M NotificationID: 9^M State: Cleared^M Time: May 31 07:39:47 2005^M

Appendix C- Increasing the size of a file system on a Sun server Application

Use one of the following procedures to increase the size of a file system on a Succession Server Platform Foundation Software (SSPFS)-based server:

- Simplex configuration (one server)

- High-availability configuration (two servers)

It is recommended you perform this procedure during off-peak hours.

The Succession Server Platform Foundation Software (SSPFS) creates file systems to best fit the needs of applications. However, it may be necessary to increase the size of a file system.

Not all file systems can be increased. The table below lists the file systems that cannot be increased, and lists examples of those that can be increased.

SSPFS file systems

Cannot be increased	Can be increased (examples)
/ (root)	/data
/var	/opt/nortel
/opt	/data/oradata
/tmp	/audio_files
/PROV_data	
/user_audio_files	
/data/qca	
/data/mg9kem/logs	

During the time file systems are being increased, writes to the file system are blocked, and the system activity increases. The more size that is added to the file system, the greater the impact on performance.

Prerequisites

Before you perform this procedure, verify that the file system is full or nearly full and that its content is valid application data. Remove any unneeded files or files generated in error that could be taking up disk space.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

At your workstation

1> Telnet to the Sun server by typing

> telnet <server>

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server that has the file system you want to increase

2> When prompted, enter your user ID and password.

3> Change to the root user by typing

$ su - root

and pressing the Enter key.

4> When prompted, enter the root password.

5> Access the command line interface by typing

cli

and pressing the Enter key.

Example response

Command Line Interface 1 - View

2 - Configuration

3 - Other
X - exitselect -

6> Determine which file system to increase by checking the current disk capacity utilization as follows:

a> Enter the number that corresponds to the “View” option in the menu.

Example response

View 1 - sspfs_soft (Display Software Installation Level Of SSPFS) 2 - chk_sspfs (Check SSPFS Processes) 3 - sw_conf (The software configuration of the znc0s0jx) 4 - cpu_util (Overall CPU utilization) 5 - cpu_util_proc (CPU utilization by process) 6 - port_util (I/O port utilization) 7 - disk_util (Filesystem utilization) X - exitselect -

b> Enter the number that corresponds to the “disk_util” option in the menu.

Example response

7> Determine the appropriate size for the file systems based on your specific needs.

8> Exit each menu level of the command line interface to eventually exit the command line interface, by typing

select - x

and pressing the Enter key.

9>

ATTENTION
Once you increase the size of a file system, you cannot decrease it.

Increase the size of the file system by typing

filesys grow -m <mount_point> -s <size>{m,g}

Where

mount_point
is the name associated with the file system

- /data
- /opt/nortel
- /data/oradata
- /PROV_data
- /audio_files
- /user_audio_files
- **/data/qca**
- /data/mg9kem/logs

size
is the size in megabytes (m) or gigabytes (g) you obtained in step 7

Example# filesys grow -m /data/qca -s 512m

Note: The example above increases the “/data” file system by 512 megabytes (MB).

10> You have completed this procedure.

High-availability configuration (two servers)

ATTENTION
During this procedure, the cluster will be running without a standby node. The duration is estimated at approximately one hour.

At your workstation

1> Telnet to the inactive node of the server cluster by typing

> telnet <server>

and pressing the Enter key.

where

server
is the physical IP address of the inactive node in the server cluster

2> When prompted, enter your user ID and password.

3> Change to the root user by typing

$ su - root

and pressing the Enter key.

4> When prompted, enter the root password.

5> Ensure the cluster is in a good state as follows:

a> Run the udstat command by typing

udstat

and pressing the Enter key.

If the system response contains “nodaemon”, “offline”, “down, “not mounted”, contact your next level of support. Otherwise, proceed to the next step.

b> Run the ubmstat command by typing

ubmstat

and pressing the Enter key.

If the system response is other than “ClusterIndicatorSTBY”. contact your next level of support. Otherwise, proceed to the next step.

c> Run the CheckConfiguration command by typing

CheckConfiguration

and pressing the Enter key.

If the system response is other than “Checking local cluster configuration against <other node>, contact your next level of support. Otherwise, proceed to the next step.

At the Inactive node

6>

ATTENTION
Once you increase the size of a file system, you cannot decrease it.

Increase the size of the desired file system by typing

GrowClusteredFileSystem.ksh <mount_point> <size>{m,g}

Where

mount_point
is the name associated with the file system, for example

- /data
- /opt/nortel
- /data/oradata
- /PROV_data
- /audio_files
- /user_audio_files

•/data/qca

•/data/mg9kem/logs

size
is the size in megabytes (m) or gigabytes (g)

Example# GrowClusteredFileSystem.ksh **/data/qca** 10m

Note: The example above increases the “/data/qca” file system by 10 megabytes (MB).

7> Reboot the Inactive node by typing

init 6

and pressing the Enter key.

8> Wait for the Inactive node to reboot, then log in again using its physical IP address.

9> Telnet to the active node of the Sun server cluster by typing

> telnet <server>

and pressing the Enter key.

where

server
is the physical IP address of the active node in the Sun server cluster

10> When prompted, enter your user ID and password.

11> Change to the root user by typing

$ su - root

and pressing the Enter key.

12> When prompted, enter the root password.

At the Active node

13> Stop the cluster by typing

StopCluster

and press the Enter key.

This action causes a cluster failover and makes the active node inactive, and the inactive node active.

At the newly Active node

14> Clone the other node using procedure Cloning the image of one node in a cluster to the other node on page 9 in this document.

15> You have completed this procedure.

Document Reference:

For increasing the size of a file system on an SSPFS-based server refer NN10402-600.

Appendix D: List of GWs that Report End of Call QoS Statistics.

12.1 GWs Supported

Table 1 : SN06

GW	SN06 Validation Level	SN06 Comments	Future Plans (Beyond SN06)
UAS (H.248)	Full	Does not currently report all stats. The stats that are reported depend on the mode: SendOnly: PS, OS SendRecv: PS, OS, PR, OR, PL RecvOnly: PR,OR,PL	
Motorola CG4500 (NCS)	Full	5.x stream. all stats reported. Latency calculation is not PacketCable compliant.	
PVG (Aspen/ VSP2)	Full	All stats reported.	
PVG (Aspen/ VSP3)	None	All stats reported.	
PVG (H.248)	None	All stats reported.	
Mediatrix (MGCP)	Partial		
Arris PacketPort (MGCP)	Full		
Arris TTM/ TTP (NCS)	Partial		

Table 1 : SN06

GW	SN06 Validation Level	SN06 Comments	Future Plans (Beyond SN06)
Askey	Partial	Validated basic functionality during End to End IT. Will do further testing during PV.	
CICM	None	CICM does not currently report end of call stats to the GWC.	Requirement submitted to CICM team, negotiating inclusion into SN07.

Table 2

GW	SN06.2 Validation Level	SN06.2 Comments	Future Plans (Beyond SN06.2)
UAS		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
MS2010 (Megaco/ H.248)		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
PVG (H.248)		All stats reported.	
H.248M2K		All Stats reported.	
Ambit MG1K		All Stats reported.	
Ambit 32		All Stats supported.	
PVG PP15K (VSP3 and VSP3oCard)		All Stats supported.	
PVG PP15K and PP7k (VSP2)		All parameters reported other than Jitter and inter-arrival latency which not measured.	

GW	SN06.2 Validation Level	SN06.2 Comments	Future Plans (Beyond SN06.2)
UAS		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	

GW	SN06.2 Validation Level	SN06.2 Comments	Future Plans (Beyond SN06.2)
MS2010 (Megaco/ H.248)		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
PVG (H.248)		All stats reported.	
H.248M2K		All Stats reported.	
Ambit MG1K		All Stats reported.	
Ambit 32		All Stats supported.	
PVG PP15K (VSP3 and VSP3oCard)		All Stats supported.	
PVG PP15K and PP7k (VSP2)		All parameters reported other than Jitter and inter-arrival latency which not measured.	

GW	SN07.0 Validation Level	SN07.0 Comments	Future Plans (Beyond SN07.0)
UAS		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
MS2010 (Megaco/ H.248)		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
PVG (H.248)		All stats reported.	
H.248M2K		All Stats reported.	
Ambit MG1K		All Stats reported.	
Ambit 32		All Stats supported	
PVG PP15K (VSP3 and VSP3oCard)		All Stats supported	
PVG PP15K and PP7k (VSP2)		All parameters reported other than Jitter and inter-arrival latency which not measured.	

GW	SN08.0 Validation Level	SN08.0 Comments	Future Plans (Beyond SN08.0)
Motorola MTA2	Y	All Stats Reported	
TTM/TTP Profile	Y	All Stats Reported	
ASKEY (4/12/ 30 Port Profile)	Y	All Stats Reported.	
Mediatrix 1104/1124 Profile	Y	All Stats Reported.	
UAS	Y	Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
MS2010 (Megaco/ H.248)	Y	Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
PVG (H.248)	Y	All stats reported.	
H.248M2K		All Stats reported.	
Ambit MG1K		All Stats reported.	
Ambit 32	Y	All Stats supported	
PVG PP15K (VSP3 and VSP3oCard)		All Stats supported	
PVG PP15K and PP7k (VSP2)	Y	All parameters reported other than Jitter and inter-arrival latency which not measured.	

Appendix E - QCA Versions available and the Binary content for each version

The following are the QoS Binary versions generated by loads in various releases. Version 1, 2, and 3 are for SN07, SN08 and SN09 Releases. Version 4, 5 are for patched SN07 and patched SN08 loads.

For Version 1:

132 byte - QoS binary message. Bytes are counted from 0 to N-1.

Header – 8 bytes (byte 0 to 7)
Codec – 2 bytes (byte 8 and 9)
Port Number – 2 bytes (byte 10 and 11)
IP Address – 4 bytes (byte 12 to 15)
GW Name – 32 bytes (byte 16 to 47) (first 32 bytes of FQDN)
End Point – 32 bytes (byte 48 to 79)
CLLI – 16 bytes (byte 80 to 95)
CorrID – 10 bytes (byte 96 to 105)
Two Byte Filler – 2 bytes (byte 106 and 107)
PacketSent – 4 bytes (byte 108 to 111)
PacketReceived – 4 bytes (byte 112 to 115)
OctetSent – 4 bytes (byte 116 to 119)
OctetReceived – 4 bytes (byte 120 to 123)
packetLost – 4 bytes (byte 124 to 127)
Jitter – 2 bytes (byte 128 and 129)
Latency – 2 bytes (byte 130 and 131)

For Version 4: (Jitter and latency mapping)

132 byte - QoS binary message. Bytes are counted from 0 to N-1.

Header – 8 bytes (byte 0 to 7)
Codec – 2 bytes (byte 8 and 9) (**Byte 8 and 9** holds information about the MSBytes of Jitter)
Port Number – 2 bytes (byte 10 and 11)
IP Address – 4 bytes (byte 12 to 15)
GW Name – 32 bytes (byte 16 to 47) (first 32 bytes of FQDN)
End Point – 32 bytes (byte 48 to 79)
CLLI – 16 bytes (byte 80 to 95)
CorrID – 10 bytes (byte 96 to 105)
Two Byte Filler – 2 bytes (byte 106 and 107) (**Byte106 and 107** holds the MSBytes of Latency component)

PacketSent – 4 bytes (byte 108 to 111)
PacketReceived – 4 bytes (byte 112 to 115)
OctetSent – 4 bytes (byte 116 to 119)
OctetReceived – 4 bytes (byte 120 to 123)
packetLost – 4 bytes (byte 124 to 127)
Jitter – 2 bytes (byte 128 and 129)
Latency – 2 bytes (byte 130 and 131)

Jitter and latency in Version 4 is of 4 bytes each, MSBytes of Jitter and Latency are obtained from Codec field and Filler byte fields of Version 1 respectively.

For Version 2:

136 byte - QoS binary message. Bytes are counted from 0 to N-1.

Header – 8 bytes (byte 0 to 7)
Codec – 2 bytes (byte 8 and 9)
Port Number – 2 bytes (byte 10 and 11)
IP Address – 4 bytes (byte 12 to 15)
GW Name – 32 bytes (byte 16 to 47) (first 32 bytes of FQDN)
End Point – 32 bytes (byte 48 to 79)
CLLI – 16 bytes (byte 80 to 95)
CorrID – 10 bytes (byte 96 to 105)
Two Byte Filler – 2 bytes (byte 106 and 107)
PacketSent – 4 bytes (byte 108 to 111)
PacketReceived – 4 bytes (byte 112 to 115)
OctetSent – 4 bytes (byte 116 to 119)
OctetReceived – 4 bytes (byte 120 to 123)
packetLost – 4 bytes (byte 124 to 127)
Jitter – 4 bytes (byte 128 and 131)
Latency – 4 bytes (byte 132 and 135)

For Version 5: (Timestamp Patched load)

144 byte - QoS binary message. Bytes are counted from 0 to N-1.

Header – 8 bytes (byte 0 to 7)
Codec – 2 bytes (byte 8 and 9)
Port Number – 2 bytes (byte 10 and 11)
IP Address – 4 bytes (byte 12 to 15)
GW Name – 32 bytes (byte 16 to 47) (first 32 bytes of FQDN)
End Point – 32 bytes (byte 48 to 79)
CLLI – 16 bytes (byte 80 to 95)
CorrID – 10 bytes (byte 96 to 105)
Two Byte Filler – 2 bytes **(removed)**
STime – 5 bytes (byte 106 to 110)
ETime – 5 bytes (byte 111 to 115)
PacketSent – 4 bytes (byte 116 to 119)
PacketReceived – 4 bytes (byte 120 to 123)
OctetSent – 4 bytes (byte 124 to 127)
OctetReceived – 4 bytes (byte 128 to 131)
packetLost – 4 bytes (byte 132 to 135)
Jitter – 4 bytes (byte 136 and 139)
Latency – 4 bytes (byte 140 and 143)

For Version 3:

180 byte - QoS binary message. Bytes are counted from 0 to N-1.

Header – 8 bytes (byte 0 to 7)
Codec – 2 bytes (byte 8 and 9)
Port Number – 2 bytes (byte 10 and 11)
IP Address – 4 bytes (byte 12 to 15)
GW Name – 64 bytes (byte 16 to 79) (first 64 bytes of FQDN)
End Point – 32 bytes (byte 80 to 111)
CLLI – 16 bytes (byte 112 to 127)
CorrID – 10 bytes (byte 128 to 137)
STime – 5 bytes (byte 138 to 142)

ETime – 5 bytes (byte 143 to 147)
PacketSent – 4 bytes (byte 148 to 151)
PacketReceived – 4 bytes (byte 152 to 155)
OctetSent – 4 bytes (byte 156 to 159)
OctetReceived – 4 bytes (byte 160 to 163)
packetLost – 4 bytes (byte 164 to 167)
Jitter – 4 bytes (byte 168 and 171)
Latency – 4 bytes (byte 172 and 175)
32 Bit Filler – 4 bytes (byte 176 and 179)

Header Field details:

```
// ------------------ Report Header variables ----------------------------
private int mgcType = -1;        // bits 0 to 3 of byte 0
private int messageType = -1;    // bits 4 to 7 of byte 0
private int sequenceNumber = -1; // bytes 1 to 3
private int reportType = -1;     // bits 0 to 3 of byte 4
private int version = -1;        // bits 4 to 7 of byte 4
private int mgcNumber = -1;      // byte 5
private int msgLength = -1;      // byte 6
private int ipVersion = -1;      // byte 7 (IP version 2-bits plus 6-bit filler)
// ------------------ End of Report Header variables ----------------------
```

25: Functional Description (FN): A0009321

25.1 Feature name and Feature ID

A00009321 - NMC Code Blocking

25.2 Description

25.2.1 Introduction

This feature is to enhance the Mass Call function on the CS2Kc system.

GAP is a existing hidden CBK option which is the time interval between completed calls. In Code Blocking feature, another CBK option PCT is provided. Within the implementation of this activity, following will be covered:

- *Percentage*(PCT) is a CBK option which allows calls to be blocked from proceeding based upon the destination code(digits). Calls can be blocked by a specified percentage ranges from 1 to 100. Blocked calls can have one of three possible treatments applied: NCA, EA1, or EA2.

Whether a CBK control should be applied only depends on the destination digits. it does not care the call agent is line or any kind of trunk.

25.2.2 Block calls with the percentage

The Code Blocking control provides a means to block calls from progressing further into the Network. Because the route taken by a call is determined by the destination code, the control provides a means to limit traffic over particular routes.

A certain percentage(between 1 and 100 percent) can be defined in PCT option and the specified percentage of calls should be blocked based on the preset destination code.

Calls which are blocked from proceeding further into the Network can be sent to one of three possible treatments:

- No Circuit Announcement (NCA);

- Emergency Announcement 1 (EA1); or
- Emergency Announcement 2 (EA2).

25.2.3 PCT option is available in MASSCALL command

MASSCALL command is implemented to List/Apply/Remove mass call control. PCT is available in MASSCALL command as a CBK option.

Following are some examples:

Example 1

```
MASSCALL APPLY CBK PCT PX CSXLA '8308001' '8308004'
60 NCA
```

In this example, only 40 percent of calls which enters:

1. UXLA with an XLASYS of PX
2. XLANAME of CSXLA with called party digits starting in range from ’8308001’ to ’8308004’

will be allowed to complete, all other calls will be sent to NCA treatment.

Example 2

```
MASSCALL APPLY CBK GAP PX CSXLA '8308001' '8308004'
'60.0' NCA
```

In this example, only one call per 60 seconds which enters:

1. UXLA with an XLASYS of PX
2. XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’

will be allowed to complete, all other calls will be sent to NCA treatment.

Example 3

```
MASSCALL LIST CBK PCT PX CSXLA ALL
```

In this example, all the percentage code blocking controls that applied which enters UXLA with an XLASYS of PX and an XLANAME of CSXLA will be listed.

Example 4

```
MASSCALL LIST CBK GAP PX CSXLA ALL
```

In this example, all the gap code blocking controls that applied which enters UXLA with an XLASYS of PX and an XLANAME of CSXLA will be listed.

Example 5

```
MASSCALL REMOVE CBK PCT PX CSXLA '8308001' '8308004'
```

In this example, the percentage code blocking control which enters

1. UXLA with an XLASYS of PX

2. XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’

will be removed.

Example 6

```
MASSCALL REMOVE CBK GAP PX CSXLA '8308001' '8308004'
```

In this example, the gap code blocking control which enters

1. UXLA with an XLASYS of PX

2. XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’

will be removed.

25.2.4 PCT option is available in MAPCI commands

PCT is available in MAPCI commands as a CBK option. Direct access to the CodeCtrl menu level is from the Command Interpreter (CI) level by entering the commands “`MAPCI;NWM;CODECTRL`”. This level can also be entered indirectly by selecting the appropriate menu item until the desired level is reached.

CodeCtrl commands are to List, Apply and Remove code controls. PCT option is available in these code control commands.

Followings are some examples:

Example 1

```
APPLY CBK PCT PX CSXLA '8308001' '8308004' 60 NCA
```

In this example, only 40 percent of calls which enters:

1. UXLA with an XLASYS of PX

2. XLANAME of CSXLA with called party digits starting in range from ’8308001’ to ’8308004’

will be allowed to complete, all other calls will be sent to NCA treatment.

Example 2

```
APPLY CBK GAP PX CSXLA '8308001' '8308004' '60.0' NCA
```

In this example, only one call per 60 seconds which enters:

1. UXLA with an XLASYS of PX

2. XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’

will be allowed to complete, all other calls will be sent to NCA treatment.

Example 3

```
LIST CBK PCT PX CSXLA ALL
```

In this example, all the percentage code blocking controls that applied which enters UXLA with an XLASYS of PX and an XLANAME of CSXLA will be listed.

Example 4

```
LIST CBK GAP PX CSXLA ALL
```

In this example, all the gap code blocking controls that applied which enters UXLA with an XLASYS of PX and an XLANAME of CSXLA will be listed.

Example 5

```
REMOVE CBK PCT PX CSXLA '8308001' '8308004'
```

In this example, the percentage code blocking control which enters

1. UXLA with an XLASYS of PX
2. XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’

will be removed.

Example 6

```
REMOVE CBK GAP PX CSXLA '8308001' '8308004'
```

In this example, the gap code blocking control which enters

1. UXLA with an XLASYS of PX
2. XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’

will be removed.

25.2.5 TRAVER routines

A new message is created to be displayed if PCT option is activated while doing TRAVER which is as following:

- ‘A Mass Call Code Block Control with percentage may affect this call.’

The message which displayed if GAP option is activated while doing TRAVER is also modified to indicate that this condition is encountered. Followoing is the message:

- ‘A Mass Call Code Block Control with gapping may affect this call.’

A TRAVER example of a call encountering a PCT Code Blocking Control is shown in Figure 1.

Figure 1 TRAVER example displaying Mass Call warning message

```
>traver l 8306007 8306008 b
TABLE IBNLINES
LG 00 1 00 06 0 DT STN IBN 8306007 CSGRPA 0 0 131 $
……

TABLE DIGCOL
TUPLE NOT FOUND
Default is RPT
TABLE IBNXLA: XLANAME CSXLA
CSXLA 830 NET N N 0 N CSDIG Y Y DOD N CSIDXA CSGRPA CS_NIL NONE $
TABLE DIGCOL
TUPLE NOT FOUND
Default is RPT
TABLE LINEATTR
CSIDXA IBN DAT1 NT 0 0 NILSFC 0 PX CSXLA TESTTONE 00 CSGRPA CS_NIL $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
CSGRPA NSCR 131 NPRT NONE N $ $
TABLE RATEAREA
CS_NIL NLCA NIL NILLATA $
NOTE: A Mass Call Code Block Control with percentage may affect this call.
TABLE PXHEAD
CSXLA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                          8306008
TABLE PXCODE
CSXLA 83060 83060 CONT ( MM 7 7) ( XLT PX CSTERM)$
TABLE PXHEAD
CSTERM SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                          8306008
TABLE PXCODE
CSTERM 830 830 DNRTE ( CLASS NATL) ( DN 131 830)$

……
```

25.3 Hardware Requirements or Dependencies

No hardware dependency.

25.4 Software Requirements or Dependencies

None.

25.5 Limitations and restrictions

Please refer to the activity AU3395-Mass Call Control FN document for limitations and restrictions as there are no new restrictions are added by this feature to the functionality.

The ‘MM’ option in translation allows the possibility of creating an "unreachable" Mass Call Control tuple. (i.e. A Mass Call tuple with more digits than the Min value of the associated call's translations.) This attempt at setting a Mass Call Control is unreachable and could never be exercised. To avoid this issue, the minimum value in ‘MM’ should be datafilled not less than the digits in the masscall control code.

The Pass and Block counters are reset to 0 when they reach the maximum value 65536.

25.6 Interactions

This feature is a enhancement of Mass Call Control feature. A new CBK option PCT is implemented to provide the function to block calls with percentage based upon destination digits. This feature does not extend the capacity of the Code block control. The sum of CBK, PRP and HTRF entries still can not exceed 256.

25.7 Glossary

Term	Description
CBK	Code Blocking
PCT	Code Blocking with percentage
GAP	Code Blocking with gapping
TRAVER	Translation verification

25.8 References

1. AU3395 - Mass Call Control

2. 2990 - RFF - CHT NMC Code Blocking RFF v2

26: Functional Description (FN): A0009322

26.1 Feature name and Feature ID

A00009322 - Call Lock and Do Not Disturb Enhancements

26.2 Description

26.2.1 Call Lock

26.2.1.1 Introduction

CEPT ILR feature gives the administrator the capability to restrict outgoing calls for the subscriber according to the predefined restriction classes. The administrator can assign, de_assign, activate or deactivate this feature on a line via Service Order or assign and de_assign the feature by using the default option functionality. Subscribers are able to activate, deactivate or interrogate ILR feature by dialing access codes.

The following enhancements are provided by this activity over existing Call Lock Feature:

- To support dial tone during the deactivation procedure.The user can originate a new call directly after the successful deactivation without going on hook.
- To allow class of restriction to be overwritten by new entry without doing a feature deactivation.
- To allow the user to change the password according to the required dialing sequence LH DT*SC*PWO*PWN#CT. The password is 4 digits.
- To generate report and disallow any feature modification (activation, deactivation, change) until the following day upon 3 times of wrong password entry in succession, or until the administration by operator. The following day is the time after the next 00:00 midnight. The 3 times is the value of field MAX_PIN_RETRY which is datafilled in CEPTPW tuple of table ISERVOPT. The password is 4 digits.

26.2.1.2 General Considerations

These enhancements are provided for IBN lines. There are some prerequisites to implement these enhancements which are:

- For the first two enhancements the subscriber should assigned ILR option.
- For the last two enhancements the subscriber should assigned CEPTPW option.

For the assignment of ILR and CEPTPW option, please refer to References 1,2,3.

26.2.1.3 To support dial tone during the deactivation procedure

The subscriber will hear dial tone instead of confirm tone when deactivating the ILR successfully, and the subscriber can originate a new call directly after the successful deactivation without going on hook.

Dial tone is optional and determined according to the field ALLOW_ORIG_AFTER_DEACT of ILRCLS tuple in table ISERVOPT.

- ALLOW_ORIG_AFTER_DEACT {BOOLEAN}: indicates that the dial tone will be generated or confirm tone will be generated. If it is set as ‘Y’, dial tone is generated and the user can originate a new call directly after the successful deactivation without going on hook. Otherwise, confirm tone is generated. The default value for the field is ‘N’.

Figure 1 :The View of CEPT_FTR_DIALTONE tuple in ISERVOPT table

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ilrcls
OPTION:
>ilrcls
ILR_PROG:
>n
SDT:
>n
CR_PSWD:
>y
SHOW_CHG_PSWD:
>y
ALLOW_ORIG_AFTER_DEACT:
>y
OVERRIDE_ILR_CLASS:
>y
TUPLE TO BE ADDED:
            ILRCLS ILRCLS N N Y Y Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
...
```

26.2.1.4 To allow class of restriction to be overwritten by new entry without doing a feature deactivation

The subscriber can overwrite the class of restriction when activating the ILR option without doing a ILR deactivation first by using the following dialing sequence:

LH DT*SC*PW*CR#CT

This enhancement is optional and determined according to the field OVERRIDE_ILR_CLASS of ILRCLS tuple in table ISERVOPT.

- OVERRIDE_ILR_CLASS{BOOLEAN}: indicates whether the user can overwrite the class of restriction when activating the ILR option without doing a ILR deactivation first or not. If it is set as ‘Y’, the user can overwrite the class of restriction, otherwise can’t. The default value for the field is ‘N’.

Figure 2 The view of ILRCLS Tuple in ISERVOPT Table

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ilrcls
OPTION:
>ilrcls
ILR_PROG:
>n
SDT:
>n
CR_PSWD:
>y
SHOW_CHG_PSWD:
>y
ALLOW_ORIG_AFTER_DEACT:
>y
OVERRIDE_ILR_CLASS:
>y
TUPLE TO BE ADDED:
            ILRCLS ILRCLS N N Y Y Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
...
```

Please refer to References 1,2.

26.2.1.5 To allow the user to change the password according to the required dialing sequence LH DT*SC*PWO*PWN#CT

The user can change the password according to the required dialing sequence LH DT*SC*PWO*PWN#CT when CEPTPW line option is assigned to the subscriber.

This enhancement is optional and determined according to the field NEW_PWD_ONCE of tuple CEPTPW in table ISERVOPT.

- NEW_PWD_ONCE{BOOLEAN}: indicates whether the user can change the password by the dialing sequence LH DT*SC*PWO*PWN#CT or not. If it is set as ‘Y’, the user can change the password by this dialing sequence. Otherwise the subscriber can change the password by the dialing sequence LH DT*SC*PWO*PWN*PWN#CT. The default value for the field is ‘N’.

Figure 3 The view of CEPTPW Tuple in ISERVOPT Table

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ceptpw
OPTION:
>ceptpw
MAX_PIN_RETRY:
>3
DEFAULT_PIN:
>1111
PIN_VALID:
>n
COLLECT_DNPIN_IN_DIFF_STAGES:
>n
ANNOUNCE:
>n
NEW_PWD_ONCE:
>y
AUTO_UNLOCK:
>y
TUPLE TO BE ADDED:
            CEPTPW CEPTPW 3 1111 N N N Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

Please refer to References 3.

26.2.1.6 Password Unlock

When CEPTPW and ILR line option is assigned to the subscriber, upon 3 times of wrong password entry in succession the subscriber will be disallowed any feature modification (activation, deactivation, change) until the following day , or until the administration by operator.The following day is the time after the next 00:00 midnight. The 3 times is the value of field MAX_PIN_RETRY which is datafilled in CEPTPW tuple of table ISERVOPT. The password is 4 digits.

CEPT102 log is generate when subscriber is locked. This log has four fields which are:

- Date and time

- feature
- action of the third wrong password
- calling DN

This enhancement is optional and determined according to the field AUTO_UNLOCK of tuple CEPTPW in table ISERVOPT.

- AUTO_UNLOCK{BOOLEAN}: indicates whether the information of locked user will be recorded and the locked user will be unlocked in the following day automatically. If it is set as 'Y', the locked user will be unlocked automatically in the following day. The default value for the field is 'N'.

Figure 4 The view of CEPTPW Tuple in ISERVOPT Table

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ceptpw
OPTION:
>ceptpw
MAX_PIN_RETRY:
>3
DEFAULT_PIN:
>1111
PIN_VALID:
>n
COLLECT_DNPIN_IN_DIFF_STAGES:
>n
ANNOUNCE:
>n
NEW_PWD_ONCE:
>y
AUTO_UNLOCK:
>y
TUPLE TO BE ADDED:
            CEPTPW CEPTPW 3 1111 N N N Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

26.2.2 Do Not Disturb

26.2.2.1 Introduction

When a called subscriber has CEPT Do Not Disturb feature active then the calling subscriber receives a busy tone or an announcement.

The following enhancements are provided by this activity over existing CDND Feature:

- To support Special Dial Tone if the feature is activated.
- To disable the ring splash.
- To support dial tone upon feature deactivation dialing sequence, the user is able to originate new call without hanging up.

26.2.2.2 General Considerations

These enhancements are developed for IBN lines.

26.2.2.3 To support special dial tone if the feature is activated

This function has been implemented by feature AT.59019083 and updated by feature AT.59022097. In table ISERVOPT, if the SPECIAL_DIAL_TONE field of CEPT_CFX tuple set to Y and CFD_CFB_INDICATION field of CEPT_CFX set to Y and CDND is active, the special dial tone will be given. A verify will be done in PV stage.

26.2.2.4 Disable the ring splash

CEPT CDND has no ring splash.

26.2.2.5 To support dial tone instead of confirmation tone during the deactivation procedure

The subscriber will hear dial tone instead of confirm tone when deactivating the CDND successfully, and the subscriber can originate a new call directly without hanging up.

Dial tone is optional and determined according to a datafill at table ISERVOPT. There is a new tuple CDND defined in table ISERVOPT, and a new field ALLOW_ORIG_AFTER_DEACT is added in this tuple.

- ALLOW_ORIG_AFTER_DEACT {BOOLEAN}: indicates that the dial tone will be generated or confirm tone will be generated. If it is set as ‘Y’, dial tone is generated. Otherwise, confirm tone is generated. The default value for the field is ‘N’.

Figure 5 :Example of ISERVOPT table datafill

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>CDND
OPTION:
>CDND
ALLOW_ORIG_AFTER_DEACT:
>y
TUPLE TO BE ADDED:
CDND CDND Y

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
...
```

26.3 Hardware Requirements or Dependencies

Please refer to the hardware requirements or dependencies part of References 1,2,3,4,5.

26.4 Software Requirements or Dependencies

This feature does not affect the provision method of CEPT ILR, CEPTPW and CDND. It takes effect when the subscriber is using CEPT ILR, CEPTPW and CDND and it is controlled by following datafill:

- in table ISERVOPT, tuple ILRCLS, the ‘Allow_orig_after_deact’ field

- in table ISERVOPT, tuple ILRCLS, the ‘Override_ilr_class’ field

- in table ISERVOPT, tuple CEPTPW, the ‘New_pwd_once’ field

- in table ISERVOPT, tuple CDND, the ‘Allow_orig_after_deact’ field

Please refer to the software requirements or dependencies part of References 1,2,3,4,5 for more details.

26.5 Limitations and restrictions

- The user will not be locked when user input wrong password three times in succession in the period of ONP Swact.
- The max locked users who can be unlocked automatically simultaneously in the following day is limited to 10000. When the number of locked users exceed 10000, the new locked user cann't be unlocked automatically in the following day, but CEPT 102 log will still be generated.

For the other details of limitations and restrictions, please refer to References 1,2,3,4,5.

26.6 Interactions

Please refer to the interaction part of References 1,2,3,4,5.

26.7 Glossary

Term	Description
LH	Lift Handset
SC	Service Code
CR	Class Restrict
PW	Password
DT	Dial Tone
DN	Dial Number
CT	Confirm Tone
PWO	Old Password
PWN	New Password
CM	Core Machine
CEPT	European Conference of Postal and Telecommunications Administrations
ILR	International Line Restriction
CDND	CEPT Do not Disturb

26.8 References

1. A59019295 - CEPT International Line Restriction

2. A00001914 - CEPT International Line Restriction Enhancements

3. A00001919 - CEPT Services Password Enhancement

4. A59019083 - CEPT Call Diversion and CEPT Do Not Disturb
5. A00002755 - China PSTN Line Service Compliance
6. SFR2992 - CHT Call Lock
7. SFR2993 - CHT Do Not Disturb

27: Functional Description (FN): A00009373

27.1 Feature name and Feature ID

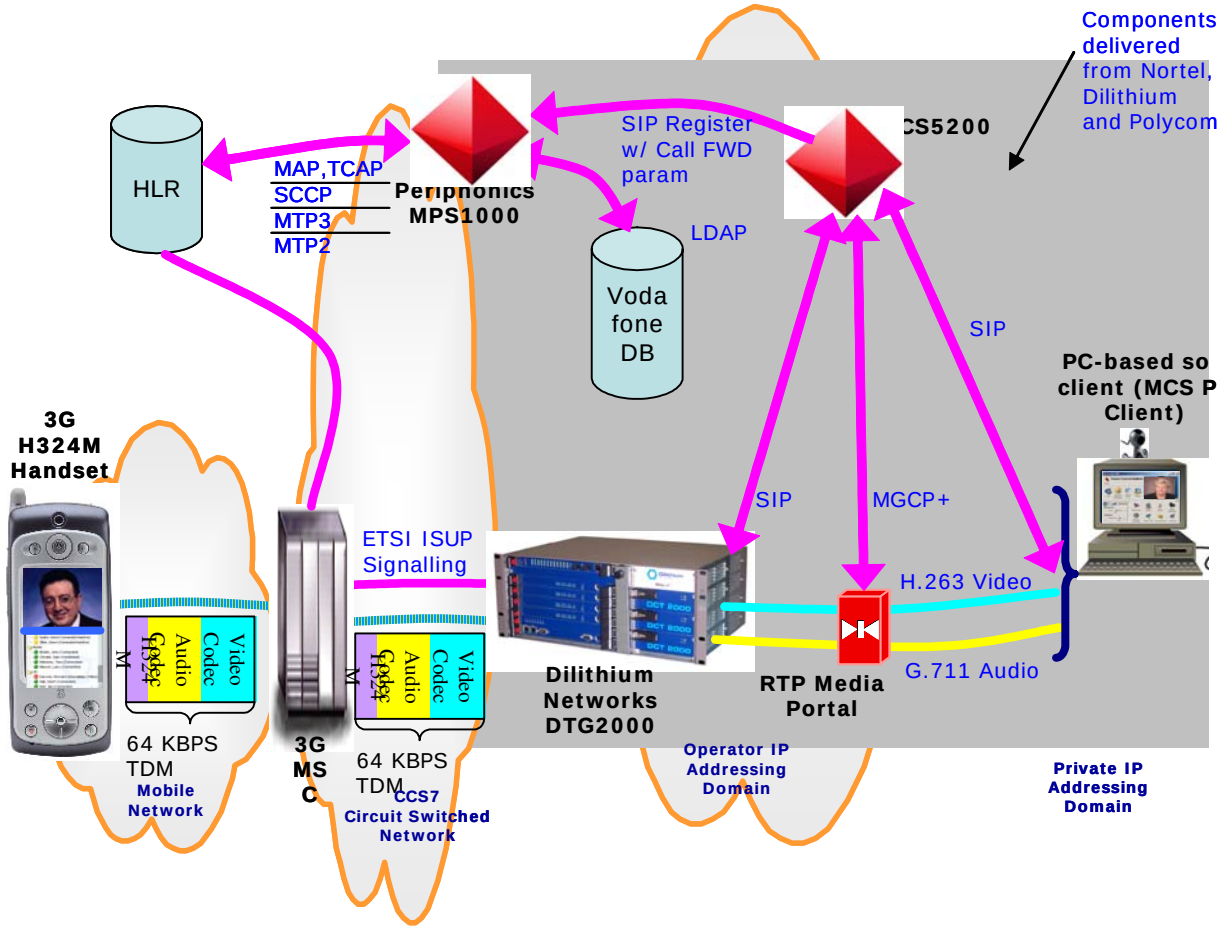
A00009373 - Vodafone Portugal 3G Video Features (Interworking)

27.2 Description

Vodafone Portugal 3G Video Features is an infrastructure that allows MTS R99 H.324M terminal users to have conversational video sessions with users based in a fixed packet network, and it also allows those UMTS R99 H.324M terminal users to access fixed network based application servers. The infrastructure will support sessions that are mobile to MCS client, MCS client to mobile and MCS client to MCS client.

This feature redirects calls destined to a mobile subscriber's wireless number to that subscriber's MCS client, if the subscriber is logged on to their MCS client and is requesting the forwarding of calls. Mobile subscribers will just have the basic 2 way voice and video call in this phase.

Figure 1 Functional Behavior Diagram

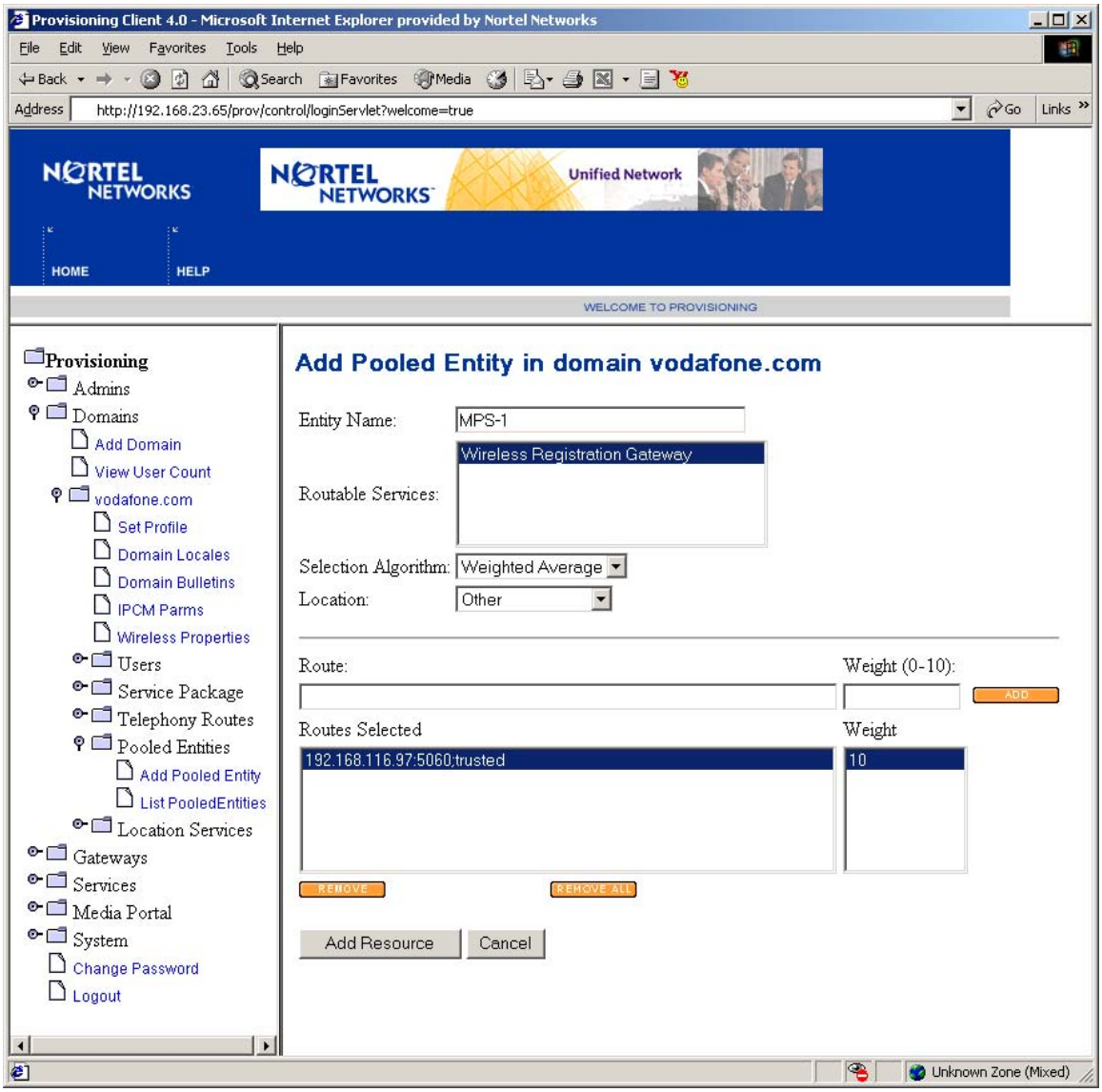


27.3 Network Configuration

27.3.1 MPS1000 Provisioning

The MCS supports multiple MPS1000 servers, and routes outbound calling traffic across them in a load balanced fashion. MPS1000 servers will be provisioned as a pooled resource by the MSC. This will allow multiple MPS IP addresses and associated weights to be provisioned for the support of load balancing and load sharing. See the figure 2 for an example of provisioning MPS servers with the MCS Provisioning Client.

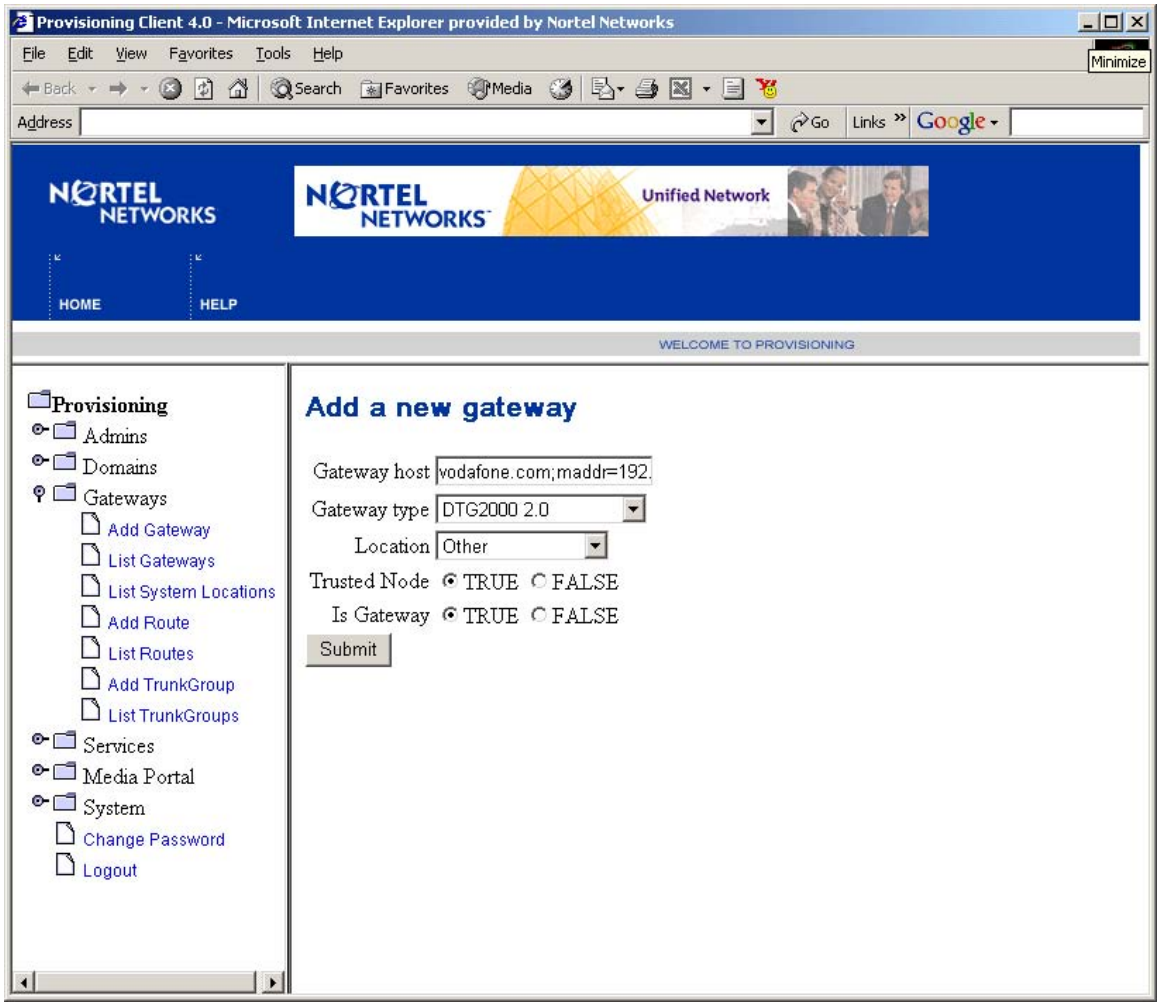
Figure 2 Provisioning MPS1000 as a Pooled Entity



27.3.2 DTG Provisioning

The MCS will support multiple Dilithium gateways. The DTG2000 will be provisioned as trusted gateways by the MCS. Telephony Translation will be used to determine which specific DTG to route outgoing calls through. See figure 3 for an example the DTG2000 gateway provisioning.

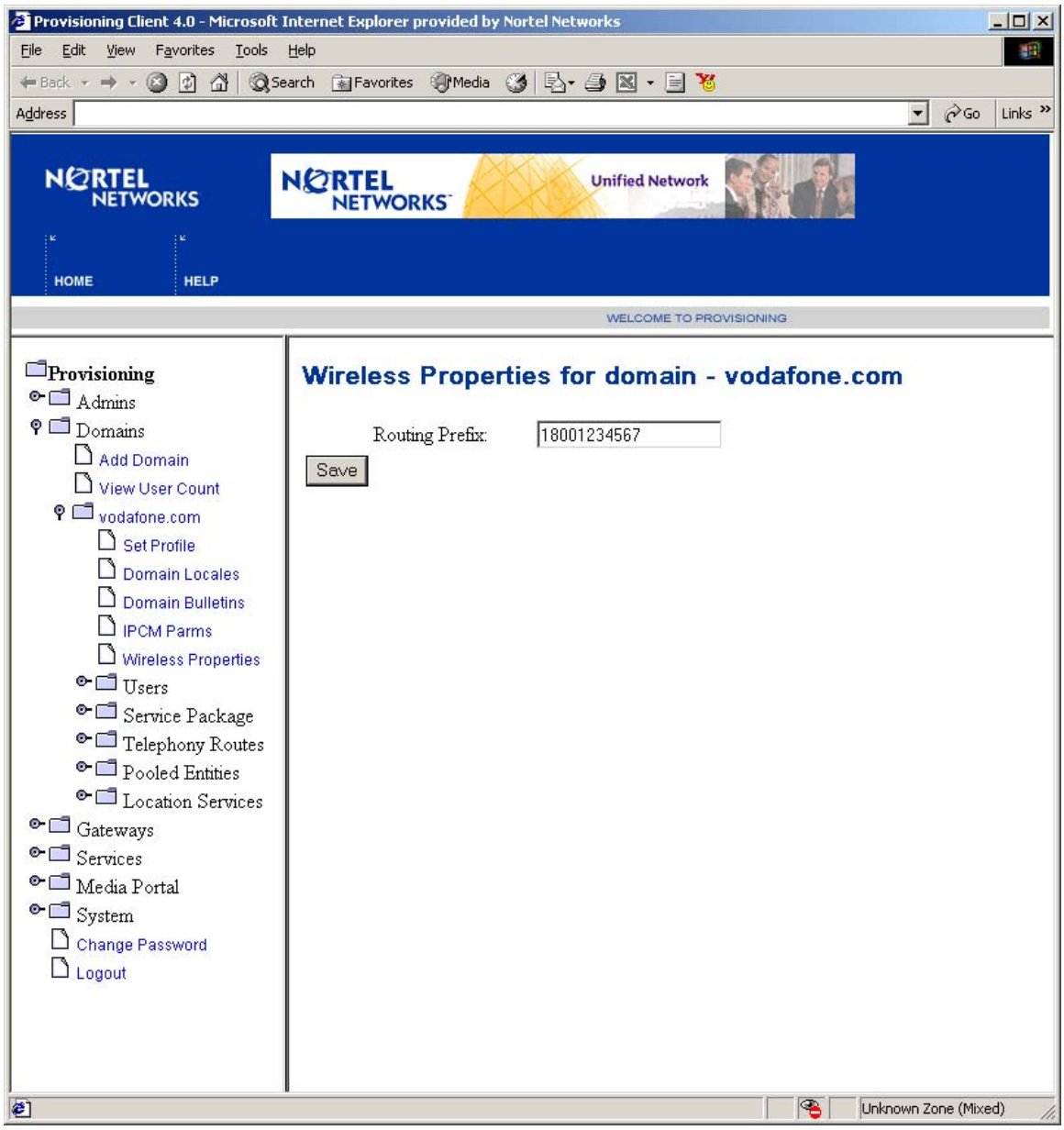
Figure 3 Provisioning DTG2000 as a trusted gateway



27.3.3 Wireless Properties

Wireless properties allow the operator to provision a single routing number that will be used across the MCS for all subscribers. This number will be used to route incoming wireless calls to the appropriate MCS system via the DTG2000. This routing prefix is sent to the MPS during registration. See Figure 4 for an example provisioning screen.

Figure 4 Provisioning the Routing Prefix



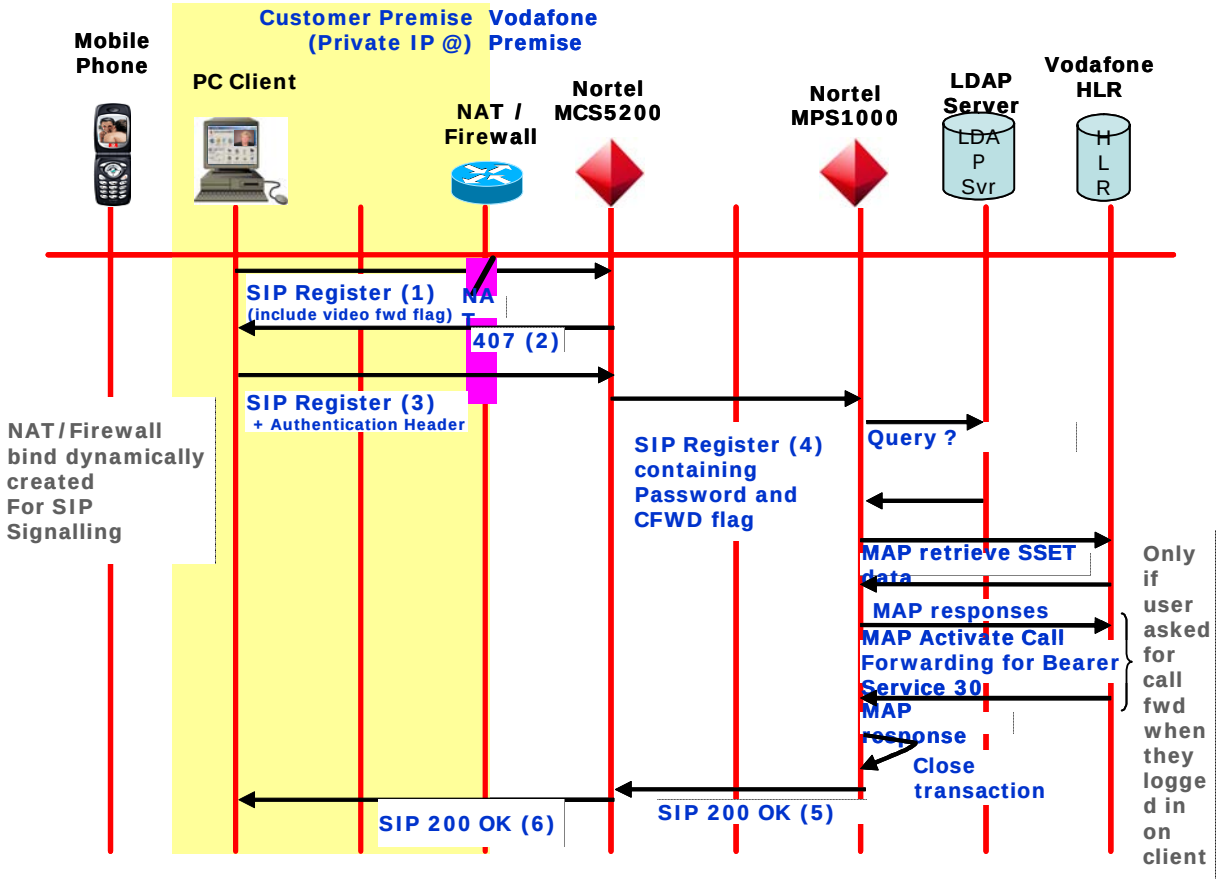
27.3.4 Subscriber Registration Requirements

User registration occurs when a subscriber logs into a client which triggers the client to send a registration message to the MCS. Since these subscribers are dynamic, and not initially provisioned on MCS, the MCS will challenge the subscriber and require proper credentials. After the subscriber supplies credentials, the MCS sends a SIP REGISTER message to the MPS1000 with the subscriber's credentials, routing prefix, and the state of the CFWD checkbox from the MCS PC Client. After doing a successful query, the MCS creates a user account for this subscriber using the user-id supplied by the user.

The MCS also populates the subscriber's record with data received in the 200OK from the MPS1000. This data includes the call barring state, pre-paid or post-paid, called prefix, and call forwarding information for the subscriber. A default service package and locale will be set for all subscribers. The subscriber will be able to only change the locale, but not the service package. See figure 5 for a call flow that describes this requirement.

If the MCS cannot create a dynamic account for any reason, the registration response returned to the subscriber must indication failure to register due to lack of system resources.

Figure 5 Figure 5 Registration Message flow



26.3.5 Registration SIP Messages

The following are examples of registration SIP messages.

(1) (3)REGISTRATION (from PC Client to MCS)

Required changes in BLUE italic. The cfwd flag is added to the Contact.

```
REGISTER sip:vodaphone.com:5060 SIP/2.0
Via: SIP/2.0/UDP 47.102.116.97:5060
Call-ID: 5211-93bc-92f0-854c924c@47.102.116.97
To: <sip:8888@vodaphone.com>
From: <sip:8888@vodaphone.com>;tag=897-93bc-92f0-
854c924c
Contact:
<sip:8888@47.102.116.97>;expires=7200;description="Login
";cfwd="True"
Expires: 7200
CSeq: 1 REGISTER
User-Agent: Nortel PCC 3.0.203
x-nt-GUID: 005fd1344a044c204e13085f30140aef4e2ff6
x-nt-location: 14050
Accept-Encoding: nt-im-2.0
l: 0
```

(4) REGISTRATION (from MCS to MPS)

The mobile DN is specified in the from header.

```
REGISTER sip:vodaphone.com:5060 SIP/2.0
Via: SIP/2.0/UDP 47.102.116.97:5060
Call-ID: 5211-93bc-92f0-854c924c@47.102.116.97
To: <sip:8888@vodafone.com>
From: <sip:8888@vodafone.com>;tag=897-93bc-92f0-854c924c
Contact:
<sip:8888@47.102.116.97>;expires=7200;description="Login
"
Expires: 7200
CSeq: 1 REGISTER
User-Agent: Nortel PCC 3.0.203
x-nt-GUID: 005fd1344a044c204e13085f30140aef4e2ff6
x-nt-location: 14050
Accept-Encoding: nt-im-2.0
l: 202
c: application/com.nortelnetworks.applications.3g-
registration+xml
```

```
<?xml version="1.0" encoding="UTF-
8"?><registration><msgType>register</
msgType><password>zzzz2x</password><forwardNumber>45</
forwardNumber><forwardCall>true</forwardCall></
registration>
```

(5) SUCCESS REGISTRATION RESPONSE (from MPS to MCS)

Required changes in BLUE italic.

```
SIP/2.0 200 Registration Successful
t: <sip:8888@vodaphone.com>;tag=675143675
f: "8888 Mr" <sip:8888@vodaphone.com>;tag=897-93bc-92f0-
854c924c
i: 5211-93bc-92f0-854c924c@47.102.116.97
CSeq: 1 REGISTER
v: SIP/2.0/UDP 47.102.116.97:5060
m: <sip:8888@47.102.116.97>;expires=7199
k: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
l: 202
c: application/com.nortelnetworks.applications.3g-
registration+xml

<?xml version="1.0" encoding="UTF-
8"?><registration><msgType>response</
msgType><barred>false</barred><paymentType>prepaid</
paymentType><forwardNumber>8888</
forwardNumber><calledPrefix>66</calledPrefix></
registration>
```

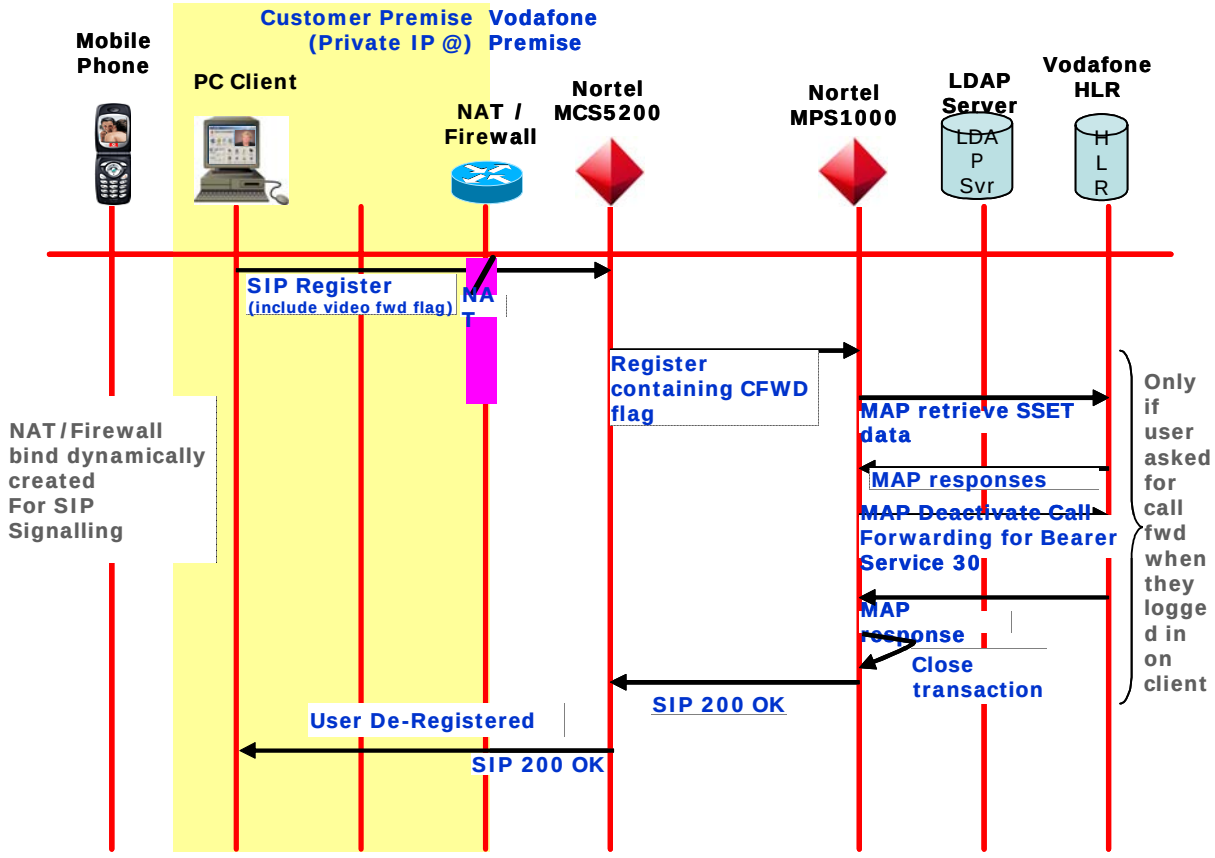
27.3.6 Subscriber De-registration Requirements

When a user logs out of the client or is unreachable, the MCS will de-register the dynamic user by restoring the original CFWD information, if needed, in the HLR and deleting the local subscriber info. Restoring the CFWD information is done by sending a SIP REGISTER with ‘expires=0’ and the original CFWD information to the MPS1000 which will restore the HLR via MAP. This is done only if the subscriber checked the CFWD check box on the MCS PC Client during registration. Once the MPS1000 responds to the MCS will delete the dynamic subscriber and all information related to the user. If the CFWD checkbox was not checked, the MCS will delete the local subscriber info without any interaction with the MPS1000.

An unreachable subscriber is a subscriber that cannot be contacted when an incoming call, SIP INVITE, arrives for the subscriber. There can be several scenarios of when this would occur and these are just a few:

- MCS PC Client crash
- Computer crash
- Loss of network connectivity

Figure 6 De-Registration Call Flow



27.3.7 De-Registration (from MCS to MPS)

The following is an example of a de-registration SIP message.

DE-REGISTRATION (from MCS to MPS)

Required changes in BLUE italic.

```
REGISTER sip:vodaphone.com:5060 SIP/2.0
Via: SIP/2.0/UDP 47.102.116.97:5060
```

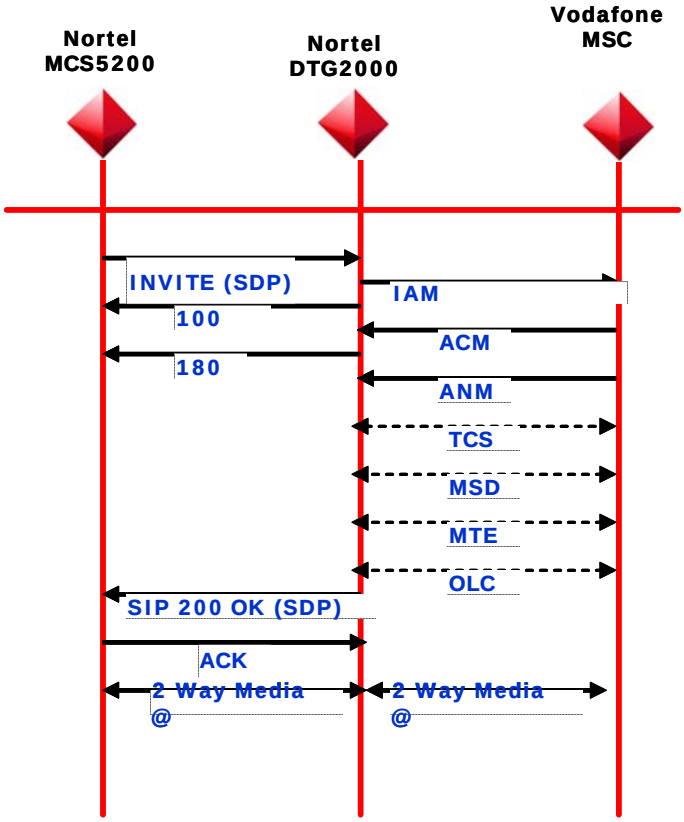
```
Call-ID: 5211-93bc-92f0-854c924c@47.102.116.97
To: <sip:8888@vodafone.com>
From: <sip:8888@vodafone.com>;tag=897-93bc-92f0-854c924c
Contact:
<sip:8888@47.102.116.97>;expires=0;description="Logout"
CSeq: 1 REGISTER
User-Agent: Nortel PCC 3.0.203
x-nt-GUID: 005fd1344a044c204e13085f30140aef4e2ff6
x-nt-location: 14050
Accept-Encoding: nt-im-2.0
l: 202
c: application/com.nortelnetworks.applications.3g-
registration+xml


<?xml version="1.0" encoding="UTF-
8"?><registration><msgType>deregister</
msgType><password>zzzz2x</password><forwardNumber>8888</
forwardNumber></registration>
```

27.3.8 Call Processing Requirements

The MCS routes all calls originating at an MCS PC Client outward to the TDM network, via the Dilithium DTG2000 gateway, towards a mobile operator MSC. As a result, MCS client to MCS client calls “trombone” through an MSC.

The MCS checks the subscriber record of all subscribers placing outbound calls. If their subscriber record indicates that they are in a call barred state, MCS will disallow the call. See figure 8 for an example call flow.

Figure 7 Outbound INVITE Call Flow



When a subscribers make an outgoing call from the MCS PC Client the called number in the request URI should be changed to Called Prefix + called number. The Called Prefix is obtained from the MPS1000 during registration and will be stored with the subscriber data. See the following example of INVITE with the required Called-Prefix.

27.3.9 Outbound SIP INVITE message

REGISTRATION (from MCS to DTG)

The routeing prefix is appended to the subscriber digits in the request URI.

```
INVITE sip:662201@192.168.1.233 SIP/2.0
Via: SIP/2.0/UDP
192.168.1.61:5060;branch=z9hG4bK13774530930000000015.
From: <sip:6112@192.168.1.61>;tag=7e2c8527
To: <sip:2201@192.168.1.233>
Call-ID: 412ADC67-0000009D@vodafone.com
```

```
CSeq: 1 INVITE
Contact: <sip:6112@192.168.1.61>
Supported: 100rel
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 281

v=0
o=Anomymous 1234567890 1234567890 IN IP4 192.168.1.61
s=-
c=IN IP4 192.168.1.61
t=0 0
m=audio 6006 RTP/AVP 8 3 0
a=rtpmap:8 PCMA/8000
a=rtpmap:3 GSM/8000
a=rtpmap:0 PCMU/8000
m=video 6008 RTP/AVP 34 42
a=rtpmap:34 H263/90000
a=rtpmap:42 MPEG4/90000
```

27.3.10 MCS PC Client

The MCS PC Client presents a logon screen checkbox option (in the same area as the current “remember my password” and “auto login” options) to allow the subscriber to select video call forwarding for all calls made to the subscriber’s mobile DN, from that DN to their MCS PC Client. Not selecting the checkbox allows subscribers to use both their mobile phone and their MCS PC client at the same time. Logging into the MCS PC Client doesn’t preclude receipt of calls destine for the mobile subscriber.

27.4 Hardware Requirements or Dependencies

This feature introduces two new hardware dependencies that must be deployed along with the MCS5200 Sip Server:

- Perphonics MPS1000
- Dilithium Networks DTG2000
- RTP Media Portal

The MPS1000 provides the MAP and LDAP interface into the 3G Network for registration services.

The DTG2000 is a Transcoding Media Gateway Controller intended for 3G carrier operators. The DTG 2000 supports a variety of voice and video protocols, and performs signaling interworking and transcoding to end-points such as mobile phones, PDAs, ISDN phones, and IP terminals.

The primary function of the RTP Media Portal is to extend the reach of multimedia services so that they are accessible to obscured endpoints, devices residing behind a firewall, or a Network Address Translation (NAT) and/or Network Address Port Translation (NAPT) device.

See the network diagram in figure 1 to see the interfaces for these hardware dependencies.

27.5 Software Requirements or Dependencies

This feature is part of the MCP 9.0 release, the RTP Media portal software loads will be bundled with this release.

This feature requires a MCS PC Client release that aligns with the MCP 9.0 release.

This feature requires the DTG2000 2.0 release.

This feature requires the MPS 2.1, SIP software release CCSS 6.3, and SS7 software release CCSS 6.3 for the MPS1000 component.

27.6 Limitations and restrictions

One default service package is allowed per domain which will only include wireless gateway (for accessing the DTG gateway), video with h.263 enabled and multiple login restrictions.

Multiple normal domains or wireless domains are allowed but a mix of domain types is not supported.

Only supports voice plus video calls.

The DTG2000 only supports a maximum of 5 calls per gateway.

The subscriber will not receive wireless calls if the subscriber forgets to logout of the MCS PC Client.

The following list of services are not supported:

- Multiple MCS PC Client logins not supported.
- Mid-call codec changes are not supported.

- Call Waiting Not supported
- Any collaborative service like File Transfer, White Board etc.
- Any MAS services like Treatment, branding, no unified communication service including voicemail
- MCS hosted Voicemail service
- Instant Messaging
- Presence
- Network Call Logs
- Call Park
- Call Transfer
- Call Forward to another user
- No Personal Agent access and no services from the personal agent like call routing, privacy.
- No CPL access
- No Privacy control

In short just to reiterate, only basic voice and video calls from the Vf PCC are supported.

27.7 Interactions

This feature does not interact with other call services on the MSC5200. Most of the call services will be disabled at the MCS and will be inaccessible from the PC Client.

27.8 Glossary

Term	Description
CFWD	Call Forward
MSC	Mobile Switching Center
RTP	Real Time Protocol
HLR	Home Location Registrar
MAP	Mobile Application Part
MCS	Multimedia Communication System

28: Functional Description (FN): A00009446

28.1 Feature name and Feature ID

A00009446: M2UA/SCTP Protocol for PVG SS7 backhaul support

28.2 Description

This feature implements the M2UA protocol thus providing the USP with the ability to backhaul MTP3 message, allowing the termination of MTP2 or SAAL on a remote node.

The USP always acts as the client with respect to SCTP associations and use SCTP port 2904. The USP implements the ASP portion of the M2UA while the PVG supports the SG portion.

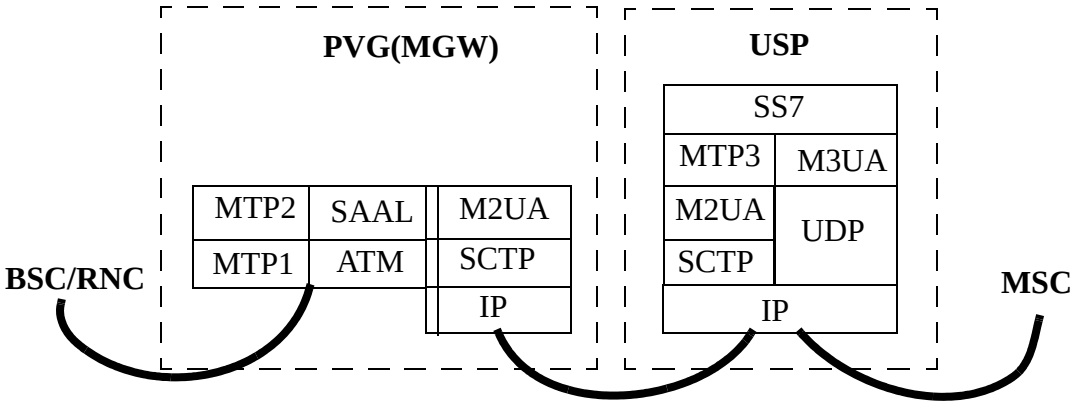
For the requirement, please refer to [2].

28.3 Support M2UA in USP

28.3.1 Functional overview

Broadband SS7 (MTP3b/SAAL/ATM) is the signaling transport used on the UMTS Iu interface, Iu-RANAP from the UTRAN is backhauled to the MSC over IP. The MGW provides the interworking function between bbSS7 and SIGTRAN over IP. The SG/USP accepts the SIGTRAN interface from the MGW and converts it to the proprietary interface required by the MSC.

In addition to the requirement for bbSS7 backhaul, narrowband SS7 (MTP3/ MTP2/MTP1) backhaul over IP is also applicable. Narrowband SS7 is used for control signaling on the GSM A interface and ISUP signaling on the PSTN interfaces. Narrowband SS7 is carried over IP in much the same way as bbSS7. MTP2 is terminated on the MGW and transported over M2UA/SCTP/IP to MSC. The enables the MTP2 physical interface to be geographically separated from the MTP3 layer running on the USP.



28.3.2 Function provided by the M2UA Adaptation Layer

28.3.2.1 Mapping

Interface Identifier (IID) is used to tie the SCTP association/stream with the SS7 physical link in the SGP (PVG/MGW). When an ASP (USP) sends an ASP Active message for a particular IID, the SGP will try to provide the Signalling Link Terminal service to an SS7 link tied by the IID.

28.3.2.2 Support for the management of SCTP associations

The M2UA layer may be instructed by local management (LM) to establish an SCTP association to a peer M2UA node. This can be achieved using the MSCTP_ESTABLISH primitive to request, indicate and confirm the etablishment of an SCTP association with a peer M2UA node.

The M2UA layer MAY also need to inform local management of the status of the underlying SCTP associations using the M-SCTP_STATUS request and the indication primitive.

28.3.2.3 SCTP Stream Management

M2UA requires a stream for each ss7 link provisioned. The M2UA layer residing on a card can handle maximum 32 ss7 links. Each association (determined by far-endpoint ip address, local and remote port) can have up to

8 traffic streams and one more stream for management - stream '0' is reserved for ASP Management (ASPM) messages.

The SS7IPLink running M2UA can handle approx 1792 messages/sec at 80% capacity or 2300 messages/sec in overload regardless of message size. The bandwidth of 1792 messages/sec per card is shared among the M2UA links provisioned on that card.

28.3.3 M2UA Message Structure

28.3.3.1 Common Message Header

Table 1 Common Message Header for M2UA

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Version	Spare	Message Class	Message Type
Message Length			

Table 2: Message Class List

Value	Description
0	Management (MGMT) Message
3	ASP State Maintenance (ASPSM) Messages
4	ASP Traffic Maintenance (ASPTM) Messages
6	MTP2 User Adaptation (MAUP) Messages

Table 3: Message Type List

Message Class	Value	Description	Notes
0	0	Error (ERR)	
	1	Notify (NTFY)	

Message Class	Value	Description	Notes
3	1	ASP Up (UP)	
	2	ASP Down (DOWN)	
	3	Heartbeat (BEAT)	never send BEAT
	4	ASP Up Ack (UP ACK)	
	5	ASP Down Ack (DOWN ACK)	
	6	Heartbeat Ack (BEAT ACK)	
4	1	ASP Active (ACTIVE)	
	2	ASP Inactive (INACTIVE)	
	3	ASP Active Ack (ACTIVE ACK)	
	4	ASP Inactive Ack (INACTIVE ACK)	
6	1	Data	
	2	Establish Request	
	3	Establish Confirm	
	4	Release Request	
	5	Release Confirm	
	6	Release Indication	
	7	State Request	
	8	State Confirm	
	9	State Indication	
	10	Data Retrieval Request	
	11	Data Retrieval Confirm	
	12	Data Retrieval Indication	
	13	Data Retrieval Complete Indication	
	14	Congestion Indication	
	15	Data Acknowledge	

28.3.3.2 M2UA Message Header

For MAUP messages, there is a M2UA specific message header immediately follow the common message header. The format like the below.

Table 4 MAUP Specific Message Header

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x01)		Length (=8)	
Interface Identifier			

28.3.3.3 Parameters

M2UA messages consist of a Common Header followed by zero or more variable-length parameters, as defined by the message type. The variable-length parameters contained in a message are defined in a Tag-Length-Value format.

The common parameter tags (can be used by all User Adaptation layers) is supported as below.

Table 5: Common Parameters Tags

Value	Description	Notes
1	Interface Identifier (Integer)	
3	Interface Identifier (Text)	Not supported
4	Info String	Not supported
7	Diagnostic Information	Not supported
8	Interface Identifier (Integer Range)	Not supported
9	Heartbeat Data	
11	Traffic Mode Type	
12	Error Code	
13	Status Type/Information	
17	ASP Identifier	

Value	Description	Notes
19	Correlation Id	Not supported

Besides the common parameters, there are M2UA specific parameters.

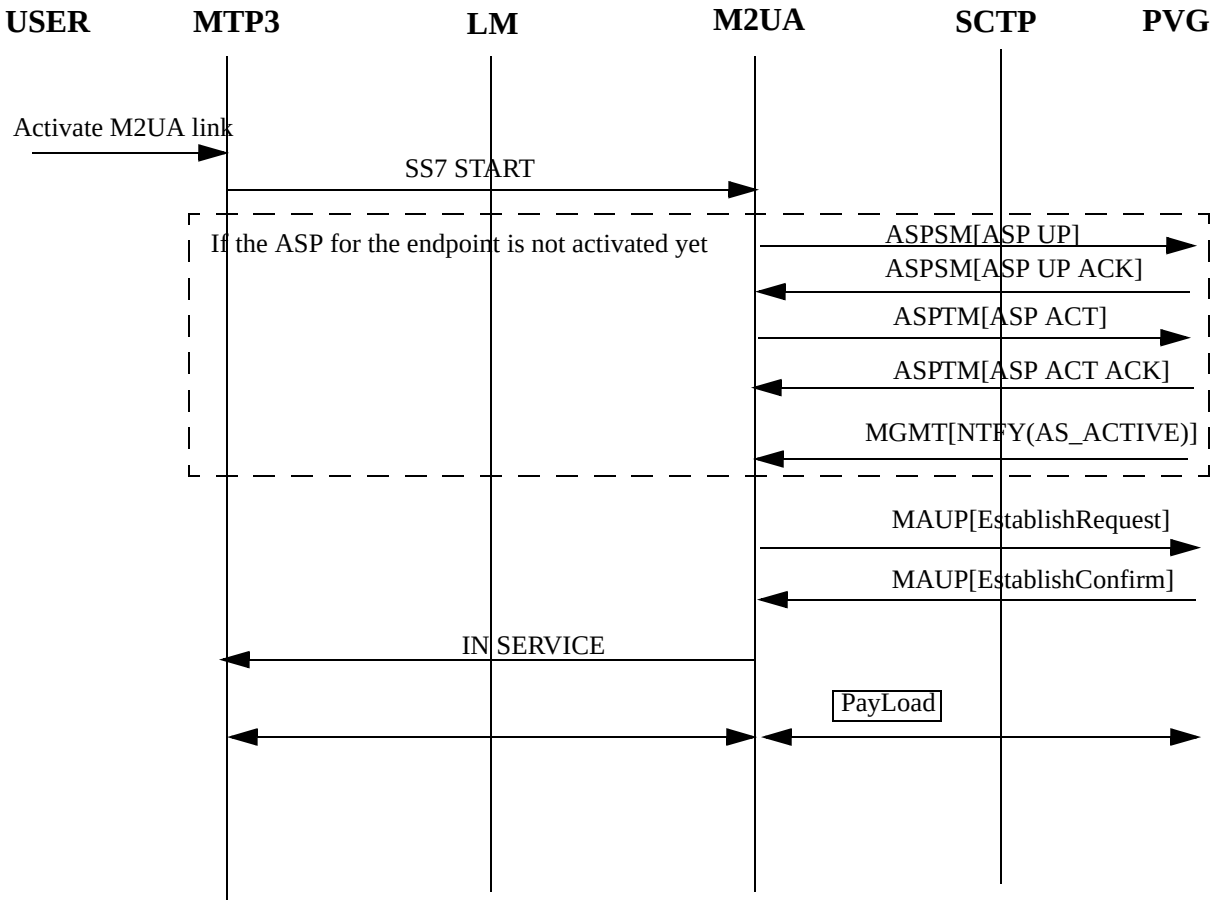
Table 6: M2UA Specific Parameters Tags

Value	Description	Notes
768	Protocol Data 1	
769	Protocol Data 2 (TTC)	Not supported
770	State Request	
771	State Event	
772	Congestion Status	
773	Discard Status	Not supported
774	Action	
775	Sequence Number	
776	Retrieval Result	
777	Link Key	Not supported
778	Local-LK-Identifier	Not supported

28.3.4 RFC M2UA procedures supported by USP

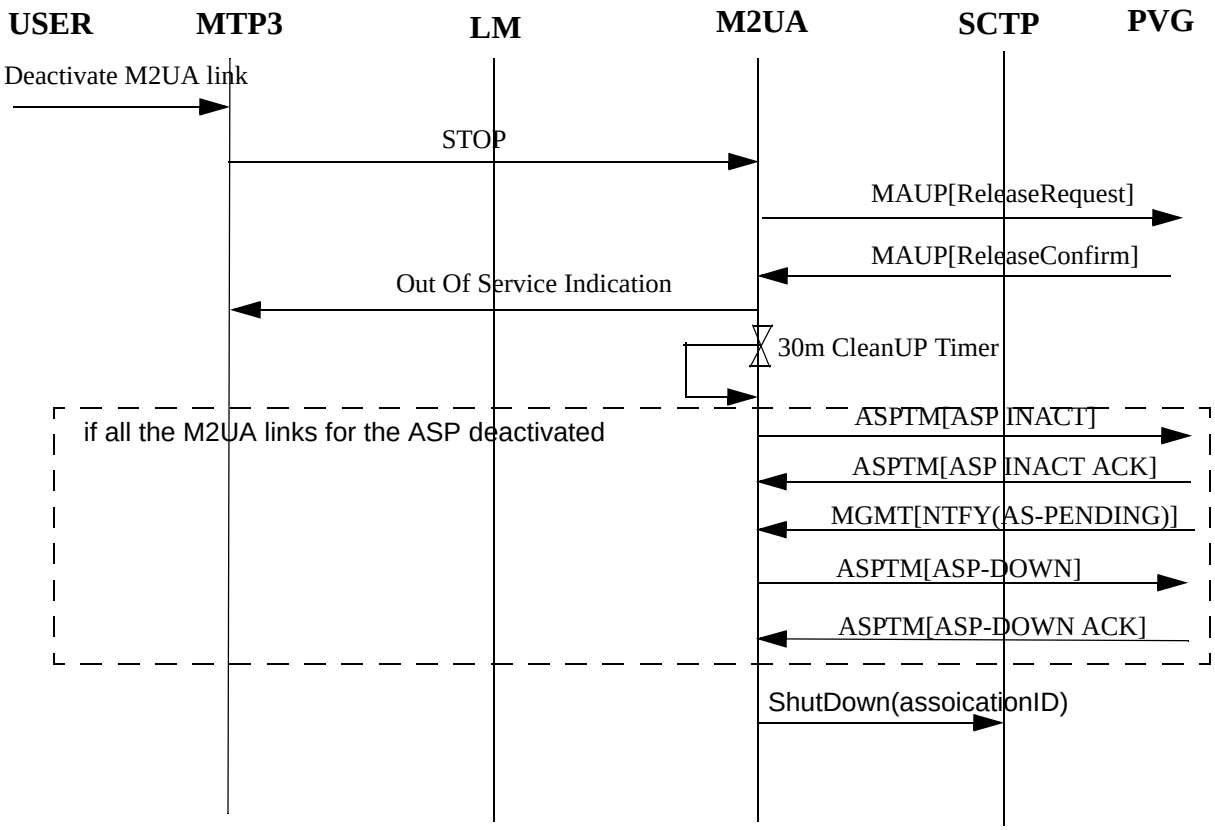
28.3.4.1 Activate M2UA link

Figure 7: Activation of M2UA link and ss7 link alignment



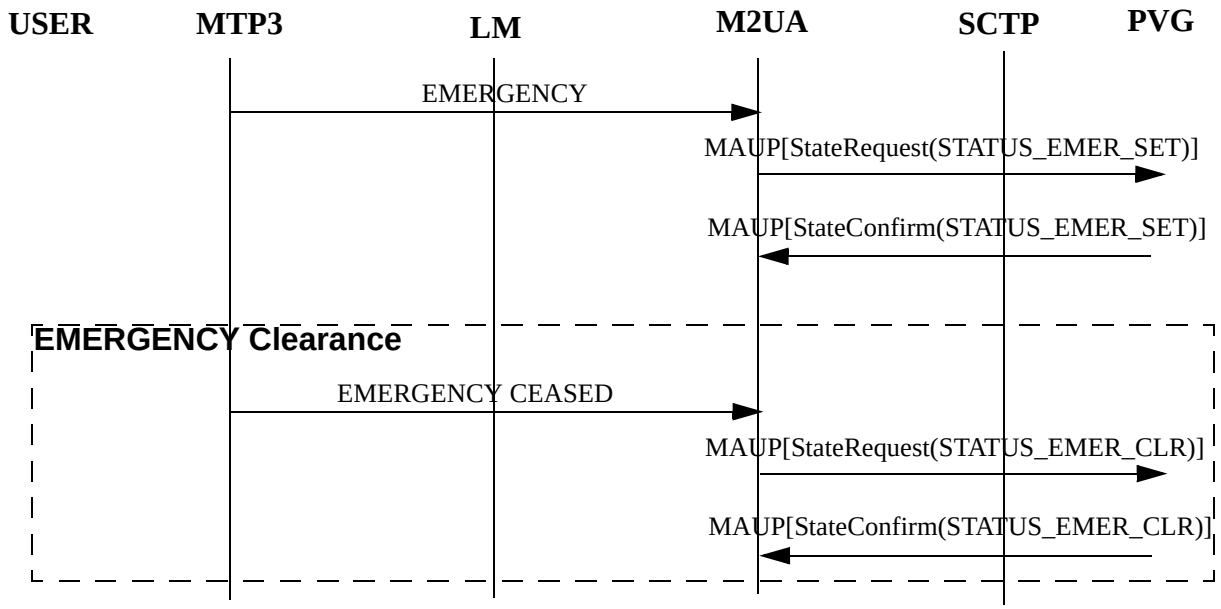
28.3.4.2 Deactivate M2UA link

Figure 8: Deactivation of M2UA link



28.3.4.3 Emergency and Emergency Clearance

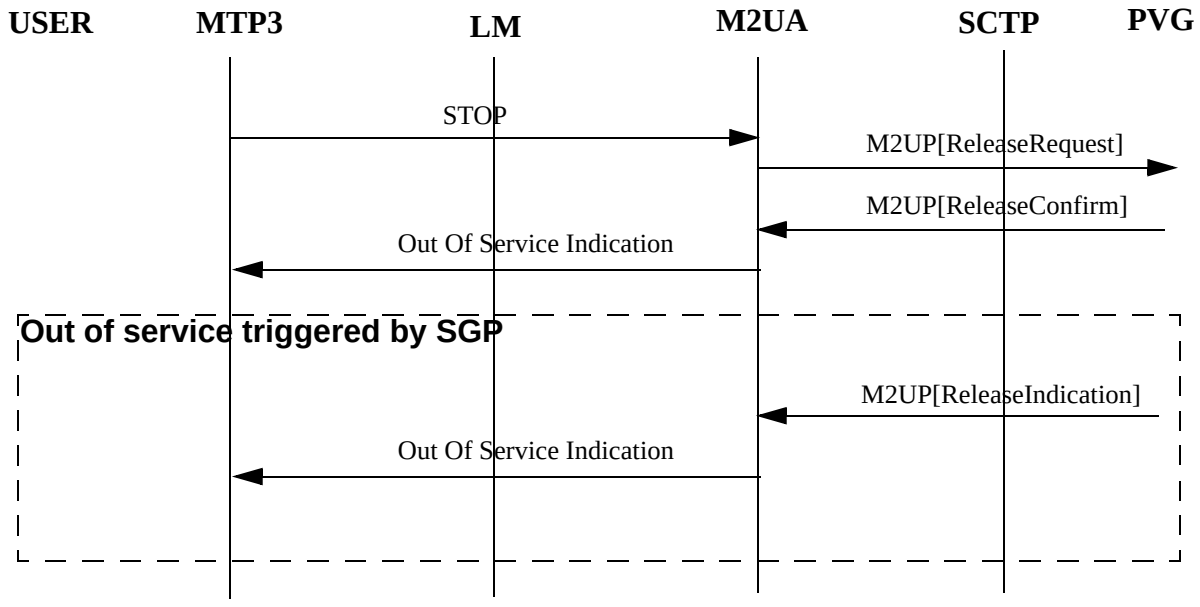
Figure 9: Emergency and Emergency Clearance



28.3.4.4 SS7 Link Deactivate

Refer to RFC3331 5.3.2

Figure 10: SS7 Link Deactivate

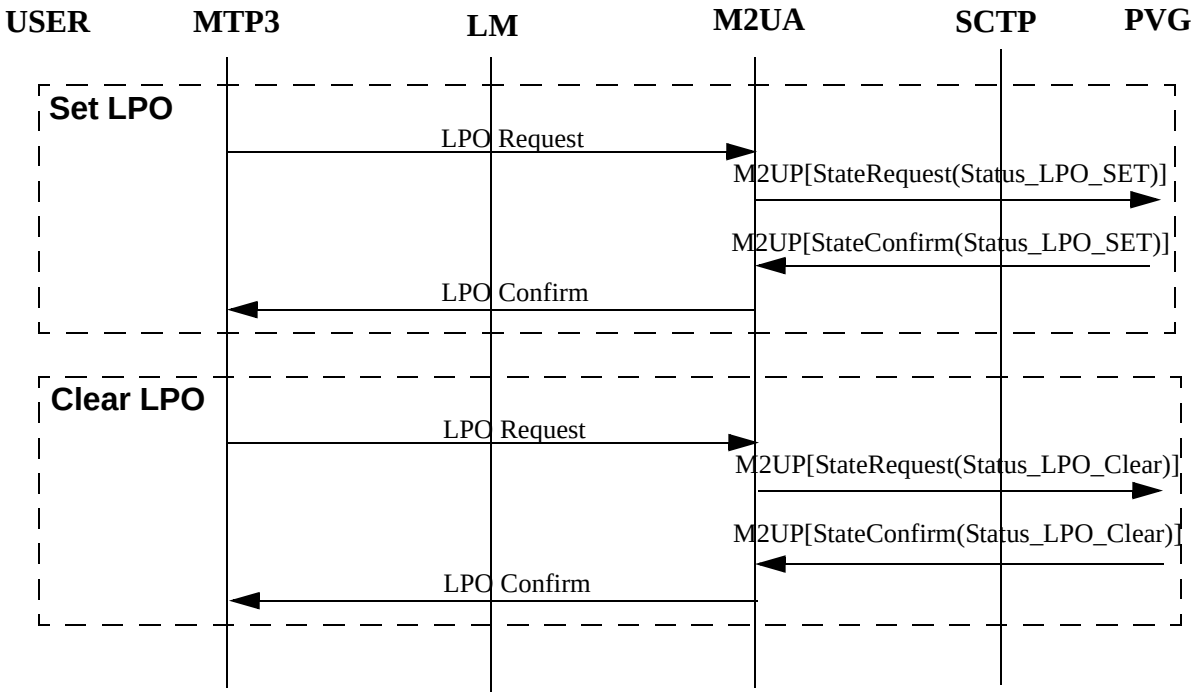


STOP is sent by L3 SLM (Signalling Link Management), if it thinks the l2 link is really needed to be stopped in some cases including some failure ones.

28.3.4.5 Set and Clear Local Processor Outrage

Refer to RFC3331 5.3.3

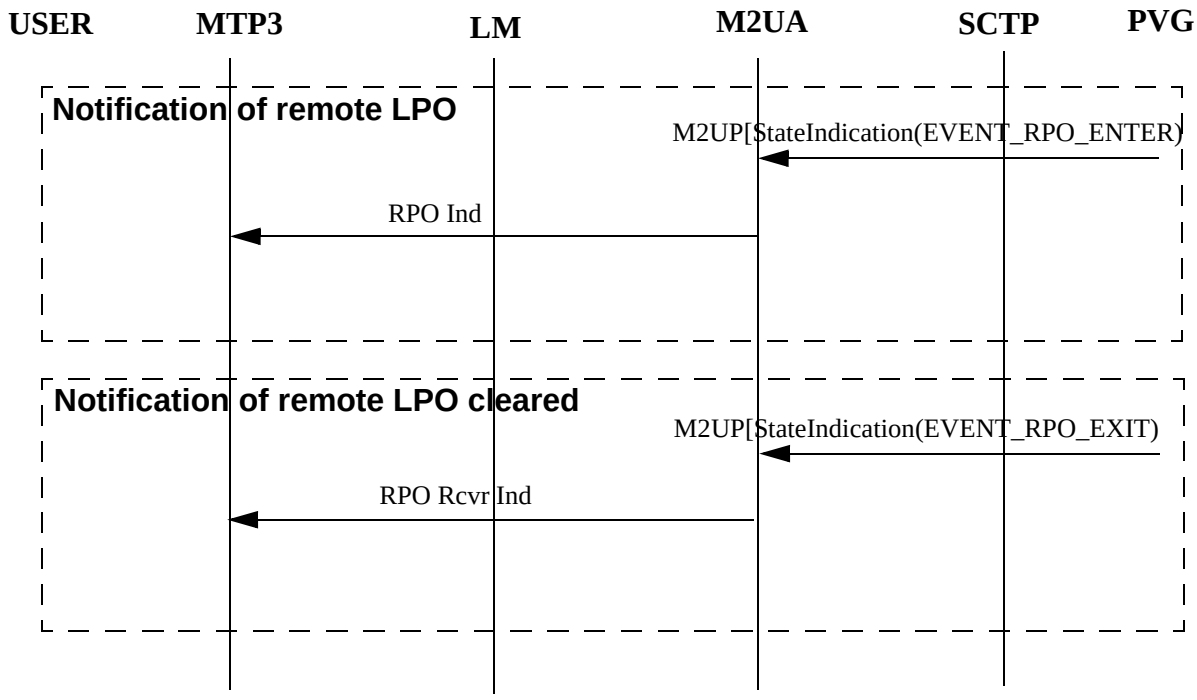
Figure 11: Set and Clear Local Processor Outrage



28.3.4.6 Remote processor outrage

Refer to RFC3331 5.3.4

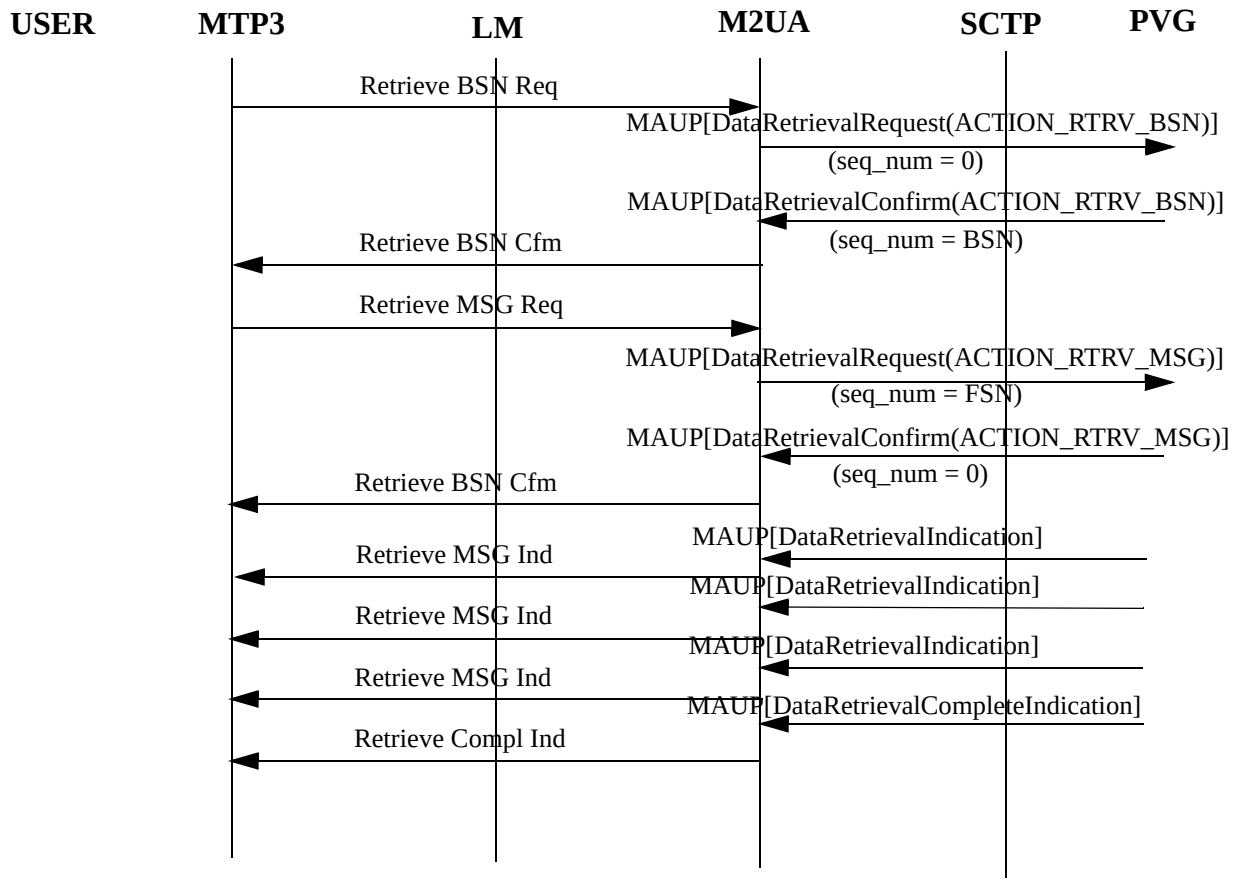
Figure 12: Remote Processor Outrage



28.3.4.7 SS7 Link Changeover

Refer to RFC3331 5.3.6.

Figure 13: SS7 Link Changeover

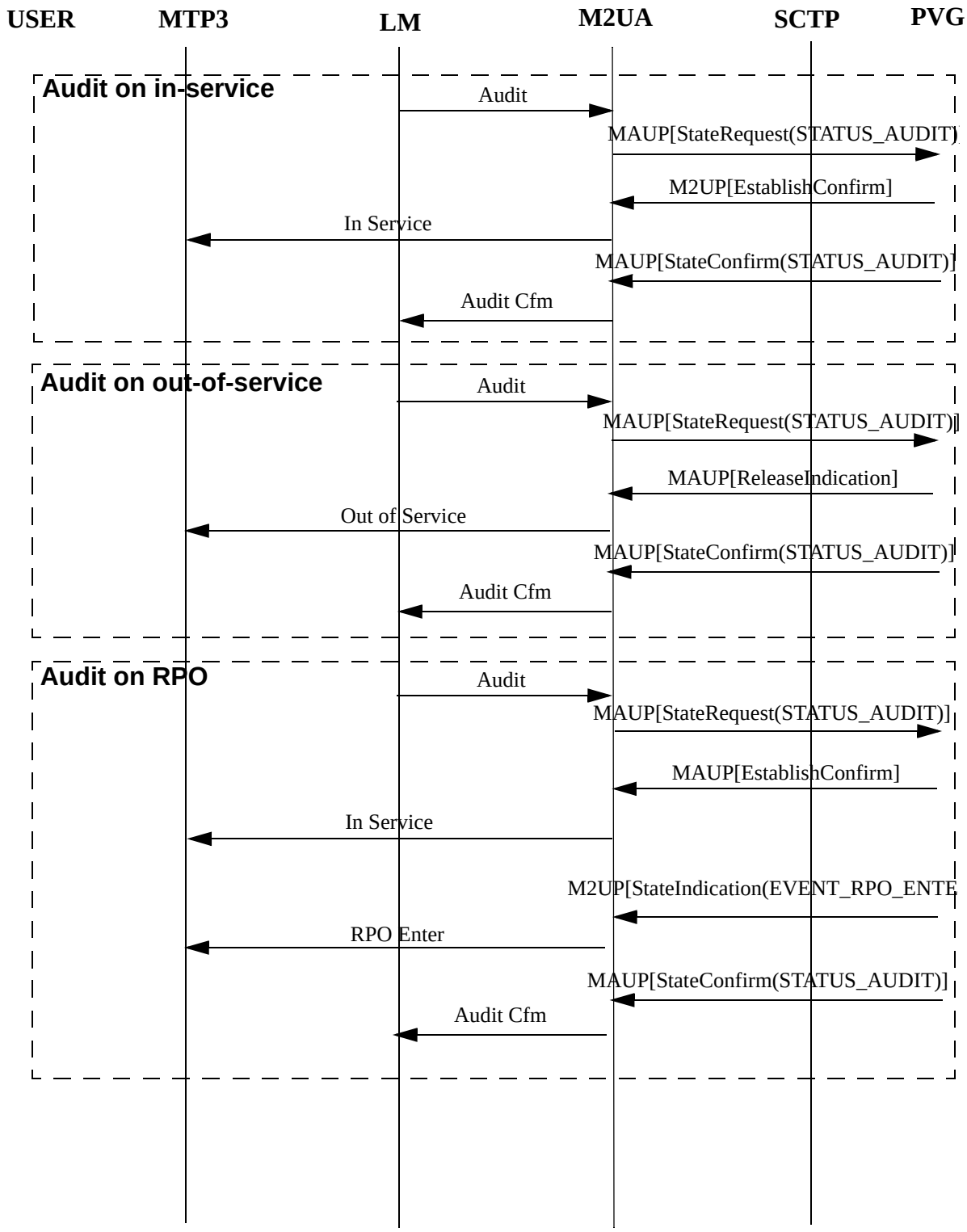


28.3.4.8 Auditing of SS7 link state

Refer to RFC3331 5.3.8

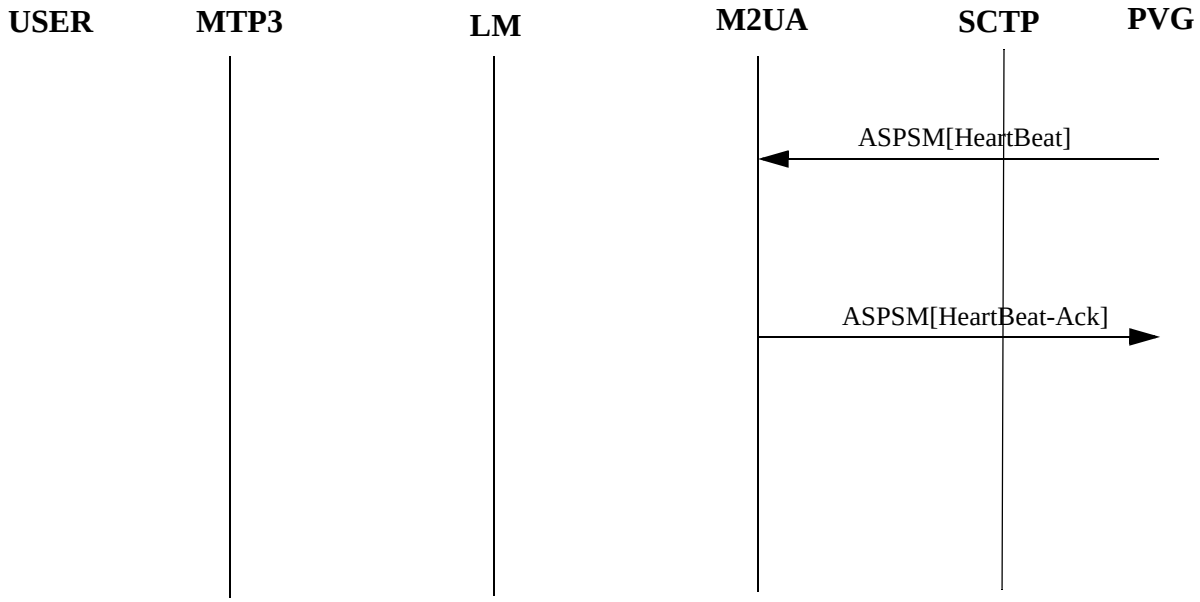
Audit on in-service, out-of-service and RPO are supported.

Figure 14: Auditing of SS7 link State



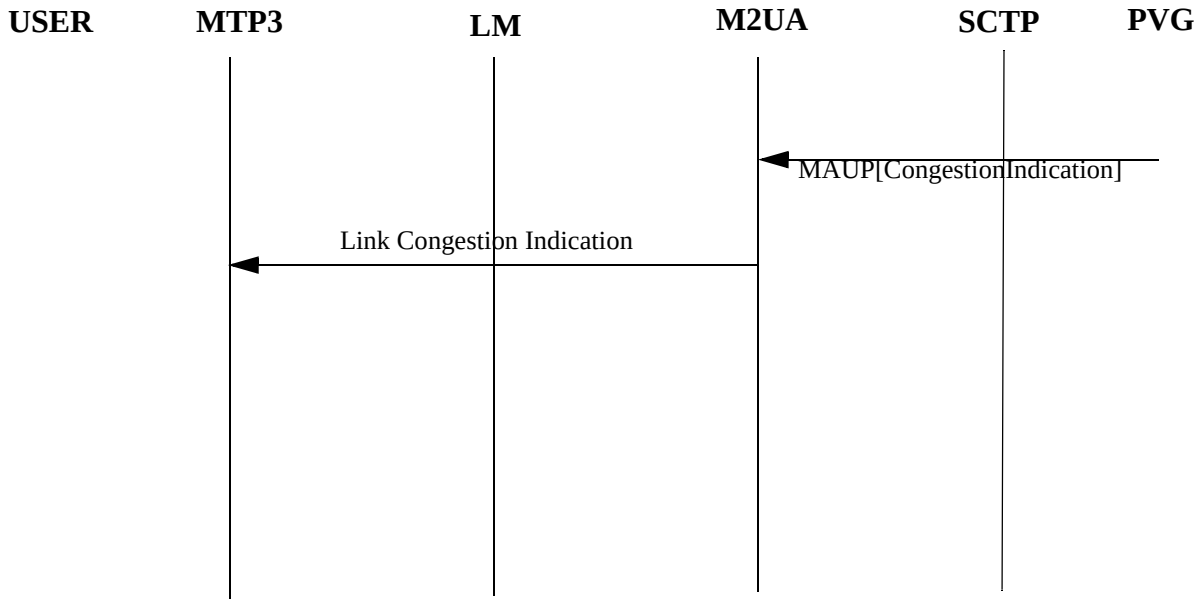
28.3.4.9 Heartbeat (and Ack)

Figure 15: BEAT and BEAT-ACK



28.3.4.10 Notification of SS7 link Congestion

Figure 16: Congestion Indication



28.3.5 Messages Contents

28.3.5.1 MAUP - Data (PDU of MTP3)

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x300)		Length (=8)	
Protocol Data			
Tag (0x13)		Length (=8)	
Correlation ID (optional)			

The purpose of Correlation ID is to permit the newly active ASP to synchronize its processing of the traffic in each ordered stream with other ASPs in the broadcast group. It’s optional and not supported by the feature.

TTC protocol data is not supported.

28.3.5.2 MAUP - Establish (Request, Confirm)

No specific parameters except for the Common Message Header.

28.3.5.3 MAUP - Release (Request, Confirm, Indication)

No specific parameters except for the Common Message Header.

28.3.5.4 MAUP - State (Request, Confirm)

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x302)		Length (=8)	
State			

State is Mandatory IE, the valid values for it are shown below.

Value	Define	Note
0x0	STATUS_LPO_SET	
0x1	STATUS_LPO_CLEAR	
0x2	STATUS_EMER_SET	
0x3	STATUS_EMER_CLEAR	
0x4	STATUS_FLUSH_BUFFERS	

0x5	STATUS_CONTINUE	
0x6	STATUS_CLEAR_RTB	
0x7	STATUS_AUDIT	
0x8	STATUS_CONG_CLEAR	
0x9	STATUS_CONG_ACCEPT	
0xa	STATUS_CONG_DISCARD	

28.3.5.5 MAUP - State Indication

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x302)		Length (=8)	
Event			

Event is Mandatory IE, the valid values for it are shown below.

Value	Define	Note
0x1	EVENT_RPO_ENTER	
0x2	EVENT_RPO_EXIT	
0x3	EVENT_LPO_ENTER	
0x4	EVENT_LPO_EXIT	

28.3.5.6 MAUP - Retrieval Request

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x306)		Length (=8)	
Action (Mandatory)			
Tag (0x307)		Length (=8)	
Sequence Number (Optional)			

The valid values for Action are shown below.

Value	Define	Note
0x1	ACTION_RTRV_BSN	
0x2	ACTION_RTRV_MSGS	

28.3.5.7 MAUP - Retrieval Confirm

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x306)		Length (=8)	
Action (Mandatory)			
Tag (0x308)		Length (=8)	
Result (Mandatory)			
Tag (0x307)		Length (=8)	
Sequence Number (Optional)			

The valid values for Result are shown below.

Value	Define	Note
0x1	RESULT_SUCCESS	
0x2	RESULT_FAILURE	

28.3.5.8 MAUP - Retrieve Indication

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x300)		Length (=8)	
Protocol Data			

The Retrieval Indication message is sent by the Signalling Gateway with a PDU from the transmit or retransmit queue. The Retrieval Indication message does not contain the Action or Sequence Number fields, just a MTP3 Protocol Data Unit (PDU) from the transmit or retransmit queue.

28.3.5.9 MAUP - Retrieve Complete Indication

The MTP2 Retrieval Complete Indication message is exactly the same as the MTP2 Retrieval Indication message except that it also indicates that retrieval is complete. In addition, it MAY contain a PDU (which MUST be the last PDU) from the transmit or retransmit queue.

28.3.5.10 MAUP - Congestion Indication

The Congestion Indication message can be sent from a Signalling Gateway Process to an ASP to indicate the congestion status and discard status of a SS7 link.

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x304)		Length (=8)	
Congestion Status (Mandatory)			
Tag (0x308)		Length (=8)	
Discard Status (Optional)			

For the Congestion Status, there are the following values can be selected.

Value	Define	Note
0x0	LEVEL_NONE	
0x1	LEVEL_1	Not supported
0x2	LEVEL_2	Not supported
0x3	LEVEL_3	

28.3.5.11 ASPM - ASP UP

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x11)		Length (=8)	
ASP Idenfifier (optional)			
Tag (0x4)		Length (=8)	
Info String (optional)			

The optional ASP Identifier parameter would contain a unique value that is locally significant among the ASPs that support an AS. The SGP should save the ASP Identifier to be used, if necessary, with the Notify message.

28.3.5.12 ASPM - ASP UP Ack

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x4)		Length (=8)	
Info String (optional)			

28.3.5.13 ASPM - ASP Down

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x4)		Length (=8)	
Info String (optional)			

28.3.5.14 ASPM - ASP Down Ack

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0x4)		Length (=8)	
Info String (optional)			

28.3.5.15 ASPM - ASP Active (Ack)

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0xb)		Length (=8)	
Traffic Mode Type (Optional)			
Tag (0x1, 0x8)		Length (=8)	
Interface Identifier(s) (Optional)			
Interface Identifier Start1			
Interface Identifier End1			
.....			
Interface Identifier StartN			
Interface Identifier EndN			
Tag (0x4)		Length (=8)	
Info String (Optional)			

28.3.5.16 ASPM - ASP Inactive (Ack)

The same format as ASP Active.

28.3.5.17 MGMT - ERR

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0xc)		Length (=8)	
Error Code (Mandatory)			
Tag (0x1,0x8)		Length (=8)	
Interface Identifier(s) (optional)			
Tag (0x7)		Length (=8)	
Diagnostic Information (optional)			

The Error (ERR) message is used to notify a peer of an error event associated with an incoming message. An Error message MUST not be generated in response to other Error messages.

The valid values for Error Code are shown below.

Value	Define	Note
0x1	Invalid Version	
0x2	Invalid Interface Identifier	
0x3	Unsupported Message Class	
0x4	Unsupported Message Type	
0x5	Unsupported Traffic Handling Mode	
0x6	Unexpected Message	
0x7	Protocol Error	
0x8	Unsupported Interface Identifier Type	
0x9	Invalid Stream Identifier	
0xa	Not Used in M2UA	
0xb	Not Used in M2UA	
0xc	Not Used in M2UA	
0xd	Refused - Management Blocking	
0xe	ASP Identifier Required	
0xf	Invalid ASP Identifier	

0x10	ASP Active for Interface Identifier(s)	
0x11	Invalid Parameter Value	
0x12	Parameter Field Error	
0x13	Unexpected Parameter	
0x14	Not Used in M2UA	
0x15	Not Used in M2UA	
0x16	Missing Parameter	

28.3.5.18 MGMT - NTFY

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Tag (0xd)		Length (=8)	
Status Type (Mandatory)		Status info (Mandatory)	
Tag (0x11)		Length (=8)	
ASP Identifier (Optional)			
Tag (0x1,0x8)		Length (=8)	
Interface Identifier(s) (optional)			
Tag (0x4)		Length (=8)	
Info String (optional)			

The Error (ERR) message is used to notify a peer of an error event associated with an incoming message. An Error message MUST not be generated in response to other Error messages.

The valid values for Error Code are shown below.

Value	Define	Note
0x1	Invalid Version	
0x2	Invalid Interface Identifier	
0x3	Unsupported Message Class	
0x4	Unsupported Message Type	
0x5	Unsupported Traffic Handling Mode	
0x6	Unexpected Message	
0x7	Protocol Error	

0x8	Unsupported Interface Identifier Type	
0x9	Invalid Stream Identifier	
0xa	Not Used in M2UA	
0xb	Not Used in M2UA	
0xc	Not Used in M2UA	
0xd	Refused - Management Blocking	
0xe	ASP Identifier Required	
0xf	Invalid ASP Identifier	
0x10	ASP Active for Interface Identifier(s)	
0x11	Invalid Parameter Value	
0x12	Parameter Field Error	
0x13	Unexpected Parameter	
0x14	Not Used in M2UA	
0x15	Not Used in M2UA	
0x16	Missing Parameter	

28.4 LOG

Log group M2UA_GROUP is defined for the M2UA.

Log Name	Type	Description
M2UA_SWEER	LOG_SWEER	generated when software error are detected in M2UA
M2UA_INFO	LOG_INFO	generated when an important event happened in M2UA that needs to be shown to the user

28.5 OM

N/A

28.6 Provisioning

28.6.1 Provisioning - CLI interface

CMD: mtp link add <linkset-name> <slc> ss7iplink <shelf> <slot> <periodic-slt-option> <dest-ipaddr> <local-port> <remote-port> { m2ua client <sctp-

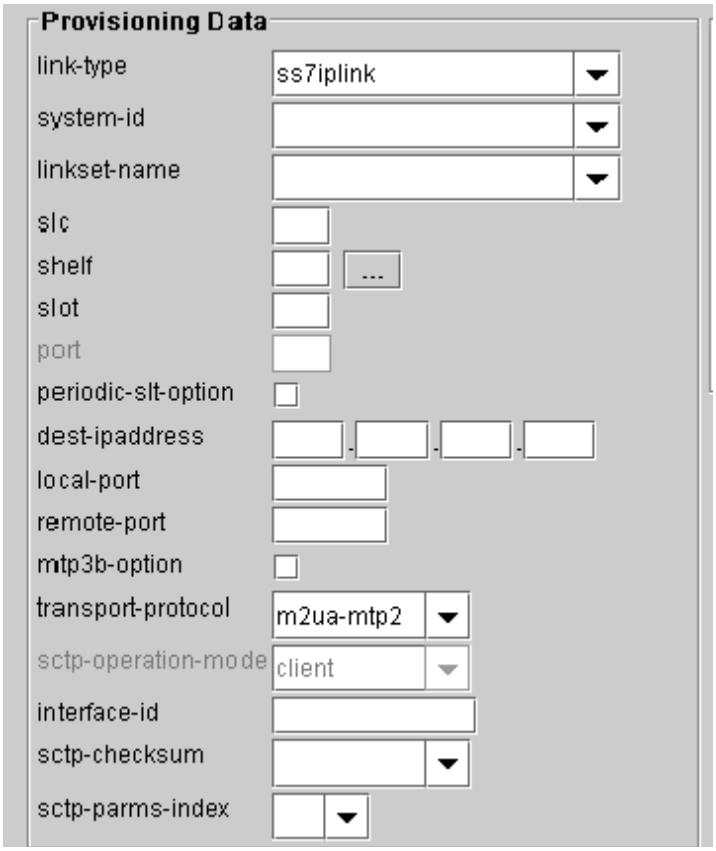
checksum> <sctp-parm-index> | m2ua <interface-id> <sctp-checksum> <sctp-parm-index> }

CMD: mtp link mod <linkset-name> <slc> ss7iplink interface-id <interface-id>

CMD: mtp link mod <linkset-name> <slc> ss7iplink transport-protocol { m2ua client <sctp-checksum> | m2ua <interface-id> <sctp-checksum> }

CMD: mtp link show <linkset-name> <slc>

28.6.2 GUI



Some fileds are needed to be noticed when protocol M2UA is selected.

Field Name	Value	Description
transport-protocol	m2ua-mtp2/ m2ua-saal	select different value depending on the far-end l2 type in the PVG/MGC
local-port	2904	2904 is dedicated for M2UA

remote-port	2904	2904 is dedicated for M2UA

28.7 Hardware Requirements or Dependencies

N/A

28.8 Software Requirements or Dependencies

N/A

28.9 Limitations and restrictions

1. USP can only be configured as SCTP Client

2. The M2UA layer supports a n+k redundancy model(active-standby, load sharing, broadcast) where n is the minimum number of redundant ASPs required to handle traffic and k ASPs are available to take over for a failed or unavailable ASP. A simplex 1+0 model is also supported as a subset, with no ASP redundancy is supported by the feature. (ASP identifier <-> number of ASP, link(set) <-> ASP), (send it PVG team)

3. Registration procedure is not supported by the feature.

28.10 Interactions

N/A

28.11 Glossary

Term	Description
AS	A logical entity serving a specific application instance
ASP	A process instance of an Application Server
ASPSM	ASP State Maintenance
ASPTM	ASP Traffic Maintenance
M3UA	Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) -User Adaptation Layer
SCTP	Stream Control Transmission Protocol
SCTP	Stream Control Transmission Protocol
SG	Signaling Gateway

28.12 Reference

1. RFC3331 Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Adaptation Layer

2. Feature Requirement: POR #153
http://livelink.us.nortel.com/livelink/
livelink.exe?func=ll&objId=7218991&objAction=browse

29: Functional Description (FN): A00009489

29.1 Feature name and Feature ID

A00009489 - CHT: Call Waiting Enhancement

29.2 Description

This ISN09 activity enhances the CEPT Call Waiting for CS2Kc IP platform. Only IBN lines and TW ISUP, TW PRI are supported.

The feature is to enhance the existing CEPT Call Waiting in the aspects as below:

- To support generating the second Call Waiting Tone B for both parties during Call Waiting scenario.
- To support answer the call and toggle between held parties by hook-flash only, no need to enter any digit right after hook-flash.

29.2.1 Call Waiting Scenario

The feature supports the following scenario.

Assume that subscriber A with ICWT option is talking with subscriber B, when a new call to subscriber A comes from subscriber C. The call waiting operation with the implementation of the feature shall be as follows:

a) Subscriber C shall receive a ring back tone.

b) Subscriber A shall receive Call Waiting Tone A.

After 2 seconds (which can be datafilled in CWT_TONE_CYCLE_TIME tuple of table OFCVAR), Call Waiting Tone B shall then be sent periodically to both talking subscribers A and B until A answers the new call.

c) Subscriber A may answer the new call by flashing the cradle hook of his telephone set; the previous talking path connection is still held.

d) Subscriber B shall receive a SILENCE Tone if he continues to hold his telephone off hook.

e) Flashing action by turns shall cause the change over of talking path to subscriber B or subscriber C as desired.

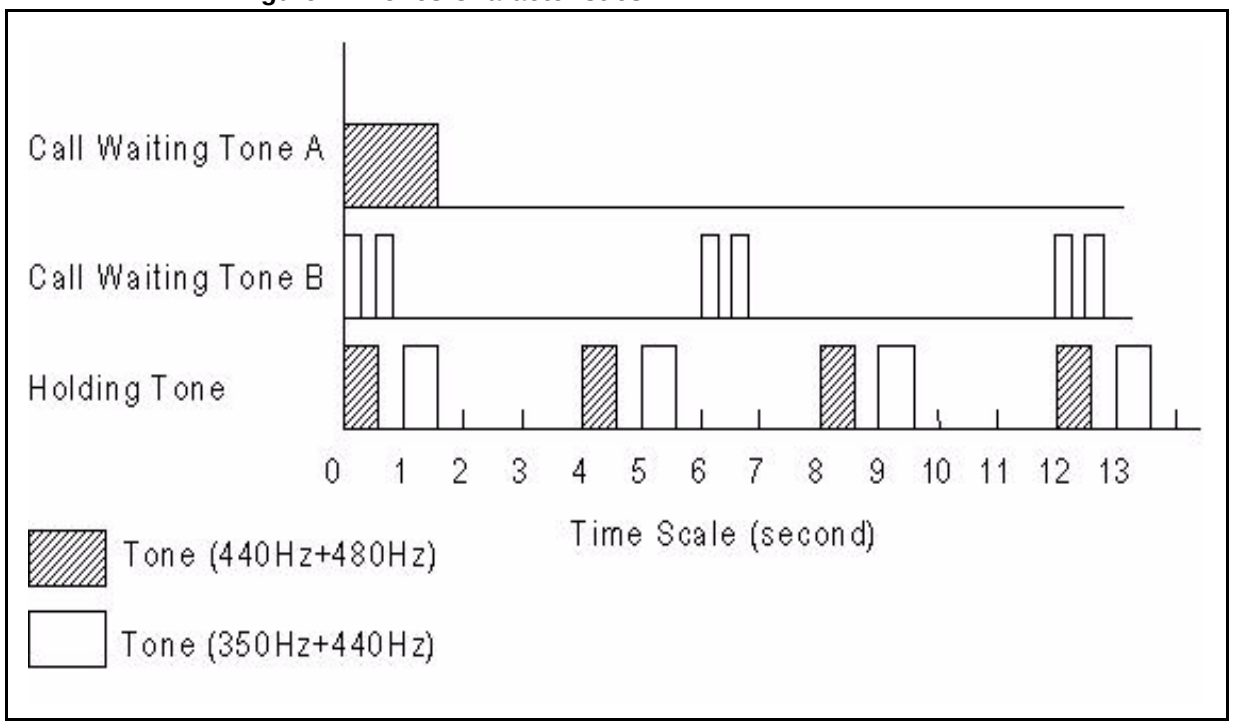
f) When subscriber B or C hangs up, another terminating call shall be able to reach subscriber A, and the call waiting action proceeds as before.

29.2.2 TONES CHARACTERISTICS

Table 17: Tones Characteristics

Tones	Frequency	Level(dBm0)	Cadence ON-1	Cadence OFF-1	Cadence ON-2	Cadence OFF-2	Duration
Call Waiting Tone A	440+480	-13	One pulse ON				1.5 sec
Call Waiting Tone B	350+440	-13	0.25 sec	0.25 sec	0.25 sec	5.25 sec	INFI-NITE

Figure 1 Tones Characteristics



29.2.3 Example of ISERVOPT table datafill

When ICWT_2PTY_TONE_B is changed from ‘N’ to ‘Y’, a warning message will be displayed: ‘* WARNNING * - If icwt_2pty_tone_b is datafilled YES, field icwt_ignore_waiting_tmo will be disabled.’.

When ICWT_DFLT_RCODE is changed from ‘N’ to ‘Y’, a warning message will be displayed: ‘ If icwt_dflt_rcode is datafilled YES, only TOGGLE ACTION is supported, and Rcode tuple with toggle action in table ISERVOPT should be datafilled.’.

Figure 2 The view of ICWT Tuple in ISERVOPT Table

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>icwt
OPTION:
>icwt
ICWT_IGNORE_WAITING_TMO:
>11
ICWT_ANN_ACTIVE:
>y
ICWT_TMO_ANN_ACTIVE:
>y
ICWT_TIMEOUT_TREATMENT:
>BUSY
ICWT_2PTY_TONE_B:
>y
ICWT_DFLT_RCODE:
>y
* WARNNING * -
If icwt_2pty_tone_b is datafilled YES,
field icwt_ignore_waiting_tmo will be disabled.
* WARNNING * -
If icwt_dflt_rcode is datafilled YES,
only TOGGLE ACTION is supported, and Rcode tuple with
toggle action in table ISERVOPT should be datafilled.
TUPLE TO BE ADDED:
                ICWT
                                        ICWT 11 Y Y BUSY Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
...
```

29.3 Hardware Requirements or Dependencies

Table 18: Signals should be supported in Media Gateways

	Call Waiting Tone A	Call Waiting Tone B
MGCP	L/wt1	L/wt2

	Call Waiting Tone A	Call Waiting Tone B
Megaco/H.248	alert/cw{pattern=1}	alert/cw{pattern=2}

VG201, MG1K and PVG should support Taiwan Tonesets including the signal above. While Call Waiting Tone B is OFF, speech path should NOT be killed by VG201, MG1K and PVG.

29.4 Software Requirements or Dependencies

This feature does not affect the provision method of CEPT ICWT. It takes effect when the subscriber is using CEPT ICWT and it is controlled by following datafill:

- In table OFCVAR, tuple CWT_TONE_CYCLE_TIME should be set to 2, which is the inteval between the begining of CWT tone A and CWT tone B.

- In table ISERVOPT, tuple ICWT, the ICWT_2PTY_TONE_B field. If datafilled ‘Y’, Call Waiting Tone B will be applied to both talking side infinitely after applying Call Waiting Tone A to the controller and field icwt_ignore_waiting_tmo will be disabled.

- In table ISERVOPT, tuple ICWT, the ICWT_DFLT_RCODE field. If datafilled ‘Y’, R-code is not needed while toggling between held parties. The RCODE tuple in table ISERVOPT must exist and the ACTION “TOGGLE” must be datafilled. If not , a nack tone will be given when flash and after the tone is over, the call will revert to the former state before flash.

Please refer to the software requirements or dependencies part of References b,c for more details.

29.5 Limitations and restrictions

Please refer to References b,c.

29.6 Interactions

Please refer to References b,c.

29.7 Glossary

Term	Description
CEPT	European Conference of Postal and Telecommunications Administrations
ICWT	Line Option on CEPT Call Waiting
Megaco/H.248	ITU-T and IETF Media Gateway Control Protocol
MGCP	Media Gateway Control Protocol
VG201	4 Port Intergated Access Device
MG1K	Media Gateway MG1000
PVG	Packet Voice Gateway
I3WC	International Three Wall Calling

29.8 Reference

a. SFR 2991 - CHT Call Waiting Tone

b. A59019288 - CEPT Call Waiting

c. A59019281 - CEPT I3WC and ICT

29.9 Appendix: Q01097743 FN (I3WC Default Rcode)

CR.Q01097743: ISN09, ICWT&I3WC Enhancement, I3WC default RCODE.

The CR is to enhance the existing CEPT International Three Way Calling in the aspects as below:

- To support using hook-flash only without dialing RCODE in I3WC scenario.

29.9.1 I3WC Scenario

This feature supports following scenario:

Assume that line A has the I3WC feature. A is talking with B, and then A flashes to calls C to make a three way call. The scenario with the implementation of this feature will be described as follows:

a) If C is busy, A will hear a busy tone. Then A can flash and resume the two parties connect with B.

b) If C is not busy and answers the call from A, the active parties are A and C and B is the holding party. If A flashes, **without dialing RCODE**, a three way conference is established. A is the controller.

c) In 3-way conference state, if A flashes, **without dialing RCODE**, party C is disconnected, A and B are still in talking mode.

d) In 3-way conference state, if B or C goes on hook, then A will be connected to the remaining 3wc party. That means if B disconnect, A will be connected to C and A can make another conference call by hook-flash.

e) In 3-way conference state, if the controller A goes on hook, then the conference call is over. i.e. all calls drop.

To implement the above requirement needs supporting I3WC without dialing RCODE.

29.9.2 Support I3WC Without Dialing RCODE

A new tuple I3WC with field I3WC_DFLT_RCODE(Y/N) will be defined in table ISERVOPT. When the I3WC_DFLT_RCODE is ‘N’, the existing behavior will be used. When the I3WC_DFLT_RCODE is set to ‘Y’, the scenario described above will be used. The default value for the field is ‘N’.

When I3WC_DFLT_RCODE is changed from ‘N’ to ‘Y’, two warning messages will be displayed: ‘RCODE tuple in table ISERVOPT must exist and the ACTION CON_3WC and DISC_ACT must be datafilled.’ and ‘Default RCODE only supports CON_3WC and DISC_ACT actions.’

Figure 3 :Example of ISERVOPT table datafill

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>I3WC
OPTION:
>I3WC
I3WC_DFLT_RCODE:
>y
TUPLE TO BE ADDED:
I3WC I3WC Y

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
* WARNNING * - RCODE tuple in table ISERVOPT must exist and the
ACTION CON_3WC and DISC_ACT must be datafilled.
* WARNNING * - Default RCODE only supports CON_3WC and
DISC_ACT actions.
TUPLE ADDED
```

Notes: the interaction between I3WC, ICWT, I6WC and ICT features will change accordingly.

- Assume that subscriber A with ICWT option is talking with subscriber B, when a new call to subscriber A comes from subscriber C. In this case, the ICWT feature has the highest priority. That means when A flashes, the default flash action is toggle if icwt_dflt_rcode datafill Y even the I3WC or I6WC or ICT feature exist on the line A.
- If not in the ICWT case described above , the I6WC feature has the highest priority. Suppose ICWT, I6WC, I3WC and ICT exist on the line at the same time but not in ICWT scenario, due to we don't disable the Rcode for I6WC, after flashing, we need dialing rcode to select the action we want. Everything seems like before, but if we select establish 3-way call, and after we enter the 3-way call scenario, whether we need rcode in 3-way call is decided by i3wc_dflt_rcode datafill.
- If not in the ICWT case and line A has not I6WC feature, the I3WC feature will take the highest priority. Suppose ICWT, I3WC and ICT exist on the line at the same time but not in ICWT scenario, after flashing, if i3wc_dflt_rcode datafilled Y, we don't need Rcode to setup the 3-way call and don't need Rcode to disconnect party C as well.

- If not in the ICWT case and line A has not I6WC and I3WC feature, the ICT feature will take effect. In this case, Rcode is needed.

29.9.3 Software Requirements or Dependencies

This feature does not affect the provision method of CEPT I3WC. It takes effect when the subscriber is using CEPT I3WC and it is controlled by following datafill:

- In table ISERVOPT, tuple I3WC, the I3WC_DFLT_RCODE field. If datafilled ‘Y’, R-code is not needed in I3WC scenario. The RCODE tuple in table ISERVOPT must exist and the ACTION “CON_3WC” and “DISC_ACT” must be datafilled. If not , a nack tone will be given when flash and after the tone is over, the call will revert to the former state before flash.

30: Functional Description (FN): A00010168

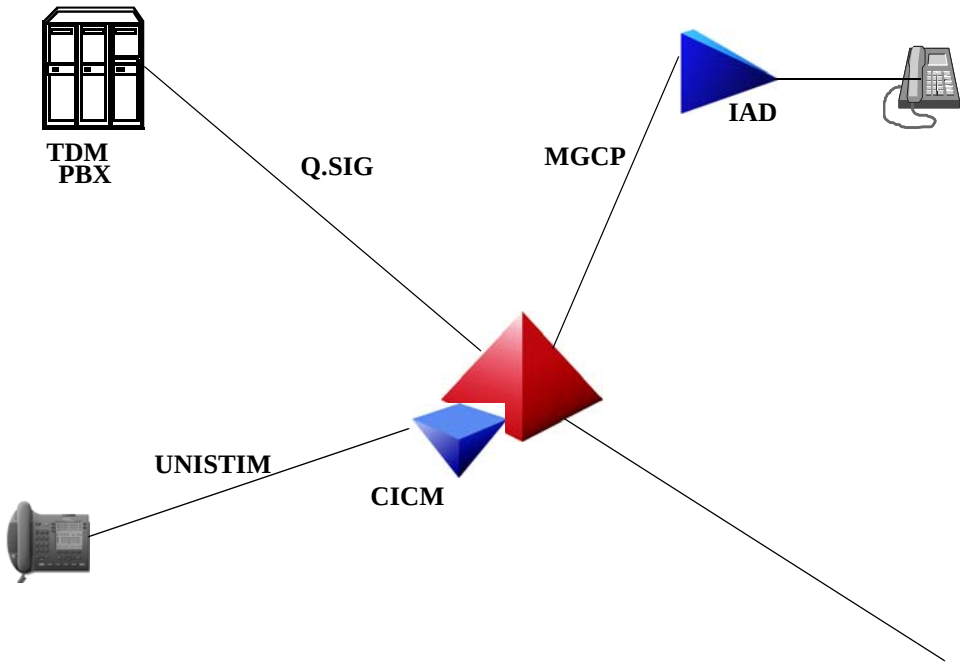
30.1 Feature name and Feature ID

A00010168: H.323 support for COnnected Line Presentation/COnnected Line Restriction (COLP/COLR)

30.2 Description

This feature is to support COLP/COLR on International H.323 Gateways.
In the context of H.323, QSIG (Q-reference point SIGnalling) is a private (i.e. corporate) network signaling protocol for communication between ISDN Private BranchExchanges (PBX). In respect to H.323 GWs Q.SIG will be used between H.323 and the core. COLP/COLR are existing QSIG functionalities. No new COLP/COLR capabilities are introduced by this feature.
Please refer to ìFigure 1 COLP/COLR Supplementary Servicesî on page 30.

Figure 1: Agent Interworkings over which COLP/COLR Mapping will be supported



2.2.1 COnnected Line Identification Presentation

COnnected Line Identification Presentation (COLP) supplementary service (SS) provides the calling party with the possibility to receive the connected users number.

COLP has the following functionalities:

Provides the calling user with the connected number (CNN).

The CNN IE is provided in the CONNECT message.

The service is provided on a per trunk-group basis, datafilled in table LTDATA.

When the COLP SS is activated, the Connected Party Subaddress Information Element (CNS IE), if provided by the connected user is included in the CONNECT message if COLR is not activated.

For a Private call provisioning is not required for the presentation of the CNN or the CNS IEsí. Whenever a CNN IE and CNS IE are received they are transparently passed on.

Supposing no information is provided by the connected user, the network provides the Default Number associated with the connected user. The DFLTCNN option in table LTDATA stores the Default Connected Number for the terminating side. If this is not datafilled then no digits are sent across to the originating side.

If the Presentation number is datafilled, then COLP enables the originator to receive the connected presentation number.
If NOSCRN option is datafilled, then the COLP enables the originator to receive the unscreened connected number.

For a call originated by a QSIG trunk which does not have COLP datafilled in table LTDATA, the COLP SS is not supported. To invoke the COLP SS, the originating QSIG trunk must be defined with the COLP option in table LTDATA. Please refer to ìTable 1 Sample Datafill for COLP in Table LTDATAon page 31.

Table 1 Sample Datafill for COLP in Table LTDATA

LTDKEY LTDRSLT
ISDN 4 SERV SERV N N ALWAYS ALWAYS **COLP**

Default Connected Number :
In case, the COLP SS is activated for the originator QSIG trunk and no information (CNN IE) is provided by the connected user or the information provided is invalid, the network provides the DeFauLT CoNnected Number (DFLTCNN) associated with the connected userís QSIG access in the destination local network. The default connected number is obtained from the DFLTCNN option in table LTDATA associated with the terminating QSIG trunk. The maximum number of connected number digits is 15.

Please refer to Table 2 Sample Datafill for Default Connected Number in Table LTDATA on page 32.

Table 2 Sample Datafill for Default Connected Number in Table LTDATA

LTDKEY LTDRSLT
ISDN 4 SERV SERV N N ALWAYS ALWAYS **DFLTCNN 6966970**

2.2.3 COnnected Line Identification Restriction

COnnected Line Identification Restriction (COLR) supplementary service (SS) enables the connected party to prevent presentation of its number to the calling party.

COLR has the following functionalities:

ï The COLR SS is offered at the terminating end.

ï It prevents the presentation of the connected number (CNN).

ï The service is provided on a per trunk-group basis. For COLR temporary, the default value (allowed/restricted) can be overwritten on a per call basis.

ï It prevents the presentation of the Connected Party Subaddress (CNS).

ï The COLR SS is offered by a permanent mode (PERM), or by a temporary mode (TEMP):

PERM mode: The COLR SS is invoked automatically by the network on all calls. If the calling party has subscribed to COLP SS, and the COLR SS datafilled as PERM RESTRICT is invoked and the valid CNN IE is sent from the terminating side, then the calling party receives the Connected Number IE with the indication of ìpresentation restrictedî and the digits not included.

TEMP mode: The COLR SS is invoked on a per call basis. This means that one of the following scenarios occurs, according to the default value set in the network:

a. If the Presentation Indicator (PI) value is supplied into the Connected Number Information Element (CNN IE), then the PI remains as received from the connected user.

b. If the PI value is not supplied into the Connected Number IE, the presentation indicator is set according to the COLR TEMP sub option that could be Allow or Restrict.

Please refer to Table 6 Sample Datafill for COLR: Table LTDATA on page 39.

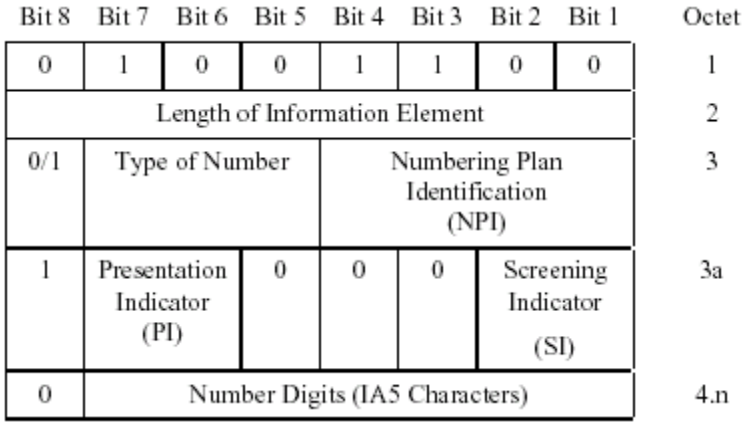
Table 6 Sample Datafill for COLR: Table LTDATA

LTDKEY LTDRSLT
ISDN 3 SERV SERV N N ALWAYS ALWAYS **COLR TEMP ALLOW**
ISDN 3 SERV SERV N N ALWAYS ALWAYS **COLR PERM RESTRICT**
ISDN 3 SERV SERV N N ALWAYS ALWAYS **COLR TEMP RESTRICT**

2.2.4 Values supported for SI, PI, TON, NPI in CNN IE

The connected number information is contained in the optional connected number information element (CNN IE) of the Q.931 connect message. The CNN IE is coded as shown in fig. 6. Please observe that octet 3 can have 0 or 1 value depending upon the usage. The maximum length of this information element is 24 octets. Please refer to ìFigure 5 Connected Number Information Element (CNN IE)î on page 41.

Figure 5 Connected Number Information Element (CNN IE)



The different option values of Screening Indicator (SI), Presentation Indicator (PI), Type Of Number (TON), Numbering Plan Indicator (NPI) as supported on the DMS100, are explained below.

Please refer to Figure 6 Option Values on page 34.

Figure 6 Option Values

Screening Indicator (SI)

2	1	
0	0	user-provided, Not Screened
0	1	user-provided, Verified, and Passed
1	0	user-provided, Verified and Failed
1	1	Network Provided

Presentation Indicator (PI)

7	6	
0	0	Allow
0	1	Restrict
1	0	Not available

Type Of Number (TON)

7	6	5	
0	0	0	Unknown
0	0	1	International Number
0	1	0	National Number
1	0	0	Subscriber number

Numbering Plan Identification (NPI)

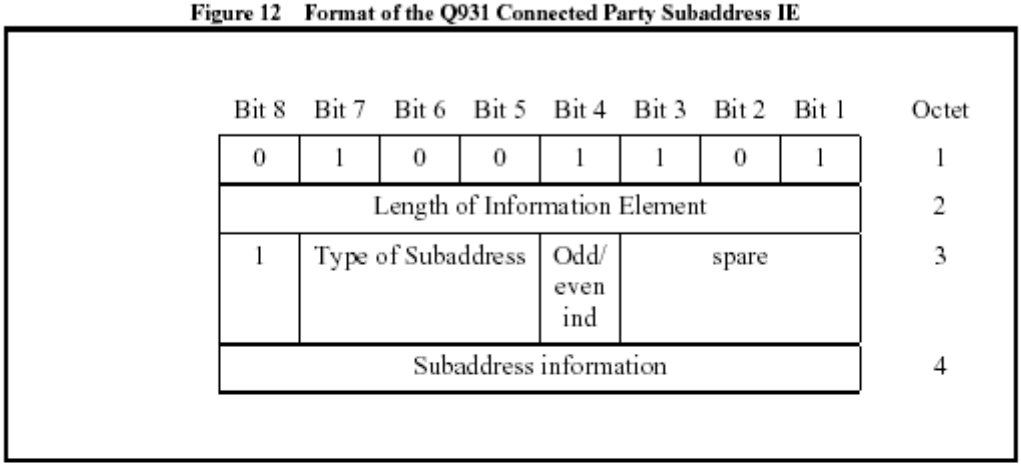
4	3	2	1	
0	0	0	0	Unknown
0	0	0	1	ISDN Telephony Numbering Plan (E164)
1	0	0	1	Private Numbering Plan

An incoming CNN IE at the terminating side is considered as valid only if the NPI field has "Unknown" or "ISDN Telephony Numbering Plan (E164)" values. Otherwise the information is discarded. The CNN fields from CONNECT message are updated at the CM level to reflect the CNN information that is delivered to the originating interface.

2.2.6 Connected Party Subaddress (CNS)

The purpose of the Connected party subaddress information element is to identify a subaddress associated with the terminator of a call. Please refer to "Figure 12 Format of the Q931 Connected Party Subaddress IE" on page 54.

Figure 12 Format of the Q931 Connected Party Subaddress IE



Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
0	1	0	0	1	1	0	1	1
Length of Information Element								2
1	Type of Subaddress			Odd/ even ind	spare			3
Subaddress information								4

For the Connected Party Subaddress the following is done,

- The CNS is mapped to the APP-PSS1 parameter. (For QFT only)
- The CNS is mapped to the ATP parameter in case of ISUP.
- If COLP SS is activated, add the Connected Party Subaddress Information Element to the CONNECT message.
- If COLR SS is activated, the Connected Party Subaddress Information Element is not added to the CONNECT message.
- If the calling user has not subscribed to COLP, then the CNN IE and the CNS info are not sent in the CONNECT message.
- On interworking of QSIG to QSIG, the CNS IE shall be mapped independently of the COLP SS.

The Presentation of the CNS IE depends on the following:

Public call:

- When COLP SS is not subscribed, the CNN IE and CNS IE are not sent to the calling user.

- When COLP SS is subscribed and PI = allowed, the CNN IE and CNS E (if available) are sent to the calling user.

- When COLP SS is subscribed and PI = restrictd, an 'empty/restricted' CNN IE is sent to the calling user. The CNS IE is not sent in this case.

Private Call:

- The CNN IE and CNS IE are mapped transparently.

- Exception for Originating and END PINX:

- When COLP SS is subscribed and PI = restricted, and empty/restricted' CNN IE is sent to the calling user. The CNS IE is not sent in th

2.2.8 Interworkings

Networked services support for interworking QSIG for H.323-based originating/ terminating at a 3rd party based PBX (e.g., Siemens HiPath) should include the following:

. i.COnnected Line Identification Presentation (COLP) supplementary service (SS).
ii.COnnected Line Identification Restriction (COLR) supplementary service (SS).

Networked services support for interworking QSIG for H.323-based originating/ terminating at a Nortel PBX (e.g., BCM50, BCM 200/400) should include the following:

i.COnnected Line Identification Presentation (COLP) supplementary service (SS).
ii.COnnected Line Identification Restriction (COLR) supplementary service (SS)

30.3 Limitations and restrictions

There is no attempt within this feature to map MCDN versions of COLP/ COLR to H.323 or to Q.SIG. This feature merely maps Q.SIG versions of COLP/COLR to H.323 versions of COLP/COLR (and vice versa). The following provide specific examples of messaging in MCDN environments

This feature is implemented exclusively for the support of International H.323 COLP/COLR. Refer to A59027747 QSIG Support for COLP/COLR for additonal restrictions on COLP/COLR.

30.4 Glossary

TERM	DESCRIPTION
CNN	Connected Number
CNN IE	Connected Number Information Element
CNS	Connected Number Subaddress
CNS IE	Connected Number Subaddress Infoma-tion Element

TERM	DESCRIPTION
COLP	COnnected Line identification Presentation
COLR	COnnected Line identification Restricton
QSIG	Q Interface Signaling
SS	Supplementary Service

30.5

References

1. AF7494, PLS DOC, COLP/COLR
2. AR2191, PLS DOC, ND ISDN SVCs:WT: Basic Call Services
3. AJ5284, PLS DOC, Presentation CLI Support
4. AU3248, PLS DOC, COLP/COLR Phase I
5. COLPRDOC in FMDOC, PRI COLP/COLR Phase II
6. A59012493 in FMDOC, PRI COLP/COLR Phase III
7. ETS 300-173 Specs
8. ECMA 148 Specs
9. ITU Q.699 Interworking Between ISDN access and non-ISDN access over ISUP SS #7
10. AE0975, CLIP/CLIR, Supplementary Services
11. A59027747 QSIG support for COLP/COLR.

31: Functional Description (FN): A00011363

31.1 Feature name and Feature ID

A00011363: International H.323 2CLI (Calling Line Identity) Support

31.2 Description

The activity provides support for 2 CLI delivery to a H.323 terminating Gateway/terminal[1] in the International CS2000 ISN load, for public calls.

This feature provides support for 2 CLI delivery for the following originating agent scenarios in a French market configuration, with functional equivalency to a terminating PRI trunk:

- ETSI ISUP v2 Base Variant -> International H.323 in Section 5.2.2.1.
- SPIROU -> International H.323 in Section 5.2.2.2.
- ETSI PRI -> International H.323 in Section 5.2.2.3.
- International H.323 -> International H.323 in Section 5.2.2.3.
- International H.323 -> ETSI PRI in Section 2.2.2.3
- International H.323 -> ETSI ISUP V2 Base Variant in Section 2.2.2.4
- International H.323 -> SPIROU in Section 2.2.2.5

Other originators and market configurations may also work but are not formally verified by this feature.

Support for 2 CLI delivery on outgoing ISUP/PRI trunks for a call originating from H323 is already supported and not changed by this feature.

The 2 CLI functionality is associated with ISDN supplementary service provisioning option Calling Line Identification Presentation (CLIP) and Calling Line Identifiation Restriction (CLIR). With 2 CLI the calling line has two identities namely the Network Number (NN) and Presentation Number (PN).

The standard 2 CLI handling mode described as “special arrangement” in H.246 and Q.699 is supported by this feature. In this mode of operation a User Provided CLI is passed on without verification and a 2nd Network Provided CLI is added to the call signalling by the 1st public network exchange.

[1]A H.323 terminating Gateway/terminal is referred to as the “International H.323 terminator” through out this document.

- A Network Number is a CLI provided by the public network,which identifies the actual network termination point from which a call originates.
- A Presentation Number (PN) is a dialable number that the calling user wishes to display to the called user. It is normally User provided and not verified by the network (Q699/H.246 “special arrangement” case).

The NN and PN may or may not be the same. The PN can be used to return a call to the originator or an associated number. For example, a calling salesperson may want to display a free phone number , in order to provide the incentive of a free call, when a purchase is made.

For the International H.323 terminator, if 2 CLIs are available they are delivered in the SETUP message by sending the Presentation Number in the CGN IE (Calling Party Number Information Element) field and the Network number in the additionalSourceAddresses field. If only 1 CLI is available then it is delivered in the CGN IE whether it is a Network Number or Presentation Number.

This complies with ITU-T H.246.0 Annex C(07/2003)[1] as ammended by the ITU-T H.323 System Implementors’ Guide(30th Januay 2004), for the case of interworking to a Gateway/terminal in “special arrangement” mode.

For this feature to work functionally a Gateway that also supports this capability per these versions of the specifications is required eg.OneAccess.

This feature extends the existing functionality implemented by French market 2 CLI feature A59027509 to provide equivalent behaviour for International H323 terminators. A59027509 is a refinement and extension of MMP14 feature A59016672 that developed 2CLI delivery for an ETSI PRI terminator. A59016672 in turn works only in conjunction with feature AJ5284 “Presentation CLI Support” and enhanced it to support Special Arrangement on selected agents. The “Special Arrangement” feature introduced by AJ5284 was developed to give selected customers the possibility to deliver Calling Party Numbers to the terminator which are not screened.

If Special Arrangement applies to a customer, the CGN digits delivered by him are not screened , however the NPI (Number Plan Indicator) and TON (Type of Number) information elements are screened to check public E.164 numbers are provided.

[1]Older versions of the H.323 and H246 specifications had different unrobust schemas.

31.2.1 Datafill control

This feature A00007329 will reuse the same datafill options that control 2 CLI delivery and behaviour for PRI trunks. Reference A59016672 & A59027509.

31.2.1.1 2 CLI delivery control options on the Terminating H323

31.2.1.1.1 2CLI Delivery Control option for International H.323 Terminator

Delivery of 2 CLIs vs only 1 CLI for an International H.323 terminator is enabled on a trunk group basis by datafilling the 2CLI option on the H.323 QSIG trunk. When the "2CLI" option is not data filled the QSIG interface will not generate 2CLI's in the outgoing SETUP message. A sample datafill in table LTDATA is as follows:

Table 1 Table LTDATA - Datafill 2CLI Option(New Datafill)

LTDKEY	LTDRSLT	LTCLI_OPTION	LTCLI_OPTION
H323TST CLI	CLI	2CLI	$

The 2CLI option is an existing option in table LTDATA previously only functional for PRI trunks.

31.2.1.1.2 CLIP option Table LTDATA

The CLIP option is applicable to ETSI PRI and International H.323 terminator. Sample datafill for International H.323 terminator is as follows :

Table 2 Table LTDATA CLIP option

LTDKEY	LTDRSLT	AUDTRMT	CGNREQD	CGNDELV	CDNDELV
H323TST 1 SERV	SERV	N	Y	SCREENED	ALWAYS

31.2.1.2 Related CLI options on the Originating H323

The availability of 2 CLIs for delivery is dependent on several factors. For PRI/ H323 to H323 the following options on the originating trunk are relevant (all are existing options and unchanged by this feature):

- CLIR option provisioned for the originator
- Screening for originator (Table LTDATA)
- CUSTGROUP public call (relation between originator and terminator)
- PN_SUPPORTED = Y

31.2.1.2.1 CLIR option Table LTDATA

The CLIR option is applicable for ETSI PRI and International H.323 originators. Sample datafill allowing presentation of the CLI unless overridden by per call CLIR activation code .

Table 3 Table LTDATA CLIR option

LTDKEY	LTDRSLT	LTCLI_OPTION	PI	MODE
H323TST 1 CLI	CLI	DFLTPI	ALLOW	TEMP

31.2.1.2.2 Screening in Table LTDATA

For “special arrangement” behaviour as required in France no screening is performed on the received CLI from the user . This is configured by using the NOSCRN option in a LTDATA CLI tuple.

Table 4 Table LTDATA

LTDKEY	DATATYPE	OPTION
H323TST 1 CLI	CLI	**NOSCRN**

In this NOSCRN case the Network Number is taken from the DFLTCGN option in LTDATA

Table 5 Table LTDATA

LTDKEY	DATATYPE	DFTLTCGN
H323TST 1 DN	DN	017 230 3680 $

Note)

For other markets other CLI options are used to configure different screening behaviour. eg: SCRNPN (screen the received CLI but use it as a PN) or SCRNLTID and SCRNDFLT (“no special arrangement scenarios to screen the

received CLI and use after editting as a single User provided Verified and Passed CLI)

31.2.1.2.3 CUSTGROUP Table CUSTNTWK

This option is applicable for ETSI ISUP V2, SPIROU, ETSI PRI and International H.323. It is a prerequisite for the 2CLI feature that the call must be a public call.

31.2.1.2.4 PN_SUPPORTED Table OFCENG

This option is applicable for ETSI ISUP V2, SPIROU, ETSI PRI and International H.323. The office parameter has two fields. They are ACTIVE and BTUP_SIM_HANDLING. For this feature, the field ACTIVE must be set to Y to enable 2 CLI behaviour for PRI/H323 to H323. It should not affect the ISUP interworkings. Datafill for PN_SUPPORTED option is illustrated below:

Table 6 Table OFCENG

PARMNAME	PARMVAL
PN_SUPPORTED	**Y** N

31.2.1.3 Example datafill for French 2 CLI configuration

```
>
2004/09/23 06:11 SWC00007.PPC3 V:12
TABLE: TRKGRP

>pos oa_4
OA_4
PRA 0 NPDGP NCRT MIDL 0172303690 (QSIG 9) $ $
>pos oa_2
OA_2
PRA 0 NPDGP NCRT MIDL 0172303688 (QSIG 10) $ $
>

TABLE: LTDATA
>lis all
TOP
LTDKEY LTDRSLT
--------------
QSIG 9 DN DN 017 230 3690 $
QSIG 9 SERV SERV Y N SCREENED ALWAYS (DAS PRIOVLP)
(NET_RINGBACK_ON )
(PRI_IP_PROT H323) $
QSIG 9 CLI CLI (DFLTPI ALLOW TEMP) (NOSCRN ) $
QSIG 10 DN DN 017 230 3680 $
```

QSIG 10 SERV SERV Y N SCREENED ALWAYS (DAS PRIOVLP)
(NET_RINGBACK_ON)
(PRI_IP_PROT H323) $
QSIG 10 CLI CLI (DFLTPI ALLOW TEMP) (NOSCRN) $

31.2.2 2CLI Mapping for Interworking Scenarios Supported:

31.2.2.1 ETSI ISUP v2 Base Variant to International H.323

There are three possible cases:

31.2.2.1.1 "Calling party Number" parameter in IAM complete

If a CGPN is present and complete in the IAM then one or two "calling party number" IE may be created according to the presentation indicator and the category of the served subscriber,i.e.

— If the presentation indicator of the CGPN is set to 0 (Presentation allowed), one or two "calling party number" IE may be created.

— If the presentation indicator of the CGPN is set to 1 (Presentation restricted) and called subscriber has the CLIR override category one or two "calling party number" IE may be created.

If the above condition is met and if the served subscriber is subscribed to the CLIP[1] supplementary service, then:

GNP presentation - If a "Generic Number" qualified to "additional calling party number" is present, it shall be sent in a first "calling party number" IE. This IE contains the address signal received in the IAM and is coded as follows:

Table 7 Generic Number mapped to CGN IE in International H.323SETUP

Bits	Value
Octet 3 bits 765	Type of Number is mapped transparently according to bits BA of identity of the calling line.

[1]Data filled in table LTDATA for the International H.323 terminator
Sample Datafill :
LTDKEY LTDRSTL CGNDELV CDNDELV

QSIG 1 CLI SERV SCREENED ALWAYS

Bits	Value
Octet 3 bits 4321	Numbering Plan Identification is mapped transparently.
Octet 3a bits 76	Presentation Indicator is mapped transparently
Octet 3a bits 21	Screening Indicator is mapped transparently
Octet 4 and above	Address signals

A second CLI (the Network Number) is sent to the terminating International H.323 agent in the additionalSourceAddresses parameter. The Calling party number parameter from the IAM is used to encode the additionalSourceAddresses Information element as follows:

Table 8 Coding of the additionalSourceAddresses Information Element According to the Calling party number parameter

IAM Calling Party Number parameter	SETUP additionalSourceAddresses
Nature of Address National number International number	Type of number National number International number
Numbering Plan Indicator	"Numbering plan identification"
ISDN/Telephony Numbering Plan	ISDN/Telephony Numbering Plan
Address Presentation Restricted Indicator Presentation allowed Presentation Restricted	Presentation Indicator Presentation Allowed Presentation restricted
Screening Indicator User provided, verified and passed Network Provided	Screening Indicator User provided, verified and passed Network Provided
Address signals	Number digits

31.2.2.1.2 Calling Party Number absent or incomplete

If the “calling party number” parameter received in the IAM is absent or incomplete then only one “calling party number” IE shall be created. The IE contains no address signal and is coded as follows:

Table 9 Calling Party Number in the SETUP (International H.323)

Bits	Value
Octet 3 bits 765	The "type of number" is set to unknown (000).
Octet 3 bits 4321	"Numbering plan identification" is set to unknown (0000)
Octet 3a bits 76	"presentation indicator" is set to number not available due to interworking (10).
Octet 3a bits 21	"Screening indicator" is set to network provided (11)

31.2.2.1.3 Identity complete, presentation restricted (without CLIR override)

If the "calling party number" received in the IAM is complete and available, and the presentation indicator is set to restricted, and the served subscriber does not have the CLIR override category, then only one "calling party number" IE shall be created. The IE contains no address signal. It shall be coded as follows:

Table 10 "Calling Party Number" in SETUP

Octet 3 bits 765	The "type of number" is set to unknown (000).
Octet 3 bits 4321	"Numbering plan identification" is set to unknown (0000).
Octet 3a bits 76	"presentation indicator" is set restricted (01).
Octet 3a bits 21	"Screening indicator" is set to network provided (11)

31.2.2.2 SPIROU to International H.323

The CLI handling is the same as Figure 5.2.2.1, "ETSI ISUP v2 Base Variant to International H.323".

31.2.2.3 International H.323/ ETSI PRI to International H.323/ ETSI PRI

The mapping of parameters for International H.323/ETSI PRI to International H.323 according to ETSI/ITU Q.699for the following configurations is supported:

Configuration	Calling user provisioned to:	Called user provisioned to:
I as described 5.2.2.3.1	CLIR option provisioned; PI = **allowed**	**CLIP** option provisioned 2CLI option provisioned;
II as described in 5.2.2.3.2	CLIR option provisioned; PI = **restricted**	**CLIP** option provisioned 2CLI option provisioned;
III as described in 5.2.2.3.3	CLIP option provisioned; PI = restricted	CLIP override option provisioned 2CLI option provisioned.

31.2.2.3.1 Configuration I:

- Calling User: Special arrangement applies
- Called User: CLIP
- Terminator : Two number delivery supported

Originator: ETSI-PRI/International H.323	optional: ETSI-ISUP V2	Terminator: International H.323/ ETSI PRI
Calling party number IE: TON = international national subscriber ***1** NPI = unknown or ISDN PI = Presentation allowed SI = not relevant digit = any digits	**Generic number parameter:** NOA = international national subscriber ***1** NPI = ISDN/Telephony PI = Presentation allowed SI = User provided, not verified digit = digits as received	**1. Calling party number IE:** TON = international national subscriber ***1** NPI = ISDN/Telephony PI = Presentation allowed SI = User provided, not screened digit = digits as received
	Calling party number parameter: NOA = national NPI = ISDN/Telephony PI = Presentation allowed SI = Network provided digit = Default DN	**2. Calling party number IE:** TON = national NPI = ISDN/Telephony PI = Presentation allowed SI = Network provided digit = Default DN

Originator: ETSI-PRI/International H.323	optional: ETSI-ISUP V2	Terminator: International H.323/ ETSI PRI
Calling party number IE: TON = 'unknown' or 'private network' or NPI != unknown or ISDN or digits = not available	**Generic number parameter:** not mapped **Calling party number parameter:** NOA = national NPI = ISDN/Telephony PI = Presentation allowed SI = Network provided digit = Default DN	**Calling party number IE:** TON = national NPI = ISDN/Telephony PI = Presentation allowed SI = Network provided digit = Default DN

Notes: 1 - only for certain markets, eg Germany. N/A to France. Controlled by Market of Office or other market datafill.

31.2.2.3.2 Configuration II:

- Calling User: Special arrangement applies
- Calling User: Temporary CLIR, Presentation restricted
- Called User: CLIP
- Terminating ETSI-PRI: Two number delivery supported

Originator: ETSI-PRI/International H.323	optional: ETSI-ISUP V2	Terminator: International H.323/ETSI PRI
Calling party number IE: TON = international national subscriber ***1** NPI = unknown or ISDN PI = Presentation restricted SI = not relevant digit = any digits	**Generic number parameter:** NOA = international national subscriber ***1** NPI = ISDN/Telephony PI = Presentation restricted SI = User provided, not verified digit = digits as received **Calling party number parameter:** NOA = national NPI = ISDN/Telephony PI = Presentation restricted SI = Network provided digit = Default DN	**Calling party number IE:** TON = unknown NPI = unknown PI = Presentation restricted SI = Network provided digit = not included/empty
Calling party number IE: TON = 'unknown' or 'private network' or NPI != unknown or ISDN or digits = not available	**Generic number parameter:** not mapped **Calling party number parameter:** NOA = national NPI = ISDN/Telephony PI = Presentation restricted SI = Network provided digit = Default DN	**Calling party number IE:** TON = unknown NPI = unknown PI = Presentation restricted SI = Network provided digit = not included/empty

Notes: 1 - only for certain markets, eg Germany. N/A to France. Controlled by Market of Office or other market datafill.

31.2.2.3.3 Configuration III :

- Calling User: Special arrangement applies
- Calling User: Temporary CLIR, Presentation restricted
- Called User: CLIP **override category**
- Terminating ETSI-PRI: Two number delivery supported

Originator: ETSI-PRI / International H.323	optional: ETSI-ISUP V2	Terminator: International H.323/ ETSI-PRI
Calling party number IE: TON = international national subscriber ***1** NPI = unknown or ISDN PI = Presentation restricted SI = not relevant digit = any digits	**Generic number parameter:** NOA = international national subscriber ***1** NPI = ISDN/Telephony PI = Presentation restricted SI = User provided, not verified digit = digits as received	**1. Calling party number IE:** TON = international national subscriber ***1** NPI = ISDN/Telephony PI = Presentation allowed SI = User provided, not screened digit = digits as received
	Calling party number parameter: NOA = national NPI = ISDN/Telephony PI = Presentation restricted SI = Network provided digit = Default DN	**2. Calling party number IE:** TON = national NPI = ISDN/Telephony PI = Presentation allowed SI = Network provided digit = Default DN
Calling party number IE: TON != international/national(or subscriber ***1**) or NPI != unknown or ISDN or digits = not available	**Generic number parameter:** not mapped	**Calling party number IE:** TON = national NPI = ISDN/Telephony PI = Presentation allowed SI = Network provided digit = Default DN
	Calling party number parameter: NOA = national NPI = ISDN/Telephony PI = Presentation restricted SI = Network provided digit = Default DN	

Notes: 1 - only for certain markets, eg Germany. N/A to France. Controlled by Market of Office or other market datafill.

31.2.2.4 International H.323 to ETSI ISUP V2 Base Variant

This functionality already exists and is not changed by this feature, but is not explicitly documented for H323 yet, hence this section is included for information only.

In the French market configuration the mapping is identical to that for PRI to ETSI ISUP V2 Base Variant as documented in feature A59027509. Any additionalSourceAddresses field or 2nd CGN IE received from H323 will be ignored by the CS2000.

This is in alignment with the mapping as specified in Q.699 with Special Arrangement and ITU-T H.246 Annex C Gateway/Terminal interworking case with Special Arrangement. A59027509 has some clarifications to the handling of some field coding cases not explicitly defined in Q699/H.246 and not normally expected.

31.2.2.5 International H.323 to SPIROU

This functionality already exists and is not changed by this feature, but is not explicitly documented for H323 yet, hence this section is included for information only.

In the French market configuration the mapping of Calling Party Number and Generic Number Parameter in the IAM from the SETUP message are as described in the TWOCLI FN document.

31.2.3 Network Number editing

When the Network Number is delivered on H323 in the additionalSourceAddresses field the digits contained may be editted by the CLGDMI option against the outgoing H323 trunk.

The Presentation Number sent in the CGN IE will also be editted by CLGDMI as in the current 1 CLI delivery case.

31.3 Hardware Requirements or Dependencies

This feature requires a Gateway supporting ITU-T H.246.0 Annex C(07/2003)[1] as ammended by the ITU-T H.323 System Implementors' Guide(30th Januay 2004). The terminating International H.323 Gateway/terminal must be capable of receiving 2CLIs in the H.225.0 SETUP message. The first CLI is coded in the Calling Party Number Information Element and the second CLI in the additionalSourceAddresses field .

31.4 Software Requirements or Dependencies

None

31.5 Limitations and restrictions

- This feature requires a Gateway supporting ITU-T H.246.0 Annex C(07/2003)[2] as ammended by the ITU-T H.323 System Implementors' Guide(30th Januay 2004). This feature will not work with gateways implementing older versions of the ITU-T H.246 Specification.
- Only Public E164 type (User Provided) Presentation Number CLIs are supported and will always be sent in the Calling Party Number IE field.

[1]Older versions of the H.323 and H246 specifications had different unrobust schemas.
[2]Older versions of the H.323 and H246 specifications had different unrobust schemas.

- as per Section 5.8.1 Interworking for Conveying Two Calling Party Number, Section C.7.2.3 Calling Line Identification Presentation (CLIP) /Calling Party Name Presentation (H.450.8), Table C.56/ H.246 “CLIP information sent to the called user” of the ITU-T H.323 System Implementors’ Guide shall not use the SourceAddress of the SETUP message and shall use the Calling Party Number IE field because the number being sent is a public number.
- As per Section 7.8.2.1 Calling party address information of the ITU-T H.323 (07/2003) the SourceAddress field of the SETUP message is used to encode numbers belonging to the Private numbering plan.
- The mapping of parameters from the H.225.0 SETUP to ISUP IAM as per Table C.20.1/H.246 Calling Party Number and Table C.20.2/ H.246 Calling Party Number of the ITU-T H.323 System Implementors’ Guide which referes to cases where SourceAddress fields are received is not supported.

- The Gatekeeper to Gatekeeper scenarios described in H.246 are not supported,
  - — any received additionalSourceAddresses field will be ignored by the CS2000. Only the 1st CGN IE is used.
  - — The mapping of parameters from the H.225.0 SETUP to ISUP IAM for SETUP messages received from the Gatekeeper when Special Arrangement applies is not supported.
  - — The mapping of 2CLIs received from the Gatekeeper as per Section 5.8.1 Interworking for Conveying Two Calling Party Numbers, Section C.6.2.1.1 Special Arrangement Applies - “Setup Received from the Gatekeeper” of the ITU-T H.323 System Implementors’ Guide is not supported.
- ‘Special Arrangement does not apply’ scenarios are not applicable - these are 1 CLI scenarios:
  - This feature does not support carrying of the GNP in the IAM message for International H.323 to ETSI ISUP v2 Base Variant for “without special arrangement” case.
  - The mapping of parameters from the H.225.0 SETUP to ISUP IAM as per Table C.21/H.246 “CLIP - Special Arrangement does not apply” of ITU-T H.246.0 Annex C is out of the scope of this feature and should be provided by the base H.323 feature.
  - The mapping of parameters from the H.225.0 SETUP to the ISUP IAM as outlined in Section 5.8.1 Interworking for Conveying Two Calling Party Number, Section C.6.2.1.2 Special Arrangement does not apply “Setup Received from the Gatekeeper” of the ITU-

T H.323 System Implementors' Guide is not a supported configuration for this feature.

31.6 Interactions

None

31.7 Applicable customer facing sections

Fault Management

Logs	__N/A__
Alarms	__N/A__

Configuration

Data Schema	___X___
User Interface	__N/A__
Element Management	__N/A__
Security	__N/A__
Service Order	__N/A__
Office Parameters	__N/A__

Accounting (includes AMA billing) __N/A__

AMA billing information is not changed by this feature.

The NDS Billing feature as documented in fmdoc PRNDSBIL has been verified for the International H.323 to ETSI ISUP v2 calls by this feature in response to a request from N9UF telecom for this feature. The Table 11, "Digits captured in Module 046 and the OOD of the AMA record," on page 561 shows the digits captured in the OOD field of the AMA record and that captured in the Module 046 for International H.323 to ETSI ISUP v2 calls in which the incoming SETUP message has a CGN IE present, that have been verified by this feature.

AMACLID_IC_PRI_CGN is a option present in table AMAOPTS.

Table 11 Digits captured in Module 046 and the OOD of the AMA record

BILLDN	AMACLID	DFLTCGN in table LTDATA	AMACLID _IC_PRI_C GN	OOD(AMA Base Record)*	Screening/ Editing of Incoming CLI provisioned?	OOD MODULE 46
-	TRUE	Datafilled	-	DFLCGN from table LTDATA.	-	-

BILLDN	AMACLID	DFLTCGN in table LTDATA	AMACLID _IC_PRI_CGN	OOD(AMA Base Record)*	Screening/ Editing of Incoming CLI provisioned?	OOD MODULE 46
-	TRUE	No		CLI from the SETUP message.	-	-
Datafilled	TRUE	No	ON	BILLDN	CLI Screening Passes	Unscreened/ Unedited CLI (CLI from the SETUP message).
Datafilled	TRUE	Datafilled	OFF	BILLDN	CLI Screening Passes	Screened/ Edited CLI (DFLTCGN from table LTDATA)
Datafilled	TRUE	No	ON	BILLDN	N	CLI from the SETUP message. If AMACLID_IC_PRI_CGN is OFF then 0's only are appended to the module 046.
-	-	No	-	CLI from the CGN IE in the SETUP message	Screening passes or screening fails.	-
Datafilled	-	No	-	BILLDN	Screening passes or screening fails	-

31.8 Glossary

Term	Description
CGN	Calling Number
CLI	Calling Line Identification
CLID	Calling Line Identification
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
DN	Directory Number

ETSI	European Telecommunications Standards Institute
GN	Generic Number
GWC	GateWay Controller
H.323	A protocol supporting the Packet-based Multimedia Communications Systems
IE	Information Element
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
NN	Network Number
NPI	Numbering Plan Identifier
PI	Presentation Indicator
PN	Presentation Number
PRI	Primary Rate Interface
QSIG	Q Interface Signalling
SI	Screening Indicator
SPIROU	Signalisation Pour l'Interconnexion des Réseaux Ouverts
TON	Type of Number
VPN	Virtual Private Network

31.9 References

Table 12 References

Document	Title
Requirement Document NC/ France/22 v1.0	CLI Handling between ISUP V2, SPIROU and Access Protocols
NC/France/21 v2.0	CLI Handling between ISUP V2, SSUTR2 and Access Protocols PRI VN, ETSI PRI, BRI VN, ETSI BRI and Ananlogue line.
AJ5284	Presentation Number Feature
A59027509	ISUP 2CLI Support with VN4(PRI) and ETSI (PRI,BRI)
A59016672	ETSI-PRI CLIP/CLIR Enhancement
ITU-T Recommendation Q.699 (09/97)	Interworking between ISDN Access and Non-ISDN Access over ISDN User Part of Signalling System No. 7

Table 12 References

Document	Title
ITU-T H.225.0 (07/2003)	Call Signalling protocols and media stream packetizarion for packet-based multimedia communication systems.
ITU-T H.323 (07/2003)	Packet-based multimedia communications systems.
ITU-T H.246.0 Annex C (07/ 2003)	Annex C :ISDN User Part Function - H.255.0 Interworking
ITU-T H.323 System Implementors' Guide(30th Januay 2004)	Implementors' Guide for Recommendations of the H.323 System ("Packed-based multimediacommunications systems") : H.323, H.225.0, H.245, H.246,H.283, H.235, H.341, H.450 Series, H.460 Series and H.500 Series
TWOCLIFN (in FMDOC)	TWO CLI support for SPIROU and ETSI ISUP V2 interworking with PRI/BRI.

32: Functional Description (FN): A00012291

32.1 Feature name and Feature ID

A00012291: MG15K Call-waiting Tone Support & Additional International Tones

32.2 Description

This feature extends the existing PVG Toneset support to include several new international variants. This feature also modifies several currently supported tonesets per business requirements. Finally, this feature provides support for multiple call-waiting tones within a given country toneset.

Specifically, this feature provides:

- New Support for Pakistan Toneset
- New Support for Brazil (Custom 1) Toneset
- New Support for Mexico (Custom 1) Toneset
- Modifications to Venezuela Toneset
- Modifications to Turkey Toneset
- Modifications to Taiwan Toneset
- General Support for Multiple (Up to 15) Call Waiting Tone Patterns per Country Toneset
  - —Support for 2 (specific) Call Waiting Tones for Mexico Toneset
  - —Support for 2 (specific) Call Waiting Tones for Taiwan Toneset
- Improved Support for Spare Toneset Patching (Patchability for up to 5 spare tonesets per release)

The primary driver for this feature is to allow for PVG market penetration into new countries and/or new telecommunication companies in the newly supported countries.

32.3 Overview

This feature does not require any changes to the basic external operation of the existing PVG toneset.

As per the requirements, this feature does provide the following customer/ subscriber visible changes:

- New Support for Pakistan Toneset
- New Support for Brazil (Custom 1) Toneset

- New Support for Mexico (Custom 1) Toneset
- Modifications to Venezuela Toneset
- Modifications to Turkey Toneset
- Modifications to Taiwan Toneset
- General Support for Multiple (Up to 15) Call Waiting Tone Patterns per Country Toneset
    - Support for 2 (specific) Call Waiting Tones for Mexico Toneset
    - Support for 2 (specific) Call Waiting Tones for Taiwan Toneset
- Improved Support for Spare Toneset Patching (Patchability for up to 5 spare tonesets per release)

Primary internal areas impacted:

- SPM - Connection Manager
- SPM - Tones Database
- PDC - Provisioning options for new country tonesets
- PDC - Improved Support for Spare Toneset Patching

32.4 Provisioning procedures

There are no significant changes to the provisioning procedures for PVG tones. However, as the feature provides for some previously unsupported country tonesets, (Pakistan, Brazil Custom 1, Mexico Custom 1) provisioning options for these tonesets are now available.

Below is a summary of the provisioning areas changed. As each of these areas provide for the provisioning of a toneset attribute, and since the list of supported tonesets is expanded with this feature (per above), these areas now provide the new choices.

- Nsta/n Vgs - *defaultToneset*
- Nsta/n Vgs Brag/n - *toneset*
- Nsta/n Vgs BragS/n - *toneset*
- Nsta/n Vgs TProf/n - *toneset*

The above now include options for provisioning “*pakistan*”, “*mexicoCustom1”*, and “*brazilCustom1*”.

33: Functional Description (FN): A00012349

33.1 Feature name and Feature ID

A00012349: U3WC Support For SIP Lines

33.2 Description

This feature expands the existing Three Way Call (3WC) and Usage Sensitive Three Way Call (U3WC) services to IBN and RES type SIP Lines.

The 3WC/U3WC service provides the activation/deactivation of the Three Way Calling on the line. In SIP Lines case, actual conferencing service is provided by edge device like Optical Network Terminator (ONT) or by the CS2K Session Server, on an ad-hoc basis, as in the case of a PC Client. To the CS2K Core, the calls appear as separate ones.

This feature supports both possible methods to invoke U3WC from a UA (User Agent), that is, via the access code or via flash access (same as normal 3WC, no access code).

When a UA, in a stable call state, invokes this feature, it triggers the core to first check for the 3WC or U3WC option provisioning, for that SIP line. If any of these options are provisioned correctly, the second (consultation) leg origination attempt is allowed to proceed. Otherwise, the origination attempt is denied and the caller is sent to treatment for the add-on leg. If the second leg call is successful, the UA can flash again to conference the three parties involved. This activity will not pre-empt the other features from allowing the second leg call origination.

33.2.1 Billing

Each time DPL U3WC is invoked, a billing record based on Structure Code 00001 with Call Type of 048 and Service Feature of 018 is created. For DPL, the conferencing is done at the client or on ad-hoc basis at the CS2K SS and hence no conference resources are used in the core. Also, the conference notification from User Agent is not being implemented as part of this activity. Because of this, the DPL U3WC billing record will be made always consistent with the TOTAL_DURATION setting of the U3WC_ELAPSED_TIME, irrespective of this parm being set to any other values. Also the billing record will be generated for every successful U3WC consult call termination, regardless of whether a conference is ever established.

The module code 260 will be appended to the DPL U3WC billing records to indicate that they pertain to SIP lines, when the RECORD_MC260 tuple is set

to ON in table AMAOPTS. An example DPL U3WC billing record is shown below.

Figure 1 Example call code 048 for U3WC billing

```
*HEX ID:AA  STRUCTURE CODE:40001C  CALL CODE:048C  SENSOR TYPE:036C
 SENSOR ID:0619351C  REC OFFICE TYPE:036C  REC OFFICE ID:0619351C
 DATE:50929C  TIMING IND:00000C  STUDY IND:0000000C  CLD PTY OFF-HK:0C
  SERVICE OBSERVED:0C  OPER ACTION:0C  SERVICE FEATURE:018C  ORIG
NPA:613C ORIG NUMBER:6215674C  OVERSEAS IND:0C  TERM NPA:00613C TERM
NUMBER:6216004C  CONNECT TIME:1408247C  ELAPSED TIME:000000467C
 MODULE CODE:260C  COMPONENT ROLE:101C  IP SERVICE PROTOCOL:001C
 MODULE CODE:260C  COMPONENT ROLE:201C  IP SERVICE PROTOCOL:001C
 MODULE CODE:000C
```

33.2.2 Operational Measurements (OMs)

Currently in the CS2K core, for non-DPL case, the U3WC OM registers are being pegged for the User Three Way Call service. This OM has the U3WCATT (U3WC Attempts), U3WCCONS (U3WC consultations) and the U3WCCONF (U3WC conferencing) registers that are pegged.

For DPL case, the conferencing service is provided by the UA or the CS2K SS and the conference notification from User Agent or CS2K SS is not available to the core. Hence for DPL, it is not possible to peg the U3WCCONF register. If the other two registers are pegged, it could lead to an imbalance over time. For this reason, none of the U3WC OM registers will be pegged for the DPL case.

33.3 Hardware Requirements or Dependencies

Not Applicable

33.4 Software Requirements or Dependencies

Not Applicable

33.5 Limitations and restrictions

The following are the restrictions and limitations of this service:

- The conferencing capability shall be enabled in the clients (for UAs like ONTs) or ad-hoc conferencing shall be provided by the CS2K SS (for UAs like PC clients).
- For DPL case, none of the U3WC OM registers will be pegged. Please refer to the "Operational Measurements (OMs)" section above.
- This activity supports consult leg originations with or without the VSCs. However, for originations with only the U3WC VSCs, then followed by

CDN digits after second dial tone, the PMA/AMS setup needs to be configured, so that digit collection can take place.

- Client based refer or redirect requests will not be screened or blocked by 3WC/U3WC options.
- The 3WC option must be explicitly datafilled for SIP lines, for IBN type and when U3WC is not applicable, for the RES type also, in order to establish additional sessions, once the first session has been answered.
- Conference Notification from User Agent (ONT or PC Client or a SIP Phone) is not planned to be implemented as part of this activity. Hence the DPL U3WC billing record will be always consistent with the TOTAL_DURATION setting of the U3WC_ELAPSED_TIME, irrespective of this parm being set to any other values. Also the billing record will be generated for every successful U3WC consult call termination, regardless of whether a conference is ever established. Module code 260 will be appended to the DPL U3WC billing records to indicate that they pertain to SIP lines, when the RECORD_MC260 tuple is set to ON in table AMAOPTS.

33.6 Interactions

- U3WC option is not compatible with the CXR (Call Transfer) option (refer to the U3WC related FN sections of actids AQ1302). U3WC if active on a RES line, will disappear (become inactive), once the CXR option is assigned to that line.
- For 3WC option, if the client needs to transfer the call, will have to invoke REFER before exiting. While 3WC is active, call transfer screening will occur when the controller gets out of the conference. At that point, the CXR option provisioning will determine if the call between the remaining 2 parties will survive or not.
- 911 calls on consult leg are treated the same way as any other calls and don’t have any preferential processing.

33.7 Glossary

Term	Description
3WC	Three Way Call
CS2K	Communication Server 2000
CS2K SS	Communication Server 2000 - Session Server
DPL	Direct Packet Lines
ONT	Optical Network Terminator
PC	Personal Computer

Term	Description
SIP	Session Initiation Protocol
U3WC	Usage Sensitive Three Way Call
UA	User Agent

34: Functional Description (FN): A00012477

34.1 Feature name and Feature ID

A00012477: Session Initiation Protocol (SIP) Services - Call Completion to Busy Subscriber (CCBS)

34.2 Description

This activity provides support for Call Completion to Busy Subscriber collectively called CCBS, for Dynamic Packet Lines (DPL).

CCBS supplementary service enables user A, encountering a busy destination B to have the call completed without having to make a new call attempt. Originator A activates CCBS after getting busy tone from terminator B and goes onhook. When the terminator B is idle, originator A is notified by recall ringing. If A answers the call, normal call setup with B is carried and the call proceeds. If B becomes busy after A gets recall ringing, the CCBS request is queued again. For call scenarios and detailed information please refer to document A59011976, CCBS to Analog Lines.

CCBS is similar in functionality to the North American RAG (Ring AGain) service but is based on ETSI specification and therefore different in implementation.

Network CCBS is an integral part of CCBS, it is invoked when and if the called party is in another office, there is an ISUP V2 link and TCAP messages are carried between switches.

This activity **only** supports for single digit activation of CCBS and CEPT CCBS functionalities on SIP lines.

34.3 User Agent Requirements

In order to be integrated with the CS2000 CCBS service, the User Agent (UA) must be able to support the interface specified by this feature. A User Agent must be able to handle SIP Refer and Hold methods. To be able to provide the CS2000 CCBS service fully, they must also support callerid, distinctive ringing.

34.4 Hardware Requirements or Dependencies

Not applicable

34.5 Software Requirements or Dependencies

This activity is implemented in ISN09 drop 2 release. This activity requires the activity A00012317 SIP - Automatic Call Back (ACB) and Automatic Recall (AR) which is being also implemented for ISN09 drop2.

34.6 Limitations and restrictions

In this functionality CCBS will work as

- Line should have CCBS option,
- SINGLE_DIGIT_ACTIVATION for CCBS feature should be set to Y as in ISERVOPT table (CCBS tuple)
- The single_digit_activation digit should be datafilled in this tuple
- CCBS owner (ragor) calls busy agent, and receives CCBS announcement,
- Ragor dials activation digit and receives confirmation or negative acknowledgement

The following limitations and restrictions are needed for this activity.

- Activating of CCBS feature via sending INFO messages is not supported in this activity
- Activating of CCBS feature via opening a new session and dialing service code is not supported. Since SIP phone is not able to open a new session if the it is not received 200 OK message.
- The announcement resources should be provided in the office

34.7 Interactions

34.7.1 Network Based Interactions

34.7.1.1 Destination Line - Network Determined Idle

If the CS2000 is monitoring a destination line for an CCBS request, and that line is a DPL line, the line will be determined to be idle when there are no network based sessions for that line. User Agent based sessions and User Agent based services (e.g. Do Not Disturb) will not be taken into account by the CS2000.

34.7.1.2 CCBS Subscriber - Network Determined Idle

If the CS2000 is about to recall notify a DPL CCBS subscriber, that subscriber will be determined to be idle for recall when there are no network based sessions for that line. User Agent based sessions and User Agent based services (e.g. Do Not Disturb) will not be taken into account by the CS2000.

34.7.2 User Agent Interactions

34.7.2.1 Normal Call Termination Failure

If the CS2000 is attempting to terminate to a DPL line that the CS2000 has determined to be “network idle”, but the termination fails for any of the following reasons:

- User Agent not registered
- User Agent registered, but not responding

the CS2000 will not accept an CCBS activation on that call (either via flash and dial access code).

34.7.2.2 CCBS Recall Notification Failure

If the CS2000 attempts to recall notify a DPL CCBS subscriber, and that recall attempt fails due to any of the following:

- User Agent not registered
- User Agent registered, but not responding
- User Agent registered, User Agent responds with any response other than a “100 Trying” or “180 Ringing”, (e.g.busy indication due to Do Not Disturb, or currently in dialing state),

the CS2000 will check ccbs_recall_time expires, if so request is removed.

34.7.2.3 CCBS Call Setup Failure

If the DPL CCBS subscriber has answered the recall notification, and the CS2000 is attempting to setup the call to the destination line (using the REFER method), but the Call Setup request fails due to any of the following:

- User Agent not registered
- User Agent registered, but not responding
- User Agent registered, User Agent responds with anything other than a “202 Accepted” or “NOTIFY:Terminated” (e.g a busy/reject indication)

the CS2000 will check if ccbs_term_recall_time timer expires. if so request is removed.

34.7.2.4 CCBS Call Termination Failure

If the CS2000 is attempting to terminate to a DPL line because of an CCBS request, and the CS2000 has determined that DPL line to be “network idle”, but the termination fails for any of the following reasons:

- User Agent not registered
- User Agent registered, but not responding

the CS2000 will not accept an CCBS activation on that call (either via flash and dial access code).

34.8 Glossary

Term	Description

35: Functional Description (FN): A00012509

35.1 Feature name and Feature ID

A00012509: SIP Services Wake up Call Reminder

35.2 Description

This activity provides support for WUCR (Wake Up Call Reminder) and CEPT IWUC for SIP Lines.

WUCR is assigned as a line option and is activated and deactivated by the end user through the use of access codes.

Upon activation of WUCR, a wake-up call request is programmed by the end user to ring the end user's line at a particular time within the next 24 hours. The end user can deactivate the feature and cancel the wake-up call request at any time after it is programmed.

This activity will also provide the Wake Up Call features for SIP Lines CEPT variant (IWUC).

The differences between two variants are:

- IWUC feature requires * (star) after the activation code of IWUC. Examples of digit sequences are shown below;

  Centrex variant activation digit sequence: *SC<RDT>HHMM#
  *CEPT variant activation digit sequence: *SC*<RDT>HHMM#*
  Centrex variant deactivation digit sequence: #SC#
  CEPT variant deactivation digit succulence: #SC#
  Centrex variant interrogation digit sequence: not applicable
  *CEPT variant interrogation digit sequence: *#SC*HHMM#*

- For the interrogation issue which is only applicable for CEPT variants; if the request is valid, then the subscriber will receive a confirmation tone, if the request is invalid, or a wakeup request is not active on the line; then the subscriber will receive a NACK treatment.

35.3 Hardware Requirements or Dependencies

Not applicable

35.4 Software Requirements or Dependencies

This activity is implemented in ISN09 drop 2 release.

35.5 Limitations and restrictions

The limitations stated in the previous document Wake Up Call for International with ID AE0240FN.AB01 are also valid except the limitations for the line capacity of both LCM and the switch since these limitations are not valid for DPL lines.

35.6 Interactions

35.6.1 Network Based Interactions

35.6.1.1 WUCR Subscriber - Network Determined Idle

If the CS2000 is about to ring a DPL subscriber, that subscriber will be determined to be idle when there are no network based sessions for that line.

35.6.2 User Agent Interactions

35.6.2.1 Normal Call Termination Failure

If the CS2000 is attempting to terminate to a DPL line that the CS2000 has determined to be “network idle”, but the termination fails for any of the following reasons:

- User Agent not registered
- User Agent registered, but not responding
- User Agent registered, User Agent responds with busy indication (e.g. Do Not Disturb, or currently in dialing state),

35.6.2.2 Treatment tones

When the client answers during to the wakeup ringing, the WUCR treatment to be applied (defined as extended_treatment_type) is set in the call. Then this can be mapped to the initial tone (in table tones) via TMTCNTL table.

So when WUCR treatment is applied, TMTCNTL and TONES table should be datafilled accordingly. We can datafill initial tone patterns, cadence, time value, tone ids etc. in table TONES.

Consequently there is an opportunity to datafill supported tone ids in table TONES for WUCR treatment, there is no hard coded tone id for WUCR.

35.6.2.3 User Agent Based Sessions

User Agent based sessions and User Agent based services (such as user based Do Not Disturb) will not be taken into account by the CS2000 and will not factor into determining if the line is available.

35.6.2.4 Client Dependencies

Different SIP clients show different behaviors during applications and this causes different flows.

Until now we had the chance to test PC SoftClient and that's why the documentation is depending on the results retrieved with PC SoftClient.

35.6.3 Service Interactions

35.6.3.1 Core Based Services

- **911 Network Hold:** No interaction.
- **ACB/AR:** Not available in Drop 2 content. Out of scope.
- **AIN:** No interaction.
- **Anonymous Call Rejection:** No interaction
- **Auth/Account Codes:** No interaction
- **Busy Line Verification:** Not available in Drop 2 content. Out of scope.
- **Call Forward**: There is no interaction if activation or deactivation of WUCR is attempted on a line that is call forwarded. If a wake-up call attempts to call an end user who has Call Forwarding active, the wake-up call is treated as if it were not answered, and WUCR follows the rules for unanswered first attempts.
- **Call Park - Directed Call Park:** No interaction.
- **Call Pickup / Directed CPU:** Not available. Out of scope.
- **Call Transfer Screening:** No interaction.
- **Calling Name Delivery:** No interaction, user line rings with an anonymous call.
- **Calling Number Delivery:** No interaction, user line rings with an anonymous call.
- **Calling Name/Number Blocking:** No interaction.
- **Customer Originated Trace:** No interaction.

- **Directed CPU w/Barge In:** Incompatible.
- **Hunting:** Incompatible.
- **Lawful Intercept:** No interaction.
- **LNP:** No interaction.
- **`MADN:** Not available in Drop 2 content. Out of scope.
- **MADN/SCA:** Not available in Drop 2 content. Out of scope.
- **Malicious Call Trace:** No interaction.
- **No Double Connect:** No interaction.
- **SIMRING:** No interaction.
- **Speed Calling:** No interaction.
- **Subscriber Activated Call Blocking:** No interaction.
- **Call Completion Busy Subscriber (CCBS):** No interaction.
- **CLF & B-Party Control:** No interaction.
- **Payment Ceiling Advice (PCA):** No interaction.

35.6.3.2 Session Server Based Services

- **SIMRING:** No interaction, if the pilot activates a wakeup call, the members will not be affected by wakeup call.
- **Ad-hoc conferencing (3 and 6 way):** No interaction
- **Personal Agent Screening / Routing:** No interaction, the wakeup call will not be routed.

35.6.3.3 Client Based Services

- **Blind Transfer:** No interaction

• **Call Forwarding / Redirect:** No interaction, the wakeup call will not be forwarded.

• **Call Hold:** No interaction

• **Call Waiting:** No interaction.

• **Cancel Call Waiting:** No interaction

• **Consultative Transfer:** No interaction

35.7 Glossary

- DPL: Dynamic Packet Lines
- GWC: Gateway Controller
- PMA: Packet Media Anchor
- UA: User Agent
- FPE: Future Processing Environment
- RDT: ReDial Tone

35.8 References

- CEPT IWUC with activity ID A59019097,
- Wake up Call for International with ID AE0240

36: Functional Description (FN): A00012510

36.1 Feature name and Feature ID

A00012510: SIP Services: Malicious Call Trace

36.2 Description

This feature introduces the following two services for SIP Line users. These two services will be presented in this FN in two separate sections.

- CLF for SIP Lines in International Markets
- B-Party Control on ETSI ISUP for SIP Lines in International Markets

36.3 CLF for SIP Lines in International Markets

36.3.1 Description

CLF is a service that enables the subscribers to catch the DN of a malicious caller and report this as a log in their local exchange.

MCT (Malicious Call Trace) is the common name used for features CLF and MCH:

- CLF stands for Calling Line Identification with Flash and is used in IBN lines
- MCH stands for Malicious Call Hold and used in KSETs.

This activity deals only with CLF feature, since SIP Lines use the features of IBN and RES lines.

The markets shown below are chosen as the markets with high priority and CLF for these markets will be implemented initially.

Australia[1] (ATUP[2], AISUP[3], ACIF-ISUP[4] and CA30-ISUP[5])

Israel[6] (Israel ISUP)

UK[7] (BTUP and UKISUP)

36.3.2 Feature Activation

In TDM IBN lines “flash + activation code” is used to activate CLF service. However, SIP lines cannot use flash since there is no equivalent way of sending a flash message in SIP and the clients currently don’t support it. The way to activate features using SIP lines is sending the access code to CS2000 in a new session with an invite message.

When the user wants to activate CLF feature, he/she will initiate a new session (the 2nd session) and dial * + the access code. Note that, this activity assumes that there will be only one existing session in addition to the one that is used for dialling the access code.

The second session will be initiated by an Invite message including the * followed by the access code datafilled in table IBNXLA.

Datafill Example:

In the office of the victim (term), give option CLF to the terminating line in servord and datafill the table IBNXLA with MCH option.

SO:
>ado $ 5551201 clf $

>qdn 5551201

DN: 5551201
TYPE: SINGLE PARTY LINE
SNPA: 216 SIG: DT LNATTIDX: N/A
LINE EQUIPMENT NUMBER: PHNX 00 0 00 01
LINE CLASS CODE: IBN
IBN TYPE: STATION
CUSTGRP: CUST783 SUBGRP: 0 NCOS: 0
CARDCODE: GWLPOT GND: N PADGRP: PKNIL BNV: NL MNO: N
PM NODE NUMBER : 85
PM TERMINAL NUMBER : 2
OPTIONS:
CLF DGT DPL Y 10

Then datafill the table IBNXLA with MCH option.

CI:
>table ibnxla
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: IBNXLA
>add
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
KEY:
>STARCEPT 89
TRSEL:
>FEAT

```
ACR:
>N
SMDR:
>N
FEATURE:
>MCH
TUPLE TO BE ADDED:
STARCEPT              89 FEAT N N      MCH
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
>lis
KEY RESULT
----------
STARCEPT 89 FEAT N N MCH
>
```

To activate CLF in this example, the victim makes a new call with the digits *89 on the second session upon receiving a malicious call on the first session.

(Note for the Israel market:
In Israeli market, the TDM IBN lines activate the CLF by a hook-flash only. In order to implement this in SIP Lines, there will be an arrangement with MTA vendors so that when using IBN sets as SIP Lines through MTA, the MTA should be capable of converting the flash message into a SIP INVITE message bearing the activation code as dialled digits.)

36.3.3 AFTER ACTIVATION:

If the activation is successful, the second session (i.e. the session where we activated CLF) will receive confirmation tone. If the activation is not successful, like in the case of having less than or more than two active sessions (one for activation and one for the malicious call), a nack tone will be received.

The activation of CLF will result in production of a Malicious Call log in logging device - logutil in the switch of the victim (the term office). The calling line information (i.e. the malicious caller) will be visible in this log.

36.3.4 B-PARTY CONTROL:

The B-party control will give the control of the call to the called party (i.e. the victim). So, the call will not be released until the called party goes on-hook or the timer expires, depending on the individual market specifications. This means the malicious caller can not make any other calls as long as the call is held. If the malicious caller tries to make a new call after hanging up on the victim, he/she will be connected back to the existing held connection to the

victim's line. This will enable tracing the malicious caller in cases of the Calling Line Identity (CLI) can not be received. In case of timer expiry, this will allow a regret time to the victim to activate the CLF after the malicious caller hangs up.

The B-Party Control behavior in SIP Lines for CLF will be transparent to the B-Party Control behavior in TDM IBN Lines for CLF. The only difference is that we can not hold the subscriber's agent as in TDM world but instead we connect it back to the held connection when it tries to make a new connection.

36.3.5 Hardware Requirements or Dependencies

Not Applicable.

36.3.6 Software Requirements or Dependencies

This feature has dependency on feature "A00012402 - SIP Lines: 911 Hold/ Ringback" for the Session Server load.

36.3.7 Limitations and restrictions

The CLF can be activated by sending a new invite message with the access code. There can only be one active session in addition to the session in which the access code is sent. If this is not the case, then the session will receive a nack tone.

In TDM IBN lines, the CLF feature can also be activated by CLF_ACCESS_CODE that is datafillable in table OFCVAR. CLF feature for SIP Lines does not support this method of activation.

Please see the note at the end of Section 9.3.2 for the arrangement in Israeli market.

36.3.8 Interactions

There are no new interactions introduced by this feature.

36.3.9 References

1. ISN04 (TDM) Product Description - Part E: Features and Services, p.755
2. AJ1063 - ATUP-MCT Interworking
3. AJ1243 - AISUP Feature Interactions
4. a) ISN04 (TDM) Software Portfolio - s.3.3 Network Interfaces, p.151
   b) ACIF G500:2000 PART D - Sec. 2.1.3
5. A59028026 - CA30 ISUP for Australia
6. E0444C - TELRAD Product Spec ETSI ISUP V2 Part C - Sec. 4.17
7. ISN04 (TDM) Product Description - Part E: Features and Services, p.752

36.4 B-Party Control on ETSI ISUP for SIP Lines in International Markets

36.4.1 Description

This feature provides the functionality to give the control of the call to the called party where the called party is an emergency service line.

B-Party Control on ETSI ISUP for TDM IBN Lines was handled by activity AJ5441. This activity brings the same functionality to SIP Lines.

When a call is made from a SIP Line to an emergency service (CLASS=EMRG), and the caller goes on-hook, the network resources from the emergency's line to the Session Server of the calling SIP Line will be held. When the caller tries to make a new connection, it will be connected back to the existing held connection.

The resources will be held until either the terminating line goes on-hook or the timer expires.

36.4.2 Hardware Requirements or Dependencies

Not Applicable.

36.4.3 Software Requirements or Dependencies

This feature has dependency on feature "A00012402 - SIP Lines: 911 Hold/ Ringback" for the Session Server load.

36.4.4 Limitations and restrictions

In TDM activity "AJ5441 - B-Party Control on ETSI ISUP", it is also required that CALLCTRL should be set to CALLED in table OFCHEAD to give the call control to the called party. This is because in TDM IBN lines, the Call Control can have 3 separate values: CALLING, CALLED and MUTUAL. However in SIP Lines, the Call Control is always MUTUAL. It is unnecessary to check if the CALLCTRL is CALLED here. Therefore, this requirement has been taken off the requirements list here with the agreement of PLM.

36.4.5 Interactions

There are no new interactions introduced by this feature.

36.4.6 References

AJ5441 - B-Party Control on ETSI ISUP

36.5 Glossary

Term	Description
CLF	Calling Line Identification with Flash

Term	Description
ETSI	European Telecommunications Standards Institute
IBN	Integrated Business Network
ISUP	ISDN (Integrated Services Digital Network) User Part
KSET	Key Set
MCH	Malicious Call Hold
MCT	Malicious Call Trace
RES	Residential Enhanced Services
SIP	Session Initiation Protocol
TUP	Telephone User Part

37: Functional Description (FN): A00012511

37.1 Feature name and Feature ID

A00012511: SIP Services: Payment Ceiling Advice (PCA)

37.2 Description

The following two sections summarize Payment Ceiling Advice (PCA).

37.2.1 NAOC (Tariff Database Part)

Network Advice Of Charge (NAOC) implements the tariffing of calls over the network boundaries. Two network configurations are supported:

1. It operates in a single/multiple carrier environment, where the originating exchange is able to determine the tariff. This improves the performance and reduces the messaging over the network (see Figure , ""). This is generic functionality which supports all versions of ETSI ISUP interconnection trunks.
2. It operates in a multiple carrier environment, where the originating exchange (named Charged Generation Point, CGP) does not know the tariff that will be applied to the call for every call, so it has to retrieve the information over the network from the selected carrier's exchange (called Charge Determination Point, CDP, see Figure 2, "NAOC messages are exchanged between different networks (Germany only)").

Figure 1 CGP tracking for a Combined CGP and CDP is supported (generic)

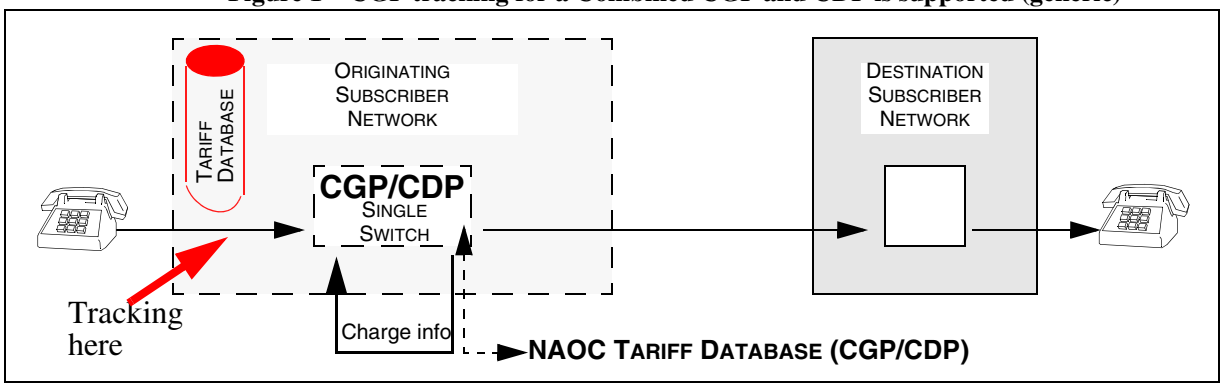
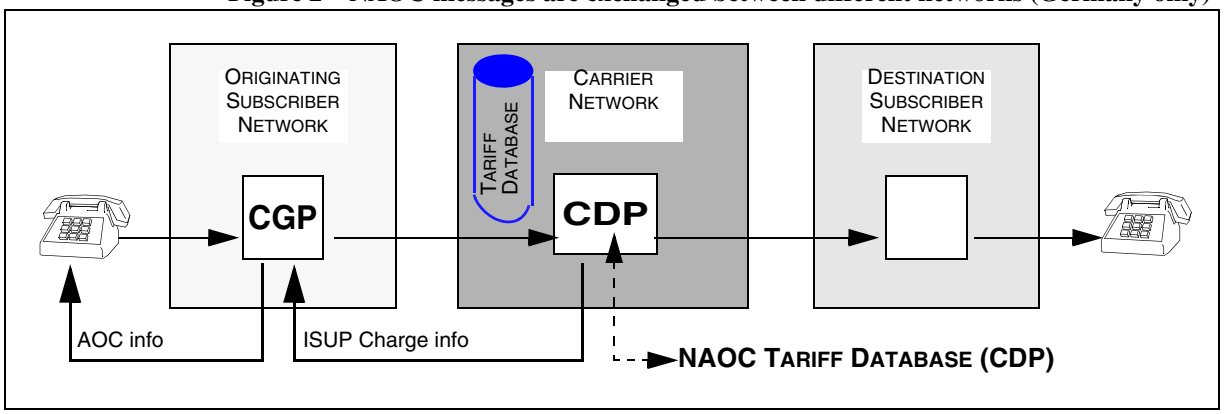


Figure 2 NAOC messages are exchanged between different networks (Germany only)



37.2.2 PCA (Hot Billing Part)

A SIP line may request that the PCA option be added to his or her directory number (DN). When ordering this service, the subscriber must specify a particular payment ceiling amount. This amount applies to each of the subscriber's billing cycle (generally every 29 - 32 days, but it can be any period of the year in terms of PCA). If no billing cycle is provided, the subscriber's account will never get reset.

PCA comes with the following abilities:

- When performing a call, the subscriber's charges are counted during the call and written into the PCA database (PCADB) at the end of the call. This operation is done in real time, so that PCA can provide hot-billing abilities.
- The PCA database can be queried at any point of time to retrieve the information regarding a specific subscriber's account.
- The PCA database information can be displayed in either currency units or virtual pulses (which correspond to 1/1000 of one currency units)
- Complex tariff structure described by the NAOC tariffs is fully supported.
- Several complex call scenarios are supported.
- PCA database can be automatically reset based on the provisioned information.
- PCA Essential functionality prevents a subscriber from originating line-to-ETSI ISUP calls that do not provide PCA charging information.
- PCA tracking per access provides a possibility to use one base DN for multiple lines with separate DNs. That is, call charges for all lines of that access are tracked via one dedicated DN (referred to as base DN).
- Announcements are provided for approaching or exceeding the PCA limit:
    - Prepaid or tracking phone bill

  - When a subscriber approaches the PCA limit by exceeding the 80% PCA limit, he hears a (provisionable) announcement he is approaching his limit (80% announcement).
  - When he exceeds his PCA limit, he hears the announcement, that he exceeds his limit. Depending on the datafilled information, he might not be able to do any additional phone calls (prepaid) or only some specific call classes (100% or mid-call announcement).
- Bonus notification
  - When a subscriber exceeded the 80% limit, he hears an announcement that encourages him to perform additional calls to get the discount.
  - When he exceeded his PCA limit, he hears the announcement that he qualified to get a bonus.

- PCA supports prepaid functionality and selective force release:
  - Prepaid
    - When exceeding his PCA limit, the subscriber cannot perform any calls except emergency calls and charge free calls.
    - When the prepaid account expires, the account is reset, so that the subscriber cannot perform any calls except emergency calls and charge free calls.
  - Selective force release
    - Depending on the datafilled information, only specific call classes are allowed after the subscriber reached his PCA limit during a call or during the last call.

For more details please refer to the following activities:

a. A59034497 - Payment Ceiling for Succession International Integrated Access-Cable

b. A59039121 - NAOC and PCA Feature Interworkings with 3WC, CFx, HOLD and CWT

c. A89007461 - Payment Ceiling Regulatory Enhancements

37.3 Hardware Requirements or Dependencies

None.

37.4 Software Requirements or Dependencies

None.

37.5 Limitations and restrictions

The limitations and restrictions introduced by the above activities (A59034497, A59039121, A89007461) are all inherited by this activity. In addition to these:

- Metering for more than 2 sessions are not supported.

37.6 Interactions

37.7 Glossary

Term	Description
NAOC	Network Advice Of Charge
PCA	Payment Ceiling Advice
SIP	Session Initiation Protocol

38: Functional Description (FN): A00012847

38.1 Feature name and Feature ID

A00012847: CS2K DPNSS Message Waiting Indicator for UMS

38.2 Description

The UMS (Unified Messaging Server) optionally connects via SIP or SMDI to the CS2K and will send MWI activation or deactivation requests as appropriate to the CS2K where they will enter the CS2K core software component ‘EMWI’. The EMWI framework has two concepts:-

Controlling User - *The user that activates and deactivates the message waiting indication - i.e., the Voice Mail System.*

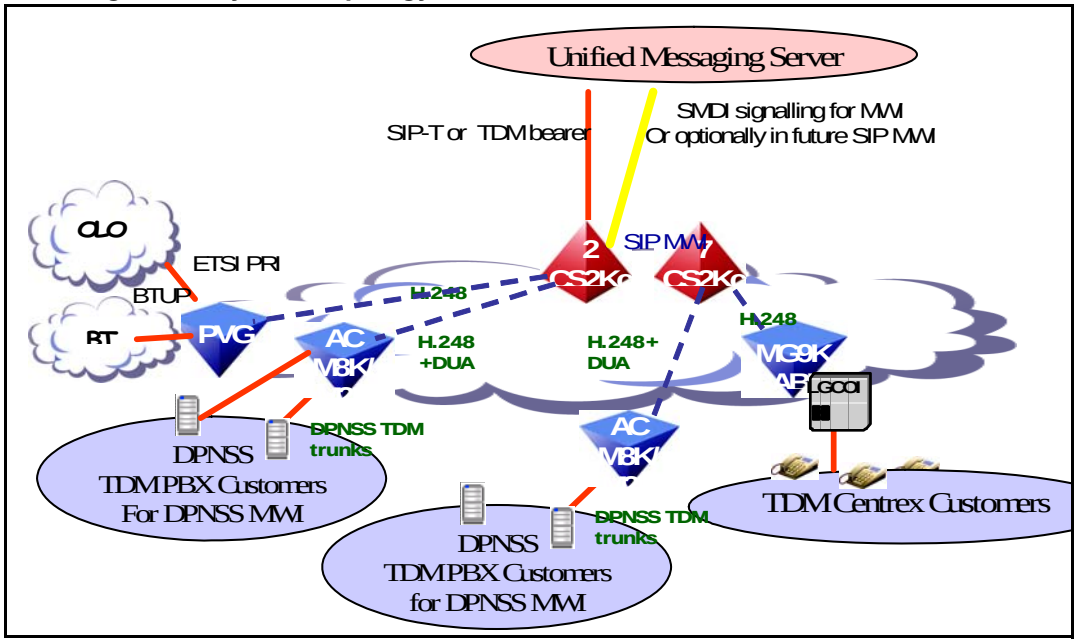
Receiving User - *(served user) The user that receives the message waiting indication - i.e., the PBX Line connected to CS2K via DPNSS.*

This feature provides the new functionality inside the EMWI component for these requests to be mapped by the CS2K software and transmitted using native DPNSS signalling[1] to the PBX where the end user’s line would have the message waiting lamp light up, or be extinguished. Therefore, this feature provides DPNSS Receiving User functionality.

The feature is controlled by SOC code PBXA0022

[1]Through a suitable DUA gateway such as the Nortel MG3200, or DTCOi for MMP.

Figure 1 System Topology



38.2.1 Configurable NSI Strings per DPNSS trunk group

The DPNSS specification does not standardize the contents of the NSI (Non-Specified Information) string that is sent to the PBX in the Layer 3 DPNSS ISRM message to indicate MWI activation or deactivation.

This has led to PBX systems using different NSI strings, and so is born the requirement for the activation and deactivation NSI strings to be defined in the CM such that they can be selected per DPNSS trunk group.

In order to increase compatibility between Nortel products (Nortel CS2K & Nortel M1 PBX) and to minimize the amount of 'datafill work' by the customer, the CS2K will create a 'default' tuple, set to the activation and deactivation strings used by the M1 PBX. All DPNSS trunks will use this NSI string unless overridden.

If the NSI string is required to be overridden for a particular trunk group, then a new tuple would be added in new table DPNSSNSI to map the MWI NSI strings to a particular NSINAME, and then an entry in TRKOPTS to map the NSINAME to a particular trunk CLLI.

For example, the datafill for a customer that has a Nortel M1 and a Plessey/ GPT ISDX (connected over CLLI DPNSSISDX1) would be as follows:-

TABLE DPNSSNSI

```
NSINAME OPTION
--------------
DEFAULT   (MWI ( ACT B N N 1) (DEACT B N N 0)$)$
ISDX      (MWI ( ACT B A N 1) (DEACT B A N 0)$)$
```

TABLE TRKOPTS

```
OPTKEY      OPTINFO
-------------------
DPNSSISDX1  DPNSS DPNSS (NSINAME ISDX) $
```

The craftsperson can alter the information in the DEFAULT tuple, but will receive the warning:-

```
** WARNING ** : Changes to DEFAULT tuple detected.
These changes will affect all DPNSS trunk groups that
have not had their CLLI overridden with the DPNSS
NSINAME option in table TRKOPTS. You have been
warned.
```

Table 1 DPNSSNSI Table Specification

Field Name & Hierarchy			Description & Format		Mandatory
NSINAME			Table Key	= 16 Chars	Yes
OPTION			Options list, currently 1 option of MWI		
	MWI		Message Waiting Indicator		Yes
		ACT	Activation NSI String		Yes
			Vector of 4 parameters		
			SIS_ID_SUFFIX	= 1 Char	
			MFR_ID	= 1 Char	
			MFR_SERVICE	= 1 Char	
			OTHER_PARM	= 3 Chars	
		DEACT	Deactivation NSI String		Yes
			Vector of 4 parameters		
			SIS_ID_SUFFIX	= 1 Char	
			MFR_ID	= 1 Char	
			MFR_SERVICE	= 1 Char	
			OTHER_PARM	= 3 Chars	

Table Restrictions & Notes

- Table can support up to a maximum of 255 tuples.
- The default tuple cannot be deleted.
- It is recommended that the NSINAME reflect the type of PBX.
- The format of the NSI Activation & Deactivation string is as follows:-
  `*58<SIS_ID_SUFFIX>*<MFR_ID><MFR_SERVICE>*<OTHER_PARM>#`

  *e.g., the DEFAULT entry of 'B N N 1' would be sent as *58B*NN*1#*

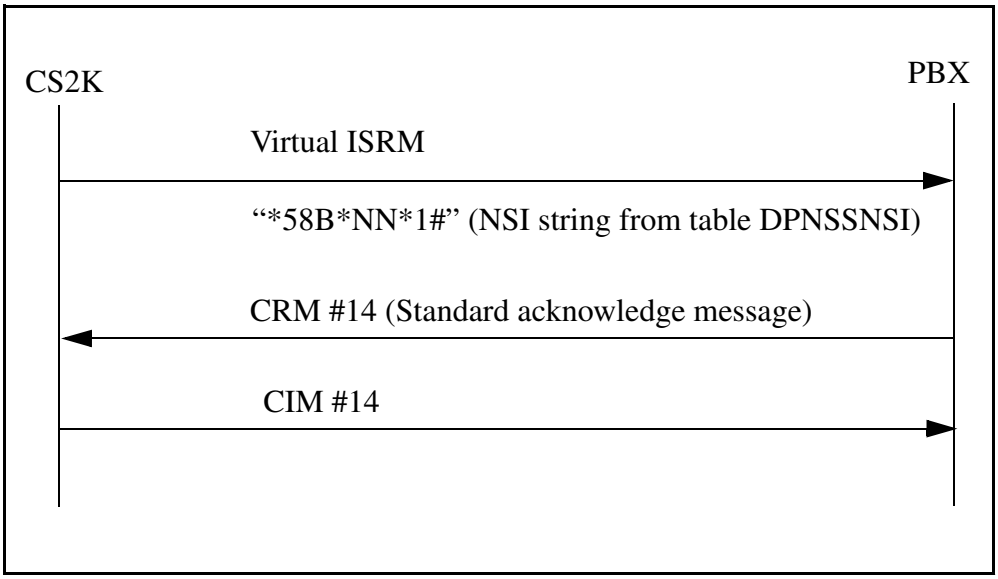
Table 2 Manufacturer Identities

MFR_ID	Manufacturer
A	GEC-Plessey
B	BT/E
C	Mitel
D	GEC-Plessey
E	STC
F	Ferranti
G	Philips

MFR_ID	Manufacturer
H	AT&T
I	IBM
J	Ericsson
K	GEC-Plessey
L	BT
M	Siemens
N	Nortel

11.2.1 DPNSS Signalling to convey the MWI command

The Layer 3 DPNSS signalling that is generated to convey the NSI string to the PBX will use a Virtual DPNSS trunk with the NSI string in the ISRM message. E.g.:-



When the PBX receives the ISRM message, it will then translate the destination digits in the message to find the line, and then parse the NSI string to decide if the line should have it’s message waiting lamp light up, or be extinguished.

Here is an example of the DPNSS Layer 3 bytes for activating MWI on the PBX line 4506070 using the DEFAULT NSI:-

```
Msgcode: #00 ISRMC(INITIAL SERVICE REQUEST
(COMPLETE))
          10 2A 31 23 2A 35 38 42 2A 4E
<.*1#*58B*N>
          4E 2A 31 23 34 35 30 36 30 37
<N*1#450607>
          30                              <0          >
```

11.3 Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced by this feature.

11.4 Software Requirements or Dependencies

No new software requirements or dependencies are introduced by this feature.

11.5 Limitations and restrictions

Because this feature reside in the native DPNSS stack on the CM, it is compatible with MMP/hybrid solutions (e.g., DTCOi) or with CS2K solutions using DUA gateways (MG3200).

The feature is not compatible with the Westell DPNSS gateway as this is not true DPNSS in the CM.

11.6 Interactions

No interactions between this feature and others are introduced.

11.7 Glossary

Term	Description
CS2K	Communication Server 2000
GW	Gateway
GWC	Gateway Controller
IP	Internet Protocol
MWI	Message Waiting Indication
MWT	Message Waiting
NCAS	Non-Call-Associated Signaling
PBX	Private Branch Exchange
PSTN	Public Switched Telephony Network
SCTP	Session Control Transport Protocol
SIP	Session Initiation Protocol
SMDI	Simplified Message Desk Interface
SOC	Software Optionality Control
UM	Unified Messaging
VM	Voicemail System

39: Functional Description (FN): A00013275

39.1 Feature name and Feature ID

A00013275: SESM Flex Large Line GWC Profile Support - Phase 1

39.2 Description

This feature provides generic support for large line gateways supporting up to a maximum of 2047 endpoints within a single virtual media gateway. This is initially aimed at supporting the Audiocodes TP6310 card as used within the Mediant 8000 chassis on behalf of C&W.

Additionally support is provided for the Audiocodes TP6310 card when configured as a trunk carrier gateway in order to support DPNSS.

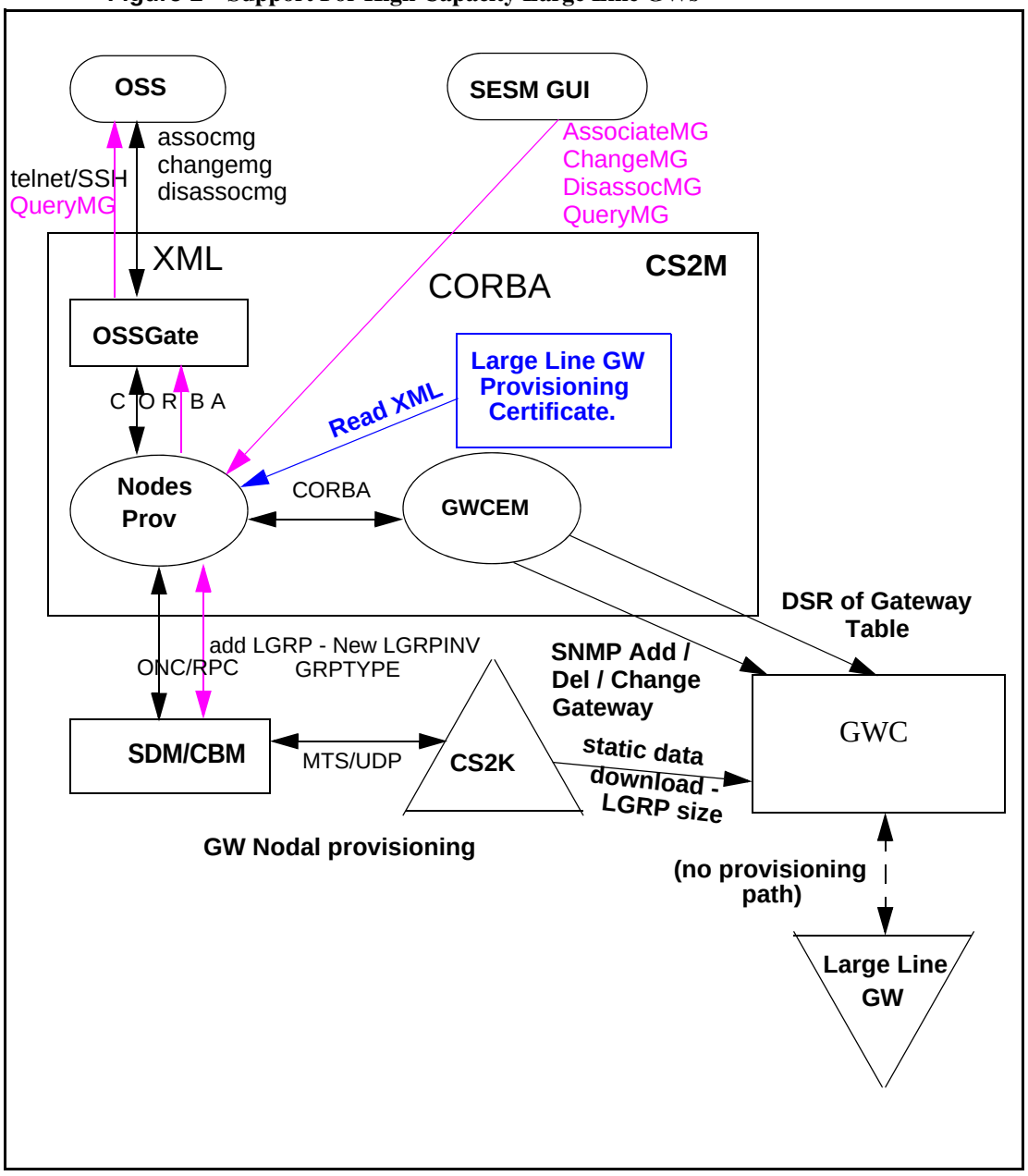
The support for the Audiocodes TP6310 configured as a trunk gateway is restricted to this feature only, the corresponding associated GWC and CM features only cover the TP6310 when provisioned as a high capacity large line GW.

Prior to this feature large line gateways were limited to a maximum of 1024 endpoints, and in situations where additional endpoints were required this has been modelled by treating the gateway as multiple gateways from the perspective of the CM - examples being the CICM and SIP voice gateways.

This feature adds the following functionality to the CS2M:

- Support for the Audiocodes TP6310 card provisioned as a large line GW for use in the Mediant 8000 Gateway chassis.
- Support for the Audiocodes TP6310 card provisioned as a trunk GW for use in the Mediant 8000 Gateway chassis.
- Support for large line GWs of capacity <= 2047 endpoints.
- Support for both International and North American market fit.
- Support for both 750 and 905 GWC types.

Figure 1 Support For High Capacity Large Line GWs



39.2.1 Pre-Requisites

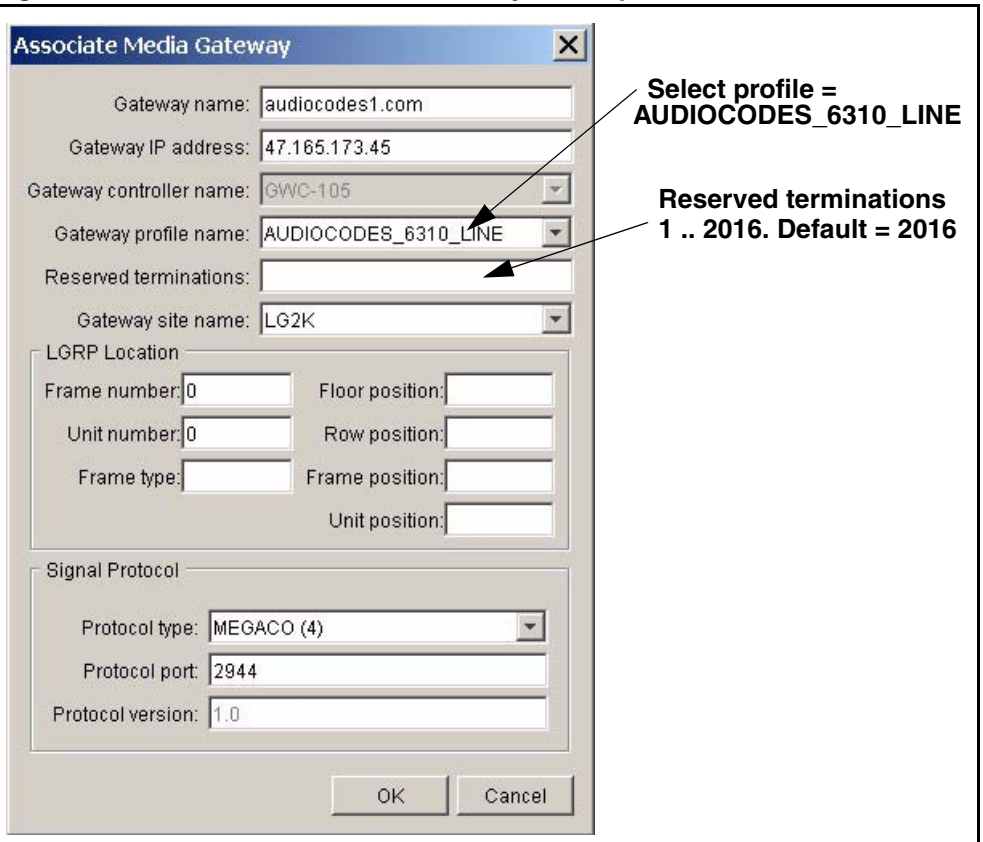
The following pre-requisites must be met before attempting to provision an Audiocodes M8K GW:

- The CS must be running an SN09.1 or later load.
- The CS2M should be running the SESM SN09.1 or later load.
- The GWC which will host the Audiocodes M8K GW must be provisioned with a profile supporting Large Line GWs and must be running the SN09.1 or later load.

39.2.2 Provisioning Of Audiocodes TP6310 Large Line GW - GUI Interface

Provisioning of the Audiocodes TP6310 Large Line GW is similar to existing 3rd party line GWs. The provisioning of 3rd party line type GWs is as per SN08 features A00007071 and A00007072. On selecting the "AUDIOCODES_6310_LINE" profile the Associate Media Gateway dialog will be populated as follows:

Figure 2 CS2M Associate Media Gateway GUI Population For TP6310 Line GW



The Audiocodes TP6310 is a 3rd party GW. This means that the provisioning crafts person must define the LGRPINV tuple to be provisioned at the CM.
The LGRPINV tuple consists of Site + Frame + Unit. In this example we are specifying and LGRPINV tuple of "LG2K 0 0".

Table 1 Associate Media Gateway Field Population

Field	Contents
Gateway name	Provisioned GW Name. Max 32 characters. Follows DNS naming convention.
Gateway IP address	IP address for Audiocodes GW
Gateway controller name	GWC-nnn Name of a valid GWC provisioned with a large lines supporting profile.
Gateway profile name	AUDIOCODES_6310_LINE for TP6310 card as large line GW
Reserved terminations	In range 1 .. 2016. Defines number of terminations to reserve for use with this GW. If the field is left empty the default behaviour is to reserve 2016 terminations.
Gateway site name	From CM table SITE. Chosen site must be capable of supporting manually provisioned LGRPs of size 2048 (maximum 2047 endpoints)
Frame number	Logical frame number in range 0 .. 511 Combines with Site and unit number to form LGRP. The combination of all 3 must be unique.
Unit number	Logical unit number in range 0 .. 9 Combines with Site and Frame number to form LGRP. The combination of all 3 must be unique
Protocol type	MEGACO - H.248
Protocol port	defaults to 2944 but may be edited if desired
Protocol version	Fixed to version 1.0

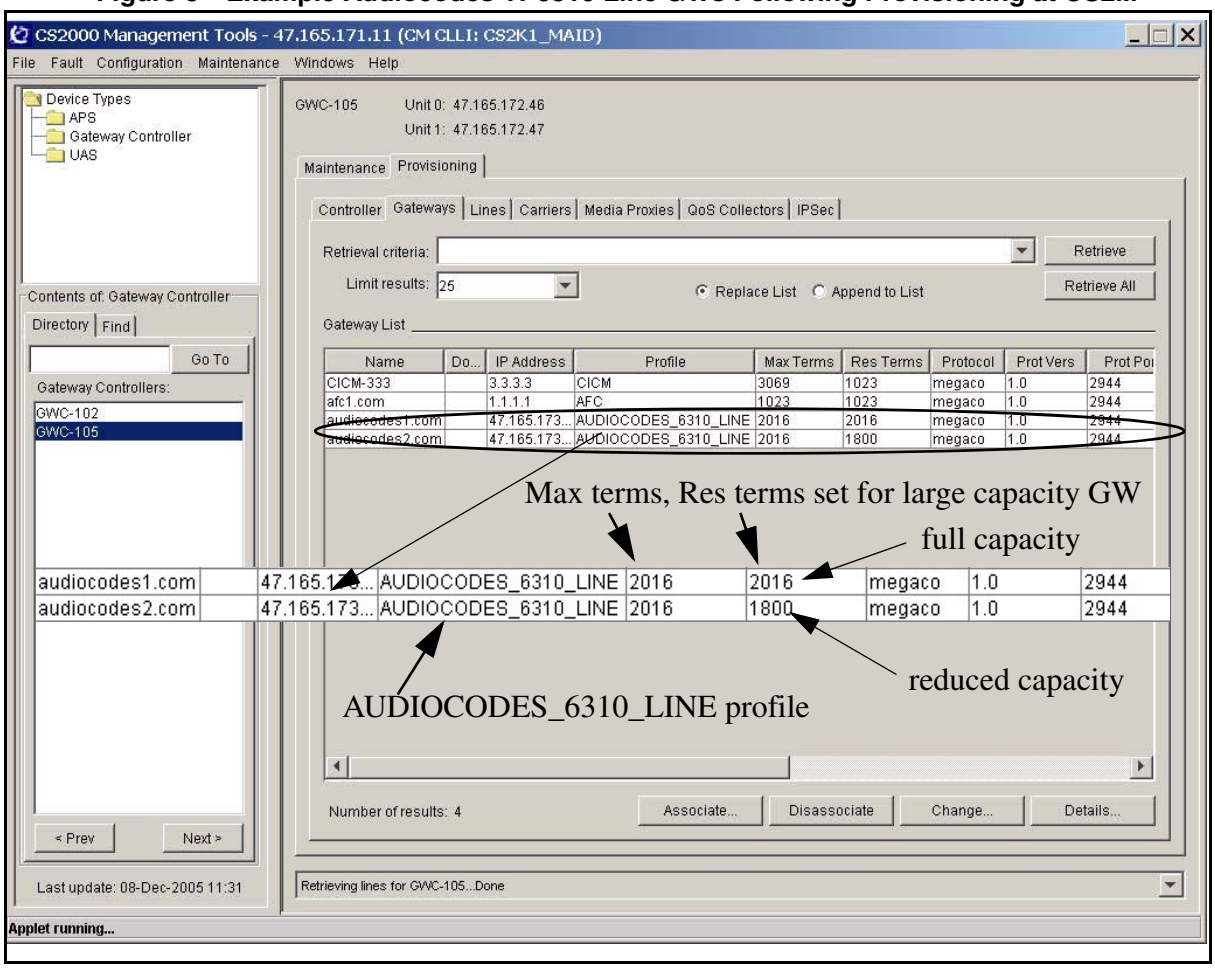
Following successful provisioning of the Audiocodes TP6310 Line GW, the following will have occurred:

- GW will have been created at GWC.
- LGRP entry will have been created at CM.
- GW will exist within CS2M database.
- GW will be displayed at CS2M GUI (upon gateway list refresh).

Initially there will be no endpoints and associated LENs provisioned at the GWC or CM, however the capacity to provision the required number of terminations will have been reserved.

The following figure shows an example of 2 provisioned Audiocodes GW as displayed by the CS2M Gateway List GUI.

Figure 3 Example Audiocodes TP6310 Line GWs Following Provisioning at CS2M



The Audiocodes TP6310 large line GWs when provisioned have LGRPs of size 2048. This will have a direct impact on the number of gateways addressable by a GWC. The rules governing the number of provisionable GWs with relation to LGRP size are as follows:

- 1024 size LGRPs - Max 27 large line GWs.
- 2048 size LGRPs - Max 13 large line GWs.
- GWs comprising multiple LGRPs are considered to be multiple GWs from the perspective of this discussion.
- Number of supported GWs independent of reserved terminations.
- Total number provisionable large line GWs between 13 and 27 dependant on mix of 1024 and 2048 size LGRPs.

As the Audiocodes TP6310 large line GW requires the provisioning of a 2048 size LGRP, this will reduce the capability of a given GWC to support new GWs by 2.

39.2.3 Deprovisioning Of Audiocodes TP6310 Large Line GW

Deprovisioning of the Audiocodes TP 6310 Large Line GW uses the standard "Disassociate Media Gateway" GUI interface or the disassocmg XML interface from OSSGate.

As this type of gateway is treated as 3rd party for endpoint creation and deletion the user must ensure that all endpoints for the target GW are removed from the system prior to attempting the deletion operation.

39.2.4 Modifying An Audiocodes TP6310 Large Line GW

The only change interface supported in this release is the "change gateway capacity" interface to modify the number of reserved terminations.

Specifying Root / Adjacent ITRANS zones is currently unsupported for the Audiocodes TP6310 Large Line GW.

39.2.5 Provisioning Of Audiocodes TP6310 Large Line GW - OSSGate XML Interface

Provisioning of the Audiocodes TP6310 Large Line GW using the OSSGate XML interface is unchanged by this feature. Please refer to the OSSGate documentation for details of this interface.

39.2.6 Querying Of Provisioned GWs via the OSSGate XML Interface

The response from the queryMG interface is unchanged by this feature. Please refer to the OSSGate documentation for details of this interface.

39.2.7 Provisioning Endpoints For The Audiocodes TP6310 Large Line GW

Before an Audiocodes TP6310 Large Line GW endpoint may be used it must first be pre-provisioned. The pre-provisioning is a manual activity using the OSSGate or bulk provisioning tool functionality introduced by feature A00007072 to support 3rd party GW endpoint provisioning.

The reader of this document should be fully conversant with the information specified in the FN of feature A00007072 and the OSSGate user guide as we will only cover that information of direct relevance to the Audiocodes TP6310 Large Line GW here.

Examples for the addition and deletion of an endpoint associated with an Audiocodes TP6310 Large Line GW are shown in Figure 4 and Figure 5.

Figure 4 Example addLineEndpoint Request For Audiocodes TP6310 Large Line GW

```
<?xml version=”1.0” encoding=”UTF-8”?>
<CommandList>
        <Command>
                <Interface>cs2kCfgMgrIf</Interface>
                <Methods>
                <addLineEndpoint usn=”1” version=”1.0”>
                <Parameters>
                <mgUIName>audiocodes1.com</mgUIName>
                <endpointName>tp/2016</endpointName>
                <circuitNumber>2015</circuitNumber>
                <cardCode>GWLPOT</cardCode>
                <padGroup>PKNIL</padGroup>
                <ground>N</ground>
                </Parameters>
                </addLineEndpoint>
                </Methods>
        </Command>
</CommandList>
```

Multiple addLineEndpoint operations may be submitted as part of a single XML document

Figure 5 Example delLineEndpoint Request For Audiocodes TP6310 Large Line GW

```
<?xml version=”1.0” encoding=”UTF-8”?>
<CommandList>
        <Command>
                <Interface>cs2kCfgMgrIf</Interface>
                <Methods>
                <delLineEndpoint usn=”1” version=”1.0”>
                <Parameters>
                <mgUIName>audiocodes1.com</mgUIName>
                <endpointName>tp/2016</endpointName>
                </Parameters>
                </delLineEndpoint>
                </Methods>
        </Command>
</CommandList>
```

Multiple delLineEndpoint operations may be submitted as part of a single XML document

39.2.7.1 Audiocodes M8K Shelf Brief Overview

The Audiocodes M8K GW shelf is comprised of one or more STM-1 / OC-3 TP6310 or lower capacity TP1610 cards.

The TP1610 can be used to support Trunk carriers and makes use of the existing AUDIOCODES profile (2 x AUDIOCODES profile trunk GWs per TP1610 card). This will not be discussed further as it is existing functionality.

The TP6310 can be configured for use as either a Trunk or a high capacity Large Line GW. The configuration of the TP6310 as a Trunk GW is considered later in this document - see section 12.2.14 on page 608. The remainder of this section refers only to the use of the TP6310 as a Large Line GW.

When operating in line mode each TP6310 card can terminate 2016 POTS type lines via additional external demuxing.

Each TP6310 card in the Audiocodes M8K shelf operates as a separate independent gateway with its own unique IP address / protocol port, and will therefore be treated as a separate gateway by the CS2M and subtended GWC modules. Therefore the Audiocodes TP6310 Large Line GW as described by this document refers to a single TP6310 card configured within an M8K shelf to terminate lines.

The CS2M may have multiple Audiocodes TP6310 GWs provisioned which are in fact all line cards within a single Audiocodes M8K shelf. This is analogous to multiple independent CICM GWs occupying a SAM21 shelf.

The Audiocodes TP6310 Large Line Gateway must be configured via the Audiocodes element manager to expect the endpoint naming convention and range as present in this document so as to match what the CS2M is expecting to provision.

39.2.7.2 Endpoint Naming Convention

Endpoints as provisioned on the Audiocodes TP6310 Large Line GW will be of the following format:

tp/nnnn where:

- nnnn = endpoint number on card with nnnn in the range 1 - 2016.
- nnnn is not padded (no leading zeros for padding to 4 digits).

As an example the endpoints for a TP6310 Large Line GW will be as follows:

tp/1, tp/2, tp/3.... tp/2014, tp/2015, tp/2016.

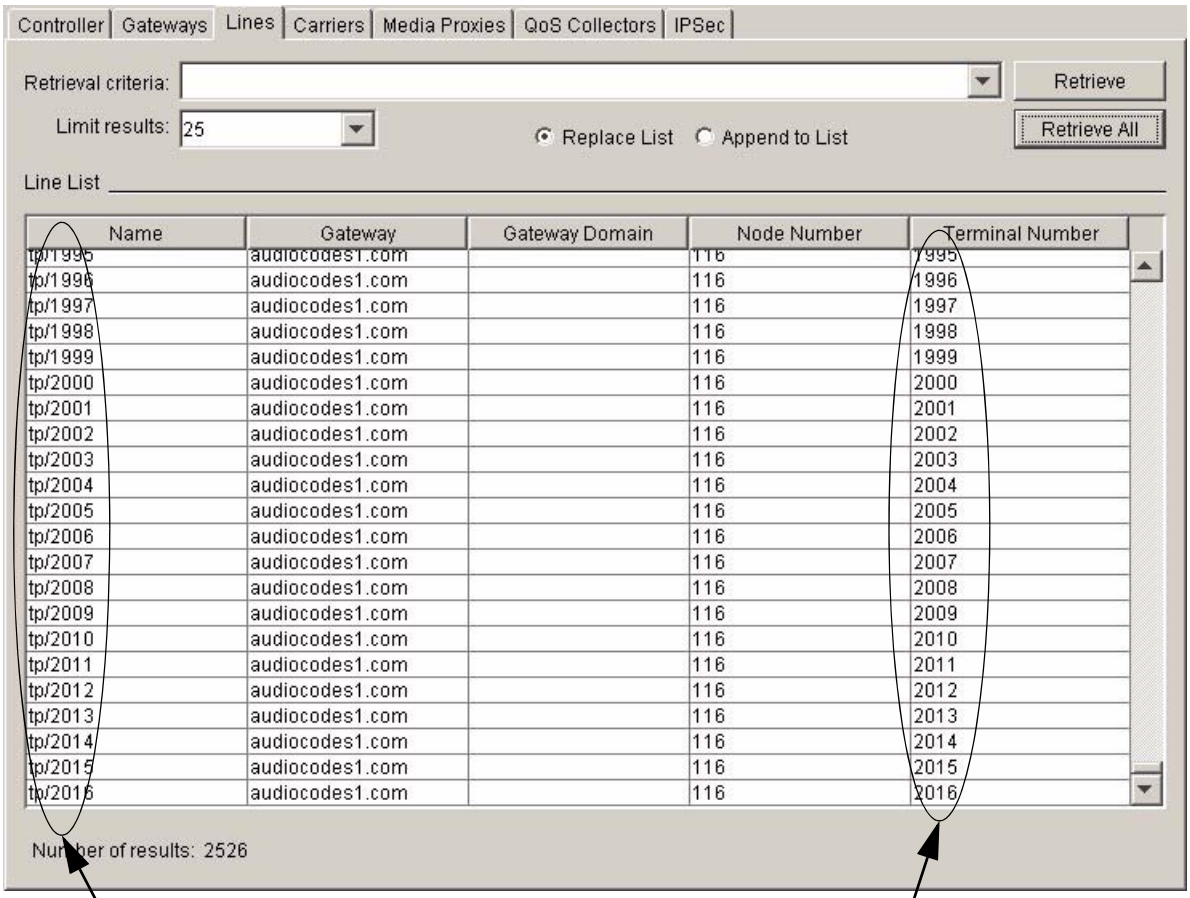
39.2.7.3 Circuit Number Allocation

The 3rd party GW provisioning interface allows flexible allocation of the LEN circuit number (and hence endpoint terminal number) independently of the endpoint name. The circuit number allocated for an endpoint must be unique and in the range 0 - 2046. This identifies directly the LEN to be created.

It is recommended that the circuit number be equal to the endpoint “nnnn” component -1. This will allow for easy correlation of endpoint to LEN and assist with maintenance. For example tp/1 associated with LEN <LGRP> 00 00.

39.2.8 Lines Panel Indication Extended Endpoint Range

Figure 6 Extended Endpoint Range Display At Line List Tab



Due to the larger LGRP size supported for the Audiocodes M8K, additional endpoints are directly addressable. This results in the endpoint range being increased for this GW as opposed to a normal pre SN09.1 GWs such as AFC.

Figure 6 shows the display of additional endpoints for the Audiocodes TP6310 Large Line GW provisioned using a 2048 size LGRP. Supported endpoints will be in the range tp/1 to tp/2016.

> ***Note:*** Total number of possible endpoints is 2047 for the 2048 member LGRP as one TID will be reserved for signaling purposes.

39.2.8.1 Mapping Endpoint to LEN:

The mapping of endpoint to LEN is performed based on the terminal number which in turn is considered GW type independent. For the Audiocodes TP6310 Large Line GW there is no guaranteed logical mapping between the endpoint name and its associated terminal number. This is due to the terminal number being generated from the supplied circuit number at provisioning time.

It is recommended that the circuit number be set equal to the endpoint number - 1 at provisioning time to produce a 1:1 mapping but this is not enforced.

For LENs with LGRPType = LL_3RDPTY_2K the endpoint format is as follows:

LENs will be of the format <Node Name> <TT> <tt> where:

- Node Name - LGRPINV entry as auto generated on GW addition. Formed from <Site> <Frame> <Unit> where <Site> is used specified on GW addition, frame and unit are auto allocated.
- TT is in range 00 .. 20
- tt is in the range 00 .. 99 where TT < 20 and 00 .. 46 where TT = 20

For example with LGRP = “LG2K 01 5” the possible range of LENs for the LGRP as a whole will be:

LG2K 01 5 00 00 - LG2K 01 5 20 46 dependant on circuit number allocation.

It is recommended that the circuit number be tied to the endpoint name which would mean the range of recommended LENs for an Audiocodes TP6310 Large Line GW is:

LG2K 01 5 00 00 - LG2K 01 5 20 15.

The corresponding Terminal numbers will be as follows:

terminal number = (TT x 100) + tt + 1

And the reverse mapping will be:

TT = terminal number - 1 - tt

tt = (terminal number - 1) MODULUS 100

Assuming the recommendation on allocating circuit numbers at endpoint provisioning is followed, the endpoint name would be directly generated from the terminal number as:

tp/<terminal number>.

39.2.9 Line Provisioning Using the SERVORD+ Interface

Line provisioning using the servord interface is unchanged by this feature. Lines may be provisioned using either LENs or endpoints as specified in the OSSGate documentation.

The OSS must however take into account the extended endpoint / LEN range introduced for the Audiocodes TP6310 Large Line GW.

39.2.10 Audits - CS2K and Line Audit

The CS2K Data integrity audit and Line Data integrity Audit are unchanged by this feature.

Please be aware that the Line Data Integrity Audit will report a greater range of lines where an Audiocodes TP6310 Large Line line GW is provisioned due to the greater capacity supported by this GW type.

39.2.11 Line Maintenance Manager

There will be no functional changes to the Line Maintenance Manager introduced by this feature. Currently Large Line H.248 gateways are unsupported by the Line Maintenance Manager. This restriction will apply equally to the Audiocodes TP6310 Large Line gateway.

39.2.12 Bulk Provisioning Tool

The bulk provisioning tool used for provisioning line data fill will not be impacted by this feature. Line provisioning for the Audiocodes TP6310 Large Line GW is supported as is, however the range of valid LENs / endpoints is increased in accordance with the additional endpoint / LEN range.

39.2.13 Third Party Gateway Profile Certificate Changes

Third party gateway certificate profiles produced to support new large line type gateways generated in accordance with the guidelines for feature A00007071 and A00007072 are now required to indicate the size of CM LGRP to be generated to support the new GW. In addition the LGRP generated may be 1 of 2 sizes:

1024 - identical to all releases prior to SN09.1

2048 - double sized for higher capacity large line GWs.

A new tag value pair <LgrpSize>value</LgrpSize> is introduced to the certificate XSD to carry size information. This should be set to 1024 or 2048. The higher capacity size of 2048 should only be used where absolutely necessary as this will reduce the provisionable number of GWs that can be associated with a given GWC.

The value of the <LgrpType> tag value pair must be set to indicate the type of LGRP to be generated at the CM. For 3rd party large line GWs this will be

either LL_3RDPTY or LL_3RDPTY_2K dependant on whether a size of 1024 or 2048 is required.

The certificate files for all new 3rd party large line GWs should therefore contain either of the following entries:

Figure 7 LGRP of Size 2048: Between 1 and 2047 Endpoints Supported

```
<EndpointType>thirdPartyLens</EndpointType>
 <LgrpType>LL_3RDPTY_2K</LgrpType>
 <LgrpSize>2048</LgrpSize>
```

Figure 8 LGRP of Size 1024: Between 1 and 1023 Endpoints Supported

```
<EndpointType>thirdPartyLens</EndpointType>
 <LgrpType>LL_3RDPTY</LgrpType>
 <LgrpSize>1024</LgrpSize>
```

Note 1: LgrpSize tag should directly follow LgrpType

Note 2: If the LgrpSize tag is not present in a certificate the default size of 1024 is assumed to ensure backwards compatibility with existing certificates.

Note 3: Specifying LgrpSize for a non large line GW will result in a corrupt profile alarm being raised and the certificate will not be loaded.

39.2.14 Provisioning Of Audiocodes TP6310 Trunk GW - GUI Interface

The Audiocodes TP6310 card when provisioned as a Trunk GW can be considered as a higher capacity version of the existing Audiocodes Trunk GW as supported in both this and prior releases.

All functionality provided by the existing Audiocodes GW profile is adopted, with the range of possible carriers being increased due to the larger capacity offered by the OC-3 / STM-1 interface supported by this card.

A new gateway profile "AUDIOCODES_6310_TRUNK" is introduced by this feature to support the provisioning of the TP6310 as a Trunk GW. On selecting the "AUDIOCODES_6310_TRUNK" profile the Associate Media Gateway dialog will be populated as follows:

Figure 9 CS2M Assoc. Media Gateway GUI Population For TP6310 Trunk GW

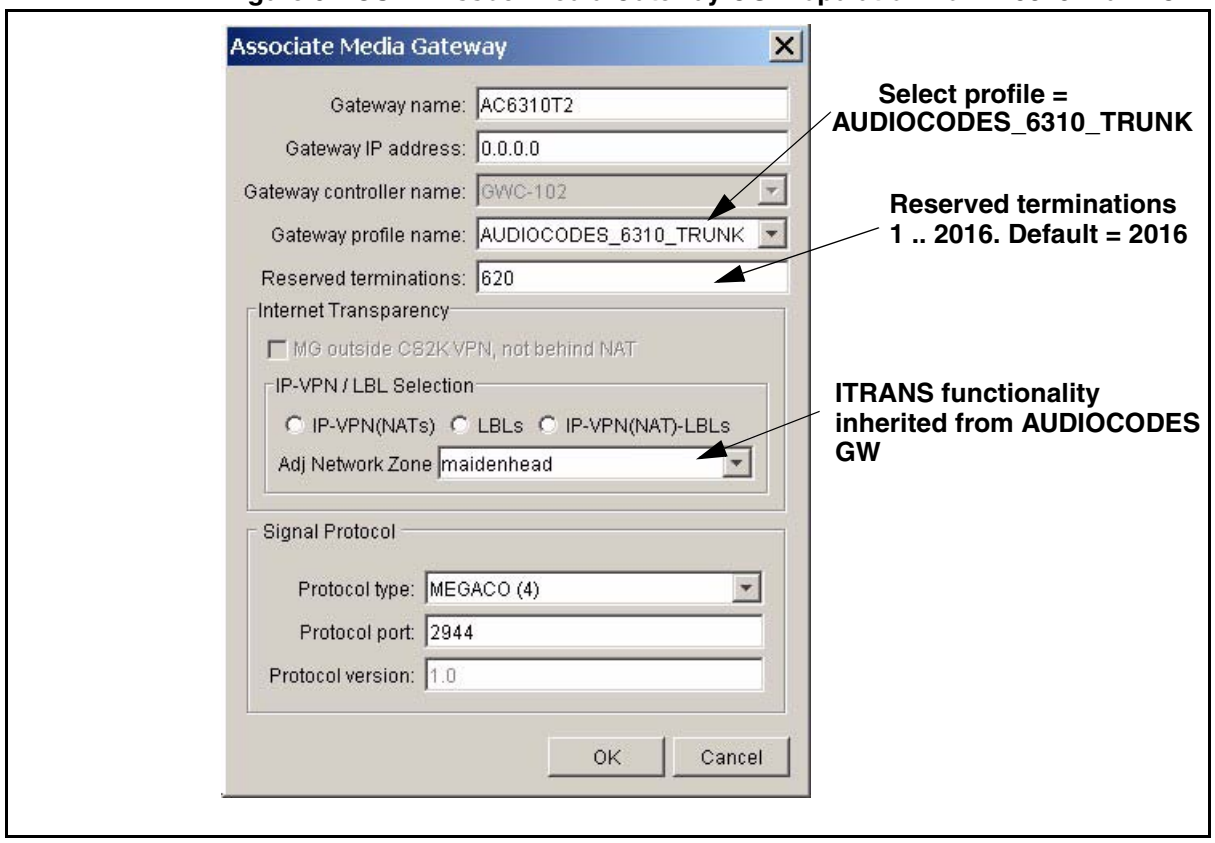


Table 2 Associate Media Gateway Field Population

Field	Contents
Gateway name	Provisioned GW Name. Max 32 characters. Upper case alphanumerical characters only.
Gateway IP address	IP address for Audiocodes GW - or 0.0.0.0 if behind a NAT / LBL
Gateway controller name	GWC-nnn Name of a valid GWC provisioned with a large lines supporting profile.
Gateway profile name	AUDIOCODES_6310_LINE for TP6310 card as large line GW
Reserved terminations	In range 1 .. 2016. Defines number of terminations to reserve for use with this GW. If the field is left empty the default behaviour is to reserve 2016 terminations. As DS1 carriers require 24 terminations and E1 carriers 31 terminations the actual number of reserved terminations should form a multiple of 24 or 31 to avoid wastage. Note: A fully equipped TP6310 Trunk GW with E1 carriers will require 1953 terminations.
Adj Network Zone	ITRANS network zone GW is adjacent to if behind a NAT / LBL.
Protocol type	MEGACO - H.248
Protocol port	defaults to 2944 but may be edited if desired
Protocol version	Fixed to version 1.0

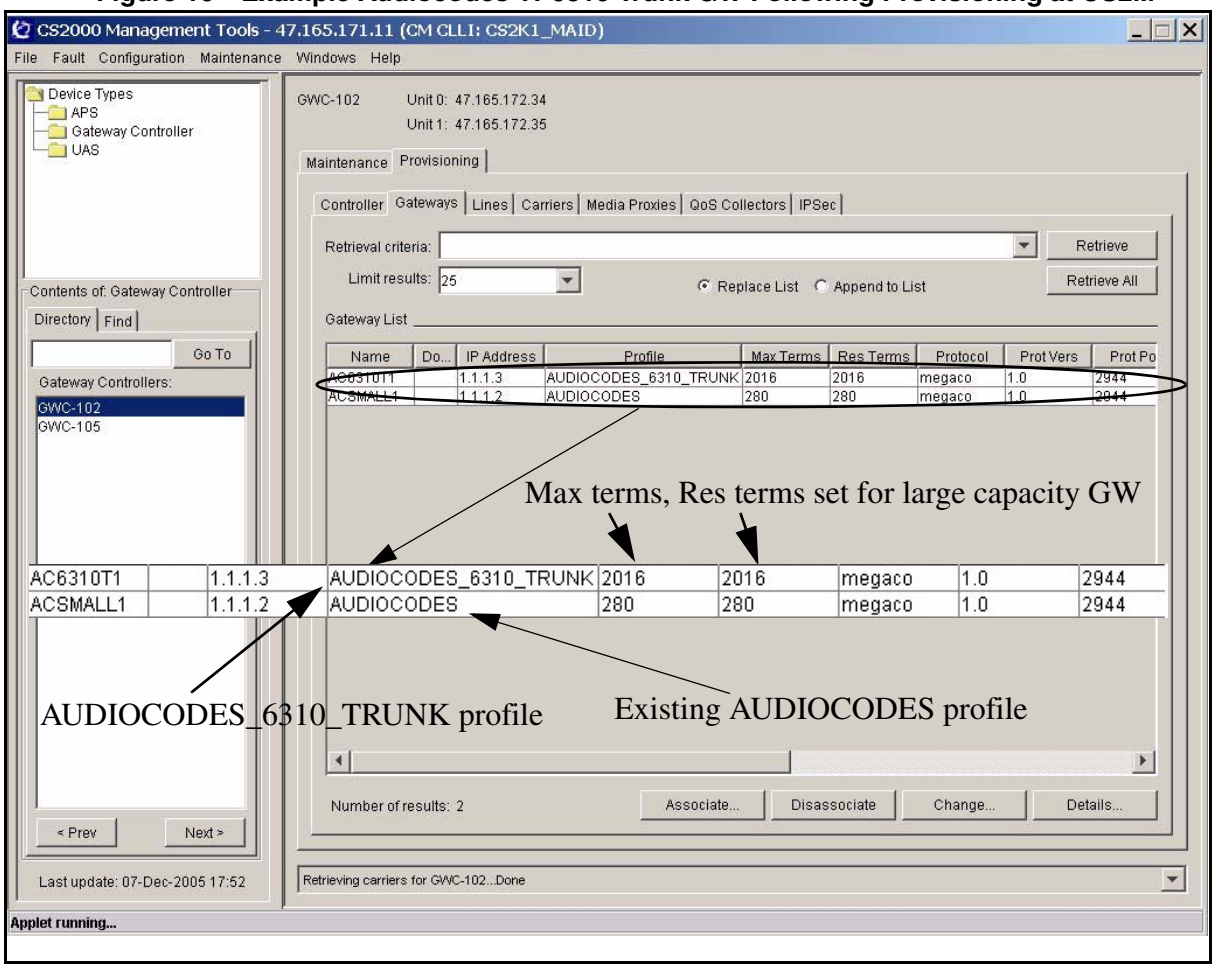
Following successful provisioning of the Audiocodes TP6310 Line GW, the following will have occurred:

- GW will have been created at GWC.
- GW will exist within CS2M database.
- GW will be displayed at CS2M GUI (upon gateway list refresh).

Initially there will be no carriers provisioned at the GWC or CM, however the capacity to provision the required number of carrier terminations will have been reserved.

Figure 10, on page 610 shows an example of 2 provisioned Audiocodes GW as displayed by the CS2M Gateway List GUI.

Figure 10 Example Audiocodes TP6310 Trunk GW Following Provisioning at CS2M



39.2.15 Deprovisioning Of Audiocodes TP6310 Trunk GW

Functionality is identical to existing Audiocodes GW.

39.2.16 Modifying An Audiocodes TP6310 Large Line GW

Functionality is identical to existing Audiocodes GW.

39.2.17 Provisioning Of Audiocodes TP6310 Large Line GW - OSSGate XML Interface

Functionality is identical to existing Audiocodes GW.

39.2.18 Querying Of Provisioned GWs via the OSSGate XML Interface

Functionality is identical to existing Audiocodes GW.

39.2.19 Provisioning Carriers For The Audiocodes TP6310 Trunk GW

The Audiocodes TP6310 Trunk GW supports the provisioning of either E1 or DS1 carriers based on market fit. The trunk range is a super set of that supported by the existing Audiocodes profile.

Carriers may be added / deleted using the existing addCarrier interfaces from either the CS2M GUI or the OSSGate interface.

39.2.19.1 E1 Carrier Provisioning

E1 Carrier support is as follows:

- Carrier range: E1/01 ... E1/63
- Optional DPNSS IID range: 1 .. 63
- Each E1 carrier supports 31 terminations and the appropriate number of terminations must be reserved in advance. A fully equipped TP6310 with E1 carriers will require 63 x 31 = 1953 terminations.

39.2.19.2 DS1 Carrier Provisioning

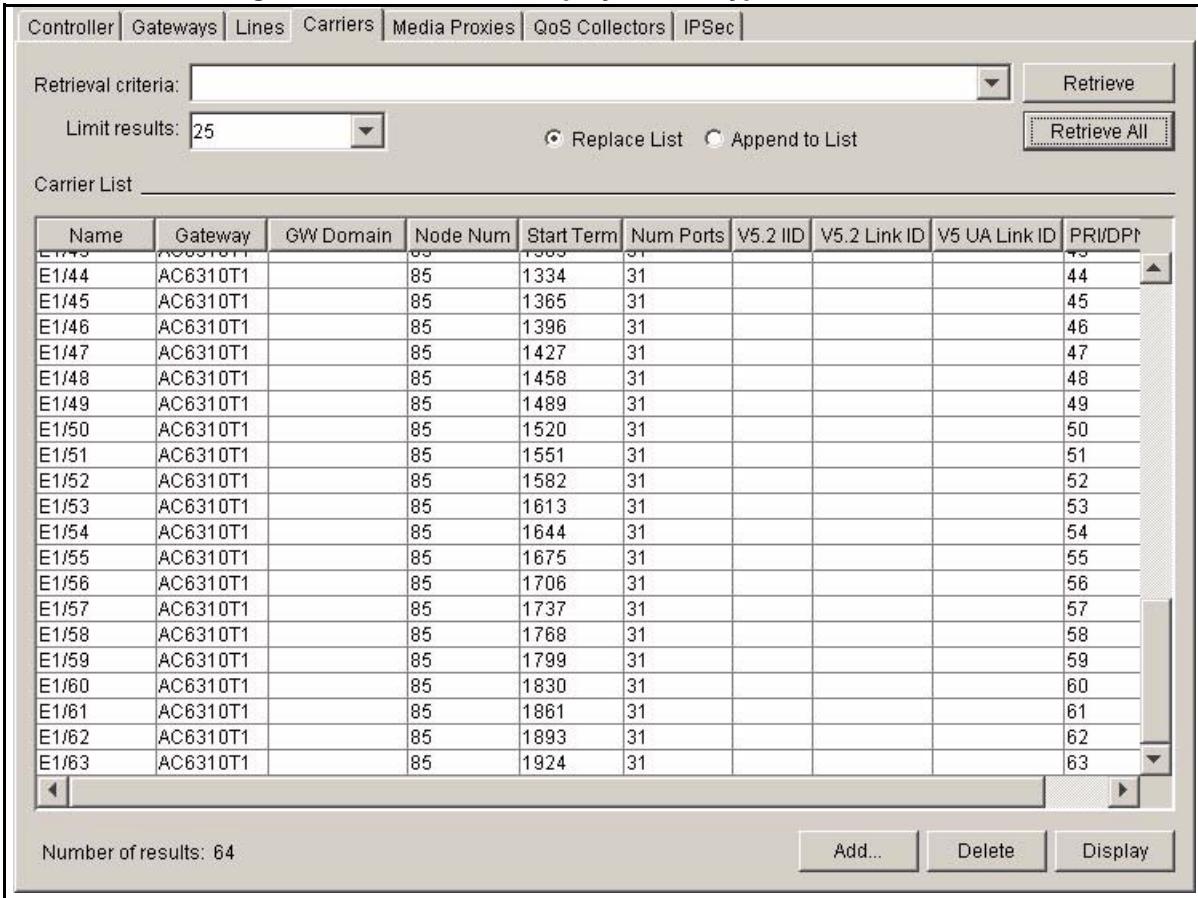
DS1 Carrier support is as follows:

- Carrier range: DS1/01 .. DS1/84
- Optional PRI IID range: 0 .. 31
- PRI IID value must be unique for a given GW.
- Each DS1 carrier supports 24 terminations and the appropriate number of terminations must be reserved in advance. A fully equipped TP6310 with DS1 carriers will require 84 x 24= 2016 terminations.
- PRI IID range upper bound may be set in the range 32 .. 63 as functionality is shared with DPNSS IID although the extended range is not supported.

39.2.20 Carrier Panel - E1 Carriers For Audiocodes TP6310 Trunk GW

The following figure shows the carrier list panel displaying E1 type carriers for an Audiocodes TP6310 Trunk GW.

Figure 11 Carrier List Display For E1 Type Carriers



Carrier names are an extension of that support for the existing Audiocodes GW

39.2.21 Data Logging

There are no changes to data logging associated with this feature.

39.3 Hardware Requirements or Dependencies

This feature requires the presence of an Audiocodes M8K shelf equipped with one or more TP6310 cards for line GW use. Where trunk GW use the M8K should be equipped with either TP1610 or TP6310 cards as appropriate.

39.4 Software Requirements or Dependencies

39.4.1 SN09FF Formal Delivery

Software should be at the following release level or later:

GWC: Gx091FC

CM: PSNW090FC + 2K LGRP Support Patch

CS2M: SESM_091_FC

Note: FC software versions will not be known until the end of the SN09.1 release.

39.5 Limitations and restrictions

Provisioning of large line GWs with 2048 size LGRPs reduces number of provisionable GWs at the GWC.

CM must be patched with the 2K LGRP patch when running the PSNW090FC load (SN09FC). For SN10 onwards this patch will not be required.

39.6 Interactions

N/A

39.7 Glossary

Term	Definition
CM	Call Server 2000 Switch
CS2M	Call Server 2000 Management Platform
DNS	Directory Naming Service
ETSI	European Telecom Standards Institute
GUI	Graphical User Interface
GW	Gateway
GWC	Gateway Controller
HASU	Hardware Assigned Software Unassigned
LEN	Line Entity
LGRP	Line Group
OSS	Higher Level Management Platform
POTS	Plain Ordinary Telephone Service
TID	Termination ID
XML	External Markup Language

40: Functional Description (FN): A00013286

40.1 Feature name and Feature ID

A00013286: Core Flex Large Line GWC Prof (Ph1)

40.2 Description

This feature is intended to address the following requirement:

- Add generic support for 2048 size LGRPs.

The current support for large line GWs has the following restrictions:

LGRPs are always a fixed 1024 elements regardless of the number of endpoints that a GW supports and the actual number of reserved terminations. Currently the available GWC TID size for subtending nodes other than trunks is 27000. So a maximum of 26 LGRPs can be configured per GWC if the existing LGRPs (1024) are used.

Due to time scale and resources issues it is intended that this feature will only address the following issue - specifically adding support for a 2047 size LGRP to be used initially in conjunction with the Audiocodes M8K GW. With the introduction of the new LGRP type, 13 to 27 LGRPs can be provisioned per GWC.

As part of this activity, the following changes will be made:

- Creation of a new LGRP type, LL_3RDPTY_2K which will support 2047 endpoints.
- Enhanced LNINV table to support 2047 LENs for the newly created LGRP type.

The new lgrp is an enhancement of the existing lgrp, LL_3RDPTY. The major difference between the newly created LGRP type, LL_3RDPTY_2K and the existing 3rd party profile, LL_3RDPTY is that, the new type supports 2047 lines per LGRP whereas the existing type supports only 1024 lines per LGRP. Total number of possible endpoints is 2047 for the 2048 member LGRP as one TID will be reserved for signaling purposes.

40.2.1 LGRP Type Data - Table LGRPINV

Table LGRPINV is an existing table that is used to associate a LGRP type to a gateway. This activity shall allow support of a new LGRP type, LL_3RDPTY_2K. The new type will support large line gateways with 2047 endpoints. Total number of possible endpoints is 2047 for LL_3RDPTY_2K as one TID will be reserved for signaling purposes.

The following figure shows sample datafill for table LGRPINV.

Figure 1 Prompting sequence and Range values for LGRPINV table.

```
TABLE: LGRPINV
>add
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
GRPNO:
>LG2K 25 0
SRVRNAME:
>gwc 24
GRPTYPE:
TYPE OF GRPTYPE IS LGRP_TYPE
TYPE IS LGRP_TYPE {S,M,C,LL_3RDPTY,CALIX_C7,SSDPL, LL_3RDPTY_2K}
GRPTYPE:
>LL_3RDPTY_2K
LGRPOPTS:
>$
WARNING: Adding tuples MUST be done via SESM node provisioning
      to avoid data mismatch between the CS2K and SESM components!
CAUTION: Confirming the operation could result in an impact to service.
TUPLE TO BE ADDED:
LG2K 25 0 GWC 24 LL_3RDPTY_2K $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
```

40.2.2 LEN Entry - Table LNINV

In LNINV table 2047 LEN entries can be made corresponding to the new LGRP type, LL_3RDPTY_2K. The slots/drawer and circuit ranges supported for the new LGRP type are given below.

Slot - 0 - 20

Circuits - 00 - 99 for slots 0 - 19

00 - 46 for slot 20

The following figure shows sample tuple for table LNINV. The two tuples shown are the boundary conditions for the LGRP type, LL_3RDPTY_2K.

Figure 2 Sample LNINV Tuples

```
LEN                  CARDCODE  PADGRP  STATUS  GND  BNV  MNO  CARDINFO
-------------------- --------- ------- ------- ---- ---- ---- ---------

LG2K 25 0 00 00      RDTLSG    NPDGP   HASU    N    NL   N    NIL

LG2K 25 0 20 46      RDTLSG    NPDGP   HASU    N    NL   N    NIL
```

40.3 Hardware Requirements or Dependencies

N/A

40.4 Software Requirements or Dependencies

This feature requires the Core load to be a succession load greater than or equal to SN09FF. The required GWC load is GC09 and the CS2M load should be CS2M9.1 or greater.

40.5 Limitations and restrictions

N/A

40.6 Interactions

N/A

40.7 Glossary

Term	Description
GW	Gateway
GWC	Gateway Controller
LGRP	Logical Group

Fault Management (FM)

Introduction

This chapter describes impacts to fault management, such as logs and alarms, for the features planned for this release. Only those features with fault-management impacts are listed.

Featid	Title
A000006663.AB02	DDRM Alarms and Audits
A000008556.AA35	SIP Lines Core OAMP support
A00009120.AA17	Multi-Time Zone Enhancements
A000009245.AA12	Succession Test Trunks: T904 Support
A00009282	MG9KEM - International ESA and MLPP Support

1: Fault Management (FM): A00006663

1.1 Feature Name

DDRM Alarms and Audits

1.2 Fault management strategy

Hardware failure alarm messages for DDRM produces PM179 H/W exception report logs on DMS. Reason of the fault can be viewed from MAPCI maintenance level via QUERYPM FLT command. The faulty DDRM hardware is detected in this way and it should be corrected to remove the fault condition on DDRM node.

1.3 Fault management tools and utilities

MAPCI maintenance tools are employed as fault management tools and utilities for DDRM node.

1.4 Logs

1.4.1 Explanation

Log Title: PM179 HW EXCEPTION REPORT

Name: PM HW EXCEPTION REPORT

Description: PM hardware fault reported.

Event type: Severity depends on hardware fault type.

1.4.2 Format

Refer to DMS-100 MMP, Log Report Reference Manual Volume 6 of 7.

1.4.3 Field descriptions

Refer to DMS-100 MMP, Log Report Reference Manual Volume 6 of 7.

1.4.4 Action

Follow the standard procedures for maintenance of a faulty hardware on a PM

1.4.5 Associated Operational Measurements or Performance Measurements

No OM or PM is affected by this log in this feature.

1.5 Alarms

DDRM hardware alarms are expressed in terms of unit/node alarms because they lead to unit/node malfunction.

DDRM hardware fault alarms are maintained through MAPCI tool.

Alarm reason information is displayed with QueryPM FLT command.

To remove the alarm condition, related hardware fault must be fixed. PM179 HW Exception Report Log is generated with alarms.

2: Fault Management (FM): A00008556

2.1 Feature Name

SIP Lines Core OAMP support

2.2 Fault management strategy

The fault management information is provided using logs. The logs are generated due to maintenance and provisioning operations. In addition to these logs, the logs are generated when a NCAS link is established and when it is taken down. This feature uses the existing framework to add new logs.

2.3 Fault management tools and utilities

The LOGUTIL command interpreter is the utility used in the CS2K Core software. This utility will provide access to the log information. All existing tools and utilities are applicable in case of CS2K Core software.

2.4 Logs

The following logs are added as a part of this activity:

- SCPL100-It is generated when a NCAS link is established between Core and CS2KSS.
- SCPL200-It is generated when a NCAS link is lost between Core and CS2KSS.

2.4.1 Log Title/Log ID: SCPL100

2.4.1.1 Formats

- The format of SCPL100 log is

<Switch ID> SCPL100 <DATE> <TIME> INFO NCAS LINK UP

NCAS LINK FOR INSTANCE NUMBER &I CAME UP

DUE TO &25A

Example:

RTP308AS SCPL100 OCT01 12:54:31 7510 INFO NCAS Link UP

NCAS LINK FOR INSTANCE NUMBER 1 CAME UP

DUE TO COMMUP

2.4.1.2 NTSTD
Not Applicable.

2.4.1.3 SCC2
Not Applicable.

2.4.1.4 Syslog
Not Applicable.

2.4.1.5 SNMP
Not Applicable.

2.4.1.6 Explanation

- The CS2K server listens for an establish message from the CS2KSS. This establish message is a kind of notification received from the CS2KSS server.
- When a COMMUP notification is received by the application, an acknowledgement message will be sent to the CS2KSS. A corresponding log (SCPL100) is generated on the core side.

2.4.1.7 Field descriptions
There are no fields in the log. The string is self explanatory.

2.4.1.8 Action
Check the communication between the CS2K and CS2KSS.

2.4.1.9 Associated Operational Measurements or Performance Measurements
None.

2.4.1.10 Additional information
N/A

2.4.2 Log Title/Log ID: SCPL200

2.4.2.1 Formats

- The format of SCPL200 log is

<Switch ID> SCPL200 <DATE> <TIME> INFO NCAS LINK DOWN

NCAS LINK FOR INSTANCE NUMBER &I WENT DOWN

DUE TO &25A

Example:

RTP308AS SCPL200 OCT01 12:54:31 7510 INFO NCAS LINK DOWN

NCAS LINK FOR INSTANCE NUMBER 1 WENT DOWN

DUE TO SENDFAILURENOTIFICATION

2.4.2.2 NTSTD

Not Applicable.

2.4.2.3 SCC2

Not Applicable.

2.4.2.4 Syslog

Not Applicable.

2.4.2.5 SNMP

Not Applicable.

2.4.2.6 Explanation

- When a NCAS link is lost, the re-initiation of the NCAS link will be done from CS2KSS. The link is not supposed to be established from the core side. When a NCAS link is lost, a corresponding log(SCPL200) is generated on the core side.
- The core gets notified when a NCAS link is taken down in one of the following ways:
  - A STATUSCHG notification is received with status as SCTP_SHUTDOWN_RCVD and event as COMM_DN.
  - A COMMLOST notification is received.
  - A COMMERROR notification is received.
  - A SENDFAILURENOTIFICATION is received.

2.4.2.7 Field descriptions

There are no fields in the log. The string is self explanatory.

2.4.2.8 Action

Check the communication between the CS2K and CS2KSS.

2.4.2.9 Associated Operational Measurements or Performance Measurements

None.

2.4.2.10 Additional information

N/A.

2.5 Alarms

No new alarm added. This section is not applicable.

2.6 Related documentation

Appropriate NTP contains the details of various existing logs.

3: Fault Management (FM): A00009120

3.1 Feature Name

Multi-Time Zone Enhancements

3.2 Fault management strategy

Uses existing CS2K core fault management strategy

3.3 Fault management tools and utilities

3.3.1 Faults, Alarms and Logs

LOGUTIL level in CI

3.4 Logs

Log Title/Log ID: LINE125. LINE126, MCT103, MCT105

3.4.1 Formats

Note: Modification to DMS core logs only. Logs LINE125 and LINE126 appear in both North American and International products. Logs MCT103 and MCT105 in international products only.

3.4.1.1 NTSTD

New formats of logs LINE 125 & 126 and MCT 103 & 105

The log report format for LINE125 is as follows:

LINE125 mmmdd hh:mm:ss ssdd INFO TRACE_ON_MALICIOUS_CALL_INI...
len DN dn INCOMING TRUNK = CKT trkid
CALLID = callid
CALLING NUMBER = dn
SOURCE = source
LOCAL TIME = <Time>

An example of log report LINE125 follows:

LINE125 APR01 12:00:00 2112 INFO TRACE_ON_MALICIOUS_CALL_INITIATED
HOST 00 0 19 20 DN 2557811999
INCOMING TRUNK = CKT ICCAMA 15
CALLID = 123456
CALLING NUMBER = 2149975015
SOURCE = CALLING NUMBER

LOCAL TIME = 10:00:00

The format for log report LINE126 is as follows:

LINE126 mmmdd hh:mm:ss ssdd INFO TRACE_ON_MALICIOUS_CALL_ INITIATED
len DN dn
CALLING LINE = LEN len DN dn onitxt
CALLID = callid
LOCAL TIME = <Time>

An example of log report LINE126 follows.

LINE126 APR01 12:00:00 2112 INFO TRACE_ON_MALICIOUS_CALL_INITIATED
HOST 00 0 19 20 DN 2557811999
CALLING LINE = LEN HOST 05 1 15 16 DN 7812001
CALLID = 123456
LOCAL TIME = 10:00:00

The log report format for MCT 103 is as follows:

MCT103 mmmdd hh:mm:ss ssdd INFO TRACE_ONMALICIOUS_CALL_ACTIVATED
CALLING_PARTY : <cli> <originating agent>
CALLED_PARTY : <full number><terminating agent>
CALLING_PARTY_CATEGORY : <cpc>
LOCAL TIME = <Time>

An example of log report MCT 103 follows:

MCT103 APR01 12:00:00 2112 INFO TRACE_ON_MALICIOUS_CALL_ACTIVATED
CALLING_PARTY : CKT ICATUPTRUNK 1
CALLED_PARTY : 2762345 LEN HOST 00 0 01 10
CALING_PARTY_CATEGORY : 16
LOCAL TIME = 10:00:00

The log report format for MCT 105 is as follows:

MCT105 mmmdd hh:mm:ss ssdd INFO TRACE_ONMALICIOUS_CALL_ACTIVATED
CALLING_PARTY : <full number> CKT <originating agent>
CALLED_PARTY : <full number> CKT <terminating agent>
LOCAL TIME = <Time>

An example of log report MCT 105 follows:

MCT105 APR01 12:00:00 2112 INFO TRACE_ON_MALICIOUS_CALL_ACTIVATED
CALLING_PARTY : 9717718745 CKT ICATUPTRUNK 1
CALLED_PARTY : 2762345 CKT ICATUPTRUNK 12
LOCAL TIME = 10:00:00

3.4.1.2 SCC2

n/a

3.4.1.3 Syslog

n/a

3.4.1.4 SNMP

n/a

Table 1 NTSTD/SCC2 Optional Header Fields

Field Name	Used (Y/N)	Value	Fixed/ Variable	type	size	Description
Event Label						
Equipment ID						

Table 2 Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Location:				
Notification Id:				
State:				
Category:				
Cause:				
Time:				
Component Id:				
Specific Problem:				
Description:				
Fabric				
Frame Location				

3.4.1.5 Integrated Element Manager GUI Fields

For each new log, populate the following table with the values displayed in the IEMS Alarm Manager GUI. (Non-legacy logs only). n/a

Table 3 IEMS Alarm GUI Field descriptions

Field	Value
Category	
Severity	
LogName	
LogNumber	
EventType	
EventLabel	
ProbableCause	
SpecificProblem	
BodyText	

3.4.2 Explanation

Description: The new field LOCAL TIME is added to the MCT logs specified to support multiple time zones. It's value is calculated based on the switch time modified by the value in table MULTITM assuming option MTZ is assigned to that line. If the MTZ option isn't assigned it is populated with the switch time.

3.4.3 Field descriptions

One new field added to LINE125 &126 and MCT103 &105

Table 4 Field descriptions

Field	Value	Description
LOCAL TIME	time - hours, minutes, seconds	The local time for this line, which may differ from the callserver time if the line is in a different time zone than the callserver

3.4.4 Action

The new field is present irrespective of whether the line is in a different time zone or not. It is either populated with the amended local time or the switch time.

3.4.5 Associated Operational Measurements or Performance Measurements

n/a

3.4.6 Additional information

n/a

3.5 Alarms

Not applicable

3.6 Related documentation

1. 297-9051-840 - DMS-100 Family MMP Log Report Reference Manual Volume 4 MMP15 and up
2. 297-8021-840P - North American DMS-100 log report reference manual

4: Fault Management (FM): A00009245

4.1 Feature Name

Succession Test Trunks: T904 Support

4.2 Fault management strategy

T904 is a two-way transmitting test. Five logs exist for legacy T904 when the test is executed from the TTP MAP level. They are:

- TSTK940: Test Success
- TSTK941: Communication establishment failure
- TSTK942: Tone transmit and receive failure
- TSTK943: Tone analysis failure on the terminating side.
- TSTK944: Tone analysis failure on the originating side.

The TSTK940 log remains unchanged from legacy. The TSTK941, TSTK942, TSTK943 and TSTK944 logs are reused for succession but may contain new fault reasons. Additional information on these logs are outlined below.

4.3 Fault management tools and utilities

4.3.1 Faults, Alarms and Logs

No change to Fault management tools and utilities.

4.4 Logs

Log Title/Log ID: **TSTTK941** (changed)

4.4.1 Formats

TEST FL

Switch ***+TSTK941 mmmdd hh:mm:ss 6600 FAIL T904 ABORTED

CKT trunk id

Test eq. test equipment id

Reason: text

Example:

TEST FL

RTPY08AY ***+TSTK941 FEB25 09:41:17 6600 FAIL T904 ABORTED

CKT ISNETSIISUPV2OUT 1

Test eq. TESTTRKANN 0

Reason: TESTTRKANN OOS

4.4.2 Explanation

Description: The originating switch generates this log message after the T904 test has failed. The reason varies but occurs when there is no connection between the originating and terminating switches, outpulsing failed, no connection with the test equipment, etc.

4.4.3 Field descriptions

Table 1: Field descriptions

Field	Value	Description
Reason	NO ANNOUNCEMENT TID	No announcement members on free queue
	NO TLINE ACCESS CODE	Cannot find digits to dial for test
	TESTTRKANN DATAFILL	Datafill for the announcement CLLI may be missing from table CLLI
	TESTTRKANN OOS	All announcement members on this AUD node are on busy queue
	TESTTRKANN BUSY	This announcement member is CP busy or CP busy deload
	CONNECTION TIMEOUT	Did not receive an integrity found message in the expected time
	CONNECTION FAULT	If the TLT tasks times out waiting for integrity, it sends an integrity lost message.
	NO TEST EQUIPMENT	GWC reports test equipment unavailable
	TEST EQUIPMENT FAULT	GWC reports test equipment fault
	NO RESPONSE RECEIVED	Receive timeout while waiting for the test results.
	UNEXPECTED MESSAGE	Receive unexpected message
	INVALID RESPONSE MSG	Incoming TLT response not valid for this test

Table 1: Field descriptions

Field	Value	Description
	UNEXPECTED RESPONSE	Incoming tlt result msg not what is expected
	MAX TEST CONNECTIONS	Maximum connections defined in table anns has been reached
	FAR END DISCONNECTED	Receive clear back message from call processing
	HIGH AND DRY	No answer or tone received from far end
	CONNECTION LOST	Receive integrity lost message while waiting for test response.
	SOFTWARE FAULT	Basic software failure
	GWC FAULT	GWC reports GWC internal fault
	NO GATEWAY RESOURCES	GWC reports gateway pool unavailable or busy
	GW RESOURCES INUSE	GWC reports test equipment in use
	GATEWAY UNAVAILABLE	GWC reports gateway unavailable
	GATEWAY FAULT	GWC reports gateway internal fault
	UNKNOWN FAULT	Unknown reason
	GW NO BEARER PATH	AMS does not have a bearer path connected.

Table 1: Field descriptions

Field	Value	Description
	TRK HARDWARE FAILED STOP DIAL SIG RCVD NO START DIAL SIGNAL OUTPULSING TROUBLE INVALID REPLY SUBSCRIBER BUSY ADDRESS INCOMPLETE LINE OUT OF SERVICE FAR-END UNAVAILABLE SWITCH EQP CONGESTED SUBSCRIBER XFERRED	Test call errors where test call did not return a pass. Gets output when outpulsing trouble is identified.

4.4.4 Action

Depending on the reason, check the datafill, verify translations, and verify that trunks (outgoing and incoming) and test trunk announcement are in service.

4.4.5 Associated Operational Measurements or Performance Measurements

N/A

4.4.6 Additional information

None

Log Title/Log ID: **TSTTK942** (changed)

4.4.7 Formats

TEST FL

Switch ***+TSTK942 mmmdd hh:mm:ss 6700 FAIL T904 ABORTED

CKT trunk id

Test eq. test equipment id

Reason: text

Example:

TEST FL

RTPY08AY ***+TSTK942 FEB25 09:45:17 6700 FAIL T904 ABORTED

CKT ISNETSIISUPV2OUT 1

Test eq. TESTTRKANN 0

Reason: F-N UNSTEADY TONE

4.4.8 Explanation

Description: The originating switch generates this log message after the T904 test has failed. It fails when the originating switch receives the answer message, but the tone to/from the terminating switch is not correct.

4.4.9 Field descriptions

Table 2: Field descriptions

Field	Value	Description
Reason	NO TONE DETECTED	Answer received, but no tone detected from far end
	NO TONE AFTER TPT	Test was attempted but the tone was not detected from the far end - assumed that the TPT (test progress tone) was received if max db value is given
	F-N UNSTEADY TONE	Far to near tone is unsteady

4.4.10 Action

Verify all connections. Try other trunk members. Check padding datafill.

4.4.11 Associated Operational Measurements or Performance Measurements

N/A

4.4.12 Additional information

N/A

Log Title/Log ID: **TSTTK943** (changed)

4.4.13 Formats

TEST FL

Switch ***+TSTK943 mmmdd hh:mm:ss 6800 FAIL T904 FAILED

CKT trunk id

Test eq. test equipment id

Reason: text

Example:

TEST FL

RTPY08AY ***+TSTK943 FEB25 09:47:17 6800 FAIL T904 FAILED

CKT ISNETSIISUPV2OUT 1

Test eq. TESTTRKANN 0

Reason: N-F EXCEEDED Q1

4.4.14 Explanation

Description: The TSTK943 log message is generated after the T904 test has failed. The reasons that get displayed occur when the terminator detects limits deviation (Q1 or Q2).

4.4.15 Field descriptions

Table 3: Field descriptions

Field	Value	Description
Reason	N-F EXCEEDED Q1	Near to far tone exceeds Q1 limitation
	N-F EXCEEDED Q2	Near to far tone exceeds Q2 limitation

4.4.16 Action

Verify all connections. Try other trunk members. Check padding datafill.

4.4.17 Associated Operational Measurements or Performance Measurements

N/A

4.4.18 Additional information

N/A

Log Title/Log ID: **TSTTK944** (changed)

4.4.19 Formats

TEST FL

Switch ***+TSTK944 mmmdd hh:mm:ss 6800 FAIL T904 FAILED

CKT trunk id

Test eq. test equipment id

Reason: text

EML = n.n DB F_N DEV = n.n DB

Example:

TEST FL

RTPY08AY ***+TSTK944 FEB25 09:47:17 7000 FAIL T904 FAILED

CKT ISNETSIISUPV2OUT 1

Test eq. TESTTRKANN 0

Reason: F-N EXCEEDED Q2

EML = 0.0 DB F_N DEV = 24.5 DB

4.4.20 Explanation

Description: The TSTK944 log message is generated after the T904 test has failed. The reasons that get displayed occur when the originator detects limits deviation (Q1 or Q2).

4.4.21 Field descriptions

Table 4: Field descriptions

Field	Value	Description
Reason	F-N EXCEEDED Q1	Far to near tone exceeds Q1 limitation
	F-N EXCEEDED Q2	Far to near tone exceeds Q2 limitation

4.4.22 Action

Verify all connections. Try other trunk members. Check padding datafill.

4.4.23 Associated Operational Measurements or Performance Measurements

N/A

4.4.24 Additional information

N/A

4.5 Alarms

N/A

4.6 Related documentation

5: Fault Management (FM): A00009282

5.1 Feature Name

MG9KEM - International ESA and MLPP Support

5.2 Fault management strategy

The standard MG9k EM Fault Management strategy will apply to the faults for this feature. Alarms will be displayed by the MG9K EM Alarm Browser, logged in NT standard format to the SSPFS CUST logs and forwarded to northbound OSS.

5.3 Fault management tools and utilities

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

5.4 Logs and Alarms

No new alarms will be added. A new alarm reason will be generated for ESA download problems from the Core when the timestamp of the Core file is more than 48 hours old.

The alarm will be displayed at the Alarm Browser at the subnet as well as the well as the alarm browser for each corresponding network element. A log is also generated. Both are NE level alarms.

5.4.1 Explanation

5.4.1.1 ESA311

Title: Core Download Failed

Name: ESA

Description: This log is generated by the EM in when a problem is detected when trying to download the datafile from the core.

This new condition is when the Core datafile is more than 48 hours old, indicating that the file on the Core is not being generated nightly.

Severity: Minor

Event type: ESA Core Data Download

5.4.2 Field descriptions

5.4.2.1 ESA311 (nnEsaCoiFault)

Table 1 Field descriptions ESA304

Field	Value	Description
office identification	String	Identifies the switch that generates the log. This field is optional. The maximum length of this field is 12 characters.
alarm	***,**,*, or blank	Indicates the alarm type of the log report. ***=critical, **=major, *=minor, blank = no alarms/warning
threshold	+ or blank	Indicates if a threshold is set for the log report. Plus (+) sign indicates that a threshold was set; if a blank, a threshold was not set.
report identification	AAAA nnn	Identifies the log subsystem that generates the report. This field uses 2-4 alphabetical characters and the number 100-999 of the log report in this subsystem. For this log AAAA= MGC and nnn=600.
day	String	Identifies the day of the week.
mmmmdd	January-December (01-31)	Identifies the month and date the report generates.
hh:mm:ss	00-23 00-59 00-59	Identifies the hour, the minute, and the second the report generates.
zone	PST, EST, MST, CST, AST	Identifies the time zone.
yyyy	0000-9999	Year

Table 1 Field descriptions ESA304

Field	Value	Description
ssdd	0000-9999	Defines a different sequence number for each log report generated.
event type	TBL, INFO, etc	Trouble, Service Summary, State Change, Information, Threshold and Expert. TBL for this log.
event id	String	The Log Title.
NE Number	integer	Number of the NE
NE Name	string	Name of the NE
Fault Type	string	The type of the fault: ESA Community of Interest
nnUemgEventTime	DateandTime	The Date and Time the event occurred in the following format: day mmmmdd hh:mm:ss zone yyyy
nnUemgAlarmSeverity	String	Major
Description	string	Failed to ping members of community of interest

5.4.2.2 ESA312 (Internodal ESA Provisioning Fault)

Table 2 Field descriptions ESA304

Field	Value	Description
office identification	String	Identifies the switch that generates the log. This field is optional. The maximum length of this field is 12 characters.
alarm	***,**,*, or blank	Indicates the alarm type of the log report. ***=critical, **=major, *=minor, blank = no alarms/warning
threshold	+ or blank	Indicates if a threshold is set for the log report. Plus (+) sign indicates that a threshold was set; if a blank, a threshold was not set.

Table 2 Field descriptions ESA304

Field	Value	Description
report identification	AAAA nnn	Identifies the log subsystem that generates the report. This field uses 2-4 alphabetical characters and the number 100-999 of the log report in this subsystem. For this log AAAA= MGC and nnn=600.
day	String	Identifies the day of the week.
mmmmdd	January-December (01-31)	Identifies the month and date the report generates.
hh:mm:ss	00-23 00-59 00-59	Identifies the hour, the minute, and the second the report generates.
zone	PST, EST, MST, CST, AST	Identifies the time zone.
yyyy	0000-9999	Year
ssdd	0000-9999	Defines a different sequence number for each log report generated.
event type	TBL, INFO, etc	Trouble, Service Summary, State Change, Information, Threshold and Expert. TBL for this log.
event id	String	The Log Title.
NE Number	integer	Number of the NE
NE Name	string	Name of the NE
Fault Type	string	The type of the fault: Processing Error
nnUemgEventTime	DateandTime	The Date and Time the event occurred in the following format: day mmmmdd hh:mm:ss zone yyyy
nnUemgAlarmSeverity	String	Major
Description	string	Internodal ESA provisioning failure

5.4.3 Action

ESA304 (nnEsaCoiFault):

Check failure cause in alarm or log text and perform corrective action This will typically require network route troubleshooting. The MG9000 will clear the alarm autonomously once the root cause is fixed.

ESA312 (Internodal ESA provisioning failure):

Check failure log in the alarm or log text (most common is communication failure between the MG9000 EM and the MG9000). Once the root cause is fixed the alarm can be cleared by running and audit on the affected NE, or hitting “Apply” button on the Internodal ESA configuration GUI.

5.4.4 Associated Operational Measurements or Performance Measurements

None.

5.5 Related documentation

1. NORTEL-UEMG-BASE-MIB - MG9000’s Enterprise MIB, contains the Alarm Log Table.

2. PLOA and SLOA Logs and Alarms for UE9kMG EM (DID) - MG9000s design documentation for logs and alarms on the MG9000 Element Manager.

3. Logs and Alarms Strategy for WUA Components - MG9000 Alarm strategy guide - version 1.4

3. Reliable Alarms and Alarm Robustness Design Intent Document (DID) - MG9000 Element Manager design document.

4. PLOA and SLOA Alarm Forwarding to OSS(DSUM) - MG9000 Alarm forwarding feature.

Configuration Management (CN)

Introduction

This chapter describes impacts to configuration management, such as hardware/software requirements, data schemas, and service orders for the International features planned for this release. Only those features with configuration-management impacts are listed.

Featid	Title
A00006664.AB05	DDRM Line Testing
A00007289.AA06	RT Selector Enhancement for Metering
A00008429.AA09	Ring Back When Free (RBWF) Enhancements
A00008477.AA10	Increase size of table MSGRTE
A00008484.AA07	IN Terminating Trigger Feature Interactions
A00008556.AA35	SIP Lines Core OAMP support
A00009037.AA06	CORE - Enhanced ESA for International MG9000
A00009145.AA10	Record Feature Usage
A00009216.AA10	JI-ISUP to Base ETSI ISUP V2 Mapping Enhancement
A00009282	MG9KEM - International ESA and MLPP Support
A00009321.AA15	NMC Code Blocking
A00009322.AA16	Call Lock and Do Not Disturb Enhancements
A00009489.AA11	CHT: Call Waiting Enhancement
A00013275	C&W: CS2M support for variable sized LGRP

1: Configuration (CN): A00006664

1.1 Feature Name

DDRM Line Testing

1.2 Hardware and Software Requirements

N/A

1.3 Initial Configuration

N/A

1.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

1.5 Upgrade Impact

N/A

1.6 Data schema (DS) (CM, MIBS, RDB)

N/A

1.7 Service Orders (SO) (CM & SESM)

N/A

1.8 Software optionality control (SOC)

N/A

1.9 Element Management

N/A

1.10 Command interface changes

This feature affects MMI at LTP and subtending levels (LTPMAN and LTPLTA) when a DDRM line is posted. The affected commands are listed in Table 1, on page 646.

Table 1 New/Changed/Deleted LTP level commands for DDRM lines

Command	NEW/CHANGED/ DELETED	NEW NAME (renamed)	DIRECTORY NAME
Diag	CHANGED		MAPCI;MTC:LNS:LTP
LCO_	CHANGED		MAPCI;MTC:LNS:LTP
Loss	CHANGED		MAPCI;MTC:LNS:LTP;LTPMAN
Noise	CHANGED		MAPCI;MTC:LNS:LTP;LTPMAN
ToneGen	CHANGED		MAPCI;MTC:LNS:LTP;LTPMAN
TstRing	CHANGED		MAPCI;MTC:LNS:LTP;LTPMAN
RlsConn	CHANGED		MAPCI;MTC:LNS:LTP;LTPMAN
MonLTA	CHANGED		MAPCI;MTC:LNS:LTP;LTPLTA
TalkLTA	CHANGED		MAPCI;MTC:LNS:LTP;LTPLTA
LnTst	CHANGED		MAPCI;MTC:LNS:LTP;LTPLTA
VDC	CHANGED		MAPCI;MTC:LNS:LTP;LTPLTA
VAC	CHANGED		MAPCI;MTC:LNS:LTP;LTPLTA
Res	CHANGED		MAPCI;MTC:LNS:LTP;LTPLTA
Cap	CHANGED		MAPCI;MTC:LNS:LTP;LTPLTA
LTA	CHANGED		MAPCI;MTC:LNS:LTP;LTPLTA
Ring	CHANGED		MAPCI;MTC:LNS:LTP;LTPLTA
DgtTst	CHANGED		MAPCI;MTC:LNS:LTP;LTPLTA

1.10.1 Command: Diag

1.10.1.1 Command type: MENU

1.10.1.2 Command target: BRISC

1.10.1.3 Command availability: RES

1.10.1.4 Command description

The Diag command is used to perform an diagnostic test suit on a posted line in the control position that is in the IDL or MB state and to display the results on the LTP screen.

1.10.1.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types.

1.10.1.6 Qualifications and warnings

- The command is applicable for only testable DDRM lines (DRDLCP and DRMLCP).
- Optional parameters are not applicable for DDRM lines.
- The following message is printed for unavailable test cards such as LTT and TMS:

'LTT/TMS test cards are not available in DDRM.'

1.10.1.7 Responses

????????

1.10.1.8 Example

Table 2 Usage example for Diag command

Description of task	Diagnose the posted line.
Command:	diag
MAP response:	NNN ***+LINE100 JUN30 00:44:05 3000 PASS LN_DIAG HOST 03 0 01 01 DN 26216200 DIAGNOSTIC RESULT Card Diagnostic OK ACTION REQUIRED None CARD TYPE DRDLCP

1.10.2 Command: LCO

1.10.2.1 Command type: MENU

1.10.2.2 Command target: BRISC

1.10.2.3 Command availability: RES

1.10.2.4 Command description

The LCO command is used to operate or release the cutoff relay of the line circuit in the control position.

1.10.2.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types. There are no changes to command syntax or functions.

1.10.2.6 Qualifications and warnings

- The command is supported for only DDRM lines with over voltage (DRBLCP, DRDLCP and DRMLCP).

- When the LCO command is entered with o parameter, the line state changes to CUT. When the LCO command is entered with r parameter, the line returns to its previous state.

1.10.2.7 Responses

This command responses on supported DDRM lines in the same manner as for other POTS line types. The following message is printed for unsupported DDRM lines:

'Command is not valid on this type of DDRM line.'

1.10.2.8 Example

Table 3 Usage examples for LCO command

Description of task	Operates the cutoff relay for the line circuit in the control position
Command:	lco o
MAP response:	Cutoff Relay Operated
Description of task	Release the cutoff relay for the posted line
Command:	lco r
MAP response:	Cutoff relay released

1.10.3 Command: Loss

1.10.3.1 Command type: MENU

1.10.3.2 Command target: BRISC

1.10.3.3 Command availability: RES

1.10.3.4 Command description

The LOSS command measures the insertion loss of a test tone sent from the subscriber end of a loop to the switch.

1.10.3.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types. There are no changes to command syntax or functions.

1.10.3.6 Qualifications and warnings

- The RlsConn command released the DDRM line and test resources.

1.10.3.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types.

1.10.3.8 Example

Table 4 Usage example for LOSS command

Description of task	Measure the insertion loss of a test tone
Command:	loss
MAP response:	A number is displayed under the header RESULT for the line in the control position in dBm.

1.10.4 Command: Noise

1.10.4.1 Command type: MENU

1.10.4.2 Command target: BRISC

1.10.4.3 Command availability: RES

1.10.4.4 Command description

The NOISE command measures the C-message weighted circuit noise on a subscriber loop.

1.10.4.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types. There are no changes to command syntax or functions.

1.10.4.6 Qualifications and warnings

- The RlsConn command releases the DDRM line and test resources.

1.10.4.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types.

1.10.4.8 Example

Table 5 Usage example for NOISE command

Description of task	Display the C-message weighted circuit noise on a subscriber loop.
Command:	noise
MAP response:	A number is displayed under the header RESULT for the line in the control position in dBRNC.

1.10.5 Command: ToneGen

1.10.5.1 Command type: MENU

1.10.5.2 Command target: BRISC

1.10.5.3 Command availability: RES

1.10.5.4 Command description

The ToneGen command is used to transmit a tone on a subscriber loop.

1.10.5.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types.

1.10.5.6 Qualifications and warnings

- The command is supported for only testable DDRM lines (DRDLCP and DRMLCP).
- The RlsConn command releases the DDRM line and test resources.
- The metallic option is not available for DDRM lines.

1.10.5.7 Responses

This command responses on supported DDRM lines in the same manner as for other POTS line types.

1.10.5.8 Example

Table 6 Usage examples for ToneGen command

Description of task	Generate a default tone of 1004 Hz, 0 dB to the subscriber loop through the line card.
Command:	tonegen
MAP response:	Requested tone is connected
Description of task	Generate a default tone of 100 Hz, 10 dB to the subscriber loop through the line card.
Command:	tonegen 100 10
MAP response:	Requested tone is connected

1.10.6 Command: TstRing

1.10.6.1 Command type: MENU

1.10.6.2 Command target: BRISC

1.10.6.3 Command availability: RES

1.10.6.4 Command description

The TSTRING command tests the ringing relay in the line card for proper functioning.

1.10.6.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types. There are no changes to command syntax or functions.

1.10.6.6 Qualifications and warnings

- The command is supported for only testable DDRM lines (DRDLCP and DRMLCP).

1.10.6.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types. Exceptional cases are listed below:

- The following message is printed for unsupported DDRM lines:

'Command is not valid on this type of DDRM line.'

1.10.6.8 Example

Table 7 Usage example for TstRing command

Description of task	Test the ringing relay in the line card.
Command:	tstring
MAP response:	TEST PASSED

1.10.7 Command: RlsConn

1.10.7.1 Command type: MENU

1.10.7.2 Command target: BRISC

1.10.7.3 Command availability: RES

1.10.7.4 Command description

The RLSCONN command releases test equipment that is connected to line.

1.10.7.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types. There are no changes to command syntax or functions.

1.10.7.6 Qualifications and warnings

- The command is supported for only testable DDRM lines (DRDLCP and DRMLCP).

1.10.7.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types. Exceptional cases are listed below:

- The following message is printed for unsupported DDRM lines:

'Command is not valid on this type of DDRM line.'

1.10.7.8 Example

Table 8 Usage example for RlsConn command

Description of task	Release the test resources that are used.
Command:	rlsconn
MAP response:	Connections released.

1.10.8 Command: MonLTA

1.10.8.1 Command type: MENU

1.10.8.2 Command target: BRISC

1.10.8.3 Command availability: RES

1.10.8.4 Command description

The MONLTA command connects a monitor circuit to a subscriber line. It establishes a monitor connection between a HSET trunk and a CPB or MB subscriber line via a direct network connection (MB) or a 3-port conference circuit (CPB).

1.10.8.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types.

1.10.8.6 Qualifications and warnings

- Before establishing talk connection, the line state should be Call Processing Busy (CPB), Call Processing Deload (CPD) or Maintenance Busy (MB).

- The monitor connection is released by using LTA RLS command.

1.10.8.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types. Exceptional cases are listed below:

- The state of the line in the control position is not valid for the TalkLTA command (Valid line states are Call Processing Busy (CPB), Call Processing Deload (CPD), Maintenance Busy (MB)). The following message is printed to inform that:

  'Line state INVALID, must be MB or CPB'

- The following message is printed for the command when no 3-port conference circuits are currently available.

  'Conference circuit not available'

1.10.8.8 Example

Table 9 Usage example for TalkLTA command

Description of task	Make a monitor connection.
Command:	monlta
MAP response:	Monitor connected to line

1.10.9 Command: TalkLTA

1.10.9.1 Command type: MENU

1.10.9.2 Command target: BRISC

1.10.9.3 Command availability: RES

1.10.9.4 Command description

The TALKLTA command connects a talk circuit to a subscriber line. It establishes a talk connection between a HSET trunk and a CPB or MB subscriber line via a direct network connection (MB) or a 3-port conference circuit (CPB).

1.10.9.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types.

1.10.9.6 Qualifications and warnings

- The battery option is not available for DDRM lines.

- Before establishing talk connection, the line state should be Call Processing Busy (CPB), Call Processing Deload (CPD) or Maintenance Busy (MB).
- The talk connection is released by using LTA RLS command.

1.10.9.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types. Exceptional cases are listed below:

- The state of the line in the control position is not valid for the TalkLTA command (Valid line states are Call Processing Busy (CPB), Call Processing Deload (CPD), Maintenance Busy (MB)). The following message is printed to inform that:

  'Line state INVALID, must be MB or CPB'

- The following message is printed for the command when no 3-port conference circuits are currently available.

  'Conference circuit not available'

1.10.9.8 Example

Table 10 Usage example for TalkLTA command

Description of task	Make a talk connection.
Command:	talklta
MAP response:	Talk connected to line

1.10.10 Command: LnTst

1.10.10.1 Command type: MENU

1.10.10.2 Command target: BRISC

1.10.10.3 Command availability: RES

1.10.10.4 Command description

The LNTST command performs resistance, capacitance, and voltage tests on a line.

1.10.10.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types. There are no changes to command syntax or functions.

1.10.10.6 Qualifications and warnings

- The command is supported for only testable DDRM lines (DRDLCP and DRMLCP).

1.10.10.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types. Exceptional cases are listed below:

- The following message is printed for unsupported DDRM lines:

  '**Command is not valid on this type of DDRM line.**'

- The following message is printed for unavailable test cards such as LTT and TMS:

  '**LTT/TMS test cards are not available in DDRM.**'

1.10.10.8 Example

Table 11 Usage example for LnTst command

Description of task	Perform the command on a line control position that is not in the state call processing busy (CPB) or the state call processing deload (CPD).
Command:	lntst
MAP response:	Resistance, capacitance, and voltage measurements are displayed in the lower part of the command interpreter (CI) output area. The measurements are displayed under the headers RES, CAP, VAC and VDC respectively; and in line with line identifiers TIP, RING and TIP to RING: Test OK RES CAP VAC VDC TIP 999.0K 0.020UF 0 0 RNG 999.0K 0.020UF 0 0 TIP TO RNG 999.0K 0.000UF

1.10.11 Command: VDC

1.10.11.1 Command type: MENU

1.10.11.2 Command target: BRISC

1.10.11.3 Command availability: RES

1.10.11.4 Command description

The VDC command performs a dc voltage measurement on a subscriber loop.

1.10.11.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types.

1.10.11.6 Qualifications and warnings

- The command is supported for only testable DDRM lines (DRDLCP and DRMLCP).
- Voltages are measured from -150 to +150 in one volt steps.
- The c parameter is not applicable for DDRM lines.

1.10.11.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types. Exceptional cases are listed below:

- The following message is printed for unsupported DDRM lines:

  'Command is not valid on this type of DDRM line.'

- The following message is printed for unavailable test cards such as LTT and TMS:

  'LTT/TMS test cards are not available in DDRM.'

1.10.11.8 Example

Table 12 Usage example for VDC command

Description of task	Perform the specified DC voltage measurement and display the result under the VDC header.
Command:	vdc
MAP response:	A voltage measurement is displayed in the lower part of the command interpreter (CI) output area under the header VDC, and in line with the line identifier TIP, RING, or both of them: Test OK T 0 R -51

1.10.12 Command: VAC

1.10.12.1 Command type: MENU

1.10.12.2 Command target: BRISC

1.10.12.3 Command availability: RES

1.10.12.4 Command description

The VAC command performs a ac voltage measurement on a subscriber loop.

1.10.12.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types.

1.10.12.6 Qualifications and warnings

- The command is supported for only testable DDRM lines (DRDLCP and DRMLCP).
- Voltages are measured from 0 to 150 in one volt steps.
- The c parameter is not applicable for DDRM lines.

1.10.12.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types. Exceptional cases are listed below:

- The following message is printed for unsupported DDRM lines:

  'Command is not valid on this type of DDRM line.'

- The following message is printed for unavailable test cards such as LTT and TMS:

  'LTT/TMS test cards are not available in DDRM.'

1.10.12.8 Example

Table 13 Usage example for VAC command

Description of task	Perform the specified voltage measurement.
Command:	vac
MAP response:	A voltage measurement is displayed in the lower part of the command interpreter (CI) output area under the header VAC, and in line with the line identifier TIP, RING, or both of them: Test OK T 0 R 0

1.10.13 Command: Res

1.10.13.1 Command type: MENU

1.10.13.2 Command target: BRISC

1.10.13.3 Command availability: RES

1.10.13.4 Command description

The RES command performs a resistance measurement on a subscriber loop.

1.10.13.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types.

1.10.13.6 Qualifications and warnings

- The command is supported for only testable DDRM lines (DRDLCP and DRMLCP).
- Resistance is measured from 0 to 999 in one ohm steps, and from 1K to 1M to three significant digits.
- The c parameter is not applicable for DDRM lines.

1.10.13.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types. Exceptional cases are listed below:

- The following message is printed for unsupported DDRM lines:

  '**Command is not valid on this type of DDRM line.**'

- The following message is printed for unavailable test cards such as LTT and TMS:

  '**LTT/TMS test cards are not available in DDRM.**'

1.10.13.8 Example

Table 14 Usage example for Res command

Description of task	Perform the specified DC voltage measurement and display the result under the VDC header.
Command:	res
MAP response:	A voltage measurement is displayed in the lower part of the command interpreter (CI) output area under the header VDC, and in line with the line identifier TIP, RING, or both of them: Test OK T 0 R -51

1.10.14 Command: Cap

1.10.14.1 Command type: MENU

1.10.14.2 Command target: BRISC

1.10.14.3 Command availability: RES

1.10.14.4 Command description

The CAP command performs a capacitance measurement on a subscriber loop.

1.10.14.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types.

1.10.14.6 Qualifications and warnings

- The command is supported for only testable DDRM lines (DRDLCP and DRMLCP).
- Capacitance is measured from 0 to 5 microfarads in .001 microfarad steps.
- The c parameter is not applicable for DDRM lines.

1.10.14.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types. Exceptional cases are listed below:

- The following message is printed for unsupported DDRM lines:

  '**Command is not valid on this type of DDRM line.**'

- The following message is printed for unavailable test cards such as LTT and TMS:

  '**LTT/TMS test cards are not available in DDRM.**'

1.10.14.8 Example

Table 15 Usage example for Cap command

Description of task	Perform the command
Command:	cap
MAP response:	Test OK T 0.020UF R 0.020UF TR 0.010UF

1.10.15 Command: LTA

1.10.15.1 Command type: MENU

1.10.15.2 Command target: BRISC

1.10.15.3 Command availability: RES

1.10.15.4 Command description

The LTA command is used to connect the line test access (LTA) to a line card, or release the LTA from it.

1.10.15.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types.There are no changes to command syntax or functions.

1.10.15.6 Qualifications and warnings

- The command is supported for only testable DDRM lines (DRDLCP and DRMLCP).
- When the command LTA is used without a parameter, each subsequent use will alternate the connection of the LTA between the ‘in’ and ‘out’ modes.

1.10.15.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types. Exceptional cases are listed below:

- The following message is printed for unsupported DDRM lines:

  ‘Command is not valid on this type of DDRM line.’

- The following message is printed for unavailable test cards such as LTT and TMS:

  ‘LTT/TMS test cards are not available in DDRM.’

1.10.15.8 Example

Table 16 Usage example for LTA command

Description of task	Prepare the line for testing into the line card and out to the loop.
Command:	lta in
MAP response:	LTA IN

1.10.16 Command: Ring

1.10.16.1 Command type: MENU

1.10.16.2 Command target: BRISC

1.10.16.3 Command availability: RES

1.10.16.4 Command description

The Ring command is used to place ringing voltage on the loop of a subscriber line.

1.10.16.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types.

1.10.16.6 Qualifications and warnings

- There are no optional parameters for DDRM lines.
- A monitor or talk connection should be established before using the command.

1.10.16.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types.

1.10.16.8 Example

Table 17 Usage example for Ring command

Description of task	Transmit a ringing signal from the on-hook line in the control position to the subscriber's station.
Command:	ring
MAP response:	****RINGING LINE****

1.10.17 Command: DgtTst

1.10.17.1 Command type: MENU

1.10.17.2 Command target: BRISC

1.10.17.3 Command availability: RES

1.10.17.4 Command description

The DgtTst command is used to test the Digitone (DGT) pad or dial on the subscriber action.

1.10.17.5 Command syntax

This command operates on DDRM lines in the same manner as for other POTS line types.

1.10.17.6 Qualifications and warnings

- A talk connection should be established before using the command.

1.10.17.7 Responses

This command responses on DDRM lines in the same manner as for other POTS line types.

1.10.17.8 Example

Table 18 Usage example for DgtTst command

Description of task	Perform the command to test the dial on the subscriber action.

Command:	dgttst
MAP response:	TEST PASSED, DIGITS RECEIVED: <n>

Note: The system received and displayed the expected digits. The character <n> represents the digits that were received at the LTP.

1.11 Security

N/A

1.12 Configuration Walkthrough

N/A

2: Configuration (CN): A00007289

2.1 Hardware and Software Requirements

N/A

2.2 Feature Name

RT Selector Enhancement for Metering

2.3 SOC

This feature is activated and deactivated by the SOC option METR0018. The details of the SOC are listed below.

Table 1 SOC

SOC option name:	METR0018
SOC option title:	Retrans Selector
SOC option control type:	State
New SOC option?	Yes
SOC option order code	METR0018
Option defined in DRU:	WT
Affected products:	MMP / GMP

3: Configuration (CN): A00008429

3.1 Feature Name

Ring Back When Free (RBWF) Enhancements

3.2 Hardware and Software Requirements

This feature uses the Enhanced Digital Recorded Announcement Machine (EDRAM) to provide the announcement for RBWF service. The RBWF simple phrases are loaded into EDRAM as voice files.

3.3 Initial Configuration

N/A

3.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

3.5 Upgrade Considerations

N/A

3.6 Data schema (DS) (CM, MIBS, RDB)

3.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
CUSTSTN	CHANGED	UNCHANGED
IBNXLA	CHANGED	UNCHANGED
ISERVOPT	CHANGED	UNCHANGED
AMAOPTS	CHANGED	UNCHANGED

3.6.2 Table/MIB/Remote Database Schema information

3.6.2.1 Name: CUSTSTN

Customer Station Table

3.6.2.1.1 Functional description

The function of the table is unchanged.

3.6.2.1.2 Usage sequence and implications (CM Only)

Current datafill order is unchanged.

3.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CUSTSTN	Same	Same	Current limits are maintained

3.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for <abbreviated name of table.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTION	Changed	OPTION	RAGTIM	
OPTION	Changed	RAGCANTO	0, or a value from 2 TO 185	Determines how long nodal ring again request can remain active at the switch

3.6.2.1.5 Datafill example

The following example shows sample datafill for table CUSTSTN.

Figure 1 Sample Datafill For RAGTIM tuple in table CUSTSTN

```
TABLE CUSTSTN
CUSTNAME     OPTNAME                                        OPTION
-------------------------------------------------------------------
CUSTRAG      RAGTIM                                  RAGTIM 8  45
```

3.6.2.1.6 Table release history update

Range of RAG CANCELLEATION TIMER, datafilled with RAGCANTO field of RAGTIM tuple, is increased from - 2 TO 30 OR 0 - , to - 2 TO 180 OR 0.

3.6.2.1.7 Supplementary information
N/A

3.6.2.1.8 Translation verification and other tools

TABLE CUSTSTN does not use translation verification tools.

3.6.2.2 Name: AMAOPTS

AMA Options Table

3.6.2.2.1 Functional description

The function of the table is unchanged.

3.6.2.2.2 Usage sequence and implications (CM Only)

Current datafill order is unchanged.

3.6.2.2.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
AMAOPTS	Same	Same	Current limits are maintained

3.6.2.2.4 Fields/OIDs
The following table lists fields/OIDs for <abbreviated name of table.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODAL_RAG_BILL	New	None	ON or OFF	Enables metering of Nodal RBWF Calls when it is ON. Please note that SVBI RBWF Enh SOC must also be ON.

3.6.2.2.5 Datafill example
The following example shows sample datafill for table AMAOPTS.

Figure 2 Sample Datafill For NODAL_RAG_BILL option in Table AMAOPTS

```
TABLE AMAOPTS
OPTION                SCHEDULE
-----------------------------
NODAL_RAG_BILL        ON
```

3.6.2.2.6 Table release history update

New AMA option NODAL_RAG_BILL is added to table AMAOPTS. Its default value is OFF, when not datafilled.

3.6.2.2.7 Supplementary information

N/A

3.6.2.2.8 Translation verification and other tools

TABLE AMAOPTS does not use translation verification tools.

3.6.2.3 Name: ISERVOPT

International Service Options Table

3.6.2.3.1 Functional description

The function of the table is unchanged.

3.6.2.3.2 Usage sequence and implications (CM Only)

Current datafill order is unchanged.

3.6.2.3.3 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	Same	Same	Current limits are maintained

3.6.2.3.4 Fields/OIDs

The following table lists fields/OIDs for <abbreviated name of table.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSKEY	New	-	RBWFENH	New ISERVOPT option for RBWF Enhancements.
SOPTSKEY	New	MAX_RBWF_REQ	1 TO 6	Determines the maximum number of RBWF requests That can be activated by a RAGOR simultaneously. Please note that SVBI Multiple RBWF SOC must be ON in order to use this functionality.
SOPTSVAR	New	IGNORE_INTRAGRP	Y OR N	Allows Nodal RBWF to work between different customer groups regardless of INTRAGRP flag, when IGNORE_INTRAGRP is Y and SVBI RBWF Enh SOC is ON.

3.6.2.3.5 Datafill example

The following example shows sample datafill for table RBWFENH tuple of ISERVOPT.

Figure 3 Sample Datafill For RAG tuple in table ISERVOPT

```
TABLE ISERVOPT
SOPTSKEY                                        SOPTSVAR
-------------------------------------------------------------
RBWFENH                                           RBWFENH 5 Y
```

3.6.2.3.6 Table release history update

N/A

3.6.2.3.7 Supplementary information

N/A

3.6.2.3.8 Translation verification and other tools

TABLE ISERVOPT does not use translation verification tools.

3.6.2.4 Name: IBNXLA

IBN Tranlations Table

3.6.2.4.1 Functional description

The function of the table is unchanged.

3.6.2.4.2 Usage sequence and implications (CM Only)

Current datafill order is unchanged.

3.6.2.4.3 Size

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IBNXLA	Same	Same	Current limits are maintained

3.6.2.4.4 Fields/OIDs

The following table lists fields/OIDs for <abbreviated name of table.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FEATURE	Changed	None	RAGD	RAG Deactivation
FEATURE	Change	None	RAGINT	RAG Interrogation

3.6.2.4.5 Datafill example

The following example shows sample datafill for table IBNXLA.

Figure 4 New datafills for RBWF act, deact and interrogation access codes

```
TABLE IBNXLA
KEY                       RESULT
-----------------------------------------
FTRSTAR  37       FEAT N N RAG
FTROCT   37       FEAT N N RAGD
FTRSTAR  C37      FEAT N N RAGINT
```

3.6.2.4.6 Table release history update

New features RAGD and RAGINT are added to IBN_LOG_FEATUREs usde in table IBNXLA.

3.6.2.4.7 Supplementary information

N/A

3.6.2.4.8 Translation verification and other tools

Traver Sample for RAGINT.

Figure 5 Traver Sample for RAGINT

```
>traver l 7835304 bc37 b
TABLE IBNLINES
HOST 02 0 00 18 0 DT STN IBN 7835304 CUST783A 0 3 102 (RAG) $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP:  no subscribed trigger.
INAP Info Collected TDP:  no subscribed trigger.
TABLE NCOS
CUST783A 3 0 0 $ ( XLAS PTTXLA FTRSTAR FTRCOLL) ( OCTXLA
FTROCT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA,
VACTRMT, AND DIGCOL
CUST783A NXLA NETXLA1 NXLA 0 NDGT
TABLE DIGCOL
FTRCOLL STAR POTS N
TABLE IBNXLA: XLANAME FTRSTAR
FTRSTAR C37 FEAT N N RAGINT

+++ TRAVER: SUCCESSFUL CALL TRACE +++

Feature RAG        not supported by TRAVER


+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

3.7 Service Orders (SO) (CM & SESM)

N/A

3.8 Software optionality control (SOC)

Main functionalities of this activity are controlled by two new SOC options, SVBI Multiple RBWF and SVBI RBWF Enh. Both of these SOCs are state SOCs, which can be either in SOC_ON or SOC_IDLE state.

SVBI Multiple RBWF SOC controls the following:

- Allowing N RBWF request to be activated by the RAGOR.
- Rejecting N+1th request.

Table 10 SVBI Multiple RBWF SOC

SOC option name:	SVBI0037
SOC option title:	Multiple RBWF
SOC option control type:	State
New SOC option?	Yes
SOC option order code	
Option defined in DRU:	WT22
Affected products:	DMS100 - MMP

SVBI RBWF Enh SOC controls the following:

- Allowing nodal RBWF between different customer groups via ignoring INTRAGRP flag.
- Billing of nodal RBWF usage.
- Deactivation and interrogation functionalities with new dialling sequences.

Please note that datafilling of any option, which is introduced by this activity, is allowed even if these SOCs are IDLE. But new functionalities are only available when related SOC(s) is ON.

Table 11 SVBI RBWF Enh SOC

SOC option name:	SVBI0036
SOC option title:	RBWF Enh
SOC option control type:	State
New SOC option?	Yes
SOC option order code	
Option defined in DRU:	WT22

Affected products:	DMS100 - MMP

3.9 Element Management

N/A

3.10 User interface changes

N/A

3.11 OSSGate Interface Changes

N/A

3.12 Security

N/A

3.13 Configuration Walkthrough

4: Configuration (CN): A00008477

4.1 Feature Name

Increase size of table MSGRTE

4.2 Hardware and Software Requirements

N/A

4.3 Initial Configuration

N/A.

4.4 Data schema (DS) (CM, MIBS, RDB)

4.4.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MSGRTE2	New	New

4.4.2 Table/MIB/Remote Database Schema information

4.4.2.1 Name: MSGRTE2

Message Routing Table (2)

4.4.2.1.1 Functional description

New table MSGRTE2 is used for routing and processing of facility messages of some protocols (e.g. PRA, DPNSS, etc.) in a manner identical to that performed by the existing table MSGRTE (Please refer to FN section of AD1315 for more details about the functional model of the table MSGRTE). This table determines if the message terminates on the current switch or is sent to another switch. This is done through the use of the origination and destination information elements.

New table MSGRTE2 has the same format as the existing table MSGRTE, and shares the same functionality provided by the MSGRTE table. The difference, and hence the need for a new table, is that the new table supports upto 100,000 entries while the existing table has a limit of 32K-1 digilator blocks. The selection of which table will be active is achieved by the SOC XLAS0057.

4.4.2.1.2 Usage sequence and implications (CM Only)

Datafill order of the new table MSGRTE2 is the same as the current datafill order of the existing table MSGRTE.

The following tables must be datafilled before the table MSGRTE2:

- NETNAMES
- TRKMEM
- C7RTESET

All network names in the table MSGRTE2 must already exist in table NETNAMES. Table MSGRTE2 is indexed by the NETID datafilled in Table NETNAMES, so this table must be datafilled before the table MSGRTE2. When an entry tried to deleted from the table NETNAMES, table MSGRTE2 is checked if there is a datafill with the specified NETID. The deletion from NETNAMES table is not allowed if the specified NETID is also datafilled in Table MSGRTE2.

To datafill a DPNSS selector, a source ISUP trunk CLLI must be specified along with a DPNSS selector, and the ISUP trunk CLLI must exist in tables TRKGRP and TRKSGRP.

4.4.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MSGRTE2	0	100,000*	Memory is allocated dynamically on per tuple

* ***Note :*** *Table MSGRTE2 supports upto 100,000 tuples depending on the amount of the available free memory. The maximum number of tuples may vary due to compression and expansion of tuples.*

4.4.2.1.4 Table Fields

The following table lists fields for the Table MSGRTE2.

Table 3 Table MSGRTE2 field descriptions

Field	New or Changed	Subfield or Refinement	Range of Values	Description
MSGRTKEY	New			*Message Route Key* This is the key to table MSGRTE2 and consists of subfields NETID and DIGRANGE.
		NETID	String up to 32 characters	*Network Identifier* Network name datafilled in table NETNAMES
		DIGRANGE		*Digit Range* This field consists of subfields FROMDIGS and TODIGS.
		FROMDIGS	Alphanumeric (vector up to 10 characters, 0 to 9, A to F)	*From Digits* Digit string for the lower bound of the digit range to which the route list applies
		TODIGS	Alphanumeric (vector up to 10 characters, 0 to 9, A to F)	*To Digits* Digit string for the upper bound of the digit range to which the route list applies
MSGRTRES	New			*Message Route Result.* The list of routes used to transmit messages. Up to four routes can be datafilled.

Field	New or Changed	Subfield or Refinement	Range of Values	Description
		MSGRTSEL	DPNSS, LOCAL, PRA or SS7	*Message Route Selector* • DPNSS if TCAP NRAG messages are sent over DPNSS virtual trunks. • LOCAL if the message terminates on this switch. • PRA if the message is routed out on a specified PRA-D channel. • SS7 if a the message is routed over a specific SS7 route set.

Each Message Route Selector such as DPNSS, LOCAL, PRA and SS7 has its own special refinement.

MSGRTESEL = LOCAL

If the entry for field MSGRTSEL is LOCAL, the refinement is as followed.

Table 4 Structure of LOCAL Refinement

Field	Subfield or Refinement	Range of Values	Description
	DELDIGS	0 to 15	*Delete Digits* Number of deleted digits from the destination address
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix Digits* Digit string prefixed to the destination address

MSGRTESEL = DPNSS

If the entry for field MSGRTSEL is DPNSS, the refinement is as followed.

Table 5 Structure of DPNSS Refinement

Field	Subfield or Refinement	Range of Values	Description
	ISUPTRK	Alphanumeric (up to 16 characters)	*ISUP Trunk CLLI Name*
	DELDIGS	0 to 15	*Delete digits*
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix digits*
	OPTIONS	NEWNET	*DPNSS Option*
	NETNAME	String up to 32 characters	*Network Identifier* Network name datafilled in table NETNAMES

MSGRTESEL = PRA

If the entry for field MSGRTSEL is PRA, the refinement is as followed.

Table 6 Structure of PRA Refinement

Field	Subfield or Refinement	Range of Values	Description
	TRKCLLI	Alphanumeric (up to 16 characters)	*Trunk Common Language Location Identifier* Trunk CLLI name
	DELDIGS	0 to 15	*Delete Digits*
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix Digits*
	OPTIONS	NEWNET or NEWTOR	*PRA Options* • NEWNET for a new network and datafill subfield NETNAME. • NEWTOR for a new type of route and datafill subfield TYPEOFRT.
	NETNAME	String up to 32 characters	*Network Identifier* Network name datafilled in table NETNAMES

Field	Subfield or Refinement	Range of Values	Description
	TYPEOFRT	PUB or PVT	*Type of Route* • PUB for a public route. • PVT for a private route.

MSGRTESEL = SS7
If the entry for field MSGRTSEL is SS7, the refinement is as followed.

Table 7 Structure of SS7 Refinement

Field	Subfield or Refinement	Range of Values	Description
	DPC	Alphanumeric (up to 16 characters)	*Destination Point Code*
	DELDIGS	0 to 15	*Delete Digits*
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix Digits*
	OPTIONS	NEWNET	*SS7 Option*
	NETNAME	String up to 32 characters	*Network Identifier* datafilled in table NETNAMES

4.4.2.1.5 Datafill example

The following example shows sample datafill for table MSGRTE2.

Figure 1 Sample Datafill of Table MSGRTE2

```
TABLE: MSGRTE2
MSGRTKEY
MSGRTRES
-------------------------------------------------------------
PUBLIC 12345 12345 (SS7 ANSIAB_ROUTES 4 0 (NEWNET NEWPUB) $)$
```

4.4.2.1.6 Table release history update

Table is newly created.

4.4.2.1.7 Supplementary information

None.

4.5 Service Orders (SO) (CM & SESM)

N/A

4.6 Software optionality control (SOC)

Table 8 SOC

SOC option name:	XLAS MSGRTE2
SOC option title:	XLAS
SOC option control type:	STATE
New SOC option?	Yes
SOC option order code	XLAS0057
Option defined in DRU:	WT
Affected products:	ISN09

MSGRTE and MSGRTE2 tables are not effective at the same time - both tables could be datafilled but only one of them will be in effect. The selection of which table will be used is achieved through the SOC option XLAS0057. When the state of the SOC option is ON, MSGRTE table will be disabled and call processing will begin to use the new table MSGRTE2. When the SOC option is IDLE, MSGRTE2 table will be disabled and the MSGRTE table will be in effect.

4.7 Element Management

N/A.

4.8 Security

N/A.

4.9 Configuration Walkthrough

N/A.

5: Configuration (CN): A00008484

5.1 Feature Name

IN Terminating Trigger Feature Interactions

5.2 Hardware and Software Requirements

N/A

5.3 Initial Configuration

5.4 Office/Subnet parameters (OP/SP) (CM & SESM)

5.5 Upgrade Considerations

5.6 Data schema (DS) (CM, MIBS, RDB)

5.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SERVINFO	CHANGED	UNCHANGED

5.6.2 Table/MIB/Remote Database Schema information

5.6.2.1 Name: SERVINFO

Service Information Table

5.6.2.1.1 Functional description

It is not a new table.

5.6.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

5.6.2.1.3 Size

It is not a new table and the new option does not change the size.

5.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for SERVINFO.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FI	Changed		CONV_DESK option is added to the possible values.	When CONV_DESK is added to a tuple under FI then the corresponding IN triggers show converged desktop behaviour as follows: IN can co-exist with line based DMS services as described in the FN along with some limitations and restrictions to the existing IN functionality.

5.6.2.1.5 Datafill example

The following example shows sample datafill for table SERVINFO.

Table 3 SERVINFO Sample Datafill

```
SERVIDX                                                    OPTION
-------------------------------------------------------------------------------
    19   (INITDP_PARMS ( SERVKEY) (CDPA) (CLI) (EVENT_TYPE) (OCN) (RDN)
         (RD_INFO) $)
         (FI (RETRIG_OPTION ALLOW GTE 1) (CONV_DESK ) $)$
```

5.6.2.1.6 Table release history update

IN can co-exist with line based DMS services as described in the FN along with some limitations and restrictions to the existing IN functionality.

5.6.2.1.7 Supplementary information

None.

5.6.2.1.8 Translation verification and other tools

The new option does not change the way SERVINFO and translation verification tools interact.

5.7 Service Orders (SO) (CM & SESM)

5.8 Software optionality control (SOC)

5.9 Element Management

5.10 User interface changes

5.11 OSSGate Interface Changes

5.12 Security

5.13 Configuration Walkthrough

6: Configuration (CN): A00008556

6.1 Feature Name

SIP Lines Core OAMP support

6.2 Hardware and Software Requirements

No new hardware or software requirements are created by this activity.

6.3 Initial Configuration

At initial configurations, it is assumed that standard datafill exists in the DMS/CS2K, GWC and CS2KSS. Since a usage SOC is used for this feature, the SOC limit decides whether any service will be provided initially by the design components applicable after the DPL line is provisioned.

6.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

6.5 Upgrade Considerations

None.

6.6 Data schema (DS) (CM, MIBS, RDB)

6.6.1 New/modified tables, MIBs, or Database Schema

Table 1 below shows a list of new/modified tables.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SERVRINV	CHANGED	UNCHANGED
LGRPINV	CHANGED	UNCHANGED
IPAPPL	CHANGED	UNCHANGED
IBNFEAT	CHANGED	UNCHANGED
LCCOPT	CHANGED	UNCHANGED
OPTOPT	CHANGED	UNCHANGED

6.6.2 Table/MIB/Remote Database Schema information

6.6.2.1 Name: SERVRINV

SERVER INVENTORY

6.6.2.1.1 Functional description

Server Inventory table stores the information on GWC. Each entry in this table provides information about a specific GWC which includes the following:

- Server type and numeric ID, e.g. GWC 7.
- Packet network type (IP or ATM).
- GWC IP address.
  Note: The last element of this address must be a multiple of four, because four IP addresses are used by each GWC; the three IP addresses next in sequence are assigned automatically.
- The server exec(s) to be used, which determines the type of call processing to be performed by the GWC. A new entry is specified for this field by this feature.
- Toneset to be used.
- Bearer Networks.
- Optional attributes to be associated with this GWC.

6.6.2.1.2 Usage sequence and implications (CM Only)

The table SERVRINV can be datafilled independently through SESM. There is no change in the current table datafill order.

6.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVRINV	0	256	Memory is dynamically allocated at 16 tuples per allocation.

6.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for SERVRINV.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SRVREXEC	Changed	TERM_TYPE EXEC_LINEUP	DPL_TERM DPLEX	This field now supports a new term_type DPL_TERM and a new exec_lineup DPLEX.

6.6.2.1.5 Datafill example

The following example shows sample datafill for table SERVRINV.

Table SERVRINV:

SRVRNAME SRVRADDR ***SRVREXEC*** *SRVRTONE BEARNETS SRVROPTS*
GWC 0 IP 45 46 47 48 ***(DPL_TERM DPLEX)*** *$ NORTHAA (NET_IP Y) $ $*

6.6.2.1.6 Table release history update

The table SERVRINV is enhanced to support new SRVREXEC entry DPL DPLEX. This entry for a new terminal_type and new exec_lineup is specifically going to be used to support the DPL agents on the GWC.

6.6.2.1.7 Supplementary information

None.

6.6.2.1.8 Translation verification and other tools

None.

6.6.2.2 Name: LGRPINV

LOGICAL GROUP INVENTORY

6.6.2.2.1 Functional description

Logical group inventory table defines the gateways or nodes supported under the gateway controller. The gateway or node entries are:

- Logical group number (site name, frame no, shelf no) e.g. LG 2 3
- Server name (GWC datafilled in table SERVRINV)e.g GWC 7
- Logical group type: This field is to specify the group type. Existing logical group types are

S MG9K large lines gateways
M CICM large lines gateways
C Small lines gateways
LL_3RDPTY Large Line Third Party gateways
SSDPL DPL lines.

- When the LGRPINV is provisioned with a LGRP ‘SSDPL’, then a termtype ‘DPL’ is specified in LNINV table. When lines are provisioned in table LNINV, then an exec_lineup DPLEX corresponding to termtype ‘DPL’ will be downloaded to the GWC. Also, the cardcode of the DPL lines is restricted to RDTLSG for North American market and GWLPOT for International market.
- Logical group options
  Existing options are:(MTSTAPT, LGRPLOC, GTWYKEY)

6.6.2.2.2 Usage sequence and implications (CM Only)

The table LGRPINV depends upon the table SERVRINV. It references the server name from the table SERVRINV.

6.6.2.2.3 Size

The following table lists the size of LGRPINV table.

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LGRPINV	0	1000	Memory is dynamically allocated at 10 tuples per allocation.

6.6.2.2.4 Fields/OIDs

The following table lists fields/OIDs for LGRPINV

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GRPTYPE	Changed	N/A	SSDPL	A new LGRP SSDPL has been introduced to support DPL lines.

6.6.2.2.5 Datafill example

The following example shows sample datafill for table LGRPINV

Table LGRPINV:

LGRP_NO	*SRVR_NAME*	***GRPTYPE***	*LGRPOPTS*
LG 1 1	*GWC 5*	***SSDPL***	*$*

6.6.2.2.6 Table release history update

The table LGRPINV is enhanced to support DPL agents. As part of this enhancement new lgrp_type ‘SSDPL’ is introduced.

6.6.2.2.7 Supplementary information

None.

6.6.2.2.8 Translation verification and other tools

None.

6.6.2.3

6.6.2.4 Name: IPAPPL

Internet Protocol Application

6.6.2.4.1 Functional description

Table IPAPPL datafill provides instance of various connections to the DMS. The use of SCTP transport requires that the application store the specific remote IP addresses and local Port number. Therefore table IPAPPL is datafilled in order to provide these details. Table IPAPPL includes following fields.

TABLE IPAPPL Fields and description are as follows:

- InstKey is datafilled in order to map this instance with an internally assigned instance number. This field is the unique key to the tuple.
- InstanceName is datafilled in order for the telco personnel to be able to distinguish one connection from the other.
- Transport is datafilled in order to classify the instance to which transport protocol be used. Currently the table will support SCTP functionality ONLY.
- IPDevice is datafilled to indicate which IP interface hardware will be used. This table currently supports EIU and HIOP.
- IP addresses (upto 4 addresses) are allowed in one instance tuple. This may be used to support multihoming. The first IP address in the list will be used as the primary address. IPV4 type IP addresses are supported.Only one IP address will be used for DPL, the IP address of the CS2KSS Provisioning Manager.
- Port Number is the local port number at which the DMS-Core will expect to receive messages from this instance. (Note that the remote port is received during the INIT message from the far-end). Valid range of Source port allowed to be configured on the CORE is from 4900 to 4982

- OptList field may be datafilled with “SETPRIME” to set any of the IP address in an instance to be used as to set the primary destination address.
- Optlist sub-field “APPLICATION” can be datafilled to specify the application eg:DPL. Here the SIPMTC(Application) option is incorporated along with AIN option.
- Optlist sub-field “mode” is to specify the mode SERVER/CLIENT.
- Optlist sub-field “multihoming” is used to specify if the remote node supports multihoming. This option is currently only supported on the HIOP ipdevice.

6.6.2.4.2 Usage sequence and implications (CM Only)

The table IPAPPL is an independent table.

6.6.2.4.3 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IPAPPL	0	64	Memory is automatically allocated for 64 Intelligent Network SCTP instances

6.6.2.4.4 Fields/OIDs

The following table lists fields/OIDs for IPAPPL.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTS	Changed	Application	SIPMTC	A new application ‘SIPMTC’ is added to option list.

6.6.2.4.5 Datafill example

The following example shows sample datafill for table IPAPPL:

Table IPAPPL:

InstKey InstName Transport IPDevice IPaddrs port optlist

*1 a sctp hiop 198.202.188.121 4982 (application **sipmtc**)*

(setprime 1)

6.6.2.4.6 Table release history update

The table IPAPPL is enhanced to create a instance for SIPMTC service.

6.6.2.4.7 Supplementary information

- The NCAS link association is going to be used for the new QSIP command.
- The SIPMTC application is supported over HIOP only.
- The multihoming functionality is not supported in SIPMTC application.
- The port number allocated for SIPMTC application is 4982.
- Multiple instances for SIPMTC are not allowed i.e. in table IPAPPL, there can be only one instance datafilled for SIPMTC.

6.6.2.4.8 Translation verification and other tools

None.

6.6.2.5 Name: IBNFEAT

IBN Feature

6.6.2.5.1 Functional description

IBNFEAT (IBN Line Feature) lists line features that are assigned to the IBN lines listed in table IBNLINES.

Table IBNFEAT fields and description are as follows:
LEN: Line equipment number. This field consists of the subfields SITE, FRAME, UNIT, DRAWER, LSG and CIRCUIT.

DNNO_RANGE: Directory number. This field specifies the DN of the LEN being referenced. Enter a value from 0 to 6 for the DN.

DF : Data feature. This field specifies the data feature assigned to the line.

FEATURE: Data feature. This field specifies the data feature assigned to the line.

DATA: SIP: Bool. Enter Y if a SIP line

MAX_NUM_CALLS: Enter a value between 1-10.

ALLOW_BSY_TERM: Bool. It determines whether or not a busy SIP line can take an additional call termination.

Only Servord can be used to datafill the DPL option. It cannot be done via table control.

6.6.2.5.2 Usage sequence and implications (CM Only)

- In table LCCOPT, DPL option should be made compatible with IBN LCC.
- The table IBNLINES should have the LEN datafilled before the DPL option can be added on it.

6.6.2.5.3 Size

6.6.2.5.4 Fields/OIDs

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IBNFEAT	0	TBD	TBD

The following table lists fields/OIDs for IBNFEAT.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DF	Changed	N/A	DPL	A new feature DPL to be assigned to an IBN line.
Feature	Changed	N/A	DPL	A new feature DPL to be assigned to an IBN line.
DATA	Changed	SIP MAX_NUM_CALLS Allow_Bsy_Term	Y/N 1-10 Y/N	Enter Y if a SIP line Max Simultaneous Call Appearances. It determines whether or not a busy SIP line can take an additional call termination.

6.6.2.5.5 Datafill example

The following example shows sample datafill for table IBNFEAT.

Table IBNFEAT:

LEN DNNO DF FEATURE DATA
LG 01 1 00 14 0 DPL DPL Y 10 Y

6.6.2.5.6 Table release history update

Table IBNFEAT has been enhanced to support a new feature DPL which will convert the IBN line into a DPL line.

6.6.2.5.7 Supplementary information

None.

6.6.2.5.8 Translation verification and other tools

None.

6.7 Service Orders (SO) (CM & SESM)

SERVORD+ will accept three new options related to DPL lines provisioning: DPL, SIP_PASSWORD and SIP_DATA. When provisioning a SIP line all three of the options described above must be present in the SERVORD+ NEW command. They can not be added later via ADO.

6.7.0.1 LCC and options

New line option DPL is introduced by this feature. It is compatible with RES and IBN line class codes only.DPL is not compatible with huntgrps, scmp, MADN, FTRG.

Table 10 Meridian digital centrex feature assignment requirements

Feature	500 2500	MDC SET	ISDN SET	MDC Set ISDN Set Relationship							
				SET	SUBSET	KEY	DN	DEDKEY	LAMP	CODE	DISPLAY
DPL	Y	N	N	N							

The feature in the table above requires a handsfree Business Set. This feature must be assigned to key 1.

6.7.1 New commands

No new commands are introduced with this feature.

6.7.1.1 How service order commands are presented

6.7.1.1.1 Description

The NEW command is used to associate a DN with a LEN due to which the line state changes from HASU(hardware assigned-software unassigned) to IDL i.e. puts the line into service.

6.7.1.1.2 Applicability

The DPL line option can only be added with the NEW command. Other commands that prompt for options such as EST, ADD, DE0, ADO and NEWACD will be rejected if the DPL option is present with these commands. A warning message will be output. The CDN and CLN commands will be blocked if the DPL option is present on the line. The line must be OUTed and NEWed to effect a change of LEN or endpoint or DN. CHG of line class code will be blocked if DPL is present on the line.
The DPL option should only be added via SESM. It cannot be added via table control.

6.7.1.1.3 Example

The examples below show how SERVORD+ command NEW can be used to provision the DPL line. Servord+ should be used to add the DPL option. Th e prompt mode is shown as an example of the fields only. Note that SIP_PASSWORD and SIP_DATA are not valid options on the core and are shown here for example only.

Figure 1 Example of the NEW command in prompt mode (SERVORD only)

```
>NEW
SONUMBER:    NOW   4 10 20 PM
>$
DN:
>6212500
LCC_ACC:
>IBN
GROUP:
>BNR
SUBGRP:
```

```
>0
NCOS:
>0
SNPA:
>613
LATA:
>NILLATA
LTG:
>0
LEN_OR_LTID:
>LG 000 0 10 13
Option:
>DPL
SIP:
>Y
MAX_NUM_CALLS:
>3
SIP_PASSWORD:
>xxx
SIP_DATA:
>bobby mb1
```

Figure 2 Example of the NEW command in no-prompt mode

In the no-prompt mode, the command as entered through SESM will be:

NEW $ 6212500 IBN BNR 0 0 613 NILLATA 0 LG 000 0 10 13 DPL Y 3 xx bobby mb1

Figure 3 Example of the CHF command in no-prompt mode

CHF $ 6212500 DPL Y 7 $

6.7.1.2 How service order options are presented

6.7.1.2.1 Description

A new option DPL is introduced as a part of this activity. This option DPL converts an IBN line into DPL line. The following sections lists how the DPL option and the sub-options associated with the DPL option are assigned through SERVORD.

6.7.1.2.2 Example

The following examples show how a new option DPL and its sub-options are added to a line to convert it into a DPL line.

Figure 4 Example of the DPL option in prompt mode (SERVORD only)

```
Option:
>DPL
SIP:
>Y
MAX_NUM_CALLS:
>3
```

Figure 5 Example of the DPL option in no-prompt mode

```
DPL Y 3 xx bobby mb1
```

6.7.1.2.3 Option prompts

Table 11 System prompts for DPL option

Prompt	Valid input	Description	Areas affected by prompt
SIP	Y	Bool	
MAX_NUM_CALLS	1-10	Integer	

6.7.1.2.4 Line class code compatibility

The new DPL option is applicable only for the IBN and RES lines.

Table 12 DPL compatibility to LCC

Line class code	Compatible?
IBN	Yes
RES	Yes

6.7.1.2.5 Assignability

DPL is not a valid keyset option.
The following functionalities apply to this option:

- set functionality: <yes or no>
- subset functionality: <yes or no>
- DN functionality: <yes or no>
- key functionality: <yes or no>

6.7.1.2.6 Option prerequisites
None.

6.7.1.2.7 Notes

The subfields SIP and MAX_NUM_CALLS which will be prompted for will have the default values of Y and 1 shown respectively. For SN08, these are the only valid values and cannot be changed.

6.7.1.2.8 SERVORD+ Exceptions
None.

6.7.2 Line equipment format changes

6.7.2.1 LEN
There are no changes made in the LEN format.

6.7.2.2 Media gateway endpoint format
The MG endpoint format is similar to the LEN format to make the mapping between them easier.

The suggested endpoint format is:
<GW NAME> <SITE>/NNN/G/TTtt where
GW_NAME = up to 32 chars
<SITE> = a site name datafilled in Table SITE and used as the first part of the LGRPINV key.
NNN = logical frame number from core table LGRPINV
G = group number 0-9 from core table LGRPINV
TT = 00 to 10
tt = 00 to 99 except when TT = 10 then tt = 00 to 22
Example:
SIPVMG1.tampa.vz.com TMP1/000/2/0478 maps to LEN: TMP1 000 2 04 78

6.8 Software optionality control (SOC)

This feature will be controlled by standard usage based SOC. The limit will define the maximum number of DPL lines that can be provisioned in the switch.

- The default usage limit will be zero, indicating that the DPL option can not be provisioned. New limits can be purchased via SOC in increments of 1 subscriber at a time if desired.
- There will not be a maximum limit. Hence, any limit can be assigned to the SOC CS2C0005.
- When a new DPL line is provisioned, the current DPL count (SOC usage count) will be compared to the purchased limit (SOC usage limit). If the limit has already been reached, the new line can not be provisioned. If the

limit has not been reached, the new line is allowed, and the SOC usage count is incremented.

- When an existing DPL line is removed, the current SOC usage count will be decremented, but the SOC limit will not change.
- If the SOC limit is ever decreased to a value below the current usage count, existing DPL line agents will continue to function properly. However, new DPL lines can not be added. Further, if existing DPL lines are removed, they can not be re-added until the current count is below the limit.
- The SOC audit will generate a warning log on each pass if the usage count is above the usage limit.
- The SOC code is functional whenver a line is provisioned with DPL option whether through table control / servord.
- The usage control of the SOC utility allows the activation/deactivation for provisioning of DPL lines.
- A new module will be created to contain the new SOC code. The new module will belong to a new user group called DPLOAMP.
- It is strongly recommended that the SOC code be sourced in SN08 if possible. This is due to the fact that patching of a usage based SOC can introduce certain obstacles regarding usage limits and usage counts being updated during ONP. To minimize these obstacles, the SOC code can be sourced in SN08.
- Table 13 below shows the SOC details.

Table 13 SOC

SOC option name:	CS2C0005
SOC option title:	Number of SIP CLient
SOC option control type:	USAGE
New SOC option?	Yes
SOC option order code	CS2C0005
Option defined in DRU:	CCM
Affected products:	CS2K

6.9 Element Management

Not Applicable.

6.10 User interface changes

6.10.1 Directory:

N/A

6.10.2 Command: QSIP

6.10.2.1 Command type: NON-MENU

6.10.2.2 Command target: BRISC, POWERPC

6.10.2.3 Command availability: NONRES

6.10.2.4 Command description

The QSIP command at the CI level will query the CS2KSS to get the SIP information. QSIP command will query the following for the DPL agent:

SIP URI

Registration State

Allow Post Busy Termination

Number of Contacts

Contacts

Service Package

Services

Endpt ID

Virtual Media Gateway

Zone ID List

Client Type

Static Client

Node number and Terminal number of the VIDs of all the Active Call Appearances

Number of Active Sessions in CS2000 Session Server

- The CS2KSS will handle the query from the CS2K via the NCAS link for the QSIP command and respond back to the CS2K with the requested data.

- The default time interval for getting a response to the QSIP query is 15 seconds. Time can be set from 1 to 30 seconds. If any value lesser than 1

and greater than 30 is given then the time value will be set to the default value of 15. It is an optional parameter in the QSIP command.

- The QSIP command's format is listed below

```
CI:
>q qsip
DISPLAY SIP LINE INFORMATION
    COMMAND FORMAT: QSIP <DR_LEN_TYPE>
    PARMS:  [<TIMEOUT> {1 TO 30}]
```

- If the NCAS Link is unavailable or the CS2KSS did not respond, the QSIP command's timer will expire with the following message:

```
>qsip 8675309
SIP DATA CANNOT BE DISPLAYED DUE TO RESPONSE
TIMEOUT FROM CS2000 SESSION
```

6.10.2.5 Command syntax

Table 14 QSIP command parameters and variables

Command	Parameters and variables
QSIP	<DR_LEN_TYPE> [<Timeout> {1 to 30}]
Parameters and variables	Description
DR_LEN_TYPE	The DN/LEN of a SIP line agent is specified
TIMEOUT	Maximum time for which QSIP waits for a response from CS2KSS. Min value:1 seconds Max value:30 seconds Default value:15 seconds

6.10.2.6 Qualifications and warnings

QSIP query takes place through the NCAS link. Hence, the command response depends upon the availability of the NCAS link.

When the response is not received in a specified time interval, a message is displayed at the console:

"NO RESPONSE FROM CS2KSS WITHIN TIMEOUT OF 15 SECONDS".

6.10.2.7 Responses

Table 15 MAP outputs with associated meanings and actions

Command
Example 1: >qsip 8675309 --- SIP USER DATA ========== SIP URI: 6138675309@NORTELNETWORKS.COM ACCOUNT STATUS: ACTIVE REGISTERED: Y ALLOW POST BSY TERMINATIONS: N NUMBER OF CONTACTS: 12 CONTACTS: 6138675309@4.3.2.1:5060 6138675309@4.3.2.1:5061 6138675309@1.2.3.4:5062 SERVICE PACKAGE: DEFAULT_PKG SERVICES: ADHOC 4 ADDRBK 50 VMAIL SIP LINE DATA ========== ENDPT ID: PHX/003/0/1000 VMG: vmg ZONE ID(s): 1234 1234 3456 CLIENT TYPE: ONT STATIC CLIENT: N SIP CALL DATA ========== ACTIVE CALL APPEARANCES: NODENO TERMNO NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12 ---
Meaning: The querying was successful. All the data obtained is displayed.
System or user actions: None.

Table 15 MAP outputs with associated meanings and actions

Command
Unsuccessful Query: **Example 2:** >qsip 8675309 SIP DATA CANNOT BE DISPLAYED DUE TO RESPONSE TIMEOUT FROM CS2000 SESSION SERVER **Meaning:** The response was not received before the QSIP timer expired either because the NCAS link is either busy/not available or the CS2KSS did not respond before the timeout occured. **System or user actions:** The user is expected to run QSIP again. **Example 3:** >qsip 122456783 QSIP SHOULD BE GIVEN FOR SIP LINES ONLY **Meaning:** The DN supplied is not a SIP line. **System or user actions:** The user is expected to give a valid SIP Line DN for QSIP. Example 4: >qsip 122456783 INVALID DN SPECIFIED FOR THE QSIP COMMAND Meaning: The DN supplied is not a valid DN. System or user actions: The user is expected to give a valid SIP Line DN for QSIP. Example 5: >qsip LG 0 2 3 4 INVALID LEN SPECIFIED FOR THE QSIP COMMAND Meaning: The LEN supplied is not a valid LEN. System or user actions: The user is expected to give a valid SIP Line LEN for QSIP. Example 6: >qsip 8675309 SIP DATA CANNOT BE DISPLAYED DUE TO BAD MESSAGE RECEIVED FROM CS2000 SESSION SERVER Meaning: The response received from CS2KSS in not valid. System or user actions: The user is expected to run QSIP again. Example 7: >qsip 8675309 SIP DATA CANNOT BE DISPLAYED BECAUSE NO DATA RECEIVED FROM CS2000 SESSON SERVER Meaning: The response received from CS2KSS does not have any data to display System or user actions: None.

Example 8:

```
>qsip 8675309
SIP DATA CANNOT BE DISPLAYED DUE TO QSIP SEND REQUEST
FAILURE
```

Meaning: An error occured while the QSIP sent the query to the CS2KSS.

System or user actions: The user is expected to run QSIP again.

Example 8:

```
>qsip 8675309
PARTIAL DATA RECEIVED FROM THE CS2000 SESSION SERVER.
--------------------------------------------------------------------------------
SIP USER DATA
=============
SIP URI: 6138675309@NORTELNETWORKS.COM
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: N
NUMBER OF CONTACTS: 12
CONTACTS:
SERVICE PACKAGE:
DEFAULT_PKG
SERVICES:
ADHOC 4 ADDRBK 50 VMAIL

SIP LINE DATA
=============
ENDPT ID: PHX/003/0/1000
VMG: vmg
ZONE ID(s): 1234 1234 3456
CLIENT TYPE: ONT
STATIC CLIENT: N

SIP CALL DATA
=============
ACTIVE CALL APPEARANCES:
  NODENO   TERMNO
NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12
--------------------------------------------------------------------------------
```

Meaning: the response from CS2KSS did not have data for all the parameters..

System or user actions: None.

6.10.2.8 Example

Table 16 Usage examples for QSIP command

Description of task	The QSIP command at the CI level will query the CS2KSS to get the SIP information.
Command: MAP response:	Example: QSIP 8731932 10 >qsip 8675309 10 ----------

```
SIP USER DATA
=============
SIP URI: 6138675309@NORTELNETWORKS.COM
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: N
NUMBER OF CONTACTS: 12
CONTACTS: 6138675309@4.3.2.1:5060 6138675309@4.3.2.1:5061
6138675309@1.2.3.4:5062
SERVICE PACKAGE:
DEFAULT_PKG
SERVICES:
ADHOC 4 ADDRBK 50 VMAIL

SIP LINE DATA
=============
ENDPT ID: PHX/003/0/1000
VMG: vmg
ZONE ID(s): 1234 1234 3456
CLIENT TYPE: ONT
STATIC CLIENT: N

SIP CALL DATA
=============
ACTIVE CALL APPEARANCES:
  NODENO   TERMNO
NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12
--------------------------------------------------------------------------------
```

6.11 OSSGate Interface Changes

Not Applicable.

6.12 Security

None.

6.13 Configuration Walkthrough

The following shows a sequence in which the tables are datafilled:

Table SERVRINV (Provisioned through SESM):

*SRVRNAME SRVRADDR **SRVREXEC** SRVRTONE BEARNETS SRVROPTS*
*GWC 0 IP 45 46 47 48 **(DPL_TERM DPLEX)** $ NORTHAA (NET_IP Y)$ $*

Table LGRPINV (Provisioned through SESM)

*LGRP_NO SRVR_NAME **GRPTYPE** LGRPOPT*
*LG 1 1 GWC 5 **SSDPL** $*

Table LNINV (Provisioned through SESM):

LEN CARDCODE PADGRP STATUS GND BNV MNO CARDINFO
LG 1 1 10 13 RDTLSG PKLNL HASU N NL Y NIL

Servord+ Command (Provisioned through SESM):

NEW $ 6212500 IBN BNR 0 0 613 LG 000 0 10 13 DPL 3 SIP_PASSWORD xx SIP_DATA bobby mb1

Table IPAPPL (Provisioned by Crafts person):

InstKey InstName Transport IPDevice IPaddrs port optlist
*1 a sctp eiu 12 12 12 12 4901 (application **sipmtc**)*
(setprime 1)

7: Configuration (CN): A00009037

7.1 Feature Name

CORE - Enhanced ESA for International MG9000

7.2 Hardware and Software Requirements

N/A

7.3 Initial Configuration

N/A

7.4 Office/Subnet parameters (OP/SP) (CM & SESM)

7.5 Upgrade Considerations

N/A

7.6 Data schema (DS) (CM, MIBS, RDB)

7.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ESADGCOD	NEW	NEW

7.6.2 Table/MIB/Remote Database Schema information

7.6.2.1 Name: ESADGCOD

Emergency Stand Alone Digit Analysis Code Table

7.6.2.1.1 Functional description

This table contains customer group information and the digit analysis data that applies to specified types of calls in ESA mode of MG9000. According to datafill in ESADGCOD, number of digits to collect in ESA mode is determined.

7.6.2.1.2 Usage sequence and implications (CM Only)

This table can be datafilled after CUSTENG is datafilled.

7.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ESADGCOD	0	3000	Memory is automatically allocated. Minimum memory consumption if it has no datafill.

7.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for ESADGCOD table.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
KEY	NEW	DGNAME	alphanumeric (up to 16 chars)	Character entries can be entered up to 16 Chars. But, only “IBN_ESA_DEFAULT” and customer group names (datafilled in CUSTENG table) can be accepted.
		FROMD	up to eight digits(0 to 9, B, or C)	From digits.
		TOD	up to eight digits(0 to 9, B, or C)	To Digits
NUMDGTS	NEW	N/A.	Number {0 to 15}	NUMDGTS:Number of digits to collect (including prefix digits).
ADDIGS	NEW	N/A.	up to fifteen digits (0 to 9, B or C)	ADDIGS: The digits stream which will be added to collected digits.
STRIP	NEW	N/A.	Number {0 to 15}	STRIP: Number of digits to be removed from collected digits.

7.6.2.1.5 Datafill example

The following example shows sample datafill for table ESADGCOD.

CUST783 0 0 8 216 1

7.6.2.1.6 Table release history update

N/A.

7.6.2.1.7 Supplementary information

ESADGCOD table has the verify procedure. Therefore, error messages are displayed if wrong datafill is entered. Followings are the error conditions and its error texts:

- If the table is full (which means table has 3000 tuple), new tuple cannot be datafilled, following error is displayed:

  "ESADGCOD TABLE IS FULL"

- If the table if full and telco worker tries to change a subset of existing key with different values. For example, table has following entry:

  CUST783 0 9 10 $ 2

  If the worker tries to change CUST783 3 3 entry with 11 $ 3 values, then table would have

  CUST783 0 2 10 $ 2

  CUST783 3 3 11 $ 3

  CUST783 4 9 10 $ 2

  The tuple is divided into 3 tuples. In this case following error would be displayed:

  "CHANGE operation is not allowed for this subrange."

  "Please change entire tuple range: <dgname> <fromdig> <todig>"

- If the table if full and telco worker tries to delete a subset of existing key. For example, table has following entry:

  CUST783 0 9 10 $ 2

  The worker tries to delete CUST783 5 5 datafill. Then Table would have following entries after deletion.

  CUST783 0 4 10 $ 2

  CUST783 6 9 10 $ 2

  The tuple divided into two tuples. In this case, if the table is full, then following error would be displayed.

"DELETE operation is not allowed for this subrange."

"Please delete entire tuple range: <dgname> <fromdig> <todig>"

- Table ESADGCOD accepts customer group names datafilled in table CUSTENG or accepts "IBN_ESA_DEFAULT" string. For the other conditions, following error would be displayed:

"The DGNAME "given name" is not datafilled in the CUSTENG table."

- TOD field should be greater than or equal to FROMD field. In case of wrong datafill, following error would be displayed:

"The TODIGs must be greater than the FROMDIGs"

- FROMD and TOD fields should contain at least one digit. In case of wrong datafill, following error would be displayed:

"At least one digit must be specified in both

the FROMD and the TOD fields."

- If the FROMD and TOD fields contain invalid digits (D, E, F, N), error would be displayed.

"Invalid digit(s) in field FROMD" if FROMD includes invalid digits.

"Invalid digit(s) in field TOD" if TOD includes invalid digits.

- Since NUMDGTS field indicates the total number of digits which will be dialled by end user, number of digits in FROMD and TOD fields should not be greater than NUMDGTS field. In case of wrong datafill, error message would be displayed:

"Number of digits in FROMD field cannot be greater than NUMDGTS." for FROMD field.

"Number of digits in TOD field cannot be greater than NUMDGTS." for TOD field.

- Telco worker tries to delete a subset of existing key. For example, table has following entry:

CUST783 0 9 4 $ 0

The worker tries to delete CUST783 50055 50055 datafill. Then Table may have following entries if deletion is permitted.

CUST783 0 50054 4 $ 0

CUST783 500056 9 4 $ 0

Since above tuples cannot be accepted, table gives following error and no tuple is deleted.

"DELETE operation is not allowed for this subrange."

"Please delete entire tuple range: <dgname> <fromdig> <todig>"

- STRIP field value cannot be greater than NUMDGTS value. In this case table gives following error message.

  "STRIP value cannot be greater than NUMDGTS value."

- If the ADDIGS field contains invalid digits (D, E, F, N), error would be displayed.

  "Invalid digit(s) in field ADDIGS"

- (Number of digits in ADDIGS field + NUMDGTS - STRIP) value cannot be greater than 15. Otherwise, following error would be displayed:

  "(ADDIGS + NUMDGTS - STRIP) value cannot be greater than 15."

7.6.2.1.8 Translation verification and other tools

N/A.

7.7 Service Orders (SO) (CM & SESM)

N/A.

7.8 Software optionality control (SOC)

N/A.

7.9 Element Management

N/A.

7.10 User interface changes

N/A.

7.11 OSSGate Interface Changes

N/A.

7.12 Security

N/A.

7.13 Configuration Walkthrough

N/A.

8: Configuration (CN): A00009145

8.1 Feature Name

Record Feature Usage

8.2 Hardware and Software Requirements

No new software and hardware requirements.

8.3 Initial Configuration

To generate a billing record for subscriber's feature usage, the option MC611_FOR_RFU in Table AMAOPTS must be set to ON.

8.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

8.5 Upgrade Considerations

None.

8.6 Data schema (DS) (CM, MIBS, RDB)

8.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
AMAOPTS	CHANGED (A new option is defined)	UNCHANGED

8.6.2 Table/MIB/Remote Database Schema information

A new option named MC611_FOR_RFU is created in Table AMAOPTS. This option is set to ON to activate the feature. The default value is OFF for this option.

While activating and deactivatingMC611_FOR_RFU , a warning is printed as given below to indicate the change in the functionality:

For activation (ON state):

“This change results feature action recording

upon subscriber feature actions.”

For deactivation (OFF state):

“This change prevents feature action recording

upon subscriber feature actions.”

8.6.2.1 Datafill example

Figure 1 New AMA option MC611_FOR_RFU in Table AMAOPTS

```
TABLE: AMAOPTS
OPTION SCHEDULE
---------------
...
MC611_FOR_RFU ON
...
```

Figure 2 Activating/deactivating the new option MC611_FOR_RFU

```
>table amaopts
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: AMAOPTS
>pos mc611_for_rfu
MC611_FOR_RFU ON
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
AMASEL: ON
>off
TUPLE TO BE CHANGED:
MC611_FOR_RFU OFF
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
This change prevents feature action recording
upon subscriber feature actions.
TUPLE CHANGED
JOURNAL FILE INACTIVE
>
>
>dis
MC611_FOR_RFU OFF
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
AMASEL: OFF
>on
TUPLE TO BE CHANGED:
MC611_FOR_RFU ON
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
This change results feature action recording
upon subscriber feature actions.
TUPLE CHANGED
JOURNAL FILE INACTIVE
>
```

8.6.2.2 Functional description

This ISN09 activity is targeted to provide recording of the subscriber initiated feature actions in the form of AMA billing records.

It is required that this capability is able to be turned off and on. Therefore, a new AMAOPTS option, MC611_FOR_RFU, is created. When this option is set to ON, a billing record is created for the feature actions (Please refer to the

FN document for the list of supported features and actions) initiated by subscribers. Otherwise, the billing flow is not impacted.

8.7 Service Orders (SO) (CM & SESM)

Not applicable.

8.8 Software optionality control (SOC)

Not applicable.

8.9 Element Management

Not applicable.

8.10 Security

Not applicable.

9: Configuration (CN): A00009216

9.1 Feature Name

JI-ISUP to Base ETSI ISUP V2 Mapping Enhancement

9.2 Hardware and Software Requirements

None

9.3 Initial Configuration

None

9.4 Office/Subnet parameters (OP/SP) (CM & SESM)

None

9.5 Upgrade Considerations

None

9.6 Data schema (DS) (CM, MIBS, RDB)

None

9.7 Service Orders (SO) (CM & SESM)

None

9.8 Software optionality control (SOC)

There is a new SOC option that is introduced with this feature: *NETK Jpn I ISUP Parm Enh***.**

NETK Jpn I ISUP Parm Enh is defined under NETK SOC group. Functionality of the feature is controlled with this SOC option. It is a controlled SOC, whose states can be ON or IDLE. When the state of the *NETK Jpn I ISUP Parm Enh* is ON, feature becomes functional.

The following warning message is displayed when the *NETK Jpn I ISUP Parm Enh* SOC NETK0087 is toggled from state ON to IDLE.

WARNING: DEACTIVATION WILL IMPACT FEATURE A00009216

The table below summarizes the SOC option NETK0087.

Table 1 SOC for Activation of Feature

SOC group:	NETK
SOC option name:	NETK Jpn I ISUP Parm Enh
SOC option title:	NETK Jpn I ISUP Parm Enh
SOC option control type:	state
New SOC option?	Yes
SOC option order code	NETK0087
Option defined in DRU:	WT22
Affected products:	ISN09

9.9 Element Management

None

9.10 User interface changes

None

9.11 OSSGate Interface Changes

None

9.12 Security

None

9.13 Configuration Walkthrough

None

10: Configuration (CN): A00009282

10.1 Feature Name

MG9KEM - International ESA and MLPP Support

10.2 Hardware and Software Requirements

This functionality is for a MG9000 EM running a SN09 or higher software version.

10.3 Initial Configuration

No changes to the initial configuration.

10.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

10.5 Upgrade Impact

10.5.1 Dump and Restore

N/A

10.5.2 Element Management Upgrade

International and MLPP ESA functionality is only applicable if the MG9000 is at a software release of SN09 or higher.

10.6 Data schema (DS) (CM, MIBS, RDB)

N/A

10.7 Service Orders (SO) (CM & SESM)

N/A

10.8 Software optionality control (SOC)

N/A

10.9 Element Management

10.9.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
ESA Config Panel	Changed
ESA Translation List View	Changed

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
ESA Customer Group List View	Changed

10.9.2 GUI information

10.9.2.1 ESA Config Panel

10.9.2.1.1 Functional description

This GUI is being enhanced to remove the reference to the North American market for the “Enhanced” ESA Mode selector. Prior to SN09 Enhanced ESA was only available for the North American Market.

10.9.2.1.2 GUI usage and implications

This is an existing GUI and there are no changes to the order that the GUIs must be datafilled.

10.9.2.1.3 GUI size

N/A

10.9.2.1.4 GUI fields

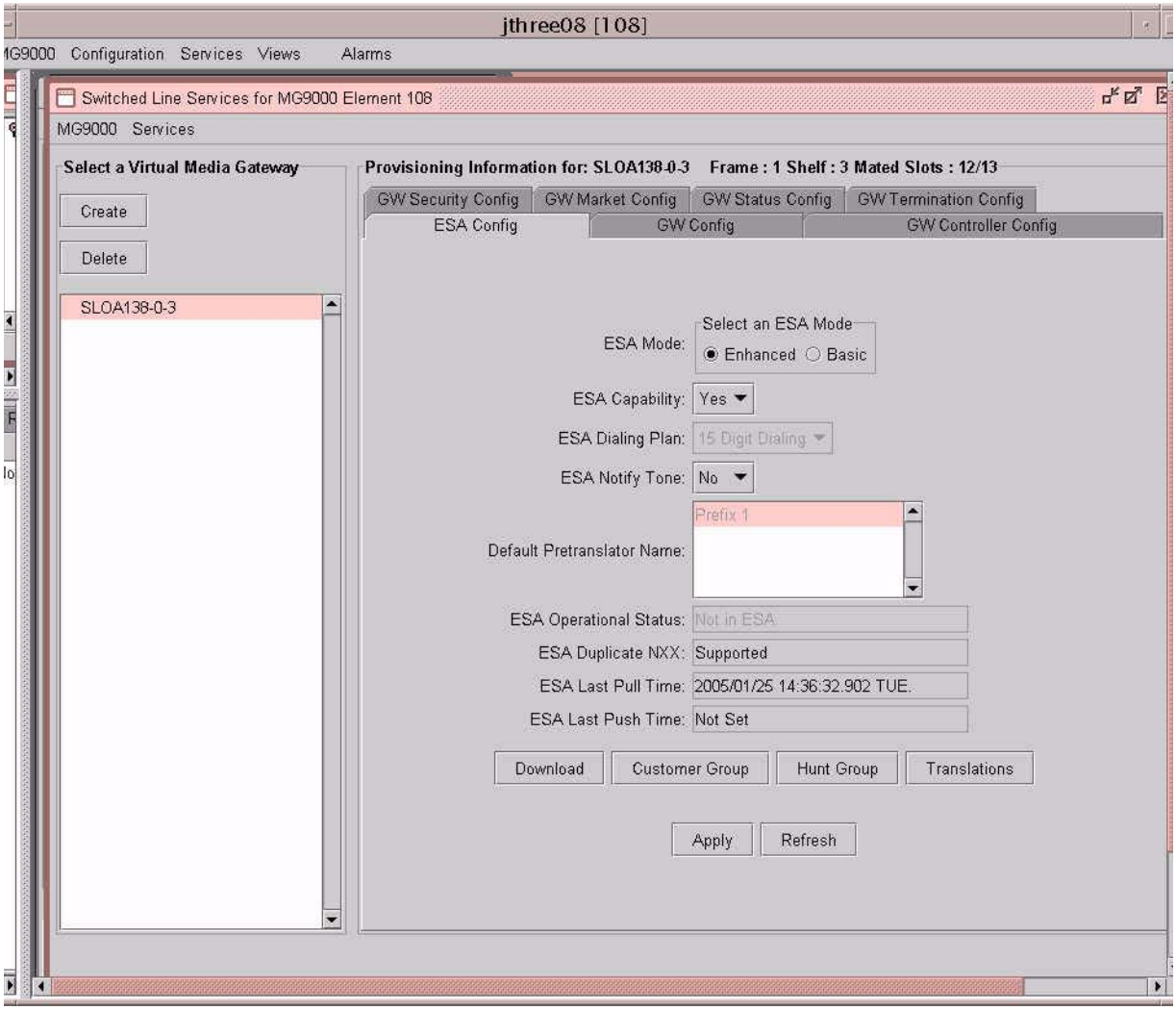
The following table lists the modified fields for the ESA Config Panel

Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
ESA Mode	Changed	N/A	“Enhanced” or “Basic”	The “Enhanced” will use the ESA data provided by the Core. This will be used by both ABI and ITP VMGs. Enhanced ESA can now be used for both the North American and International markets. The “Basic” will work in the same manner that ESA is configured in SN06 using the MG9000 EM for ITP VMGs but will not be supported for ABI VMGs.	None

10.9.2.1.5 Usage example

The following is an example of the new ESA Config Panel:



10.9.2.1.6 GUI release history update

The following fields were modified:

- ESA Mode entry labels

10.9.2.1.7 Supplementary information

None

10.9.2.1.8 CLUI Interface

N/A

10.9.2.2 ESA Translation List View

10.9.2.2.1 Functional description

This GUI is being enhanced to now indicate the source of the CORE translator that the translation entry came from. Also if the translation entry is of the type DGCOD then the existing Digits field will be split in the middle to separate the To and From digits.

10.9.2.2.2 GUI usage and implications

This is an existing GUI and there are no changes to the order that the GUIs must be datafilled. The fields added are for display only.

10.9.2.2.3 GUI size

N/A

10.9.2.2.4 GUI fields

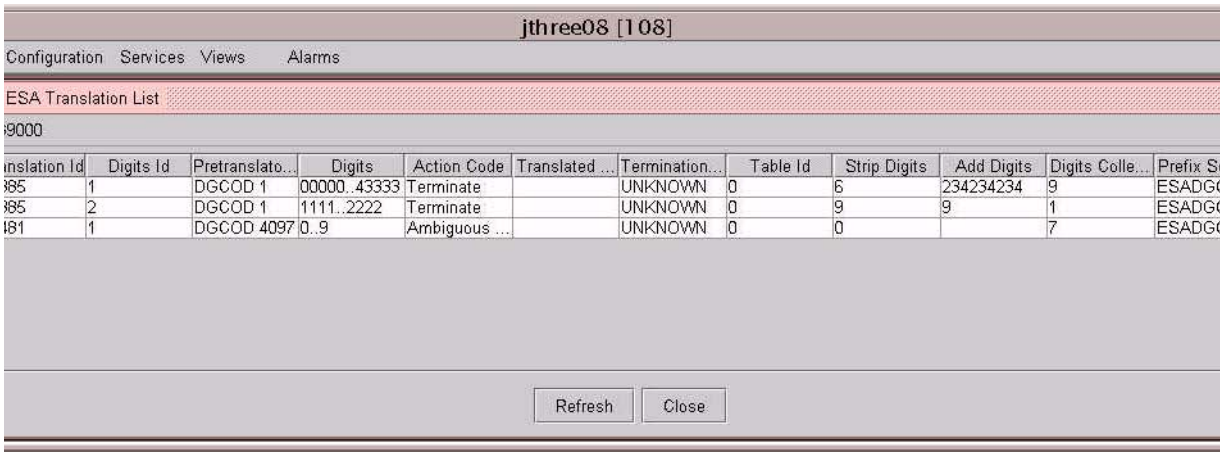
The following table lists the modified fields for the ESA Translation List View

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Source	New	N/A	ESAPLXA IBNXLA and ESADGCOD	Indicates which CORE translator the entry came from.	None
Digits	Changed	N/A	TO..From	For ESADGCOD translation entries this field will display the To and From digits in the 111..222 format.	nnESAPrefix Digits

10.9.2.2.5 Usage example

The following is an example of the new ESA Translation List View:



10.9.2.2.6 GUI release history update

The following fields were added:

- Source

The following fields were modified:

- Digits

10.9.2.2.7 Supplementary information

None

10.9.2.2.8 CLUI Interface

N/A

10.9.2.3 ESA Customer Group List View

10.9.2.3.1 Functional description

This GUI is being enhanced indicate whether the Extension IDs are actually indexes into the EXTN table or the DGCOD table. This will be performed by modifying the existing “Extension ID” column name to “DGCOD ID” when the indexes are for DGCOD.

10.9.2.3.2 GUI usage and implications

This is an existing GUI and there are no changes to the order that the GUIs must be datafilled. The fields added are for display only.

10.9.2.3.3 GUI size

N/A

10.9.2.3.4 GUI fields

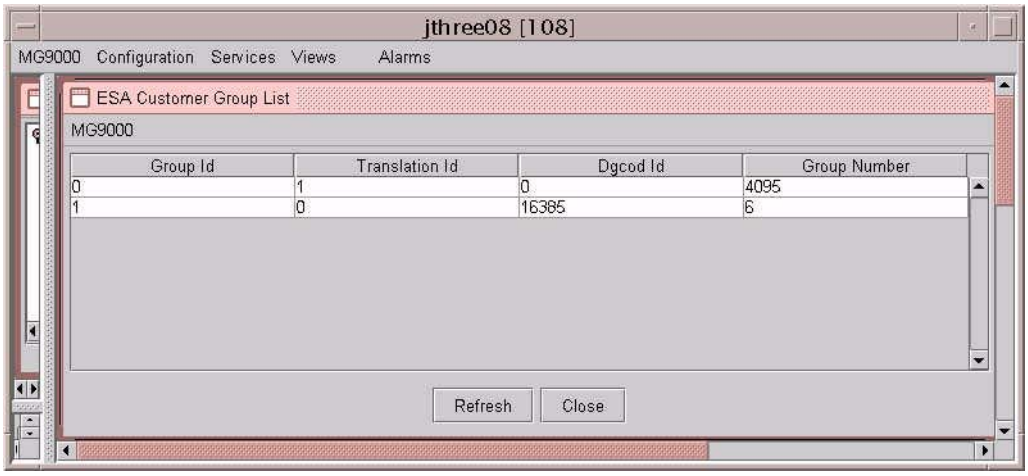
The following table lists the modified fields for the ESA Translation List View

Table 4 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Extension ID/ DGCOD ID	New	N/A	read only	The Extension or DGCOD index.	

10.9.2.3.5 Usage example

The following is an example of the new ESA Translation List View:



10.9.2.3.6 GUI release history update

The Extension ID column name will now read DGCOD ID whenever the indexes are for a DGCOD table, international.

10.9.2.3.7 Supplementary information

None

10.9.2.3.8 CLUI Interface

N/A

10.10 Command interface changes

N/A

10.11 Security

N/A

10.12 Configuration Walkthrough

N/A

11: Configuration (CN): A00009321

11.1 Feature Name

NMC Code Blocking

11.2 Hardware and Software Requirements

N/A

11.3 Initial Configuration

N/A

11.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

11.5 Upgrade Considerations

N/A

11.6 Data schema (DS) (CM, MIBS, RDB)

N/A

11.7 Service Orders (SO) (CM & SESM)

N/A

11.8 Software optionality control (SOC)

N/A

11.9 Element Management

N/A

11.10 User interface changes

11.10.1 Directory: GNWMCODEDIR

11.10.1.1 Directory description

CodeCtrl commands are to List, Apply and Remove code controls. PCT option is available in these code control commands.

11.10.1.2 Accessing directory: GNWMCODEDIR

11.10.1.2.1 Access to directory or MAP level and return to CI

To access: `MAPCI;NMW;CODECTRL`

To return to CI: `QUIT ALL`

11.10.2 Command: LIST

11.10.2.1 Command type: MENU

11.10.2.2 Command target: SUPERNODE

11.10.2.3 Command availability: RES

11.10.2.4 Command description

This command is used to display the active Code Blocking Controls. This list command is executed from the CodeCtrl menu level.

11.10.2.5 Command syntax

Table 1 CODECTRL command parameters and variables

Command	Parameters and variables
List	LIST - list code controls Parms: <CTRL> {CBK <BLOCKTYPE> {PCT, GAP}, PRP, HTRF} <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} [<XLANAME> STRING] [<Code|ALL> STRING]
Parameters and variables	Description
CTRL	Specifies the code control type
BLOCKTYPE	Specifies the Code Block type
XLASYS	Specifies the translation system
[XLANAME]	Specifies the translation name for the specified XLASYS from which the control is to be displayed.
[Code|ALL]	Control(s) should be displayed for the specified Code. ALL specifies that the control should be listed for all code for the specified XLASYS and XLANAME

11.10.2.6 Qualifications and warnings

N/A

11.10.2.7 Responses

11.10.2.7.1 Response

Table 2 MAP outputs with associated meanings and actions

Command
Response: Control not active **Meaning:** There are no controls of that type currently active. **System or user actions:** None.
Response: Specified XLANAME is not valid for specified XLASYS. Check CODE table of speified XLASYS for valid XLANAME values **Meaning:** The specified XLANAME does not exist for the XLASYS which was specified for the control **System actions:** None **User actions:** Check the CODE table to determine what range of XLANAME can be specified.
Response: No matching control **Meaning:** The command was issued with parameters that did not match any applied controls. **System actions:** None **User actions:** Select control parameters which match the control or controls which are required to be listed.

Table 2 MAP outputs with associated meanings and actions

Command
Response: XLA From To Level Ann Block Pass PX CSXLA 8308001 8308004 50.0 NCA 12345 12345 **Meaning:** The command has been entered requesting details of the CBK call percentage control applied to code from 8308001 to 8308004 in XLASYS PX and XLANAME CSXLA. The output shows the details of the control(s) within whose code range the specidied code falls. It shows that the percentage is 50% and that blocked calls are sent to NCA treatment. It also shows that 12345 calls have been blocked by the control and 12345 calls have been passed. **System actions:** The system displayed the data associated with the specified control. **User actions:** None.
Response: CBK GAP Page 1 of 1 XLA From To Level Ann Block Pass PX CSXLA 8308001 8308004 50.0 NCA 12345 12345 **Meaning:** The command has been entered requesting details of the CBK call percentage control applied to code from 8308001 to 8308004 in XLASYS PX and XLANAME CSXLA. The output shows the only one control is currently applied. It shows that the percentage is 50% and that blocked calls are sent to NCA treatment. It also shows that 12345 calls have been blocked by the control and 12345 calls have been passed. **System actions:** The system displayed the data associated with the specified control. **User actions:** None.

11.10.2.8 Example

Table 3 Usage examples for LIST command

Description of task:	Command: MAP response:
all the percentage code blocking controls that applied which enters UXLA with an XLASYS of PX and an XLANAME of CSXLA will be displayed	`LIST CBK PCT PX CSXLA ALL`

Table 3 Usage examples for LIST command

all the percentage code blocking controls that applied which enters UXLA with an XLASYS of PX will be displayed	`LIST CBK PCT PX`
all the percentage code blocking controls that applied which enters UXLA with an XLASYS of PX and an XLANAME of CSXLA and digits starting in the range from '8308001' will be displayed	`LIST CBK PCT PX CSXLA '8308001'`

11.10.3 Command: APPLY

11.10.3.1 Command type: MENU

11.10.3.2 Command target: SUPERNODE

11.10.3.3 Command availability: RES

11.10.3.4 Command description

This command is used to activate a specified control for the XLASYS, XLANAME and digit range. This apply command is executed from the CodeCtrl menu level.

11.10.3.5 Command syntax

Table 4 CODECTRL command parameters and variables

Command	Parameters and variables
Apply	APPLY - add a code control Parms: <CTRL> {CBK <BLOCKTYPE> {PCT <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} <XLANAME> STRING <FROM-CODE> STRING <TO-CODE> STRING <LEVEL> {1 TO 100} <ANN> {NCA, EA1, EA2}, GAP <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} <XLANAME> STRING <FROM-CODE> STRING <TO-CODE> STRING <GAP> STRING <ANN> {NCA, EA1, EA2}}, PRP <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} <XLANAME> STRING <FROM-CODE> STRING <TO-CODE> STRING, HTRF <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} <XLANAME> STRING <FROM-CODE> STRING <TO-CODE> STRING}

Table 4 CODECTRL command parameters and variables

Command	Parameters and variables
CTRL	Specifies the code control type
BLOCKTYPE	Specifies the Code Block type
XLASYS	Specifies the translation system
XLANAME	Specifies the translation name for the specified XLASYS from which the control is to be displayed.
From-Code	Specifies the start of the code range to which the control is being applied
To-Code	Specifies the end of the code range to which the control is to be applied
GAP	Specifies the gapping period (in seconds) for a CBK control of GAP flavor. Specified as a string of digits with a single decimal place
LEVEL	Specifies the percentage (in percent) for a CBK control of PCT.
ANN	Specifies the treatment to which blocked calls are to be sent

11.10.3.6 Qualifications and warnings

N/A

11.10.3.7 Responses

11.10.3.7.1 Response

Table 5 MAP outputs with associated meanings and actions

Command
Response: OK **Meaning:** The command has been successful. **System actions:** The specified control is applied. **user actions:** None.
Response: Specified XLANAME is not valid for specified XLASYS. Check CODE table of specified XLASYS for valid XLANAME values. **Meaning:** The specified XLANAME does not exist for the XLASYS which was specified for the control **System actions:** None **User actions:** Check the CODE table to determine what range of XLANAME can be specified.

Table 5 MAP outputs with associated meanings and actions

Command
Response: Start of digits range (FROM-CODE) must be less than end of digit range (TO-CODE). **Meaning:** The user entered FORM-CODE digits which were greater than the TO-CODE digits. It should be noted that this is not a numerical relationship. For example, the specification FORM-CODE=157 and TO-CODE=16 is valid because the 16 will be treated as 169 in digit terms and hence the control will apply to digit range 157, 158, 159 ... 169. However, the specification FORM-CODE=16 and TO-CODE=157 is invalid because in digit terms 16 (treated as 160) comes after 157. **System actions:** None **User actions:** Change the digits range specification accordingly.
Response: No room to add control. **Meaning:** The maximum number of controls have been defined, there are no available resources to add a further control. **System actions:** None **User actions:** Remove an existing control to enable new control to be added.
Response: Value not in range ‘0.0’ to ‘600.0’ **Meaning:** The GAP time speified is not within the range 0.0 seconds to 600.0 seconds. The period must be within these bounds specified in increments of 0.1. **System actions:** None. **User actions:** Re-enter the command specifying a valid GAP period.
Response: Can not apply: Control is already active in code range **Meaning:** Code control(s) is already active for the specified XLASYS, XLANAME and part or all of the specified digit range. **System actions:** None. **User actions:** Delete the pre-existing control(s) and re-enter the new control; delete the pre-existing control(s) and re-apply it over a different range which does not confilict with the new control and then apply the new control; or re-apply the new control with a digit range which does not overlap the existing control(s).

Table 5 MAP outputs with associated meanings and actions

Command
Response: Out of range: <LEVEL> {1 TO 100} **Meaning:** The percentage specified is not within the range 1 percent to 100 percent. **System actions:** None. **User actions:** Re-enter the command specifying a valid percentage.
Response: Memory allocate failed **Meaning:** No memory is allocated to store the Mass Call Control information. **System actions:** None. **User actions:** Reboot the switch or run NWMMCTCI IPL.

11.10.3.8 Example

Table 6 Usage examples for APPLY command

Description of task:	Command: MAP response:
In this example, only 50 percent of calls which enters UXLA with an XLASYS of PX and XLANAME of CSXLA with called party digits starting in range from ’8308001’ to ’8308004’ will be allowed to complete, all other calls will be sent to NCA treatment.	`APPLY CBK PCT PX CSXLA '8308001' '8308004' 50 NCA`
In this example, only one call per 60 seconds which enters UXLA with an XLASYS of PX XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’ will be allowed to complete, all other calls will be sent to NCA treatment.	`APPLY CBK GAP PX CSXLA '8308001' '8308004' '60.0' NCA`

11.10.4 Command: REMOVE

11.10.4.1 Command type: MENU

11.10.4.2 Command target: SUPERNODE

11.10.4.3 Command availability: RES

11.10.4.4 Command description

This command is used to remove a code control of specified type from the given XLASYS, XLANAME and digit range. If ALL digits are specified then all controls of the specified type will be removed from the given XLASYS and XLANAME. This remove command is executed from the CodeCtrl menu level.

11.10.4.5 Command syntax

Table 7 CODECTRL command parameters and variables

Command	Parameters and variables
Remove	REMOVE - delete a code control Parms: <CTRL> {CBK <BLOCKTYPE> {PCT, GAP}, PRP, HTRF} <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} <XLANAME> STRING <From-Code|ALL> STRING [<To-Code> STRING]
Parameters and variables	Description
CTRL	Specifies the code control type
BLOCKTYPE	Specifies the Code Block type
XLASYS	Specifies the translation system to which the control is to be applied
XLANAME	Specifies the translation name for the specified XLASYS to which the control is to be applied
[From-Code|ALL]	If a control is being removed from a specific code range, specifies the start of the code range. ALL specifies that the control should be removed from all code ranges for the specified XLASYS and XLANAME
[To-Code]	If a From-Code is specified then specifies the end of the code range from which the control is to be removed

11.10.4.6 Qualifications and warnings

N/A

11.10.4.7 Responses

11.10.4.7.1 Response

Table 8 MAP outputs with associated meanings and actions

Command
Response: OK **Meaning:** The command has been successful. **System actions:** The specified control is removed either from the specified code range for the given XLASYS and XLANAME or from ALL code ranges for the specified XLASYS and XLANAME. The status display is updateed accordingly. **user actions:** None.
Response: Control not active **Meaning:** The command was issued with parameters that did not match any currently active controls. **System actions:** None **User actions:** Select control parameters which match the control or controls which are required to be removed.
Response: Specified XLANAME is not valid for specified XLASYS. Check CODE table of specified XLASYS for valid XLANAME values **Meaning:** The specified XLANAME does not exist for the XLASYS which was specified for the control **System actions:** None **User actions:** Check the CODE table to determine what range of XLANAME can be specified..
Response: TO-CODE digits must be specified **Meaning:** If the user entered FROM-CODE digits then the TO-CODE digits must be specified in order that a control can be removed. **System actions:** None **User actions:** Remove an existing control to enable new control to be added.

Table 8 MAP outputs with associated meanings and actions

Command
Response: Start of digits range (FROM-CODE) must be less than end of digit range (TO-CODE). **Meaning:** The user entered FORM-CODE digits which were greater than the TO-CODE digits. It should be noted that this is not a numerical relationship. For example, the specification FORM-CODE=157 and TO-CODE-16 is valid because the 16 will be treated as 169 in digit terms and hence the control will apply to digit range 157, 158, 159... 169. However, the specification FORM-CODE=16 and TO-CODE=157 is invalid because in digit terms 16 (treated as 160) comes after 157. **System actions:** None **User actions:** Change the digits range specification accordingly.
Response: Memory allocate failed **Meaning:** No memory is allocated to store the Mass Call Control information. **System actions:** None. **User actions:** Reboot the switch or run NWMMCTCI IPL.

11.10.4.8 Example

Table 9 Usage examples for REMOVE command

Description of task:	Command: MAP response:
In this example, the percentage code blocking control which enters UXLA with an XLASYS of PX and XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’will be removed.	`REMOVE CBK PCT PX CSXLA '8308001' '8308004'`
The gapping code blocking control which enters UXLA with an XLASYS of PX and XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’will be removed.	`REMOVE CBK GAP PX CSXLA '8308001' '8308004'`

Table 9 Usage examples for REMOVE command

All the percentage code blocking control with an XLASYS of PX and XLANAME of CSXLA with digits starting in range from will be removed.	REMOVE CBK PCT PX CSXLA ALL
All the gapping code blocking control with an XLASYS of PX and XLANAME of CSXLA with digits starting in range from will be removed.	REMOVE CBK GAP PX CSXLA ALL

11.10.5 Command: MASSCALL

11.10.5.1 Command type: MENU

11.10.5.2 Command target: SUPERNODE

11.10.5.3 Command availability: RES

11.10.5.4 Command description

This Mass Call CI command applies, removes or lists various MC controls without necessarily accessing the NWM menus. The command alias is MASSCALL. The MASSCALL command uses a selection of the same parameters as the CBK, PRP, HTRF and STR controls of the CodeCtrl and GrpCtrl menus.

In this feature, PCT is implemented as a new CBK option which provide the capability to block calls with percentage. The syntax of MASSCALL command is changed to add this new option.

11.10.5.5 Command syntax

Table 10 MASSCALL command parameters and variables

Command	Parameters and variables
MASSCALL	Masscall - Envoke a mass calling control Parms: <Action> {LIST <CTRL> {CBK <BLOCKTYPE> {PCT <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} [<XLANAME> STRING] [<Code|ALL> STRING], GAP <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} [<XLANAME> STRING] [<Code|ALL> STRING]}, HTRF <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} [<XLANAME> STRING] [<Code|ALL> STRING], PRP <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} [<XLANAME> STRING] [<Code|ALL> STRING], STR <fsclli|ALL> STRING}, APPLY <Cntrl> {CBK <BLOCKTYPE> {PCT <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} <XLANAME> STRING <FROM-CODE> STRING <TO-CODE> STRING <LEVEL> {1 TO 100} <ANN> {NCA, EA1, EA2},

Table 10 MASSCALL command parameters and variables

Command	Parameters and variables
MASSCALL	GAP <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} <XLANAME> STRING <FROM-CODE> STRING <TO-CODE> STRING <GAP> STRING <ANN> {NCA, EA1, EA2}}, HTRF <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} <XLANAME> STRING <FROM-CODE> STRING <TO-CODE> STRING, PRP <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} <XLANAME> STRING <FROM-CODE> STRING <TO-CODE> STRING, STR <fsclli> STRING <Lev1> {0 TO 63} [<Lev2> {0 TO 63}] [<Level> {0 TO 100}]}, REMOVE <CNTRL> {CBK <BLOCKTYPE> {PCT <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} <XLANAME> STRING <From-Code|ALL> STRING [<To-Code> STRING], GAP <XLASYS> {AC, PX, CT, FA, OFC, FT,

Table 10 MASSCALL command parameters and variables

Command	Parameters and variables
MASSCALL	NSC} <XLANAME> STRING <From-Code|ALL> STRING [<To-Code> STRING]}, HTRF <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} <XLANAME> STRING <From-Code|ALL> STRING [<To-Code> STRING], PRP <XLASYS> {AC, PX, CT, FA, OFC, FT, NSC} <XLANAME> STRING <From-Code|ALL> STRING [<To-Code> STRING], STR <fsclli|ALL> STRING}}
Parameters and variables	Description
ACTION	Specifies the action to be performed on the specific control type.
CTRL	Specifies the code control type
BLOCKTYPE	Specifies the Code Block type
XLASYS	Specifies the translation system to which the control is to be applied
XLANAME	Specifies the translation name for the specified XLASYS to which the control is to be applied
Code|ALL	If a control is being listed from a code specifies the code. ALL specifies that the control should be listed for all code for the specifies XLASYS and XLANAME
From-Code	Specifies the start of the code range to which the control is being applied or removed.
To-Code	Specifies the end of the code range to which the control is to be applied or removed.
GAP	Specifies the gapping period (in seconds) for a CBK control of GAP flavor. Specified as a string of digits with a single decimal place
LEVEL	Specifies the percentage for a CBK control of PCT.
ANN	Specifies the treatment to which blocked calls are to be sent

Table 10 MASSCALL command parameters and variables

Command	Parameters and variables
fsclli	This list of up to 9 variables identifies the trunk groups which are to be acted upon (used for STR control).
ALL	Specifies that all trunks group datafilled in table CLLIMTCE which have CTRL active are to be displayed or removed. (used for STR control).
Lev1	The upper trunk group reservation threshold (used for STR control).
[Lev2]	The lower trunk group reservation threshold (used for STR control).
[Level]	Percentage of traffic to be affected when thresholds are reached (used for STR control).

11.10.5.6 Qualifications and warnings

N/A

11.10.5.7 Responses

11.10.5.7.1 Response

All response are the same as those for the respective CODECTRL level commands.

11.10.5.8 Example

Table 11 Usage examples for MASSCALL command

Description of task:	Command: MAP response:
all the percentage code blocking controls that applied which enters UXLA with an XLASYS of PX and an XLANAME of CSXLA will be displayed	`MASSCALL LIST CBK PCT PX CSXLA ALL`
all the percentage code blocking controls that applied which enters UXLA with an XLASYS of PX will be displayed	`MASSCALL LIST CBK PCT PX`
all the percentage code blocking controls that applied which enters UXLA with an XLASYS of PX and an XLANAME of CSXLA and digits starting in the range from `8308001' will be displayed	`MASSCALL LIST CBK PCT PX CSXLA ‘8308001’`
In this example, only 50 percent of calls which enters UXLA with an XLASYS of PX and XLANAME of CSXLA with called party digits starting in range from ’8308001’ to ’8308004’ will be allowed to complete, all other calls will be sent to NCA treatment.	`MASSCALL APPLY CBK PCT PX CSXLA '8308001' '8308004' 50 NCA`

Table 11 Usage examples for MASSCALL command

In this example, only one call per 60 seconds which enters UXLA with an XLASYS of PX XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’ will be allowed to complete, all other calls will be sent to NCA treatment.	`MASSCALL APPLY CBK GAP PX CSXLA '8308001' '8308004' '60.0' NCA`
In this example, the percentage code blocking control which enters UXLA with an XLASYS of PX and XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’will be removed.	`MASSCALL REMOVE CBK PCT PX CSXLA '8308001' '8308004'`
The gapping code blocking control which enters UXLA with an XLASYS of PX and XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’will be removed.	`MASSCALL REMOVE CBK GAP PX CSXLA '8308001' '8308004'`
All the percentage code blocking control with an XLASYS of PX and XLANAME of CSXLA with digits starting in range from will be removed.	`MASSCALL REMOVE CBK PCT PX CSXLA ALL`
All the gapping code blocking control with an XLASYS of PX and XLANAME of CSXLA with digits starting in range from will be removed.	`MASSCALL REMOVE CBK GAP PX CSXLA ALL`

11.11 OSSGate Interface Changes

N/A

11.12 Security

N/A

11.13 Configuration Walkthrough

N/A

12: Configuration (CN): A00009322

12.1 Feature Name

Call Lock and Do Not Disturb Enhancements

12.2 Hardware and Software Requirements

N/A

12.3 Initial Configuration

N/A

12.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

12.5 Upgrade Considerations

N/A

12.6 Data schema (DS) (CM, MIBS, RDB)

12.6.1 New/modified tables, MIBs, or Database Schema

ISERVOPT table is modified.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ISERVOPT	**CHANGED**	UNCHANGED

12.6.2 Table/MIB/Remote Database Schema information

Call Lock

12.6.2.1 Name: ISERVOPT

This table is used to configure switch wide information for service related feature.

12.6.2.1.1 Functional description

This activity extends the ILRCLS and CEPTPW tuple of the table ISERVOPT. Two new fields are added to ILRCLS tuple named ALLOW_ORIG_AFTER_DEACT and OVERRIDE_ILR_CLASS. And a new field is added to CEPTPW tuple named NEW_PWD_ONCE. The default value for these fields are ‘N’.

Fields of the ILRCLS tuple:

ALLOW_ORIG_AFTER_DEACT{BOOLEAN}: This field determines if the dial tone will be generated instead of confirm tone. If it is set as ‘Y’, dial tone is generated and the user can originate a new call directly after the successful deactivation without going on hook. Otherwise, confirm tone is generated. The default value for the field is ‘N’.

OVERRIDE_ILR_CLASS{BOOLEAN}: This field determines whether the user can overwrite the class of restriction when activating the ILR option without doing a ILR deactivation first or not. If it is set as ‘Y’, the user can overwrite the class of restriction, otherwise can’t. The default value for the field is ‘N’.

NEW_PWD_ONCE{BOOLEAN}: This field determines whether the user can change the password by the dialing sequence LH DT*SC*PWO*PWN#CT or not. If it is set as ‘Y’, the user can change the password by this dialing sequence. Otherwise the subscriber can change the password by the dialing sequence LH DT*SC*PWO*PWN*PWN#CT. The default value for the field is ‘N’.

AUTO_UNLOCK{BOOLEAN}: indicates whether the information of locked user will be recorded and the locked user will be unlocked in the following day automatically. If it is set as ‘Y’, the locked user will be unlocked automatically in the following day. The default value for the field is ‘N’.

12.6.2.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

12.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	0	1	

12.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for ISERVOPT.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ALLOW_ORIG_AFTER_DEACT	NEW		ILRCLS	Determines if the dial tone will be generated instead of confirm tone.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OVERRIDE_ILR_CLASS	NEW		ILRCLS	Determines whether the user can overwrite the class of restriction when activating the ILR option without doing a ILR deactivation first or not.
NEW_PWD_ONCE	NEW		CEPTPW	Determines whether the user can change the password by the dialing sequence LH DT*SC*PWO*PWN#CT or not.
AUTO_UNLOCK	NEW		CEPTPW	Determines whether the locked user can be unlocked in the following day.

12.6.2.1.5 Datafill example

The following example shows sample datafill for table ISERVOPT.

Figure 1 The view of ILRCLS Tuple in ISERVOPT Table

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ilrcls
OPTION:
>ilrcls
ILR_PROG:
>n
SDT:
>n
CR_PSWD:
>y
SHOW_CHG_PSWD:
>y
ALLOW_ORIG_AFTER_DEACT:
>y
OVERRIDE_ILR_CLASS:
>y
TUPLE TO BE ADDED:
            ILRCLS ILRCLS N N Y Y Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
...
```

Figure 2 The view of CEPTPW Tuple in ISERVOPT Table

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ceptpw
OPTION:
>ceptpw
MAX_PIN_RETRY:
>3
DEFAULT_PIN:
>1111
PIN_VALID:
>n
COLLECT_DNPIN_IN_DIFF_STAGES:
>n
ANNOUNCE:
>n
NEW_PWD_ONCE:
>y
AUTO_UNLOCK:
>y
TUPLE TO BE ADDED:
            CEPTPW CEPTPW 3 1111 N N N Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

12.6.2.1.6 Table release history update

None

12.6.2.1.7 Supplementary information

None

12.6.2.1.8 Translation verification and other tools

None

Do Not Disturb

12.6.2.2 Name: ISERVOPT

This table is used to configure switch wide information for service related feature.

12.6.2.2.1 Functional description

This activity introduce a new tuple CDND into the table ISERVOPT. A new field is added to CDND tuple named ALLOW_ORIG_AFTER_DEACT. The default value for this field is ‘N’.

Field of the CDND tuple:

ALLOW_ORIG_AFTER_DEACT {BOOLEAN}: indicates that the dial tone will be generated or confirm tone will be generated after the deactivation activity. If it is set as ‘Y’, dial tone is generated. Otherwise, confirm tone is generated. The default value for the field is ‘N’.

12.6.2.2.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

12.6.2.2.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	0	1	

12.6.2.2.4 Fields/OIDs

The following table lists fields/OIDs for ISERVOPT.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ALLOW_ORIG_AFTER_DEACT	NEW		CDND	Determines if the dial tone will be generated instead of confirm tone.

12.6.2.2.5 Datafill example

The following example shows sample datafill for table ISERVOPT.

Figure 3 :Example of ISERVOPT table datafill

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>CDND
OPTION:
>CDND
ALLOW_ORIG_AFTER_DEACT:
>y
TUPLE TO BE ADDED:
CDND CDND Y

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
...
```

12.6.2.2.6 Table release history update

None

12.6.2.2.7 Supplementary information

None

12.6.2.2.8 Translation verification and other tools

None

12.7 Service Orders (SO) (CM & SESM)

None

12.8 Software optionality control (SOC)

None

12.9 Element Management

None

12.10 User interface changes

None

12.11 OSSGate Interface Changes

None

12.12 Security

None

12.13 Configuration Walkthrough

None

13: Configuration (CN): A00009489

13.1 Feature Name

CHT: Call Waiting Enhancement

13.2 Hardware and Software Requirements

N/A

13.3 Initial Configuration

In table OFCVAR, tuple CWT_TONE_CYCLE_TIME should be set to 2, which is the inteval between the begining of CWT tone A and CWT tone B.

13.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

13.5 Upgrade Considerations

N/A

13.6 Data schema (DS) (CM, MIBS, RDB)

13.6.1 New/modified tables, MIBs, or Database Schema

ISERVOPT table is modified.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ISERVOPT	**CHANGED**	UNCHANGED

13.6.2 Table/MIB/Remote Database Schema information

Call Waiting Tone

13.6.2.1 Name: ISERVOPT

This table is used to configure switch wide information for service related feature.

13.6.2.1.1 Functional description

This activity extends the ICWT tuple of the table ISERVOPT. Two new fields are added to ICWT tuple: ICWT_2PTY_TONE_B and ICWT_DFLT_RCODE. The default value for these fields are ‘N’.

Fields of the ICWT tuple:

ICWT_2PTY_TONE_B{BOOLEAN}: This field determines whether the Call Waiting Tone B shall be applied to both talking side infinitely after the Call Waiting Tone A is applied to the ICWT subscriber called by waiting side. If it is datafilled as ‘Y’, CWT B will be applied. The default value for the field is ‘N’.

ICWT_DFLT_RCODE{BOOLEAN}: This field determines whether R-code is needed when the controller flash hook to toggle between held parties. If it is datafilled as ‘Y’, the subscriber can toggle between held parties without any R-Code. The default value for the field is ‘N’.

13.6.2.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

13.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	0	1	

13.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for ISERVOPT.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ICWT_2PTY_TONE_B	NEW		ICWT	Determines whether the Call Waiting Tone B shall be applied to both talking side infinitely after the Call Waiting Tone A is applied to the ICWT subscriber called by waiting side
ICWT_DFLT_RCODE	NEW		ICWT	Determines whether R-code is needed when the controller flash hook to toggle between held parties.

13.6.2.1.5 Datafill example

The following example shows sample datafill for table ISERVOPT.

When ICWT_2PTY_TONE_B is changed from ‘N’ to ‘Y’, a warning message will be displayed: ‘* WARNNING * - If icwt_2pty_tone_b is datafilled YES, field icwt_ignore_waiting_tmo will be disabled.’.

When ICWT_DFLT_RCODE is changed from ‘N’ to ‘Y’, a warning message will be displayed: ‘If icwt_dflt_rcode is datafilled YES, only TOGGLE ACTION is supported, and Rcode tuple with toggle action in table ISERVOPT should be datafilled.’.

Figure 1 The view of ICWT Tuple in ISERVOPT Table

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>icwt
OPTION:
>icwt
ICWT_IGNORE_WAITING_TMO:
>11
ICWT_ANN_ACTIVE:
>y
ICWT_TMO_ANN_ACTIVE:
>y
ICWT_TIMEOUT_TREATMENT:
>BUSY
ICWT_2PTY_TONE_B:
>y
ICWT_DFLT_RCODE:
>y
* WARNNING * -
If icwt_2pty_tone_b is datafilled YES,
field icwt_ignore_waiting_tmo will be disabled.
* WARNNING * -
If icwt_dflt_rcode is datafilled YES,
only TOGGLE ACTION is supported, and Rcode tuple with
toggle action in table ISERVOPT should be datafilled.
TUPLE TO BE ADDED:
                ICWT
                                        ICWT 11 Y Y BUSY Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
...
```

13.6.2.1.6 Table release history update

None.

13.6.2.1.7 Supplementary information
None

13.6.2.1.8 Translation verification and other tools
None

International Three Way Calling

13.6.2.2 Name: ISERVOPT
This table is used to configure switch wide information for service related features.

13.6.2.2.1 Functional description
This activity introduces a new tuple I3WC into the table ISERVOPT. A new field is added to I3WC tuple named I3WC_DFLT_RCODE. The default value for this field is ‘N’.

Field of the I3WC tuple:

I3WC_DFLT_RCODE {BOOLEAN}: This field determines whether R-code is needed in I3WC feature. If it is datafilled as ‘Y’, the subscriber can setup a 3-way conference by hook-flash only without dialing any R-Code and in 3-way conference, the subscriber can disconnect part C by hook-flash only without dialing RCODE. The default value for the field is ‘N’.

Usage sequence and implications (CM Only)
There is no requirement to datafill tables in a specific order.

13.6.2.2.2 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	0	1	

13.6.2.2.3 Fields/OIDs
The following table lists fields/OIDs for ISERVOPT.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
I3WC_DFLT_RCODE	NEW		I3WC	Determines if RCODE is needed in I3WC feature.

13.6.2.2.4 Datafill example

The following example shows sample datafill for table ISERVOPT.

When I3WC_DFLT_RCODE is changed from 'N' to 'Y', two warning messages will be displayed: 'RCODE tuple in table ISERVOPT must exist and the ACTION CON_3WC and DISC_ACT must be datafilled.' and 'Default RCODE only supports CON_3WC and DISC_ACT actions.'

Figure 2 :Example of ISERVOPT table datafill

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>I3WC
OPTION:
>I3WC
I3WC_DFLT_RCODE:
>y
TUPLE TO BE ADDED:
I3WC I3WC Y

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
* WARNNING * - RCODE tuple in table ISERVOPT must exist and the
ACTION CON_3WC and DISC_ACT must be datafilled.
* WARNNING * - Default RCODE only supports CON_3WC and
DISC_ACT actions.
TUPLE ADDED
```

13.6.2.2.5 Table release history update

13.6.2.2.6 Supplementary information

None

13.6.2.2.7 Translation verification and other tools

None

13.7 Service Orders (SO) (CM & SESM)

None

13.8 Software optionality control (SOC)

None

13.9 Element Management

None

13.10 User interface changes

None

13.11 OSSGate Interface Changes

None

13.12 Security

None

13.13 Configuration Walkthrough

None

14: Configuration (CN): A00013275

14.1 Hardware and Software Requirements

CS2M: SESM091FC

GWC: GI091FC or GN091FC dependant on market.

CM: PSNW09BS + SN09.1 2K LGRP patch.

> ***Note 1:*** The CM patch is required to provide 2K LGRP Line GW support for the Audiocodes Mediant 8000 TP6310 card configured as a large line GW. This patch is not required where the TP6310 is to be configured as a Trunk GW.

14.2 Initial Configuration

CS2M and GWC components must be running the SN09.1FC software loads.

CM must be running the PSNW09BS with the 2K LGRP patch if provisioning of the Audiocodes Mediant 8000 TP6310 cards as large line GWs is required.

No patch is required if the TP6310 cards are to be used as Trunk GWs.

There are no additional initial configuration steps.

14.3 Office/Subnet parameters (OP/SP) (CM & SESM)

None.

14.4 Upgrade Considerations

For CS2M upgrade from versions 8.0, 9.0 to SN09.1.

14.4.1 Dump and Restore (CM)

Refer to feature A00013286.

14.4.2 Element Management Upgrade

For CS2M upgrade from versions 8.0, 9.0 to SN09.1.

No additional upgrade steps are required to the CS2M over and above the normal upgrade procedure.

14.4.3 Downgrade impact

None.

14.5 Data schema (DS) (CM, MIBS, RDB)

Unchanged.

14.6 Service Orders (SO) (CM & SESM)

14.6.1 Line equipment format changes

14.6.1.1 LEN

Provisioning of 2K LGRPs results in an extension to the existing LEN range supported for LL_3RDPTY LGRPs.

Lens will be of the format:

<LGRP> TT tt

TT = 00 .. 20

tt = 00 .. 99 where TT < 20

tt = 00 .. 46 where TT = 20

The LGRP is a valid entry from CM table LGRPINV formed from the SITE + frame number + shelf number where

SITE = a valid entry from the CM table SITE.

frame number = logical frame number in range 00 .. 99

shelf number = logical shelf number in range 0 .. 9

For the Audiocodes TP6310 card provisioned as a large line GW a subset of the available LEN range will be required to support the full endpoint range (2016 endpoints / LENs in total). LEN assignment is user defined using functionality provided by features A00007071 / A00007072 however it is recommended that LENs are mapped directly to endpoints and run in the range: <lgrp> 00 00 ... <lgrp> 20 15.

14.6.1.2 Media gateway endpoint format

The Audiocodes Mediant 8000 TP6310 card provisioned as a large line GW supports endpoints for the format:

tp/nnnn where nnnn is in the range 1 ... 2016 is not padded.

i.e: tp/1 ... tp/2016

14.7 Software optionality control (SOC)

Unchanged.

14.8 Element Management

The CS2M configuration manager: GWCEM has been modified to support the provisioning of large line GWs with a capacity of up to 2047 endpoints within a single LGRP.

The CS2M configuration manager: GWCEM has been modified to support the provisioning of the Audiocodes Mediant 8000 TP6310 card configured as either a large line or a trunk GW.

14.8.1 New/modified GUIs

Unchanged.

14.8.2 Change To Certificate Model For Large Line GWs

This feature has modified the certificate schema used to process gateway certificates from that originally introduced by feature A00007071 and A00007072. Going forwards all creators of gateway certificate profiles designed for large line GWs must include LGRP Size support when generating a certificate.

Directly following the <LgrpType> tag value pair a new field <LgrpSize> is introduced. This must be set to one of the following 2 settings:

- <LgrpSize>1024</LgrpSize>
- <LgrpSize>2048</LgrpSize>

In the current release LgrpSize is directly coupled to LgrpType and the 2 must be aligned based on the following table.

Table 1: LgrpType To LgrpSize Alignment

LgrpType	LgrpSize
S	1024
M	1024
C	1024
LL_3RDPTY	1024
CALIX_C7	1024
SSDPL	1024
LL_3RDPTY_2K	2048

Any incorrect alignment of LgrpType against LgrpSize will result in either a reduction of capacity or wastage of resources.

Note 1: To maintain backwards compatibility with existing 3rd party gateway profile certificates, should the LgrpSize tag be missing from a large line GW certificate, it is assumed that the required size is 1024.

Note 2: It is forbidden to include the LgrpSize tag into gateway profiles that are not intended to support large line GWs.

14.9 User interface changes

Unchanged.

14.10 OSSGate Interface Changes

14.10.1 XML Command Changes

Extension to LEN range indirectly impacts the addLineEndpoint and delLineEndpoint interfaces. The circuitNumber tag within these interfaces will support a greater range of associated LENs.

For the TP6310 configured as a large line GW the endpoint range will be tp/1 ... tp/2016.

The TP6310 configured as a Trunk GW indirectly impacts the addCarrier and deleteCarrier interfaces as follows:

CarrierName field may be in range E1/01 ... E1/63 or DS1/01 ... DS1/84

DPNSS IID field may be in the range 1 ... 63 for E1 carriers.

14.10.1.1 Command XML

Figure 1 addLineEndpoint - Endpoint In Upper Half Of 2K LGRP

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
    <Command>
        <Interface>cs2kCfgMgrIf</Interface>
        <Methods>
            <addLineEndpoint usn="1" version="1.0">
                <Parameters>
                    <mgUIName>audiocodes1.com</mgUIName>
                    <endpointName>tp/2016</endpointName>
                    <circuitNumber>2015</circuitNumber>
                    <cardCode>GWLPOT</cardCode>
                    <padGroup>PKNIL</padGroup>
                    <ground>N</ground>
                </Parameters>
            </addLineEndpoint>
        </Methods>
    </Command>
</CommandList>
```

circuitNumber range is in range 0 - 2047 for a 2K LGRP
endpointName range increased due to large LGRP address space

Table 1 XML Command Tag Descriptions

tag name	description of valid values
endpointName	endpointName in range tp/1 ... tp/2016 for TP6310 large line GW
circuitNumber	circuitNumber in range 0 ... 2047 for 2K LGRP. Recommend 0 ... 2015 for TP6310 large line GW.

All other command tags are unchanged.

Figure 2 addLineEndpoint - Endpoint In Upper Half Of 2K LGRP

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
      <Command>
            <Interface>cs2kCfgMgrIf</Interface>
            <Methods>
                  <delLineEndpoint usn="1" version="1.0">
                        <Parameters>
                              <mgUIName>audiocodes1.com</mgUIName>
                              <endpointName>tp/2016</endpointName>
                        </Parameters>
                  </delLineEndpoint>
            </Methods>
      </Command>
</CommandList>

 endpointName range increased due to large LGRP address space
```

Table 2 XML Command Tag Descriptions

tag name	description of valid values
endpointName	endpointName in range tp/1 ... tp/2016 for TP6310 large line GW

All other command tags are unchanged.

Figure 3 addCarrier - Carrier Last E1 Carrier

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>EndptGrpProvIf</Interface>
    <Methods>
      <addCarrier usn="1" version="1.0">
        <Parameters>
          <mgName>AC6310T1</mgName>
          <carrierName>E1/63</carrierName>
          <svcData>
            <DPNSS>
              <IID>63</IID>
            </DPNSS>
          </svcData>
          <firstTN>1924</firstTN>
        </Parameters>
      </addCarrier>
    </Methods>
  </Command>
</CommandList>
```

carrierName may be in range E1/01 ... E1/63 for E1 type carriers
DPNSS IID may be in range 1 ... 63 for E1 type carriers.

Table 3 XML Command Tag Descriptions

tag name	description of valid values
carrierName	E1 carrier in range E1/01 to E1/63
IID	DPNSS IID in range 1 .. 63

All other command tags are unchanged.

Figure 4 addCarrier - Carrier Last DS1 Carrier

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>EndptGrpProvIf</Interface>
    <Methods>
      <addCarrier usn="1" version="1.0">
        <Parameters>
          <mgName>AC6310T1</mgName>
          <carrierName>DS1/84</carrierName>
          <svcData>
            <PRI>
              <IID>31</IID>
            </PRI>
          </svcData>
          <firstTN>1992</firstTN>
        </Parameters>
      </addCarrier>
    </Methods>
  </Command>
</CommandList>
```

carrierName may be in range D1/01 ... D1/84 for DS1 type carriers
PRI IID may be in range 1 ... 31 for DS1 type carriers. The upper boundary is not enforced.

Table 4 XML Command Tag Descriptions

tag name	description of valid values
carrierName	DS1 carrier in range DS1/01 to DS1/84

All other command tags are unchanged.

Figure 5 deleteCarrier - Carrier Last E1 Carrier

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>EndptGrpProvIf</Interface>
    <Methods>
      <deleteCarrier usn="1" version="1.0">
        <Parameters>
          <mgName>AC63101</mgName>
          <carrierName>E1/63</carrierName>
        </Parameters>
      </deleteCarrier>
    </Methods>
  </Command>
</CommandList>
```

carrierName may be in range E1/01 ... E1/63 for E1 type carriers

Table 5 XML Command Tag Descriptions

tag name	description of valid values
carrierName	E1 carrier in range E1/01 to E1/63

All other command tags are unchanged.

Figure 6 deleteCarrier - Carrier Last DS1 Carrier

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>EndptGrpProvIf</Interface>
    <Methods>
      <deleteCarrier usn="1" version="1.0">
        <Parameters>
          <mgName>AC63101</mgName>
          <carrierName>DS1/84</carrierName>
        </Parameters>
      </deleteCarrier>
    </Methods>
  </Command>
</CommandList>
```

carrierName may be in range DS1/01 ... DS1/84 for DS1 type carriers

Table 6 XML Command Tag Descriptions

tag name	description of valid values
carrierName	DS1 carrier in range DS1/01 to DS1/84

All other command tags are unchanged.

14.10.1.2 Response XML

Response XML is unchanged.

14.11 Security

Unchanged.

14.12 Configuration Walkthrough

14.12.1 Provisioning an AUDIOCODES TP6310 Card As Large Line GW

CS2M and GWC are running SN09.1 FC loads. GWC is provisioned with a profile supporting large line GWs and has sufficient spare termination capacity to support an AUDIOCODES TP6310 card provisioned as a large line GW.

CM is running SN09 FC Load (PSNW09BS) with patch applied for large LGRP support (patch not required for SN10 onwards).

From the CS2M GUI interface (alternatively use OSSGate assocmg interface) launch the “Associate Media Gateway” dialog.

In the “Gateway profile name” selector locate “AUDIOCODES_6310_LINE”.

Set the “Gateway Site Name” selector to be a suitable SITE entry to support this gateway.

Set the Frame number and Unit number entries to values that will generate a unique LGRP entry in conjunction with the Site Name.

Populate the remainder of the fields as per normal for a H.248 supporting gateway and press the “OK” button to confirm.

Using either the bulk provisioning tool or OSSGate addLineEndpoint interface, add the desired number of endpoints in the range tp/1 ... tp/2016, associated circuit numbers will be in the range 0 ... 2015.

Using servord+ provision POTS type line services using the assigned endpoints.

14.12.2 Deprovisioning an AUDIOCODES TP6310 Card As Large Line GW

Using Servord+, remove all line services associated with GW endpoints.

Using the bulk provisioning tool or OSSGate delLineEndpoint interface, remove all endpoints associated with the GW.

Using either the CS2M GUI or OSSGate disassocmg interface delete the GW.

14.12.3 Provisioning an AUDIOCODES TP6310 Card As A Trunk GW

CS2M and GWC are running SN09.1 FC loads. GWC is provisioned with a profile supporting trunk GWs and has sufficient spare termination capacity to support an AUDIOCODES TP6310 card provisioned as a trunk GW.

CM is running SN09 FC Load (PSNW09BS). The large LGRP patch is considered optional in this scenario.

From the CS2M GUI interface (alternatively use OSSGate assocmg interface) launch the “Associate Media Gateway” dialog.

In the “Gateway profile name” selector locate “AUDIOCODES_6310_TRUNK”.

Data fill the dialog in exactly the same way as for an AUDIOCODES MG3200 / MG3500 GW. ITRANS may be specified if required - however the maximum termination setting is increased to 2016. Be aware that if E1 carriers are provisioned a maximum of 1953 terminations will be required for a fully equipped GW so the reserved terminations value may be lowered to save GWC capacity.

Using either the CS2M GUI Add Carrier dialog or corresponding OSSGate interface add the desired number of carriers to the GW. For E1 carriers the range is E1/01 to E1/63. For DS1 carriers the range is DS1/01 to DS1/84.

Where DPNSS support is required the IID may be set in the range 1 .. 63. Where PRI support is required the IID may be set in the range 0 .. 31. Be aware that the PRI upper bound is not enforced by the provisioning system and may be incorrectly set in the range 0.. 63. Be aware that the DPNSS IID may be incorrectly set to 0 by the provisioning system.

14.12.4 Deprovisioning an AUDIOCODES TP6310 Card As A Trunk GW

Using either OSSGate or the CS2M “delete carrier” dialog remove all carriers associated with the GW.

Using either the CS2M GUI or OSSGate disassocmg interface delete the GW.

TDM/Carrier VoIP

(I)SN09U Release Change Reference Manual

Copyright © 2006 Nortel Networks
All Rights Reserved

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

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

DMS, MAP, NORTEL, NORTEL NETWORKS, NORTHERN TELECOM, NT, and SUPERNODE are trademarks of Northern Telecom.

Publication number: PLN-iSN09FF-004
Product release: (I)SN09FF
Document release: Standard 01.03
Date: May 2006
Printed in the United States of America.

NORTEL NETWORKS™

How the world shares ideas.