

(I)SN08 Release Change Reference Manual

(I)SN08

Standard 01.03

June 2005

(I)SN08 Release Change Reference Manual

TDM and Carrier VoIP

Publication number:	PLN-SN08-004
Product release:	(I)SN08
Document release:	Standard 01.03
Date:	June 2005

Copyright © 2005 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 (N. Am.)

June 2004

Version 01.03 Standard release for SN08 at FVS. The following features have been added:

- A89007819, QoS Reporting: QoS Collector Application
- Q00720293, Change in SWREL value

The following feature has been updated for clarification: A00007785, MFT Backend Security Server Integrating into IEMS.

March 2005

Version 01.02 Standard release for SN08. The following features have been added since the Preliminary release.

- A00005561, MG9K Internet Protocol Security
- A00005562, MG9000 ITP/ABI Overload Controls
- A00005646, IPSEC with MG 9000 Element Manager
- A00005991, Enable IPSec on all GWC Profiles
- A00006269, OSSGate Password No Echo
- A00006347, Solaris 9 Introduction To SSPFS
- A00006570, CS2M Robustness enhancement - Moving SDM IP & CLLI input to SSPFS
- A00006756, NSSwitch Implementation in IEMS
- A00006757, IEMS Secure Launch to PP8600
- A00006759, Secure Launch of MDM X11 Client Application
- A00006925, Virtual Media Gateway (VMG) Robustness
- A00007054, H.248 Protocol Compliance Enhancements for GWC
- A00007244, GIC and GIAC Support on CICM and MG9K
- A00007253, MADN Ring Forward Support for CICM and MG9K
- A00007369, DTAG Low Layer Intelligent Network (LLIN)

-
- A00007382, H.323 Capacity Improvements: Increase Number of Allocatable Endpoints per GWC
 - A00007546, Message Waiting Service access using H.323 network

January 2005

Version 01.01 Preliminary release for SN08.

Table of Contents

RelDoc Introduction	7
SN08 Feature Subset Cross Reference Tables: North American Features	9
Feature to Functional Group Cross Reference	9
Functional Group to Feature Impacts Cross Reference	16
Functional Descriptions List (FNs)	23
A59039138 Functional description (FN)	31
A89007819 Functional description (FN)	44
A00003953 Functional description (FN)	100
A00004741 Functional description (FN)	129
A00005561 Functional description (FN)	131
A00005562 Functional description (FN)	139
A00005646 Functional description (FN)	144
A00005932 Functional description (FN)	149
A00005991 Functional description (FN)	154
A00006226 Functional description (FN)	157
A00006269 Functional description (FN)	170
A00006347 Functional description (FN)	173
A00006450 Functional description (FN)	175
A00006570 Functional description (FN)	215
A00006635 Functional description (FN)	219
A00006657 Functional description (FN)	228
A00006659 Functional description (FN)	230
A00006693 Functional description (FN)	233
A00006731 Functional description (FN)	237
A00006756 Functional description (FN)	241
A00006757 Functional description (FN)	266
A00006759 Functional description (FN)	283
A00006772 Functional description (FN)	288
A00006780 Functional description (FN)	291
A00006865 Functional description (FN)	312
A00006893 Functional description (FN)	315
A00006894 Functional description (FN)	322
A00006901 Functional description (FN)	326
A00006905 Functional description (FN)	329
A00006906 Functional description (FN)	331
A00006925 Functional description (FN)	334
A00006944 Functional description (FN)	335
A00006957 Functional description (FN)	336
A00006979 Functional description (FN)	338

A00006986 Functional description (FN)	343
A00007000 Functional description (FN)	345
A00007007 Functional description (FN)	350
A00007024 Functional description (FN)	374
A00007054 Functional description (FN)	378
A00007071 Functional description (FN)	380
A00007072 Functional description (FN)	387
A00007074 Functional description (FN)	389
A00007100 Functional description (FN)	391
A00007101 Functional description (FN)	396
A00007102 Functional description (FN)	399
A00007107 Functional description (FN)	400
A00007108 Functional description (FN)	404
A00007113 Functional description (FN)	406
A00007114 Functional description (FN)	409
A00007115 Functional description (FN)	415
A00007120 Functional description (FN)	416
A00007121 Functional description (FN)	421
A00007135 Functional description (FN)	429
A00007140A Functional description (FN)	439
A00007140B Functional description (FN)	454
A00007196 Functional description (FN)	487
A00007213 Functional description (FN)	515
A00007232 Functional description (FN)	520
A00007242 Functional Description (FN)	529
A00007243 Functional description (FN)	560
A00007244 excerpts from test plan	566
A00007250 Functional description (FN)	569
A00007253 excerpts from the test plan	581
A00007262 Functional description (FN)	584
A00007263 Functional Description (FN)	587
A00007264 Functional description (FN)	605
A00007268 Functional description (FN)	610
A00007270 Functional description (FN)	616
A00007271 Functional description (FN)	618
A00007275 Functional description (FN)	620
A00007276 Functional description (FN)	624
A00007277 Functional description (FN)	627
A00007282 Functional description (FN)	631
A00007293 Functional description (FN)	632

A00007295 Functional description (FN)	635
A00007300 Functional description (FN)	640
A00007302 Functional description (FN)	641
A00007304 Functional description (FN)	680
A00007322 Functional description (FN)	692
A00007323 Functional description (FN)	699
A00007324 Functional description (FN)	701
A00007327 Functional description (FN)	702
A00007331 Functional description (FN)	704
A00007341 Functional description (FN)	707
A00007343 Functional description (FN)	723
A00007344 Functional description (FN)	728
A00007345 Functional description (FN)	738
A00007346 Functional description (FN)	744
A00007347 Functional description (FN)	755
A00007359 Functional description (FN)	759
A00007369 Functional description (FN)	764
A00007370 Functional description (FN)	788
A00007388 Functional description (FN)	790
A00007393 Functional description (FN)	795
A00007394 Functional description (FN)	804
A00007399 Functional description (FN)	823
A00007404 Functional description (FN)	824
A00007415 Functional description (FN)	826
A00007416 Functional description (FN)	828
A00007417 Functional description (FN)	829
A00007424 Functional description (FN)	830
A00007459 Functional description (FN)	833
A00007460 Functional description (FN)	836
A00007464 Functional description (FN)	838
A00007465 Functional description (FN)	841
A00007483 Functional description (FN)	848
A00007489 Functional description (FN)	853
A00007491 Functional description (FN)	863
A00007492 Functional description (FN)	866
A00007541 Functional description (FN)	880
A00007548 Functional description (FN)	883
A00007564 Functional description (FN)	898
A00007571 Functional description (FN)	901
A00007572 Functional description (FN)	904

A00007573 Functional description (FN)	910
A00007576 Functional description (FN)	913
A00007602 Functional description (FN)	920
A00007635 Functional description (FN)	931
A00007708 Functional description (FN)	939
A00007709 Functional description (FN)	955
A00007713 Functional description (FN)	958
A00007717 Functional Description (FN)	960
A00007744 Functional description (FN)	964
A00007752 Functional description (FN)	979
A00007785 Functional Description (FN)	985
A00007786 Functional Description (FN)	996
A00007790 Functional Description (FN)	1007
A00007927 Functional Description (FN)	1009
A00007934 Functional description (FN)	1014
A00008045 Functional description (FN)	1030
A00008229 Functional description (FN)	1041
A00008338 Functional description (FN)	1075
A00008350 Functional description (FN)	1091
A00008387 Functional description (FN)	1098
A00008431 Functional description (FN)	1100
A00008902 Corrective CAF excerpts	1116
A00008907 Functional description (FN)	1119
Q00720293 Functional Description (FN)	1122
Q00811611 Functional Description (FN)	1123
Fault Management List (FMs)	1125
A00005562 Fault Management (FM)	1127
A00005646 Fault Management (FM)	1130
A00006893 Fault Management (FM)	1134
A00006901 Fault Management (FM)	1159
A00006979 Fault Management (FM)	1161
A00007000 Fault Management (FM)	1164
A00007071 Fault Management (FM)	1179
A00007074 Fault Management (FM)	1184
A00007102 Fault Management (FM)	1186
A00007113 Fault Management (FM)	1191
A00007213 Fault Management (FM)	1195
A00007243 Fault Management (FM)	1200
A00007270 Fault Management (FM)	1202
A00007271 Fault Management (FM)	1205

A00007304 Fault Management (FM)	1207
A00007327 Fault Management (FM)	1216
A00007393 Fault Management (FM)	1218
A00007415 Fault Management (FM)	1228
A00007417 Fault Management (FM)	1235
A00007465 Fault Management (FM)	1237
A00007489 Fault Management (FM)	1246
A00007713 Fault Management (FM)	1250
A00008431 Fault Management (FM)	1252
Configuration Management (CN)	1261
A00005646 Configuration (CN)	1263
A00006226 Configuration (CN)	1273
A00006269 Configuration (CN)	1280
A00006347 Configuration (CN)	1285
A00006450 Configuration (CN)	1288
A00006570 Configuration (CN)	1290
A00006693 Configuration (CN)	1313
A00006731 Configuration (CN)	1334
A00006780 Configuration (CN)	1338
A00006865 Configuration (CN)	1400
A00006893 Configuration (CN)	1403
A00006894 Configuration (CN)	1453
A00006901 Configuration (CN)	1465
A00006979 Configuration (CN)	1478
A00007000 Configuration (CN)	1506
A00007071 Configuration (CN)	1532
A00007072 Configuration (CN)	1583
A00007074 Configuration (CN)	1614
A00007102 Configuration (CN)	1637
A00007120 Configuration (CN)	1650
A00007213 Configuration (CN)	1664
A00007243 Configuration (CN)	1676
A00007250 Configuration (CN)	1684
A00007271 Configuration (CN)	1689
A00007277 Configuration (CN)	1693
A00007293 Configuration (CN)	1699
A00007415 Configuration (CN)	1701
A00007464 Configuration (CN)	1708
A00007465 Configuration (CN)	1722
A00007489 Configuration (CN)	1747

A00007492 Configuration (CN)	1761
A00007713 Configuration (CN)	1783
A00007790 Configuration (CN)	1787
A00007934 Configuration (CN)	1789
A00008387 Configuration (CN)	1800
A00008431 Configuration (CN)	1806
Performance Management (PF)	1815
A00004741 Performance (PF)	1817
A00005562 Performance (PF)	1834
A00006693 Performance (PF)	1836
A00006780 Performance (PF)	1840
A00007000 Performance (PF)	1846
A00007074 Performance (PF)	1861
A00007120 Performance (PF)	1863
A00007213 Performance (PF)	1869
A00007270 Performance (PF)	1872
A00007271 Performance (PF)	1874
A00007293 Performance (PF)	1875
A00007327 Performance (PF)	1876
A00007393 Performance (PF)	1879
A00007465 Performance (PF)	1885
A00008350 Performance (PF)	1888

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.

SN08 Feature Subset Cross Reference Tables:

North American Features

Feature to Functional Group Cross Reference

Table 1 shows 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 CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A59039138.AB01	(Visual) Message Waiting Indicator (V)MWI/CFX	Core19
A89007819	QoS Reporting: QoS Collector Application	PNM06, updated for SN08
A00003953	Active Call Failover (ACF)	CICM8
A00004741.AA05	Enabling TRKGRP OM ON GEM and SUPPORT NODAL OMS	MG4K21, Core21
A00005561	MG9K Internet Protocol Security	MG9K08
A00005562	MG9000 ITP/ABI Overload Controls	MG9K08
A00005646	IPSEC with MG 9000 Element Manager	MG9K08
A00005932.AA06	Removing Loopback Trunks in CEPT DISA calls for Remote Feature Activation	Core21

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
<i>Note:</i> Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00005991	Enable IPsec on all GWC Profiles	GC08
A00006226.AA07	NTPOLL: Restructuring and Table Control	Core21
A00006269	OSSGate Password No Echo	Core21
A00006347	Solaris 9 Introduction To SSPFS	SPFS08
A00006450	TL1 Line Test Interface for MG9K Lines	CS2M08
A00006570	CS2M Robustness enhancement - Moving SDM IP & CLLI input to SSPFS	CS2M08
A00006635	SESM Support for Cable Gateway Event Messaging	CS2M08
A00006657.AA05	EADAS Trunk Group Buffer Expansion	Core21
A00006659.AA07	Distinctive Call Waiting Ringback and Line Reversal via NCS	GC08
A00006693.AA10	XA-Core IO Capacity Monitoring Toolset	Core21
A00006731AA08	Handle Flash on Exit	Core21
A00006756	NSSwitch Implementation in IEMS	IEMS08
A00006757	IEMS Secure Launch to PP8600	IEMS08
A00006759	Secure Launch of MDM X11 Client Application	IEMS08
A00006772.AA07	Euro-PacketCable Compliance	Core21, GC08
A00006780.AA22	Trimodal Call Server OAM & P Enhancements	Core21, GC08
A00006865	SN08 GIGE HAL (Hardware Abstraction Layer) feature	MG9K08
A00006893.AA24	TLS support for NGSS	NCGL6, NGSS08
A00006894.AA03	InterNodal Emergency Stand Alone (ESA) for MG9K	MG9K08
A00006901	Missing Patches	SPFS08
A00006905	MG9KEM Recovery Improvements	MG9KEM08

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
<i>Note:</i> Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00006906	SN08 Clock Sync Enhancements	MG9K08
A00006925	Virtual Media Gateway (VMG) Robustness	MG9KEM08
A00006944	Subnet and Logs Adaptor collapse	MG9KEM08
A00006957	MG9KEM Deserialization of Patching	MG9KEM08
A00006979	Synchronized Backup Restore Manager	CS2M08, SDM21, SPFS08, MG9KEM08
A00006986.AA09	H.248 Real-Time and Message Reduction	GC08
A00007000	GIGE Network Interface EM Portion	MG9KEM08
A00007007.A02	Session Border Controller - Application Layer Gateway	CS2M08, GC08
A00007024	Core Element Manager (CEM) Patching	SPFS08
A00007054.AA03	H.248 Protocol Compliance Enhancements for GWC	GC08
A00007071	SN08 3rd Party GW Interop Profiles	Core21, CS2M08, GC08
A00007072	3rd Party GW Interop Pre Provisioning	CS2M08
A00007074	GigE Link Maintenance	MG9K08
A00007100	Gateway Controller Card Evolution	CS2M08, GC08
A00007101. AA05	GWC Telnet Authentication	GC08
A00007102.AA11	Dual C-Side IP for GWC	CS2M08, GC08
A00007106	OAM Obsolete Patching Strategy	SPFS08
A00007107	Media Gateway 9000 5/30 Minute Operational Measurements	MG9K08
A00007108	MG9000 Session Description Protocol (SDP) Enhancements for SN08	MG9K08
A00007113	GWC External Interface Robustness	GC08

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
<i>Note:</i> Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00007114.AA05	TGCP Compliancy	GC08, Core21
A00007115.AA05	MG9K In-service Fault Isolation	MG9K08
A00007120.AA97	Packet Media Anchor for DPT	GC08, Core21
A00007121.AA05	IW Bridge MAP maintenance for deload	Core21
A00007135.AA19	GWC DPT Audits and Counter Drift Prevention	Core21
A00007140A	Succession Upgrade Manager (Phase 1)	CS2M08, SPFS08, MG9KEM08
A00007140B	Upgrade Manager Phase I -- GWC and SC parts	CS2M08, SPFS08, MG9KEM08
A00007196.AA31	PacketCable™ Event Messaging For Accounting	Core21, GC08
A00007213	MG9000 5/30 Minutes OMs	MG9KEM08
A00007232.AA08	T.38 Support for Gatekeeper - Gatekeeper Configurations	GC08
A00007242	SESM support for SPC topology	CS2M08
A00007243.AA09	Prevent Outage when CEM flash has not been erased	Core21, SP21
A00007244.AA05	GIC and GIAC Support on CICM and MG9K	CICM8
A00007250.AA12	ACDMIS Over TCP	Core21
A00007253.AA03	MADN Ring Forward Support for CICM and MG9K	CICM8
A00007262.AA08	CS2K Capacity Enhancements for Large VoIP VPN Deployments	Core21
A00007263	LCI for GigE	MG9K08
A00007264	CentrexIP Client Manager Capacity Expansion Phase 2	CICM8
A00007268.AB03	NGSS OM Subsystem Enhancement	NGSS08
A00007270.AA13	Session Server Call Processing Overload Controls	NGSS08
A00007271.AA08	TOPS EOL for SN08	TOPS21

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
<i>Note:</i> Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00007275.AB09	Session Server - Session/Application Mgmt Framework and Support for Multiple HTTPS connection to the Session Server through SSPFS	NGSS08
A00007276.AB09	Session Server Application Patching Support	NGSS08
A00007277.AA04	LOGs Throttling	Core21
A00007282	Configurable Threshold for Failed Login Attempts	SPFS08
A00007293	VLAN for Gigabit Ethernet	MG9K08
A00007295.AA07	CBM 860 OC3 Connectivity	Core21
A00007300	Enable by default IPSec on All GWC Profiles	CS2M08
A00007302	SN08 IEMS-CEM Integration	IEMS08
A00007304	SN08 CEM I & C on IEMS	IEMS08, SDM21
A00007322.AA17	Cisco Call Manager interop enhancements	GC08
A00007323.AA07	Gateway Controller notification of Media Proxy Bind Expiry Events	GC08
A00007324.AA05	RTP Portal QoS reporting to GWC	GC08
A00007327.AA08	Media Proxy 5 and 30 minute Operational Measurements	GC08
A00007331.AA06	RFC 2833 DTMF Interop with S 1000, S 1000M and BCM	GC08
A00007341	MS2000 IEMS Confutation Integration	IEMS08
A00007343	PP8600 Extended Fault Mapping	IEMS08
A00007344	IEMS Robustness/Southbound Event Throttling	IEMS08
A00007345	MDM Enhancements for IEMS	IEMS08
A00007346	Backward Compatibility in IEMS	IEMS08
A00007347	CEM Integration with IEMS	IEMS08

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
<i>Note:</i> Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00007359	USP/USP-Compact: Log Delivery Stream to IEMS [Integrated Element Management System]	USP10
A00007369	DTAG Low Layer Intelligent Network (LLIN)	USP10
A00007370	USP8.0.x/9.0.x to USP10.0.x Direct In-Service Upgrade and USPc9.0.x to USPc10.0.x In-Service Upgrade	USP10
A00007388	Performance Phase II Functional Specification	IEMS08
A00007393	Session Policy Controller	NGSS08
A00007394.AA12	Network VCAC CallP	GC08
A00007399.AA07	Network VCAC Maintenance and Upgrade	GC08
A00007404	IEMS Security Serialized Patching	SPFS08
A00007415	Internodal Emergency Standalone (ESA) Element Manager	MG9KEM08
A00007416.AA05	BASE 'IRM IP Takeover Robustness' feature	Core21
A00007417.AA04	Ethernet link overload Control	Core21
A00007424	Alarm Enhancements on SAM21	SCU11
A00007459.AA06	SBA: Upgrade Support for CBM	SDM21
A00007460.AA04	Media Proxy Insertion for IP IWSPM/MG4K	GC08
A00007464.AA07	SBA PacketCable Event Messaging	SDM21, Core21
A00007465.AB01	Integrated Accounting Application (IAA)	SDM21
A00007483.AA05	GR740 Secure using SSH	SDM21
A00007489.AA15	Integration of SuperNode Data Manager (SDM) User Authentication with the Integrated Element Manager System (IEMS)	SDM21
A00007491.AA07	SuperNode Data Manager (SDM) File Integrity Audit	SDM21

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
<i>Note:</i> Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00007492.AA11	SDM User Group Improvements. This feature is part of the SDM21/SN08 release	SDM21
A00007541.AA06	NGSS XML Framework	NGSS08
A00007548.AA17	SN08 PacketCable Electronic Surveillance	Base21
A00007564	SAM21 EM support for new hardware - MCPN905	CS2M08
A00007571	MTP3b/SAAL/ATM BB-SS7 Protocol	USP10
A00007572	M3UA RFC Peer to Peer Protocol	USP10
A00007573	MTP3b/SAAL/ATM BB-SS7 Protocol	USP10
A00007576	Message Trace	USP10
A00007602.AA12	SDM Software Authenticity	SDM21
A00007635.AA08	CBM Upgrades	SDM21
A00007708	Unistim Security	CICM8, MG9K08
A00007709.AA13	MCS CD Phase 2 Support	CICM8, Core21
A00007713.AA02	TOPS-IP Robustness	TOPS21
A00007717	Health Monitor Logs	IEMS08
A00007744.AA02	File Naming Convention for Nortel Carrier Grade Linux (NCGL)	NCGL6
A00007752.AA06	Universal Billing Correlation ID	Core21
A00007785	MFT Backend Security Server Integration	IEMS08
A00007786	IEMS Config RADIUS Secret	IEMS08
A00007790.AA08	P-phone Expansion for CICM Lines	Core21
A00007927	SAM21 Enhancements from Bell Canada	CS2M08
A00007934.AA29	E800 Routing Enhancements	Core21

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release
<i>Note:</i> Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A00008045.AA03	CICM interoperability with SRG-500 for failover/recovery	CICM8
A00008229	CICM i2033 IP Conference Terminal	CICM8
A00008338	QCA Log/Alarm Consolidation	CS2M08
A00008350.AA04	Trunk group OM registers for establish bearer path failures	Core21
A00008387	GLC-32 AB Card Support	MG9K08
A00008431.AA04	Support for CS2Kc Geo Redundant	NCGL6
A00008902	Adding Category and Cause Values to SAM21 Alarm Logs in Syslog	IEMS08, CS2M08
A00008907	CEM Log Key Changes for CEM Logs	IEMS08
Q0072093	Change in SWREL value	Core 21
Q00811611	SSPFS – HA Support for user administration and passwords	SPFS08

Functional Group to Feature Impacts Cross Reference

Table 2 is organized alphabetically by functional group. Within each group, the features are listed numerically. 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	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
Core19	A59039138.AB01	Y				
PNM06, updated for SN08	A89007819	Y				

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
CICM8	A00003953	Y				
MG4K21, Core21	A00004741.AA05	Y				Y
MG9K08	A00005561	Y				
MG9K08	A00005562	Y	Y			Y
MG9K08	A00005646	Y	Y	Y		
Core21	A00005932.A06	Y				
GC08	A00005991	Y				
Core21	A00006226.AA07	Y		Y		
Core21	A00006269	Y		Y		
SPFS08	A00006347	Y		Y		
CS2M08	A00006450	Y		Y		
CS2M08	A00006570	Y		Y		
CS2M08	A00006635	Y				
Core21	A00006657.AA05	Y				
GC08	A00006659.AA07	Y				
Core21	A00006693.AA10	Y		Y		Y
Core21	A00006731.AA08	Y		Y		
IEMS08	A00006756	Y				
IEMS08	A00006757	Y				
IEMS08	A00006759	Y				
Core21, GC08	A00006772.AA07	Y				
Core21, GC08	A00006780.AA22	Y		Y		Y
MG9K08	A00006865	Y		Y		
NCGL6, NGSS08	A00006893.AA24	Y	Y	Y		
MG9K08	A00006894.AA03	Y		Y		

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
SPFS08	A00006901	Y	Y	Y		
MG9KEM08	A00006905	Y				
MG9K08	A00006906	Y				
MG9KEM08	A00006925	Y				
MG9KEM08	A00006944	Y				
MG9KEM08	A00006957	Y				
CS2M08, SDM21, SPFS08, MG9KEM08	A00006979	Y	Y	Y		
GC08	A00006986.AA09	Y				
MG9KEM08	A00007000	Y	Y	Y		Y
CS2M08, GC08	A00007007.AB02	Y				
SPFS08	A00007024	Y				
GC08	A00007054.AA03	Y				
Core21, CS2M08, GC08	A00007071	Y	Y	Y		
CS2M08	A00007072	Y		Y		
MG9K08	A00007074	Y	Y	Y		Y
CS2M08, GC08	A00007100	Y				
GC08	A00007101.AA05	Y				
CS2M08, GC08	A00007102.AA11	Y	Y			
SPFS08	A00007106	Y				
MG9K08	A00007107	Y				
MG9K08	A00007108	Y				
GC08	A00007113	Y	Y			
GC08, Core21	A00007114.AA05	Y				

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
MG9K08	A00007115.AA05	Y				
GC08, Core21	A00007120.AA97	Y		Y		Y
Core21	A00007121.AA05	Y				
Core21	A00007135.AA19	Y				
CS2M08, SPFS08, MG9KEM08	A00007140A	Y				
CS2M08, SPFS08, MG9KEM08	A00007140B	Y				
Core21, GC08	A00007196.AA31	Y				
MG9KEM08	A00007213	Y	Y	Y		Y
GC08	A00007232.AA08	Y				
CS2M08	A00007242	Y				
Core21, SP21	A00007243.AA09	Y	Y	Y		
CICM8	A00007244.AA05	Y				
Core21	A00007250.AA12	Y		Y		
CICM8	A00007253.AA03	Y				
Core21	A00007262.AA08	Y				
MG9K08	A00007263	Y				
CICM8	A00007264	Y				
NGSS08	A00007268.AB03	Y				
NGSS08	A00007270.AA13	Y	Y			Y
TOPS21	A00007271.AA08	Y	Y	Y		Y
NGSS08	A00007275.AB09	Y				
NGSS08	A00007276.AB09	Y				
Core21	A00007277.AA04	Y		Y		
SPFS08	A00007282	Y				

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
MG9K08	A00007293	Y		Y		Y
Core21	A00007295.AA07	Y				
CS2M08	A00007300	Y				
IEMS08	A00007302	Y				
IEMS08, SDM21	A00007304	Y	Y			
GC08	A00007322.AA17	Y				
GC08	A00007323.AA07	Y				
GC08	A00007324.AA05	Y				
GC08	A00007327.AA08	Y	Y			Y
GC08	A00007331.AA06	Y				
IEMS08	A00007341	Y				
IEMS08	A00007343	Y				
IEMS08	A00007344	Y				
IEMS08	A00007345	Y				
IEMS08	A00007346	Y				
IEMS08	A00007347	Y				
USP10	A00007359	Y				
USP10	A00007369	Y				
USP10	A00007370	Y				
IEMS08	A00007388	Y				
NGSS08	A00007393	Y	Y	Y		Y
GC08	A00007394.AA12	Y				
GC08	A00007399.AA07	Y				
SPFS08	A00007404	Y				
MG9KEM08	A00007415	Y	Y	Y		

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
Core21	A00007416.AA05	Y				
Core21	A00007417.AA04	Y	Y			
SCU11	A00007424	Y				
SDM21	A00007459.AA06	Y				
GC08	A00007460.AA04	Y				
SDM21, Core21	A00007464.AA07	Y		Y		
SDM21	A00007465.AB01	Y	Y	Y		Y
SDM21	A00007483.AA05	Y				
SDM21	A00007489.AA15	Y	Y	Y		
SDM21	A00007491.AA07	Y				
SDM21	A00007492.AA11	Y		Y		
NGSS08	A00007541.AA06	Y				
Base21	A00007548.AA17	Y				
CS2M08	A00007564	Y				
USP10	A00007571	Y				
USP10	A00007572	Y				
USP10	A00007573	Y				
USP10	A00007576	Y				
SDM21	A00007602.AA12	Y				
SDM21	A00007635.AA08	Y				
CICM8, MG9K08	A00007708	Y				
CICM8, Core21	A00007709.AA13	Y				
TOPS21	A00007713.AA02	Y	Y	Y		
IEMS08	A00007717					
NCGL6	A00007744.AA02	Y				

Functional Group	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
Core21	A00007752.AA06	Y				
IEMS08	A00007785	Y				
IEMS08	A00007786	Y				
Core21	A00007790.AA08	Y		Y		
CS2M08	A00007927	Y				
Core21	A00007934.AA29	Y		Y		
CICM8	A00008045.AA03	Y				
CICM8	A00008229	Y				
CS2M08	A00008338	Y				
Core21	A00008350.AA04	Y				Y
MG9K08	A00008387	Y		Y		
NCGL6	A00008431.AA04	Y	Y	Y		
IEMS08, CS2M08	A00008902	Y				
IEMS08	A00008907	Y				
Core21	Q00720293	Y				
SPFS08	Q00811611	Y				

Functional Descriptions (FN)

Introduction

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

Featid	Title
A59039138	(Visual) Message Waiting Indicator (V)MWI/CFX
A89007819	QoS Reporting: QoS Collector Application
A00003953	Active Call Failover (ACF)
A00004741.AA05	Enabling TRKGRP OM ON GEM and SUPPORT NOD-AL OMS
A00005561	MG9K Internet Protocol Security
A00005562	MG9000 ITP/ABI Overload Controls
A00005646	IPSEC with MG 9000 Element Manager
A00005932.AA06	Removing Loopback Trunks in CEPT DISA calls for Remote Feature Activation
A00005991	Enable IPsec on all GWC Profiles
A00006226.AA07	NTPOLL: Restructuring and Table Control
A00006269	OSSGate Password No Echo
A00006347	Solaris 9 Introduction To SSPFS
A00006450	TL1 Line Test Interface for MG9K Lines
A00006570	CS2M Robustness enhancement - Moving SDM IP & CLLI input to SSPFS

A00006635	SESM Support for Cable Gateway Event Messaging
A00006657.AA05	EADAS Trunk Group Buffer Expansion
A00006659.AA07	Distinctive Call Waiting Ringback and Line Reversal via NCS
A00006693.AA10	XA-Core IO Capacity Monitoring Toolset
A00006731.AA08	Handle Flash on Exit
A00006756	NSSwitch Implementation in IEMS
A00006757	IEMS Secure Launch to PP8600
A00006759	Secure Launch of MDM X11 Client Application
A00006772.AA07	Euro-PacketCable Compliance
A00006780.AA23	Trimodal Call Server OAM & P Enhancements
A00006865	SN08 GIGE HAL (Hardware Abstraction Layer) feature
A00006893.AA24	TLS support for NGSS
A00006894.AA03	InterNodal Emergency Stand Alone (ESA) for MG9K
A00006901	Missing Patches
A00006905	MG9KEM Recovery Improvements
A00006906	SN08 Clock Sync Enhancements
A00006925	Virtual Media Gateway (VMG) Robustness
A00006944	Subnet and Logs Adaptor collapse
A00006957	MG9KEM Deserialization of Patching
A00006979	Synchronized Backup Restore Manager
A00006986.AA09	H.248 Real-Time and Message Reduction
A00007000	GIGE Network Interface EM Portion
A00007007.AB02	Session Border Controller - Application Layer Gateway
A00007024	Core Element Manager (CEM) Patching

A00007054.AA03	H.248 Protocol Compliance Enhancements for GWC
A00007071	SN08 3rd Party GW Interop Profiles
A00007072	3rd Party GW Interop Pre Provisioning
A00007074	GigE Link Maintenance
A00007100	Gateway Controller Card Evolution
A00007101.AA05	GWC Telnet Authentication
A00007102.AA11	Dual C-Side IP for GWC
A00007106	OAM Obsolete Patching Strategy
A00007107	Media Gateway 9000 5/30 Minute Operational Measurements
A00007108	MG9000 Session Description Protocol (SDP) Enhancements for SN08
A00007113	GWC External Interface Robustness
A00007114.AA05	TGCP Compliancy
A00007115.AA05	MG9K In-service Fault Isolation
A00007120.AA98	Packet Media Anchor for DPT
A00007121.AA05	IW Bridge MAP maintenance for deload
A00007135.AA19	GWC DPT Audits and Counter Drift Prevention
A00007140A	Succession Upgrade Manager (Phase 1)
A00007140B	Upgrade Manager Phase I -- GWC and SC parts
A00007196.AA31	PacketCable TM Event Messaging For Accounting
A00007213	MG9000 5/30 Minutes OMs
A00007232.AA08	T.38 Support for Gatekeeper - Gatekeeper Configurations
A00007242	SESM support for SPC topology
A00007243.AA09	Prevent Outage when CEM flash has not been erased

A00007244.AA05	GIC and GIAC Support on CICM and MG9K
A00007250.AA12	ACDMIS Over TCP
A00007253.AA03	MADN Ring Forward Support for CICM and MG9K
A00007262.AA08	CS2K Capacity Enhancements for Large VoIP VPN Deployments
A00007263	LCI for GigE
A00007264	CentrexIP Client Manager Capacity Expansion Phase 2
A00007268.AB03	NGSS OM Subsystem Enhancement
A00007270.AA13	Session Server Call Processing Overload Controls
A00007271.AA08	TOPS EOL for SN08
A00007275.AB09	Session Server - Session/Application Mgmt Framework and Support for Multiple HTTPS connection to the Session Server through SSPFS
A00007276.AB09	Session Server Application Patching Support
A00007277.AA04	LOGs Throttling
A00007282	Configurable Threshold for Failed Login Attempts
A00007293	VLAN for Gigabit Ethernet
A00007295.AA07	CBM 860 OC3 Connectivity
A00007300	Enable by default IPSec on All GWC Profiles
A00007302	SN08 IEMS-CEM Integration
A00007304	SN08 CEM I & C on IEMS
A00007322.AA17	Cisco Call Manager interop enhancements
A00007323.AA07	Gateway Controller notification of Media Proxy Bind Expiry Events
A00007324.AA05	RTP Portal QoS reporting to GWC
A00007327.AA08	Media Proxy 5 and 30 minute Operational Measurements

A00007331.AA06	RFC 2833 DTMF Interop with S 1000, S 1000M and BCM
A00007341	MS2000 IEMS Configuration Integration
A00007343	PP8600 Extended Fault Mapping
A00007344	IEMS Robustness/Southbound Event Throttling
A00007345	MDM Enhancements
A00007346	Backward Compatibility in IEMS
A00007347	CEM Integration with IEMS
A00007359	USP/USP-Compact: Log Delivery Stream to IEMS [Integrated Element Management System]
A00007369	DTAG Low Layer Intelligent Network (LLIN)
A00007370	USP8.0.x/9.0.x to USP10.0.x Direct In-Service Upgrade and USPc9.0.x to USPc10.0.x In-Service Upgrade
A00007388	Performance Phase II Functional Specification
A00007393	Session Policy Controller
A00007394.AA12	Network Virtual Call Admission Control (VCAC) CallP
A00007399.AA07	Network VCAC Maintenance and Upgrade
A00007404	IEMS Security Serialized Patching
A00007415	Internodal Emergency Standalone (ESA) Element Manager
A00007416.AA05	BASE 'IRM IP Takeover Robustness' feature
A00007417.AA04	Ethernet link overload Control
A00007424	Alarm Enhancements on SAM21
A00007459.AA06	SBA: Upgrade Support for CBM
A00007460.AA04	Media Proxy Insertion for IP IWSPM/MG4K
A00007464.AA07	SBA PacketCable Event Messaging
A00007465.AB01	Integrated Accounting Application (IAA)

A00007483.AA05	GR740 Secure using SSH
A00007489.AA15	Integration of SuperNode Data Manager (SDM) User Authentication with the Integrated Element Manager System (IEMS)
A00007491.AA07	SuperNode Data Manager (SDM) File Integrity Audit
A00007492.AA11	SDM User Group Improvements. This feature is part of the SDM21/SN08 release
A00007541.AA06	NGSS XML Framework
A00007548.AA16	SN08 PacketCable Electronic Surveillance
A00007564	SAM21 EM support for new hardware - MCPN905
A00007571	MTP3b/SAAL/ATM BB-SS7 Protocol
A00007572	M3UA RFC Peer to Peer Protocol
A00007573	MTP3b/SAAL/ATM BB-SS7 Protocol
A00007576	Message Trace
A00007602.AA12	SDM Software Authenticity
A00007635.AA08	CBM Upgrades
A00007708	Unistim Security
A00007709.AA13	MCS CD Phase 2 Support
A00007713.AA02	TOPS-IP Robustness
A00007717	Health Monitor Logs
A00007744.AA02	File Naming Convention for Nortel Carrier Grade Linux (NCGL)
A00007752.AA06	Universal Billing Correlation ID
A00007785	MFT Backend Security Server Integration
A00007786	IEMS Config RADIUS Secret
A00007790.AA08	P-phone Expansion for CICM Lines

A00007927	SAM21 Enhancements from Bell Canada
A00007934.AA29	E800 Routing Enhancements
A00008045.AA03	CICM interoperability with SRG-500 for failover/recovery
A00008229	CICM i2033 IP Conference Terminal
A00008338	QCA Log/Alarm Consolidation
A00008350.AA04	Trunk group OM registers for establish bearer path failures
A00008387	GLC-32 AB Card Support
A00008431.AA04	Support for CS2Kc Geo Survivability
A00008902	Adding Category and Cause Values to SAM21 Alarm Logs in Syslog
A00008907	CEM Log Key Changes for CEM Logs
Q00720293	Change in SWREL value
Q00811611	SSPFS – HA Support for user administration and passwords

1: A59039138 Functional description (FN)

1.1 Feature name

(Visual) Message Waiting Indicator (V)MWI/CFX

Note: This feature was developed in SN05 and SN06 but was not activated for those releases in the North American market. It is now active and available in the North American market starting in SN07.

1.2 Description

1.2.1 Overview

This activity provides the following functionality for the Integrated Access Cable IP Solution:

- CMWI (Class Message Waiting Indicator) for CEPT and Bellcore lines on Succession.
- Announcement as an optional replacement for the MWT stuttered dial tone indications for MWT suboptions CMWI and STD.

1.2.2 Background Information

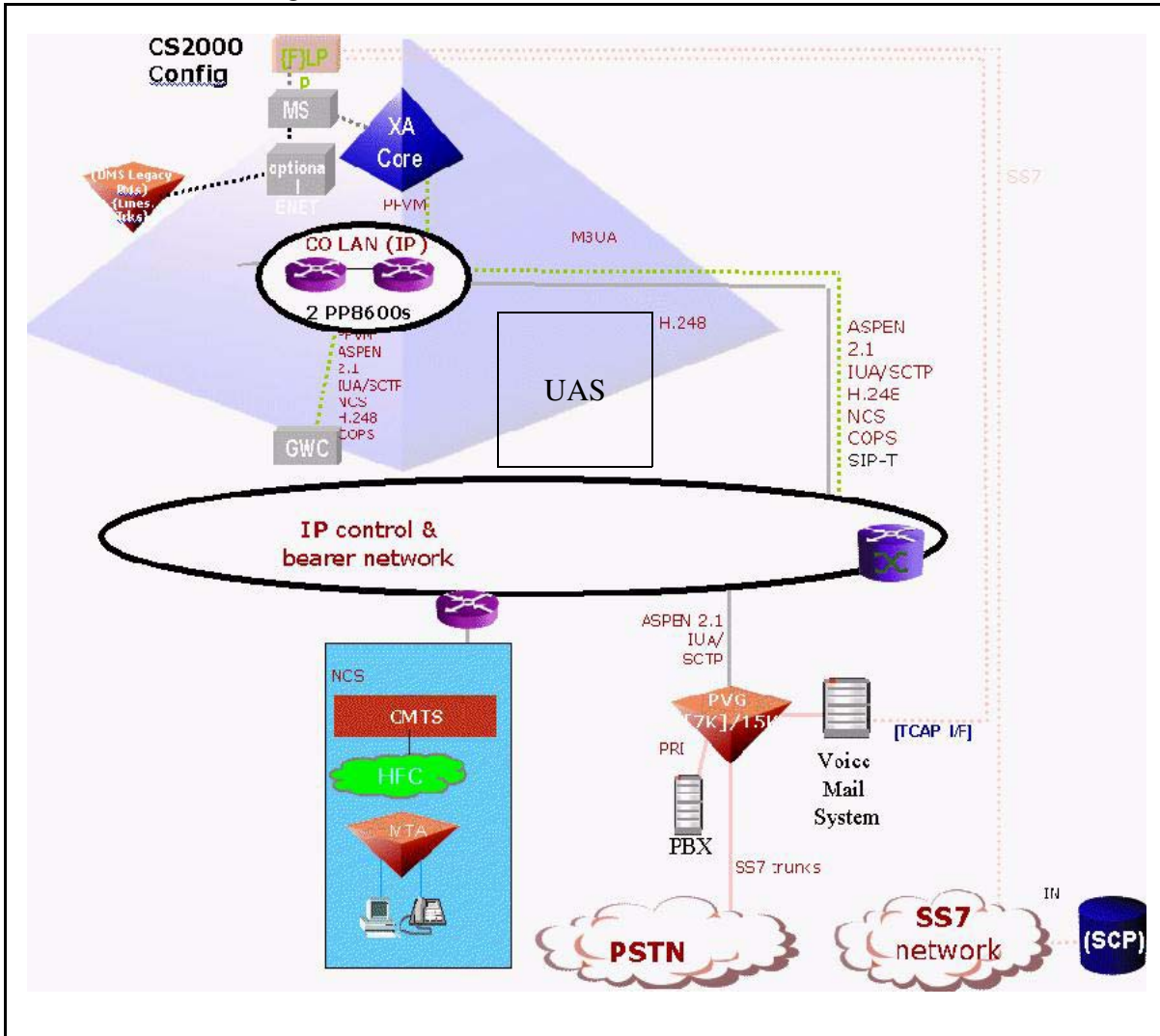
Message Waiting allows a user to have a list of messages stored against their station. When a message is queued for a station, the MWI (Message Waiting Indicator) associated with the line is activated. When the last message is retrieved, the MWI is deactivated.

The MWT option has several sub options (STD, MWL, CMWI, PRN, MWL_STD). This activity focuses on STD and CMWI suboptions.

- CMWI (Class Message Waiting)¹ is used for sets which are capable of displaying a MWI request in a display or as a flashing lamp. In addition it provides audible (stuttered dial tone) or ring splash notification. The last can be activated and deactivated by dialing an activation code.
- STD (Stuttered Dial Tone) This is only used for applying a stuttered dial tone if a message is waiting.

¹AG1954 'CLASS: VISUAL MESSAGE WAITING INDICATOR'

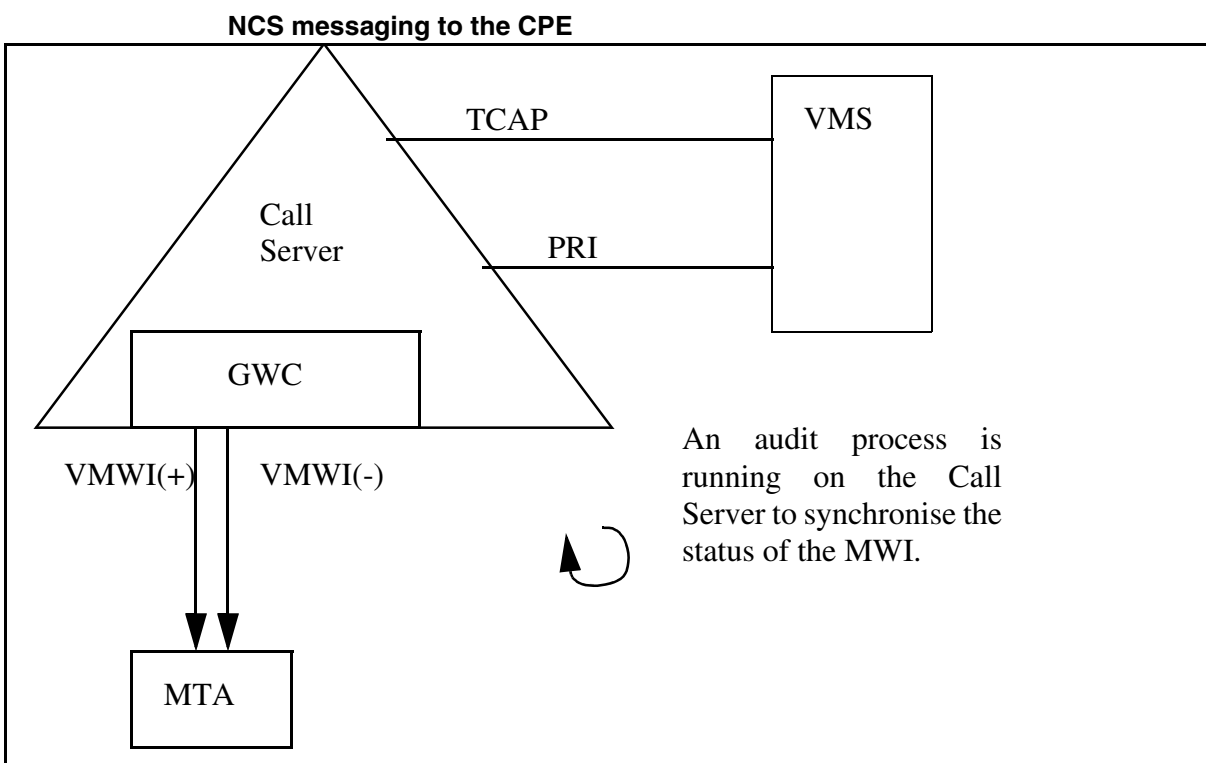
Configuration VMWI



On MMP the Visual Message Waiting was signalled to the user by a special Line Class Tone. For Integrated Access Cable Media an NCS¹ message is used. For activating the MWI a VMWI(+) message is sent. For deactivation a VMWI(-).

In addition to this the Call Server should periodically refresh the CPE's (Customer Premise Equipment) visual indicator (Audit).

¹PKT-SP-EC-MGCP-I02-991201



1.2.3 Agent Interworking

The Controlling user is a VMS (Voice Mail System) connected over

- PRI (PVG, PDTC)
- TCAP (LPP, USP)

to the Call Server.

The receiving user can be an IBN line connected via

- GWC - hosted on Motorola CG4500E MTA
- PLGC

1.2.4 Provisioning of the MWT service

The message waiting service can be provisioned with the following options: {**STD**,MWL,**CMWI**,PRN,MWL_STD}.

When the MWTANN announcement option is selected for MWT, datafill is required for the announcement. The CLLI for this announcement must be MWT. The CLLI can not be changed by the telco.

Below is sample datafill from a lab switch for the MWTANN feature:

```

> table clli
TABLE: CLLI
>pos mwt
MWT 433 5 TEST
>quit
CI:
>table anns
TABLE: ANNS
>pos mwt
MWT ALL 1 1 1 STND N 59 60
>quit
CI:
>table annmems
TABLE: ANNMEMS
>pos mwt 1
MWT 1
DRAM DRA
( 0 DTM 7 3)$
>quit
CI:
>table annphlst
TABLE: ANNPHLST
>pos mwt 0
MWT 0
( HAVE_MSG)$
>quit

***Create the announcement using DRAMREC***
> DRAMREC
> connect the HSET to a DRAM with available space.....
>Record have_msg 3 nopad 8 3 12
> QUIT

```

****This in turn creates a tuple in table dramphrs in a SN06 and beyond load. ****

```

>table dramphrs
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: DRAMPHRS
>pos 8 have_msg
8 HAVE_MSG 12 4 3 Y N 4

```

1.2.5 Table IBNFEAT

This feature adds the new announcement field MWT_ANNOUNCEMENT to the MWT feature in table IBNFEAT. A datafill example follows.

```

>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
LEN:

```

```

>HOST 01 0 07 00
DNNO:
>0
DF:
>mwt
FEATURE:
>mwt
NOTICE:
>std
MWT_ANNOUNCEMENT: N
>y
CAR:
>n
CRX: N
>n
TUPLE TO BE ADDED:
HOST 01 0 07 00

          0      MWT      MWT      STD      Y      N      N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
>

```

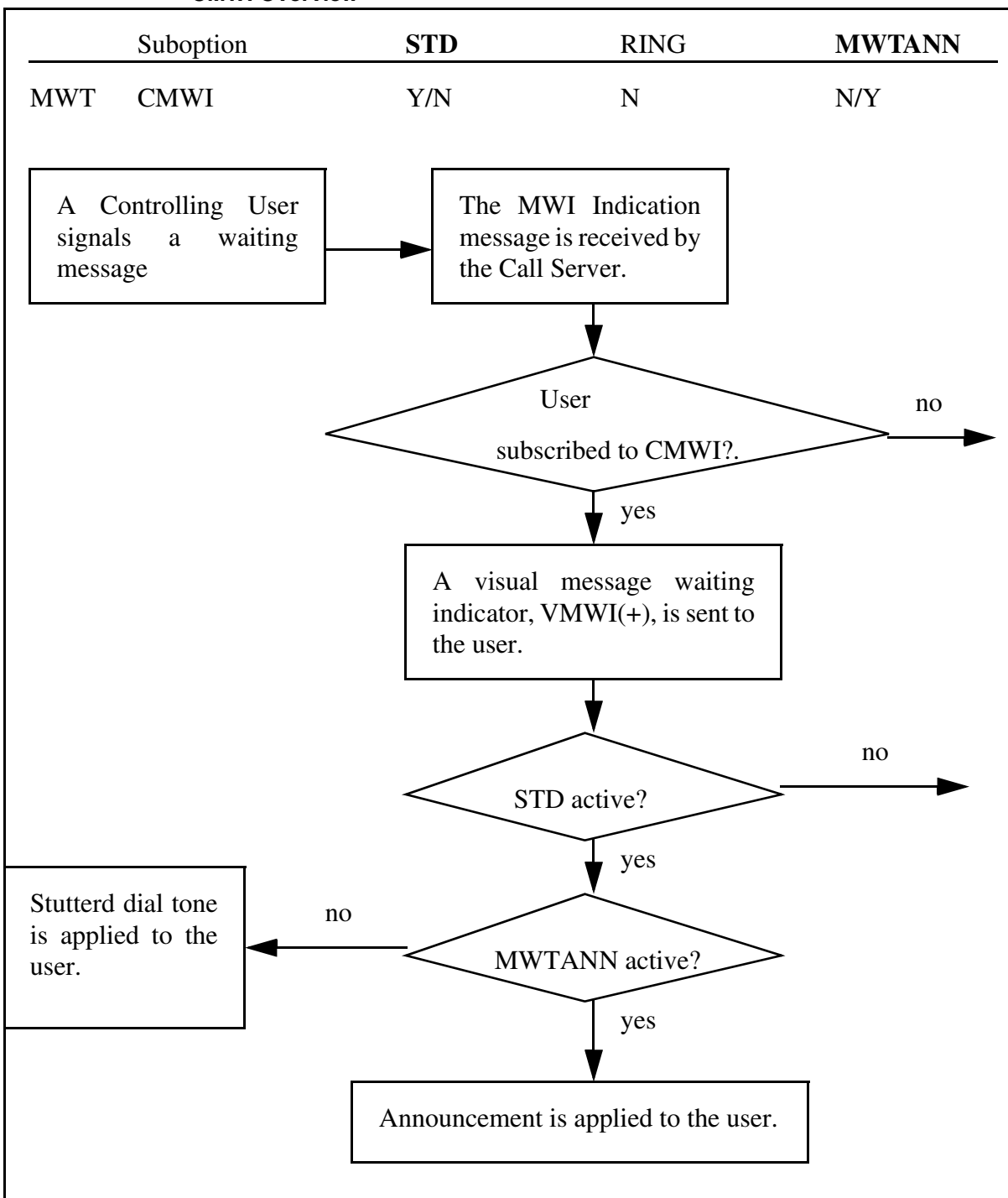
1.2.6 Overview of the CMWI Service

CLASS Message Waiting Indicator (CMWI) was developed under feature AG1954. The CMWI allows a subscriber to combine the visual message waiting indicator with audible indication types.

- **STD - Stuttered Dial Tone**
On active message waiting a stuttered dial tone is applied when the user goes off-hook
- **Ring Splash**
On active message waiting a ring burst is applied to the users' phone
- **MWTANN - Announcement**
On active message waiting an announcement is applied to the user.

For the Integrated Access Cable IP solution the signaling to the end user was shown in “NCS messaging to the CPE” on page 33.

Figure “CMWI Overview” on page 36 shows a functional overview on how the different indication components work together.

CMWI Overview

This feature creates a new SERVORD prompt called MWT_ANNOUNCEMENT. The provisioning for the CMWI service looks as follows:

SERVORD example for CMWI

```
>DN_OR_LEN:
>8838441020

OPTION:
>mwt

NOTICE:
>cmwi

CMWISTD:
>y

MWT_ANNOUNCEMENT:

>y

CMWIRING:
>y

STATUS:
>act

CAR:
>y

CRRCFW:
>all

CRX:
>n

OPTION:
>$

COMMAND AS ENTERED:

ADO NOW 1 12 4 AM 8838441020 ( MWT CMWI Y y Y ACT Y ALL N ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
```

The CMWI option must be activated in table RESOFC.

Table RESOFC

KEY	ENABLED	ACCESS	FEATDATA
CMWI	Y	SUBSCR CMWI	SINGLE 5

The datafill above shows an example of the CMWI entry where the feature is enabled, using the Single Data Message format and allows 5 retransmissions per activation/deactivation request.

1.2.6.1 STD suboption

The STD option enables a subscriber to hear a stuttered dial tone if a message is waiting for them. This example shows the new SERVORD prompt called MWT_ANNOUNCEMENT.

SERVORD example for STD suboption

```
>DN_OR_LEN:
>8838441020

OPTION:
>mwt

NOTICE:
>STD

MWT_ANNOUNCEMENT:

>Y

OPTION:
>$

COMMAND AS ENTERED:

ADO NOW 1 12 4 AM 8838441020 ( MWT STD Y Y ALL N ) $

ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
```

1.2.7 Datafilling the Audit for CMWI

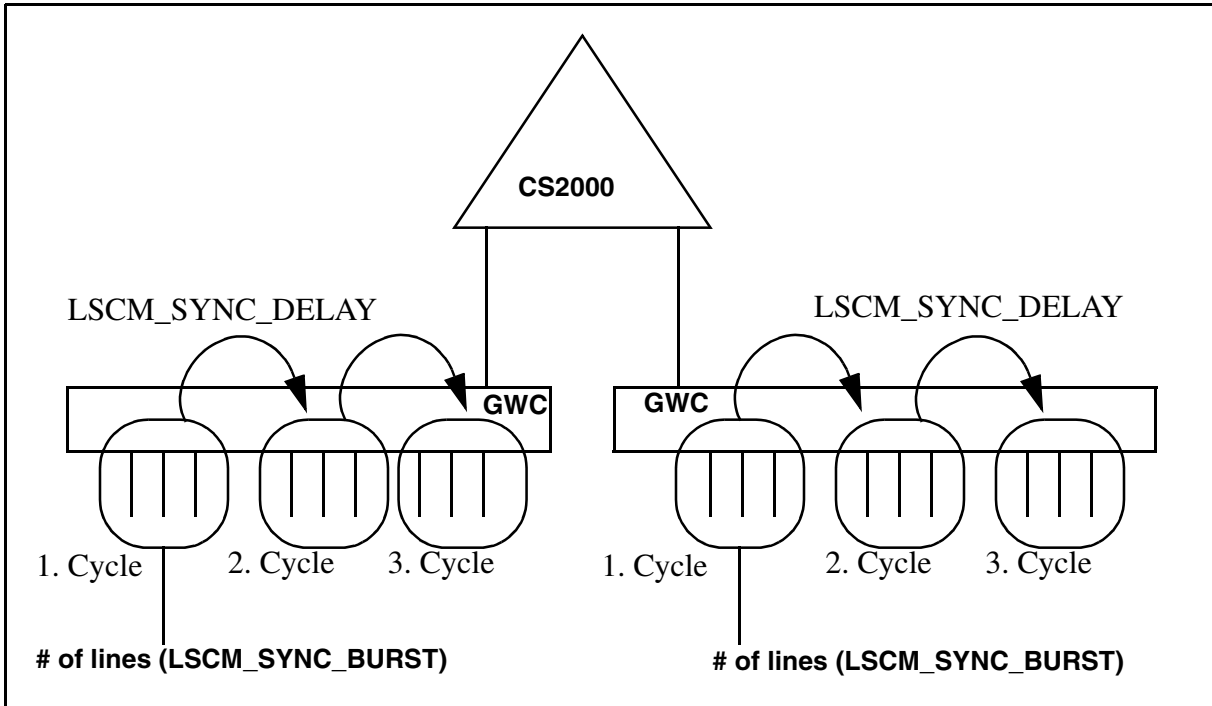
In table OFCENG two tuples have to be datafilled in order to start the audit.

OFCENG - Audit

Tuple	Value
LSCM_SYNC_BURST	# of lines audited per peripheral in one cycle (0..10)
LSCM_SYNC_DELAY	delay between audit cycles (5 to 6000 s)

The next figure shows the how the audit based on the two datafillable parameters works. LSCM_SYNC_BURST gives the number of lines on an each peripheral which is audited by one cycle. The LSCM_SYNC_DELAY defines the time between the cycles.

Audit Process



Engineering information is provided below.

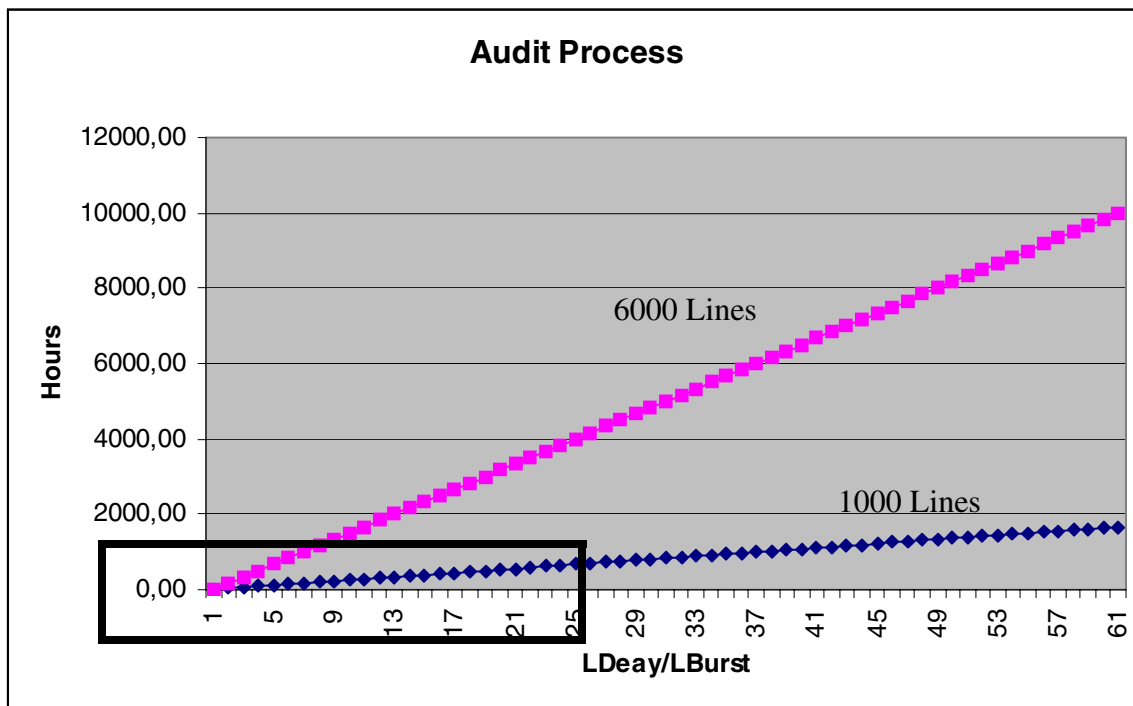
The following variables are defined:

- L_{Burst} (as datafilled)
- $L_{SyncDelay}$ (as datafilled)
- N_{all} (Number of all Lines connected to Peripherals)
- t_{circle} (Time for one complete Circle for all Lines)
- t_{c1} (Time for one circle)

For the first calculation $t_{c1} \ll 1s$ and is not be considered.

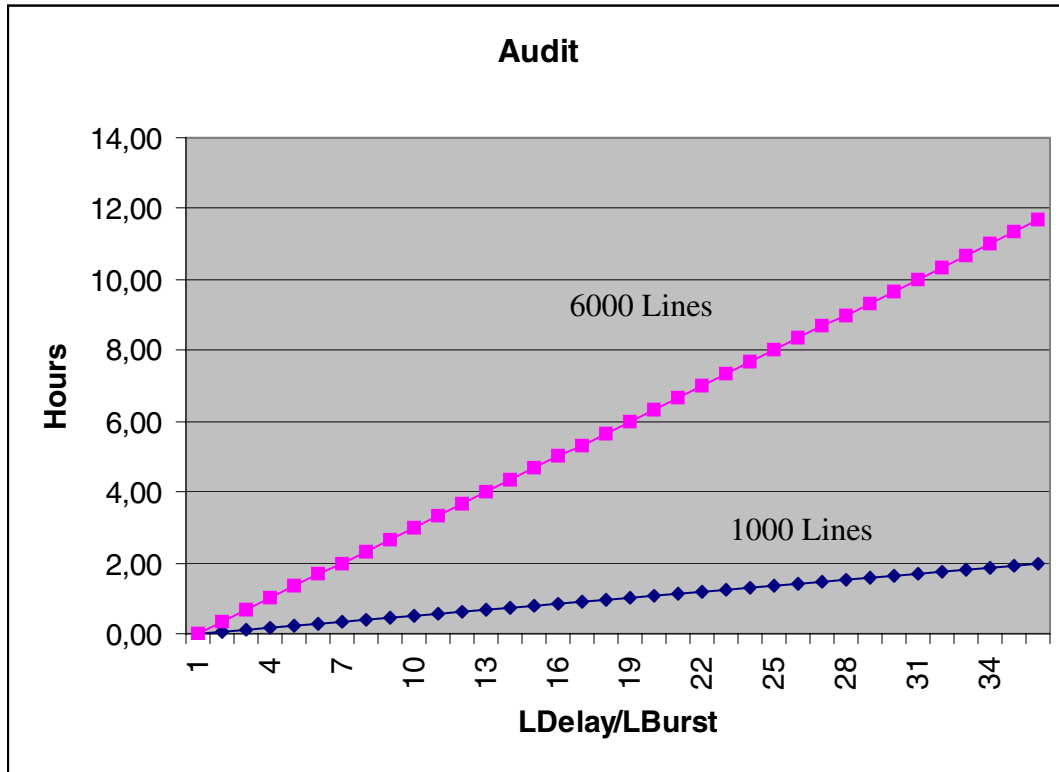
$$\left(\frac{L_{Burst}}{L_{SyncDelay} \cdot N_{all}} \right)^{-1} = t_{circle}$$

Diagram for Audit Process



A detailed view of the marked area is shown in the next figure.

Diagram for Audit Process--detail



If t_{c1} is not considered to be small in comparison with the complete cycle time the equation will change into:

$$\left(\frac{L_{Burst}}{(L_{SyncDelay} + t_{c1}) \cdot N_{all}} \right)^{-1} = t_{circle}$$

t_{c1} is not only dependent on the time of the audit itself. Traffic and System Usage need to be considered.

1.3 Hardware Requirements or Dependencies

n/a

Software Requirements or Dependencies

n/a

1.4 Limitations and restrictions

- SMDI as a Controlling User is not included in this activity.
- No CEPT style user activation/deactivation for CMWI Ring Splash supported
- V5.2 Receiving Users are not covered by this activity.
- MWT_ANNOUNCEMENT will not be visible in KSETFEAT table for ISDN lines,
- Since MWT_ANNOUNCEMENT is not supported for ISDN lines, this field automatically set to FALSE, during addition of MWT option to ISDN lines.

1.5 Interactions

- CFIND: CFIND has precedence over MWI when Call Forwarding is active
- WML: The warm line timer is started after the announcement for MWT has finished playing.
- CEPT CFU (Call Forwarding Universal): CFU always gives a special dial tone to the user if CFU is active. If CFU and MWI are active and the user has the MWI announcement option, and first the announcement is played and then the user will hear the CEPT CFU tone.
- CEPT CFB/CFD: No interaction

1.6 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface _____

Element Management _____

Security _____

Service Order _____X_____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

Glossary

Term	Description
VMS	Voice Mail System
CMWI	Class Message Waiting Indicator
MWI	Message Waiting Indicator
PRI	Primary Rate Interface
CEPT	European Conference of Post and Telecommunications Administrations
CFx	Call Forwarding
CLASS	Custom Local Area Signalling Service

1.7 References

- PKT-SP-EC-MGCP-I02-991201 PacketCable Network-Based Call Signalling Protocol Specification

2: A89007819 Functional description (FN)

2.1 Feature name

QoS Reporting: QoS Collector Application (QCA)

2.2 Description

This document covers the QoS Collector Application functionality supported in SN08 time frame.

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.

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 will report these statistics via end-of-call reporting mechanisms specific to the protocol used for MGC - VMG communication.

It is the purpose of this activity is 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 ATM and hybrid networks as well. In the SN06 time frame, however, QoS Reporting will be 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.

The proposed architecture for QoS Reporting in SN06 consists of the following components;

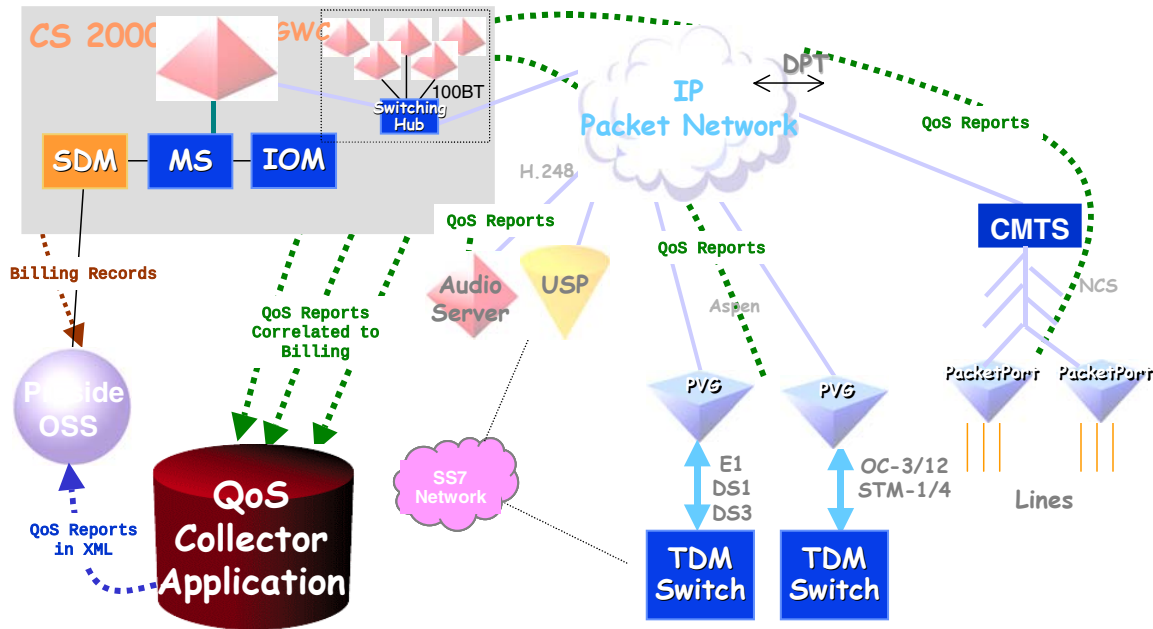
1. QoS Correlation ID and billing
2. QoS Reporting Application (on GWC)
3. Provisioning
4. QoS Report collection
5. QoS Report processing

This activity implements component 4. QoS Report collection, the QoS Collector Application (QCA).

2.2.1 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 Network".

Figure 1 QoS Reporting in a VoIP Network

2.2.2 Configuration

The configuration details for the QoS Collector Application are provided by a properties file. 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 46 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	1
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
fileExt	the output file extension	N/A	String	xml
nodeName	the node name to be used in the output files	N/A	String	QCA

Table 1 QCA properties

Name	Description	Units	Range	default
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.

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.properties` 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 QCA001 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

```

2.2.3 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`.

2.2.4 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.

2.2.5 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).

2.2.6 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.

2.2.7 QCA File Management

The active output file is in the active directory. When a file is closed it is moved to the today directory.

2.2.7.1 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.

2.2.7.2 Output directory

The directory used for the current QCA output is:

`/data/qca/"port number"/output/active`

Note: In SN08, 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.

2.2.7.3 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:

¹servman is the application service manager on the SSPFS platform starting SN06.2. servman manages registration and de registration of all client applications running on the SSPFS machine whether it is simplex or clustered.

QCA.Telco_Switch_35.QoS.2002.04.11_02.45_EDT.xml

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.

2.2.7.4 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. These values are MaxFileSize and MaxFileTime, respectively, in qca.properties.

2.2.7.5 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 as 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 in disk space requirements. And without 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.

2.2.7.6 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 required 'per day' disk space requirements and therefore 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:

$$\frac{8000 \text{ MBytes}}{1000 \text{ MBytes}} = 8 \text{ days}$$

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.

2.2.7.7 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.

2.2.8 Growing the Size of /data/qca

See Appendix B for the Procedure to grow the size of Partition /data/qca.

2.2.9 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.

2.2.9.1 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 Table 2, “Binary QoS record fields,” on page 56.

Table 2 Binary QoS record fields

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

Table 2 Binary QoS record fields

Name	Description	Range
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 the endpoint	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 2147483647
Packets Received	The total number of packets received	0 to 2147483647
Octets Sent	The total number of payload octets transmitted	0 to 2147483647
Octets Received	The total number of payload octets received	0 to 2147483647
Packets Lost	The total number of packets lost	0 to 2147483647
Jitter	Estimate of packet interarrival time (milliseconds)	0 to 32676
Latency	Estimate of network latency (milliseconds)	0 to 32676

2.2.9.2 QCA IPDR record format

The output of the QCA is a single stream (file) of IPDR Version 3.1-A.0.2 compliant records.

2.2.9.2.1 QCA IPDR elements

The IPDR elements used in the QoS output format are shown in Table 3, “QCA IPDR tags,” on page 57.

Table 3 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.

Table 3 QCA IPDR tags

QoS Field Tag	Type	Range
originalDestinationId	String	Called-party (designation) number
hostName	String	0 to 22 characters
subscriberId	String	0 to 65 characters
uniqueCallId	String	20 hexadecimal digits
ipAddress	String	7 to 15 numerical characters
portNumber	String	0 to 65535
seqNum	integer	0 to 16777215
averagePacketLatency	integer	0 to 32676
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 32676

An example QCA IPDR record:

```

<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>GWC3@COMITIP</hostName>
<subscriberId>aaln/1@http018.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>

```

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. in SN06 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.

2.2.9.3 QCA IPDR element values

See Table 4, “Mapping of input binary QoS Record fields to output QCA IPDR record elements,” on page 59.

Table 4 Mapping of input binary QoS Record fields to output QCA IPDR record elements

Output QCA IPDR elements	Input Binary QoS field	Comment
StartTime	N/A	Not applicable. Hardcoded value used: 1970-01-01T00:00:00.000Z
EndTime	N/A	Not applicable. Hardcoded value used: 1970-01-01T00:00:00.000Z
timeZoneOffset	N/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 less than 0, indicating that the GW did not support the statistic.
inboundByteCount	Octets Received	
outboundByteCount	Octets Sent	
inboundPacketCount	Packets Received	
outboundPacketCount	Packets Sent	
inboundLostPacketCount	Packet Loss	
packetDelayVariation	Jitter	

The following elements are 'required' IPDR elements so have been included in the QCA output for IPDR compliancy.

- StartTime
- EndTime
- timeZoneOffset
- CallCompletionCode
- originalDestinationId

2.2.9.4 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.

Please see Figure 3, "QCA IPDR file format" for an example QoS XML file format.

Figure 3 QCA IPDR file format

Line no.	Line	Description
1	<code><?xml version="1.0" encoding="UTF-8" ?></code>	File header
2	<code><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"></code>	IPDRDoc is the file open tag
3	<code><IPDR></code> <code>.</code> <code>.</code> <code>.</code> <code>.</code> <code>.</code>	Start of record
n-1	<code></IPDR></code>	End of record
n	<code></IPDRDoc></code>	/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"

2.2.10 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 5 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

Table 5 QCA Error and Event actions

Error/Event	QCA Action
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
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.

2.2.10.1 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:

- StartTime - 1970-01-01T00:00:00.000Z
- EndTime - 1970-01-01T00:00:00.000Z
- 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, is given in Table 6, “Error IPDR record elements,” on page 64.

Table 6 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
Connection closed: Unrecognised 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

Table 6 Error IPDR record elements

Error/Event	Element	Value
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
	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.

2.2.10.1.1 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: Unrecognised 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>

```

2.2.11 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

2.2.12 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     = 70961557517088778@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: 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 proprietaryErrorCode and displays it as a separate field, Previous seq num.

2.2.13 Installation

The QCA application (NTQCA.pkg) is available in the CS2M¹ 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
```

¹CS2M (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.

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`.

2.2.14 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.

In-service upgrade, with no loss of records, is only supported if two, or more, QCAs are operating in the network. This can be in two configurations; QCAs on different hosts, or multiple QCAs on a single host.

The new QCA should be started and run in parallel with the original QCA for a soak period. After the new QCA has successfully passed the soak period the original QCA can be stopped.

Installing the new QCA software overwrites the original QCA software. So it is suggested to take a backup of the original QCA software in the event that the new QCA software needs to be backed out.

2.2.15 QCA customer logs

In addition to QCA Error IPDR Records the QCA raises alarms and events via the customer logging stream.

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.

2.2.16 Patchability

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.

2.2.16.1 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.

2.2.16.2 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.

2.2.16.3 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.

2.2.16.4 Restart and Auto Restart 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.

2.2.17 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.

2.3 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.

2.4 Software Requirements or Dependencies

- SSPFS 3d party software suite Version 06.

2.5 Limitations and restrictions

2.5.1 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). 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.

2.6 Interactions

- Syslog daemon server

2.7 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) _____

2.8 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

Term	Description
GWC	Gateway Controller
IP	Internet Protocol
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
PFRS	Patch File Receipt System
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
XML	eXtensible Markup Language

2.9 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

2.10 Appendix A - QCA Customer logs

Table 7 Service summary (initialization) warning logs

Event / Error	Report #	Priority	Event Type	Description	QCA Action	Cust-omer 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
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

Table 7 Service summary (initialization) warning logs

Event / Error	Report #	Priority	Event Type	Description	QCA Action	Cust-omer Action
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
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

Table 7 Service summary (initialization) warning logs

Event / Error	Report #	Priority	Event Type	Description	QCA Action	Cust-omer Action
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: <i>directory</i> as it is older than x days.	Director y remove d	None
File found in active directory when QCA started.	202	None	INIT	File Recovery: <i>file name</i> found in active directory. This could indicate that the QCA failed. Please check debug logs.	File complet ed (if necessa ry) and moved to today director y.	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 8 Trouble logs

Event / Error	Report #	Priority	Event Type	Description	QCA Action	Customer Action
File handler or server socket could not be started.	300	None	FAIL	QCA not started: Could not open server socket: <i>+reason</i> or QCA not started: Could not create File Handler: <i>+reason</i>	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 = ' <i>record sequence number</i> ' previous sequence number = ' <i>last record sequence number</i> '	XML Error record generated.	None
Problem processing binary QoS record.	302	None	FLT	Problem processing binary QoS record: Sequence number = ' <i>record sequence number</i> ' Relevant MGC is mentioned in <i>Component ID</i> attribute of the log.	XML Error record generated. XML QoS Record not written to file.	None
QoS Record received with Unsupported Length. (Notification Id: 9)	301	Minor	FLT	Location: <hostName> Notification ID: 9 State: Raise Category:Processig 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:Processig 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

Event / Error Report #	Priority	Event Type	Description	QCA Action	Customer Action	
QoS Record received with Unsupported Version. (Notification Id: 57)	301	Minor	FLT	Location: <hostName> Notification ID:57 State: Raise Category:Processig 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:Processig 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
The binary QoS Record header could not be processed.	305	None	FLT	Connection closed: Error while processing QoS record header: Client at, IP Address ' <i>client IP Address</i> '. Local Port ' <i>local port number</i> ' 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:Processig 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:Processig 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.

Event / Error Report #	Priority	Event Type	Description	QCA Action	Customer Action	
Disk space is below the minimum threshold. Initially set at 1Gb.	310	Minor	TBL	Location: <hostName> Notification ID: 49 State: Raise Category:Processig 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.
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.

Event / Error	Report #	Priority	Event Type	Description	QCA Action	Customer Action
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.
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 <i>output</i> directory. Cannot write records. QCA shutting down	QCA is stopped.	Check: directory structure, active and old files.

Event / Error	Report #	Priority	Event Type	Description	QCA Action	Customer Action
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 <new File Name>. 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 COnection: ' <i>MGC Type MGC number</i> ': sequence number = ' <i>record sequence number</i> '	XML Error record generated	

Table 9 Information and alarm clear logs

Event / Error	Report #	Priority	Event Type	Description	QCA Action	Customer Action
Connection closed.	305	None	INFO	Connection closed. Client at, IP Address ' <i>client IP Address</i> '. Local Port ' <i>local port number</i> ' 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 #	Priority	Event Type	Description	QCA Action	Cus-tomer 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."	Connec- tion to client closed	None
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

Event / Error	Report #	Priority	Event Type	Description	QCA Action	Customer Action
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	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: CONNECTIONCLOSED Description: Client at, IP Address: closed connection	None	None

Examples of Error messages given below:

Table 3 201 Message

Report #	Message
201	May 27 16:41:45 rtpysesm1 QCA: _V2_~l=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

Table 4 202 Message

Report Message #	
202	Aug 19 22:22:02 wnc0s0qu QCA: _V2_~l=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

Table 5 203 Message

Report Message #	
203	May 30 22:55:50 india1sesm QCA_STOP: _V2_~l=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

Table 6 300 Message

Report Message #	
300	May 31 04:22:08 india1sesm QCA: _V2_~l=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^M ComponentID: GWC-99^M SpecificProblem: Socket creation error.^M Description: QCA not started:^M

Table 7 302 Message

Report Message #	
302	May 31 04:22:08 india1sesm QCA: _V2_~l=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

Table 8 305 Message

Report Message	
#	
305	Aug 19 22:18:34 wnc0s0qu QCA: _V2_~l=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

Table 9 310 Message

Report Message	
#	
310	May 30 22:52:45 india1sesm QCA: _V2_~l=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 thereis less than ^M 104857600 bytes available on the local disk.^M Description: More Disk space is required immedietly.^M

Table 10 315 Message

Report Message	
#	
315	Aug 19 22:15:43 wnc0s0qu QCA: _V2_~l=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

Table 11 322 Message

Report Message	
#	
322	Aug 19 22:15:43 wnc0s0qu QCA: _V2_~l=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

Table 12 399 Message

Report Message #	
399	Aug 18 06:49:08 wnc0s0qu QCA: _V2_~l=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 is no changes in Alarms as a result of feature A00008338)

There are 3 different Types of Alarms uniquely identified by the Notification ID:

- 1 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.
- 2 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.
- 3 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 13 301 Message- Raise

Report Message #	
301	May 31 07:37:20 india1sesm QCA: _V2_~l=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 14 399 Message- Clear

Report Message #	
399	May 31 07:39:47 india1sesm QCA: _V2_~l=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 B- 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

```
# filesystems 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# filesystems 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 udfstat command by typing

udfstat

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.

3: A00003953 Functional description (FN)

3.1 Feature name

Active Call Failover

3.2 Overview

The Dual-Node Redundancy feature implemented in SN06.2 took the first steps in shifting the CICM's architecture away from a load-sharing model to one with a master-slave relationship. However, DNR restricted itself to implementing takeover redundancy on the northbound interface (i.e. H.248) only. The south-side of the CICM continued to maintain its load-sharing capacity allowing terminals to connect to either node.

The obvious implication of this is that on failure of a node, while communication to the GWC is maintained, all terminals hosted off the defunct node experience an outage as they reboot and reconnected to the mate. If the user happens to be on a call, then the call is lost.

The Active Call Failover feature aims to address this shortcoming by completing the shift away from a load-sharing model on the terminals interface to one of full takeover redundancy. With ACF, all terminals only ever connect to the master node of the CICM. Should this node fail, the mate assumes the role of the master and begins the recovery of terminals while maintaining active calls.

3.3 Description

The ACF feature is developed and tracked as 4 separate sub-activities. Each activity tracks a somewhat independent component. Together, the 4 activities each contribute to the overall ACF feature.

The 4 sub-activities and software components are:

- A00003953 – Base
- A00007637 – Authority
- A00007619 – Call Processing
- A00007639 – OAMP

Although this document is maintained under the A00003953 activity, it applies equally to all 4 activities listed above.

3.4 System Description

The following figure shows the relationships between software components of the CICM as they interact in SN06.2 following the implementation of Dual Node Redundancy.

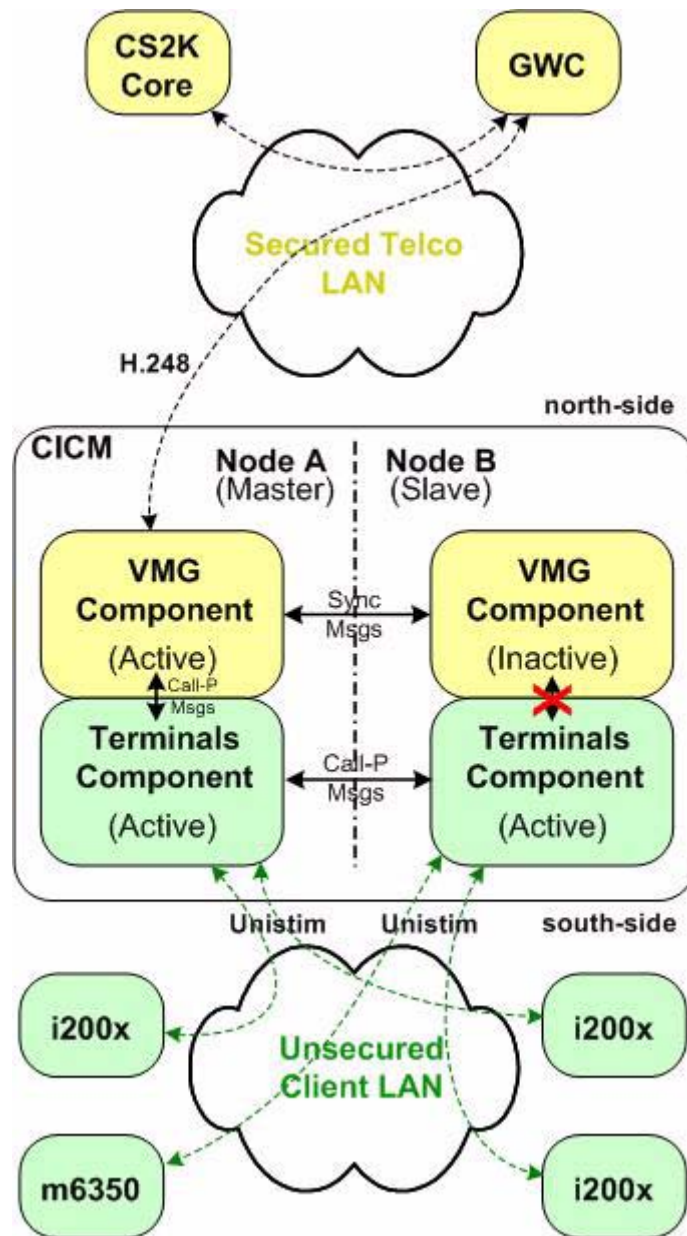


Figure 1: The pre-ACF CICM

The figure shows that communication to the GWC (with H.248) is provided by a single active interface managed by the master node. However, communication to the terminals takes place equally on both nodes regardless

of which node is the master. Each node presents its own interface (or IP address) to the terminals.

The following figure illustrates the overall architecture of the CICM with ACF. The significant differences from Figure 1 are highlighted in italicised red.

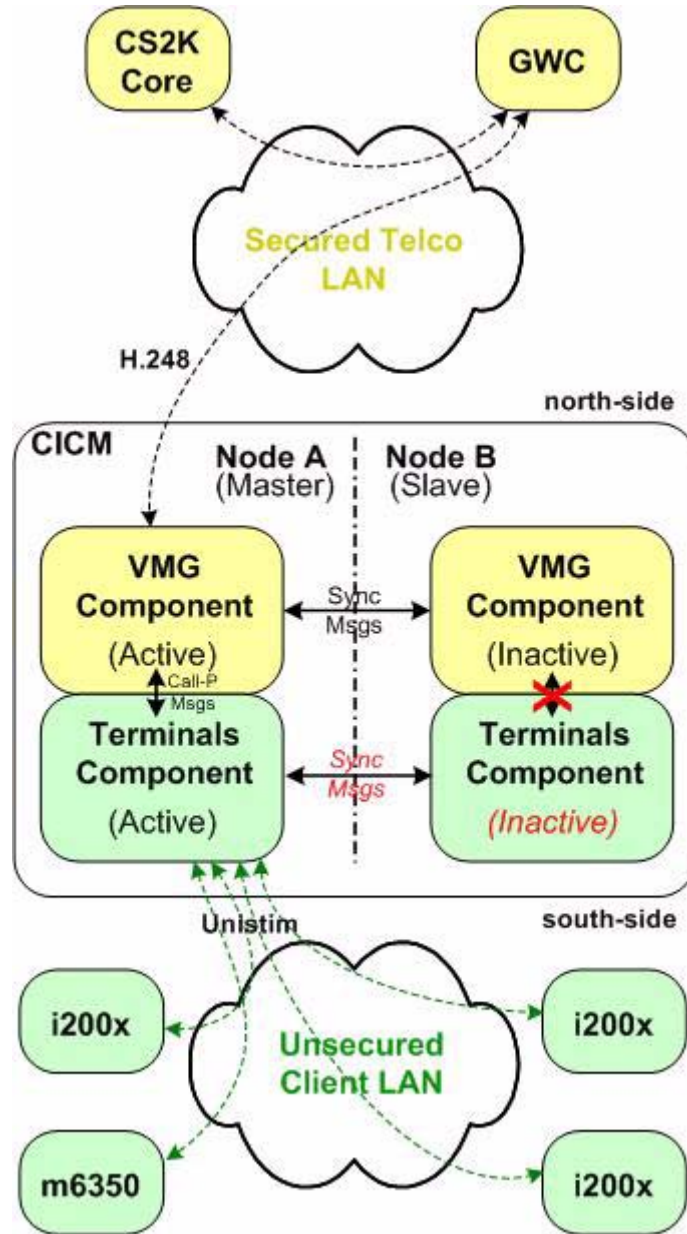


Figure 2: The ACF CICM

As shown, the north-side of the CICM continues to communicate with the GWC using the H.248 protocol via a single interface. This remains consistent with the SN06.2 behaviour.

However, Active Call Failover changes the CICM's architecture such that the south side now also presents a single, but unique interface. Terminals no longer have an option to connect to one node vs. the other as in SN07. Instead, they are now only aware of a single IP address towards which all Unistim messaging must be directed. This address is bound to the master node.

Thus both the H.248 and Unistim interfaces each make use of their own "floating" IP address that is bound dynamically to the master node's interface. Each component shown in Figure 2 is responsible for managing its floating address and to ensure it is swapped to the mate on a switch of activity.

The inactive VMG component keeps in constant near-full synchronization with the active side. The double-headed arrow connecting these components on both nodes of the CICM illustrates this. This is necessary to ensure that both nodes have an accurate view of the state of call processing at anytime thus allowing the inactive side to take over control of these functions on a switch of activity.

As for the Terminals component, the inactive component also maintains a state of synchronization with the active component. However, the level of this synchronization is kept to a minimum for various reasons that are outside the scope of this document. The impacts and limitations of this minimal synchronization will be addressed in more detail in the sections that follow.

3.5 Switch of activity

A switch of activity (or SWACT) occurs when the role of the master is transitioned from one node to the other. From Figure 2, this implies that following a SWACT, communication with the GWC and the terminals is maintained by the newly promoted master (in this case node B). This is illustrated in Figure 3.

As perhaps suggested by the figures, a platform switch of activity is carried out internally one component at a time. The process begins with the VMG and ends with the Terminals component. It is therefore possible that as the switch of activity is in progress, one node may find itself hosting the active VMG component while simultaneously hosting the inactive Terminals component.

However, such a state is transient and there is no facility for the operator to selectively choose to SWACT an individual component over another or stop the maintenance action mid-stream once initiated. By definition, a switch of activity is carried out atomically over the entire platform such that once completed, both nodes will have entirely exchanged roles.

previous role. A manual SWACT is generally executed in order to perform maintenance activities.

An uncontrolled SWACT is autonomously initiated by the system on failure of the master node. No immediate operator intervention is required for the slave node to assume the role of the master in such a circumstance.

3.5.1 Technical details of a switch of activity

A switch of activity requires a number of actions to be performed before it can be considered completed. In the context of ACF, some of these actions can be lengthy. This section aims to provide a summary of what occurs on a SWACT in order to help highlight and explain the reasons behind some of the durations stated later.

The first thing to understand is that each component of the CICM switches its activity rather independently of the other components in the system. Only once a component reports that it has completed its SWACT does the system proceed on to the next. Once all components have switched activity, a final step is performed allowing all new master components to complete any needed clean-up activities.

On the CICM, this translates to the following steps:

- 1 The system detects the need for a switch of activity
- 2 The VMG component undergoes a switch of activity
- 3 The Terminals component undergoes a switch of activity
- 4 Each component gets a chance to perform clean-up actions
- 5 The system marks the switch of activity complete

Note that, implicitly, the steps just listed mean that for some time between steps 2 and 3, each node finds itself running one but not all active components.

3.5.1.1 Virtual Media Gateway

The VMG component is the first to switch its activity. The process to SWACT this component has not been impacted by ACF and remains unchanged since it was first implemented for DNR (see reference [1]). In short, the active component unbinds and simply hands off ownership of the floating H.248 address to the inactive component. The new active component (previously the inactive), binds the address and resumes communication with the GWC thus taking over the call processing role.

Although the switch of activity of the VMG component is short, during the switch only “stable” calls are guaranteed to survive. Unstable calls may or may not survive.

A stable call is defined as a call in which the parties have achieved the talking state and for which no user interaction is in progress. Anything else is considered to be an unstable call. The following list provides a few examples of possible problem cases that could occur during a SWACT of the VMG component:

- 1 A call in the middle of being setup may not terminate and could be lost.
- 2 A user interacting with a feature such as setting up a 3 way call could find herself losing both parties should a SWACT occur before speech path is established between all parties.
- 3 General terminal stimulus could be lost during a SWACT that could in turn lead to a misdialled call.

3.5.1.2 Terminals

Once the VMG has completed its switch of activity, the system begins the Terminals component SWACT. Similarly, the active component unbinds and simply hands off ownership of the floating Unistim address to the inactive component. The previously inactive component binds the address thus assuming the role of the active component. This is where similarities to the VMG SWACT end.

In order to understand what the new active Terminals component does next, it helps to understand some of the details about the nature of the communication between the CICM and its terminals.

When a terminal first boots up, it sends an initial Unistim message to the CICM to advise it that it wishes to establish a session. As part of the initial exchange, the CICM and terminal agree on some sequence numbers to use.

Sequence numbers are part of RUDP's inbuilt retransmission mechanism and serve to ensure that neither party loses any messages. By sequentially numbering each message the CICM sends to the terminal, the terminal can easily determine the sequence number (and therefore message) it is meant to process next. This mechanism naturally allows it to detect the loss of any messages. CICM to terminal messages use one set of sequence numbers while terminal to CICM messages use a different set of numbers.

Due to the large number of terminals that the CICM supports, it is not possible for the active Terminals component to actively sync across to its mate each terminal's sequence number for each Unistim message it exchanges with the terminal. This approach would be impractical and would be much too real-time intensive.

As a result, the Terminals component syncs only the minimal set of information needed for its counterpart to actively recover the terminal on a switch of activity.

Therefore, after the new active Terminals component has bound the Unistim floating IP address, it begins actively recovering each terminal in order to re-learn the sequence numbers that the terminal expects to use (RUDP provides a mechanism for this). As the CICM supports a large number of terminals, such an operation can take a while to complete.

Between the time that the Unistim floating address is moved and a terminal has been recovered, the CICM has effectively lost its virtual connection to the terminal. However, so long as the terminal does not attempt to communicate with the CICM during this time, it remains unaware of the lost connection. Should it be a in a call, it takes no notice of this situation and continues happily transmitting and receiving audio (RTP and RTCP). Neither party in the call experiences an outage or interruption in the audio stream. Likewise, the core is also unaware of this temporary situation so billing is unaffected.

Naturally, the CICM's goal is to recover all terminals. However, due to the terminal watchdog mechanism, it must do this quickly before any terminal times out and reboots.

A quick recap of this mechanism also seems in order. The keep-alive is driven by the Terminals component and periodically sends a message to each terminal effectively telling it to "Reboot in N seconds". Although N currently defaults to 120 seconds, it is configurable. Therefore, if the CICM fails to send a subsequent "Reboot in N seconds" message before the timer expires, the terminal reboots and attempts to reconnect.

Thus, in order to maximize its chances of recovering all terminals before any reboots, the Terminals component begins recovery with the terminal that was least recently sent the "Reboot in N seconds" message and begins the recovery from this point. Assuming the current default, the Terminals component must therefore recover sequence numbers and transmit the "Reboot in N seconds" message to all terminals within at most 2 minutes.

As suggested earlier, while the recovery process is executing, it is important to consider that external events may occur. Two types of events could occur between the time the Unistim floating address is transferred and an individual terminal is recovered:

- 1 A Unistim message is received from the terminal itself
- 2 A call processing event destined for the terminal is received from the GWC

The first event type can originate from simple user interaction with the terminal. This could be anything from going on hook, switching between calls (streams) or simply changing some user settings (in the case of an IP Phone). In order to avoid the terminal rebooting and to give the user as responsive

feedback as possible, the session is placed at the head of the queue for immediate recovery.

Because of this support for early recovery, no user generated events are lost during the SWACT of the Terminals component. However, as the recovery introduces a delay before the user's input may be acted upon, a delay in the response to the first few key events should be expected.

The second event type would most typically occur with the interaction of the user at the far end. In such cases, the resulting events from the GWC cause an immediate update to the VMG component's state for the terminal. The VMG component then instructs the Terminals component to queue up the terminal targeted by the message for immediate recovery. As in the first case, this need for a recovery introduces a delay to the GWC message being acted upon by the Terminals component. Although it is approximately of the same period as in the first case, it is far less likely to be noticeable by the user in this case due to the nature of the event.

The last point worth mentioning about a system SWACT is that once initiated, it cannot be stopped or aborted. This restriction follows naturally once the effort required to recover individual terminals is considered.

Once the master Terminals component releases the floating Unistim address, all terminals **MUST** be actively recovered. Allowing a SWACT to be aborted could see the floating IP address easily returned to the original node without problem, but then the terminals recovery would once again need to be restarted. Given the minimal window available to recover all terminals without having any of them timeout and reboot, the additional delay introduced by an abort would surely result in a loss of some (and possibly many) terminals.

As a result, should a failure of the master node occur while terminal recovery is in progress, it follows that an autonomous SWACT must occur to attempt and recover the situation as best as possible. In this rare case, it cannot be guaranteed that all terminals will be recovered. These terminals would likely reboot and any calls hosted lost.

3.6 System start and stop

This section describes the behavior that can be expected from the CICM in normal circumstances during start and stop scenarios.

3.6.1 First node start-up (master)

As the first node of the CICM initializes and begins operation, it broadcasts periodic heart beat messages on its private admin LAN directed to its mate node. As it does not observe corresponding heartbeats from its mate, it assumes the role of the master.

The north-side binds the floating H.248 address and begins sending H.248 messages to the GWC advising it when it is available for service. A number of initial is at ion messages are exchanged between the CICM and the GWC. Meanwhile the south-side likewise binds the floating Unistim address and begins accepting incoming connections from terminals.

Once in service, users at connected terminals may login, make and receive calls and also use other available CICM services.

3.6.2 Second node start-up (slave)

As the second node initializes, it also begins broadcasting periodic heartbeats directed to its mate. As the master is already broadcasting, the second node notices this and assumes the role of the slave.

Both the VMG and Terminals components are advised by the system to initialize as slaves. The VMG therefore does not begin communicating with the GWC and the Terminals component does not expect incoming connection requests from terminals.

Instead, the VMG requests a bulk synchronization of all call processing data from its mate and the Terminals component makes a similar request from its counterpart. Once these operations are completed, each component on the master node continues dynamically sending synchronization information to keep the corresponding inactive components constantly up to date on the mate node.

Only when all software components have started and the bulk synchronizations have completed is it possible to manually initiate a switch of activity.

3.6.3 Manually stopping a node

A node may be stopped or restarted using the element manager's maintenance page. For the purpose of our redundancy discussion, both actions are effectively equivalent and are therefore treated as such in software. For simplicity we will therefore always refer to a system stop and simply ignore node restarts.

Two legal scenarios exist:

- Both nodes are running; Operator stops slave
- Only master is running; Operator stops master

It is not possible to stop the master node while the slave node is running. To stop a node running as master, the operator must first issue a SWACT, wait for it to complete and then stop the node that is now slave.

Initiating a stop or restart from the CICM element manager performs the appropriate checks and presents the operator with appropriate warning or error messages in order to enforce the desired behavior. In some cases, the system may recommended courses of action in order to minimize any impact on service.

Stopping the slave causes the software load on that node to systematically cease. This action has no adverse effects on the master node and it continues normal call processing. However, the CICM can of course not offer any failover functionality while in this state. Stopping the master node when it is on its own obviously causes a service outage.

3.7 Node failures

Only two interesting scenarios exist. We are interested in the case where both the master and slave nodes are running and one or the other of the following occurs:

- The master node fails
- The slave node fails

The only other case in which a failure is possible is that of a node running in standalone mode and subsequently fails. In this case, as the node is running on its own, it would of course have already assumed the role of the master. However, this case is uninteresting simply because if the node fails, no action can be taken. There is no redundant node to fall back on.

A “node failure” may have any number of possible causes. The term applies equally to both hardware failures of the physical CPU card running the CICM load or to some critical software error for which no recovery action is possible. The following is a non-exhaustive list of just some of possible node failures:

- Should any of the software components that make up the CICM load experience a software exception (i.e. trap), monitoring software automatically initiates an immediate restart of the node.
- A general failure of the CPU card

From the remaining node's perspective, the above cases are identical in that its mate suddenly stops providing heartbeats. The surviving node thus takes appropriate action as described in the following sections.

All but LAN adapter failures are treated equally by the redundancy functionality. When physically possible, any critical failure will result in the node automatically restarting a preset number of times (default is 3) that can be configured by the operator. Following the last restart, the boot controller will not start the CICM software load.

3.7.1 Master fails

When the master node experiences an unexpected failure, the slave node detects it and performs an autonomous switch of activity to assume the role of the master.

The SWACT occurs transparently to the GWC as the new active VMG component binds the floating H.248 IP address. Some inbound messages from the GWC may be lost during the takeover, but the retransmission algorithm built in to H.248 ensures that they are eventually delivered. However, during this component's SWACT, only "stable" calls are guaranteed to survive. Unstable calls may or may not survive.

Likewise, the switch of activity occurs semi-transparently to the terminals as the new active Terminals component binds the floating Unistim IP address. We say "semi-transparently" because the Terminals application must now proceed to recover the individual terminals as previously described. Despite this recovery procedure, the end user experiences no loss of any currently active stable calls.

3.7.2 Slave fails

When the slave node experiences an unexpected failure, the master detects it, but does nothing except make note of the failure. No SWACT occurs and so no H.248 messages from the GWC are lost and no terminal recovery actions are required. All stable and unstable calls survive the failure on this node.

3.8 Network adapter failures

As hinted in the previous section, LAN adapter failures on the CPU cards are treated differently to other types of failures. These cases call for special consideration.

Before continuing, it is worth defining the difference between a node's critical and non-critical adapter. A node's critical physical adapter hosts both the H.248 and Unistim interfaces when it is the master. Therefore, on a given node, these 2 floating IP addresses can only ever be bound to the critical adapter.

The critical adapter also hosts one of the Admin LAN interfaces able to support cross node communication. The non-critical physical adapter simply hosts a second Admin LAN interface thus providing redundant cross-node communication paths.

3.8.1 Master loses critical adapter

When the master node detects that it has lost layer-2 connectivity on its critical adapter, the master initiates an autonomous SWACT. This is done in order to conserve connectivity to the GWC and terminals thus maintaining call processing.

In such an event, all terminals are transferred to the newly promoted master node (previously slave). As always, unstable calls may experience problems on SWACT of the VMG component.

3.8.2 Master loses both adapters

In the event that the master detects layer-2 loss of connectivity on both its physical adapters, it decides that it is at fault and demotes itself to a slave-like state. The actual slave of course considers the master to have failed and promotes itself to master.

When either of the isolated node's adapters becomes available, it looks for its mate. If found, the node restarts itself in order to come up afresh as the slave and ensure that all its MIB data is synchronised with the master node.

If upon regaining either physical adapter the node does not find a mate, it re-promotes itself to master and proceeds accordingly. Appropriate monitoring software ensures that only one node is ever master at any given time.

In this case, terminals hosted off this node lose their connection when the adapters are first lost (but are recovered by the newly promoted master if available). Communication to the terminals and GWC (if the node resumes its role as master in the future) can of course only be re-established if the critical adapter is regained.

3.8.3 Slave loses critical adapter

Should the slave node lose layer-2 connectivity on its critical adapter, it simply updates its own local state and advises the master node of the state change. This is necessary in order to ensure that a SWACT is not inadvertently initiated either manually or autonomously. No switch of activity occurs.

3.8.4 Slave loses both adapters

In the event that the slave detects layer-2 loss of connectivity on both its physical adapters, it acts almost exactly as described previously. The only difference being that the node does not need to demote itself. It is already the slave.

3.9 Hardware and Software Requirements

3.9.1 Hardware requirements

Active Call Failover introduces no new hardware dependencies or requirements. However due to the redundancy nature of ACF, it is of course necessary for the 8.10 CICM software load to be installed on a *pair* of matching CPU cards.

The 8.10 load is supported on:

-
- Motorola 5370 CPU cards in a SAM16 chassis, or
 - Motorola 5385 CPU cards in a SAM21 chassis

3.9.2 Software requirements

Active Call Failover is introduced in the 8.10 CICM release (SN08). This load level must therefore be installed on a pair of CPU cards (as listed above) in order to take advantage of the functionality.

The 8.10 CICM release introduces no mandatory requirements on either the m6350 or the IP terminal firmware. However, some enhancements have been made to both the firmware and the m6350 software in order to minimise the impact on the user experience over a SWACT. It is therefore recommended that the terminals be upgraded to the latest versions that ship as part of the CICM release.

3.10 Maintenance Aspects

3.10.1 Initial Installation and Configuration

The initial installation process of the 8.10 CICM remains largely unchanged from 7.20. Please see reference [2] for a full description of the existing installation process.

Active Call Failover introduces changes to a single preboot step run at initial installation.

3.10.2 Unistim VLAN

The main goal of ACF is to expose a single IP address through which all Unistim communication with the terminals takes place. Despite this, the CICM continues to require 2 static Unistim addresses in addition to the new floating address. However, it is not possible to route to either of the static addresses as they are blocked to all incoming traffic. They exist solely for internal system purposes.

The Unistim preboot configuration step is now practically identical to the H.248 configuration step. When this step is reached, it prompts:

```
Enter the Floating Unistim IP address for this CICM:
```

Followed by the familiar prompts:

```
Enter the Static Unistim IP address for Node A:
```

```
Enter the Static Unistim IP address for Node B:
```

As always, the user is expected to enter the same information on both nodes of the CICM. Failing to do so will lead to undesirable erroneous behaviour.

Next, preboot asks:

```
Enter the network mask for the Unistim IP network:
```

Simply enter the network mask of the Unistim VLAN. Finally, it prompts:

```
Enter the default route for the Unistim IP network
(Enter 0.0.0.0 for no route):
```

As prompted, enter the default route or “0.0.0.0” for none.

Finally, it is worth pointing out that should it become necessary to carry out a network reconfiguration, the Unistim preboot step can be manually re-executed by issuing the following command through a CICM terminal window:

```
preboot unistim /interactive
```

All information is prompted for once again upon issuing these commands, thus allowing the operator to change any aspect of the configuration. However, executing this command can only be done safely when neither node is in service thus making an outage unavoidable.

3.11 System Upgrade from 7.20 to 8.10

The only supported upgrade path to 8.10 is from 7.20. As always, the Element Manager must be upgraded to 8.10 before any of the CICMs in the network are upgraded. The upgrade process of the Element Manager from 7.20 to 8.10 remains unaffected by this activity and should be carried out in the same manner as the upgrade from 7.10 to 7.20. It is effectively the same process followed when applying a Maintenance Release (MR) to the EM.

As for the CICM, this system upgrade effectively increases the number of addresses needed on the Unistim LAN from 2 to 3. Of the 2 existing static addresses, the software assumes and in fact enforces that node A's existing address (before the upgrade) is used as the floating Unistim address following the upgrade. Furthermore, the role of node B's static address through the upgrade cannot change. In other words, node B's static address before the

upgrade must remain node B's static address following the upgrade. The 3rd and new address must therefore be used as node A's new static address.

Warning: As always, it is strongly recommended that upgrades be performed when call processing activity on the CICM is low.

3.12 Maintenance and Monitoring Interface

The operator aspects of system redundancy can be accessed from the status and maintenance pages of the Element Manager. Active Call Failover introduces a number of new fields and changes others. As a result, an overall review and consolidation exercise has been carried out on these pages in order to present a more consistent look and feel. The changed fields or those that are of particular relevance to redundancy are discussed next.

3.12.1 System Status

This page changes only slightly in 8.10. Although previously present, the "virtual media gateway" summary table changes only in how the existing information is presented. The "terminals" table entry changes in function and now reflects the new failover ability of this component.

Both of the component tables present 2 identical fields in common. The "Active on" field indicates on which node the active component is running. The field may display one of 3 values:

- node A
- node B
- unavailable

The significance of the first 2 values is obvious. A value of "unavailable" typically indicates that neither node is running. In fact, the "unavailable" state applies to all table fields discussed next when neither node is running. However, when this is so, this fact also appears in the more prominent overall summary at the top of the status page.

The "Peer state" field shows if the inactive component on the mate is in synchronisation with the active component. It may assume one of the 3 following values:

- in sync
- out of sync
- unavailable

A state of "in sync" obviously indicates that it is running and in a state of synchronisation with the active unit. A state of "out of sync" may indicate that

the mate component has not yet (normal on start-up) or not correctly reached a state of synchronisation with the active unit. If the component is not running (e.g. the node may be down; which would appear in the summary section at the top of the page), the “out of sync” state is also displayed.

The “virtual media gateway” table also maintains a third field labelled “State”. This field serves to show the state of the VMG as controlled at the CS2K. It may assume one of the following values:

- in service
- out of service
- unavailable

A state of “in service” indicates that communication with the GWC is established and that the CICM has been instructed as such.

Centrex IP Client Manager

c1cm-180 c1cm status

C1CM-180 - Status - System in Service - No Alarm Refresh 18:21:55 (30 seconds)

Slot	C1CM-180-A	C1CM-180-B
Fault	●	●
Active	●	●
Maint	●	●

Node A, 47.165.168.180 Service = **running**
Node State = slave
Fault code = 0 :
- No faults detected

Node B, 47.165.168.185 Service = **running**
Node State = master
Fault code = 0 :
- No faults detected

virtual media gateway ?

State: **in service**

Active on: node A

Peer state: **in sync**

terminals ?

Active on: node A

Peer state: **in sync**

network ?

IP address	Adapter	Physical Port	Active
192.168.52.33	Intel 8255x-based PCI Ethernet Adapter (10/100) - Packet Scheduler Miniport		Yes
192.168.52.37	Intel(R) Advanced Network Services Virtual Adapter - Packet Scheduler Miniport		Yes
192.168.52.38	Intel 8255x-based PCI Ethernet Adapter (10/100) - Packet Scheduler Miniport		Yes
192.168.52.34	Intel(R) Advanced Network Services Virtual Adapter - Packet Scheduler Miniport		Yes

C1CM-EM 7.0 .administrator

Done Internet

Figure 4: Element Manager Status Page

A state of “out of service” (despite having a node running as master) can be due to the VMG having been manually taken out of service at the CS2K. Otherwise, the VMG typically fails to go into service when communication with the GWC simply cannot be established. This in turn may be due to a

general network problem or could also be due to a failed critical adapter (if a node is running stand-alone) or a failure of both critical adapters (if both nodes are running). However, adapter failures show up in the “network” table on the same page.

The connections and terminals performance monitoring pages that are available from the status page are modified to provide a consistent data set. However, these pages are not shown.

3.12.2 Maintenance Status

The 8.10 maintenance status page is updated in line with the system status page.

In the central area of the page, each node provides a table showing maintenance information about the node. The "Status" field (previously named “Node status”) indicates the platform level state of the node in question and assumes one of the following values:

- idle
- master
- slave
- swacting master→slave
- swacting slave→master
- master (no slave)

The new “VMG status” field shows the current state of the virtual media gateway component on the node in question. It effectively combines into a single field the information contained in the “State”, “Active on” and “Peer state” fields of the “virtual media gateway” table from the system status page. It may assume one of the following values:

- active (in service)
- active (out of service)
- inactive (in sync)
- inactive (out of sync)
- swacting master→slave
- swacting slave→master

Related to the VMG and just beneath it is the “Active half calls” field. When the node’s VMG is active and in service, this field provides the number of currently active half calls (with the total historical number in brackets). When

the VMG is inactive, this field is greyed out and displays a value of “n/a” indicating “not applicable”.

The screenshot shows the 'maintenance status (cicm-180)' page in the Centrex IP Client Manager. The page is divided into three main sections: a left-hand navigation menu, a central table of maintenance status for two nodes, and a right-hand panel with various maintenance actions.

Left-hand navigation menu:

- CICM**
 - status
 - configuration
 - terminals
 - users
 - maintenance
- CICM-EM 8.0**
 - status
 - synchronization
 - maintenance
- profiles**
 - audio
 - enterprise
 - language
 - network
 - user
 - feature
- diagnostics**
 - diagnostics

Central Table: maintenance status (cicm-180)

Node A (47.165.168.180)	
Status	master
Application	running
Maintenance status	system idle (current reboot count: 0)
Version	CICM 8.10 Base Release (Build 8.10.xxx)
VMG status	active (in service)
Active half calls	5 (total calls=342)
Terminals status	active
Logged in users	43 (total logins=262)
Active terminals	54
Terminal recovery status	n/a

Node B (47.165.168.180)	
Status	slave
Application	running
Maintenance status	system idle (current reboot count: 0)
Version	CICM 8.10 Base Release (Build 8.10.xxx)
VMG status	inactive (in sync)
Active half calls	n/a
Terminals status	inactive (in sync)
Logged in users	n/a
Active terminals	n/a
Terminal recovery status	n/a

Right-hand panel: maintenance actions

- apply maintenance release**
 - Node: Node A (47.165.168.180)
 - Maintenance Release: No files found
 - Note: Maintenance releases should be securely transferred to "D:\CentrexIP\support\firmware\gateway_MRs" on the master Element Manager Node
- restart terminal service on node A**
- node A service control**
 - Action: Stop
- node B service control**
 - Action: Stop
- switch activity**
- reset counter**
 - Node: Node A
 - Reset Counter: Current Reboot Count
- start auto refresh**
- refresh now**
- system status**

Bottom left: CICM-EM 7.0 administrator

Bottom center: maintenance home

Figure 5: Element Manager Maintenance Page

Similarly, the “Terminals status” field shows the overall state of this component and combines the information of the “Active on” and “Peer state” fields of the “terminals” table from the system status page. It assumes one of the following values:

- active

- inactive (in sync)
- inactive (out of sync)
- swacting master→slave
- swacting slave→master

Related to the Terminals component and just beneath this field appear 2 additional fields:

- Active terminals
- Logged in users

Similarly, when the Terminals component on the node is active, these 2 fields are enabled and display the information as suggested by their names. When the component is inactive on the node, the fields appear greyed out and display a value of “n/a”.

A third field applicable to the Terminals component serves a purpose only during a switch of activity of the component. Accordingly, it is named “Terminals recovered”. Under normal operation (i.e. no terminals are in the process of being recovered), it shows “n/a” for “not applicable”. During a switch of activity, the newly promoted active unit shows the progression of the recovered terminals as a percentage of the total active terminals.

In the actions section of the maintenance page, the "switch activity" link is only displayed when the functionality is actually available. However, once clicked, a number of automated tests are performed before the system proceeds. The operator may be provided with a number of warnings regarding the consequence(s) of proceeding (if any).

Warning: Once a SWACT is initiated, it CANNOT be manually aborted. The operator must allow for the switch of activity to complete before any further maintenance can be attempted (e.g. performing a second SWACT, applying MRs, etc.).

Following a switch of activity, the roles of both nodes should be exchanged. Initiating this switch of activity manually would generally be desirable for maintenance purposes just prior to taking a node out of service (to swap a faulty CPU blade for instance).

The "node N service control" (where N is either “A” or “B”) box appears for each available node and offers 3 context sensitive options:

- Restart: Stop all services on this node and reinitialise the CPU card. Services restart automatically following the nodal restart and processing should also be resumed.
- Stop: Stops the CICM service from running thus halting processing on the node in question. However, the CPU card remains active.
- Start: Starts a stopped CICM service and resumes processing on the node in question.

Centrex IP Client Manager - Microsoft Internet Explorer provided by Nortel Networks

Address: http://element_manager/centrexip/

Centrex IP Client Manager

maintenance status (cicm-180)

Node A (47.165.168.180)	
Status	master
Application	running
Maintenance status	system idle (current reboot count: 0)
Version	CICM 7.10 Base Release (Build 7.10.xxx)
VMG status	active (in service)
Active half calls	5 (total calls=342)
Terminals status	active
Logged in users	43 (total logins=262)
Active terminals	54
Terminal recovery status	n/a

Node B (47.165.168.180)	
Status	slave
Application	running
Maintenance status	system idle (current reboot count: 0)
Version	CICM 8.10 Base Release (Build 8.10.xxx)
VMG status	inactive (in sync)
Active half calls	n/a
Terminals status	inactive (in sync)
Logged in users	n/a
Active terminals	n/a
Terminal recovery status	n/a

apply maintenance release

Node:

Maintenance Release:

Note: Maintenance releases should be securely transferred to "D:\CentrexIP\support\firmware\gateway_MRs" on the master Element Manager Node

transfer terminals

Node:

Terminal Shutdown Timeout:

node A service control

Action:

node B service control

Action:

switch activity

reset counter

Node:

Reset Counter:

start auto refresh

refresh now

system status

CICM-EM 7.0 .administrator

[maintenance home](#)

Figure 6: Maintenance page during an upgrade

In 7.20, the terminal transfer functionality offered a simple mechanism to automate the migration of terminals from one node to the other. This was useful when performing maintenance activities as both nodes actively hosted terminals.

In 8.10, the terminal transfer functionality becomes redundant as there is no longer any such concept. All terminals are always hosted by the master node. As a result, the functionality is no longer offered on the maintenance page when the Element Manager is inspecting an 8.10 (or later) CICM. The functionality continues to be offered when inspecting a pre-8.10 CICM.

However, there is one exception to the above statement. As previously mentioned, the functionality remains available in the special case when the Element Manager detects that only one of the nodes is running 8.10. The terminal transfer functionality is thus available (and needed) during the actual upgrade process.

The "system status" link box on this page offers the operator a quick and easy method of navigating to the corresponding node's status page. This may often be useful after some maintenance activity has been carried out on the CICM.

3.13 Procedure: Taking a node out of service

The following provides the proper procedure to follow to take one of the CICM nodes out of service. This procedure aims to provide the operator with the best method of removing a node from the CICM chassis with the least possible impact on service.

Warning: *Although this procedure aims to minimise the impact on service, it does not eliminate it. It is strongly recommended that such maintenance procedures only be executed during low activity periods.*

3.13.1 Step 1: Perform a SWACT

If the node that is to be taken out of service is currently the master, a switch of activity should be executed. This can be initiated from the Element Manager's maintenance page using the "switch activity" link. Upon clicking the link, the operator is presented with a warning message and asked to confirm the action.

Once the SWACT is initiated, the operator must wait for the switch of activity to complete. As the Terminals component must recover all terminals, the SWACT takes a while to complete. Transient states are displayed during the switch and the operator should not proceed to the next step until the switch of activity has fully completed.

A SWACT is complete only once the "Status" field of each node on the maintenance page shows "master" on the node to be kept in service and "slave" on the node that is intended to be taken out of service for the maintenance.

3.13.2 Step 2: Stopping the slave node

Once the switch of activity (if needed) is completed, a stop of the slave node can be initiated. No further special actions are needed as the node should no

longer be supporting traffic at this point. The "node N service control" function on the maintenance page can be used to stop the slave node.

3.13.3 Step 3: Perform desired maintenance

Once the node has stopped, it is safe to proceed with removing the CPU blade, etc.

3.14 Event Monitoring

3.14.1 Logs

As introduced in SN07, the IEMS logging system continues to be used as high level log unification platform. The CICM reports only its most significant logs to it.

Although the Active Call Failover activity introduces no new logs destined for the IEMS, a number of logs pertaining to platform (or node) level redundancy were introduced as part of the activity addressed by reference [3]. Please refer to that document for further details.

The CICM's own local logging system continues to operate in parallel and is used to capture additional and more detailed information about local events.

These local system logs continue to be generated following existing practices. The three existing severity levels of logs are:

- 1** Error: serious and often unrecoverable events
- 2** Warning: unexpected, but recoverable events
- 3** Information: expected but significant events

As has been suggested throughout this document, it makes sense to differentiate between a node's status and the state of the individual components running on that node. Please refer to section for details.

The concept of a node's status (master vs. slave) was introduced in SN06.2 with the Dual Node Redundancy functionality. At the time, a number of logs were introduced to mark significant platform level events from a redundancy perspective.

The Active Call Failover activity does not introduce any new platform level redundancy logs. As such, please see reference [1] to review these logs.

This activity does however introduce a number of local logs to clearly identify significant events that occur to the individual components of the system.

Information logs are generated by both the VMG and Terminals components for the following normal start-up events:

- On master: Component initialises as the active component
- On slave: Component initialises as the inactive component
- On master: Slave component requests a bulk sync
- On slave: Bulk sync of data completes; Ready for SWACT

A number of information logs are generated by each component as it performs an operator-initiated switch of activity:

- On master: Component receives notification to SWACT
- On slave: Component receives request from its counterpart to assume the role of the master
- On slave: Component completes transition to active
- On master: Component receives acknowledgement from mate that it is now active; completes transition to inactive

3.14.2 SNMP

This feature introduces no new SNMP nodes or traps. Therefore, the original behaviour of the Dual Node Redundancy feature (see reference [1]) combined with the changes made in SN07 (see reference [3]) remain valid.

However, for a CICM installation that does not make use of the IEMS to monitor SNMP, a subtle clarification is of value. Some slight changes have been introduced to the Element Manager's status page with this feature. The "virtual media gateways" section of the page no longer displays its states as:

- In Service
- Out of Service
- Hot Standby
- Stopped

Instead, it now splits the active vs. inactive state of the component from the overall VMG state to make things clearer and more explicit. On the maintenance page, the "VMG status" combines this information into a summary and now reports either:

- active (in service)
- active (out of service)
- inactive (in sync)

- inactive (out of sync)
- swacting master→slave
- swacting slave→master
- stopped

As originally implemented in SN06.2 and described in [1], the *cicmVLCMUnit0State* and *cicmVLCMUnit1State* nodes are located in the MIB hierarchy under:

...|cicm|cicmVLCM|cicmVLCMTable|cicmVLCMTableEntry

and are used to reflect the status of the VMG. These SNMP nodes may have one of the following states:

- inService(0): VMG is in service as the active component
- stopped(1): VMG is not running
- outOfService(2): VMG is not in service
- hotStandby(3): VMG is in service as the inactive component

For backwards compatibility reasons and given that the non-IEMS SNMP system is likely to be phased out over time, instead of changing the SNMP nodes as such, a simple mapping to the new status names is offered in the following table.

Table 1: VMG Status to SNMP Mapping

	VMG status as displayed on EM status page	SNMP status reported
master	active (in service)	inService(0)
	active (out of service)	outOfService(2)
	stopped	stopped(1)
Slave	inactive (in sync)	hotStandby(3)
	inactive (out of sync)	outOfService(2)
	Stopped	stopped(1)

3.15 Alarms

This feature introduces no changes to the alarm system. As a result, the original behaviour introduced with the Dual Node Redundancy feature discussed in reference [1] and subsequent changes made in SN07 as described in reference [3] remain valid.

3.16 Limitations and Restrictions

This section aims to summarise the limitations and restrictions of the Active Call Failover functionality. Many points will have already been discussed in previous sections.

- 1 During the switch of activity of the VMG component, only stable calls are guaranteed to survive. Unstable calls may or may not survive. The definition of stable versus unstable calls was discussed earlier.
- 2 It is not permitted to stop or restart the master node. To do so, the operator must first initiate a SWACT, wait for it to complete and stop or restart the now slave node. The element manager does however provide errors or warnings as appropriate if such and unsupported maintenance action is attempted.
- 3 Once initiated, a SWACT cannot be cancelled despite its possibly long duration. To return the system to its original pre-SWACT state, a second SWACT must be carried out once the first one completes.
- 4 The only supported upgrade path to 8.10 is from 7.20 for both the CICM and EM. The 8.10 Element Manager may be used to manage 2.5, SN06.2, SN07 and SN08 CICMs.
- 5 With 8.10, the CICM ceases to support a load-sharing mode. This feature's goal is to shift the role of the secondary node from providing a load-sharing capability to providing full failover redundancy.
- 6 Because of the amount of processing work involved in the terminal recovery process, some real-time impact on call processing may arise during a SWACT.
- 7 The terminal recovery process on a SWACT may be long (as discussed earlier).
- 8 The terminal recovery process does not currently prioritise terminals in active calls over idle terminals. The recovery process aims to recover all terminals sequentially and without prejudice. However, the recovery process does give immediate priority to a terminal that experiences an incoming event (either user interaction or from the GWC).
- 9 In the rare case that the new master node should experience an outage while a switch of activity is in progress, it cannot be guaranteed that all terminals will be recovered. Some terminals may timeout, reboot and any calls active at that time would be lost.

3.17 Feature Impacts and Interactions

Active Call Failover impacts some existing functionality of the CICM and results in a few changes to the overall system:

- 1 The terminal transfer functionality is no longer relevant on an 8.10 CICM as the system now manages terminal recovery (or hand-over) automatically on a switch of activity. The option is therefore not available when managing an 8.10 CICM (or later) with the Element Manager.
- 2 Prior to ACF, each terminal typically would have its S1 IP address pointed to one node of the CICM with S2 directed to the other node as a back-up. Given that the south-side of the CICM now only provides a single IP address to which clients can connect, the S2 IP entry has been made redundant from the CICM's perspective. The entry is now free to be used for other purposes such as directing it to a local SRG for a local back-up system. As always, S1 and S2 can be configured manually or via DHCP. The configuration details of the terminals falls outside the scope of this document.

3.18 References

- [1][H.248 Dual Node Redundancy - FN](#) (A00002715, SN06.2); Paul Richard
- [2]CICM 7.1 Initial Installation and Commissioning (24-0479, SN07); Jeff Cole
- [3][Alarms Logs and Performance - FN](#) (A00003718, SN07); Martyn Hollins; Karen Davies
- [4]Series 8.0 Centrex IP Client Manager Product Specification; Paul Richard

4: A00004741 Functional description (FN)

4.1 Feature name

Enabling TRKGRP OM ON GEM and Support Nodal OMS

4.2 Description

This feature provides Nodal Based Operational Measurements for MG4K-IP and IW-IP nodes. These nodal statistics are necessary for Link Bandwidth Engineering and to determine the network usage and transmission errors.

The Nodal Based Operational Measurements includes the statistics for:

- Gigabit Ethernet Link usage
- Bearer traffic injected into the network.

To support above statistics two new Nodal Based OM groups are added by this activity:

- MNGEMLNK

This OM group has pegs for:

- The number of packets/octets transmitted/received on the Gigabit Ethernet Link connected to a MG4K-IP/IW-IP node.
- The number of packets/octets transmitted/received with different types of error.

- MNGEMTRF

This OM group has pegs for:

- The number of RTP packets/octets transmitted/received for bearer traffic.
- The number of packets/octets transmitted/received for different types of call.

4.3 Hardware Requirements or Dependencies

None

4.4 Software Requirements or Dependencies

This functionality requires SN08 load in the Call Server, MG4K-IP CEM and GEM RM.

4.5 Limitations and restrictions

- The OM peg counts stored in the MG4K-IP and IW-IP that have not been reported to the Call Server will not be maintained over MG4K-IP/IW-IP GEM Sparing and Restarts.
- The OM pegging for Voice Band Data connection shall be implemented in later release.

4.6 Interactions

None.

4.7 Glossary

Term	Description
CEM	Common Equipment Module
GEM	Gigabit Ethernet Module
IW Node	Interworking Node
MG4K-IP	Multi-Service Gateway 4000-Internet Protocol.
OM	Operational Measurement
RM	Resource Module

5: A00005561 Functional description (FN)

5.1 Feature name

MG9K Internet Protocol Security

5.2 Description

This feature implements IP security and user authentication capabilities on the MG9K. There are two broad goals, first is to ensure that all users, local and remote, are validated before access is granted to a MG9K node. Secondly, all IP traffic between the MG9K and a remote peer (Element Manager or Gateway Controller) will be authenticated. These goals will be accomplished by authenticating user through a RADIUS client/server network. IP traffic will be protected with IP Security suites. As a result of this feature all peers connecting to the MG9K will also need to enable IP Security unless an explicit bypass policy is in place. Notably, the Element Manager and the Gateway Controller are affected and are the only devices that currently have to implement IPsec. Other devices that access the MG9K will do so with other secure protocols such as SSL, or SFT. See the following figure. The MG9K Security parameters can be configured from the LCI at initial commissioning or from the Element Manager.

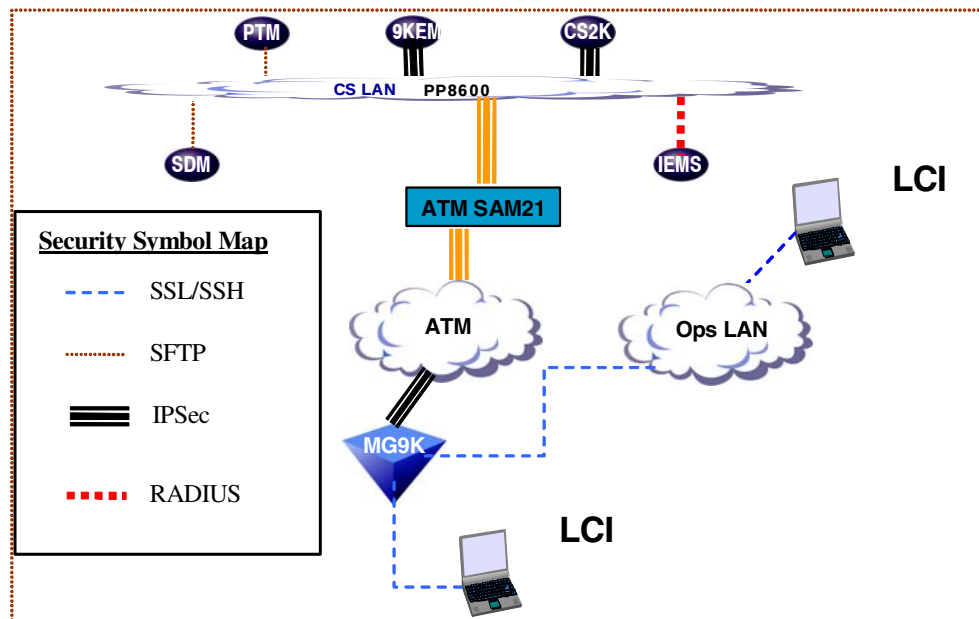


Figure 1 IP Security Network

The security features are enabled when the MG9K node is commissioned via the Local Craft Interface (LCI). One of the first steps is to configure the shared

keys between the MG9K and its Element Manager and the key shared with GWC if known. Shared keys are protected in three ways by the MG9K. The key, of size TBD, is protected from being displayed on the LCI and EM. The same key has to be entered twice before it is accepted by the GUI, and it is stored in an encrypted format. The key is also never transmitted insecurely over the network.

The Local Craft Interface and the Element Manager are used to enable and configure MG9K security features. Configuration is done on a per-network element basis. There is no flow thru of the security options. Therefore careful coordination is required when security is enabled on codependent devices.

Below are sample LCI Security configuration screen shots. The Element Manager interfaces will be discussed in a separate document.

5.2.1 RADIUS Configuration

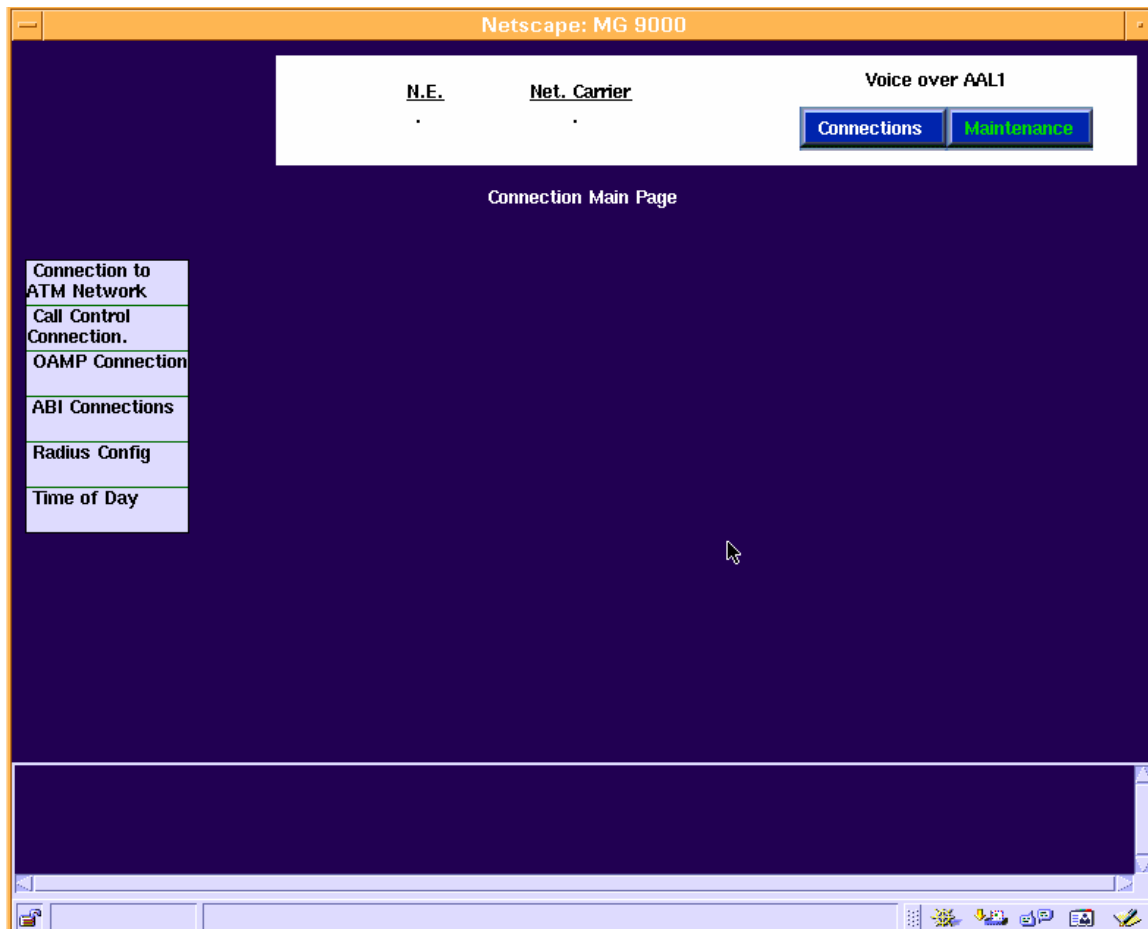


Figure 2 RADIUS Configuration

Netscape: MG 9000

N.E. Net. Carrier Voice over AAL1

• •

Connections Maintenance

RADIUS Configuration

Primary IEMS Address

Secondary IEMS Address

Primary IEMS Shared Key

Secondary IEMS Shared Key

Submit Query

Figure 3 RADIUS Parameter set

5.2.2 IP Security Configuration

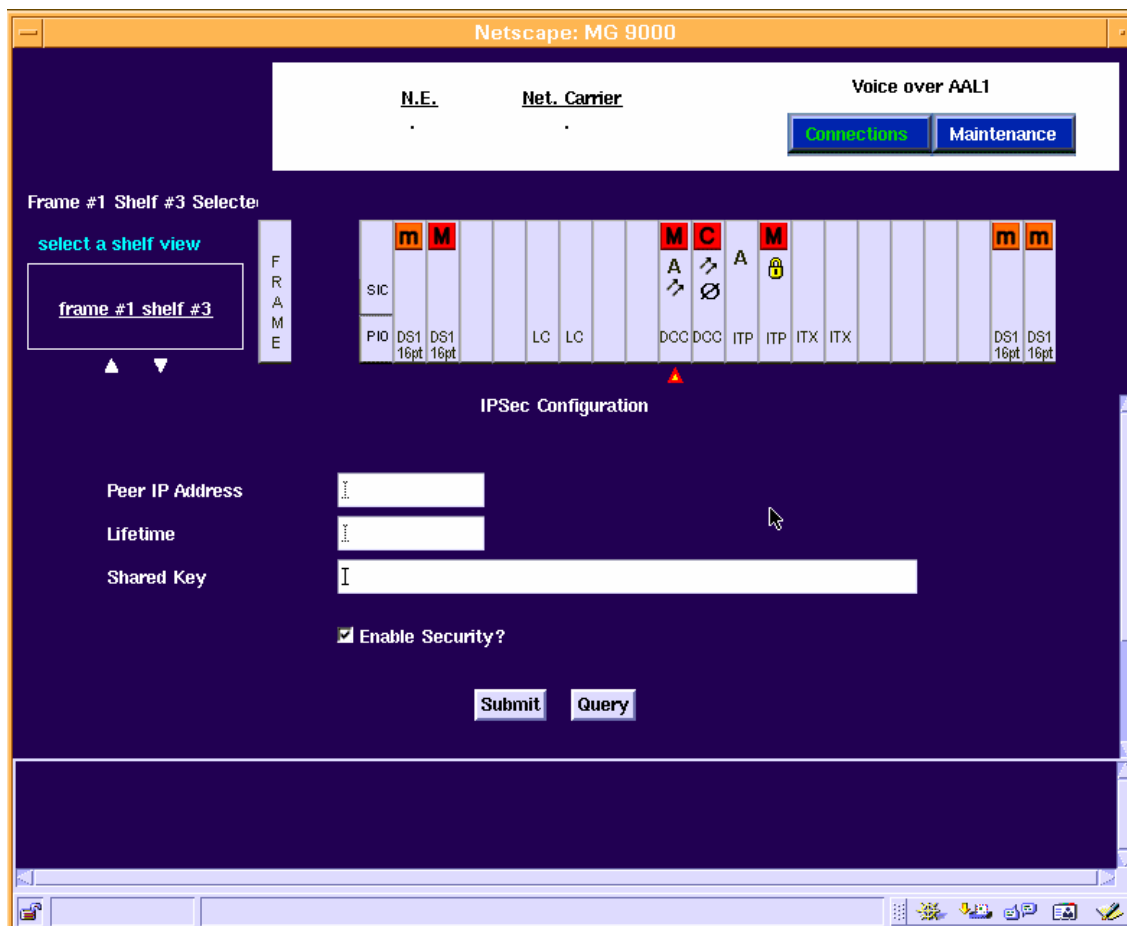


Figure 4 IP Security Parameter set

Table 1 Configuration Summary

	Action	Description	Expected Results
1	Craft person logs on to MG9K Node with default Admin password		User authenticated locally on MG9K. (No access to RADIUS server). Access permitted if password is correct.

2	Set Security parameters	1 Enable Security 2 Set Element Manager's Pre-shared Key 3 Set IP addresses of RADIUS Servers 4 Set GWC Preshared Key if known 5 Change Default Admin password if desired.	
3	Continue normal MG9K commissioning		When the WAN interface becomes operational, links to the EM and GWC will be secured with IPSec. (Secure link establishment continues until success) MG9K sends a cold start trap to trigger EM discover.
4	VMG Provisioning		EM to set GWC-GW pre-shared key

5.2.3 Alarms, Logs, and Statistics

5.2.3.1 Security Alarms (displayed at the EM and the LCI)

- Non-responsive RADIUS Server
- Expired Links to Security Peers
- Replayed Packet threshold
- Packet Discard threshold

5.2.3.2 Security events logs (accessible at the EM)

- IKE negotiation errors
 - Key mismatch
 - Proposal errors
 - Time out
- IP packet authentication failures
- Packet discard
- Replayed packets

5.2.3.3 Security statistics

Number of Packets

- Transmitted
- Received
- Discarded

5.3 2.3 Applicable customer facing sections

Fault Management:

Not Applicable _____

Logs _____X_____

Alarms _____X_____

Configuration:

Not Applicable _____

Data Schema/MIBs _____X_____

User Interface _____

GUI _____

Element Management _____X_____

Local Craft Interface _____X_____

Security _____X_____

Service Order _____X_____

SOC _____

Office Parameters _____

Upgrades impact _____X_____

Accounting _____

Not Applicable _____

Billing changes _____

Performance _____

Not Applicable _____

Operational Measurements _____

Performance Measurements X

5.4 Hardware Requirements or Dependencies

None

5.5 Software Requirements or Dependencies

IP Security on the MG9K runs in concert with security enabled on the Element Manager and GWC.

5.6 Limitations and restrictions

None

5.7 Interactions

None

5.8 Glossary

Term	Description
New term	Definition

6: A00005562 Functional description (FN)

6.1 Feature name

MG9000 ITP/ABI Overload Controls

6.2 Description

The Access Bridging Interface (ABI) card provides the functionality to support legacy XPM hardware on an MG9K node. The ABI cards are configured in pairs to provide a dual network plane that converts between DS30 speech and maintenance channels on the XPM to a packet format used on the MG9K and in the Succession network. The active ABI card must also process H.248 Megaco messaging from the Gateway Controller (GWC) to perform the actions required for call processing. In addition the active ABI and inactive ABI must maintain datasync.

Although a subtended XPM has its own built in overload controls, it is possible for the active ABI to exceed its real-time CPU capacity before the XPM reaches its overload threshold. Overload controls will be put in place on every ABI pair to stabilize the system and reduce real-time usage in the event of excessive call processing demands. When a sustained call processing demand placed on an ABI card exceeds the rated capacity for the system, selective work shedding may take place to offload work from the active ABI CPU.

The Internet Telephony Processor (ITP) card doesn't have as high a pside channel concentration as the ABI, but it is responsible for processing requests on its own line agents that require work for tone generation, digit collection, and ringing. It must also handle and send H.248 Megaco messaging.

The desired system output for both ABI and ITP cards is to maintain a minimum required level of processed work, even as the offered load exceeds the rated capacity. Rated capacity is based on customer call model requirements and the number of channels available to serve the demand. The feature implementation comprises two main categories, the monitoring for overload conditions, and the work shedding taking place when an overload state is present.

Feature work in SN06.2 under CAF A00002105 implemented Overload Controls on the Supercore DCC card. The framework developed for the SN06.2 feature will be reused extensively in this feature.

6.2.1 Overload Resource Monitor

A set of critical datapoints are defined as overload resources for the MG9K. Common resources include CPU usage, application specific messaging rates,

queue utilization, etc. These individual overload resources are monitored against predefined enter and exit thresholds, and provide benchmarks for system capacity and performance. An SNMP alarm notification is displayed at the MG9K Element Manager when an overload resource exceeds its threshold, and is cleared when the exit threshold is reached. An overload resource threshold crossing is not a direct indication of system overload, but does provide an indication of high resource utilization.

Operational measurements are collected every fifteen minutes for each of the defined overload resources. These datapoints provide engineering benchmarks for the throughput of the gateway. These operation measurements are retrievable through either the MG9K Element Manager Performance Browser or the OM collector.

For the ITP and ABI cards the resources that will be monitored are CPU utilization, SLOA call connection messaging rates, messaging queue delays for the SLOA connection task, and AAL5 PDU messaging rates.

6.2.2 Overload State Detector

The SLOA messaging queue delay overload resource will be used as the key indicator of call processing throughput on the DCC card. There is a finite time limit for processing a connection request. When the time limit is exceeded, other messaging subsystems on the ITP or ABI and the gateway controller will time out, and the connection attempt will fail. A system overload detector will use periodic averaged queue delay samples to determine the incoming work backup on the connection broker task. Once the incoming connection request work load becomes large enough to force the queue delay measurement to exceed its engineered limit to process the message and successfully setup the speech path connection, an overload alarm is raised to the MG9K element manager, and a work shedding process is activated. The magnitude of the connection broker queue delay measurement determines the throttling rate used to deny calls.

To exit overload the connection queue delay must fall below a predetermined safe level that indicates normal connection processing can resume.

An SNMP alarm system overload notification is sent to the MG9K Element Manager when system overload is declared or cleared.

6.2.3 Work Shedding

Once activated, the work shedding process will selectively deny call processing connection requests based on discard percentage rates determined by the overload detector. The connection denial is selective because it uses emergency call indication flags included in Megaco add termination requests that permit emergency calls to complete during an overload condition. Emergency call marking is provided in SN06.2 feature A00002322.

Any connection request denied by overload controls will have a response message sent to the GWC indicating the reason for denial is MG9K overload.

A LINE 162 log is generated on the XA-Core for every denied call indicating overload condition.

A counter tracking the number of connection denials on the MG9K due to overload is accessible by the MG9K EM. An associated OM will also be pegged on the XA-Core. Work shedding continues until deactivated by the overload detector when it clears the overload state.

6.2.4 Alarms and OMs

Whenever an overload resource crosses its threshold, notifications are sent to the MG9K EM. When an overload condition is declared, an alarm is raised to the MG9K EM. Alarms will be raised for any overload resource threshold crossing event with a warning severity. An actual overload alarm will be raised with a critical severity.

Boundary values for each of the overload resource enter and exit thresholds are determined using system modeling results and actual lab testing under overload scenarios. The MG9K EM provides an interface to change these threshold settings in case a customer site has unique requirements.

Each of the defined overload resources will have operational measurements recorded in 96 fifteen minute intervals. OMs are also defined to track the number of denied calls while in overload. The defined OMs listed below are captured on a per card basis.

6.2.4.1 CPU Utilization

CPU utilization is reported as the percentage of available CPU cycles that are in use. It is reported as an integer but contains two decimal places. A value of 5512 is a measurement of 55.12%.

6.2.4.2 SLOA Call Connection Messaging Rate

Specific intercard connection broker messages are required to establish the voice over packet transmission path. The messaging rate for these specific messages provide a measure of the offered connection attempt load on the card. Values are reported as an integer but contain two decimal places with the units messages per second. A value of 345 is a measurement of 3.45 messages/second.

6.2.4.3 SLOA Call Connection Queue Delay

The connection broker messages defined in 2.2.4.2 must all be processed off a task specific queue. The time spent waiting on the queue to be processed is a measure of the call processing load for the card. Values are reported as an integer but contain two decimal places with the units of milliseconds. A value of 10000 is a measurement of 100 milliseconds.

6.2.4.4 AAL5 PDU Messaging Rate

All incoming IP messaging is converted from ATM AAL5 Protocol Data Units (PDU) to IP. Hardware pegs to track the number of AAL5 PDUs provide a measure of the messaging load on the card. The AAL5 PDU message rate is reported with the units messages/second.

6.2.4.5 Overload Deny Counter

A separate counter of the total number of connection denials due to overload conditions will be maintained. It is maintained on a per card basis. The reported value is zero if an overload state did not exist for the specified interval.

6.3 Hardware Requirements or Dependencies

N/A

6.4 Software Requirements or Dependencies

N/A

6.5 Limitations and Restrictions

ActId A00005646 provides the element manager functionality to include the ITP and ABI in the overload controls framework. It includes work for updating threshold settings, collecting OMs, and displaying alarms. The work is an extension of SN06.2 DCC overload controls actid A00002007.

6.5.1 MG9K Manager

The MG9000 Element Manager Overload Controls work is required to provide the necessary OAM&P support for MG9000 Overload Controls. This includes real-time access to critical performance engineering measurements, overload thresholds provisioning, and processing of threshold crossing faults.

- MG 9000 Overload Faults - Faults will be raised and cleared from the MG 9000 when overload thresholds are crossed. The Overload faults will be displayed on the MG 9000 Manager Alarm Browsers, logged to the MG 9000 Manager CUST logs and forwarded to northbound OSS.
- MG 9000 Overload Performance OMs - OMs associated with MG 9000 Manager Overload controls will be made available by the MG 9000. These OMs will be collected and displayed in the MG 9000 Manager Performance Browser. The OMs will also be collected by the Performance Collector Formatter for OSS retrieval.
- MG 9000 Overload Threshold Provisioning - Several Overload thresholds for raising and clearing alarms will be supported by the MG 9000. Viewing and provisioning of these thresholds will be made available from the MG 9000 Mgr Graphical User Interface.

6.6 Applicable customer facing sections

Fault Management

Logs ☐ N/A ☐

Alarms ☒ X ☐

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) ☐ N/A ☐

Performance (includes operational measurements) ☒ X ☐

6.7 Glossary

Term	Description
GWC	Gateway Controller
CB	Connection Broker
MG9K	Media Gateway 9000
DCC	Data Control Card
OM	Operational Measurement

6.8 References

TR-NWT-001358, "Switching System Overload Control Generic Requirements", November 1993

7: A00005646 Functional description (FN)

7.1 Feature name

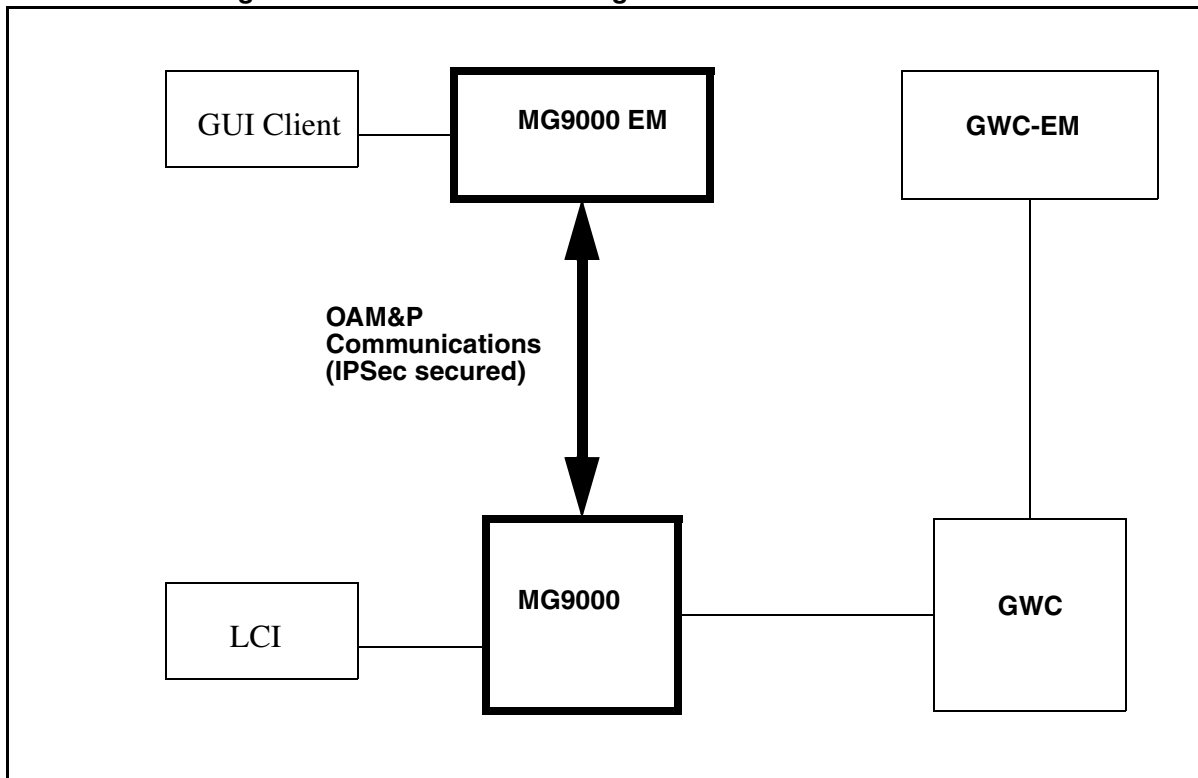
IPSec with MG 9000 Element Manager

7.2 Description

This feature implements IPSec for MG9000 Element Manager to MG9000 Line Gateway OAMP communications. The craftsman will be able to independently manage IPSec parameters for all OAM&P communications to and from MG9000 network elements. This feature will enable/disable/modify IPSec on the OAM&P messaging channel from the MG9000 EM to an MG9000. Encryption (Confidentiality) may not be enabled in this release as it is not supported by the MG9000 Line Gateway.

The MG9K Element Manager will be used to manage IPSec security associations on the server-side portion of the OAM&P communications. The MG9000's LCI will be used to manage IPSec security associations on the gateway-side of the OAM&P communications. See Figure 1.

Figure 1 Desired Behavior Diagram



For securing the OAM&P communications channel on the MG9000EM, a new **Security View** will be made available from the MG9000 EM subnet. This GUI

will manage the IPsec (and Internet Key Exchange) configuration file(s) that are present in the SSPFS common platform. Parameters in these files are used to setup security associations, keys, and protection mechanisms. Enforcement of IPsec policies will be system-wide and per-socket as provided by the Solaris IPsec implementation. The craftsperson will not be limited to securing the EM to GW connection, but will be able to manage all network connectivity in and out of the MG9000 Element Manager Server.

Also the **Office Wide Defaults View** is changed to support IPsec. This will enable the customer to configure one set of IPsec parameters and have them applied to all, or a subset of, the provisioned MG9000s.

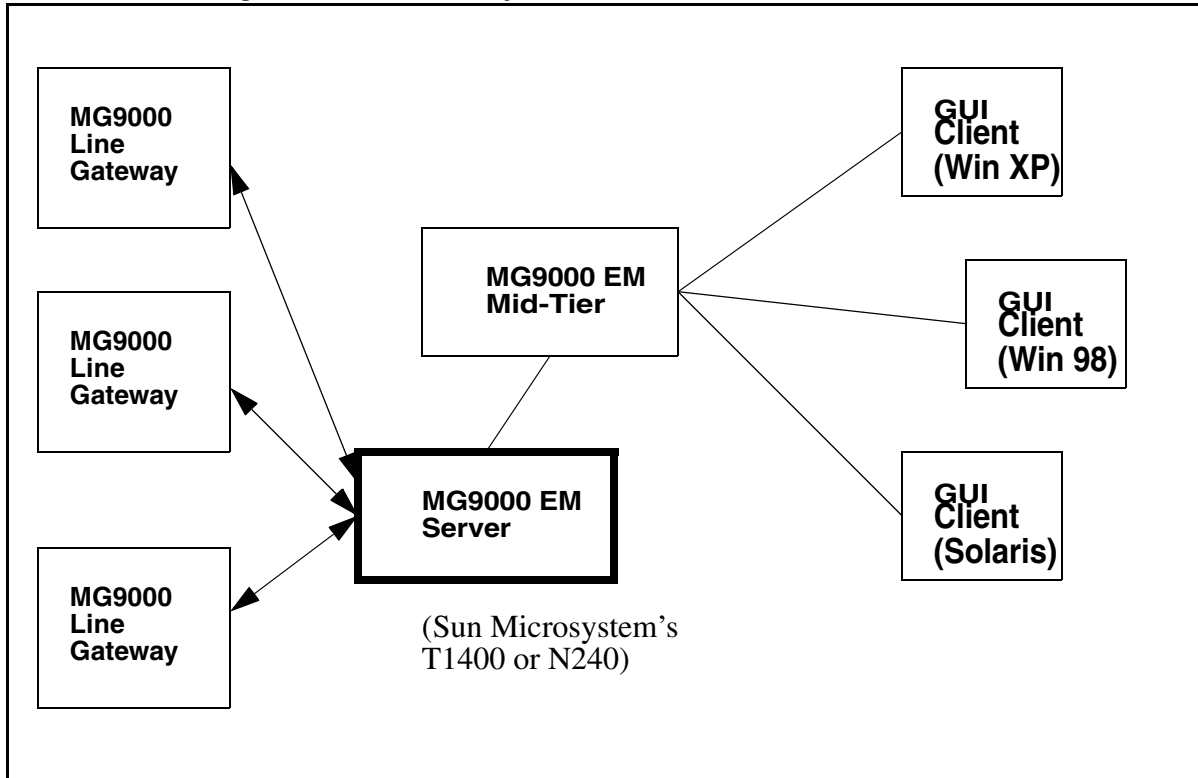
This feature does not affect security on the MG9000 Element Manager Mid-Tier or client machines. All security views in the MG9000EM will only be accessible from EMSADM login class.

For proper operation of IPsec, all security parameters provisioned for an MG9000 Network Element in the Element Manager **MUST** also be provisioned in the corresponding MG9000 Line Gateway. **IF THE PARAMETERS DO NOT MATCH, COMMUNICATIONS BETWEEN THE GATEWAY AND ELEMENT MANAGER WILL NOT BE POSSIBLE.**

7.3 Hardware Requirements or Dependencies

No new hardware is being introduced by this feature. Existing Sun Microsystems T1400 and N240 hardware used as MG9000 EM server platform will be used.

Figure 2 Hardware Layout



7.4 Software Requirements or Dependencies

SN008 release or later of the MG9000EM application will support IPsec.

Software loads in the MG9000 Line Gateway will be SN008 release or later.

7.5 Limitations and restrictions

7.5.1 Security

For proper operation of IPsec, all security parameters provisioned for an MG9000 Network Element in the Element Manager **MUST** also be provisioned in the corresponding MG9000 Line Gateway. **IF THE PARAMETERS DO NOT MATCH, COMMUNICATIONS BETWEEN THE GATEWAY AND ELEMENT MANAGER WILL NOT BE POSSIBLE.**

7.5.2 IPsec Precedence Order

If the IPsec configuration contains multiple policy entries, for example, they are assumed to be listed in the order in which they are to be applied. In cases of multiple entries matching the outbound and inbound datagram, the first

match will be taken. The system will reorder the policy entry, that is, add the new entry before the old entry, only when:

- The level of protection is "stronger" than the old level of protection. Currently, strength is defined as:

AH and ESP > ESP > AH

Entries with both AH and ESP present in the policy entry protection are ordered after all the entries with AH and ESP and before any AH-only and ESP-only entries.

- If the new entry has bypass as action, bypass has the highest precedence. It can be added in any order, and the system will still match all the bypass entries before matching any other entries.

In all other cases the order specified by the user is not modified, that is, 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.

7.5.3 IP Addresses

No IPv6 128 bit format IP addresses will be supported, only IPv4 (xxx.xxx.xxx.xxx) format 32 bit addresses will be supported.

7.6 Interactions

No interactions between IPSec and existing features will be seen by the craftsperson.

7.7 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__

7.8 Glossary

Term	Description
GWC	Gateway Controller
GUI	Graphical User Interface
IPSec	IP Security

8: A00005932 Functional description (FN)

8.1 Feature name

Removing Loopback Trunks in CEPT DISA calls for Remote Feature Activation

8.2 Description

8.2.1 Introduction

This feature enhances the digit collection in DISA features which are CEPT Call Forwarding Remote Access (CFRA) and CEPT Remote Access (CEPTRA). In existing functionality, digit collection is performed via loopback CAS trunks for all originating agents although they have capability to use UTR; that means, following kinds of originating agents below, loopback trunk is inserted between the agent and DISA feature by default:

- ISDN BRI lines
- ETSI ISUP trunks
- ETSI PRI trunks

This feature changes this behaviour, and provides flexibility in digit collection as in following hierarchical order.

- 3 collect digits via UTR if possible
- 4 collect digits via DTMF receiver (for PRI agents only)
- 5 collect digits via LOOPBACK trunk

This feature provides the possibility not to use superfluous loopback equipment and optimize the digit collection for mentioned agents on CEPT markets; when the user of CFRA/CEPTRA feature will need to send digits for remote call activation, UTR or DTMF receivers (on MTMs) will be used for it. If both of them are not available, loopback trunk will be inserted as in existing functionality.

Note: Throughout this document, “originating agent” refers to the originating agent of the call in the switch where DISA feature is located on.

8.2.2 General Considerations

This feature is applicable for only CEPT features related with DISA framework, and provides the algorithm as explained below.

- a. Firstly, digit collection via UTR is tried to perform if it's already available.

- b. Secondly, if UTR is not available for originating agent, digit collection via DTMF receiver on MTMs is tried to perform. (for PRI agents only)
- c. Thirdly, if both of them are not available, digit collection is performed via LOOPBACK trunks.

The following table illustrates the originating agents versus supported digit collection types.

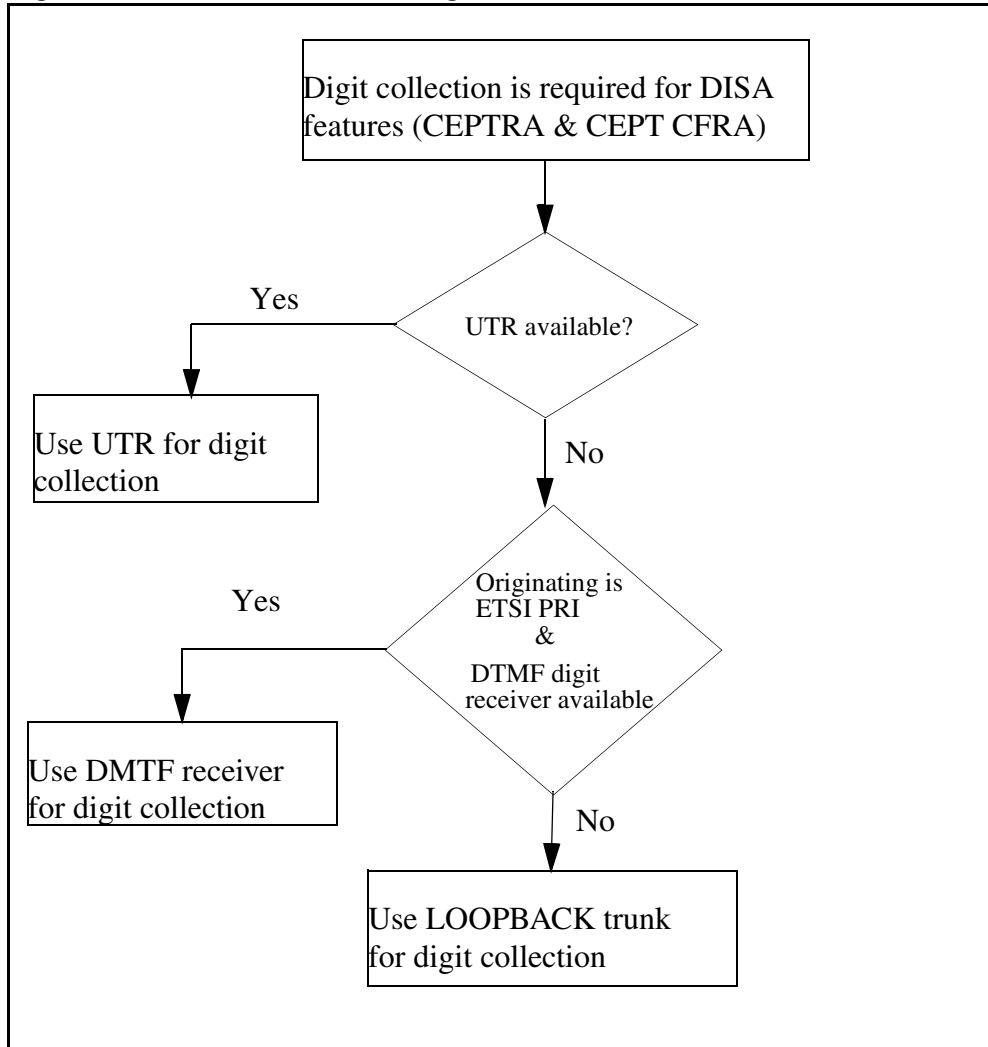
Table 1 Supported digit collection types versus originating agents

Originating Agents	Digit collection type		
	via UTR	via DTMF digit receiver	via LOOPBACK trunks
ETSI ISUP	X		X
ETSI PRI	X	X	X
R1 (NTLS01, 02, 09), R2 (Base)	X		
ETSI BRI lines	X		X
IBN/EBS lines	X		

X abbreviates this type of digit collection is supported on that agent.

As seen from Table 1, Digit collection via DTMF digit receiver cards is supported for only ETSI PRI trunks on which digit collection can be performed by UTR or Loopback trunks also.

Algorithm of choosing of which digit collection type used is simple. UTR has the first priority, DTMF digit receiver has the second, whereas loopback trunk has the last priority. The functional behavior diagram is as shown below.

Figure 1 Functional Behavior Diagram

8.3 Hardware Requirements or Dependencies

The RCVRDGT pool will be used as DTMF digit receiver in this activity, and digit receiver cards (2X48xx, where xx refers to "AB, BA, CC") should be located in MTMs.

Table RECEIVER should be provisioned as illustrated in Figure 2 below for using DTMF digit receiver in DISA calls. In order to be in service, each RCVRDGT must be taken in service by "**bsy;rts**" using the "**mapci;mtc;trks;ttp**" level.

Figure 2 DTMF digit receiver provisioning

TABLE: RECEIVER

>lis all

TOP

	RCVRKEY	RCVRTYPE	TMTYPE	TMNO	TMCKTNO
CARDCODE					

RCVRDGT	0	D	MTM	0	6	2X48CC
RCVRDGT	1	D	MTM	0	7	2X48CC

8.4 Software Requirements or Dependencies

N/A

8.5 Limitations and restrictions

In case of originating agent is ETSI PRI agent, Dial Tone is applied to the subscriber instead of SDT where it requires.

8.6 Interactions

N/A

8.7 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)

8.8 Glossary

Term	Description
BRI	Basic Rate Interface
CAS	Channel Associated Signaling
CEPT	Counsel for European Postal and Telecommunications
DISA	Direct Inward System Access
DTMF	Dual-Tone Multifrequency
DTM	Digital Trunk Module
EBS	Electronic Business Set
ETSI	European Telecommunications Standards Institute
IBN	International Business Network
ISDN	Integrated Services Digital Network
MTM	Maintenance Trunk Module
SDT	Special Dial Tone
UTR	Universal Tone Receiver

9: A00005991 Functional description (FN)

9.1 Feature name

Enable IPSec on all GWC Profiles

9.2 Description

This feature adds the IPSec capability to the following GWC profiles:

- LARGE_LINENA
- LARGE_LINEINTL
- SIP-T
- SIP-TINTL
- V52TRUNK
- VRDN
- VRDNINTL
- BICC
- H.323_NA
- H.323_INTL

The code changes to add the IPSec capability to the listed profiles were completed in SN07. However, the IPSec GUI was left disabled for the modified GWC profiles in SN07.

The SESM “configure” script must be used in the SN08 release to completely enable IPSec for all GWC profiles.

9.2.1 Configure script usage

A hidden menu within the SESM “configure” tool is used to enable IPSec for all GWC profiles. The “configure” menu has the following options.

```
SESM configuration
1 - SESM common configuration (IP addresses, Market, CM CLI)
2 - SESM database tools
3 - SESM related applications configuration (MG9K, LMM, CICM)
4 - SESM provisioning configuration
5 - SESM logging configuration (syslog, sesm debug log)
6 - view sesm configuration settings
7 - SESM refresh properties

X - exit

select -
```

In order to access the hidden menu used to enable IPsec, enter “IPSEC” or “ipsec” at the “select” prompt of this menu level. The IPsec menu will then be displayed.

IPSec configuration

- 1 - Enable IPsec for all GWC profiles
- 2 - Restore IPsec settings to original configuration

X - exit

select -

At the “select” prompt, enter “1” to enable IPsec for all GWC profiles.

select - 1

IPSec is now enabled for all GWC profiles.

If the CS2M Management Tools GUI is running, it must be restarted for changes to be recognized by the GUI.

If, at any time, the IPsec settings need to be restored to the original configuration, enter “2” at the “select” prompt.

select - 2

IPSec settings have been restored to original configuration.

If the CS2M Management Tools GUI is running, it must be restarted for changes to be recognized by the GUI.

Note that after entering option 1 or option 2 to alter the IPsec configuration, any running CS2M Management Tools GUIs will need to be stopped and restarted to reflect the IPsec setting change. The SESM server **does not** have to be stopped after altering the IPsec configuration.

Enter “X” to exit the IPsec menu and return to the main “configure” menu.

9.3 Hardware Requirements or Dependencies

Not applicable.

9.4 Software Requirements or Dependencies

Not applicable.

9.5 Limitations and restrictions

IPsec for the modified GWC profiles is disabled until activated using the SESM “configure” script.

9.6 Interactions

Not applicable.

9.7 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_

9.8 Glossary

Term	Description
GWC	Gateway Controller
IPSec	IP Security
SESM	Succession Element & Sub-element Manager

10: A00006226 Functional description (FN)

10.1 Feature name

NTPOLL: Restructuring and Table Control

10.2 Description

This feature, “NTPOLL: Restructuring and Table Control” (A00006226), is scheduled for release in SN08.

10.2.1 NTPOLL Background

NTPOLL is an existing DMS feature which automatically polls various data from the switch and stores the results in data files on either SFDEV or NTDEV. NTDEV is a virtual type DMS disk similar to SFDEV but which has been set aside specifically for storage of the poll data files. Typically, NTDEV stores the results of the polling, although the option to use SFDEV exists.

The output of the polling is one or several poll data files named POLLDATA, POLLDATA1, POLLDATA2, POLLDATA3, etc. The maximum size of each file is limited (to approximately 30,000 lines), so when a poll data file reaches its maximum length, it is closed and a new file (named with the next number in the numbering scheme) is opened. A small switch might only output one POLLDATA file during a polling. However, large switches have been known to output as many as four or five POLLDATA files. Optionally, these poll data files may be compressed automatically. Compressed files are denoted by the letter “Z” (ex. POLLDATAZ, POLLDATA1Z, POLLDATA2Z, etc.).

The data polled and collected by the system is currently defined by the system. There are two types of poll steps done during the polling. A “table step” is simply the collection of data from a DMS table (either listings of tuples or a count of tuples in the table). A “complex step” involves the collection of various other types of data from the switch, for example software version, patch, SOC, DMSMON, memory, and other configuration information. In a full polling, there are currently over 440 total polling steps. Approximately 85% of the steps are table steps.

Two CI commands are used in the administration of polling:

- POLLSCHD - used for the weekly scheduling of pollings, defining polling parameters (ex. date and time of the polling, disk devices to use and whether to compress or not), and querying scheduled polls
- POLL - used to do an immediate poll, define the parameters thereof (ex. disk devices to use and whether to compress or not), or query certain information about the polling system.

Script file background

Because the polling steps are defined internally within the polling code, it can be expensive (i.e. requires a patch) to add a new desired polling step once a load is released. Special scripts have been designed, used, and maintained to supplement the base polling data. Special demarcations within the script files allow the polling code to recognize, run, and collect the output of these scripts as part of the regular polling when the script is placed on NTDEV

10.2.2 New Feature Functionality

The purpose of this feature is to allow the user the ability to modify the NTPOLL data collection template and address known software deficiencies. Currently, the poll steps performed during a polling are set in stone at initialization time and are not subject to changes, additions, or deletions of steps by the craftsperson. To enhance the NTPOLL polling system, the following will be implemented:

- Creation of a new table, NTPOLL, which contains a visual representation of the poll steps to be done during the next polling, as well as the ability modify, add, or delete poll steps at the users discretion via Table Control.
- Consolidate existing polling scripts into the NTPOLL tool.
- A series of smaller, internal fixes within the polling code to improve the robustness and security of the polling system.

NOTE 1: This feature is being done in conjunction with feature “NTDEV POLLING DEVICE and FTP ACCESSIBILITY FROM SDM” (A00006219). The two features are independent and can stand alone, but the ability to FTP to NTDEV (where poll files are stored) is an enhancement to the overall polling functionality.

NOTE 2: It is suggested that access to Table NTPOLL be privclassed so that only certain administrative users may change it.

10.2.2.1 Table NTPOLL

This feature adds a new table to the system, Table NTPOLL.

This table can be used to view or customize the poll steps that will be taken the next time a polling occurs (NOTE: the “pollsched qsched” command can be used to query when the next polling is scheduled for).

Assuming there are n polling steps, when a polling begins, it will start at tuple 0 (zero), in Table NTPOLL, execute that step, and proceed through tuple n-1 to complete the polling.

Table NTPOLL is automatically datafilled with the default polling template by the system upon initialization. It reflects the internal data structures which track all of the poll steps to be taken.

Because the polling steps will now be stored in a DMS table instead of just in internal data structures, any changes made by the user to the polling steps will be preserved over system restarts and upgrades (ONP).

The following shows sample portions of Table NTPOLL (NOTE: initially there may be more than 430 steps in the table). The table's keys are kept in order from 0 to n-1 (n=total # of poll steps), even if changes are made to the table (i.e. steps added or deleted).

The key contains the step number and an "insert bool". The insert bool is only necessary when a new step is being added between existing steps. For example, if a new step is being added as step 33, the current step 33 becomes step 34, 34 becomes 35, 35 becomes 36, and so on.

The next four bools determine whether or not that step is included in each of the four report types (LONG, SHORT, USAGE, and MEMCALC).

Finally, the step type and associated data are listed:

- CMPLX = complex step. A string name of the step is listed. A complex step involves a single or series of CI commands which are executed. Please see the explanation below of complex step fields for more information.
- TABLE = table step. The name of the table and the option whether to list out the table or count it is included. Please see the explanation below of table step fields for more information.

NTPOLLCI:

>list 50

TOP

NTPOLLKY

NTPDATA

```

-----
0 N      N Y N N CMPLX INT Display BCS Number
1 N      N Y N N CMPLX INT Display IMAGENAME
2 N      N Y N N CMPLX INT Display Log Message
3 N      N Y N N CMPLX INT CPID counts
4 N      N Y N N CMPLX INT PRSM List ACT Patches Turned On
5 N      N Y N N CMPLX INT PRSM List Act Patches
6 N      Y Y N N CMPLX INT PRSM INFORMLIST
7 N      Y N N N CMPLX INT PRSM INFORMSITE
8 N      Y N N N CMPLX INT PRSM INFORMLOAD
9 N      Y Y N Y CMPLX INT Dynamic Memory Size Information
10 N     Y Y N N CMPLX INT Display PM Loads
11 N     Y Y Y N CMPLX INT Display SOC Data
.
.
.
33 N     Y Y N N TABLE      OFCENG LIST ALL

```

34 N	Y Y N N TABLE	OFCOPT LIST ALL
35 N	Y Y N N TABLE	OFCSTD LIST ALL
36 N	Y Y N N TABLE	OFCVAR LIST ALL
37 N	N N N Y CMPLX INT	Display MEMCALC Office Parm
38 N	Y Y N Y TABLE	OFCAUT LIST ALL
39 N	Y Y N Y CMPLX INT	Gathering Table Counts Header
40 N	Y N N N TABLE	ACDAGENTS COUNT
41 N	Y Y N N TABLE	ACSCRN1 COUNT
42 N	Y Y N Y TABLE	ACSCRN2 COUNT

Table NTPOLL fields

Four types of tuples can be added to Table NTPOLL:

- Table step (COUNT) - counts the number of tuples in the table.
- Table step (LIST) - lists tuples in the table. There are several list options. Typically, a table step is simply to LIST ALL tuples in the table. However, options exist also to list the first or last n tuples in the table (ex. LIST FIRST 20 or LIST LAST 200).
- Complex step (INT) - an “internal” complex step. These are added to the table by the system and are not modifiable by the user (although they may be deleted). These complex steps execute a procedure internal to the code.
- Complex step (EXT) - an “external” complex step. These are defined by the user. the DMS command interface will attempt to execute, as a CI command, whatever string the user enters in the tuple.

The following fields are common to every tuple in Table NTPOLL:

NTPOLLKY - The key for Table NTPOLL. It is a two-part key:

- STEPNUM - The step number. The system will keep these numbered from 0 to n-1 (n = the total number of steps) whenever tuples are added or deleted.
- INSERT - This is a bool which is only used when a tuple is being inserted between two existing tuples. It should be set to ‘Y’ in that case, and ‘N’ any other time.

LONG - A bool which tells the system if this step is part of a long format polling report.

SHORT - A bool which tells the system if this step is part of a short format polling report.

USAGE - A bool which tells the system if this step is part of a usage format polling report.

MEMCALC - A bool which tells the system if this step is part of a memcalc format polling report.

STPTYP - The step type, either table or complex: {TABLE, CMPLX}

The following fields appear in the table based on the step type (STPTYP):

- **Table step fields**

TABNAME - The string name of the table

TSOPER - Table step operation - either list or count: {COUNT, LIST}

LISTOP - a LIST operation: {ALL, FIRST, LAST}

HOWMANY - If LISTOP is FIRST or LAST, this field will be prompted for and the number of tuples to be listed should be entered in this field

- **Complex step fields**

CMPLXTYP - An “internal” (code-defined) or “external” (user-defined) complex step: {INT, EXT}

CMPLXNAME - The string name of the complex step. For an internal complex step, this is just a name and the actual internal procedure which gets run is stored in internal data structures. For an external complex step, this string is actually run as if it was a CI command entered by the user.

NOTES on external complex steps: The maximum length string the user can enter is 40 characters. Also, because table control prompting only accepts everything up to the first space, the underscore, “_”, should be used where spaces are desired. If a true underscore is desired, enter two consecutive underscores and the code will interpret this as an underscore rather than two spaces. For example, if “OPEN SWER” is the complex command the user wishes to be executed, “OPEN_SWER” should be entered.

Table NTPOLL datafill examples

Ex. 1 - Datafilling a “table count” step in Table NTPOLL

TABLE: NTPOLL

>

>add

MACHINES NOT IN SYNC - DMOS NOT ALLOWED

JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED

```
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
NTPOLLKY:
>441 n
LONG: N
>y
SHORT: N
>y
USAGE: N
>
MEMCALC: N
>
STPTYP:
>table
TABNAME:
>MNATMIF
TSOPER:
>count
TUPLE TO BE ADDED:
    441 N      Y Y N N TABLE      MNATMIF COUNT
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

Ex. 2 - Datafilling a "table list all" step in Table NTPOLL

```
TABLE: NTPOLL
>
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
NTPOLLKY:
>442 n
LONG: N
>y
SHORT: N
>
USAGE: N
>
MEMCALC: N
>
STPTYP:
>table
```

```

TABNAME:
>e911psap
TSOPER:
>list
LISTOP:
>all
TUPLE TO BE ADDED:
  442 N    Y N N N TABLE      E911PSAP LIST  ALL
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE

```

Ex. 3 - Datafilling a "internal complex" step in Table NTPOLL

Internal complex commands are added by the system, but a "change" on a complex command tuple is below to show the different fields. For an internal complex command, the string name (CMPLXNAME) is merely a description of the command. The actual CI command(s) and/or procedure(s) to be run are stored internal to the code.

```

>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
LONG: N
>
SHORT: Y
>
USAGE: N
>
MEMCALC: N
>
STPTYP: CMPLX
>
CMPLXTYP: INT
>
CMPLXNAME: Display_IMAGENAME
>
TUPLE TO BE CHANGED:
  1 N          N Y N N CMPLX Display_IMAGENAME
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>n

```

DMO REJECTED

Ex. 4 - Datafilling a “external complex” step in Table NTPOLL

When a complex step is datafilled as EXT (external), the user is actually defining the exact CI command(s) which will run. The CMPLXNAME field will be run as a CI command at polling time. Note that due to table control prompting functionality, underscores must be used where spaces would normally be on the CI command line. Internally, the underscore will be converted to spaces. If a true underscore is desired in the CMPLXNAME, the user should enter a double underscore (i.e. two consecutive underscores).

The following example shows the addition of the “OPEN SWER” command to Table NTPOLL. This command is executed within the LOGUTIL CI level, so presumably the previous user-added step (step # 443) was an external complex command “LOGUTIL” to get into the LOGUTIL level so that OPEN SWER could be executed.

```
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
NTPOLLKY:
>444 n
LONG: N
>y
SHORT: N
>
USAGE: N
>
MEMCALC: N
>
STPTYP:
>cmplx
CMPLXTYP:
>ext
CMPLXNAME:
>open_swer
TUPLE TO BE ADDED:
      444 N          Y N N N CMPLX    OPEN_SWER
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```


The steps for restoring the polling defaults are:

The steps for restoring the polling defaults are:

(1) Delete all existing tuples from Table NTPOLL.

HINT: There are several ways to do this. If the “override” and “verify off” commands are available, the simplest way to do this would be the following:.

```
TABLE: NTPOLL
> count
BOTTOM
SIZE = 437
> ove;ver off
> repeat 437 (del;up)
```

With most tables, only the “del” part would be required. The “up” is included for this table because for every tuple delete, the tuples are renumbered. A repeat loop like this would only delete half of the tuples because the next tuple to be deleted actually gets moved up in the ordering, and the delete happens on the next tuple.

(2) Perform the POLL RESTORE_DEFAULTS command.

```
>poll restore_defaults
Deleting any existing poll steps and recreating from defaults...
Done - default poll_steps restored.
```

10.2.2.4 Execute a step in Table NTPOLL

A new option to the POLL CI command is added so that the user can execute a single step from Table NTPOLL. For example, using the sample NTPOLL table in section 10.2.2.1 “Table NTPOLL” on page 158, step number 33 (a “list all” on Table OFCENG) is executed:

```
> POLL DO_STEP 33
```

10.2.2.5 Minor changes to default polling template

Several minor changes are made to the default polling template defined internally by the system.

- Existing steps that are not currently part of the LONG report are added to the LONG report. The LONG report is the mostly commonly gathered poll report, and certain steps that desired in the LONG report were only in the SHORT report in the past. The names of these steps are:

Display BCS Number
 Display IMAGENAME
 Display Log Message
 DMSMON - LOGCOUNT,
 DMSMON - RESTARTINFO,
 DMSMON - PMCONFIG,
 DMSMON - PMLOADS,
 DMSMON - ASSESS,
 Display CM/MS IDPROM

The output of all of these commands is relatively short and should not increase the length of the LONG report by much.

- The “SOC DBAUDIT” command is added to the complex step that gathers various SOC information (the “Display SOC Data” complex step).
- The processor type the polling is running on is queried so that only commands applicable to that processor type (ex. 88k vs. XA-Core) will be executed.

10.2.2.6 NTPOLL Robustness

While mostly invisible to the user, a number of internal robustness fixes have gone into the polling code for SN08. Among them are:

- A security fix for the POLLUSER remaining permitted after the polling. Each time a scheduled polling occurs, a new DMS user called POLLUSER is permitted to the system, is logged in, and the work of the polling is done under this login session. Problems in the field have been seen where POLLUSER is not properly unpermitted after the polling. A new fix that has gone into the TL21 stream addresses this and ensures the POLLUSER is unpermitted after polling occurs.
- The file compression algorithm will be changed so as to avoid disk space issues on NTDEV. For example, suppose that there is enough data on the switch that a polling has created three data files, POLLDATA, POLLDATA1, and POLLDATA2 and that the compression option was chosen when the polling was scheduled. Currently, the system will create the three files and then compress all three after the polling is done. Under the new algorithm, each file will be automatically compressed as soon as it is closed. This will allow more space for new files to be created and guard against running out of disk space.
- An issue has been discovered where a polling may prematurely halt under certain conditions when one of the poll data files reaches its maximum line limit (approx. 30,000 lines). Rather than close the file and create a new poll data file (as is normally the case), the polling simply stops. Safeguards will

be put in the code to monitor for this condition and properly close the file and create a new one in order to allow the polling to continue.

10.2.2.7 “Push” poll data files to a network location (future)

IMPORTANT NOTE: The POLL PUSH functionality was not implemented. The description is left here for reference as part of a potential future feature, but this functionality is not available at this time.

A desired functionality of the polling system is for the code to automatically FTP the poll data files to a pre-specified network location once a polling has completed. The PUSH option is added to the POLL command. By default, poll pushing is OFF, but it may be turned on and configured with the IP address, userid, password, and remote directory that FTP would need to properly store the files at the remote location.

Ex. Turn automatic file pushing off.

```
> POLL PUSH OFF
```

Ex. Turn automatic file pushing on.

The format is:

```
POLL PUSH ON <ip_addr> <remote_userid> <passwd> <directory>
```

```
> POLL PUSH ON 47.142.211.3 myuserid mypasswd /home/polldude/  
polldata
```

Entering valid parameters for the POLL PUSH command is entirely up to the user. The polling system will do no error checking on the parameters and if any of them are invalid, the FTP storing of the files on the remote system will simply fail.

10.3 Hardware Requirements or Dependencies

No new dependencies.

10.4 Software Requirements or Dependencies

This feature is being developed for SN08 (built on CSP21, which contains TL21 and BAS22).

10.5 Limitations and restrictions

N/A

10.6 Interactions

N/A

10.7 Glossary

Term	Description
DMS	Digital Multiplexing System
FTP	File Transfer Protocol
NTDEV	Nortel device (memory resident disk device)
NTPOLL	DMS polling system which gathers various information about the switch and stores results in POLLDATA files. Pollings can be scheduled.
POLL	CI command to do a polling or query polling parameters
POLLSCHD	CI command to schedule a polling or query poll schedule parameters

11: A00006269 Functional description (FN)

11.1 Feature name

OSSGate Password No Echo

11.2 Description

This document details the OSSGate login changes. It describes the changes being made to OSSGate application which is part of CS2K Management Tools (CMT).

This feature is introduced to make OSSGate consistent with other user interfaces in the CS2K Configuration Management System.

This feature provides the following new or amended functionality:

- No echo of password to the screen when logging in to OSSGate using telnet client
- Ability to turn on or off this functionality using SESM configuration option
- Change to BPT tool to support either login modes

An important change to point out as a consequence of this feature is that OSS vendor software will be impacted by this change. In order to get existing OSS software to work when this new functionality is turned on by SESM configuration, there are couple of changes which need to be implemented in the OSS software. The following are the changes, only if OSSGate Password Control option is turned on (default: off).

- recognize the new login prompt. Prior to SN07, the user name and password was prompted in the same line separated by space. Now, the username and password are prompted one after the other
- OSSGate sends telnet protocol bytes to client to tell it to turn off echo and turn on echo. This is needed for telnet client software. OSS vendor software just needs to ignore these bytes.

11.3 Hardware Requirements or Dependencies

N/A

11.4 Software Requirements or Dependencies

N/A

11.5 Limitations and restrictions

N/A

11.6 Interactions

N/A

11.7 Applicable customer facing sections

Fault Management	
Logs	_____
Alarms	_____
Configuration	
Upgrade	___X___
Data Schema	_____
Service Order	_____
Element Management	_____
User Interface	___X___
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)	_____

11.8 Glossary

Acronym	Definition
BLM	Business Line Management
CLLI	Common Language Location Identifier
CM	Computing Module
CMT	Call Server 2000 Management Tools
CPE	Customer Premises Equipment
CS	Call Server
CS2K	Call Server 2000
DDMS	DMS Data Management System
DMS	Digital Multiplex System
GPS	Global Product Support
GUI	Graphical User Interface

HLD	High Level Design
HTML	HyperText Markup Language
IP	Internet Protocol
ITA	Internet Transparency Agent
LAN	Local Area Network
MI2	Manatee Iteration II
MTC	Maintenance
NA	North American
OAM&P	Operations, Administration, Maintenance and Provisioning
OSS	Operation Support System
OSSDI	OSS Data Interface
PLM	Product Line Management
PTM	Packet Telephony Manager
SDM	SuperNode Data Manager
SESM	Succession Element and Sub-Element Manager [system]
SSPFS	Succession Solaris Platform Foundation Software
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing

12: A00006347 Functional description (FN)

12.1 Feature name

Solaris 9 Introduction To SSPFS

12.2 Description

This feature will cover the SSPFS introduction to the use of Solaris 9 4/04 as the operating system. This feature will cover the following areas:

- New Installations - Installing SSPFS based on Solaris 9 formatting the drives in the process.
- Upgrade Installations - Upgrading the SSPFS unit from SN07 to SN07.1VSD transitioning from Solaris 8 to Solaris 9.
- Third-party Software Recompilations

It needs to be noted that the fresh installations will be impacted and this will require changes to the IM documentation.

12.3 Applicable customer facing sections

Fault Management

Not applicable _____

Logs _____

Alarms _____

Configuration

Not applicable _____

Data Schema/MIBs _____

User Interface _____

GUI _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

SOC _____

Upgrades impact _____Y_____

Accounting (includes AMA billing) _____

Not Applicable	_____
Billing changes	_____
Performance	_____
Not Applicable	_____
Operational Measurements	_____
Performance Measurements	_____

12.4 Hardware Requirements or Dependencies

To test the reduced SSPFS upgrade, you must have fieldgrade hardware on the t1400 or N240 with the proper disk sizes.

12.5 Software Requirements or Dependencies

N/A

12.6 Limitations and restrictions

N/A

12.7 Interactions

N/A

12.8 Glossary

Term	Description

13: A00006450 Functional description (FN)

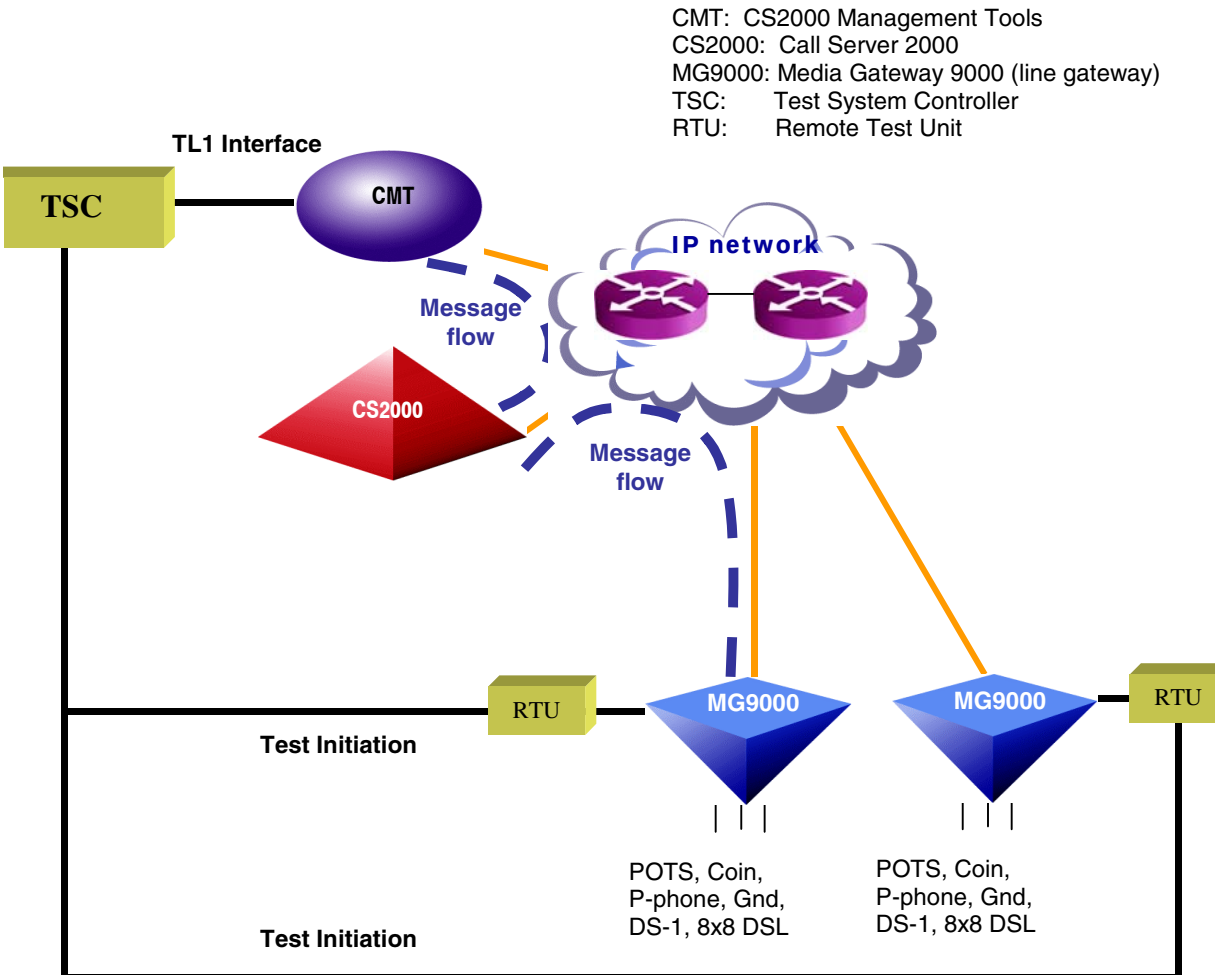
13.1 Feature name

TL1 Line Test Interface for MG9K Lines

13.2 Description

As Nortel Networks rolls out the carrier next generation networks, customers require the new network to support line testing from different test OSS vendors. An open-line test access interface is needed to allow test OSS vendors to operate line test access relays. This feature introduces a TL1 interface in the CS2M that provides a common point of access for MG9K line test. TL1 provides an accepted, standards-based interface for this purpose. This feature adds a standards-based command set as an overlay to pre-existing line test functionality on the MG9K.

13.2.1 Overview



Succession Networks MG9000 line gateway supports POTS, coin, P-phone, ground start, 8x8 POTS and ADSL and DS-1 circuits. Line test access is via MTA (Metallic Test Access) matrix built in the gateway. Each gateway has eight (8) test access ports available; each of which supports 2-wire (one tip-ring pair) test access. Test directions supported by the circuits are:

- Test in (towards the circuit).
- Test out (towards subscriber loop).
- Test bridged configuration.

Although the high impedance isolation is not provided by the MTA in test bridged configurations, it is believed that nearly all currently available test heads have such isolation built in them. The MTA is designed to support both

narrowband and wideband line test, provided the configuration meets Nortel Networks' guide lines.

A MG9000 node can have multiple frames which can house up to four (4) shelves each.

Each shelf has multiple cards serving subscribers. Each card has multiple circuits which each support a subscriber loop. In an MG9000 node, any test access port can reach any loop for testing. A maximum of two concurrent line test access connections can be established on each shelf. One concurrent line test connection can be established per card.

13.2.2 Open Line Test Interface Coverage

The following will be supported in SN08:

- Line test access of MG9000 lines.
- Line testing on all Succession Networks supported POTS lines, 8x8 POTS & ADSL lines on MG9000;
- Both narrowband and wideband line test wherever applicable; although the test access ports only support 2-wire test access

13.2.3 Communication and Interface Protocols

The Test System Controller (TSC) communicates with the CMT (Call server Management Tools) for line test access request. CMT is connected to a secured IP network. The communication between TSC and CMT is via the SSH (Secured SHell). Details on the configuration of SSH and OSSGate usage can be found in the OSSGate User's Guide (NTP# NE10004-512).

Once logged in to the OSSGate, the user will need to change modes to enable the TL1 interface.

From the OSSGate prompt, the user will enter ^B (control-B)

```
>^B <enter>
?
```

A question-mark will be displayed indicating the user is now in control mode. To change to TL1 mode, enter:

```
? mode tl1 <enter>
```

The user will see a message:

```
mode is TL1
>
```

OSSGate is now ready to forward TL1 commands to the TL1 server for processing.

13.2.4 User Authorization

For an OSSGate login user to have permission to execute line test commands, the user must belong to the “**linemtc**” authorization group on the CMT server. This can be done as “root” user from the UNIX command line on the CMT. See the document: NN10276–500 “ATM/IP Configuration Management” for details.

By default, members of “linemtc” have permission to run all TL1 line test commands.

13.2.5 Line Test Access Functionality

13.2.5.1 TL1 Interface Behavior and Dependencies

- 6 Users are required to login to the OSSGate on the CMT via the SSH protocol using a user ID and password.
- 7 The same user ID and password can be used to login more than one TL1 session.
- 8 The MG9000 maintains an inactivity timeout for line test connections of 180 seconds. If the timeout expires, the TL1 user’s existing test access connection will be disconnected and further commands will fail until a new test connection is established. The user login session will not be impacted by this timeout.
- 9 The OSSGate application maintains an inactivity timeout of 5 minutes (300 seconds). If this timeout expires, the TL1 user will be logged out of the system.
- 10 Each TL1 login session can have multiple active test connections. The maximum number of test connections of each TL1 login user will be determined during the implementation.
- 11 There will not be unsolicited messages sent to the user. One TL1 request can expect one TL1 response.
- 12 Directory numbers **must** be specified in their fully qualified form (FQDN) for commands that operate on test access relays. It is optional *only* for the RTRV-SLACC-INFO.

13.2.6 SN08 : TL1 Line Test Access Command Summary

Command Code	Description
CONN-SLACC-MET	Connect the subscriber loop on the test bus.
CHG-SLACC-DIR	Set the test direction to IN (towards the line circuit), OUT (towards the subscriber loop) or BRIDGED.
CHG-SLACC-BW	Change the test access band between narrowband access and wideband access.

REPT-STAT	Reset the 180 second inactivity timer in the system.
DISC-SLACC	Reset all the test access relays to their default state.
RTRV-SLACC-INFO	Retrieve a subscribers' line information.

Note: Transaction Language 1 (TL1) is the line test access protocol used for this interface. It is based on the Telcordia specifications GR-831-CORE and GR-834-CORE. The following sections describe the commands and syntax supported by this interface.

13.2.7 TL1 Syntax Rules:

The following are the TL1 syntax rules enforced by this implementation:

- All TL1 fields are delimited by “:” characters.
- The first 5 fields are mandatory - even if blank. This includes Command code, Target Id, Access Id, Correlation Tag, and General Block.
- If a specific field allows white-space, then it must be enclosed by double quotes “” if the white-space is to be preserved, otherwise it is ignored.
- Each field may consist of one or more parameters separated by white-space or optional comma. This implementation uses commas to delimit parameters within a given field.

These components will each be discussed in turn.

13.2.8 Command Code - (mandatory)

This is the actual command name to be executed and is typically defined in several parts:

<TL1Verb>-<Modifier1>-<modifier2>

A dash “-” character is used to delimit these components.

For this feature, the following command codes are supported:

- CONN-SLACC-MET
- CHG-SLACC-DIR
- CHG-SLACC-BW
- RTRV-SLACC-INFO
- REPT-STAT
- DISC-SLACC

Valid characters for this field are: letters, digits, or hyphen “-”. Any other characters found in this field will cause the operation to fail. This field is **not** case sensitive.

13.2.8.1 Target Identifier (TID) - (mandatory)

As per the TL1 specification (GR-831), this field can consist of up to 20 characters and must be letters, digits, or hyphens. In this implementation, *it is used to define the address format* of the request and must be set to one of the following values:

- DN
- LEN

Although this field is mandatory, certain commands require that it be left empty. This field is **not** case sensitive.

13.2.8.2 Access Identifier Block - (mandatory)

This field can consist of one or more parameters. The parser mainly checks for illegal white-space in unquoted parameters.

In this implementation, this field is used to specify the DN or LEN to be tested and is **not** case sensitive.

13.2.8.3 Correlation Tag (CTAG) - (mandatory)

This field can have a maximum size of 6 alphanumeric characters. This is a mandatory field for all commands. This field **is** case sensitive.

13.2.8.4 General Block - (mandatory)

This field is not used in this implementation. However, it is still mandatory and must be specified as an empty field.

13.2.8.5 Payload Block - (optional)

The payload block contains user-defined data and can consist of zero or more fields. Each Field may contain one or more data elements separated by commas.

Parameters within each field can be specified as either *Positional* or *Name-defined*

- **Positional parameters** have a fixed number of components. Empty components are specified by omitting the data, but inserting the delimiter in its place to show the data as missing. The rules are basically the same as that used when using CSV. All positional components must be specified even if the data is not present.
- **Named-defined** parameters specify their components using a NAME=VALUE approach. The order of components is not enforced and can be omitted if desired.

Important Note: For this feature, all commands defined contain either zero or one parameter in the payload block. Only Name-defined parameters are used and contain a variable number of components (depending on the command).

All tag names and enumerated values are case insensitive. All other values are treated as case sensitive.

13.2.9 TL1 Responses

There are two types of TL1 response message formats used in this feature:
(note that spaces are represented by the ^ (caret) character).

13.2.9.1 Typical response containing header and optional parameter fields

Success Response:

```
<cr> <lf> <lf>
^^^<af>^<date>^<time> <cr> <lf>
M^^<ctag>^<cs> <cr> <lf>
^^^["<optional comma-delimited parameters>"]
<cr> <lf>;
```

where:

<af> : address format

<lf> : line feed

<cr> : carriage return

<cs> : command state (COMPLD == success, DENY == error)

Error Message Format:

```
<cr><lf><lf>
^^^<af>^<date>^<time> <cr><lf>
M^^<ctag>^DENY <cr><lf>
^^^<TL1 ERROR CODE><cr><lf>
^^^["<optional comma-delimited error parameters>"]<cr><lf>
^^^/*<GR-834 error code description>*/<cr><lf>
^^^/*<System-specific error description>*/<cr><lf>
;
```

Error Message Example:

```
> CONN-SLACC-MET:DN:1418420217:CTAG2::TAP=2,BW=NB,DIR=O,sz=1;
```

```
DN 04-06-17 14:13:51
```

```
M CTAG2 DENY
```

```
IPMS
```

```
DN=1418420217,TYPE="SINGLE PARTY LINE",LEN="UAIP 00 2 02
17",OPTIONS=DGT,GW_NAME=UAIP000-0-2,EP_NAME=tp/02/17,GW_NAME=UAIP000-0-
2,NE_NUM=2,LF=UE900MG,LS=IDL,CLLI=COMPACT3 ,BW=NB,DIR=O,sz=1
```

```
/* PARAMETER MISSING */
```

```
/* Missing command parameter "FA". */
```

```
;
```

13.2.9.2 Acknowledgement

This response type is used by the application to construct TL1 acknowledgements to user commands. This type of TL1 response contains no data. It is used to simply ACK specific queries. In this implementation, it is returned as a response to the REPT-STAT command.

```
OK^<CTAG><cr><lf>
```

```
<
```

```
> rept-stat::8420217:ctag2;
```

```
OK ctag2
```

```
<
```

13.2.10 Connect Subscriber Loop on the Test Bus (CONN-SLACC-MET)

The command CONN-SLACC-MET connects the subscriber loop on the test bus. The input, output and the behavior of this command are described in the following sections.

13.2.10.1 Input Fields

- Syntax:

```
CONN-SLACC-MET: <af>: <DN | LEN>: <ctag>: :TAP=<tap>, BW=<bw>, DIR=<dir>, FA=<fa>, SZ=<sz>;
```

Connect a subscriber line on the test bus (CONN-SLACC-MET)	Corba I/F Input Parameters	Description
Input:		
AF (Address Format) (Mandatory input)	N/A	For DN access, enter DN . For LEN access, enter LEN For EPI access, enter EPI
DN, LEN, EPI (Mandatory input)	DN and LEN use two separate field	

Connect a subscriber line on the test bus (CONN-SLACC-MET)	Corba I/F Input Parameters	Description
DN format (# of digits)		If DN is entered, only numerical digits (0-9) are valid input. Min # of digits: 1 Max # of digits: 30 In order to support both North American and international DN format, the TL1 command parser should not reject the number of digits within MIN and MAX above. If the number of digits is invalid to the call server, it should be rejected by the call server.
LEN format		This is the traditional Line Equipment Number stored in CS2K Core. If LEN is entered, alphanumeric character values (0-9, A-Z, a-z) and dash (-) are valid input. Internally, tl1 should convert the alpha characters to either upper case or lower case before processing the command. LEN format in call server will be used, i.e. SITE name + LEN number For example: CARY 000 1 01 12 CARY is the physical location where the line is originating. 000: physical frame number in Cary 1: shelf number 01: slot number 12: circuit number leading zero (0) is required. For Multiple Appearance Directory Number (MADN), line test access is via LEN only. Note: LENS must be enclosed in double quotes ""
EPI (End Point Identifier)		End Point Identifier (EPI) is for future use. It is a string. The format will be defined in future. It is NE type dependent.
CTAG (correlation tag) (Mandatory input)	CTAG	Correlation tag (max 6 ASCII characters)
TAP (Test Access Port) (0-999) (Mandatory input)	MTAPId	Test access port ID For MG9000, it is 1 to 8.

Connect a subscriber line on the test bus (CONN-SLACC-MET)	Corba I/F Input Parameters	Description
BW (Access Bandwidth) (Mandatory input)	Bandwidth Access Care sets it to narrowband Initial connection is always NB option. If WB is desired, the <i>change bandwidth</i> command allows the switch to WB. Access Care does not know what card it is (POTS or ADSL). When Access Care needs wideband test, it always issues, the <i>change bandwidth</i> command to wideband. Then it will instruct the test head to perform the wideband measurement. Once it is completed, Access Care will issue the <i>change bandwidth</i> command to switch back to narrow band	
NB		Narrowband. For MG9000 POTS and SAA card, there is only one test access path. NB or WB will result in the test access on the same path, i.e., no difference. For the 8x8 ADSL card on MG9000, NB line test access allows for the narrowband test access. The test access point is between the POTS circuit card and LPF (Low Pass Filter), when the test direction is OUT (towards the equipment side or subscriber loop side), the test head sees the subscriber loop through LPF. This test access does not cut off the ADSL service.
WB		Wideband Currently is for the 8x8 ADSL card on MG9000 wideband access. The test access is at the subscriber loop side of the splitter. It cuts off both POTS and ADSL services. In Phase 1.1, the WB connection option will not be rejected, unless it is an ADSL circuit.
DIR (Initial test DIRection) (Mandatory input)	desiredDir	

Connect a subscriber line on the test bus (CONN-SLACC-MET)	Corba I/F Input Parameters	Description
O (OUT)		For lookout towards the subscriber loop. It is also called Equipment side.
B (BRIDGED)		Tap the test pair from the test head to the subscriber line. High impedance isolation is not provided.
I (IN)		For look in towards the circuit.
FULL (not supported)		
FA (Forced access flag) (Mandatory input)	Access Care always inputs Force for this parameter.	
Flag=1, if the line state is CPB or CPD, set the connection up and in BRIDGED mode. Do not allow the user to change the test direction. Flag=2, if the line state is CPB or CPD, reject the connection state. See the table below for the detailed description of the behavior of the forced access flag and seize fields.		Flag=1 Flag=2
SZ (SeiZe) (Mandatory input)	Seized Access Care sets this field to Normal	
1	Normal	Seize the line This mode allows the test head to perform the loop testing. However, it does not allow the test head to draw dial tone test. The POTS circuit will not supply the dial tone. In this mode, the voice service is in out-of-service state. The call server will route the caller to this line for a treatment, e.g. supply busy tone or an announcement

Connect a subscriber line on the test bus (CONN-SLACC-MET)	Corba I/F Input Parameters	Description
2		Do not seize the line. This mode allows the test head to perform not only the loop testing, but draw dial tone test when the test direction is in either bridged state or in state. In this mode, the voice service on the line will behave as follows: The line remains in service. The caller to this line will get the normal ring back tone. Since the called party is under test, the loop is cut off. The called party will not hear the ringing tone
N/A	Bandwidth Access Care sets it to narrowband	
N/A	Timeout	
N/A	OwnerID	

- MG9000 Responses to TL1 Force and Seize Parameters

Seize	Force	Requested Connection	MG9000 Response				Notes
			Line is in an Active Call State		Line is Idle		
			Connection	Seize	Connection	Seize	
No	No	Split-In	Request Rejected	N/A	Split-In	No	With no-seize requests, the MG9000 only checks the line for call activity on the initial request.
		Split-Out			Split-Out		
		Bridged			Bridged		
	Yes	Split-In	Bridged	No	Split-In		
		Split-Out	Bridged		Split-Out		
		Bridged	Bridged		Bridged		
Yes	No	Split-In	Request Rejected	N/A	Split-In	Yes	
		Split-Out			Split-Out		
		Bridged			Bridged		
	Yes	Split-In	Bridged	No	Split-In		
		Split-Out	Bridged		Split-Out		
		Bridged	Bridged		Bridged		

This table is valid for CONNSLACC-MET commands. In cases where the initial connection has been made, this table is also valid for CHG_SLACC_DIR commands.

When the MG9000 seizes a line for testing, the line state at the call server becomes SB.

For the purposes of this table, the call state column headings map to the following call server states:

- Active Call States: CPB, CPD.
- Idle States: IDL, INB, MB, PLO, LO.

Regarding Line States not supported by this feature—DEL, LMB, NEQ, SB¹: The TL1 interface implementation in SESM checks for these call server line states. For lines in these states, connection requests are not forwarded to the MG9000.

TL1 parameter mapping to SNMP MTA request entries:

- The SEIZE parameter maps directly.
- FORCE=Yes in TL1 maps to FORCE=Normal in SNMP.
- FORCE=No in TL1 is new. It will map to the new value ForceDont (6) in SNMP.

The following is a description of the line status and behavior during the line testing:

State	Action	No Seize	Seize
CPB	The CS2K/MG9K must give the test system an indication that it has accessed a line that is in an active call. If desired, the test system can test the line in a non-disruptive bridged state.	Must allow bridged connections.	Must allow split-in, split-out and bridge connections.
	The CS2K/MG9K must not allow a disruptive test action on a line involved in an active call.	Must not affect the line state.	Must set the line to an Out of Service state.
CPD	The CS2K/MG9K must give the test system an indication that it has accessed a line that is in an active call. If desired, the test system can test the line in a non-disruptive bridged state.	Must allow split-in, split-out and bridge connections.	Must allow split-in, split-out and bridge connections.
	The CS2K/MG9K must not allow a disruptive test action on a line involved in an active call.	Must not affect the line state.	Must set the line to an Out of Service state.
DEL	The CS2K/MG9K will not support testing a line in the DEL state.		
IDL	The CS2K/MG9K must allow testing a line in the IDL state. This includes testing with a non-disruptive bridged connection and testing with disruptive split connections.	Must allow split-in, split-out and bridge connections.	Must allow split-in, split-out and bridge connections.
		Must not affect the line state.	Must set the line to an Out of Service state.
INB	The CS2K/MG9K must allow testing a line in the INB state. This includes testing with a non-disruptive bridged connection and testing with disruptive split connections.	Must allow split-in, split-out and bridge connections.	Must allow split-in, split-out and bridge connections.
		Must not affect the line state.	Must set the line to an Out of Service state.
LMB	The CS2K/MG9K will not support testing a line in the LMB state.		

State	Action	No Seize	Seize

¹ Testing is not supported if SB is the initial state. This does not apply to lines that have gone SB because the MG9000 has seized them for testing,.

LO	The CS2K/MG9K must allow testing a line in the LO state. This includes both non-disruptive bridged connections and disruptive split connections.	Must allow split-in, split-out and bridge connections. Must not affect the line state.	Must allow split-in, split-out and bridge connections. Must set the line to an Out of Service state.
MB	The CS2K/MG9K must allow testing a line in the MB state. This includes both non-disruptive bridged connection and disruptive split connections.	Must allow split-in, split-out and bridge connections. Must not affect the line state.	Must allow split-in, split-out and bridge connections. Must set the line to an Out of Service state.
NEQ	The CS2K/MG9K will not support testing a line in the NEQ state.	Must allow split-in, split-out and bridge connections. Must not affect the line state.	Must allow split-in, split-out and bridge connections. Must set the line to an Out of Service state.
PLO	The CS2K/MG9K must allow testing a line in the PLO state. This includes both non-disruptive bridged connections and disruptive split connections.	Must allow split-in, split-out and bridge connections. Must not affect the line state.	Must allow split-in, split-out and bridge connections. Must set the line to an Out of Service state.
SB	The CS2K/MG9K will not support testing a line in the SB state.		

13.2.10.2 Input format and examples

- Syntax:

```
CONN-SLACC-MET:<af>:<DN or LEN or EPI>:<ctag>::
TAP=<tap>, BW=<bw>, DIR=<dir>, FA=<fa>, SZ=<sz>;
```

- Example 1 (access via DN):

```
CONN-SLACC-MET:DN:4166213000:CTAG1:: TAP=1, BW=NB, DIR=O, FA=1, SZ=2;
```

- Example 2 (access via LEN):

```
CONN-SLACC-MET:LEN:"CARY 000 1 01 12":CTAG1::TAP=1, BW=NB, DIR=O, FA=1, SZ=2;
```

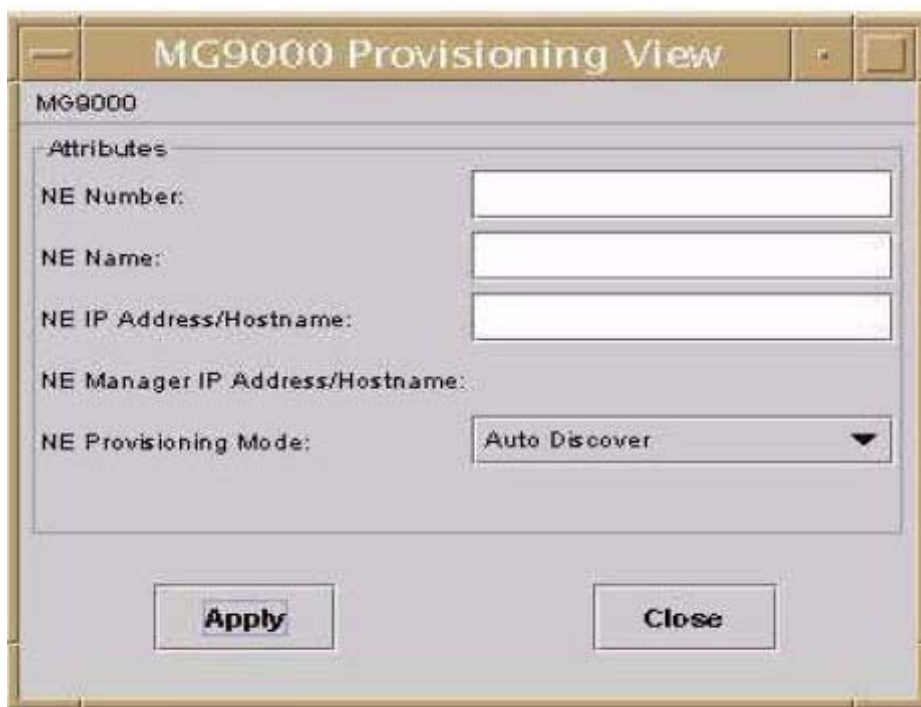
Within a parameter field, when there is more than one field, a comma ‘,’ is placed between the two adjacent fields as separator. There must not be space before and after the comma.

13.2.10.3 Output Fields

Connect a subscriber line on the test bus (CONN-SLACC-MET)	Description

Output:	
CTAG	Correlation tag
CS (Command Status)	COMPLD: command is executed successfully. DENY: command is executed unsuccessfully.
TAP (Test Access Port) (0-999)	Test access port ID
BW (Access Bandwidth)	NB for NarrowBand WB for WideBand
DIR (The actual connection direction) (In, Out, Bridged, AC monitor, not connected, full)	MG9000: I (IN), O (OUT), B (BRIDGED) LCM: O, B The test direction is dependant upon what the NE can support.
NE Number	The NE NUMBER is a numeric digit defined for each MG9000 node. This ID is unique to all MG9000 nodes associated with the same call server. It is limited to 3 digits. It is not enforced that it is in sequential order. For example, if the NE NUMBER for the first installed MG9000 node is defined as 0, the NE NUMBER of the next installed MG9000 node does not have to be 1, as long as it is not 0 (it has to be unique). This NE NUMBER is displayed with label: NE Number with the MG9000 node name (NE Name) (See the following screen shot)
NE name	It is required for the subsequent command request, NE Number and Tap are the mandatory input parameters for the commands after the test connection is setup. For the other NE, return -1.
CS2000 CLLI	The NE name defined for MG9000. For the other NE, return -1.
LS (Line Status)	The Line status after the test access. 9 Note: the Line status can be obtained via the POST command in Succession MAPCI the same way as it is in DMS MAPCI.

EN (Equipment Number)	Site name and LEN e.g. CARY 000 1 01 09 This information is useful, when the address is DN. Note: The Equipment Number can be obtained via QDN from the OSS Gate.
LT (Line Type) (POTS, ISDN, P-phone, etc.)	The Line Type as specified by the QDN/QLEN command
LF (Line Frame type) (UE9000MG, LCM, GR-303 DLC, etc.)	For MG9000 return UE9000MG. This field is populated with the gateway type defined in the CMT database.



The image shows a software window titled "MG9000 Provisioning View". Inside the window, there is a section labeled "MG9000" followed by "Attributes". Below this, there are five input fields: "NE Number:", "NE Name:", "NE IP Address/Hostname:", "NE Manager IP Address/Hostname:", and "NE Provisioning Mode:". The "NE Provisioning Mode:" field is a dropdown menu currently showing "Auto Discover". At the bottom of the window, there are two buttons: "Apply" and "Close".

Warning:

If the test connection is in the bridged or in state, Nortel recommends that the test controller may only execute passive commands, i.e., those which do not require applying voltage, current, or tones to the loop or line card (such as AC/DC voltage measurements) to subscriber test functions. For example, do not perform the 12 metallic loop test function. The reason is that MG9000 POTS card has a hazard voltage protection feature to protect the POTS circuit from foreign voltage. If the voltage applied on the line in BRIDGED (or IN state) is

above the hazardous voltage threshold, the subscriber line will be cut off. This may cut off an active call.

13.2.10.4 Output Format and Examples

- Syntax:

```
<cr> <lf> <lf>
^^^<af>^<date>^<time> <cr> <lf>
M^^<ctag>^<cs> <cr> <lf>
^^^^'TAP=<tap>,BW=<bw>,DIR=<dir>,NE_NUM=<ne number>,NE_NAME=<ne
name>,CLLI=<CS2000CLLI>,LS=<line status>"<cr> <lf>;
```

- Example:

```
DN 03-12-12 03:23:43
M CTAG1 COMPLD
"TAP=1,BW=N,DIR=0,NE_NUM=005,NE_NAME=GATEWAYID005,CLLI=RTP2,LS=IDL"
```

- Syntax:

```
<cr><lf><lf>
^^^<af>^<date>^<time> <cr><lf>
M^^<ctag>^DENY <cr><lf>
^^^<TL1 ERROR CODE><cr><lf>
^^^[``<optional comma-delimited error parameters>"]<cr><lf>
^^^/*<TL1 error description>*/<cr><lf>
^^^/*<System-specific error description>*/<cr><lf>
;
```

[See Tables 1 and 2 for TL1 Error mapping for the TL1 server and MG9K](#)

13.2.10.5 Dependencies

This command must be rejected, if a connection has already been setup for the same session.

13.2.11 Change Test Direction – CHG-SLACC-DIR

Command CHG-SLACC-DIR allows a user to set the test direction to IN, OUT and BRIDGED. IN means connect the tip-ring test pair to the circuit on a line card. OUT means connect the tip-ring test pair to a subscriber loop. BRIDGED means connect the tip-ring test pair to the line. In the BRIDGED state, the high impedance isolation is not provided by the MTA at test bridged configuration for the Nortel product. This command is valid if CONN-SLACC-MET was executed successfully. The input, output and the behavior of this command are described in the following sections.

13.2.11.1 Input Fields

Change test access direction (CHG-SLACC-DIR)	Corba I/F Input Parameters	Description
Input		
AF (Address Format) (Mandatory input)	N/A	For DN access, enter DN . For LEN access, enter LEN For EPI access, enter EPI
DN, LEN, EPI (Mandatory input)	DN and LEN use two separate field	
DN format (# of digits)		If DN is entered, only numerical digits (0-9) are valid input. Min # of digits: 1 Max # of digits: 30 In order to support both North American and international DN format, the TL1 command parser should not reject the number of digits within MIN and MAX above. If the number of digits are invalid to the call server, it should be rejected by the call server.
LEN format		This is the traditional Line Equipment Number stored in the CS2K Core. If LEN is entered, alphanumeric character values (0-9, A-Z, a-z) and dash (-) are valid input. Internally, tl1 should convert the alpha characters to either upper case or lower case before processing the command. The LEN format in the call server will be used, i.e. SITE name + LEN number For example: CARY 000 1 01 12 CARY is the physical location where the line originates. 000: physical frame number in Cary 1: shelf number 01: slot number 12: circuit number leading zero (0) is required. For the Multiple Appearance Directory Number (MADN), line test access is via LEN only. Note: LENs must be enclosed in double quotes ""
EPI (End Point Identifier)		The End Point Identifier (EPI) is for future use. It is a string. The format will be defined in future. It is NE type dependent.
CTAG (Mandatory input)	N/A	Correlation tag (max 6 ASCII characters)

DIR (Test direction) (Mandatory input)	desiredDir	The test direction change will be rejected, if, for example, the line is in the CPB (Call Processing Busy) state, the test direction is in the BRIDGED state. Changing the test direction to OUT or IN will be rejected, since cut-off of the subscribers' conversation is not allowed. If the test access direction change is rejected, the response must not produce an error message. It should response with COMPLD and with no error message. This behavior is consistent with the current no-test trunk interface behavior. And Access Care does not expect an error message, if the desired test access direction cannot be changed.
O (OUT)		Toward the subscriber loop. If the line is busy and the original state is BRIDGED, changing the line test direction to OUT is not allowed.
B (BRIDGED)		Tap the test pair from the test head to the subscriber line. High impedance isolation is not provided.
I (IN)		Toward the line circuit. If the line is busy and the original state is BRIDGED, changing the line test direction to IN is not allowed.

13.2.11.2 Input Format and Examples

- Syntax:

CHG-SLACC-DIR::<DN>|<LEN>|<EPI>:<ctag>::DIR=<dir>;

- Example:

CHG-SLACC-DIR::4166213000:CTAG2::DIR=I;

13.2.11.3 Output Fields

Change test access direction (CHG-SLACC-DIR)	Description
Output	
CS (Command Status)	COMPLD: command is executed successfully. DENY: command is executed unsuccessfully.
CTAG	Correlation tag

DIR (The actual connection direction) (In, Out, Tee (Bridged), AC monitor, not connected, full)	The test direction is the one after the command is executed. If the response status is DENY, the direction will not change. MG9000: I (IN), O (OUT), B (BRIDGED) LCM: O, B The test direction is dependant upon what NE can support. FULL, AC monitor will not be supported in phase 1

13.2.11.4 Output Format and Examples

- Syntax:

```
<cr> <lf> <lf>
^^<af>^<date>^<time> <cr> <lf>
M^^<ctag>^<cs> <cr> <lf>
^^"DIR=<dir>"
<cr> <lf>;
```

- Example:

```
DN 03-12-12 03:23:43
M      CTAG2 COMPLD
      "DIR= I"
```

- Syntax:

```
<cr><lf><lf>
^^<af>^<date>^<time> <cr><lf>
M^^<ctag>^DENY <cr><lf>
^^<TL1 ERROR CODE><cr><lf>
^^[''<optional comma-delimited error parameters>"]<cr><lf>
^^/*<TL1 error description><cr><lf>*/
^^/*<System-specific error description>*/<cr><lf>
;
```

[See Tables 1 and 2 for TL1 Error mapping for the TL1 server and MG9K](#)

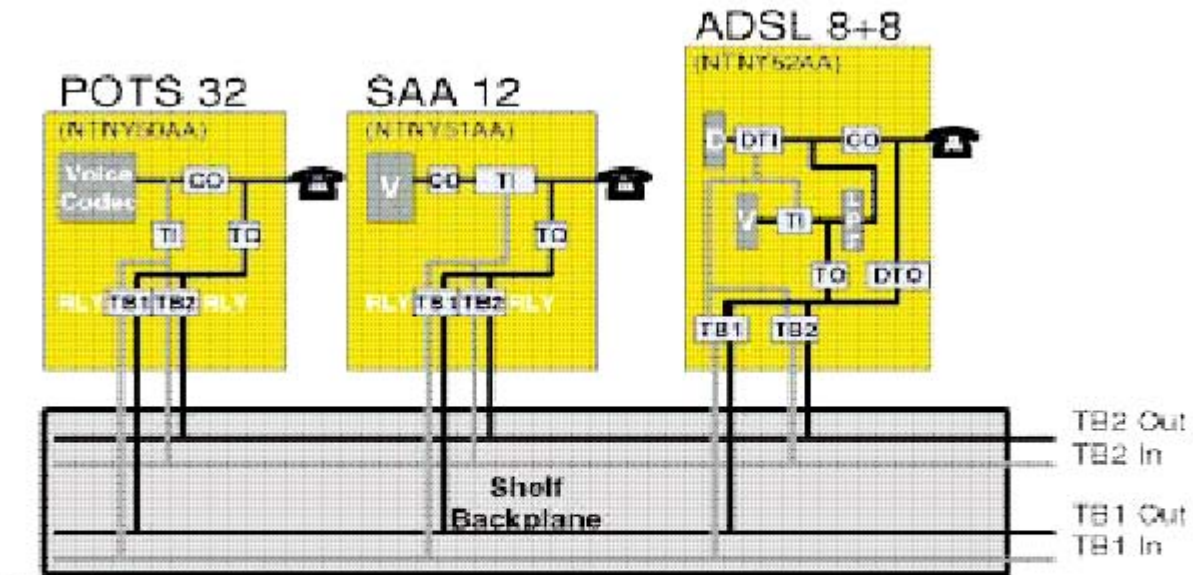
13.2.11.5 Dependencies

This command is valid only

- After the successful execution of CONN-SLACC-MET.
- The line is not BUSY

13.2.12 Change Test Access Bandwidth – CHG-SLACC-BW

Command CHG-SLACC-BW allows for changing the test access between narrowband access and wideband access. In MG9000, the POTS and SAA cards have only one physical test access. It supports wideband testing. CHG-SLACC-BW will not physically change the test access relays. The 8x8 ADSL card has different test access. If the narrowband test access is requested, the test access point will be between the voice circuit and LPF (Low Pass Filter). In this case, the voice service will be cutoff and the ADSL service will still be available to the customer. If the wideband test access is requested, the cutoff relay is on the customer loop side. Both the voice and the ADSL service will be cutoff. The CHG-SLACC-BW command is independent from the current test direction. For example, if the current test direction is narrowband OUT, CHG-SLACC-BW will set the test access to wideband OUT and vice-versa. This logic applies to test direction IN and BRIDGED as well. If the line is voice busy during the initial test access, the test direction will be set to BRIDGED. CHG-SLACC-BW is allowed to switch between wideband BRIDGED and narrowband BRIDGED. However, changing CHG-SLACC-DIR to IN or OUT is not allowed in both cases.



Legend:

TI - test in

TO - test out

CO - cut off

TB1 - Puts card's MTA bus on shelf test bus 1

TB2 - Puts card's MTA bus on shelf test bus 2

DTI - Combination cut off and data test in. When operated, cuts loop off from ADSL chip set, and connects the ADSL chipset to the test-in bus.

13.2.12.1 Input Fields

Change test access direction (CHG-SLACC-BW)	Corba I/F Input Parameters	Description
Input		
AF (Address Format) (Mandatory input)	N/A	For DN access, enter DN . For LEN access, enter LEN
DN, LEN (Mandatory input)	DN and LEN use two separate field	
DN format (# of digits)		If DN is entered, only numerical digits (0-9) are valid input. Min # of digits: 1 Max # of digits: 30 In order to support both North American and international DN format, the TL1 command parser should not reject the number of digits within MIN and MAX above. If the number of digits is invalid to the call server, it should be rejected by the call server.
LEN format		This is the traditional Line Equipment Number stored in the CS2K Core. If LEN is entered, alphanumeric character values (0-9, A-Z, a-z) and dash (-) are valid input. Internally, tl1 should convert the alpha characters to either upper case or lower case before processing the command. The LEN format in the call server will be used, i.e. SITE name + LEN number For example: CARY 000 1 01 12 CARY is the physical location where the line originates. 000: physical frame number in Cary 1: shelf number 01: slot number 12: circuit number leading zero (0) is required. For Multiple Appearance Directory Number (MADN), line test access via LEN only. Note: LENs must be enclosed in double quotes ""
CTAG (Mandatory input)	N/A	Correlation tag (max 6 ASCII characters)
BW (Access Bandwidth) (Mandatory input)	Bandwidth – narrowband or wideband	

NB		Narrowband. For the MG9000 POTS and SAA card, there is only one test access path. NB or WB will result in the test access on the same path, i.e., no difference. For the 8x8 ADSL card on MG9000, NB line test access allows for the narrowband test access. The test access point is between the POTS circuit card and LPF (Low Pass Filter), when the test direction is OUT (subscriber loop side), the test head sees the subscriber loop through LPF. This test access does not cut off the ADSL service.
WB		Wideband Currently this is for the 8x8 ADSL card on MG9000 wideband access. The test access is at the subscriber loop side of the splitter. It cuts off both the POTS and ADSL services.

13.2.12.2 Input Format and Examples

- Syntax:

CHG-SLACC-BW : : <DN> | <LEN> : : <ctag> : : BW=<bw> ;

- Example:

CHG-SLACC-BW::4166213000:CTAG3::BW=NB;

- Output Fields

Change test access direction (CHG-SLACC-BW)	Description
Output	
CTAG	Correlation tag
CS (Command Status)	COMPLD: command is executed successfully. DENY: command is executed unsuccessfully.

See Tables 1 & 2 for TL1 Error mapping for the TL1 server and MG9K

13.2.12.5 Dependencies

This command is valid after the successful execution of CONN-SLACC-MET.

13.2.13 Report Status – REPT-STAT

Command REPT-STAT is used for refreshing the 180-second access disconnect timer kept by the gateway. If the gateway does not receive a valid command within the timeout period, it disconnects test access from the subscriber circuit that was specified in the initial CONN-SLACC-MET command.

13.2.13.1 Input Fields

Report status (used for timeout refresh) (REPT-STAT)	Corba I/F Input Parameters	Description
Input		
AF (Address Format) (Mandatory input)	N/A	For DN access, enter DN . For LEN access, enter LEN
DN, LEN, EPI (Mandatory input)	DN and LEN use two separate field	
DN format (# of digits)		If DN is entered, only numerical digits (0-9) are valid input. Min # of digits: 1 Max # of digits: 30 In order to support both North American and international DN format, the TL1 command parser should not reject the number of digits within MIN and MAX above. If the number of digits is invalid to the call server, it should be rejected by the call server.

LEN format		This is the traditional Line Equipment Number stored in the CS2K Core. If LEN is entered, alphanumeric character values (0-9, A-Z, a-z) and dash (-) are valid input. Internally, tl1 should convert the alpha characters to either upper case or lower case before processing the command. The LEN format in the call server will be used, i.e. SITE name + LEN number For example: CARY 000 1 01 12 CARY is the physical location where the line originates. 000: physical frame number in Cary 1: shelf number 01: slot number 12: circuit number leading zero (0) is required. For Multiple Appearance Directory Number (MADN), line test access is via LEN only. Note: LENs must be enclosed in double quotes ""
CTAG (Mandatory input)	N/A	Correlation tag (max 6 ASCII characters)

13.2.13.2 Input Format and Examples

- Syntax:

REPT-STAT : : <DN> | <LEN> : <ctag> ; ;

- Example:

REPT-STAT : : 4166213000 : CTAG4 ; ;

13.2.13.3 Output Fields

Report status (used for timeout refresh) (REPT-STAT)	Description
Output	
OK	
CTAG	Correlation tag

13.2.13.4 Output Format and Examples

- Syntax:

OK <ctag> <cr> <lf>

<

- Example:

OK CTAG2 <cr><lf>

<

13.2.13.5 Error Response:

- Syntax:

```
<cr><lf><lf>
^^^<af>^<date>^<time> <cr><lf>
M^^<ctag>^DENY <cr><lf>
^^^<TL1 ERROR CODE><cr><lf>
^^^["<optional comma-delimited error parameters>"]<cr><lf>
^^^/*<TL1 error description><cr><lf>*/
^^^/*<System-specific error description>*/<cr><lf>
```

See Tables 1 and 2 for TL1 Error mapping for the TL1 server and MG9K

13.2.13.6 Dependencies

This command is valid after the successful execution of CONN-SLACC-MET.

13.2.14 Disconnect the Test Connection – DISC-SLACC

The command DISC-SLACC disconnects the test connection. This command restores the circuit under test to its through state and opens all TAP connections to that access point. The input, output and the behavior of this command are described in the following sections.

13.2.14.0.1 Input Fields

Disconnect a subscriber line from the test bus (DISC-SLACC)	Corba I/F Input Parameters	Description
Input		
AF (Address Format) (Mandatory input)	N/A	For DN access, enter DN. For LEN access, enter LEN
DN, LEN, EPI (Mandatory input)	DN and LEN use two separate field	
DN format (# of digits)		If DN is entered, only numerical digits (0-9) are valid input. Min # of digits: 1 Max # of digits: 30 In order to support both North American and international DN format, the TL1 command parser should not reject the number of digits within MIN and MAX above. If the number of digits is invalid to the call server, it should be rejected by the call server.

LEN format		This is the traditional Line Equipment Number stored in CS2K Core. If LEN is entered, alphanumeric character values (0-9, A-Z, a-z) and dash (-) are valid input. Internally, tl1 should convert the alpha characters to either upper case or lower case before processing the command. LEN format in call server will be used, i.e. SITE name + LEN number For example: CARY 000 1 01 12 CARY is the physical location where the line originates. 000: physical frame number in Cary 1: shelf number 01: slot number 12: circuit number leading zero (0) is required. For Multiple Appearance Directory Number (MADN), line test access via LEN only. Note: LENs must be enclosed in double quotes ""
EPI (End Point Identifier)		End Point Identifier (EPI) is for future use. It is a string. The format will be defined in future. It is NE type dependent.
CTAG (Mandatory input)	N/A	Correlation tag (max 6 ASCII characters)

13.2.14.1 Input Format and Examples

- Syntax:

DISC-SLACC::<DN>|<LEN>|<EPI>:<ctag>;

- Example:

DISC-SLACC::4166213000:CTAG4;;

13.2.14.2 Output Fields

13.2.14.3 1Output Format and Examples

Disconnect a subscriber line from the test bus (DISC-SLACC)	Description
Output	
CTAG	Correlation tag
	Phase 1.1
CS (Command Status)	COMPLD: command is executed successfully. DENY: command is executed unsuccessfully. Phase 1.1

- Syntax:

```
<cr> <lf> <lf>
^^^<af>^<date>^<time> <cr> <lf>
M^^<ctag>^<cs> <cr> <lf>
<cr> <lf>;
```

- Example:

```
DN 03-12-12 03:23:43
M      CTAG4 COMPLD
;
```

13.2.14.4 Error Response:

- Syntax:

```
<cr><lf><lf>
^^^<af>^<date>^<time> <cr><lf>
M^^<ctag>^DENY <cr><lf>
^^^<TL1 ERROR CODE><cr><lf>
^^^["<optional comma-delimited error parameters>"]<cr><lf>
^^^/*<TL1 error description><cr><lf>
^^^<System-specific error description>*/<cr><lf>
```

[See Tables 1 and 2 for TL1 Error mapping for the TL1 server and MG9K](#)

13.2.15 Retrieve Line Information – RTRV-SLACC-INFO

Command RTRV-SLACC-INFO queries the CS2000 to obtain information related to a line. This command does not operate the test access relays, such as the ones in MG9000 MTA and line circuit. It can be executed without a connection up. The input, output and the behavior of this command are described in the following sections.

13.2.15.1 Input Fields

Query line info (RTRV-SLACC-INFO)	No existing Corba IDL for this command	Description
Input:		
AF (Address Format) (Mandatory input)		For DN access, enter DN . For LEN access, enter LEN
DN, LEN, EPI (Mandatory input)		
DN format (# of digits)		If DN is entered, only numerical digits (0-9) are valid input. Min # of digits: 1 Max # of digits: 30 In order to support both North American and international DN format, the TL1 command parser should not reject the number of digits within MIN and MAX above. If the number of digits are invalid to the call server, it should be rejected by the call server.
LEN format		If LEN is entered, alphanumeric character values (0-9, A-Z, a-z) and dash (-) are valid input. Internally, tl1 should convert the alpha characters to either upper case or lower case before processing the command. The LEN format in the call server will be used, i.e. SITE name + LEN number For example: CARY 000 1 01 12 CARY is the physical location where the line originates 000: physical frame number in Cary 1: shelf number 01: slot number 12: circuit number leading zero (0) is required. For Multiple Appearance Directory Number (MADN), line test access via LEN only. Note: LENs must be enclosed in double quotes "" Correlation tag (max 6 ASCII characters)
CTAG (correlation tag) (Mandatory input)		

13.2.15.2 Input Format and Examples

- Syntax:

RTRV-SLACC-INFO:<af>:<DN | LEN>:<ctag>;

- Example 1 (access via DN):

RTRV-SLACC-INFO:DN:4166213000:CTAG6;

- Example 2 (access via LEN):

RTRV-SLACC-INFO:LEN:"CARY 000 1 01 12":CTAG6;

13.2.15.3 Output Fields

Query line info (RTRV-SLACC-INFO)	Description
Output:	
CTAG	Correlation tag
CS (Command Status)	COMPLD: command is executed successfully. DENY: command is executed unsuccessfully.
NE Number	The NE Number is a numeric digit defined for each MG9000 node. This ID is unique to all MG9000 nodes associated with the same call server. It is limited to 3 digits. It is not enforced that it is in sequential order. For example, if the NE Number for the first installed MG9000 node is defined as 0, the NE Number of the next installed MG9000 node does not have to be 1, as long as it is not 0 (it has to be unique). This NE Number is displayed with label: NE Number with the MG9000 node name (NE Name) (See the following screen shot). It is required that for the subsequent command request, NE Number and Tap are the mandatory input parameters for the commands after the test connection is setup. For other NE, return -1.
NE name	The NE name defined for MG9000. For the other NE, return -1.
CS2000 CLLI	
LS (Line Status)	Line status before the test access.
EN (Equipment Number)	Site name and LEN e.g. CARY 000 1 01 09 This information is useful, when the address is DN.
LT (Line type) (POTS, ISDN, P-phone, etc.)	Line type as specified by the QDN/QLEN command
LF (Line Frame type) (MG9000, LCM, GR-303 DLC, etc.)	For MG9000 return UE9000MG This field is populated with the gateway type defined in the CMT database.

13.2.15.4 Output Format and Examples

- Syntax:

```
<cr> <lf> <lf>
^^^<af>^<date>^<time> <cr> <lf>
M^^<ctag>^<cs> <cr> <lf>
^^^DN=<FQDN>,LEN=<LEN>,OPTIONS=<options>,TYPE=LineType>,GW_NAME=<gatewayName>,EP_NAME=<endpointName>,LS=<line state>,CLLI=<CS2K CLLI>,NE_NUM=<ne number>,NE_NAME=<ne name>,CLLI=<CS2000CLLI>,LF=<frame Type><cr> <lf>;
```

13.2.15.5 Output Example:

```
DN 04-06-30 20:25:40
M CTAG5 COMPLD
"DN=4166213000,LEN="VOIP 42 2 09 13",OPTIONS=DGT,TYPE="SINGLE PARTY
LINE",GW_NAME=VOIP042-0-2,EP_NAME=tp/09/13,LS=IDL,CLLI=RTP7,GW_NAME=VOIP042-0-
2,NE_NUM=42,LF=UE9000MG"
;
```

- Example (LEN):

```
LEN 04-05-31 23:35:05
M CTAG6 COMPLD
"LEN="SLOA 04 1 00 00",TYPE="SINGLE PARTY
LINE",DN=9196200000,OPTIONS=DGT,GW_NAME=SLOA004-0-1, LS=SB,CLLI=RTP7,NE_NUM=0,
LF="UE9000MG" "
;
```

13.2.15.6 Error Response:

- Syntax:

```
<cr><lf><lf>
^^^<af>^<date>^<time> <cr><lf>
M^^<ctag>^DENY <cr><lf>
^^^<TL1 ERROR CODE><cr><lf>
^^^["<optional comma-delimited error parameters>"]<cr><lf>
^^^/*<TL1 error description><cr><lf>*/
^^^/*<System-specific error description>*/<cr><lf>
```

[See Tables 1 and 2 for TL1 Error mapping for the TL1 server and MG9K](#)

13.2.15.7 Dependencies

This command has no dependencies and can be executed at any time. The input DN or LEN can be the same as the DN or LEN of the active connection, but it is not required

13.2.15.8 Error code listings

The following tables list the TL1 error codes and descriptions generated by the TL1 Server and the MG9K.

Table 1 TL1 Error Codes - TL1 Server

TL1 Error Code	TL1 Category	TL1 Error Text	Description
ESPG	EQUIPAGE	SOFTWARE PROGRAM	An error occurred in the application software while processing a request. All accumulated line information up to the point of error will be displayed. A comment line will be displayed in the TL1 response message indicating the source of failure.
ICNV	INPUT	COMMAND NOT VALID	The command code entered is invalid for this interface.
IDNV	INPUT	DATA NOT VALID	One of the input fields contains invalid data. A comment line will be displayed in the TL1 response message indicating the source of failure.
IIAC	INPUT	INVALID ACCESS IDENTIFIER (AID)	An invalid DN or LEN has been found in the access identifier field of the request message. A comment line will be displayed in the TL1 response message indicating the source of failure.
IICM	INPUT	INVALID COMMAND	The command entered is missing required fields. A comment line will be displayed in the TL1 response message indicating the source of failure.

IICT	INPUT	INVALID CORRELATION TAG	The correlation tag entered violates the one of the following constraints: -must be non-null -must be alpha-numeric -must be between 1-6 characters in length A comment line will be displayed in the TL1 response message indicating the source of failure.
IISP	INPUT	INVALID SYNTAX OR PUNCTUATION	Missing or invalid command terminator.
IITA	INPUT	INVALID TARGET IDENTIFIER	An invalid address format has been found in the target identifier field of the request message. A comment line will be displayed in the TL1 response message indicating the source of failure.
IPMS	INPUT	PARAMETER, MISSING	A required parameter has not been specified in the command entered. A comment line will be displayed in the TL1 response message indicating the source of failure.
IPNC	INPUT	PARAMETER NOT CONSISTENT	An entered parameter has both Positional and Named components. As per GR-831 syntax rules, a parameter components must be of the same type. A comment line will be displayed in the TL1 response message indicating the source of failure.
IPNV	INPUT	PARAMETER NOT VALID	An illegal parameter tag or value has been found in the command string. A comment line will be displayed in the TL1 response message indicating the source of failure

ISPC	INPUT	SYNTAX PUNCTUATION	A syntax error has been detected in the command string. An example would be a missing “ around a quoted string. A comment line will be displayed in the TL1 response message indicating the source of failure
ITSN	INPUT	INVALID/INACTIVE TEST SESSION NUMBER	The test session for the DN or LEN entered does not exist. Either there has been no test session established yet, or the test session has been terminated due to an inactivity time-out. A comment line will be displayed in the TL1 response message indicating the source of failure
SCSN	STATUS	INVALID COMMAND SEQUENCE	A TL1 command has been entered for which a required requisite command has not yet been executed. For example, CHG-SLACC-DIR cannot be executed successfully until CONN-SLACC-MET has been run to establish a test session. A comment line will be displayed in the TL1 response message indicating the source of failure
SDBE	STATUS	INTERNAL DATA BASE ERROR	An internal database error has been detected during command execution. A comment line will be displayed in the TL1 response message indicating the source of failure
SNVS	STATUS	NOT IN VALID STATE	The target circuit is not in a state valid for line test. A comment line will be displayed in the TL1 response message indicating the source of failure
SROF	STATUS	REQUESTED OPERATION FAILED	This is a general error indicating that the request could not be processed successfully. A comment line will be displayed in the TL1 response message indicating the source of failure.

SRQN	STATUS	INVALID REQUEST	The operation cannot be performed on the specified target. Possible reasons are: -Unsupported gateway type -NLT option on line (no line test) -line is specified by DN and is member of a MADN group. A comment line will be displayed in the TL1 response message indicating the source of failure

TL1 Error Code	TL1 Error Text	MG9K Error Text (user-visible)	MG9K Error Description
RCBY	CIRCUIT BUSY	"Line Busy, Try Again Later"	The MG sends this if the line appears to be in a call.
SNVS	NOT IN VALID STATE	"Line can't be accessed. Check Line at Gateway Manager."	The MG sends this if the linecard has been pulled, the line circuit is busy, or otherwise inaccessible.
ENEQ	NOT EQUIPPED	"Gateway Not Equipped for This Request. Check Gateway Manager"	The MG sends this when the required equipment is missing. Currently for MTA access, this may never be returned by the MG9000. It might be a good return code if the EM finds that there is not a corresponding tap provisioned for the request.
RANB	ACCESS NETWORK BUSY	"A Gateway Test Resource is Busy. Try Again Later."	This is returned when internal resources are all in use, such as verticals and shelf test buses, or if there is another test on the same linecard (there is only one test bus per line card)

SROF	REQUESTED OPERATION FAILED	"Problem with a Gateway Test Resource. Check Gateway Manager"	The MG sends this when there is nothing wrong with the request, but there is something wrong with required equipment on the MG9000. Could not find a better match in the list.
EFON	FEATURE OPTION NOT PROVIDED	"The request or one of its requested options is not supported."	For example, request for full-split would return not_supported.
SRQN	INVALID REQUEST	"Invalid Request. Check MTAPT and line exists, and for conflicting parameters."	MG sends this for scenarios such as conflicting parameters, e.g., a test-out connection requested when seize is false (test-out interferes with call-p, so the line must be seized for test-out).
SABT	ABORTED	"Test session abandoned, connection dropped. Check Test System."	Line test session inactivity time-out expired on the gateway.
SABT	ABORTED	"The gateway encountered a problem. Try Again. If problem recurs, check line and test Resources at Gateway Manager."	Line test session terminated by the gateway due to a maintenance event or failure.
SROF	REQUESTED OPERATION FAILED	"Try Again. If problem recurs, check line and test Resources at Gateway Manager."	Miscellaneous internal system error.
SROF	REQUESTED OPERATION FAILED	"Try Again. If problem recurs, check line and test Resources at Gateway Manager."	Miscellaneous internal system error.
SROF	REQUESTED OPERATION FAILED	"Try Again. If problem recurs, check line and test Resources at Gateway Manager."	Miscellaneous internal system error.

13.3 Hardware Requirements or Dependencies

There are no hardware dependencies introduced by this feature.

13.4 Software Requirements or Dependencies

There are no new software requirements introduced by this feature.

13.5 Limitations and restrictions

As stated earlier, directory numbers must be specified in their fully qualified form (FQDN) for test commands that manipulate test connections on the MG9K. This includes the following commands:

- CONN-SLACC-MET
- CHG-SLACC-DIR
- CHG-SLACC-BW
- REPT-STAT

Since RTRV-SLACC-INFO has no dependencies and only queries the call server, FQDN is optional for this command.

13.6 Upgrade Dependencies

This feature introduces a dependency in the upgrade sequence of the Access Care system with the rest of the Succession components.

When upgrading from releases prior to SN07 to SN07 and greater, it is required that Access Care be upgraded **ONLY** after the CMT, MG9K-EM and MG9K upgrades are complete. Failing to do so will disable Line test capabilities between Access care and the MG9K.

13.7 Interactions

There are no new interactions visible to the user introduced by this feature.

13.8 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___

Upgrade considerations	___X___

Accounting (includes AMA billing) ____N/A____

Performance (includes operational measurements) ____N/A____

13.9 Glossary

Term	Explanation
CMT	Call server Management Tools
CPB	Call Processing Busy
CS2000	Call Server 2000
GW	GateWay
LPF	Low Pass Filter
MG9000	Media Gateway 9000 (line gateway)
MTA	Metallic Test Access
MTAP	Metallic Test Access Port on MG9000
MTM	Metallic Test access Module
NE	Network Element
CMT	
RMM	Remote Maintenance Module
RTU	Remote Test Unit
SSH	Secure Shell
TL1	Transaction Language 1
TSC	Test System Controller
UPC	User Privilege Code

13.10 References

- 1 Telcordia GR-834-CORE, “Network Maintenance: Access and Testing Messages”, Chapter 6, “TSC-RTU NE Interface”
- 2 Refer to Telcordia GR-834-CORE Appendix A-G for conventions, error codes etc.
- 3 Telcordia GR-831-CORE

14: A00006570 Functional description (FN)

14.1 Feature name

CS2M Robustness enhancement - Moving SDM IP & CLLI input to SSPFS

14.2 Description

14.2.1 Existing Functionality

Prior to SN08, SDM IP/CLLI/CM IP are configured both in SSPFS, CS2M and NPM.

Table 1 SDM IP / CLLI / CM IP Configuration areas in CS2M/NPM (SN07)

Property	Component	Required	Command	Save in
SDM_IP	SESM	Required	configure	sesm.properties
SDM_IP	SAM21 EM	Required	cli (SSPFS)	/etc/profile
SDM_IP	NPM	N/A	N/A	N/A
CM_CLLI	SESM	Required	configure	sesm.properties
CM_CLLI	SAM21 EM	Optional (For GUI display)	cli (SSPFS)	/etc/profile
CM_CLLI	NPM	Required for PFRS	cli (SSPFS)	NPM Database
CM_IP	SESM	N/A	N/A	N/A
CM_IP	SAM21 EM	N/A	N/A	N/A
CM_IP	NPM	N/A	N/A	N/A

In SN07, For SESM application, the SDM IP and CLLI configuration are required for the communication between SESM and SDM/CBM/Core. User should run the command “**configure**” to set the SDM IP and CM CLLI to file **sesm.properties**.

In SN07, for SAM21 EM application, the SDM IP configuration by cli tool is required for the SAM21 EM server. The CM CLLI configuration is the optional one for displaying on the GUI of SAM21 EM. The SDM IP and CM CLLI configuration could be finished by **cli** tool.

In SN07, For NPM application, the step of configure CLLI is required for PFRS enable. The CLLI value is stored in the NPM database. User should run the command “**pfrsCli**” to enable the PFRS service as well as configure the CM CLLI to NPM database.

14.2.2 Feature Functionality

In the SN08 release, the robustness enhancement is implemented to improve the SDM IP/CM CLLI configuration and reusing for CS2M/IEMS server. This feature seeks to stop user to input CM CLLI manually and retrieve it by SDM IP automatically.

The SDM IP / CM CLLI will be set to /etc/profile as system environment variables during SSPFS installation process or by cli tool after SSPFS installation for each application reading and using. Each application will stop to reserve the entry for these two parameters.

14.2.2.1 SSPFS installation

In SN08, SSPFS will be changed to prompt the user to enter the SDM IP during SSPFS installation. CM CLLI is retrieved automatically from Core by SDM IP.

Whenever CLLI is retrieved successfully, SDM IP and CLLI will be set in the system environment file /etc/profile, which is easy access and read.

14.2.2.2 SSPFS cli tool

In cli tool, the command “sdm_conf” adds the function of SDM IP validation and CM CLLI retrieving automatically by SDM IP.

14.2.2.3 SESM configuration & starting up

1. Configuration

In SN08, SDM IP and CLLI duplicate configuration in SSPFS and SESM will be eliminated.

The SESM script *configure* is changed to stop to require for user to input SDM IP and CLLI manually. It will reuse the SDM IP and CM CLLI which are set as system environment variables in SSPFS level.

2. Starting up

SESM startup script will add a process to check whether SDM IP and CLLI are configured or not. If not, the SESM start up script will prompt user to configure the SDM IP & CM CLLI by *cli tool*. The start up process will fail.

14.2.2.4 SESM applications

SDM IP/CLLI related parameters are not provided in file sesm.properties any more. All related applications which retrieve these parameters transfer to retrieve them from system wide environment variables (in /etc/profile).

Parameters removed from sesm.properties/PTM.properties:

- ptm.base.cmcli=CMCLLI
- lmm.cmcli=CLLI
- ptm.cmcli.<CMCLLI>=<SDMIP>

Parameters removed from NetworkView.properties

- nv.callserver.name

14.2.2.5 SAM21 EM starting up

When SAM21 EM is starting up, in the case of SDM IP is configured but the CLI is NOT configured, it will retrieve CLI automatically by SDM IP and set it to /etc/profile. The starting up process will continue.

14.2.2.6 NPM configuration & starting up

In SN08, NPM will reuse the common configuration of CLI in file /etc/profile. It will stop user to input it manually when enabling PFRS.

14.2.2.7 CS2M Installation and Configuration

In SN08, User should not have to know to go run X configure steps to complete CS2M installation. The system should walk them through it, perhaps with the option of bypassing it to be done manually later.

14.2.2.8 Upgrading

The SSPFS upgrade & CS2M upgrade should transfer the CM_CLI and SDM IP settings from sesm.properties to /etc/profile smoothly.

14.3 Hardware Requirements or Dependencies

No new hardware or hardware dependencies are introduced.

14.4 Software Requirements or Dependencies

No new customer software or firmware dependencies are introduced in this feature.

14.5 Limitations and restrictions

No limitations or restrictions that is visible to any user are planned as part of this feature.

14.6 Interactions

No interactions between this feature and existing features.

14.7 Glossary

Term	Explanation
CS2M	CS2000 Management Components
SESM	Succession Element Sub-element Manager
SAM21 EM	CS2000 SAM21 Manager
NPM	Network Patch Manager

SSPFS	Succession Server Platform Foundation Software
CLLI	The coding system used to identify Central Offices uniquely, entered as a string not longer than 16 characters
SDM	SuperNode Data Manager

15: A00006635 Functional description (FN)

15.1 Feature name

Event Messaging Support on GWCEM

15.2 Description

In SN08, a new table NENDPT will be introduced to the Core which is used to map the gateway/endpoint with LEN in CM, which can be used to create the event messaging records that are sent to north bound OSS. In order to meet this, all the small gateways need to be pre-provisioned when they are associated to system.

15.2.1 Existing Functionality

Prior to SN08, only MG9K and CICM gateways have been pre-provisioned when the gateway is associated to the system. For small gateways ("C" LGRP type gateways), the endpoint in GWCEM and lens in the Core are populated/deleted by Line Provisioning when customer configure service for the gateway using NEW/OUT command.

On the other hand, Core has no knowledge about the mapping relationship of Lens and endpoint and gateways.

15.2.2 Feature Functionality

In SN08 release, the provisioning data will be added to CS2K from CS2M-SESM component. It is used to do the datafill of CM table LNENDPT. LNEDNPT is a new table for SN08, which is used to map gateway/endpoints and Lens in CM.

Cable gateways (small line gateways) will be pre-provisioned when the MG is associated to system, which means endpoints and Lens will be pre-populated in GWCEM and the Core during the MG addition period.

The general strategy is, for those Dqos gateways, generate endpoints in SESM and populate both LNINV and LNENDPT table in the Core; for other small line gateways, only populate endpoints and LNINV table.

Due to the pre-provisioning in SN08, the gateways which are associated to the system prior this feature need to be converted to populate endpoints and Lens, which means a upgrade process must be provided.

And since all the Lens pre-provisioned for small gateways have HASU status in LNINV table, it is necessary to provide a new interface for OSSGate to retrieve these HASU lens.

15.2.3 Node Provisioning

15.2.3.1 Associate MG

MG association requires an additional process to populate LNINV&LNENDPT in the Core and generate endpoints in GWCEM.

This functionality has no affect on CS2K GUI.

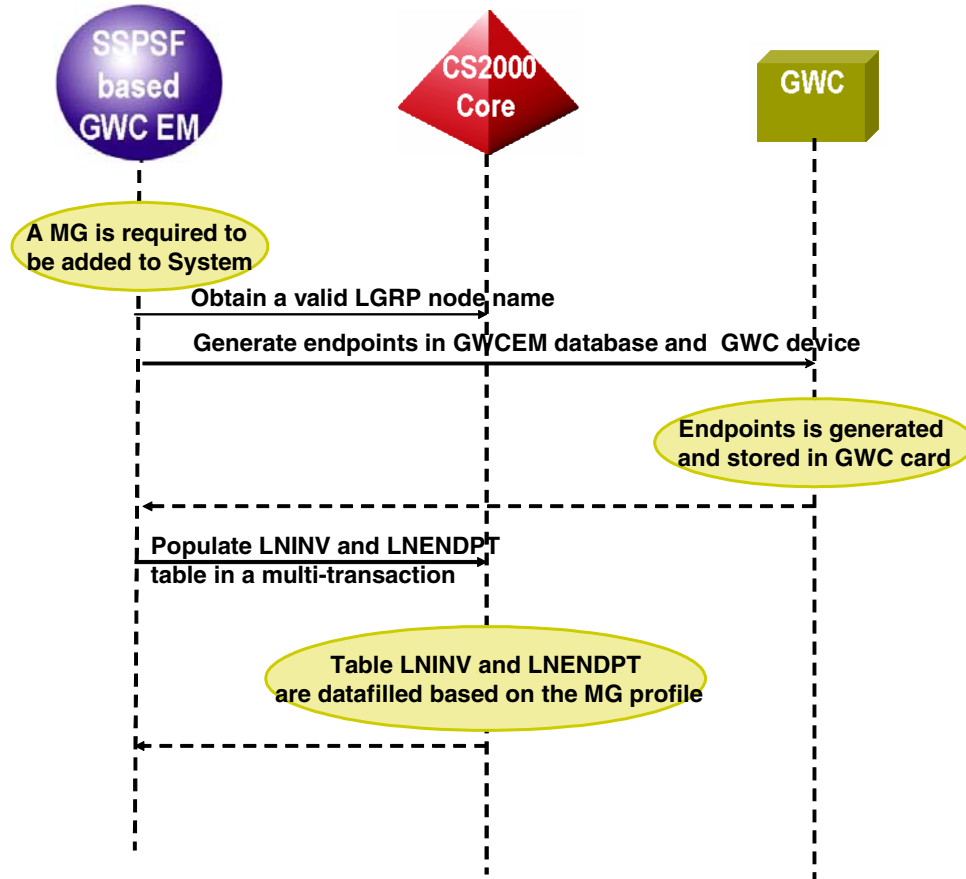
1. Cs2kCfgMgr receive the MG association request and verify whether it is a small line gateway.
2. If the MG request is a small line gateway, Cs2kCfg will retrieve the CCM layer version from the Core through XaCore. If the Core is upgraded to SN08, endpoints will be pre-provisioned in GWCEM and GWC Device, then LNINV table will be populated (LNENDPT is also populated as well if the MG is a Dqos gateway).
3. If the Core is still SN07 or before, the MG is added to system just like what was done in SN07.

Table 1 Table LNENDPT example datafill

TABLE: LNENDPT		
LEN	ENDPOINT	GATEWAY

LG 00 0 00 00	aaln/1	test_gw1.nortel.com
LG 00 0 00 01	aaln/2	test_gw1.nortel.com
LG 00 0 00 02	aaln/3	test_gw1.nortel.com
LG 00 0 00 03	aaln/4	test_gw1.nortel.com
LG 00 0 00 04	aaln/1	test_gw2.nortel.com
LG 00 0 00 05	aaln/2	test_gw2.nortel.com

Figure 1 GWCEM flow through for small line MG Association in SN08



15.2.3.2 Disassociate MG

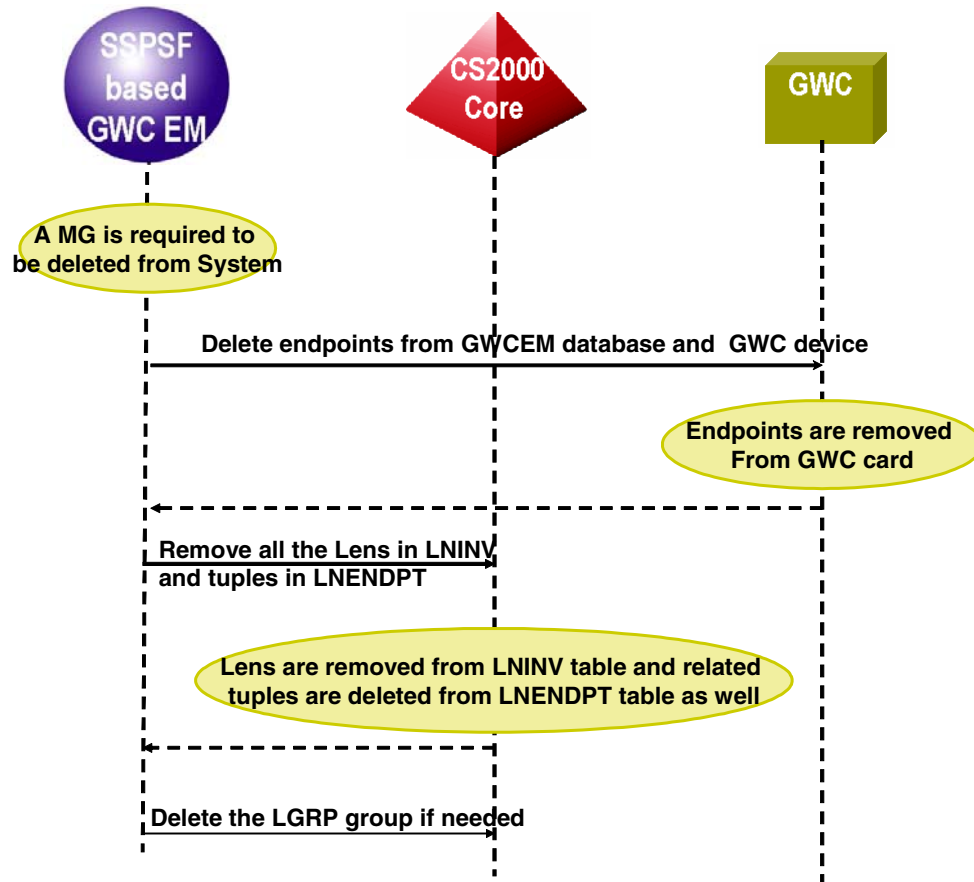
Cs2kCfgMgr will take different actions based on the Core CCM layer version when a delete MG request is arriving.

This functionality has no affect on CS2K GUI.

1. Before the request is performed, Cs2kCfgMgr will first retrieve the CCM layer version of the Core.
2. If Core is SN07 or before, the MG will be delete as it was in SN07, which means backward compatibility must be supported.
3. If the Core is upgraded to SN08, Lens will be first delete from the Core, then the endpoints in GWCEM will be deleted as well.

An automatic rollback will be done when the disassociateMG operation fails to rollback the lens and endpoints deleted before failure occurs. And an appropriate message like following will be returned to client.

Figure 2 GWCEM flow through for MG disassociation in SN08



15.2.3.3 Change MG

Only changing reserved endpoints capacity for a specific MG is affected by this functionality.

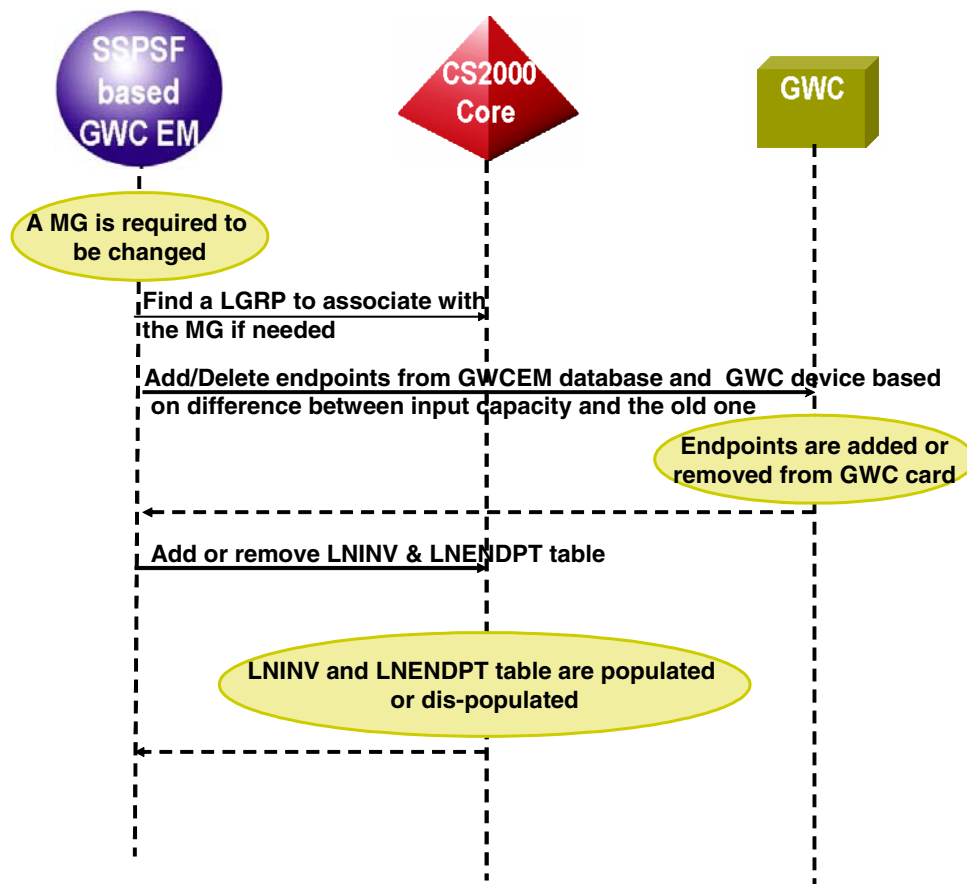
Again, CS2K GUI has not been affected for this functionality.

1. When a changing reserved endpoint request is arriving, Cs2kCfgMgr will first retrieve the Core CCM layer version and take corresponding action based on the CCM version.
2. If the Core is prior to SN07, the gateway will be changed just as what has been done in SN07.
3. If the Core is upgraded to SN08, the additional endpoint/lens will be populated if the input changed reserved capacity is larger than the prior one. Otherwise, some endpoints/lens will be delete.

The total amount of adding/deleting is equal to the difference between input capacity and the prior one.

And also, an automatic rollback process will be done once the changeMG operation fails. All the Lens and endpoints populated before failure occurs will be deleted and an appropriate message like following will be returned to client.

Figure 3 GWCEM flow through for changing MG in SN08



15.2.3.4 OSSGate enhancement

Since all the small line gateways will be pre-provisioned in SN08, the lens pre-populated in the Core should be in HASU status. So it is necessary to provide a interface for OSSGate to show the HASU lens so that customer can select one to configure service.

The detail request/response/error message will be defined later.

15.2.3.5 Node Provisioning Recovery

This functionality provides an activity to allow node provisioning to be recovered when a provisioning operation (Associate/Disassociate/Change MG) is abort or disrupted by a server switch over or crash.

The recovery can be running without user's participation and has no affect on GUI.

This functionality is running at the server side and has no affect on the CS2K GUI. And this activity will be finished automatically without customer's participating.

15.2.4 Upgrade

Due to the pre-provisioning for small line gateway, for those gateways which was added prior to SESM/Core upgrading to SN08, an automated upgrade process will be responsible for pre-provisioning LNINV and possibly LNENDPT tables in the XACore following the XACore upgrade.

This functionality has no affect on CS2K GUI. But probably a alarm will be raised if upgrade is failed or disturbed.

The alarm detail will be:

Alias Name: EventMessagingUpgrae
 Category: Processing Error
 Alarm Time: hh:mm:ss DD-MM-YYYY <TimeZone Info>
 Severity: Major
 Probable Cause: "Upgrade Failure"
 SpecificProblem: The Event Messaging Upgrade failed or has been interrupted

Notes:

In the case of following gateway upgrade or for gateways provisioned following the CS2K upgrade, the LEN may be used in OSSGate commands interchangeably with gateway/termination. Use of LEN will NOT cause data corruption as is currently documented in the OSSGate User's Guide.

Limitations:

Upgrade process probably last several hours to convert all the gateways in a large lab. During the upgrade period,

1. Conversion begins when CM completes upgrade to SN08 load. SESM detects upgrade and SN07 behavior for Lines Provisioning of Small MG's (C type LGRPs) is disabled and SN08 behavior commences. SN08 behavior requires LEN to be pre-populated in LNINV
2. New service requests or move service requests that include a LEN not yet populated in LNINV will fail. OSSGate will return SERVORD error message from the CM. Any Line Prov command that references an empty LNINV tuple fails. Line is not HASU in LNINV thus SERVORD fail.

The following error message indicating Lens is not existing might be returned to client if user attempt to execute NEW commands at upgrade time on a gateway which is not yet pre-provisioned.



3. A minor alarm will be provide to identify the conversion progress on a GWC basis. Alarm clears when conversion is completed.
4. Line Prov audit will be disabled to prevent delaying completion of the conversion and possibly erroneous results.
5. Node provisioning (change MG / Disassociate MG) will be block during the MG's converting. Following error message will be returned to client if user want to change/Disassociate a specific MG during this gateway upgrade.

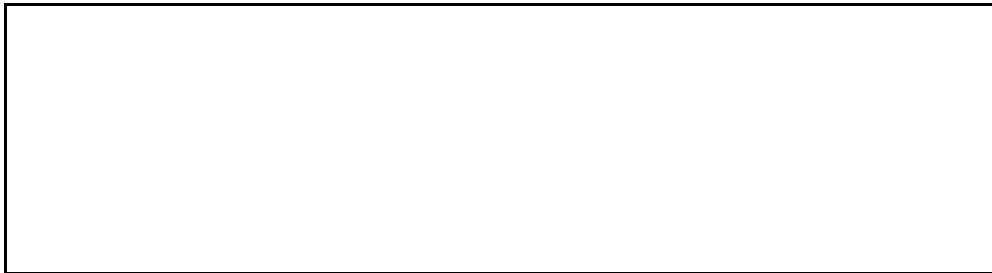
ChangeMG error message from OSSGate during upgrade

```
<?xml version="1.0" encoding="UTF-8" ?> <CommandList>
  <Response><Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <changeMG usn="1" version="1.0">
        <RC>20</RC><mgUIName>mg1.nortel.net</mgUIName>
        <MsgTxt> mg1.nortel.net Change MG Failed - The MG is under upgrade.Please try
again later.
        </MsgTxt>
      </changeMG>
    </Methods>
  </Response>
</CommandList>
```

DisassociateMG error message from OSSGate during upgrade

```
<?xml version="1.0" encoding="UTF-8" ?> <CommandList>
  <Response><Interface>cs2kCfgMgrlf</Interface>
  <Methods>
    <disAssocMG usn="1" version="1.0">
      <RC>20</RC><mgUIName>mg1.nortel.net</mgUIName>
      <MsgTxt> mg1.nortel.net DisAssocMG Failed - The MG is under upgrade.Please try
again later.
    </MsgTxt>
    </disAssocMG>
  </Methods>
</Response>
</CommandList>
```

The error message shown on GUI will be filled later.



15.2.5 Audit Enhancement

Prior to SN07, any HASU lens which LGRP type is “C” will be considered as an error. But in SN08, since all the “C” type LGRP gateways will be pre-provisioned, the case above is no longer an error. So Audit system must be enhanced to handle the case.

On the other hand, a new table LNENDPT has been introduced into SN08, which also needs audit to ensure that GWCEM keeps consistent with the Core.

The following error situation will be detected and corrected.

1. Endpoint exists in GWCEM but the corresponding Len is NOT existed in Core.

-
2. Lens exists in Core but the corresponding endpoint is NOT existed in GWCEM.

Note: The two scenarios above has already cover by current LineDataIntegrity Audit.

3. Endpoint exists in GWCEM but the corresponding tuple is NOT existed in LNENDPT table of Core.
4. The tuple exists in LNENDPT table but the corresponding endpoint is NOT existed in GWCEM.

During the process, audit will not raise the alarm, instead, the correct matched data will be logged into a report file, and the detected problem will be logged into another report file. The file will be loaded into a report shown on GUI when audit completes.

Limitations:

Line Audit will be disabled when upgrade is in progress. If a Line Audit is scheduled to start when the upgrade is running, a message like “Gateways upgrade is in progress. Please run Audit again later.” will be returned to client.

If the upgrade process finds that the Line Audit is running when it starts, it will sleep for a while and retry to restart until the Line Audit finishes.

15.3 Hardware Requirements or Dependencies

N/A.

15.4 Software Requirements or Dependencies

This feature requires SN08 XA-Core Load or later.

15.5 Limitations and restrictions

N/A.

15.6 Interactions

15.7 Glossary

16: A00006657 Functional description (FN)

16.1 Feature name

EADAS Trunk Group Buffer Expansion

16.2 Description

16.2.1 Introduction

Engineering and Administrative Data Acquisition System (Eadas) is an operational support system that provides near real time data collection and surveillance from many central offices. The Eadas package has two components, Eadas/DC (Data Collection) and Eadas/NM (Network Management). This activity deals with the Eadas/DC component.

Eadas/DC has three OM (operational measurements) classes, and each class is divided into 255 sections. Each section is defined by a set of OMs which collectively form the standard set. The standard set is defined by Telcordia for each software release.

16.2.2 Section Buffer Expansion

The report and accumulation for each section is stored in an internal buffer. In the case of section 112, this buffer size is not adequately large enough to support the number of trunk groups (TG) required by the customer. The current limit for this section is 727 TGs.

This activity will alter the internal memory architecture to support up to 1024 TGs so that it's consistent with TR-746 requirement. This increase will apply to all 255 sections.

16.3 Hardware Requirements or Dependencies

None.

The data store used by Eadas will be consistent with the amount used before this feature.

16.4 Software Requirements or Dependencies

None.

16.5 Limitations and restrictions

None.

16.6 Interactions

This activity does not alter HMI.

16.7 Glossary

Term	Description
EADAS	Engineering and Administrative Data Acquisition System.
EADAS/DC	EADAS/Data Collection.
EADAS/NM	EADAS/Network Management.
HMI	Human Machine Interface
OM	Operational Measurements
TG	Trunk Group

17: A00006659 Functional description (FN)

17.1 Feature name

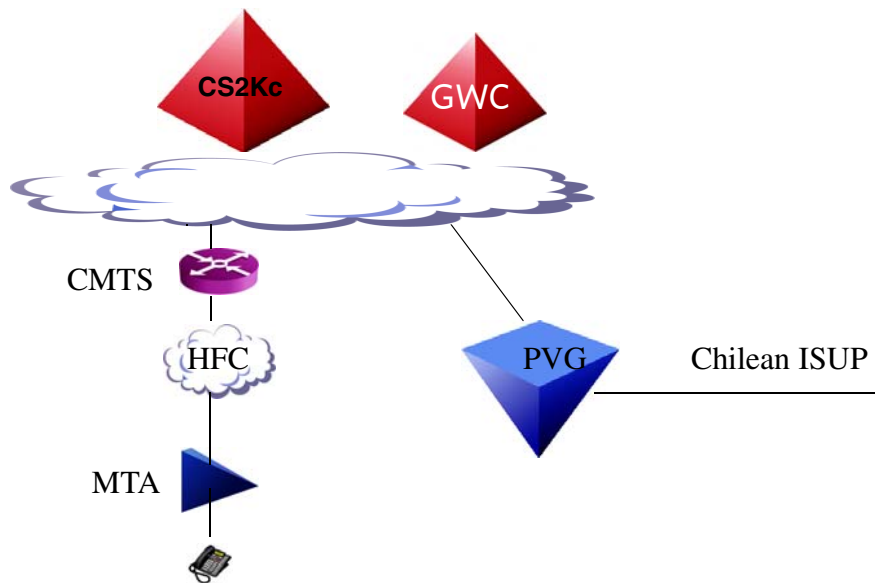
Distinctive Call Waiting Ringback and Line Reversal via NCS

17.2 Description

Call Waiting Ringback service has been implemented on TDM side, but on IP side, the standard ring back tone is played to caller due to distinctive call waiting tone is not supported by NCS at present. This feature targets to support the Distinctive Call Waiting Ringback (CWR) on succession CS2Kc for both line to line (NCS-based only) and trunk to line calls (Chilean ISUP only).

From a CM perspective, the function and operation of line reversal (line reversal on answer and line reversal on seizure) and cut off disconnect services are the same as with legacy DMS systems. This feature implements the package definition and signal mapping of the line reversal and cut off disconnect for NCS protocol.

The network topology is shown below.



17.2.1 Distinctive Call Waiting Ringback Tone

In a call waiting scenario, when the third party is trying to call the termination which has call waiting (CWT) and call waiting ringback (CWR) options, a

distinctive call waiting ringback tone is applied to the calling party to indicate the called party has call waiting and is currently involved in a call.

In a line to line call, the Distinctive Ringback Tone is provided by the MTA where the calling party phone set is connected, by instructing it to apply *sst/cw* signal. So the MTA must support NCS *sst* package, or else GWC would instruct the MTA to play ordinary ringback tone with *rt* signal. NCS *sst* is a new package and it is possible that some MTA doesn't support it, to achieve so the MTA must be upgraded. And during the system upgrade, GWC is upgraded prior to the MTA so there is still a period of time *sst* is not utilized.

In a trunk (Chilean ISUP) to line call the Distinctive Ringback Tone is provided by the PVG where the incoming trunk is connected, by instructing it to apply *cg/cr* signal. So the PVG must support MEGACO (H.248) *cg* package. This has been covered by A00002365 in SN07.

When the Distinctive Ringback Tone is applied to calling party, there is not timeout mechanism to the tone (i.e. infinite), which is compliant with today's TDM side CWR behavior.

17.2.2 Line Reversal on Answer and Line Reversal on Seizure

If line option LROA is added to the line, line reversal signal *XAL/rev(+)* is applied to the MTA of this line that is calling when the called party answers the call, so that the polarity of this line is reversed. When the call ends line reversal back signal *XAL/rev(-)* is applied to get the polarity back to normal.

If line option LRS is added to the line, line reversal signal *XAL/rev(+)* is applied to the MTA of this line that is being called to mark this line is seized, so that the polarity of this line is reversed. When the called party line answers line reversal back signal *XAL/rev(-)* is applied to get the polarity back to normal.

If *XAL* package is not supported by the gateway however *x-XL* is, *x-XL/rev(+)* and *x-XL/rev(-)* are used. If *x-XL* is not supported either, GWC doesn't instruct the gateway to perform line reversal. NCS *XAL* is a new package and it is possible that some MTA doesn't support it, to achieve so the MTA must be upgraded. And during the system upgrade, GWC is upgraded prior to the MTA so there is still a period of time *XAL* is not utilized.

17.3 Hardware Requirements or Dependencies

For distinctive call waiting ringback tone, the MTA must support NCS *sst* package, or else GWC would instruct the MTA to play ordinary ringback tone with *rt* signal as a compatible alternative (at least some ringback tone is applied to the calling party). For line reversal on answer/seizure, the MTA must support NCS *XAL* and/or *x-XL* package. And the MTA must support audit endpoint capabilities methods of the NCS protocol to report to the GWC that it does support the *XAL* and/or *x-XL* and *sst* package.

The PVG must support MEGACO (H.248) *cg* package.

Note: At present, the Arris MTA doesn't support NCS package SST and XAL.

17.4 Software Requirements or Dependencies

N/A

17.5 Limitations and restrictions

This feature is not required to and understood that it will not work on DPT calls.

17.6 Interactions

N/A

17.7 Glossary

Term	Description
NCS	Network Call Signalling
GWC	Gateway Controller
CMTS	Cable Modem Termination System
MTA	Multimedia Terminal Adaptor
HFC	Hybrid Fiber Coaxial
PVG	Passport Voice Gateway
CWT	Call Waiting
CWR	Call Waiting Ringback

18: A00006693 Functional description (FN)

18.1 Feature name

XA-Core IO Capacity Monitoring Toolset

18.2 Description

The IO Capacity monitoring toolset (IOCAP) provides the customer telemetry for messaging over HIOP and HCMIC.

XA-Core counts messages and bytes for each service. Software on the XA-Core accesses the measurements, calculates the messaging occupancy level, and displays the results on the IOCAP MAPCI level and the IOCAP OM group.

This feature will cause no more than 3% capacity degradation in IO capacity.

18.2.1 IOCAP MAPCI display

Following is a prototype of the IOCAP MAPCI display, which will subtend from the CAPACITY level. The display will be updated once per minute.

CATMP/HR	SMS/HR	VLR_UPD/HR	CAP	ENGBHCA	CCOVRD	CMICOVRD	PESC
303001	180	398700	128	233643	OFF	OFF	NO

Service	IOUTIL%	TxMsg/s	TxSize	RxMsg/s	RxSize
ETHR	64	15324	107	13234	91
CMIC	17	4102	202	1254	102
AMDI	0	0	0	0	0

The Service column identifies the type of IO service (Ethernet, CMIC, or AMDI). IOUTIL is the calculated percentage utilization of the available system messaging capacity, based on the known IO system capacity, the average rate through other services on the same card, and the throughput on other cards. TxMsg/s, TxSize, RxMsg/s and RxSize report average transmit and receive message rates and sizes through that service. Because the MAPCI display is updated once per minute, high water mark information will not be displayed.

18.2.2 IOCAPCI tool

The information in the MAP display is also available through the IOCAPCI tool, in addition to the following tools:

- one month's history of hourly high water mark percent utilization for each service (Ethernet, CMIC, and AMDI), similar to DMSMON HIGHCAP.
- one month's history of hourly average percent utilization for each service.

- current hour and last hour utilization and throughput for each service

An example of the CMIC high water mark data follows. A similar output will be available for each service.

```
> iomax cmic
Maximum CMIC Utilization
```

Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
2/2	8	7	9	10	4	5	9	12	16	21	27	29	39	49	53	43	51	56	57	61	57	41	29	18
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8	7	8	10	8	9	7																	
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

18.2.3 IO capacity OM

The information displayed in the IOCAP MAP command is also recorded in the IOCAP operational measurement, as shown below.

IOCAP

CLASS: HOLDING

START:2003/12/03 09:30:00 WED; STOP: 2003/12/03 09:45:00 WED;

SLOWSAMPLES: 9 ; FASTSAMPLES: 90 ;

INFO (IO_SERVICE_TYPE)

	IOUTIL	IOHWM	TXMSGPS	TXSIZE
	RXMSGPS	RXSIZE	IOTHRESH	
1 ETHR				
	64	72	15204	105
	13234	84	0	

2	CMIC	17	18	1254	102
		1254	63	0	
3	AMDI	0	0	0	0
		0	0	0	

The IOCAP OM provides measurements of messaging rates and sizes for each service. The IO_SERVICE_TYPE indicates the service provided. IOUTIL refers to percentage utilization of the services on the switch. IOHWM refers to the highest level that the corresponding utilization has reached in the sample period. TXMSGPS, TxSIZE, RXMSGPS and RxSIZE report the average transmit and receive message rates and sizes through the service. The IOTHRESH register is pegged every time the service average utilization for one minute exceeds the value of new OFCENG office parameter IO_WARNING_THRESHOLD. This register is intended to give the customer a flexible warning that they are approaching the need to upgrade their IO system.

18.2.4 Office parameter

A new office parameter in table OFCENG, IO_WARNING_THRESHOLD, indicates the minimum IO service utilization at which the IOTHRESH register in the IOCAP OM will be pegged.

18.3 Hardware Requirements or Dependencies

This feature is unavailable for CMIC, Ethernet and AMDI packets (NTLX05AB, NTLX09AA, NTLX05BA respectively).

This feature is supported on all versions of NTLX04 HIOP cards and NTLX17 HCMIC cards.

18.4 Software Requirements or Dependencies

None.

18.5 Limitations and restrictions

This feature will be submitted into CSP21 and patched back to CSP20.

When the system is in transition from IOP to HIOP, the utilization of all IO services will not be available.

18.6 Interactions

The MAPCI level display will sub tend from the CAPACITY MAP level. It will be shown as an option from that level.

18.7 Applicable customer facing sections

Fault Management

Logs ☐ NA ☐

Alarms ☐ NA ☐

Configuration

Data Schema ☐ NA ☐

User Interface ☐ X ☐

Element Management ☐ NA ☐

Security ☐ NA ☐

Service Order ☐ NA ☐

Office Parameters ☐ X ☐

Accounting (includes AMA billing) ☐ NA ☐

Performance (includes operational measurements) ☐ X ☐

18.8 Glossary

Table 1

Term	Description
New term	Definition

19: A00006731 Functional description (FN)

19.1 Feature name

Handle Flash on Exit

19.2 Description

On TMX100 switches, hook flash is only enabled on those RES lines that have flash features assigned. Most customers do not use flash features. RES customers without hook flash features who flash are treated as exiting the current call and receive standard dial tone allowing them to initiate a new call.

When TMX100 sites migrate to ISN04 or later, customers are converted from RES to IBN line functionality and by default have hook flash enabled and will get second dial tone if they Flash (go on/off hook) instead of Exit. This difference in behavior is causing confusion and customer complaints at the Coteor site in Bolivia, the first local exchange migrating from TMX100 to ISN04. Similar complaints are expected when other sites convert (100-150 sites).

The purpose of the Exit on Flash (EOF) option is to resolve these customer complaints and to provide for a more seamless migration from TMX100 to ISN04.

Customer requirement of this activity is to develop a new line option that treats Flash as EXIT for IBN lines.

Without EOF:

- A Calls B
- B Answers
- A Flashes
- A gets Special Dial Tone
- A Calls C
- A Receives Feature Not Allowed (FNAL) treatment

With EOF:

- A has EOF option
- A Calls B
- B Answers
- A Flashes
- A and B Disconnect

A gets Dial Tone
A calls C
A to C call is established

This feature uses line option datafill. The advantages of offering this as a line option are:

- consistency with the current FIG (Flash IIgnore) option
- ability to define option compatibilities using OPTOPT table

19.3 Hardware Requirements or Dependencies

There is no hardware dependency. The option can be added to any line with an LCC of IBN.

19.4 Software Requirements or Dependencies

None.

19.5 Limitations and restrictions

EOF feature is only applicable to IBN lines in NA and WT.

EOF feature is not compatible with the following options:

CHD, CNF, CWI, CWX, CWT, CXR, FXR, DCBX, HLD, LDSA, LDSO, LDSR, LDST, LNPTST, MPB, PCWT, PRK, 3WC, 3WCPUB, VOWDN.

19.6 Interactions

CWO and CWD compatible with EOF feature. If another agent imposes CWT on an agent with EOF, this agent still has the ability to flash to the waiting call and maintain the original call.

A has EOF option
A Calls B
B Answers
C with CWO/CWD calls A and imposes CWT on A
A Flashes
A to C call established while B is on hold
A flashes again and A to B call established while C is on hold

19.7 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) ☐

20: A00006756 Functional description (FN)

20.1 Feature name

NSSwitch Implementation in IEMS

20.2 Introduction

This document explains how NSSwitch (Name Service Switch) can be implemented in IEMS. This document covers the following:

- A brief description about the proposed design for NSS implementation in IEMS with a workflow chart
- NSS implementation details
- Major work items involved
- New C APIs that are to be added
- Changes on the client side

Basically, NSSwitch is a standard used in all Unix flavor operating systems, founded by Sun Micro Systems. The OS uses a number of databases of information about hosts, users (passwd/shadow), groups etc., Data for these hostnames and addresses may be found in /etc/hosts,NIS,NIS+ or dNS. Supporting NSSwitch enables IEMS as NSSwitch complaint.

20.3 Overview of the NSSwitch Design

The following list depicts the workflow of the implementation of the method “isAuthorized”.

- 1 Request comes in to the Authorization Engine.
- 2 Gets all the groups for the user through NSSwitch. Here, just a call of the URL will return the required data.
- 3 For each group, gets the authorized operations from the Database through Relational classes.
- 4 Applies Security Policy and returns the result.

- 5 For Admin user who wants to create a new user, first authorization check is done (as to whether he is authorized to create a new user).
- 6 If the admin user has got the permission, he directly invokes the AdminAPI and creates a new user. Here NSSwitch API will not be invoked.

20.4 Overview of the NSSwitch Implementation

The following list depicts NSSwitch implementation details in IEMS.

- 1 The call getGroup comes from AuthEngine API.
- 2 AuthEngine invokes the Https URL and gets the result regarding Group Information.
- 3 The Servlet calls the **PamPlus.java** which contains the native call for getpwnam(), getgrnam(). (This part is already done.)
- 4 NSSwitch SPI will be invoked since this entry is given in the *nsswitch.conf*. This SPI will contact the Security Server through socket.
- 5 The Security Server gets data from the Security DB through RelationalAPI and returns back to the AuthEngine.

20.5 Major Work Involved

Two new Tables PLATFORMUSERDETAILS, PLATFORMGROUPDETAILS have to be created with detailed information about users and groups. These two tables will contain all the information of */etc/passwd*, */etc/shadow*, */etc/group* files.

Schema for the new tables will look like following:

PLATFORMUSERDETAILS:

S.N o	COLUMN_NAME	DATA_TYPE	PRIMARY_KEY	REMARKS
1	USERNAME	VARCHAR2	YES	
2	USER_UID	NUMBER		
3	GROUP_GID	NUMBER		Primary Group ID, It should be any one of the value from PLATFORMGROUPDETAILS.GROUP_GID
4	GECOS	VARCHER2		
5	HOME_DIR	VARCHER2		
6	LOGIN_SHELL	VARCHER2		

7	LAST_CHANGE	NUMBER		
8	MIN	NUMBER		
9	WARN	NUMBER		
10	INACTIVE	NUMBER		

PLATFORMGROUPDETAILS:

S.No	COLUMN_NAME	DATA_TYPE	PRIMARY_KEY	REMARKS
1	GROUPNAME	VARCHAR2	YES	
2	GROUP_GID	NUMBER		
3	GROUPPASSWORD	VARCHAR2		NOT USED.

20.6 C API implementation:

The following apis needs to be implemented as part of this operation.

/etc/passwd:

- 1 struct passwd *getpwnam(const char *name);
- 2 struct passwd *getpwnam_r(const char *name, struct passwd *pwd, char *buffer, int buflen);
- 3 struct passwd *getpwent(void);
- 4 struct passwd *getpwent_r(struct passwd *pwd, char *buffer, int buflen);
- 5 struct passwd *getpwuid(uid_t uid);
- 6 struct passwd *getpwuid_r(uid_t uid, struct passwd *pwd, char *buffer, int buflen);
- 7 void setpwent(void);
- 8 void endpwent(void);

/etc/shadow:

- 1 struct spwd *getspnam(const char *name);
- 2 struct spwd *getspnam_r(const char *name, struct spwd *result, char *buffer, int buflen);
- 3 struct spwd *getspent(void);
- 4 struct spwd *getspent_r(struct spwd *result, char *buffer, int buflen);
- 5 void setspent(void);

```
6 void endspent(void);
```

/etc/group:

```
1 struct group *getgrnam(const char *name);
2 struct group *getgrnam_r(const char *name, struct group *grp, char
  *buffer, int bufsize);
3 struct group *getgrent(void);
4 struct group *getgrent_r(struct group *grp, char *buffer, int bufsize);
5 struct group *getgrgid(gid_t gid);
6 struct group *getgrgid_r(gid_t gid, struct group *grp, char *buffer, int
  bufsize);
7 void setgrent(void);
8 void endgrent(void);
9 getgroupsbymember();
```

20.6.1 Sample result of some of the new APIs:

The `getpwnam(char* username)` will return a structure. This structure will contain following data from the new table.

S.No	Structure Variable	Definition	Data
1	char *pw_name	user's login name	The incoming argument <OR> <i>PLATFORMUSERDETAILS.USERNAME</i>
2	char *pw_passwd	no longer used	Empty String
3	uid_t pw_uid	user's uid	<i>PLATFORMUSERDETAILS.USER_UID</i>
4	gid_t pw_gid	user's gid	<i>PLATFORMUSERDETAILS.GROUP_GID</i>
5	char *pw_gecos	typically user's full name	<i>PLATFORMUSERDETAILS.GECOS</i>
6	char *pw_dir	user's home dir	<i>PLATFORMUSERDETAILS.HOME_DIR</i>
7	char *pw_shell	user's login shell	<i>PLATFORMUSERDETAILS.LOGIN_SHELL</i>

Result for getsppnam(char* username) is tabulated below

S.No	Structure Variable	Definition	Data
1	char *sp_namp	login name	The incoming argument <OR> <i>PLATFORMUSERDETAILS.USERNAME</i>
2	char *sp_pwdp	encrypted passwd	UserPasswordTable.PASSWORD
3	long sp_lstchg	date of last change	<i>PLATFORMUSERDETAILS.LAST_CHANGE</i>
4	long sp_min	min days to passwd change	<i>PLATFORMUSERDETAILS.MIN</i>
5	long sp_max	max days to passwd change	<i>UserConfTable.PASSWORDAGE</i>
6	long sp_warn	warning period	<i>PLATFORMUSERDETAILS.WARN</i>
7	long sp_inact	max days inactive	<i>PLATFORMUSERDETAILS.INACTIVE</i>
8	long sp_expire	account expiry date	<i>UserConfTable.USERAGE</i>
9	unsigned long sp_flag	not used	(Integer ZERO) 0

Result for getgrnam(char* name) is tabulated below:

S.No	Structure Variable	Definition	Data
1	char *gr_name	the name of the group	The incoming argument <OR> <i>PLATFORMGROUPDETAILS.GROUPNAME</i>
2	char *gr_passwd	the encrypted group password	<i>PLATFORMGROUPDETAILS.GROUPPASSWORD</i>

3	gid_t gr_gid	the numerical group ID	<i>PLATFORMGROUPDETAILS.GROUP_GID</i>
4	char **gr_mem	vector of pointers to member names	Achieved through our implementation.

20.6.2 Client Side Changes

In the Security UI, we changed the createUser wizard such that the wizard will prompt for additional User Attributes. A few additional attributes specific to each user are obtained from the IEMS Client GUI. The list of additional attributes is as follows.

- a** gecost - Descriptive text field which contains information about the user.
- b** min - The minimum number of days required between password changes(default=1).
- c** warn - The number of days before the password expires that the user is warned(default=7).
- d** inactive - The number of days of inactivity allowed for each user after which the account will be disabled(default=0).
- e** Login Shell - The login shell that will be invoked after a successful login. User has two options (a) no-access (b) restricted. Currently '/usr/bin/nash' is populated if no-access option is chosen and '/bin/sh' is populated if restricted option is chosen. The default value is 'no-access'.

Note: Changes will be made to show UID,GID & LOGINSHELL

The following is a screen shot provided to enter the additional User attributes in the Add User Wizard. This screen can be invoked from the 3rd screen of the Add User Wizard, by clicking on the “Advanced” Button. If the user does not click on this button, or no operation is performed on this GUI, default values for these fields will be populated in the database.

The screenshot shows a Java Application Window titled "ScreenTitle". Inside the window, there is a section titled "Additional Details" which contains several input fields and a "Login Shell" section. The fields are:

- Gcos**: A text input field.
- Min (days)**: A text input field with the value "1".
- Inactive (days)**: A text input field with the value "7".
- Warn (days)**: A text input field with the value "7".
- Login Shell**: A section with two radio buttons: ☒ **no-access** and ☐ **restricted**.
- Expiry**: A text field showing "Sun, 8 Aug 2004".

Below these fields, there is a large text area with the instruction: "Please enter the user's real Name in this field (Mr. Foo Boo)". At the bottom right of the window, there are two buttons: "OK" and "Cancel".

The default values given for each of the above fields is configurable. The default values which can be provided currently are present in the following location: `IEMSHOME/conf/defaultUserAttribute.prop`. The format of this file is as below.

Currently the file contents are as follows.

Security Default Values. The values for the following 5 should be integers

MIN=1

WARN=7

INACTIVE=0

PASSWORDAGE=30

ACCOUNTAGE=0

LOGIN_SHELL can have noaccess/restricted for other values the behavior is undefined

LOGIN_SHELL=noaccess

Changes done in this file will be reflected in the IEMS Client GUI after the client is restarted successfully.

20.6.3 Modifying the attributes of a User

The additional attributes of each user can be modified from the IEMS Client GUI. To modify the user attributes, please perform the following steps.

- 1** Invoke the Security Administration GUI by clicking on Tools->SecurityAdministration (or) Alt+S keys.
- 2** All the users will be listed under the “Users” Node in the Tree.
- 3** Click on the user for whom the user attributes has to be modified.
- 4** Click on the “User Profile” tab on the right hand side of the user list tree.
- 5** Click on the “Setting Profile” button on this panel, a panel which has user attributes will be popped up.
- 6** Click on the “Advanced” Button in this panel to view the additional properties of the user. After modifying the attributes, click on the OK button to modify the additional user attributes.

20.6.4 Password Complexity

Password complexity is a set of rules based on which passwords for users are set. The main objective behind this feature is to make a password complex while assigning a password for a user. The rules are as follows.

- Each password shall have a minimum number of characters(default=6)
- Each password shall have a maximum number of characters(default=256)
- Each password shall have at least 3 types of characters
 - lowercase characters(default=1)
 - uppercase characters(default=1)
 - numbers(default=1)
 - special characters(default=0)
- Password shall not be the same as login id of the user.
- While changing a user's password he shall re-use his old password.
- Special characters should be configurable by the administrator.

20.6.5 Configuring the default values for Password complexity values

The default values provided above are present in the following file. IEMSHOME/conf/defaultUserAttribute.prop. The format of this file is as explained above.

```
PASSWD_MIN_LENGTH=6
PASSWD_MAX_LENGTH=256
LOWERCASE_COUNT=1
UPPERCASE_COUNT=1
SPECIAL_CHAR_COUNT=0
NUMBER_COUNT=1
SPECIAL_CHARS=`~!@#$%^&*()-_+=[]{}\\|;:'",<.>/?`
```

If the administrator needs to change the above default values it can be changed from the above file.

20.7 Upgrade Process.

The process of using a revised version of software after using an old version is called the Upgrade process. First the software will be upgraded and then old data will be migrated to the new version. Migration should be manually initiated by the user.

Procedure to invoke the migration script. To migrate the data from SN07 to SN07.1 please follow the steps given below.

- 1 cd /opt/nortel/iems/current/bin
- 2 sh migrationTool.sh UPGRADE
- 3 The above command will migrate the data from SN07 to SN07.1
- 4 Now start the IEMS server

Order of migration

- 1 Add Succession 25 groups
- 2 Migrate list of groups created in IEMS in SN07 with GID & empty password
- 3 Migrate list of users created in IEMS including iemsadm,guest

During IEMS Server start up, all the succession 25 groups will be added to the IEMS database. Then all the operations relevant to these groups will be added to IEMS DB from the SuccessionGroupInfo.xml file. After this operation

IEMS will migrate the list of groups created in IEMS along with enumerated GID. Now the users created in IEMS will be migrated with primary group ID as successn.

20.8 Succession 25 group-Operations Mapping

The following table contains the initial mapping of groups & their corresponding mapping permission these operations are provided below.

Brief description of **Succession 25 groups Domains**.

<i>Domains</i>	<i>Application Mapping</i>
Trk	Trunks, trunk based services, small trunking gateways (port level), carrier, carrier based services.
Ln	Line services, line cards, small line gateways.
Mgc	Media Gateway Controllers: CS2K, GWC, SAM21, 3PC, Storm...
Mg	Media gateways: UAS, Line Gateways, Trunk Gateways.
Ems	SSPFS based EMSs, GWCEM, SAM21EM, UASEM, etc.

Brief Description of **Succession 25 group Roles**

<i>Roles</i>	<i>Application Mapping</i>
Adm	Reconfiguration, access to all functions, setup of fundamental configuration, can commission (add/deletet/rehome) base frames/ systems (SAM21 frames, Call servers, large gateways), can run service impacting diagnostics.
Rw	Can see and change configuration and status, can commission and reconfigure elements (GWCs, cards, shelves). Also called improv, for infrastructure provisioning.
Sprov	Subscriber provisioning; can see status and configuration and change provisioning data, but cannot change mtc state or do base component configuration.
Mtc	Maintenance role can see configuration and status, can make changes to status,can run service impacting diagnostics
Ro	The "read only" role can see configuration and status, but cannot make changes to them

It is available as below.

Operation/ Groups	em sad m	em sr w	em ss pro v	em sm tc	em sro	mg ad m	mg rw	mg spro v	mg mtc	mg ro	mg cad m	mg cr w	mg csp rov	mg cmtc	mg cro	ln ad m	ln r w	ln sp rov	ln mtc	ln ro	tr kad m	tr kr w	tr ks pro v	tr kmtc	tr kro
User Admin- istration	TRUE					FALSE					FALSE					FALSE					FALSE				
User Config- uration	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Add Users	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Assign User To Group	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Remove Us- ers	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Remove User from From Group	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Change Pass- word	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE

Get List of Users	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Set User Permission	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Set User Profile	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Clear Audit Trails	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Alerts	TRUE					TRUE					TRUE					TRUE					TRUE			
Alter Filters	TRUE					TRUE					TRUE					TRUE					TRUE			
Get Alert Filters	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Set Alert Filters	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE
Alert User Operations	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE

Set Alert An-notation	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E
Get Alert De-tails	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E
Save Alerts To File	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E
Print Alert View	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E
Clear Alerts	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E
Get Alert An-notation	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E
Get Alert History	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E
Alert Pickup	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E
Delete Alerts	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E

Maps	T R U E	T R U E	T R U E			T R U E	T R U E	T R U E			T R U E	T R U E	T R U E			T R U E	T R U E	T R U E			T R U E	T R U E	T R U E		
Map Editing Operations	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E
Threshold Object	T R U E	T R U E	T R U E			T R U E	T R U E	T R U E			T R U E	T R U E	T R U E			T R U E	T R U E	T R U E			T R U E	T R U E	T R U E		
Add Threshold Object	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E
Modify Threshold Object	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E
Delete Threshold Object	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E
Get Threshold Objects	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E
Events	T R U E	T R U E				T R U E	T R U E				T R U E	T R U E				T R U E	T R U E				T R U E	T R U E			
Event Filters	T R U E	T R U E				T R U E	T R U E				T R U E	T R U E				T R U E	T R U E				T R U E	T R U E			

Get Event Filters	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	T R U E	
Set Event Filters	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	
Event User Operations	T R U E	T R U E				T R U E	T R U E				T R U E	T R U E				T R U E	T R U E				T R U E	T R U E			
Save Events To File	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E
Print Event View	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E
Event Clean-up	T R U E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	
Administrative Operation	T R U E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	T R U E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	
Configure Log Levels	T R U E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	
Runtime Administration	T R U E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	

System Administration	T R U E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E
Northbound Configuration	T R U E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E
NTSTD NB Config	T R U E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E
SCC2 NB Config	T R U E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E
SNMP NB Config	T R U E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E
Security Administration	T R U E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E
Group Operations	T R U E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E
Add Group	T R U E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E	F A L S E

Add Job	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E
Delete Job	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E
Topology	T R U E	T R U E				T R U E	T R U E				T R U E	T R U E				T R U E	T R U E				T R U E	T R U E			
Modify Ob- ject	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E	T R U E	T R U E	T R U E	F A L S E	F A L S E
Manage And Unmanage Objects	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E
Add Node	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E
Delete Ob- ject	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E	T R U E	T R U E	F A L S E	F A L S E	F A L S E
Dump Inven- tory Details	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E	T R U E	T R U E	T R U E	T R U E	F A L S E

TRUE -> Indicates that the operation is allowed to the group

FALSE -> Indicates that the operation is not allowed to the group

BLANK FIELD denotes that it is not allowed by the child operation may allow

or disallow

Operations and permission settings are done as part of the IEMS migration process. The user **will not be able to set any operation/permission from the IEMS Client GUI. The succession groups is non modifiable & non deletable groups.**

20.9 Procedure to add a group to existing succession 25 groups.

- 1 Invoke the IEMS Client GUI.
- 2 Add a group using the Add group Wizard [Provision to enter/modify GID will be provided].
- 3 Then add the groupname along with its group id in the successiongroups.prop present in IEMSHOME/conf/ directory.
- 4 The group name and id should be added to the file in the following format.
- 5 groupname=GID

20.10 Adding a group name and group id to a reserved list.

This provision helps the user to stop adding a group which is already available in group datasource other than IEMS.

- 1 Edit the file in IEMSHOME/conf/reservedgroups.prop
- 2 Add the reserved groupname in this file in the following format:
reservedgroupname=GID

Configurable group ID Range can be given in NmsProcessesBE.conf present in IEMSHOME/conf directory, as an argument to Security Process as groupIDRange 12001-14000

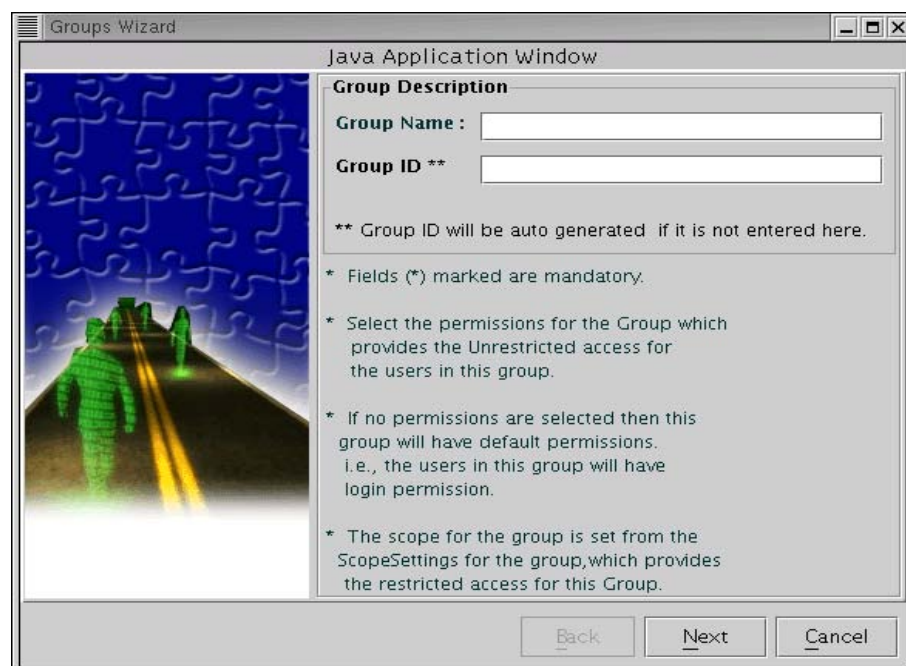
20.11 Group ID support

While adding a group the customer has the option to provide a group ID. If this field is left blank then a group ID will be selected from the configurable range provided by the user. The configurable values can be given in the file /opt/nortel/iems/current/conf/NmsProcessesBE.conf.

The contents of this file will be as below.

```
#java com.adventnet.security.authentication.SecurityProcess
PROCESS com.adventnet.security.authentication.SecurityProcess
ARGS SecurityServerPort 7777 maximum_allowed_login_failed_count 0
userIdRange 10001-12000 groupIdRange 12001-14000
```

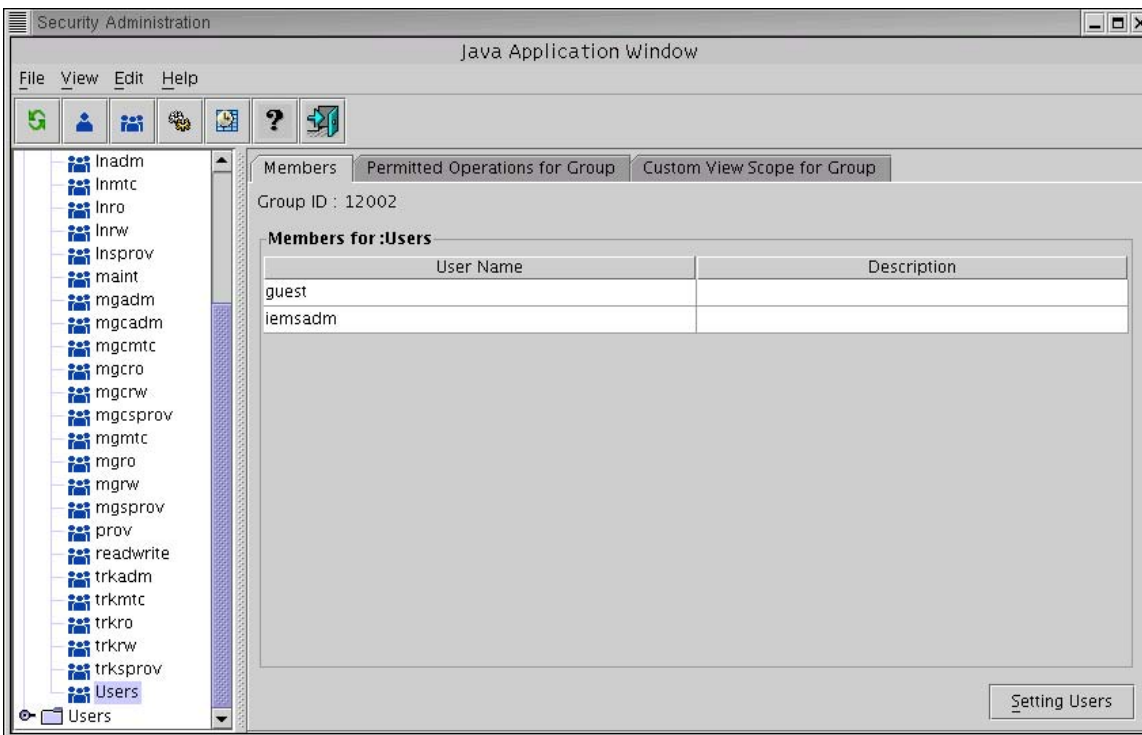
The text given in bold shows the configurable range of group ID's that can be provided by the user. In this configurable range the lower limit is 12001 & the upper limit is 14000. The user can change these values according to their requirements. During group ID enumeration the values will be chosen from this range. The following is a screen shot added to show the group id in IEMS Security Client.



If the number of groups is equal to the range specified in IEMSHOME/NmsProcessesBE.conf then error message stating that the GID range has exhausted will be logged to nmserr.txt file.

To view the group id

The group ID for each user can be viewed in IEMS Security Client. To view a group id in IEMS Security Client, click on a group name in IEMS Security Client Tree. In the right hand side, click on the Members tab. The screen shot below shows the group id of a selected group "Users".



20.12 Conclusion

With the above specifications and design, we can implement NSSwitch support in IEMS.

20.13 Device Vs. Domain

S.No	Device Type	Auth. Domain
1	APS Mgr	EMS
2	CS2K Core Mgr	EMS
3	CEM Mgr	EMS
4	MCS Mgr	EMS
5	GWC Mgr	EMS
6	MG9K Mgr	EMS
7	MG9K	MG
8	Preside MDM	EMS
9	SAM21	MGC
10	SAM21Mgr(shelf Controller)	EMS

11	IEMS Mgr	EMS
12	USP	MG
13	PP8600	MGC
14	MS2000	MG
15	STORM	MGC
16	MAS	MG
17	Session Server	MGC
18	CICM	MG
19	CICM EM	EMS
20	MDM Platform	EMS
21	SSPFS	EMS
22	LMM	LN
23	TMM	TRK
24	OSSGate	LN, TRK, MG
25	NPM	EMS
26	QOS Collector	EMS
27	Call Agent Core	MGC
28	Call Agent Plat	MGC
29	CS2K XA-Core	MGC
30	SDM	EMS
31	CBM	EMS

20.14 Operation Description

Following table describes the operations name with their explanation.

Configure Log Levels	This operation can be used to set the logging and the corresponding levels for various modules in the Integrated EMS Server.
Runtime Administration	This operation is a powerful tool to configure the Integrated EMS Server settings from the Integrated EMS without a need for the user to restart the server for the new settings to take effect.

SystemAdministration	This Operation is the entry point all the Administrative operations.
Security Administration	Security Management is about authenticating a user from logging into Integrated EMS to providing permissions to perform operations.
Northbound Configuration	This operation will enable to set/get Northbound configuration devices using NTSTD,SCC2,SNMP
User Configuration	This operation is used to obtain the link for User Administration.
Add Users	This operation is used to create a new user.
Assign User To Group	This operation is used to assign the user to a new or existing group.
Remove Users	This operation is used to remove the whole account for a particular user.
Remove User From Group	This operation is used to remove the particular user from a particular group only.
Change Password	This operation is used to change the existing password for a particular user.
Get List of Users	This operation is used to view the list of users present in the database.
Set Users Permission	This operation is used to sets operations or permissions for the existing users.
Set User Profile	This operation is used to set profiles for the existing users.
Clear Audit Trails	This operation is used for clearing audit trails for the user.
Add Threshold Object	This operation is used to create a new Threshold Object to create Threshold Events for a new device or the existing device.
Modify Threshold Object	This operation is used to modify the existing Threshold Object for making performance analysis better.
Delete Threshold Object	This operation is used to remove the existing Threshold Object.
Get Threshold Object	This operation is used to view the particular Threshold Object.
Manage and Unmanage Objects	This operation is used to set the management status of the particular object at run time.
Add Node	This operation is for adding a new node in the topology.

Delete Object	This operation is for removing a particular object from the topology.
Dump Inventory Details	This operation is used to collect the list of discovered devices from the topo database and print them in a text file.
Map Editing Operations	This operation is mainly used to configure the maps, such as creation of new maps, customization of map hierarchy, map symbol layout, and map symbol renderers through the Integrated EMS.
Get Event Filters	This operation is for viewing the Event Filters present in the server.
Set Event Filters	This operation is for modifying existing Event Filters or creating a new Event Filter.
Save Events To File	This operation is for saving the selected events or the events displayed in the Events Panel.
Print Event View	This operation is for printing either the selected events or events displayed in the Events Panel.
Event Cleanup	This Operation will cleanup all the events in the datastore
Get Alert Filters	This operation is for viewing the Alert Filters present in the Server.
Set Alert Filters	This operation is for modifying existing Alert Filters or for creating new Alert Filter
Set Alert Annotation	This operation is for adding notes (annotation) to an alarm.
Get Alert Details	This operation is for viewing the details of a particular alarm.
Save Alerts To File	This operation is for saving either the selected alarms or the alarms displayed in the current Alarm Panel into a file.
Print Alert View	This operation is for printing either the selected alarms or the alarms displayed in the current Alarm Panel.
Clear Alerts	This operation is for changing the Alarm Severity to Clear.
Get Alert Annotation	This operation is for viewing a particular existing alarm annotation.
Get Alert History	This operation is for viewing the alarm history, that is, the change in status of an alarm from the first alarm to the latest alarm.

Alert Pickup	This operation is used to pick up the alarm. (specify person or allocate resources to handle it)
Delete Alarms	This operation is used to remove a particular alarm, which is of no interest or has been resolved.
Add Job	This operation is for creating a new job.
Delete Job	This operation is for removing an existing job from the system.

21: A00006757 Functional description (FN)

21.1 Feature name

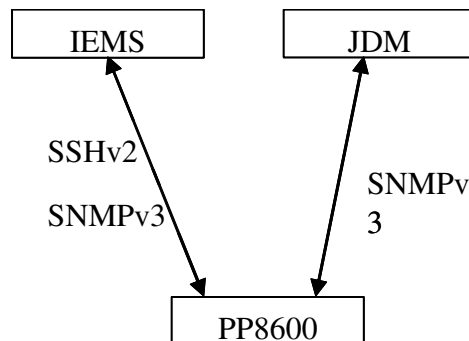
IEMS Secure Launch to PP8600

21.2 Description

This feature defines security measures to be applied to communications between Succession management applications and the Passport 8600 Routing Switch.

The management applications include IEMS and the PP8600 graphical configuration and management tool known as the Java Device Manager (JDM).

All communications between OAM applications and the PP8600 must be authenticated and encrypted. The means for doing this are provided by SNMPv3 and SSHv2.



Configuration is required for all three objects in the diagram above. The bulk of the configuration is in the PP8600. It must be completed before the configuration of IEMS or JDM is performed. There is no interaction between IEMS and JDM, hence, the configuration of one is independent of the other.

21.3 Configure the PP8600

The following configuration steps must be performed on the PP8600. This is accomplished by using telnet to log in to the PP8600 configuration console. If the PP8600 is contained in a VLAN, telnet must be performed from a workstation that has access. The IEMS Server would be a logical choice.

The default userid/password is “rwa/rwa”

```
> telnet 47.142.126.223
```

```
*****
* Copyright (c) 2004 Nortel Networks, Inc.      *
* All Rights Reserved                          *
* Passport 8010                                *
* Software Release 3.7.0.0                      *
*****
```

```
Login: rwa
```

```
Password: ***
```

The Software Release level must be 3.7 or greater. After successful login the prompt will appear.

```
PP8600:5#
```

The string shown as a prefix (in this case, PP8600) is the mib-2 object, SNMPv2-MIB::sysName.0. It can be changed with the command,

```
config cli prompt <new-prompt>
```

Entering a question mark (?) will display a list of commands that are available at the current context. It will also display a list of sub-contexts that can be entered via the sub-context name. This is akin to traversing a hierarchy of commands.

The command info will display the state of current context and list the available sub-contexts. The state of a context is a list of attributes and corresponding values.

Configuration is done via the config context. Enter the context name.

```
PP8600:5# config
```

The prompt will change to

```
PP8600:5/config#
```

21.3.1 Notes on shell cursor movement and editing

- Left and Right arrow keys will move the cursor backward and forward on command line.
- Up and Down arrow keys move backward and forward in the command stack

- Ctrl-a moves the cursor to beginning of command line
- Ctrl-e moves the cursor to end of command line
- Ctrl-h is a destructive backspace. The Backspace key does nothing.
- You are always in insert mode.
- Ctrl-d is passed to telnet/ssh and will the close session

21.3.2 Load Encryption Modules

From the `config` context, enter the commands,

```
load-encryption-module DES
load-encryption-module 3DES
```

Encryption modules must be loaded onto the PP8600 flash using ftp or tftp or by use of PCMCIA slot. Refer to the applicable installation guide for Passport 8600 Routing Switch.

If the DES encryption module is not available then SNMPv3 –USM can not be configured. This means that authenticated and encrypted communications between Succession OAM applications and the PP8600 will not be available. SNMP communications will only be via

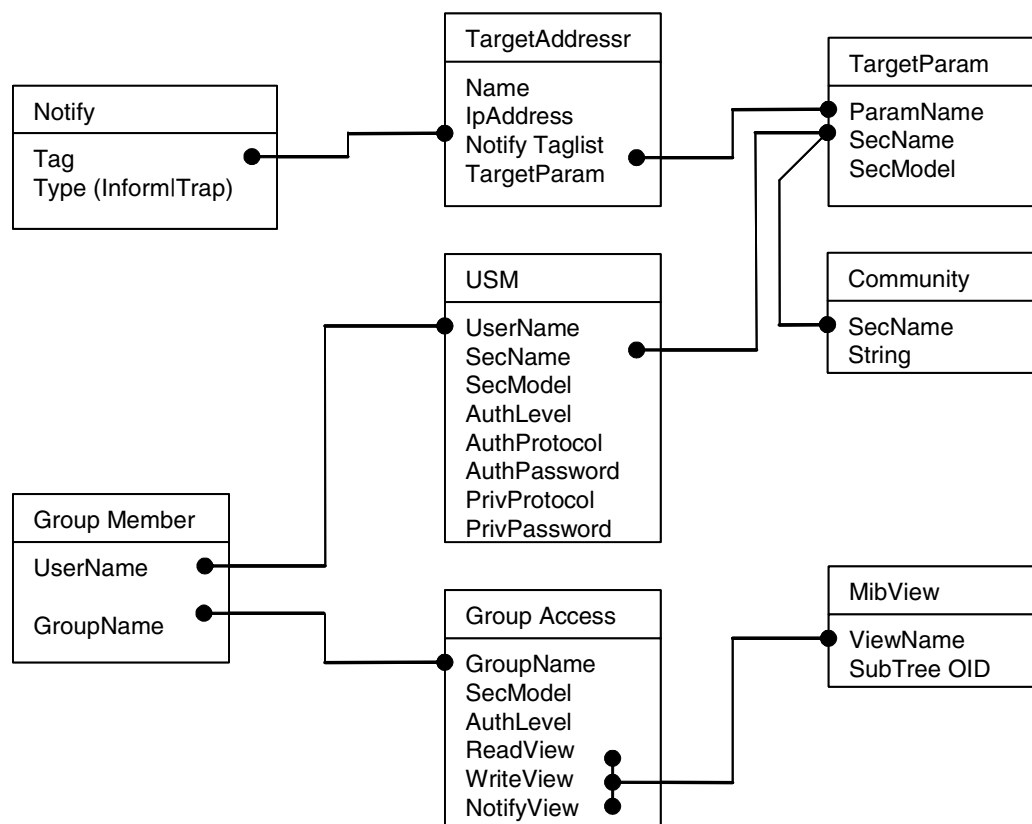
If the Triple DES (3DES) encryption module is not available then SSH can not be configured. Telnet will be the only available communications protocol for accessing the PP8600 command line.

21.3.3 SNMPv3 Tables

The following tables are used to configure SNMPv3 authentication and privacy.

- **USM** table defines users, authentication/privacy protocols, and passwords.
- **Group-Member** table defines which groups each USM user belongs to
- **Group-Access** table defines the access rights each user has to the objects in the MIB tree.
- **Notify** table defines the types of notifications (TRAP or INFORM) that are sent.
- **Target-Parm** table defines which USM user will receive a notification.
- **Target-Address** table defines the network managers that receive notifications. Each row denotes a unique manager. It will have 1 or more references into the Notify table to determine which notification type. It will also have a 1 reference into Target-Parm table to determine the user credentials used to send the notification.

- **Community Table** contains the Read and Write community strings for SNMPv1/v2c. Note that the Target-Param table references the Community Table for the purposes of sending v1/v2c traps.



21.3.4 Configure SNMP-v3

Change into the `snmp-v3` context by entering context name. The new prompt will display as,

```
PP8600:5/config/snmp-v3#
```

- 1 Add users `iems` and `jdm`. We create a different user for each application so that a password change made using the JDM will not break the IEMS application. SNMPv3-USM uses an authentication protocol and password and also a privacy protocol and password. Entering the command the command syntax is,

```
usm create <user> <auth_prot> auth <pw1> priv <pw2>
```

where `<auth_prot>` is one of: `sha` | `md5`

Enter the commands,

```
usm create iems sha auth iemspass1 priv iemspass2
usm create jdm sha auth jdmpass1 priv jdmpass2
```

will create the 2 users: `iems` and `jdm` with:

- authentication protocol of SHA-1 and authentication password of `iemspass1` and `jdmpass1`
- privacy password of `iemspass2` and `jdmpass2`. The privacy encryption protocol is DES. This is the only one supported by the PP8600.

The information above should be noted as it will be used to configure both the IEMS and JDM.

Attribute	Value
User Name	<code>iems</code>
Authentication Protocol	<code>sha</code>
Authentication Password	<user specified>
Privacy Protocol	DES (only allowed value on PP8600)
Privacy Password	<user specified>

Enter the command, `usm info`, to display the current context. It should look like,

User/Sec Name	Engine Id	Protocol
<code>iems</code>	800008E00300E07BA7B400	HMAC_SHA, DES PRIVACY
<code>initial</code>	800008E00300E07BA7B400	NO AUTH, NO PRIVACY
<code>jdm</code>	800008E00300E07BA7B400	HMAC_SHA, DES PRIVACY

The user name `initial` is a pre-configured value for SNMPv1.

- 2 Add user `iems` to `vacm`. This will create a group `iemsgrp` and add the users `iems` and `jdm` to it.

The command syntax is,

```
group-member create <user_name> <model> <group_name>
```

where <model> is one of: `snmpv1` | `snmpv2c` | `usm`

Enter the commands,

```
group-member create iems usm iemsgrp
```

```
group-member create jdm usm iemsgrp
```

3 Now create an access control list for the iemsgrp.

The empty double quoted string is the context name. This is equivalent to a null context. It is not used and not supported by the PP8600.

The command syntax is,

```
group-access create <group_name> <prefix> <model>
<level>
```

where:

<model> is one of: snmpv1 | snmpv2c | usm

<level> is one of: noAuthNoPriv | authNoPriv |
authPriv

Enter the command,

```
group-access create iemsgrp "" usm authPriv
```

Note that the <prefix> is saved as the context name but is not use in the current level of firmware.

4 Finally indicate the branches of the mib tree that iemsgrp is allowed to access.

The command syntax is,

```
group-access view <group_name> <prefix> <level> read
<view_name> write <view_name> notify <view_name>
```

Enter the command,

```
group-access view iemsgrp "" usm authPriv read org
write org notify org
```

Values for <view_name> can be see with the command,

```
mib-view info
```

These define which part of the mib tree can be accessed. The value org specifies every object under the prefix .iso.org.

5 Add/verify the available notification types. There should be two pre-configured types. These can not be altered or deleted and is sufficient for our needs. Enter the command, `notify info` and the Notify Table should display as,

Notify Name	Tag	Type
Inform	informTag	inform
Trap	trapTag	trap

If this is not correct add the information via,

The command syntax is,

```
notify create <notify_name> tag <value> type <type>
```

where:

<type> is one of: trap | inform

Enter the commands,

```
notify create tag Inform informTag type inform
```

```
notify create tag Trap trapTag type trap
```

6 Add target address for traps. First we must add an entry into target-param,

The command syntax is,

```
target-param create <tparam_name> mp-model <value>
sec-level <value> sec-name <value>
```

where the value for:

mp-model is one of: snmpv1 | snmpv2c | usm

sec_level is one of: noAuthNoPriv | authNoPriv |
authPriv

sec-name is the usm user entered in step 1. --
either iems or jdm

Enter the commands,

```
target-param create TparamV3iems mp-model usm sec-
level authPriv sec-name iems
```

```
target-param create TparamV3jdm mp-model usm sec-
level authPriv sec-name jdm
```

This will create a new row in the table with name TparmsV3iems referencing our iems user in the USM table. Enter the command, target-param info and the table should display as,

Target Name	MP Model	Security Name	Sec Level
TparamV1	snmpv1	readview	noAuthNoPriv
TparamV2	snmpv2c	readview	noAuthNoPriv
TparamV3iems	usm	iems	authPriv
TparamV3jdm	usm	jdm	authPriv

TparamV1 and TparamV2 are pre-configured default entries for SNMP v1 and v2c. They should not be deleted.

7 Add the ip-address of the IEMS that will receive our traps. Repeat for each IEMS.

The command syntax is,

```
target-add create <target_name> <ip_addr>
<target_parm> taglist <value>
```

Enter the command,

```
target-addr create bumrot 47.142.94.68:162
TparamV3iems taglist trapTag
```

...or...

```
target-addr create bumrot 47.142.94.68:162
TparamV3jdm taglist trapTag
```

This will create an entry for,

- a host called bumrot. This is an arbitrary string and does not match the real host name. ERS8600 will not use a DNS to resolve the ip-address.
- The ip-address to receive the trap.
- A reference to the user who receive the trap at the specified ip-address. This is designated via the target-parm name of TparamV3iems TparmV3jdm.
- A reference to the kind of notification to be sent. This is designated via the notify name of trapTag and points back to the Notify Table we verified earlier.

Note that the <ip_addr> is the primary key in this table. A trap can be sent to only one user (one target_parm) on the specified address, i.e., one can not issue

both of the commands listed above. The second will elicit an error indicating a duplicate ip address.

If SNMP v1/v2c traps are being configured enter the command above but specify either TparamV1 or TparamV2 as the <target_parm>. For example,

```
target-addr create bumrot 47.142.94.68:162 TparamV1
taglist      trapTag
```

21.3.5 Enable SSH

Enter the `config` sub-context. From the `config/snmp-v3` sub-context you can enter the context name, `config`, to jump to the correct context or enter a single period (.) to move up one context level. The new prompt will display as,

```
PP8600:5/config#
```

Enter the following command,

```
bootconfig flags sshd true
sys set ssh action dsa-keygen 1024
sys set ssh action rsa-keygen 1024
sys set ssh enable
```

21.3.6 Disable Non-secure Services

From the `config` sub-context, enter the following commands,

```
bootconfig flags ftpd      false
bootconfig flags tftpd     false
bootconfig flags rlogind   false
web-server disable
```

We also want to disable telnet but not just yet.

21.3.7 Verify SSH is working and Disable telnet

Log in using SSH and from the `config` sub-context enter,

```
bootconfig flags telnetd false
save bootconfig
```

21.3.8 1.2.1.8Disable SNMPv1/v2c

Access via SNMPv1 and v2c is controlled using community strings. From the `config/snmp-v3` context enter the command, `community info`, to display the current table. The pre-configured values for public and private community names are contained in the Security Names readview and initialview respectively. The column designated as, `name`, is the community name string

and is shown as a list of asterisks. The pre-configured values are “public” and “private”.

Index	Name	Security Name	Transport Tag

first	*****	readview	
second	*****	initialview	

The PP8600 does not allow pre-configured values to be deleted in most tables. It does not allow either row shown above to be deleted. It does, however, allow the Name field to be changed. We can change the public community string to some real long value, but the PP8600 would be subject to brute force attacks as the community name string is part of the SNMP PDU.

Alternatively, if we alter the Security Name field we can effectively disable SNMPv1/v2c. The Security Name field is used to access the GroupMember table to determine authority to access various elements of the MIB tree. To change the sec-name enter the commands,

```
snmp-v3 community secname first new-secname was
readview

snmp-v3 community secname second new-secname
was_initialview
```

Now all v1/v2c get and set requests will fail VACM access checks due an inability to find the Security Name in the GroupMember table. The PP8600 is not subject to brute force attacks as the Security Name is not included in the SNMP PDU.

21.3.9 Change default SNMPv1 community strings

The read and write community name strings of public and private are trivial and well know and must be changed. From the config/snmp-v3 context enter the command, community info, to display the current table. The pre-configured values for public and private community names are contained in the Security Names readview and initialview respectively. The column designated as, name, is the community name string and is shown as a list of asterisks.

Index	Name	Security Name	Transport Tag

first	*****	readview	

```
second          *****          initialview
```

To change community strings enter the commands,

```
community commname first new-commname <publicvalue>
community commname second new-commname <privatevalue>
```

21.3.10 Change the login passwords

Passwords are changed via the configuration context,

```
cli password
```

It is recommended that the passwords for the rwa and rw, at a minimum, be changed. Enter the commands and follow the prompts.

```
cli password rw rw
cli password rwa rwa
```

21.3.11 Save the configuration

Enter the following commands,

```
save bootconfig
save config
```

21.4 Configure JDM

Start the JDM. The following dialog will appear. Enter a host name or IP-Address in the “Device Name” field and select the “v3 Enabled” checkbox. The Read and Write Community names are not used with SNMPv3. Fill in all SNMPv3 fields using the same information used to create the SNMPv3-USM user in step 1 of Configure SNMP-v3.

This includes:

```
UserName:                      jdm
Authentication Protocol: SHA-96
Authentication Password: jdmpass1
Privacy Protocol:              DES
Privacy Password:              jdmpass2
```

Device Manager 5.8.0.0 - Open Device

Device Name: 47.142.126.223

Read Community: *****

Write Community: *****

SNMPv3

☒ v3 Enabled

User Name: jdm

Authentication Protocol: SHA-96

Authentication Password: *****

Privacy Protocol: DES

Privacy Password: *****

Open Ping... Telnet... Close

Depress the “Open” key and the device should be displayed.

21.5 Configure IEMS Manage Object

Start the IEMS client. Create a Network Element manage object. This is a 3 page dialog. Fill in the first page with IP Address, a Type of NE, the PP8600 Device Type and Device Version.

Java Application Window

Press the “Next” button to move to page 2 and fill in the information for receiving faults. Specify the SNMP version as “v3” from the combo box and enter the V3 Security Details using the same information used to create the SNMPv3-USM user in step 1 of Configure SNMP-v3. The Security Level should be specified as “AuthPriv”. The Context name field is not used by the PP8600 and can be left blank.

The screenshot shows a Java Application Window titled "Add EMS,NE". The window contains two main sections: "SNMP Details" and "V3 Security Details".

SNMP Details:

- Port: 161
- Community: (empty field)
- Version: v3 (dropdown menu)

V3 Security Details:

- Security Level: AuthPriv (dropdown menu)
- User name: iems
- Context name: (empty field)
- Auth Protocol: SHA (dropdown menu)
- Auth Password: (masked with asterisks)
- Privacy Protocol: CBC-DES
- Privacy Password: (masked with asterisks)

At the bottom of the window, there are four buttons: "Back", "Next", "Help", and "Cancel". Below these buttons is a green bar with the "Add" button. The status bar at the bottom indicates "Java Application Window".

Press the “Next” button to move to page 3 and fill in the information for receiving performance data. Specify the SNMP version as “v3” from the combo box and enter the V3 Security Details using the same information used to create the SNMPv3-USM user in step 1 of Configure SNMP-v3. The Security Level should be specified as “AuthPriv”. The Context name field is not used by the PP8600 and can be left blank.

Add EMS,NE

Performance Interface

SNMP Details

Port: 161

Community:

Version: v3

V3 Security Details

Security Level: AuthPriv

User name: iems Context name: x

Auth Protocol: SHA Auth Password: *****

Privacy Protocol: CBC-DES Privacy Password: *****

Back Finish Help Cancel

Add

Java Application Window

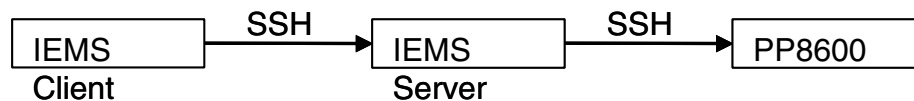
Press the “Finish” button to complete the creation. IEMS will discover the device and update the map.

21.6 Configure IEMS Command Line Launch to PP8600

The PP8600 configuration console we used, via telnet, in Configure SNMP-v3, can be accessed via the IEMS Map.

In SN07 the IEMS Client creates an SSH session with the IEMS Server. The IEMS Server acts as proxy and forwards the connection, using telnet, to the PP8600.

In SN08 the PP8600 will enable the SSH protocol and disable the telnet protocol. The second connection from IEMS Server to PP8600 will change from telnet to SSH.



The first time a client using an SSH application (such as MindTerm) connects to another host, that host will send a public key to the client. The client will be asked if they would like to accept the key. The message may alternatively ask if this host should be added to the set of known hosts on the client machine. Failure to respond affirmatively will cancel the connection.

Because there are two SSH connections it is possible that two prompts will be displayed -- one for each SSH session. This will occur anytime the server changes the public/private keypair; which is seldom. Note that the public key from the IEMS Server will be saved onto the client's machine. The public key from the PP8600 will be saved onto the IEMS Server in the file

21.7 Hardware Requirements or Dependencies

None

21.8 Software Requirements or Dependencies

- 1 The Passport 8600 must be running v3.7 of the microcode and both the DES and 3DES encryption modules (p80c3700.des, p80c3700.img) should be present in flash.
- 2 The JDM should be version 5.8 or later.

21.9 Limitations

None

21.10 Interactions

None

21.11 References

- Important Security Information for the 8000 Series Switch
- Passport 8600 Software Release 3.7 – Configuring Network Management
- Passport 8600 Software Release 3.7 – Configuring and Managing Security
- Configuring SNMPv3 on the Passport 8600 (version 1.0 - April 2003)
- <http://www142.nortelnetworks.com/bvdoc/setips/july03/csx8600snmpv3con.pdf>
- Nortel web site <http://worcester.us.nortel.com/Products/p8600/>
- “SNMP, SNMPv2, SNMPv3, and RMON 1 and 2”, 3rd Edition by William Stallings
- Security Features of SNMPv3
- <http://www.simple-times.org/pub/simple-times/issues/5-1.html#operations>

21.12 Glossary

Term	Description
3DES	Triple DES
DES	Data Encryption Standard
JDM	Java Device Manager
MAC	Message Authentication Code
MD5	Message Digest (version 5)
PP8600	Passport 8600 Routing Switch
SHA-1	Secure Hash Algorithm (version 1)
SNMP	Simple Network Management Protocol
SSH	Secure Shell
USM	User-based Security Model
VACM	View-based Access Control Model

22: A00006759 Functional description (FN)

22.1 Feature name

Secure Launch of MDM X11 Client Application

22.2 Introduction

MDM Client applications which are available in MDM Server can be launched in local machine via X11 protocol. This mean of communication needs to be secured via SSHTunneling/Port Forwarding. This document explains the functional details of X11 Port Forwarding for MDM in IEMS.

22.3 X11 Port Forwarding

Application from remote server will communicate to X11 server running on local client machine via SSH Tunnel which has already been established between the client and the server. The ssh server, running on the remote server machine forwards display of X clients to the ssh client, running on local client machine. The ssh client will inturn forwards the display content to the X server on local client machine.

22.4 X11 Port Forwarding For MDM

The X11 Port forwarding for MDM Client application is achieved using MindTerm tool. The MindTerm tool provides a secure session with x11 port forwarding parameter as true. This will enable a secure X11 communication for MDM Client Application/MDM Gui Launches.

The X11 Port forwarding requires Xserver needs to be run in the local client machine. In the case of solaris/linux, Xserver runs by default and in the case of Windows, Hummingbird's Exceed is used as Xserver.

The steps to launch a MDM Client Application involves,

- 1 Click on MDM ManagedObject's MenuItem - "MDM Mgr GUI", which will launch a "NortelMDMGUILauncher" dialog.
- 2 Now in the dialog, XServer's(Exceed) path has to be provided in the case of Windows OS Only.
- 3 The MDM Centralized Account - username/password will be automatically filled and these fields will not be editable.
(Use "ChangeMDMCentralizedAccount" - Managed Object menu item to change the same.)
- 4 MDM Client application(say *nmstool*) which needs to be launched, has to be provided in Command field.

- 5 Now clicking on "Execute" button will execute Exceed (in the case of Windows) followed by launching the MDM Client Application.

Please refer [usecase](#) to see with snapshots.

The actual mechanism involves is that, Mindterm creates a ssh client by establishing a ssh tunnel with the ssh server running in MDM Manager Device. It provides a secure *ssh session* with DISPLAY variable set, where in the MDM Client Application is launched.

After successful execution, the mentioned MDM Client Application (say *nmstool*) is only visible. Exiting MDM Application will terminate both the application and the ssh session with MDM Manager Device.

For unsuccessful execution of invalid client application (given in Command field), the ssh session will be simply terminated.

22.5 Testing Considerations

- 1 Launching MDM Client Application in Linux, Windows and Solaris systems.
- 2 Test the launch functionality after changing the MDM Manager settings like Client-Server IP Provisioning, MDM Centralized Account etc.
- 3 Usability Testings- NortelMDMGUILauncher dialog

22.6 UseCase

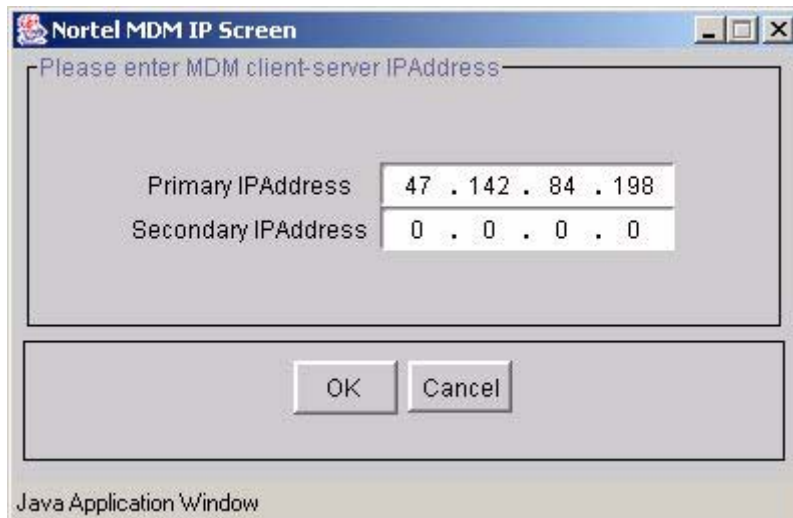
The procedure to provision the client server ipaddress and launch the MDM Manager are as follows:

22.6.1 Provisioning client-server IP address for MDM Manager

To provision a client-server IP address for MDM object in Integrated EMS, follow these steps:

At Integrated EMS workstation

- Launch the Integrated EMS Java Web Start Client
- Select the **Element Managers** topology node in the Integrated EMS tree.
- Select the required **MDM** map symbol in the Integrated EMS display panel.
- Right-click the map symbol and select the **Client-Server IP provisioning** menu item. The system displays a window similar to the following figure.



- Enter the MDM Client-Server primary IP address in the **Primary IP Address** field. The primary ipaddress is that which is configured during adding the MDM device in the “simplex” mode in the Integrated EMS.
- Enter the MDM Client-Server secondary IP address in the **Secondary IP Address** field. The secondary ipaddress is configured when adding a MDM device in the “duplex” mode in the Integrated EMS.
- Click the **OK** button.

Note: The above steps must be carried out only once.

22.6.2 Launching MDM Manager for MDM

To launch MDM Manager GUI for MDM, follow these steps:

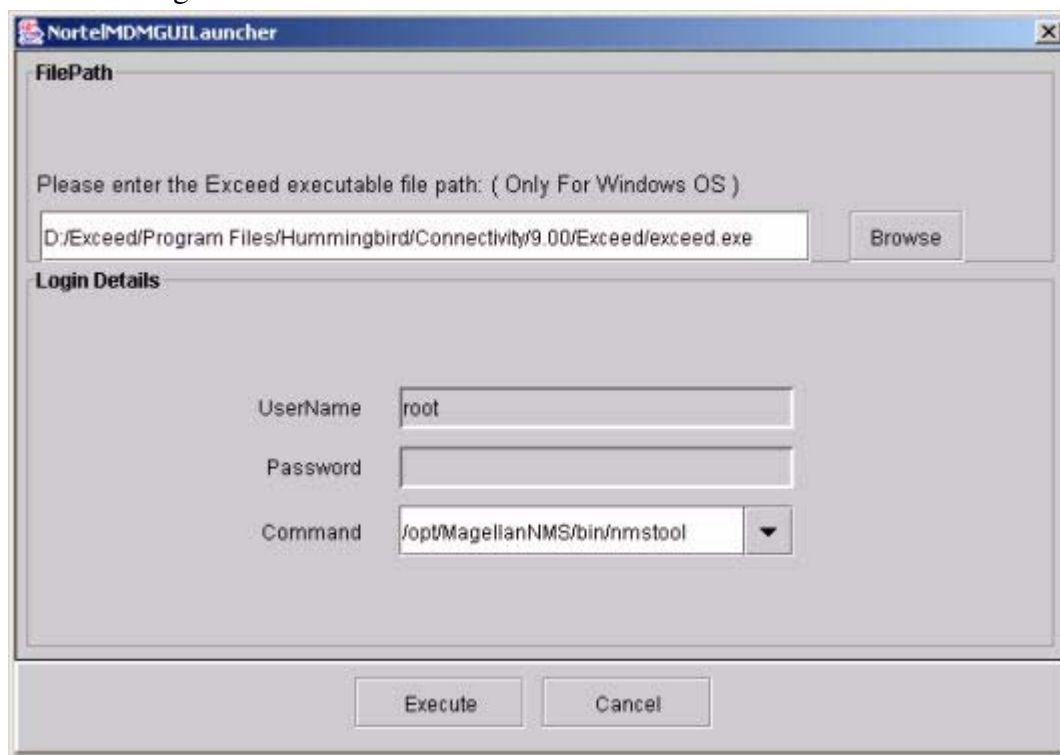
At Integrated EMS workstation

- Launch the Integrated EMS Java Web Start Client
- Navigate to the **Element Managers** topology in the Integrated EMS tree.
- Select a **MDM** map symbol.
- Right-click the map symbol and select the **MDM Mgr GUI** menu item. The Client Server List window is launched as shown below.



- Select the IP address of the device from where the MDM manager is to be launched, from the list box.

Click the **OK** button. The system displays a window similar to the following figure.



- Click the **Browse** button to select Exceed executable file path.
- For the MDM Centralized Account the username and password are automatically filled and these fields are not editable.

- Type the command “/opt/MagellanNMS/bin/nmstool” in the **Command** editable list box.
- Click the **Execute** button to execute the specified command. This launches the nmstool application as the one shown below.



23: A00006772 Functional description (FN)

23.1 Feature name

Euro-PacketCable Compliance

23.2 Description

This feature addresses capabilities required by tComLabs Euro-PacketCable CMS Qualification testing.

This feature includes the following components:

1. Graceful Restart Method

The Call Management Server (CMS) will support receiving a Restart In-Progress (RSIP) message with a restart method of “Graceful” from MTA’s, to be used as a method to deload lines on a Gateway. When RSIP Graceful is received, the endpoint(s) specified in the message will no longer be able to make or receive new calls. Any active calls (which have at least reached the alerting stage) will be allowed to complete, but will be brought down after the restart delay expires (if one was specified). Lines still in a call will appear in the Call-Processing Deloaded “CPD” state in the Core and Succession Line Maintenance Manager (LMM), and will transition to System Busy “SB” when the call hangs up or is brought down due to timer expiration. Lines that are IDLE will transition to “SB” immediately when RSIP Graceful is received.

All the LTP-level MAP commands will continue to work for CPD lines. A BSY command on a CPD line will maintain the existing behavior, such that the state will change to MB when the line hangs up. A FRLS command on a CPD line will cause the line to move to the MB state, to be consistent with the behavior for CPB and IDL states.

Note: If RSIP Graceful with restart-delay is received by the GWC after a MAP BSY command has been executed, the line will appear CPD but will move to the SB state when the timer expires. A FRLS command is required to make the line MB.

The CMS will also support receiving RSIP cancel-graceful from MTA’s. The purpose of this message is to inform the CMS that the endpoint(s) in question are still in-service and should be allowed to make or receive new calls again. If a restart delay was specified in the original RSIP Graceful message, cancel-graceful will only be allowed if the restart delay timer has not yet expired. If no restart delay was specified, cancel-graceful will be allowed at any time. Lines that are “CPD” in the Core will transition back to “CPB”. Lines that are “SB” will transition back to “IDL”.

This feature adds support for Graceful Restart Method strictly for the NCS protocol.

2. DNS Support for Multiple Addresses

For MTA's which are provisioned in SESM as using dynamic IP addressing, the CMS will support multiple IP addresses being provisioned in the DNS Server (up to 2 will be supported). The MTA will be allowed to come into service from either address via an RSIP message. The IP address at which the Gateway is in-service will be considered the "primary" address, and the other address is considered the "alternate".

Note that the latest DNS response will always overwrite any previous IP address information. For example, if the DNS server responds with 2 addresses initially, and later responds with only 1 address, the alternate address will be deleted after the second response.

If the DNS response contains more than 2 A-records for a given MTA, the first 2 A-records will be considered and the rest will be ignored. A syslog entry will be generated when this happens. Testing has shown that some DNS Software returns multiple A-records in different order over many queries, in which case the 2 records to be accepted cannot be pre-determined. It is recommended that customers do not provision more than 2 A-records for a given MTA.

When the DNS TTL timer expires, the CMS will query the DNS server to refresh its mapping. If the DNS response contains 2 addresses, one of which matches the current "primary" address, the primary will remain unchanged. If the DNS response contains 1 or 2 addresses, none of which match the current "primary" address, then the gateway will go out-of-service until it RSIP's (or responds to a heartbeat) from one of the new addresses.

If an MTA has been provisioned with two IP Addresses in DNS, then when a CMS Cold Swact occurs, the CMS will receive both IP addresses of that MTA. The CMS will attempt to contact the MTA at both addresses, alternating back and forth until it receives a response. The same behavior occurs when such an MTA is first provisioned on the CS 2000 via SESM. Once the CMS has received any message from the gateway, it will no longer swap IP addresses when heartbeat loss occurs.

If a customer is using multiple DNS Servers, they have a responsibility to ensure the contents of each DNS Server are synchronized. If one Server fails to respond to a DNS query, the CMS will retry the alternate Server.

3. NCS Error-handling enhancements

This component provides minor NCS changes related to return code usage with non-compliant MTAs or in error scenarios. As well, message retransmission logic is enhanced in a low-runner error scenario.

23.3 Hardware Requirements or Dependencies

In order for a customer to make use of RSIP Graceful, they must have a MTA that supports this operation.

In order for a customer to make use of multiple addresses for a MTA, they must operate a DNS Server that is capable of provisioning multiple A-records against a single host.

23.4 Software Requirements or Dependencies

23.5 Limitations and restrictions

23.6 Interactions

23.7 Glossary

24: A00006780 Functional description (FN)

24.1 Feature name

Trimodal Call Server OAM & P Enhancements

24.2 Description

Trimodal Call Server is a Nortel Networks Call Server which supports all the following three Bearer Network Fabric types: ATM, IP and TDM. It is a solution being provided by Nortel Networks to its customers who want to:

- Make a smooth transition from VoATM Carriers to a VoIP network solution.
- Move into the IP Space, leveraging the already existing ATM equipment at their premises.

This activity is in continuation of the Enhancements done in SN07 under the following ACTIDs:

- A00003487: Tri Modal Provisioning
- A00003947: Tri Modal Logs and OMs

The SN08 Trimodal Enhancements include:

- OAMP Enhancements
 - TRK2NET2 and TRK2NET1 OM tuple allocation enhancement.
 - Enhancements to include Bearer Network information on (a) SPM PM, Carrier and Perfmon MAPs (b) ABI XPM MAPs (c) GWC MAP (d)TTP, LTP MAPs and (e) DPT MAPs.
 - Enhancements to the Servord Query Commands QDN, QLEN, QLENWRK, QDNWRK, QHASU, QGRP, QLT and QCUST command outputs to include Bearer Network Information.
 - When a tuple is added in table NETBRDGE, a Bridge Pool without members is allocated.
 - Introduce restriction in the table NETBRDGE to the DISPLAY field contains unique and non-null values, as these values are used in the MAP display and query command enhancements.
 - New table OFCVAR parameter OSS_PROV_VERSION is added to enable/disable the Servord Query Command enhancements.
 - Tool QOSSVER is introduced to print out the list of activity IDs of features delivered in various loads which have OSS impact.

24.2.1 OMs Enhancement

TRK2NET2 and TRK2NET1 OM tuples are allocated for all bearer networks provisioned in table BEARNETS, for each Trunk Group datafilled in table TRKGRP i.e. even if there are no Trunk Members against the Trunk Group in a bearer network.

Details are captured in the Performance Management Document for the feature.

24.2.2 MAP Enhancements

The following MAP enhancements are implemented as a part of this feature.

- Posting of nodes on a Bearer Network basis
- Refining the trunk post set based on the bearer network
- Display of Bearer Network Information on (a) SPM PM, Carrier and Perfmon MAP displays, (b) ABI XPM MAP displays as a part of QUERYPM MENU command, (c) GWC MAP display as a part of QUERYPM MENU command (d) TTP CktInfo MENU command, (e) LTP MAP displays and (f) DPT MAP displays.
 - The value displayed in new display field “Bear” is picked up from the DISPLAY field of the table BEARNETS tuple corresponding to the Bearer Network.
 - The value displayed in new display field “Netbrdge” is picked up from the DISPLAY field of the table NETBRDGE tuple corresponding to the Bridge Pool CLLI of the Bridge Pool to which an IW SPM belongs.

Notes:

- Refresh of the MAP displays of a currently posted PM or Line does not automatically update when table BEARNETS or NETBRDGE is changed. Reposting the PM or line reflects the change.

24.2.2.1 PM MAP level enhancements

The enhancements at the MAPCI;MTC;PM level enable the user to do the following:

- To display all PMs associated with a bearer network. This is applicable to all packet node types including SPMs, GWCs and ABI hosted XPMs which are currently maintained from PM MAP level.
- To post SPM type nodes based on the associated bearer network and the SPM node class. The valid SPM node classes for this command are SMG4 and DPT.

Note: All enhancements/additions are displayed in **BOLD** in figures.

Enhancements to post command:

The following figure shows the enhancements to the post command at the PM level.

- The new option <BN> allows the query by bearer network datafilled in DISPLAY field of the table BEARNETS tuple for a bearer network.

Note 1: The Parms <PM Type> and the Parm <PM BEARNETS> cannot be used together.

Note 2: For the user inputs and the MAP responses please refer the Configuration Document for the feature(CN Document). For more information see “User interface changes” on page 92.

Note 3: The Bearer Networks displayed in the Parameter list for new option <BN> does not include Bearer Network for fabric=ENET.

Figure 1 POST command with the new parameters

```
Post:Post specified PMs for maintenance
Parms: [<All PMs> {AllPMs}]
      [<PM Type>... {TM2 [<All> {All}]}
      ....
      [<PM State>... {SysB,
      ....
      InSv}]
      [<PM Alarm>... {Minor,
      Major,
      Crit}]
      [<BN> {A1_P [<PM Type> {SPM [<SPM Type> {SMG4,
      DPT}}]}}]
      A1_S [<PM Type> {SPM [<SPM Type> {SMG4,
      DPT}}] },
      IP_P [<PM Type> {SPM [<SPM Type> {SMG4,
      DPT}}] },
      IP_S [<PM Type> {SPM [<SPM Type> {SMG4,
      DPT}}] }]
```

QUERYPM command for ABI XPMs:

The querypm command for on posting a ABI XPM from the MAPCI;MTC;PM level is enhanced to display the bearer network of the GWC from where it subtends.

This enhancement is for PMs datafilled in the following tables: LTCINV, LTCRINV, RCCINV, LCMINV, RDTINV, LGRPINV, SERVINV (except DPT GWCs) and RMMINV. Also the QueryPM command of ESA nodes has been enhanced to display Bearer Network information.

E.g., Datafill from Table LTCINV for an ABI hosted XPM:

```
SMA2 4 62 MVDD 1 57 21 R 21 MX85AB XM220CE (POTS POTSEX) (KEYSET KSETEX)
$ (4 16) (4 17) (4 18) (4 19) $ (UTR6 ) (MSGMX76 HOST ) (ISP 4) $
NORTHAA AX74AA AX74AA 0 NILLOAD ( EXTDS512 HOST ABI 5 ) $ 6X40FB N
```

Figure 2 QueryPM enhancements for LTC

```
>mapci nodisp prtmap;mtc;pm;post LTC 1
>querypm
PM Type: LTC  PM No.: 1  PM Int. No.: 6  Node_No.: 149
PMs Equipped: 113  Loadname: QLI20CE  EEPROM Load: SXFWAJ02
WARM SWACT is supported but not possible: node redundancy lost.
LTC 1 is included in the REX schedule.
REX on LTC 1 has not been performed.
Node Status: {OFFLINE, TRUE}
Unit 0  Status: {OFFLINE, TRUE}
Unit 1  Status: {OFFLINE, TRUE}
Site Flr RPos Bay_id Shf Description      Slot      EqPEC
VOIP  01 AA05  LTEI 018  18  LTC : 001      6X02NA
MG9K Information:
HOST  01 MM04 MG9F 004 02 ABI : 0006  20/21 042 172.31.165.18
Bearer Network: IP_P
```

Figure 3 QueryPM enhancements for LCME

```
>post LCME HOST 2 0;querypm
PM:
POST:
PM Type: LCME  Int. No.: 2  Status index: 1  Node_No: 107
LCME HOST 02 0  Memory Size - Unit 0: 256K , Unit 1: 256K
Loadnames: LCMINV - LCME18AW
LCM REX is      ON; Not run since last Reload Restart.
Node Status: {OFFLINE, TRUE}
Unit 0 Status: {OFFLINE, TRUE}          /RG: 0
Unit 1 Status: {OFFLINE, TRUE}          /RG: 0
Ring Generator Status:
  RG 0 Status: {OK}          Preferred
  RG 1 Status: {OK}          Standby
  RG in Overload : NO
Site Flr RPos Bay_id Shf Description      Slot      EqPEC
HOST  01  N25  LCEI 02  38  LCME 02 0      BX30AB
Services : ISDN Equipped
MG9K Information:
Bearer Network: A1_P
```

Figure 4 QueryPM enhancements for RCS

```
>querypm
PM Type: RCS  Int. No.: 15  Node_No: 169
Site Flr RPos Bay_id Shf Description      Slot      EqPEC
SLC   01  K31  RTS 000  58  RCS  00 0
MG9K Information:
Bearer Network: IP_P
```

Figure 5 QueryPM enhancements for RCC

```
>querypm
PM Type: RCC Int. No.: 15  Node_No: 169
Site Flr RPos Bay_id Shf Description      Slot      EqPEC
SLC   01  K31  RTS 000  58  RCS  00 0
MG9K Information:
Bearer Network: A1_P
```


Figure 6 QueryPM enhancements for IDT

```

PM Type: IDT  Int. No: 56  Status index: 0  Node No: 110
Prot-Switch: Unavailable
Cside Host Name: SMA2 4
RDT Name: RDT1 23 0
Network element: 12 ANODE_2_CUFED
Lines allocated to IDT 23: 671
Lines defined for SMA2 4: 671
Lines available to SMA2 4: 4705
MG9K Information:
  Bearer Network: A1_P

```

Figure 7 QueryPM enhancements for LGRP

```

PM Type:LGRP Node No:150  Int.No:0  Off.LM:18  Type:S
Cside Host: GWC 0  Node_No: 89  IP: 47.142.92.68
Node_Status      MTC_Node_Status      Callp_Node_Status
{OFFL FALSE}      {OFFL FALSE}      {OFFL FALSE}
Site  Flr  RPos      Bay_id  Shf      Description
HOST  1    A 1      MG9F  1    3      LGRP  1 3
Node Information:
  Bearer Network: A1_P

```

Figure 8 QueryPM enhancements for ESA

```

PM Type: ESA  PM No.: 0  PM Int. No.: 0  Node_No.: 110
PMs Equipped: 79  Loadname: ESA10AQ
NODE STATUS: {OFFLINE, TRUE}
Site Flr RPos Bay_id Shf Description Slot EqPEC
RLCM 01 N15 RLCM 00 00 ESA : 000
MG9K Information:
  Bearer Network: A1_P

```

Figure 9 QueryPM enhancements for RMM

```

PM TYPE: RMM  PM NO.: 0  NODE NO.: 105
PM_STATUS: Offl  NODE_STATUS: OFFLINE,TRUE, CHKSUM: #BDB0
PP LOAD: VALID  PP EXECS: VALID  FNAME: RMM10A
PMS EQUIPPED: 79  PM INT. #: 3
Site Flr RPos Bay_id Shf Description Slot EqPEC
USMA 01 D39 MIS 000 65 RMM : 000 6X13AA
TM Entries: 0 TO 10
MG9K Information:
  Bearer Network: AAL1

```

QUERYPM command for GWCs:

The querypm command is on posting a GWCs from the MAPCI;MTC;PM level is enhanced to display the bearer network it supports under Node Information. For DPT GWCs, the message “Signaling Only - No Associated Bearer Network” is displayed.

E.g., Datafill from Table SERVINV for GWCs.

```

GWC 0 IP 47 142 92 68 (POTS POTSEX) (KEYSET KSETEX) $ NORTHAA
(AAL1_PRIMARY Y) $ $
GWC 19 IP 47 142 92 148 (ABTRK GWCEX) $ NORTHAM $ $

```

Figure 10 QueryPM enhancements for GWCs

```
>mapci;mtc;pm;post gwc 0
>querypm
PM Type: GWC  PM No.: 0  PM Int. No.: 0  Node_No.: 89
IP Address: 47.142.92.68
Unit 0:
  Load: GN080BK
Unit 1:
  Load: GN080BK
Node Information:
  Bearer Network: A1_P
```

Figure 11 QueryPM enhancement for DPT GWCs

```
>querypm
PM Type: GWC  PM No.: 19  PM Int. No.: 19  Node_No.: 199
IP Address: 47.142.92.148
Unit 0:
  Load: GN080BK
Unit 1:
  Load: UNKNOWN
Node Information:
  Bearer Network: Signaling Only - No Associated Bearer Network
```

24.2.2.2 Enhancements to SPM MAP display (mapci;mtc;pm;post spm <spm no>)

Enhancements to Non-Menu POSTCLS command:

To post SPM type nodes based on the SPM node class. In case of IW SPM (Bridge _only Type), nodes are posted based on their associated bridge pool.

The following figure shows the enhancements to the post command at the PM level.

- Enhancements to the existing command POSTCLS.
 - To Post the IW DPT SPMs
 - To POST IW SPMs associated with a specific Bridge Pool CLI. Parameters which are passed to POSTCLS command are linked to the values datafilled in DISPLAY field of table NETBRDGE tuples.

Note: For the user inputs and the MAP responses please refer the Configuration Document for the feature (CN Document). For more information see “User interface changes” on page 92.

Figure 12 POSTCLS command Enhancements

```
POSTCLS: Post SPM by CLASS for maintenance.
Parms: <Class Type> {DMSCP,
  IWBRG [<Netbridge_clli>...{E_A1,E_A2}}
  SMG4,
  IWDPT};
```

MAP Display for DMSCP/SMG4/IW DPT SPM node types:

Below are the MAP displays for a) DMSCP SPM b)SMG4 SPM c) IW DPT SPM. The DISPLAY field of the bearer network of the SPM node as datafilled in table BEARNETS is displayed in the new field “Bear”.

Figure 13 PM MAP display for DMSCP node

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	Istb	NODLOG	.	3 SPM	.	SYSB	69C..	.	ATM_6
M				*C*		*C*	*C*		*C*
SPM				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		4	1	52	2	6	48
2 Post_		SPM		0	0	6	0	3	4
3 ListSet									
4 ListRes	SPM	8	ISTb	Class: DMSCP				BEAR: ENET	
5 Trns1									
6		Shlf0	SL A Stat	Shlf0	SL A Stat	Shlf1	SL A Stat	Shlf1	SL A Stat
7 ATMConn	-----	1 -	----	CEM 1	8 A ISTb	DLC 0	1 A InSv	-----	8 -
8 IPConn	-----	2 -	----	OC3 0	9 A InSv	DLC 1	2 I OffL	-----	9 -
9 OfClk	-----	3 -	----	OC3 1	10 I InSv	-----	3 -	-----	10 -
10	-----	4 -	----	-----	11 -	-----	4 -	DSP 1	11 A InSv
11 Disp_	-----	5 -	----	VSP 0	12 I OffL	DSP 0	5 I InSv	-----	12 -
12 Next	-----	6 -	----	VSP 1	13 A InSv	-----	6 -	-----	13 -
13 Select_	CEM 0	7 I	ISTb	-----	14 -	-----	7 -	-----	14 -
14 QueryPM									
15 ListAlm	POST:								
16 Clock	SPM:								
17 SPERFORM									
18 Upgrade_									
ADMIN									

Figure 14 PM MAP display for SMG4 node

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	Istb	NODLOG	.	3 SPM	.	SYSB	68C..	.	ATM_6
M				*C*		*C*	*C*		*C*
SPM				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		4	1	52	2	6	48
2 Post_		SPM		0	0	6	0	3	4
3 ListSet									
4 ListRes	SPM	0	OffL	Class: SMG4			BEAR: A1_P		
5 TrnsL									
6		Shlf0	SL A Stat	Shlf0	SL A Stat	Shlf1	SL A Stat	Shlf1	SL A Stat
7 ATMConn	ATM 0	1 I OffL	CEM 1	8 I OffL	-----	1 -	-----	8 -	-----
8 IPConn	ATM 1	2 I OffL	OC3 0	9 I OffL	-----	2 -	-----	9 -	-----
9 OfClk	-----	3 -	-----	OC3 1	10 I OffL	-----	3 -	-----	10 -
10	-----	4 -	-----	VSP 1	11 I OffL	VSP 0	4 I OffL	-----	11 -
11 Disp_	-----	5 -	-----	VSP 2	12 I OffL	VSP 6	5 I OffL	VSP 5	12 I OffL
12 Next	-----	6 -	-----	VSP 3	13 I OffL	-----	6 -	-----	VSP 7
13 Select_	CEM 0	7 A OffL	VSP 4	14 I OffL	-----	7 -	-----	-----	14 -
14 QueryPM									
15 ListAlm	POST:								
16 Clock	SPM:								
17 SPERFORM									
18 Upgrade_									
ADMIN									

Figure 15 PM MAP display for IW DPT node

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	NO AMA	.	2 SPM	3 RS	.	34C..	.	SPM_26
		C		*C*	*C*		*C*		M
SPM				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		5	0	6	0	10	19
2 Post_		SPM		0	0	4	0	7	6
3 ListSet									
4 ListRes	SPM	1	InSv	Class: IW		DPT_Only	BEAR: AAL1		
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 InSv	-----	1 -	-----	8 -
8 IPConn	-----	2 -	-----	ATM 0	9 A InSv	-----	2 -	-----	VSP 2
9 OfClk	-----	3 -	-----	ATM 1	10 I InSv	-----	3 -	-----	10 -
10	-----	4 -	-----	-----	11 -	-----	VSP 0	4 A InSv	DSP 1
11 Disp_	-----	5 -	-----	-----	12 -	-----	DSP 0	5 A InSv	-----
12 Next	-----	6 -	-----	-----	13 -	-----	VSP 1	6 A InSv	-----
13 Select_	CEM 0	7 A InSv	-----	14 -	-----	-----	7 -	-----	14 -
14 QueryPM	Next								
15 ListAlm									
16 Clock									
17 SPERFORM									
18 Upgrade_									
ADMIN									

MAP Display for IW bridge_only SPM node:

Below is the display of a IW bridge only SPM node. The value datafilled in DISPLAY field of the table NETBRDGE tuple corresponding to the NetBridge CLLI of the SPM node is displayed in the new field “Netbridge”.

Figure 16 PM MAP display for IW bridge only node

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	Istb	NODLOG	.	3 SPM	.	SYSB	69C..	.	ATM_6
M				*C*		*C*	*C*		*C*
SPM				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		4	1	52	2	5	49
2 Post_		SPM		0	0	6	0	3	4
3 ListSet									
4 ListRes	SPM	3	InSv	Class: IW	BRG_Only	NETBRDGE: E_AP			
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 A InSv	-----	1 -	-----	8 -
8 IPConn	-----	2 -	-----	ATM 0	9 A InSv	-----	2 -	-----	9 -
9 OfClk	-----	3 -	-----	ATM 1	10 I InSv	-----	3 -	VSP 6	10 A InSv
10	-----	4 -	-----	VSP 0	11 A InSv	VSP 4	4 A InSv	VSP 7	11 A InSv
11 Disp_	-----	5 -	-----	VSP 1	12 A InSv	DSP 2	5 A InSv	VSP 8	12 I InSv
12 Next	-----	6 -	-----	VSP 2	13 A InSv	DSP 3	6 A InSv	DSP 0	13 A InSv
13 Select_	CEM 0	7 I	InSv	VSP 3	14 A InSv	-----	7 -	DSP 1	14 I InSv
14 QueryPM	Next								
15 ListAlm									
16 Clock									
17 SPERFORM									
18 Upgrade_									
ADMIN									

24.2.2.3 Enhancements to CARRIER MAP display

The CARRIER level of MAPCI is enhanced for SPM PMs to display the SPM node type and the Bearer Network or Network Bridge Information as appropriate.

In the case of DMSCP, SMG4 and IW DPT node types, the additional information displayed is the SPM node class type and the value datafilled in DISPLAY field of the table BEARNETS tuple corresponding to the Bearer Network associated with the node.

In the case of Bridge Only IW nodes, the additional information displayed is the SPM node class type and the value datafilled in DISPLAY field of the table NETBRDGE corresponding to the bridge pool CLLI with which the IW SPM is associated.

Figure 17 Carrier MAP display for DMSCP

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL		
AMDI	Istb	NODLOG	.	3 SPM	.	SYSB	69C..	.	ATM_6		
M				*C*		*C*	*C*		*C*		
POST	CLASS	ML	OS	ALRM	SYSB	MANB	UNEQ	OFFL	CBSY	PBSY	INSV
0 Quit	TRUNKS	75	0	0	0	0	0	527	0	0	89
2 Post_	REMOTE	0	0	0	0	0	0	42	0	0	0
3	PROTLN	0	0	0	0	0	0	3	0	0	0
4	HSCARR	85	0	0	0	0	0	545	0	0	95
5 Loop_	OC3S	Type: DMSCP Bear: ENET									
6 Tst_	N CLASS	SITE	SPM	RM	OC3S	CKT	STATE	TR	MA		
7 Bsy_	0	HSCARR	HOST	8	0	0	169	OFFL	--	--	
8 RTS_	1	HSCARR	HOST	8	1	0	170	OFFL	--	--	
9 Offl_											
10											
11 Disp_											
12 Next	SIZE OF POSTED SET	:	175						MORE...		
13											
14 Detail_	POST:										
15 ListAlm_											
16											
17 Perfmon_											
18											
ADMIN											

Figure 18 Carrier MAP display for SMG4

XAC	MS	IOD	Net		PM	CCS	Lns	Trks	Ext	APPL		
AMDI	Istb	NODLOG	.		3 SPM	.	SYSB	69C..	.	ATM_6		
M					*C*		*C*	*C*		*C*		
POST		CLASS	ML	OS	ALRM	SYSB	MANB	UNEQ	OFFL	CBSY	PBSY	INSV
0 Quit		TRUNKS	75	0	0	0	0	0	527	0	0	89
2 Post_		REMOTE	0	0	0	0	0	0	42	0	0	0
3		PROTLN	0	0	0	0	0	0	3	0	0	0
4		HSCARR	85	0	0	0	0	0	545	0	0	95
5 Loop_	OC3S	Type: SMG4 Bear: A1_P										
6 Tst_	N	CLASS	SITE	SPM	RM	OC3S	CKT	STATE	TR	MA		
7 Bsy_	0	HSCARR	HOST	0	0	0	1	OFFL	--	--		
8 RTS_	1	HSCARR	HOST	0	1	0	2	OFFL	--	--		
9 Offl_	2	HSCARR	HOST	0	0	0	176	OFFL	--	--		
10	3	HSCARR	HOST	0	1	0	177	OFFL	--	--		
11 Disp_												
12 Next		SIZE OF POSTED SET				:	180			MORE...		
13												
14 Detail_		POST:										
15 ListAlm_												
16												
17 Perfmon_												
18												
ADMIN												

Figure 19 Carrier MAP display for IW DPT SPM

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	NO AMA	.	2 SPM	3 RS	.	34C..	.	SPM_26
		C		*C*	*C*		*C*		M
POST		CLASS	ML	OS ALRM	SYSB	MANB	UNEQ	OFFL	CBSY PBSY INSV
0 Quit		TRUNKS	0	0	0	0	0	477	0 0 618
2 Post_		HSCARR	0	0	1	0	0	503	0 0 692
3		OC3S	Type: DPT Bear: AAL1						
4		N CLASS	SITE	SPM RM	OC3S	CKT	STATE	TR MA	
5 Loop_		0 HSCARR	HOST	1 0	0	1	INSV		
6 Tst_		1 HSCARR	HOST	1 1	0	2	INSV	.S ..	
7 Bsy_									
8 RTS_									
9 Offl_									
10		SIZE OF POSTED SET : 5						MORE...	
11 Disp_									
12 Next		POST:							
13									
14 Detail_									
15 ListAlm_									
16									
17 Perfmon_									
18									
ADMIN									

Figure 20 Carrier MAP display for IW DPT SPM On Next Command

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	NO AMA	.	2 SPM	3 RS	.	34C..	.	.
		C		*C*	*C*		*C*		
POST		CLASS	ML	OS ALRM	SYSB	MANB	UNEQ	OFFL	CBSY PBSY INSV
0 Quit		TRUNKS	0	0	0	0	0	477	0 0 618
2 Post_		HSCARR	0	0	1	0	0	503	0 0 692
3		STS3L	Type: DPT Bear: AAL1						
4		N CLASS	SITE	SPM RM	OC3S	STS3L	CKT	STATE	TR MA
5 Loop_		0 HSCARR	HOST	1 0	0	0	3	INSV	
6 Tst_		1 HSCARR	HOST	1 1	0	0	4	INSV	.S ..
7 Bsy_									
8 RTS_									
9 Offl_									
10		SIZE OF POSTED SET : 3						MORE...	
11 Disp_		next							
12 Next									
13									
14 Detail_									
15 ListAlm_									
16									
17 Perfmon_									
18									
ADMIN									

Carrier MAP Display for IW bridge only SPM node:

Below is the carrier level map display of a IW bridge only SPM node. The Class of the SPM Node and the value datafilled in DISPLAY field of table NETBRDGE tuple corresponding to the Bridge Pool CLLI with which the SPM node is associated, are displayed in the new fields ‘Type” and “Netbrdge”.

Figure 21 Carrier MAP display for IW Bridge only SPM

[illegible]

Figure 22 Carrier MAP display for IW Bridge only SPM On Next Command

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL		
AMDI	Istb	NODLOG	.	3 SPM	.	SYSB	69C..	.	ATM_6		
M				*C*		*C*	*C*		*C*		
POST	CLASS	ML	OS	ALRM	SYSB	MANB	UNEQ	OFFL	CBSY	PBSY	INSV
0 Quit	TRUNKS	75	0	0	0	0	0	527	0	0	89
2 Post_	REMOTE	0	0	0	0	0	0	42	0	0	0
3	PROTLN	0	0	0	0	0	0	3	0	0	0
4	HSCARR	0	0	0	0	0	0	545	0	0	95
5 Loop_	STS3L	Type: IW Netbrdge: E_AP									
6 Tst_	N CLASS	SITE	SPM	RM	OC3S	STS3L	CKT	STATE	TR	MA	
7 Bsy_	0 HSCARR	HOST	3	0	0	0	3	OFFL	--	--	
8 RTS_	1 HSCARR	HOST	3	1	0	0	4	OFFL	--	--	
9 Offl_											
10											
11 Disp_											
12 Next	SIZE OF POSTED SET : 3							MORE...			
13	next										
14 Detail_											
15 ListAlm_											
16											
17 Perfmon_											
18											
ADMIN											

24.2.2.4 Enhancements to CARRIER PERFMON MAP display

The CARRIER/PERFMON level of the MAP is enhanced for SPM PMs to display the SPM node type and the Bearer Network or Network Bridge Information as appropriate.

In the case of DMSCP, SMG4 and IW DPT node types, the additional information displayed is the SPM node class type and the value datafilled in the DISPLAY field of the table BEARNETS tuple corresponding to the Bearer Network associated with the node.

In the case of IW Bridge nodes, the additional information displayed is the SPM node type and the value datafilled in the DISPLAY field in table NETBRDGE corresponding to the Bridge Pool CLLI with which the node is associated.

Figure 23 MAP display for DMSCP/SMG4/DPT node

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL			
AMDI	Istb	NODLOG	.	3 SPM	.	SYSB	70C..	.	ATM_6+			
M				*C*		*C*	*C*		*C*			
PERFMON	CLASS	ML	OS	ALRM	SYSB	MANB	UNEQ	OFFL	CBSY	PBSY	INSV	
0 Quit	TRUNKS	75	0	0	0	0	0	527	0	0	89	
2	REMOTE	0	0	0	0	0	0	42	0	0	0	
3	PROTLN	0	0	0	0	0	0	3	0	0	0	
4	HSCARR	0	0	0	0	0	0	545	0	0	95	
5	OC3S	Type: DMSCP Bear: ENET										
6 SilMl	PERFMON	0	SPM	8	OC3RM	0	OC3S	0				
7	Interval:	4:30\$			Status:							
8	Parm	Count	M	D	Parm	Count	M	D	Parm	Count	M	D
9 MeterPP	LBC-N	255			OPT-N	255			OPR-N	UNSET		
10	CV-N	0			ES-N	0			SES-N	0		
11	SEFS-N	0										
12												
13	PERFMON:											
14 PPQuery												
15												
16												
17												
18												
ADMIN												

24.2.2.5 DPTTRM MAP Level

The MAP screen displayed on accessing the MAPCI;MTC;TRKS;DPTTRM level is enhanced to display the DPT protocol used on posted DPT terminal node.

Figure 24 MAP display for DPTRM MAP

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	Istb	NODLOG	.	2 SPM	.	.	60C..	.	SDM
M				*C*		CR C	*C*		
0 Quit	PM: SPM	1		POSTED SET: SPM ALL	1 OF	5			
2 Post_									
3	SUB	STA	PROT INB	MANB	PMB	SYSB	CPB	CPD	IDL
4 Disp_	1	OFFL	BICC 2016	0	0	0	0	0	0
5 Bsy_									
6 RTS_									
7									
8 Frls_									
9									
10 Alrm									
11									
12 Next									
13									
14									
15									
16									
17									
18									
ADMIN									

24.2.2.6 Enhancements to DPTRKS MAP display

The MAP screen displayed on accessing the MAPCI;MTC;TRKS;DPTRKS level is enhanced to display the DPT protocol used on the posted DPT trunk group. This also displays the bearer network associated with the trunk group from table TRKOPTS.

Figure 25 MAP display for DPTTRKS

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	Istb	NODLOG	.	2 SPM	.	.	60C..	.	SDM
M				*C*			*C*		
0	Quit								
2	Post_	CKT TYPE	COM LANG			STATE	RANGE		
3		2W ISP	DPTINATM			INS	41	59	
4						PROT:	BICC	BEAR:A1_P	
5	BSY_	IDL:	19						
6	RTS_	CPB:	0						
7	OP_	MTC:	0						
8	FRLS_	PV: 0		FE_BLK: 0			FE_UNEQ: 0		
9	Reset_								
10		PENDING: 0							
11	PREV								
12	NEXT								
13									
14									
15	TrkQry_								
16	QrySig								
17	RouteSet								
18	QryMtc								
	ADMIN								

24.2.2.7 Enhancements to TTP MAP level

The Enhancements to the MAPCI;MTC;TRKS;TTP level to be able to post trunk members associated with a bearer network, within a existing POST set. After a post set has been created using any of the existing POST commands, the post-set can be refined to POST the trunk members of a particular bearer network. The parameter range BEARNETS_DISPLAY for parameter passed to POST command for new Option BN, is the values datafilled in DISPLAY field of table BEARNETS tuples. Refer to Figure 26 below.

The CktInfo command at MAPCI;MTC;TRKS;TTP level is enhanced to display Bearer network as shown in Figure 27 below.

Figure 26 POST command with new parameters

```

POST-- POST A NEW SET
Parms: [<SET TYPE> {T [<CLLI1> STRING
                      [<CNRI1> {0 TO 9999}}]
                      [<....> STRING],
      G <CLLI> STRING
        [<CLNR> {0 TO 9999}}]
        [<TO> {TO}}]

      ....
      WB <CLLI> STRING
        <CKTN> {0 TO 9999}},
      BN [<ENET> STRING]
        [<A1_P> STRING]
        [<A1_S> STRING]
        [<IP_P> STRING]
        [<IP_S> STRING]]]

```

Figure 27 TTP level MAP display

```

>mapci;mtc;trks;ttp;<post any trunk ckt>
>cktinfo
SPM 0 95 : INSV
SPM 0 : InSv
Ckt state : IDL
Ckt Bearer net : A1_P

```

24.2.3 Enhancements to LTP MAP display

The MAP screen displayed on accessing the MAPCI;MTC;LNS;LTP level is enhanced to display the bearer network of the posted line.

Figure 28 LTP level MAP display

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	Istb	NODLOG	.	3 SPM	.	SYSB	69C..	.	ATM_6
M				*C*		*C*	*C*		*C*
LTP									
0 Quit		POST	DELQ		BUSYQ		PREFIX		
2 Post_		LEN HOST 00 0 01 19					BEAR ENET		
3		LCC PTY RNG					STA F S LTA TE	RESULT	
4		1FR			DN 613 621 2590 IDL				
5 Bsy									
6 RTS									
7 Diag									
8									
9 AlmStat									
10 CktLoc		post d 6212590							
11 Hold									
12 Next									
13									
14									
15 FullDn									
16 Prefix									
17 LCO_									
18 Level_									
ADMIN									

24.2.4 Line Query Command Enhancements

24.2.4.1 Overview

Enhanced output of Line Query commands QDN, QLEN, QDNWRK, QLENWRK, QHASU, QGRP and QCUST to display Bearer Network Information associated with a subscriber line.

- Bearer Network Information for a subscriber line is added to the command outputs for CI commands QDN, QLEN, QDNWRK, QLENWRK, QHASU, QGRP, QLT and QCUST.
- In case of CI commands QLENWRK, QDNWRK and QHASU, the query run on a range of lines can be restricted to a Bearer Network.

No Servord Commands are being enhanced.

Details are captured in the Configuration Document for the feature.

24.2.5 New table OFCVAR Parm OSS_PROV_VERSION

A new table OFCVAR Parm OSS_PROV_VERSION has been introduced. The value of this Parm can be used as an ON/OFF feature switch control mechanism for features delivered on the Nortel Succession XA_CORE which impact the OSS interface. This is so that these kind of features are turned ON/

OFF on the switch using this OFCVAR Parm, only when OSS software for switch is upgraded to accommodate the feature code changes.

Details are provided in the User Interface Section of Configuration Document for the feature.

24.2.6 New CI Tool QOSSVER

A new CI tool, QOSSVER, is made available to user on the Nortel Succession XA-CORE. This tool lists the feature ACTIDs of features delivered in an XA-CORE software load which have an impact on the OSS interface and which make use of the table OFCVAR Parm OSS_PROV_VERSION control mechanism described above. Feature ACTIDs which do not use this mechanism will not be listed.

Details about the new tool are provided in the User Interface Section of Configuration Document for the feature.

24.2.7 Tables MNNODE, BEARNETS and NETBRDGE Table Control Response Messages

There are some changes to the Response messages to Users for table control operations performed on tables MNNODE, BEARNETS, NETBRDGE.

Changes are listed in User Interface Section of Configuration Document for feature.

24.3 Hardware Requirements or Dependencies

All variants of bearer networks and SPMs to be data filled in the lab.

24.4 Software Requirements or Dependencies

Succession release SN08 software load lineup.

24.5 Limitations and restrictions

In SN08, if number of OM Tuples belonging to OM Groups TRK2NET2 or TRK2NET1 exceeds 16,000 during the OM Tuple creation:

No more OM tuples will be created and the following Warnings are displayed to the user:

- **While adding tuple in table TRKGRP**

“Warning: Maximum number of allowed TRK2NET2 and TRK2NET1 OM tuples has been exceeded.

Require 4 tuples

Only 3 tuples are available

The OM tuples for TRK2NET1 and TRK2NET2 could not be allocated and this

OM data will not collected for any bearer network for the newly added trunk group when MULTINET_DISPLAY_ACTIVE is on”

- **While adding tuple in table BEARNETS**

“Warning: Maximum number of allowed TRK2NET2 and TRK2NET1 OM tuples has been exceeded.

Require 5000 tuples

Only 1000 tuples are available

The OM tuples for TRK2NET1 and TRK2NET2 could not be allocated and this

OM data will not collected for trunk groups using this new Bearer Network when MULTINET_DISPLAY_ACTIVE is on”

- **All SN07 limitations and restrictions as documented in A00003487 are inherited by this activity, unless specifically noted otherwise.**

24.6 Interactions

Not Applicable.

24.7 Glossary

Term	Description
ABI	Access Bridge Interface
APG	Anchor Packet Gateway
CDIS	Call Discrimination Service. This is a service provided by the Broadcom DSP that differentiates normal voice calls from VBD or Fax.
CICM	Centrex IP Client Manager
CLLI	Common Language Location Identifier
DMSCP	DMS Call Processing SPM
DN	Directory Number
DPT	Dynamic Packet Trunk
GWC	Gate Way Controller
IP	Internet Protocol
IW	Inter-Working SPM
LEN	Line Equipment Number
LTP	Line Test Position
MAP	Maintenance and Administration Position
NGSS	Next Generation Session Server
OM	Operational Measurements
PM	Peripheral Module
QCUST	Query Customer Information

Term	Description
QDN	Query Directory Number
QDNWRK	Query Working DN
QGRP	Query Group
QHASU	Query Hardware Assigned Software Unassigned LEN
QLEN	Query Line Equipment Number
QLENWRK	Query Working LEN
SERVORD	Service Order
SMG4	Media Gateway 4000 SPM
SPM	Spectrum Peripheral Module
TDM	Time Division Multiplexing
TTP	Trunk Test Position
SIP-T	Session Initiation Protocol - Telecommunications
VoATM	Voice Over ATM
VoIP	Voice Over IP
XPM	XMS-Based Peripheral Module

25: A00006865 Functional description (FN)

This document is intended for MG9000 customers as well as internal Nortel functional groups (design teams, test teams, etc).

This document will cover the functional description of the SN08 GIGE HAL (Hardware Abstraction Layer) feature, A00006865.

Please refer to A00006865 documentation for more information on the SN08 GIGE HAL feature.

25.1 Feature name

SN08 GIGE HAL Feature

25.2 Description

A new Supercore card with 4 Gigabit Ethernet ports (SCG - Supercore Gigabit Ethernet, PEC code NTNY4540 / NTNY45FA) will be introduced in SN07.

This feature will implement the necessary device drivers (MAC drivers, GigE HAL, etc) and mesh design (network processor, switch fabric, host side code, etc) to support Gigabit Ethernet.

This feature will not implement the upper layer changes (Connection Maintenance, WanBuilder, Link Mtc, etc) and there will be other features to implement these upper layer changes.

This feature does not have any visible customer interaction. Other GigE feature will support EM and LCI changes and those features documentation should be referred for more information.

Fault Management

Not applicable ☒

Logs ☐

Alarms ☐

Configuration

Not applicable ☒

Data Schema/MIBs ☐

User Interface ☐

GUI ☐

Element Management ☐

Security	_____
Service Order	_____
Office Parameters	_____
SOC	_____
Upgrades impact	_____
Accounting (includes AMA billing)	_____
Not Applicable	___X___
Billing changes	_____
Performance	_____
Not Applicable	___X___
Operational Measurements	_____
Performance Measurements	_____
Realtime	_____
Not applicable	___X___
Engineering Information	_____
Not applicable	___X___

25.3 Hardware Requirements or Dependencies

This feature (along with other GIGE features) introduces the support for the following PEC codes:

SCG: NTNY45FA

25.4 Software Requirements or Dependencies

N/A

25.5 Limitations and restrictions

N/A

25.6 Interactions

N/A

25.7 Glossary

Term	Description
GigE	Gigabit Ethernet
SCG	SuperCore GigE

26: A00006893 Functional description (FN)

26.1 Feature name

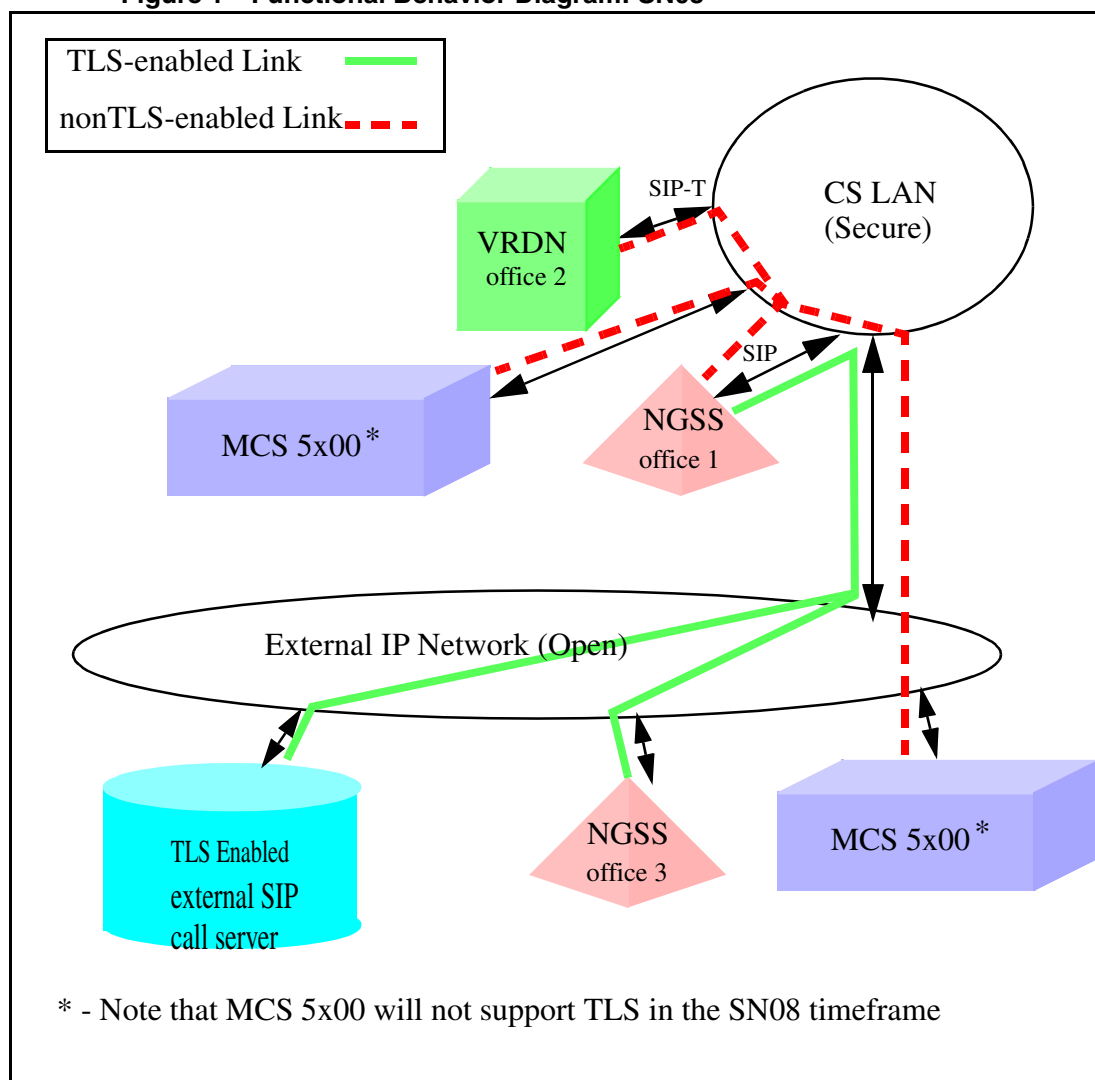
TLS support for NGSS

TLS = Transport Level Security, a security protocol that enables secure data transmission between two communicating applications.

NGSS = Next Generation Session Server, a SIP CallP Server in Nortel's Succession Networks portfolio of products.

26.2 Description

The SIP RFC (3261) stipulates that TLS version 1.0 (RFC 2246) should be utilized for secure SIP message communication between two SIP enabled devices. This feature is meant to implement this functionality for the NGSS for Peer to Peer communication (i.e. Inter-call server communication). With the support of TLS by the NGSS, connections to a SIP enabled server can be secured over a non-secure network.

Figure 1 Functional Behavior Diagram: SN08

The TLS feature will allow the NGSS to establish TLS sessions with a remote Call Server that is SIP and TLS aware. Transport Layer Security (TLS) protocol provides secure communications over non-secured networks (like the internet). The protocol allows client/server applications to communicate with privacy, integrity, and communication. Beyond a simple implementation of TLS for the NGSS, capacity degradation is mitigated through connection throttling.

Provisioning decisions will enable non-TLS UDP or TCP connections to be established and utilized as required as well UDP or TCP.

On top of developing support for the TLS RFC, this feature will implement certain logs, OMs, and alarms for scenarios including security failures, attacks, and session establishment. It will also develop provisioning interfaces for

security-related provisioning. See the configuration (CN) and fault management (FM) sections for details on these interfaces.

26.3 Hardware Requirements or Dependencies

No new hardware dependencies are introduced in SN08.

26.4 Software Requirements or Dependencies

This feature requires only the standard SN08 load on the NGSS.

26.5 Limitations and restrictions

The following limitations exist for this feature:

Provisioning

- NGSS CallP must be restarted anytime a new server certificate is provisioned (CallP is not required to be restarted if remote servers' certificates are provisioned).
- NGSS CallP must be restarted for new values of many security-related parameters to take effect.
- Self-Signed Certificates from other servers must be datafilled on the NGSS in order to have the NGSS recognize those certificates.
- Any Self-Signed Certificate from the current NGSS must be datafilled on other NGSS'es -- and other SIP servers in general -- in order to have the remote servers recognize those certificates.

Note: Restarting NGSS CallP means restarting the SIP gateway application.

Provisioning: FQDN requirement for TLS.

- FQDN stands for "Fully Qualified Domain Name", a domain name that completely describes the address of a computer on the internet. It consists of at least a machine identifier (at the start) plus a top level domain (at the end). It may contain one or more subdomains in the middle. Example: www.nortel.com
- FQDNs are required to provision certificates for TLS under certain circumstances. According to RFC 3280, an FQDN must be no longer than 64 characters.
- Therefore the following limitations have been imposed on domain names for remote server provisioning on the NGSS in SN08:
 - New server names must be 64 or less characters (previous limit: 127 characters).
 - Previously provisioned server names cannot be longer than 64 characters if their provisioning is changed to use TLS. I.E. to use TLS, when the old server name is longer than 64 characters, the server must be renamed.

- The MGC server name on the NGSS Config Data page now has a size limit of 64 characters.

Performance

- Client-side session caching will not be supported on the NGSS. Server-side session-caching is supported. This will mean that session caching cannot be utilized between two SN08 NGSS units. Performance during mass session establishment events may be degraded as a result.

Cryptography

- Only RSA and AES ciphers will be enabled for use on the NGSS by default. These will be the only ciphers supported by Nortel on the NGSS. Specifically, the supported ciphers will be:
 - TLS1_TXT_RSA_WITH_AES_128_SHA and
 - TLS1_TXT_RSA_WITH_AES_256_SHA.
- RSA keys used on the NGSS 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 NGSS will require a minimum of 128 bits.
- Imported certificates will be expected to be in PKCS #12 format, and coded in PEM, in order to be imported for use by the NGSS.

Licensing

- Licenses apply to certain open-source code (OpenSSL, Cryptlib) that we are using in the NGSS 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.

26.6 Glossary

Term	Description
FQDN	Fully Qualified Domain Name, a domain name that completely describes the address of a computer on the internet
TLS	Transport Level Security, a security protocol that enables secure data transmission between two communicating applications.
NGSS	Next Generation Session Server, a SIP CallP Server in Nortel's Succession Networks portfolio of products.

26.7 References

- (a) RFC 2246 The TLS Protocol Version 1.0

(b) RFC 3261 SIP: Session Initiation Protocol

26.8 Appendix for A00006893

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 */

27: A00006894 Functional description (FN)

27.1 Feature name

InterNodal Emergency Stand Alone (ESA) for MG9K

27.2 Description

InterNodal ESA provides the ability to make calls while in ESA between MG9K nodes. In doing so, the Telco's also provide the ability to provision a "Community of Interest" (COI), which defines which MG9K nodes can make ESA calls between one another. Calls cannot be made between the two communities, only within a given community. If an MG9K does not have access to a LAN Switch, it will operate in the pre-SN08 manner of routing calls between VMGs within a single MG9K node. Also, although a Community of Interest is defined, each node must be in ESA for it to participate in the community. Nodes are not forced to enter ESA.

27.3 Hardware Requirements or Dependencies

This feature applies to all supported hardware platforms, per the SN08 Succession server platform foundation software specification. No new hardware is required. A MG9K node in a community must have access to a LAN Switch (i.e. Passport 15000 or equivalent) in order for InterNodal ESA calls to complete.

27.3.1 Passport 15000 Configuration

The inter-MG9000 communication will be provided by the Passport 15000 switch, using the Virtual Router capability to route the IP-based ESA traffic between MG9K gateways.

To deploy this feature in the field, the existing Passport 15000 switches must be configured to support it. This configuration/provisioning consists of: provisioning the Passport 15000 software component and the required engineering to configure the Passports in the field.

A typical deployment scenario for this feature is a collapsed office ("a remote"), which typically consists of a single Passport 15000 switch connecting a group of MG9K gateways to a set of PNNI links back to the CS2000 site. If necessary, the collapsed office can use several Passport 15000 switches.

- Spare pair of 1+1 OC12 or OC3 ports on either 4pOC12 (PQC12) or 4pOC3 (assume ipRoutes > 0).
- Pair 16pOC3 with ipRoutes enabled - there are actually 26 free protected connection entries available when cards are loaded up with the “maximum” of 14 ports.
- Change lp eng arc apc ov to use those 26 connection entries on that APC (pre-SN09 use the eggshell command or HCA in SN09 to do this in service).
- Connect port 14 to 15 on both cards.
- Provision AtmIf - this can theoretically support up to 26 MG9000.

27.4 Software Requirements or Dependencies

This ESA activity on the MG9K is dependent upon two additional activities for successful completion:

- InterNodal Emergency Standalone (ESA) Element Manager (A00007415).
- Passport 15000 Support for MG9000 Inter-node ESA.

27.5 Limitations and restrictions

- No security will be implemented on the ESA SIP Callp Messaging for SN08.
- InterNodal ESA is designed to support a maximum of 15 MG9K nodes. Each node can support a maximum of 4 ABI pairs on the primary shelf and a maximum of 15 sub-tending shelves for a total of 20 VMGs per node. Each COI must be restricted to containing no more than 170 VMGs.
- An ESA Community of Interest (COI) must have access to a LAN Switch (i.e. Passport 15K or equivalent) in order for InterNodal ESA calls to complete.
- If an MG9K does not have access to a IP router (Passport VR), it will operate in the pre-SN08 manner of routing calls between VMGs within a single MG9K node.
- Although a Community of Interest is defined, each node must be in ESA for it to participate in the community. Nodes are not forced to enter ESA.
- A MG9K node can belong to only one Community of Interest at a time.
- All VMGs in a MG9K node must belong to the Community of Interest.
- All VMGs in a MG9K node can independently enter ESA.
- VMGs configured for ESA as either Basic (North American) or Enhanced will be supported within the same Community of Interest. However, VMGs configured as Basic will not be able to handle MADN, hunt group, or other feature specific behaviors included in the Enhanced feature suite.

- Emergency numbers should be provisioned per MG9K node. It is not recommended to rely on accessibility of remote nodes within the community.
- VMGs configured on non-North American Call servers only support ESA Basic (International). Therefore, InterNodal ESA on international switches will only support VMGs configured for ESA Basic within the Community of Interest.
- InterNodal ESA will be supported for both the SLOA (ATM) and SLOIP (IP), and SLOG (GigE) solutions in the SN08 time frame.

27.6 Interactions

None. InterNodal ESA must not inhibit existing ESA functionality. InterNodal ESA must support the Enhanced ESA line services feature set across all nodes in the Community of Interest (COI).

27.7 Glossary

Table 1

Term	Description
ABI	Access Bridge Interface
COI	Community of Interest
ESA	Emergency Stand Alone
I-ESA	InterNodal ESA
LAN	Local Area Network
MG9K	Media Gateway 9000
PVC	Permanent Virtual Circuit
PVR	Passport Virtual Router
SLOA	Switched Lines Over ATM
SLOG	Switched Lines Over Gigabit-Ethernet
SLOIP	Switched Lines Over IP
SVC	Switched Virtual Circuit
VMG	Virtual Media Gateway
VR	Virtual Router

28: A00006901 Functional description (FN)

28.1 Feature name

The name of this feature is Missing Patches

28.2 Description

This feature, Missing Patches, is a feature that addresses several items. The main purpose of this feature is to aid the customer in getting and applying patches to his office in a timely and routine fashion. This feature also address items that will aid the user/customer in maintaining data over an upgrade as well as adding some clean up mechanisms that the user/customer can implement. The following is a list of items that this feature will provide:

- The ability to perform PFRS (Patch File Receipt System) capabilities on demand from the NPM User Interfaces.
- A new PFRS GenReport (pfrsGenReport) task will be available to the user from the Network Patch Manager User Interfaces. This task will allow the user to create an INFORM list that will be automatically dropped off at the customers patch drop off box.
- A new PFRS GetPatch (pfrsGetPatch) task will be available to the user from the Network Patch Manager User Interfaces. This task will go to the customers/users patch drop off box and get the patches that have been newly downloaded and add them to the NPM database.
- A new PFRSGETPATCH_FAIL Major alarm and log will be raised in the event that the PfrsGetPatch Task does not executed successfully. The alarm can only be cleared after a successful execution of the PfrsGetPatch Task.
- A new PFRSGENREPORT_FAIL Major alarm and log will be raised in the event that the PfrsGenReport Task does not executed successfully. The alarm can only be cleared after a successful execution of the PfrsGenReport Task.
- This feature also creates two new system plans for the PFRS functions; one plan will contain the PfrsGetPatch task and the other plan will contain the PfrsGenReport task. Each plan can be scheduled through the NPM Scheduler. This allows flexibility for the customer to schedule and execute PFRS functions according to when each site needs to execute them.
- This feature provides a mechanism that can be accessed from the NPM User Interface that will allow the user to delete patches from the “patch drop off” box. If this function is set in the NPM, the NPM will delete the patches after the PFRS GetPatch function has been executed.
- An automatic audit of a device immediately after a reload. This will provide immediate information back to the user/customer about the device and if patches need to be re-applied.

- This feature adds a new alarm for R-status or released patches; REL_GEN_NOT_APP. This alarm will have a priority of Major.
- The current alarm for GEN patches: GEN_NOT_APP will continue to have a priority of NO_ALARM for all GEN patches.
- This feature also addresses issues with retaining information over upgrades of the NPM and this is responsible for adding the following functions to the NPM. The user will no longer have the ability to change System Defined Reports, Tasks, Sets and Alarms. Users will only be able to modify the execution time and enabled status for System Defined Plans. The user will still have the ability to view the definition of these items via a new “View” button that will be provided on the NPM GUI. The user will still have the ability to create and modify their own reports, plans, tasks, sets and alarms.
- This feature adds a new system plan to the NPM scheduler that will automatically delete reports out of the /data/npm/reports directory. The user will be able to specify the frequency that the reports are deleted through the NPM Scheduler. A default value of thirty days will be set initially in the NPM.
- This feature provides an enhancement to the NPM GUI which will improve overall usability. A process monitor will be added which will provide a visual indicator to the user that a submitted request is in progress. This monitor will be specific to each instance of the NPM GUI and will not indicate activity of multiple GUIs.
- This feature will enhance the NPM GUI Maintenance window. A new refine or filter button will be available which will allow the user to quickly determine which patch(es) are applicable to which device(s) and vice versa.
- This feature will provide the CM CLLI to each NPM GUI window. This will provide clarification when the user is performing patching operations on multiple offices.

28.3 Hardware Requirements or Dependencies

None.

28.4 Software Requirements or Dependencies

None.

28.5 Limitations and restrictions

This feature cannot be patched back to earlier releases due to NPM database changes that must occur with this feature.

28.6 Interactions

None.

28.7 Glossary

Term	Description
NPM	Network Patch Manager
PFRS	Patch File Receipt System
GUI	Graphical User Interface
CLUI	Command Line User Interface

29: A00006905 Functional description (FN)

29.1 Feature name

MG9KEM Recovery Improvements

29.2 Description

The recovery time for the MG9KEM at the 110,000 native SLoA line capacity is 25 minutes. Considering outage risks for our customers, there is a strong business need to limit downtime that may occur from an unplanned OAM&P outage. To this end, this design will lower the MG9KEM recovery to less than 15 minutes.

29.3 Hardware Requirements or Dependencies

This feature will apply to all supported hardware platforms, per SN08 Succession Server Platform Foundation Software specification.

29.4 Software Requirements or Dependencies

None

29.5 Limitations and restrictions

No additional limitations or restrictions

29.6 Interactions

None

29.7 Applicable customer facing sections

Fault Management	
Logs	_____
Alarms	_____
Configuration	
Data Schema	_____
User Interface	_____
Element Management	___X___
Security	_____
Service Order	_____
Office Parameters	_____
Accounting (includes AMA billing)	_____

Performance (includes operational measurements) _____

29.8 Glossary

Table 1

Term	Description
New term	Definition

30: A00006906 Functional description (FN)

30.1 Feature name

SN08 Clock Sync Enhancements

30.2 Description

This Feature covers the software development on the Succession MG9000 (MG9K) node and specifically on the DCC and ITP cards. The clock sync code on the DCC is used to recover a synchronization signal from a Building Integrated Timing Source (aka. BITS, BITS is North American usage) or a Synchronization Supply Unit (aka SSU, International usage) signal. This signal is forwarded to the MG9K ITP card which uses the signal to synchronize the MG9K node.

Prior to SN08, the MG9K only supports the North American standard timing reference (BITS). This system uses DS-1 interfaces which are incompatible with the international standard 2048kHz interface. Lack of 2048kHz interfaces complicates the introduction of MG9K into international markets.

This feature introduces the capability for the NY45FA GiGE DCC circuit pack to connect to an International standard Synchronization Supply Unit (SSU) using 2048kHz interfaces. The NY45FA can use an SSU or BITS signal as a timing reference.

30.3 Hardware Requirements or Dependencies

The new content provided by this feature is only activated if the MG9K NY45FA GiGE card is present in the node. The content of this feature will actually exist in the other DCC loads but will not be activated. Software will determine what behavior (BITS or SSU) to activate based on the PEC code of the DCC hardware along with provisioning information.

30.4 Software Requirements or Dependencies

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

30.5 Limitations and restrictions

- This feature will only be activated if the MG9K has a NY45FA GiGE DCC card(s) in the node.
- This feature only supports 2048kHz signal formats that conform to G703 section 13 and 120 ohm (twisted pair) interfaces. This signal is a 2048 kHz signal, i.e. it does not conform to G.704 frame format. Therefore the following is NOT supported

- 75 ohm load impedance is NOT supported.
- 2048 kbit/s interface is NOT supported. (G.704 frame format)
- This feature is not backward compatible, i.e. downgrading the DCC to a load previous to SN08 will result in a loss of SSU synchronization since that functionality is not provided by previous software releases.
- GiGE DCC cards will not have the ability to obtain a timing reference from the network interface. Provisioning for network timing will be blocked.

30.6 Interactions

In SN08, the MG9K Element Manager (EM) is planning to implement a GUI for the GiGE circuit pack. As part of that GUI is included a Clock sync interface. The intent of the GUI is to represent all of the information that is currently displayed on the clock sync LCI pages plus the inclusion of the new SSU information. The infrastructure for the data is already in place so the interaction with the Element Manager takes place using standard SNMP Gets and Puts. No functionality changes to the Clock Sync code are expected as a result of this related but independent feature.

30.7 Applicable customer facing sections

Functional Description (Mandatory)	<u> X </u>
Fault Management	
Not applicable	<u> </u>
Logs	<u> X </u>
Alarms	<u> X </u>
Configuration	
Not applicable	<u> </u>
Data Schema/MIBs	<u> X </u>
User Interface	<u> X </u>
GUI	<u> X </u>
Element Management	<u> </u>
Security	<u> </u>
Service Order	<u> </u>
Office Parameters	<u> </u>

SOC	_____
Upgrades impact	_____
Accounting (includes AMA billing)	_____
Not Applicable	__X__
Billing changes	_____
Performance	_____
Not Applicable	__X__
Operational Measurements	_____
Performance Measurements	_____

30.8 Glossary

Term	Description
LCI	Local Craft Interface – A web based user interface
SSU	Synchronization Supply Unit

31: A00006925 Functional description (FN)

31.1 Feature name

Virtual Media Gateway (VMG) Robustness

31.2 Description

The purpose of this activity is to improve maintainability and customer usability of VMG and termination provisioning code. Currently, the most frequently seen and most customer-impacting problems involve error handling, GUI displays, audits, and the introduction of new code that breaks existing functions. This activity will focus on design and code improvements in these areas. This activity will not change the current VMG and termination behavior except to make it more robust and user friendly.

31.3 Hardware Requirements or Dependencies

There are no new hardware requirements or dependencies..

31.4 Software Requirements or Dependencies

This activity will be in the SN08 software release.

31.5 Limitations and restrictions

There are no new limitations or restrictions.

31.6 Interactions

This activity may improve the speed of some of the current VMG functions such as audits. In general, the activity will not change existing interactions between VMGs and terminations and other components.

31.7 Glossary

NA

32: A00006944 Functional description (FN)

32.1 Feature name

This feature is the Subnet and Logs Adaptor collapse

32.2 Description

This feature has two purposes:

1. The integration of the MG9000 Subnet Manager server process into the MG9000 Element Manager Factory process.
2. The integration of the MG9000 Element Manager Logs Adaptor into the frameworks of all the other MG9000 Element Manager processes, hence removing the need for a separate Logs Adaptor process.

32.3 Hardware Requirements or Dependencies

No new hardware requirements for this feature.

32.4 Software Requirements or Dependencies

No new software requirements. All external interfaces (IDL) will function as before; hence there will be no dependencies upon other processes. As far as processes external to the MG9000 Element Manager system are concerned, nothing will have changed - this is purely an implementation change internal to the MG9000 EM system.

32.5 Limitations and restrictions

As the external interfaces will not change, external processes will not encounter any extra limitations or restrictions by way of this feature.

32.6 Interactions

Due to external interfaces remaining the same, interactions as currently defined will remain as such; external parties that communicate with the MG9000 Element Manager will maintain there current interaction methods.

32.7 Glossary

Table 1

Term	Description
IDL	Interface Definition Language; the language used to describe CORBA interfaces.

33: A00006957 Functional description (FN)

33.1 Feature name

MG9KEM Deserialization of Patching

33.2 Description

This activity has been created to decrease the time taken to create/build patches.

The process (as it works today) has the following steps

1. The Patch writer creates a branch containing the patch source
2. After the patch branch is tested to work fine, the OPATUI tool is used to create the patch. The following steps are performed by the OPATUI tool
 - i. Copy the FC official load
 - ii. Apply all the V-Status and Released-Status Patches to this load
 - iii. Add the config specs of all V-STATUS and Released Patches (till date for this release) to the current view's config spec
 - iv. Modify the config spec of the current view to include the changes needed for the “current” patch being created
 - v. Build a load in this view (with the updated config spec)
 - vi. Do a diff of all jar files (and scripts?) between the load (as specified in step (b) and the load created in step (e). The diff should only contain the changes introduced by the “current” patch
 - vii. Create a binary of these changes with some wrapper containing some checksum information and this becomes the “patch” binary.
3. This “patch” binary is sent (via NPM) at runtime to the MG9KEM and the patch applied by running a “reverse” diff and applying the changes to the affected jar files

The issue of “serialization” of patch creation occurred because every time the status of a patch changed to V-Status, all other patches (not yet at V-Status), had to be rebuilt after taking into account the changes that went into this new V-Status Patch (since it affected the same jar file). Thus seemingly unrelated patches had to be serialized since it affected the same jar file, and the checksums (and diffs which were used to create the patch binary file) were done at a jar file level.

This activity has been created to address the above mentioned delay in creation of patches.

33.3 Hardware Requirements or Dependencies

None

33.4 Software Requirements or Dependencies

None

33.5 Limitations and restrictions

None

33.6 Interactions

None

33.7 Glossary

Table 1

Term	Description
New term	Definition

34: A00006979 Functional description (FN)

34.1 Feature name

Synchronized Backup Restore Manager

34.2 Naming Conventions

Throughout this document, the backup restore functionality delivered under this feature will be referred to in 3 distinct ways:

Synchronous Backup Restore Manager (SBRM) refers specifically to the IEMS launched synchronized backup/restore software. The SRBM will control/synchronize the backup related activities across other components/devices which contain related backup software.

Device Backup Restore Manager (DBRM) refers specifically to the component/device level backup software which is controlled by the SBRM.

Backup Restore Manager is a generic term encompassing both SBRM and DBRM functionalities and in general simply refers to the software which is common to both.

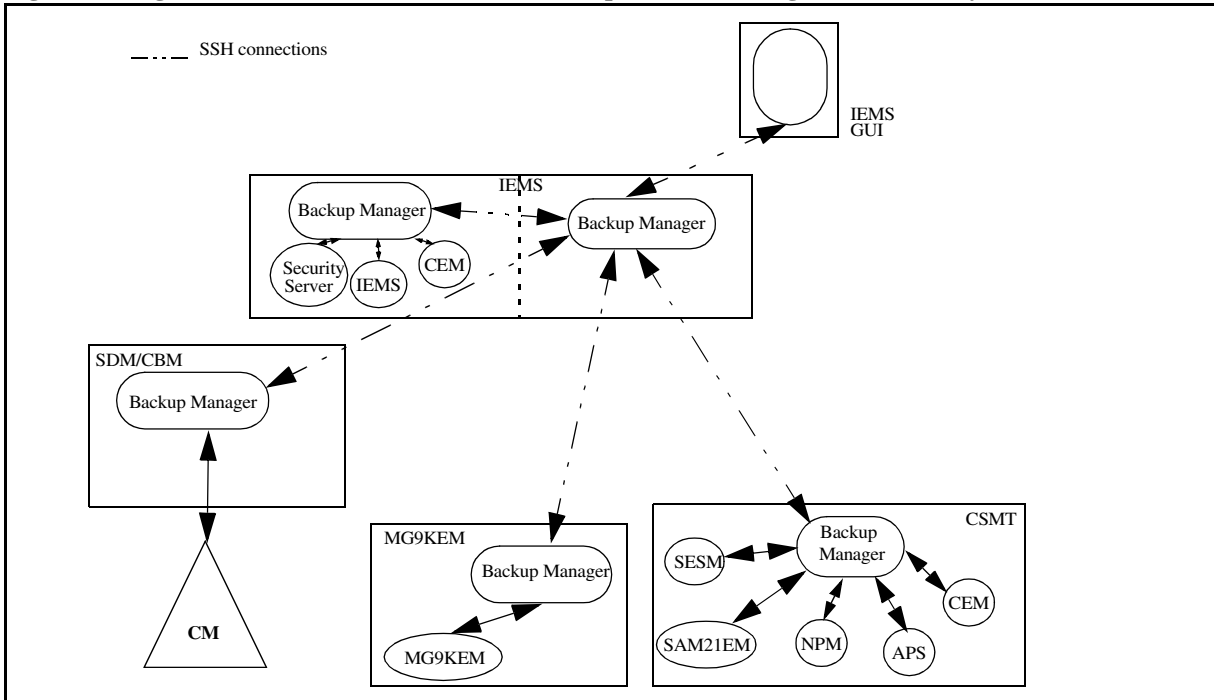
34.3 Description

The feature provides a centralized mechanism allowing the user to initiate a synchronous backup for the core components of the Succession Call Server. Providing this capability reduces the possibility of error caused by manual backup procedures on the various component platforms spread across the Succession Call Server solution.

In SN08, the Synchronous Backup Restore Manager will provide synchronous centralized control of the backup functionality resident within the following Succession Call Server components:

- CallServer 2000 Management Tools (CSMT) server
- MG9000 Element Manager (MG9KEM) server
- Supernode Data Manager (SDM) / Core Billing Manager (CBM) server. The software on the SDM/CBM acts only to allow control of the XACore/3PC backup. No SDM/CBM data is backed up via the Backup Restore Manager software.
- Integrated Element Management System (IEMS) server

Note: The IEMS may reside with the CSMT (and other applications) on the CSMT server.

Figure 1 High Level Functional Overview of Backup Restore Manager Functionality**Functional Description:**

From the IEMS GUI, the user launches the Synchronous Backup Restore Manager command line interface and initiates a backup for the core components of the Succession Call Server. The Synchronous Backup Restore Manager receives the user request, and subsequently initiates a backup command sequence (using CLI commands over SSH) to execute a synchronous backup of the components. Once the backup is complete, the backup files are stored locally on each component.

34.4 Hardware Requirements or Dependencies

None.

34.5 Software Requirements or Dependencies

All platforms requiring Synchronous Backup Restore Manager driven imaging are required to package, install and configure the Backup Restore Manager software. This software should be incorporated within the specific build process of each individual platform.

All platforms requiring Backup Restore Manager software functionality should be Java compatible and should provide a resident Java runtime system (installation).

34.6 Limitations and restrictions

- Restore of generated synchronized backup images is NOT supported in the SN08 Synchronous Backup Restore Manager software. Existing manual restore procedures must be followed in order to utilize the backup images produced by the Backup Restore Manager.
- The Backup Restore Manager system does not perform automatic spooling of backup data/image files to secure/redundant servers. Customers are required to manage their own secure server archiving capabilities. The Backup Restore Manager system will publish data/image files in pre-determined/configurable directories on various servers:
 - SSPSF Platform data/image file location: /data/bkresmgr/backup
 - XACore/3PC data/image file location: *Configurable* - see the CN section of this feature document.
- Backup of program store and associated patches is not covered as part of the functionality associated with Synchronous Backup Restore Manager. If a customer needs to completely 'restore' a server/component, they will need to reinstall their applications and reapply the associated patches.
- The backup "abort" command may require manual cleanup/removal of some backup files. The user will be notified at "abort" command completion time if this is the case.
- The backup process itself can not be executed while certain constructive/destructive system audits are in progress (e.g. SESM's CS2K Data Integrity Audit). In general, if a backup is attempted while these audits are in progress, the backup attempt will be rejected. However, some constructive/destructive audits will be postponed when a backup request is received (e.g. MG9KEM Network Element Audit). The architecture of the system in question determines the appropriate behavior. In general, any system rejections of the backup request will result in an appropriate message being displayed to the Synchronous Backup Restore Manager client user. See section "34.7 Interactions" on page 341 for a full description of system interaction limitations.
- No system wide coordination between Synchronous Backup Restore Manager and other applications (e.g. UpgradeManager, CS2K Audits, CM dump scheduling, etc.) is delivered in SN08. All application activity interdependencies must be manually managed by the user. For example, scheduled activities such as audits should be stopped during system backup. Also, any automated CM image dumps should be cancelled since the Synchronous Backup Restore Manager will be used to drive the dump within a synchronized system wide backup window.
- APS and NPM queries will be disallowed during backup. This is due to the applications being shut down during backup. Active clients will be informed of the application shutdown.

-
- Backup of the MG9KEM in isolation is not recommended due the CSMT platform data dependency. The MG9KEM database is hosted on the CSMT server.
 - Synchronous Backup Restore Manager user authorization only controls the launch of the CLI. CLI Command specific authorization is not provided, therefore only users authorized to actually launch the Synchronous Backup Restore Manager CLI will be allowed to perform query commands at the Synchronous Backup Restore Manager CLI.
 - The software on the SDM/CBM acts only to allow control of the XACore/3PC backup. No SDM/CBM data is backed up via the Backup Restore Manager software.

34.7 Interactions

During the period when the backup is executing, user's of the various GUI and command line provisioning interfaces will be restricted from attempting actions which result in configuration and provisioning data changes. These restrictions include, but are not limited to the following:

- Adding/deleting/updating GWCs at the Call Server Management Tools (CSMT) GUI or OSSGate interface.
- Adding/deleting/updating gateways at the CSMT GUI or OSSGate interface.
- Adding/deleting/updating line service at the at the CSMT OSSGate interface.
- Manually invoking (or running via the scheduler) the various audits at the CSMT GUI.
- Adding/deleting/updating objects in the Integrated Element Management Server (IEMS) topology via the IEMS client.
- Adding/modifying collection jobs via the IEMS client.
- Using the Runtime Administration interface at the IEMS client to perform OSS configuration.
- Using the Security Administration interface at the IEMS client to add/delete Users/Groups/Operations.
- Using the Security Administration interface at the IEMS client to change a user password.
- Adding/deleting/updating Trunks/Carriers via the CSMT
- Node provisioning/deprovisioning via the SAM21EM
- ATM connection set provisioning/deprovisioning via the SAM21EM

34.8 Glossary

Table 1

Term	Description
	Definition
CSMT	Call Server Management Tools
MG9KEM	Media Gateway 9000 Element Manager
SDM	Supernode Data Manager
CBM	Core Billing Manager
IEMS	Integrated Element Management System
SESM	Succession Element and Subelement Manager
OSS	Operations Support System

35: A00006986 Functional description (FN)

35.1 Feature name

H.248 Real-Time and Message Reduction

35.2 Description

The purpose of this feature, H.248 Real Time and Message Reduction, is to reduce real-time usage in the MGC. This will be achieved through the reduction of messages between the MGC and the MG and/or through the reduction of messages internal to the MGC. Although the focus of this feature is ISUP trunking, other call types may receive some benefit.

In the current implementation, two messages are sent for the physical termination on call setup. The first message occurs when a trunk changes from idle to answered or seize. On the outgoing MGC, the second message (for PCM cut through) occurs when an ACM (Address Complete Message) is received from the far end. On the incoming MGC, PCM cut through occurs when answer is detected.

In the new implementation, the two messages are combined and only one message is sent to the gateway for the physical termination during call setup. On the outgoing MGC, this occurs when an ACM (Address Complete Message) is received from the far end. On the incoming MGC, this occurs when answer is detected.

35.3 Hardware Requirements or Dependencies

None.

35.4 Software Requirements or Dependencies

None.

35.5 Limitations and restrictions

The scope of this feature is H.248 ISUP Trunking.

35.6 Interactions

None.

35.7 Applicable customer facing sections

Functional Description (Mandatory)	☒
Fault Management	
Not applicable	☒
Logs	☐

Alarms	_____
Configuration	
Not applicable	___X___
Data Schema/MIBs	_____
User Interface	_____
GUI	_____
Element Management	_____
Security	_____
Service Order	_____
Office Parameters	_____
SOC	_____
Upgrades impact	_____
Accounting (includes AMA billing)	_____
Not Applicable	___X___
Billing changes	_____
Performance	_____
Not Applicable	___X___
Operational Measurements	_____
Performance Measurements	_____

35.8 Glossary

Table 1

Term	Description
ACM	Address Complete Message
ISUP	ISDN User Part
MG	Media Gateway
MGC	Media Gateway Controller
PCM	Pulse Code Modulation

36: A00007000 Functional description (FN)

36.1 Feature name

GIGE Network Interface EM Portion

Reference: DID: A00007000 GigE Network Interface

Livelihood URL: http://livelink.us.nortel.com/livelink/livelink.exe/fetch/2000/2743299/2894744/5685304/5693238/7378022/7409403/A00007000_GIGE_NetwInterface_RQ_v1.pdf?nodeid=7444658&vernum=0

36.2 Description

This document describes the functional description of the new Gigabit Ethernet interface for MG9000. Existing VOIP MG9000 is ATM based IP network Interface. The GigE interface will provide IP connectivity to the MG9000. A new SuperCore Gigabit Ethernet card (known as SCG) which has four ports (one WAN port, other three subtending ports) is being introduced to support GigE configuration. In SN08, subtending ports are not supported.

36.2.1 Display

The user can view the following GigE related parameters:

1. Card data (physical attributes, activity status and software load)
2. Link data (physical attributes, link attributes)
3. Link protection status
4. Performance parameters through Performance Browser:
 - PM/ OM per link
 - RMON per link
 - SMON per VLAN
5. GigE card and link alarms through Alarm Browser.
6. Network interface bandwidth data through Bandwidth Manager:
 - Current ITP voice usage (in bits/second)
 - Current ABI voice usage (in bits/second)
 - Overall network interface utilization (in bits/second)

Note: In SN08, only Switched Lines and ABI services are supported.

7. Clock Synchronization status:
 - Clock status (active/inactive)
 - Chosen reference
 - DAC voltage

36.2.2 Provisioning

The user can view and provision the following attributes:

1. Card state (administrative and configuration state)
2. Link state (administrative and configuration state)

Note: User cannot lock the active WAN port from EM.

3. Facility loopback (enable/disable)
4. Frequency and loss rate for Link Integrity Monitoring
5. Tx RFI and Rx RFI:

Tx RFI and Rx RFI will be ON by default. On disabling, warning message will be displayed to the user.

6. SES to generate UAS:

By default, 10 SES will generate 1 UAS. If it is changed to some other value, a warning message will be displayed to the user.

7. Clock synchronization:

User can provision the Primary and Alternate clock references and their encoding formats. The available references are DCC BITS, ITX BITS and NETWORK (supported by SCO and SCI cards). GigE does not support NETWORK reference. Besides supporting SF and ESF encoding formats (as supported by the SCO and SCI cards), GigE also supports SSU format.

8. Link Reversion:

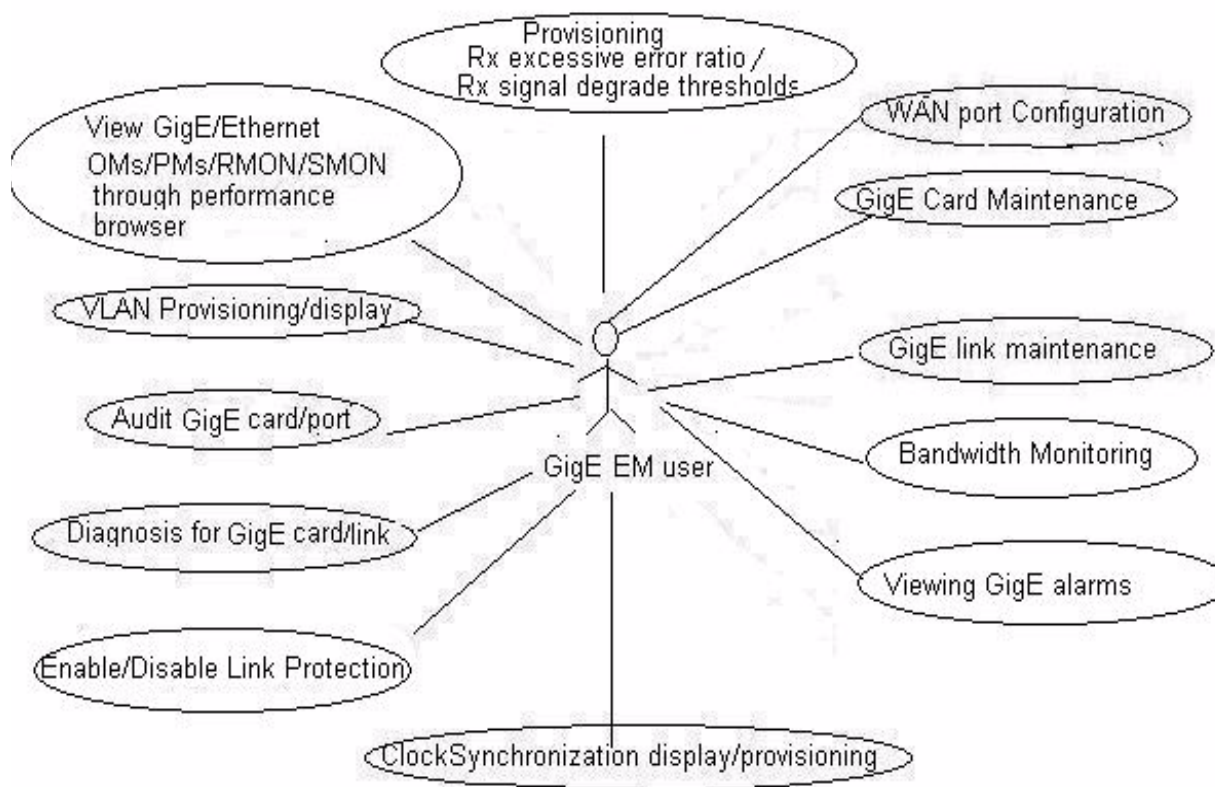
User needs to specify the preferred and non-preferred link along with the wait to revert time for link reversion.

9. VLAN data:

The user can view modify the peak rate and priority for the following VLANs: OAM&P, Bearer, Call Control, 1 for the fixed IP addresses of the active and inactive cards.

10. Inactive WAN configuration:

WAN port can be changed for only inactive SCG card from EM.

Figure 1 Use Case Diagram

More details on this feature can be found in the GigE DID document mentioned Section 2.1.

36.3 Hardware Requirements or Dependencies

A new SuperCore card to support GigE configuration is required.

36.4 Software Requirements or Dependencies

The MG9K GIGE load is required to test EM code changes

36.5 Limitations and restrictions

NONE

36.6 Interactions

NONE

36.7 Glossary

Table 1

Term	Description
ATM	Asynchronous Transfer Mode
RMON	Remote Network Monitoring
UAS	Unavailable Second
SSU	Synchronization Supply Units
SMON	Switched Network Monitoring
SES	Severely Errored Second
RFI	Remote Failure Indication
BITS	Building Integrated Timing Supply
OM	Operational Measurement
WAN	Wide Area Network
ABI	Access Bridge Interface
DSL	Digital Subscriber Line
GigE	Gigabit Ethernet
PM	Performance Monitoring
VLAN	Virtual Local Area Network
DCC	Data Control Card
ITX	Internet Telephony Extender
ITP	Internet Telephony Processor
SCO	SuperCore OC3
SCI	SuperCore DS1 IMA
SF	DS1 Super Frame
ESF	Extended Super Frame
SSU	Synchronization Supply Unit
DAC	Digital to Analogue Converter

37: A00007007 Functional description (FN)

37.1 Feature name

Session Border Controller - Application Layer Gateway

37.2 Description

This activity provides a way for a network operator to separate the Cable hosted network IP address space from the service provider operator IP address space. It will allow the connection of two different IP address space domains without having to understand the exact IP address within the other domain.

This is accomplished through the use of an Application Layer Gateway (ALG). ALGs are NATs that understand the application (in this case, NCS protocol) and enable the application to continue to work even though it is “behind” the NAT. The ALG provides a single IP address interface to the CS2K via a GWC while interfacing to multiple small gateways each with its own unique IP address. For the purposes of this document, these small gateways are said to “subtend” the ALG. The IP address of the gateways which subtend the ALG are not known to the CS2K and thus will be set to 0.0.0.0 during provisioning.

The ALG is positioned in the path of packets flowing from media gateways and media gateway controllers. In this level the ALG provides a level of packet translation without directly participating in the media flow, that is to say the ALG does not directly establish a media path like a gateway, instead it serves as a proxy for the media through a request from the Call Server.

Generally the ALG is transparent to the call server; however to support the insertion of an ALG, the call server must be able to let multiple gateways share a single IP address.

37.2.1 Adding an ALG through SESM

To add an ALG and associate it to a gateway, the following steps must be taken:

1 - From the Network Device view click on the new ALG tab (see section 1.3.1)

2 - Click Add

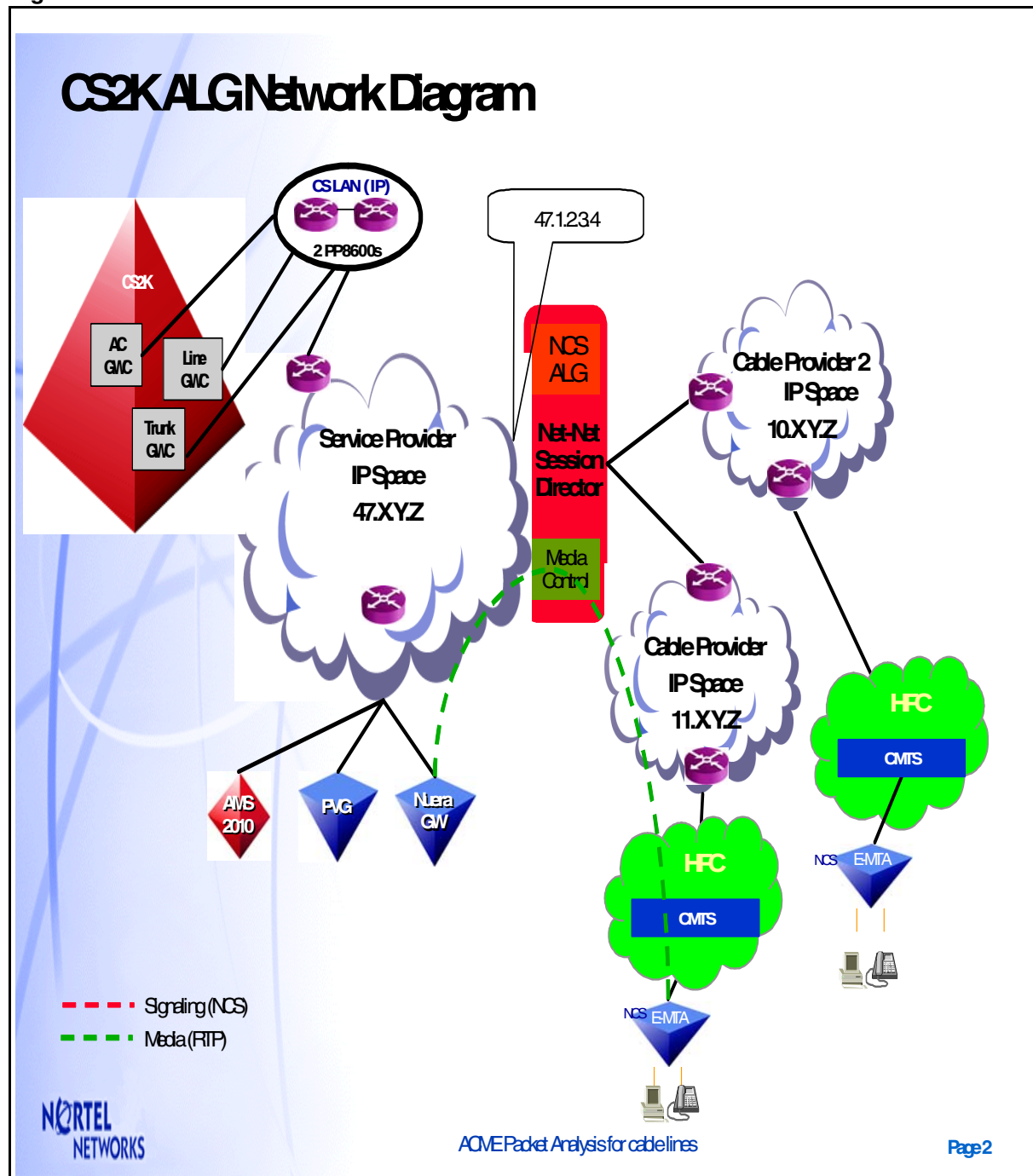
3 - The new ‘Add ALG’ panel is presented, enter the appropriate data. Note: the Port field will be pre-set to the NCS well known port value. It can however be changed by the user (see section 1.3.2)

4 - To associate an ALG while provisioning a new gateway, select the ‘Associate Gateway’ pull down option from the Configuration pull down menu. When the new panel is presented, provide the gateway name, the

gateway profile and the gwc number. When the gateway profile selected is the NCS supported profile, two radio buttons will appear, one for Pep Server and one for ALG. Once the ALG radio button is selected the ALG name must be provided in the field next to the radio button. At this point, the ip address of the gateway will be presented as 0.0.0.0 (see section 1.3.3)

5 - To change ALG assigned to a particular gateway, or to associate an ALG to an existing gateway, select the GWC associated with the gateway, select the Provisioning tab, Gateways tab and retrieve all the gateways. Highlight the gateway to be changed, select 'Change' at the bottom. The 'Change Gateway' panel is presented. Select 'Change ALG'. Enter the new ALG name to be associated (see section 2.8.4)

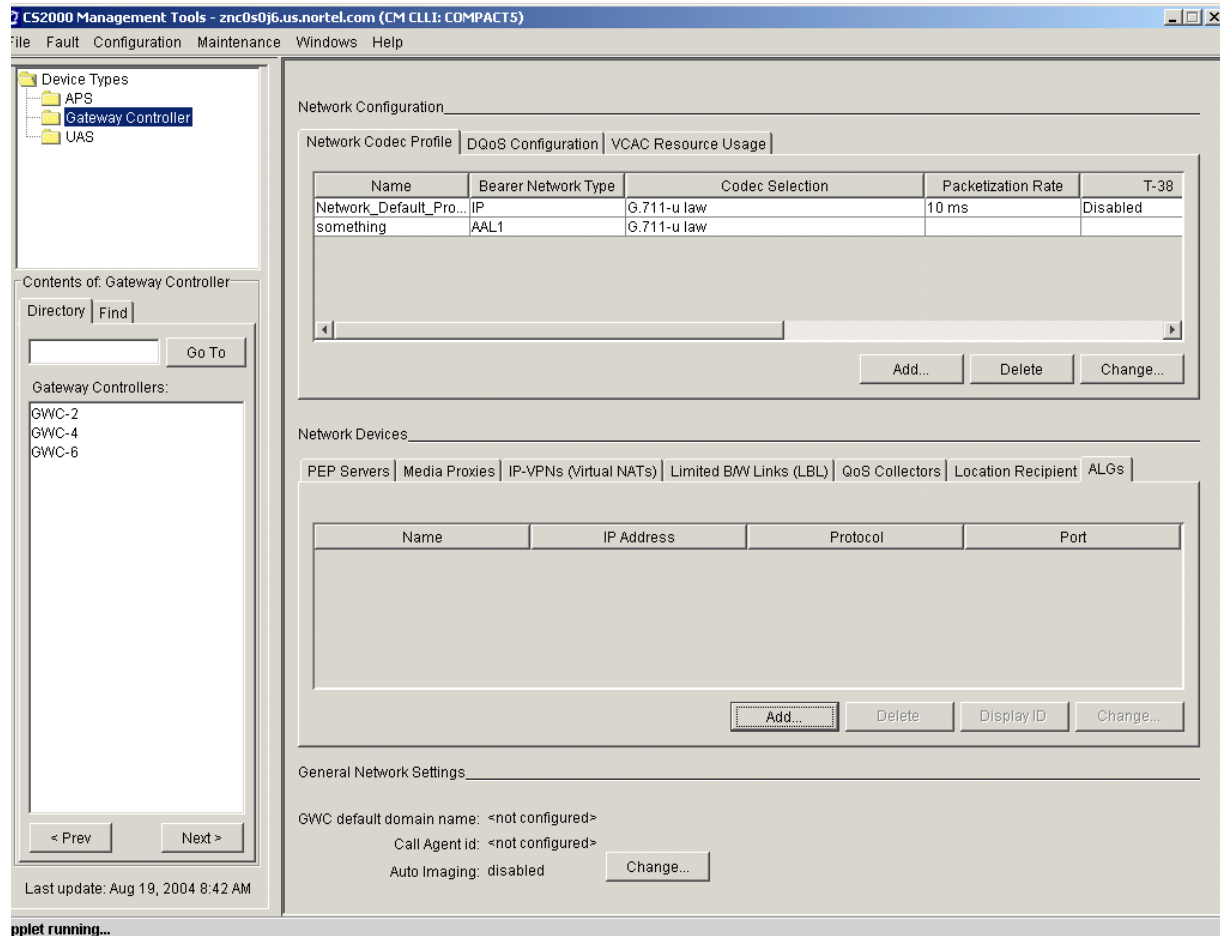
Figure 1 A view of how the ALG will be inserted into our network.



37.3 GWC-EM ALG Provisioning

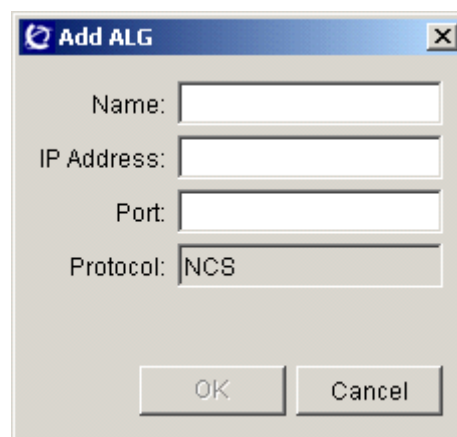
37.3.1 New ALG Nat Tab

The main GUI panel will be modified to add a new tab to allow provisioning of the ALG Nat. The GUI will be presented as follows:



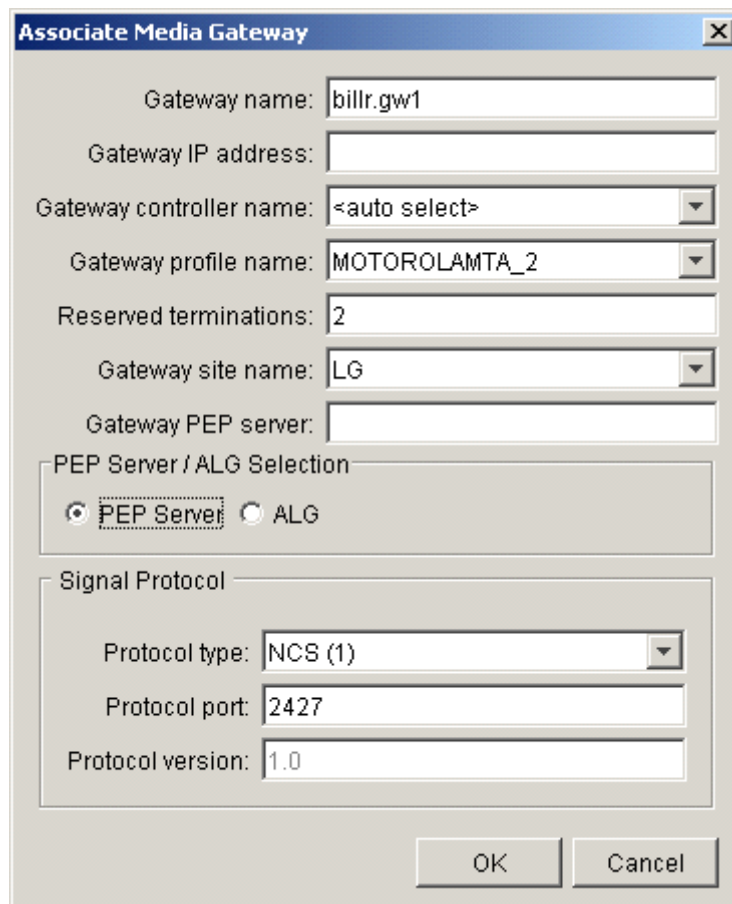
37.3.2 New ALG provisioning Panel

A new pop panel will be provided to add an ALG to the network. The panel will be presented as follows:



37.3.3 Associate Gateway GUI

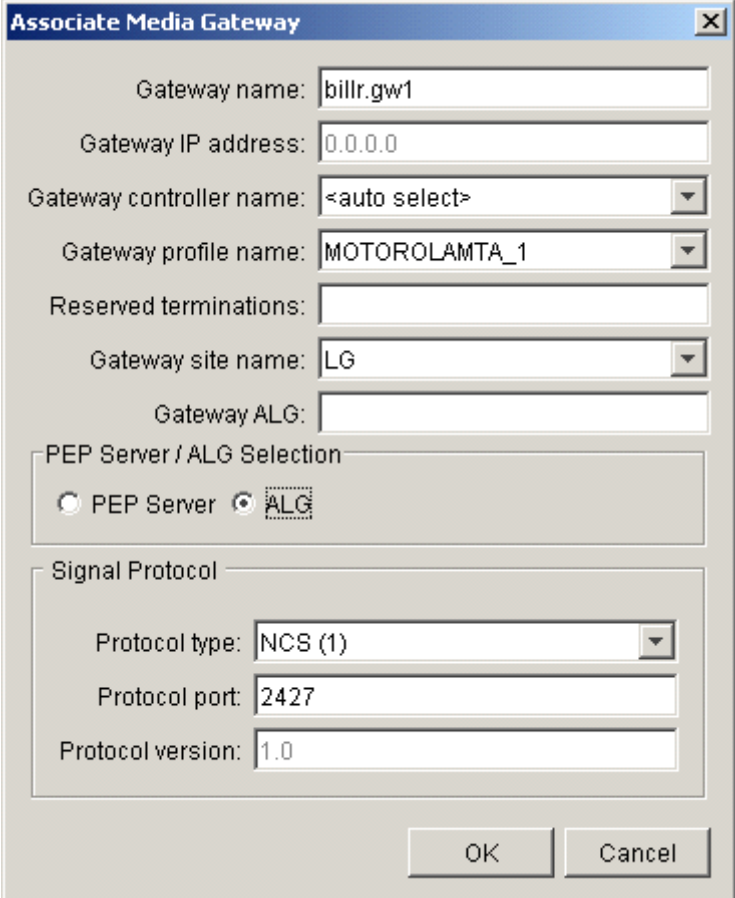
The associate gateway dialogue has been modified to allow the user to associate a new gateway to a GWC, at which time you can associate an ALG Nat to the new gateway. Two options will be provided to allow for either a Pep Server or ALG to be assigned. When the Pep Server radio button is selected the panel will appear as follows:



The image shows a Windows-style dialog box titled "Associate Media Gateway". It contains several input fields and two main sections. The fields are: "Gateway name" with text "billr.gw1", "Gateway IP address" (empty), "Gateway controller name" with a dropdown menu showing "<auto select>", "Gateway profile name" with a dropdown menu showing "MOTOROLAMTA_2", "Reserved terminations" with text "2", "Gateway site name" with a dropdown menu showing "LG", and "Gateway PEP server" (empty). Below these is a section titled "PEP Server / ALG Selection" containing two radio buttons: "PEP Server" (which is selected) and "ALG". Below that is a section titled "Signal Protocol" containing three fields: "Protocol type" with a dropdown menu showing "NCS (1)", "Protocol port" with text "2427", and "Protocol version" with text "1.0". At the bottom right are "OK" and "Cancel" buttons.

Field	Value
Gateway name	billr.gw1
Gateway IP address	
Gateway controller name	<auto select>
Gateway profile name	MOTOROLAMTA_2
Reserved terminations	2
Gateway site name	LG
Gateway PEP server	
PEP Server / ALG Selection	☒ PEP Server ☐ ALG
Signal Protocol	
Protocol type	NCS (1)
Protocol port	2427
Protocol version	1.0

When the ALG radio button is selected, a field will be provided to enter the ALG name. The panel will be presented as follows:

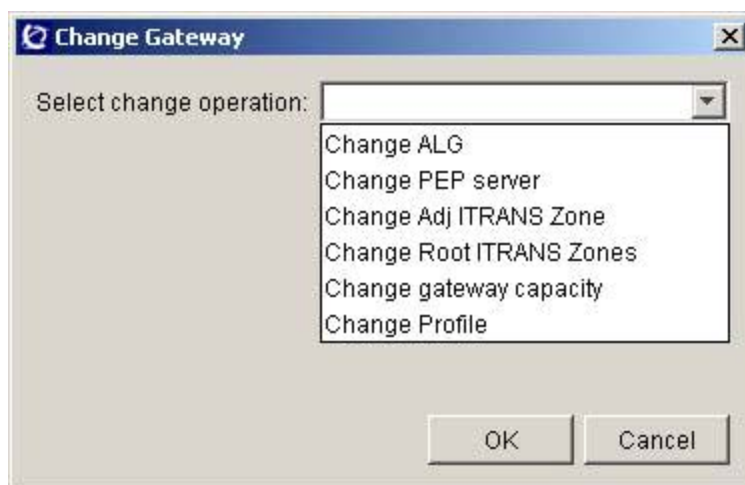
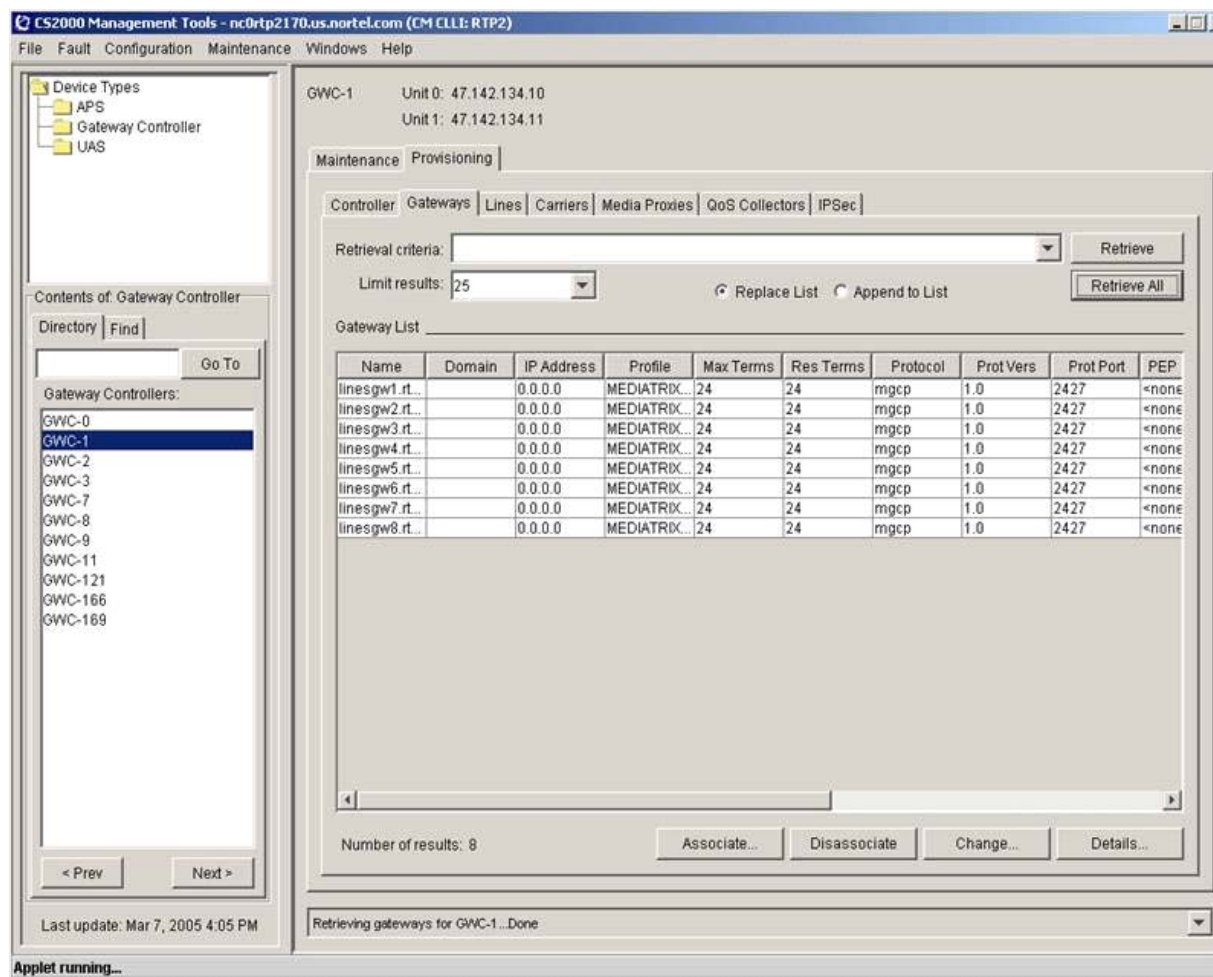


The image shows a Windows-style dialog box titled "Associate Media Gateway". It contains several input fields and a section for selecting between PEP Server and ALG. The fields are: Gateway name (billr.gw1), Gateway IP address (0.0.0.0), Gateway controller name (<auto select>), Gateway profile name (MOTOROLAMTA_1), Reserved terminations (empty), Gateway site name (LG), and Gateway ALG (empty). Below these is a "PEP Server / ALG Selection" section with two radio buttons: "PEP Server" (unselected) and "ALG" (selected). Below that is a "Signal Protocol" section with three fields: Protocol type (NCS (1)), Protocol port (2427), and Protocol version (1.0). At the bottom right are "OK" and "Cancel" buttons.

Gateway name:	billr.gw1
Gateway IP address:	0.0.0.0
Gateway controller name:	<auto select>
Gateway profile name:	MOTOROLAMTA_1
Reserved terminations:	
Gateway site name:	LG
Gateway ALG:	
PEP Server / ALG Selection	
☐ PEP Server	☒ ALG
Signal Protocol	
Protocol type:	NCS (1)
Protocol port:	2427
Protocol version:	1.0

37.3.4 Change Gateway Association

An additional option will be added to the existing change gateway panel to include ALG option. Once the ALG option is selected another panel is provided which allows input of the ALG name to be associated to the gateway. The two panels will be presented as follows:



37.4 XML Interface

This feature implements an XML based command and response protocol. XML command documents are transported via Telnet within the context of a session to the OSSGate component in the SESM. The session is established via a secure logon sequence.

The application supporting this feature receives the XML document instance validates it and then processes the command.

A reply or response XML document instance is returned to the originating Telnet session.

The XML command and response documents for each of the new and modified operations are described in the following sections.

The AssocMG and QueryMG interface has been modified to allow/display ALGs configured in the system.

The following new XML commands have been provided:

- AssocMG
- QueryMG
- ChangeMGGWCEMData
- GetALGData
- getAlgNamesbyGWCId

37.4.1 AssocMG command

Figure 2 XML command AssocMG

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <assocMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>MGXML.5</mgUIName>
          <mgProfileName>MOTOROLAMTA_2</mgProfileName>
          <mgIpAddress>0.0.0.0</mgIpAddress>
          <mgProtocolType>4</mgProtocolType>
          <mgProtocolVersion>1.0</mgProtocolVersion>
          <mgProtocolPort>2427</mgProtocolPort>
          <gwcUIName>GWC-113</gwcUIName>
          <reservedTerminations>4</reservedTerminations>
          <algName>ALG1-0</algName>
        </Parameters>
      </assocMG>
    </Methods>
  </Command>
</CommandList>
```

37.4.2 QueryMG command

Figure 3 XML command for queryMG (No change)

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <queryMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>MGXML.5</mgUIName>
        </Parameters>
      </queryMG>
    </Methods>
  </Command>
</CommandList>
```


Figure 4 XML response for queryMG

```

<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
<Response>
<Interface>cs2kCfgMgrIf</Interface>
<Methods><queryMG usn="1" version="1.0">
<ReturnData>
<Row>
    <mgUIList>MGXML.5</mgUIList>
    <mgIpList>0.0.0.0</mgIpList>
    <callServerId>CABLAB</callServerId>
    <gwcUIName>GWC-0</gwcUIName>
    <svcTypeList>0</svcTypeList>
    <svcTypeList>4</svcTypeList>
    <nodeName>LG 00 0</nodeName>
    <pepServerName>NOT_SET</pepServerName>
    <algName>ALG1-0</algName>
    <engrEndPoints>2</engrEndPoints>
    <protType>ncsprotocol</protType>
    <protVersion>1.0</protVersion>
    <protPort>2427</protPort>
    <profileName>MOTOROLAMTA_2</profileName>
    <maxEngrEndPoints>2</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>
</Row>
    <RC>0</RC>
    <MsgTxt>Query of a Single MG was
    successful</MsgTxt>
</ReturnData>
</queryMG>
</Methods>
</Response>
</CommandList>

```

37.4.3 ChangeMGGWCEMData Command and Response

An example instance of a ChangeMGGWCEMData command follows:

Figure 5 ChangeMGGWCEMData command instance example

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>ALGOSSIf</Interface>
    <Methods>
      <changeMGGWCEMData usn="135" version="1.0" >
        <Parameters>
          <MGUIName>MG1</MGUIName>
          <algName>billr.alg1</algName>
        </Parameters>
      </changeMGGWCEMData>
    </Methods>
  </Command>
</CommandList>
```

An example instance of the response to ChangeMGGWCEMData command follows:

Figure 6 ChangeMGGWCEMData Response XML instance example

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Response>
    <Interface>ALGOSSIf</Interface>
    <Methods>
      <changeMGGWCEMData usn="135" version="1.0">
        <ReturnCode value="0" text="Successful result" />
        <MsgTxt>MG ALG association changed successfully</MsgTxt>
      </changeMGGWCEMData>
    </Methods>
  </Response>
</CommandList>
```

37.4.4 GetALGData Command and Response

An example instance of a GetALGData command follows:

Figure 7 GetALGData command instance

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>ALGOSSIf</Interface>
    <Methods>
      <getALGData usn="1" version="1.0" >
        <Parameters>
          <algName>billr.alg1</algName>
        </Parameters>
      </getALGData >
    </Methods>
  </Command>
</CommandList>
```

A response example to the GetALGData command follows:

Figure 8 GetALGData Response XML document

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Response>
    <Interface>ALGOSSIf</Interface>
    <Methods>
      <getALGData usn=123 version=1.0>
        <ReturnCode value="0" text="Successful result" />
        <MsgTxt>Data Available</MsgTxt>
        <algName>billr.alg1</algName>
        <ServerType>DQoS</ServerType>
        <IPAddress>47.192.234.88</IPAddress>
        <Port>2427</Port>
      </getALGData>
      <getALGData usn=124 version=1.0>
        <ReturnCode value="0" text="Successful result" />
        <MsgTxt>Data Available</MsgTxt>
        <algName>billr.alg1</algName>
        <ServerType>DQoS</ServerType>
        <IPAddress>47.192.234.100</IPAddress>
        <Port>2427</Port>
      </getALGData>
    </Methods>
  </Response>
</CommandList>
```

37.4.5 getAlgNamesbyGWCIId Command and Response

An example instance of a getAlgNamesbyGWCIId command follows:

Figure 9 getAlgNamesbyGWCIId example XML document instance

```
<?xml version="1.0"?>
<CommandList>
  <Command>
    <Interface>ALGOSSIf</Interface>
    <Methods>
      <getAlgNamesbyGWCIId usn="1", version="1.0">
        <Parameters>
          <GWC>GWC_1</GWC>
        </Parameters>
      </getAlgNamesbyGWCIId>
    </Methods>
  </Command>
</CommandList>
```

An example getAlgNamesbyGWCIId response is shown below:

Figure 10 getAlgNamesbyGWCIId example XML instance response

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Response>
    <Interface>ALGOSSIf</Interface>
    <Methods>
      <getAlgNamesbyGWCIId usn="1" version="1.0">
        <ReturnCode value="0" text="Successful result" />
        <MsgTxt>Data Available</MsgTxt>
        <GWC>GWC_1</GWC>
        <algName>billr.alg1</algName>
        <algName>billr.alg2</algName>
        <algName>billr.alg3</algName>
        <algName>billr.alg4</algName>
        <algName>billr.alg5</algName>
      </getAlgNamesbyGWCIId>
      <getAlgNamesbyGWCIId usn="2" version="1.0">
        <ReturnCode value="0" text="Successful result" />
        <MsgTxt>Data Available</MsgTxt>
        <GWC>GWC_5</GWC>
        <algName>billr.alg6</algName>
        <algName>billr.alg7</algName>
        <algName>billr.alg8</algName>
      </getAlgNamesbyGWCIId>
    </Methods>
  </Response>
</CommandList>

```

37.5 Hardware Requirements or Dependencies

No new hardware is required. The application components provided by this feature execute as part of the SESM and GWC.

Integration will be performed with the ACME Net-Net Session Director.

37.6 Software Requirements or Dependencies

No new software or firmware dependencies are introduced by this feature.

37.7 Limitations and restrictions

37.7.1 ALG Limitations

- The CS2K has a limit of 2000 “middleboxes” which is the number of ALGs, PEP servers, NATs and media Proxies combined.
- The CS2K has a limit of 200 ALG middlebox.
- A single GWC on the CS2K has a limit of 20 ALG middleboxes.
- ALGs can only be provision against MTA gateways.
- ALG only supports the NCS protocol.
- Although the ALG solution does not require it, 64 character FQDN support requires that each domain (cable hosted customer) use separate GWC pairs.
- If the ALG does not transmit Audit Endpoint (AUEP) messages to the MTA before the MTA sends its first message (typically an RSIP) then the lines in the CS2K will appear SYSB because the Audit Endpoint is rejected or not responded to. This could happen in the event that the ALG loses all state information and requires the first MTA originated message to re-establish its bindings. To correct this problem, the MTA needs to send any message, e.g. an RSIP or an offhook and this will re-establish the binding and clear the SYSB state on the line. This problem will not occur if the ALG vendor supports discovery through the use of DNS of the MTA IP Address before the MTA sends its first message.

37.7.2 Packet Cable Protocol Limitations

- DQoS is not supported on an MTA behind an ALG. Nortel is not aware of any ALG on the market that supports DQOS.
- IPSEC is not supported since a NAT device will cause end to end (GWC to MTA) security to fail because of the IP address and message content manipulation done by the ALG.
- Packetcable Electronic Surveillance can not be fully supported with an ALG. This is because the specification requires the transport of the MTA IP address which is not available to the CS2K. However, regular DMS packet electronic surveillance is supported.
- Event Messaging is partially supported. We support event messaging, but since DQoS is not supported, CMTS records will not appear.

37.7.3 DNS Limitations

- If a Redirecting Media Gateway Controller (RMGC) is configured, the DNS servers must be configured correctly. For example the ALG upon receiving the response from the RMGC on the CS2K, must be able allow

the gateway to resolve the Fully Qualified Domain Name (FQDN) in the message thru DNS queries.

- DNS is not supported by the CS2K to discover the ALG IP address. We only support static configuration of the IP address of the ALG since it is not expected that there will be many ALGs.
- DNS is not required by the CS2K to discover the IP address of the MTA (although it may be used in the cable IP space) because the CS2K no longer needs the cable MTA IP address. Therefore DNS discovery is automatically disabled for gateways behind ALGs.

37.7.4 Other CS2K Limitations

- The GWC specified must have the small lines gateway profile in order to support provisioning of ALG.
- When an ALG is associated to a gateway a DQOS PEP Servers, Low Band Width (LBL), IP-VPN Nats will not be allowed on the same gateway.
- The IP address of the gateway being associated with an ALG will not be modified. If the IP address field is left blank, the default value of 0.0.0.0 will be provision against the gateway.
- CS2K QoS collector will collect statistics as reported by the ALG. There is no separation of statistics between the ALG boundaries.
- A Nortel Media Proxy is not supported for the cable MTAs that are behind an ALG since they are both performing a similar function. However, the Media Proxy is supported for other gateways in the solution that need it.
- The real IP address of the MTA is not known by the call server and therefore the ALG IP address will be used in those cases.

37.8 Interactions

The following existing GUIs have been modified:

- New ALG dialog for creating the ALG
- Associate Media Gateway Dialog
- Change Gateway Dialog

The following XML commands have been modified:

- AssocMG
- QueryMG
- ChangeMGGWCEMData
- GetALGData
- getAlgNamesbyGWCId

The on-line help facility will be updated with information on the use, syntax and valid values for all the above modifications/additions.

37.9 Applicable customer facing sections

Fault Management

Logs _N/A_

Alarms _N/A_

Configuration

Data Schema _X_

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_

37.10 Glossary

Term	Description
New term	Definition
ALG	Application Layer Gateway
GW	Gateway
SBC	Session Border Controller
NAT	Network Address Translation

37.11 Appendix A - XSD changes

The following changes will be made to support XML schema:

Module: albase.xsd:

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  version="1.0"
  xml:lang="en" >
```

```

<xsd:include schemaLocation="../../../algossif/algcommon.xsd"/>
<xsd:include schemaLocation="../../../algossif/changemggwcemdata.xsd"/>
<xsd:include schemaLocation="../../../algossif/getalgdata.xsd"/>
<xsd:include schemaLocation="../../../algossif/getalgbygwcid.xsd"/>
<!--
*****
***** -->
<!-- ** Define Parser Convention Required elements -->
<!-- ** These are CommandList (root element), Comand, Interface, Methods -->
<!--
*****
-->
<xsd:element name="CommandList" >
  <xsd:complexType >
    <xsd:sequence>
      <xsd:element name="Command" type="CommandType" />
    </xsd:sequence>
  </xsd:complexType >
</xsd:element>

<!-- Define CommandType -->
<xsd:complexType name="CommandType">
  <xsd:sequence>
    <xsd:element name="Interface" type="ALGOSSIfType" />
    <xsd:element name="Methods" type="ALGOSSIfMethodsType" />
  </xsd:sequence>
</xsd:complexType>

***** -->
<!-- ** Define ALGOSSIfType -->
<!-- ***** -->

<!-- ALGOSSIfType -->
<xsd:simpleType name="ALGOSSIfType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="ALGOSSIf" />
  </xsd:restriction>
</xsd:simpleType>

<!-- ***** -->

<!-- * Define interface ALGOSSIfMethodsType -->
<!-- ***** -->

<xsd:complexType name="ALGOSSIfMethodsType">
  <xsd:choice minOccurs="0" maxOccurs="unbounded">
    <xsd:element name="changeMGGWCemData"
type="changeMGGWCemDataMethodType" />
    <xsd:element name="getALGData" type="getALGDataMethodType" />
    <xsd:element name="getAlgNamesbyGWCId"
type="getAlgNamesbyGWCIdMethodType" />

```

```

    </xsd:choice>
  </xsd:complexType>
</xsd:schema>

```

Module : changemggwcemdata.xsd:

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
            xml:lang="en" >

  <!-- ***** -->
  <!-- * Define GWCCConfiguration changeGateway Method Parameters -->
  <!-- ***** -->
  <xsd:complexType name="changeMGGWCEMDataMethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="changeMGGWCEMDataParamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="changeMGGWCEMDataParamsType">
    <xsd:sequence>
      <xsd:element name="MGUIName" type="NoSpaceNameType" />
      <xsd:element name="algName" type="xsd:token" minOccurs="0" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

```

Module : getALGdata.xsd:

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
            xml:lang="en" >

  <!-- ***** -->
  <!-- * Define GWCCConfiguration getALGByFilter Method Parameters -->
  <!-- ***** -->
  <xsd:complexType name="getALGDataMethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="getALGDataType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="getALGDataType">
    <xsd:sequence>
      <xsd:element name="algName" type="NoSpaceNameType" />
    </xsd:sequence>
  </xsd:complexType>

```

</xsd:schema>

Module : ALGcommon.xsd:

```
<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="1" />
      <xsd:pattern value="\d{1}" />
    </xsd:restriction>
  </xsd:simpleType>

```

```

    </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 IpPortTypeType-->
<!-- ***** -->
<xsd:simpleType name="IPPortType">
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="0" />
    <xsd:maxInclusive value="65535" />
  </xsd:restriction>
</xsd:simpleType>
</xsd:schema>

```

Module : getALGbygwcid.xsd:

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  version="1.0"
  xml:lang="en" >

  <!-- ***** -->
  <!-- * Define GWCConfiguration getAlgNamesbyGWCID Method Parameters -->
  <!-- ***** -->
  <xsd:complexType name="getAlgNamesbyGWCIdMethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="getAlgNamesbyGWCIdType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="getAlgNamesbyGWCIdType">
    <xsd:sequence>
      <xsd:element name="GWC" type="GWCNameType" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

```

37.12 Appendix B: XML Commands: description of method parameters

37.12.1 Parameter definitions

- **encoding??**
- **version** - The version refers to the version of the method or operation - e.g., the changeALGMiddleboxNames operation may have version 1.0 and 2.0, where version 1.0 takes parameters X and Y and version 2.0 takes parms X, Y, and Z. TYPE *decimal*.
- **usn** - Unique Sequence Number. This parameter is introduced to facilitate sending multiple XML commands in one file. This parameter value will be used to match the responses with the requests. TYPE *integer*.
- **ReturnCode value**- A numeric value indicating the result of the attempted operation (see Table 3, for range and definitions of each possible value). TYPE *string*.
- **Return code text**- Appropriate text that describes the result of the operation. TYPE *string*.
- **ALGMiddleboxName1** - The Middlebox name(s) of the ALG node middlebox(es). TYPE *NoSpaceNameType*. (32 character token without spaces, see xsd definitions in Appendix A.

37.12.2 Method Parameters

Method parameters are defined below. Input data is mandatory except where indicated otherwise.

1. **AssocMG** - Method to associate a gateway to the CS2K. This method has the following NEW parameters: (only NEW ones described, see standard documentation for the other definitions).
 - Input data:
 - usn
 - version
 - ALGMiddleboxName (Optional, Cannot be included as well as pepServerName) - defines the ALG (optional) for this gateway.
 - 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. **QueryMG** - Method that gets the gateway information from a CS2K. This method has the following NEW Output parameters: (only NEW ones described, see standard documentation for the other definitions):
 - Output data:
 - ALGMiddleboxName - defines the ALG Middlebox for this gateway.
 -
 3. **changeALG**- Method that changes the ALG for a given gateway. This method has the following parameters:
 - Input data:
 - usn
 - version
 - MGname indicates the gateway that this change command is for.
 - ALGName - defines the new ALG name
 - 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.

38: A00007024 Functional description (FN)

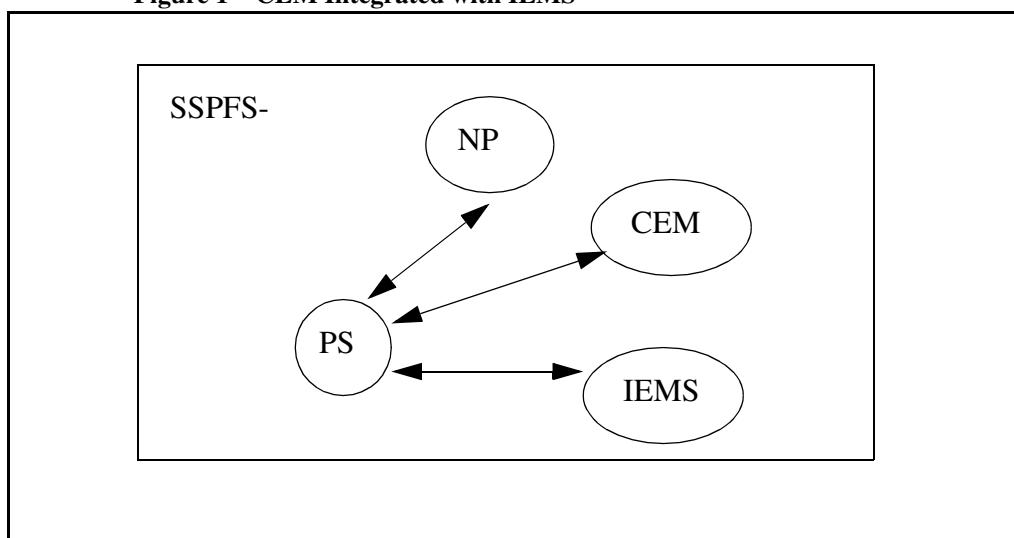
38.1 Feature name

Core Element Manager (CEM) Patching

38.2 Description

In SN08, the CEM will be integrated with the Integrated Element Management System (IEMS) on Solaris. IEMS is patched via the Network Patch Manager (NPM). It is required that one patch management system be used with all applications on the same node, therefore the CEM integrated with IEMS will also be patched by the NPM.

Figure 1 CEM Integrated with IEMS



38.2.1 Incremental Cumulative Patching

CEM patches are incremental cumulative. Each patch contains the fixes that prior patches introduced, but only the fix content that has been introduced since the final compile version of the CEM load is included in each patch. This allows a customer to apply only the latest patch if desired since it will contain all of the fix content included in previous patches. CEM patches are delivered by RPS. There is only one Released patch at any given point in time, unless it is the first patch for the load which can be at Verified or Released status. After a patch is Released, 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 CEM patches and perform maintenance patching activities on the CEM. All patching functionality available in NPM is available for CEM patching.

With this methodology of patching, if 3 patches have been released 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. If only patch 3 is applied, when patch 3 is removed, patch 2 and patch 1 are also removed.

38.2.2 Patching Maintenance

When the new NPM patchable CEM application is installed, the NPM automatically becomes aware of it. CEM appears in reports and the device list of the GUI. The following functions that exist for other targets are now available for CEM.

- apply
- remove
- audit
- restart
- set/report creation
- plans/automation
- alarms

38.2.2.1 CEM Patch Application and Removal

Like existing OAM Java-based applications such as SESM, SAM21EM, or IEMS components, the CEM 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)
- restart command from the NPM GUI or CLUI on IEMS (sets patch to applied/enabled)

removal

- remove command from the NPM GUI or CLUI (sets patch to removed/enabled)
- restart command from the NPM GUI or CLUI on IEMS to disable the patch (sets patch to removed/disabled)

When CEM is running in a clustered configuration, the 2 step application and removal of patches is necessary only on the active side of the SSPFS-based machine. A restart from the NPM GUI or CLUI on the inactive instance of the CEM application is not required to enable or disable patches. When a patch

is applied or removed on the inactive CEM application, the patch is automatically enabled or disabled since the CEM application is not running on the inactive SSPFS-based machine

The apply and restart operations from the NPM GUI and CLUI can be automatically scheduled via NPM plans (autoapply and autorestart).

38.2.3 Patchid Modification

The patchid has been modified to allow greater than 8 character patchids. The patchid format for CEM patches can have up to 32 alpha-numeric characters. The CEM patchid does not contain records that identify the target or release to which the patch is applicable. An example CEM patchid is CEM_PATCH.17.1-20040901.

In SN08, CEM will be the only product to take advantage of the expanded patchid. The current 8 character patchid format will remain for all other products for which NPM manages patches.

38.2.4 Patch File Format Modifications

The patch file format is modified with this feature to implement the incremental cumulative nature of CEM patching. The following additions and changes have been made.

- A new **H** record is introduced to track included patches. This new record is stored in the ADM section of the patch file and is included only in CEM patches. Zero to many of these records can exist.
H INCLUDED_PATCH <patchid> where patchid is the name of the patch included
- A new **V** record is introduced to track the patch file format version. This record is added to all NPM managed patches.
- The **I** record is enhanced. If a patchid is greater than 8 characters it will not fit in the normal patchid position of the I record. The placement for patchid will be filled with 8 characters of something other than the real patchid, and the E record will contain the actual patchid.

38.3 Hardware Requirements or Dependencies

None.

38.4 Software Requirements or Dependencies

The MTX18 CEM load is required to interact with NPM

38.5 Limitations and restrictions

None

38.6 Interactions

Feature A00007304 - CEM I & C on IEMS

38.7 Glossary

Table 1

Term	Description
NPM	Network Patch Manager
CEM	Core Element Manager
RPS	Regional Patch Selector

39: A00007054 Functional description (FN)

39.1 Feature name

H.248 Protocol Compliance Enhancements for GWC

39.2 Description

This feature enhances the compliance of the GWC implementation of H.248 to the H.248.1 version 1 specification. Specifically, this feature adds the following capabilities to the GWC H.248 implementation:

- Parser overhaul
- Reorganization of Package Code
- Root Terms
- Outgoing ServiceChange Commands
- Incoming ServiceChange on Ephemerals
- Update H.248 Package Compliancy
- Move H.248 debug into TAPITRACE
- Support for DNS Addresses
- Support for the Wildcard Response (W-) and Optional Command (O-) flags
- Support for Incremental Compliance by MGs
- Package Inheritance and Versioning Framework

39.3 Hardware Requirements or Dependencies

None.

39.4 Software Requirements or Dependencies

None.

39.5 Limitations and restrictions

None.

39.6 Interactions

This feature introduces several new signalling scenarios that could cause the MGs to cease working correctly over a GWC upgrade. In order to manage this, the GWC will make use of the profiles mechanism of the H.248 protocol in order to determine when certain MGs become capable of utilizing the more compliant messaging. The affected MGs are: PVG, MG9000ATM, MG9000IP, CICM, UAS and AMS. When these MGs upgrade with newer, more compliant

loads, they will announce their new capability by sending the profile string to the GWC. The GWC will then use the compliant messaging with the MG.

These differences will not affect customer-visible function of the CS2000.

39.7 Glossary

Term	Description
AMS	AudioCodes Media Server
ATM	Asynchronous Transfer Mode
CICM	Centrex IP Communications Manager
CS2000	Communications Server 2000
GWC	Gateway Controller
IP	Internet Protocol
MG	Media Gateway
PVG	Passport Voice Gateway
UAS	Universal Audio Server

40: A00007071 Functional description (FN)

40.1 Feature name

SN08 3rd Party GW Interop Profiles

40.2 Description

This document describes provisioning aspects associated with the 3rd Party Gateway (GW) Interop activity which is introduced into the SN08 release. GW profiles are used as a means to define various aspects of a GW such as the number of Endpoints (EP), Protocol, etc. These attributes and others are updated on the Call Server 2000 Management Tools (CMT) platform and distributed to the GWC and XaCore platforms.

Prior to this activity, introducing a new profile was a cumbersome task that required software updates and typically required the formal process of creating a new “feature”. As a result, turnaround time to introduce a new profile was excessive.

Starting in SN08, many new 3rd Party GWs will be “Interop Tested” with the Nortel Succession Hardware and Software. Interop testing is a process where a vendor makes their product available (a GW in this case) and Nortel Networks personnel test to insure that the equipment integrates into the system and functions correctly.

To facilitate the rapid introduction of new profiles, this activity will make updates that allow Interop personnel to introduce a new profile by creating a file and putting it in a predefined location on the CMT platform. Creation of the file is accomplished by including a list of predefined attributes that will uniquely describe a profile. In theory, all attributes that a vendor needs to define the new profile are made available for inclusion in the profile. The file that describes the profile has been given the generic label of “Certificate” and will be referenced as such in subsequent sections of this document and other associated documents.

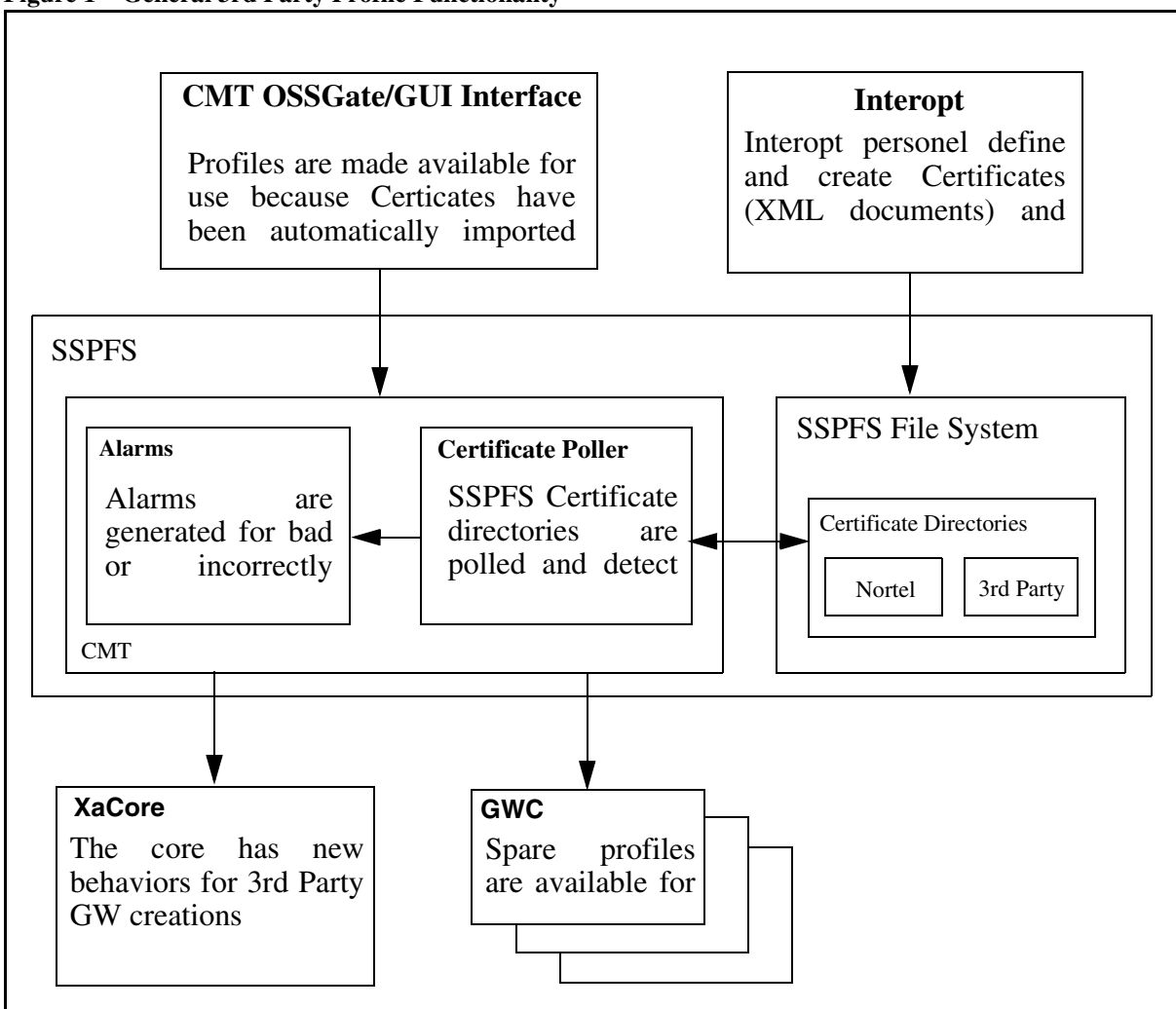
The diagram below depicts the major components of the 3rd Party Profiles feature and the general functionality. For specific details for creation and installation of a new Certificate refer to the accompanying documentation in the CN.

In order to provide these new functionalities, the customer will see changes in the following areas:

- SESM
 - Certificates which define a profile are read into the system and made available for provisioning.

- GWC
 - Spare profiles numbers are made available and should be used for new profiles.
- Core
 - Table LGRPINV is a Core table which is (with only minor expectations) auto-provisioned from the SESM. A new optional field is added by this feature. While this field will be visible, it will not be provisionable until a later release. For details on this optional field, refer to Data Base Schema Information which is located in the Configuration section of this design document.

Figure 1 General 3rd Party Profile Functionality



40.3 Hardware Requirements or Dependencies

There are no hardware dependencies required to execute this feature.

40.4 Software Requirements or Dependencies

Each of the following components must be at the specific software load for this feature to function properly:

- SESM - SN08 release
- GWC - SN08 release
- CORE - SN08 release (BCS 56) or later

40.5 Limitations and restrictions

40.5.1 CMT

- The Succession system is set up so that the upgrade of the CMT is performed prior to the upgrade of the GWC and XaCore. If an attempt is made to add a new 3rd Party Certificate prior to the upgrade of the XaCore the request will fail. This is because a new field value for the LGRPINV table is introduced by this activity and this value is not valid until XaCore software is upgraded to SN08. In addition, if the GWCs are at a pre-SN08 version attempts to use a “spare” GWC profile number introduced in the SN08 stream will fail also.
- If a GW needs modifications to a profile, manipulation of the Certificate is not allowed; to accomplish this change, a new Certificate should be added and the Change GW Profile operation should be used.
- This activity has removed the Protocol and Version field from the Associate MG OSSGate command. Therefore, existing Associate MG XML documents must be modified to remove these fields.

40.5.2 GWC

Limitation on the number of spare profiles are:

- 25 spare profiles for each existing unique GW profile of small line GW type,
- 25 spare profiles for each existing unique GW profile of large line GW type,
- 25 spare profiles for each existing unique GW profile of trunk GW type,
- 20 spare profiles for each existing unique GW profile of H.323 GW type.

The setting of flags of the spare profiles are pre-defined, so that if none of the spare profile supports the requirements of the new gateway, then it is expected

that the GW will be modified to work correctly with one of pre-defined spare profile. In addition, the spare profiles flags could be updated via patch.

40.5.3 CORE

- Even though a new optional field GTWY_ID is visible in table LGRPINV with this feature, datafilling this value is blocked until a later release.

40.6 Interactions

The following are the feature interactions for A00007071 feature:

- Features which A00007071 is dependant on:
 - none
- Feature which are dependant on A00007071:

A00007072 - 3RD PARTY GW INTEROP PREPROVISIONING

- A00007072 required the new Logical GroupType to be defined in the Core. This new GroupType is provided by A00007071.
- Features which have an interaction with A00007071:
 - none

40.7 Applicable customer facing sections

Fault Management

Logs	_____
Alarms	__X__

Configuration

Upgrades	__X__

Data Schema	__X__

User Interface	__X__

Element Management	__X__

Security	_____

Service Order	_____

Office Parameters	_____

Accounting (includes AMA billing)	_____

Performance (includes operational measurements)	_____

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	<u> X </u>
Engineering Information	<u> X </u>

40.8 Glossary

Acronym	Definition
ASPEN	Nortel proprietary GW control protocol (not an acronym).
BLM	Business Line Management
CLLI	Common Language Location Identifier
CM	Computing Module
CMT	Call Server 2000 Management Tools
CORBA	Common Object Request Broker Architecture
CPE	Customer Premises Equipment
CS	Call Server
CS2K	Call Server 2000
DDMS	DMS Data Management System
DMS	Digital Multiplex System
DTC	Digital Trunk Controller
DTCI	ISDN Digital Trunk Controller
DTD	Document Type Definition
EPID	End Point Identifier
ETSI	European Telecommunications Standards Institute
GPS	Global Product Support
GUI	Graphical User Interface
GW	Gateway
GWC	Gateway Controller
GWC EM	Gateway Controller Element Manager
H.323	Industry protocol for GW/GK<->GW/GK communication (not an acronym).
HLD	High Level Design
HTML	HyperText Markup Language
IDL	Interface Definition Language

IP	Internet Protocol
ITA	Internet Transparency Agent
JAR	Java Archive
JDBC	Java Database Connectivity
JNLP	Java Network Launching Protocol
JWS	Java Web Start
LAN	Local Area Network
LTC	Line/Trunk Controller
MEGACO	H.248. Industry protocol for MG/MGC <->MG/MGC communication.
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Block
MI2	Manatee Iteration II
MOP	Method of Procedure
MTC	Maintenance
NA	North American
NAT	Network Address Translator
NN	Node Number
NPM	Network Patch Manager
NTNA	Northern Telecom North American (proprietary PRI variant)
NV	Network View
OAM&P	Operations, Administration, Maintenance and Provisioning
OSS	Operation Support System
OSSDI	OSS Data Interface
PRI	Primary Rate Interface
PLM	Product Line Management
PSTN	Public Switched Telephone Network
PTM	Packet Telephony Manager
RMGC	Redirecting Media Gateway Controller

SDM	SuperNode Data Manager
SESM	Succession Element and Sub-Element Manager [system]
SNMP	Simple Network Management Protocol
SQL	Structured Query Language (for DBs)
SSPFS	Succession Solaris Platform Foundation Software
SS7	Signaling System 7
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TID	Terminal Identifier
TMM	Trunk Maintenance Manager
TN	Terminal Number
XML	Extensible Markup Language

41: A00007072 Functional description (FN)

41.1 Feature name

3rd Party GW Interop Pre Provisioning

41.2 Description

Feature A0007072 will deliver end-point pre-provisioning capability in the Succession Element and Sub-element Manager (SESM) required for the third party GW inter-op with Succession OAMP system.

This feature provides the following major functionalities:

- Ability to associate a third party large line GW with its GWC and assign a node in the CS2K Core based on user specified frame and the unit numbers.
- Ability to pre-provision the GW end-points from the OSSGATE interface using XML.
- Ability to delete GW end-points from the OSSGATE interface using XML.
- Ability to query GW end-points from the OSSGATE interface using XML.
- Ability to export a query end-point XML output response as an add end-point input XML request.
- Ability to perform bulk provisioning using Batch Provisioning Tool (bpt).
- Ability to view the output from all the above XML operations in a nicely formatted html.

41.3 Hardware Requirements or Dependencies

Not applicable.

41.4 Software Requirements or Dependencies

Not applicable.

41.5 Limitations and restrictions

- Only XML based machine interface is provided for end-point provisioning of third party large line GWs.
- Change end-point command is not supported.

41.6 Interactions

This feature facilitates end-point provisioning of third party GWs. End-point format is defined by the GW profile specified during the provisioning of the GW. The profile definitions are facilitated by the GW Profile feature, Activity A00007071.

The gateway end-points must be pre-provisioned before attempting to assign service to these end-points.

41.7 Applicable customer facing sections

Fault Management

Logs ☐ N/A ☐

Alarms ☐ N/A ☐

Configuration

Data Schema ☐ X ☐

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 ☐

41.8 Glossary

Term	Description
GW	GateWay
GWC	GateWay Controller
XML	eXtended Markup Language

42: A00007074 Functional description (FN)

42.1 Feature name

GigE Link Maintenance

42.2 Description

Link maintenance provides two major areas of functionality for the GigE physical link, configuration and monitoring.

42.2.1 Configuration

Attributes for each of the links are provisioned by the LCI and maintained by Link Maintenance. Attributes include the auto-negotiation parameters and service state for a given link.

Link protection groups are managed as well. Protection group types and the link to protection group mappings are associated in link maintenance. Currently only 1+1 protection groups are supported in SN08. Revertive behavior is provided allowing preferred paths through the network.

A complete listing of the settable attributes can be found in the MIB section of the CN.

42.2.2 Monitoring

Link maintenance provides the operational interface for each of the GigE ports. The service state of each port can be changed and the operational state reported. On going service metrics are collected and reportable through the MIBs. Threshold crossings are also reported if so provisioned.

When configured, link maintenance provides a means to ensure that each link in a protection group is both transmitting and receiving data. This heartbeat is bi-directional between the links and uses a layer 2 frame. Frames are sent periodically between the links and verified at the receiving link. Manual testing is available through the LCI.

Link maintenance maintains and reports fault conditions of each port. These include events such as loss of signal. Recovery actions are taken if possible to provide continuing service. Types of faults and actions are detailed in the FM section of this document.

42.3 Hardware Requirements or Dependencies

Not Applicable

42.4 Software Requirements or Dependencies

Not Applicable

42.5 Limitations and restrictions

Not applicable.

42.6 Interactions

Link Maintenance interacts with the following systems for configuration and operational management:

- CMT
- LCI

42.7 Glossary

Term	Description
GigE	Gigabit Ethernet
LCI	Local Craft Interface

43: A00007100 Functional description (FN)

43.1 Feature name

Gateway Controller Card Evolution.

43.2 Description

The GWC hardware platform was selected in 1999. At the time, the 366 Mhz CPU and 128 Mbytes of memory were more than sufficient for its planned use. As always, the requirements placed on the platform became greater and greater. The CPU and especially memory resources dwindled quickly. A cost efficient solution was needed quickly, with the following general guidelines:

- Compact PCI / PowerPC for shelf and load build tools compatibility
- Greater RAM capacity
- At least 2X CPU speed improvement
- Comparable cost per port to the current GWC
- 1-Gigabit Ethernet

43.2.1 Overview

The MCPN905 is a high-performance hot-swap CompactPCI Peripheral Slot CPU board. The MCPN905 incorporates the MPC7455/57 CPU, the Marvell MV64360 System Controller, and the Intel 21555 PCI-to-PCI bridge. The MCPN905 supports up to 3 GB of DDR DRAM, two PMC slots, 8 MB of boot Flash, up to 64 MB of soldered Flash, three Gigabit Ethernet ports and one IDE port. The MCPN905 supports a 64bit, 33/66 MHz PCI interface to the CompactPCI backplane. The MCPN905 also supports the CompactPCI Packet Switching Backplane (PICMG 2.16) and the CompactPCI System Management (PICMG 2.9) specifications.

43.2.2 Features

43.2.2.1 Processor

- Single MPC7455/7457 Processor
- Core Frequency to 1.3 GHz
- Bus Frequency of 133 MHz
- Integrated L1 and L2 cache
- Address and data bus parity

43.2.2.2 Flash Storage

- Bank A: 16-64 MB soldered Flash using two Intel StrataFlash devices

- Bank B: 8 MB Flash using two Intel StrataFlash devices
- Reset vector is jumper selectable between Banks A and B

43.2.2.3 System Memory

- Up to 3 GB of DDR266 (133 Mhz) SDRAM onboard
- Double-Bit-Error detect, Single-Bit-Error correct across 72 bits
- Memory controller function provided by Marvell MV64360 System Controller
- 32KB NVRAM provided by M48T37V

43.2.2.4 PMC Slots

- PMC 2: 64-bit, 33/66 MHz PCI or 66/100/133 MHz PCI-X with front-panel I/O plus rear I/O
- PMC 1: 32/64-bit, 33/66 MHz PCI or 66 MHz PCI-X (33/66 MHz PCI only with 21555 bridge, 33 MHz PCI only with IDE, 32-bit only with front-panel Gigabit Ethernet)
- Both slots support Processor PMCs

43.2.2.5 Ethernet Interface

- Three Gigabit Ethernet channels provided by the Marvell MV64360
- Two to J3 for PICMG 2.16 compliance
- One to front panel (optional)

43.2.2.6 PCI Interface

- One local PCI/PCI-X bus supporting 32/64-bit, 33/66 MHz PCI or 66/100/133 MHz PCI-X to PMC 1
- One local PCI/PCI-X bus supporting 32/64-bit, 33/66 MHz PCI or 66 MHz PCI-X to PMC 2, the 21555 PCI bridge, and optional IDE controller (33/66 MHz PCI only if 21555 is populated, 33 MHz PCI only if IDE is populated)



43.3 Hardware Requirements or Dependencies

The Motorola MCPN905 requires a chassis containing a compactPci backplane and system boards providing bus arbitration. Both the 8221 and the MXP chassis are supported. The MCPN905 itself can act as a system slot or non-system slot board without reconfiguration – the Sentinel “universal-mode” PCI-to-PCI bridge can provide bus control when the card is occupying a system slot.

43.4 Software Requirements or Dependencies

The new GWC hardware may only be provisioned after the shelf controller and GWC element manager software are upgraded to SN06. Older revisions of the shelf controller will not recognize the new hardware.

43.5 Limitations and restrictions

N/A

43.6 Interactions

43.6.1 Shelf Controller

The maintenance system that is currently in place allows the customer to manage the various cards in the SAM21 via the SAM21 Element Manager and the SAM21 Shelf Controllers. The currently deployed hardware (MCPN750) has full support for the various maintenance actions available via the shelf controller.

This includes:

- Detection of board removal and insertion from the SAM21
- Detection of board type, MAC address (es), memory size, Power-On-Self-Test errors, and firmware version
- Provisioning of IP Address, Gateway IP Address, load path and name, and application specific firmware settings.
- Unlocking (Booting) and Locking (halting) of the provisioned application
- Automatic firmware flash of board
- Out-of-Service Diagnostics (brief and full)

The Shelf Controller uses a Motorola firmware utility known as VTERM to acquire serial access to the MCP750 over the backplane, this same firmware utility will be available with the MCPN905 firmware.

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
New term	definition

44: A00007101 Functional description (FN)

44.1 Feature name

GWC Telnet Authentication

44.2 Description

The GWC has a command line interface (CLI) which is used for debugging, testing, data collection, etc. In this activity it will be referred to as “PMDebug”, whether this CLI is accessed through the faceplate serial port, by telnetting to a card IP address, or by using the core “pmdebug” command. Currently, the GWC only prompts for a password for telnet access, and only for telnet from a non-EM IP address. This activity replaces the existing login mechanism for accessing PMDebug (telnet to GWC IP address, “gonow”; or using the serial port) with a user-id/password login system which has a standard look and feel. Login from the core via “pmdebug” command is not changed (no password is needed).

Every user connecting to a GWC will see a standard login banner and login prompt, which will ask for user-id and password. When entering the password, it will not be echoed. Telnet connections from any device or the serial port connections behave identically for logging in. The output sent currently over the serial port will continue to be output there, but to enter any commands a login will be required. User-ids are defined on the IEMS security server, and any account defined there which has “mgcadm” group privileges will be able to login to a GWC. Five failing login attempts will result in a disconnected telnet session, and you will have to telnet again. Successful login will connect directly into PMDebug, and it will function as it currently does. A login session left idle with no input (default time probably 30 minutes) will be automatically disconnected.

Functionality similar to the existing “force out” command will be available. Any user-id which can login, may force out another user using either interface.

Although it is preferable to use the accounts defined on the security server for normal operation, there will also be a new default “local” access user-id/password always available on the GWC. Planning for this local account schema is ongoing (see the discussion in DID section Design Component 2), but it should be something like user-id of “admin” and a password made of the MAC address of the card. The local password can be changed on the GWC by anyone who can login to it, and changes will be stored persistently, even across lock/unlock of the unit. This local password can be reset to the default value, or changed to a new password, by anyone who can login to the device. If the local password has been changed and the security server is unavailable, card

replacement will be required if urgent recovery of access is needed (except from core pmdebug access).

This activity will add a number of new customer (syslog local1/info) and security logs (syslog local3/info) which will be stored in /var/log/*log on the CS2M server and forwarded upstream. There will be a custlog generated if:

- the security server is not accessible or not responding
- the provisioned EM IP address of the GWC is changed (also used as the security and log server address)

Based on interpretation of the reference docs and requirements, there will be security events logged for the following:

- telnet connection login attempt
- serial connection login attempt
- login retry threshold exceeded
- login attempt fails because of authorization failure (authentication succeeds, but not group membership check)
- logout (by request, force out, or idle timeout)
- local account login (success or failure)
- local password change/reset by command
- GWC restarting (if telnet is connected)

44.3 Hardware Requirements or Dependencies

None

44.4 Software Requirements or Dependencies

Authorization of defined or new users is controlled by group memberships managed by the IEMS security system, which includes a set of standard group privileges. Only and All user-ids which are members of the “mgcadm” group will be able to login to GWCs. All SN08 GWCs will utilize the new login system, and there is no backwards compatibility allowing the old “gonow” login mechanism after the feature completes.

If a SSPFS box hosting IEMS is not accessible from the CS2M, the CS2M will respond with authentication reflecting its local password/group setup, so if the IEMS security server is not available, the accounts/authorizations defined on the CS2M server will be the ones controlling access to the GWC.

44.5 Limitations and restrictions

Only as noted above in descriptions.

44.6 Interactions

Other authentication/logins for the GWC are not affected (e.g. SNMP community, FTP login). The interruption from the core login to retrieve trap data (“CC Trapinfo logged on”) will still occur.

45: A00007102 Functional description (FN)

45.1 Feature name

Dual C-Side IP for GWC

45.2 Description

This feature will eliminate the requirement to provision a default gateway IP address when provisioning a GWC. The gateway IP will be automatically provisioned for all GWCs. This eliminates provisioning errors. When the call server is an XA-Core, the two available core IP addresses will be automatically distributed across the GWCs.

45.3 Hardware Requirements or Dependencies

None

45.4 Software Requirements or Dependencies

This is a new gateway controller element manager feature contained within the CS2M software load.

45.5 Limitations and restrictions

None

45.6 Interactions

None

45.7 Glossary

Table 1

Term	Description
GWC	Gateway Controller

46: A00007107 Functional description (FN)

46.1 Feature name

Media Gateway 9000 5/30 Minute Operational Measurements

46.2 Description

The OM collector currently collects OM's from different tables on a fixed 15 minute schedule. The MG9K stores the previous 96 15 minute interval data so it covers 24 hours of information. This feature changes the timing of these intervals to be configurable from the EM. The user can select any number of minutes as the standard interval. Also, the MG9K will be changed to store only 48 of blocks of interval data for non RFC-driven MIB tables. RFC-compliant tables will continue to have 96 blocks of intervals stored. The feature also provides for a second or extended OM interval. This extended interval is longer than the standard interval and is a time that is a multiple of the time in a standard interval. The data in the extended interval is computed based on the data for the appropriate number of standard intervals.

The new interval requirement does not apply to all OM's. It only applies to those that are collected by the OM collector. These tables are listed in the following table.

Table 1 Impacted OM Tables

OM Table	Subsystem
SNMP miscellaneous	SNMP
nnPmSnmPomIntervTable	SNMP
nnPmUtilOmIntervTable	PerfMon
nnPmOvldRscIntervTable	PerfMon-Ovld
nnPmOvldConnDenyIntervTable	PerfMon-Ovld
norCarrSonetMediumIntervalTable	Carrier-Sonet
sonetSectionIntervalTable	Carrier-Sonet
sonetLineIntervalTable	Carrier-Sonet
sonetPathIntervalTable	Carrier-Sonet
apsChanStatusTable	Carrier-Sonet
imaGroupIntervalTable	Carrier-IMA
imaLinkIntervalTable	Carrier-IMA
nnClkSyncSignalTable	ClkSync
nnClkSyncRefTable	ClkSync
nnBwShelfCurrentSloaBandwResrvdTable	Bandwidth
nnBwShelfIntervalSloaBandwResrvdTable	Bandwidth
nnBwAbiCurrentBandwResrvdTable	Bandwidth
nnBwAbiIntervalBandwResrvdEntry	Bandwidth
nnBwIntervalBandwUtilTable	Bandwidth
nnBwIntervalQueueFillTable	Bandwidth
nnMegacoOMDSPIntervalTable	Megaco

nnMegacoOMCESIntervalTable	Megaco
nnMegacoOMECAIntervalTable	Megaco
nnMegacoOMMedGwyIntervalTable	Megaco
nnRelMsgSctpAssocOmIntervalTable	SCTP
nnMegacoQoSIntervalTable	Megaco-IP
nnIpsecOmIntervalTable	IpSec

A user can change the OM interval at any time. The most common usage is expected to be a change from 15 minute intervals to 5 minute intervals. If the user makes a change at 9:37 then at the next hour boundary (10:00), the historical data for OM intervals is flushed. The first interval with the new timing will be from 10:00 to 10:05. If the user also configures an extended interval of 30 minutes, then the first extended interval will be 10:00 to 10:30 and will just be a rolup of the 6 5 minute intervals.

46.3 Hardware Requirements or Dependencies

There are no new hardware requirements for this feature.

46.4 Software Requirements or Dependencies

The only other software required for this feature is the regular SN08 version of the MG9K EM which contains the functionality to configure the OM intervals.

46.5 Limitations and restrictions

There are restrictions on the values that may be configured for the standard and extended intervals. Both intervals are specified in minutes and the extended interval must be evenly divisible by the standard interval. The minimum standard interval is 1 minute.

When the intervals are changed at the EM, the historical values for the previous 96 intervals are flushed from the MG9K. Also, the change to the new interval is not made until the hour boundary following the EM change. For example, if a user changes from 15 minute to 5 minute intervals at 9:37, the transition will be delayed until 10:00.

46.6 Interactions

46.7 Applicable customer facing sections

Functional Description (Mandatory) X

Fault Management

Not applicable

Logs

Alarms	_____
Configuration	
Not applicable	_____
Data Schema/MIBs	_____X_____
User Interface	_____
GUI	_____
Element Management	_____X_____
Security	_____
Service Order	_____
Office Parameters	_____
SOC	_____
Upgrades impact	_____
Accounting (includes AMA billing)	_____
Not Applicable	_____
Billing changes	_____
Performance	_____
Not Applicable	_____
Operational Measurements	_____X_____
Performance Measurements	_____

46.8 Glossary

ABI	Access Bridge Interface
ATM	Asynchronous Transfer Mode
IP	Internet Protocol
ITP	Internet Telephony Processor
MIB	Management Information Base
MG9K	Media Gateway 9000
NV	Network View
OM	Operational Measurement
PM	Performance Measurement (term used for OM's in Carrier Maintenance)
SCTP	Stream Control Transmission Protocol
SNMP	Simple Network Management Protocol

47: A00007108 Functional description (FN)

This document is intended to provide a high-level view of the enhancements being made within the MG9000 during the SN08 time frame. These enhancements are focusing on those related to the handling of the Session Description Protocol (SDP) and include the following:

- Increase the maximum supported SDP size to 1000 bytes for both Local and Remote SDP strings.
- Interwork with MCS and NGSS based SIP phones. The MCS Interworking will be addressed under ICAF A00007474 and the NGSS Interworking will be addresses under ICAF A00007475.
- Reduce memory usage.
- Improve real-time.

47.1 Feature name

MG9000 Session Description Protocol (SDP) Enhancements for SN08

47.2 Description

The purpose of this SN08 activity is to provide some means of recovering memory and real-time on both the ITP and ABI cards. By doing so, the life expectancy of the older ITP and ABI boards can be extended. This provides our current customers with some added benefits and delays their need to upgrade to the newer boards that were introduced in SN07.

In addition, this feature is tasked with being able to provide support for longer SDP strings. This change will lay the foundation needed to support MCS and SIP interworking with MG9K lines. With the introduction of T.38 looming on the horizon, the need to support longer SDP strings is a must. This feature will increase the size to allow for SDP strings up to 1000 bytes in length.

Note: SDP strings in excess of 1000 bytes will result in an error code being returned to the GWC.

47.3 Hardware Requirements or Dependencies

There are no new hardware requirements or dependencies introduced by this feature.

47.4 Software Requirements or Dependencies

There are no new software requirements or dependencies introduced by this feature.

47.5 Limitations and restrictions

The maximum supported SDP length will be increased from 511 to 1000 bytes.

47.6 Interactions

SDP is needed to establish the bearer path for all types of calls, so these base changes will have an impact on every call. Other than the modifications to SDP handling, this feature has no other special interactions with other features.

47.7 Glossary

Table 1

Term	Description
GWC	GateWay Controller
MG9000	Media Gateway 9000
SDP	Session Description Protocol

48: A00007113 Functional description (FN)

48.1 Feature name

GWC External Interface Robustness

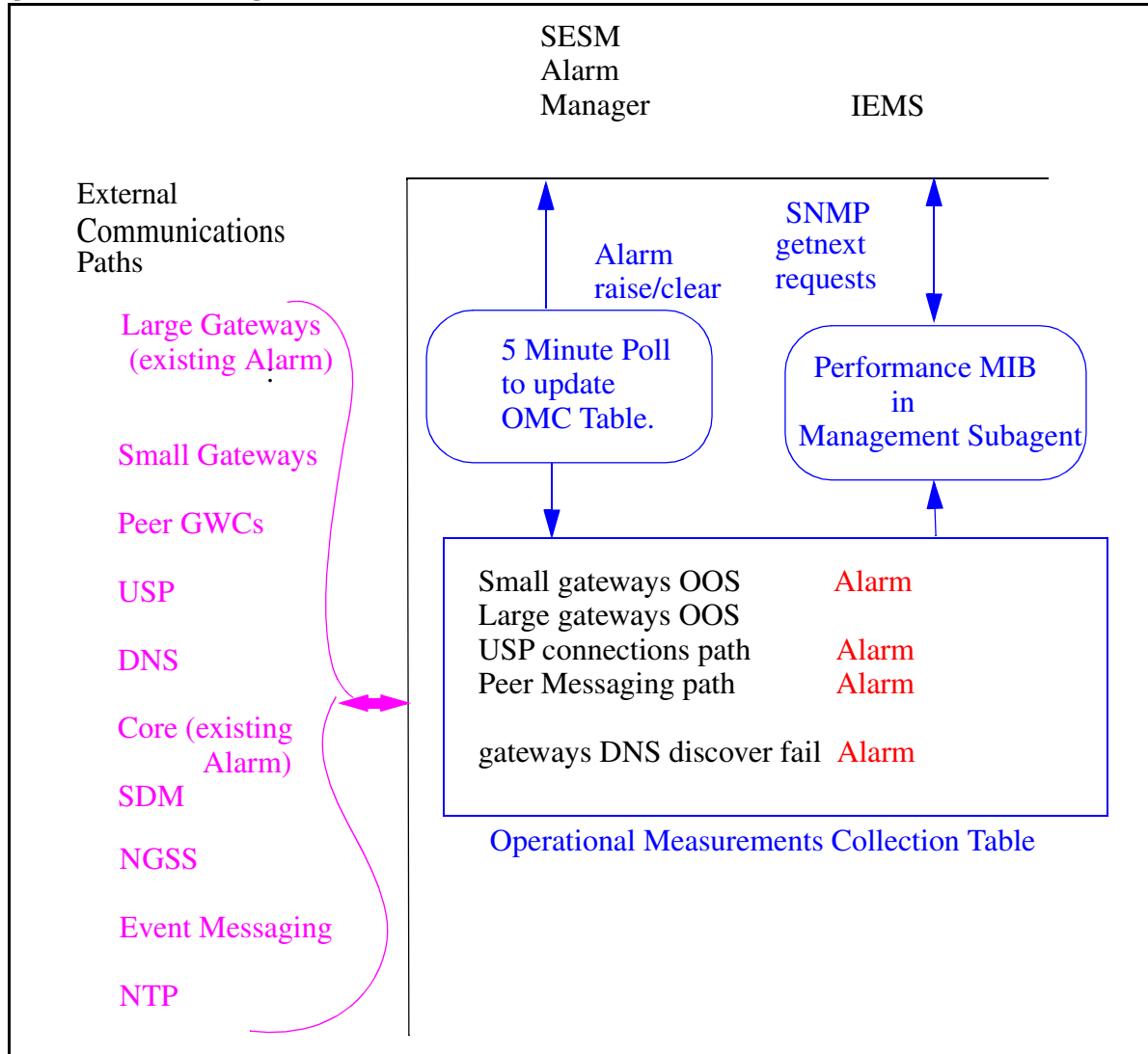
48.2 Description

This feature is aimed at enhancing error reporting of external communication paths from the Gateway Controllers (GWCs) and External hosts such as gateways, peer GWCs and USP. New alarms are added to report communication path lost and new Operational Measurements (OMs) are collected by IEMS every 5 minutes.

The customer will use the existing SESM alarm manager for the new alarms. IEMS will be configured to receive the new OMs every 5 minutes. Only the Active GWC will report the OMs, while the inactive will report no OMs found in table.

The behavior diagram below shows all the GWC communication paths and which ones have been included for OM collections as part of this feature.

Five new alarms are introduced in this feature and their detail description is in the optfm.did section of the document.

Figure 1 Behavior Diagram

48.3 Hardware Requirements or Dependencies

Not Applicable.

48.4 Software Requirements or Dependencies

This functionality is available for SN08 and above.

48.5 Limitations and restrictions

Due to time constraints, the following interfaces will be handled in future releases:

SDM - This interface is used for the bootptab file. In future releases the bootptab file will be moved to the SSPFS host where the SAM21-EM resides.

NTP - Network Time Protocol Server. When this interface is not there, the battery operated clock on the GWC is used to get the time.

NGSS - counters and alarms will be added in later releases.

Event Messaging - counters and alarms will be added in later release.

48.6 Interactions

Not Applicable.

48.7 Glossary

Table 1

Term	Description
GWC	Gateway Controller
OM	Operational Measurements

49: A00007114 Functional description (FN)

49.1 Feature name

TGCP Compliancy

49.2 Description

The TGCP Compliancy feature builds upon the SN07 activity “TGCP for the Cable Market” (A00003630) which implemented the Trunking Gateway Control Protocol (TGCP) for ISDN User Part (ISUP) and Per Trunk Signaling (PTS) trunk groups on the Succession Call Server 2000 (CS2K).

Specifically, this activity provides further compliancy in the Media Gateway Controller (MGC) towards the TGCP PKT-SP-TGCP-I08-040721 specification with respect to:

- providing audible ring tones to the Public Switch Telephone Network (PSTN) operators for operator ringback;
- support of the MF Terminating Protocol (MT) Package changes(i.e., call block (MT/bl) event);
- new return codes (i.e., 407 and 538);
- receiving TGCP Media Gateway (MG) messages specifying an endpoint range;
- RestartInProgress messages for graceful restart methods (including specified restart delay timings); and
- RestartInProgress messages for cancel-graceful restart methods.

The capability provided by this activity is supported for the North American Integrated Access - Cable (IAC) solution.

For more detail regarding the TGCP ISUP and PTS functionality supported on the CS2K, refer to SN07 activity “TGCP for the Cable Market” (A00003630) documentation.

49.3 Functional Description

The functionality for audible ringing via Multimedia Terminal Adapter (MTA) for Operator Ringback is described here due to the lack of documentation in the TGCP specification. For the other compliancy items not described below, refer to the TGCP PKT-SP-TGCP-I08-040721 specification for more details.

49.3.1 Operator Ringback Audible Ringing via MTA

The Operator Ringback capability requires audible ringing to be played to the PSTN operator while physical ringing or Receiver Off Hook (ROH) tone is being applied to caller. The TGCP MF FGD Operator Services (MO) package

does not provide a ring tone signal which may be applied to the PSTN operator over the connection.

CableLabs and PacketCable multi-vendor community expects the audible ringing towards the PSTN operator be provided by the Multimedia Terminal Adapter (MTA) via the RTP stream by signalling the Call Management Server (CMS) to instruct the MTA.

In SN08/GC080, due to lack of support by MTAs, Operator Ringback audible ringing will continue to be provided by trunk gateway as in SN07/GC070. Operator Ringback audible ringing via MTA, although present, will be defaulted to disabled. For now, Operator Ringback audible ringing via MTA will be enabled using a private GWC load or patch when functionality is required.

49.3.2 Graceful/Cancel-Graceful Restart Methods

The graceful restart method provides a means for the MG to instruct the MGC to not create any new connections and to gradually take down established calls, after the time period specified in the RestartDelay parameter. For the CS2K, a graceful restart transitions call processing busy (CPB) trunks to a call processing de-load (CPD) state and idle (IDL) trunks to a carrier fail (CFL) state. After the RestartDelay period, all affected trunks are placed in a CFL state.

A cancel-graceful restart cancels the graceful tear down of established calls and transitions CPD trunks back to CPB on the CS2K. All affected CFL trunks are transitioned back to IDL on the CS2K.

49.3.3 Call Block (MT/bl) Event

Notification of the call block event (MT/bl) from the MG indicates to the MGC that a trunk seizure from the PSTN has occurred due to some maintenance activity. As a result, the CS2K transitions the affected trunk to a remote make busy (RMB) state.

In SN08/GC080, MT/bl event request notification and handling functionality will be submitted under CRs once MT/bl event is supported by Nuera. Submission is being deferred to ensure continued inter-operability with Nuera.

49.4 Hardware Requirements or Dependencies

This activity has the following hardware dependencies:

- The MG functionality is provided by a third party gateway vendor supporting TGCP as described in the PKT-SP-TGCP-I08-040721 TGCP specification.
- A PacketCable-certified MTA is responsible for applying of audible ringing to the PSTN operator for Operator Ringback.

49.5 Software Requirements or Dependencies

This activity enhances the CS2K core and GWC to support a TGCP MG hosting ISUP IT, ISUP ATC, MF OP, and MF ES trunks. The SN08 software load is required on the CS2K core. The GC080 software load is required in the GWC. The PNM07 or greater software load is required on the CS2M.

The reporting of call blocking (MT/bl) events on 2-way PTS trunks is dependent on the TGCP MG software distinguishing a permanent seizure from a trunk seizure for call processing coming from the PSTN.

49.6 Limitations and restrictions

The PKT-SP-TGCP-I08-040721 TGCP specification limits support of MF trunk interconnection to a LEC Access Tandem. Interconnection to an Inter-Exchange Carrier (IEC) operator system is not supported.

IAC (hybrid) configurations involving TDM elements are not supported in SN08.

Audible ringing to the PSTN operator for Operator Ringback may not be applied if non-certified MTAs are involved.

Only DS-1 carrier endpoint ranges are supported, i.e., 1-24. Endpoint ranges for other types of carriers, such as E1 and DS3, are not supported.

49.7 Interactions

No new interactions have been introduced by this activity.

49.8 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__

49.9 Glossary

Table 1

Term	Description
CFL	Carrier Fail
CPB	Call Processing Busy
CPD	Call Processing De-load
CS2K	Call Server 2000
CS2M	Call Server 2000 Manager
CMS	Call Management Server
DA	Directory Assistance
EO	End Office
ES	Emergency Service
GWC	Gateway Controller
IAC	Integrated Access - Cable
IDL	Idle
IEC	Inter-Exchange Carrier
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISUP	ISDN User Part
LEC	Local Exchange Carrier
MF	Multi-Frequency
MG	Media Gateway
MGC	Media Gateway Controller
MTA	Multimedia Terminal Adapter
OP	Operator
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTS	Per Trunk Signaling
RMB	Remote Maintenance Busy

Table 1

Term	Description
RSIP	ReStartInProgress
SS7	Signaling System Number 7
TGCP	Trunking Gateway Control Protocol

50: A00007115 Functional description (FN)

50.1 Feature name and Feature ID

A00007115 - MG9K In-service Fault Isolation

50.2 Description

This is a robustness activity which improves fault detection and recovery of MG9K ITP DSPs (Digital Signal Processors). This activity does raise 2 alarms under new conditions (described under the fault management section of this document).

50.3 Hardware Requirements or Dependencies

None. This activity applies only to MG9K ITP cards.

50.4 Software Requirements or Dependencies

No dependencies are introduced.

50.5 Limitations and restrictions

No new limitations are introduced by this activity.

50.6 Interactions

None.

50.7 Glossary

51: A00007120 Functional description (FN)

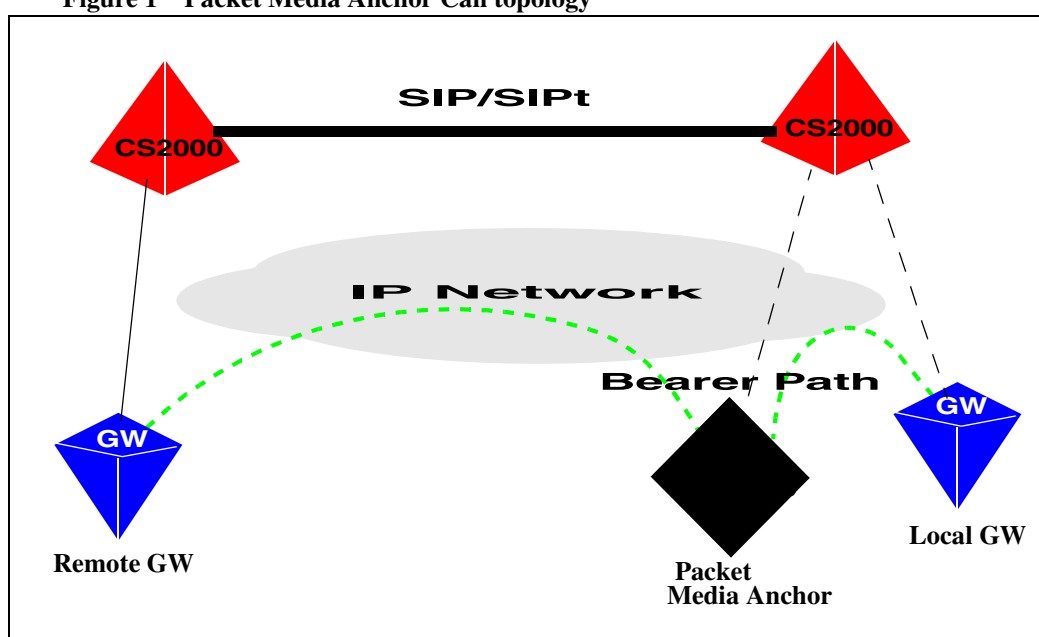
51.1 Feature name

Packet Media Anchor for DPT

51.2 Description

This activity introduces the Packet Media Anchor for the Dynamic Packet Trunking SIP/SIPt application. The role of the Media Anchor is to provide tone, digit collection and bearer path anchoring capabilities for SIP/SIPt call types.

Figure 1 Packet Media Anchor Call topology



The Audiocodes 2010 has been chosen as the packet gateway to supply media anchoring functionality. The Packet Media Anchor solution uses the bearer channel tandeming (BCT) capability of the AMS to provide media stream anchoring functionality. The media anchor is directed by the CS2K, which is responsible for managing call topology, resource allocation/deallocation and resource usage. Media anchoring through the AMS does not require conversion from packet to TDM back to packet again, thus impact on bearer path latency will be minimal.

This activity has 4 main customer impacting deliverables:

- Table Provisioning
- MAPCI
- Operational Measurements (OMs)

- Logs

51.2.1 Table Provisioning

The bearer channel tandeming (BCT) capability of the AMS is provisioned in table SERVSINV. The Packet Media Anchor will share the BCT resources with the Lawful Intercept (ALTTERMS application in the table), however the Packet Media Anchor resources must be provisioned as a separate Subtending Application on a particular GWC. The Packet Media Anchor also requires audio resources, thus an audio application may also be provisioned on the same GWC with the BCT applications.

Figure 2 Table SERVSINV - Packet Media Anchor (PKTMA) provisioning

SRVSNAME	SRVRNAME	NUMTERMS	OPTIONS
AUD 4	GWC 20	4095	(3PORT 30) (6PORT 30) (ANNC 300) \$
BCT 0	GWC 20	1024	(ALTTERMS 100) \$
BCT 1	GWC 20	4095	(PKTMA_MAX_CALLS 150) \$

51.2.2 MAPCI

A new MAPCI interface is being provided to monitor the availability of Announcement, Conference, Lawful Intercept and Packet Media Anchor resources subtending from a particular GWC.

Figure 3 MAPCI;PM Posting GWC Media Resources

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	.	NODLOG	Istb	1 SPM	.	SYSB	48C..	.	SDM
M				*C*		*C*	*C*		
GWC				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		11	1	42	8	7	60
2 Post_		GWC		3	0	0	0	0	15
3 Listset									
4 Listres		GWC	20 InSv						
5		Unit0:	Act ISTb						
6		Unit1:	Inact ISTb						
7		Listres							
8				MaxPorts	InsvPorts	BsyPorts	CPBports		ResType
9									
10		Conf3		30	30	0	0		CONF
11 Disp_		Conf6		30	30	0	0		CONF
12 Next		Announcements		300	50	0	0		ANNC
13		Lawful Intercept		90	8	0	0		BCT
14 QueryPM		PKT Media Anchor		90	0	0	0		BCT
15									
16									
17									
18									

51.2.3 Operational Measurements

To enable the monitoring of Packet Media Anchoring facilities by downstream OSS systems, a new operational measurement group is being created. The number of PKTMA insertion attempts (PMAREQST), number of insertion failures to do resource exhaustion/no resources (PMAFLNR), and high-water mark (PMAHWM) will be reported.

Figure 4 Packet Media Anchor OMs

PKTMA				
CLASS: ACTIVE				
START:2004/05/13 17:35:00 THU; STOP: 2004/05/13 17:37:15 THU;				
SLOWSAMPLES: 2; FASTSAMPLES: 14;				
INFO (PKTMA_OM_INFO)				
PMAREQST PMAFLNR PMAFLMSC PMAHWM				
1	PKTMA	1	200	
	38	0	0	12

51.2.4 Logs

To better enable troubleshooting of the Announcement, Conference and Packet Media Anchor call setup and configuration issues a new core log (XPKT340) is introduced. This log will inform the craftsperson about the potential announcement, conference or BCT resource set up issues that require addressing. Examples of this log follow:

Figure 5 Packet Media Anchor Logs

RTP7		XPKT340 OCT25 08:16:40 4500 INFO PKTMA Call Failure		
		Location: AUD 4		
		Type: GWC		
		Orig Agent: LG 23 9 00 07 DN 6195200007		
		Orig Node: LG 23 9		
		Term Agent: CKT UASBLDNANN 0		
		Term Node: AUD 4		
		Called Number: 5209999		
		CallID: 49905667		
		Cause: Number 16 - Audio Operation Failure		
		IP Address: 47.142.134.147		
		Signal ID: 51		
		Phrase ID: 999		
		0000 0000 0000 0000 0100 0000 1000 0000 0000 0000 0000		

51.2.5 Background

Many services and call processing capabilities on SIP/SIPt require interaction with a call's bearer path to provide progress indications (i.e. tones) into or to collect digits out of the bearer stream. DPT endpoints are logical entities and do not have physical bearer facilities of their own. As well, SIP/SIPt signalling has limited capability to convey tone and/or digit collection requests to preceding offices. Due to this limitation the SIP specification allows for the introduction of a media server into a call topology to perform media functions. The Packet Media Anchor is Nortel's answer to tone insertion and digit extraction on SIP/SIPt.

51.3 Hardware Requirements or Dependencies

51.3.1 AudioCodes AMS

The AMS audio server 2010 is required for Packet Media Anchor functionality. Both BCT and Audio resources must be provisioned on each AMS that will be used for the PKTMA. The device will register with a CS2K gateway controller and it is expected that multiple AMS devices will be used to comprise the pool of available resources required.

51.4 Software Requirements or Dependencies

51.4.1 Provisioning

Provisioning for DPT Media Anchors will be provided through CS2K Table Control. Table SERVSINV is the only table that must be provisioned in order to enable Media Anchor endpoints. For additional information on provisioning the Media Anchor see the Configuration section of this feature.

51.5 Limitations and restrictions

- The AudioCodes UAS can not support the Packet Media Anchor functionality.
- The Codec Profile for GWCs that control PKTMA resources must only allow the GW to use the G.711 codec.

51.6 Interactions

The packet media anchor will be inserted into SIP/SIPt calls that require bearer facility interaction. Some of these scenarios include:

- Local Treatment on a SIP trunk (tone treatment only).
- Digit collection (e.g. DISA service, Auth/Account Codes, CFRA, etc.).
- Interactions with CS2K line or network services (e.g. IN Send-To-Resource) could request digit collection on the trunk, Blind Call Transfer or ACD queuing could request audible ringback on a SIP Trunk after the SIP session has been established. After successful SIP session setup

(i.e. “200 OK”) any inband application of tones must be accomplished via the Packet Media Anchor).

51.7 Glossary

Term	Description
PMA	Packet Media Anchor
PKTMA	Packet Media Anchor
UAS	Universal Audio Server

52: A00007121 Functional description (FN)

52.1 Feature name

IW Bridge MAP maintenance for deload

52.2 Description

This feature has the following component.

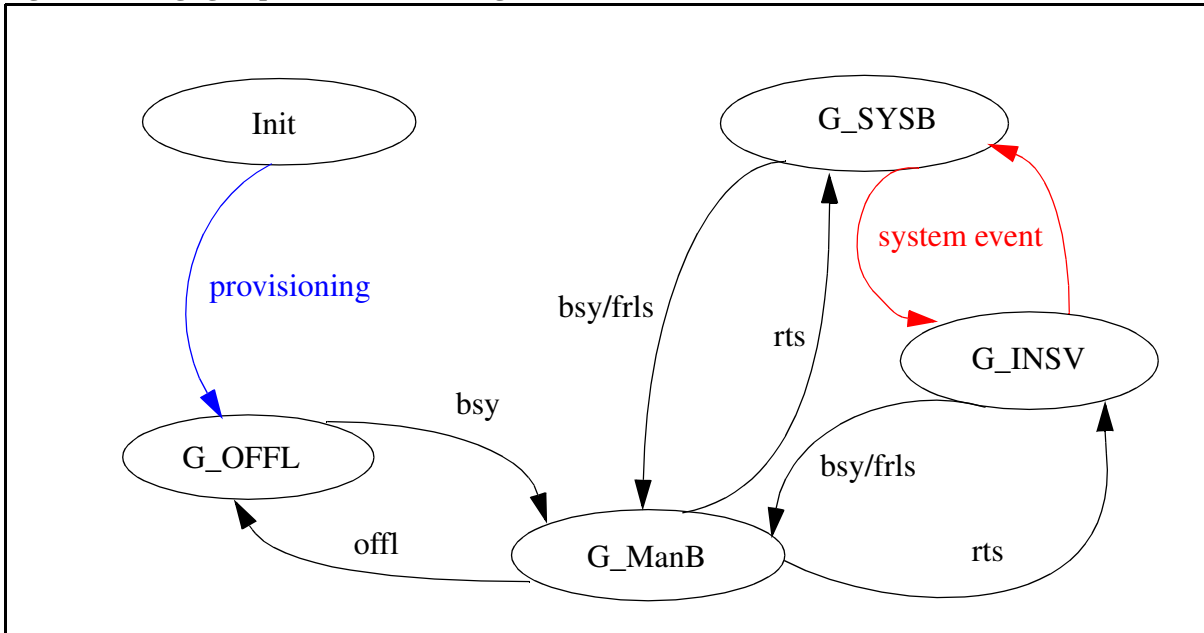
- Provide an IW bridge Map maintenance for deload.
 - This feature introduces an IW bridge maintenance MAP level (BrgMtce) which provides a method to deload call processing from IW bridges.

52.2.1 IW Bridge Maintenance

A new MAP level 'BRGmtce' will be provided to manage the state of the IW SPM bridge terminals. **Offl**, **Bsy**, **Rts**, **Frls**, **Post** and **Next** commands will be provided at this command subdirectory.

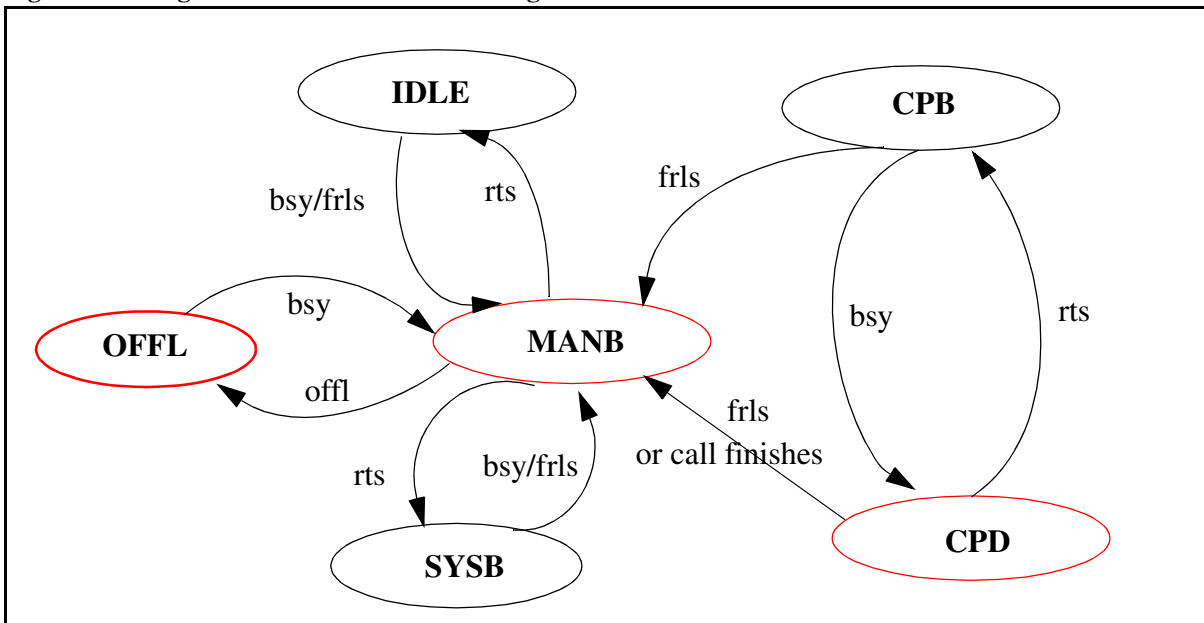
A new status for all terminals on an IW SPM bridge is going to be introduced: deload, which means that the bridge involving in a call will be put in a pending deload state before the call is terminated. The bridge will no longer be available to CallP when the old call terminates. This state will be set via the **Bsy** command. Prior to having deload status, the IW SPM bridge terminal has the following states: Idle, Call Processing Busy and System Busy. When combining the deload state with these three states, the following new terminal states are introduced: Call Processing Deload and Manual Busy. In addition, Offl state will be introduced to the state of bridge terminals. This will be the initial state and can only be set when the group state of bridges in a DS512 link is G_ManB.

A new group state of bridge terminals in each DS512 link, {G_OFFL, G_MANB, G_SYSB, and G_INSV}, will be introduced. These states are used to determine the individual bridge terminal state, which can be OFFL, MANB, SYSB, CPB, CPD, and IDLE. The state transition diagram for the bridge group state is depicted as follows:

Figure 1 bridge group state transition diagram

Note that rts command will be rejected if the group state of bridges in a DS512 link is G_SYSB.

The bridge terminal state transition due to manual actions is shown in the following figure:

Figure 2 Bridge terminal state transition diagram

The following list describes the required IW SPM bridge terminal state transitions that result from the Bsy command:

- Idle to Manual Busy - this transition results from a 'Busy' command being issued to a bridge terminal that is in the 'idle' state.
- Call Processing Busy to Call Processing Deload - this transition results from a Bsy command being issued to a bridge terminal that is in the 'call processing busy' state.
- System Busy to Manual Busy - this transition results from a Bsy command being issued to a bridge terminal that is in the 'system busy' state.
- Off line to Manual Busy - this transition results from a Bsy command being issued to a bridge terminal that is in the 'Off Line' state.

Two options, "all" and "DS512_link_number", will be provided. "Bsy all" will "busy" all the bridge terminals of the posted IW SPM, while "Bsy number" will just busy the bridge terminals of the specified DS512 link. The group state of the DS512 link will be set to MANB.

Command **Offl** will be supported to allow the craftsmen to set the state of IW SPM bridge terminals to off line. This command can be issued on the bridge terminal link that is in a ManB state. The group state of the DS512 link will be set to OFFL.

Two options, "all" and "DS512_link_number" will be provided. "Offl all" will "offl" all the bridge terminals of the posted IW SPM, while "Offl number" will just offl the bridge terminals of the specified DS512 link.

Command **Rts** will be supported to allow the craftperson to allow the IW SPM bridge terminals to be used by call processing. The following list illustrates the required IW SPM bridge terminal state transitions that result from the 'Rts' command:

- Manual Busy to Idle - this transition results from an 'Rts' command being issued to a bridge terminal that is in the 'manual busy' state and the associated IW SPM node is in service.
- Call Processing Deload to Call Processing Busy - this transition results from an 'Rts' command being issued to a bridge terminal that is in the 'call processing deload' state.
- Manual Busy to System Busy - this transition results from an 'Rts' command being issued to a bridge terminal that is in the 'manual busy' state and the associated IW SPM node is out of service.

Two options, "all" and "DS512_link_number", will be provided. "Rts all" will "Rts" all the bridge terminals of the posted IW SPM, while "Rts number" will just Rts the bridge terminals of the specified DS512 link. The group state of the DS512 link will be set to INSV.

Command **Frls** will be supported to allow the craftsperson to remove the IW SPM bridge terminals from use by call processing immediately. The following list illustrates the required IW SPM bridge terminal state transitions that result from the 'Frls' command:

- Idle to Manual Busy - this transition results from a 'Frls' command being issued to a bridge terminal that is in the 'idle' state.
- Call Processing Busy to Manual Busy - this transition results from a 'Frls' command being issued to a bridge terminal that is in the 'call processing busy' state.
- Call Processing Deload to Manual Busy - this transition results from a 'Frls' command being issued to a bridge terminal that is in the 'call processing deload' state.
- System Busy to Manual Busy - this transition results from a 'Frls' command being issued to a bridge terminal that is in the 'system busy' state.

Two options, "all" and "DS512_link_number", will be provided. "Frls all" will "Frls" all the bridge terminals of the posted IW SPM, while "Frls number" will just Frls the bridge terminals of the specified DS512 link. The group state of the DS512 link will be set to MANB.

Command **Post** will be supported to display the terminal states of the IW SPM currently posted. It supports the option "all" and "spm #". The following information will be displayed on the map:

- Number of bridge terminals in an 'Idle' state
- Number of bridge terminals in a 'Call Processing Busy' state
- Number of bridge terminals in a 'Call Processing Deload' state
- Number of bridge terminals in a 'Manual Busy' state
- Number of bridge terminals in a 'System Busy' state
- Number of bridge terminals in a 'Offl Line' state

The above terminal status window will be updated continuously.

Command **Next** will be supported to display the terminal states of the next IW SPM in the post set (post set is created via "post all"). If the current IW SPM is the last one in the post set, Next will clear the display on the map.

Note 1: The newly introduced deload state is independent of the IW node state. This means that the IW SPM bridge terminal states can be driven separately from the state of the IW SPM node.

Note 2: The requirements described above will be applicable to all types of IW SPMs.

52.2.1.1 Accessing 'BrgMtce' from PKT MAPCI level

BrgMtce subdirectory is created up the MAPCI;MTC;APPL;PKT level of MAPCI as shown in Figure 1.

Figure 3 Accessing BRGMtce level from PKT level

```

XAC      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
.      MSpair  1DDUOS  2CBsy  1EIU  10 RS      .      333C..  2Crit  2 PKT
*C*      M      M      *C*      *C*      *C*      *C*      *C*      M
PKT
0 Quit      .      .      .      .      .      .      2 PKT      .
2
3
4 SPM_ATM   Summary of PKT failures:
5 SPM_ATM   SPM_ATM:
6
7
8 BRGMTCE
9
10
11
12
13
14
15
16
17          PKT:
18
    MAP1
Time 02:28

```

Figure 4 BRGmtce MAP level

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	MSpair	2MPCOS	2CBsy	1EIU	8	RS	46C..	.	.
	C	M	M	*C*	*C*		*C*		
BRGMTCE		OAMAP	ATMFW	SDM	SPMCP	SWMTC	SDMBIL	PKT	TOPSIP
0 Quit		.	.	.	.	.	.	.	.
2 Post_									
3									
4		SPM_ATM = .							
5 Bsy_									
6 Rts_		IWSPM:	SPM 3	OFFL		NETBRDGE:	E_A1		
7 Offl_		Link:	BRGMTCE	STATE:	CPD:	CPB:	SYSB:	IDL:	MANB:
8 Frls_		0		OFFL	0	0	0	0	0
9		1		OFFL	0	0	0	0	504
10		2		OFFL	0	0	0	0	504
11		3		OFFL	0	0	0	0	504
12 Next		-----							
13					0	0	0	0	2016
14		POST SPM 3							
15		POSTED SET: SPM 3							
16									
17									
18									
YD									
Time	18:26	>							

52.2.1.2 New Logs

Four new logs are created: IWBM502, IWBM503, IWBM504, IWBM505.

The following new logs will be created to keep the users informed about the group state transitions:

- IWBM502 - A Bsy command being requested for a set of IW SPM bridge terminals

```
RTP708AK  ** IWBM502 AUG12 00:37:09 5900 INFO MBSY IW Bridge Terminals
           SPM Number: 3
           DS512 link: 3
           IW bridge group state changed from SYSB to MANB
           IW bridge terminal range: 1 through 504
           Reason: Manual Request
           Issued by: YD2
```

- IWBM503 - A Rts command being requested for a set of IW SPM bridge terminals

```

RTP708AK      IWB503 AUG12 00:37:19 6700 INFO RTS IW Bridge Terminals
               SPM Number: 3
               DS512 link: 0
               IW bridge group state changed from MANB to SYSB
               IW bridge terminal range: 1513 through 2016
               Reason: Manual Request
               Issued by: YD2

```

- IWB504: An Offl command being requested for a set of IW SPM bridge terminals

```

RTP708AK      ** IWB504 AUG12 00:04:26 3200 INFO OFFL IW Bridge Terminals
               SPM Number: 3
               DS512 link: 3
               IW group terminal state changed from MANB to OFFL
               IW bridge terminal range: 1 through 504
               Reason: Manual Request
               Issued by: YD2

```

- IWB505 - A Frls command being requested for a set of IW SPM bridge terminals

```

RTP708AK      ** IWB505 AUG12 00:37:51 8000 INFO FRLS IW Bridge Terminals
               SPM Number: 3
               DS512 link: 3
               IW bridge group state changed from SYSB to MANB
               IW bridge terminal range: 1 through 504
               Reason: Manual Request
               Issued by: YD2

```

52.3 Hardware Requirements or Dependencies

N/A

52.4 Software Requirements or Dependencies

52.5 Limitations and restrictions

Since the newly introduced Offl state will be set as an initial bridge terminal state in SN08, the group state of bridges in each DS512 link and bridge terminal state need to be restored on the newly active side over swact. The bridge terminal state transition over swact will be as follows:

From SN07 to SN08, SysB -> SysB, Idle -> Idle, CPB -> CPB

From SN08 to SN08: OFFL -> OFFL, SysB -> SysB, Idle -> Idle, CPB -> CPB, ManB -> ManB, CPD -> CPD

52.6 Interactions

Once the deload state is ON (ManB) on a bridge terminal, new calls cannot be established using that bridge.

52.7 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) ☐

52.8 Glossary

Table 1

Term	Description
CI	Command Interpreter
CPB	Call Processing Busy
CPD	Call Processing Deload
IWSPM	InterWorking Spectrum Peripheral Module

53: A00007135 Functional description (FN)

53.1 Feature name

GWC DPT Audits and Counter Drift Prevention

Note: This activity also applies to MG4k and DPT SPM, not just GWC.

53.2 Description

This feature addresses two areas of weakness in the existing DPT application:

1. Counter drift.

DPT software has several counters, e.g., the total number of DPT terminals in use, that have been observed to drift from their proper values over time. Negative consequences of counter drift include network management and OM distortions, SWERRs on certain scenarios (e.g. dead shelf recovery), and artificially reduced DPT capacity.

2. Trunk OM anomalies

DPT OMs are both unlike regular trunk OMs and sometimes quite similar also. This “split personality” has led to issues both with documentation and behavior.

53.2.1 Counter drift

Any changes made by this activity to handle counter drift will be visible in greater accuracy of the OMs described in the next section of this document.

53.2.2 Trunk OM anomalies

The changes made by this activity to the OMs TRK, DPTOFC, DPTOFCP, and DPTNODE are behavioral and/or documentation clarifications:

- No new OMs are introduced by this activity.
- No new registers are introduced by this activity.
- No existing OMs are removed by this activity.
- No existing registers are removed by this activity.

53.2.3 Behavioral Changes

53.2.3.1 OMs DPTOFC, DPTOFCP, and DPTNODE

For registers DPTNODE::DPTGTAT, DPTOFC::DPGTAT/DPGTAT2, and DPTOFCP::DPGTATT/DPTTATT2, the “attempts” counted at the nodal level exclude failed optimization attempts whereas the office level OM includes them. The pegging of these registers will be changed such that both the nodal level and the office level are counted at the same point (except in cases where the code exits prior to knowing a particular node).

The DPTOFC::DPGTFLO/DPGTFLO2 registers, DPTOFCP::DPOTFLO/DPOFLO2, and DPTNODE::DPTGTFLO registers will be changed such that failed optimized attempts on nodes “not DPT-enabled” are not pegged against these registers.

53.2.3.2 OM TRK

Register MAXBU is effectively disabled for DPT trunk groups. The value of the MAXBU register for a DPT trunk group will always be equal to zero.

The MAXBU register was designed to be used with non DPT trunks. The DPTOFC, DPTOFCP, and DPTNODE usage registers and high water registers are directly applicable to DPT trunks and should be used in the place of the MAXBU register.

This change was sourced in the SN07 stream by CR Q00868638.

53.2.4 Documentation Clarification

53.2.4.1 OM - DPTOFC

Customers have requested that the documented descriptions of the DPTOFC and DPTNODE OMs be clarified. The CR Q00881441, states “*Customer would like better explanation or data to reflect exactly what we are trying to determine with this field*”, i.e., the DPTNODE OM register DPTHWT. As well, Nortel employees have noted that the documentation is confusing for these OMs, especially the high water registers.

The intent of this activity is to increase the accuracy of the DPT OMs and to rewrite the customer facing documentation for OM DPTOFC, DPTOFCP, and OM DPTNODE. To help understand the DPT OMs the following definitions are provided:

Definitions

— optimized

In the context of the DPT OMs this means “occurring on the same device”. An “optimized” attempt is an attempt to get a TID from the same device (where “device” is an MG4K, DPT SPM, or DPT GWC) that hosts the other agent in the call.

— non-optimized

A “get” attempt not constrained to be on the same device (where “device” is an MG4K, DPT SPM, or DPT GWC).

— port depletion

The exhaustion of the DPT terminal pool, because the DPT SOC limit on usable DPT tids has been exceeded.

— cpb

The number of terminals that are call processing busy.

— cpd

The number of terminals that are call processing deloaded. Where CPD is a terminal that is CPB on a device that is no longer in service, such as, during an upgrade.

The DPTOFC OM provides information for the entire office and is composed of the registers described in “Table 1 OM - DPTOFC” shown below.

Table 1 OM - DPTOFC

Register	Extension Register	Description
DPGTAT	DPGTAT2	The number of attempts to get a DPT Terminal. This is an incremental register. The register is pegged every time an attempt to get a DPT terminal is made within a given transfer period. For a typical SIPT call the number of pegs is in the range of 1 peg per DPT agent per call. For a typical BICC^a call the number of pegs is in the range of 1 to 3 pegs per DPT agent per call.
DPGTFL	DPGTFL2	The number of attempts to get a DPT Terminal that failed (non-optimized). This is an incremental register. The register is pegged every time an attempt to get a <i>non-optimized</i> DPT terminal fails within a given transfer period.

Table 1 OM - DPTOFC

Register	Extension Register	Description
DPUSAG	DPUSAG2	The number of DPT Terminals in use. This is an accumulator register. The register is pegged every one-hundred seconds within a given transfer period. The formula used for calculating the usage is as follows: $\text{current\_usage} = (\text{current\_cpb} + \text{current\_cpd})$ $\text{usage\_om} = \text{usage\_om} + \text{current\_usage}$ Since this register is an accumulator and is added to itself the register can be misleading. To interpret the usage register divide the value by the number of slow samples to determine the average usage for a given transfer period.
DPGTFLO	DPGTFLO2	The number of attempts to get a DPT Terminal that failed (optimized). This is an incremental register. The register is pegged every time an attempt to get an <i>optimized</i> DPT terminal fails within a given transfer period. Optimized failure attempts on nodes “not DPT-enabled” are not pegged against this register. Pegs to this register do not signify call failures. The optimized failure attempt to get an optimized terminal is immediately followed by an attempt to get a non-optimized terminal instead.

Table 1 OM - DPTOFC

Register	Extension Register	Description
DPHWT	DPHWT2	The high water mark for number of DPT Terminals in use. This register is pegged every ten seconds within a given transfer period. The formula used for calculating high water mark is as follows: <pre> current_usage = (current_cpb + current_cpd) if current_usage > high_water_mark_om then high_water_mark_om = current_usage else register is <i>NOT</i> updated endif </pre>
DPDPL	DPDPL2	The number of attempts to get a DPT Terminal that failed due to port depletion. This is an incremental register. The register is pegged every time an attempt to get a DPT terminal fails due to port depletion within a given transfer period.

a. For further information about BICC OMs see the FN of A89007299 in PLS FM-DOC.

Considerations

When using a customer-defined long duration OM by using a customer defined “accumulating” class (rather than the active or holding class) the meaning of the high water registers (DPHWT/DPHWT2) changes. In this case the value of the high water mark is only valid when divided by the number of transfer periods within the duration of the long duration OM. The result of which is the *average* high water mark for the long term duration. For example, if we define a “weekly” long duration class, with 15 minutes transfer periods, we would need to divide the high water mark by 672 [(7days * 24 hours * 60 minutes)/15 minute transfer period].

Note: It is recommended that the DPTOFC/DPTOFCP/DPTNODE high water registers **not** be used in conjunction with long duration “accumulating” OMs. For more information on “accumulating” registers see NTP 297-1001-300, Section 1, Understanding the Operational

Measurement System, sub section Measurement Classes, pg 1-9, v 03.08,
May 2000.

Figure 1 below shows an example of the DPTOFC OM.

Figure 1 OM DPTOFC

>omshow dptofc holding				
DPTOFC				
CLASS: HOLDING				
START:2004/06/30 17:30:00 WED; STOP: 2004/06/30 18:00:00 WED;				
SLOWSAMPLES: 18 ; FASTSAMPLES: 180 ;				
DPGTAT	DPGTAT2	DPGTFL	DPGTFL2	
DPUSAG	DPUSAG2	DPGTFL0	DPGTFL02	
DPHWT	DPHWT2	DPDPL	DPDPL2	
0	0	0	0	0
	0	0	0	0
	0	0	0	0

53.2.4.2 OM - DPTOFCP

The DPTOFCP OM provides office-wide information per DPT protocol, i.e. it separates out the office totals for SIPT and BICC. All material presented above for DPTOFC applies as well to DPTOFCP, except that the register names are changed for DPTOFCP.

Figure 2 below illustrates the register correspondence.

Figure 2 OM DPTOFC

DPTOFC Register Names				
DPGTAT	DPGTAT2	DPGTFL	DPGTFL2	
DPUSAG	DPUSAG2	DPGTFL0	DPGTFL02	
DPHWT	DPHWT2	DPDPL	DPDPL2	
DPTOFCP Register Names				
DPGTATT	DPGTATT2	DPGETFL	DPGETFL2	
DPUSAGE	DPUSAGE2	DPOTFLO	DPOTFLO2	
DPHWTR	DPHWTR2	DPRTDPL	DPRTDPL2	

Note that OM Group DPTOFCP is only available in the Trimodal configuration of the Succession Call Server.

Please refer to the Succession Operational Measurements Reference Guide, NN10264-709, for further details.

53.2.4.3 OM - DPTNODE

The DPTNODE OM provides information per DPT node. Each is composed of the registers described in “Table 2 OM - DPTNODE”

Table 2 OM - DPTNODE

Register	Extension Register	Description
DPTGTAT	DPTGTAT2	The number of attempts to get a DPT Terminal for a particular DPT node. This is an incremental register. The register is pegged every time an attempt to get a DPT terminal is made within a given transfer period. For a typical SIPT call the number of pegs is in the range of 1 peg per DPT agent per call. For a typical BICC^a call the number of pegs is in the range of 1 to 3 pegs per DPT agent per call.
DPTGTFL	n/a	The number of attempts to get a DPT Terminal that failed (non-optimized) for a particular DPT node. This is an incremental register. The register is pegged every time an attempt to get a <i>non-optimized</i> DPT terminal fails within a given transfer period.
DPTUSAG	DPTUSAG2	The number of DPT Terminals in use for a particular DPT node. This is an accumulator register. The register is pegged every one-hundred seconds within a given transfer period. The formula used for calculating the usage is as follows: $\text{current\_usage} = (\text{current\_cpb} + \text{current\_cpd})$ $\text{usage\_om} = \text{usage\_om} + \text{current\_usage}$ Since this register is an accumulator and is added to itself the register can be misleading. To interpret the usage register divide the value by the number of slow samples to determine the average usage for a given transfer period.

Table 2 OM - DPTNODE

Register	Extension Register	Description
DPTGTFLO	n/a	The number of attempts to get a DPT Terminal that failed (optimized) for a particular DPT node. This is an incremental register. The register is pegged every time an attempt to get an <i>optimized</i> DPT terminal fails within a given transfer period. Optimized failure attempts on nodes “not DPT-enabled” are not pegged against this register. Pegs to this register do not signify call failures. The optimized failure attempt to get an optimized terminal is immediately followed by an attempt to get a non-optimized terminal instead.
DPTHWT	n/a	The high water mark for number of DPT Terminals in use for a particular DPT node. This register is pegged every ten seconds within a given transfer period. The formula used for calculating high water mark is as follows: <pre> current_usage = (current_cpb + current_cpd) if current_usage > high_water_mark_om then high_water_mark_om = current_usage else register is <i>NOT</i> updated endif </pre>

a. For further information about BICC OMs see the FN of A89007299 in PLS FM-DOC.

Figure 3 below shows an example of the DPTNODE OM.

Figure 3 OM DPTNODE

```

>omshow dptnode holding
DPTNODE
CLASS: HOLDING
START:2004/06/30 17:30:00 WED; STOP: 2004/06/30 18:00:00 WED;
SLOWSAMPLES: 18 ; FASTSAMPLES: 180 ;
INFO (DPT_NODE_OM_PM_INFO)
      DPTGTAT  DPTGTAT2  DPTGTFL  DPTGTFL0
      DPTUSAG  DPTUSAG2  DPTHWT
0      GWC      4      83
      0      0      0      0
      0      0      0      0

```

Note that in a Trimodal configuration of the Succession Call Server, the output from OMSHOW is modified to display bearer network information and the protocol supported, (i.e., BICC or SIPT), for each node displayed.

Please refer to the Succession Operational Measurements Reference Guide, NN10264-709, for further details.

53.3 Hardware Requirements or Dependencies

None.

53.4 Software Requirements or Dependencies

None.

53.5 Limitations and restrictions

None.

53.6 Interactions

None.

53.7 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)	__X ¹ __

53.8 Glossary

Term	Description
DPT	Dynamic Packet Trunk
OM	Operational Measurement

¹There is no performance section within this document since there are no visible changes to the OMs. However, the definitions documented in this FN supercede definitions stated by activity A59015752.

54: A00007140A Functional description (FN)

54.1 Feature name

Succession Upgrade Manager (Phase 1)

54.2 Description

This feature introduces a CLUI interface on the MG9k Element Manager to drive upgrades of the MG9k devices such as MTA, XDSL, DS1, ABI, ITP, ITX, SCO and SCI. This CLUI interface can be leveraged by IEMS so the upgrade of the MG9k devices can be driven from a centralized location.

The feature prevents the customer from making any provisioning changes during an MG9k upgrade. It also automates the patching of the devices after the upgrade completes.

The pre-download feature of the CLUI will be added as an enhancement to the existing upgrade GUI. The pre-download prepare phase separates the downloading of the card loads from the actual upgrade of the MG9k cards. The customer will now be able to download all cards outside of a maintenance window. Then once inside the maintenance window, the upgrade of the cards can be performed. Thus allowing the customer to utilize the on-site personnel's time more effectively since they would not have to be on-site and wait for all of the cards to be downloaded.

This feature does not cover upgrade automation of single card replacement (i.e. load from mate). It does not cover node growth (i.e. card pair installation). It does not cover upgrade automation of a protection group. It does not provide a reset upgrade functionality nor a resume capability. It does not provide automatic image functionality.

54.3 Hardware Requirements or Dependencies

None

54.4 Software Requirements or Dependencies

None

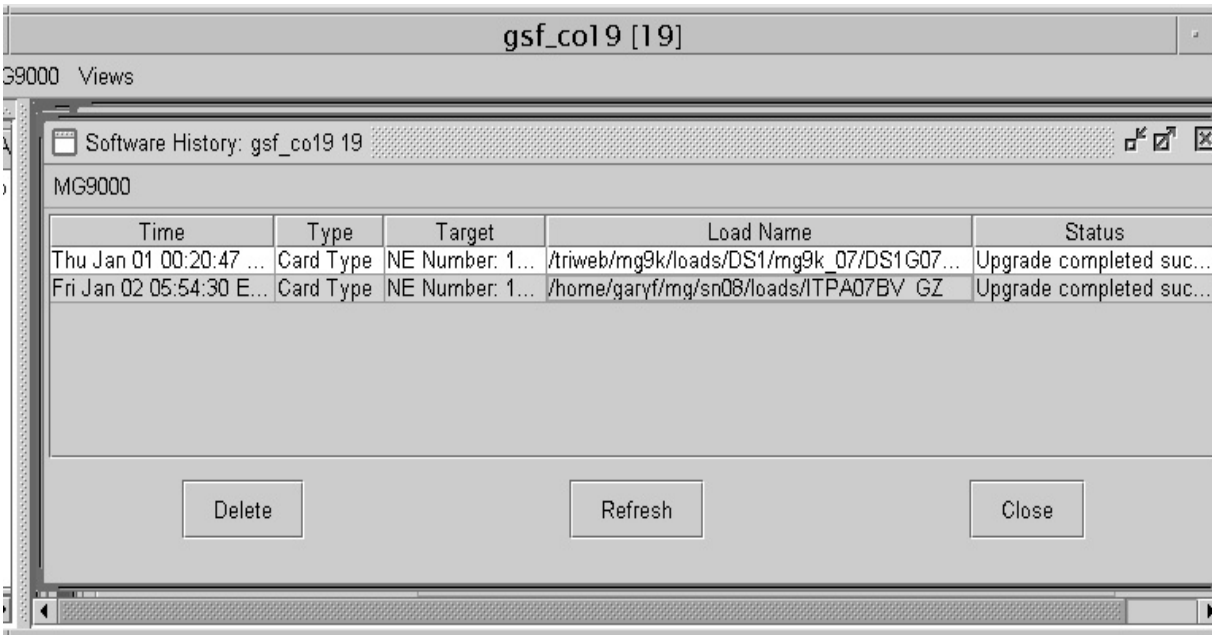
54.5 Limitations and restrictions

1. This version will not support multiple users. For example, a 10 node office would not be able to ask 2 crafts people to upgrade 5 nodes each at the same time. The second person will receive an error message.

2. This version will not support progress or status type messages back to the user during the execution of an *mg9kuptool* command. The user will need to create a new telnet session and issue a *mg9kuptool -query* command to obtain this type of information.
3. This design does not prevent two users from modifying the config data.
4. This design does not go to the SDM and give the user a list of loadnames to choose from. The customer has to enter the loadname manually.
5. We are not validating that the customer actually has put the patch files on NPM.
6. We are not validating that the NE alarms have been cleared as part of the prepare phase. NE alarms are checked in the precheck and upgrade phases since they could change between the prepare phase and the precheck phase.
7. A comparison between the NPM patchlist and the prepatched loads on the SDM are not performed in order to calculate the patch times. For example, if the NPM knows that an ITP card has 15 patches and the prepatched load contains 14 patches, the patching time is calculated based on 15 patches and therefore is a worst case estimate. This can be refined in a future release. With prepatched loads patching time should be considerable shorter.
8. The number of simultaneous NE upgrades is limited to four, to prevent overload of SDM.
9. The configuration data, created by the configure command, is used for the upgrade. If the GUI is used to prep download, the config command must be re-executed to ensure upgrading of the correct NE. GUI changes do not update the CLUI plan. They are separate interfaces.
10. When the user performs a prep download, the gateway will download the specified load -- even if the gateway already has that load.
11. After a successful prep download on a card, a normal download will download a new patched image (PI) only if the requested PI base loadname is different from the PI base loadname specified for the prep download. Note that patch content does not alter the PI base loadname.
12. If the customer creates a new image of a load that already exists on the gateway, the only way the customer can download the new load to the cards is to use the prep download functionality.
13. The validation performed prior to a prep download is the same as the validation performed prior to a regular download.
14. Prep download is not supported for card types MTA and XDSL.
15. The user cannot perform a prep download on an individual card basis. The user cannot perform a prep download on a protection group basis.

-
16. The mate load functionality on the MG9k gateway does not copy over prep download files.
 17. The reset upgrade system functionality on the MG9k gateway, which should only be used as a last resort, may remove any prep download files. Therefore, the customer should check each card after performing a reset upgrade system request to ensure the prep download file required is shown in the Restart Flash Backup field on the card view in the Software Load area on the GUI. A new prep download should be performed if the Restart Flash Backup field does not show the proper prep download loadname.
 18. The *mg9kuptool* only provides support for a full node upgraded. It does not allow single cards to be upgraded. It does not allow protection group upgrades. And it does not allow load from mate.
 19. If an upgrade fails, there is no retry mechanism in this release.
 20. The customer does not receive any autonomous updates showing the upgrade status or patching status. The customer can query to find out where the upgrade/patching process is at. The customer can also look at the existing upgrade GUI and see the upgrade progress. We are not including patching progress in any GUI. The only way to see the patching status is to perform a query or look at the customer logs.
 21. The abort command stops processing the card type which is upgrading. If other card types are already upgraded, they remain on the upgraded or downgraded load. This is the same as if the customer invoked the abort from the GUI.
 22. Auto processes on the NPM are not automatically turned off nor automatically turned on. The customer must turn off auto processing at the NPM prior to upgrading. The precheck only alerts the customer to ensure auto processes are turned off in the NPM. The post check alerts the customer to manually check and turn auto processing on again.
 23. The down load and upgrade times are only rough estimates generated by simple calculations using static timings collected from lab tests. To obtain more accurate estimates or progress status would require significant development effort in the Mg9K which is out of the scope of this release.
 24. This feature does not allow patching of cards which have completed upgrading while other cards are upgrading. For example, if the ABI cards complete upgrades and the ITP cards are being upgraded, patching of the ABI cards is not started.
 25. There is no indication to the customer showing which patches are already in the imaged load and which patches are going to be applied after upgrading is complete.
 26. If the prepatched image contained an obsolete patch, NPM does not remove the patch. An NPM alarm indicating that there is an obsolete patch is raised and the customer can see the obsolete patch in the postcheck.
-

27. Prior to upgrading MTA or XDSL cards, the EM verifies that all the cards are in an unlocked/enabled state. If any card is not in the correct state, the EM will not perform the upgrade.
28. To upgrade MTA and XDSL cards, the EM will lock the card, download the load and then unlock the card. The order in which the EM upgrades XDSL cards cannot be specified as part of the upgrade.
29. If the upgrade of any MTA or XDSL card fails, the EM halts the upgrade process. If the lock or unlock of any card fails, the EM halts the upgrade process.
30. If an MTA or XDSL card already has the specified load file, the EM will consider the card already upgraded and move on to the next card to upgrade.
31. If the user aborts an upgrade while the EM is upgrading the XDSL cards, the EM will return all cards to an unlocked state. However, the EM will not roll back the loads on any of the cards. For instance, assume the user is upgrading all five XDSL cards on a given node. Assume the user aborts the upgrade after the first two cards have upgraded and a third card is in the process of upgrading. The EM halts the upgrade process after the third card completes its upgrade. In the end, three XDSL cards are running the new load and two XDSL cards are running the old load.
32. The “Software History” window does NOT display entries for MTA and XDSL card upgrades. The following figure shows an example of the “Software History” window.



-
- 33. The existing GUI will not allow the user to perform the specific phases that are defined in the CLUI.
 - 34. The existing GUI will not allow the user to perform the following imbedded functions that are available in the CLUI:
 - audit of flash data
 - autopatching
 - 35. When the user attempts an upgrade, the GUI prints the following warning message:

Each card will download the specified load ONLY IF the specified load file does not already exist in the card's file system. If the card has the specified file, the gateway will NOT download the file -- even if the card's load has different patch content.

This warning applies to all upgrade types: nodal upgrade, card-type upgrade (excluding MTA and XDSL cards), card-specific upgrade (excluding MTA and XDSL cards) and protection group upgrade.

Consider the following scenario:

- User creates a new patched image for the ITP card ITPA07BV_GZ
- User attempts a card type upgrade and specifies load ITPA07BV_GZ

Since the ITP cards already have this load, the user's upgrade will not change the load file on the ITP cards. Furthermore, the GUI will not warn the user that the request upgrade will not result in any changes.

54.6 Interactions

54.6.1 Existing GUI Upgrade Tool

Currently, the user of the MG9K EM GUI can initiate an upgrade from either the frame view or the card view:

- From the frame view, the user can select “Actions” and “Software Upgrade”. From this selection the user can perform a nodal upgrade to upgrade cards of various card types on a given node.
- From the card view of an upgradable card, the user can select “Actions” and “Software Upgrade”. From this selection the user can perform three types of upgrade: card only, protection group only, and single card type only.

This feature impacts the user interface for nodal upgrade only.

When the user selects “Actions” and “Software Upgrade” from the frame view, the user sees the “MG 9000 Software Upgrade Element” GUI. On this GUI, the user clicks “Configure” to set up an upgrade request. When the user clicks “Configure”, the GUI displays the “MG Upgrade Wizard”.

In SN08, the “MG Upgrade Wizard” has significant changes. First, the wizard asks the user if the EM should perform a “prep download” or a “complete upgrade”. The panel displaying this prompt is shown below.

Figure 1 MG Upgrade Wizard - Card Type Selection



When the user clicks “Next”, the “MG Upgrade Wizard” displays the “Card Type Selection” panel. This panel allows the user to choose the card types to upgrade. In addition to the existing choices such as “DS1”, “ITP”, “ITX”, and others, in SN08 the user can also choose “XDSL Cards” and “MTA Cards”. If the user selected “prep download” on the previous screen, the buttons for “XDSL Cards” and “MTA Cards” are disabled. (If the node being configured does not have any cards of a particular type, the Card Type Selection panel does not even display that card type as a choice.) The following figure shows the Card Type Selection Panel when the user has selected to upgrade a node that does not have any ABI cards and the user has selected to perform a “prep download” only.

Figure 2 MG Upgrade Wizard - Card Type Selection

Once the user clicks “Next” on the “Card Type Selection” panel, the “MG Upgrade Wizard” prompts the user for the load information for each of the selected card types. The order in which the GUI gathers the load data for the different card types does not matter.

The prompts for the load information have not changed. Assuming the user selected “one load server” on the “Card Type Selection Panel”, the following two figures show the next two panels displayed by Upgrade Wizard.

Figure 3 MG Upgrade Wizard: Load Server Selection

MG Upgrade Wizard: gsf_col 9 19

Select a load server for selected cards: Step 3 of 7

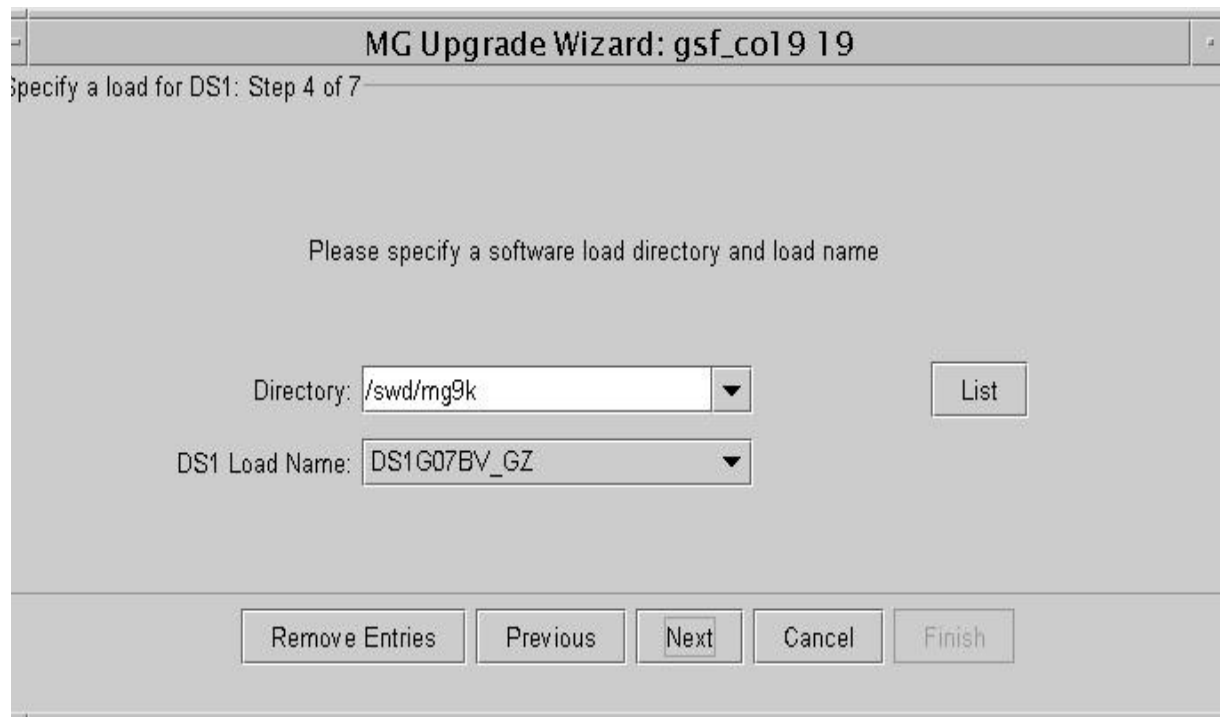
Please enter a new load server address or select from existing addresses. Also, specify a user identifier and password for the selected server.

Server Address: 47.142.106.220 ▼

Server User Identifier: maint

Server Password: *****

Remove Entries Previous Next Cancel Finish

Figure 4 MG Upgrade Wizard: Load Name Selection for Card Type

MG Upgrade Wizard: gsf_col 9 19

Specify a load for DS1: Step 4 of 7

Please specify a software load directory and load name

Directory: /swd/mng9k ▼

DS1 Load Name: DS1G07BV_GZ ▼

List

Remove Entries Previous Next Cancel Finish

Once the user has entered the load information for all of the selected card types, the user clicks “Finish” on the last panel. The “MG Upgrade Wizard” goes away and the GUI redisplay the “MG 9000 Software Upgrade Element” GUI with the settings the user has entered. Field “Upgrade Type” indicates if the user selected a “prep download” or a “complete upgrade”. The subsection “Upgrade Type Data” contains a tab for each selected card type. The user can click the tabs to see the load information for each card type. Finally, the user can click the “Upgrade” button at the bottom of the screen to start the upgrade. The following figure shows the top portion of the “MG 9000 Software Upgrade Element” GUI.

Figure 5 MG 9000 Software Upgrade Element

The screenshot displays the "MG 9000 Software Upgrade Element" GUI. The window title is "gsf_co19 [19]". The main content area is titled "MG9000" and contains several sections:

- Upgrade Originator:**
 - MG 9000 Name: gsf_co19 19
 - Originating View: MG9000 Element 19
- Upgrade State:**
 - Upgrade Status: Configure step completed.
 - Upgrade Action: Configure
 - Upgrade Type: Card Type -- prep download only!
- Upgrade Type Data:**
 - Upgrading: DS1 Card Type
 - DS1 | ITP | ITX | Supercore OC3 (selected)
 - Load Server: 47.142.106.220
 - Load Server User Id: maint
 - Load: /swd/rng9k/DS1G07BV_GZ
- Upgrade Instructions & Results:**
 - performing abort

54.6.2 CLI Interface

Command Syntax:

`mg9kuptool <option> <-n NE_number_list>`

Table 1

Command Options	Description
-configure	This option provides the configuration of the upgrade tool. This includes the list of NEs to upgrade, the name and location of the card loads, etc.
-prepare	This option is largely informative to allow the user to determine if they are prepared to upgrade the system. It is executed for each node in the target node list <-n>.
-precheck	This option reviews the overall system health of each node defined in the target node list <-n> in preparation for the upgrade. Any problems discovered are returned so that action can be taken to correct the issue before the upgrade begins.
-download	This option down loads the card loads as defined in the upgrade plan. It is executed for each node in the target node list <-n>.
-upgrade	This option executes the actual upgrade process defined in the upgrade plan. It is executed for each node in the target node list <-n>. This may include the down loading of card loads if that was not executed earlier as a separate step. When the upgrade is complete all available patches will be applied. If patches are applied, a new image of the patched load will be created.
-postcheck	This option checks to see if any alarms were raised, asks the customer to run any test calls or test scripts and reports any patches that were not applied. It is executed for each node in the target node list <-n>.
-query	This option provides status information regarding the upgrade process for each node in the target node list <-n>.
-abort	This option terminates the upgrade step being executed for each node in the target node list <-n>.
-n	This option describes the list of nodes on which to apply the operation. This is a comma separated list of numbers. If the list is specified as '*' then the operations is applied to all nodes in the plan. This option may be used on all commands except <configure>.

54.6.2.1 CLI - Interactive Mode No Options

Issuing the *mg9kuptool* command without options will result in an interactive conversation with the user to determine which command option to process.

`mg9kuptool`

1 configure

2 prepare

3 precheck

4 download

5 upgrade

6 postcheck

7 abort

8 query

x exit

Please select an option:

54.6.2.2 CLI - Interactive Mode configure Option

Issuing the *mg9kuptool -configure* command or selecting this option from the interactive list will bring up the following dialog:

NOTE: All input is case sensitive.

In which directory on the imaging server do the loads reside?

/swd/mg9k

Enter MTA loadname:

MTAG07EJ_1_GZ

Enter XDSL loadname:

DSL06_2EI

Enter DS1 loadname:

DS1G08BV_GZ.tar

Enter ABI loadname:

ABIG08BV_GZ.tar

Enter ITP loadname:

ITPA08BV_GZ.tar

Enter ITX loadname:

ITXA08BV_GZ.tar

Enter SCO loadname:

```
SCOA08BV_GZ.tar
```

```
Enter SCI loadname:
```

```
SCIA08BV_GZ.tar
```

```
Verifying loads on SDM.....
```

```
Loads valid.
```

```
Which NE(s) do you want to upgrade/downgrade? Enter NE  
number. If more than 1 NE separate with commas (e.g. 8,9):
```

```
8
```

```
Plan name is /data/mg9kem/persistdata/MG9kUpgradePlan.dat
```

54.6.2.3 CLI - Interactive Mode prepare Option

Issuing the *mg9kuptool -prepare* command or selecting this option from the interactive list will bring up the following dialog:

```
Have you put the patch files on the NPM? Y/N
```

```
Y
```

```
Upgrading to loads:
```

```
/swd/mg9k/MTAG07EJ_1_GZ
```

```
/swd/mg9k/DSL06_2EI
```

```
/swd/mg9k/DS1G08BV_GZ.tar
```

```
patchlist:
```

```
none
```

```
/swd/mg9k/ABIG08BV_GZ.tar
```

```
patchlist:
```

```
AMZ005
```

```
/swd/mg9k/ITPA08BV_GZ.tar
```

```
patchlist:
```

```
AMZ006
```

```
HDD013
```

```
HDD014
```

```
HDD015
```

```
/swd/mg9k/ITXA08BV_GZ.tar
```

```

patchlist:

none

/swd/mg9k/SCOA08BV_GZ.tar

patchlist:

AMZ007

AMZ008

HDD016

/swd/mg9k/SCIA08BV_GZ.tar

patchlist:

AMZ008

Please compare the patchlists above against the Nortel web
page.

NE# 8: time to download is 1 hour

time to upgrade is 1.5 hours
time to patch is 27 minutes

```

54.6.2.4 CLI - Interactive Mode precheck Option

Issuing the *mg9kuptool -precheck* command or selecting this option from the interactive list will bring up the following dialog:

Enter the node number or node number list for the precheck request:
 <the displayed default is the list of all NEs in the plan>

54.6.2.5 CLI - Interactive Mode download Option

Issuing the *mg9kuptool -download* command or selecting this option from the interactive list will bring up the following dialog:

Enter the node number or node number list for the download request:
 <the displayed default is the list of all NEs in the plan>

54.6.2.6 CLI - Interactive Mode upgrade Option

Issuing the *mg9kuptool -upgrade* command or selecting this option from the interactive list will bring up the following dialog:

This process will affect DSL traffic and should be performed during a maintenance window only.

Enter the node number or node number list for the upgrade request:
 <the displayed default is the list of all NEs in the plan>

54.6.2.7 CLI - Interactive Mode postcheck Option

Issuing the *mg9kuptool -postcheck* command or selecting this option from the interactive list will bring up the following dialog:

Enter the node number or node number list for the postcheck request:

<the displayed default is the list of all NEs in the plan>

54.6.2.8 CLI - Interactive Mode abort Option

Issuing the *mg9kuptool -abort* command or selecting this option from the interactive list will bring up the following dialog:

Enter the node number or node number list for the abort request:

<the displayed default is the list of all NEs in the plan>

54.6.2.9 CLI - Interactive Mode query Option

Issuing the *mg9kuptool -query* command or selecting this option from the interactive list will bring up the following dialog:

Enter the node number or node number list for the query request:

<the displayed default is the list of all NEs in the plan>

54.6.3 Customer Logs

Customer logs will be created each time the *mg9kuptool* is executed. A new NT standard log number will be defined as follows:

MGEM714

54.6.3.1 Format

Here is an example of the new MGEM 714 log:

```
Aug 18 15:07:28 apex-unit0 MGEM: 714 Executing
mg9kuptool command precheck
```

54.6.3.2 Field descriptions

Table 2 Field descriptions

Field	Description	Example
Date/Time	Date and time stamp of the log	Aug 18 15:07:28
Host Name	Host machine name	apex-unit0
Application Name	The application producing the log	MGEM
Log Number	The log number	714
Log Text	The action being taken	Executing mg9kuptool command precheck

54.7 Glossary

Table 3

Term	Description
CLI	Command Line Interface
CLUI	Command Line User Interface
EM	Element Manager
GUI	Graphical User Interface
IEMS	Integrated Element Manager System
MG9K	Media Gateway 9000
MR	Maintenance Release
NE	Network Element
NPM	Network Patch Manager
SDM	Succession Data Manger

55: A00007140B Functional description (FN)

55.1 Introduction

55.1.1 Feature name

Upgrade Manager Phase I -- GWC and SC parts.

55.1.2 Overview

As of SN07, Succession CallServer subnetwork upgrades have been performed using a purely manual process which has required a significant amount of human power to orchestrate. Also, the upgrade technician has been forced to navigate hundreds of pages of documentation in order to successfully plan and complete the end-to-end system upgrade. As a result, Succession CallServer subnetwork upgrades have been extremely difficult to manage and have been a constant source of concern/dissatisfaction with Nortel customers.

The SN08 Succession Upgrade Manager delivers:

- a robust SC upgrade tool.
- a robust GWC upgrade tool.
- a robust MG9K upgrade tool. (This FN covers only the GWC and SC upgrade tools. The MG9K is in another document.)

The SC and GWC upgrade tools serve as the underlying per-network element tools for the end architecture. The intent for SN08 is to focus as much effort as required to make these underlying tools as robust and complete as possible.

As part of the SN08 Succession upgrade tools, the SC and GWC upgrade tools both provide a pure CLI for the customer or upper-level coordinator to invoke upgrade functionalities. In addition, an interactive CLUI is also provided to customers for easy using the tool. The following content will give a detailed description on SC and GWC.

55.1.3 Internally used options

SC and GWC upgrade tool are designed to be working with upper level MOP automation tool. So there are some internal used options which will not appear in the customer documentations.

55.2 Deployment

Basically the GWC and SC upgrade tool will be packaged within the GWC and SC element manager servers.

55.2.1 SC upgrade tool

It will be part of the NTsam21em package, when the SAM21EM is configured and running properly, the SC upgrade tool is ready to use.

In the SSPFS running environment, SC upgrade tool will be located in

- /opt/nortel/sam21em/bin/*scuptool.sh* -- Program entry
- /opt/nortel/sam21em/classes -- Jar files

55.2.2 GWC upgrade tool

GWC uptool will be part of NTsesm package, and it will be located in

- /opt/nortel/NTsesm/gwcuptool -- Base directory
- /opt/nortel/NTsesm/gwcuptool/bin -- All scripts
- /opt/nortel/NTsesm/gwcuptool/jars -- Jar files
- /opt/nortel/NTsesm/gwcuptool/bin/*gwcuptool.sh* -- Program entry

If you want to use the GWC upgrade tool the following applications must be configured, and running properly:

- SAM21EM is running;
- SESM Service is running;
- NPM/PSE is configured properly

55.2.3 Running restriction

Users must belong to one of these groups “mgcmte, mgcadm, emsmte, emsadm”, who has permission to run the upgrade tools.

55.3 GWC Upgrade Tool

In SN08, GWC will provide a basic CLI interface and an interactive CLUI that based on the basic CLI interface.

GWC upgrade tool provides the basic functions that GWC upgrading needs. They are:

- Start GWC upgrade manager server prior to client launching.
- Configure upgrade options before actual upgrade.
- Prepare necessary steps for getting the tool and system ready prior to the actual upgrade.
- Pre-check relevant EM and configured GWC states including alarms.
- Upgrade configured GWC with configured options.
- Post-check upgraded GWC states including alarms.
- Query GWC upgrade states in progress.

- Query GWC info and list them by profile types.
- Query configurations currently used.
- Stop upgrade manager server.
- The help of the functions.

All these functions are provided by a shell named ***gwcuptool.sh***. End user should run the corresponding commands in an order which will be shown in appendix. The order can let you meet as little as possible warnings and errors. It's a mandatory order.

55.3.1 Restriction for GWC upgrade

Because GWC upgrade tool need SESM, SAM21EM, and NPM to execute the real device operations, during the GWC upgrade is in progress, following functions will be disabled to prevent from unexpected problems:

- All provisioning actions in SESM;
- All (CS2k/V5.2/Trunk/Line) Data Integrity Audits;
- GWC auto imaging in GWCEM;
- GWC auto patching in NPM;

When upgrade is finished, provisioning functions will be enabled automatically by GWC upgrade tool.

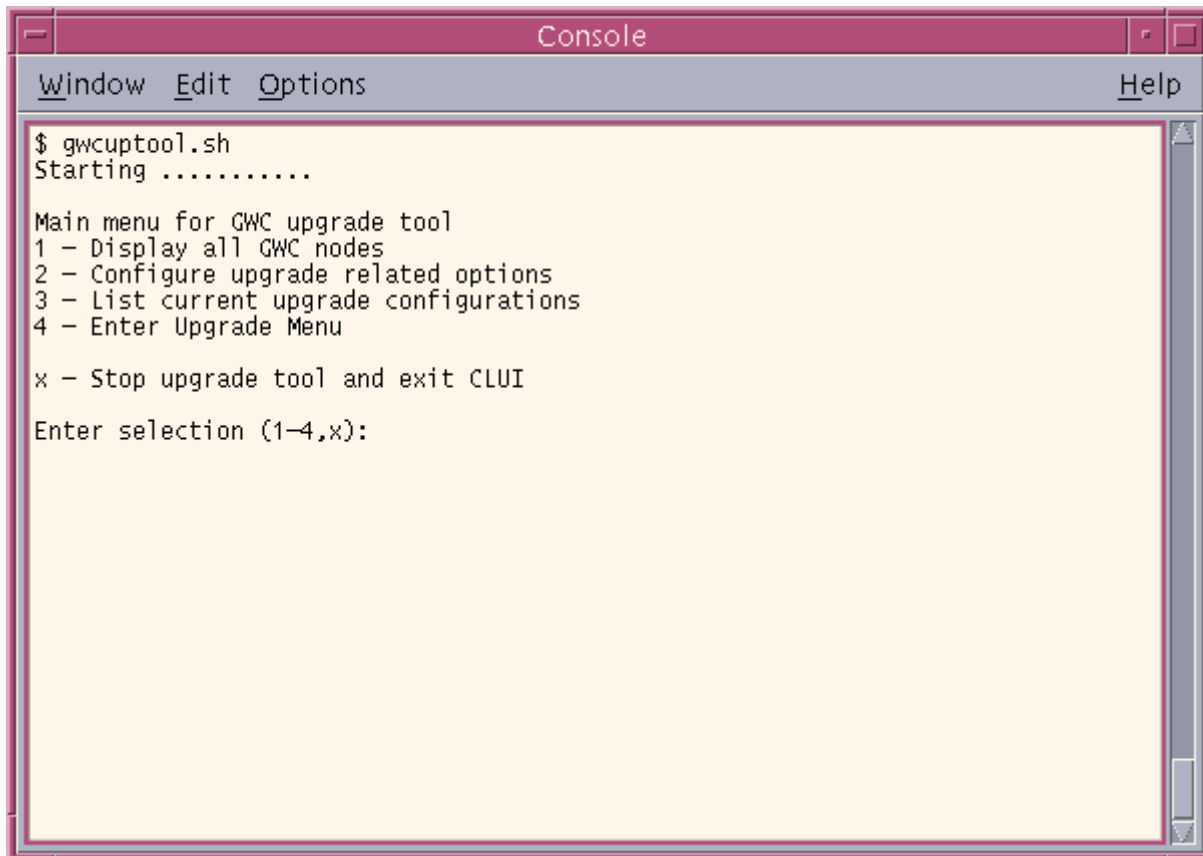
Before using this tool, end user must make sure that PSE in the same SSPFS must be configured properly.

When user/password is required, end user must make sure that the login user belongs to one of these groups "mgcmte, mgcadm, emsmte, emsadm". Otherwise, operation is denied.

55.3.2 Interactive CLUI

The interactive CLUI is a shell that wraps basic CLI. It provides a "restricted" tool to achieve upgrade goal.

Issue "gwcuptool.sh" to launch GWC upgrade tool CLUI. The main menu is as following.



```
$ gwcuptool.sh
Starting .....

Main menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade related options
3 - List current upgrade configurations
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

There are total five selections in main menu. They are:

1. Display all GWC nodes

This selection is to query all GWC nodes info, includes name, ip and state.

2. Configure upgrade related options

This selection is to configure upgrade options manually. CLUI will prompt end user to input necessary info step by step. These options are effective in the whole upgrade process.

3. List current upgrade configurations

This selection is to list all options currently used.

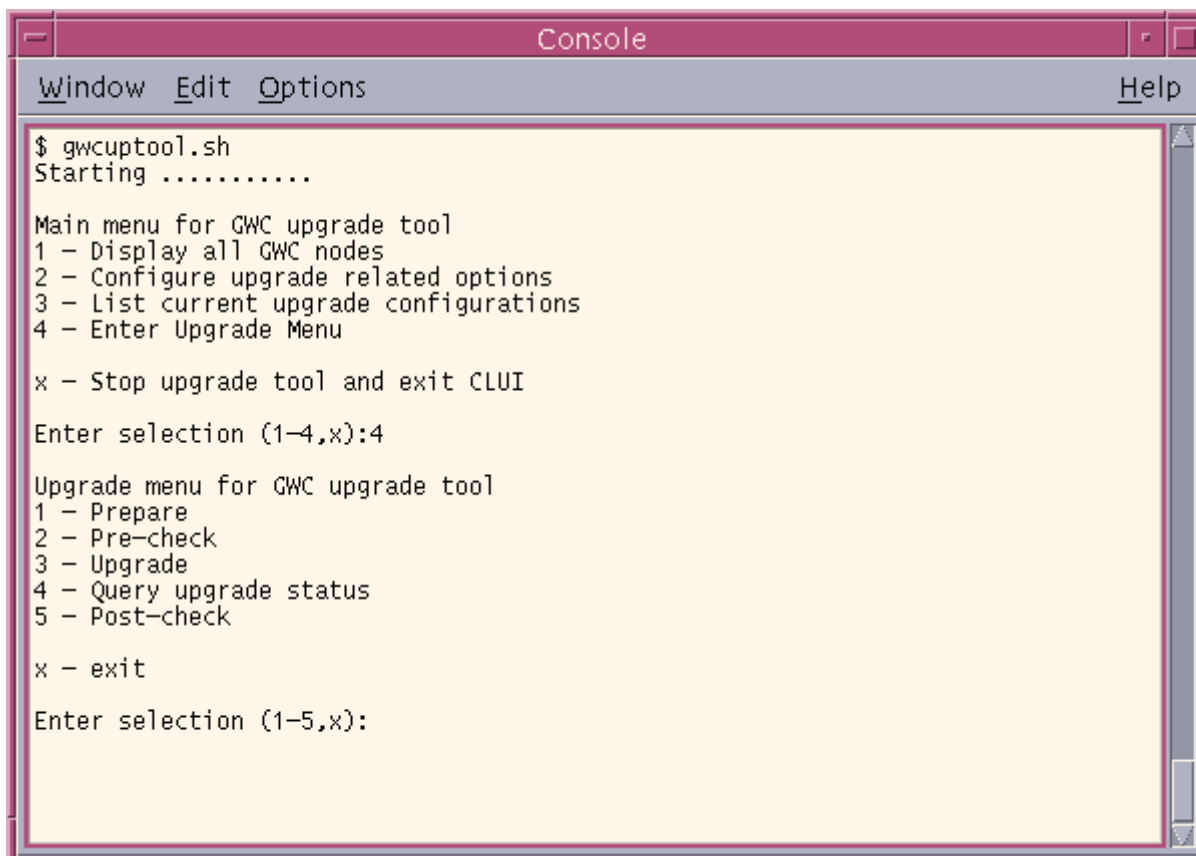
4. Enter upgrade menu

This selection is to enter upgrade submenu.

5. Stop upgrade tool and exit CLUI

This selection is to stop GWC upgrade tool and exit CLUI.

When selection 4 is selected, end user will enter upgrade submenu to do real upgrade process. The follow figure is upgrade submenu.



```
Console
Window Edit Options Help
$ gwcuptool.sh
Starting .....

Main menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade related options
3 - List current upgrade configurations
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):4

Upgrade menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

Enter selection (1-5,x):
```

There are total six selection in upgrade submenu. All these selections are based on the options configured in main menu.

- Prepare
This selection is to do preparation prior to actual upgrade.
- Pre-check
This selection is to do pre-check prior to actual upgrade.
- Upgrade
This selection is to do real upgrade.
- Query upgrade status
This selection is to query upgrade status.
- Post-check
This selection is to do post-check after actual upgrade.

- exit

This selection is to exit upgrade submenu and enter main menu.

55.3.3 Basic CLI

According to the above functions, gwcuptool.sh provides its corresponding command to achieve these functions. The following gives the details.

55.3.3.1 Start GWC upgrade manager server prior to client launching.

```
gwcuptool.sh -start [-gwcm ip:port] [-sam21em ip:port] [-sid sid]
```

Command description:

Start GWC upgrade tool server, it will do the following actions.

- Request end user to input user name/password if not apply session ID in command.
- Connect to GWCEM / SAM21EM through CORBA;
- Check whether this user has permission to perform the upgrade operations.

Options:

[1] -gwcm

Requirement: Internally used options.

Description: Provide CORBA server ip and port GWCEM server registered.

Default: localhost:2001

[2] -sam21em

Requirement: Internally used options.

Description: Provide CORBA server ip and port SAM21EM server registered.

Default: localhost:2001

[3] -sid

Requirement: Internally used options.

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: gwcuptool.sh -start

If end user only issues "gwcuptool.sh -start", only the user who belongs to one of "mgcmte, mgcadm, emsmte, emsadm" groups, can run the tool.

55.3.3.2 Configure upgrade options before actual upgrade.

```
gwcuptool.sh -config [-n <GWC list>] [-o [value]]...
```

Command description:

Configure upgrade options. These options are useful to upgrade, pre-check, post-check and query commands.

Note:

1. All configurations' default value will be stored in a property file on upgrade manager server machine. We don't support customers to modify it themselves.
2. When only "gwcuptool.sh -config -list" is issued, upgrade manager server will return all current configurations. Its functionality is query configuration.
3. If end user only issues "gwcuptool.sh -config", shell will prompt end user to input necessary info step by step.
4. When the second configuration command is issued, all prior configurations will be replaced.

The following are detailed options.

[1] -pa load_directory_name

Requirement: Optional

Description: Specify the load file path in SDM/CBM. If no directory name applied, the default directory '/swd/gwc/' will be used.

Default: "/swd/gwc/"

Example: -pa /swd/gwc/

[2] -f new_load_file_name

Requirement: Mandatory

Description: Target load file name. User must specify a load file name here. Otherwise, config function will return error message.

Default: ""

Example: -f gn080ak.imag

[3] -l new_load_name

Requirement: Optional

Description: Target load name of given GWC load file. The new load name will be used to query the patch list from NPM. If the file name doesn't contain GWC load name, end user MUST specify a valid GWC load name here.

Default: new load file name except ".imag"

Example: -l GN080AK

[4] -o old_load_name

Requirement: Optional

Description: The load upgrade from. If end user ignores it, upgrade manager server will bypass old load checking. By default user don't need to specify the old load name, and all selected GWC node will be upgraded automatically.

Default: ""

Example: -o GN070BK

```
[5] -m <single | bulk | mix>
```

Requirement: Optional

Description: Upgrade mode

- single: all GWC nodes will be upgraded one by one ordered by GWC profile type and GWC ID.
- bulk: All GWC nodes within the same service group (e.g. TRUNK, LINE) will be upgraded at the same time. If patching is needed, the first selected “seed” GWC node which is used to create the soak image will use single mode and the others that don’t need patching will use bulk mode.
- mix: In the same GWC profile group (e.g. TRUNK GWCs, Line GWCs), One GWC node will be upgraded firstly.(Purpose: end user can do verification on specified type of GWC.) After it is upgraded successfully, all other GWC nodes within the same profile group will be upgraded at the same time.

See “Appendix 3: Upgrade mode examples in GWC upgrade tool” on page 484.

Default: bulk.

Example: -m bulk

```
[6] -p [0,1,2,3,4,5,6]
```

Requirement: Optional

Description: Upgrade pause points. If end user doesn't provide this option, no pause point during upgrading.

The following shows what the number means.

1. For the first GWC node within the same GWC group.
 - 1, before lock the first upgrade unit of “seed” node.
 - 2, after patch applied to the “seed” unit.
 - 3, before warm-swact.
 - 4, after “seed” node upgraded.
 - 5, pause on all above conditions.
2. For bulk upgrade GWC nodes with same GWC profile type.
 - 6, before warm-swact.

Default: 0, without any pause points.

Example: -p '1,3,4'

The example option means upgrade will pause on condition 1,3, 4.

```
[7] -d [VRB | MAJ | MNR | CRT ]
```

Requirement: Optional

Description: Define logging level for the upgrade log file.

VER: Logging verbose info.

MAJ: Logging major info.

MNR: Logging minor info.

CRT: Logging critical info.

Default: MAJ.

Example: -d MNR

[8] -s

Requirement: Optional. Internally used by designer.

Description: Skip patching because the given load is soaked. Don't apply patches on the new GWC load.

Example: -s

[9] -n <GWC list>

Description: Define the GWC list which should be upgraded. And it will be the default GWC list for pre-check, upgrade, post-check and query commands.

Default: all

Example: -n 'GWC-1,GWC-2,GWC-3,GWC-5'

[10] -t <mins>

Description: Define a time limitation for doing upgrade. If upgrade can't complete all nodes within the given time slot. The un-upgraded GWC nodes will be kept there. And the upgrade will be finished. If "0" is specified as the time limitation, the limitation check will be disabled.

Default: 0

Example: -t 180

Note: The time begins when "gwcupptool.sh -up" command is executed.

Second "gwcupptool.sh -up" command does not reset time slot.

[11] -np <max parallel number>

Requirement: Optional. Internally used by designer.

Description: Max parallel number during bulk upgrade.

Default: 32

Example: -np 16

[12] -a [CRT | MAJ] -an [number]

Requirement: Optional.

Description: Allowed highest alarm level during upgrade, and allowed max alarm number during upgrade. It is a dynamic alarm checking values. If current alarm state has higher priority than its defined here, the upgrade program will be paused and notify this to end user.

For examples, if we specify "-a MAJ -an 2" in config step,

- If there are 3 MAJ alarms raised in EM Server for this node, the upgrade tool will be paused
- If there is 1 MAJ alarm raised in EM Servers for this node, the upgrade tool will ignore it. And continue the upgrade process.
- If there is 1 CRT alarm raised in EM Server for this node, the upgrade tool will be paused too because CRT has high priority than MAJ alarms.

Default: MAJ 2

Example: -a CRT -an 2

[13] -sid sid

Requirement: Optional, Internally used by MOP automation tool,

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option. This option is not a part of configuration

Default: 0

Example: gwcuptool.sh -config -f gn080ak.imag -sid
312308CDA87F5C7ECD3185F639892BC2

A whole command format likes:

```
gwcuptool.sh -config -f gn080ak.imag -o GN070BV -m
bulk -p '1,3,4' -d CRT -n 'GWC-1' -t 120 -a CRT -an
4 -sid 312308CDA87F5C7ECD3185F639892BC2
```

55.3.3.3 Prepare necessary steps for getting the tool and system ready prior to the actual upgrade.

```
gwcuptool.sh -prep [-sid sid]
```

Command description:

Show the end user the necessary preparations which include upgrade steps and order, notes and warnings.

The following actions should be checked in prepare command.

1. Check the load available in SDM/CBM.
2. Get the patch list from NPM, display the patch list to end user, and ask end user to confirm.
 - This will based on the load name specified in the “-config” step, by default the load file name will be used as load name.
 - GWC Upgrade tool will use the load name to query the list of patches that NPM knows about;
 - The list of patches will be presented to the user;
 - And prompt the user to tell them that they need to go to the Nortel web site and verify that the list they have is the list that they should have, and make them type “Y”/“yes” to confirm that they've verified this before we allow the prepare to succeed.
3. Display the upgrade plan for GWC.
4. And calculate the estimated time of upgrade.

Options:

```
[1] -sid sid
```

Requirement: Optional, Internally used by MOP automation tool,

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option. This option is not a part of configuration

Default: 0

Example: gwcuptool.sh -prep -sid
312308CDA87F5C7ECD3185F639892BC2

55.3.3.4 Pre-check relevant EM and configured GWC states including alarms.

```
gwcuptool.sh -precheck [-n <GWC List>] [-sid sid]
```

Command description:

Pre-check the necessary conditions before upgrade.

If there isn't any given GWC list, the configured GWC list will be used here.

Perform the following actions:

- A. GWCEM, SAM21EM and NPM server status
- B. Load is available on load server. (Get from SAM21EM server.)
- C. Alarm status.
- D. Hardware level health check. If the node has two physical units, and both of them are in service.
- E. Software level health check. The inactive unit is hot-standby.

[1] -n <GWC List>

Requirement: Internally used by MOP automation tool

Description: GWC nodes which should be upgraded. If there isn't any given GWC list, the configured GWC list will be used here.

[2] -sid sid

Requirement: Optional, Internally used by MOP automation tool,

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: gwcuptool -precheck -sid
312308CDA87F5C7ECD3185F639892BC2

55.3.3.5 Upgrade configured GWC with configured options.

```
gwcuptool.sh -up [-n <GWC list>] [-sid sid]
```

Command description:

Does the real upgrade work. Still perform the pre-check / post-check in this command. During upgrade the client side will display the logs sent from server side, and may need to answer some question or do some confirmation for

different conditions. If end user enabled break points, this tool will work as an interactive mode.

When the “seed” GWC node’s inactive unit was patched, the GWC upgrade tool will invoke the function provide by NPM to query the patch applying status, and display this to end user.

[1] -n <GWC List>

Requirement: Internally used by MOP automation tool

Description: GWC nodes which should be upgraded. If there isn't any given GWC list, the configured GWC list will be used here.

[2] -sid sid

Requirement: Internally used by MOP automation tool

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: gwcuptool.sh -up -sid 312308CDA87F5C7ECD3185F639892BC2

55.3.3.6 Post-check upgraded GWC states including alarms.

```
gwcuptool.sh -postcheck [ -n <GWC list>] [-sid sid]
```

Command description:

Do the post-check for the given GWC nodes.

If there isn't any given GWC list, the configured GWC list will be used here. The following status will be checked.

1. Application status from GWCEM.
2. Alarm state
3. Query the patch applied status from NPM

[1] -n <GWC List>

Requirement: Internally used by MOP automation tool

Description: GWC nodes which should be upgraded. If there isn't any given GWC list, the configured GWC list will be used here.

[2] -sid sid

Requirement: Internally used by MOP automation tool

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: gwcuptool.sh -postcheck -sid
312308CDA87F5C7ECD3185F639892BC2

55.3.3.7 Query upgrade states in progress.

```
gwcuptool.sh -query [ -n <GWC list> ] [-sid sid]
```

Command description:

Query the status of GWC units and upgrade status.

The status includes two parts. If no upgrading GWC, no part A status exists.

If there isn't any given GWC list, the configured GWC list will be used here.

A. Upgrade status report.

Report includes following items:

- 1) GWC-ID: e.g. GWC-3
- 2) Current upgrade step: e.g. SWACT (7 / 12)
- 3) Spent time: e.g. 10 minutes
- 4) Time left: e.g. about 13 minutes.

B. Unit status report

Report items.

- 1) GWC Unit name: GWCUnit IP
- 2) GWC type and profile.
- 3) GWC load info. Upgraded or not.
- 4) Status from GWCEM
- 5) Status from SAM21EM

```
[1] -n <GWC List>
```

Requirement: Optional

Description: Only the specified GWC node status will be showed out.

```
[2] -sid sid
```

Requirement: Internally used by MOP automation tool.

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: gwcuptool.sh -query -sid

```
312308CDA87F5C7ECD3185F639892BC2
```

55.3.3.8 Query GWC info and list them by profile types.

```
gwcuptool.sh -query -n all [-sid sid]
```

Command description:

Query all GWC info including name, ip and state.

This command reuses “gwcuptool.sh -query” interface, it can list all GWCs' info and show them by profile types.

Example: gwcuptool.sh -query -n all -sid

```
312308CDA87F5C7ECD3185F639892BC2
```

55.3.3.9 Query configurations currently used.

```
gwcuptool.sh -config -list [-sid sid]
```

Command description:

Query current configurations. It reuses the “gwcuptool.sh -config” interface.

Example: gwcuptool.sh -config -list -sid
312308CDA87F5C7ECD3185F639892BC2

55.3.3.10 Stop upgrade manager server.

```
gwcuptool.sh -stop [-sid sid]
```

Command description:

Stop upgrade server.

Options:

```
[1] -sid
```

Requirement: Internally used by MOP automation tool

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: gwcuptool.sh -stop -sid
312308CDA87F5C7ECD3185F639892BC2

55.3.3.11 Help of the functions.

```
gwcuptool.sh -start -h
gwcuptool.sh -config -h
gwcuptool.sh -prep -h
gwcuptool.sh -precheck -h
gwcuptool.sh -up -h
gwcuptool.sh -postcheck -h
gwcuptool.sh -query -h
gwcuptool.sh -stop -h
```

Command description:

Show end user the help of the functions. It includes function description, option meaning and usage.

How to use above separate commands to achieve a complete upgrade task, appendix 1 gives you an example.

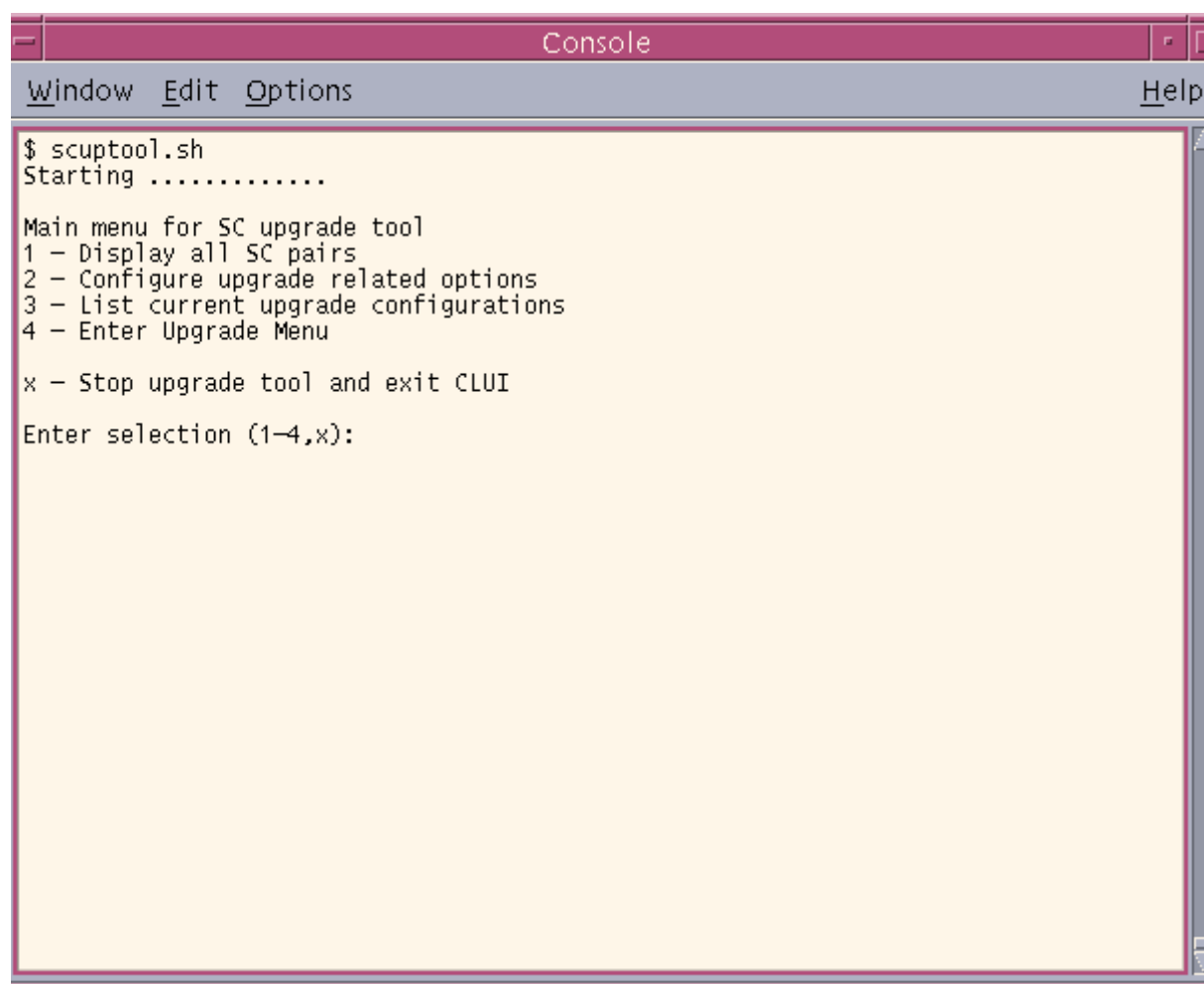
55.4 SC Upgrade Tool

In SN08, SC will provide a basic CLI interface and an interactive CLUI that based on the basic CLI interface.

55.4.1 Interactive CLUI

The interactive CLUI is a shell that wraps basic CLI. It provides a “restricted” tool to achieve upgrade goal.

Issue “suptool.sh” to launch SC upgrade tool CLUI. The main menu is as following.

A screenshot of a terminal window titled "Console". The window has a menu bar with "Window", "Edit", "Options", and "Help". The terminal content shows the execution of "suptool.sh", which starts a main menu for the SC upgrade tool. The menu lists four options: 1 - Display all SC pairs, 2 - Configure upgrade related options, 3 - List current upgrade configurations, and 4 - Enter Upgrade Menu. It also includes an option 'x' to stop the tool and exit the CLUI. The prompt "Enter selection (1-4,x):" is displayed at the bottom of the menu.

```
$ suptool.sh
Starting .....

Main menu for SC upgrade tool
1 - Display all SC pairs
2 - Configure upgrade related options
3 - List current upgrade configurations
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI
Enter selection (1-4,x):
```

There are total five selections in main menu. They are:

1. Display all SC pairs

This selection is to query all SC nodes info, includes name, ip and state.

2. Configure upgrade related options

This selection is to configure upgrade options manually. CLUI will prompt end user to input necessary info step by step. These options are effective in the whole upgrade process.

3. List current upgrade configurations

This selection is to list all options currently used.

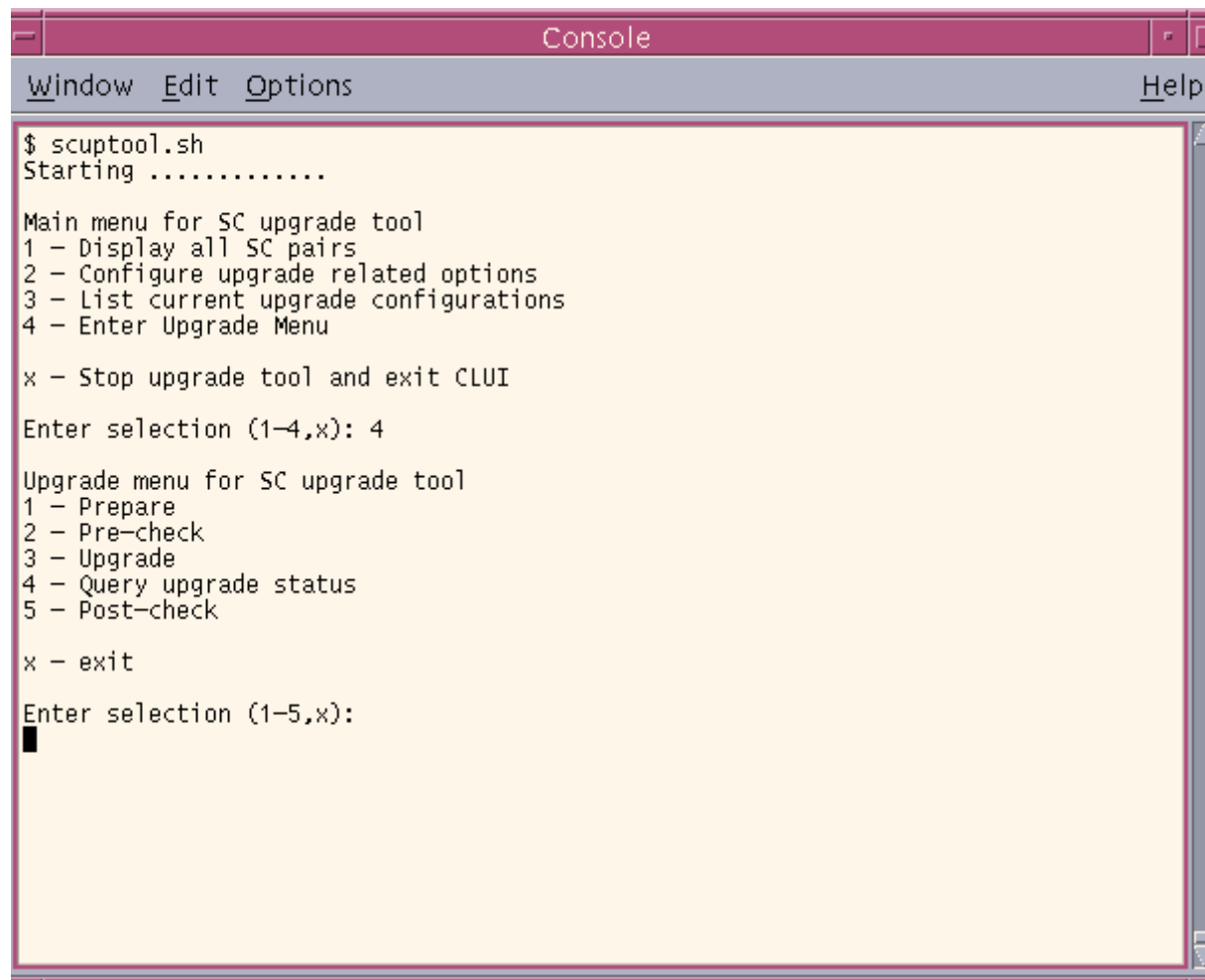
4. Enter upgrade menu

This selection is to enter upgrade submenu.

5. Stop upgrade tool and exit CLUI

This selection is to stop SC upgrade server and exit CLUI.

When selection 4 is selected, end user will enter upgrade submenu to do real upgrade process. The follow figure is upgrade submenu.



```
$ scuptool.sh
Starting .....

Main menu for SC upgrade tool
1 - Display all SC pairs
2 - Configure upgrade related options
3 - List current upgrade configurations
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x): 4

Upgrade menu for SC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

Enter selection (1-5,x):
█
```

There are total six selection in upgrade submenu. All these selections are based on the options configured in main menu.

- Prepare

This selection is to do preparation prior to actual upgrade.

- Pre-check

This selection is to do pre-check prior to actual upgrade.

- Upgrade

This selection is to do real upgrade.

- Query upgrade status

This selection is to query upgrade status.

- Post-check

This selection is to do post-check after actual upgrade.

- exit

This selection is to exit upgrade submenu and enter main menu.

55.4.2 Basic CLI

The basic CLI provides the basic functions that SC upgrading needs. They are:

- Start SC upgrade manager server prior to client launching.
- Configure upgrade options before actual upgrade.
- Prepare necessary steps for getting the tool and system ready prior to the actual upgrade.
- Pre-check relevant EM and configured SC states including alarms.
- Upgrade configured SC with configured options.
- Post-check upgraded SC states including alarms.
- Query SC upgrade states in progress.
- Query SC info and list them.
- Query configurations currently used.
- Stop upgrade manager server.
- The help of the functions.

All these functions are provided by a shell named *scuptool.sh*. Although end user can use every function without order, we recommend that you should run the corresponding commands in an order which will be shown in appendix. The order can let you meet as little as possible warnings and errors. It's a mandatory order.

According to the above functions, *scuptool.sh* provides its corresponding command to achieve these functions. The following gives the details.

55.4.2.1 Start SC upgrade manager server prior to client launching.

```
scuptool.sh -start [-sam21em ip:port][-sid sid]
```

Command description:

Start SC upgrade tool server, it will do the following actions.

- Request end user to input user name/password if not apply session ID in command.
- Connect to SAM21EM through CORBA;
- Check whether this user has permission to perform the upgrade operations.

Options:

[1] -sam21em

Requirement: Internally used options.

Description: Provide CORBA server ip and port SAM21EM server registered.

Default: localhost:2001

[2] -sid

Requirement: Internally used by MOP automation tool

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: `suptools.sh -start -sam21em localhost:2001 -sid 312308CDA87F5C7ECD3185F639892BC2`

If end user only issues “`suptools.sh -start`”, only the user who belongs to one of “`mgcmte`, `mgcadm`, `emsmte`, `emssadm`” groups, can run the tool.

55.4.2.2 Configure upgrade options before actual upgrade.

```
suptools.sh -config [-n <SC list>] [-o [value]] ...
```

Command description:

Configure upgrade options. These options are useful to upgrade, pre-check, post-check and query.

Note:

1. All configurations' default value will be stored in a property file on upgrade manager server machine.
2. When only “`suptools.sh -config -list`” is issued, upgrade manager server will return all current configurations.
3. If end user only issues “`suptools.sh -config`”, shell will prompt end user to input necessary info step by step.
4. When the second configuration command is issued, all prior configurations will be replaced.

The following are detailed options.

[1] -pa load_directory_name

Requirement: Optional

Description: Specify the load file path in SDM/CBM. If no directory name applied, the default directory '/swd/sam21/' will be used.

Default: “/swd/sam21/”

Example: -pa “/swd/sam21/”

[2] -f new_load_file_name

Description: Target load file name. This option is mandatory.

Default: “”.

Example: -f “11.0.0.047231351”

[3] -o old_load_name

Requirement: Optional

Description: The load upgrade from. If end user ignores it, upgrade manager server will bypass old load checking. By default user don’t need to specify the old load name, and all selected SC pair will be upgraded automatically.

Default: “”.

Example: -o “10.0.0.047231351”

[4] -m <single | bulk >

Description: Upgrade mode (Optional)

single: all SC pairs will be upgraded one by one ordered by SC ID.

bulk: All other SC pairs will be upgraded at the same time.

Default: bulk.

Example: -m bulk

[5] -p [0,1,2,3,4,5]

Description: Upgrade pause points. (Optional) If end user doesn't provide this option, no pause point during upgrading.

The following shows what the number means.

1. For the first SC pair.
 - 1, before lock the first upgrade unit of “seed” pair.
 - 2, before warm-swact.
 - 3, after “seed” pair upgraded.
 - 4, pause on all above conditions.
2. For bulk upgrade SC pairs.
 - 5, before warm-swact.

Default: 0, without any pause points.

Example: -p '1,2,3'

The example option means upgrade will pause on condition 1,2,3.

[6] -d [VRB | MAJ | MNR | CRT]

Requirement: Optional

Description: Define logging level for the upgrade log file.

- VER: Logging verbose info.
- MAJ: Logging major info.
- MNR: Logging minor info.
- CRT: Logging critical info.

Default: MAJ.

Example: -d MNR

[7] -n <SC list>

Description: Provide a SC list for pre-check, upgrade, post-check and query.

Default: all

Example: -n 'SC1,SC2,SC3,SC5'

[8] -t <mins>

Description: Define a time limitation for doing upgrade. If upgrade can't complete all pairs within the given time slot. The un-upgraded SC pairs will be kept there. And the upgrade will be finished. If "0" is specified as the time limitation, the limitation check will be disabled.

Default: 0

Example: -t 180

Note: The time begins when "suptool.sh -up" command is executed. Second "suptool.sh -up" command does not reset time slot.

[9] -np <max parallel number>

Requirement: Optional. Internally used by designer.

Description: Max parallel number during bulk upgrade.

Default: 8

Example: -np 8

[10] -a [CRT | MAJ] -an [number]

Requirement: Optional.

Description: Allowed highest alarm level during upgrade, and allowed max alarm number during upgrade. It is a dynamic alarm checking values. If current alarm state has higher priority than its defined here, the upgrade program will be paused and notify this to end user.

For examples, if we specify "-a MAJ -an 2" in config step,

- If there are 3 MAJ alarms raised in EM Server for this pair, the upgrade tool will be paused.
- If there is 1 MAJ alarm raised in EM Servers for this pair, the upgrade tool will ignore it. And continue the upgrade process.
- If there is 1 CRT alarm raised in EM Server for this pair, the upgrade tool will be paused too because CRT has high priority than MAJ alarms.

Default: MAJ 2

Example: -a CRT -an 2

[11] -sid sid

Requirement: Internally used by MOP automation tool

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: suptool.sh -config -f 11.0.0.047231351 -sid 312308CDA87F5C7ECD3185F639892BC2

Note: This option is not a part of configuration.

A whole command format likes:

```
scuptool.sh -config -f 11.0.0.047231351 -o
10.0.0.047231351 -m bulk -p '1,3' -d CRT -n 'SC1' -t
120 -np 16 -a CRT -an 4 -sid
312308CDA87F5C7ECD3185F639892BC2
```

55.4.2.3 Prepare necessary steps for getting the tool and system ready prior to the actual upgrade.

```
scuptool.sh -prep [-sid sid]
```

Command description:

Show end user the necessary preparations which include upgrade steps and order, notes and warnings.

The following actions should be checked in prepare command.

1. Check the load available in SDM/CBM.
2. Make an upgrade plan for SC and calculate the estimated time of upgrade.

Options:

```
[1] -sid
```

Requirement: Internally used by MOP automation tool

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: scuptool.sh -prep -sid 312308CDA87F5C7ECD3185F639892BC2

55.4.2.4 Pre-check relevant EM and configured SC states including alarms.

```
scuptool.sh -precheck -n <SC list>] [-sid sid]
```

Command description:

Pre-check the necessary conditions before upgrade.

If there isn't any given SC list, the configured SC list will be used here.

Perform the following actions:

- A. SAM21EM server status
- B. Load is available on load server.
- C. Alarm status.
- D. Hardware level health check. If the pair has two physical units, and both of them are in service.
- E. Whether the inactive unit is hot-standby.

```
[1] -n <SC List>
```

Requirement: Internally used by MOP automation tool

Description: SC pairs which should be upgraded. If there isn't any given SC list, the configured SC list will be used here.

[2] -sid sid

Requirement: Internally used by MOP automation tool

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: `suptool.sh -precheck -sid 312308CDA87F5C7ECD3185F639892BC2`

55.4.2.5 Upgrade configured SC with configured options.

```
suptool.sh -up [ -n <SC list>] [-sid sid]
```

Command description:

Does the real upgrade work. Still perform the pre-check / post-check in this command. During upgrade, the client side will display the logs sent from server side, and end user may need to answer some question or do some confirmation for different conditions. If end user enabled break points, this tool will work as an interactive mode.

If there isn't any given SC list, the configured SC list will be used here.

Note: Must prompt end user to do pre-check before upgrading. Pre-checked SC list is stored in server side. If no pre-checked SC, server will refuse upgrading.

[1] -n <SC List>

Requirement: Internally used by MOP automation tool

Description: SC pairs which should be upgraded. If there isn't any given SC list, the configured SC list will be used here.

[2] -sid sid

Requirement: Internally used by MOP automation tool

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: `suptool.sh -up -sid 312308CDA87F5C7ECD3185F639892BC2`

55.4.2.6 Post-check upgraded SC states including alarms.

```
suptool.sh -postcheck [ -n <SC list>] [-sid sid]
```

Command description:

Do the post-check for the given SC pairs.

If there isn't any given SC list, the configured SC list will be used here.

Following status will be checked.

1. Hardware status from SAM21EM.

2. Alarm state

[1] -n <SC List>

Requirement: Internally used by MOP automation tool

Description: SC pairs which should be upgraded. If there isn't any given SC list, the configured SC list will be used here.

[2] -sid sid

Requirement: Internally used by MOP automation tool

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: `scuptool.sh -postcheck -sid
312308CDA87F5C7ECD3185F639892BC2`

55.4.2.7 Query upgrade states in progress.

`scuptool.sh -query [ -n <SC list> ] [-sid sid]`

Command description:

Query the status of SC pairs and upgrade status.

The status includes two parts. If no upgrading SC, no part A status exists.

If there isn't any given SC list, the configured SC list will be used here.

A. Upgrade status report.

Report includes the following items:

- SC-ID: e.g. SC3
- Current upgrade step: e.g. SWACT.
- Spent time: e.g. 4 minutes
- Time left: e.g. about 5 minutes.

B. Unit status report

Report items.

- SC Unit name: SC Unit IP
- SC load info. Upgraded or not.
- Status from SAM21EM

[1] -n <SC List>

Requirement: Internally used by MOP automation tool

Description: SC pairs which should be upgraded. If there isn't any given SC list, the configured SC list will be used here.

[2] -sid sid

Requirement: Internally used by MOP automation tool

Description: Provide session ID upgrade manager uses. Upper-level upgrade

manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: `scuptool.sh -query -sid
312308CDA87F5C7ECD3185F639892BC2`

55.4.2.8 Query SC info and list them.

```
scuptool.sh -query -n all [-sid sid]
```

Command description:

Used to query all SC info including name, ip and state.

This command reuses “scuptool.sh -query” interface, it can list all SCs' info.

Example: `scuptool.sh -query -n all -sid
312308CDA87F5C7ECD3185F639892BC2`

55.4.2.9 Query configurations currently used.

```
scuptool.sh -config -list [-sid sid]
```

Command description:

Query current configurations. It reuses the “scuptool.sh -config” interface.

Example: `scuptool.sh -config -list -sid
312308CDA87F5C7ECD3185F639892BC2`

55.4.2.10 Stop upgrade manager server.

```
scuptool.sh -stop [-sid sid]
```

Command description:

Stop upgrade server.

Options:

[1] -sid

Requirement: Internally used by MOP automation tool

Description: Provide session ID upgrade manager uses. Upper-level upgrade manager can provide valid session ID to avoid re-login. End user needn't input this option.

Default: 0

Example: `scuptool.sh -stop -sid 312308CDA87F5C7ECD3185F639892BC2`

55.4.2.10.1 Help of the functions.

```
scuptool.sh -start -h
```

```
scuptool.sh -config -h
```

```
scuptool.sh -prep -h
scuptool.sh -precheck -h
scuptool.sh -up -h
scuptool.sh -postcheck -h
scuptool.sh -query -h
scuptool.sh -stop -h
```

Command description:

Show end user the help of the functions. It includes function description, option meaning and usage.

How to use these separate commands to achieve a complete upgrade task, appendix 2 gives you an example.

55.5 Hardware Requirements or Dependencies

No new hardware or hardware dependencies are introduced.

55.6 Software Requirements or Dependencies

No new customer software or firmware dependencies are introduced in this feature.

55.7 Limitations and restrictions

The limitations and restrictions work on both GWC and SC upgrade manager except for the items specified.

1. For Upgrade Manager Phase I, the upgrade tools must be running in the same SSPFS box with GWCEM/SESM and SAM21EM.
2. This version will not support multiple users. But end user can upgrade GWC nodes or SC pairs in parallel.
3. This version does not support automatically downgrade. End user must downgrade NE manually.
4. Both GWC and SC upgrade server only provide support for a full node upgraded. They do not allow single card/unit to be upgraded.

55.8 Interactions

No interactions between this feature and existing features.

55.9 Appendix 1: An example that how to use gwcuptool.sh to complete GWC upgrade in an office.

For SN07, GWC upgrade order:

- * 1. Audio
- * 2. BICC (UA-AAL1 solutions only)

- * 3. VRDN
- * 4. Session Server (SN07 to SN07 upgrades only)
- * 5. SIP-T/APG/RA
- * 6. APG/RA
- * 7. SIP-T/APG
- * 8. APG
- * 9. SIP-T
- * 10. Trunk
- * 11. H.323 (new in SN06.2)
- * 12. Proxy [RTP MP])
- * 13. V5.2 Trunk
- * 14. Lines (includes CICM)

Assumption:

* 1. Audio	GWC-1, GWC-3, GWC-5
* 2. BICC	GWC-7, GWC-9, GWC-11
* 3. VRDN	GWC-13, GWC-15, GWC-17
* 4. SIP-T/APG/RA	GWC-19, GWC-21, GWC-23
* 5. APG/RA	GWC-25, GWC-27, GWC-29
* 6. SIP-T/APG	GWC-31, GWC-33, GWC-35
* 7. APG	GWC-37, GWC-28, GWC-39
* 8. SIP-T	GWC-32, GWC-34, GWC-36
* 9. Trunk	GWC-26, GWC-28, GWC-30
* 10. H.323 (new in SN06.2)	GWC-20, GWC-22, GWC-24
* 11. Proxy [RTP MP])	GWC-14, GWC-16, GWC-18
* 12. V5.2 Trunk	GWC-8, GWC-10, GWC-12
* 13. Lines (includes CICM)	GWC-2, GWC-4, GWC-6

Note: You also can get the information by “gwcuptool.sh query -n all” command.

Step 1: Create a soak image on GWC-1. [Which GWC will be selected is determined by yourself.]

Create SSH communication channel.
ssh

//start um server by inputting the following command.

gwcuptool.sh -start

//If fails, Upgrade-man checks CORBA naming service and EM server state. /

//Retry after checking.

//configure all options for upgrading the first GWC and creating soak image.

gwcuptool.sh -config -pa “/swd/gwc/” -f pn080ak.imag -m single -p 5 -d VRB
-n “GWC-1” -t 120 -a CRT -an 4

//If fails, check, retry or abort.

```
//print what upgrade-man needs to prepare.  
gwcuptool.sh -prep
```

```
//Pre-check configured GWC  
gwcuptool.sh -precheck  
//If fails, check and retry or abort.
```

```
//Upgrade configured GWC  
gwcuptool.sh -up  
//If fails, check and retry or abort.
```

```
//Post-check configured GWC  
gwcuptool.sh -postcheck  
//If fails, check and retry or abort.
```

```
//Stop um server  
gwcuptool.sh -stop  
//If fails, check and retry or abort.
```

Step 2: Using the soak image to upgrade other GWCs.

Create SSH communication channel.

```
ssh  
//start um server.  
gwcuptool.sh -start  
//If fails, check and retry or abort.
```

```
//Query available GWC. Shell will print out name, ip etc.  
gwcuptool.sh -query -n all
```

```
//Configure all options for upgrading. Pause points are removed for bulk  
//upgrading. Upgrade-man can select GWC list for configuration by above one  
//command.
```

```
gwcuptool.sh -config -pa "/swd/gwc/" -f pn080ak.imag -m bulk -d VRB -n  
'GWC-7,GWC-9,GWC-11' -t 120 -a CRT -an 4  
//If fails, check and retry or abort.
```

```
//Print what upgrade-man needs to prepare.  
gwcuptool.sh -prep
```

```
//Pre-check configured GWC  
gwcuptool.sh -precheck  
//If fails, check and retry or abort.
```

```
//Upgrade configured GWC  
gwcuptool.sh -up
```

```
//If fails, check and retry or abort.

//Upgrade-man can query upgrading state until upgrade completes.
gwcuptool.sh -query
//If fails, check and retry or abort.

//Post-check configured GWC
gwcuptool.sh -postcheck
//If fails, check and retry or abort.

//Stop um server
gwcuptool.sh -stop
//If fails, check and retry or abort.
```

55.10 Appendix 2: An example that how to use scuptool.sh to complete SC upgrade in an office.

Assumption: There are total 8 SC pairs in an office. They are from SC1 to SC8.

Step 1: Upgrade one SC. Pause at all pause points to make upgrade-man has chance to verify.

Create SSH communication channel.

```
ssh
```

//start um server by inputting the following command.

```
scuptool.sh -start
```

//If fails, Upgrade-man checks CORBA naming service and EM server state. Retry after checking.

//configure all options for upgrading the first SC.

```
scuptool.sh -config -pa "/swd/sam21/" -f 11.0.0.0.2222 -m single -p 4 -d VRB  
-n SC1 -t 120 -a CRT -an 4
```

//If fails, check, retry or abort.

//print what upgrade-man needs to prepare.

```
scuptool.sh -prep
```

//Pre-check configured SC

```
scuptool.sh -precheck
```

//If fails, check and retry or abort.

//Upgrade configured SC

```
scuptool.sh -up
```

//If fails, check and retry or abort.

//Post-check configured SC

```
scuptool.sh -postcheck
```

//If fails, check and retry or abort.

```
//Stop um server
scuptool.sh -stop
//If fails, check and retry or abort.
```

Step 2: Bulk upgrading other SCs. No pause point.
Create SSH communication channel.

```
ssh
//start um server.
scuptool.sh -start
//If fails, check and retry or abort.
```

```
//Query SC info.
scuptool.sh -query -n all
```

```
//Configure all options for upgrading.
scuptool.sh -config -pa "/swd/sam21/" -f 11.0.0.0.2222 -m bulk -d VRB -n
'SC1,SC2,SC3' -t 120 -a CRT -an 4
//If fails, check and retry or abort.
```

```
//Print what upgrade-man needs to prepare.
scuptool.sh -prep
```

```
//Pre-check configured SC
scuptool.sh -precheck
//If fails, check and retry or abort.
```

```
//Upgrade configured SC
scuptool.sh -up
//If fails, check and retry or abort.
```

```
//Upgrade-man can query upgrading state until upgrade completes.
scuptool.sh -query
//If fails, check and retry or abort.
```

```
//Post-check configured SC
scuptool.sh -postcheck
//If fails, check and retry or abort.
```

```
//Stop um server
scuptool.sh -stop
//If fails, check and retry or abort.
```

55.11 Appendix 3: Upgrade mode examples in GWC upgrade tool

Here is an example, we can explain the GWC upgrade mode much more clearly.

In the customer office, there are following GWCs:

Audio GWC: GWC-1

Trunk GWC: GWC-12, GWC-13, GWC-14

Line GWC: GWC-5, GWC-6, GWC-7, GWC-8, GWC-9, GWC-10

Based on the “Upgrading the Gateway Controller, NN10196-461”, we need to upgrade Audio GWC first, then Trunk GWCs, and Line GWCs at last.

In the single mode: running with “gwcuptool.sh -config -f NewLoadFileName -m single”

GWCs will be upgraded one by one, and obey the service type order. So the upgrade order will be:

- a. GWC-1 (Audit GWC. apply patch; create soak image for other GWCs)
- b. GWC-12 (Trunk GWC)
- c. GWC-13 (Trunk GWC)
- d. GWC-14 (Trunk GWC)
- e. GWC-5 (Line GWC)
- f. GWC-6 (Line GWC)
- g. GWC-7 (Line GWC)
- h. GWC-8 (Line GWC)
- i. GWC-9 (Line GWC)
- j. GWC-10 (Line GWC)

In the bulk mode: running with “gwcuptool.sh -config -f NewLoadFileName -m bulk”

All GWCs within the same service type will be upgraded at the same time. the upgrade order will be:

- k. GWC-1 (Audit GWC. apply patch; create soak image for other GWCs)
- l. GWC-12, GWC-13, GWC-14 (Trunk GWC)
- m. GWC-5, GWC-6, GWC-7, GWC-8, GWC-9, GWC-10 (Line GWC)

In mix mode: running with “gwcuptool.sh -config -f NewLoadFileName -m mix”

The first GWC node within the same service type group will be upgraded firstly, then all other GWCs in the same group will be upgraded parallel at the same time. The upgrade order will be:

- n. GWC-1 (Audit GWC. apply patch; create soak image for other GWCs)
- o. GWC-12 (Trunk GWC)
- p. GWC-13, GWC-14 (Trunk GWC)
- q. GWC-5 (Line GWC)
- r. GWC-6, GWC-7, GWC-8, GWC-9, GWC-10 (Line GWC)

55.12 Glossary

Table 1

Term	Explanation
CS2M	CS2000 Management Components
SESM	Succession Element Sub-element Manager
SAM21 EM	CS2000 SAM21 Manager
NPM	Network Patch Manager
SSPFS	Succession Server Platform Foundation Software
CLUI	Command line user interface
CLI	Command line interface.
SDM	SuperNode Data Manager

56: A00007196 Functional description (FN)

56.1 Feature name

PacketCable™ Event Messaging For Accounting

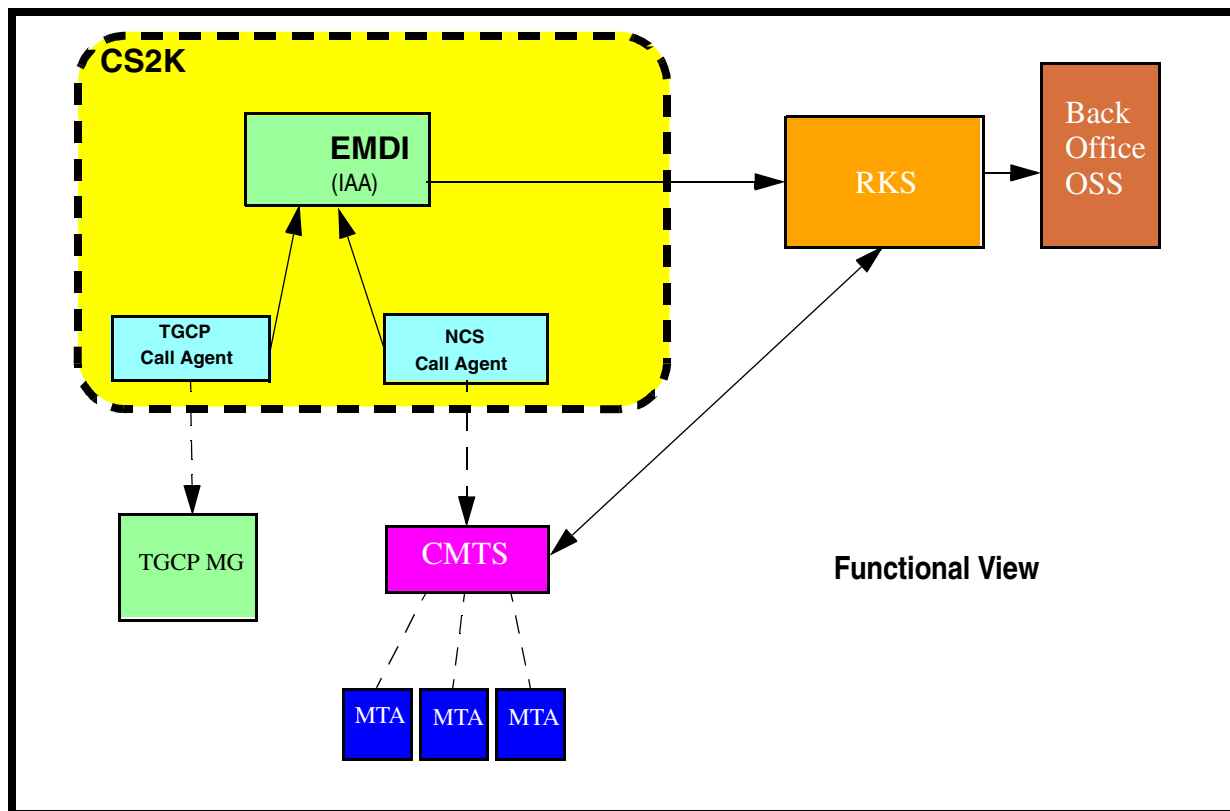
56.2 Description

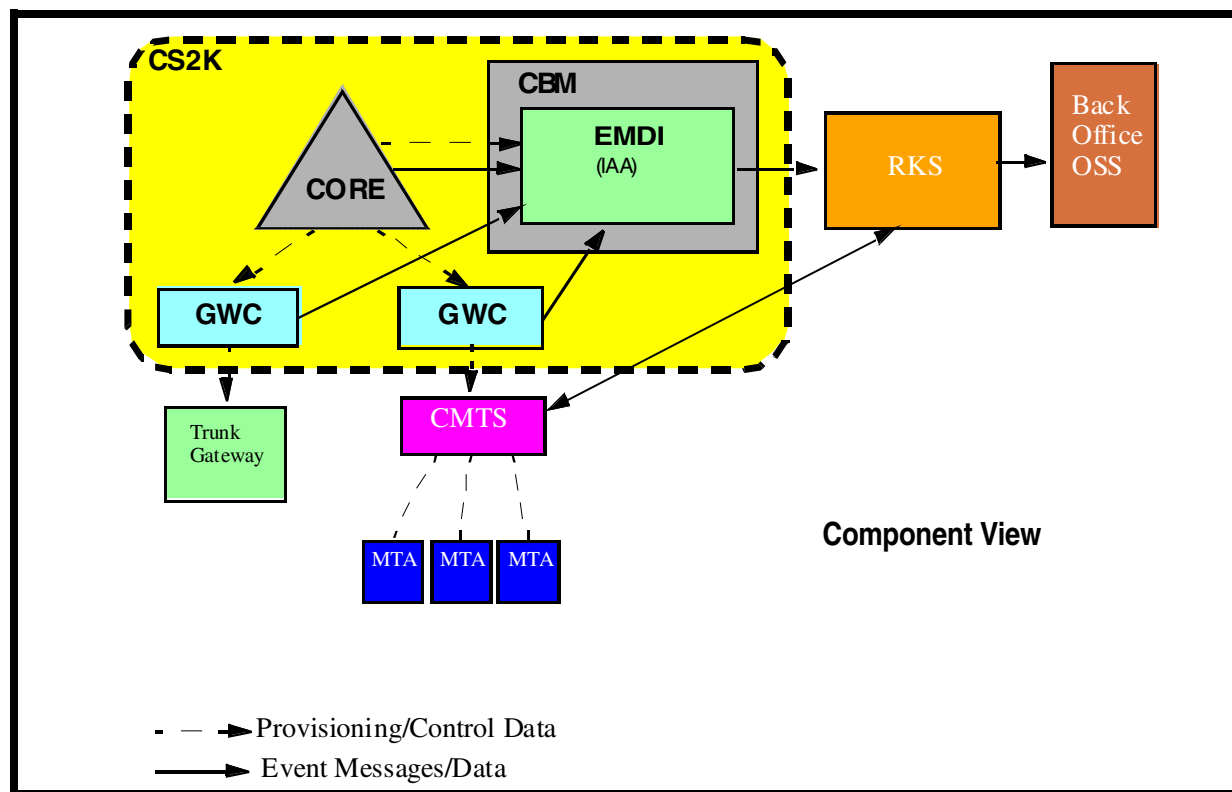
56.2.1 Background

CableLabs is a consortium of cable operators and cable equipment vendors that creates specifications for cable. This work is done under the “PacketCable™” project(www.packetcable.com). The purpose of the PacketCable™ project is to ensure Cable Network Operators’ desired functionality is available and to promote vendor inter-operability. In order to provide a billing capability, PacketCable™ has created a specification for an event reporting mechanism that is called “PacketCable™ Event Messaging” (PCEM). PCEM uses RADIUS accounting (RFC 2866) to deliver event messages to a record keeping server (RKS). This activity provides an implementation of PCEM for the Succession Cable Solution.

This activity provides CMS and MGC PacketCable™ event messaging compliance to the PKT-SP-EM-I10 specification.

56.2.2 Component Architecture





The EMDI (Event Messaging Delivery Interface) encapsulates the capability of formatting event messages with RADIUS headers and sending to the RKS (including retries). For this activity, the EMDI is provided by the IAA (Integrated Accounting Application) on the CBM. The IAA may also receive event messages from the GWC for ES (Electronic Surveillance).

The RKS (Record Keeping Server) is third party equipment provided by any RKS vendor. The RKS receives event messages from the EMDI and the CMTS.

The CMS, or call management server, is PacketCable™'s line solution. Nortel implements the CMS by using functionality in the core, the CBM and small-lines GWCs. The MGC, or media gateway controller (not to be confused with our GWC), is PacketCable™'s trunk solution. Nortel implements the MGC using the core, the CBM and trunk GWCs controlling TGCP MGs.

56.2.3 Event Messages

Event messages are generated at different points in the call and they contain information which can be used for billing purposes. For example: a signaling_start event message contains the calling and called DNs.

Unlike traditional billing systems which generate one billing record when the call is released, packet cable event messaging generates several event messages for each call at various times during the call. Another difference is that event messages are generated for each half call. Generally, each leg of a call consists of two half calls (one for the originator and one for the terminator). Therefore, separate event messages are generated for the originating and terminating call halves.

56.2.3.1 Message Structure

Refer to the Packet Cable specification PKT-SP-EM-I10 for details regarding the individual components in the Packet Cable event messages. Event messages have dynamic lengths. Generally, a message that contains a full 247 byte FEID would have a length of approximately 400 bytes. Typically, FEIDs are shorter than 247 bytes and result in message lengths that average less than 400 bytes.

56.2.3.2 Message Types

Table 2: PacketCable™ Event Messages

Name	Description
Signaling_Start	Start of signaling for originating or terminating half of the call
Signaling_Stop	End of signaling for originating or terminating half of the call
Database_Query	An inquiry into an external database; for example 800, LNP. A TCAP with multiple return values from a single query is not supported.
QoS_Reserve*	Reservation of QoS for originating or terminating half of the call
QoS_Commit*	Commitment of QoS for originating or terminating half of the call
QoS_Release*	Release of QoS for originating or terminating half of the call
Service_Activation	Indicates a subscriber has activated a service
Service_Instance	Indicates an occurrence of a service
Service_Deactivation	Indicates a subscriber has deactivated a service
Call_Answer	Indicates that all network resources have been allocated for originating or terminating half of the call
Media_Alive	Indicates if the call is still active. A media alive event message is generated after an agent (line or trunk) has been active for more than 24 hours. For the report interval and time, PCEM only supports the default value for LONGCALL in table AMAOPTS which is every 24 hours at midnight.
Call_Disconnect	Indicates that all network resources have been released for originating or terminating half of the call

Name	Description
Media_Report	Indicates a change in media session information. ES (Electronic Surveillance) ONLY.
Signal_Instance	Indicates an NCS signal instance. ES(Electronic Surveillance) ONLY.
Interconnect_Start	Start of network interconnect signaling (between PacketCable and PSTN) for originating or terminating half of the call
Interconnect_Stop	Stop of network interconnect signaling (between PacketCable and PSTN) for originating or terminating part of the call
Time_Change	Indicates time change on a network element.

*QOS_XXXX messages are generated by the CMTS and sent directly to the RKS from the CMTS.

56.2.4 Agents Generating Event Messages

PCEM supports the CS2K components that form the packet cable solution. Specifically, PCEM supports event messaging for calls and agents hosted on MTA cable line gateways and trunk agents hosted on TGCP cable gateways.

Agents Types that generate event messages:

- NCS (POTS and RES) Lines (flat rate and measured rate)
- PRI Trunks (PRA)
- ISUP Trunks (IT, ATC, T2, TI, and TO)
- OP MF Trunks
- ES MF Trunks

Agent types that do not generate event messages:

- SIP and SIPT
- Announcements
- Non-NCS line agents

In SN08, the North American, non-IXC, non-Centrex trunk group types (IT, ATC, T2, TI, and TO) are supported.

Typically, tandem trunking is not done in a packet cable solution, however, call forwarding can cause a trunk to trunk call.

56.2.5 Features Generating Event Messages

Table 3: PacketCable EM Spec / CS 2000 Supported EM Features

<i>PKT-SP-EM-I10 Feature Title</i>	<i>Nortel CS2k RES Feature(s)/Notes</i>
Interconnection with circuit-switched PSTN	Various Trunk Agent Call Types
Support for 911 emergency services	911 Routed Calls to PSTN or ES Trunk
n11 (411, 611, etc.) assume outside directory service	Directory Assistance
Toll-free services (800, 888, 877...)	Toll Free Service (TFS on AIN) or E800
Operator services	PSTN or OP Trunk
Call block service	Selective Call Rejection(SCRJ) Anonymous Call Rejection(ACRJ) Subscriber Activated Call Blocking(SACB)
Call waiting service	Call Waiting (CWT) and Cancel Call Waiting (CCW)
Call forwarding/call redirection services	Call Forwarding (CFW/CFDA/CFBL)
Return call service	Automatic Recall (AR)
Repeat call service	Automatic Call Back (ACB)
Voice mail service	Nortel Call Pilot or Non-Nortel using SMDI
Message waiting indicator service (E-mail/voice mail notification)	Message Waiting (MWT)
Three-Way Call	Three Way Call (3WC)
Customer Originated Trace	Customer Originated Trace (COT)

Note: The CS2K supports more features than listed. However, these are the only features contained in the event messaging spec and are therefore the only features that have a defined set of event messages. Activation of event messaging does NOT cause the CS2K to have a diminished feature set.

56.2.6 Configuration and Provisioning

To configure the CS 2000 CMS for event messaging, carry out the following steps in order. Detailed instructions for each step appear in subsequent sections.

1. Configure the PCEM Accounting Stream.
2. Configure the Element-ID.

3. Add a COMMON tuple entry in table PCEMENTT.
4. Add an EMDI tuple entry in table PCEMENTT.
5. Add a Timezone tuple entry in table PCEMENTT.
6. Add RKS tuple entries in table PCEMENTT.
7. Add RKSPAIR tuple entries in table PCEMENTT.
8. Add a Financial Entity ID (FEID) in table PCEMFEID.
9. Configure Network Time Source and UTC Offset.
10. Configure RKSPAIR(s)/FEID on IAA/CBM
11. Online the RKS pairs.
12. Offline RKS pairs, if needed.
13. Activate PCEM.

In addition to the above, refer to the IAA documentation for instructions on configuring the server for event message reception/distribution.

Moreover, consult the FN for activity A00006635 regarding details on provisioning of table LNENDPT. In order for a line to generate event messages, table LNENDPT must contain gateway and endpoint name information for the line.

Furthermore, instructions to change the EMDI and the RKS data in table PCEMENTT are described in this section as well.

56.2.6.1 STEP 1: Configure Accounting Streams

Add PCEM and PCES stream data fill in table CRSFMT.

```
>table crsfmt
>add<key><format><datadump><cdrscrch><alarms><timerdmp><timerval>
```

For example:

```
>add PCEM PCEMFMT N NIL_FM N N 0
>add PCES PCESFMT N NIL_FM N N 0
```

The resulting CRSFMT table will appear similar to the following:

TABLE: CRSFMT						
KEY	FORMAT	DATADUMP	CDRSRCH	ALARMS	TIMERDMP	TIMERVAL
PCEM	PCEMFMT	N NIL_FM	N	N	0	
PCES	PCESFMT	N NIL_FM	N	N	0	

Change the PCEM and PCES stream datafill in table CRSMAP.
 >table crsmap

>replace <key> <stream>

For example:

>replace PCEM PCEM
>replace PCES PCES

The resulting CRSMAP table will appear similar to the following:

TABLE: CRSMAP	
KEY	STREAM
PCES	PCES
PCEM	PCEM

At this point, consult A00007464/A00007465 for additional details regarding the configuration of the PCEM and PCES streams for delivery of event messages to the EMDI/IAA. The streams must be brought INSV after CRSMAP is datafilled. Add the IAA application must be INSV. Refer to the A00007464 FN for the procedures required to bring the streams INSV. In addition, the IAA application must be active in the CBM. For IAA refer to A00007465.

56.2.6.2 STEP 2: Configure Element-ID

The element ID is a number between 0 and 99999 that uniquely identifies the network element within the network. Typically an element ID would be assigned for the CMS and MGC. However, since the CS2K combines the MGC and CMS, a single element ID can be used for the CS2K. The default element ID will be 0 and must be changed to a setting compliant with Packet Cable specifications for each MSO's network.

Set the element ID in table OFCENG:

```
>table OFCENG
>pos Element_ID
>rwok on
>change
PARVAL:0
>12345
TUPLE TO BE CHANGED:
ELEMENT_ID          12345
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
>rwok off
```

In this example, the element has been set to 12345.

56.2.6.3 STEP 3: Add the COMMON tuple entry

The COMMON tuple entry contains configuration for the Accounting Sending Mode, and Accounting Indicator and Electronic Surveillance Indicator flags.

```
> table pcementt
> add common 0 common <accounting sending mode> <accounting
  indicator> <surveillance indicator>.
```

For example:

```
> add common 0 common realtime y y
```

Where **realtime** is the EM delivery mode, **y** means that EM accounting is enabled and **y** means that EM for electronic surveillance is enabled.

- i. <accounting sending mode> can be set to either real-time, batch or ftp (Realtime Mode - Sends event messages to the RKS as they are generated) (Batch Mode- Multiple event messages are batched in a RADIUS message before sending to the RKS) (FTP Mode- Multiple event messages are stored in a file which are sent to the RKS for processing, using FTP as the transport protocol)

Important! See “Changing Accounting Sending Mode” on page 504 for procedures to change the accounting sending mode without data loss.

- ii. <accounting indicator> is set to y if PacketCableTM event messages are desired, n otherwise.

- iii. <surveillance indicator> is set to y if PacketCableTM Electronic Surveillance event messages are desired, n otherwise.

Consult activity A00007548 for information regarding Electronic Surveillance configuration.

56.2.6.4 STEP 4: Add an EMDI Tuple Entry

From the CS2K point of view, the EMDI encapsulates the capability of formatting event messages with RADIUS headers and sending to RKS/DF (including retries).

In the SN08 release, the EMDI capability will be provided by the IAA on the CBM.

```
>table pcementt
>add emdi <index> <entity><ip address><port>
```

For example:

```
>add emdi 0 emdi 1 2 3 4 7109
```

Where the EMDI IP address is 1.2.3.4 and the EMDI port is 7109. In SN08, the IAA default configuration uses port 7109.

The IP address used in this tuple is the IP address of the CBM. For further details, refer to Table 10 in Section 11.5.2.2 of the Configuration document.

56.2.6.5 STEP 5: Add the Timezone tuple entry

```
> table pcementt
> add timezone 0 timezone <DST> <direction> <UTC Offset>.
```

For example:

```
>add timezone 0 timezone y plus 053000
```

Where Y indicates that the office is in Daylight Savings Time (DST).

Note-

The DST indicator values are:

- Y: The local time of the office is currently in Daylight Savings Time.
- N: The local time of the office is currently in Standard Time.

The value used for the UTC offset does not matter since the system will automatically update the UTC offset to the correct value. See Section 2.2.6.9.

56.2.6.6 STEP 6: Add RKS tuple entries

```
>table pcementt
>add rks <index> rks <ip address> <port>
```

For example:

```
>add rks 21 rks 168 24 0 0 1813
```

Where the RKS entry number is 21, the RKS IP Address is 168.24.0.0, and the RKS Port Number is 1813. Repeat for other RKS IP addresses and ports. The index must be a unique value(i.e, no RKS already assigned for that index) between 0 and 31. A maximum of 32 RKS entries may be added.

Typically, an RKS uses a port number of 1813. However, this must be confirmed with the RKS vendor in order to properly data fill RKS tuples in table PCEMENTT.

56.2.6.7 STEP 7: Add RKSPAIR tuple entries

Provision RKS pair(s).

If more than one RKS pair is provisioned, event messages will be evenly distributed across the set of online RKS pairs in a round-robin fashion. All event messages for a given BCID (Billing Correlation ID) will be sent to the same RKS pair.

```
> table pcementt.
> add rkspair # rkspair <primary rks> <secondary rks> <associated emdi>
```

For example:

```
> add rkspair 0 rkspair 21 31 0
```

Where 21 and 31 are RKS entries and 0 is an EMDI entry in table PCEMENTT.

The index must be a unique value(i.e., no RKSPAIR already assigned for that index) between 0 and 15. A maximum of 16 RKSPAIR entries may be added.

The associated EMDI identifies the “EMDI” (Refer to section 2.2.6.5) that this RKSPAIR expects to receive event messages from.

If desired, both the primary RKS and the secondary RKS can reference the same RKS entry. This allows for support of high-availability RKS systems that present only a single IP address and port for both units.

56.2.6.8 STEP 8: Configure Financial Entity ID (FEID)

```
>table pcemfeid
>add <msodef> <msodmn> [<msodmsn> <msodmn><msodmn>]
```

For example:

```
>add 0 12345678 'test.feid' $
```

Where 12345678 is the MSO defined data, and the MSO domain name is test.feid. The MSO domain name may be up to 239 characters. Refer to Section 11.5.2.1 of Configuration document for further details.

56.2.6.9 STEP 9: Configure Network Time Source and UTC Offset

The network time source is a NTP server which can be configured from the succession SAM21 element manager where the 3PC call agent is installed. Its UTC offset is based on the timezone the Linux OS is set to use.

Here are steps about how to configure a NTP server to use for 3PC.

1. Start the SAM21 element manager from web.
2. Under Configuration pull down menu, select adding or modifying the SAM21 element manager for the lab.
3. Enter the primary and secondary NTP servers' IP addresses in Primary NTP and Secondary NTP fields.
4. Save the changes.
5. Lock and unlock all SAM21 cards for the NTP server address change to take effect.

The steps to configure a timezone to use under Linux OS where 3PC application is running must be performed on all 3PC blades. The steps that must be performed on each 3PC blade are:

1. telnet to the 3PC call agent IP address which can be found from the SAM21element manager where the card is provisioned.
2. login as a root user.
3. cd to directory: /usr/sbin.
4. Run tzconfig and then following the directions to set it.

The system will use the timezone information to set the UTC in table PCEMENTT automatically.

After using tzconfig changed time zone, the last step is to check timezone tuple in PCEMENTT table to make sure the DST flag (Y/N) is set correctly. If not, the appropriate change needs to be made. The UTC OFFSET in the tuple will be adjusted automatically with the DST flag.

When the DST flag is changed from Y/N to N/Y in table PCEMENTT, the UTC OFFSET will be adjusted automatically by one hour in that tuple. But there is no event message reported in this case since the local system time is not changed.

Another thing to notice is that when changing time zone, it may take several steps for the underline OS to adjust the local time to the correct one, in some cases, the local time may be adjusted to GMT time first and then back to the time zone requested. In this case, there will be 2 event messages generated since the local system time is changed twice. Some times, it even takes more then 2 steps to adjust the time zone. So when checking event messages during the process, care needs to be taken because it may have more than one event messages spilled out. The event message system reports all the time adjustment notified by 3PC during this process. And the time will be synchronized automatically with NTP server.

56.2.6.10 STEP 10: Configure RKSPAIR(s)/FEID on IAA/

CBM

For full details regarding IAA configuration, please refer to the IAA documents directly (Activity A00007465).

The core is capable of distributing event messages in round robin fashion over the online RKS pairs. Each RKS pair consists of a PRIMARY and a SECONDARY RKS. Please note, it is acceptable to configure the PRIMARY and SECONDARY RKS of an RKS pair to be the same RKS.

As each RKS pair is added to table PCEMENTT, the CS2K core will assign a “channel ID” to the RKS pair. These channel IDs are used in communications between the CS2K and the IAA application as a means of uniquely identifying RKS pairs. Please note, the channel ID is not the same as the RKSPAIR index in table PCEMENTT.

When configuring the IAA, the channel IDs (as assigned by the CS2k core) must be assigned to the RKS pairs in the IAA. In order to obtain the channel ID information for use when configuring the IAA, use the PCEMCI tool on the CS2k as follows:

```
>pcemci
> cidmap
```

The output will appear similar to:

```
Collector   Channel ID
-----
RKSPAIR 0 -> 1
```

In this example, channel ID 1 has been assigned to RKS pair 0.

At this point, you may telnet to the CBM and invoke the `iaa_config_cli` tool to begin adding output destinations (RKS Pairs). Refer to the A00007464 documentation for full details. The following is a brief example of configuring an output destination on the IAA/CBM. At the time this document was written, the provisioning was only possible via the `iaa_config_cli`. However, the IAA application is anticipate to provide a web server interface for configuration. Refer to A00007465 for the latest information regarding the web configuration gui.

Telnet to the CBM maintenance interface. At the prompt, enter “`iaa_config_cli`”.

For example:
maint: iaa_config_cli

This will display the IAA config “Main” menu:

```
Status: None
=====
=
Main Menu           Page 1 of 1
=====
==
```

1. Global Parameters
2. Output Destinations

```
=====
==
[S]ave    e[X]it    [N]extPage    [P]revPage    [Q]uit
```

Select:

Enter 2 to select “Output Destinations” this will display the “Output Destinations” menu:

Status: None

```
=====
==
                                Output Destinations                                Page 1 of 1
=====
==
```

1. Delivery Function Destinations
2. Record Keeping Server Destinations

```
=====
=
[S]ave    [R]eturn    [N]extPage    [P]revPage    [Q]uit
```

Select:

Select option 2 for “Record Keeping Server Destinations” this will display the RKS destinations menu:

Status: None

```
=====
==
                                Record Keeping Server Destinations                                Page 1 of 1
=====
==
```

1. List
2. New
3. Copy
4. Edit
5. View
6. Delete

```
=====
==
[S]ave    [R]eturn    [N]extPage    [P]revPage    [Q]uit
```

Select:

From this menu select option 2 “New” to display the “RKS Destination Parameter” menu:

Status: None

```
=====
==
RKS Destination Parameters                Page 1 of 3
=====
==
1. Channel ID                [ ]
2. Description                [ ]
3. Primary IP Address        [ ]
4. Primary RADIUS Port       [ ]
5. Secondary IP Address      [ ]
6. Secondary RADIUS Port     [ ]
7. Retry Limit               [3]
8. Retry Interval            [3]
9. Shared Secret             [0000000000000000]
10. Batch Interval           [3]
11. Messages In Batch        [5]
=====
==
[A]dd    [R]eturn  [N]extPage  [P]revPage  [Q]uit
```

Select:

Select each field and enter the appropriate information for the primary and secondary RKS for this RKS pair. Although not required, a suggested value for the description field would be the RKS pair index from table PCEMENTT on the CS2k core. For example “RKSPAIR 0”.

Be sure to enter the Channel ID (use the channel ID provided by the PCEMCI>CIDMAP command on the CS2K core for this RKS pair).

There are several pages of information that must be entered for each RKS destination. Please refer to the A00007464 documents for details.

When all data has been entered, select option “A” to add the new RKS pair data in the IAA.

After adding the RKS pair to the IAA, you can list the RKS destination from the “RKS Server Destinations” menu as follows:

Status: None

```
=====
=
Record Keeping Server Destinations        Page 1 of 1
=====
=
1. List
2. New
3. Copy
4. Edit
5. View
```

6. Delete

```
=====
==
[S]ave   [R]eturn  [N]extPage  [P]revPage  [Q]uit
```

Select:

Select option 1 to list the Channel IDs and RKS destinations configured in the IAA:

```
=====
==
                Record Keeping Server Destinations List
=====
==
    Ch ID  Description
=====
1.   1    RKSPAIR 0
```

Hit Enter to Return

In addition to the RKS destination information, various “Global” parameters must be configured on the IAA, To do this, select option 1 “Global Parameters” from the IAA config “Main” menu. The global parameters menu will be displayed:

Status: None

```
=====
==
                Global Parameters                Page 1 of 1
=====
==
1. Element ID                [99887]
2. Packet Cable Format Version [1]
3. Enable Daylight Saving    [1]
4. UTC Offset                [-050000]
5. Sending Mode              [0]
* 6. Base EM File Path        [/cbmdata/00/iaa/ftpout/]
7. EM File Path              [stockroom]
```

Note: * Fields are not Editable

```
=====
==
[S]ave   [R]eturn  [N]extPage  [P]revPage  [Q]uit
```

Select:

Select each of the fields and enter the data. Be sure to enter the element ID (as configured on the CS2K in STEP 2 of this procedure). When all data has been entered, save the changes (option s)

Once all of the RKS pairs and Global Parameters have been added in the IAA, proceed to the next step “Online the RKS pairs”.

56.2.6.11 STEP 11: Online the RKS pairs

RKS pairs must be online to be included in the set of RKS(s) that the CMS will use as destinations when sending event messages. The event messages will be distributed over the set of online RKS pairs in round-robin fashion.

To enable an RKSPAIR to receive accounting event messages, set the RKSPAIR status to ONLINE:

```
>pcemci
> rkspair <desired pair #> online
```

For example:

```
> rkspair 0 online
```

where 0 is an RKSPAIR entry in table PCEMENTT.

56.2.6.12 STEP 12: Offline RKS pairs, if needed

RKS pairs must be online to be included in the set of RKS(s) that the CMS will use as destinations when sending event messages. The event messages will be distributed over the set of online RKS pairs in round-robin fashion.

If an RKSPAIR must be removed from the round-robin selection for delivery of event messages, set the RKSPAIR to offline as follows:

```
>pcemci
> rkspair <desired pair #> offline
```

For example:

```
>rkspair 0 offline
```

Offlining an RKS pair will prevent the RKS pair from being selected as a destination for EM delivery for new calls. Already existing calls queued against a particular RKS pair will continue using the RKS pair until the current call has concluded.

56.2.6.13 STEP 13: Activate PCEM

Activating PCEM with Accounting active in table PCEMENTT will cause event message generation for all lines and trunks in the CS2K.

```
>table ofceng
>pos pcem_is_active
>rwok on
>change
PARMVAL:N
```

```

>Y
TUPLE TO BE CHANGED:
  PCEM_IS_ACTIVE          Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
>rwok off

```

All of the previous step must be done prior to activation of PCEM or an error message will be generated. See Section 11.3.2.1 in the Configuration document for details.

56.2.6.14 Changing EMDI tuple in table PCEMENTT

The following ordered steps **MUST** be followed **before** changing the EMDI IP address in table PCEMENTT:

1. Stop the IAA application in the CBM. (See Note below.)
2. Perform the EMDI IP address/port change in the IAA.
3. Start the IAA application in the CBM. (See Note below.)

Note: The SDM Application Manager (SAM) controls the starting and stopping of the IAA. (See FN Sections 2.2.3 and 2.2.4 of A00007465.) While the IAA application is stopped, the Accounting Event Messages from the CORE are saved in the PCEM SBA stream.

After the above ordered steps, change the EMDI IP address in table PCEMENTT.¹

56.2.6.15 Changing RKS data in table PCEMENTT

To change an RKS IP address/port.

1. Perform the RKS IP address/port change in the IAA application in the CBM. Use the RKS Output Destination (RKSOD) GUI as described in Configuration Section 12.4.2.1 of A00007465.
2. Change the RKS tuple with the new IP address/port in table PCEMENTT in the CORE. Between steps (1) and (2), QoS_Commit and QoS_Release messages for existing calls in the GWCs will be sent to the old RKS IP address.

56.2.6.16 Changing Accounting Sending Mode

If at any point after your system is operational and sending accounting event messages you should decide to change the accounting sending mode, it is very important that you follow the procedures in this section to avoid data loss.

¹Event messages from the GWCs will be lost until after the EMDI IP address/port has been changed in the CORE. This is because the GWCs are only notified of the new EMDI data when the EMDI tuple in table PCEMENTT is changed in the CORE.

Table 4: Changes to Accounting Sending Mode

Current Setting	Desired Setting	Procedure
realtime	batch	1
realtime	ftp	2
batch	realtime	1
batch	ftp	2
ftp	realtime	3
ftp	batch	3

Procedure 1: Changing between realtime and batch modes

1. First change the IAA application to the desired mode.
2. Next change the common tuple in CORE table pcementt to the desired mode.

Procedure 2: Changing from realtime or batch modes to ftp mode

1. First change the IAA application to ftp mode.
2. Next change the common tuple in CORE table pcementt to ftp mode.

Procedure 3: Changing from ftp mode to realtime or batch modes

1. First change the common tuple in CORE table pcementt to the desired mode.
2. Next change the IAA application to the desired mode.

56.2.7 PCEM Operational Measurements (OMs)

In SN08, a new OM group “PCEM” is introduced. It pegs a success or failure for every event message generated by the core for Accounting (CMTS generated event messages are not pegged). Also please note, OM counts are not incremented for event messages generated for Electronic Surveillance.

Note: This OM group pegs success and failure based on the core (i.e. it does not peg failures for messages that fail to arrive at the RKS after leaving the core).

The register names and definitions are shown in the table below.

Table 5: PCEM OM Group Register Definitions

<i>PCEM Register Name</i>	<i>Definition</i>
EMSENT	Event message successfully generated
EMFAIL	Failed to build event message.
EMSYSFL	System unable to send event message.
EMSENT2	Extension register for EMSENT
EMFAIL2	Extension register for EMFAIL
EMSYSFL2	Extension register for EMSYSFL

The current PCEM OM register counts may be displayed using the OMSHOW CI command as follows:

```
>omshow pcem active
PCEM
CLASS: ACTIVE
START:2004/12/03 11:30:00 FRI; STOP: 2004/12/03 11:47:28 FRI;
SLOWSAMPLES: 11 ; FASTSAMPLES: 105 ;
KEY (EVENT_MESSAGE_TYPE)
    EMSENT  EMFAIL  EMSYSFL  EMSENT2
    EMFAIL2  EMSYSFL2
1 SIGNALING_START
    0      0      0      0
    0      0
2 SIGNALING_STOP
    0      0      0      0
    0      0
3 DATABASE_QUERY
    0      0      0      0
    0      0
6 SERVICE_INSTANCE
    0      0      0      0
```

0	0		
9 SERVICE_ACTIVATION			
0	0	0	0
0	0		
10 SERVICE_DEACTIVATION			
0	0	0	0
0	0		
12 SIGNAL_INSTANCE			
0	0	0	0
0	0		
13 INTERCONNECT_START			
0	0	0	0
0	0		
14 INTERCONNECT_STOP			
0	0	0	0
0	0		
15 CALL_ANSWER			
0	0	0	0
0	0		
16 CALL_DISCONNECT			
0	0	0	0
0	0		
17 TIME_CHANGE			
0	0	0	0
0	0		
20 MEDIA_ALIVE			
0	0	0	0
0	0		

Refer to OM system configuration NTPs for details regarding register holding and transfer periods (NTP 297-9051-8551).

56.3 Hardware Requirements or Dependencies

Table 6: Packet Cable CS2K PCEM Hardware Dependencies

Device	Baseline Hardware
GWC	SN08 Baseline
CS2K Core	3PC SN08 Baseline
CS2M	SN08 Baseline
CBM/SBA/IAA	SN08 Baseline
CMTS	*compliant to PKT-SP-DQOS-I10-040721 & PKT-SP-EM-I10-040721
RKS	*compliant to PKT-SP-EM-I10-040721
DF (only required for electronic surveillance)	*compliant to PKT-SP-EM-I10-040721 and corresponding PacketCable electronic surveillance specification
TGCP MG	*compliant to PKT-SP-EM-I10-040721 and PKT-SP-TGCP-I08-040721
NCS GW (eMTA)	*compliant to PKT-SP-MGCP-I10-040402

* Contact Nortel Networks for inter operability testing results.

56.4 Software Requirements or Dependencies

In order to support the generation of event messages, the various network elements must contain at least the following baseline software.

Table 7: Network Element Software Baselines For PCEM

Device	Baseline PCEM Software Load
GWC	SN08 Load Lineup
CS2K Core(3PC)	SN08 Load Lineup
CS2M	SN08 Load Lineup
Telesciences IAA	SN08 Load Lineup
CBM/SBA	SN08 Load Lineup
CMTS	*compliant to PKT-SP-DQOS-I10-040721 & PKT-SP-EM-I10-040721
RKS	*compliant to PKT-SP-EM-I10-040721

Table 7: Network Element Software Baselines For PCEM

Device	Baseline PCEM Software Load
DF (only required for electronic surveillance)	*compliant to PKT-SP-EM-I10-040721 and corresponding PacketCable electronic surveillance specification
TGCP MG	*compliant to PKT-SP-EM-I10-040721 and PKT-SP-TGCP-I08-040721
NCS GW (eMTA)	*compliant to PKT-SP-MGCP-I10-040402

* Contact Nortel Networks for inter operability testing results.

56.5 Limitations and restrictions

56.5.1 Core ONP/SWACT/Upgrade Maintenance Behavior

Table 8: ONP/SWACT Accounting EM Behavior

MTC Action	Stable Calls (i.e., answered)	Unstable Calls
No Restart SWACT	Calls Remain Active, but the following EMs are prematurely generated ^a : - Call Disconnect, - Interconnect Signaling Stop (for trunks), and - Signaling Stop	Calls Remain Active, but the following EMs are prematurely generated: - Interconnect Signaling Stop (for trunks), and - Signaling Stop
Warm Restart	Calls Remain Active, accounting EMs continue to generate after Restart	Calls Released, the following EMs are generated when the calls are released after the restart: - Interconnect Signaling Stop (for trunks), and - Signaling Stop
Cold Restart	Calls Released, No Further Event messages. Unmatched signaling start and signaling stop possible.	Calls Released, No Further Event messages. Unmatched signaling start and signaling stop possible.

Table 8: ONP/SWACT Accounting EM Behavior

MTC Action	Stable Calls (i.e., answered)	Unstable Calls
Reload Restart	Calls Released, No Further Event messages. Unmatched signaling start and signaling stop possible.	Calls Released, No Further Event messages. Unmatched signaling start and signaling stop possible.

a. Similar behavior as with premature billing records.

56.5.2 GWC SWACT/Upgrade Maintenance Behavior

In general, the CS2K will continue to generate accounting event messages for calls that survive GWC warm swact.

Table 9: GWC Maintenance Behavior

MTC Action	Stable Calls	Unstable Calls
Warm SWACT	Survives SWACT, accounting EMs continue to be generated normally after the SWACT	Call Released, EMs generated at release.
Cold SWACT	Call Released, EMs generated for end of call (GWC generated EMs[i.e. PCES media report] will not be generated at the end of the call)	Call Released, EMs generated for end of call.(GWC generated EMs[i.e. PCES media report] will not be generated at the end of the call)
Reload (Lock/Unlock, assumes both units locked)	Call Released, EMs generated for end of call. (GWC generated EMs[i.e. PCES media report] will not be generated at the end of the call)	Call Released, EMs generated for end of call.(GWC generated EMs[i.e. PCES media report] will not be generated at the end of the call)
GWC Shelf Power Cycle	Call Released, EMs generated for end of call. (GWC generated EMs[i.e. PCES media report] will not be generated at the end of the call)	Call Released, EMs generated for end of call.(GWC generated EMs[i.e. PCES media report] will not be generated at the end of the call)

56.5.3 CBM Failure

In the event of CBM failure, the SBA subsystem will queue accounting event messages for later delivery to the CBM. Refer to “SBA Packet Cable Event Messaging” activity A00007464 for further details.

56.5.4 RKS Failure

In the event of an RKS failure, the IAA will store accounting event messages for up to seven days or until the RKS becomes available at which time the accounting message information will be delivered to the RKS. Refer to IAA and CBM documentation for further details. This will utilize the IAA FTP delivery mechanism to the RKS.

56.5.5 BHCA Capacity

Refer to the IAA/CBM documentation (A00007464) for the call capacity limitations.

56.5.6 XA Core Platform Not Supported

PCEM for SN08 is only supported on the 3PC CS2K platform. XA Core is not supported.

56.5.7 IBN and MBS Lines

PCEM supports RES and POTS line types in SN08. IBN lines and MBS (Meridian Business Set) lines are not supported.

56.5.8 CS2K Trunk Variants

In SN08, only the North American, non-IXC, non-Centrex trunk variants will be supported. This includes OP, ES, PRA, IT, ATC, T2, TI, and TO.

56.5.9 SIP-T Trunks

SIP and SIP-T trunks do not generate event messages for their call half since they may be used for inter-CMS/MGC calls. However, the exchange of the FEID and Related BCID is not supported by SIP or SIP-T.

56.5.10 Media_Alive Event Message

Generation of the Media_Alive event message is supported. If an agent (line or trunk) is active on an answered call for more than 24 hours, a Media_Alive event message will be generated for each half call. However, for the report time and interval, PCEM only supports the default value for LONGCALL in table AMAOPTS which is every 24 hours at midnight.

56.5.11 Trunk Endpoint Names

MGC trunk agents do not support endpoint names. Therefore, the signaling_start event message will not contain the mta_endpoint_name attribute.

56.5.12 Off-net to Off-net Call Forwarding

If an off-net call comes in over an ISUP trunk to a line which is call forwarded to an off-net destination via an ISUP trunk, the Interconnect_Start event message will not be generated until answer.

56.5.13 Database_Query Multiple Return Values

The Database_Query event message does not support a TCAP response that contains multiple returned numbers from a single query.

56.5.14 SACB Service_Instance Event

When the SACB feature is active and the subscriber dials a blocked number, a Service_Instance event message is generated with a service name of Call_Block. The Service_Instance event message is generated even if SACB prompts for a PIN and the user overrides the blocking by dialing the correct PIN.

56.5.15 PCEM and PCES on DIRP

PCEM and PCES on DIRP are not supported. Hence, PCEM and PCES are not required to be datafilled in any of the DIRP tables.

56.6 Interactions

PCEM accounting does not require AMA to be present in the office.

PCEM accounting is independent of PacketCable Electronic Surveillance (i.e. you can run PCES with or without PCEM accounting and you can run PCEM accounting with or without PCES).

56.7 Glossary

TERM	Description
ACB	Automatic Call Back
ACRJ	Anonymous Call Rejection
AIN	Advanced Intelligent Network
AMA	Automated Message Accounting
AR	Automatic Recall
Batch Mode	Multiple Event Messages are batched in a single RADIUS message before sending to RKS

TERM	Description
BCID	Billing Correlation ID
BHCA	Busy Hour Call Attempts
CFW	Call Forward
CMS	Call Management Server - refers to GWC/CS2K for lines
CMSS	Call Management Server Signaling
CMTS	Cable Modem Termination System
COT	Customer Originated Trace
CW	Certification Wave
DF	Delivery Function
DIRP	Device Independent Recording Package
DST	Daylight Saving Time
EMDI	Event Messaging Delivery Interface
eMTA	Embedded Multimedia Terminal Adapter (NCS line gateway)
FCM	Fabric Control Message
FEID	Financial Entity ID
FTP Mode	File Transfer Protocol Mode: Multiple event messages are stored in a file which are sent to the RKS for processing, using FTP as the transport protocol.
GWC	Gateway Controller
IAA	Integrated Accounting Application
LI	Lawful Intercept
LNP	Local Number Portability
MGC	Media Gateway Controller - refers to GWC/CS2K for trunks
MTA	Multimedia Terminal Adapter (NCS line gateway)
OM	Operational Measurement
ONP	One Night Process (Procedure followed on office upgrade)

TERM	Description
PCEM	Packet Cable Event Messaging
PCES	Packet Cable Electronic Surveillance - packet cable LI
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
Real-time Mode	Event Messages are sent to RKS as they are generated.
RFC	Request For Change
RKS	Record Keeping Server
RTP	Real-time Transport Protocol
SACB	Subscriber Activated Call Blocking
SCP	Service Control Point
SCRJ	Selective Call Rejection
SMDI	Simple Message Desk Interface
SS7	Signaling System Number 7
SWACT	Switch of Activity (From active to standby unit)
TCAP	Transactions Capability Application Part
TCP	Transmission Control Protocol
TGCP	Trunk Gateway Control Protocol
UDP	User Datagram Protocol
UTC	Universal Time Coordinated

57: A00007213 Functional description (FN)

57.1 Feature name

MG9000 5/30 Minutes OMs

57.2 Description

This feature consists of following deliverable.

1. This feature allows the user to configure Sample interval and Summary intervals on SN08 MG9K from MG9KEM. This configuration is supported through a new configuration GUI "Configure Collection Interval", which will be introduced under the submenu option MG9KEM Subnet view ->Performance. All the MG9Ks in a Subnet are configured with same intervals.

In SN08, user is allowed to select following combinations of Sample and Summary intervals from GUI.

- Sample and Summary intervals of 5 and 30 minutes respectively.
- Sample interval of 15 minutes and no Summary interval.

In the new configuration GUI, Sample and Summary intervals are specified in terms of minutes.

Example: For the Sample and Summary intervals of 5 and 30 minutes, user has to select the value "5/30 minutes" in the GUI. For the 15 minutes Sample interval, user has to select the value "15 minutes" in the GUI.

2. Whenever Collection intervals are changed, Performance browser and OM Collector behave as follows.
 - OM Collector will start collecting OMs at new collection intervals, starting from next collection interval.
 - After Collection interval is changed, if User tries to collect performance data, Performance browser will collect OMs at new Sample collection interval.

Refer to the limitation mentioned in section 2.5.

3. Following changes are done in Performance browser.
 - The intervals shown in Performance browser are based on the Sample interval. That means, intervals shown in the fields "From" and "To" of Performance browser are based on Sample interval.

Note that, Only Sample intervals are shown on Performance browser. 96 intervals are shown irrespective of sample interval value.

4. OM Collector generates CSV files named with appropriate tag to indicate the collection interval of the OM data, which is stored in CSV file. To be inline with the tag used today for 15 minutes interval, following tags will be used for new intervals in SN08.

For 5 minutes interval: 5_MIN_TRAFFIC

For 30 minutes interval: 30_MIN_TRAFFIC

CSV filename convention:

<NEType>.<NodeName>.OMs.<ReportName>.<Year>.<Month>.<Day>_<Hour>.<Minute>_<TimeZone>.<fileextension>

Example CSV file names:

- MG9000.CO18.OMs.5_MIN_TRAFFIC.2003.06.06_13.15_EDT.csv
 - MG9000.CO18.OMs.15_MIN_TRAFFIC.2003.06.06_13.15_EDT.csv
 - MG9000.CO18.OMs.30_MIN_TRAFFIC.2003.06.06_13.15_EDT.csv
5. Once CSV file is generated successfully, OM Collector sends CORBA notification with following information.
 - Source IP address (IP address of the EM workstation, where CSV file is available. In a HA system, this is the Virtual IP address).
 - CSV filename with complete path
 - NE IP address (IP address of the NE for which the CSV file is generated)
 6. When OMs are not available, reason for the same would be available in the SFTP response. When OMs are not available, OM Collector will raise a minor alarm. OM Collector will try to extract the reason from SFTP response and will put the same in appropriate field/s of the alarm. OM Collector also logs these alarms in Customer log. OM Collector will clear the alarm when OMs are available again.
 7. OM Collector is integrated with MG9KEM as detailed below
 - Configuration of OM Collector will be integrated with that of MG9KEM server.
 - OM Collector will be started and stopped along with MG9KEM server.

Even though OM Collector is brought inside MG9KEM, OM Collector is retained as a separate JAR and is delivered as a separate package.

57.3 Hardware Requirements or Dependencies

None

57.4 Software Requirements or Dependencies

This feature depends on A00007107 (MG9K feature to support 5/30 minutes).
This feature requires A00007107 at least by the time of its Integration testing.

With reference to the requirement #5 mentioned in [1], this feature sends a notification. The IEMS feature A00007388 (MG9K Performance integration). uses this notification. Hence, IEMS feature A00007388 depends on the delivery of A00007213.

57.5 Limitations and restrictions

When MG9KEM changes Collection interval, any data collected by OM Collector and/or Performance browser till the end of current collection interval after MG9KEM changes collection intervals, may not be accurate. Following paragraphs explains the reason for this.

Example #1:

Let us consider that, MG9KEM changes the collection intervals say from 15 to 5/30 minutes, at 9:06 AM. In this scenario, MG9KEM and OM Collector will switch over starting from next collection interval time as explained below.

- OM Collector will collect new Sample interval (i.e, 5 min in this example) starting from 9:10 AM and Summary interval starting from 9:30 AM.
- Performance browser will changeover immediately. i.e, it will show Collection time period in terms of new Sample collection interval.

However, MG9K changes over to new collection interval at end of current collection interval (i.e., at 9:15 AM in the scenario explained above). Also, MG9K flushes its history performance data at 9:15 AM.

Because of this behavior difference between MG9K and MG9KEM PM components (i.e., performance browser and OM Collector), any data collected by OM Collector and/or Performance browser till and including 9:15 AM, may not be accurate.

Example #2:

Let us consider that, MG9KEM changes the collection intervals say from 5/30 to 15 minutes, at 9:06 AM. In this scenario, MG9KEM and OM Collector will switch over starting from next collection interval time as explained below.

- OM Collector will collect new Sample interval (i.e, 15 min in this example) starting from 9:15 AM.

- Performance browser will changeover immediately. i.e, it will show Collection time period in terms of new Sample collection interval.

However, MG9K changes over to new collection interval at end of current collection interval (i.e., at 9:10 AM in the scenario explained above). Also, MG9K flushes its history performance data at 9:10 AM.

Because of this behavior difference between MG9K and MG9KEM PM components (i.e., performance browser and OM Collector), any data collected by OM Collector and/or Performance browser till and including 9:15 AM, may not be accurate.

57.6 Interactions

This feature interacts with the SN07 feature, A00003531 (MG9KEM - Frame location enhancements) as follows;

- The SN07 feature A00003531 replaces Internal frame number by Office frame number in the CSV files for 15 minutes interval. This capability is utilized in SN08 for the new intervals 5 and 30 minutes also.
- This feature uses the capability introduced by A00003531 to either enable or disable OM data collection for a particular MG9K.

57.7 Glossary

Term	Description
Collection interval or interval	Time interval for which MG9K either periodically or upon request from application such as OMC, generates performance data.
Collection time period	This is the time period shown in Performance browser. User is allowed to select one or more collection intervals from this time period and can request to collect history data for those many number of past intervals. Based on the Sample collection interval, Collection intervals are shown within this time period.
EM	Element Manager
Internal (logical) frame number	Frame number, which is unique within a MG9K
MG9K	Media Gateway 9000

Term	Description
MIB	Management Information Block. RFC-driven MIBs are standard MIBs defined in RFC. Enterprise MIB is one written by Nortel.
Office (External) frame number	Frame number, which is unique within an office
OM	Operational Measurement
OMC	OM Collector
Performance Browser	It is a component of MG9K EM. It collects performance data (both previous and current) from MG9K through SNMP interface and shows them in tabular format.
PV	Product Verification
Sample Interval	The interval which the MG collects and stores OM information in its MIBs. Interval to be 5 or 15 minutes
Summary Interval	An aggregation of sample intervals calculated at the MG. This interval is expected to be 30 (6x5) or 1.

57.8 Recommended Reading/References

[1] A00007213_5_30_MINUTE_OM_DID.fm Version 1.0

[2] A00007107_OMs_5_30.doc Version 1.0

58: A00007232 Functional description (FN)

58.1 Feature name

T.38 Support for Gatekeeper - Gatekeeper Configurations

58.2 Description

58.2.1 Overview

This SN08 feature provides the ability to support T.38 fax calls to/from endpoints residing on H.323 gateways within carrier and enterprise networks where gatekeepers communicate via ACME SD signaling proxy.

The ACME SD proxy acts as a H.323 gateway and relays H.323 signalling between the Gatekeepers. Both RAS and RAS-less procedures are supported. On CS2K side, GK-routed call signaling applies.

This feature provides T.38 fax interworking between Nortel and other vendor Communication Servers / Gatekeepers:

- CS2K
- CS1000/M
- MCS 5200 connected to CS2K via SIP
- Cisco 3600/3700, Cisco 7200

This feature provides T.38 fax interworking between H.323 gateways and non-H.323 gateways:

- H.323 GWs:
CS1000/M, Westell iQ 2030, BCM, Cisco IOS 2600/3600/3700, Model 50
- H.248 GWs:
PVG 15k with VSP3/VSP3-O card
- MGCP GWs:
Mediatrix IAD 1104

An example of VoIP Network model with signaling flow and media flow is given in chapter 2.2.2. Chapter 2.2.4 specifies the supported and verified interworking over H.323 Proxy (ACME SD box) in detail.

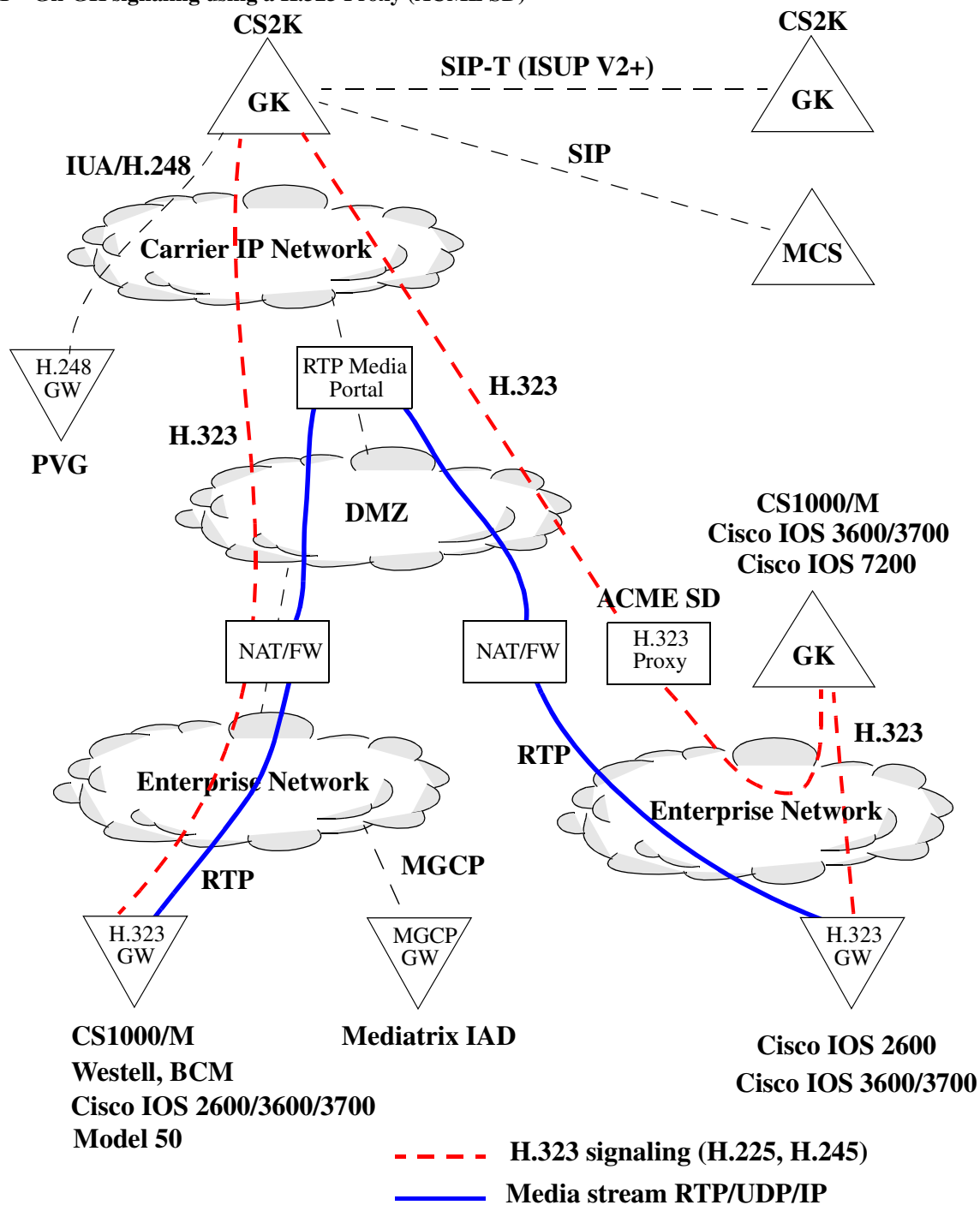
This feature supports T.38 fax calls over H.323 Proxy for International and NA CS2K load. Feature validation for International CS2K load is part of this activity. Feature validation for NA CS2K load is done by a separate activity (tbd).

This feature is based on ITU-T T.30 [1], T.38 [2, 3], H.323 [4], H.225 [5], H.245 [6] and on SN07 features A00002550 [10] and A00003627 [11].

58.2.2 VoIP Network Model

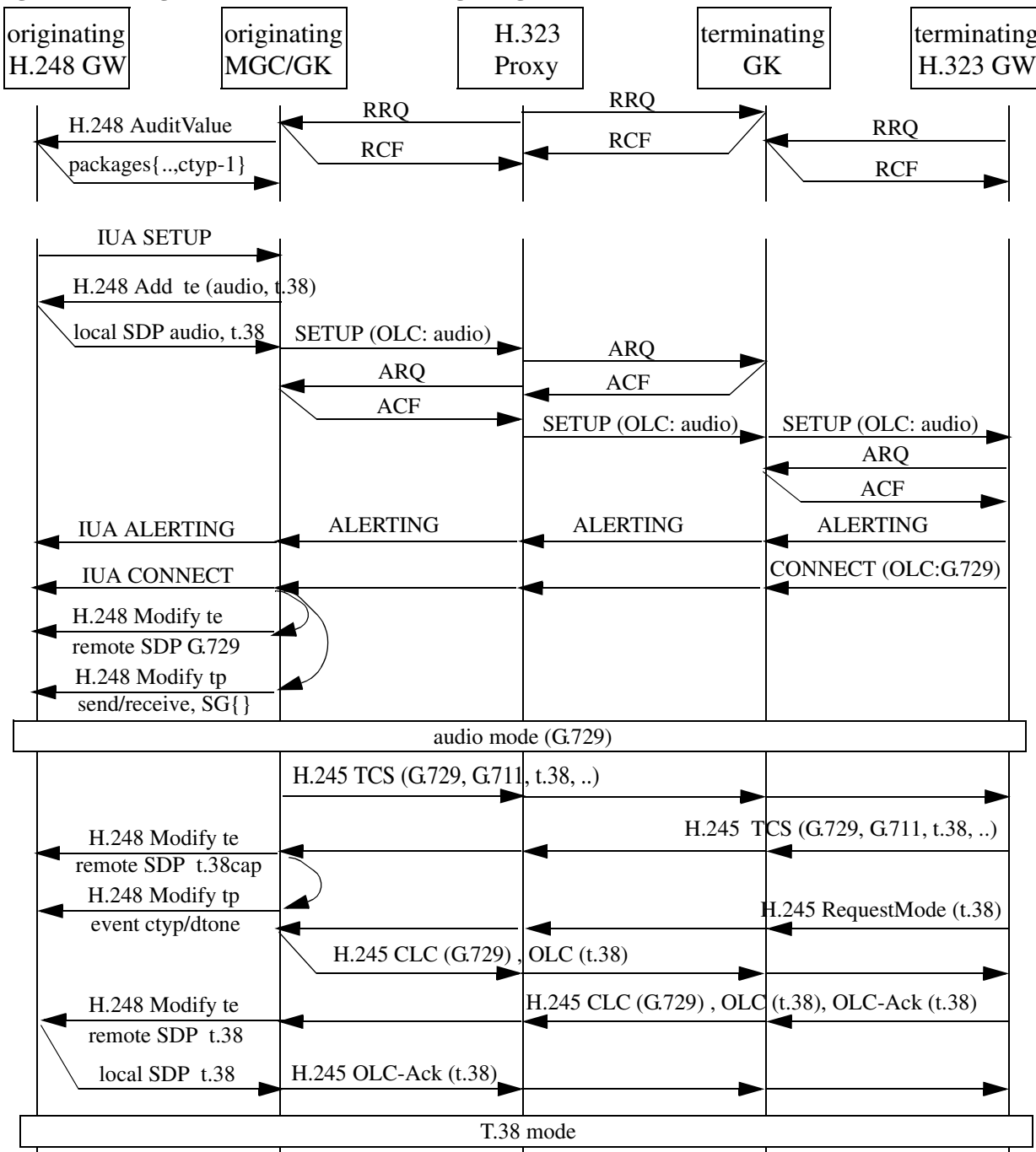
H.323 call signaling is routed from one Gatekeeper (GK) over a H.323 Proxy (ACME SD box) to the other GK. The ACME SD box relays H.323 signaling between both GKs.

Figure 1 Gk-GK signaling using a H.323 Proxy (ACME SD)



58.2.3 Message Flows

Figure 2 shows a flow example for interworking H.248 GW to H323 GW using GK-routed H.323 signaling, H323 RAS procedure and H.323 Fast start procedure. In this flow example, the media path is opened with G.729 codec first. The terminating H.323 GW detects CED fax tone and requests switching to T.38.

Figure 2 Message flow for GK-routed H.323 signaling

In this call flow example the H.245 Terminal capability set (TCS) message is exchanged after the CONNECT message.

The H.248 GW or H.323 GW must not invoke switchover to T.38 mode (or G.711 mode), till the remote side has indicated T.38 (G.711) capability.

Note 1: The most time critical case for successful switching to T.38 was assumed. The terminating H.323 GW may detect a fax call via CED tone or V.21 preamble. CED tone (2100 Hz with a duration of 2.6 to 4.0 sec) is sent 0.2 sec after the terminating fax device answered the call. The V.21 preamble is sent ca. 75ms after end of CED tone.

Note 2: If a GW does not support T.38 codec or Network option T.38 is switched off, CS controlled switchover from G.729 to G.711 shall occur.

Note 3: For clarity some messages (e.g. H.225 Call Proceeding, H.245 Ack-messages) have been omitted in Figure 2. The H.245 messages may also be tunnelled in H.225 Facility messages.

58.2.4 Interworking

Table 1 lists the provided T.38 fax calls via H.323 Proxy (ACME box). Interworkings which do not use the H.323 proxy are out of scope for this feature.

Table 1 Supported T.38 fax interworkings via H.323 Proxy

Originating agent:	Terminating agent				
	H.323 GW (Note 1)	MGCP GW (Note 1)	H.248 GW (Note 2)	SIP-T /SIP (Note 3)	H.323 GW (Note 4)
H.323 GW (Note 1)	out of scope for this feature				✓
MGCP GW (Note 1)					✓
H.248 GW (Note 2)					✓
SIP-T / SIP (Note 3)					✓
H.323 GW (Note 4)	✓	✓	✓	✓	✓

Note 1: GW connected on CS2K, GW located behind NAT/FW
H.323 GWs: CS1000/M, Westell, BCM, Cisco IOS 2600/3600/3700, Model 50
MGCP GW: Mediatrix IAD 1104

Note 2: GW connected on CS2K carrier network
H.248 GWs: Passport 15k with VSP3/VSP3-O card

Note 3: Agent connected on other CS2K or MCS 5200. The remote Call Server is connected via SIP-T (tunneling ISUP V2+) or SIP.

Agents: e.g. IP-phones, TDM agents, analog lines

Note 4: GW connected on Gatekeeper: CS1000/M, Cisco IOS 3600/3700/7200

H.323 GWs: Cisco IOS 2600/3600/3700

Within this activity H.323 Gatekeeper routed T.38 fax calls is provided for:

- Interworking SPM
- Inter-CS call over SIP/SIP-T using NGSS and VRDN GWC

Note 5: Interworking via VRDN GWC has lower priority - support is updated at end of this activity.

58.3 Hardware Requirements or Dependencies

- H.323 interworking with other vendor Gatekeeper requires a H.323 Proxy (ACME SD box, Session Border Controller).
- T.38 fax calls over PVG requires Passport VSP3 or VSP3-O cards.

58.4 Software Requirements or Dependencies

- CS2K with SN08 load
This feature is planned to be patched back to SN07+ release.
- CS1000/M with release 4
- MCS 5200 load version 3.0. (Note: Eventually 4.0 load will be used in SN08)
- H.248 GW - supporting H.248.1, H.248.2 ctyp package, T.38 codec, CS controlled switching to T.38 codec
- H.323 GW - supporting T.38 codec, CS controlled switching to T.38 codec
- MGCP GW - supporting Generic media package/fax tone (G/ft), T.38 codec, CS controlled switching to T.38 codec

58.5 Limitations and restrictions

- Interworking to MCS 5200 is verified only, no development by this feature
- Interworking SPM, SIP-T (NGSS, VRDN) is verified only, no development by this feature.
- Feature validation for NA CS2K load is out of scope for this feature. Feature validation is done by a separate activity (Note: NA activity-id will be included, when available)
- Interworking to Cable gateways is out of scope

58.6 Interactions

Not identified.

58.7 Glossary

Term	Description
BCM	Business Communication Server (H.323 Gateway)
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
CLC	Close Logical Channel (H.245 message)
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.
CS1000, CS1000M	Communication Server 1000, S1000/M, S1K/M Meridian Succession 1000 (H.323 Gateway & GK)
CS2000, CS2K	Communication Server 2000
GK	Gatekeeper
GWC	Gateway Controller
ISN07, ISN08	International Succession Product Release
ISUP	ISDN User Part
MCS 5200	Multimedia Communication Server 5200
MGC	Media Gateway Controller
NGSS	Next-Generation Session Server GWC supporting SIP-T (RFC 3261)
OLC	Open Logical Channel (H.245 message)
PVG	Passport Packet Voice Gateway
RTP	Real-time Transport Protocol (IETF 1889, 3550)
SBC	Session Border Controller, H.323 Proxy, ACME box
SDP	Session Description Protocol (IETF RFC 3266)
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.
TCS	Terminal Capability Set message (H.245 message)
UDP	User Datagram Protocol (IETF RFC 768)

Term	Description
V.21 Preamble	Series of flag sequences 01111110, 1 sec +/- 15%
VRDN	Virtual Routing Distribution Node GWC supporting SIP-T (pre-RFC3261)

58.8 References

- [8] ITU-T Recommendation T.30
Procedures for document facsimile transmission in the general switched telephone network, 04/1999
- [9] ITU-T Recommendation T.38
Procedures for real-time Group 3 facsimile communications over IP networks, 03/2002
- [10] Draft Amendment 1 to Recommendation T.38 (2002) (for Consent)
- [11] ITU-T Recommendation H.323 (Version 4)
Packet-based multimedia communications systems, 11/2000
- [12] ITU-T Recommendation H.225.0 (Version 4)
Call signalling protocols and media stream packetization for packet-based multimedia communication systems, 11/2000
- [13] ITU-T Recommendation H.245 (Version 7)
Control protocol for multimedia communication, 07/2001
- [14] ITU-T Recommendation H.248.1
Gateway Control Protocol, 03/2002
- [15] ITU-T Recommendation H.248.2
Gateway control protocol: Facsimile, text conversation and call discrimination packages, 11/2000
- [16] Feature A00001895 'H.323 Base Support'
PLS library FMDOC
- [17] Feature A00002550 'H.323 GK to CS2K GK Interoperability'
PLS library FMDOC
- [18] Feature A00003627 'T.38 FAX Support for International H.323'
PLS library FMDOC
- [19] CS2000 Product Specification for SN07
<http://product-planning.europe.nortel.com/product-description>

59: A00007242 Functional Description (FN)

59.1 Feature name

SESM support for SPC topology

59.2 Description

In SN08, a new succession component, the SPC (Session Policy Controller) is being introduced. Its purpose is to provide the capability to apply policies during call-processing, e.g. policy-based codec selection, connection admission control etc. In general the policy may be implemented on the SPC itself, or (in the future) the SPC may communicate with other devices, such as intelligent middleboxes, in order to apply the policy.

In SN08, the SPC will support exactly one policy, that of Network Resource Reservation, using Virtual Connection Admission Control (VCAC) as the enforcement mechanism. Hence counting of available resource across Limited Bandwidth Links (LBLs) and connection admission decisions will be carried out on the SPC, instead of being done on the GWCs as in SN07 (SN07 feature A00002512). The SN08 GWCs communicate with the SPC to determine whether a call can be set-up. This will allow LBLs to be shared across different GWCs.

The SPC will reside on the NGSS platform. In SN08, the SPC encompasses a Topology Server application. In order to carry out VCAC, middlebox/zone topology information must be provisioned both into the SESM and into the SPC's Topology Server. The network configuration is shown in figure 1.

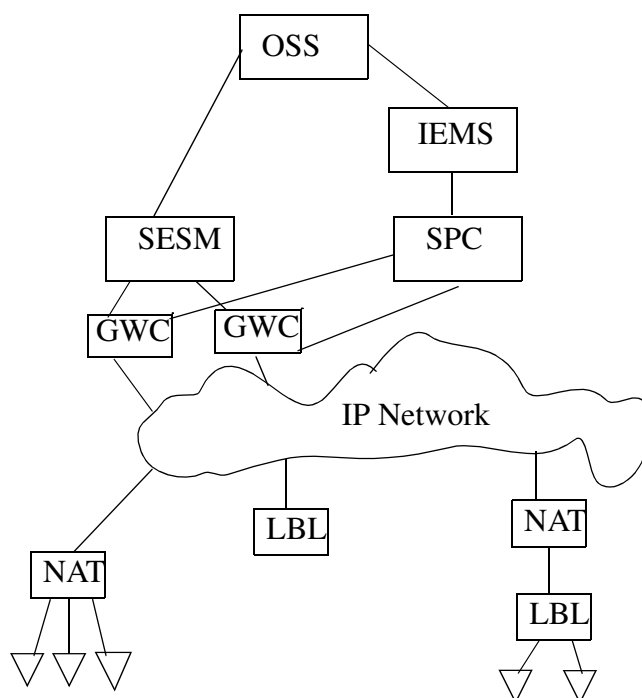
The SPC (Topology Server) will not communicate directly with the SESM. In addition there is no Succession flow-through provisioning interface to both systems. Hence the user (i.e. OSS/GUI user) is responsible for provisioning identical NAT and LBL topology information into both the SESM and the SPC. If identical information is not input into the two systems, VCAC may not work correctly.

For the GUI interface, the user should provision the information first into SESM and then into the SPC. It is important that the information is provisioned in the same order into each system. In particular, adding/deleting NATs & LBLs should be carried out identically in both systems. For example this could be achieved by adding an LBL to SESM and then to SPC, followed by adding the next LBL to SESM and then the SPC etc.

Hence in SN08, feature ACTID A00007242 covers the modifications required in SESM to integrate with the SPC and to provide provisioning for GWCs which support external counting. The resulting functional changes/additions are described in this document.

- Related activities are:
- ACTID A00007398_SPC_Topology_Manager
- GWC modifications for provisioning for external counting

Figure 1 SN08 Network Configuration with SPC



The user operations provided by this feature which effect the GUI client are:

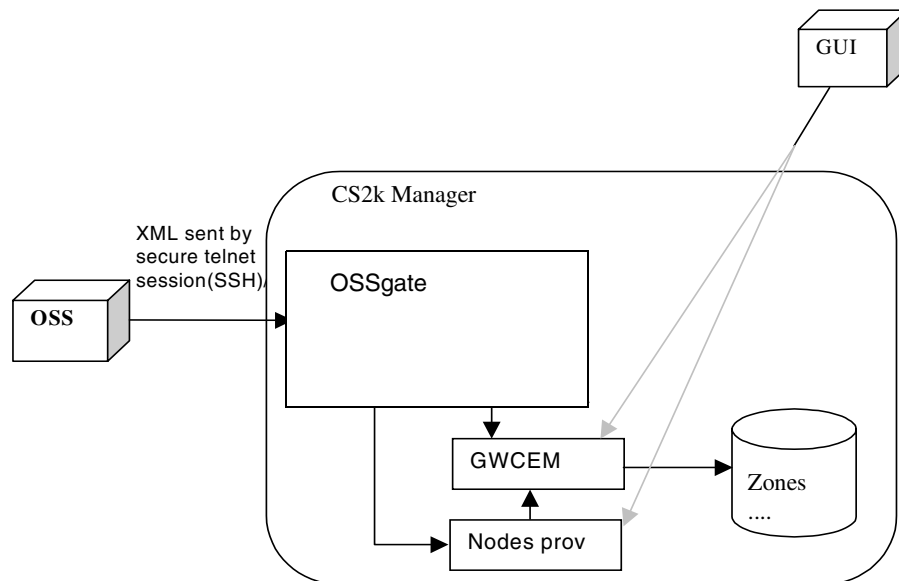
- Provide new GUI to set/change SPC parameters:
 - SPC name
 - SPC IP address

If there is only one supported protocol type and version in SN08 then these will be selected by default and the selections disabled.

- Provide new GUI to set Network VCAC on/off. If Network VCAC is set to 'on' (this requires an SPC to be provisioned), a warning message is provided indicating that:
 - VCAC counting will now be done on the SPC
 - all GWCs and XA-core should be at version SN08 (or above)
 - Reversion to internal counting ('Basic VCAC') is provided on a best effort basis
- Modifications to the existing GWCEM GUI as follows:
 - NAT and LBL panels will be situated on a new 'Network Zones' tab

- It will be possible to provision (add/change/delete) a Network Zone which contains a NAT and an LBL. These Zones will be displayed on a new composite 'NAT & LBL' panel on the new 'Network Zones' tab
- VCAC counting will now be done on the SPC
- all GWCs and XA-core should be at version SN08 (or above)
- Reversion to internal counting ('Basic VCAC') is provided on a best effort basis

Figure 2 GUI Client and OSSGate interfaces



59.3 Hardware Requirements or Dependencies

No new hardware is required or introduced by this feature. The application components provided by this feature execute as part of the SESM.

59.4 Software Requirements or Dependencies

Dependencies:

- CR.xxx: Extend Gateway Controller to support SPC provisioning and Network VCAC

59.5 Limitations and restrictions

- No MCS in SN08, but will be required in future releases
- Only one SPC per CS2k in SN08, but may be more in future releases
- VCAC will be supported with SPC and without SPC.
- There will be no provisioning connection between SPC and SESM in SN08. All topology information must be provisioned first into SESM and then into the SPC.
- Topology data transfer from SESM to SPC when SPC is commissioned will be done manually using existing SESM GUI/OSS interfaces and minor interface enhancements to support bulk query of topology data. Automatic bulk data transfer from SESM to SPC will NOT be provided.
- SESM will not provide an 'undo' capability to the GUI/OSS user.
- In order to facilitate the flow-through provisioning function carried out by the OSS, each SPC command must map to the same SESM command.
- Centralized authentication of passwords is not provided by base platform.
- SPC will not co-reside with any other NGSS based application.
- Bandwidth on-demand requests are incompatible with VCAC solution.
- Upgrade to SN08 should be carried out as described in and limitations on operation of VCAC during upgrade as described there will apply.
- Once Network VCAC is switched on, the SESM will remove any topology provisioning constraint checks which apply to Basic VCAC (internal counting). If Network VCAC is subsequently switched off, the internal counting checks will NOT be restored. It is not recommended to switch Network VCAC off once it has been switched on. Also, if it is switched off, Basic VCAC will only work correctly if the topology still meets the Basic VCAC/'internal counting' topology constraints. In normal use it is expected that Network VCAC will be switched on as soon as the upgrade and soak process is complete and SPC commissioned and will not be switched off.

59.6 Interactions

The following existing GUIs have been modified:

- Network Devices Panel
- Network Devices Panel, NATs tab.
- Network Devices Panel, LBLs tab.
- Add/change/delete NAT Dialogs
- Add/change/delete LBL dialogs
- change adjacent MB dialogs
- change root mb dialogs

The following GUIs have been added:

- SPC provisioning network panel.
- Add/change/delete SPC dialogs
- Network Zone tabbed Panel
- Composite NAT/LBL zone tabbed Panel
- Add/change/delete composite NAT/LBL zone dialogs

The following XML commands have been added:

- Add/change/delete/query Network Zone

The on-line help facility will be updated with information on the use, syntax and valid values for all the above modifications/additions.

59.7 Applicable customer facing sections

Fault Management

Logs	_N/A_

Alarms	_N/A_

Configuration

Data Schema	_X_

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_

Realtime _N/A_

Engineering Information _X_

59.8 SPC Provisioning (including Network VCAC)

The General Network Settings display and change dialog will be modified to include a new panel which will allow setting/change of the SPC provisioning information and Network VCAC flag. Note that for SN08, at most one SPC can be provisioned.

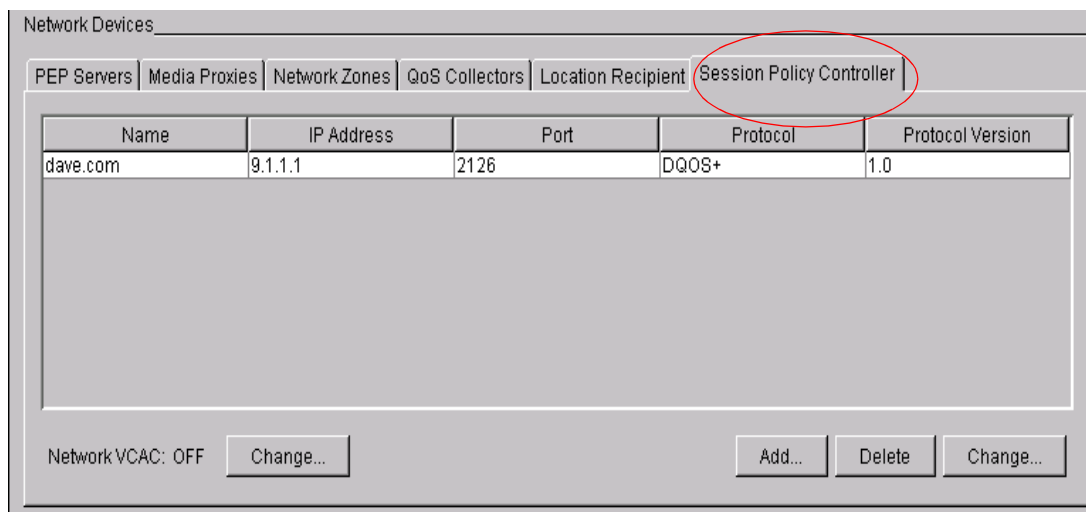
Provisioning constraints will be applied as per the GWCEM GUI guidelines, i.e. with disallowed input data resulting in a red outline to the input field and disabling of appropriate 'ok' buttons etc.

Note that in order to ensure optimum system operation is maintained during an upgrade, the upgrade of GWCs to SN08 should follow details specified in section xxxx.

59.8.1 Provision SPC information

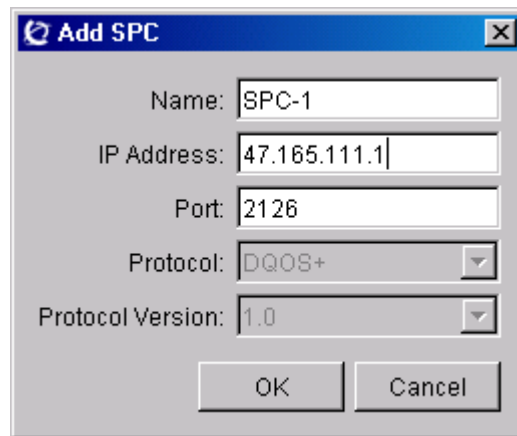
The SPC information is displayed in the Gateway Controller Main Panel, as a tab in the 'Network Devices' area. This is shown in Figure 3

Figure 3 SPC Tab



Add SPC

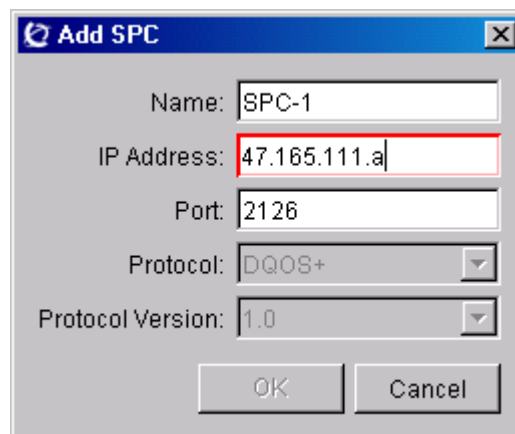
An SPC can be added via the 'Add' button and Add SPC dialog, Figure 4

Figure 4 Add SPC DialogA screenshot of the 'Add SPC' dialog box. It has a title bar with a blue background and a close button. The dialog contains five input fields: 'Name' with the text 'SPC-1', 'IP Address' with '47.165.111.1', 'Port' with '2126', 'Protocol' with a dropdown menu showing 'DQOS+', and 'Protocol Version' with a dropdown menu showing '1.0'. At the bottom are 'OK' and 'Cancel' buttons.

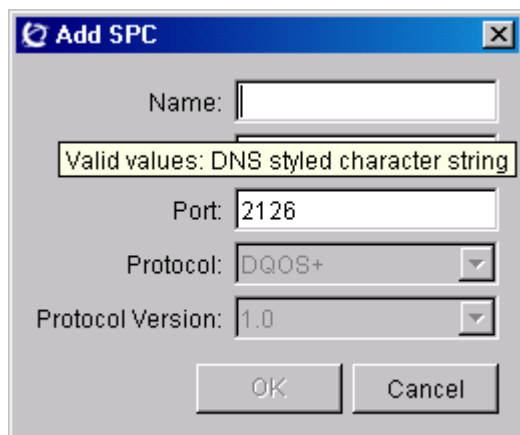
Following information must be added:

- Name (FQDN characters only)
- IP address (a.b.c.d) where a, b, c, d are integers between 0 and 255.
- Port (1 to 65535), defaults to DQOS port 2126.
- Protocol version (selected from list, or fixed at value if only one available)
- Protocol type (selected from list, or fixed at value if only one available)

If invalid data is entered, the corresponding input field is outlined in red and the ok button is disabled, Figure 5

Figure 5 Add SPC Dialog - invalid dataA screenshot of the 'Add SPC' dialog box showing an invalid IP address. The 'IP Address' field contains '47.165.111.a' and is outlined in red. The 'Name' field contains 'SPC-1', 'Port' contains '2126', 'Protocol' is set to 'DQOS+', and 'Protocol Version' is set to '1.0'. The 'OK' button is disabled (grayed out), and the 'Cancel' button is active.

Tool tips describe the valid input data for each text field, e.g. as shown in Figure 6

Figure 6 Add SPC dialog - example tool tip

The image shows a Windows-style dialog box titled "Add SPC". It contains the following fields and controls:

- Name:** A text input field that is currently empty. A yellow tooltip box is displayed below it with the text "Valid values: DNS styled character string".
- Port:** A text input field containing the value "2126".
- Protocol:** A dropdown menu currently showing "DQOS+".
- Protocol Version:** A dropdown menu currently showing "1.0".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

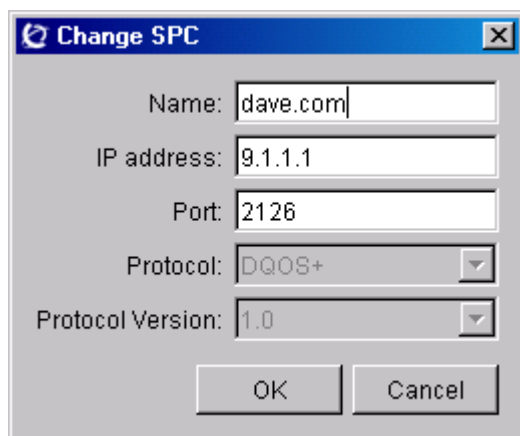
Delete SPC

If an SPC is selected in the table then the 'delete' button is enabled. If delete is clicked then a confirmation message is displayed and if the user confirms the action, the SPC is deleted.

An error dialog is displayed and the delete is not performed if a policy is enabled for the SPC.

Change SPC

If an SPC is selected in the table then the 'change' button is enabled. If change is clicked then a change dialog is displayed, Figure 7

Figure 7 Change SPC Dialog

The image shows a Windows-style dialog box titled "Change SPC". It contains the following fields and controls:

- Name:** A text input field containing the value "dave.com".
- IP address:** A text input field containing the value "9.1.1.1".
- Port:** A text input field containing the value "2126".
- Protocol:** A dropdown menu currently showing "DQOS+".
- Protocol Version:** A dropdown menu currently showing "1.0".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

The following fields can be changed:

- Name
- IP address

- Port
- Protocol type (only one protocol in SN08)
- Protocol version (only one protocol version in SN08)

If invalid data is entered, the corresponding input field is outlined in red and the ok button is disabled. Tool tips describe the valid input data

Set Network VCAC on/off

The SN08 Gateway Controllers can operate in two VCAC modes: they can either attempt to count resource usage on the GWC itself (internal counting, Network VCAC 'off') or they can rely on the SPC to count resource usage and signal to the SPC for admission control during call set-up (Network VCAC 'on').

The current state of Network VCAC is shown on the SPC Panel. The user can set the Network VCAC on/off by using the Network VCAC change button on the SPC panel, see Figure 8, "Network VCAC field". A confirmation message is displayed stating

- VCAC counting will now be done on the SPC
- all GWCs and XA-core should be at version SN08
- If this is the first time Nw VCAC is set on, warning indicating that internal counting provisioning checks will no longer be supported.

Figure 8 Network VCAC field

The screenshot shows a software interface titled "Network Devices". It has several tabs: "PEP Servers", "Media Proxies", "Network Zones", "QoS Collectors", "Location Recipient", and "Session Policy Controller". The "Session Policy Controller" tab is selected. Below the tabs is a table with the following data:

Name	IP Address	Port	Protocol	Protocol Version
dave.com	9.1.1.1	2126	DQOS+	1.0

Below the table, there is a section for "Network VCAC: OFF". The "Change..." button next to it is circled in red. To the right of this section are three buttons: "Add...", "Delete", and "Change...".

Note that after Network VCAC is set on for the first time, SESM will no longer carry out 'internal counting' related provisioning checks, regardless of whether Network VCAC is later switched off or not.

59.9 Network Zone provisioning

59.9.1 XML Interface

New XML interfaces are added are implemented by this feature for use in network installations where the SESM platform is required to operate in conjunction with an SPC. These interfaces align with the provisioning model used by the SPC for NAT and VCAC functionality and is described in terms of Network Zones and Zone characteristics.

The XML interfaces are identical to those supported by the SPC. In order to provision any entity, the information must first be provisioned into SESM and then, if successful, the same information must be provisioned into the SPC. The provisioning should be done first on SESM because SESM has more constraints to check (e.g. whether the Zone is currently associated with a Gateway) and hence is more likely to fail the provisioning request. The XML and XSD for these interfaces are specified in the SPC FN [Ref: <http://livelink-asiapac.us.nortel.com/asiapac/livelink.exe?func=ll&objId=1534787&objAction=browse&sort=name>] and will not be repeated here.

The SESM model only supports a subset of the information used by the SPC. The following general rules will be used:

- Add/change/delete commands: where a parameter is specific to the SPC and of no meaning to SESM, it will be ignored. Where a parameter is interpretable by SESM, its value will be validated
- queries: all relevant parameters for the specific query that are supported by SESM will be returned with valid data. No other parameters will be returned

The SN07 ITRANS VCAC interfaces for NAT and LBL provisioning are still available. However, when a SPC is deployed in the network configuration, the SPC consistent provisioning model is provided via use of the Zone provisioning interfaces and the SN07 ITRANS VCAC interfaces for NAT and LBL provisioning are not required. A mapping is available in table 3.

Note that, when adding a Network Zone, Resource Usage Factor and Max Count values are not required as long as Network VCAC is on (Details of Logical Network Link sent in XML messages 'addNetworkZone' and 'changeNetworkZone' are ignored by SESM. However if Network VCAC is 'off', resource usage factor and max count details ARE required and hence the XML command 'addLBL' should be used to add LBL Network Zones. However it is not recommended to switch Network VCAC off once it has been switched on. Also, if it is switched off, Basic VCAC will only work correctly if the topology still meets the Basic VCAC/'internal counting' topology constraints.

59.9.1.1 Supported Interfaces For SPC Interworking

Add, Change and Delete Network Zone interfaces are implemented by SESM. In general, the Zone and the Zone parent can be referenced by either name or Zone ID, but not by both. For 'Add Network Zone', the Zone ID is optional and will be generated by SESM if not specified.

Table 1 XML Interfaces Specific To SPC Topology Server Interworking For ITRANS

Interface	SN07 VCAC ITRANS Equivalent	Description
addNetworkZone	addNAT or addLBL	Add either a NAT, LBL or Composite type network zone
changeNetworkZone	changeNAT or changeLBL	change either a NAT, LBL or Composite type network zone
deleteNetworkZone	deleteNAT or deleteLBL	delete either a NAT, LBL or Composite type network zone
queryNetworkZone	queryNAT plus queryLBL	query on NAT, LBL and Composite data fill

59.9.1.1.1 addNetworkZone Interface

This interface will add a new NAT, LBL or Composite type Network Zone. A composite Network Zone is one comprising the attributes of both a NAT and LBL type Network Zone.

The following parameters will be interpreted when adding a new Network Zone, with all other SPC specific parameters being ignored:

- <Name>NZ-Name</Name> - Unique name for the new Network Zone (NAT, LBL or Composite Name).
- <ID>1234</ID> - Unique ID for the Network Zone (NAT, LBL or Composite) to be created. If this is not specified, it is generated by SESM.
- <Parent> - Optional tag. Specified if Network Zone has a parent and contains tags ParentID or ParentName.
 - <ParentID>5678</ParentID> - ID of parent Network zone. Mutually exclusive with ParentName.
 - <ParentName>Parent-Name</ParentName> - Name of parent Network zone. Mutually exclusive with ParentID.
- </Parent>
- <Service>NAT</Service> - Optional. Identifies Network Zone as being a NAT or Composite type Network Zone. For a Composite Network Zone the LogicalNetworkLink tag should also be present.
- <LogicalNetworkLink> - Optional. Identifies the Network Zone as being an LBL or Composite Network zone. For a Composite Network Zone the Service tag should also be present.

- ... Contents of LogicalNetworkLink are ignored but should be correctly populated.
- </LogicalNetworkLink>

At least one of the tags Service and LogicalNetworkLink must be present.

If both Service and LogicalNetworkLink tags are present, the Zone is a composite NAT & LBL zone.

All other input data is ignored by SESM.

59.9.1.1.2 changeNetworkZone Interface

This interface will modify either a NAT, LBL or Composite type Network Zone.

For the change command, the user will specify tags for the parameters that are to be changed. Unchanged parameters do not have to be specified. The Network Zone name and ID cannot be changed. All other parameters can be changed. SESM will ignore changes to parameters that it does not hold (e.g. bandwidth, link types etc.).

Interpreted parameter tags are as follows:

- <Name>NZ-Name</Name> - Network Zone Name
- ** or **
- <ID>1234</ID> - Network Zone ID
- <Parent> - Optional tag identifying a new Parent Network Zone. Contains either ParentName or ParentID tags but not both.
 - <ParentID>5678</ParentID> - new parent ID. Set to 0 if no parent required. Mutually exclusive with ParentName.
 - <ParentName>New-Parent-Name</ParentName> - new parent Network Zone name. Mutually exclusive with ParentID.
- </Parent>
- <LogicalNetworkLink> - optional. If present the Network Zone type is checked to ensure it is not a NAT as the presence of this tag implies a change of Network Zone type which is not supported.
 - ... contents of LogicalNetworkLink are ignored
- </LogicalNetworkLink>

59.9.1.1.3 deleteNetworkZone Interface

This interface will delete either a NAT, LBL or Composite type Network Zone.

Interpreted parameter tags are as follows:

-
- `<Name>NZ-Name</Name>` - Name of Network Zone to be deleted.

**** OR ****

- `<ID>1234</ID>` - ID of the Network Zone to be deleted.

59.9.1.1.4 queryNetworkZone Interface

This interface will perform a selective query on the provisioned NAT, LBL and Composite type network zones. Based on the population of the request it is possible to retrieve a single network zone name or all network zones names. The network zone IDs may also be optionally retrieved. This command differs from the SN07 queryNAT and queryLBL interfaces in that the returned data is a combination of the provisioned NATs and LBLs. It is not possible to selectively retrieve those network zones of a particular service type.

In general, since SESM holds a subset of the topology information held by SPC (i.e. it has no link information), the user should carry out queries on SPC. SESM will support both individual and bulk queries, however it is expected that only the bulk queries will be used. Bulk queries will be needed e.g. to audit the SESM-SPC data consistency. The result of the bulk query will be sorted by ID.

Interpreted input parameter tags are as follows:

Name or ID - Optional parameter indicating we wish to query a specific Network Zone. If not specified it is assumed that all Network Zones should be queried.

- `<Name>Bob</Name>` - requests retrieval of “Bob” Network Zone OR
- `<ID>1234</ID>` - requests retrieval of Network Zone with ID 1234.

Filtering parameters to limit the number of zones returned. These are optionally present but only for bulk zone queries (i.e. when no name or id is specified)

- `<IDMax>12000</IDMax>` - maximum Network Zone ID
- `<IDMin>11001</IDMin>` - minimum Network Zone ID
- `<MaxZones>1234</MaxZones>` - maximum number of Zones to be returned. If more Zones exist than the maximum specified, this will be indicated via an error code.

Returned parameter tags are as follows:

- `<ID>1234</ID>` - Unique ID for a Network Zone.
- `<Name>NZ-Name</Name>` - Unique Network Zone name.
- `<ParentID>5678</ParentID>` - ID of parent Network Zone. Where there is no parent this will be set to 0.

Additionally for query of individual Network Zone, the following information is also returned:

- <Service>NAT</Service> - Service type indicating if this Network Zone is a NAT. If the zone is has no services, no service tag is returned.
- <LogicalNetworkLink> - returned only if the Network Zone type is LBL or Composite. This will contain LayerInfo, Layer and LinkLayerInfo tags, with the LinkLayerInfo tag assigned a dummy value of “UNKNOWN” as SESM has no knowledge of Network Zone parameter values.

59.9.1.2 Unsupported Interfaces

The SESM platform only supports a subset of the SPC Topology server VCAC ITRANS interfaces. In SN08, add/change/delete/query LinkLayer type are not supported by SESM. However, to aid simple XML command replication by the OSS, these will be a dummy commands in SESM & will always return an error code 306 and text 'SPC Interface Unsupported By Platform'. (The alternative is for SESM not to support this, however this means a single XSD cannot be published and requires OSS to understand which commands go only to the SPC.)

Unsupported interfaces are described in the following table:

Table 2 SPC Topology Server ITRANS Interfaces Unsupported By SESM

Interface	Description
addLinkLayerType	add a new link layer
changeLinkLayerType	change an existing link layer
deleteLinkLayerType	delete a link layer
queryLinkLayerType	query provisioned link layers

59.9.1.3 NAT/LBL provisioning interfaces

The SN07 ITRANS VCAC interfaces for NAT and LBL provisioning are still available. When a SPC is deployed in the network configuration, a consistent provisioning model is provided via use of the Zone provisioning interfaces.

However the SN07 interfaces remain valid ITRANS VCAC interfaces for NAT and LBL provisioning (table 3) and should be used when the SPC is not present in the network configuration.

Table 3 SN07 SESM ITRANS VCAC Interfaces.

Interface	Description
addNAT	Add NAT - use addNetworkZone.
changeNAT	Change NAT - use changeNetworkZone

Table 3 SN07 SESM ITRANS VCAC Interfaces.

Interface	Description
deleteNAT	Delete NAT - use deleteNetworkZone
queryNAT	Query NAT - use queryNetworkZone. See Note following table.
addLBL	Add LBL - replaced by addNetworkZone. Resource usage and counter functionality is set to default values.
changeLBL	ChangeLBL - replaced by changeNetworkZone. Resource usage and counter functionality is set to default values.
deleteLBL	Delete LBL - replaced by queryNetworkZone.
queryLBL	Query LBL - use QueryNetworkZone Interface (safe but deprecated)
changeRootMiddleBoxes	Change Root Middle Boxes - use changeNetworkZone interface
changeAssocMB	Change associated middlebox - use changeNetworkZone interface
addRU	Add Resource Usage. SESM has no concept of resource usage where SPC Topology server is present. Internally default settings will be used for modelling purposes, and attempting manipulation would make no sense.
changeRU	Change Resource Usage.
deleteRU	Delete Resource Usage
queryRU	Query Resource Usage

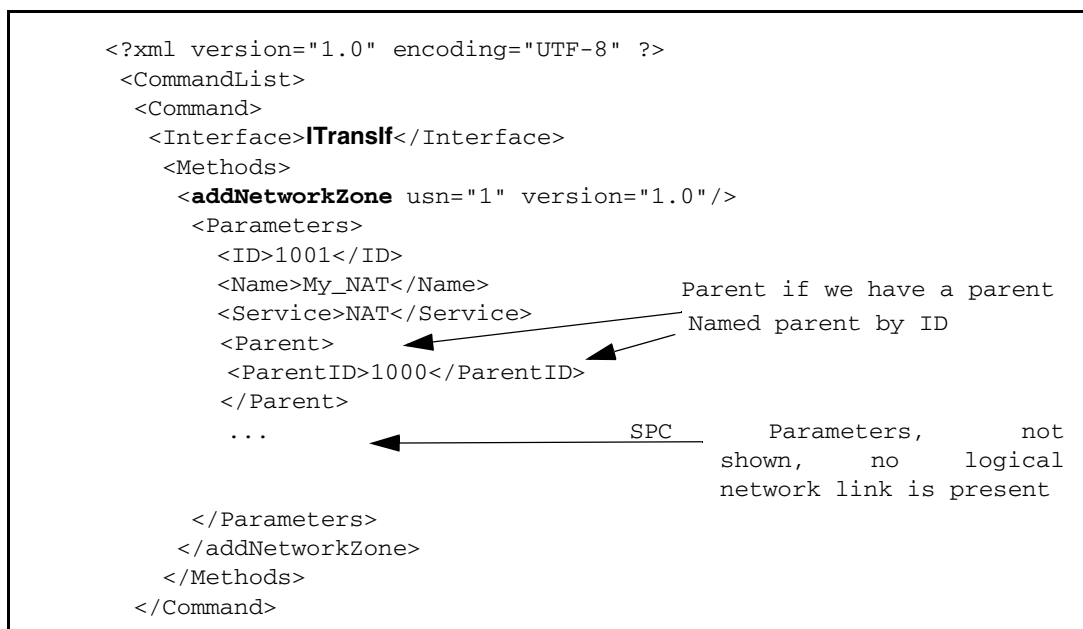
Note: Interface remains used by CICM Element Manager.

59.9.2 Error codes

Each error code will have a descriptive text string associated with it. It is not possible to guarantee that the same error will result in the same error code being returned by SPC and SESM. However the sequential provisioning required (first into SESM and then into SPC) means that typically the OSS will get an error code back from one machine only - since if the SESM command fails, it will not continue to do the provisioning into SPC.

59.9.2.1 Examples Of XML Interface Usage

59.9.2.1.1 Add NAT using addNetworkZone (Request)



59.9.2.1.2 Add LBL using addNetworkZone (Request)

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <addNetworkZone usn="1" version="1.0">
        </Parameters>
        <Name>My_LBL</Name>
        <Parent>
          <ParentName>MyParent</Parent>
        </Parent>
        <LogicalNetworkLink>
          <BandwidthInfo>
            <Symmetry>true</Symmetry>
            <UpBWInfo>
              <BWCIR>1000</BWCIR>
              ... SPC specific parameters
            </UpBWInfo>
            <DownBWInfo>
              <BWCIR>1000</BWCIR>
              ... SPC specific parameters
            </DownBWInfo>
          </BandwidthInfo>
          ...SPC specific parameters
        </LogicalNetworkLink>
        ... SPC specific parameters
      </Parameters>
    </addNetworkZone>
  </Methods>
</Command>
</CommandList>

```

Parent if we have a parent
 Named using NZ Name
 Contents of BandwidthInfo
 losely interpreted.
 Contents are ignored.

59.9.2.1.3 Add Composite NAT/LBL using addNetworkZone (Request)

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <addNetworkZone usn="1" version="1.0">
        </Parameters>
        <Name>My_LBL</Name>
        <Service>NAT</Service>
        <Parent>
          <ParentID>1010</ParentID>
        </Parent>
        <LogicalNetworkLink>
          <BandwidthInfo>
            <Symmetry>>false</Symmetry>
            <UpBWInfo>
              <BWCIR>1000</BWCIR>
              ... SPC specific parameters
            </UpBWInfo>
          </BandwidthInfo>
          ...SPC specific parameters
        </LogicalNetworkLink>
      </Parameters>
    </addNetworkZone>
  </Methods>
</Command>
</CommandList>

```

Optional ID not specified

Name parent using ID

Contents of BandwidthInfo
loosely interpreted.
Contents are ignored.

... SPC specific parameters

...SPC specific parameters

59.9.2.1.4 Change Network Zone (LBL or NAT) (Request)

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <changeNetworkZone usn="1" version="1.0">
        <Parameters>
          <Name>My_Zone</Name>
          <Parent>
            <ParentName>New-Parent</ParentName>
          </Parent>
          ...
        </Parameters>
      </changeNetworkZone>
    </Methods>
  </Command>
</CommandList>
```

Change parent using name

SPC specific parameters not shown

59.9.2.1.5 Delete Network Zone (LBL or NAT) (Request)

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <deleteNetworkZone usn="1" version="1.0">
        <Parameters>
          <Name>My_Zone</Name>
        </Parameters>
      </deleteNetworkZone>
    </Methods>
  </Command>
</CommandList>
```

Target Network Zone using Name

59.9.2.1.6 Query Network Zone (All) (Request)

```
<?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>
```

59.9.2.1.7 Query Network Zone (Range Min ID Max ID) (Request)

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <queryNetworkZone usn="1" version="1.0">
        <Parameters>
          <IDMin>500</IDMin>
          <IDMax>900</IDMax>
        </Parameters>
      </queryNetworkZone>
    </Methods>
  </Command>
</CommandList>
```

59.9.2.1.8 Query Network Zone (Range Min ID MaxZones) (Request)

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <queryNetworkZone usn="1" version="1.0">
        <Parameters>
          <IDMin>500</IDMin>
          <MaxZones>200</MaxZones>
        </Parameters>
      </queryNetworkZone>
    </Methods>
  </Command>
</CommandList>
```

59.9.2.1.9 Query Network Zone (Individual ID Based) (Request)

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <queryNetworkZone usn="1" version="1.0">
        <Parameters>
          <ID>101</ID>
        </Parameters>
      </queryNetworkZone>
    </Methods>
  </Command>
</CommandList>
```

59.9.2.1.10 Query Network Zone (Individual Name Based) (Request)

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <queryNetworkZone usn="1" version="1.0">
        <Parameters>
          <Name>Peter67</Name>
        </Parameters>
      </queryNetworkZone>
    </Methods>
  </Command>
</CommandList>
```

59.9.2.1.11 Query Network Zone (All / Range) (Response)

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
      <queryNetworkZone usn="1" version="1.0">
        <ReturnData>
          <NetworkZone>
            <ID>235</ID>
            <Name>NZ1</Name>
            <ParentID>0</ParentID>
          </NetworkZone>
          <NetworkZone>
            <ID>891</ID>
            <Name>NZ2</Name>
            <ParentID>235</ParentID>
          </NetworkZone>
          <NetworkZone>
            <ID>65539</ID>
            <Name>Nat.1</Name>
            <ParentID>0</ParentID>
          </NetworkZone>
          <NetworkZone>
            <ID>65540</ID>
            <Name>lbl1</Name>
            <ParentID>0</ParentID>
          </NetworkZone>
          <NetworkZone>
            <ID>65541</ID>
            <Name>comp1</Name>
            <ParentID>0</ParentID>
          </NetworkZone>
          <ReturnCode value="0" text="Successful result" />
        </ReturnData>
      </queryNetworkZone>
    </Methods>
  </Response>
</CommandList>
```


59.9.2.1.12 Query Network Zone (Individual) (Response)

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
      <queryNetworkZone usn="1" version="1.0">
        <ReturnData>
          <ID>65541</ID>
          <Name>comp1</Name>
          <Service>NAT</Service>
          <Parent>
            <ParentID>0</ParentID>
          </Parent>
          <LogicalNetworkLink>
            <LayerInfo>
              <Layer>
                <LinkLayerType>UNKNOWN</LinkLayerType>
              </Layer>
            </LayerInfo>
          </LogicalNetworkLink>
          <ReturnCode value="0" text="Successful result" />
        </ReturnData>
      </queryNetworkZone>
    </Methods>
  </Response>
</CommandList>
```

59.9.3 GUI Client

The GUI client for internet transparency NAT and VCAC entity provisioning will be available for network deployments where the SPC is present and for deployments where the SPC is not present. Hence the GUI must effectively support both the SN07 and SN08 models. Hence the GUI will not be changed significantly from the SN08. The changes are as follows:

59.9.3.1 Network Zone Display

There will be a new panel on the Network Devices tabbed panel, this will be a tabbed panel with tab 'Network Zones'.

The NAT and LBL provisioning panels will be moved from the Network devices tabbed panel the Network Zones tabbed panel. In addition, there will be a new provisioning panel for provisioning composite NAT/LBL Network Zones (this functionality to be confirmed), see Figure 9

Figure 9 Network Zones tabbed panel

The screenshot shows a software interface with a tabbed panel titled "Network Devices". The "Network Zones" tab is selected. Below the tabs, there are sub-tabs: "NAT Zone", "LBL Zone", and "NAT&LBL Zone". The "NAT Zone" sub-tab is active, displaying a table with the following data:

Name	NAT Type	
Fred.1	Non-Controlled	<none> (To
MFNAT.1	Non-Controlled	<none> (To
MFNAT.2	Non-Controlled	<none> (To
MFNAT.3	Non-Controlled	<none> (To
MFNAT.4	Non-Controlled	<none> (To
MFNAT.5	Non-Controlled	<none> (To
MFNAT.6	Non-Controlled	MFLBL.4

At the bottom right of the panel are two buttons: "Add..." and "Delete".

59.9.3.2 Add/Change/Delete Zone

In the add/change/delete NAT & LBL dialogs and for add/change NAT/LBL associated to gateway, the word 'Middlebox' will generally be replaced with either 'Zone' or 'Network Zone', for example as in Figure 10.

Figure 10 Add NAT Zone

The screenshot shows a dialog box titled "Add IP-VPN (NAT Zone)". It contains the following fields and controls:

- Name:** A text input field.
- Shared Zone:** A checkbox that is currently unchecked.
- NAT Type:** A dropdown menu showing "Non-Controlled".
- Parent Zone Selection (create hierarchy):** A section containing:
 - Three radio buttons: "ALL" (selected), "IP-VPNs", and "LBLs".
 - A "Parent Zone" dropdown menu showing "<none>".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

59.9.3.3 LBL provisioning

When the SPC is present, the user does not need to provision the RU Profile Name and Max Count Value when provisioning an LBL. Hence, when the Network VCAC flag is switched 'on', fields to provision and change RU Profile and Max count information will be hidden. Internally, the RU Profile will be set to a system provisioned RU Profile created on system initialization, SPC_DEFAULT and the Max count set to 0 (tbc). Fields which display this information in the LBL zone table will also be hidden. If the Network VCAC flag is switched off, the RU Profile and max count information is displayed again.

Similarly, the RU provisioning panel will be hidden/displayed when the Network VCAC flag is switched on/off.

59.9.3.4 Composite NAT & LBL provisioning (this work item tbc)

Similar dialogs will be supported for add/change/delete composite NAT/LBL zone as for NAT zones. This option is only available when the SPC is used and RU Profile and max count information is not required. Hence similar dialogs/display will be supported for add/change/delete/display composite NAT/LBL zone as for NAT zones. Note that in this case, NO profile or max count information is sent to the GWC and, for internal counting, the zone is treated as a NAT zone.

59.10 Authorization for Commands

The security for the GUI Client and OSSgate interface includes support for permission or 'Authorization' levels for commands. Each command is associated with one or more user groups. In order to execute a command, a user must belong to at least one of the associated user groups. The user groups associated with the new /modified commands associated with this feature are specified in the table below.

Table 4 Internet Transparency Commands Authorization

Command	User Group				
	mgcadm	mgcrw	mgcmte	mgcsprov	mgcro
add SPC	X				
delete SPC	X				
change SPC	X				
display SPCs	X	X	X	X	X
set Network VCAC	X				
add Network Zone	X	X		X	

Table 4 Internet Transparency Commands Authorization

Command	User Group				
	mgadm	mgrw	mgmtc	mgspov	mgcro
delete Network Zone	X	X		X	
change Network Zone	X	X		X	
query Network Zone	X	X	X	X	X
query all Network Zones	X	X	X	X	X

59.11 Upgrade

In order to ensure optimum system operation is maintained during an upgrade, the upgrade of GWCs to SN08 should follow details specified in the FN for feature A00007394

59.12 Glossary

Term	Description
CS2K	Communication Server 2000
GUI	Graphical User Interface
GWC	Gateway Controller
GWCEM	Gateway Controller Element Manager
ID	Identifier
IEMS	Integrated Element Manager System
LBL	Limited Bandwidth Link
ME	Media Endpoint
NAT	Network Address Translation
NGSS	Next Generation Sessions Server
OSS	Operations Support System
SESM	Succession Element and Sub-element Manager
SPC	Session Policy Controller
VCAC	Virtual Connection Admission Control
VPN	Virtual Private Network

Term	Description
XML	Extensible Markup Language

59.13 Appendix A: Error codes and messages

Table 5 Return codes when command is unsuccessful

Error meaning	Return code	Example return messages
Platform applications internal error: OSS Interface applications cannot connect to required server application	302	Interfacing error
Unable to provision requested data because a database error occurred	303	Database error occurred during setting of Network Zone
Unable to provision requested data because of problem with the GWCEM component of the CS2k Mgr.	304	Element Manager Initialization in progress
No data for this query meets selection criteria or the filtering criteria specified do not exist	305	No Network Zones found
Interface is valid based on ITrans XSD schema but is unsupported by SESM (SPC specific)	306	SPC Interface Unsupported By Platform
User is not a member of any of the user groups allowed to perform this action	501	Insufficient permissions to perform this operation

59.13.1 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>
```

59.14 Appendix B: XML Commands: description of method parameters

59.14.1 Parameter definitions

Only those parameters that are read / returned by the VCAC ITrans interface are described.

- **encoding** - UTF-8.
- **version** - The version refers to the version of the method or operation - e.g., the addNAT operation may have version 1.0 and 2.0, where version 1.0 takes parameters X and Y and version 2.0 takes parms X, Y, and Z. TYPE *decimal*.
- **usn** - Unique Sequence Number. This parameter is introduced to facilitate sending multiple XML commands in one file. This parameter value will be used to match the responses with the requests. TYPE *integer*.
- **Name** - Unique Network Zone name.
- **ID** - Unique Network Zone ID.
- **ParentName** - Name of parent Network Zone.
- **ParentID** - ID of parent Network Zone.
- **Service** - Network Zone service type. Only supported value is "NAT".
- **Symmetry** - LogicalNetworkLink - BandwidthInfo symmetry field. Boolean value but setting ignored by SESM but has meaning to SPC.
- **BWCIR** - LogicalNetworkLink - BandwidthInfo - UpBWInfo / DownBWInfo BWCIR setting. Value is ignored by SESM but has meaning to SPC.
- **LinkLayerInfo** - LogicalNetworkLink - LayerInfo - Layer - LinkLayerType field. Value is ignored by SESM being SPC specific.
- **IDMin** - Minimum Network Zone ID for a query.
- **IDMax** - Maximum Network Zone ID for a query.
- **MaxZones** - Maximum number of Network Zones for a query.
- **ReturnCode value**- A numeric value indicating the result of the attempted operation (see Table 3, for range and definitions of each possible value). TYPE *string*.
- **Return code text**- Appropriate text that describes the result of the operation. TYPE *string*.

59.14.2 Method Parameters

Method parameters are defined below. Input data is mandatory except where indicated otherwise.

-
1. **addNetworkZone** - Method that adds a new Network Zone. This method has the following parameters:
 - Input data:
 - usn
 - version
 - Name
 - ID (optional internally generated if not specified)
 - ParentName (optional and mutually exclusive with ParentID)
 - ParentID (optional and mutually exclusive with ParentName)
 - Service (optional only if NAT / Composite Network Zone required)
 - Symmetry (optional only if LBL / Composite Network Zone required)
 - BWCIR (optional only if LBL / Composite Network Zone required).
 - 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. **changeNetworkZone** - Method that modifies a parent Network Zone. This method has the following parameters:
 - Input data:
 - usn
 - version
 - Name (Mutual exclusive with ID parameter)
 - ID (Mutual exclusive with Name parameter)
 - ParentName (optional and mutually exclusive with ParentID)
 - ParentID (optional and mutually exclusive with ParentName)
 - 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.
-

3. **deleteNetworkZone** - Method that deletes a Network Zone. This method has the following parameters:
- Input data:
 - usn
 - version
 - Name (Mutual exclusive with ID parameter)
 - ID (Mutual exclusive with Name parameter)
 - 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.
4. **queryNetworkZone** - Method that queries the Network Zones provisioned on the SESM platform. This method has the following parameters:
- Input data:
 - usn
 - version
 - Name (optional and mutually exclusive with ID. Presence restricts query to a single Network Zone)
 - ID (optional and mutually exclusive with Name. Presence restricts query to a single Network Zone)
 - IDMin (Optional. Not valid if query targets a specific Network Zone).
 - IDMax (Optional. Not valid if query targets a specific Network Zone).
 - MaxZones (Optional. Not valid if query targets a specific Network Zone).
 - Output data:
 - usn (value should be the same as the input)
 - version (value should be the same as the input)
 - ID
 - Name
 - ParentID
 - Service - where individual Network Zone is targeted and type is NAT or Composite. Value is set to "NAT"

-
- LinkLayerType - where individual Network Zone is targeted and type is LBL or Composite. Value is set to “UNKNOWN”
 - 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.

60: A00007243 Functional description (FN)

60.1 Feature name

Prevent Outage when CEM flash has not been erased.

60.2 Description

CSR.Q00854598 reported an outage in the field, where a CEM card without erasing Flash from one SPM was inserted into another SPM. When the newly inserted CEM card tried recover to in-service, another in-service CEM present in SPM from which the CEM card was originally removed went down leading to an outage on that SPM. This occurred due to duplicate IP addressing causing the message to reach the incorrect CEM unit resulting in that unit being brought down.

This feature will ensure that when a CEM card is being inserted into a MG4K node, no other MG4K nodes in the office experience an outage due to this card insertion. This feature is applicable only for MG4K variant of the SPM.

When a CEM card is being inserted into a MG4K node, CEM card replacement MOP (Method of Procedure) for MG4K SPMs should be followed as described in the NTP document (**NN10076-911 Title: MG4000 Fault Management**).

If the MOP is not followed (either Flash is not erased or MAC address is not modified), it could lead to duplicate IP addressing and incorrect messaging between MG4K nodes. This incorrect addressing can cause an outage on another MG4K nodes in the office.

This activity in SN08 ensures that when a CEM card is being re-seated there is no outage on other MG4K nodes under following scenarios where CEM cards can obtain wrong IP addresses-

- a) the CEM's flash was not erased and the MAC address is wrong in Table MNCKTPAK
- b) the CEM's flash was not erased and the fiber cable had not been plugged in prior to insertion
- c) the CEM's flash was not erased and the WAN is slow to provide connectivity to the Call Server

Note: This feature is only a best effort to prevent outage on another MG4K nodes in the office in case a CEM card is replaced without changing MAC in table MNCKTPAK or Flash is not erased. This feature does not replace the documented MOP to replace a CEM card in MG4K node. The MOP must be followed for all card replacements.

The feature supports the following scenarios when a CEM card is being re-seated or replaced -

60.2.1 CEM card replaced in BootP suppressed node with Mate CEM available

In a Bootp suppressed node MAC address is not used to provide node addressing information to the CEM unit. Node addressing information is provided by Mate CEM.

60.2.1.1 MAC address of CEM card is not present in table MNCKTPAK

- a. Once the CEM card is replaced Mate CEM initiates recovery and tries to recover the CEM card by mateloading.
- b. If the Mate recovery fails and load in flash is valid and not corrupt then the CEM card will recover by autoboot.
- c. RTS command takes the CEM card to ISTb state. MAP response to RTS command indicates MAC address mismatch.
- d. SPM313 log on the Call Server and NODE 300 log in SPM AER buffer are generated to indicate MAC address mismatch.
- e. QueryPM flt reason command displays MAC mismatch as non-critical fault on the CEM.
- f. Craftsperson should change the MAC address in table MNCKTPAK to contain the CEM MAC address as per NTP - **NN10076-911**

60.2.1.2 MAC address of CEM card present in table MNCKTPAK but against a different MG4K node

The result is same as mentioned in “MAC address of CEM card is not present in table MNCKTPAK” on page 561.

60.2.1.3 MAC address of CEM card properly datafilled in table MNCKTPAK

- a. As MAC address is correctly datafilled there will not be any NODE300 or SPM313 log.
- b. If no other faults are raised on the CEM then it recovers INSV state when RTS command is issued

60.2.2 CEM card replaced in BootP suppressed node with Mate CEM not available

The CEM card will not be provided with correct node addressing information as the Mate CEM is not available. The CEM card will not be able to recover to in-service due to incorrect node addressing. LCI shall be used to provide node addressing and load information to recover the CEM card to INSV. This

feature will prevent outages on other CEM units due to incorrect node addressing information during this scenario.

60.2.2.1 MAC address of CEM card is not present in table MNCKTPAK

- a. If the load in flash is valid and not corrupt then it will autoboot from Flash.
- b. Since Node addressing information is incorrect it will not recover to INSV.
- c. CEM stays in SysB state till LCI is used to recover it.
- d. No outage will occur on other CEM units in the office due to incorrect node addressing.

60.2.2.2 MAC address of CEM card present in table MNCKTPAK but against a different MG4K node

The result is same as mentioned in “MAC address of CEM card is not present in table MNCKTPAK” on page 562.

60.2.2.3 MAC address of CEM card properly datafilled in table MNCKTPAK

- a. If the load in flash is valid and not corrupt then it will autoboot from Flash.
- b. Since node addressing information is correct, it will recover to INSV state.
- c. There will not be any NODE300/SPM313 log.

60.2.3 CEM card replaced in Non-BootP suppressed node with Mate CEM available

60.2.3.1 MAC address of CEM card is not present in table MNCKTPAK

- a. BootP reply will not be sent by the Call Server.
- b. BOOT201 log will be generated to indicate that MAC address to IP address mapping could not be found.
- c. The node addressing information is provided by the Mate CEM.
- d. The CEM card recovers through mate loading.
- e. If Mate recovery fails then it tries to recover through autoboot.
- f. RTS command takes the CEM card to ISTb state. MAP response to RTS command indicates MAC address mismatch.
- g. SPM313 log on the Call Server and NODE 300 log in SPM AER buffer are generated to indicate MAC address mismatch.

-
- h. QueryPM flt reason command displays MAC mismatch as non-critical fault on the CEM.
 - i. Craftsperson should change the MAC address in table MNCKTPAK to contain the CEM MAC address as per NTP - **NN10076-911**

60.2.3.2 MAC address of CEM card present in table MNCKTPAK but against a different MG4K node

- a. QUNI the CEM unit on which the BootP request is made. Reject the BootP request if the CEM unit is in software and accept the BootP request if the CEM unit is in firmware.
- b. If BootP request is rejected, a BOOT201 log will be generated if permission denial exceeds throttle number to indicate that BootP request was denied permission.
- c. Allow the CEM unit at firmware to recover through BootP.
- d. For the CEM card being replaced the node addressing information is provided by the Mate CEM.
- e. The CEM card recovers through Mate loading.
- f. If Mate loading fails then Unit tries to recover through autoboot.
- g. RTS command takes the CEM card to ISTb state. MAP response to RTS command indicates MAC address mismatch.
- h. SPM313 log on the Call Server and NODE 300 log in SPM AER buffer are generated to indicate MAC address mismatch.
- i. QueryPM flt reason command displays MAC mismatch as non-critical fault on the CEM.
- j. Craftsperson should change the MAC address in table MNCKTPAK to contain the CEM MAC address as per NTP - **NN10076-911**

60.2.3.3 MAC address of CEM card properly datafilled in table MNCKTPAK

The CEM card will recover to service either through BootP framework or through the Mate CEM with autonomous mate loading based on which request (BootP request or Mate Fallen signal) is processed first on the Call Server.

60.2.4 CEM card replaced in Non-BootP suppressed node with Mate CEM not available

60.2.4.1 MAC address of CEM card is not present in table MNCKTPAK

- a. BootP reply will not be sent by the Call Server.
- b. BOOT201 log will be generated to indicate that MAC address to IP address mapping could not be found.

- c. The CEM card will autoboot from Flash but cannot recover to in-service since it does not have the correct node addressing information.
- d. This incorrect node addressing will not result in an outage of another MG4K node in the office.
- e. CEM will be recovered by correcting the MAC address in datafill as per NTP - NN10076-911.

60.2.4.2 MAC address of CEM card present in table MNCKTPAK but against a different MG4K node

- a. QUNI the CEM unit on which the BootP request is made. Reject the BootP request if the CEM unit is in software and accept the BootP request if the CEM unit is in firmware.
- b. If BootP request is rejected, a BOOT201 log will be generated if permission denial exceeds throttle number to indicate that BootP request was denied permission.
- c. Allow the CEM unit at firmware to recover through BootP.
- d. BootP reply will not reach the CEM card that is replaced.
- e. The CEM card will autoboot from Flash but cannot recover to in-service since it does not have the correct node addressing information.
- f. This incorrect node addressing will not result in an outage of another MG4K node in the office.
- g. CEM will be recovered by correcting the MAC address in datafill as per NTP - NN10076-911.

60.2.4.3 MAC address of CEM card properly datafilled in table MNCKTPAK

The CEM card will send a BootP request. QUNI the CEM card when the BootP request is made, if the card is at firmware then accept the request. Node address and load information is provided by BootP framework and the CEM card recovers to in-service.

This feature provides the functionality to detect MAC address mismatch between datafilled value in table MNCKTPAK and actual MAC address of the CEM card. A SPM 313 log on the Call Server and a NODE 300 log on the CEM is generated when the MAC address mismatch is detected.

RTS operation on the CEM card will take the CEM to ISTB state immediately if a MAC address mismatch is present followed by a response to MAP to indicate the reason as MAC mismatch. QUERYPM FLT REASON is enhanced to display MAC address mismatch.

60.3 Hardware Requirements or Dependencies

None.

60.4 Software Requirements or Dependencies

This functionality needs SN08 loads on the Call Server and MG4K21 CEM loads on MG4K SPMs.

60.5 Limitations and restrictions

- a. This functionality is applicable only on MG4K nodes.
- b. LCI shall be used for provisioning node address and load information during simultaneous replacement of both CEM cards or during initial commissioning.
- c. Whenever MAC mismatch is found please refer NTP document (NN10076-911 **MG4000 Fault Management**) for steps to correct the mismatch.
- d. When a MAC address mismatch is found on a CEM card, no maintenance operations on that CEM should **not be performed**. Due to MAC address mismatch, the command could cause an outage on another CEM unit in the office. MAC address mismatch must be first corrected before any maintenance operations are performed.

60.6 Interactions

None.

60.7 Glossary

Term	Description
CEM	Common Element Module
MG4K	Media Gateway 4000 (SSPM)
LCI	Local Craft Interface
BootP	Bootstrap Protocol
MNCKTPAK	Managed Node Circuit Pack
ISTB	InService Trouble state
MOP	Method Of Procedure
MAC	Media Access Control

60.8 References

NN10076-911 Title: MG4000 Fault Management Ver:6.2 (NTP document for replacing CEM card in MG4K node)

61: A00007244 excerpts from test plan

61.1 Feature name

GIC and GIAC Support on CICM and MG9K

61.2 Feature Overview

61.2.1 GIC Feature Overview

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 ten members, 1000 members, or 10 000 members. End users in a ten 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.

To activate MBS Group Intercom, the end user presses the GIC key. The end user dials the correct number of digits. If the call terminates on another MBS, the system rings the GIC key associated with the originating GIC group. The called party must press the GIC key to answer. If the call terminates on a Unity or 500/2500 set, the called party goes off-hook to answer the call. Digits dialed after the end user presses a GIC key appear as dialed. Calls incoming on a GIC key display the GIC member number of the originator.

61.2.1.1 GIC Individual Paging

Individual GIC paging provides for one member of a group intercom (GIC) groups, using the GIC key of MBS set, to activate built-in alerting speaker of another GIC group member's MBS for paging purposes. Both GIC group members must be in same GIC group.

To use GIC individual paging feature, the caller presses the GIC key and dials appropriate GIC member number. Following the first ring, the caller again presses the GIC key. A one-way connection is established, and the caller can then talk over speaker. The called group member can establish a two-way conversation by either pressing the ON key of the handsfree-unit or by lifting the handset.

GIC Individual Paging feature requires GICPAGE option in table CUSTSTN for related customer group

61.2.1.2 GIC and SERVORD command

The assignment of option GIC to an MBS using the ADO command appears in the following SERVORD example. Assignment of option GIC occurs to key

5. The designated name of the line is SMITH. The GIC member number (GICMEMNO) is 24. The SMDR records are a requirement.

SERVORD example for MBS Group Intercom in no-prompt mode

```
>ADO $ 2 0 1 25 2 GIC SMITH 24 Y N $
```

QGRP show the output of GIC group:

```
>qgrp gic HOST 02 0 01 26 4
```

```
SORT_BY_LEN_OR_MEM: LEN
```

```
>len
```

GIC GROUP

```
-----
```

```
HOST 02 0 01 26      KEY 4      MEMBER 23
  DN 1027835002
```

```
HOST 02 0 01 25      KEY 2      MEMBER 24
  DN 1027835001
```

The number of members in the GIC GROUP "SMITH" is 2

61.2.2 GIAC Feature Overview

Group Intercom All Call (GIAC) allows an MBS end user to page up to 100 members (with MDC00077 SOC option) for one-way speech path and up to 30 members for two-way speech path in his or her designated Group Intercom (GIC) group simultaneously, and establish a conference with the paged members. This functionality is extremely useful in situations where common announcements need to be broadcast to several individuals in the same GIC group. These individuals must be equipped with Meridian business sets (MBS). An individual group member hears the page over his or her own set's built-in speaker, and can (when required) respond to the originator.

To activate **manual** GIAC paging, a member lifts the handset, presses the GIC key, and presses the octothorpe (#) key on the dial pad. The member who activates GIAC is known as the originator of the call. Then originator presses GIC key again to start paging. When GIAC is activated, a conference bridge is established, and each member of the GIAC group is placed on a port of the conference circuit. The paged group members can establish a two-way conversation by either pressing the ON key of the handsfree-unit or by lifting the handset.

To use **automatic** GIAC paging (PAGING field is datafilled as “Y”), a member lifts the handset, presses the GIC key. The member who activates GIAC is known as the originator of the call. Then when GIAC is activated, a conference bridge is established, and each member of the GIAC group is placed on a port of the conference circuit. The paged group members cannot establish a two-way conversation by either pressing the ON key of the handsfree-unit or by lifting the handset. Automatic GIAC paging only supports one-way speech path (from originator to paged members).

To use automatic paging function of GIAC feature, MDC00077 SOC implemented by activity A0004007 status should be set to ON.

In order to use GIAC, an individual with an MBS must be a member of an intercom group that has GIAC datafilled in Table KSETFEAT (Business Set and Data Unit Feature). When a member activates GIAC, the other members that belong to the same GIAC group are paged. A GIAC group can have a maximum of 100 (with MDC00077 SOC option) members (including the originator).

61.2.2.1 GIAC and SERVORD command

The following SERVORD example shows how Group Intercom All Call is added to a line using the ADO command.

SERVORD example for MBS Group Intercom in no-prompt mode

```
>ADO $ 02 0 01 25 2 GIAC 7 Y N $
```

QGRP show the output of GIAC group:

```
>qgrp
```

```
GRP_TYPE:
```

```
>giac
```

```
LEN_OR_LTID:
```

```
>HOST 02 0 01 26
```

```
KEY:
```

```
>4
```

```
GIAC GROUP
```

```
-----
```

```
HOST 02 0 01 25      KEY 2      MEMBER 24
```

```
HOST 02 0 01 26      KEY 4      MEMBER 23
```

```
THE NUMBER OF MEMBERS IN THE GIAC GROUP "7" IS 2
```

62: A00007250 Functional description (FN)

62.1 Feature name

ACDMIS Over TCP

62.2 Description

The ACDMIS feature provides informational ACD messaging concerning ACD events that are occurring on the DMS-100/CS2K to a downstream processor (DSP). Currently, the ACDMIS connectivity between the DMS-100/CS2K and DSP is via an X.25 link that is implemented on the DMS-100/CS2K through an MPC (Multi-Protocol Controller) card in the IOC (Input-Output Controller) module using X.25 protocol.

This SN08 activity will implement the necessary changes to enable the transport of ACDMIS messaging over TCP/IP to a DSP. The new TCP/IP transport will be in addition to the X.25 transport that already exists. The new TCP/IP transport will interface to the ethernet network via the EIU (Ethernet Interface Unit) or via the ethernet port that resides on a Call Agent card for the CS2KCompact.

62.2.1 Functional Overview

The ACDMIS link is a messaging interface provided by the DMS-100//CS2K to the host MIS computer (or DSP). The information carried across the messaging link allows ACD applications running on the DMS-100/CS2K to communicate with MIS applications running on the host computer. The two-way information flow allows the DMS and host computer to provide enhanced services to an ACD customer.

This feature will provide an ACDMIS link between the switch and the host computer using the TCP/IP protocol via EIU or Call Agent card that uses port 2700. This TCP/IP link may be used as an alternative to the X.25 MPC ACDMIS link. The transport (TCP/IP vs. MPC X.25) used is transparent to any application using the ACDMIS link to communicate with a host computer.

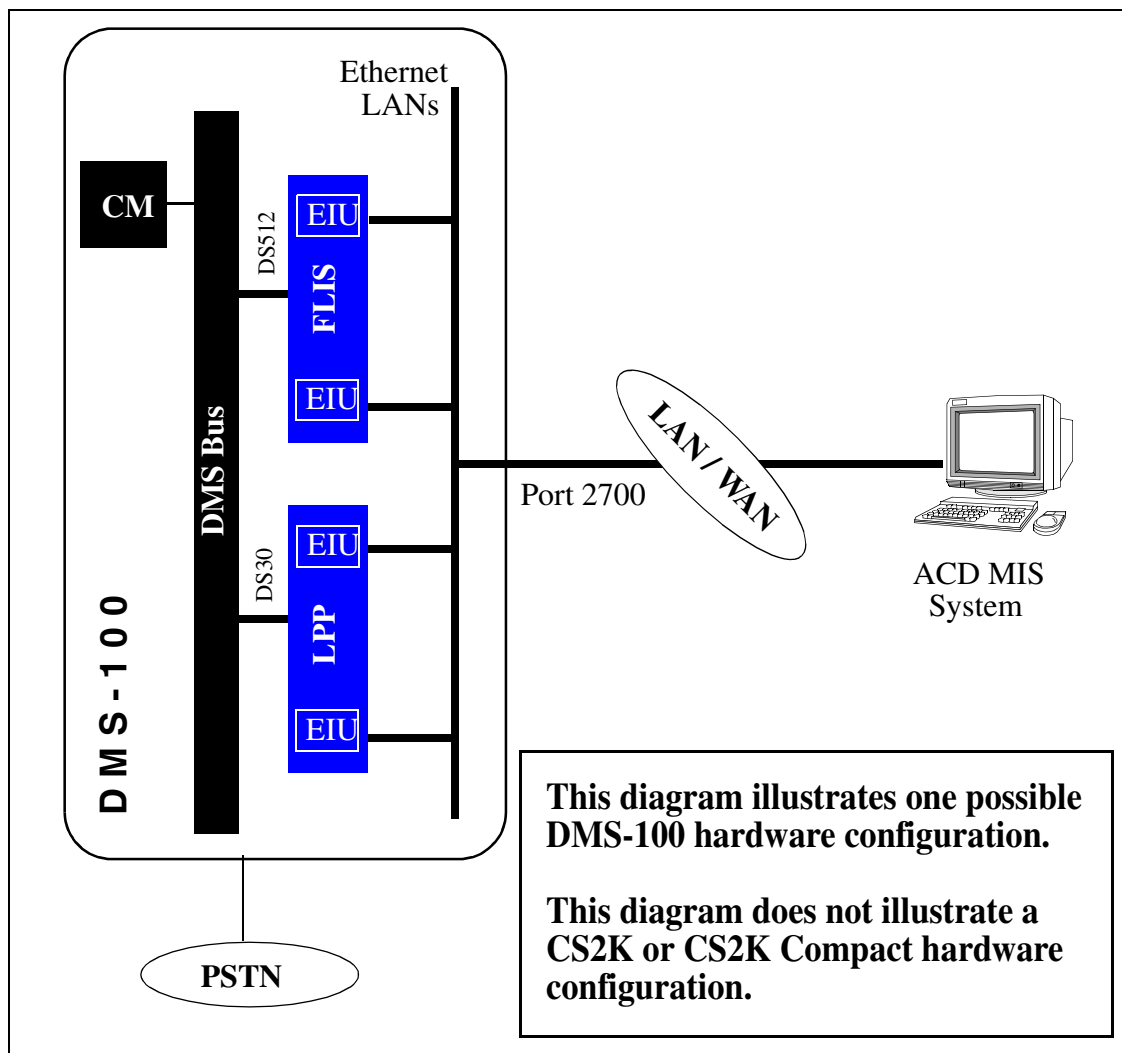
The functional areas of the feature are:

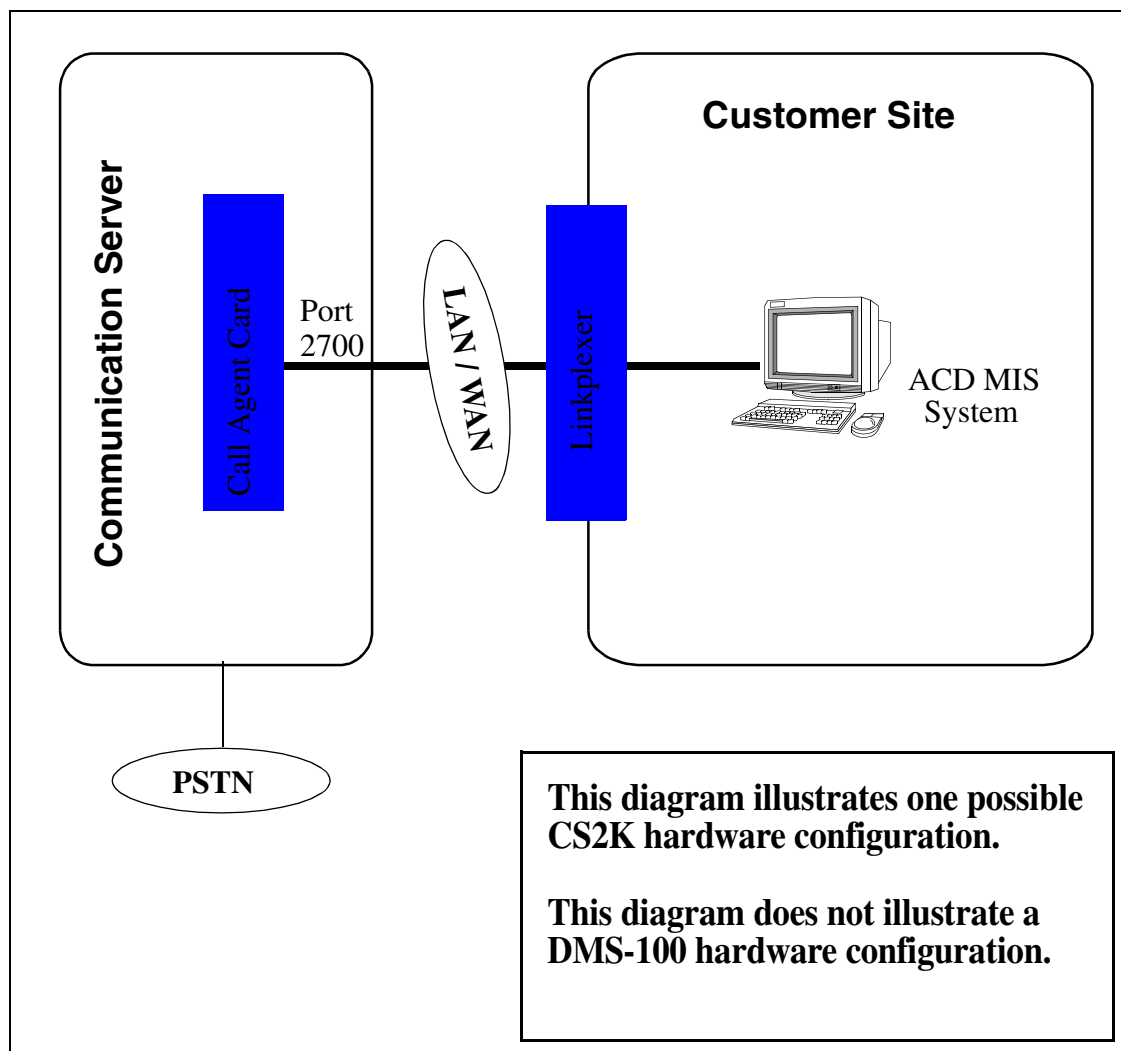
- **TCP/IP transport:** TCP/IP connectivity between the DMS-100/CS2K and the remote DSP through the EIU or Call Agent card on the switch and network access.
- **Table Control:** ACDMIS link datafill to support either X.25 or TCP/IP transport via the ACDMISPL table.
- **Operational Measurements:** There are no functional changes as a result of this feature however, existing ACDMIS OMs will be updated / pegged as necessary.

62.2.2 Hardware

The X.25 protocol is currently available on the DMS using the Multi-Protocol Controller (MPC 1X89AA/BA card). The MPC is a downloadable input/output device that resides on a DMS I/O Controller (IOC) shelf. The MPC has two programmable data communication links. The MPC accomplishes real time savings in the CM by performing low-level data communications functions.

The TCP/IP transport uses the existing TLI interface to provide connectivity between the DMS-100/CS2K and a DSP. The DMS is provided with Local Area Network (LAN) connectivity by an Ethernet Interface Unit (EIU) or in the case of a CS2KCompact, the Call Agent card. This activity will utilize port 2700 for incoming and outgoing TCP message traffic. Messages originated from the DSP are routed via the network and terminate on the EIU/Call Agent which forwards the messages to the destination port (2700) on the DMS. For some hardware configurations internet routers may be used between the DMS-100/CS2K and DSP.





62.2.3 Software

This feature enhances existing ACDMIS software to handle the following areas:

- TCP/IP Transport.
- Table Control mechanism to support TCP/IP transport.
- OMs and Logs specific to the TCP/IP transport.

62.2.4 TCP/IP Transport

- **TCP and X.25 ACD MIS Message Components**

ETHERNET HEADER		LAPB HEADER
IP HEADER		INFO FRAME
TCP HEADER		X.25 HEADER
ACDS MIS MESSAGE		X.25 DATA
		ACD MIS MESSAGE
TCP/IP Message		X.25 Message

- **TCP connection checking**

For this feature the ACDMISPL table will be modified to include a LNKSEL type of either X25 or TCP that will be associated with each datafilled pool. The LNKSEL field for a TCP connection will contain a “TCP” designation as well as the remote ACD System’s IP Address, an Alternative ACD System IP Address, a User ID and a Login Password¹.

Prior to establishing a TCP connection, the DMS-100/CS2K will crosscheck the incoming remote ACD System’s IP address against those IP addresses that are datafilled in the ACDMISPL. The incoming remote ACD System’s IP address must match either the IP Address or Alternative IP Address that is datafilled under the LNKSEL field for a given Pool in table ACDMISPL. Only one ACDMIS link/session is allowed per datafilled Pool.

If the incoming remote ACD System’s IP address is verified the events to establish a TCP connection will proceed, otherwise the connection will not be allowed.

- **Establishing a TCP connection**

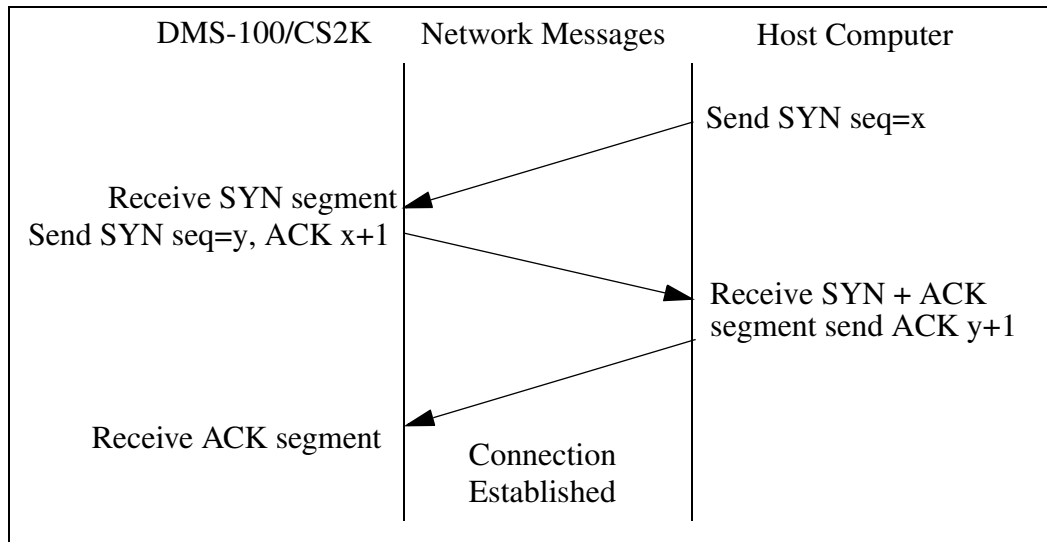
Establishing the base TCP connection is a function of the existing base TCP/IP layers which will not be impacted by this feature. The following is provided as informational only and not as an indication of the work being done by this feature.

To establish a connection, TCP uses a three-way handshake. The DMS-100/CS2K will wait passively for the handshake that is initiated by the remote host (DSP) application.

¹Please see Section 1.2.5 for details on the table control changes associated with table ACDMISPL.

The IP address and the port number of the DMS-100/CS2K will be needed by the remote host application in order to establish a connection. Initially a SYN segment is sent by the host computer application requesting a connection to the DMS-100/CS2K. The DMS-100/CS2K will then send an acknowledgment along with the SYN segment to the ACDMIS subscriber to indicate that it is ready to establish a session. The Host computer of the subscriber will then send an acknowledgment. Once the DMS-100/CS2K receives the acknowledgment, the connection is fully established as shown in Figure 1 below.

Figure 1 Sequence of messages in Three way handshake.



- **Establishing an ACDMIS Session**

When establishing the ACD MIS Session the remote ACD MIS System must initiate a nosLogon¹ message that is sent to the DMS-100/CS2K.

The nosLogon message contains the following arguments: Protocol Version, Userid, Password and Profile. As a result of this feature it is required that the Userid and Password that is sent in the nosLogon message match the Userid and Password that has been datafilled in table ACDMISPL² for a given Pool.

Other standard existing DSP Control messaging i.e. dspAssociatePool, dspRequestInit, dspStartTransfer etc. will be used to establish and setup the ACDMIS Session once the base TCP connection has been made.

- **Terminating TCP connection**

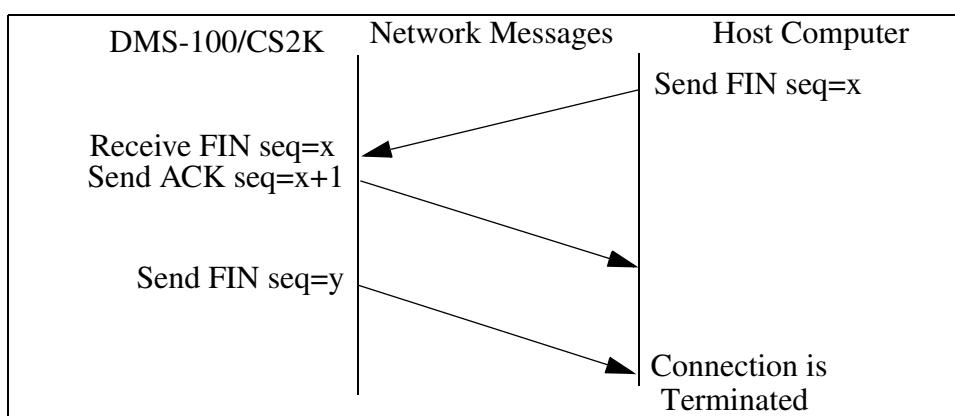
¹Please reference the NT NIS-Q209-2 ACD-MIS Interface Specification for detailed information on the nosLogon message and related arguments.

²Please see Section 1.3.5 for details on the table control changes associated with table ACDMISPL.

Terminating the base TCP connection is a function of the existing base TCP/IP layers which will not be impacted by this feature. The following is provided as information only and not as an indication of the work being done by this feature.

To close the TCP connection, the remote host application will send the FIN segment as shown in Figure 2. The DMS-100/CS2K acknowledges the FIN segment and acknowledges that no more data is available. Once the connection is closed by the remote host application, TCP refuses to accept more data from the remote host application. The DMS-100/CS2K will then send a FIN segment. When both directions have been closed, the connection is deleted.

Figure 2 Sequence of messages in terminating a TCP connection



- **TCP connection Reliability**

TCP connection reliability is a function of the existing base TCP/IP layers which will not be impacted by this feature. The following is provided as information only and not as an indication of the work being done by this feature.

TCP has a “Keep Alive” option consisting of an out-of-band packet which is sent during idle line conditions. This is mainly used to detect any connection failures. The default delay is 45 seconds before the keep alive packet is sent. The keep alive timer value is configurable between 5 to 60 seconds by the user application via the TLI mechanism. An acknowledgment must be received from the peer, or TCP will retransmit the keep alive packet three times with the delay equal to the maximum of Round trip time-out or 10 seconds. If the peer does not respond, the connection is closed.

62.2.5 Table Control Mechanism

The existing ACDMISPL table will be modified to define the relationship between the ACDMIS pool and the transport type, X.25 or TCP/IP. This

feature will introduce a new field named LNKSEL to the ACDMISPL table. The new LNKSEL field will be datafillable with either X25 or TCP with the TCP designation having additional refinements of an IP address that refers to the remote DSP, an Alternative IP address for the remote DSP, a UserID and a Password. The newly created LNKSEL field will serve a dual purpose of defining which remote IP addresses are allowed access to the DMS-100/CS2K as well as defining the relationship between the pool and session link.

• ACDMISPL Field Description

Table 1 ACDMISPL Field Description

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
POOL		n/a		ACD Pool Name
PASSWORD		n/a		Pool Password
PROTOCOL		n/a		ACD MIS Protocol Version
OUTEVENT		n/a	10 to 200	Message Buffers
BUNDLING		n/a	Y or N	Message Bundling
LNKSEL	NEW	n/a	X25 or TCP	Indicates whether this pool will use a X25 or TCP transport.
X25	NEW	n/a	n/a	If X25 is chosen no additional refinements are needed as existing X25 tables and datafill are used.
TCP	NEW	IP_ADDR	IP Address	If TCP is chosen an additional refinement is required to indicate the remote systems IP Address.
	NEW	ALT_IP_ADDR	IP Address	Refinement to allow an alternative or “back-up” IP Address for the remote system.
	NEW	USER_ID	Alphanumeric >=5 and <= 8 Characters	Mandatory refinement which will be used to verify the Userid field of the nosLogon message.
	NEW	LOGIN_PASSWD	Alphanumeric >=5 and <=16 Characters	Mandatory refinement which will be used to verify the Password field of the nosLogon message.

• ACDMISPL - LNKSEL Field Information

The TCP refinement to the LNKSEL field allows datafilling of an alternative IP Address (ALT_IP_ADDR) to be used as a “back-up”. If there is no alternative IP Address the ALT_IP_ADDR field should be datafilled with the same address used for the IP_ADDR field. Historically

only one link is allowed per ACD Pool, therefore only one IP Address per ACD Pool is allowed to be active at any given time.

The TCP refinement to the LNKSEL field includes the mandatory refinements USER_ID and LOGIN_PASSWD that will be used for login validation in conjunction with the nosLogon message that is sent by the DSP.

LNKSEL field datafill changes from X25 to TCP/IP or TCP/IP to X25 will require the ACDMIS link to be brought down and may require datafill changes to other X25 related tables as needed.

- **ACDMISPL Table Enhancement Example**

TABLE: ACDMISPL

POOL PASS	PROTOCOL	OUTEVENTBUND	LNKSEL
POOL01POOL01	BCS43		110NX25
POOL02POOL02	BCS43		110N
TCP 47 245 5 247 246 6 3	USER2	PASS2	

- **ACDMISPL Datafill Example for TCP Transport**

POOL:

>ACDPOOL

PASSWORD:

>PASSWD1

PROTOCOL:

>BCS35

OUTEVENT: 200

>110

BUNDLING:

>N

LNKSEL:

>TCP

IP_ADDR:

>47 245 5 2

ALT_IP_ADDR:

>47 246 6 3

USER_ID:

>USER2

LOGIN_PASSWD:

>PASS2

TUPLE TO BE ADDED:

ACDPOOL PASSWD1 BCS35 110 N TCP 47 245 5 2 47 246 6 3 USER2

PASS2
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

- **ACDMISPL Datafill Example for X25 Transport**

POOL:
>ACDPOOL
PASSWORD:
>PASSWD1
PROTOCOL:
>BCS35
OUTEVENT: 200
>110
BUNDLING:
>N
LNKSEL:
>X25

TUPLE TO BE ADDED:
ACDPOOL PASSWD1 BCS35 110 N X25
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

62.2.6 Operational Measurements

This feature makes no functional changes to ACD MIS OMs, however the ACD MIS related OMs as described below will be updated / pegged as necessary using the new TCP transport.

62.2.6.1 ACDMISPL - OM Group

The ACDMISPL OM Group will not be impacted by this feature. The following is provided as information only and not as an indication of the work being done by this feature.

The OM group ACDMISPL monitors the ACD MIS output message buffer and provides buffer usage and peg count registers for messages lost or transmitted. The following is a brief description of the ACDMISPL OM registers:

- **MISLOST:** Pegs the number of valid MIS event messages that fail to enter the outgoing message buffer because the buffer is full. The message is subsequently discarded and no retransmission is attempted and further buffering is offered.
- **MISQUSAG:** Records the number of messages waiting to be transmitted in the outgoing message buffer every 100 seconds. Under normal traffic conditions, MISQUSAG should be zero since all messages are dispatched as soon as they enter the outgoing message buffer.

- **MISTRANS:** Pegs the number of valid outgoing messages that are transferred successfully to the MIS downstream processor via the X.25 data link through the MPC/EMPC card. The register counts each call event, return_result, or initialization message that is transmitted.

62.3 Software Requirements or Dependencies

Not Applicable

62.4 Limitations and restrictions

- Maximum number of TCP/IP connections to a single DMS-100/CS2K is 96.
- The number of ACDMIS TCP/IP Links per single DMS-100/CS2K will be limited to 60.

62.5 Interactions

Not Applicable

62.6 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__

Performance (includes operational measurements) __N/A__

62.7 Glossary

Table 2

Term	Description
3PC	Third Party Core

Table 2

ACD	Automatic Call Distribution
CS2K	Communication Server 2000
DMS	Digital Multiplex System
DSP	Down Stream Processor
EIU	Ethernet Interface Unit
IOC	Input-Output Controller
IP	Internet Protocol
MIS	Management Information System
MPC	Multi-Protocol Controller
OM	Operational Measurements
TCP	Transmission Control Protocol
TLI	Transport Layer Interface

63: A00007253 excerpts from the test plan

63.1 Feature name

MADN Ring Forward Support for CICM and MG9K

63.2 Feature Overview

63.2.1 MADN description

A directory number (DN) that is assigned to more than one business set or single line set is called a MADN. The telephone sets that are assigned this DN form a MADN group. MADN groups can be comprised of 2 to 32 members and configured in either a single call arrangement (SCA) or multiple call arrangement (MCA). The option MDN must be assigned to the telephone line appearance.

63.2.2 Single call arrangement (SCA)

Single call arrangement allows only one call to be active on the SCA group. The active call may be an origination by a SCA member or an incoming call presented to all the SCA members. The originator or answering member will have privacy on the call that excludes all other members. The lamps associated with the SCA appearances on all business set members will be on. The call will remain private, with the active member controlling the option, privacy release (PRL). When the controlling member depresses the PRL key or dials the privacy release activation code (PRLA), the other members will be notified by a blinking lamp associated with the SCA appearance. Upon activation of privacy release, one SCA member may conference into the call.

The MADN ring forward (MRF) option provides four ringing options for calls offered to SCA groups. The ringing options are:

- **abbreviated** - the line appearance rings from call termination until the timer expires.
- **delayed** - the line appearance rings after the timer expires.
- **always** - the line appearance rings from the time the call terminates until it is answered or the caller abandons the call.
- **never** - the line appearance does not ring when a call terminates on the SCA group.

The timer that controls the delayed or abbreviated ring is set on a SCA basis. (0 or 12-60 seconds).

The MADN ring forward manual (MRFM) option provides for the forwarding of ringing of SCA group appearances. The MRFM option allows a station with

MRF and the abbreviated ringing option to manually stop its ringing before the timer expires. This is done by pressing a MRFM key. Once the MRFM key is pressed any set with the delayed ringing option begins to ring. MRFM is a subset feature. Therefore, each DN that requires this manual capability must be key listed when this feature is assigned to the business set. One business set can have several MRFM keys. The MADN ring forward (MRF) option must be assigned to the SCA group before an appearance of that SCA may be assigned to the keylist of the MRFM key.

63.2.3 MADN Ring Forwarding and SERVORD command

The following SERVORD example shows how MADN Ring Forward is added to an existing SCA MADN line using the SERVORD ADO command. The group is assigned MRF. The system prompts the end user for the MRF_RING to assign special ringing to the MADN group member.

SERVORD example for Assigning MADN Ring Forward to an existing SCA MADN line in prompt mode.

```
> ADO
SONUMBER :      NOW      92      1      2      AM
>
DN_OR_LEN:
>00 0 00 04
OPTKEY:
>1
OPTION:
>MRF
AUTO:
>Y
MRF_TIMER:
>12
MRF_RING:
>ABBR
OPTKEY:
>$
```

SERVORD example for MADN Ring Forward in no-prompt mode

```
> ADO $ 00 0 00 04 1 MRF Y 12 ABBR $
```


The following SERVORD example shows how MADN Ring Forward is added to an existing SCA MADN line using the SERVORD ADO command. The group is assigned MRF. The system prompts the end user for the MRF_RING to assign special ringing to the MADN group member.

SERVORD example for Assigning MADN Ring Forward to an MBS key in prompt mode

```
> ADO
SONUMBER :      NOW      90      1      2      AM
>
DN_OR_LEN:
>02 01 02 22
OPTKEY:
>5
OPTION:
>MRFM
KEYLIST:
>1
KEYLIST:
>2
KEYLIST:
>$
KEYLIST:
>$
```

SERVORD example for MADN Ring Forward Manual in no-prompt mode

```
> ADO $ 02 01 02 22 5 MRFM 1 2 $ $
```

64: A00007262 Functional description (FN)

64.1 Feature name

CS2K Capacity Enhancements for Large VoIP VPN Deployments

64.2 Description

Activity A00007262 (CS2K Capacity Enhancements for Large VoIP VPNs), is intended to increase the number of PRI D-channels from 2176 to 4094, for the CS2K (DMS100). The functionality provided by this feature is to help address the need for accommodating gateways in excess of the current limits of 2176, on a per CS2K basis.

Table 1 SN08 changes due to feature A00007262

Max Parameter	SN07	SN08 (due to A00007262)
GWCs per CS2K	60	60
D-Channels per CS2K	2175	4094
H.323 GWs per CS2K	2175	4094
D-Channels per GWC	254	254
H.323 GWs per GWC	254	254

64.3 Hardware Requirements or Dependencies

N/A

64.4 Software Requirements or Dependencies

N/A

64.5 Limitations and restrictions

Following are some of the assumptions made for this activity. Any work that may be needed to address the situations where any of these assumptions do not hold good, could need additional effort within or outside this feature activity.

- The messaging framework between CS2K and GWC, is assumed to be able to handle the messaging (including callp and maintenance) with the additional PRI D-channels and the consequently added B-channels.
- Upon system recovery, the recovery time for bringing up the PRI D-channels is supposed to be within acceptable limits.
- The CM is assumed to be able to process callp and maintenance for these additional PRI D-channels and B-channels.

- The translations and routing framework is assumed to support the added PRI D-channels to the CS2K. Limitations with respect to the translations/routing (if any), will not be addressed under this activity.
- There are no GWC changes anticipated, considering that the current limits on the maximum PRI D-channels per GWC remains unchanged.

64.6 Interactions

N/A

64.7 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__

64.8 Glossary

Table 2

Term	Description
CS2K	Call Server 2000
VoIP	Voice over IP
VPN	Virtual Private Network
GWC	Gateway Controller
GW	Gateway

65: A00007263 Functional Description (FN)

65.1 Feature name

LCI for Gigabit Ethernet

65.2 Description

This feature will make the necessary modifications to the LCI software to support the new Gigabit Ethernet Network Interface for MG9K.

The LCI modifications (without affecting the existing functionalities of the SCO/SCI cards) for the new SCG (Super Core GigabitEthernet) card are as follows:

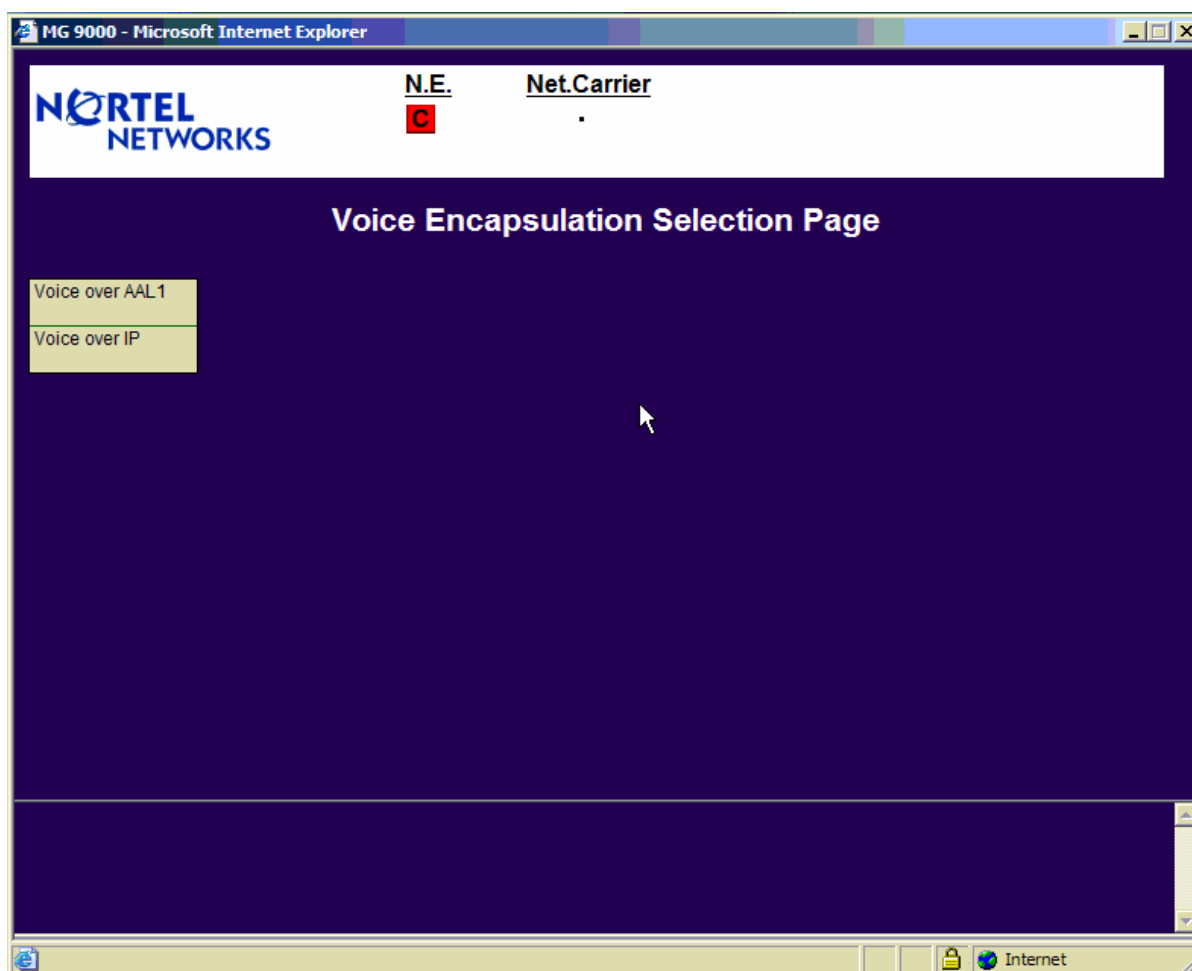
- 1 Card maintenance of the SCG card – which would be same as the existing SCO/SCI cards' Card-Maintenance
- 2 Carrier maintenance – where the new GigE link can be:
 - Provisioned – also includes the ability to request for auto-negotiation
 - Controlled – the admin and config state of the links can be controlled
 - Status can be viewed – the alarm(s) on the links will be displayed
 - Perform OOS (Out of Service) test and monitor Link-Integrity
 - Have Link Protection – to be able to set the working (preferred) and non-working (non-preferred) links and also enable/disable link-reversion
- 3 Connection side changes -- VLAN – to be able to provision (set the VLAN ids.), shape (set the peak rate) and also prioritize the different types of VLANS (OAMP, Bearer, Call-Control and for the fixed IP addresses of the SCG cards) from the connections button on the LCI.
- 4 Miscellaneous –
 - Dynamic updating of the alarm severities at the N.E and Net.Carrier links on LCI.
 - Update the following terms as applicable to GigE:

- ‘Carrier’ will be changed to ‘Link’
- ‘APS’ will be changed to ‘Protection’
- ‘Net.Carrier’ will be changed to ‘Net.Link’

Note: The following sub-sections explain the above modifications. Most of them contain screen-shots that are self-explanatory. Texts are added to explain the screens wherever necessary. They are not in any particular order.

65.2.1 Solution type selection

Since the SCO/SCI had support for both VoAAL1 and VoIP, the solution type selection was required when we login to LCI. Now, for SCG, it goes directly into VoIP as this is the only solution type supported on SCG cards. So the following screen will not appear in LCI for SCG cards.

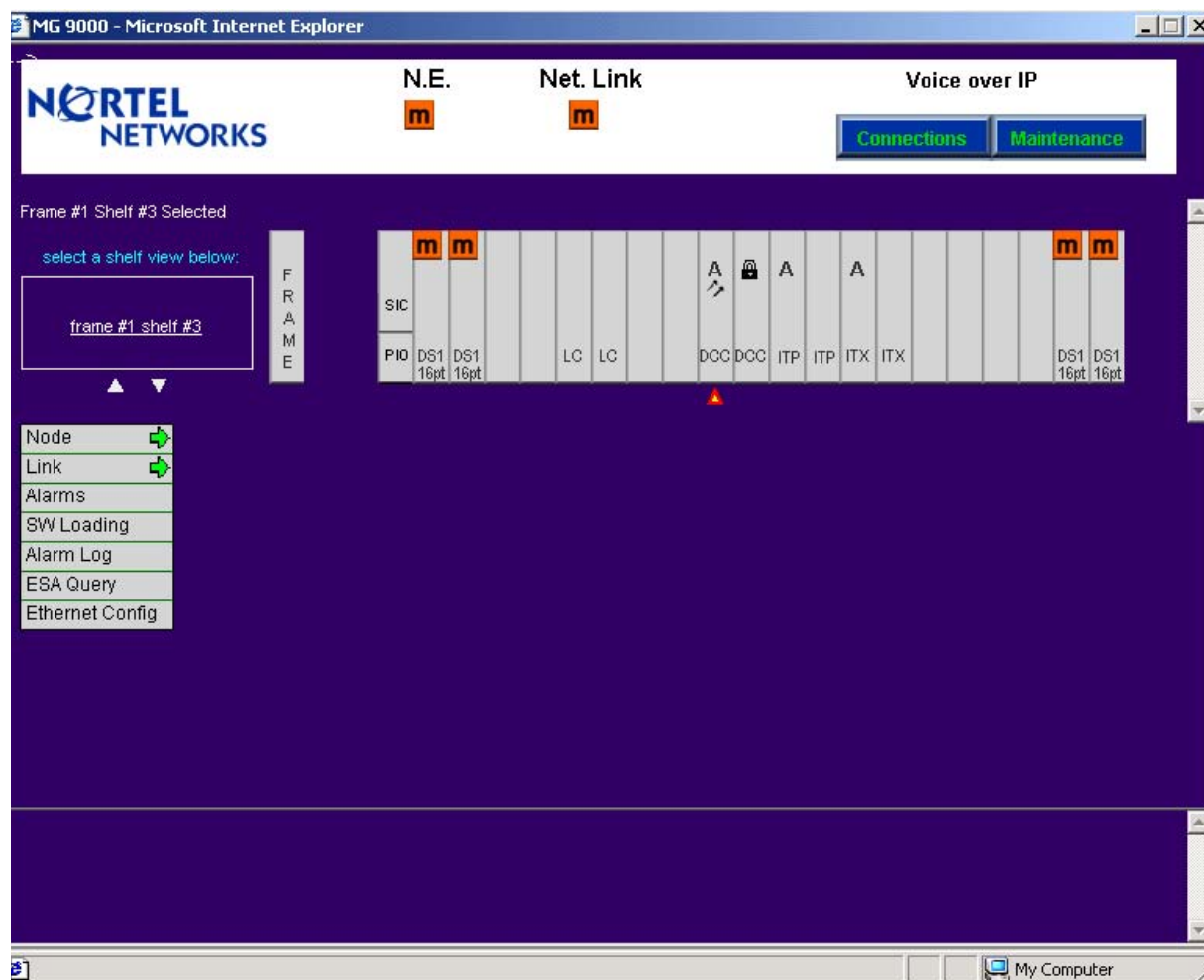


65.2.2 Change the terms

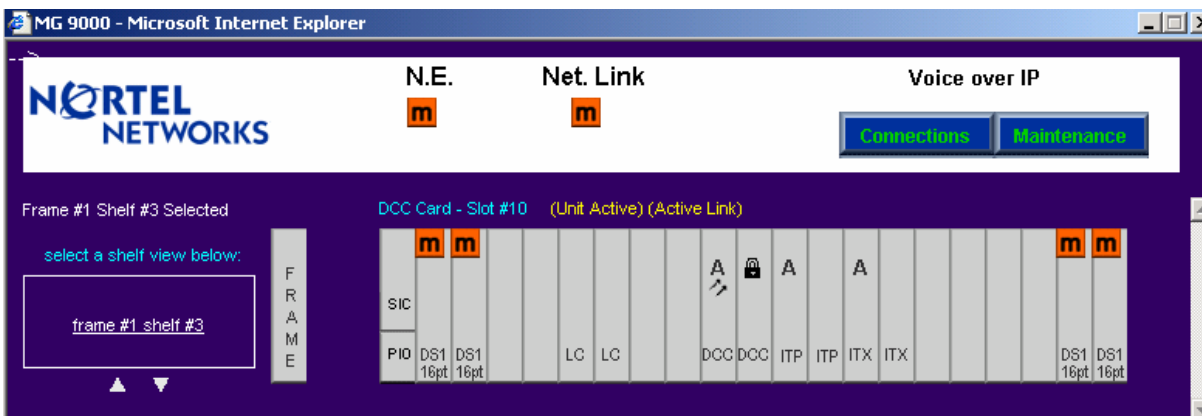
The term 'Net. Carrier' applies to SONET & SDH for SCO/SCI cards. But for SCG cards, this will be changed to 'Net. Link' as shown in the screen below:



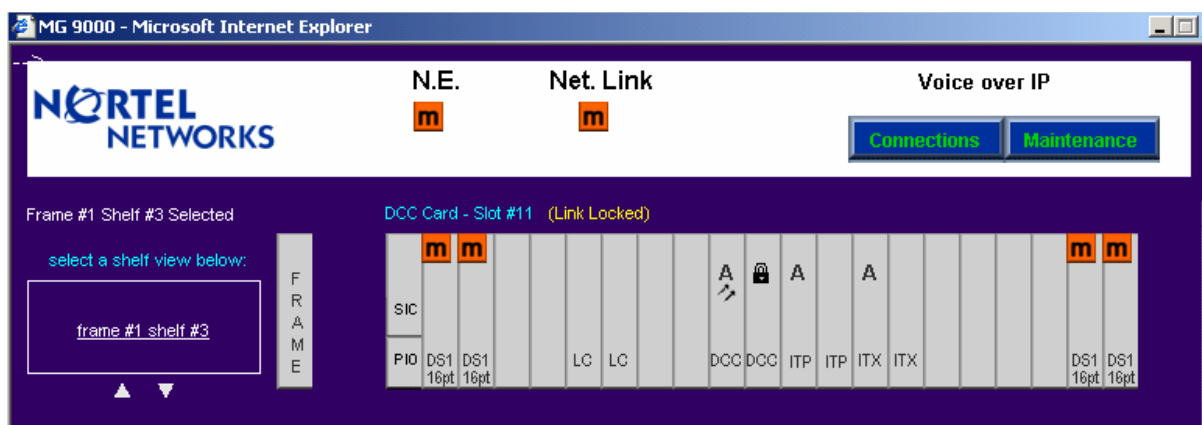
The menu items when you click on the DCC card will contain 'Link' instead of 'Carrier' as shown in the screen below:



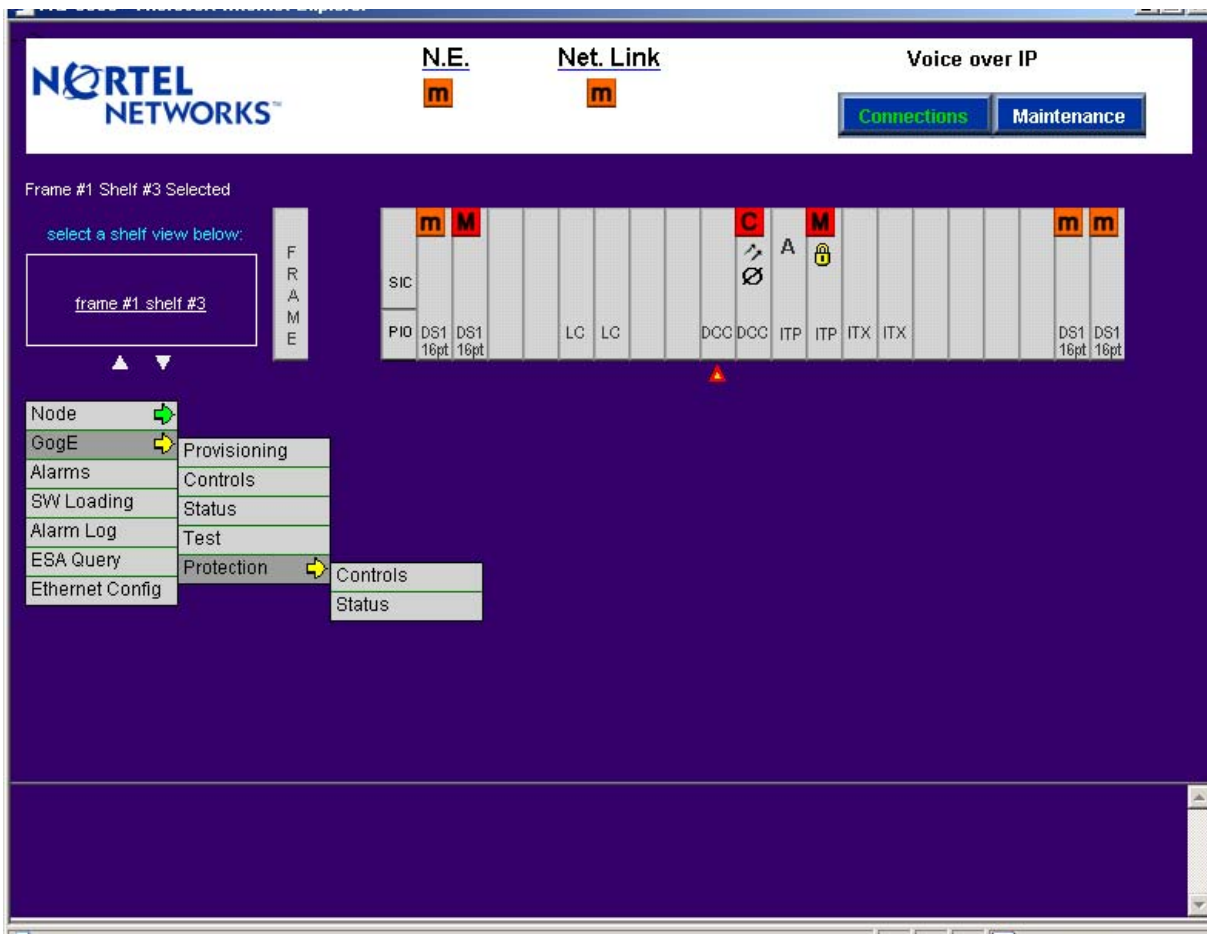
When the mouse is moved over the DCC card, the text that displays the information in yellow displays 'Active Link' instead of 'Active Carm.' as shown in the screen below.



When the link is locked a lock symbol is displayed on the DCC card and when the mouse is pointed on the card, the text 'Link locked' is displayed instead of 'Carm. Locked' as shown in the screen below:



The sub-menu option 'APS' under 'Carrier' on the DCC card will be changed to 'Protection' as shown in the screen below:

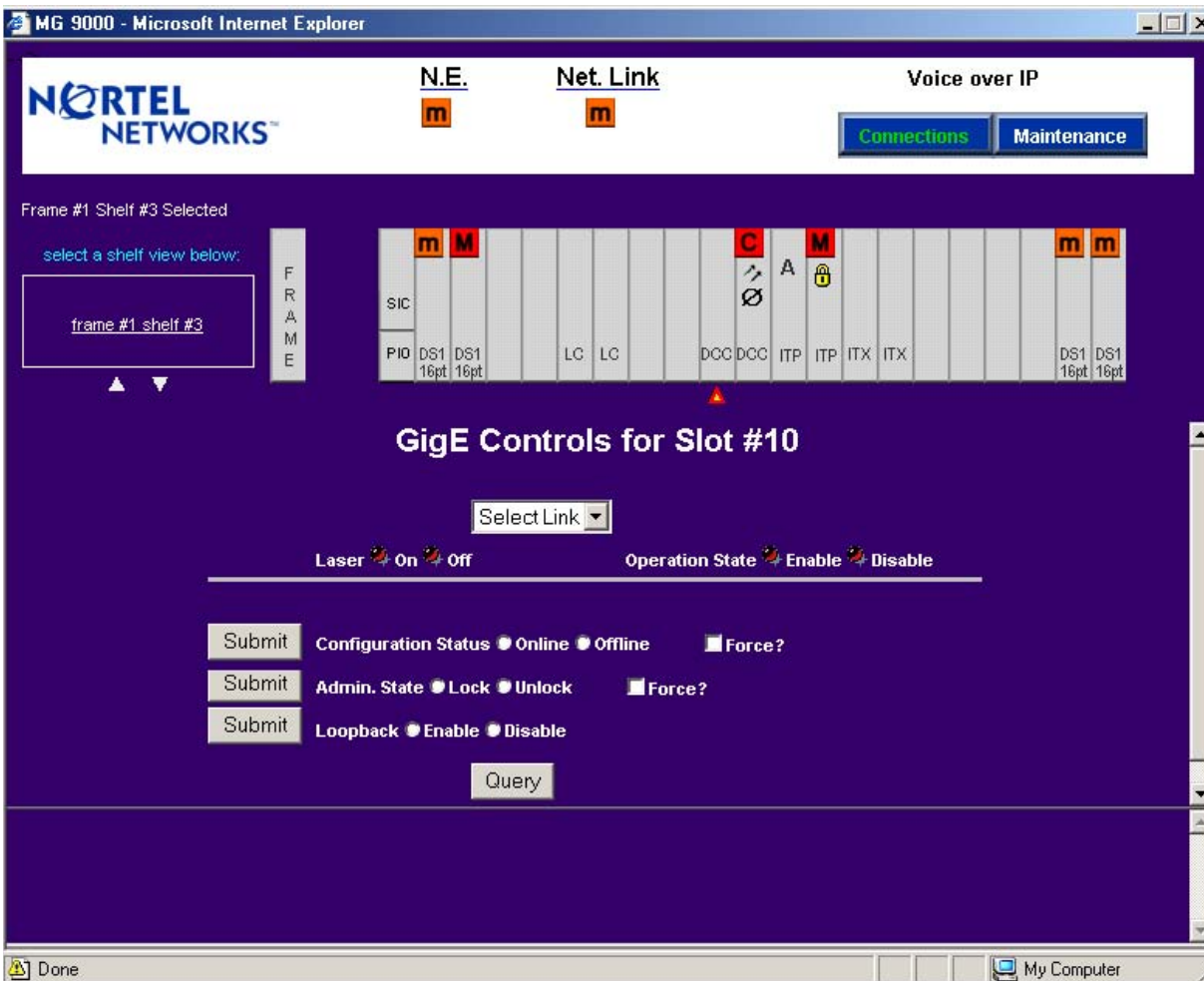


65.2.3 GigE Provisioning

The GigE provisioning screen will be as shown below. More details on each of the fields will be provided in the DSUM document.



65.2.4 GigE Controls



65.2.5 GigE Status

This page lists the alarms for GigE Links as shown below:

MG 9000 - Microsoft Internet Explorer

NORTEL NETWORKS™

N.E. Net. Link Voice over IP

Connections Maintenance

Frame #1 Shelf #3 Selected

select a shelf view below:

frame #1 shelf #3

querying status...

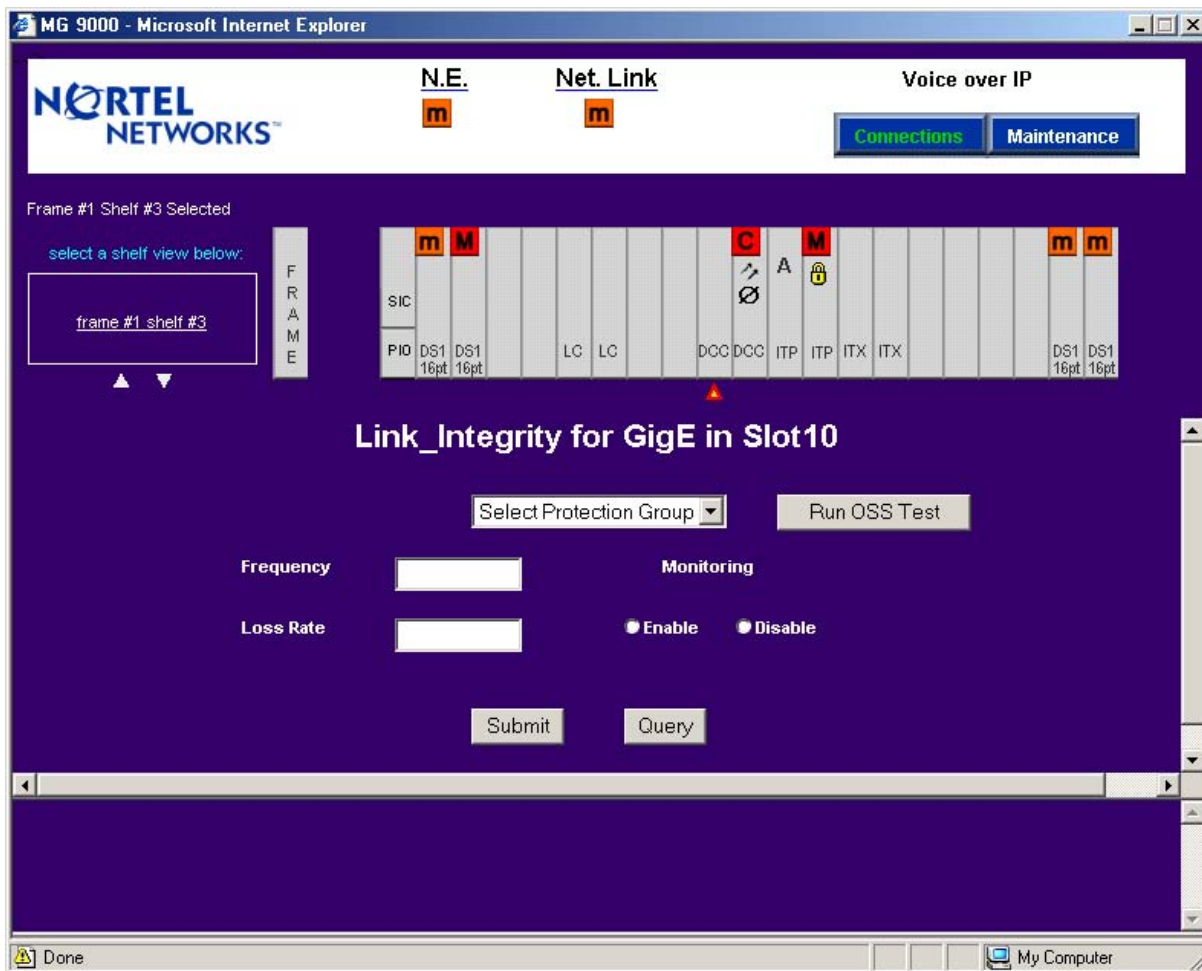
GigE Status for Slot #10

GigE#	Oper State	Admin State	Loopback	LOS	RFI	TX	AUTONE	RxEER	LINT	OPT	OPR	GARP	LKINT	TEM	POW	RxSD	TBC
GIGE 0	Up	Unlocked	NoLpbk	■	▲		■		■	▲		■		■	▲		■
GIGE 1	Up	Unlocked	NoLpbk	■	▲		■		■	▲		■		■	▲		■
GIGE 2	Up	Unlocked	NoLpbk	■	▲		■		■	▲		■		■	▲		■
GIGE 3	Up	Unlocked	NoLpbk	■	▲		■		■	▲		■		■	▲		■

Done My Computer

65.2.6 2.2.6GigE Test

The GigE Test page that is used for running the OOS test as well as to monitor link-integrity looks as below:



First the user needs to select the Protection-Group (which would have been configured in the protection-controls page).

Then, for the selected protection group the following can be done:

- Run the OOS test by clicking on the “Run OOS Test” button. After the test, the result will be displayed to the user.
- Setting the frequency, loss-rate and the Monitoring enable/disable by clicking on the SUBMIT button.
- Read the values previously set for the fields Frequency, Loss-rate and Monitoring Enabled/Disabled by clicking on the QUERY button. Note that this will not be able to get the result of the OOS Test.

65.2.7 GigE Protection

The GigE Protection contains 2 sub-menus - Controls and Status.

The Controls screen looks as below:

MG 9000 - Microsoft Internet Explorer

NORTEL NETWORKS™

N.E. Net. Link Voice over IP

Connections Maintenance

Frame #1 Shelf #3 Selected

select a shelf view below:

frame #1 shelf #3

FRAME

SIC	PID	DS1 16pt	DS1 16pt	LC	LC	DCC	DCC	ITP	ITP	ITX	ITX	DS1 16pt	DS1 16pt

Link_Protection control for GigE in Slot10

Group No. Group Type Working link Protection link

Select Group Type Select Working Link Select Protection Link

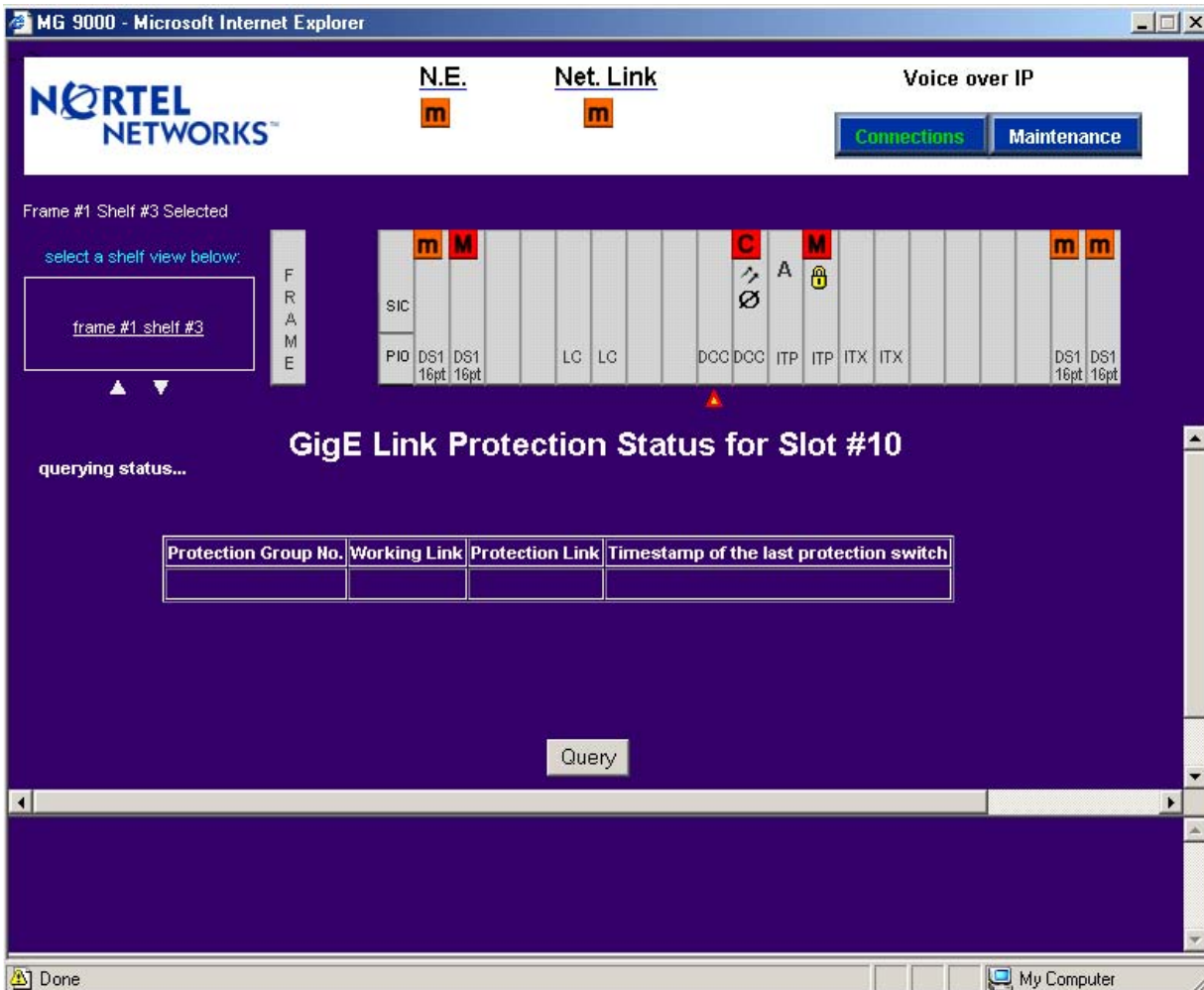
Link reversion ☐ Enable ☐ Disable

Wait To Restore

Submit Query

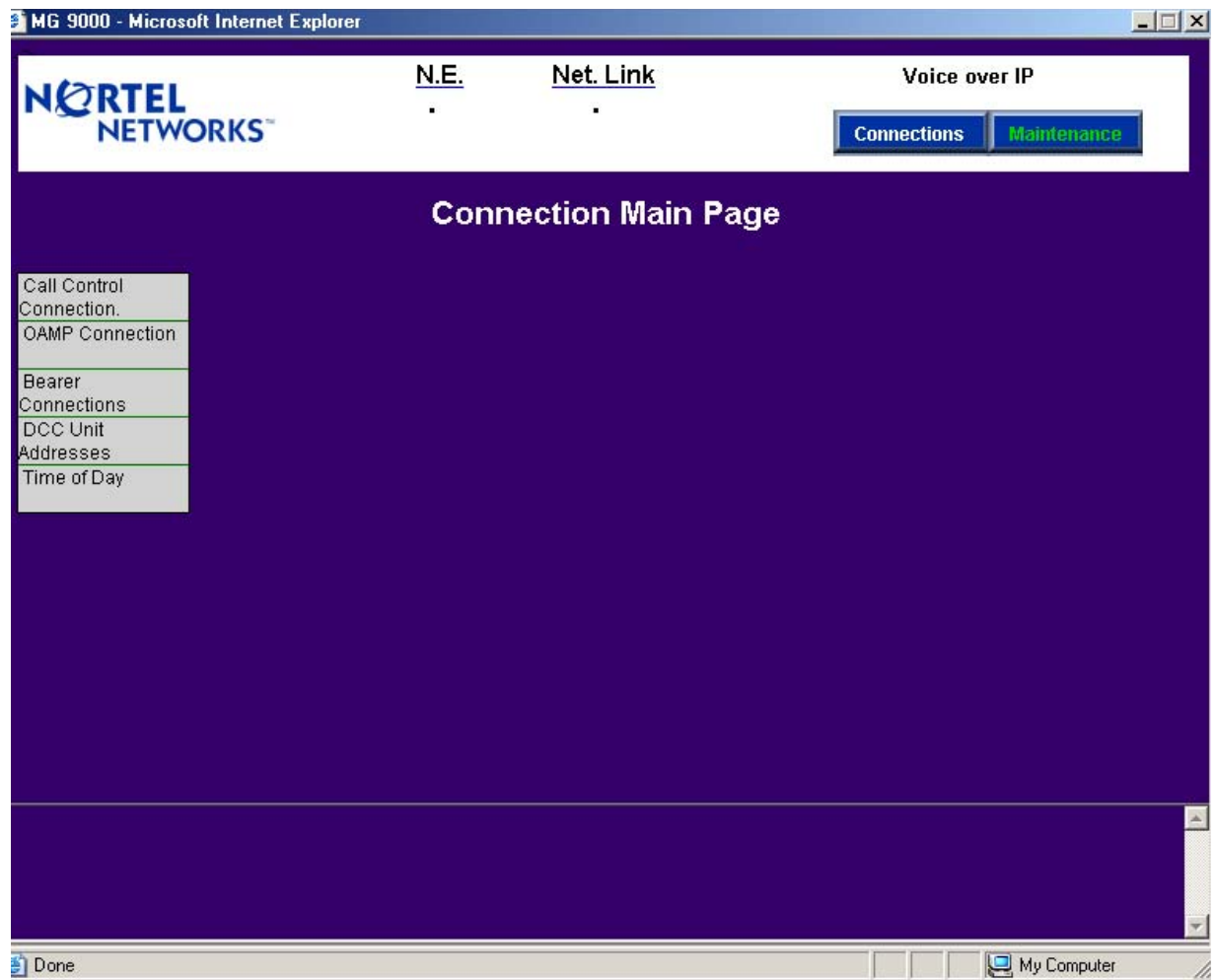
Done My Computer

The Status screen looks as below:



65.2.8 VLAN

The Connections menu will be changed to the following options as shown in the screen below:



The Call Control screen will look as below:

The screenshot shows a web browser window titled "MG 9000 - Microsoft Internet Explorer". The page has a dark blue header with the "NORTEL NETWORKS" logo on the left. In the center of the header, there are two labels: "N.E." and "Net. Link", each followed by a period. On the right side of the header, there is a "Voice over IP" section containing two buttons: "Connections" and "Maintenance". The main content area has a dark blue background with the title "Call Control Connection" in white. Below the title, there are four input fields arranged in two columns. The left column contains "Default Gateway (optional)", "Heartbeat Ping IP", "Call Control IP", and "Subnet Mask". The right column contains "VLAN ID", "VLAN Peak rate", and "VLAN Priority" (which is a dropdown menu). At the bottom of the form, there are two buttons: "Submit" and "Query". The browser's status bar at the bottom shows "Done" and "My Computer".

Call Control Connection			
Default Gateway (optional)		VLAN ID	
Heartbeat Ping IP		VLAN Peak rate	
Call Control IP		VLAN Priority	
Subnet Mask			

The OAMP Connection screen will look as below:

MG 9000 - Microsoft Internet Explorer

NORTEL NETWORKS™

N.E. Net. Link

• •

Voice over IP

Connections Maintenance

OAMP Connection

Default Gateway (optional)		VLAN ID	
Heartbeat Ping IP		VLAN Peak rate	
Active OAMP IP		VLAN Priority	
Inactive OAMP IP			
IP Address of MG 9000 Element Manager		IP Port of MG 9000 Element Manager	
OM Collector Server IP (optional)			
Subnet Mask			

Submit Query

Done My Computer

The Bearer Connection screen will look as below:

The screenshot shows a web browser window titled "MG 9000 - Microsoft Internet Explorer". The page has a dark blue header with the "NORTEL NETWORKS" logo on the left. In the center of the header are two underlined labels: "N.E." and "Net. Link", each followed by a small dot. On the right side of the header is the text "Voice over IP" and two buttons: "Connections" and "Maintenance". The main content area has a dark blue background with the title "Bearer Connection" in white. Below the title, there are two columns of input fields. The left column contains: "Default Gateway (optional)" with a text box, "Heartbeat Ping IP" with a text box, "Bearer IP" with a text box, and "Subnet Mask" with a text box. The right column contains: "VLAN ID" with a text box, "VLAN Peak rate" with a text box, and "VLAN Priority" with a dropdown menu. At the bottom center of the form area are two buttons: "Submit" and "Query". The browser's status bar at the bottom shows "Done" on the left and "My Computer" on the right.

Bearer Connection			
Default Gateway (optional)		VLAN ID	
Heartbeat Ping IP		VLAN Peak rate	
Bearer IP		VLAN Priority	
Subnet Mask			

Submit Query

The DCC Unit Addresses screen will look as below:

65.3 Hardware Requirements or Dependencies

There will be a new SCG card that replaces the SCO/SCI cards on the DCC slots of the MG9K to provide GigE network interface.

The existing standard LCI setup holds true to support this feature – Windows-based-PC or Sun-workstation to connect to the SCG card on the MG9K

65.4 Software Requirements or Dependencies

Currently supported browsers will be supported for this feature too: Netscape 7+ on Win2K, Internet Explorer 5.5+, Netscape 4.7+ on Solaris/HPUX

65.5 Limitations and restrictions

No new limitations/restrictions will be imposed on LCI as a result of this feature.

65.6 Interactions

LCI subsystem will interact with other gateway subsystems as it currently does in the existing architecture. The LCI client to server interaction will also be the same way as it currently exists.

65.7 Glossary

AAL1 – ATM Adaptation Layer

ABI – Access Bridge Interface

APS – Automatic Protection Switching

ATM – Asynchronous Transfer Mode

BDP – Business Decision Point

BITS – Building Integrated Timing Supply

CAF - Content Access Form

ClockSync – Clock Synchronization

DCC – Data Control Card

DID – Design Intent Document

DS1 – Digital Signal level 1

GigE – Gigabit Ethernet

HAL – Hardware Abstraction Layer

ICAF –Integrated CAF

IMA – Inverse Multiplexing over ATM

IP – Internet Protocol

ITP – Internet Telephony Processor

ITX – Internet Telephony Extender

LAN – Local Area Network

LCI – Local Craft Interface

MG9K – Media Gateway 9000

MTU – Max Transfer Unit

OAMP – Operation, Administration, Maintenance, Performance

PING – IP Tool/Utility used to find out if a network host is alive or not

POR – Plan of Record

Ref/Sig – Reference/Signal

RFI – Remote Fault Indicator

Rx - Receiver

SC – Super Core

SCG – Super Core GigE

SCI – Super Core IMA

SCO – Super Core OC3

SN08 – Succession Networks Release 08

SSU – Synchronization Supply Unit

TRACEROUTE – IP Tool/Utility used to print the route a packet takes to the network host

Tx - Transmission

VLAN – Virtual LAN

VOIP – Voice over IP

66: A00007264 Functional description (FN)

66.1 Feature name and Feature ID

CentrexIP Client Manager Capacity Expansion Phase 2

66.2 Description

This is phase 2 of the CICM capacity increase feature. This phase covers increasing the BHHCA, maximum concurrent calls and introduces improved capacity throttling. For details of the phase 1 activity see A00003952 in PLS FMDOC.

66.2.1 New System Parameters

	5370 cards	5385 Cards
BHHCA	7,200	21,600
RUDP msg/s	500	500
H.248 msg/s	100	250
Max terminal sessions	2500	4096
Lines	1023	3069
Ephemerals	512	3069

Busy Hour Half Call Attempts (BHHCA) - the maximum number of half call attempts per hour, each CICM line involved in a call equals 1 half call, e.g. a CICM line to CICM line call requires 2 half calls, CICM line to trunk call 1 half call and a 3-way call involving 3 lines hosted off the same CICM equals 3 half calls.

Reliable User Datagram Protocol (RUDP) - this is the transport for Unistim messaging between the CICM and the terminals. The incoming message rate is throttled to prevent the CICM becoming overloaded.

H.248 - this is the transport for H.248 communication with the GWC. Similarly the incoming message rate is throttled to prevent the CICM becoming overloaded. The threshold has been increased for the 5385 platform to facilitate the higher BHHCA capacity.

Terminal Sessions - the maximum number of terminal sessions will be increased to 4096 on the 5385 platform. Active terminal sessions includes both logged in users and terminals connected to the CICM but without a logged in user (e.g. displaying the login prompt). Joint sessions require 2 terminal

sessions. For the 5370 platform the maximum number of session will remain at 2500.

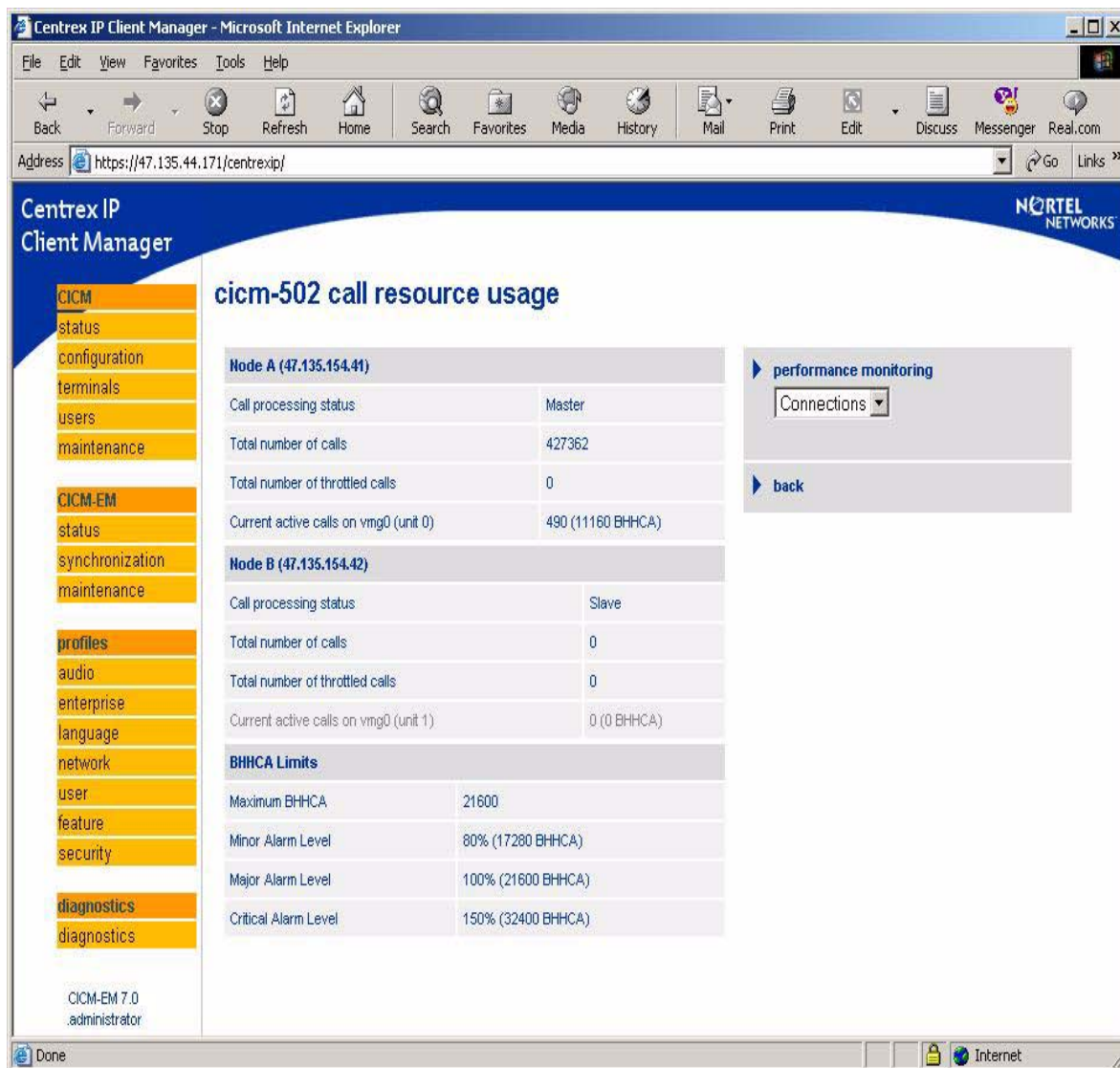
Lines - the maximum number of lines/users will be increased to 3069 on the 5385 platform. Please refer to A00003717 for more information on configuring 3069 CICM lines.

Ephemeral terminations - 1 ephemeral termination is required for each half call, therefore the number of ephemerals effectively control the maximum number of concurrent calls. For the 5385 platform the number of ephemerals will be increased to 3069 allowing all lines to be involved in concurrent calls.

66.2.2 BHHCA throttling

At present the only BHHCA throttling that exists is at the RUDP/H.248 layers, call processing is limited by the number of unistim and H.248 messages that can be processed per second. As such the actual BHHCA level is dependant on the number of unistim/H.248 messages per call. This is not a reliable method of controlling CICM resource usage and it could lead to the CICM becoming overloaded and unstable.

This activity introduces a throttling mechanism based on BHHCA. Once the BHHCA reaches 80% (17,280 BHHCA) a minor alarm will be raised. At 100% (21,600 BHHCA) a major alarm will be raised and at 150% (34,400) a critical alarm will be raised. Calls above the 150% threshold are throttled. The count of throttled calls can be viewed from the Call Resource Usage page on the Element Manager (accessed by clicking Active Calls on the maintenance status page). Although the CICM attempt to process calls up to the 150% limit, call levels above 100% BHHCA may result in call failures.

Figure 1 Call Resource Usage Page on the Element Manager

66.2.3 Perflog Service

A New Windows service has been introduced to the gateway image to enable the CICM performance to be monitored. To use the service connect to the gateway using CICMCONNECT. Type 'net start perflog' to start monitoring and 'net stop perflog' to stop. Performance log files are placed in the d:\debuglog directory named 'pflog_x.txt'.

The files generated are in comma delimited text format. These can be imported into a spreadsheet package such as Microsoft Excel by opening the file and selecting delimited data type, click next then uncheck the Tab delimiter and check the comma box, then finish. The data is organized in columns for each

counter, the CPU % for each process and general memory counters have been included.

Figure 2 Example Perflog file (some data columns have been removed)

```
Performance monitoring Log File
Date, \\CICM-002-A\\Process\\Idle\\% Processor Time, ..., \\CICM-002-A\\Memory\\%
Committed Bytes In Use, \\CICM-002-A\\Memory\\Available MBytes,
Wed Oct 27 10:23:07 200, 99, ..., 16, 656,
Wed Oct 27 10:23:08 200, 100, ..., 16, 656,
Wed Oct 27 10:23:09 200, 99, ..., 16, 656,
Wed Oct 27 10:23:10 200, 98, ..., 16, 656,
Wed Oct 27 10:23:11 200, 100, ..., 16, 656,
...
```

If additional processes start after the perflog service, new columns will be added to the right of the data, this will also cause a new header row to be written across in order to capture the names of the new counters. So if you see a new header row across the data its because a new process has started.

66.3 Hardware Requirements or Dependencies

The BHHCA, maximum concurrent calls and terminal sessions capacity increases are only available on the 5385 hardware. There are no capacity changes to the 5370 platform.

66.4 Software Requirements or Dependencies

SN07 GWC, GWC-EM.

66.5 Limitations and restrictions

The capacity increases are only available on the 5385 platform.

66.6 Interactions

66.7 Glossary

Table 1

Term	Description
BHHCA	Busy Hour Call Attempts
CICM	Centrex IP Client Manager
EM	Element Manager
GWC	Gateway Controller
RUDP	Reliable User Datagram Protocol
UniStim	Unified Network IP Stimulus protocol

67: A00007268 Functional description (FN)

67.1 Feature name

NGSS OM Subsystem Enhancement

67.2 Description

In SN07 Release, NGSS OM subsystem pegs counts for one set of registers per OM group.

OM enhancement activity is to enhance the existing OM subsystem to support the notion of dynamic number of tuples for OM groups i.e. tuples can be added/deleted to/from OM groups dynamically.

The SIP Gateway OM groups defined in SN07(SIPGW_CALLP, SIPGW_SERVICES and SIPGW_MISC) are enhanced to track measurements based on SIPLINK.

OM CLI (i.e. **OM SHOW**) is enhanced to support querying of OM peg counts based on TUPLES.

The omshow command syntax at the CLI will be as follows:

```
>omshow <groupname>
<class> {ACTIVE,
HOLDING,
FIVEMIN,
ZERO}
[<num> {0 to 4294967295}]
[<to_num> {0 to 4294967295}]
[<Key> string]
[<Key to> string]
```

The first parameter will be the **OM Group Name**, the second parameter will be the **Query Type** (ACTIVE/HOLDING/LAST5MIN).

Note 1: “ALL” is no longer supported for the groupname parameter.

Note 2: *Tuple key* will be a mandatory integer key provided by application that wants to peg OMs, with an optional text keyname (if provided must be unique).

Note 3: *Tuple Key Range:-* The max tuple key range is calculated as “4294967295” by applying the formula “ $2^{32}-1$ ”.

67.3 Hardware Requirements or Dependencies

None.

67.4 Software Requirements or Dependencies

None.

67.5 Limitations and restrictions

None.

67.6 Interactions

None.

67.7 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__

67.8 Glossary

Table 1

Term	Description
OM	Operational Measurement
NGSS	Next Generation Session Server
CLI	Command Line Interface

67.9 Appendix A: NGSS OM CSV File Format

This section details the CSV file formats, its location, and shows examples.

67.9.1 CSV File Location

SSH Login Access

If the user desires to login to a session server unit via an account such as MTC and look at the CSV files, the main directory path is /opt/apps/ngsspm. Two subdirectories are located here:

stdhist - This directory contains the 24 hour long term values.

trafhist - This directory contains the 30 minute short term values.

FTP Access

This future section will contain the access information when FTP is utilized using the NGSSPM account to pull CSV files from a session server unit.

67.9.2 CSV File Format

The CSV file format is shown below. Note that the below format uses an example consisting of two OM groups. The first example OM group has 32 registers and 1 tuple of peg counts. The second example OM group has 9 registers and 3 tuples of peg counts.

```
PMFile=Begin
MeasurementCategory,FileCreationTime,EarliestStartTime,LatestCaptureTime,RegisterTypeDefault,ValueTypeDefault
<string="pm">,<string>,<string>,<string>,<string="counter">,<string="integer">
System=Begin
SystemId
<string="SessionServer">
Entity=Begin
EntityId
<string= Unit IPAddress>
SubEntity=Begin
SubEntityId
<string=["Unit0" | "Unit1"]>
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime,Reliability
<string>,<string="PeriodBased">,<string>,<integer>,<string="Valid">
Labels=Begin
TupleKey,KeyName
<string>,<string>
Reg1Name,Reg2Name,Reg3Name,Reg4Name
<string>,<string>,<string>,<string>
Reg5Name,Reg6Name,Reg7Name,Reg8Name
<string>,<string>,<string>,<string>
Reg9Name,Reg10Name,Reg11Name,Reg12Name
<string>,<string>,<string>,<string>
Reg13Name,Reg14Name,Reg15Name,Reg16Name
<string>,<string>,<string>,<string>
Reg17Name,Reg18Name,Reg19Name,Reg20Name
<string>,<string>,<string>,<string>
Reg21Name,Reg22Name,Reg23Name,Reg24Name
<string>,<string>,<string>,<string>
Reg25Name,Reg26Name,Reg27Name,Reg28Name
<string>,<string>,<string>,<string>
Reg29Name,Reg30Name,Reg31Name,Reg32Name
<string>,<string>,<string>,<string>
Labels=End
RowOfValues=Begin
TupleKey,KeyName
<integer>,<string>
Reg1Value,Reg2Value,Reg3Value,Reg4Value,Reg5Value,Reg6Value,Reg7Value,Reg8Value
<integer>,<integer>,<integer>,<integer>,<integer>,<integer>,<integer>,<integer>
Reg9Value,Reg10Value,Reg11Value,Reg12Value,Reg13Value,Reg14Value,Reg15Value,Reg16Value
<integer>,<integer>,<integer>,<integer>,<integer>,<integer>,<integer>,<integer>
Reg17Value,Reg18Value,Reg19Value,Reg20Value,Reg21Value,Reg22Value,Reg23Value,Reg24Value
<integer>,<integer>,<integer>,<integer>,<integer>,<integer>,<integer>,<integer>
Reg25Value,Reg26Value,Reg27Value,Reg28Value,Reg29Value,Reg30Value,Reg31Value,Reg32Value
<integer>,<integer>,<integer>,<integer>,<integer>,<integer>,<integer>,<integer>
RowOfValues=End
Table=End
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime,Reliability
<string>,<string="PeriodBased">,<string>,<integer>,<string="Valid">
Labels=Begin
TupleKey,KeyName
<string>,<string>
Reg1Name,Reg2Name,Reg3Name,Reg4Name
<string>,<string>,<string>,<string>
Reg5Name,Reg6Name,Reg7Name,Reg8Name
<string>,<string>,<string>,<string>
Reg9Name
<string>
Labels=End
RowOfValues=Begin
TupleKey,KeyName
<integer>,<string>
Reg1Value,Reg2Value,Reg3Value,Reg4Value,Reg5Value,Reg6Value,Reg7Value,Reg8Value
<integer>,<integer>,<integer>,<integer>,<integer>,<integer>,<integer>,<integer>
Reg9Value
<integer>
TupleKey,KeyName
<integer>,<string>
Reg1Value,Reg2Value,Reg3Value,Reg4Value,Reg5Value,Reg6Value,Reg7Value,Reg8Value
<integer>,<integer>,<integer>,<integer>,<integer>,<integer>,<integer>,<integer>
Reg9Value
<integer>
```

```

TupleKey, KeyName
<integer>, <string>
Reg1Value, Reg2Value, Reg3Value, Reg4Value, Reg5Value, Reg6Value, Reg7Value, Reg8Value
<integer>, <integer>, <integer>, <integer>, <integer>, <integer>, <integer>, <integer>
Reg9Value
<integer>
RowOfValues=End
Table=End
SubEntity=End
Entity=End
System=End
PMFile=End

```

67.9.3 Examples

An example CSV file is shown below. Note that the below example shows three OM groups. The first OM group has 6 registers, the second has 10 registers and the third has 5 registers. All of the sample OM groups have 2 tuples of peg counts.

```

PMFile=Begin
MeasurementCategory, FileCreationTime, EarliestStartTime, LatestCaptureTime, RegisterTypeDefault, ValueTypeDefault
t
pm, 2004.8.30_15.25_EDT, unknown, unknown, counter, integer
System=Begin
SystemId
SessionServer
Entity=Begin
EntityId
47.174.74.179
SubEntity=Begin
SubEntityId
Unit0
Table=Begin
TableId, MeasurementKind, IntervalDuration, CaptureTime, Reliability
SIPGW_CALLP, PeriodBased, 5, unknown, Valid
Labels=Begin
TupleKey, KeyName
Key, KeyName
Reg1Name, Reg2Name, Reg3Name, Reg4Name
IC_CALL_ATTEMPTS, OG_CALL_ATTEMPTS, CALLS_ABANDONED, CALLS_ANSWERED
Reg5Name, Reg6Name
CALLS_REJECTED, CALLS_REDIRECTED
Labels=End
RowOfValues=Begin
TupleKey, KeyName
0, SIPLINK_0
Reg1Value, Reg2Value, Reg3Value, Reg4Value, Reg5Value, Reg6Value
2, 1, 0, 0, 1, 0
TupleKey, KeyName
1, SIPLINK_1
Reg1Value, Reg2Value, Reg3Value, Reg4Value, Reg5Value, Reg6Value
0, 1, 0, 1, 0, 5
RowOfValues=End
Table=End
Table=Begin
TableId, MeasurementKind, IntervalDuration, CaptureTime, Reliability
SIPGW_SERVICES, PeriodBased, 5, unknown, Valid
Labels=Begin
TupleKey, KeyName
Key, KeyName
Reg1Name, Reg2Name, Reg3Name, Reg4Name
REFER_ATTEMPTS, REFER_SUCCESS, IC_DTMF_SUBSCRIBES, OG_DTMF_SUBSCRIBES
Reg5Name, Reg6Name, Reg7Name, Reg8Name
IC_DTMF_NOTIFYS, OG_DTMF_NOTIFYS, IC_FAX_SUBSCRIBES, OG_FAX_SUBSCRIBES
Reg9Name, Reg10Name
IC_FAX_NOTIFYS, OG_FAX_NOTIFYS
Labels=End
RowOfValues=Begin
TupleKey, KeyName
0, SIPLINK_0
Reg1Value, Reg2Value, Reg3Value, Reg4Value, Reg5Value, Reg6Value, Reg7Value, Reg8Value
2, 1, 0, 0, 1, 0, 1, 3
Reg9Value, Reg10Value
2, 0
TupleKey, KeyName
1, SIPLINK_1
Reg1Value, Reg2Value, Reg3Value, Reg4Value, Reg5Value, Reg6Value, Reg7Value, Reg8Value
3, 0, 1, 0, 1, 0, 2, 0
Reg9Value, Reg10Value
1, 1

```

```

RowOfValues=End
Table=End
Table=Begin
TableId, MeasurementKind, IntervalDuration, CaptureTime, Reliability
SIPGW_MISC, PeriodBased, 5, unknown, Valid
Labels=Begin
TupleKey, KeyName
Key, KeyName
Reg1Name, Reg2Name, Reg3Name, Reg4Name
TCP_CALLS, UDP_CALLS, SIP_MSG_SEND_FAILURES, INCOMING_SDP_INCOMPATIBLE
Reg5Name
OUTGOING_SDP_INCOMPATIBLE
Labels=End
RowOfValues=Begin
TupleKey, KeyName
0, SIPLINK_0
Reg1Value, Reg2Value, Reg3Value, Reg4Value, Reg5Value
3, 0, 1, 0, 1
TupleKey, KeyName
1, SIPLINK_1
Reg1Value, Reg2Value, Reg3Value, Reg4Value, Reg5Value
4, 1, 1, 1, 0
RowOfValues=End
Table=End
SubEntity=End
Entity=End
System=End
PMFile=End

```

68: A00007270 Functional description (FN)

68.1 Feature name

A00007270 - Session Server Call Processing Overload Controls

68.2 Description

This feature provides for Overload Controls on the Session Server for the SIP Gateway Call Processing Application.

The Session Server is a platform for delivery of multiple applications. It consists of a NEBS Level 3 compliant hardware platform and a software framework and architecture for developing Carrier Grade applications and services. The SIP Gateway Application is the initial application for the Session Server Platform

The new functionality that will be implemented under this Session Server Overload Controls activity consists of the overload controls mechanism created specifically for Call Processing on the SIP Gateway Application.

68.2.1 SIP CallP Gateway Application Overload Controls

For SIP Gateway Application's overload monitoring purposes, Queue Monitor Thread will be monitoring the size of the Call Processing Origination Queue to make the determination on call processing capacity and thus overload state. The overload state thresholds will be pre-defined and thus not provisionable. It is not in the scope of this feature to provide an interface to allow for provisioning of threshold values.

The overload thresholds are as follows:

- Overload will be triggered for UDP traffic over 1.170 M BHCCA
- Pending Overload will be triggered for UPD traffic over 1.080 M BHCCA

In the event that Queue Monitor has indicated that a Call Processing Origination Queue overload condition exists, Sip Gateway Application will discard any new origination (INVITE) messages coming in from remote SIP servers. Outgoing origination messages will continue to be processed as received. Logs and Alarms will be raised to indicate a problem. A new OM register (OVRD_CALLS_REJECTED) in the SIPGW_CALLP group will be pegged every time an INVITE is rejected due to an overload condition. Logs and alarms are defined in section 11 of this document. The OM register is discussed in section 14 of this document

Following are the Overload States and the corresponding actions:

- Overload - Logs and major Alarms are raised and action taken to stabilize the system by rejecting new incoming origination messages. OVRD_CALLS_REJECTED OM register is pegged
- Overload Pending - Logs and minor Alarms raised, but no action taken to reject CallP messages.
- No Overload - All prior Alarms cleared.

68.3 Hardware Requirements or Dependencies

This feature doesn't introduce any new hardware requirements or dependencies.

68.4 Software Requirements or Dependencies

This feature doesn't introduce any new software requirements or dependencies.

68.5 Limitations and restrictions

This feature will not provide an user interface for provisioning the Overload Threshold values.

In the event of a Call Processing Origination Queue overload condition, ONLY new origination messages coming in from remote SIP servers will be discarded. The processing of the outgoing calls will not be affected. The reason behind this restriction is that on the outgoing calls, the call processing has already been completed on the XA-core and on the SIPT GWC, and the therefore these calls have passed the point of alternate disposition (such as alternate route or treatment).

68.6 Interactions

This feature implements a Session Server Overload Manager process, which is designed to interact with SIP CallP Gateway Application and other "future" applications on the Session Server.

68.7 Glossary

Table 1

Term	Description
CallP	Call Processing
GWC	Gateway Controller
NEBS	Network Equipment Building System
Session Server	Platform for the SIP Gateway Application
SIP	Session Initiated Protocol

69: A00007271 Functional description (FN)

69.1 Feature name and Feature ID

TOPS EOL for SN08

69.2 Description

This feature addresses all activities needed to support the TOPS End Of Life (EOL) program through SN08, including the following:

- Disables the TOPS Position via the Enhanced TOPS Message Switch (ETMS) functionality.
- Disables the TOPS Operator Centralization (OC) via the ETMS functionality.
- Identifies usage of the OSSAIN Management Information System (MIS) in the TOPS EOL logs.
- Removes the tables, parms, and OM groups which are obsolete.

Upgrades to SN08 or higher will result in loss of functionality if proper conversions to replacement features are not performed prior to the upgrade.

69.3 Hardware Requirements or Dependencies

None.

69.4 Software Requirements or Dependencies

None.

69.5 Limitations and restrictions

A position, using an ETMS for data connectivity to a host, will not be able to RTS or login once the host is upgraded to SN08 or higher.

A remote, using an ETMS for data connectivity to a host, will not be able to send calls to that host once the host is upgraded to SN08 or higher.

A host, using an ETMS for data connectivity to a remote, will stop receiving calls from that remote once the remote is upgraded to SN08 or higher.

69.6 Interactions

Positions, connected via ETMS, must be replaced by IP positions prior to an upgrade to SN08 or higher.

TDM-OC links must be replaced by OC-IP links prior to an upgrade to SN08 or higher. **Any OCHOST or OCHOSTQ tuple which references a TDM-**

OC link will cause a TABXFR to halt if not replaced prior to such an upgrade.

69.7 Glossary

Table 1

Term	Description
EOL	End Of Life
ETMS	Enhanced TOPS Message Switch
IP	Internet Protocol
OC	Operator Centralization
MIS	Management Information System
TOPS	Traffic Operator Position System

70: A00007275 Functional description (FN)

70.1 Feature name

Session Server - Session/Application Mgmt Framework and Support for Multiple HTTPS connection to the Session Server through SSPFS

70.2 Description

70.2.1 Session Server - Session/Application Mgmt Framework and Support

This feature is one of three features whose primary requirements are to provide thread trap recovery as well as overload controls for the (SIP) Gateway Application.

The other features are:

- A00007270 - Session Server - Overload Controls
- A00007276 - Session Server - Application Patching Support

This feature implements light-weight thread-safe message queues for communicating between SIP Gateway Application threads, replacing the Unix Sockets and Inter-Process Communication (IPC) Message Queues used in Session Server Release 07. These new Message Queues provides the framework to make thread recovery and overload controls possible.

This feature introduces software into the SIP Gateway Application which monitors the health of the SIP Gateway Application threads and will attempt to recover any threads that fail rather than choosing to Swact the platform as the first course of action. Of course, if the thread cannot be recovered, the platform will Swact.

70.2.2 Support for Multiple HTTPS connection to the Session Server through SSPFS

Refer to PLS FMDOC A00008383 for more information on this activity. This feature removes the limitation of one proxy HTTPS connection from IEMS/SSPFS to the Session Server and allows multiple Session Server nodes to reside on the CS-LAN. Multiple Session Servers may be required to allow multiple applications to be deployed on separate boxes or to allow multiple Session Servers running the same application or combinations of both. For the SN08 release, the expected number of Session Servers to be provisioned on the SSPFS is aimed at 4.

At customer sites, the SSPFS acts as an HTTP proxy between the OAMP and CALLP LANS (which are separated by a firewall). Incoming requests to the SSPFS from the Session Server web provisioning interface are mapped to tag names which are in turn mapped to real URLs in the CALLP LAN to get the

request to the correct Session Server box. Tomcat requires that the tag names in the SSPFS must be the same string as the last directory in the destination URL. The destination URLs for the Session Server application's web page is hard-coded to be in the '/prov' directory and therefore the SSPFS must use a tag name of 'prov' to map the HTTPS request to the Session Server. Since tag names must be unique, the SSPFS can only direct HTTPS requests to a single Session Server box in SN07.

This feature provides the support of different tag names in the SSPFS to support multiple HTTPS connections so that the Session Server application web page will end in a variable directory name that is configured at startup. Once the hard-coded use of '/prov' is removed and replaced with the configured string, multiple HTTPS connections through the SSPFS will be possible.

The variable tag name for the Session Server applications will be obtained when the applications are installed. All Session Server applications are installed through the InstallApps script which is run after NCGL is installed. The script will prompt for a new tag name for the Session Server box. The same name must be input on both the active and inactive Session Server application during installation as well as on the SSPFS Apache proxy configuration to identify the said Session Server Application. The tagname is an alphanumeric string with period, underscore or hyphen and a maximum string length of 128 characters.

An example of how the 2 Session server applications will be configured on the Apache proxy configuration is as follows:

The tag name for this Session Server is “**ngss-spc**”

ProxyPass /10.65.99.67/ https://10.65.99.67:443/ ---> NCGL unit 0

ProxyPassReverse /10.65.99.67/ https://10.65.99.67:443/

ProxyPass /10.65.99.70/ https://10.65.99.70:443/ ---> NCGL Unit 1

ProxyPassReverse /10.65.99.70/ https://10.65.99.70:443/

ProxyPass /10.65.99.72/ https://10.65.99.72:443/ ---> NCGL active

ProxyPassReverse /10.65.99.72/ https://10.65.99.72:443/

ProxyPass /ngss-spc/ https://10.67.99.72:8443/ngss-spc/ ---> NGSS Active

ProxyPassReverse /ngss-spc/ https://10.67.99.72:8443/ngss-spc/

The tag name for this NGSS is “**ngss-trkapp**”

ProxyPass /172.65.99.67/ https://172.65.99.67:443/ ---> NCGL unit 0

ProxyPassReverse /172.65.99.67/ https://172.65.99.67:443/

ProxyPass /172.65.99.70/ https://172.65.99.70:443/ ---> NCGL Unit 1

ProxyPassReverse /172.65.99.70/ https://172.65.99.70:443/

ProxyPass /172.65.99.72/ https://172.65.99.72:443/ ---> NCGL active

ProxyPassReverse /172.65.99.72/ https://172.65.99.72:443/

ProxyPass /ngss-trkapp/ https://172.67.99.72:8443/ngss-trkapp/ --> NGSS Active

ProxyPassReverse /ngss-trkapp/ https://172.67.99.72:8443/ngss-trkapp/

70.3 Hardware Requirements or Dependencies

This feature doesn't introduce any new hardware requirements or dependencies.

70.4 Software Requirements or Dependencies

This feature doesn't introduce any new software requirements or dependencies.

The IEMS software has to be SN08 or greater release for multiple HTTPS support on the Session Server through the SSPFS.

70.5 Limitations and restrictions

The key assumption for the multiple HTTPS support of the Session Server through the NGSS activity is that the Session Server will continue to use a single launch point for accessing OAMP pages for all applications. This was the planned approach for all applications and should be an accurate assumption. If future applications do not choose to use that single launch point for their OAMP, additional feature work will be required to support additional dynamic tag names for those applications that do not conform.

The tag name for an Session Server application must be unique and cannot be changed once the application is installed using the InstallApps script. Any change of the tag name will require a re-installation of the application.

70.6 Interactions

This activity interacts with the SSPFS. The tag name that is input into the NGSS during installation for both the active and inactive units, have to match what is input into the SSPFS.

70.7 Glossary

Term	Description
HTTPS	HyperText Transport Protocol Secure
IEMS	Integrated Element Management System
IPC	Inter-Process Communication
NCGL	Nortel Carrier Grade Linux
NGSS	Next Generation Session Server
OAMP	Operation Administration Maintenance and Provisioning
SSPFS	Succession Server Platform Foundation Software
URL	Uniform Resource Locator

71: A00007276 Functional description (FN)

71.1 Feature name

Session Server¹ Application Patching Support

71.2 Description

This feature provides the basis for application patching for the NGSS. Any software installed/changed/removed on an NGSS system that is not delivered in a standard release or a maintenance release is delivered in a patch file.

This feature has associated features which are:

- A00007270 - Session Server Call Processing Overload Controls
- A00007275 - Session Server - Session/Application Mgmt Framework

A patch is a single file that contains the executables, libraries, data, scripts, and dependency information necessary to apply and remove the patch. The Session Server commands “apply_patch” and “remove_patch” which are run from the mtc account are used to install and uninstall patches. Many patches can be applied without any impact to inservice processing. Some patches must coordinate with call processing to be applied or removed successfully. Anything may be patched on the inactive side of the Session Server.

Patches are delivered using SCP and are applied or removed using SSH.

71.3 Hardware Requirements or Dependencies

None

71.4 Software Requirements or Dependencies

This feature requires NCGL_6.33.1.0.0408111208 or later.

71.5 Limitations and restrictions

In this release the Session Server patching is not integrated with any Nortel patch manager. The patches will be delivered using NPM but will not be applied to the Session Server using NPM.

71.6 Interactions

None

¹Also referred to as the NGSS or SP2K in other documents.

71.7 Glossary

Term	Description
NGCL	Nortel Carrier Grade Linux
NPM	Network Patch Manager
SCP	Secure Copy
SSH	Remote Secure Login Program

72: A00007277 Functional description (FN)

72.1 Feature name

LOGs Throttling

72.2 Description

This feature is required to implement LOGs throttling functionality for XA-Core.

The requirement of this feature is to use of datafill table for throttling logs. Customer can throttle the log report by specifying the time unit and threshold value.

There is also a requirement to throttle the DLOG when it is specified by the customer. By default throttled logs will go to DLOG, unless it is specified by the user.

Only core logs will be throttled.

Desired behavior of this feature is to implement the throttling mechanism for LOG Devices and DLOGs. New throttling functionality will allow customer to specify on Time Units and Thresholds per Report Name (REPNAME) through a Table LOGTHROT.

New threshold behavior:

- Logs to be throttled, will be output in each unit time until the log count reaches threshold value.
- Logs will then be throttle until the time unit expires.
- When the timer resets the logs will not be throttled.

The new Table LOGTHROT will contain the THRSHOLD and TUNITS values as we have them in table LOGCLASS.

Figure 1 Functional Diagram

TABLE LOGTHROT:

REPNAME	THRSHOLD	TUNITS	DLOG

TRK 113	[0-255]	[0-32767]	Y / N

Logs will be generated in each time unit until the log count reaches the threshold value. The logs will then be throttled until the time unit expires. When the timer resets, the logs will not be throttled.

e.g.

Suppose, we want to throttle TRK113 log. If the threshold value is set to 5 and t units is 1, that means we only want five TRK113 log in one minute. Any TRK113 logs over five within a minute will be throttled. Because the DLOG field is set to 'NO', we won't be throttling TRK113 DLOGs.

Figure 2 Functional Diagram

TABLE LOGTHROT:

REPNAME	THRSHOLD	TUNITS	DLOG

TRK 113	5	1	N

Recommended TUNITS value is 1 (min). Threshold value can be set based on site engineering information. Following are the some examples of threshold values used in CSP20, TUNITS id 1(mins):

REPNAME	THRSHOLD
AUDIT105	25
AUDIT106	25
TRK113	75
C7UP103	25
TRK138	75

72.3 Hardware Requirements or Dependencies

N/A.

72.4 Software Requirements or Dependencies

N/A

72.5 Limitations and restrictions

N/A

72.6 Interactions

N/A

72.7 Applicable customer facing sections

Fault Management

Logs ☐ Yes ☐

Alarms ☐ No ☐

Configuration

Data Schema ☐ No ☐

User Interface ☐ No ☐

Element Management ☐ No ☐

Security ☐ No ☐

Service Order ☐ No ☐

Office Parameters ☐ Yes ☐

Accounting (includes AMA billing) ☐ No ☐

Performance (includes operational measurements) ____No____

72.8 Glossary

Term	Description
New term	Definition

73: A00007282 Functional description (FN)

73.1 Feature name

Configurable Threshold for Failed Login

73.2 Description

This SN08 activity provides a way to configure the limit of failed login attempts for succession applications. The same retry limit will apply to the telnet and ssh access.

73.2.1 CLI Tool

The Command Line Interface of SSPFS is modified to provide an additional option to change the login retries limit value. Follow the procedure below to make changes to the retries limit value:

- 1 Start cli
- 2 Select option 2 (Configuration)
- 3 Select option 14 (Login Session)
- 4 Select option 4 (login_retries)
- 5 Enter a value in the range 1 – 15.
Any value not in this range will be rejected with an error:
“ERROR – Login Retries Limit Value Out Of Range”

If the change is successful, the following message will be shown:
=== “login_retries” completed successfully

73.3 Hardware Requirements or Dependencies

Not applicable

73.4 Software Requirements or Dependencies

Not applicable

73.5 Limitations and restrictions

Not applicable

73.6 Interactions

Not applicable

73.7 Glossary

Not applicable

74: A00007293 Functional description (FN)

74.1 Feature name

VLAN for Gigabit Ethernet

74.2 Description

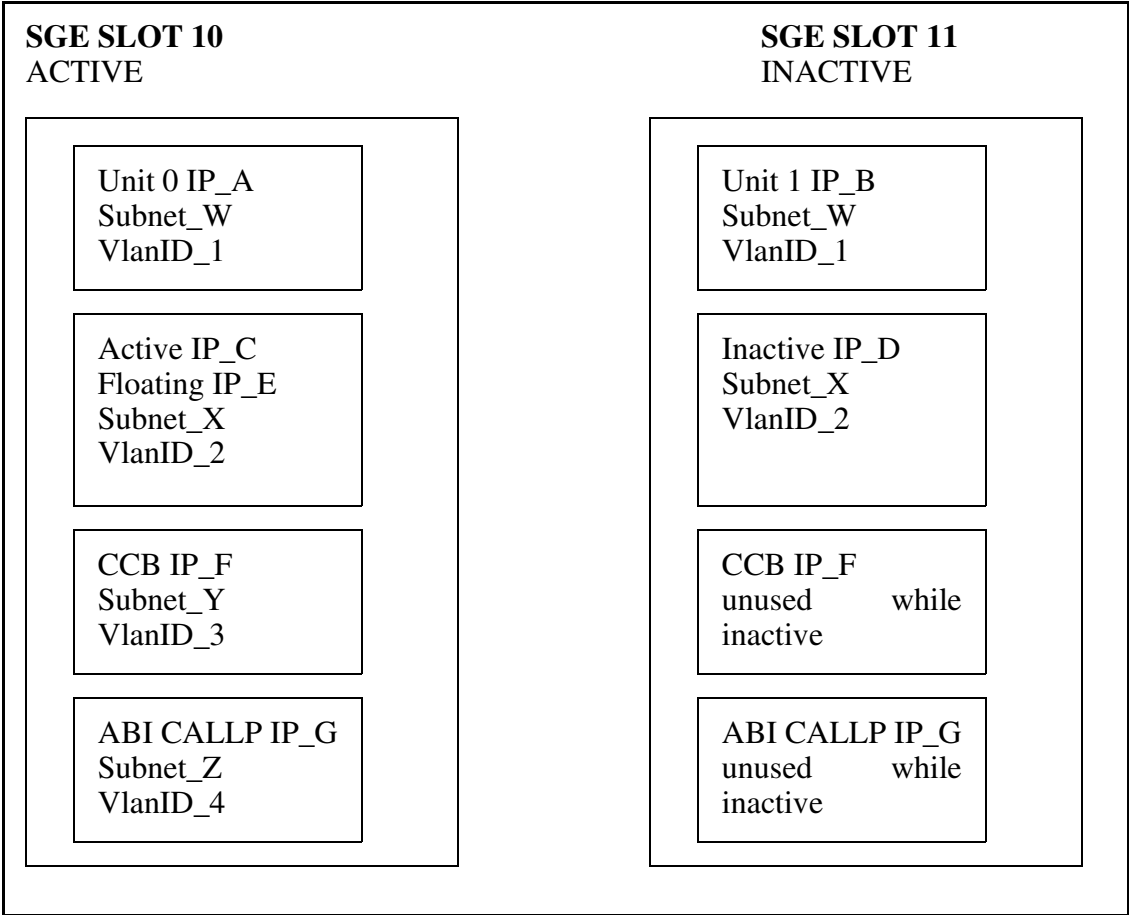
On a GigE MG9K, VLANs are used to aggregate similar IP traffic. There are four VLANs configured on the MG9K via the LCI. The four VLANs are OAM, CallControl, Bearer, and Unit. The OAM VLAN is used for SNMP, loading, ssh, etc. The CallControl VLAN is used by ITPs and ABIs for H.248 and XPM messaging. The Bearer VLAN carries all ITP and ABI bearer traffic. The Unit VLAN is used to perform GigE link integrity tests to the edge router and the mate SCG card.

In addition there are five new IP addresses required on a GigE MG9K. They are

- two static unit addresses that are assigned to a SCG card
- one floating SCG Call Control address used for ARP
- one floating SCG Bearer address used for ARP
- one floating inactive OAM address.

The figure below illustrates the relationship of the VLANs and IP addresses described above.

Figure 1 SCG VLANs and IP addresses



74.3 Hardware Requirements or Dependencies

Not Applicable.

74.4 Software Requirements or Dependencies

74.5 Limitations and restrictions

Not Applicable.

74.6 Interactions

Not Applicable.

74.7 Applicable customer facing sections

Functional Description (Mandatory) ☒ X

Fault Management

Not applicable ☒ X

Logs	_____
Alarms	_____
Configuration	
Not applicable	_____
Data Schema/MIBs	___X___
User Interface	_____
GUI	_____
Element Management	_____
Security	_____
Service Order	_____
Office Parameters	_____
SOC	_____
Upgrades impact	_____
Accounting (includes AMA billing)	_____
Not Applicable	_____
Billing changes	_____
Performance	_____
Not Applicable	_____
Operational Measurements	___X___
Performance Measurements	_____
Realtime (Mandatory)	_____
Engineering Information (Mandatory)	_____

74.8 Glossary

Table 1

Term	Description
New term	Definition
SCG	Supercore GigE

75: A00007295 Functional description (FN)

75.1 Feature name and Feature ID

Feature Name: CBM 860 OC3 Connectivity

BRISC - BNR Reduced Instruction Set Computer (DMS Core)

CBM - Core Billing Manager

OC3 - Optical Carrier- Level 3 (transmission interface)

75.2 Description

75.2.1 General Description

The CBM 860 is a High Availability Core Billing Manager that has two server units. It requires 4 Optical Carrier Level 3 (OC3) fiber links to the core through the Message Switch (MS) for connectivity. The CBM 860 will have the ability to change activity to a healthy unit in a fault scenario.

The main function of this feature is to provide the core connectivity for the CBM 860 by allowing 2 OC3 MS ports to be provisioned on the NT9X63AB/NT9X17AD card combination. The NT9X63AB is the MS OC3 paddleboard that will connect through fibers to the CBM 860. The NT9X17AD port card is the MS front card that will provide communication from the OC3 paddle board to the MS such that messages from the CBM 860 may be passed to the core.

One set of the NT9X63AB/NT9X17AD card combination will be required on each MS to provide the four OC3 fiber connections from the CBM 860 to the MS.

The changes introduced in the software can be broken down into two separate components, where one portion resides on the message switch (MS), local MS code, and the other on the computing module (CM), central MS code.

Figure 1 displays of what the MAP will look like when a NT9X63AB/NT9X17AD is posted. Currently the design objective is to display the card protocol as a DS512 instead of as an OC3. Reason for this is to provide SDM equivalency on maintenance. Hence the craftsperson will have similarity between the CBM and SDM.

Figure 1 Updated Map display for the CBM 860 Connectivity

CM	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
CM Flt	Clock	OM	B 1Shlv	1EIU	2	RS	.	74C..	1Crit
									SDM

```

M      M      *C*      *C*      *C*      *C*      *C*      *C*
CARD      Message Switch  Clock  Shelf  0      Inter-MS Link 0 1
0 Quit      MS 0      .      M Free      .      - -
2      MS 1      .      Slave      .      - -
3
4      Shelf 0      1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
5      Card 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
6 Tst_      Chain      |      |
7 Bsy_      MS 0      . . . . . . . . . . . . . . . . . . . .
8 RTS_      MS 1      . . . . . . . . . . . . . . . . . . . .
9 Offl_
10      Card 08 Protocol Port 0 1
11 LoadCd_  MS 0 . DS512 2 - -
12 QueryCd_  MS 1 . DS512 2 - -
13 Card_
14 QueryMS   CARD:
15 Trnsl_
16
17 Next
18 Port_
TAK3
Time 10:00 >

```

75.2.2 System Behavior/Feature Operation

This feature will allow two ports to be provisioned on the NT9X63AB/ NT9X17AD card combination for CBM 860 connectivity.

Please refer to the Nortel Networks MS card replacement procedure for instructions to install the required cards.

From the DMS-100 Card Replacement Procedures document (297-9051-547).

- a. go to the MS level of the MAP, bsy out MS1 (change it to the slave MS if it is not)


```

>mapci;mtc;ms
>swmast % if MS1 is not the slave MS
>bsy 1

```
- b. power down the busied MS
- c. insert the NT9X63AB paddleboard as well as the corresponding NT9X17AD into the MS for the chosen slot location¹
- d. powerup the busied MS
- e. load the MS software image onto the busied MS


```

>loadms <ms_number>

```
- f. issue an out of service test on the MS


```

>tst <ms_number>

```

¹Refer to “2.5 Limitations and restrictions” on page 31

- g. rts the busied MS, this will trigger a restart of the local MS code, which enables the software to find the OC3 paddleboard¹

>rts <ms_number>

- h. add the datafill into the MS card inventory table, MSCDINV

>table mscdinv

>ove

>format pack

>add <ms_#> <shelf_#> <card_#> <link_#> DS512 NT9X17AD
NT9X63AB 2

>yes

- i. bring the OC3 paddleboard into service

Repeat steps above for MS 0.

75.3 Hardware Requirements or Dependencies

The customer will require a set of OC3 paddle boards with associated front cards. The OC3 paddleboard inserted on the MS to be used for the CBM 860 communication is identified with the PEC (Product Equipment Code) of NT9X63AB. The front circuit pack card on the MS should be the NT9X17AD card.

75.4 Software Requirements or Dependencies

No Dependencies

75.5 Limitations and restrictions

A restriction for using the NT9X63AB OC3 paddleboards is the card location on the MS shelf that the paddleboard may be inserted into. Allowable card locations are listed in Table 1: Provisionable paddleboard locations.

The best method for choosing a slot to use is to start from the lowest card number² and use the first available location. The OC3 inserted in each MS shelf should have matching card locations.

Please note that in description and table below, slot is referred to as the physical location on the hardware frame of the MS and the card number is the logical number that is seen from the MAP level and when datafilling the card in table MSCDINV.

¹If not seen or the PEC read fails, the user will be unable to rts with a pec mismatch error given.

²Please refer to Table 1: Provisionable paddleboard location for the card numbers to use.

On an SNSE, if inserted in card 5, slot 15R, for MS0, it should also be in card 5, slot 24R, of MS1.

Or on a SN, if inserted in card 6, slot 12R, for MS0, it should also be in card 6, slot 12R, of MS 1.

Table 1 Provisionable paddleboard locations

MS Configuration	Provisionable Slots	Card Location Equivalent
SuperNode (SN)	12R up to 27R	cards #6 up to #21
Super Node System Enhanced (SNSE) MS0	11R up to 15 R	cards #5 up to #9
Super Node System Enhanced (SNSE) MS1	24R up to 28R	cards #5 up to #9

75.6 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__

75.7 Glossary

Table 2

Term	Description
BRISC	BNR Reduced Instruction Set Computer (DMS Core)
CBM	Core and Billing Manager

Table 2

Term	Description
CBM 800	OC3 connected simplex CBM
CBM 860	OC3 connected duplex HA CBM
CMIC	Computing Module Interface Card
DMS	Digital Multiplexing Switch
HA	High Availability
MAP	Maintenance and Administration Position (core I/O terminal)
MS	Message Switch
MSCDINV	Message Switch Card Inventory
OC3	Optical Carrier- Level 3 (transmission interface)
PEC	Product Equipment Code
SN	SuperNode
SNSE	SuperNode System Enhanced

75.8 Recommended Reading/References

DMS-100 Card Replacement Procedures document (297-9051-547),
DMS SN and SNSE Message Switch Maintenance Guide (297-5001-549)

76: A00007300 Functional description (FN)

76.1 Feature name

Enable by default IPSec on All GWC Profiles

76.2 Description

This SN08 activity enables IPSec on all GWC profiles that do not currently have the IPSec capability. As a result of enabling IPSec on all remaining GWC profiles, the IPSec provisioning tab will now be available in the CS2000 Management Tools GUI for all GWC profiles.

76.3 Hardware Requirements or Dependencies

Not applicable

76.4 Software Requirements or Dependencies

Not applicable

76.5 Limitations and restrictions

Not applicable

76.6 Interactions

Not applicable

76.7 Glossary

Term	Description
GWC	Gateway Controller
IPSec	IP Security

77: A00007302 Functional description (FN)

77.1 Feature name

SN08 IEMS-CEM Integration

77.2 Description

This feature integrates the functionality of CEM (Core Element Manager) to the IEMS (Integrated Element Management System).

CEM includes the Resource Discovery (RD), Fault Management (FM) and Performance Management (PM) support for wireline succession core (call server). Adding, deleting and managing CEM will be possible from IEMS.

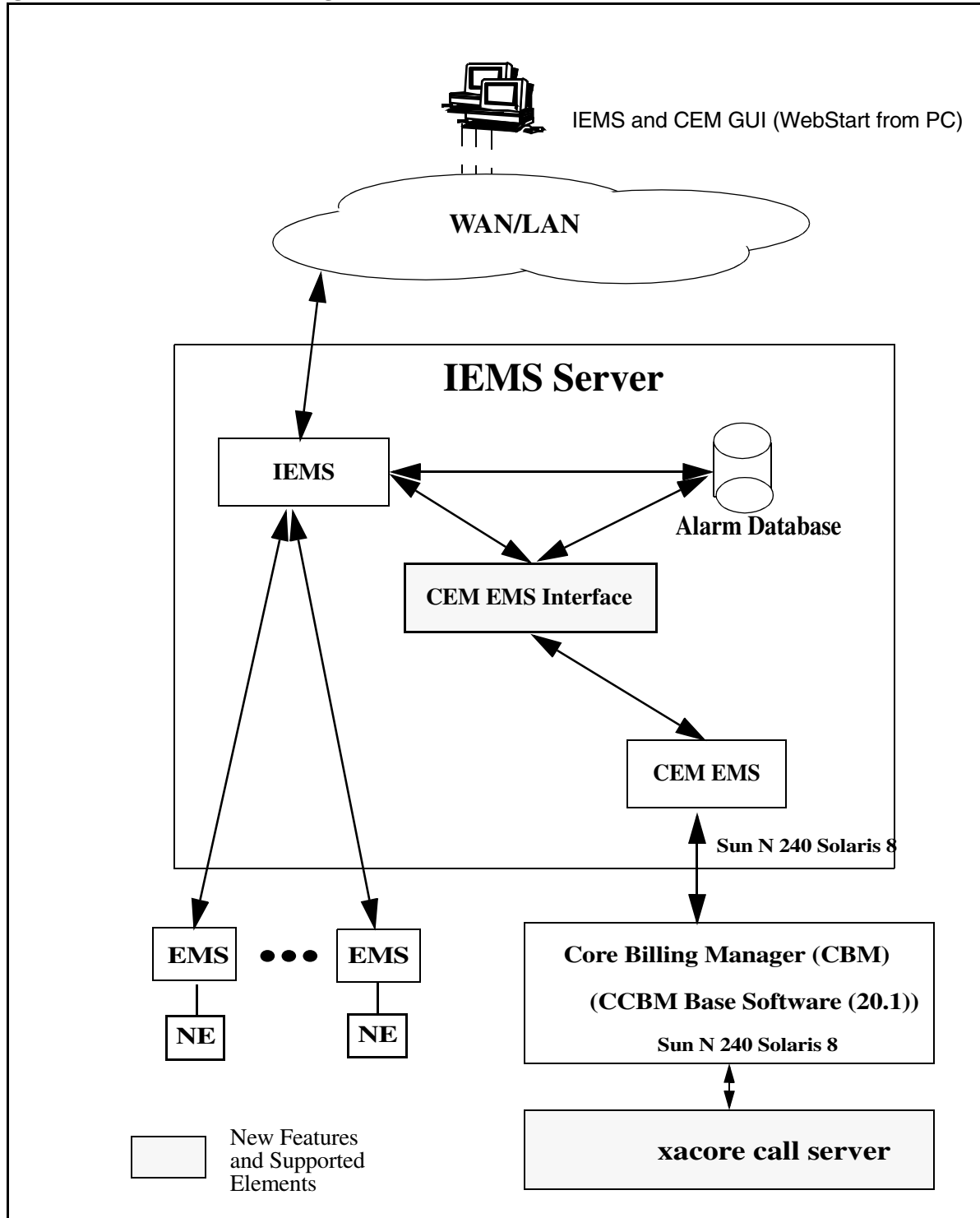
IEMS is comprehensive OAM&P solution with aggregated OSS interfaces, central browser and launching point and with unified security management.

The Core Element Manager system is the Nortel implementation of a Element Management System which provides

- An interconnection between the specific management applications that are on workstations and operated by systems personnel, over a Local Area Network/Wide Area Network (LAN/WAN) using Transmission Control Protocol/Internet Protocol (TCP/IP).
- An exchange of management information (data) between the management applications and the various elements of the Core Network elements. In the Circuit Core Network, the management application is the Core Element Manager, installed on a PC or Sun platform.
- Mediation functionality (data accumulation, filtering, manipulation, and transfer) between the network elements and the Core Element Manager workstation.

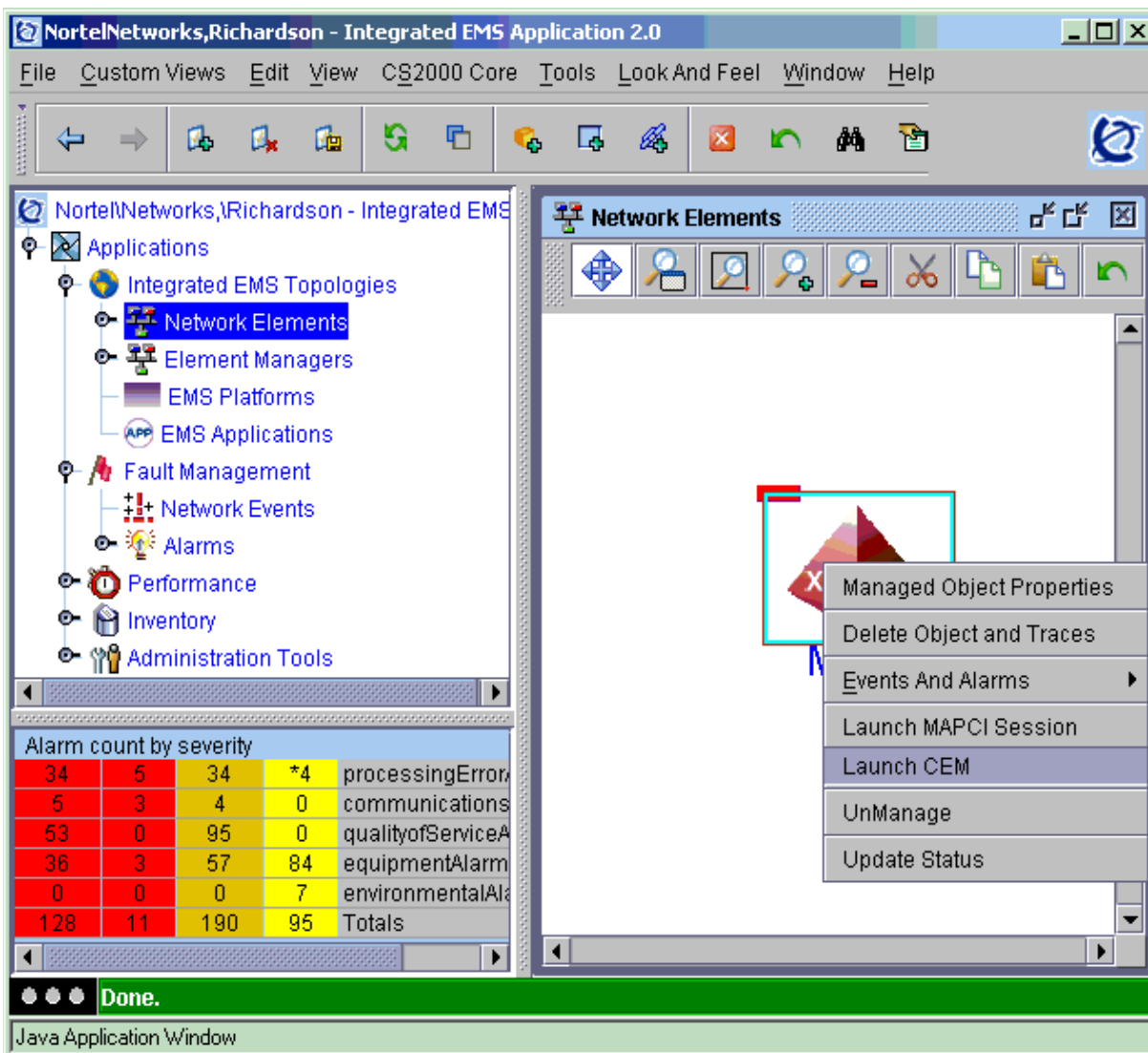
An overview for the integration of IEMS to CEM is shown in Figure 1 below:

Figure 1 Functional Behavior Diagram



77.2.1 Launching CEM From IEMS.

The CEM Browser is launched by selecting the NE from the “Element Manager” subtree in the left panel. Upon the right click on the NE icon, a menu list is invoked where “Launch CEM” can be selected to invoke the CEM Browser.



77.2.2 CEM components

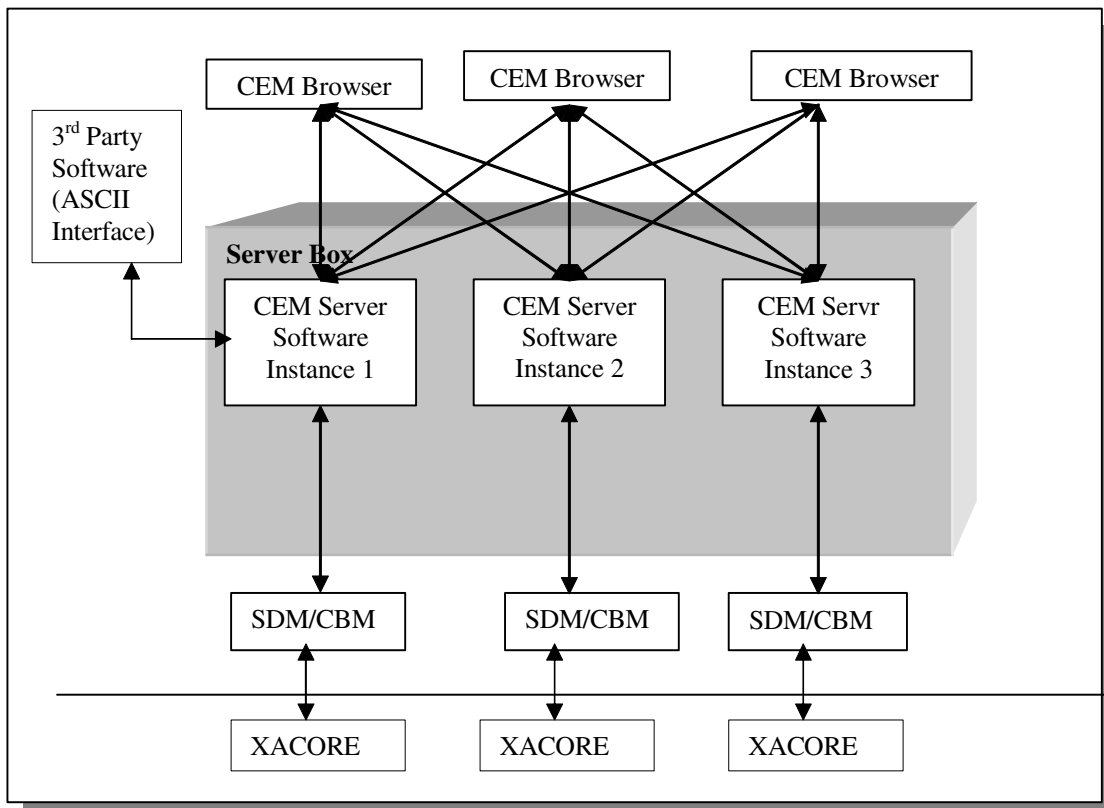
The CEM software includes the Core Element Manager GUI, CEM Server, and OMC-S in CBM.

- Core Element Manager Browser: The GUI works on a PC or SUN Platform as a facilitator interaction between operations, administration,

maintenance, and provisioning (OAM&P) personnel and the network elements.

- Core Element Manager (CEM) Server runs in a solaris box. The CEM server does back end work for performance management, fault management, configuration management and security management. Multiple instances of CEM server software can run in the sun server, each instance connecting to one cbm.
- CBM is the mediation device which connects to the network element and get raw data such as OMs, logs and also the table data and pass this information to the cem server software.

Figure 2 CEM Server Architecture



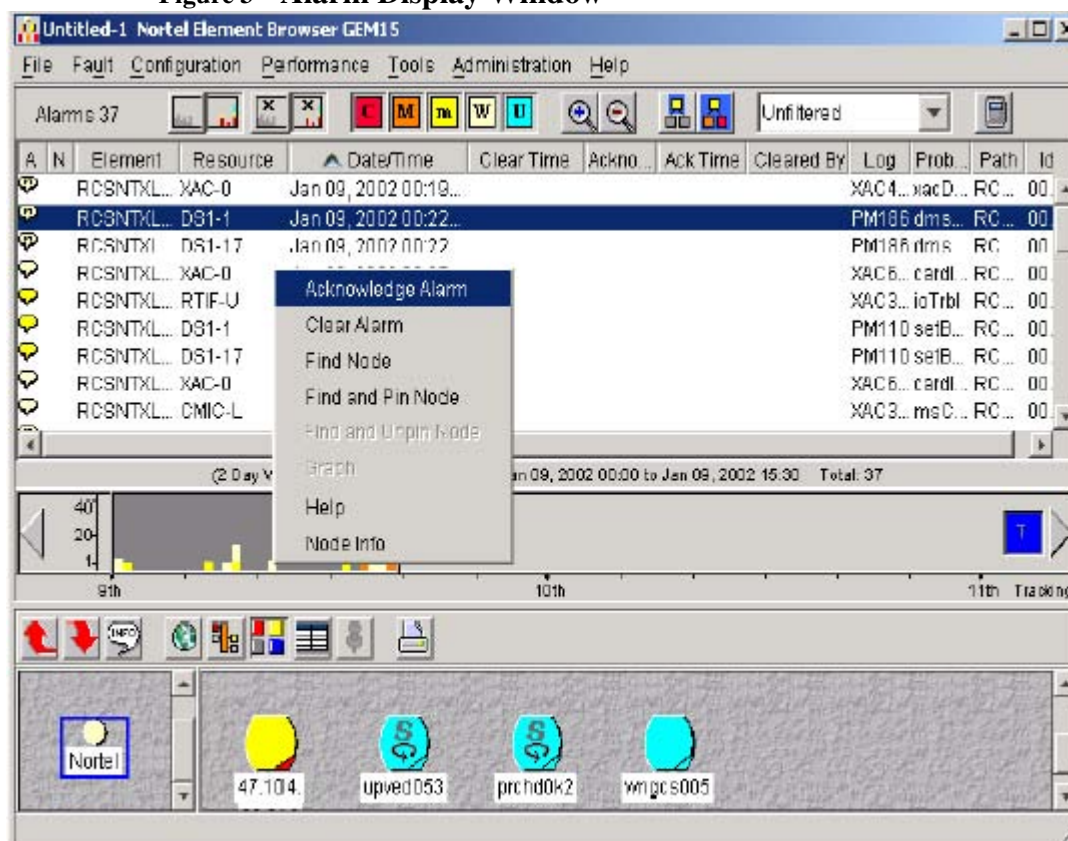
These three components together performs the performance management, configuration management, fault management and security management functionality of an element management system.

Fault Management

The Fault Management (FM) function displays logs of alarm or fault events that occur within the network usually within a switch node. These alarms or events may have an impact on the overall service of the network element. To aid you in correcting any problems with a network element, the Fault Management function gives you information about the element so you can

perform further maintenance operations. To help manage the alarms or events that occur within the network, Fault Management provides the following capabilities:

- displays alarms for a specific switch node. When a repeated alarm occurs for the same problem and the same resource, the most current alarm is shown. The previous alarms are kept as cleared alarms.
- displays a time-based histogram of alarm activity for time periods of 1 to 30 day. By default, the retention period is 30 days for uncleared alarms and 7 days for cleared alarms.
- displays alarms by alarm type (active, cleared, manual, and/or cleared manual alarms)
- displays alarms by selected severities (Critical, Major, Minor, Warning, unknown, or any combination)
- displays the element color to reflect the current alarm status
- displays alarms for specific filters, and causes specific actions to happen
- provides alarm notifications as they occur within the underlying resources
- exports alarm data to file
- prints alarm data
- provides filter criteria for alarms
- provides online help for alarms
- provides actions triggered by alarms

Figure 3 Alarm Display Window

Configuration Management

The Configuration Management function allows you to manage network elements (call server) within a circuit core network. The Configuration Management identifies the configuration and status of the network when it is initialized. The network elements are identified by icons and are arranged according to the network hierarchy. The Element Manager displays complete information for each target network element and its subordinate elements. The configuration display is updated automatically by the Configuration Manager maintaining consistency between the Element Manager display and its managed objects. This display is called containment tree.

The Configuration Manager includes the following features:

- Physical, Logical, icon, or List views from the Element Manager
- Pin and Unpin nodes
- nodes sorted by name or severity
- find carriers and linksets
- saving and retrieving of notes for nodes
- table access (add/read/delete/modify tuple operations)

- custom wizards to create/modify/delete trunks and other table access operations
- integration with performance management
- launch the Threshold Management window for a PM resource
- threshold management information in the info window for PM resources (last Value: Critical, Major, Minor)
- threshold crossed information in the info bubble
- Performance Management information in the info window for PM resources (pmCurrentData)
- Print support for CM window.

Figure 4 Configuration Management Window in Icon view

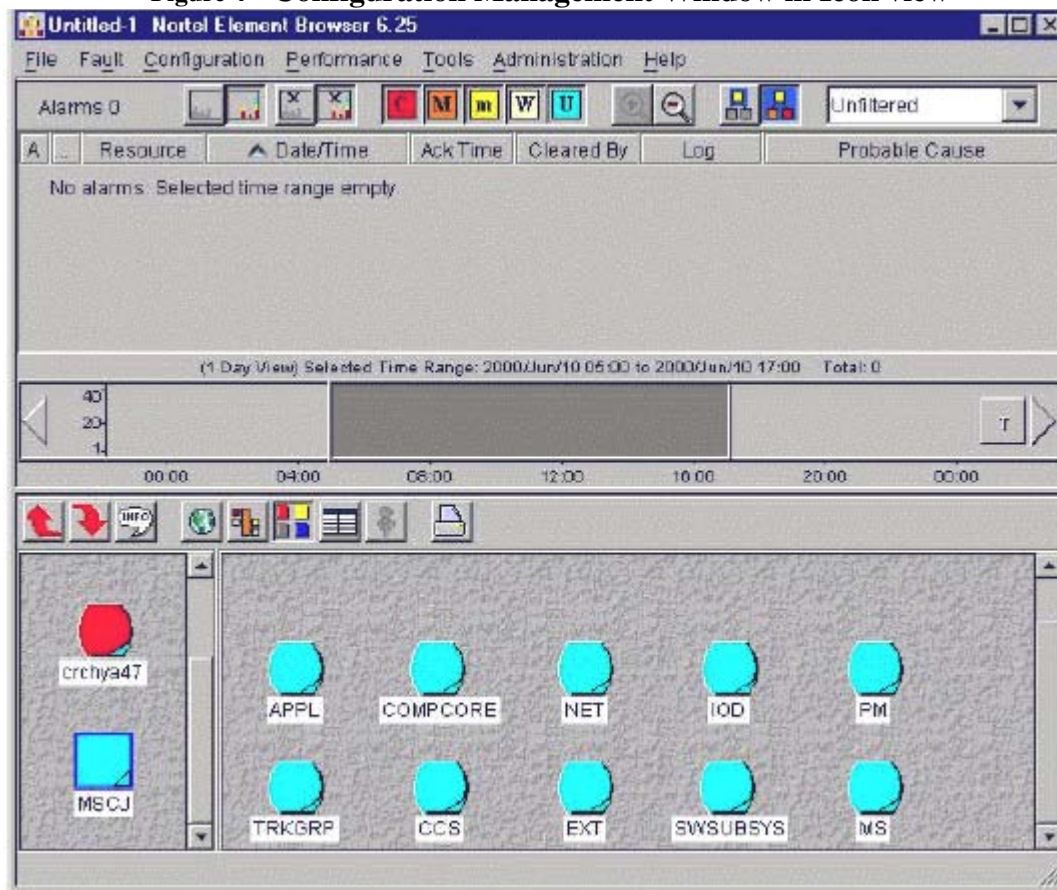


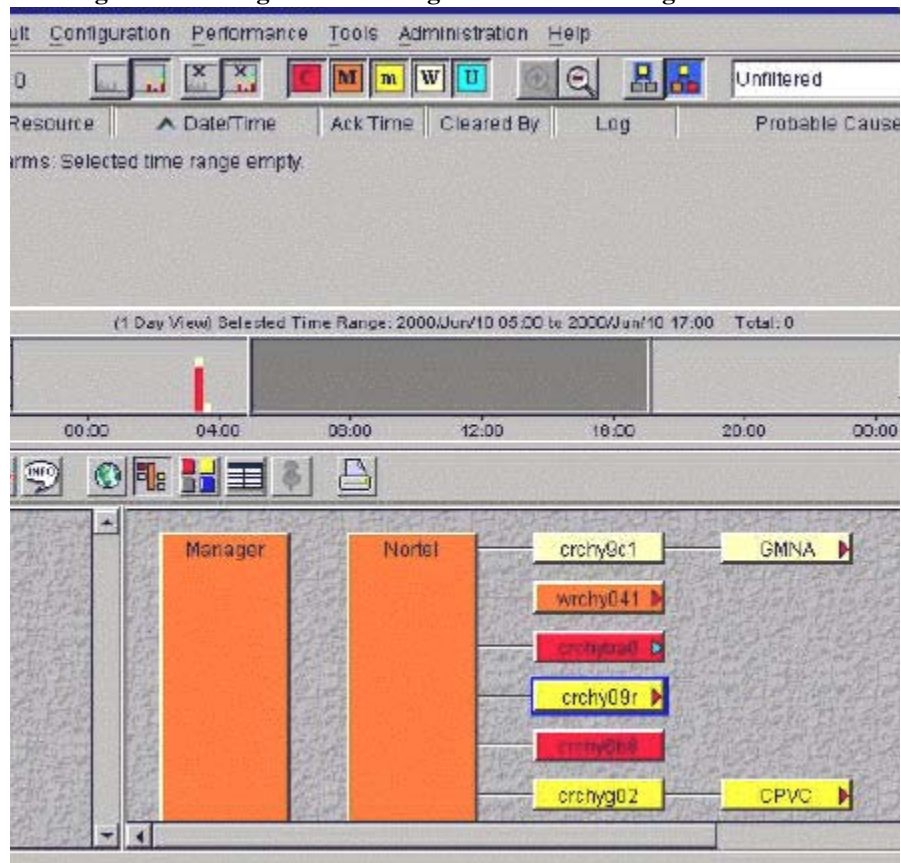
Figure 5 Configuration Management window in logical mode

Figure 6 Configuration Management Window in List view

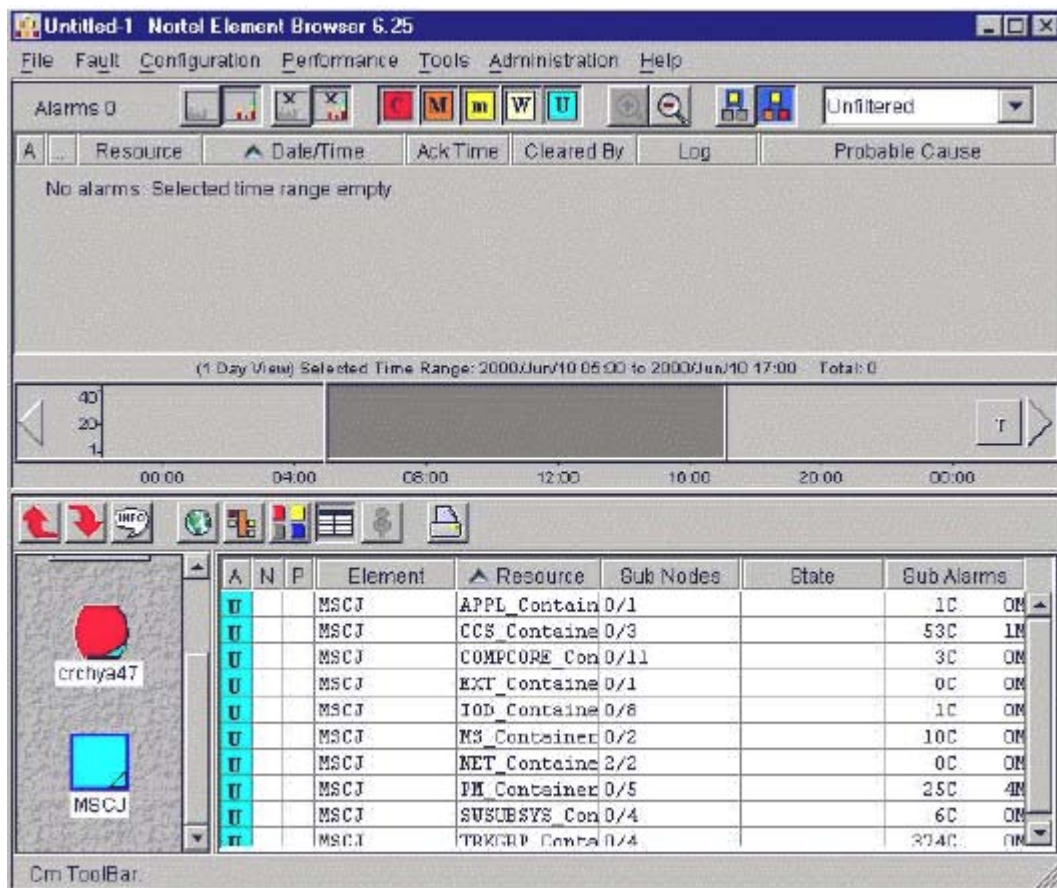


Figure 7 Configuration Management: Info Window

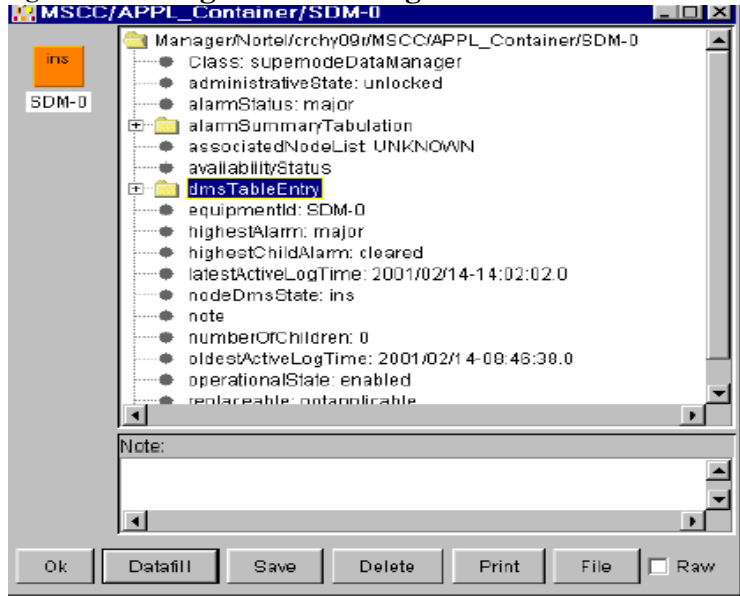
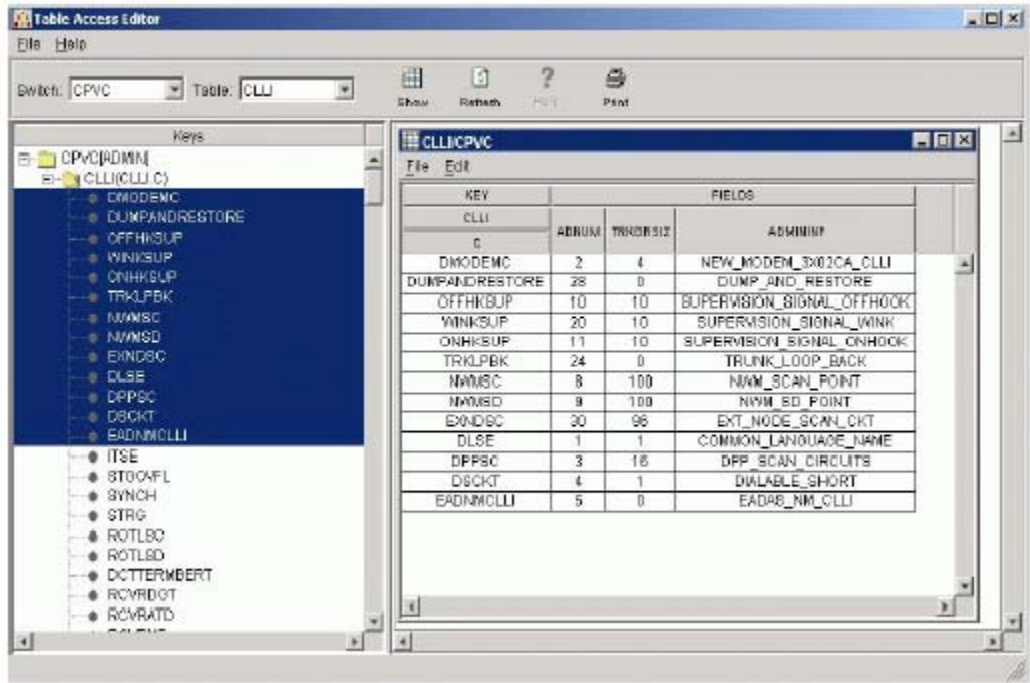


Figure 8 Table Access Editor



Performance Management

The Operational Measurements (OM) system provides the operating company with the following measurements for the Circuit Core Networks (CCN) Call Server:

- switch performance measurements
- traffic measurements
- service data

You can view OM records to ensure that the CS switch operates at its fullest potential with optimum efficiency. New OM data is transferred from the switch every transfer period, such as every 15 or 30 minutes.

The Performance Management (PM) functionality does the following:

- Provides access to OMs in predefined measurement groups
- Displays OMs in operator-configurable studies, including a graph of specific OMs over a given timeframe
- Configures real-time updates of OMs with the CS transfer period as the minimum update frequency
- Allows exports and mass exports of OMs to files in two formats, the original switch text format, or a tab-delimited format for use by third-party applications such as spreadsheets or graphing utilities
- Displays data from multiple network elements on the same graph
- Displays errors, such as incomplete OM data for the requested study
- Sends the output display to printer
- Allows OM threshold settings
- Displays summary reports on a network elements

Figure 9 Performance Management: Instant Graphing Window

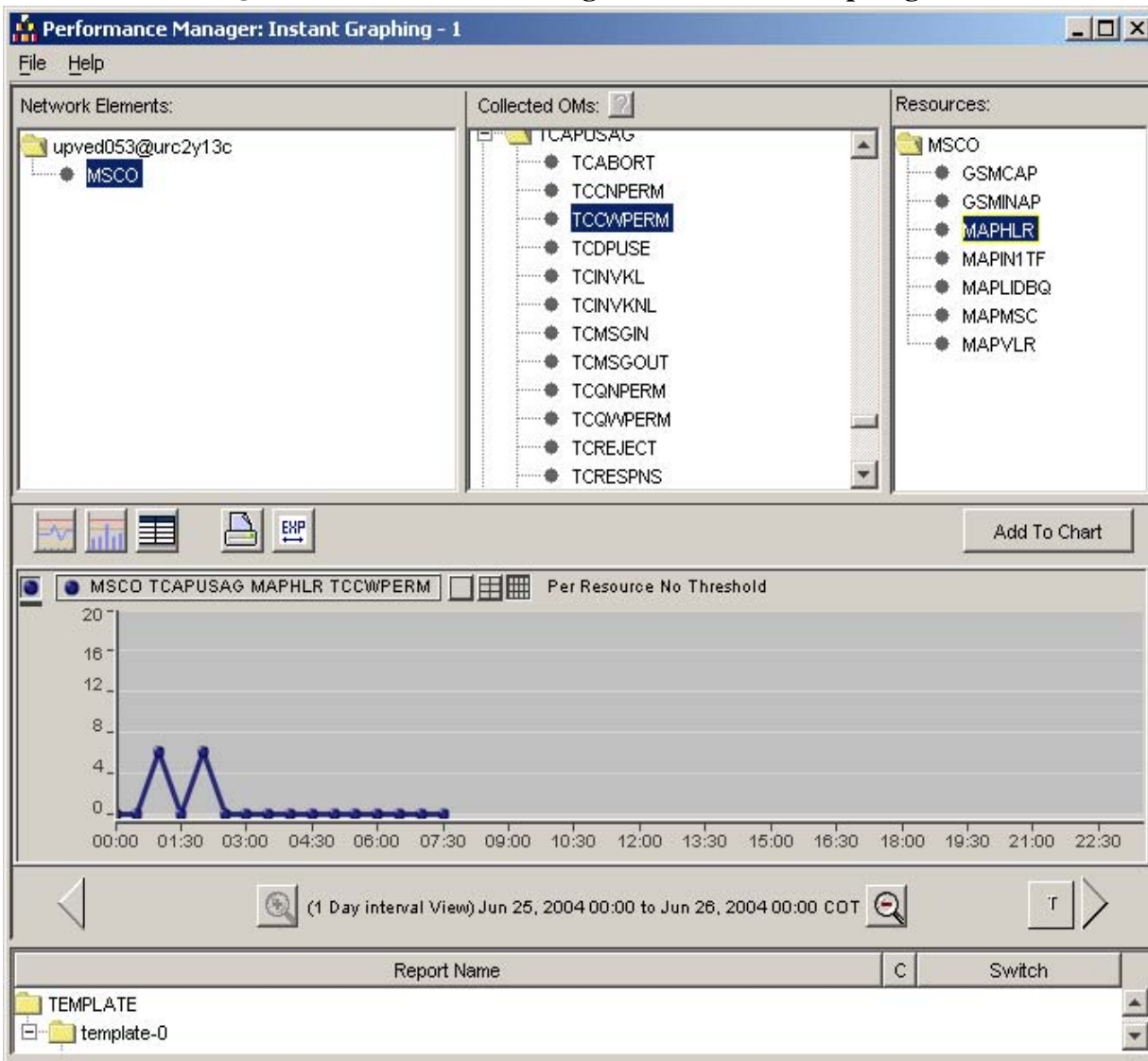
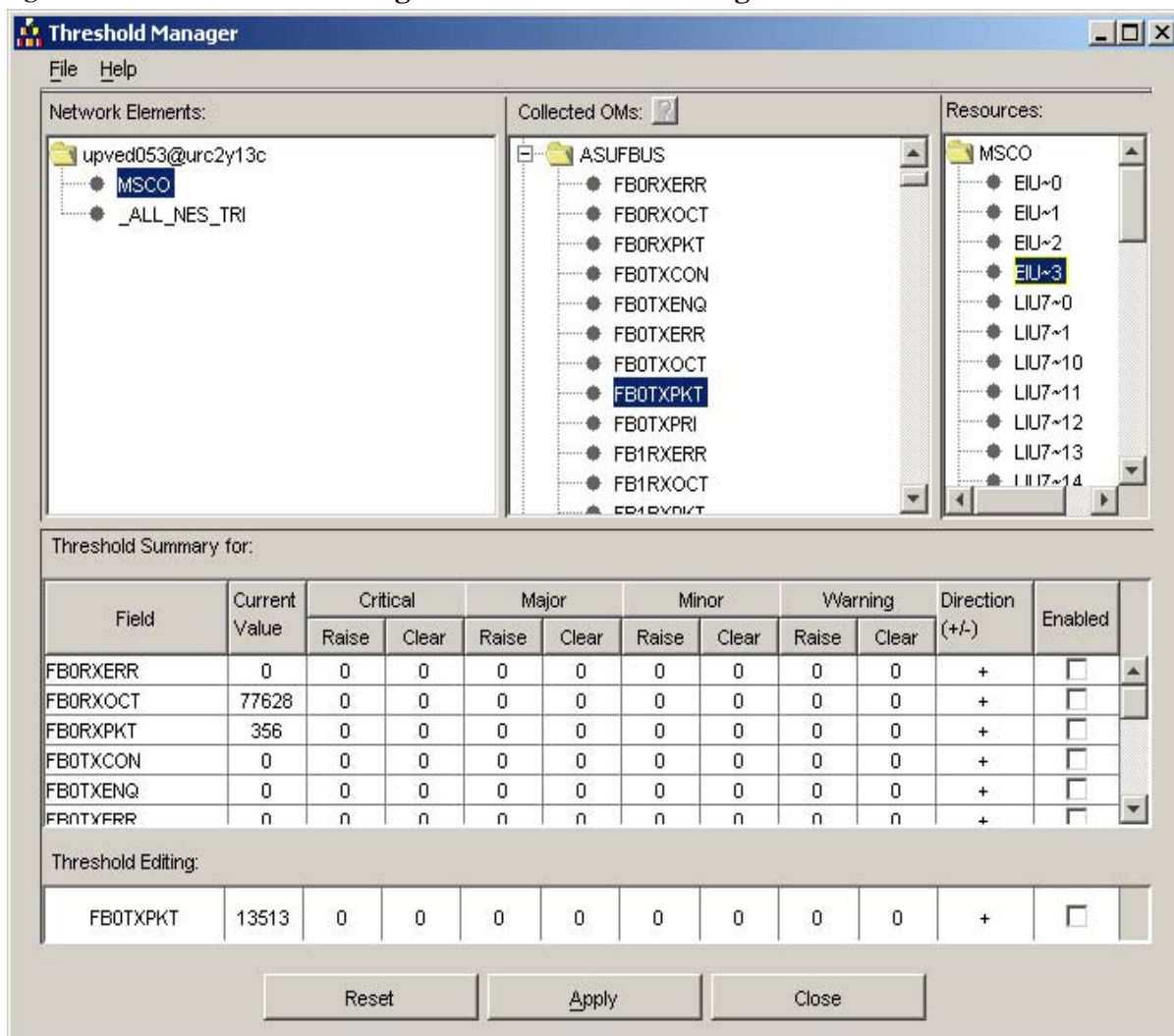


Figure 10 Performance Management: Threshold Manager Window

Security Management

It is necessary to restrict access to the CEM browser to only users with valid login credentials. The security framework on the CEM system is provisioned with the functionality like login to access the CEM browser, encrypted login credentials, account lockout due to consecutive failed login attempts, change password capability, configuration of the Telnet or FTP session, timeout interval periods, generate Security Alarms and Event Logs (Journal File).

77.2.3 Launching CEM from IEMS

The integration of CEM into IEMS will enhance the capabilities of IEMS to manage the cs2k node through the CEM. Alarms from cs2k are stored in the IEMS alarm database and displayed in the existing alarm panel in the IEMS GUI.

77.2.4 Discovery of new resources

The resource discovery is implemented by extracting call server switch configuration data via the dmsDataServer. The status of resources are discovered through remote procedure calls (RPC's) on the core from rpcServer process on CBM. This feature ensures that all the tables representing the call server switch resources are discovered. The Table Access function in the CEM Browser supports all the tables residing in the call server switch.

The new RPC's will discover following resources:

- GWC (packetized lines and trunks)
- MG4K (packetized AAL1 trunks)
- IWSPM (hybrid interworking)
- LTC, LGC, SMA (legacy lines peripheral)
- LCD type nodes (legacy lines) – LCM, RDT, RCC
- ABI (packetized legacy lines)
- DPT (virtual trunks, BICC and SIP-T)

77.2.5 Support for New OM's

For the PM functionality, accumulation for all the call server OM's are supported. Pre-canned studies for the current DMS-MSC OM's that are common to the call server are also supported. OM groups can be selected and exported in tab delimited format or switch format which is exactly the way they appear in the core. Also OM group studies (graphical and text) are possible from the CEM GUI for the past OM reports. The extension OM groups and OM registers will be combined with base groups and registers. Please refer to the Appendix B for the OM's supported in this feature. These will be available through the interfaces provided by CEM. The existing performance subsystem in IEMS does not change.

77.2.6 Mapping of new logs

Alarms from the core will be mapped to their respective components in the containment tree. Please refer to the Appendix A of DID (Design Intent Document) for the logs supported in this feature.

77.2.7 Single authentication for IEMS and CEM

User will be required to enter the user's name and password as the IEMS login window. The userid will then be passed down to CEM.

77.2.7.1 Password Management and User Access Control

All password management and user access control will be done through Succession's central security admin system. CEM will be using the SSPFS user defined groups for user access control.

77.2.8 Configuration Tools

By default CEM Server supports logs for which there is a mapping defined but An configuration script/tool can be used to configure other logs (for which there is no mapping) coming from succession core.

Using this tool any logs that are coming from succession core can be unblocked and passed through to CEM Server. Such logs that are by default blocked, but later unblocked, get mapped into default containers in the CEM containment tree.

77.2.8.1 Addrep/Delrep Tool

A tool called llClient (log list client) on the CEM Server could be used to addrep or delrep the logs coming from the core. The tool provides the below listed functionalities -

- addrep - to pass through a log coming from core so that CEM will be able to receive the log
- delrep - to block a log coming from core so that the log will not be received by CEM
- addrep all - to pass through all logs coming from core so that CEM can receive all of them

Usage:

1. On the CEM Server, login as user nortel or root and change directory to /opt/nortel/exe/coreEMS/GEM18/llClient/dat/.
2. Edit the SDM_HOST parameter value and give the hostname of the SDM/CBM, slicename or the IP Address of the SDM/CBM the server is connected to.
3. Change directory to /opt/nortel/exe/coreEMS/GEM18/llClient/bin/.
4. Issue command: ./logListClient.start <operation> <logType> <logNumber>, where, operation is addrep or delrep, logType is the log name to addrep or delrep and logNumber is the number of the log to addrep or delrep.

[Note: Use “NIL” as logNumber to addrep or delrep all logs of a type.]

5. To make the addrep of the log function, the logNormalizer process must be busy/rts'ed using command line tool applman (Application Manager) on the CEM Sun Server. This tool is used to stop and start the CEM related processes running on the CEM Sun Server. Follow steps below for doing the same -

- a) On the CEM Server, change the directory to /opt/nortel/data/coreEMS/nodes/server/bin

- b) Issue the command `./applman -c`
- c) Issue command down OMC-S
- d) Issue command down `<slicename>`
- e) Issue command `busy logNormalizer`
- f) Issue command `rts logNormalizer`
- g) Issue command `exit` to exit from `applman`
- h) Issue command `help` to know all the available options in `applman`

5. Use “all” to address all logs. Usage - `./logListClient.start address all`.
To restore to the previous configuration, follow steps below -

- a) Login to the SDM/CBM as root.
- b) Change directory to `/sdm/configdata/lsv` in case of SDM or `/cbmdata/configdata/00/lsv` in case of CBM.
- c) Issue command: `cp cmlogs.config.old cmlogs.config`
- d) Busy and Rts the `logDelivery` process using `sdmmtc` on the SDM or using `cbmmtc` on the CBM.

77.2.9 CEM Processes for handling OMs and Logs

77.2.9.1 Data Server process

The `dmsDataServer` process runs on the Core Billing Manager (CBM) platform, connects to call server node and receives both the Performance and Configuration data through Base APIs (Table Access Service and OM Access Service). Depending on whether its operational measurements (OM) or configuration data, it forwards it to performance manager or configuration manager respectively.

The following warning/error/information messages are generated in `cutlog` to reflect various problems. These messages can be seen in `/var/adm/custlog` file to find exact cause and fix.

- 1. Desc Msg: Could not read switch name

Fix Msg: Check state of switch
- 2. Desc Msg: Could not create tuple

Fix Msg: Check state of switch

-
3. Desc Msg: Could not read VRINV table
Fix Msg: Check state of switch
 4. Desc Msg: Could not initialize OM Acss
Fix Msg: Contact system administrator
 5. Desc Msg: Could not initialize OM Acss
Fix Msg: Contact system administrator
 6. Desc Msg: Could not get keyinfo object, excluding group , <group>
Fix Msg: Check OM group for bad key/info type
 7. Desc Msg: Could not get key, excluding group , <group>
Fix Msg: Check OM group for bad key type
 8. Desc Msg: Could not get info, excluding group , <group>
Fix Msg: Check OM group for bad info type
 9. Desc Msg: Could not register initialization timer
Fix Msg: Contact administrator
 10. Desc Msg: Rejecting register request for excluded group: <group>
Fix Msg: Check group key/info for validity
 11. Desc Msg: "Could not open listening connection
Fix Msg: Check /etc/services
 12. Desc Msg: Could not open listening connection: <service name>
Fix Msg: Check services file

77.2.9.2 NLClient and NLServer

The operational measurements (OM) are available on the CEM server for graphing, dashboard, thresholding, mass export and correlation. The CEM server gets all the performance data from CBM through NLServer and nlSafServer processes running on CBM platform. The nlClient process running on the IEMS server receives OM data from nlSafServer and NLServer, process it and forward it to the upstream processes. All these

processes makes the handling of OM data easier and faster. It offloads the load on CEM server in processing OM data.

The nlClient process will generate the following warning/error/information messages in cutlog to reflect various problems. These messages can be seen in /op/nortel/logs/coreEMS/custlog file to find exact cause and fix.

1. Desc Msg: Failed to Read NLClient listenconfiguration

Fix Msg: update the NLClient.cfg file

2. Desc Msg: Failed to Read NLServer Service configuration

Fix Msg: update the NLClient.cfg file

3. Desc Msg: Failed to Read ConfigBroker Service configuration

Fix Msg: update the NLClient.cfg file

4. Desc Msg: Failed to Read SafServer Service configuration

Fix Msg: update the NLClient.cfg file

5. Desc Msg: Failed to read NLClient config file

Fix Msg: Contact next level of support

6. Desc Msg: Failed to register synchronous listen connection

Fix Msg: Contact next level of support

7. Desc Msg: Failed to initialize synchronous listen connection at service

Fix Msg: Contact next level of support

8. Desc Msg: Communications not initialized

Fix Msg: Contact next level of support

9. Desc Msg: Failed to register for connection to safServer at service
<safConnectService>

Fix Msg: Contact next level of support

10. Desc Msg: Input from unknown end point

Fix Msg: Contact next level of support

11. Desc Msg: Failed to register for connection to nlServer at service <nlConnectService>

Fix Msg: Contact next level of support

12. Desc Msg: Failed to register for connection to nlServer at port <portnum>

Fix Msg: Contact next level of support

13. Desc Msg: Receive from NLServer failed

Fix Msg: Contact next level of support

14. Desc Msg: Lost connection to Cfg Broker

Fix Msg: Check CfgBroker Processes

15. Desc Msg: Receive from Data Collector failed

Fix Msg: Contact next level of support

16. Desc Msg: Unknown command received from archive client

Fix Msg: Contact next level of support

17. Desc Msg: Can not read command from synchronous client

Fix Msg: Contact next level of support

18. Desc Msg: Error while doing a send, discarding send queue

Fix Msg: Check Client Processes

19. Desc Msg: exiting due to failure in memory allocation

Fix Msg: restart the process after verifying the memory availability in the system

20. Desc Msg: Failed to Read NLClient listenconfiguration

Fix Msg: update the NLClient.cfg file

The following warning/error/information messages in cutlog will be generated by the NLServer and nlSafServer to reflect various problems. These messages can be seen in /var/adm/custlog file on the CBM to find exact cause and fix.

1. Desc Msg: Failed to register for connection to export Server at service <service name>

Fix Msg: Contact next level of support

2. Desc Msg: Failed to register for connection to Data Server at port <port number>

Fix Msg: Contact next level of support

3. Desc Msg: Failed to register for connection to Data Server at service <service name>

Fix Msg: Contact next level of support

4. Desc Msg: Failed to register for signals

Fix Msg: Contact next level of support

5. Desc Msg: Failed to send error

Fix Msg: Check SAFServer Process

6. Desc Msg: Communications not initialized

Fix Msg: Contact next level of support

7. Desc Msg: Input from unknown end point

Fix Msg: Contact next level of support

8. Desc Msg: Failed to send registration message to Data Server

Fix Msg: Check Data Server Process

9. Desc Msg: Failed to send deregistration message to Data Server

Fix Msg: Check Data Server Process

10. Desc Msg: Invalid Message from archive.

Fix Msg: Contact next level of support.

11. Desc Msg: store is disconnected:deregister the connection

Fix Msg: Check Archive Process

12. Desc Msg: Receive from Archive failed

Fix Msg: Contact next level of support

-
- 13. Desc Msg: Unreadable Data Server message type
 - Fix Msg: Contact next level of support
 - 14. Desc Msg: Unreadable OM report
 - Fix Msg: Contact next level of support
 - 15. Desc Msg: Failed to send correlation error data to Archive
 - Fix Msg: Check Archive Process
 - 16. Desc Msg: OM Registration failed
 - Fix Msg: Contact next level of support
 - 17. Desc Msg: Unreadable registration response
 - Fix Msg: Contact next level of support
 - 18. Desc Msg: OM DeRegistration failed
 - Fix Msg: Contact next level of support
 - 19. Desc Msg: Unreadable deregistration response from Data Server
 - Fix Msg: Contact next level of support
 - 20. Desc Msg: Failed to send CM info request to Data Server
 - Fix Msg: Check Data Access Layer Process
 - 21. Desc Msg: Failed to send deferred registration message to Data Server
 - Fix Msg: Check Data Access Layer Process
 - 22. Desc Msg: Failed to send re-registration message to Data Server
 - Fix Msg: Check Data Access Layer Process
 - 23. Desc Msg: Fatal status change
 - Fix Msg: Check Data Access Layer Process
 - 24. Desc Msg: Unreadable OM status received from Data Server
 - Fix Msg: Contact next level of support
 - 25. Desc Msg: Could not get GroupInfo
-

Fix Msg: Contact next level of support

26. Desc Msg: Failed to send nlGrpInfoRsp data to Archive

Fix Msg: Check Archive Process

27. Desc Msg: Unreadable CM info message from Data Server

Fix Msg: Contact next level of support

28. Desc Msg: Could not open License File

Fix Msg: Verify file existence and permission

29. Desc Msg: Unexpected message type from Data Server

Fix Msg: Contact next level of support

30. Desc Msg: Lost connection to Data Server

Fix Msg: Check Data Server Process

31. Desc Msg: Receive from Data Server failed

Fix Msg: Contact next level of support

32. Desc Msg: Communications not initialized

Fix Msg: Contact next level of support

33. Desc Msg: Failed to send end_of_report msg to store

Fix Msg: Check Archive Process

34. Desc Msg: Connection from unknown end point

Fix Msg: Contact next level of support

35. Desc Msg: Switch name unknown

Fix Msg: Contact next level of support

36. Desc Msg: Arithmetic overflow in correlation <correlation name>

Fix Msg: Contact next level of support

37. Desc Msg: Failed to send OM data to Archive

Fix Msg: Check Archive Process

38. Desc Msg: Error while doing a send to the Agent, discard send queue

Fix Msg: Check Agent Process

39. Desc Msg: Port for the service <NLservice name> is not available.

Fix Msg: Please update /etc/services file & restart NLServer

40. Desc Msg: Failed to register for connection to export Server at service <service name>

Fix Msg: Contact next level of support

41. Desc Msg: Failed to register for connection to Data Server at port <port num>

Fix Msg: Contact next level of support

42. Desc Msg: Failed to register for connection to Data Server at service <service name>

Fix Msg: Contact next level of support

77.2.9.3 log Normalizer and logNormSAF Process

The fault data on being received from call server node is processed by logNormalizer process running on CEM. The logNormSAF process(running on the CBM platform) stores and forward this data to the CEM server.

The logNormalizer process generates error/warning/information messages in custlog whenever there is a problem encountered due to improper configuration, improper log formats etc. These messages can be seen in /opt/nortel/logs/coreEMS/custlog file to find the description and fix of the problem.

1. Desc Msg: Event file <EventFileName> was not found ...logNormalizer exiting

Fix Msg: Check Path.

2. Desc Msg: Event delimiter cannot be more than one charcter long ...logNormalizer exiting

Fix Msg: check event formatter file for the delimiter after a event name and use it

3. Desc Msg: Event file "<<EventFileName<<" is empty ..logNormalizer exiting

Fix Msg: check path, file name and/or read write permission

4. Desc Msg: Event file "<<EventFileName<<" had errors ..logNormalizer exiting

Fix Msg: please look at the event file to check errors

5. Desc Msg: Mapper file "<<MapperFileName<<" was not found ...logNormalizer exiting

Fix Msg: check path, file name and/or read write permission

6. Desc Msg: Mapper delimiter cannot be more than one charcter long ...logNormalizer exiting

Fix Msg: check mapper file for the delimiter after a log name and use it

7. Desc Msg: Mapper file "<<MapperFileName<<" is empty ..logNormalizer exiting

Fix Msg: check path, file name and/or read write permission

8. Desc Msg: Mapper file "<<MapperFileName<<" has errors .."<<argv[0]<<" exiting

Fix Msg: please check the mapper file errors

9. Desc Msg: Mapping information parsing error for log "<<logName<<" empty information or wrong delimiter used

Fix Msg:

10. Desc Msg: output file "<<outputFileName<<" could not be opened

Fix Msg: No action possible

11. Desc Msg: lostLogFile "<<lostLogFileName<<" could not be opened

Fix Msg: Call Nortel Personal

12. Desc Msg: lostLogFile "<<outputFileName<<" is empty

Fix Msg: Call Nortel Personal

13. Desc Msg: lostLogFormat string is empty

Fix Msg: Call Nortel Personal

-
14. Desc Msg: lostLogTriggerSize is empty
Fix Msg: Call Nortel Personal
15. Desc Msg: lostLogVisibleMsg string is empty
Fix Msg: Call Nortel Personal
16. Desc Msg: lostLogVisLog string is empty
Fix Msg: Call Nortel Personal
17. Desc Msg: sdmLogList is empty
Fix Msg: Call Nortel Personal
18. Desc Msg: probeTimer string is empty
Fix Msg: No probe is assumed
19. Desc Msg: checkLen string is empty
Fix Msg: No checkLen is assumed
20. Desc Msg: No Lost Log Trigger message has been specified
Fix Msg: Call Nortel Personal
21. Desc Msg: Could not send events to agent. Agent removed from output list.
Fix Msg: No agents connected .. start an agent
22. Desc Msg: Unknown log format. No mapping will be done for input
Fix Msg: Contact Nortel Personal

77.3 Hardware Requirements or Dependencies

An IEMS server is required.

SDM/CBM is required

77.4 Software Requirements or Dependencies

- IEMS Load is required
- CEM Server software (GEM18) is required
- SDM/CBM (GEM18) software is required
- SN08 is required.

77.5 Limitations and restrictions

N/A

77.6 Interactions

This feature interacts with A00007304

77.7 Glossary

Table 1

Term	Description
CEM	Core Element Manager
IEMS	Integrated Element Management System
SDM	Supernode Data Manager
CBM	Core Billing Manager
PAM	Pluggable Authentication Module
OM	Operational Measurements
DMS-MSC	Digital Multiplex Switch-Mobile Switching Center

77.8 Appendix A: List of Supported Logs

Log	Event	Event Label
ESA120	INFO	ESA DATA GENERATION
ESA121	INFO	ESA DATA GENERATION FAIL
ATM 300	FLT	ATM LCD Alarm Raised
ATM 301	INFO	ATM LCD Alarm Cleared
ATM 501	INFO	ATM Signalling Status
ATM 600	INFO	ATM Address Registration
ATM 605	INFO	ATM Overload Event
ATM 806	TBL	ATM Packet Alarm
ATM 807	INFO	ATM Packet Alarm
BITS300	TBL	BITS Fault Report
BITS301	TBL	BITS Timing Link Degradation

BITS500	INFO	BITS Timing Link State Change
BITS600	INFO	BITS Fault Report Cleared
BITS601	INFO	BITS Timing Link Degradation Cleared
BITS610	INFO	Reference Quality Change
BOOT101	FAIL	(none)
C7UP104	INFO	GROUP CIRCUIT BLO/UBL
C7UP109	INFO	CQ STATE CHANGE
C7UP113	INFO	ISUP MTC TRBL
C7UP114	INFO	ISUP ALERT
C7UP120	FLT	INVALID RANGE FIELD
C7UP130	FLT	Hop Counter Expired
C7UP301	TBL	Insufficient HC Value
CARR300	RTS	CARRIER
CARR310	FLT	CARRIER
CARR320	FLT	CARRIER
CARR330	INFO	CARRIER
CARR331	INFO	CARRIER
CARR340	INFO	CARRIER
CARR341	INFO	CARRIER
CARR500	RTS	CARRIER
CARR501	CBSY	CARRIER
CARR510	MANB	CARRIER
CARR511	SYSB	CARRIER
CARR512	CBSY	CARRIER
CARR800	RTS	CARRIER
CARR801	INFO	CARRIER
CARR810	TBL	CARRIER
CARR811	TBL	CARRIER
CCMT301	FLT	Core PVC Segment Fault
CCMT501	INFO	Core Connection State Change

CCMT502	INFO	Peer Connection State Change
CCMT601	INFO	Core PVC Segment Fault Cleared
DPTM500	RTS	DPT Terminals INSV
DPTM501	SYSB	DPT Terminals OOS
DPTM502	MANB	DPT Terminals OOS
DPTM503	PBSY	DPT Terminals OOS
DPTM504	OFFL	DPT Terminals OOS
DPTM550	INFO	DPTRKS STATE CHANGE
DPTM560	INFO	DPTRKS STATE CHANGE
DPTM700	INFO	DPT Data Mismatch
DPTM701	INFO	DPT Data Mismatch Cleared
DPTM800	(none)	1st Threshold Exceeded
DPTM801	(none)	1st Threshold Cleared
DPTM802	(none)	2nd Threshold Exceeded
DPTM803	(none)	2nd Threshold Cleared
ENET308	INFO	(none)
ENET311	FAIL	ENET PSide Link Test
EXT 102	INFO	(none)
EXT 108	INFO	(none)
IWBM500	SYSB	IW_Bridges OOS
IWBM501	RTS	IW_Bridges INSV
IWBM603	INFO	IWBM Audit
IWBM800	(none)	1st Threshold Exceeded
IWBM801	(none)	1st Threshold Cleared
IWBM802	(none)	2nd Threshold Exceeded
IWBM803	(none)	2nd Threshold Cleared
LINK300	TBL	Transport Resource Fault
NODE300	TBL	Mismatch Fault
NODE301	TBL	Hardware Fault
NODE302	TBL	Software Alarm

NODE303	TBL	Wrong Application Data
NODE323	TBL	REx Fault
NODE326	TBL	Hardware Fault
NODE328	TBL	Hardware Fault
NODE450	SUMM	REx Test Summary
NODE500	INFO	Node State Change
NODE600	INFO	System Recovery Action
SDM 300	TBL	SDM Base Maintenance
SDM 301	TBL	SDM Base Maintenance
SDM 302	TBL	SDM Base Maintenance
SDM 303	TBL	SDM Base Maintenance
SDM 306	TBL / FLT	(none)
SDM 308	TBL	SDM Base Maintenance
SDM 309	TBL	SDM Base Maintenance
SDM 314	n/a	n/a
SDM 315	TBL	SDM Data Dictionary
SDM 317	TBL	SDM Base Maintenance
SDM 321	TBL	SDM Base Maintenance
SDM 327	TBL	SDM Base Maintenance
SDM 500	INFO	SDM Base Maintenance
SDM 501	RTS	SDM Base Maintenance
SDM 502	MANB	SDM Base Maintenance
SDM 503	SYSB	SDM Base Maintenance
SDM 504	TBL	SDM Base Maintenance
SDM 505	OFFL	SDM Base Maintenance
SDM 550	INFO	Node Status Change
SDM 600	INFO	SDM Base Maintenance
SDM 601	INFO	SDM Base Maintenance
SDM 602	INFO	SDM Base Maintenance
SDM 603	INFO	SDM Base Maintenance

SDM 604	INFO	Log Delivery Service: lost logs(CM side):XXX
SDM 608	INFO	SDM Base Maintenance
SDM 609	INFO	SDM Base Maintenance
SDM 617	INFO	SDM Base Maintenance
SDM 621	INFO	SDM Base Maintenance
SDM 627	INFO	SDM Base Maintenance
SDM 630	INFO	SDM Base Maintenance
SDM 650	INFO	SDM Link Report
SDM 700	INFO	SDM Base Maintenance
SDMB300	FLT	SDM BILLING SYSTEM
SDMB310	FLT	SDM BILLING COMMS
SDMB315	TBL	SDM BILLING SOFT ERROR
SDMB316	FLT	SDM BILLING PROC DEATH
SDMB320	TBL	SDM BILLING BACKUP
SDMB321	FLT	SDM BILLING BACKUP
SDMB330	FAIL	SDM BILLING CONFIG
SDMB350	FLT	SDM BILLING CONTROL
SDMB355	TBL	SDM BILLING DISK
SDMB360	TBL	SDM BILLING COMMS
SDMB365	TBL	SDM BILLING SOFT ERROR
SDMB367	FLT	SDM BILLING MIB
SDMB375	TBL	SDM BILLING FILE TRANSFER
SDMB380	FAIL	SDM BILLING CONFIG
SDMB390	TBL	SDM BILLING FILE TRANSFER SCHEDULE
SDMB400	SUMM	SDM BILLING SUMMARY
SDMB530	INFO	SDM BILLING CONFIG
SDMB531	INFO	SDM BILLING CONFIG
SDMB550	INFO	SDM BILLING CONTROL
SDMB600	INFO	SDM BILLING SYSTEM
SDMB610	INFO	SDM BILLING COMMS

SDMB615	INFO	SDM BILLING SOFT ERROR
SDMB620	INFO	SDM BILLING BACKUP
SDMB621	INFO	SDM BILLING BACKUP
SDMB625	INFO	SDM BILLING RECOVERY
SDMB650	INFO	SDM BILLING CONTROL
SDMB655	INFO	SDM BILLING DISK
SDMB660	INFO	SDM BILLING COMMS
SDMB675	INFO	SDM BILLING FILE TRANSFER
SDMB680	INFO	SDM BILLING CONFIG
SDMB820	(none)	SDM BILLING BACKUP
SOS 701	INFO	TOD Critical Alarm
SOS 702	INFO	TOD Major Alarm
SOS 703	INFO	TOD no Alarm
SPM 300	TBL	Device Fault Report
SPM 301	TBL	Device Patching Report
SPM 310	TBL	ECHO CANCELLER REPORT
SPM 311	TBL	SW Exception Report
SPM 312	TBL	Trap
SPM 313	TBL	Fault
SPM 314	n/a	IMC
SPM 330	TBL	SPM Datasync Report
SPM 331	TBL	Failed Device Protection Switch
SPM 332	TBL	SPM REX Aborted
SPM 334	TBL	SPM Clock Performance Out Of Spec
SPM 335	TBL	Device Spare
SPM 336	TBL	Clock Range
SPM 337	TBL	SPM Has Entered Holdover
SPM 338	TBL	SPM Has Been In Holdover Over 24 Hours
SPM 339	TBL	Clock Range
SPM 340	FAIL	CM WarmSwact SPM Report

SPM 341	TBL	SyncRM Entered Holdover
SPM 342	TBL	SyncRM Entered Holdover 24
SPM 344	TBL	Loss Of BITS Redundancy
SPM 350	TBL	Resource Alarm State Changed
SPM 352	TBL	SPM Entered ST3E Holdover
SPM 353	TBL	SPM Entered ST3E Holdover24
SPM 354	TBL	SPM Entered SMC Holdover
SPM 355	TBL	SPM Entered SMC Holdover24
SPM 356	TBL	SPM - Loss of Clock Unit Redundancy
SPM 357	TBL	SPM Node Timing Degradation
SPM 370	FLT	SPM Health Monitor Event
SPM 399	TBL	SPM Overload Report
SPM 500	INFO	Device State Change
SPM 501	INFO	Sync Operation Mode Change
SPM 510	INFO	Sync Reference Switch
SPM600	INFO	MS Mode Changed
SPM 619	TBL	Remote MG4K Fault Details
SPM 625	INFO	SPM XOVER NonConformity Report
SPM 630	INFO	Device Protection Switch
SPM 637	INFO	SPM Has Exited Holdover
SPM 638	INFO	SPM Has Exited 24 Hour Holdover
SPM 641	INFO	SyncRM Exited Holdover
SPM 642	INFO	SyncRM Exited Holdover 24
SPM 644	INFO	Loss Of BITS Redundancy Cleared
SPM 650	PASS	(null)
SPM 651	FAIL	(null)
SPM 652	INFO	SPM Exited ST3E Holdover
SPM 653	INFO	SPM Exited ST3E Holdover24
SPM 654	INFO	SPM Exited SMC Holdover
SPM 655	INFO	SPM Exited SMC Holdover24

SPM 656	INFO	SPM Loss of Clock Unit Redundancy Cleared
SPM 657	INFO	SPM Node Timing Degradation - Cleared
SPM 658	INFO	SPM Timing Reference Source Fail - Cleared
SPM 660	INFO	ECHO CANCELLER REPORT
SPM 661	INFO	ECHO CANCELLER REPORT
SPM 670	INFO	SPM Health Monitor Event
SPM 700	INFO	SPM Trunk Subgroup DDM Audit
SPM 701	INFO	SPM Trunk Subgroup DDM Audit
SPM 702	INFO	SPM Trunk Subgroup DDM Dynamic Update
SPM 703	INFO	SPM Trunk Member DDM Audit
SPM 704	TBL	SPM Trunk Member DDM Dynamic Update
SPM 705	TBL	SPM PTS Trunk Maintenance
SPM 706	INFO	SPM PTS Trunk Maintenance
SPM 707	INFO	SPM ISDNPARAMETER DDM Dynamic Update
SPM 708	INFO	SPM ISDNPARAMETER DDM Audit
SPM 709	INFO	SPM ISDNPROT DDM Dynamic Update
SPM 710	INFO	SPM ISDNPROT DDM Audit
TRK 882	INFO	GROUP INFO
XAC 300	FLT	LowSM (Low Shared Memory)
XAC 302	FLT	LowPE (Low Processor Element)
XAC 303	FLT	MScomm (Message Switch Communication)
XAC 304	FLT	TOD (Time Of Day Clock)
XAC 305	FLT	RTIF (Reset Terminal Interface)
XAC 306	FLT	Disk
XAC 307	FLT	Tape
XAC 308	FLT	Image Test Report
XAC 309	FLT	AMDI (ATM Multinode Data Interface)
XAC 310	MANB	ManB (Card Manual Busy)
XAC 312	FLT	IOP (Input Output Processor Fault)
XAC 320	FLT	SysBTh Alarm Raised

XAC 321	FLT	WgSlot (Shelf Audit Failure - Card Configuration)
XAC 322	TBL	PETrbl (Trouble)
XAC 323	TBL	SMTTrbl (Trouble)
XAC 324	TBL	IOTrbl (Trouble)
XAC 325	FLT	RIBKEY Detected
XAC 326	FLT	MS Link Configuration Mismatch
XAC 327	FLT	WgSlot (Card Inserted Into Wrong Slot)
XAC 329	FLT	ETHR (Ethernet)
XAC 330	FLT	FW version mismatch
XAC 333	FLT	FW loading failed
XAC 400	INFO	XA-Core Summary Report
XAC 413	SUMM	RExSch (REx Schedule Failure)
XAC 415	INFO	Routine Exercise (REx) Report
XAC 418	INFO	Split (Entry to Split Mode Failed)
XAC 420	INFO	SysBTh Ctrl Change
XAC 600	INFO	LowSM Condition Cleared
XAC 601	INFO	MemLim Condition Cleared
XAC 602	INFO	LowPE Condition Cleared
XAC 603	INFO	MScomm Alarm Cleared
XAC 604	INFO	TOD Alarm Cleared
XAC 605	INFO	RTIF Alarm Cleared
XAC 606	INFO	Disk Alarm Cleared
XAC 607	INFO	Tape Alarm Cleared
XAC 608	INFO	Image (Test Passed / Alarm Cleared)
XAC 609	INFO	AMDI link condition cleared.
XAC 610	RTS	Returned To Service
XAC 612	INFO	IOP Fault Cleared
XAC 613	SUMM	RExSch Alarm Cleared
XAC 614	INFO	XATrap Alarm Cleared
XAC 615	INFO	REx Started

XAC 618	INFO	Split (Split Mode Entered)
XAC 619	INFO	Split Mode Exited
XAC 620	INFO	SysBTh Alarm Cleared
XAC 622	INFO	PETrbl Alarm Cleared
XAC 623	INFO	SMTTrbl Alarm Cleared
XAC 624	INFO	IOTrbl Alarm Cleared
XAC 625	INFO	RIBKEY Removed
XAC 626	INFO	MS Link Configuration Restored
XAC 627	INFO	WgSlot Cleared - Card Removed
XAC 628	INFO	XA-Core Provisioning Report
XAC 629	INFO	Ethernet link condition cleared.
XAC 630	INFO	No FW version mismatch
XAC 631	INFO	FW soaking started
XAC 632	INFO	FW soaking completed
XAC 633	INFO	FW loading started
XAC 634	INFO	FW loading completed
XAC 635	INFO	FW soaking in progress
XAC 640	INFO	Test Report
XAC 641	INFO	Alarm Enable/Disable Notification
XAC 801	TBL	MemLim (Memory Limit)
XAC 814	TBL	XATrap (XA-Core High Trap Rate)
XACP300	TBL	Memory Blocking High
XACP500	INFO	Memory Blocking Normal
XACP600	INFO	Memory Blocking Summary

77.9 Appendix B: List of Supported OM's

AABS	AABSFILT	AABSHAND	AASV	ACB
ACCSBNS	ACCSBNSE	ACCSCCV	ACCSCCVE	ACDGRP
ACDMISPL	ACMS	ACRJ	ACRTS	ACRTS
ACSYSTR	ACTAKEDN	ACTRBL	ADASAPU	ADASDSGN
ADASSRV	AIN	AINACG	AINICOFF	AINICSUB
AINNCR	AINOGOFF	AINOGB2	AINOGSUB	AIOD
AL1SVCOM	AL1SVCOM	AMA	ANIOVFL	ANN
APOCCS	APSYS	AR	ARAN	ARN
ASR	ASUFBUS	ASUMEMUT	ATRK	ATRK
ATTAMA	ATTAMA2	ATTLAMA	AUDSRVS	AUTSPID
BCAPCG	BCAPOF	BCLID	BCLIDNL	BCLIDO
BCTPOOL	BCTTANDM	BLUEBOX	BLUEBSTR	C7GTLNK
C7GTWSCR	C7GWSCCP	C7HSLAL1	C7HSLAL2	C7HSLATM
C7HSLCAR	C7LINK1	C7LINK2	C7LINK3	C7LINK4
C7LKSET	C7LPP	C7LPP2	C7MTP	C7MTPRES
C7ROUTE	C7ROUTE2	C7ROUTER	C7RTESET	C7SCCP
C7SCCPCO	C7SCCPX	CAINAGOM	CAINGOM2	CAINIP
CAINLNP	CAINMGR2	CAINMGS2	CAINMSGR	CAINMSGS
CAINNCRS	CAINOM	CAINTRI2	CAINTRIG	CAINUIF
CALLFWD	CALLHOLD	CALLOG	CALLRDT	CALLWAIT
CBK	CCTOOM	CDACTS	CDCOM	CDMCCS
CDR250	CF3P	CF6P	CFRA	CFWPOTS
CMG	CMSGCARR	CMSGGEN	CNAB	CNAMD
CND	CNDB	CNDXPM	COT	CP
CP2	CPICG	CPICKUP	CPUSTAT	CSL
CSMI	CTFP	CTRYDIR	CWTPOTS	DAISGEN
DALINK	DAMISC	DCADTALG	DCAIA	DCAMCEIA
DCM	DCMEBSS	DCRDEST	DCRICTRK	DCRLINK

DCRMISC	DDU	DPTNODE	DPTOFC	DPTOFCP
DRCW	DRM	DS1CARR	DSCWID	DSINWTS
DSPRMAN	DTSR	DTSRPM	DUTLGEN	EACARR
EADLD	EASHRTRK	EATSMS	EBSMSGCT	ECANRMAN
EIUETHER	ENETMAT	ENETOCC	ENETPLNK	ENETSYS
ENG640M1	ESP	ESUP	EXNDINV	EXT
FBTRAFF	FC	FCDRALG2	FCDRALGR	FCDRLOG
FCDRTM1E	FCDRTM2E	FCDRTMP1	FCDRTMP2	FCNF
FLEXDIAL	FLEXTYPE	FPDABM	FPDEVICE	FPSCSI
FRSAGENT	FRSPM	FRT1	FTAM	FTROM
FTRQ	FTS	GIACGRP	GTID	GWOVLOM
HDBOM	HFPOM	HPCBASIC	HPCTRKGP	HTR
HUNT	IBNAC	IBNGRP	IBNSG	IBNSGLDN
ILDBD	ILDBRA	ILDMSGCT	ILDOVLD	ILDSTAT
ININTWRK	INSCTP	IOC	IOSYS	ISA
ISDD	ISDNPDOM	ISGBD	ISGBRA	ISGCPU
ISGOVLD	ISUPCGRP	ISUPCKTA	ISUPCONG	ISUPCONN
ISUPERRS	ISUPUSAG	IWBM	KSHUNT	LDS
LIDBCCV	LINAC	LINEHAZ	LM	LMD
LMSCPUST	LMSMEM	LNP	LNREDIAL	LOGS
M20CARR1	M20CARR2	M3UA	MACHCONG	MDCWAKUP
MDSACT	MDSSTAT	MNATM	MNATMA1	MNATMA5
MNATMCH	MNATMVC	MPB	MPCBASE	MPCFASTA
MPCLINK2	MPCLINK3	MPHCON	MPHGRP	MS
MSCHAIN	MSCHNLK	MSFBUS	MSFBUSTP	MSGPSOC
MTA	MTU	MULTAUTH	MWICTCAP	MWTCAR
MWTCAR2	NACDGRP1	NACDGRP2	NARUSAGE	NCMCPUST
NDS0CARR	NEMASAPL	NETMSG	NGSSOM	NIUFBUS
NIUMEMUT	NMC	NMTCLINK	NMTCNODE	NMTCTYPE

NMTCUNIT	NPAPPEG	NRS	NRS	NSC
NSCACG	NWMFRRCT	NWMFRRTG	NWMSILC	NWMTGCNT
NX25L2	NX25L3	NX25LNK	NX25MLP	OADATCOM
OAFLTRIG	OAINNODE	OAINQMS	OAINRTE	OANODEDC
OAPCALP1	OAPCALP2	OAPCALP3	OAPCALP4	OAPCALP5
OAPCALP6	OAPCALP7	OAPCALP8	OAPCALP9	OAPCP10
OAPMERRN	OAPMERRS	OAPMTYPN	OAPMTYPS	OAPNMIS
OAPNMTC	OAPSPMTC	OASNPLDC	OASNPOOL	OASVNDGP
ODBOM	OFF250	OFZ	OFZ2	OFZ2NET1
OFZ2NET2	OGTQMS	OHBTDTU	OHBTRES	OHBTTYPE
OHQCBQCG	OHQCBQR2	OHQCBQR3	OHQCBQR4	OHQCBQRT
ONI	OPCHOICE	OSACCP1	OSACCP2	OSACND
OSACSP	OSNND	OSNSP	OTS	PCMCARR
PCNF	PM	PM1	PM2	PMMSGCNT
PMOVL	PMSTAT	PMTYP	PPCO	PRADCHL2
PRAFAC	PRASERV	PRIMWIC	PRISVCS	PRKOM
PRP	PSN_ERDC	PSN_ERFM	PSN_ERPS	PSN_FCTR
PSN_NOTF	PSN_PRIM	PSN_USAG	QMSACT	QMSDATA
QMSMIS	RADR	RCF	RCHDOPT	RCVR
RECMDOVF	REVALLO	RLCDIS	RLDBD	RLDBRA
RLDMSGCT	RLDSTAT	RLT	RMANCMR	RMSGOMGP
RND	ROAPPL	ROMISC	RRTE	RSCIR
RSCIS	RSMT	RTEASUM	RTESVCS	RTFEAT
RTLTSUM	RTRSCCP	RTRTCAP	SACB	SCA
SCAISERV	SCAISRV2	SCAISRV3	SCAISRV4	SCAITRAN
SCF	SCMP	SCPOTS	SCRJ	SDS
SEIUTRAN	SERVACT	SERVBLK	SETRAF	SIMRING
SITE	SITE2	SITE3	SLLCOM	SLLNK
SLLNKINC	SLQ	SLVPOPT	SMCOM	SME

SMGENOM	SMNCOM	SMSTOPS	SOTS	SPAP
SPC	SPEEDCAL	SPMACT	SPMOVLD	SPMUSAGE
SPPIN	SPRING	SRA	SRAOM	STN
STORE	SVCT	SYSPERF	TC7WRLSS	TCAPERRS
TCAPUSAG	TCW	TDCPROT	TDCROUT	TDGTHRU
TDR	TDRFTMPL	TFCANA	TFREE533	TM
TME	TONES	TOPAAPPL	TOPASCCP	TOPPACT1
TOPPACT2	TOPPACT3	TOPPACT4	TOPPDID1	TOPPDID2
TOPPDID3	TOPPDID4	TOPPDID5	TOPPDID6	TOPPMMSG
TOPQOCPS	TOPS950	TOPSAICC	TOPSALT	TOPSARU
TOPSBRND	TOPSCCAB	TOPSDA	TOPSDACC	TOPSDEV
TOPSEA	TOPSINCC	TOPSISUP	TOPSKFAM	TOPSLNP
TOPSMISC	TOPSMTCE	TOPSOC	TOPSOLNE	TOPSOLNS
TOPSPARS	TOPSPSZ	TOPSQMS	TOPSRLT2	TOPSRON
TOPSRTRS	TOPSTRAF	TOPSUSE	TOPSVC	TRA125M1
TRA125M2	TRA250M1	TRK	TRK2NET1	TRK2NET2
TRKQOSOM	TRKVERDS	TRMSCRND	TRMSCRNO	TRMTCM
TRMTCM2	TRMTCU	TRMTCU2	TRMTCU3	TRMTER
TRMTFR	TRMTFR2	TRMTFR3	TRMTPR	TRMTRS
TRNK2	TROUBLEQ	TS	TTCCARR	TWCIBN
TWCPOTS	U3WC	UCDGRP	UNBCDC	UNBMISC
UPSNACT	UPSNFAIL	USAGSAMP	USGSECS	UTR
VAMPACG	VFGIWUSE	VFGUSAGE	VOW	VPSC
VPSC	VPTRUSAG	VSNCOM	VSNLINK	VTCAPERR
VTCAPRCV	VTCAPSNT	WBTRK	WC	WIDEBAND
WINTOPS	XACORE	XACPOM	XACSRVC	XASTAT
XIPCOMID	XIPDCOM	XIPMISC	XIPSVCS	XLIUL3
XPMLNK	XPMMSGOC	XPMOCC	XPMOVLD	

78: A00007304 Functional description (FN)

78.1 Feature name

SN08 CEM I & C on IEMS.

78.2 Description

The CEM server functionality will be provided in conjunction with the IEMS server. CEM will be installed as an overlay on IEMS and SSPFS.

The CEM server is an element manager for the DMS node. It provides powerful fault, performance and configuration management toolsets. This server works in conjunction with the CEM browser which will be integrated into the IEMS product (see feature A00007302).

This feature covers the installation of the CEM server onto the IEMS server. This feature also covers the installation of the CEM components on the SDM and CBM. This feature will also incorporate the Synchronized Backup Manager to be used by CEM (for information about the Backup Manager see feature A00006979)

78.3 CEM Installation

The procedure for adding a CEM software package to the server are as follows:

1. Obtain the cem tar file and untar it.
2. Run the cem_setup script. Use the full path to start it.
3. Use pkgadd to install the Help Package.
4. Start the CEM server using /opt/servman/bin/servstart CEM

78.3.1 Removing the CEM software

The procedure for removing a CEM software package from the server are as follows:

1. Stop the CEM server using /opt/servman/bin/servstop CEM. Note: It may take a few minutes for CEM to stop completely.
2. Run the cem_setup uninstall script.
3. Use pkgrm to remove the help package.

78.4 CEM Commissioning Manager

The CEM Commissioning Manager is a Java-based graphic user interface tool for configuring managed node instances. A command line interface is also available. The following sections describe in detail how to use the Commissioning Manager.

78.4.1 Launch The Commissioning Manager

To launch the Commissioning Manager, do the following:

1. Login on the IEMS server as root.
2. Change directory to /opt/nortel/cem/data/coreEMS/nodes/server/bin/
3. Issue the command “.configCEMS -c” for the command line interface.

The Commissioning Manager main menu will be displayed on the screen after the command line interface being invoked.

78.4.1.1 Create A Managed Node Instance

To create a new managed node instance:

1. Select “1” (Commission a new node) from the Commissioning Manager Command Line Interface main menu.

```
Nortel Networks coreEMS Commissioning Manager
Main menu
```

```
-----
[1] Commission a new node
[2] Reconfigure an existing node
[3] Delete an existing node
[4] Add a mated pair monitor
[5] Delete a mated pair monitor
[6] SDM to CBM migration
[0] Exit
Selection: 1
```

2. Then select DMS for the new node when prompted for the device type.

```
*** Configure a Node Instance ***
```

```
[1] DMS
[2] HLR200
[3] MDM
[4] NSP
[5] SESM
[6] USP_NES
[7] DS
Select a device type for the new node: 1
```

3. Input a name for the new node when prompted for the “Element Name” of the node. The element name should be a string up to 15 characters drawn from the alphabet (a-z), digits(0-9) and minus sign(-). The first character must be an alpha character and the last character must not be a minus sign. The element name can’t be “server”, “localhost”, “loghost” or the hostname of the localhost.

Hint: Input a string up to 15 characters drawn from "-a-z0-9". The 1st character must be an alpha character; the last one must not be a minus sign. Element name cannot be “server”, “localhost”, “loghost” or the hostname of the localhost.
Mandatory input.
Element Name : **SDMA2**

4. Input the region name when prompted:

Hint: Enter the region path to the node or select one from the list. Valid path characters include alpha-numeric and the '/' characters.
Mandatory input.
List of existing regions:
Nortel
Region : **Nortel**

5. Select GEM18 for this new node when prompted for “Software Release”.

Hint: Choose a software version.
Mandatory input.
[1] GEM18
Software Release (1): **1**

6. Input the target IP address when prompted for the “Target SDM IP Address”. The target IP address should be in dot-decimal format.

Hint: Input a dot-decimal representation of an IP address or the string 'localhost'.
Mandatory input.
Target SDM IP Address : **47.142.106.26**

7. Enter No Call Trace will not be used.

Hint: Answer Yes if the SDM has Call Trace installed, otherwise answer No.
Mandatory input.

[1] Yes

[2] No

Enable Call Trace (1): **2**

8. Enter No do not install Billing Manager

Hint: Answer Yes if this DMS is an MSC/TriNode, No if this DMS is an HLR.
Mandatory input.

[1] Yes

[2] No

Install Billing Manager (1): **2**

9. Answer No to USP

Hint: Answer Yes if this DMS has USP, otherwise answer No. Not valid if Billing Manager = Yes

Mandatory input.

[1] Yes

[2] No

Does This DMS Have USP (2): **2**

10. Answer “y” at the prompt “Proceed to create this node?”.

Proceed to create this node? [y/n](n): **y**

11. Answer yes the SDM is already in server mode.

Commissioning node, please wait...

Commissioning node completed successfully!

Is sdma2 already in server mode? [y/n](n): **y**

12. Answer Y to start the nodes applications

Start all applications of node susan? [y/n](n): **y**

13. Wait till you get the rts completed message

```

Returning to service all applications of node susan.
This action may take a few minutes.
Please wait...
Busy/Rts action completed!

```

14. Exit configCEMS

```

Nortel Networks coreEMS Commissioning Manager
Main menu
-----
[1] Commission a new node
[2] Reconfigure an existing node
[3] Delete an existing node
[4] Add a mated pair monitor
[5] Delete a mated pair monitor
[6] SDM to CBM migration
[0] Exit
Selection: 0

```

78.4.1.2 Delete A Managed Node Instance

Users can delete a managed node instance, and all data and configuration for that node would be permanently removed from the system.

To delete a managed node instance:

1. Select “3” (Delete an existing node) from the Commissioning Manager Command Line Interface main menu.
2. Then select the node instance to be deleted.
3. Answer “y” at the prompt “Proceed to delete this node?”

78.5 Backup of CEM

CEM will be backed up using the Synchronized Backup Manager (Feature A00006979). When this backup is run, the information needed by CEM to restore will be located in /opt/nortel/cem/data/coreEMS/configBackup.

78.6 Restore of CEM

To restore CEM, make sure that the /opt/nortel/cem/data/coreEMS/configBackup directory contains the following: data_dir, ldapConfig.tar, nodes.tar and server. Make sure CEM is stopped with servquery -status -group CEM command. If CEM is not stopped run servstop CEM. Then run /opt/nortel/cem/data/coreEMS/nodes/server/bin/postRestore.sh.

78.7 CEM SAF (Store and Forward) Process on SDM/CBM

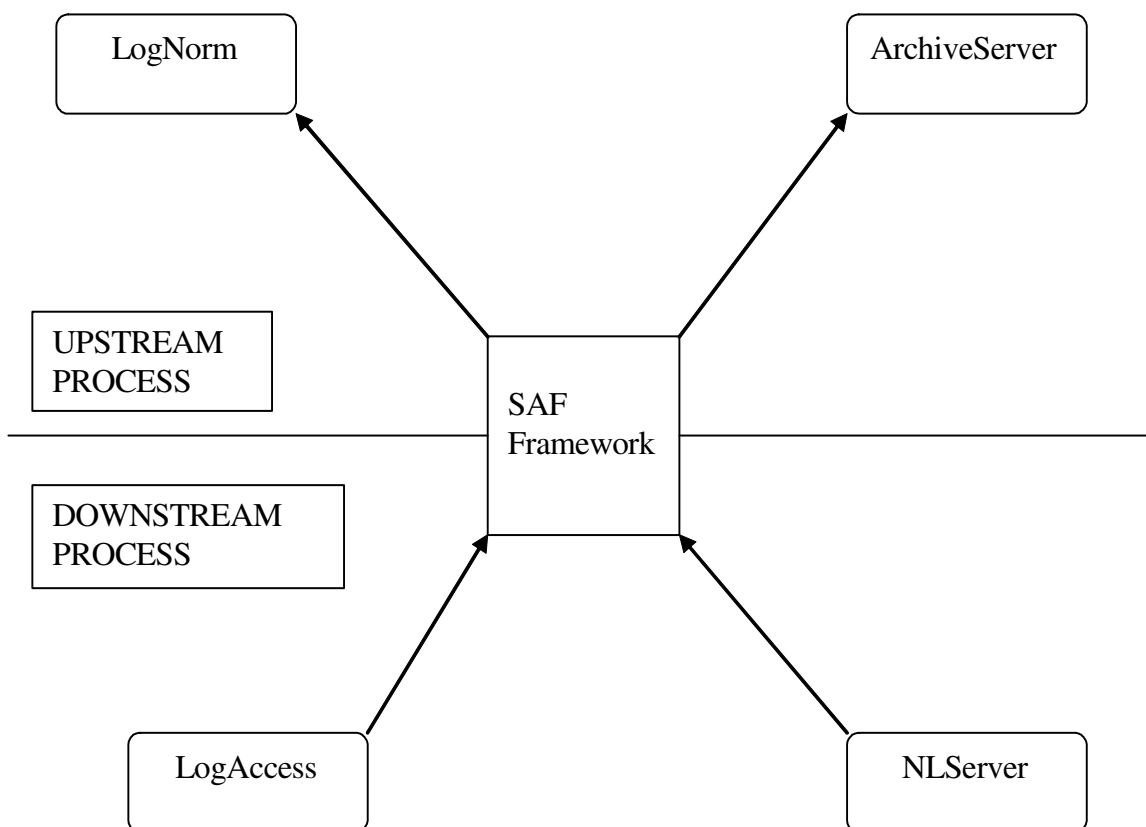
78.7.1 Introduction

CEM SAF (Store and Forward Process) Framework has been designed to serve two purposes:

1. Storing and Forwarding the SDM/CBM data on to the appropriate CEM Server process.
2. Synchronization after disconnection from the CEM server process and SDM/CBM.

Process Interaction Diagram

Data flow diagram

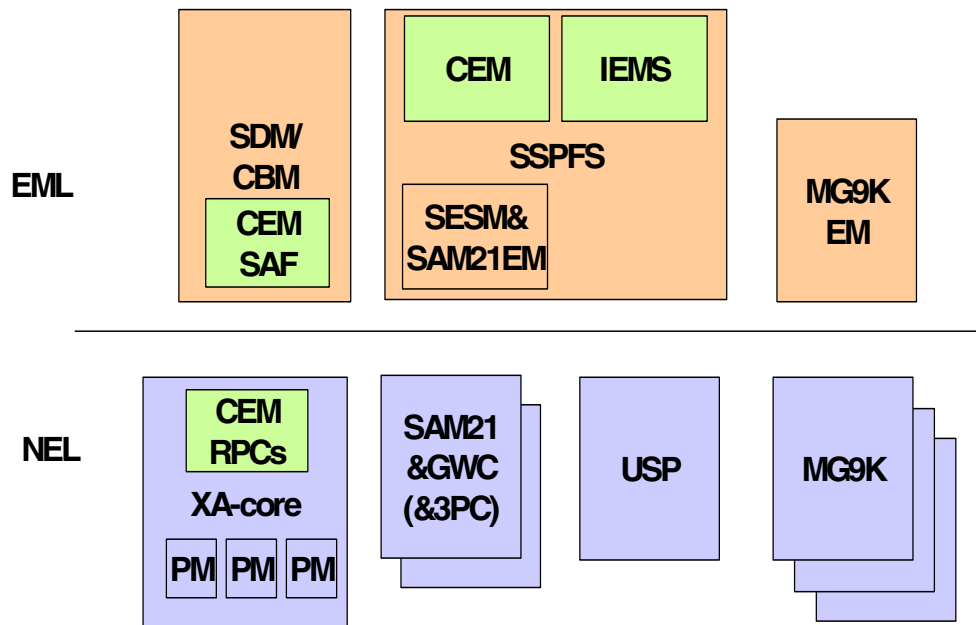


By default SAF process on the SDM/CBM will not be in service after CEM is installed. It has to be turned on to be “in service” state.

78.7.2 IEMS and CEM succession architecture

In SN08, the CEM integration with IEMS is taken to the next level, pulling the CEM and IEMS into a combination load and the launching capabilities are further refined and integrated. Additionally, the fault handling and interface between the two management systems will be extended and enhanced to provide uniform handling of alarms between the two.

The Figure below provides an overview of IEMS and CEM succession architecture.



78.8 CEM SAF logs on SDM/CBM

The processes included in CEM SAF Framework throw a number of logs depicting any Trouble or Information regarding CEM processes.

The Description of all the SAF Framework processes, warning and info logs thrown by them is documented in the FM section.

78.9 File Sets and Directory structure for CEM Processes

The File sets on sdm including CEM processes are:

SDM_CEM.SAF

SDM_GEM.dmsDataSrv

SDM_TntFTPHndl.TntFTPHndl

78.9.1 Directory Structure for SAF Data

Data Storage:

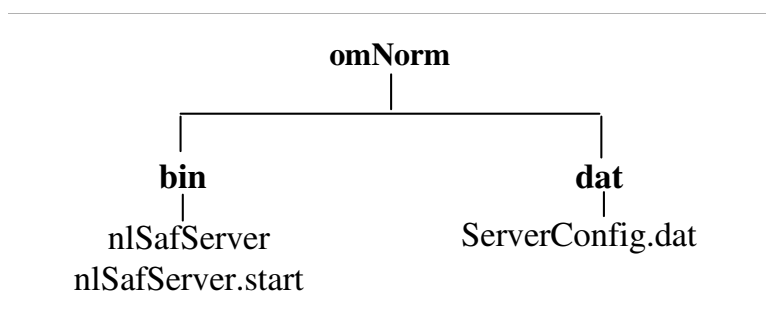
SAF Server stores data in “SAF.DB”

SAF Client stores data in the field specified in “serverConfig.dat” and stores it in the path specified in the file.

78.9.2 Directory Structure for SAF package

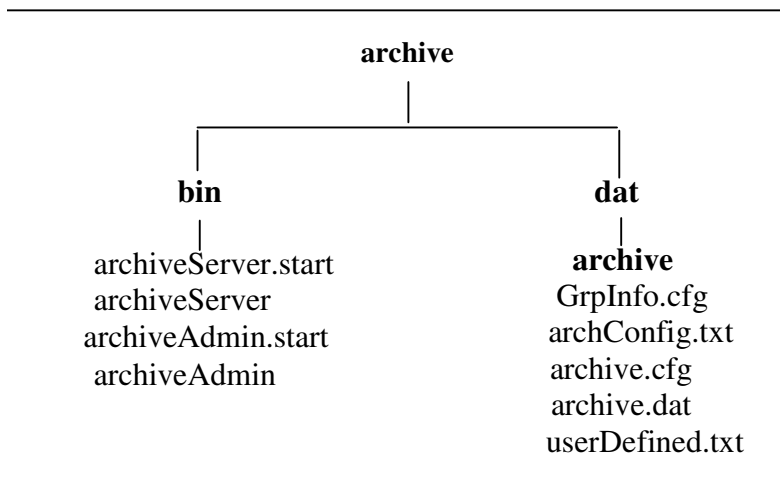
Directory Structure for SAFServer package (on sdm)

From /mscomc/OMC_S



Directory Structure for SAFClient package (on server)

From /opt/nortel/data/coreEMS/nodes/<node name>



78.10 Ports assigned for the CEM processes

Table 1:

Application	Port	Protocol	Description
switchExport	7788	tcp	switch Mass Export service
NLServer	7982	tcp	PM service
admind	8102	tcp	SDM process/link/logic volume information service
dmsDataServer	8449	tcp	tuple service
dmsDataServer	8450	tcp	table schema service
dmsDataServer	8614	tcp	table change notification service
rpcServer	22333	tcp	rpc service
migrationClient	22395	tcp	control port for Migration Client
TelnetFTPHandler	22397	tcp	MAPCI pass-through to MSC/HLR
TelnetFTPHandler	22398	tcp	ftp pass-through to MSC/HLR
TelnetFTPHandler	22399	tcp	telnet to SDM
TelnetFTPHandler	22400	tcp	ftp to SDM
TelnetFTPHandler	22402*	tcp	telnet access to 3PC application
tpcStsQuery	22403*	tcp	telnet access to 3PC application status
TelnetFTPHandler	22404	tcp	non-secure ftp access to CM
TelnetFTPHandler	22405	tcp	non-secure ftp access to SDM/FT
exportLog	23000	tcp	CAP log export service
nlSafServer	26002	tcp	NLServer store and forward port

Table 1:

Application	Port	Protocol	Description
logNormSAF	26003	tcp	logNormalizer store and forward port

78.11 Logs being delrepped for CEM application

Table 2: List of log delrepped.

Logs
AUTH
CAFT
CALM
CDPD
CHIP
CLFL
CPER
CPRT
CTID
DEPS
DFA
DIM
DROP
ERV
ESNF
FCEL
FRAU
FRS
GAME

Table 2: List of log delrepped.

Logs
HMT
IOGA
IS41
LAM
MBPG
MCD2
MCD3
MCDR
MIWF
MLNP
MTX
NCAS
NOPT
OCC
OM2
OMGA
OTAF
PCO
PVAL
RAD
RFES
RFP
RFPE
RPC
RRIF

Table 2: List of log delrepped.

Logs
RSSI
SMO
SMS
SMT
SPRF
SSR
TIER
TUPL
X75

78.12 Hardware Requirements or Dependencies

An IEMS server is required.

An SDM and CBM are also required.

78.13 Software Requirements or Dependencies

SN08 is required.

78.14 Limitations and restriction

SN08 is required.

78.15 Interactions

This feature interacts with A00007302 and A00006979

78.1 Glossary

Term	Description
CEM	Core Element Manager
DMS	Digital Multiplex Switch
IEMS	Integrated Element Management System

79.2.2 VPN topology

The activity supports VPN networks with the following topology:

- VPNs hosted by one CS 2000
- VPNs hosted by several CS 2000 interconnected by a SIP-T[ETSI ISUPv2] trunk

The VPN support comprises a set of supplementary services and a common dial plan. The dial plan typically consists of a concatenation of a location code and an extension.

79.2.3 Supported gateway Interoperability

This activity supports the interworking of the Cisco Call Manager with the following H323 gateways controlled by the CS 2000:

- BCM legacy model
- Cisco router 2600/3725 (Cisco IOS GW)
- S 1000
- S 1000M
- Westell liQ 2031, supporting 1 E1 with DPNSS
- Westell liQ 2032, supporting 2 E1 with DPNSS
- H323 signalling proxy

The interworking to these gateways is supported for local calls, i.e. GWs served by the same CS2K, and for networked calls, i.e. GWs served by different CS2Ks that are connected via a SIP-T trunk.

Furthermore the following non H323-GWs are supported:

- CICM
- PVG
- MCS 5200 using the following clients and devices
 - PC client
 - Web client
 - I2004
 - PRI gateway (UAS based)
 - MAS
- Mediatrix

The interworking to these gateways is supported for local calls, i.e. GWs served by the same CS2K, and for transit calls, i.e. GWs served by different CS2Ks that are connected via a SIP-T.

Table 1 basic call support matrix

			BCM leg.	Cisco IOS GW	CCM	S1000/ S1000M	West.	H323 sig. proxy	CICM	PVG	MCS	Medi atrix
CCM	local call	intra EN	+	+	-	+	+	+	+	+	+	+
		inter EN	+	+	-	+	+	+	+	+	+	+
	SIP- T	intra EN	+	+	-	+	+	+	+	+	+	+
		inter EN	+	+	-	+	+	+	+	+	+	+

Explanation:

- +: functionality supported
- -: functionality not supported

Depending on the call topology a call can be setup with and without RTP media portal insertion.

This activity supports G711 only.

There are two issues with CCM to CCM calls:

- inter EN calls (media portal used):
In case of a heavy load condition on the GWC the following issue was detected:
The Cisco phone sends the RTP packets on a UDP port that is different from the UDP port on which it receives RTP packets. However, the concept of the RTP media portal is based on the assumption that these ports are identical. As a consequence there is only one way speech path. A TAC request (600355128) was raised against Cisco. There is no workaround.
- intra EN calls (media portal not used):
In the H245 OLC message the CCM sends an incorrect endpoint. Instead of sending the RTCP endpoint of the terminating Cisco phone - as requested by the H323 standard- it sends an RTCP endpoint of the CCM itself. As a result the GWC sends an incorrect endpoint to the originating phone. As a consequence there is only one way speech path. A TAC request (600492669) was raised against Cisco.
As a workaround it is possible to avoid having 2 slowstart GWs located in the same enterprise network. In order to achieve this it is possible to add virtual enterprise networks in the SESM and put each GW that supports slowstart into the separate virtual enterprise network.

79.2.4 Supplementary services

The following services are supported with a Cisco Call Manager as served user:

- Calling Number Delivery
- Calling Name Delivery
- Call Forward Busy/no answer/unconditional
- Call Transfer with and without consultation: the involved parties can be connected to the CCM and other GWs for one call. This includes support of Call Hold
- Call Pickup: the pickup group must be internal to the CCM
- 3-Way Calling: the conference bridge is located on the CCM
- Meet Me conference: the conference bridge is located on the CCM
- Call Park/retrieve: the parking user and the retrieving user must be on the same CCM

Scenarios, in which another H323 GW invokes a supplementary service in a call with a CCM client, are also supported. This is dependant on the supplementary service support of the other H323 GW.

Note: This activity does not implement new supplementary services, but adapts existing services, so that they can be invoked by a CCM.

Table 2 suppl. service interaction matrix

		other party involved							
		BCM leg.	Cisco IOS GW	S1000/ S1000 M	West.	CICM	PVG	MCS	Mediatrix
service invoked on CCM	calling number delivery	+	+	+	+	+	+	+	+
	calling name delivery	+	+	+	_figure a	+	+	+	_a
	CFU/CFNR/CFB	+	+	+	+	+	+	+	+
	call transfer	+	+	+	+	+	+	+	+

Table 2 suppl. service interaction matrix

		other party involved							
		BCM leg.	Cisco IOS GW	S1000/ S1000 M	West.	CICM	PVG	MCS	Medi atrix
	call pickup	+	+	+	+	+	+	+	+
	3-way calling	+	+	+	+	+	+	+	+
	meet me conference	+	+	+	+	+	+	+	+
	call park/ retrieve	+	+	+	+	+	+	+	+

a. agent does not support calling name delivery

Explanation:

- **service invoked by CCM:** the CCM is always the served user. It can be the call originator, e.g. in case of the ‘station controlled conference’ service, or the call terminator, e.g. in case of the ‘calling number delivery’ service.
- **other party:** party that is involved in a call in which a served user invokes a supplementary service.
- +: functionality supported
- -: functionality not supported

79.3 Hardware Requirements or Dependencies

79.4 Software Requirements or Dependencies

The feature depends on the following SW version of the different gateways:

- BCM legacy model: release 3.6
- Cisco router 2600/3725 (Cisco IOS GW): release 12.3
- Cisco Call Manager: 3.3(4)sr2 and 4.0(2)a
- MCS 5200: release 3.0.11
- Mediatrix 1104: v 4.6.2.5
- S 1000: release 3.00, Signalling server 2.11.03
- S 1000M: release 3.00, Signalling server 2.11.03
- PVG: 6.1.2
- CICM: 7.11.184

- Westell liQ 2030 series, IPH-DP 1-6-11, supporting 1 E1 with DPNSS

79.5 Limitations and restrictions

The following gateways are not supported by this activity due to non-availability during IT timeframe:

- BCM model 50
- NGSS
- IW/SPM

For the Cisco Call Manager a 1:1 IP address NATing is done. Port translation is not supported.

The restrictions described in A00001895 apply for this activity, too.

For each call that is established the GWC periodically audits the CCM by sending H.323 RAS IRQ messages to the CCM. As a result the CCM floods the gatekeeper with H.323 RAS IRR messages. These messages are sent as long as the relevant call is up. This results in a performance degradation of the GWC. A TAC request (600537082) was raised against Cisco.

79.6 Interactions

79.7 Glossary

Table 3

Term	Description
BCM	Business Communications Manager
CCM	Cisco Call Manager
CICM	Centrex IP client manager
DTMF	Dual Tone Multi Frequency
EN	Enterprise Network
GWC	Gateway Controller
IW/SPM	Interworking Spectrum Peripheral Module
MAS	Media Application Server
MCS 5200	Multimedia Communication Server 5200
NAT	Network address Translation
NGSS	Next generation session server

Table 3

Term	Description
PVG	Passport Voice Gateway
PBX	Private Branch Exchange
RTP	Real Time Protocol
SIP	Session Initiation Protocol
UDP	Universal Dial Plan
VPN	Virtual Private Network

79.8 References

- A00007322, DID, Requirements section
- A00001895, FN

80: A00007323 Functional description (FN)

80.1 Feature name

Gateway Controller notification of Media Proxy Bind Expiry Events

80.2 Description

This feature implements a mechanism to allow the Gateway Controller to request notification of idle and long-call call events from the RTP Media Proxy. The Media Proxy element manager defines an Idle Session Audit Period and Long Idle/Long Call durations (measured in terms of the number of audit periods).

An idle call event is detected when a bind has been set up on the Media Proxy, and has received at least one packet but has not received any packets during the audit period.

A long call event is where a bind has been set up and is in use but has been up for the Long Call duration.

When the CS2K is notified that a call has been detected as idle or long by the Media Proxy a Syslog will be generated. If the call is known on the GWC it is allowed to continue and the Long Idle/Long call duration timers on the MP are reset. If the notification is regarding an unknown call on the GWC the MP bind will be removed and a CS2K exception generated.

80.3 Hardware Requirements or Dependencies

None

80.4 Software Requirements or Dependencies

This functionality is available for SN08 and above.

RTP Media Proxy is loaded with release 3.2

80.5 Limitations and restrictions

The generated Syslogs will include the correlation id which is passed down from the CM. By default this correlation id is not present in the CM AMA billing records. Currently in order to correlate this id with a particular billing record the Quality Of Service feature must be configured and activated (Module 612 is appended to the billing record). In SN08 this is the only available mechanism to tie generated logs with particular billing records.

80.6 Interactions

Not applicable

80.7 Glossary

Table 1

Term	Description
GWC	Gateway Controller
MP	Media Proxy

81: A00007324 Functional description (FN)

81.1 Feature name

RTP Portal QoS reporting to GWC

81.2 Description

This document covers a feature done within the scope of SN08 to implement the reporting of QoS statistics from the RTP Media Portal (MP) to the QoS Collector Application (QCA).

The parameters that make up the QoS statistics reported by the MP are:

- Packets sent
- Packets received
- Packet loss
- Octets sent
- Octets received
- Inter-arrival latency
- Jitter

The records generated will be identical to those described in the FN for feature A89007819, and that document should be used as a reference.

81.3 Hardware Requirements or Dependencies

The requirements are identical for existing QCA applications as outlined in A89007819.

81.4 Software Requirements or Dependencies

The requirements are identical for existing QCA applications as outlined in A89007819.

81.5 Limitations and restrictions

As A89007819

81.6 Interactions

-

82: A00007327 Functional description (FN)

82.1 Feature name

Media Proxy 5 and 30 minute Operational Measurements

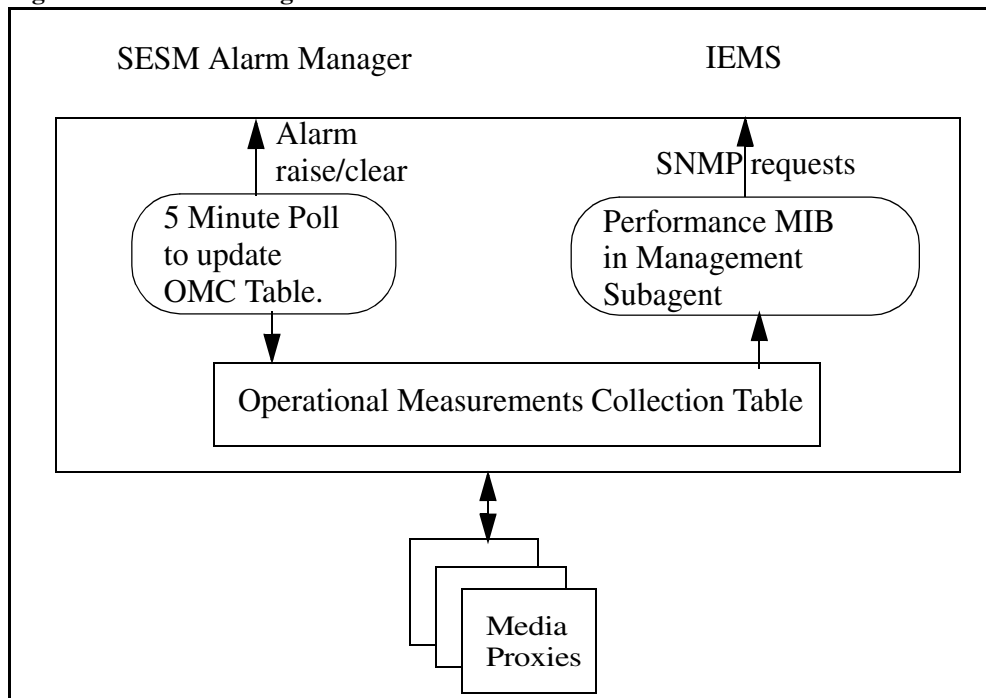
82.2 Description

This feature implements a number of Media Proxy specific Operational Measurements (OMs) on the Gateway Controller (GWC) to be collected by IEMS at 5 minute intervals. These metrics can be used by the crafts person to diagnose problems with Media Proxy usage and identify requirements to better engineer the network to handle internet transparency calls.

The OMs covered are a number of passed and failed calls per Media Proxy and per GWC for every 5 and 30 minute interval. A Media Proxy communications path lost alarm is also added by this feature. The detailed description of the OMs and alarm can be found in the Performance and Fault Management sections of the document respectively.

The customer will use the existing SESM alarm manager for the new alarm. IEMS will be configured to receive the new OMs every 5 minutes. The 30 minute OMs are only updated and reported every 30 minutes, 30 minute periods are aligned with the 5 minute OM poll period on the GWC. Only the active GWC will report the OMs, while the inactive will report no OMs found in the table.

This feature is intended to complement the OMs that are already available for the RTP Portal via IEMS and gives the GWC view of calls as opposed to the Media Proxy view.

Figure 1 Behavior Diagram

82.3 Hardware Requirements or Dependencies

Not applicable.

82.4 Software Requirements or Dependencies

This functionality is available for SN08 and above.

82.5 Limitations and restrictions

Not applicable.

82.6 Interactions

Not applicable.

82.7 Glossary

Table 1

Term	Description
GWC	Gateway Controller
IEMS	Integrated Element Management System
OM	Operational Measurement
SESM	Succession Element and Sub-Element Manager

83: A00007331 Functional description (FN)

83.1 Feature name

RFC 2833 DTMF Interop with S 1000, S 1000M and BCM

83.2 Description

83.2.1 Overview

SN08 activity A00007331 allows RFC 2833 DTMF support between Nortel S1K/KM and BCM, with H.323 and other supported VoIP VPN (non H.323) endpoints.

This activity provides also a method for interworking between gateways that support RFC 2833 and ones that do not.

83.2.2 Supported Interoperabilities

RFC 2833 Interoperability between S1K/M and BCM with other H.323 endpoints:

- a. CISCO IOS gateways (2600, 3600)
- b. Westell iQ2030

RFC 2833 Interoperability between S1K/M and BCM with other non-H.323 endpoints:

- c. MGCP lines, MGCP IAD lines (e.g. Mediatrix line)
- d. CICM line
- e. MCS Conferencing server
- f. MS 2010 [UAS]
- g. PVG (VSP3, VSP3-O)

Verification of RFC 2833 interoperability between S1K/1KM with following non-H.323 endpoints:

- I/W SPM

Note: The RFC 2833 Interoperability will be tested as soon S1K and BCM provide this functionality. This feature is primarily a test effort to verify RFC 2833 DTMF support for BCM and S1K. Most of the required design changes are covered by activity A00002550 H.323GK to GK Interop.

Note: An integration test needs to be initiated in order to verify the RFC2833 functionality for BCM and S1K.

83.3 Hardware Requirements or Dependencies

Please refer to Section 2.4.

83.4 Software Requirements or Dependencies

- Business Communication Manager (BCM) with 3.7 +(GA Q1 2006)
- Succession-1000M with Release 4+ (GA in November 2005)
- Centrex IP Client Manager (CICM) with Release 7
- Mediatix 1104
- i2004 IP with release 1.5x
- Westell iQ2030 R1.6.11 load
- PVG with PCR 6.1.2
- Media Server (MS 2010) Release x
- MCS load version 2.0

83.5 Limitations and Restrictions

- RFC 2833 DTMF transport with S1K for SIP protocol is not supported by this activity.
- RFC2833 integration testing for BCM and S1K, since this functionality is targeted for the late 2005/2006 time frame.

83.6 Interactions

None

83.7 Applicable customer facing sections

Fault Management

Logs	N/A
Alarms	N/A
Configuration	N/A
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

83.8 Glossary

Table 1

Term	Description
DTMF	Dual-Tone Multifrequency
IP	Internet Protocol

83.9 References

1. ITU-T Recommendation H.323v4(2000): Packet Based Multimedia Communications Systems
2. ITU-T Recommendation H.245v7(2000): Control Protocol for Multimedia Communication
3. RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
4. Melinda Webb, Carrier Hosted Services PLM:

[http://plm-pnd.europe.nortel.com/Succession/
Plan%20of%20RecordSN08%20PoR--2004-08-02.xls](http://plm-pnd.europe.nortel.com/Succession/Plan%20of%20RecordSN08%20PoR--2004-08-02.xls)

84: A00007341 Functional description (FN)

84.1 Feature name

MS2000 IEMS Configuration Integration

84.2 Description

In SN06.2, Nortel made a decision to begin phasing out the UAS (Universal Audio Server) and begin replacing them with a set of Media Server devices, the MS2010 and MS2020. These devices are referred to as MS2000 Series Nodes (Media Server 2000 Series Nodes). In SN06.2 the IP version of the Media Server (MS2010) was deployed. In order to provision and maintain the MS2010 node the MS2000 CLUI (Command Line User Interface) was developed. The MS2000 CLUI ran on the SESM server. In SN07 the MS2000 CLUI was enhanced to handle the provisioning and maintenance of the ATM Media Server (MS2020).

With this feature in SN08, the existing functionality of the MS2000 CLUI will be migrated to reside on the IEMS platform. All of the existing functionality that is captured in the MS2000 CLUI will be migrated to the new MS2000 EM GUI. The existing command line interface will be removed from the SESM software.

84.2.1 MS2000 EM Functionality

Below is a breakdown of the functionality that is provided by the existing MS2000 CLUI that will be migrated to the MS2000 EM.

84.2.1.1 Configuration

The following windows will be needed for configuration.

- General Configuration
 - Megaco Call Agent IP Address
 - Is Megaco Call Agent Used
 - Number of Conference Ports
 - Number of TestTrunk Ports
 - Number of Lawful Intercept Ports
 - Number of Announcement Ports
 - APS IP Address
 - Primary Language
 - Secondary Language
- SNMP config (community strings, trusted managers, trap destinations)
- WebServer config (username and password for web interface)
- Network Time Protocol (NTP) settings

The following tables can also be configured for the MS2020 ATM node

- ATM loopback table
- SVC Connection table
- ATM port table
- Remote Gateway table (AAL2 only)
- AAL2 PVC table (AAL2 only)
- SVC Profile table (AAL2 only)

84.2.1.2 Maintenance

The following maintenance activities will be supported from the client.

- Lock/Unlock of device
- Backup of INI file
- Upload of load files. (CMP, INI, DAT, XML)
- Soft Reset of device

84.2.1.3 User Access Privileges (Authorization)

The following lays out the access that a user must have to issue the following functions:

Table 1 User Authorization required for functionality

Access	Functionality
mg groups with any access	List of any configuration
mgsprov, mgrw, mgadm	Change Configuration
mgmtc, mgrw, mgadm	Lock/Unlock of device
mgmtc, mgrw, mgadm	Backup of INI file
mgmtc, mgrw, mgadm	Upload of load files. (CMP, INI, DAT, XML)
mgmtc, mgrw, mgadm	Soft Reset of device
mgadm, mgrw	Change SNMP Passwords
mgadm, mgrw	Change File Transfer Passwords

84.2.2 New functionality in SN08

Some new functionality that did not exist on the CLUI will be provided in the SN08 MS2000 EM release. These are briefly outlined below:

- The MS2000 EM will make use of the existing IEMS audit logging functionality to provide a log of what user issued a command against an MS2000 node.
- The MS2000 EM will make use of the existing IEMS alarming system to generate an alarm against the EM whenever a configuration of maintenance action by the EM has an unrecoverable failure.

84.2.3 Upgrading SN06.2 and SN07 data

Data that existed in SN06.2 and SN07 on the SESM server will need to be transferred to the SN08 IEMS. The data that needs to be transferred is contained in a properties file.

In SN06.2 the file is:

`/opt/nortel/NTsesm/bin/ams.properties`

In SN07 the file is

`/opt/nortel/NTsesm/bin/ms2000.properties`

Either a manual procedure or a script will be written to help the end user with this data migration. TBD.

84.3 Hardware Requirements or Dependencies

The MS2000 EM will run on IEMS and inherits any requirements and dependencies for hardware.

84.4 Software Requirements or Dependencies

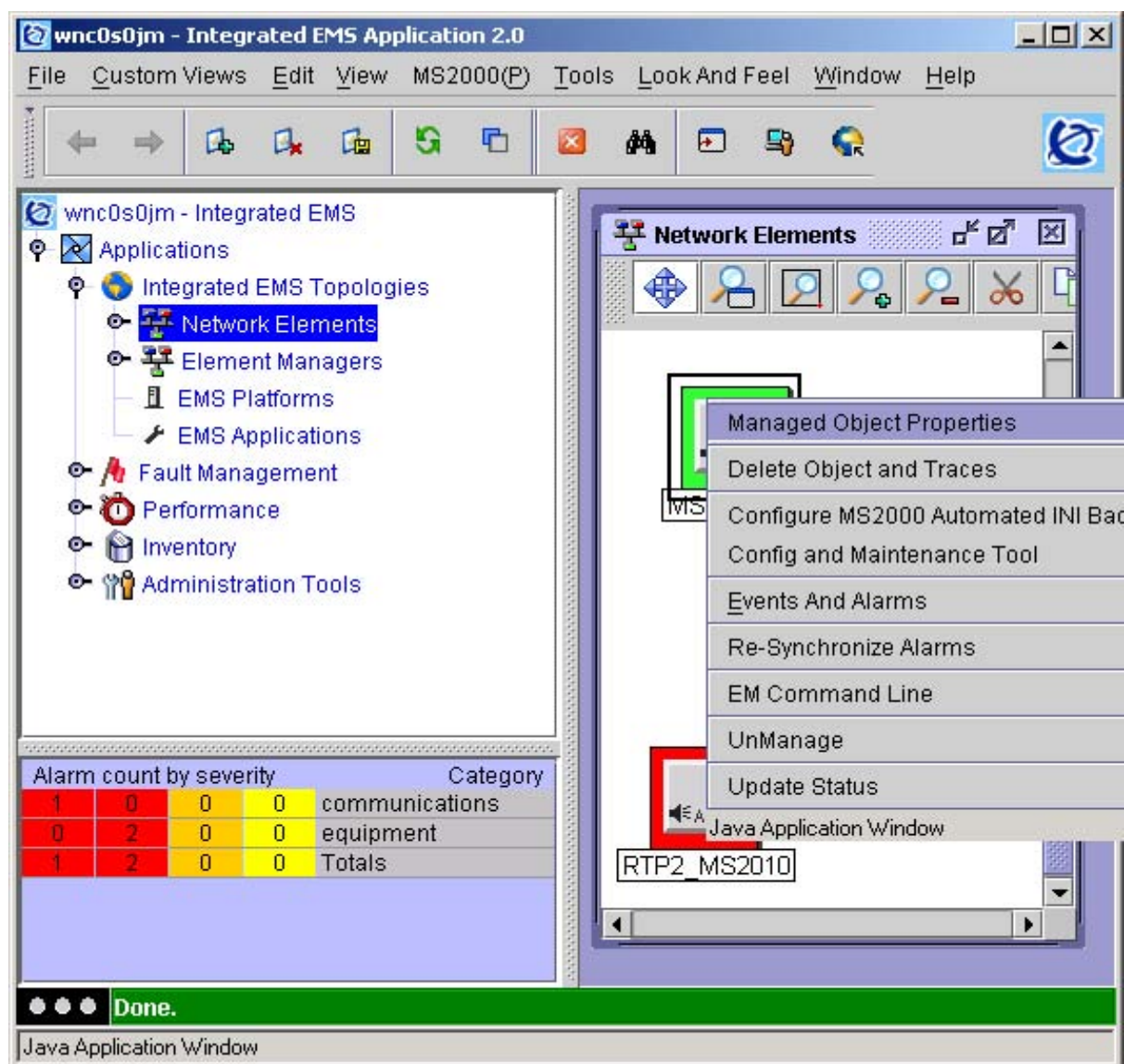
The MS2000 EM will run on IEMS and inherits any requirements and dependencies for software.

84.5 Limitations and restrictions

The existing MS2000 CLUI will be removed from the SESM software and all of its functionality will be migrated to the MS2000 EM.

84.6 Interactions

The MS2000 EM will be built into the IEMS tool such that the EM can be launched by selecting the MS2000 EM from the right click device menu as seen below.



The MS2000 Configuration and Maintenance tool is used to configure and perform some maintenance activities on an MS2010 or MS2020 device. The tool automatically adjusts the display components, behavior, and configuration options based on the node type (MS2010 or MS2020) and the software version.

The following screen is the display of the tool just after launching. The left hand side displays the Device specific information. The name given in IEMS,

the associated IP address entered when the node was added into the system, and the device type (this is determined by querying the MS node).

In the mid section of the left hand side is the Maintenance panel where the following functions can be performed.

- **Soft Reset of the node** - A soft reset of the node is essentially a re-initialization of the software running on the node. For an SN06.2 MS2000 load, only a burn reset was allowed. Starting in SN07 the user could select either to perform a configuration settings burn or to re-initialize with the previous burned settings. When a soft reset is done on the node with the burn option, the existing configuration settings are burned into flash memory and then the node goes through an initialization cycle. This will take the node out of service for a short period of time and will drop any resources in use.
- **Lock/Unlock the node** - The lock function will prevent any audio resources from being allocated on the node. In an SN06.2 MS2000 load, only a graceful lock was supported. A graceful lock will signal to the node that a lock has been requested. This will cause the node to stop allocating new audio resources and will wait for the last resource to be freed before actually locking the node. A force lock will cause the node to immediately free up any resources in use and lock the node.
- **Backup of the INI file** - The initialization file is a configuration data file used by the system to setup the node in event of a reboot. The file contains all of the user defined configuration changes. The tool allows the user to save the initialization file back to the IEMS server or to the tftp server (the SDM or CBM). By saving the INI file back to the IEMS server the user has simply saved a backup copy of the configuration changes for later use. The tool will save up to 5 initialization files for each node, deleting the oldest file once the maximum number of files have been saved. By saving the file to the tftp server, this updates the initialization file that the MS2000 node will retrieve should a hard reset occur. It is recommended that whenever configuration changes are made that the user backup the latest settings in an INI file to the tftp server.

The bottom panel on the main screen shows status logs of the activities that the tool is performing. This provides the user with feedback on what actions have been taken and also displays error when they occur.

MS2020 Maintenance and Configuration Tool

Device Name: MS2020_PV
IP Address: 47.142.89.60
Device Type: MS2020

Maintenance

☒ Burn Flash
☐ Don't Burn Flash
Reset

Lock State: unlocked

☒ Graceful Lock
☐ Forced Lock
Lock

☐ Backup INI to IEMS Server
☒ Backup INI to tftp Server
INI Backup

General Configuration | Load Management | Password

IP Address
SubNet Address
Default Gateway
MG Control Protocol
Software Version
Megaco Call Agent IP Address
Is Megaco Call Agent Used
Number of Conference Ports
Number of TestTrunk Ports
Number of Lawful Intercept Ports
Number of Announcement Ports
APS IP Address
Primary Language
Secondary Language
Syslog Server IP
ATM Default Application Type
Transmission mode

Status Logs

Successfully retrieved trusted managers table for node 47.142.89.60
Successfully retrieved trap destination table for node 47.142.89.60
Requesting data for table atmPortLoopbackConfigTable
Successfully retrieved table data

Close

Java Application Window

On the right hand side of the screen there are a series of tab selected panels for other configuration and maintenance functions that the user can perform.

84.6.1 General Configuration

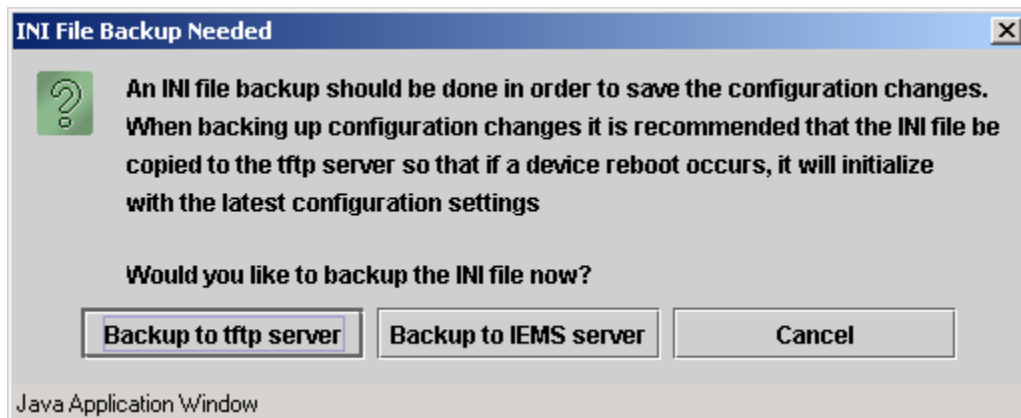
The first tab is the General Configuration tab where the basic setup of the node is performed. (Please reference the NTP for MS2010 and MS2020 for a complete description of the configuration parameters). The configurable fields have either a pull-down menu for the configuration options or a tooltip displaying the syntax and range of the field. Once the user makes the appropriate changes to the fields they can send the changes to the node by selecting the “SET” button.

General Configuration		Load Management	Password Management	SNMP Setup	Atm Configuration
IP Address	172.17.40.221				
SubNet Address	255.255.248.0				
Default Gateway	172.17.40.1				
MG Control Protocol	controlProtocol-MEGACO(2) ▼				
Software Version	4.40.9.40				
Megaco Call Agent IP Address	172.17.40.68				
Is Megaco Call Agent Used	yes(1) ▼				
Number of Conference Ports	100				
Number of TestTrunk Ports	100				
Number of Lawful Intercept Ports	100				
Number of Announcement Ports	180				
APS IP Address	47.142.89.70				
Primary Language	isoLangEnglish(2) ▼				
Secondary Language	isoLangEnglish(2) ▼				
Syslog Server IP	47.142.89.27				
ATM Default Application Type	aal2-i-366-2(2) ▼				
Transmission mode	sonet(1) ▼				

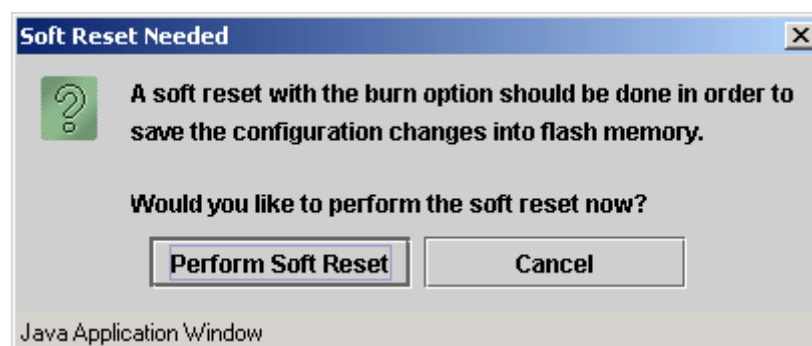
Should the user have entered in invalid data they will be prompted with a warning displaying which data is at issue. Below is an example of this.



Once corrected the user can again attempt to change the data. If successful, then the user will be prompted to save the configuration changes made by backing up the INI file. The user is given the option to either backup to just the IEMS node or to the tftp server.



Once the INI backup has been done the user will be prompted to perform a soft reset on the node in order to burn the configuration changes that were just made into flash.



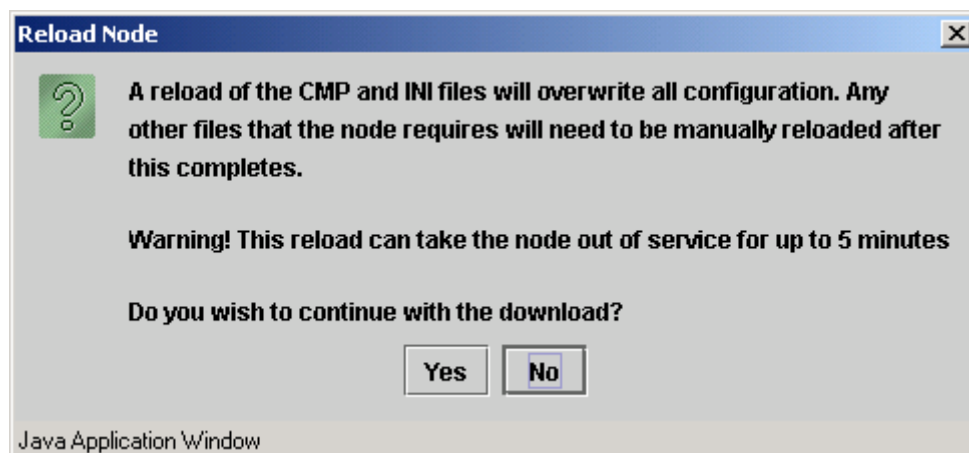
84.6.2 Load Management

The MS2000 Configuration and Maintenance tool provides a way for the user to download some of the file types used by the device. The files displayed that can be downloaded must be located on the IEMS server in the /data/loads/audiocodes directory.

The screenshot shows the 'Load Management' tab of the MS2000 Configuration and Maintenance tool. The interface includes a navigation bar with tabs for 'al Configuration', 'Load Management', 'Password Management', 'SNMP Setup', and 'Atrn Configuration'. Below the navigation bar, there are four distinct sections for selecting files to send to the node:

- Section 1:** A heading 'To reload the node select the "CMP" load and "INI" initialization files to send to the node'. It contains two dropdown menus: the first is set to 'MS2010.cmp' and labeled 'CMP File'; the second is set to '2004-11-01_21:35:53.Board.ini' and labeled 'INI File'. A 'Send Files' button is to the right.
- Section 2:** A heading 'Select a "INI" initialization file to send to the node'. It contains a dropdown menu set to '2004-11-01_21:35:53.Board.ini' labeled 'INI File' and a 'Send File' button.
- Section 3:** A heading 'Select a "DAT" call progress tones file to send to the node'. It contains a dropdown menu set to 'usa_cpt.dat' labeled 'DAT File' and a 'Send File' button.
- Section 4:** A heading 'Select a "VXML" file to send to the node'. It contains a dropdown menu set to 'testtrunk.vxml' labeled 'VXML File' and a 'Send File' button.

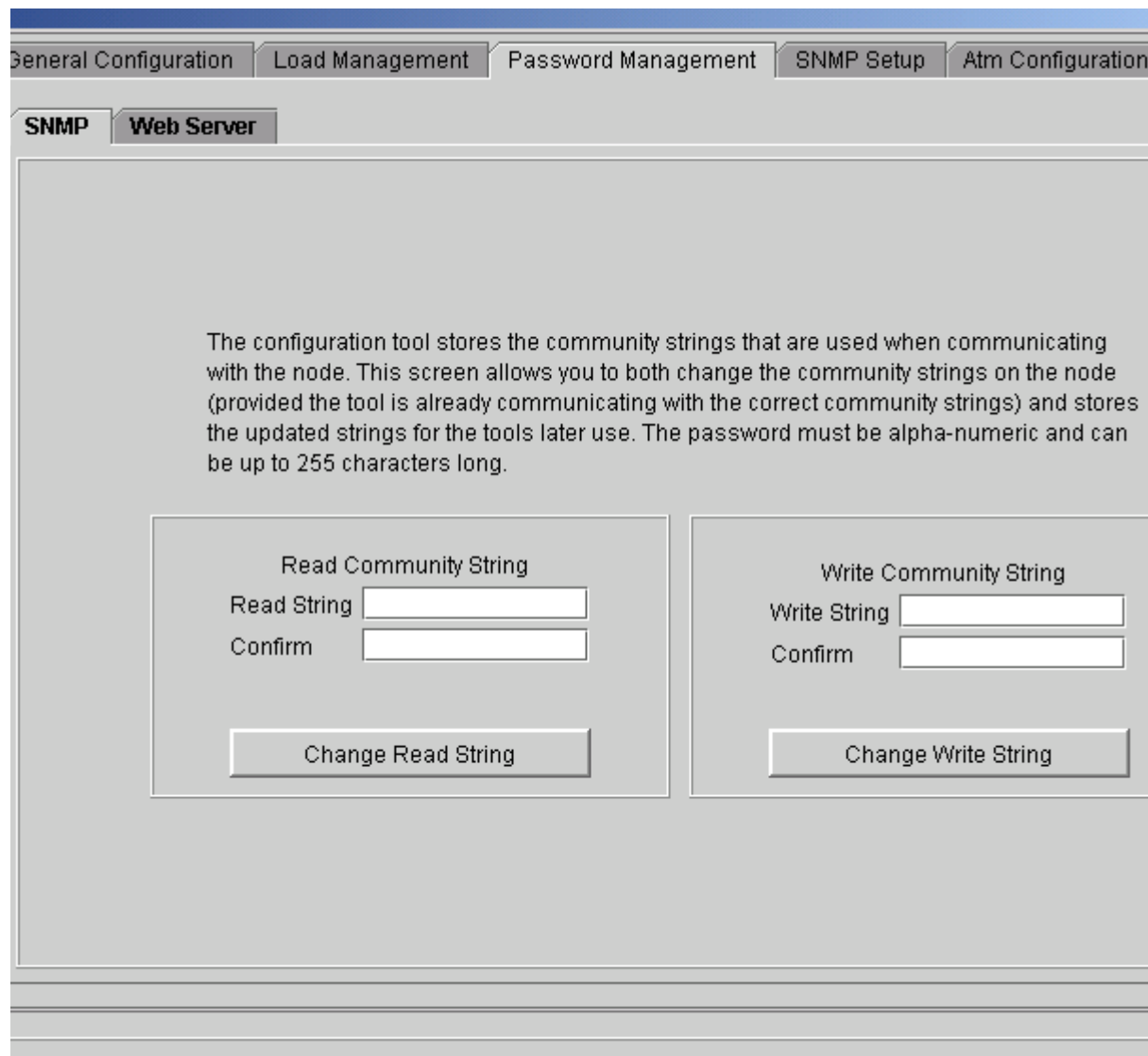
The tool provides the user with a way to remotely reload the device by downloading a CMP load file and an INI initialization file. The following display is shown when a user selects this option:



Similarly, the tool also provides the ability to download other node specific files such as a previously saved INI file (located on the IEMS server in the / data/loads/audiocodes/< node ip>/ directory).

84.6.3 Password Management

This panel allows the user to change the passwords on the node. The tool supports changing the SNMP read and write community strings as well as the node's web server username and password. Both of these panels have descriptions of the passwords and what they are used for.



The configuration tool stores the community strings that are used when communicating with the node. This screen allows you to both change the community strings on the node (provided the tool is already communicating with the correct community strings) and stores the updated strings for the tools later use. The password must be alpha-numeric and can be up to 255 characters long.

Read Community String	Write Community String
Read String	Write String
Confirm	Confirm
Change Read String	Change Write String

84.6.4 SNMP Setup

This panel allows the user to manage the Trusted Managers table and the Trap Destination Table. The node can handle up to 5 entries in each of these tables. Each of these panels has a description of the table and its use.

84.6.4.1 Trusted Managers

A trusted manager is an Element Manager (EM) from which the node accepts SNMP requests. By default, if there are no trusted managers defined then the node accepts requests from any manager that provides a valid SNMP community string.

Once a single trusted manager is configured, requests from any IP address not in the trusted managers table will be rejected. Because of this the first IP address added to the trusted managers table should be the IP address of the server where this Configuration Tool is running. If it is not then the tool will no longer be able to communicate with the device.

84.6.4.2 Trap Destinations

The Trap Destination table defines where the node should send it's SNMP traps. Most of the traps originating from the node are alarm related. The node is capable of routing these traps to multiple destinations should the user want the traps logged by different trap collection systems. Only five trap destinations may be defined.

General Configuration Load Management Password Management SNMP Setup Atm Configuration

Trap Destinations Trusted Managers

The Trap Destination table defines where the node should send it's SNMP traps. Most of the traps originating from the node are alarm related. The node is capable of routing these traps to multiple destinations should the user require the traps logged by different trap collection systems. Only five trap destinations may be defined.

	Trap Destinations	Port
1	47.142.89.73	162
2		
3		
4		
5		

Add Delete Refresh

84.6.5 ATM Configuration

This tab selection will only appear for MS2020 ATM devices. The number of tables displayed for configuration varies depending on if the MS2020 application type (AAL1 or AAL2). The panels provide both table edit, add, and delete buttons where applicable.

Please refer to the MS2020 NTP for explanation of the various fields in the tables.

General Configuration					Load Management	Password Management	SNMP Setup	Atm Configuration
Atm Port Table		Remote GW Table		AAL2 PVC Table		Svc Profile Table		
Port Loopback Table				Service Connection Table				
Port #	Admin State	Admin Address	Operational State	Operational Addr				
port0(0)	unlocked(2)		enabled(1)	47525450530000f00000000000000908f04aab300				
				Edit Entry Refresh Table				

84.7 Glossary

Table 2

Term	Description
New term	Definition

84: A00007343 Functional description (FN)

84.1 Feature name

PP8600 Extended Fault Mapping

84.2 Introduction

This document outlines the proposed implementation details for PP8600 Extended Fault Mapping in IEMS. In pre SN08 a minimal number of PP8600 events were supported in IEMS. All other events received from the PP8600 device were mapped as IEMS 602 “unknown” events.

This feature is to extend the PP8600 logs in IEMS to be transparent with the pre SN08 MDM implementation so that customers with previously deployed PP8600s that feed through MDM to SDM will have transparent cutover/migration to IEMS managed PP8600s.

84.3 Hardware Requirements or Dependencies

Not applicable.

84.4 Software Requirements or Dependencies

IEMS must have the relevant MIBs from the PP8600. This is expected to be 3.7.x.

84.5 Limitations and restrictions

Because this feature is intended to mirror the behavior of the MDM-SDM system, fault codes etc. will be used in accordance with previously decided conventions and values.

84.6 Interactions

The log format will change for all PP8600 originated logs.

84.6.1 Example old log (pre-SN08)

```
RTD ** PPES300 NOV14 12:20:47 1486 TBL
time: 2003 11 14 12 17 03
event: set
compId: PP8600 BATMAN IF 72
```

severity: major
 faultCode: C0000002
 alarmType: communications
 commentData: Link down trap interface: 72

84.6.2 Example new log (SN08+)

znc0s0jh ** PP398 May04 22:58:46 3203 TBL PP Fault
 Location: 47.142.106.1
 State: Raised
 Category: communications
 Cause: loss of communications
 Time: May 04 13:45:59 2004
 Component ID: PP8600=RTPU; ifIndex=175
 Specific Problem: OperStatus trap
 Description: Link Down: ifIndex = 175 (AdminStatus = down OperationStatus = down)

84.6.3 1.6.3 Trap to Fault Code Mapping

Trap Name	OID	Fault Code	Severity	Log Name	Log Num
risingAlarm	1.3.6.1.2.1.16.0.1	S C1220008	minor	PP	310
fallingAlarm	1.3.6.1.2.1.16.0.2	S C1220008	cleared	PP	311
Default Trap	DEFAULT	S C1229999	indeterminate	PP	312
coldStart	1.3.6.1.6.3.1.1.5.1.0	S C0000000	cleared	PP	313
warmStart	1.3.6.1.6.3.1.1.5.2.0	S C0000001	cleared	PP	315
linkDown	1.3.6.1.6.3.1.1.5.3.0	S C0000002	major	PP	317
linkUp	1.3.6.1.6.3.1.1.5.4.0	S C0000002	cleared	PP	318
authenticationFailure	1.3.6.1.6.3.1.1.5.5.0	S C0000004	warning	PP	319
rcnChasPowerSupplyDown	1.3.6.1.4.1.2272.1.21.0.6		critical	PP	322
rcnChasPowerSupplyUp	1.3.6.1.4.1.2272.1.21.0.14	S C1220007	cleared	PP	323
rcnChasFanDown	1.3.6.1.4.1.2272.1.21.0.7		critical	PP	324
rcnChasFanUp	1.3.6.1.4.1.2272.1.21.0.21	S C1220006	cleared	PP	325
rcn2kCardDown	1.3.6.1.4.1.2272.1.21.0.11	S C1220001	major	PP	326
rcn2kCardUp	1.3.6.1.4.1.2272.1.21.0.12	S C1220001	cleared	PP	327
rcn2kTemperature	1.3.6.1.4.1.2272.1.21.0.13	S C1220003	critical	PP	328
rcnErrorNotification	1.3.6.1.4.1.2272.1.21.0.3		warning, major, critical	PP	329
rcnLinkOscillation	1.3.6.1.4.1.2272.1.21.0.8		major	PP	330
rcnMacViolation	1.3.6.1.4.1.2272.1.21.0.9		warning	PP	331
rcnSonetTrap	1.3.6.1.4.1.2272.1.21.0.10	S C1220051	warning	PP	332
rcnStpNewRoot	1.3.6.1.4.1.2272.1.21.0.4		warning	PP	333

rcnStpTopologyChange	1.3.6.1.4.1.2272.1.21.0.5		warning	PP	334
rcnStpTCN	1.3.6.1.4.1.2272.1.21.0.16	S C1220017	warning	PP	335
rcn2kAtmPvcLinkStateChange	1.3.6.1.4.1.2272.1.21.0.15	S C1220012	indeterminate, minor, major	PP	336
rcnSmltIstLinkUp	1.3.6.1.4.1.2272.1.21.0.17	S C1220014	cleared	PP	337
rcnSmltIstLinkDown	1.3.6.1.4.1.2272.1.21.0.18	S C1220014	major	PP	338
rcnSmltLinkUp	1.3.6.1.4.1.2272.1.21.0.19	S C1220020	cleared	PP	339
rcnSmltLinkDown	1.3.6.1.4.1.2272.1.21.0.20	S C1220020	major	PP	340
rcnPasswordChange	1.3.6.1.4.1.2272.1.21.0.22	S C1220022	warning	PP	341
rcnPcmciaCardRemoved	1.3.6.1.4.1.2272.1.21.0.25	S C1220049	warning	PP	342
rcnSmartCpldTimerFired	1.3.6.1.4.1.2272.1.21.0.26	S C1220024	major	PP	343
rcnCardCpldNotUpDate	1.3.6.1.4.1.2272.1.21.0.27	S C1220025	warning	PP	344
rcnlgapLogFileFull	1.3.6.1.4.1.2272.1.21.0.28	S C1220026	major	PP	345
rcnCpLimitShutDown	1.3.6.1.4.1.2272.1.21.0.29	S C1220027	major	PP	346
rcnSshServerEnabled	1.3.6.1.4.1.2272.1.21.0.30	S C1220028	cleared	PP	347
rcnSshServerDisabled	1.3.6.1.4.1.2272.1.21.0.31	S C1220028	major	PP	348
rcnSshSessionLogin	1.3.6.1.4.1.2272.1.21.0.32	S C1220029	cleared	PP	349
rcnSshSessionLogout	1.3.6.1.4.1.2272.1.21.0.33	S C1220029	major	PP	350
rcnSshUnauthorizedAccess	1.3.6.1.4.1.2272.1.21.0.34	S C1220030	major	PP	351
rcnHaCpuState	1.3.6.1.4.1.2272.1.21.0.35	S C1220031	warning	PP	352
rcnInsufficientMemory	1.3.6.1.4.1.2272.1.21.0.36	S C1220032	warning	PP	353
rcnSaveConfigAction	1.3.6.1.4.1.2272.1.21.0.37	S C1220033	indeterminate	PP	354
rcnLoopDetectOnPort	1.3.6.1.4.1.2272.1.21.0.38	S C1220034	warning	PP	355
vrrpTrapStateTransition	1.3.6.1.2.1.46.1.3.0.3.0	S C1220048	warning	PP	356
rcnEmError	1.3.6.1.4.1.2272.1.21.0.23	S C1220023	warning	PP	357
ospfVirtIfStateChange	1.3.6.1.2.1.14.16.2.1	S C1220015	warning,cleared	PP	358
ospfNbrStateChange	1.3.6.1.2.1.14.16.2.2	S C1220011	warning,cleared	PP	359
ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2.3	S C1220016	minor, cleared	PP	360
ospfIfConfigError	1.3.6.1.2.1.14.16.2.4	S C122000F	major	PP	361
ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2.5	S C1220021	major	PP	362
ospfIfAuthFailure	1.3.6.1.2.1.14.16.2.6	S C122000E	major	PP	363
ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2.7	S C1220013	major	PP	364
ospfIfStateChange	1.3.6.1.2.1.14.16.2.16	S C1220010	warning,cleared	PP	365
rcnCardDown	1.3.6.1.4.1.2272.1.21.0.1		major	PP	366
rcnCardUp	1.3.6.1.4.1.2272.1.21.0.2		cleared	PP	367
rcnbgpEstablished	1.3.6.1.4.1.2272.1.21.0.39	S C1220039	cleared	PP	368
rcnbgpBackwardTransition	1.3.6.1.4.1.2272.1.21.0.40	S C1220040	cleared	PP	369
rcnAggLinkUp	1.3.6.1.4.1.2272.1.21.0.41	S C1220041	cleared	PP	370
rcnAggLinkDown	1.3.6.1.4.1.2272.1.21.0.42	S C1220041	cleared	PP	371
rcnlgmpNewGroupMember	1.3.6.1.4.1.2272.1.21.0.43	S C1220042	cleared	PP	372
rcnlgmpLossGroupMember	1.3.6.1.4.1.2272.1.21.0.44	S C1220042	cleared	PP	373
rcnlgmpNewQuerier	1.3.6.1.4.1.2272.1.21.0.45	S C1220043	cleared	PP	374
rcnlgmpQuerierChange	1.3.6.1.4.1.2272.1.21.0.46	S C1220044	cleared	PP	375

rcnDvmrplfStateChange	1.3.6.1.4.1.2272.1.21.0.47	S C1220045	cleared	PP	376
rcnDvmrpNewNbrChange	1.3.6.1.4.1.2272.1.21.0.48	S C1220046	cleared	PP	377
rcnDvmrpNbrLossChange	1.3.6.1.4.1.2272.1.21.0.49	S C1220046	cleared	PP	378
rcnFdbProtectViolation	1.3.6.1.4.1.2272.1.21.0.59	S C1220047	cleared	PP	379
rcnLogMsgControl	1.3.6.1.4.1.2272.1.21.0.60	S C1220050	cleared	PP	380
rcnSaveConfigFile	1.3.6.1.4.1.2272.1.21.0.61	S C1220052	cleared	PP	381
rcnDNSRequestResponse	1.3.6.1.4.1.2272.1.21.0.62	S C1220057	cleared	PP	382
pingProbeFailed	1.3.6.1.2.1.80.0.1	S C1220053	cleared	PP	383
pingTestFailed	1.3.6.1.2.1.80.0.2	S C1220054	cleared	PP	384
pingTestCompleted	1.3.6.1.2.1.80.0.3	S C1220054	cleared	PP	385
traceRoutePathChange	1.3.6.1.2.1.81.0.1.0	S C1220055	cleared	PP	386
traceRouteTestFailed	1.3.6.1.2.1.81.0.2	S C1220056	cleared	PP	387
traceRouteTestComplete	1.3.6.1.2.1.81.0.3	S C1220056	cleared	PP	388
UDPEapSessionEndTrap	1.3.6.1.4.1.562.42.5.1.3.2.2		cleared	PP	389
UDPEapSessionStartTrap	1.3.6.1.4.1.562.42.5.1.3.2.1		cleared	PP	390

84.7 Description

IEMS needs to support all the events indicated in the above table. As it is required to support such an extensive number of events, it is proposed that the Event mapping details be maintained in XML format in the IEMS server side. This will also provide additional flexibility in supporting any further events.

84.7.1 Implementation Details

Processing that occurs the IEMS in order to map the events received from the PP8600 device are detailed below:

- 1 The IEMS server, on addition of the first PP8600 device, initializes the event mapping details by reading them from the XML.
- 2 On receipt of an event from the PP8600 device, the event mapping details are retrieved based on the OID received in the trap.
- 3 Log/Alarm is generated by IEMS based on the event mapping details.

84.7.2 Proposed Format for persisting Event Mapping in XML

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<TRAPS>
  <TRAP
    oid = ".1.3.6.1.4.1.2272.1.21.0.11"
    name = "rcn2kCardDown"
    severity = "2"
    logName = "PP"
    logNumber = "326"
    eventType = "TBL"
    eventLabel = "PP Fault"
    category = "equipment"
    entity = "$ip_2KCardStatus"
    componentID="cardIndex=$1"
    alarmClear = "3"
    probableCause=" "
    description= "Card Down: cardIndex = $1( AdminStatus = $2 OperationStatus = $3)"
    specificProblem value = "RC 2K Card Status" >
      <VARBINDS>
        <varbind name = ".1.3.6.1.4.1.2272.1.4.9.1.1.1" property = "$1"/>
        <varbind name = ".1.3.6.1.4.1.2272.1.4.9.1.1.5" property = "$2"/>
        <varbind name = ".1.3.6.1.4.1.2272.1.4.9.1.1.6" property = "$3"/>
      </VARBINDS>
    </TRAP>
  </TRAPS>
```

84.8 Glossary

Term	Description
IEMS	Integrated Element Management System
PP8600	PassPort 8600

85: A00007344 Functional description (FN)

85.1 Feature name

IEMS Robustness/Southbound Event Throttling

85.2 Introduction to OMs

This document brings out the various Operational Measurements of IEMS. These measurements greatly help the craft person in monitoring and maintaining the IEMS, as it being the heart of managing the succession network.

85.3 High Level Design

The following table lists out the OMs that are to be collected by the IEMS. A separate MIB (IEMS OM MIB) will be defined for capturing all these OMs. Users can create templates by loading the IEMS OM MIB(Reusing the existing performance UI) and a Job can be created for periodically collecting the data. All these are done over the existing IEMS performance collection framework. These collected data will be transferred to the OSS in XML or CSV format. No SNMP Agent Implementation will be provided for querying these data as of now).

IEMS Operational Measurements:

Collection Attribute Name	Value reset for next collect. interval	Comments
database		
usedTableSpaceInBytes	No	
usedTableSpaceInPercent	No	
numOfTableCleanUpPolicyExecutions	Yes	
fault/events		
numOfEvents	No	
numOfEventsFromUnknownCustlogDevices	Yes	
numOfEventsFromUnknownSNMPDevices	Yes	
numOfEventsFromUnknownDevices	Yes	
numOfDiscardedEvents	Yes	

numOfEventsAdded	Yes	
eventQueueSize	No	
avgEventThroughputRate	Yes	
maxEventThroughputRate	Yes	Sample Period can be configurable
DeviceEventRateTable This table will have the following Columns ID DeviceName EventRate per Second	Yes	Events from Unprovisioned Devices will also be taken into account. This will be done at the level of Protocol, not at the level of device. i.e Entries will be there for SysLog and SNMP Protocols but not at the level of each SysLog and SNMP Device
fault/alarms		
numOfActiveAlarms	No	
numOfCriticalAlarms	No	
numOfMajorAlarms	No	
numOfMinorAlarms	No	
nmOfWarningAlarms	No	
numOfAlarmsCleared	Yes	
numOfAlarmsAdded	Yes	
performance		
numOfCollectionJobsProvisioned	Yes	
numOfReportJobsProvisioned	Yes	
numOfFailedReportJobs	Yes	
numOfTransferJobProvisioned	Yes	
numOfAttributesCollected	No	
numOfAttributesCollectedOverPreviousInterval	Yes	
performance/SuccessfulCollection Jobs		
numOf5MinSuccessfulJobs	Yes	
numOf15MinSuccessfulJobs	Yes	
numOf30MinSuccessfulJobs	Yes	

numOf60MinSuccessfulJobs	Yes	
numOf12HrSuccessfulJobs	Yes	
numOf24HrSuccessfulJobs	Yes	
performance/PartialSuccessfulCollection Jobs		
numOf5MinPartialSuccessfulJobs	Yes	
numOf15MinPartialSuccessfulJobs	Yes	
numOf30MinPartialSuccessfulJobs	Yes	
numOf60MinPartialSuccessfulJobs	Yes	
numOf12HrPartialSuccessfulJobs	Yes	
numOf24HrPartialSuccessfulJobs	Yes	
performance/FailedCollection Jobs		
numOf5MinFailedJobs	Yes	
numOf15MinFailedJobs	Yes	
numOf30MinFailedJobs	Yes	
numOf60MinFailedJobs	Yes	
numOf12HrFailedJobs	Yes	
numOf24HrFailedJobs	Yes	
performance/collectionJobTable		
5MinCollectionJobTable This table will have the following columns ID JobName Start Time Execution Time	Yes	Number of Jobs to include can be configurable
15MinCollectionJobTable	Yes	Number of Jobs to include can be configurable
30MinCollectionJobTable	Yes	Number of Jobs to include can be configurable
60MinCollectionJobTable	Yes	Number of Jobs to include can be configurable
performance/reportJobTable		

5MinReportJobTable	Yes	Number of Jobs to include can be configurable
15MinReportJobTable	Yes	Number of Jobs to include can be configurable
30MinReportJobTable	Yes	Number of Jobs to include can be configurable
60MinReportJobTable	Yes	Number of Jobs to include can be configurable
performance/failedTransfer Jobs		
numOf5MinFailedJobs	Yes	
numOf15MinFailedJobs	Yes	
numOf30MinFailedJobs	Yes	
numOf60MinFailedJobs	Yes	
numOf12HrFailedJobs	Yes	
numOf24HrFailedJobs	Yes	
performance/transfer JobTable		
5MinTransferJobTable	Yes	Number of Jobs to include can be configurable
15MinTransferJobTable	Yes	Number of Jobs to include can be configurable
30MinTransferJobTable	Yes	Number of Jobs to include can be configurable
60MinTransferJobTable	Yes	Number of Jobs to include can be configurable
topology		
numOfManagedObjects	No	
numOfAddedManagedObjects	Yes	
numOfDeletedManagedObjects	Yes	
numOfThrottledDevices	No	
numOfUnManagedDevices	No	
numOfUnknownDevices	No	
client		

numOfActiveClients	Yes	Includes both JAVA and HTML Clients.
numOfSuccessfulLogins	Yes	Includes both JAVA and HTML Clients. APIs are needed from MFT, as authentication is not carried out by the IEMS Server.
numOfFailedLoginAttempts	Yes	Includes both JAVA and HTML Clients. APIs are needed from MFT, as authentication is not carried out by the IEMS Server.
applicationMemory		
applicationHeapSize	No	
maxApplicationHeapSizeInAGivenInterval	No	Sample Period can be configurable
system		
systemRestartCount	No	Value will be Reset after Software Upgrade

1.2.1 OM Configurations & Table Definitions

JobConfigurationTable					
Attribute Name	Attribute Description	Data Type	Allowed Values	Default Value	Optional/ Mandatory
ID	ID which is internally generated as and when a row is getting inserted.	Integer			Mandatory
NUMOFJOBS	Number of longest duration jobs to be collected..	Integer			Mandatory

85.4 IEMS Overload Control

This functionality is aimed at reducing the impact on the IEMS when event/message rate from devices exceeds the support/affordable rate. Since IEMS plays a prominent role in managing the succession network, it should be protected from such unusual message rates. This document brings out the design for achieving the same.

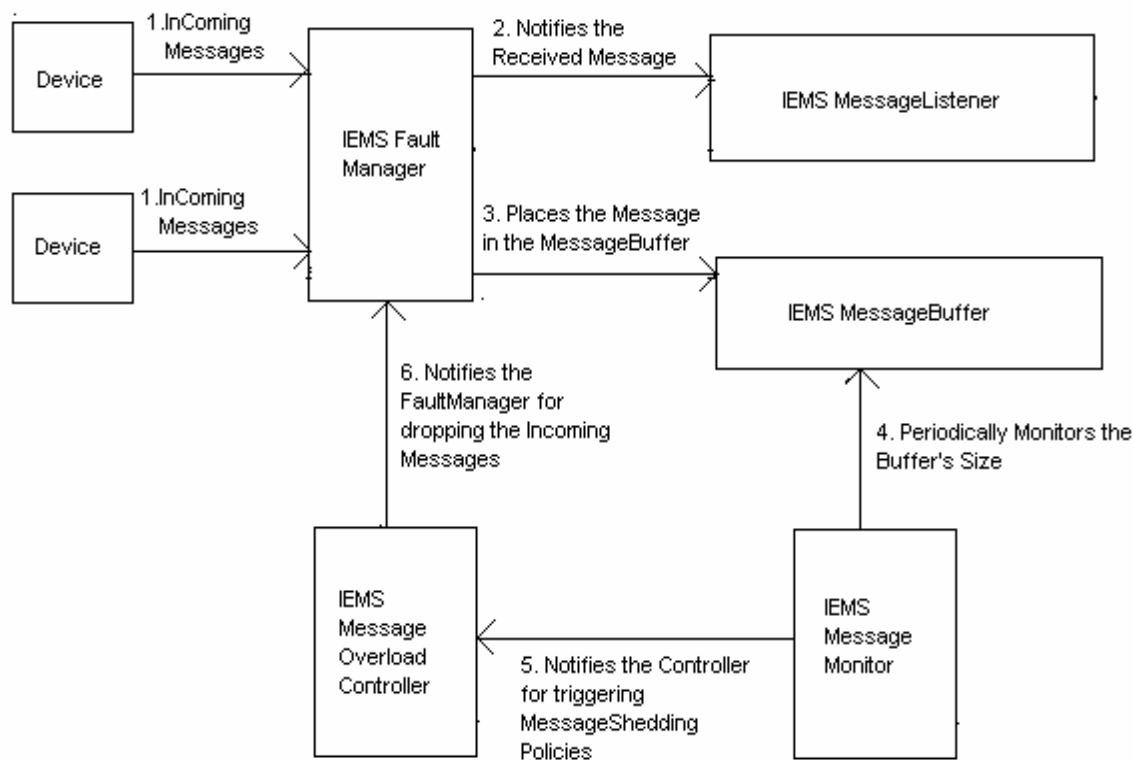
85.4.1 High Level Design

One of the ways of controlling the IEMS overload is by constantly monitoring the Event Streams of managed devices.(i.e for identifying the rouge devices). This can be achieved by implementing the following items.

- Component that monitors the message buffer size of the IEMS. This monitoring of message buffer will be done for every “n” events. (This number “n” can be configured).
- Component that captures the incoming rates of different devices/EMS, which is used by the system for identifying event babblers.
- Component that applies Event Shedding Policies for protecting the IEMS
 - Throttled State
 - Dropping the Events from UnProvisioned Devices.(i.e Devices not managed by the System)
 - Identifying the top fault interfaces
 - UnManaging and Changing the System's State to “Throttled”.
 - Generating Alarms to indicate the “Throttled” State
 - Dropping the incoming events received from this device
 - Changing the device's state to Manage after a specified timeout
 - UnManaged State
 - Changing the device state to “UnManage” if the device is in a Throttled State for a specified number of times. (This number can be configured)
 - Generating Alarms to indicate the “UnManaged” State

85.4.2 Low Level Design

Below diagram depicts the *important* sequence of events while monitoring and controlling the incoming messages to the IEMS.



(IEMS MessageOverload Controller uses the data maintained by the IEMS MessageListener, for determining the top fault interfaces of IEMS System)

85.4.3 IEMS MessageListener

This component (part of IEMS Fault Manager) listens for the incoming messages (for identifying top fault interfaces) of the various devices managed by the IEMS. Whenever an event is received by the IEMS, IEMS Message Listener will be notified about this event. This component just have a count on the number of events received for a specific device. No Time consuming work will be handled in this component as it may affect the EventProcessing rate of the IEMS.

85.4.4 IEMS MessageBufferMonitor

This component periodically monitors the message buffer of IEMS for every “n” events. A separate configuration that captures the following details will be defined for triggering the Message Shedding Policies.

- EnableMessageOverloadControl.

-
- Boolean Value that decides whether incoming messages to the IEMS need to be monitored or not. i.e OverloadControl should be enabled or not.
 - AcceptableEventBufferSize
 - Int Value representing the max number of messages in the buffer that IEMS can handle.
 - MessageMonitorCount
 - Int Value representing the number of messages to be received by the IEMS before checking the buffer size of the IEMS. i.e checking the Message Buffer for every “n” messages.
 - ThrottleStatePeriod
 - Time in MillisSeconds that a ManagedObject(MO) will be placed be in the Throttle State. After the ThrottleStatePeriod, the IEMS automatically switches the MO back to the Managed State.
 - ThrottleStateCount
 - Int Value that represents the max number of times, a Managed Object will be put in the Throttle State. Afterwards the IEMS automatically makes the MO to “System UnManaged” state.

If the Message Buffer Size exceeds the given max value (at the end of a given message count), it notifies the IEMS MessageOverload Controller to take corrective actions like triggering of Message Shedding Policies.

85.4.5 IEMS MessageOverloadController

This component triggers message shedding policies like shutting down of the fault interfaces having high message incoming rates, preventing IEMS from storing events from the unprovisioned devices etc. (It uses the data maintained by the IEMS EventListener for identifying the top fault interfaces Identifying top fault interfaces is done by taking average incoming message rate for each device.) After a specified timeout, it also take actions for receiving messages from devices, that are being identified as rogue previously.

85.4.6 New Fields in Managed Object

FISState (FaultInterface State) - String or Integer that captures the exact state of the Device.

- Normal
- Throttle UnManage
- System UnManage

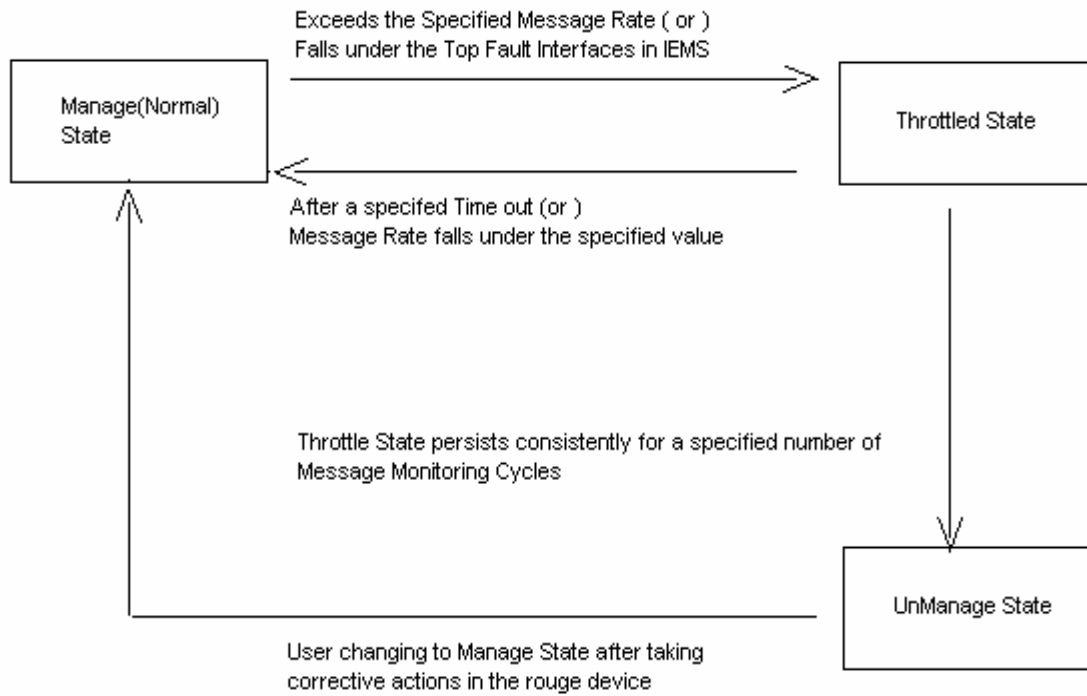
<i>Manage/ UnManage State</i>	<i>FaultInterface State</i>	<i>Comments</i>
Manage	Normal	Indicates normal functioning of the device.
UnManage	Normal	Indicates the Unmanage State of the device, which is being triggered by the User, but the device may be functioning normally.
UnManage	Throttled	Indicates the Unmanage State of the device, which is being triggered by the IEMS Overload Controller.
UnManage	UnManage	Indicates the Unmanage State of the device, which is being triggered by the IEMS Overload Controller, as the device is behaving as a rogue. This value will be automatically updated to "Normal" if the User updates the status of the device to "Manage".

UnManage - Boolean Value that captures whether IEMS is allowed to change the MO's state from "Throttled" to "UnManaged".

85.4.7 Table Definitions

Name: **MessageOverloadControlConfiguration**

Column Name	Data Type	Allowed Values	Default Values	Optional/ Mandatory
MOCID	Integer		1	Mandatory
ENABLE MESSAGE OVERLOAD CONTROL	Integer	0 or 1		Mandatory
MESSAGE_BUFFER_SIZE	Integer		500	Mandatory
MESSAGE_MONITOR_COUNT	Integer		1000	Mandatory
THROTTLE_STATE_PERIOD	Integer		5000	Mandatory
THROTTLE_STATE_COUNT	Integer		3	Mandatory

State Diagram that depicts the various states of a ManagedObject

86: A00007345 Functional description (FN)

86.1 Feature name

MDM Enhancements for IEMS

86.2 Introduction

This document presents the functional specification for the new enhancements to be done for the Preside MDM 8.0 in SN08.

86.3 Descriptions

86.3.1 Auto Discovery of Client set and Server set platforms

In SN08, the client sets and the server sets platforms will be automatically discovered when the Preside MDM 8.0 is added. IEMS discovers the client sets and the server sets platforms with the help of the following API's

IEMS registers with the Preside MDM Server with the following API,

- `_cmd`: REGISTER
- `_user_id`: chris

After registering with the Preside MDM, IEMS sends the following API to retrieve the devices (Passports, Platforms and VSPs) residing under this Preside MDM EM.

- `_cmd`: GET
- `_obj_class`: network
- `_obj_id`: networkId S compRoot
- `_scope`: NEXT
- `_filter`: objectClass EQ S node
- `_attr_id`: ALL

and the response message for the above API looks like the following one.

```

_obj_class: node
_obj_id: compId NI EM CLEVELAND
_attr: rawState E INSV
_attr: compAckState E notAked
_attr: compCriticality I 90

_obj_class: node
_obj_id: compId NI NMS FT1400-2
_attr: rawState E INSV

```

```
_attr: compAckState E notAcked
_attr: compCriticality I 80
```

If the response message contains “NMS” in the obj id, then it is modeled as MDM platforms (since there is no unique way to distinguish between the client sets/server sets platforms we are modeling it as a MDM platform). This auto discovery of client sets and server sets functionality are supported only for SN08 release and not for the pre-SN08 versions.

Just like other devices (Element Managers, platforms, Applications), the auto discovered MDM client sets and server sets platforms are also modeled as a ManagedObject and refer “Map representation of Client set and Server set platforms” for the Map display for these platforms.

Note: No support will be provided to provision the MDM platform 8.0 version from the “Add Platforms” menu.

86.3.2 Map representation of Client set and Server set platforms

The client sets and the server sets will be displayed to the topology tree under the “EMS Platforms -> MDM”. Representation for the same is shown below

```
EMS Platforms
|
|
| _ _ MDM
```

In the right side work area of the “MDM”, IEMS displays both client sets and the server sets platforms of all discovered Preside MDM Servers. In order to identify to which the Preside MDM Server the client sets/server sets belong, IEMS appends the displayName of the Preside MDM Server along with the displayName of the client sets/server sets platform in the right side work area.

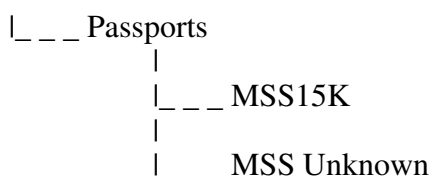
86.3.3 Map representation of Preside MDM Mgr and its associated NEs

The existing grouping of Preside MDM Mgr and its associated NE's are as follows

```
Element Manager
|
| _ _ _ Preside MDM (displayName)
```

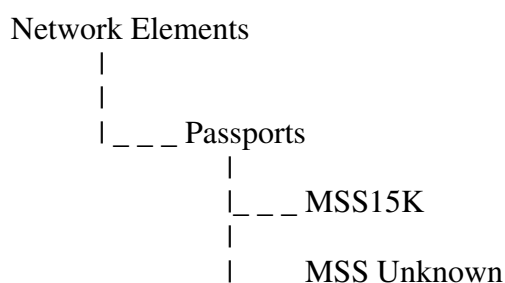
In the right side work area of the “Element Manager”, IEMS displays all discovered Preside MDM EM's. In the right side work area of the “Preside MDM (displayName)”, IEMS displays both the Units (Unit0 and Unit1) for duplex whereas for simplex it doesn't display anything.

```
Network Elements
|
```



In the right side work area of the “Passports”, IEMS displays the Passport devices (MSS15K, MSS Unknown etc) of all discovered MDM Servers, whereas in the right side work area of the “MSS15K” and “MSSUnknown”, IEMS displays the respective Passport devices.

The new grouping of Preside MDM Mgr and its associated NEs are as follows



In order to maintain consistency across the IEMS, the same tree structure is retained as like pre-SN08 release. In order to identify to which MDM Server the Passports/PVG's belongs, IEMS appends the displayName of the MDM Servers along with the displayName of the Passports/PVG's in the right side work area.

86.3.4 Fault mapping for auto discovered MDM Platforms

IEMS listens for the client sets and server sets alarms and correlates the same against the corresponding platforms. The correlation used is the same as like that of Preside MDM EM Passports etc.

Procedure to generate the Warning fault for MDM Platform from the *wcary3r6* - Preside MDM Server

- 1 Invoke the *nmstool* from *wcary3r6* (the absolute path is */opt/MagellanNMS/bin/nmstool*)
- 2 From the GUI invoke *System* menu
- 3 From the menus invoke *Administration* menu
- 4 From the menus invoke *Server Administration* menu
- 5 From the menus invoke *Security* menu
- 6 From the menus invoke *Authorize* menu

-
- 7 Click 'ok' without entering the password – This will generate a Warning alarm for the WCARY3R6 MDM platform.

86.3.5 Operator Client GUI Launch

A new menu item “MDM Operator Client GUI” will be provided to the context menu for Preside MDM Mgr. This menu will be available on the right click of the Map Symbol of Preside MDM Mgr 8.0 version. This menu is supported only for SN08 release and not for the pre-SN08 versions.

On clicking this menu item, IEMS will invoke the following URL in the client browser,

`http://<ipaddress>:8080/UI`

where <ipaddress> is the Preside MDM Server IP Address.

86.3.6 MDM X11 Client launch

In SN08, X11 communication is secured via SSH using MindTerm tool. The X11 Client launch requires X server needs to be run in the local client machine. In the case of Solaris/Linux, Xserver runs by default and in the case of Windows, Hummingbird or Exceed is used as Xserver.

A new menu item “Legacy MDM Tools” will be provided to the context menu for Preside MDM Mgr. This menu will be available on the right click of the Map Symbol of Preside MDM 8.0 version. This menu is supported only for SN08 release and not for the pre-SN08 versions.

On clicking this menu, IEMS will launch a “LegacyMDMTools” dialog, which captures the following attributes

- Text field to enter the Exceed executable file path (for Windows OS only).
- Text fields to enter Username/Password.
- Radio buttons with the following options
 - Server-Set Administrative Tools
 - Client-Set Administrative Tools
 - Client-Set Operational Tools

All the above options will invoke the nmstool with the parameter as said below

- 1 Server-Set Administrative Tools -- > “/opt/MagellanNMS/bin/nmstool admin”
- 2 Client-Set Administrative Tools -- > “/opt/MagellanNMS/bin/nmstool admin”
- 3 Client-Set Operational Tools -- > “/opt/MagellanNMS/bin/nmstool operation”



On executing the launch with proper configuration, the launch triggers an X11 connection from the corresponding device back to your desktop, and brings up the nms toolset menu with the given option.

Note: Since “LegacyMDMTools” has the same functionality of “MDM GUI Mgr”, the menu “MDM GUI Mgr” is disabled for Preside MDM 8.0 devices.

86.3.7 Command Line launch for MDM Passport

A new menu item “Command Line” will be provided to the context menu for Passport Network Elements that belong to Preside MDM 8.0 version. This menu will be available on the right click of the Map Symbol of Passport Network Elements. This menu is supported only for SN08 release and not for the pre-SN08 versions.

For “Command Line” launch, IEMS will initiate one-step login between the IEMS client and the Preside MDM server, that is IEMS will invoke an SSH client to log in to the Preside MDM Server. For this launch, IEMS will not use the SSO token for login into the Preside MDM Server. Instead, IEMS will gather credentials for login by prompting for entry of userid and password.

86.3.8 Testing Considerations

The following are some of the test considerations to be captured along with the new enhancements for backward compatibility in the test plans.

- Provision a Preside MDM 6.2 system in IEMS
- IEMS launching of the preside MDM 6.2
- Provision a Preside MDM 7.0 system in IEMS
- IEMS launching of the preside MDM 7.0
- Provision a Preside MDM 8.0 system in IEMS
- IEMS launching of the preside MDM 8.0

86.4 Glossary

SSH - Secure Shell

GUI - Graphical User Interface

MDM - MultiService Data Manager

IEMS - Integrated Element Management System

CLUI - Command Line User Interface

86.5 References

A00000000.2.doc

IEMS_Topology.pdf

IEMS_Client_Launch.pdf

A00007345_IEMS_MDM_Changes_DID_v2.pdf

87: A00007346 Functional description (FN)

87.1 Feature name

Backward Compatibility in IEMS

87.2 Introduction

IEMS serves as an integrated platform for managing various devices. This module is for providing Backward Compatibility in IEMS so that all the SN08 device versions and the previous device versions are supported in IEMS. This document lists the IEMS design changes required for the devices where an interface change was identified.

The IEMS must maintain backwards compatibility with its managed components for N-2 Succession releases. This SN08 activity required a Succession-IEMS Prime to perform the research with the help of IEMS managed component design primes to identify changes to their management interfaces that would impact their backwards compatibility with the IEMS.

The primary interfaces that needed to be analyzed through this activity included the topology, fault, performance, security (authentication and authorization), and client launch (CLUI and GUI) interfaces. Changes to the High Availability model of the IEMS managed component were also analyzed. If there were no “currently known” changes to an IEMS managed component's interface, it was so documented in the DID.

Where component interface changes have occurred, the Succession-IEMS Prime acquired information about the changes to the management interfaces of the IEMS managed components and provided the specifics to the Adventnet team.

In light of the details provided to Adventnet, design changes will be made to the IEMS to ensure that the IEMS can manage the new SN08 component version variants while being able to manage the older component versions (i.e., SN6.2, and SN07).

A regression test plan has been created in light of the research conducted for this feature. This activity is primarily targeted to perform the necessary regression testing with the IEMS managed components to ensure that backwards compatibility is maintained.

A request for information was made to various component primes for information on interface changes towards IEMS in SN08. The results of this research are documented in the DID. The DID was reviewed and updated with comments. It should be considered a snapshot in time and is based on the information available.

The following components were identified to have some SN08 changes that needed to be further explored.

- In SN08, the USP NE component had plans to make a Syslog feed available to the IEMS. USP will make the security and audit streams available to the IEMS. It is expected that the custlog stream will still not be made available to the IEMS in SN08.
- MDM related changes are being covered by a SN08 feature A00007345.
- MSS2000 related changes are being covered by a SN08 feature A00007341.
- CEM related changes are covered by a SN08 feature A00007347. In SN08, the CS2K Core Manager will provide faults to IEMS via CEM. Any SN08 changes to provisioning the CS2K Core Manager in IEMS will fall under the above-mentioned CEM feature.
- The version of MCS that lines up with SN08 is MCS4.0. A number of IEMS changes needed to cater to MCS4.0 architectural changes are slated to be addressed in SN08. The appropriate portion of the FN will address those MCS related changes.

87.3 Acronyms Used

IEMS -Integrated Element Management System

EM -Element Managers

HA -High Availability.

SM -System Manager

FPM -Fault Performance Manager.

SSH-Secure Shell

87.4 MCS Changes

SN08 lines up with MCS version 4.0.

There can potentially be more than one independent MCS network in a Central Office being monitored by IEMS.

MCS follows a HA model and may be deployed in the field in a simplex or a duplex configuration. In SN08, IEMS is adding support for the HA model (both simplex and duplex configuration).

Each independent MCS system will be represented by an “MCS NE” object in the “Network Elements” folder. This “MCS NE” is an opaque BLOB that will be the central point for aggregating faults from all corresponding SM and FPM objects provisioned into IEMS. (Note: An independent MCS system may be managing an RTP Media Portal in which case the parent object representing an entire MCS System will be an RTP Media Portal object in the “Network Elements” folder.)

The changes for MCS are divided into two categories. The first describes the changes for the System Manager and the second describes the changes related to the Fault Performance Manager.

87.4.1 System Manger

An MCS System Manager will always provide Fault and Performance capabilities.

A simplex MCS system will be represented in IEMS by a managed object signifying a logical SM and a managed object signifying a physical active System Manager.

A duplex MCS system will be represented in IEMS by a managed object signifying a logical, SM and two managed objects signifying a physical active and a physical alternate System Manager. The section below covers the various requirements for the MCS system manager.

87.4.2 Topology

The System Managers should be shown under the “Element Manager” node of the topology tree.

There can be more than one independent MCS network in the CO, each having a unique virtual IP (which will be entered into IEMS when configuring the System Managers). Therefore, the EM navigation tree will contain as many System Manager nodes under it.

In the new model, physical and logical SM servers will be displayed in the navigation tree. Logical System Mangers (which represent the Virtual IP of the MCS SM) are parents to Physical SMs. The logical System Managers will be shown directly under the EM node. The physical active and alternate System Managers will be shown as sub-nodes of a logical System Manager.

The naming convention of the System Manager is MCS_SM (UserAssignedNameOfSM).

The topology tree for the MCS system managers will be displayed as

```

Element Managers +-
                  |
                  +- MCS SM1 (logical) +-
                  |                     |
                  |                     | SM1 (physical - active)
                  |                     +- SM1 (physical - alternate)
                  |
                  +- MCS SM2 (logical) +-
                  |                     |
                  |                     | SM2 (physical - active)

```

+ - SM2 (physical - alternate)

Note: Each logical SM represents an independent MCS system.

Each MCS system will be represented by a Managed Object under the Network Element and will be an opaque BLOB. Faults from ALL SMs and FPMs should be resolved to the corresponding MCS object in the Network Elements folder.

The naming convention of the MCS Network Elements is MCS/CSE (UserAssignedNameOfTheCorrespondingSM)

Note: An independent MCS system may be managing an RTP Media Portal in which case the parent object representing the entire MCS System will be an RTP Media Portal object in the “Network Elements” folder.

The tree representation of the NE is as follows:

Network Elements

```

|
+- MCS/CSE (UserAssignedNameOfTheCorrespondingSM)
|
+- RTP Media Portal (UserAssignedNameOfTheCorrespondingSM)
|
+- MCS/CSE (UserAssignedNameOfTheCorrespondingSM)
|

```

87.4.3 Modifications to the “Add EM” GUI:

When adding an MCS System Manager, the IP that is given initially is the Virtual IP of the system.

The GUI should contain a combo box to enable a user to select a “Simplex” or a “Duplex” MCS system.

If the “Simplex” mode is selected, there should be a provision to enter one IP addresses, the physical IP of the active system manager.

If “Duplex” mode is selected, there should be provision to enter two IP addresses representing physical IP addresses of the active and the physical IP of the alternate System Manager.

Text-entry GUI elements should be introduced to let the operator enter a username and password (employed for SM CLUI launch).

87.4.4 Fault

In SN08 the protocol for the SM's fault interface continues to be SNMP traps. The fault data will be collected from the physical active SM. For data collection (resynchronize/pull), the physical IP of the SM will be used. The active System Manager will have an SNMP agent running in it while the alternate System Manager will not have an SNMP agent running in it.

The System Manager object representing the physical active system manager will show the highest severity fault status of the physical active System Manager. The System Manager object representing the physical alternate System Manager will be in an unknown state. IEMS will continue to listen for events from the alternate SM server and will thereby be able to recognize that a SWACT has taken place between mates within a MCS SM pair.

The System Manager object representing the logical system manager will display the highest severity fault status of the physical active System Manager. If IEMS is not able to contact both physical SM servers (active and alternate), the object representing the logical System Manager will display an unknown state until such time that IEMS regains contact. A "Comm. Failure" fault will be issued by IEMS if the both physical SM servers of a duplex system cannot be contacted.

Note: A "Comm. Failure" fault will be issued by IEMS if the physical SM server of a simplex system cannot be contacted.

An operator will retain the capability of manually toggling a **physical** SM server between an Unmanaged and Managed state. IEMS will not collect fault or performance data from a server in an unmanaged state. If an MCS SWACT takes place during the time a server has been set to Unmanaged via IEMS, the icons for the server in unmanaged state will only be updated after the operator manually brings back the server to a Managed state.

The MCS Object under the Network Elements will be automatically updated with the corresponding fault status due to the parent-child relationship. If IEMS is able to contact at least one physical SM server (active and alternate) or an FPM server, the object representing the Network Element will display the highest severity fault status of the aggregate SM and FPM servers. Otherwise, the MCS NE icon will be in an unknown state.

87.4.4.1 Notes:

- 1 All managed objects corresponding to MCS physical servers (SM and FPM) should have manage/unmanage capability.
- 2 All managed objects corresponding to MCS logical components (logical SM and MCS NE) should have manage/unmanage capability.
- 3 Cascading of Managed/Unmanaged state

-
- When a user sets the logical SM managed object to “Unmanaged state”, the MCS SM physical servers should be forced into “Unmanaged state”.
 - When a user sets the logical SM managed object to “Managed state”, the MCS SM physical servers should be forced into “Managed state”.
 - When a user sets the MCS NE managed object to “Unmanaged state”, the MCS SM logical, MCS SM physical and FPM physical servers should be forced into “Unmanaged state”.
 - When a user sets the MCS NE managed object to “Managed state”, the MCS SM logical, MCS SM physical and FPM physical servers should be forced into “Managed state”.

87.4.5 Detecting the Active SM Server

- 1 Polling the SNMP agent for the System Managers. The alternate system manager will not have an SNMP agent running. The SM, which has the SNMP agent running, is the active System Manager. An SNMP query to the inactive server will result in a time-out. A “Comm. Failure” fault will be issued by IEMS if the both physical SM servers of a duplex system cannot be contacted.
Note: A “Comm. Failure” fault will be issued by IEMS if the physical SM server of a simplex system cannot be contacted.
- 2 IEMS will receive a coldstart from MCS object with the active server's IP address. IEMS will use this to identify the active system manager.
- 3 If a SWACT has taken place, the fault will be received from the physical IP of the previously alternate system manager. IEMS should recognize this change in the IP and determine that a SWACT had taken place.

87.4.6 Performance

The protocol for MCS SM's performance interface in SN08 continues to be sftp. An MCS System Manager will always provide Fault and Performance capabilities. The performance data will be collected from the physical IP's of the active physical System Manager.

IEMS should have a work item to change the current way we configure our collection job for MCS. Currently we can set up only one file filter for the MCS device (as it is associated with the MCS SM MO, not the collection job). This does not allow us to collect unique sets of data with multiple MCS collection jobs in the IEMS. The ability of specifying unique directory and file filters will help in two ways:

- MCS4.0 can be configured for collecting different sets of data with multiple collection intervals (i.e., 5 min and 30 min) at the same time, and the csv files reside in different directories. An operator should have the ability to collect and report data for multiple collection intervals.
- The MCS system monitors a number of devices and the csv files for different devices reside in different directories. An operator should have the ability to collect and report data for individual devices.

Previous to MCS4.0, performance data used to reside in:

“/IMS/tss/data/oss/OM/b643net/MgmtSite/*/0”

For MCS 4.0 release, the performance data are in the directory:

“/var/mcp/oss/om/MCP_4.0/<fault-performance manager instance id>/<network element instance id>/<file format option name>”, e.g. “/var/mcp/oss/om/MCP_4.0/FPM1_0/*/csv-file” where * is a wildcard representing “network element instance id”.

87.4.7 CLUI Launch

The SM will support GUI and CLUI launch. The GUI launched will be the MCP System Management Console running on the SM.

There is a CR (#Q00963269: Menu entries for GUI launch ignore device variant) related to the SN07 device variant not being taken into consideration when a pop-up menu is invoked off an MCS Manager object. This CR will be addressed and the deficiency it points out retested during SN08 IT of MCS enhancements.

There is a CR (#Q00964269: Need unique instance of GUI launch file-chooser for each MCS Manager Object) related to the same instance of file-chooser being launch for all MCS Manager objects. This CR will be addressed and the deficiency it points out retested during SN08 IT of MCS enhancements.

In spite of the fact that the MCS4.0 SM GUI is a Java Web Start Client, the MCS team has made a decision not to support MCS SM GUI Launch on a Unix console. The MCS4.0 SM GUI (called the MCP System Manager Console) will only be launched on Windows platforms. If a Windows Client does not have the correct version of JRE needed for the MCS SM GUI, an automatic download (of the JRE) from the MCS SM server will be initiated.

The CLUI launch should proxy to the IEMS server and then SSH to the IP of the SM.

87.5 Fault Performance Manager (FPM)

A new device called the FPM is introduced in SN08. This will supplement the MCS SM in very large COs. Accordingly, there may be zero, one or more FPMs present in the MCS system. The FPMs are designed to provide fault and performance data. When the CO gets larger, more FPMs will be added to the system. FPMs DO NOT abide by the HA model followed by MCS SM.

As the FPM supplements an SM in the system, the user should not be able to provision an FPM in IEMS until an SM is added. When provisioning an FPM in IEMS, the user should choose the SM with which this FPM is associated. The FPMs that supplement the SM will need to be added manually into IEMS.

87.5.1 Topology

Similar to SMs, the FPMs will be shown under the “Element Manager” node in the topology tree. As there can be more than one FPMs in the system, there will be as many FPMs under the “Element Manager” node in the topology tree.

The naming convention of the FPM is MCS_FPM
(UserAssignedNameOfSM_UserAssignedNameOfFPM)

The tree representation of the FPMs will be as follows.

```

Element Managers +-
                  |
                  +- MCS FPM1 (utilizing a physical IP)
                  |
                  +- MCS FPM2 (utilizing a physical IP)
                  |
                  +- MCS FPM3 (utilizing a physical IP)

```

87.5.2 Introduction of a new “Add EM” GUI

The ability to provision an FPM into IEMS as a separate EM will be provided via the new “Add EM” GUI. The IP that is entered by the user is the physical IP address of the FPM.

As FPMs are subordinate to SMs, an FPM should always be associated to an MCS4.0 SM. Hence, if an MCS4.0 SM is not already added in IEMS, the user should not be able to add an FPM object in IEMS. Accordingly, in the FPM addition GUI, a combo box will be shown that will list the already added MCS4.0 SMs in IEMS. The user should associate this FPM with one of the listed MCS4.0 SMs by choosing an MCS4.0 SM from the combo box.

Note: Note: An SM which is not for an MCS4.0 Solution should NOT appear in the combo-box.

Text-entry GUI elements should be introduced to let the operator enter a username and password (employed for FPM CLUI launch).

87.5.3 Fault

The fault interface (SNMP traps) used to collect the fault information for SMs can be used for FPMs too. The fault data can be pulled (resynchronized) from the IP address of the FPMs. The MCS object in the Network Elements folder will be automatically updated with the corresponding fault status due to the parent-child relationship.

87.5.4 Performance

The protocol for MCS FPM's performance interface in SN08 will be sftp. The performance data will be collected from the physical IP's of the FPM (Fault and Performance Manager).

FPMs should be listed as a distinct entity (i.e. in addition to the SM in the "Device type" comboBox on the IEMS PM CollectionJob GUI panel

Previous to MCS4.0, performance data used to reside in:

`"/IMS/tss/data/oss/OM/b643net/MgmtSite/*/0"`

For MCS 4.0 release, the performance data are in the directory:

`"/var/mcp/oss/om/MCP_4.0/<fault-performance manager instance id>/<network element instance id>/<file format option name>", e.g. "/var/mcp/oss/om/MCP_4.0/FPM1_0/*/csv-file"` where * is a wildcard representing "network element instance id".

87.5.5 GUI/CLUI Launch

The FPM will support GUI and CLUI launch. The GUI launched will be the MCP System Management Console running on the SM.

The following CRs and GUI information were discussed earlier and are repeated here for ease of reference.

There is a CR (#Q00963269: Menu entries for GUI launch ignore device variant) related to the SN07 device variant not being taken into consideration when a pop-up menu is invoked off an MCS Manager object. This CR must be addressed and the deficiency it points out must be retested during SN08 IT of MCS enhancements.

There is a CR (#Q00964269: Need unique instance of GUI launch file-chooser for each MCS Manager Object) related to the same instance of file-chooser

being launch for all MCS Manager objects. This CR must be addressed and the deficiency it points out must be retested during SN08 IT of MCS enhancements.

In spite of the fact that the MCS4.0 SM GUI is a Java Web Start Client, the MCS team has made a decision not to support MCS SM GUI Launch on a Unix console. The MCS4.0 SM GUI (called the MCP System Manager Console) will only be launched on Windows platforms. If a Windows Client does not have the correct version of JRE needed for the MCS SM GUI, an automatic download (of the JRE) from the MCS SM server will be initiated.

The CLUI launch should proxy to the IEMS server and then SSH to the IP of the FPM.

87.6 Deleting the Managed Objects

87.6.1 Deletion of an FPM

To delete an FPM, the user can right-click on the FPM object and click on the “Delete” menu item. This will delete the selected FPM.

87.6.2 Deletion of an SM

To delete an SM, the user can right-click in the SM object and click the “Delete” menu item. This will delete the selected SM object. However, since an SM can have zero or more FPMs under it, the user should not be able to delete an SM unless all the FPMs that are associated with the SM are deleted. If a user chooses to delete an SM that contains one or more FPMs under it, the user should be informed to delete all the FPMs under it and then delete the SM.

Note: Cascade deletion of an SM and all the FPMs under it is not provided to make the user realize the effects of the operation.

87.6.3 Deletion of the NE

Since the user is not adding the NE manually, there will not be any manual deletion option for the NE. Once an SM object is deleted, the associated NE will be automatically deleted from the “Network Elements” folder.

87.6.4 Changing the IP address of the Logical or Physical System Manager

The user will be able to change the IP address of a Logical or Physical System Manager that has one or more FPMs without actually deleting and re-adding an SM object (since deletion of an SM object is disallowed for SMs with corresponding FPMs).

87.7 References

1. A00007346_IEMS_Backward_Compat_DID_v5.pdf
2. MCP_OAM_SysArch_(PDF).pdf

88: A00007347 Functional description (FN)

88.1 Feature name

CEM Integration with IEMS

88.2 Description

88.2.1 Alarm Properties

There is a new field within IEMS in the alarm properties which indicate whether the alarm is manually clearable as documented here by the IEMS design team:

IEMS Alarm Properties Dialog would include alarmClear property from now on to identify manually clearable and non clearable alarms.

The alarmClear attribute would now be shown in the Alarm Properties Dialog. The value of this would be mapped to

- other (1),
- forbidden (2),
- required (3),
- optional (4)

“This object provides guidance to a mid-level manager on the handling of this alarm. A value of forbidden indicates that a mid-level manager MUST NOT allow this alarm to be manually cleared. A value of required indicates that this alarm has no corresponding clear so MUST always be manually cleared. A value of optional indicates that this alarm does have a corresponding clear, but that is MAY also be cleared manually. A value of other indicates that the manual clear status is either unknown or not one of the specified values.”

This attribute can potentially be used to identify the manually clearable events.

Nortel Networks Custom Alarm Properties ----comp5iems [X]

Alarm User Properties

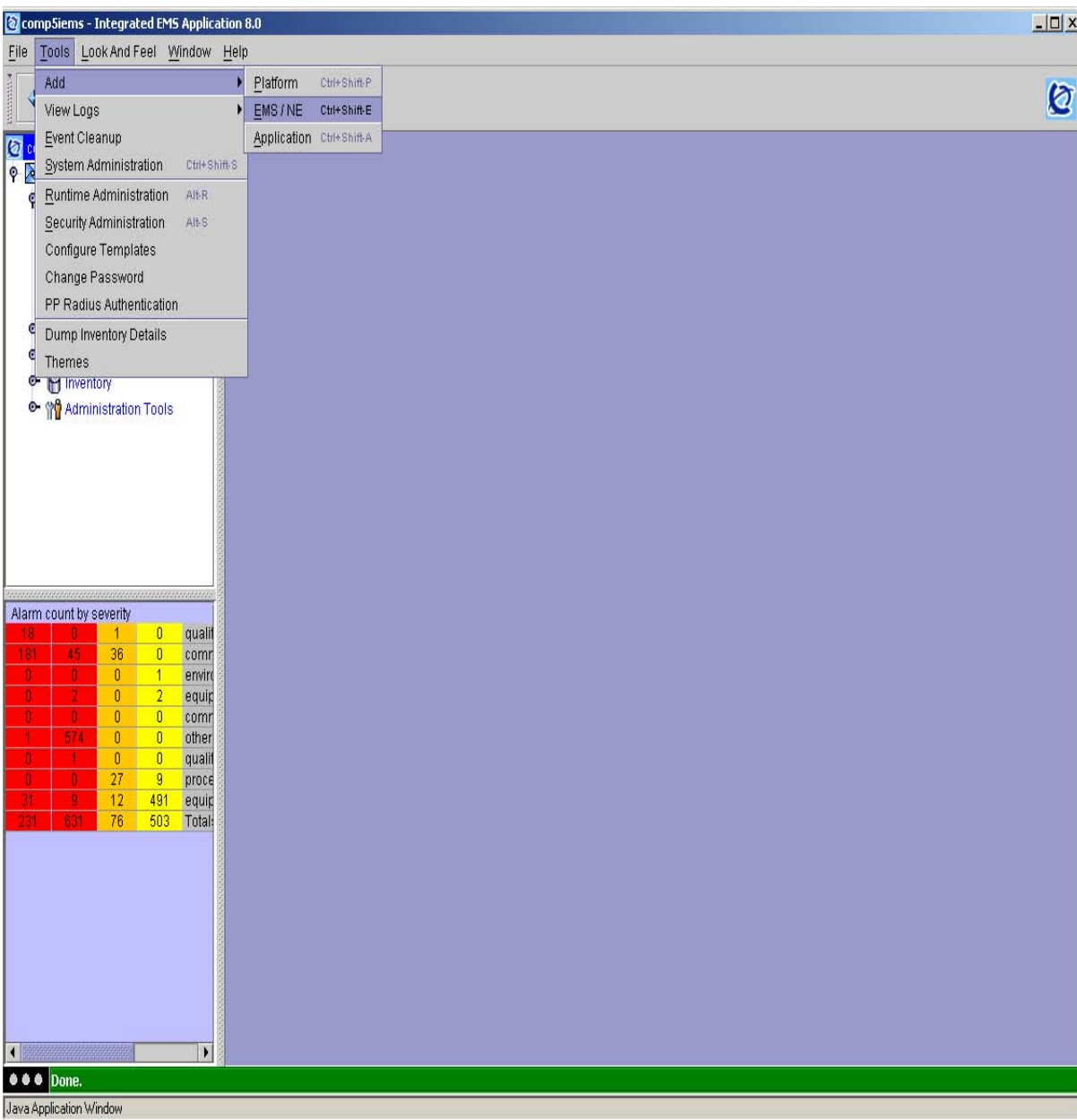
logName	IEMS
logNumber	398
componentID	anc0t0jn.us.nortel.com-SSPFS-Unit-0
eventType	FLT
eventLabel	Communication Lost
logKey	IEMS398
probableCause	communicationsSubsystemFailure
alarmClear	2
sequenceNumber	0
alarmIndex	3
bodyText	Location: 47.142.128.86 NotificationID: 0 State: Raised Category: Communications Cause: Communications subsystem failure
equipmentIdentifier	anc0t0jn.us.nortel.com-SSPFS-Unit-0
neType	IEMS

OK Close Help

Java Application Window

88.2.2 Configuring a CEM

To configure a CEM is like any other NE, simply choose tools, add EMS/NE



Enter the DNS name, or IP address along Host Name / IP Address. Display name should be the “Element Name” chosen when configuring the CEM on the SSPFS using configCEMS. Change Device Type to CEM Mgr. Click Next, Next and Finish.

88.3 Hardware Requirements or Dependencies

88.4 Software Requirements or Dependencies

88.5 Limitations and restrictions

88.6 Interactions

88.7 Glossary

Table 1

Term	Description
New term	Definition

89: A00007359 Functional description (FN)

89.1 Feature name

USP/USP-Compact: Log Delivery Stream to IEMS [Integrated Element Management System]

89.2 Description

This feature enhances the functionality of USP by supporting the delivery of security and audit logs to the IEMS syslog server or any other application. However, this feature will be tested with IEMS based syslog server. USP log data is sent to IEMS in unformatted manner using syslog.

Currently, the USP only sends Alarms via the SNMP interface (integrated into IEMS, Micromuse and some customer OSS's). This functionality will remain unchanged.

No new logs will be introduced under this feature. The current USP log format and the data contained in the USP logs will not be changed under this feature

The user could provision the following parameters from the USP GUI panel to deliver the logs to syslog server.

- Log-delivery Enable/Disable option.
- Primary IP address of the IEMS server.
- An optional backup/secondary IP address of the IEMS server.
- Non editable transport protocol used (i.e. UDP/TCP) to deliver the logs
- Non editable port number [defaulted to 514].
- Select the category of logs (i.e. security and audit logs) to be delivered.

Following mockup snapshots show how the log delivery panel can be launched and how the user can modify log-delivery information.

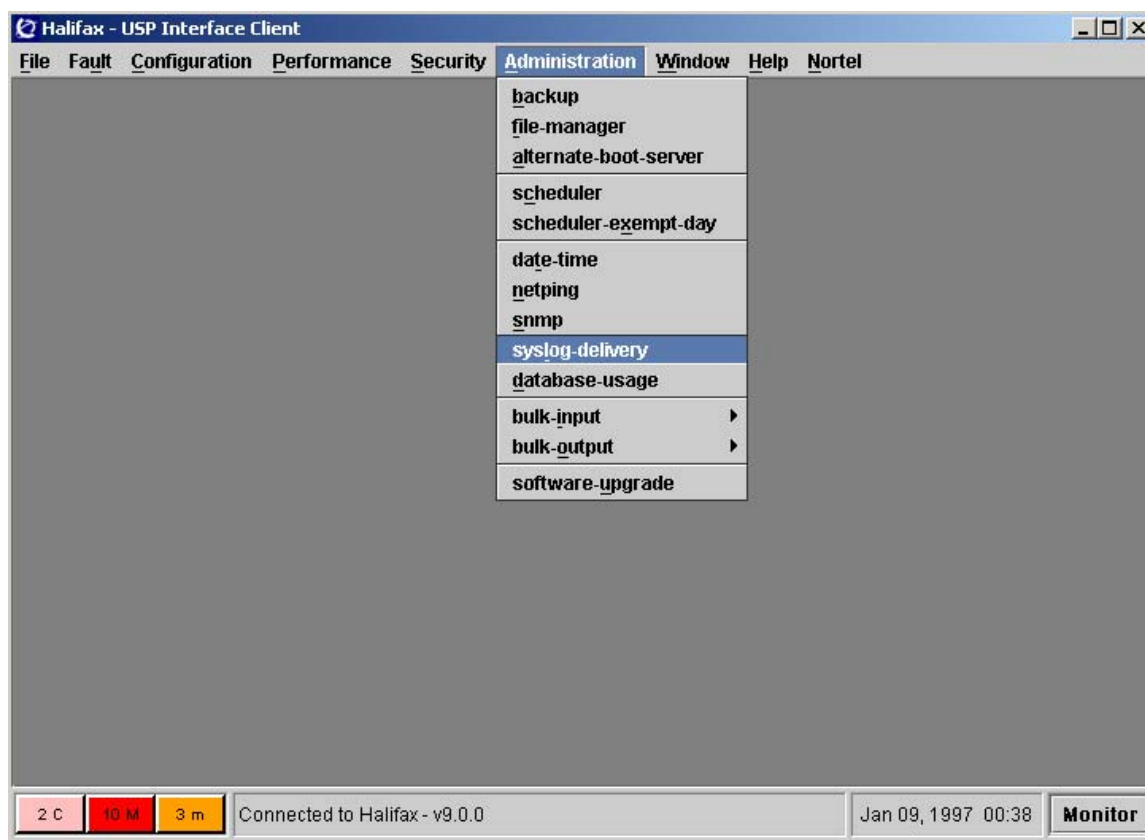


Figure 1 IEMS Log Delivery Feature Launch Panel

Figure 2 IEMS Data Provisioning Panel

Two categories of logs i.e. Audit Logs and Security Logs are supported.

The user has the flexibility of selecting to deliver either security logs or audit logs or both categories of logs to IEMS server.

USP follows syslog format for sending Audit and Security Logs.

Following is the Syslog format used for delivering security and audit logs to IEMS server.

Syslog Format:

```
<PRI> "date-time" "system name" "Message-
Version" ... USP log data with fields delimited by ;
...
```

- The <PRI> field or priority represents the Facility and Severity. The priority is a one, two or three decimal integer enclosed in an angular braces "<>"
- Date-time field follows the "<yyyymmdd>T<hhmmss.ssss>{+|Z|-}hh" format and >{+|Z|-}hh refers to daylight savings time.
- System name refers to the source device's hostname.
- Message Version indicates the USP/USP-Compact messaging version.

- USP Log data fields will follow the order as follows:
log-severity; log-group-name; log-number; system-node-name; log-description; log-date-time; data; module-name; line-number; task-name; sending-node-name; shelf; slot; context-id; log-group-id

Following are the samples of audit and security logs on USP which shall be delivered to IEMS:

Example of the security log in syslog format

```
<157> 19970101T04:23:28.0000Z-05 USP1 1 77;LOG_INFO;FTP Server;
1;sco1_12;full access enabled for user-id FIELD : ID=0x0; ;01/01/1997
04:20:18;ftpServer.cc; 892;tdbgServerTask;sco1_12; 0; 12;0x0; 46;
```

Example of the audit log in syslog format

```
<133> 19970101T05:10:24.0000Z-05 USP1 1 127;LOG_INFO;Journal Files;
1;sco1_12;FIELD@192.219.223.243:system mod:success;0x620 0x0 1 SCORPIO1
direct ;01/01/1997 05:10:24;oamUtils.c; 114;oamSrvTask;sco1_12; 0; 12;0x0; 41;
```

89.3 Hardware Requirements or Dependencies

This feature requires IEMS server and USP platforms [USP and USP-Compact].

89.4 Software Requirements or Dependencies

This feature requires USP10.0 or later of the USP software with enhanced IEMS software SN08 or later.

89.5 Limitations and restrictions

This feature does not support TCP based log-delivery.

89.6 Interactions

This feature does not change the existing functionality of USP GUI or the USP system software. There is an impact of software upgrade on this feature. If an upgrade is performed from older versions to USP10.0 or later, a new table in the RDM database will get added. This table will have information about the IEMS server.

USP interacts with IEMS server over UDP socket for sending audit and security logs.

89.7 Glossary

Term	Description
IEMS	Integrated Element Management System
IP	Internet Protocol
OSS	Operations Support System
RDM	Raima Database Manager
SNMP	Simple Network Management Protocol

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USP	Universal Signaling Point

90: A00007369 Functional description (FN)

90.1 Feature name:

DTAG LLIN

90.2 Feature Synopsis

This document describes the functionality being propagated into USP10.0 from SSR3.6.5 to support the Low Layer Intelligent Network (LLIN) application currently deployed in the DTAG network.

This feature is not introducing new functionality. This feature is responsible for propagating the functionality supported in SSR3.6. A functional description listing the functionality supported in SSR3.6 can be found in the SSR3.6 FD document entitled “Low Layer Control Point – Phase II” version 2.7.

This document outlines the differences between the SSR3.6 approach to managing a Low Layer Control Point (LLCP) product compared to the USP10 approach for functionality which is specific to the LLCP application.

90.3 References

BroadBand STP SSR3.6 Product Specification: <http://livelink.us.nortel.com/livelink/livelink.exe?func=ll&objId=3319115&objAction=browse&sort=name>

Low Layer Control Point (LLCP) – Phase II (SSR3.6 G2S FD (PDF)): <http://livelink.us.nortel.com/livelink/livelink.exe?func=ll&objId=3215551&objAction=browse&sort=name>

Universal Signaling Point (USP) USP10 Product Specification: http://livelink.us.nortel.com/livelink/livelink.exe/7577803/USP_10_Product_Spec.doc?func=doc.Fetch&nodeid=7577803

025860: New Hardware Support (PP5): <http://livelink.us.nortel.com/livelink/livelink.exe?func=ll&objId=7017774&objAction=browse&sort=name>

90.4 Feature Description

The functionality currently in the SSR3.6 stream that DTAG is using is outdated and does not contain many of the robustness items and features in the current USP10.0 release. By merging the DTAG functionality from the SSR3.6 stream onto the current USP10.0 release, the DTAG customer will receive the many new features and robustness items in the current release.

Please refer to the general feature descriptions and product specification documents for USP10.0 for information regarding the functionality provided by the general release of USP10.0.

Please refer to the general feature descriptions and product specification documents for SSR3.6 for information regarding the specific Low Layer Control Point (LLCP) functionality provided by the general release of SSR3.6.

This Feature Description only covers the additional functionality provided in USP10.0 which is different from the existing USP10.0 and SSR3.6.5 functionality. This is basically limited to discussing the new Command Line Interface (CLI) commands and the new JAVA GUI screens required to support the LLCP specific table datafill.

This feature also introduces two new mission card types based on the original Number Portability Controller (NPC) and Number Portability Server (NPS) mission cards. The new mission card types are the Low Layer Controller (LLC) and Low Layer Server (LLS). These new mission cards will use the same hardware as the NPC and NPS cards and contain the same base NPC and NPS software; but the LLC and LLS mission cards will also contain the LLCP services database application.

90.4.1 Platform Provisioning

In SSR3.6 the LLCP functionality resided on the NPC and NPS mission cards running loads which contained the related keywords npc and nps in the load name. In USP10.0 the NPC and NPS mission cards and corresponding loads do not contain the LLCP functionality.

A new set of mission cards and corresponding loads are required which contain the LLCP functionality in USP10.0. These mission cards are the Low Layer Controller (LLC) and Low Layer Server (LLS). The corresponding loads will contain the keywords llc and lls. The hardware for the LLC and LLS mission cards is exactly the same as the related NPC and NPS mission card hardware used in SSR3.6.

The provisioning of the LLC and LLS mission cards is similar to the provisioning of the NPC and NPS mission cards. For LLC mission cards the slot-type field should be set to llc. For LLS mission cards the slot-type field should be set to lls. The corresponding llc or lls load should be chosen in the boot-image field. All other mission card provisioning fields remain similar to the existing NPC and NPS mission cards in SSR3.6.

Figure 1 LLC Platform Node Provisioning

The screenshot shows a web-based GUI for provisioning a platform node. The window title is "platform - node". The top toolbar includes buttons for New, Add, Modify, Delete, Lock, Unlock, Load, Offline, Swact, and Restart. Below the toolbar are tabs for Administration, Search, and Graphical View. The main content area is divided into three sections: Provisioning Data, Operational Data, and Boot Data.

Provisioning Data		Operational Data	
slot-type	llc	operational-state	enabled
slot-name	ent02pp2	administrative-state	locked
slot-description	LLC 2	procedural-state	null
shelf	0	availability-state	null
slot	2	activity-state	inactive
ext-ip-address	47 . 135 . 60 . 90		
ext-subnet-mask	255 . 255 . 252 . 0		
ext-gateway	47 . 135 . 60 . 1		
front-pec	NTST11BB		
tm-pec	NTST09AA		
tm-type	pse		
scsi-front-pec	NTST12BA		
scsi-rear-pec	NTST09AB		

Boot Data	
status-message	
running-image	ss7llc_ppc750_10_00_00_47b
boot-image	llc_vxworks

At the bottom of the window, there is a status bar showing "loading complete" and a navigation bar with buttons for back, forward, and page navigation (1).

90.4.2 LLCP Provisioning

The table in “Mapping SSR3.6 Tables to USP10.0 TablesFigure 2: Mapping SSR3.6 Tables to USP10.0 Tables” lists the SSR3.6 tables specific to LLCP provisioned from the Visual Basic GUI used in SSR3.6 and the corresponding tables in USP10.0 provisioned from the JAVA GUI.

Only these tables will be discussed in this document. All other tables not specific to LLCP were converted during USP8.1.0. Please refer to the current release documentation for information on provisioning non LLCP specific tables from the JAVA GUI.

Figure 2 Mapping SSR3.6 Tables to USP10.0 Tables

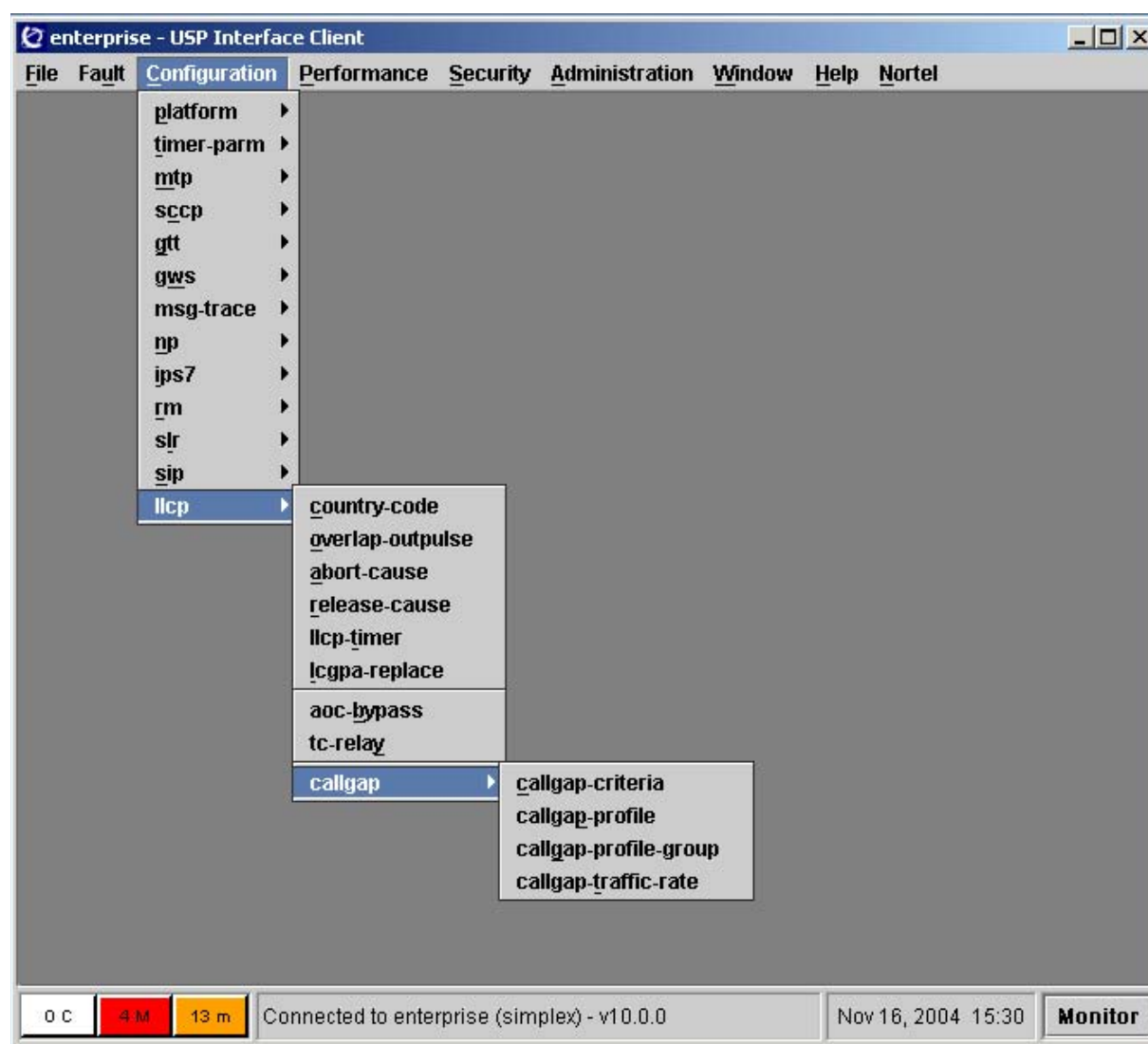
SSR3.6 table	USP10 table
Overlap Outpulsing	llcp overlap-outpulse
Abort Causes	llcp abort-cause
Release Causes	llcp release-cause
ActivityTest	llcp llcp-timer
Call Gap	llcp llcp-timer
TC-Relay	llcp tc-relay
Callgap Criteria	llcp callgap-criteria
Callgap Profile Names	llcp callgap-profile
Callgap Profile Grouping	llcp callgap-profile-group
Callgap Traffic Rate	llcp callgap-traffic-rate
AOC Bypass	llcp aoc-bypass
SCCP General (Disable SCMG message checkbox moved	llcp lcgpa-replace moved to: sccp local-subsystem)
SMI Administration	security user-account
LSS Type (country code moved)	llcp country-code

The following sections outline the individual LLCP table presentations found in USP10.0.

In many tables for LLCP specific provisioning in USP10.0 the field entitled “system-id” is equivalent to the SSR3.6 STP Identity.

90.4.2.1 Main LLCP Menu

Figure 3 LLCP Management Menu



The LLCP tables provisioning screens are accessed from the Configuration main menu as shown in the above figure. Sub menus are used to access specific LLCP functionality such as the various callgap provisioning requirements.

Each of the LLCP provisioning screens are outlined in the following sections.

90.4.2.2 Country Code Table

Figure 4 llcp country-code table



The screenshot shows a web-based administration interface for the 'llcp - country-code' table. The window has a title bar with the text 'llcp - country-code'. Below the title bar is a toolbar with buttons for 'New', 'Add', 'Modify', and 'Delete', along with several icons for navigation and actions. The main content area is divided into two sections: 'Administration' and 'Provisioning Data'. The 'Provisioning Data' section contains two fields: 'prefix-option' with a checked checkbox and 'country-code' with an empty text input field. At the bottom of the window, there is a status bar that says 'loading complete'.

The llcp country-code table allows the user to provision the country-code to be prefixed onto the number which is used for the LLCN database lookup. The fields in this table include

- prefix-option: Checkbox indicating if the country-code should actually be prefixed onto the incoming number for the database lookup.
- country-code: String of 1 to 3 digits (0-9). The country-code to use for the prefix if the prefix-option box is checked.

90.4.2.3 Overlap Outpulse Table

Figure 5 llcp overlap-outpulse table

The screenshot shows a software window titled "llcp - overlap-outpulse". At the top, there is a toolbar with icons for "New", "Add", "Modify", and "Delete". Below the toolbar are two tabs: "Administration" and "Search". The main area of the window is titled "Provisioning Data" and contains two fields: "system-id" with a dropdown menu showing "enterprise (0)" and "interdigit-timeout" with a text box containing the value "10". At the bottom of the window, a status bar displays the text "command completed".

The llcp overlap-outpulse table allows the user to provision an overlap outpulse inter digit collection timeout against a system identity. The overlap outpulse inter digit collection timeout has a pre-set initial value if the user does not provision a new value. The fields in this table include:

- system-id: Text string of the system identity that uses the provided inter digit collection timeout. A combo box is provided which lists all currently provisioned system identities.
- interdigit-timeout: Integer in the range from 1 – 60. The inter digit collection timeout value between 1-60 seconds. (initial value: 10 seconds)

90.4.2.4 Abort Cause Table

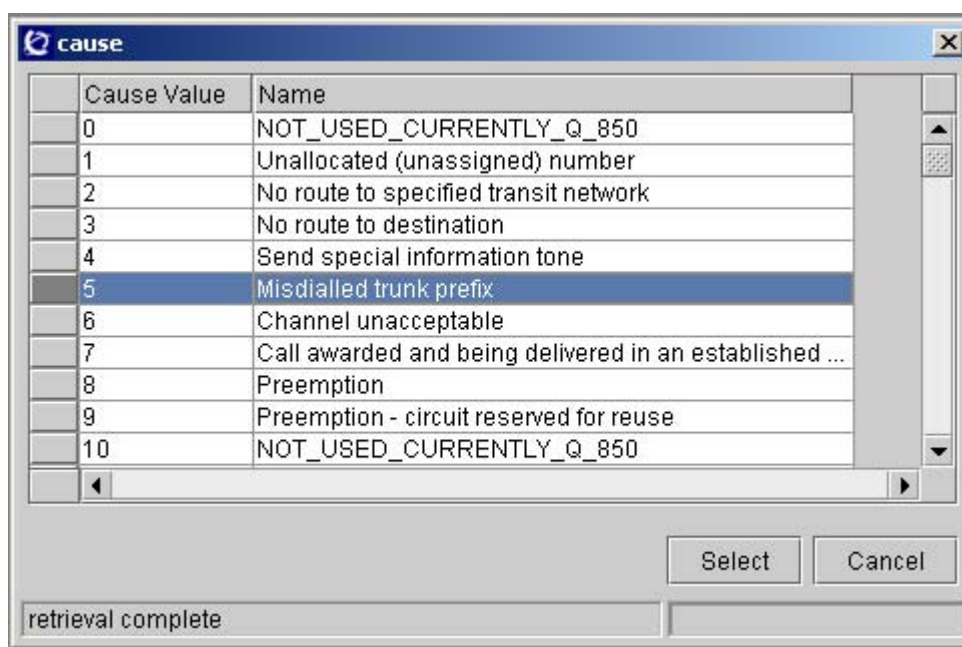
Figure 6 llcp abort-cause table

The llcp abort-cause table allows the user to provision applicable abort cause parameters to be returned to the originator as a result of a specific abort error condition that occurred during a call. Each of the abort-cause reasons has initial pre-set values for the parameters if the user does not provision new settings for the parameters. The fields in this table include:

- abort-cause: Text string for the abort cause reason. A combo box is provided which lists the valid abort cause reasons which can be provisioned of:
 - overlap-outpulsing
 - relayed-idp
 - tinap-operation-decode
 - pabort-received
- coding-standard: Text string for the coding standard to use when formatting the abort-cause response for the chosen abort-cause reason. A combo box is provided which lists the valid coding standards of:
 - itu-t-standardized
 - iso-iec-standard

- national-standard
- specific-standard
(initial value: itu-t-standardized)
- location: Integer value in the range from 0 - 15. The location value to use when formatting the abort-cause response for the chosen abort-cause reason. (initial value: 2)
- cause-value: Integer value in the range from 0 – 127. The cause value to use when formatting an abort-cause response for the chosen abort-cause reason. The selector box (“...”) provides a list of the valid cause values and their associated descriptions from which a cause-value can be selected (See “Figure 7: Cause Value Selection List”). The user can also choose to enter the associated cause-value integer between 0-127 directly in the text entry field. (initial value: 31 => Normal, unspecified)

Figure 7 Cause Value Selection List



This figure depicts an expansion of the cause values which appear as a result of the user choosing the selector box on the abort-cause screen for the cause-value field. All the valid cause-values are listed in the cause pop-up box in numeric order. The user can then select the appropriate cause-value from this selector box. The chosen cause-value integer will then appear in the abort-cause screen in the cause-value field. (Note that clicking on the “Name” heading will change the list to be in alphabetic order.)

90.4.2.5 Release Cause Table

Figure 8 Ilcp release-cause table

The Ilcp release-cause table allows the user to provision an applicable release cause to be returned to the originator as a result of a specific release condition that occurred during a call. Each of the release-cause reasons has initial pre-set values for the parameters if the user does not provision new settings for the parameters. The fields in this table include:

- release-cause: Text string for the release cause reason. A combo box is provided which lists the valid release cause reasons which can be provisioned of:
 - no-routing-instructions-found
 - overlap-outputpulse-interdigit
 - event-report-bcsm-parameter-missing
 - call-gap-congestion
- coding-standard: Text string for the coding standard to use when formatting the release-cause response for the chosen release-cause reason. A combo box is provided which lists the valid coding standards of:
 - itu-t-standardized

- iso-iec-standard
- national-standard
- specific-standard
(initial value: itu-t-standardized)
- location: Integer value in the range from 0 - 15. The location value to use when formatting the release-cause response for the chosen release-cause reason. (initial value: 2)
- cause-value: Integer value in the range from 0 – 127. The cause value to use when formatting a release-cause response for the chosen release-cause reason. The selector box (“...”) provides a list of the valid cause values and their associated descriptions from which a cause-value can be selected (See “Figure 7: Cause Value Selection List”). The user can also choose to enter the associated cause-value integer between 0-127 directly in the text entry field. (initial value: 31 => Normal, unspecified)

90.4.2.6 LLCP Timer Table

Figure 9 llcp llcp-timer table

The llcp llcp-timer table allows the user to provision specific values for the various timers used by the LLC. All these timers have pre-set initial values if the user does not provision a new value. The timers which are provisionable by this table include:

- activity-test-timeout: Integer value in the range from 1 – 70 in minutes
(initial value 40 minutes)

- default-gap-interval: Integer value in the range from 0 – 60000 in milliseconds (initial value 60000 milliseconds)
- default-gap-duration: Integer value in the range from 0 – 2047 in seconds (initial value 2047 seconds)

(Note that the context sensitive help available for each of the fields displays the units (minutes, seconds, milliseconds) for the field.)

90.4.2.7 Lcgpa Replace Table

Figure 10 llcp lcgpa-replace table

The screenshot shows a software interface for configuring the 'llcp - lcgpa-replace' table. The interface includes a title bar, a menu bar with 'New', 'Add', 'Modify', and 'Delete' options, and a toolbar with icons for search, save, and help. Below the menu bar are 'Administration' and 'Search' tabs. The main area is titled 'Provisioning Data' and contains several fields: 'system-id', 'replace-lcgpa', 'routing-indicator', 'gt-indicator', 'translation-type', 'numbering-plan', 'nature-of-address', 'gt-address', 'pointcode', 'ssn', 'pointcode-included', and 'ssn-included'. The 'gt-address' field is highlighted. At the bottom, there is a status bar showing 'loading complete' and a page number '0'.

The llcp lcgpa-replace table allows the user the option of specifying the contents of the calling party address portion of the SCCP portion of all

messages sent from the LLCP for the chosen system-id. The fields in this table are:

- system-id: Text string of the system identity that uses the provided cgpa replacement entry. A combo box is provided which lists all currently provisioned system identities.
- replace-lcgpa: Text string which indicates the type of calling party address replacement to perform. A combo box is provided which lists the valid replace-lcgpa types of:
 - do-not-replace -> No other fields apply to this replace-lcgpa entry.
 - replace-all -> Only the routing indicator, gt-address (other fields may be enabled depending on the gt-address chosen), pointcode-included and ssn-included fields apply to this replace-lcgpa entry.
 - replace-dpc-ssn -> Only the routing-indicator and pointcode-included fields apply to this replace-lcgpa entry.
- routing-indicator: Text string. If this field is enabled, depending on the replace-lcgpa, it specifies the routing type to use in the calling party address. A combo box is provided which lists the valid routing-indicator types of:
 - route-pc: route based on pointcode and SSN in the calling party address
 - route-gt: route based on the GT information in the calling party address
- gt-indicator: Integer in the range from 1 - 4. If this field is enabled based on the replace-lcgpa, it specifies the gt-indicator to use in the calling party address. The fields translation-type, nature-of-address, numbering-plan and gt-address are enabled depending on the gt-indicator chosen. A combo box is provided which lists the valid gt-indicator types of:
 - gta+noa – enables nature-of-address and gt-address fields
 - gta+tt – enables translation-type and gt-address fields
 - gta+tt+np – enables translation-type, numbering-plan and gt-address fields
 - gta+tt+np+noa – enables translation-type, numbering-plan, nature-of-address and gt-address fields.
- translation-type: Integer in the range from 0 – 255. If this field is enabled based on the replace-lcgpa and gt-indicator fields, it specifies the translation type to use in the calling party address.

-
- numbering-plan: Integer in the range from 0 – 6 with valid entries being 1. If this field is enabled based on the replace-lcgpa and gt-indicator fields, it specifies the numbering plan to use in the calling party address. A combo box is provided which lists the valid numbering-plan values of:
 - e163-e164
 - e212
 - e214
 - nature-of-address: Integer in the range from 0 – 127. If this field is enabled based on the replace-lcgpa and gt-indicator fields, it specifies the nature of address to use in the calling party address.
 - gt-address: This field is a digit string of 3-32 digits in length containing the digits 0-9 and hex digits a-f (or A-F). If this field is enabled based on the replace-lcgpa and gt-indicator fields, it specifies the gt-address digits to use in the calling party address.
 - pointcode: This field is not provisionable by the user. It provides the pointcode of the selected system-id for information purposes only when the replace-lcgpa chosen is replace-all or replace-dpc-ssn.
 - ssn: This field is not provisionable by the user. It provides the ssn of the LLCP local subsystem for the chosen system-id for information purposes only when the replace-lcgpa chosen is replace-all or replace-dpc-ssn.
 - pointcode-included: Checkbox. If this field is enabled based on the replace-lcgpa it indicates if the current pointcode of the selected system-id should be included in the calling party address.
 - ssn-included: Checkbox. If this field is enabled based on the replace-lcgpa, it indicates if the current ssn of the LLCP local subsystem for the selected system-id should be included in the calling party address.

90.4.2.8 AOC Bypass Table

Figure 11 llcp aoc-bypass table

The screenshot shows a web-based interface for managing the 'llcp - aoc-bypass' table. The window has a title bar with the text 'llcp - aoc-bypass'. Below the title bar is a menu bar with 'New', 'Add', 'Modify', and 'Delete' options. To the right of the menu bar is a toolbar with icons for refresh, save, and help. The main content area is divided into two tabs: 'Administration' and 'Search'. The 'Administration' tab is currently selected, displaying a 'Provisioning Data' section. This section contains a single input field labeled 'inap-cgpa'. The status bar at the bottom of the window displays the text 'loading complete'.

The llcp aoc-bypass table allows the user to provision up to 50 calling party numbers that are exempt from the Advice of Charge (AOC) functionality. The fields in this table are:

- inap-cgpa: The calling party number to exempt from the Advice of Charge functionality. This field is a digit string of 1-23 digits in length containing the digits 0-9 and hex digits a-e (or A-E)

90.4.2.9 TC Relay Table

Figure 12 llcp tc-relay table

The screenshot shows a window titled "llcp - tc-relay". At the top, there is a toolbar with icons for "New" (document), "Add" (green plus), "Modify" (orange plus), and "Delete" (red X). Below the toolbar are two tabs: "Administration" and "Search". The main area is titled "Provisioning Data" and contains two fields: "service-key" with a text input box, and "tc-type" with a dropdown menu. At the bottom of the window, a status bar displays the text "loading complete".

The llcp tc-relay table associates a service key (which is retrieved from the incoming TCAP message) to either the tc-transfer routing procedure or tc-relay routing procedure. This table supports up to 50 service key entries. Entries not found in this table default to the tc-transfer routing procedure. The fields in this table are:

- service-key: Integer value in the range from 0 – 32767. The service-key that the routing procedure (tc-type) will apply to.
- tc-type: Text string to indicate to either use tc-relay routing for this service key, or tc-transfer routing for this service key. A combo box is provided which lists the valid tc-types of:
 - tc-transfer
 - tc-relay

90.4.2.10 CallGap Criteria Table

Figure 13 llcp callgap-criteria table

The screenshot shows a web-based administration interface for the 'llcp - callgap-criteria' table. The window has a title bar with the text 'llcp - callgap-criteria'. Below the title bar is a toolbar with icons for 'New' (document), 'Add' (plus), 'Modify' (pencil), and 'Delete' (X). To the right of the toolbar are icons for refresh, save, and help. Below the toolbar are two tabs: 'Administration' and 'Search'. The 'Administration' tab is active. The main content area is titled 'Provisioning Data' and contains three input fields: 'criteria-name', 'traffic-contribution-factor', and 'gap-duration'. The 'criteria-name' field is a text box, while the other two are numeric input boxes. At the bottom of the window, there is a status bar that says 'loading complete'.

The llcp callgap-criteria table allows the user to provision a load contribution factor and its associated gap-duration value against a user defined criteria name. The fields in the callgap-criteria table are:

- criteria-name: Text string from 1 to 7 characters to identify this entry in the table
- traffic-contribution-factor: Integer value in the range from 1 – 1000. This is the interval period factor used in conjunction with the BHCA value datafilled to calculate the actual gap interval which is incorporated in the CallGap message the LLCP sends to the SSP.
- gap-duration: Integer value in the range from 0 – 2047 seconds. This is the duration time-out value the SSP needs to apply in support of the CallGap procedure which is incorporated in the CallGap message the LLCP sends to the SSP.

90.4.2.11 CallGap Profile Table

Figure 14 llcp callgap-profile table

The screenshot shows a web-based interface for managing the 'llcp - callgap-profile' table. The interface includes a title bar with the text 'llcp - callgap-profile'. Below the title bar is a toolbar with buttons for 'New', 'Add', 'Modify', and 'Delete', each accompanied by a small icon. To the right of these buttons are several utility icons, including a refresh button, a print button, and a help button. Below the toolbar is a navigation bar with two tabs: 'Administration' and 'Search'. The main content area is titled 'Provisioning Data' and contains a single text input field labeled 'profile-name'. At the bottom of the interface, there is a status bar that displays the text 'loading complete'.

The llcp callgap-profile allows provisioning of a set of up to 150 profile names which can then be used to build up call gap profile groups which are associated with a single profile name. The fields in the callgap-profile table are:

- profile-name: Text string from 1 to 7 characters to identify this entry in the table

90.4.2.12 CallGap Profile Group Table

Figure 15 llcp callgap-profile-group table

The llcp callgap-profile-group table allows associating a callgap criteria specified by the criteria-name with an SSP pointcode under a given profile-name. Up to 2000 callgap-profile-groups can be created. The fields in this table are:

- **profile-name:** Text string from 1 to 7 characters to identify this entry in the table. The profile-name must match a profile-name provisioned in the callgap-profile table. A combo box is provided which lists the previously provisioned profile-names.
- **system-id:** Text string of the system identity that the remote point code is associated with. A combo box is provided which lists all currently provisioned system identities.
- **remote-pointcode:** Text string of the remote pointcode that this callgap criteria will apply to. The selector box (“...”) provides a list of the currently provisioned remote pointcodes for the chosen remote system-id.

- criteria-name: Text string from 1 to 7 characters to identify the callgap criteria to be applied to the chosen remote-pointcode. The selector box (“...”) provides a list of the currently provisioned criteria-names.

90.4.2.13 CallGap Traffic Rate Table

Figure 16 llcp callgap-traffic-rate table

The llcp callgap-traffic-rate table allows the user to associate a service key, possibly in conjunction with a calling party number, to a traffic rate (KBHCA) and a CallGap profile name. Up to 3000 callgap-traffic-rate entries can be created. The fields in this table are:

- traffic-rate-type: Text string to indicate the type of traffic rate entry this will be. This field once set is not modifiable. A Combo box is provided which lists the valid traffic-rate-type entries of:
 - office-wide -> Only the kbhca field applies to this type of traffic rate entry. Only one office-wide entry is permitted.
 - service-key -> Only the service-key, kbhca and profile name fields apply to this type of traffic rate entry.
 - service-key-in-number -> All fields apply to this type of traffic rate entry
- service-key: Integer in the range from 0 – 32767 to identify the service-key this entry applies to which is to be matched to the service-key in the received message.

- **in-number:** The calling party number associated with the service-key which is to be matched to the calling party number in the received message. This field is a digit string of 1-23 digits in length containing the digits 0-9 and hex digits a-e (or A-E)
- **kbhca:** Integer in the range from 1 - 10000. The kbhca value to be applied when a matching entry is encountered on the message path.
- **profile-name:** Text string from 1 to 7 characters to identify this entry in the table. The profile-name must match a profile-name provisioned in the callgap-profile table. A combo box is provided which lists the previously provisioned profile-names.

90.4.2.14 Local Subsystem Table

Figure 17 sccp local-subsystem table

The screenshot shows a configuration window titled "sccp - local-subsystem". It features a toolbar with icons for "New", "Add", "Modify", "Delete", "Activate", and "Deactivate". Below the toolbar are two tabs: "Administration" and "Search". The main content area is split into two sections: "Provisioning Data" and "Operational Data".

Provisioning Data:

- system-id: enterprise (0)
- lss-class: LLCP
- lss-application: LLCP
- ssn: 10
- required-instances: 1
- app-cap-code: (empty)
- replicated-pointcode: 1-1-3
- scmg-disabled-option: ☒
- crp-option: ☒
- sar-option: ☒

Operational Data:

- avail-status: prohibited
- admin-state: deactivated

At the bottom of the window, there is a status bar that says "loading complete" and a pagination control showing "1 of 1".

The sccp local-subsystem table is an existing table used to provision the local subsystems. This table has the following fields added to support the LLCP local subsystem class:

- **scmg-disabled-option:** Checkbox. This option allows the user to indicate if scmg management messages of type subsystem allowed (ssa) and subsystem prohibited (ssp) should be sent for this local subsystem and on this system-id when the subsystem changes state. This option is applicable to the lss-class type of LLC. For other lss-class types this option is always unchecked and is not displayed.
- **crp-option:** Checkbox. The Circular Routing Prevention option indicates if circular routing prevention should be performed on the outgoing messages. This option is applicable to the lss-class type of LLC. For other lss-class types this option is always unchecked and is not displayed.
- **sar-option:** Checkbox. The Segmentation and Reassembly option indicates if segmentation and reassembly can be used on the outgoing messages. This option is applicable to the lss-class type of LLC. For other lss-class types this option is always unchecked, and is not displayed.

90.5 Hardware Information

The new hardware supported in USP9.0.0 under feature 025860: New Hardware Support (PP5) will be available in this release except for support of the LLC services database based on the LLC and LLS mission card types on the PP5 3G cards.

90.6 GUI/CLI Information

GUI/CLI changes for added functionality to USP10.0 are required to support the LLC specific datafill merged from SSR3.6, and also to support the new mission card types LLC and LLS. Please see previous document sections for full details of the GUI screens which are created/impacted by this feature.

90.6.1 CLI changes

New CLI commands created to support the LLC specific database merged from SSR3.6 include:

- **llcp country-code**
- **llcp overlap-outpulse**
- **llcp abort-cause**
- **llcp release-cause**
- **llcp llcp-timer**
- **llcp aoc-bypass**
- **llcp tc-relay**
- **llcp callgap-criteria**
- **llcp callgap-profile**

- llcp callgap-traffic-rate
- llcp lcgpa-replace

CLI commands changed to support the LLCP subsystem type include:

- platform node add: Addition of LLC and LLS as valid slot-type entries.
- sccp local-subsystem add: Addition of LLCP as a valid lss-class entry, and additional optional parameters.
- sccp local-subsystem mod: Addition of LLCP as a valid lss-class entry, and additional optional parameters.
- sccp shared-lss-instance add: Addition of LLCP as a valid lss-class entry.

90.6.2 GUI

Please see previous document sections for full details of the GUI screens which are created/impacted by this feature.

90.7 OMs

No new OMs are added by this feature, however any existing OMS in SSR3.6.5 which are not in USP10.0 are propagated.

90.8 Logs and Alarms

No new logs or alarms are added by this feature, however any existing logs and alarms in SSR3.6.5 which are not in USP10.0 are propagated.

90.9 Interactions

No new interactions are introduced by this feature.

90.10 Restrictions and Limitations

Support for the LLCP services database based on the LLC and LLS mission card types on the PP5 3G cards is not included in this feature.

There is no in-service software upgrade provided from SSR3.6.5 to USP10.0.0. An out-of-service upgrade must be performed, and the provisioning data re-entered once USP10.0.0 is active.

90.11 Compliance Impact

There are no changes to the current compliancy documents.

90.12 Definitions and Terms

CLI – Command Line Interface

GUI – Graphical User Interface

LLC – Low Layer Controller

LLCP – Low Layer Control Point

LLS – Low Lay Server

NPC – Number Portability Controller

NPS – Number Portability Server

OM – Operational Measurement

PP5 – Processor Platform 5

91: A00007370 Functional description (FN)

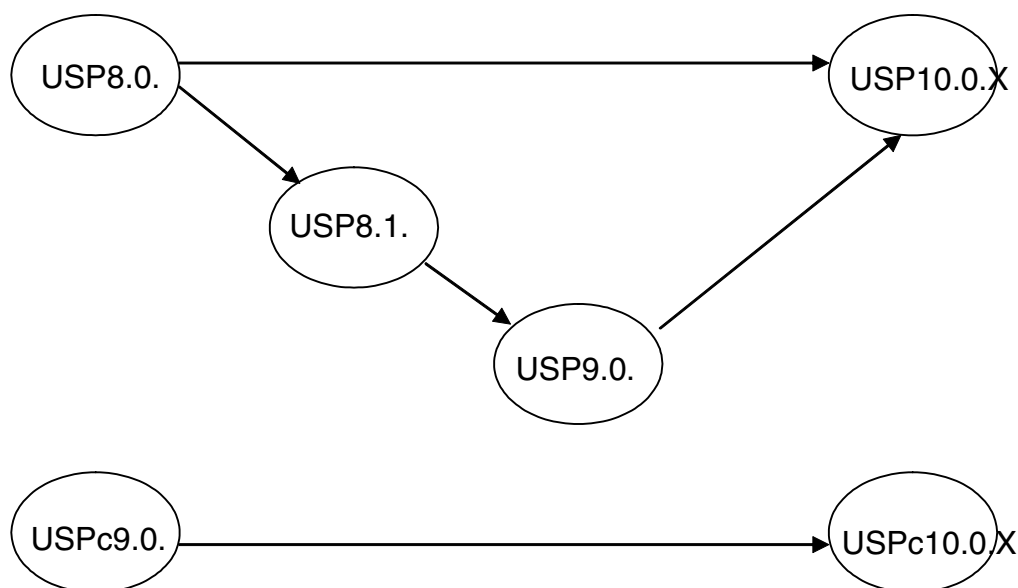
91.1 Feature name:

USP8.0.x/9.0.x to USP10.0.x Direct In-Service Upgrade and USPc9.0.x to USPc10.0.x In-Service Upgrade

91.2 Description

The USP10 Software Upgrade supports direct in-service software upgrade from USP9.0/SN07 to USP10.0/SN08 and USP8.0/SN06 to USP10.0/SN08. Currently a double USP software upgrade is required when a customer skips a CS2K release. This feature is required to align with the Succession policy of allowing a customer to skip a Succession release.

The USPc10 Software Upgrade supports in-service software upgrade from USP9.0/SN07 to USP10.0/SN08. There is no USPc8 release so there is no upgrade.



The USP10 and USPc10 Software Upgrade maintain connectivity of the USP to the Application Servers. This connectivity may be simplex.

The USP10 and USPc10 Software Upgrade maintain connectivity of the USP to the SS7 network. This connectivity may be simplex.

91.3 Hardware Requirements or Dependencies

There are no hardware requirements for USP10 software upgrade. There may be a memory recovery effort required to support the USPc10 software upgrade with the current hardware.

91.4 Software Requirements or Dependencies

All USP10.0 features are evaluated for Software Upgrade requirements. Each USP10.0 feature includes in their feature changes, support for the USP8.0.x and USP9.0.x upgrade paths, where x is the latest point release for USP8 and USP9 respectively.

All USPc10.0 features are evaluated for Software Upgrade requirements. Each USPc10 feature includes in their feature changes, support for the USP9.0.x upgrade path, where x is the latest point release for USP9.

91.5 Limitations and restrictions

USP10 does not support a direct upgrade from USP8.1.x. Customers with USP8.1.x will upgrade to USP9.0.x and then upgrade to USP10.

USPc10 does not support a direct upgrade from USPc7.0.x. Customers with USPc7.0.x will upgrade to USPc9.0.x and then upgrade to USPc10.

The USP10/USPc10 Software Upgrade supports Solution upgrade scenario, where the USP is upgraded before the Application Server. In a CS2K environment the USP is upgraded before the Core. This implies that USP8.0 must inter-work with SN04 and SN05 Cores.

The USP10/USPc10 Software Upgrade supports Solution upgrade scenario, where the USP is upgraded after the Application Server. In a CS2K environment USP is upgraded after the GWCs. This implies that USP8.0 need not inter-work with SN04 or SN05 GWCs, but SN06 GWCs must inter-work with USP6.0 and USP7.0/USPc7.0. SN08 GWCs must inter-work with USP8.0 and USP9.0/USPc9.0. This is not a requirement for USP10/USPc10.

91.6 Interactions

See the Functional Description.

91.7 Glossary

Term	Description
USP	Universal Signalling Point
CS2K	Communication Server 2000
GWC	Gateway Controller

92: A00007388 Functional description (FN)

92.1 Feature name

IEMS Performance Phase II

92.2 Triggering Support

To achieve minimum time for OM collection attributes, execution of data collection, report generation and transferring the same to OSS can be combined together using triggering support of Performance interface. An easier and simple GUI will be provided in order to configure collection, reporting and transfer job details in one shot with triggering support. After the completion of data collection, report generation will be triggered while data is being written to the database in order that the report can be generated without reading data from the database. Once report generation has been completed, a transfer job will be triggered so that all the reports are transferred to OSS.

92.2.1 Triggering data collection

CollectionJob should be triggered by a configured event of the device, if the device supports the same, or as the usual way based on the granularity period of the Collection Job. Say, for a particular device MG9000, if an event of category Performance has been added from CORBA notification, then CollectionJob should be triggered for that device. If the device doesn't support these kind of notifications, then the Collection Job would be executed based on the granularity period.

92.2.2 Triggering report generation

Report jobs can be configured to run as scheduled mode based on the granularity period, as well as by triggered mode by the configured Collection job. Mode of executing the reports, either scheduled mode or triggered mode, would be captured in Report Job itself by using the *executionMode* property. In the case of triggered mode, name of the Collection job which would trigger the report would be identified by using *colJobList* parameter. It should be noted that only one Collection Job would be allowed to associate with the Report Job for triggering the same.

For Report jobs created with triggered mode, *executionMode* property will be set to 'triggered' and 'colJobList' property will be set to the name of the Collection Job, on whose completion this report should be triggered. For Report jobs created with scheduled mode, *executionMode* property will be set to 'scheduled' and *colJobList* should be set to 'none'.

In the scheduled mode, reports are generated based on the granularity period. For triggered mode, after the Collection job's completion, a report configured with trigger mode for this Collection Job will be triggered. Report generation will be triggered while data is being written to the database in order that the

report can be generated without reading data from databases. This will reduce the time required to read the data from database for report generation.

92.2.3 Triggering report transfer to OSS

Transfer jobs can be configured to run as scheduled mode based on the granularity period, as well as by triggered mode by the Report job. Mode of executing transfer jobs, either scheduled mode or triggered mode, should be captured in Transfer Job itself by using the *executionMode* property. In the case of triggered mode, name of the Report job which should trigger the transfer job would be identified by using *reportJobList* parameter. It should be noted that only one Report Job would be allowed to be associated with Transfer Job for triggering the same.

For Transfer jobs created with triggered mode, *executionMode* property will be set to 'triggered' and 'reportJobList' property will be set to the name of the Report job, on whose completion this Transfer job should be triggered. For Transfer jobs created with scheduled mode, *executionMode* property will be set to 'scheduled' and *reportJobList* should be set to 'none'.

In the scheduled mode, transfer has been done based on the granularity period. For triggered mode, after the Transfer job's completion, transfer jobs configured with trigger mode for this Report job will be triggered.

92.3 Performance interface support for new devices

S.No	Device Type	Supported Performance Interfaces
1	GWC	SNMP
2	UAS	SNMP
3	SAM 21 SC	SNMP
4	SSPFS	SNMP
5	MG9000	CSV
6	USP	CSV

92.4 Logging support

- Log of the Unauthorized Access Attempt: Any unauthorized configuration access attempts of measurement collection jobs should be logged in security log.
- Log of the Unauthorized Access Attempt: Any unauthorized configuration access attempts of measurement transfer jobs should be logged in security log.

- Log of the Unauthorized Access Attempt: Any unauthorized configuration access attempts of measurement report jobs should be logged in security log.

92.5 Enhanced GUI support

- Easier and simple GUI for configuring Collection job, Report job and Transfer job in single shot with built in triggering capability. (low priority)
- Current Measurement Collection job display should also include the status of the current/previous collection activity and the scheduled time of the next collection (if applicable)
- The display of Current Measurement Transfer job should also include the status of the current/previous transfer activity and the scheduled time of the next transfer (if applicable).
- The display of current Measurement Report jobs should also include the status of the current/previous report job activity and the scheduled time of the next report generation (if applicable).

92.6 Intuitive Reports

Presentation of Analysis Result: IEMS shall provide the mechanism through which the result of performance analysis can be shown as intuitive formats (e.g. graphical performance report, report/table forms etc).

92.7 Suspending Collection Jobs

Support would be given such that Collection job would be suspended, if topology component corresponds to this Collection job gets unmanaged.

92.8 Multiple folder support for CSV devices (MAS & MCS)

"Currently when we configure the MCS and MAS devices in our topology we are prompted for the device's performance interface attributes. These attributes include collection directory, file name, transfer type (sftp, ftp or push), userid, pw. These attributes are used for all collection jobs defined against these managed object types. The current issue is that we are unable to define multiple collection jobs for these devices that use unique file collection criteria (file filters). In the case of MCS, it is a rather complex device with ~ 25 sub directories where data could be collected from. While customers may want to configure multiple collection jobs in the IEMS for these devices to collect portions of the data with different collection intervals it can not be done with our current design."

To overcome the above design issue, the IEMS Performance Metrics Collection Job wizard should be able to get the Directory Name and File Name for the MCS and MAS devices (CSV collection devices).

Java Application Window

IEMS Performance Metrics CollectionJob Details

Name: mcsJob

Status: Enabled

Start Time: Aug 19 2004 05 : 42 : 13 : PM

☐ StopTime: Aug 20 2004 09 : 46 : 44 : AM

Device Type: MAS

Excluded Device List:

- ☐ 192.168.112.108
- ☐ 192.168.112.217

Granularity Period: 5 min

Offset: 0 (mins.)

Template Name:

OK Close Help

In the above image, the red highlighted portion will be changed based upon the selected "Device Type". If the selected device type is SNMP-collection-based device, then the red highlighted portion should be changed to ask associated Template Name. If the selected device type is CSV-collection-based device

(MAS or MCS), then the red highlighted portion should be changed to ask the Directory Name and the File Name. By default IEMS will take the directory name and file name provided in the collection job. If there is no configuration (directory name, file name) made in the collection job, the IEMS will automatically get the directory name and file name from the topology module which configured during the Add device operation.

93: A00007393 Functional description (FN)

93.1 Feature name

Session Policy Controller

93.2 Background

In SN07, the CS2000 delivered admission control functionality by means of virtual call admission control (VCAC) on the Gateway Controller (GWC) component of the CS2000 architecture. The limitations of this as policy control platform along with the need to support CS2000 and potentially other application servers together behind the same access links drove the requirements to move VCAC onto a common platform which could serve multiple applications.

93.3 Overview

The SPC product functionality is implemented by the following feature activities:

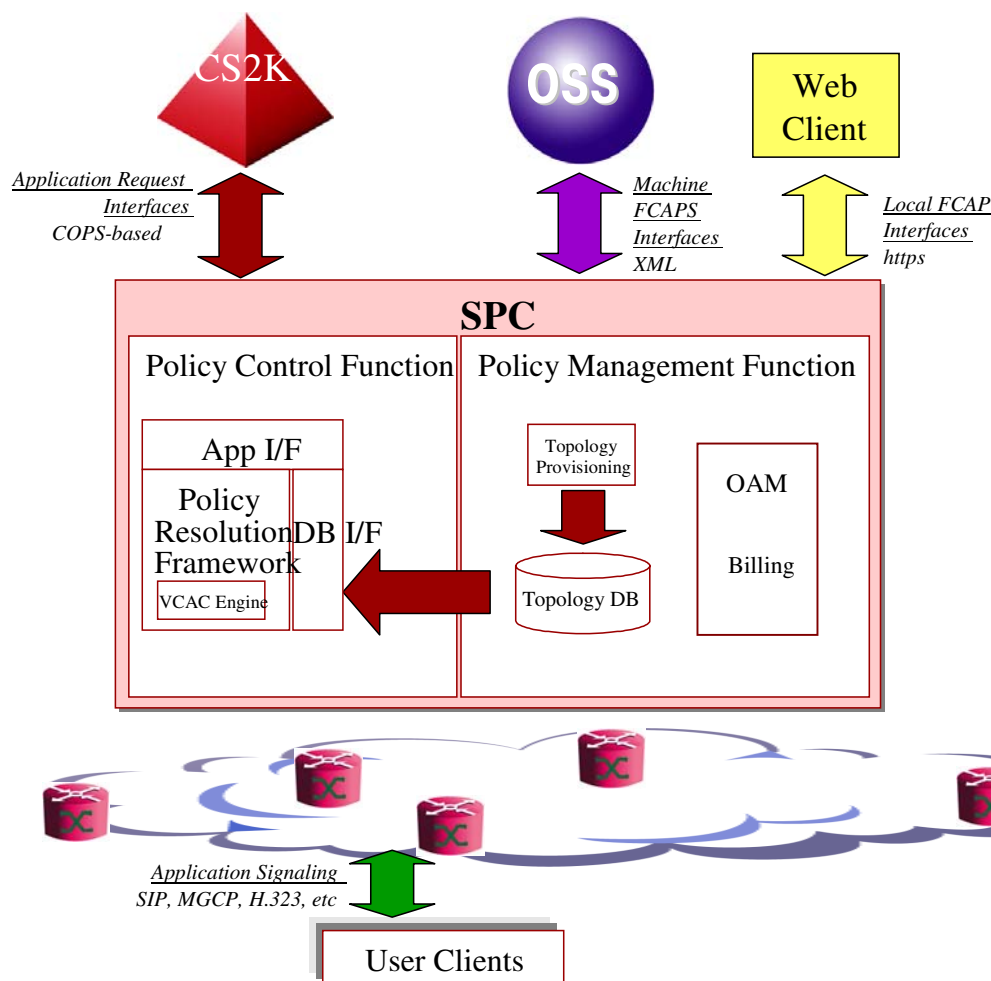
- A00007389 SPC Policy Control Framework
- A00007390 SPC Protocol Handler
- A00007391 SPC Provisioning Framework
- A00007392 SPC OAM
- A00007393 SPC Base
- A00007398 SPC Topology Manager

This FN document serves as the “umbrella” FN for the all above activities.

93.4 Feature Description

The Session Policy Controller monitors, controls, and enforces use of network resources. The SPC main functions are policy control and management. The SPC software application is delivered on the SAM-XTS hardware platform and the product is developed and based on the NGSS (Nortel General-purpose Session Server) software platform. The general model describing the Release 1 Session Policy Controller application functional components and interfaces is shown below.

Figure 1- Session Policy Controller (SPC) functional components



93.4.1 Policy Control Framework

The SPC has a Policy Control Framework (PCF) that is responsible for processing requests for resources and applying the necessary policy enforcement mechanisms to the requests. All relevant network topology information needed is retrieved from a Topology Database.

93.4.1.1 Policy Definition

In SN08 there will only one policy supported – VCAC Bandwidth Policy. This default policy exists to carry out network resource reservation function.

93.4.1.2 Policy Enforcement Action

The SPC applies the default policy to all requests for network resources to enforce call admission control. Resource requests could be in the form of a flow specification or an amount of bandwidth requested. VCAC Bandwidth

usage calculations are used to monitor the bandwidth usage status, and ensure there are enough resources for a new call requests.

When an Application Server agrees to provide service to a client, it sends a request to the SPC that contains:

- Identity and location of the client to whom service is to be provided
- FlowSpec specifying traffic requirement for the session

Network Reservation using VCAC

The Network Reservation requests are processed using Virtual Call Admission Control (VCAC) functionality. The initial release of the Session Policy Controller supports a VCAC capability that is substantially equivalent to that introduced on the CS2000 in SN07. One of the main advantages of moving the VCAC functionality off-board to the SPC is that, in SN07, GWCs cannot share count information among themselves. In SN08, resource modeling is performed on the SPC and since the SPC would have a full view of the topology, VCAC could be performed on application server-wide basis instead of just within one particular GWC's scope of control.

VCAC is a policy based Call Admission Control model used to provide Network Resource Based Admission Control by setting service class bandwidth limits based on the bandwidth available on the subscriber's access link. VCAC

VCAC Bandwidth Calculations

The VCAC function can handle the tracking of bandwidth usage in terms of an Explicit or Implicit calculation of encapsulation overhead and link bandwidth. The mechanism is dependent on the definition of a Network Zone and associated Network link. The SPC topology model allows the customer to either describe a Network Link in terms of established Predefined protocol layers or by a custom link layer type.

Implicit calculation

The customer can choose to describe a network link in terms of the protocol layers (e.g. PPP/Ethernet/ATM) which comprise the link. These link layer types are predefined for use by the customer and are accessible via the SPC provisioning interface. A protocol layer is specified as having either a variable (e.g. Ethernet) or fixed (e.g. ATM) protocol data unit (PDU). In each case there is an encapsulation overhead, and in the fixed PDU case there is also the unit size & overhead. The SPC implicitly derives the value of the link overhead based on the definition of the predefined link layer type because the encapsulation overhead is associated with the protocol. For example, in the case of a fixed length PDU, the customer would also specify the unit size (e.g. ATM cellsize=53) and unit overhead amount (e.g. ATM header of 5 bytes).

Explicit calculation

If the customer prefers a simpler approach, they can choose not to model the specific protocol layers of the network link, but instead create a custom link layer and provision the bandwidth available on the link with a single value for the overhead. In this calculation no assumption is made about multiple link layers and the associated encapsulation overhead of each. It is expected that the craftsperson explicitly accounts for any overhead required for the link layer. In other words, the customer creates a "fudge factor" to account for overhead when they define the bandwidth available on the link. The overall bandwidth is explicitly calculated based on the bandwidth values and overhead provisioned by the customer.

Networks Service Class (NSC)

Nortel Networks has an established set of subscriber service classes that can be used to map traffic categories, DSCP, and other QoS/CoS parameter designations. NNSC names can be used to define individual traffic flow policies based on traffic conditions independently of the underlying bearer link protocol or network element resource. This could provide scalability for large networks that interoperate with various policy standards, including: DiffServ, IEEE 802.1p, COPS-PR, and LDAP.

In SN08, only voice calls are supported from the CS2000. All voice calls will be tagged as Premium.

Table 1 - Sample NNSC Mappings

Traffic Category	Nortel Networks Service Class	Default DSCPs	ATM		Frame Relay		Ethernet 802.1p	MPLS E-LSP EXP	Scheduler	AQM
			CoS	CLP	CoS	DE				
Network Control	Critical	CS7	rt-VBR	0	3	0	7	111	PQ	None
	Network	CS6	rt-VBR	0	3	0	7	111	WFQ	None
Interactive	Premium	EF, CS5	rt-VBR	0	3	0	6	110	PQ	None
	Platinum	AF41, AF42, AF43, CS4	rt-VBR	0 1	3	0 1	5	101	WFQ	WRED
Responsive	Gold	AF31, AF32, AF33, CS3	nrt-VBR	0 1	2	0 1	4	100	WFQ	WRED
	Silver	AF21, AF22, AF23, CS2	nrt-VBR	0 1	1	0 1	3	011	WFQ	WRED
Timely	Bronze	AF11, AF12, AF13, CS1	nrt-VBR	0 1	1	0 1	2	010	WFQ	WRED
	Standard	DF	UBR	1	0	1	0	000	WFQ	WRED

93.4.2 Protocol Handler

The Protocol Handler provides a standard application interface specification to the Policy Control Framework. The Protocol Handler parses request messages that are delivered by the protocol stack and converts those requests into generic request messages which are passed to the Policy Control Framework. The protocol handler also receives generic responses from PCF, encodes the response in the required format for the specified protocol, and then sends this response back to application server.

Various protocols could be used between the application server and the SPC, such as COPS, Diameter, SOAP, etc... In release 1, an extension of the COPS based DQos protocol is the only protocol supported over the signaling interface between the CS2000's GWC and the SPC.

93.4.3 Provisioning Framework

The Session Policy Controller functions as its own element manager. This means that provisioning and maintenance activities for a Session Policy Controller takes place on the Session Policy Controller itself. The SPC provision framework provides a web based interface to configure SPC system parameters, provision network topology, perform application maintenance, and display SPC specific OMs, alarms, and logs. The SPC GUI has a similar look and feel some other Nortel Networks products. It shares a common 'look and feel' with other NGSS based applications such as SIP-GW. An OSS interface is also provided.

The SPC uses a database for persistent data storage of topology data and run-time configuration parameters. There are many components in SPC that access database to retrieve, insert, or update data. For example, PCF may need to retrieve topology from the database to construct the topology in the memory and Topology data needs to be input from the OSS into the database. Topology data and system tunable parameters can be changed by system operator or externally while the SPC is running and the internal components of the SPC must be notified of the change. An internal change notification mechanism is used to notify the internal components of the SPC what information has been changed.

The OSS and web browser are the only interfaces to manage provisioned data.

93.4.4 OAM Function

The SPC provides functionality for application maintenance such as Logs, Alarms, and OMs. The OMs, Logs, and Alarm information are recorded on the internal hard disk. These subsystems provide an interface to export the data off-board to IEMS. The Web Server can also retrieve active alarms and logs so that they can be displayed on the Web GUI.

Access to Application Maintenance commands is available from Web GUI.

The OM format is presented in the Performance Management section of this document.

The Alarm format is presented in the Fault Management section of this document.

The Log format is presented in the Fault Management section of this document.

93.4.5 Topology Management

The Session Policy Controller provides a topology database, topology configuration tools and schemas to support the VCAC capability. These topology configuration tools allow the craftsperson to manage topology data such as network zones and network links. There are topology provisioning interfaces for the web GUI and OSS.

93.5 Hardware Dependencies

93.5.1 SAM-XTS

The hardware platform is the SAM-XTS (Service Application Module – eXtremely Thin Server). It is the Intel Langley Prestonia OEM'd by Hewlett Packard as the HP-CC3310. The HP-CC3310 provides processing, memory, and disk capacity for Session Policy Controller application.

The HP cc3310 carrier-grade server is a Network Equipment Building Standards (NEBs) Level 3-certified platform in a 2U form factor. The server is designed for telecommunications central offices or data centers and deployed in a rack-mounted, space-saving configuration. Based on IA-32 processors and tuned for the Linux operating system, the HP cc3310 carrier-grade server is modular and based on industry standards.

The SAM-XTS is a platform for the delivery of multiple applications. Other applications that would reside on the SAM-XTS are the SIP Gateway application or STORM application.

93.5.2 SAMF Frame

The SAM-XTS server is mounted on the SAMF (NTRX51HA) frame.

93.6 Software Dependencies

93.6.1 Nortel Networks Software Dependencies

93.6.1.1 NGSS

The Session Policy Controller product is developed on the NGSS (Nortel General-purpose Session Server) software platform. The NGSS software platform has a layered architecture, which consists of an application layer, a shared layer, and a Nortel Carrier-Grade Linux base layer. The Session Policy Controller software resides in the NGSS application layer, and the Session

Policy Controller uses the NGSS Application Maintenance Module to interface with the NGSS shared and base layer functions. In SN08, the NGSS platform does not support multiple applications to co-run together. Only one application can be enabled to operate on the platform.

93.6.2 Non Nortel Networks Software Dependencies

The SPC application relies on several 3rd party software libraries and utilities.

93.6.2.1 ACE

The Adaptive Communication Environment (ACE) is a freely available, open-source object-oriented tool framework that implements many core patterns for concurrent communication software. It is free to use and distribute without compromising Nortel IPR. The license can be found at <http://www.cs.wustl.edu/~schmidt/ACE-copying.html>

93.6.2.2 Xerces

Xerces is one of the Apache Foundation projects. Xerces is a library that provides XML parsing and generation. Fully-validating parsers are available for both Java and C++, implementing the W3C XML and DOM (Level 1 and 2) standards, as well as the de facto SAX (version 2) standard. The parsers are highly modular and configurable. Initial support for XML Schema is also provided. It is free to use and distribute without compromising Nortel IPR. The license can be found at <http://apache.org/licenses/>

93.6.2.3 Struts

Struts is one of the Apache Foundation projects. Struts is an open source framework for building Java web applications. The core of the Struts framework is a flexible control layer based on standard technologies like Java Servlets, JavaBeans, ResourceBundles, and XML. It is free to use and distribute without compromising Nortel IPR. The license can be found at <http://apache.org/licenses/>

93.7 Network Component Dependencies

Refer to the SPC product specification for more information concerning supported configurations.

93.7.1 Nortel Networks Components

93.7.1.1 IEMS

The Nortel Networks Integrated Element Management System (IEMS) is used to provide proxy connections for SPC OAM functions. The SPC provisioning web client can be launched from IEMS. A secure shell (SSH) connection to SPC from IEMS is required for OSS operations. The OSS operator position can log into the SPC via IEMS secure proxy and SSH.

IEMS can be used as:

- Web proxy for SPC OAM operations via Web GUI
- Secure proxy for SPC logon
- Secure proxy for SPC OAM operations via OSS

Refer to IEMS documentation for information on how to configure IEMS interfaces for web server proxy and secure proxy for OSS.

93.7.2 Non Nortel Networks Components

Not Applicable

93.8 Restrictions and Limitations

- Only one CS2000 per SPC.
- Initial commissioning of SPC in SN08 requires a transfer topology data from SESM to SPC. This requires customer involvement via OSS to query the data on SESM and then add it to SPC.
- Centralized authentication of passwords is not supported by base platform.
- SPC will not co-run with any other NGSS based application.
- There is no synchronization of topology data between the SPC and SESM. If a topology mismatch is encountered during SPC call processing, the call attempt would be still be allowed. However, VCAC would not be applied for that leg of the call, and log would be generated to indicate that there is a topology mismatch between the SPC and GWC/SESM.

93.9 References

93.9.1 Specifications

COPS-Dqos Specification

93.9.2 Internal Documents

NGSS Fault Management guide

IEMS Configuration guide

OSSgate Users guide

93.10 Definitions & Abbreviations

API	Application Programming Interface
CAC	Call Admission Control
COPS	Common Object Policy Service
DQOS	Dynamic Quality of Service
IEMS	Integrated Element Management System
GUI	Graphical User Interface
GWC	Gateway Controller
KRS	Keycode Retrieval System
NGSS	Nortel General Purpose Session Server
NCGL	Nortel Carrier Grade Linux
PCF	Policy Control Framework
PEP	Policy Enforcement Point
QOS	Quality of Service
SESM	Succession Element Subsystem Manager
SSPFS	Succession Server Platform Foundation Software
SPC	Session Policy Controller
SIP	Session Initiation Protocol
VCAC	Virtual Call Admission Control
XML	Extensible Markup Language

94: A00007394 Functional description (FN)

94.1 Feature name

Network VCAC CallP

This FN mainly covers Network Virtual Call Admission Control (network VCAC), Actid A00007394. In addition, it also contains some information on following features.

- Network VCAC Maintenance & Upgrades (A00007399)
- Session Policy Controller (A00007393)
- Network VCAC Topology Provisioning (A00007242)

94.2 Description

Network Virtual Call Admissions Control (Network VCAC) is a Quality of Service (QoS) mechanism that allows the Communication Server 2000 (CS 2000) to cancel post-dial, pre-ringing calls that would overload a segment of the packet network. This is an enhancement of Basic VCAC (SN07, ACT.A00002739).

94.2.1 Network VCAC vs. Basic VCAC

For those familiar with Basic VCAC, its worth mentioning the main differences between Network VCAC and Basic VCAC.

The first notable difference is that bandwidth is tracked on the GWC in SN07. Whereas in SN08, the tracking is done externally to the GWC on a Session Policy Controller (SPC).

In SN08, Network VCAC removes the critical restrictions on deploying VCAC on sites with a mix of gateway types, which is imposed by Basic VCAC in SN07. It also removes the limitation of an LBL and the gateway behind it having to be on the same GWC.

In addition, the presence of a Session Policy Controller (SPC) adds new network management flexibilities through its management interface. It also provides additional logs and Operational Measurements (OM). For further information on the SPC see reference 1.

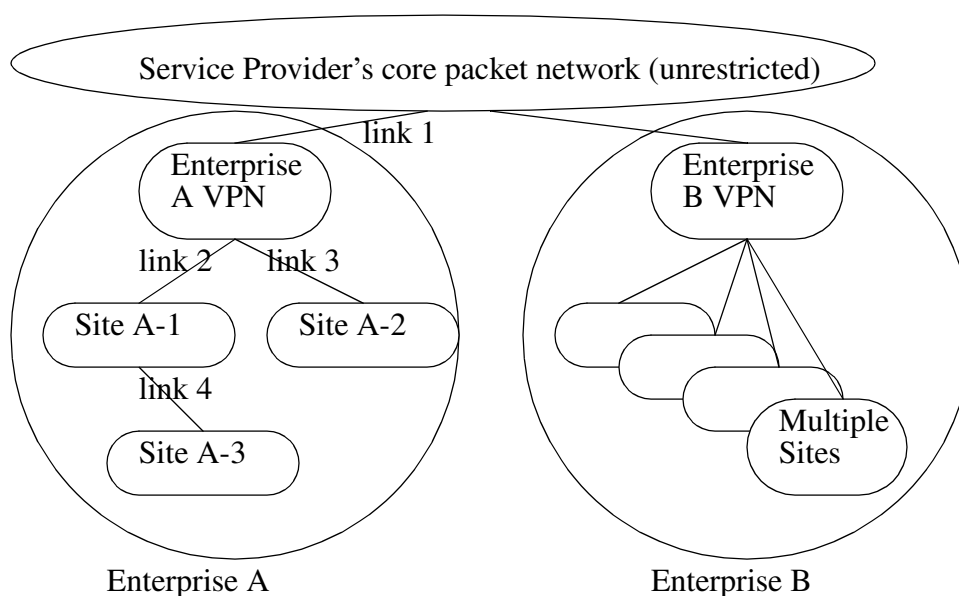
Network VCAC also supports composite network zones (a zone type that is a NAT and LBL at the same time). This type of zone is not supported by the SN07 Basic VCAC.

94.2.2 Detailed description

Network VCAC depends on a logical model of the packet network. This starts with the Service Provider's core packet network and points of bandwidth concentration. These could, for example, be customer enterprises that are made up of a collection of sites or a regional broadband aggregation point. These sites are connected by a mix of Limited Bandwidth Links (LBLs) and NATs. The Voice over IP (VoIP) Gateways (GWs) and hence the lines are located within the sites in each enterprise.

It should be noted that when we say a 'site' or a 'network zone', we are really talking about the same thing. Similarly, when we say a 'link' it is the same as a 'network link'.

Figure 1, High level view of a sample VCAC topology



The logical model that network VCAC uses is based on the links between the sites. The GWs are described as being behind or below a particular link. So, in Enterprise A in Figure 1, A GW in Site A-3 is behind link 4, which is behind link 2, which in turn is behind link 1.

Each of these links will be either a Limited Bandwidth Link (LBL) or a NAT. The LBLs have a provisioned level of resources available and know how many resources each call type consumes. NAT traversal was handled in Feature ACT.89007980 in SN06.

Once a call is made, the CS 2000 identifies the LBLs and NATs that the GWs are behind and informs the Session Policy Controller (SPC) that a call is being

made using these LBLs and NATs as the entry and exit points on the network. The SPC looks up the LBLs along the speech path between the two endpoints, and calculates if there are sufficient resources available on all the LBLs not to exceed the provisioned limits. The SPC provides a response allowing or not allowing the call as follows:

- 1) If all the LBLs can handle the new call, then the call progresses as normal.
- 2) If one or more LBLs cannot handle the call the originator receives a treatment provisioned by the carrier. The terminator has not reached a ringing stage so is unaware of the call attempt.

An example would be a call between a GW in Site A-3 and Site A-2. This call will use resources on links, 2, 3 and 4, but not on link 1 as the call doesn't leave the enterprise. An insufficient resources failure on any of the links will result in the call going to treatment.

The CS2M provisioning is described in activity ACT.A00007242CS2M, Network VCAC topology Provisioning and the SPC provisioning is described in activity ACT.A00007393SPC

It should be noted that if the SPC application is not available or the TCP connection between the GWC and the SPC is down, the call will be allowed to go through without doing any checks on bandwidth availability. Also, should the SPC topology not know about any particular link it is queried on it will reply with an error and the GWC will allow the call to proceed without any Admissions Control. These types of error can degrade the VCAC application as it allows calls access to the network without accounting for them.

Detailed description

The Logical Network Model

VCAC requires an operator to create a logical model of their network, made up of Limited Bandwidth links (LBL) and NATs. NAT traversal was added in ACT.89007980 in SN06, so the remainder of this description will focus on LBLs. This topology is provisioned on to the CS2M and the SPC using the OSS if it is present or onto each system separately if no OSS is present.

A LBL can represent a physical part of the network that has a bandwidth restriction (e.g. an ADSL line running at 600kbs) or a logical 'QoS point' (e.g. a customer has purchased a maximum of 1Mb/s of simultaneous VoIP calls). Each LBL has a maximum count associated with it. This is the maximum amount of bandwidth for calls available over the LBL.

The logical network model is a tree structure made up of LBLs and NATs according to the following rules (a generic term used to represent a LBL or NAT is network zone or zone; middlebox (MB) was used in SN07):

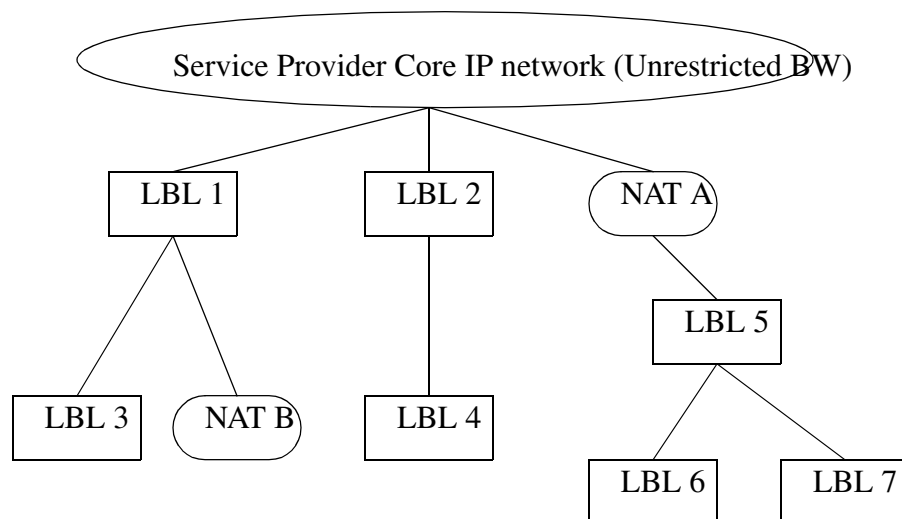
- A zone can be either an LBL, a NAT or a composite NAT & LBL at the same time.
- A top level zone must be connected to a non-bandwidth constrained 'core network'.
- A zone can have only one parent zone (closer to the core network) or the core network.
- A zone can have any number of children (subject to the maximum number of zones that may be datafilled per GWC).

These rules mean that:

- There can be no circular network paths.
- There can only be one route from a particular zone back to the core network

This logical model of the network must contain the key connectivity routes in the modeled network. E.g. If a set of duplicate routes exist between 2 zones, they must be modeled as one link, not two, as otherwise the network VCAC capacity counting will not be accurate.

Figure 2, Sample VCAC network model



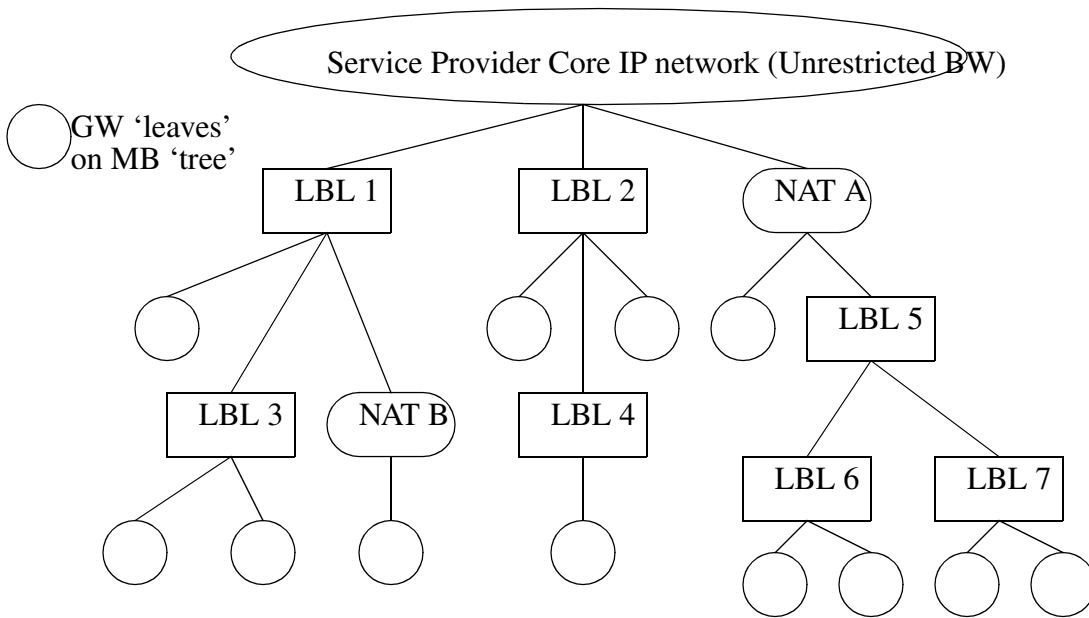
Adding GWs to the Model

GWs can be added to any zone in the logical model. A zone can have any number of GWs hanging off it. This is usually described as having GW 'leaves' on the zone 'tree'.

Note: PVG and UAS/AMS GWs are assumed to be within the core network. Similarly, Interdomain SIP-T trunks are assumed to start and finish in the core network

This means that any GW will have a single path through the model to the core network, and to any other GW that is within the model.

Figure 3, GWs attached to the zone network model



Network VCAC

Network VCAC works by calculating the path between the originating and terminating GWs, looking at the negotiated codec and ptime for the call and checking that each LBL in the path has sufficient resources for the call to be set up. If so, the call proceeds as normal, if not the call is released and a user provisionable treatment (which must be a tone) is applied to the originator. The terminator has not reached a ringing stage.

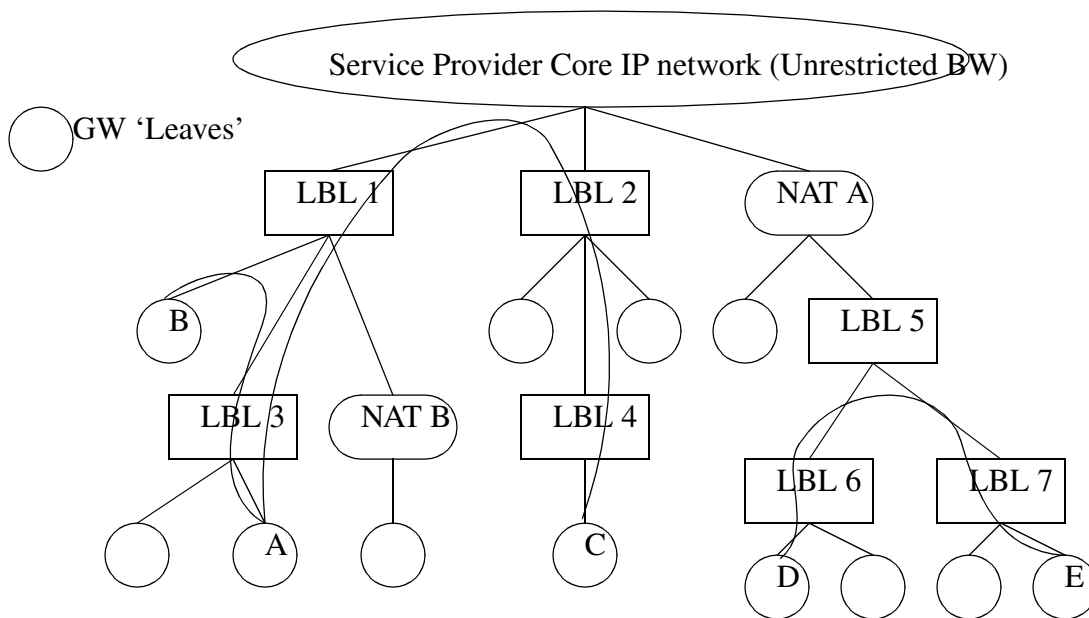
Note: Network VCAC uses the real, negotiated codec for the call. There are exception for certain call types (e.g. fax, modem) that are detailed below.

Note: Only the zones on the path are used - resources are not always used all the way to the core network if there is a shorter route through the network.

For example in Figure 4 below:

- An A-to-B call uses resources on LBL 3. LBL 1 is not used even though it is a part of the zone chain as the path between the GWs does not use it.
- An A-to-C call uses resources on LBL 3, LBL 1, LBL 2 and LBL 4. All the zones in the originator and terminator chains are on the GW path.
- A D-to-E call uses resources on LBL 6 and LBL 7. They are both behind the same NAT so no Media proxy is required.

Figure 4, VCAC path finding

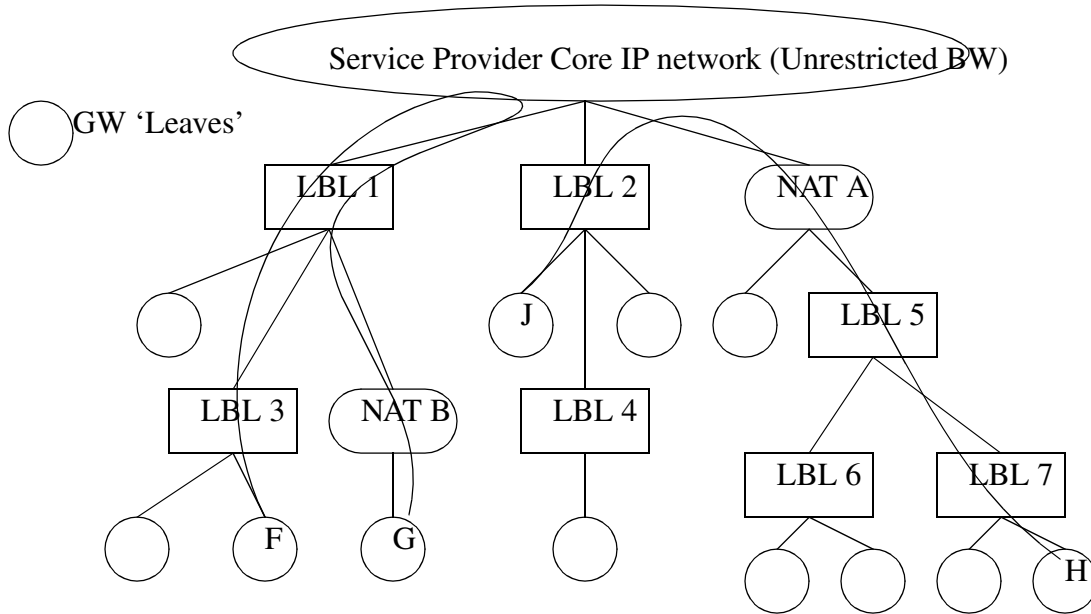


If there is a NAT zone on the call path then the call must extend as far as a Media Proxy (MP) (as described in ACT.89007980). These are located in the core network, so both the originator and terminator must use resources up to the core network, even if there is a shorter path between them.

Figure 5 below has examples of path finding when there is a NAT on the path between the GWs.

- An F-to G call uses resources on LBL 3 and LBL 1. LBL 1 has two call flows on it as both the originator and terminator need to use it to reach the Media Proxy (MP) in the Core network
- A H-to-J call uses resources on LBL 7, LBL 5 and LBL 2. This call will require a MP but the path between the GWs already traverses all the zones in the chain so there is no need to change this.

Figure 5, VCAC path finding though NATs



Basic VCAC is controlled by state SOC order code CS2Q0002. This has two states:

- ON, which will display ON and have VCAC enabled.
- OFF, which will display IDLE and will disable VCAC.

This SOC option also controls Network VCAC. It has to be in the ON state for Network VCAC to be usable.

In addition to the SOC option, Network VCAC is also controlled by a Service enabled flag, provisioned from the CS2M as part of feature ACT.A00007242CS2M, Network VCAC topology Provisioning.

Treatment

When a call fails due to VCAC failure (i.e. not enough bandwidth on the LBL to carry the call), an NBLN treatment is applied to the originating agent of the node. This can be complex to datafill particularly in a network scenario where the originating agent of the switch is a trunk. There are some caveats relating to SIP-T trunking below, and some limitations relating to services in the restrictions section at the end of the document.

For line originations that are blocked by VCAC a LINE138 log is produced with the treatment set to NBLN. For trunk originations that are blocked by VCAC a TRK138 log is produced with the treatment set to NBLN.

Note that NBLN can be generated by TDM peripherals which experience congestion but are still capable of call processing. This can also be generated by MG9K peripherals that experience congestion on intraswitched calls. The logs identify the originating parties and the dialed digits so it is possible to identify which set of circumstances has produced it.

Treatment Datafill

The significant tables are TMTCNTL, TMTMAP and FLXCMAP.

Table TMTCNTL is used to identify treatments to be played to lines. It is made up of several subtables, dependant on datafill. Each of these subtables must have the following tuple

NBLN Y S <tone>

NBLN is the treatment, Y signals that the event must be logged, S means the tone is defined by a CLLI and <tone> is the preferred tone, identified by the telco, to be played to the user. This <tone> can be a standard tone, e.g. T120 or a custom tone defined through table TONES, e.g. CONGESTION.

Warning: This MUST be set to a tone. Setting this to an announcement can result in a treatment loop as there is insufficient bandwidth to play the announcement.

Table TMTMAP is used to map signalling protocol and treatment pairs to a trunk release cause. These are used to signal to the previous node that this switch has rejected the call. They must be added for each signaling protocol used on trunks on this node. There is no dedicated VCAC release cause for any protocol, however each protocol does contain a number of release causes that are appropriate for VCAC. It is up to the telco to identify a release cause that will map into their signaling network. Examples of the TMTMAP datafill are:

Q764 NBLN ALLBC ISUP NOLOCAL NORMUNSP LOCLNET Y

Q767 NBLN ALLBC ISUP NOLOCAL NORMUNSP LOCLNET Y

Q931 NBLN ALLBC PRI NOLOCAL NORMUNSP LOCLNET Y

In these examples, Qxxx NBLN is the protocol pair, NOLOCAL indicates the treatment should not be played locally, NORMUNSP is the release cause and the ending Y signals the treatment should be logged.

The examples above will send Normal Unspecified as the release cause to the originating node. The originator of the call will hear a treatment specific to that release cause, not the NBLN treatment used on the terminating node. It is up to the telco to arrange the mappings from the line treatment to tone and release causes to tone if they require consistent tones for both line and trunk NVCAC failures.

Warning: The treatment MUST NOT be played locally (NOLOCAL in the example above) if any of the trunks using this node are based on SIP or H323. This can result in a treatment loop as there is insufficient bandwidth to play the announcement.

Warning: The release cause MUST NOT allow immediate reattempts. If the terminating line/trunk is blocked a reattempt will create a release loop as a different incoming trunk member will be attempted.

Table FLXCMAP is used to map release causes to treatments. in our example above the release cause is NORMUNSP so an example might be:

NORMUNSP CCITT_STANDARD RODR N

This will map the NORMUNSP to the RODR treatment. The RODR treatment will be used to index in to the TMTCNTL tables to identify what the user hears. In this example the originator is not guaranteed to hear the same tone (for RODR) as they would for a local NVCAC failure (for NBLN).

Note: In these multi-node scenarios it is up to the telco to configure the signaling to ensure the NBLN treatment can reach the originator. If any of the nodes do not support NVCAC (e.g. MCS5200) or do not have the SOC enabled (not configured or running pre-SN07 load) it may not be possible to get the NBLN treatment in all scenarios. The originator will receive a treatment based on the release cause the reaches the originating node instead.

Note: If the originating gateway does not support the release cause or the audible signal (e.g. MGCP, H.248) that it is mapped to, the end-user may not hear any tone when the NBLN treatment is provided.

Note: The datafill above is an example only. There are regulatory requirements for some aspects of the behaviour of signaling links and each customer may have different requirements for the mapping of release codes to treatments and for the management of their signaling network.

Inter-domain SIP-T vs Intra-domain SIP-T

When a SIP-T call is blocked by VCAC, the release could be initiated locally or from the switch on the other end of the trunk, depending on whether the trunk is intra-domain or inter-domain.

In the case where the SIP-T trunk is intra-domain, we assume that the switch on the other end of the trunk understands VCAC. So on a call where the originator is behind an LBL with not enough bandwidth to carry the call, we would let the call continue. This is because, the terminator could be behind the same LBL as the originator, hence eliminating the need to use the failing LBL, and therefore the call can be completed successfully. On the other hand, if the terminator is not behind the same failing LBL as the originator, at that point

the call would then be blocked. A release message would be sent in the backward direction using the release caused datafilled in TMTMAP for the NBLN treatment.

If the switch on the other side of the SIP-T trunk does not understand VCAC, then an inter-domain trunk should be used instead of intra-domain. Failure to do so, could result in a ring-splash/ringing problem when a call is blocked by VCAC. For example, the MCS5200 does not understand the VCAC extensions, so if it is configured with an Intra-domain trunk a person calling to it will hear ringing until answer, when they will be routed to treatment. This is because the MCS5200 uses slow start when it provides SDP. A GW that uses fast start over the same configuration would result in the originator hearing a ringsplash before being routed to treatment.

In the scenario where the SIP-T trunk is inter-domain, we assume that the far end switch does not understand VCAC. Therefore, any inter-domain SIP-T call originating from a gateway behind a low bandwidth link with not enough bandwidth to carry the call will be blocked before leaving the originating switch.

94.3 Migration from Basic VCAC to Network VCAC

The resource usage database in Network VCAC is located on the SPC, whereas it is on the GWCs in Basic VCAC. Sites that are already running Basic VCAC, and wish to migrate to Network VCAC, should follow the procedures outlined in this section to ensure the migration of the database is successful.

The migration from Basic VCAC to Network VCAC can be performed once the CS2000 has been upgraded to the SN08 software load. During the upgrade of the CS2000 software Basic VCAC will be operational. When the software upgrade is complete, the migration to Network VCAC can commence. Basic VCAC may be used for as long as desired following the upgrade before activating Network VCAC. Basic VCAC is supported for migration purposes from SN07 to SN08 and SN09. Support for Basic VCAC may be discontinued after these releases.

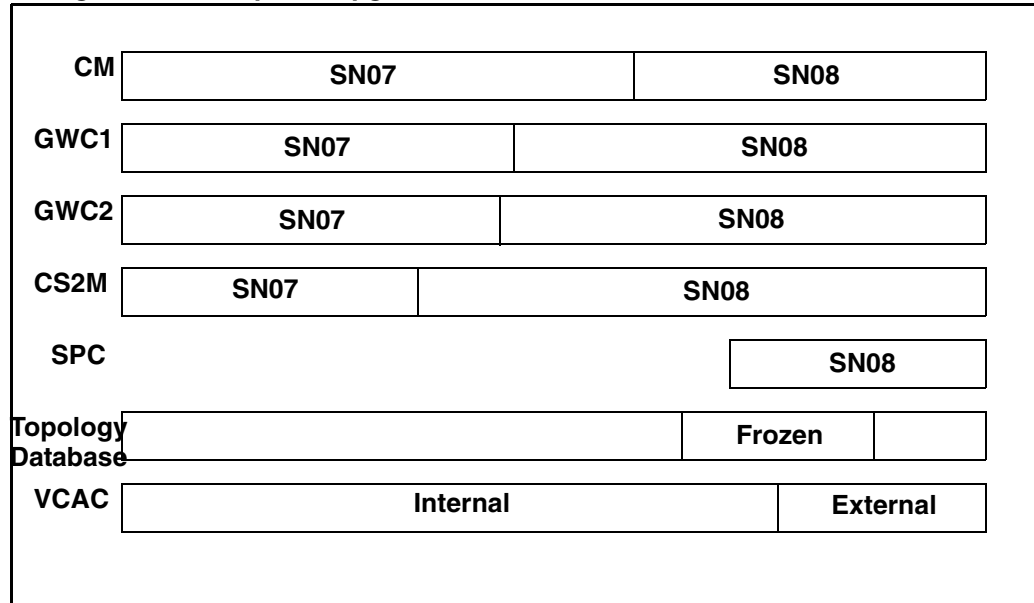
Figure 1 Anticipated Upgrade Timeline

Figure 1 illustrates the anticipated timeline over which the various switch components are upgraded. Initially the CS2M system is upgraded, as this is required prior to upgrading GWC cards. Following this, the GWC cards can then be upgraded. When the GWC cards are upgraded, they will continue to run the Basic VCAC software as before. The Network VCAC software in the new load will be dormant for the time being.

Following upgrade of all GWC cards, the core may be upgraded. After this, the switch has been upgraded to SN08, but the SPC and its associated external VCAC application have not been enabled. For customers not wishing to deploy these, this is as far as they need proceed.

Following verification of the upgrade of the main switch components to SN08, the switch to external VCAC can be considered. From now on, it is necessary to freeze the topology database and not allow any further changes to it until the migration process is complete. This is required in order to maintain consistency of the database during the migration.

When the SPC is commissioned, the topology model must be identically entered onto the SPC. This does not occur automatically, and should be done in accordance with the corresponding SPC documentation. The Basic VCAC software in use will still be using the database from CS2M, but the SPC will now contain a version in preparation for the switch to network VCAC. These two topology databases are separate and there is no automated synchronization process. Even after this procedure is complete, and topology changes are again allowed, care must be taken to ensure that both remain up to date.

Next, the SPC should be provisioned into the CS2M system, but Network VCAC not enabled. This will cause the GWCs to establish connections to the SPC. At this stage, it should be ensured that all is well with the SPC, that it's TCP links to the GWC are up, and that no alarms have been generated.

The switch to Network VCAC is controlled by the Network VCAC flag in CS2M. When Network VCAC is enabled via this option, the GWCs will cease to run Basic VCAC, and switch to using the SPC for VCAC policy decisions. Due to the significant change to call processing, it is recommended that the changeover should be performed at a quiet time, when few calls are in progress. Also, the Network VCAC software will not be aware of LBL resource usage of calls in progress at the time of the cutover. This anomaly will be cleared as these calls terminate.

If, for some reason, it is desired to revert to Basic VCAC, the Network VCAC option may be disabled in CS2M. The GWCs will then use revert to Basic VCAC and, as previously, use the topology model from CS2M. LBLs which are provisioned into SESM while Network VCAC in 'ON', cannot have VCAC correctly applied to them if the system is then reverted to Basic VCAC. Therefore, LBL provisioning should only be carried out once Network VCAC software has soaked for a sufficient length of time.

Note: Both the SPC and CS2M topology databases must be manually kept synchronized following the switch to Network VCAC. Failure to do this could result in malfunction of the feature.

94.4 Step-by-step Migration Procedure

This section describes the migration procedure in a step-by-step fashion. This is in anticipation of it being used to prepare an official MOP procedure document.

94.4.1 Purpose

This procedure describes how to convert a switch already running Basic VCAC with a particular topology, to run Network VCAC with the exact same topology. If any changes are required to the topology, e.g. new gateway associations or LBLs, then this must be done either before or after execution of this procedure.

Use of this procedure is not required for green-field installations of Network VCAC or for offices upgrading to SN08 Basic VCAC.

94.4.2 Documentation used by this procedure

The procedure references the following documents. Please ensure that you have them to hand and are familiar with them before starting.

SPC Provisioning Guide

A cook book is available at: <http://livelink-asiapac.us.nortel.com/asiapac/livelink.exe?func=ll&objId=1729558&objAction=browse&sort=nameRegards>. This has been captured in the Policy Controller Configuration Management NTP.

SESM Provisioning Guide

FN A00007242 (PLS FMDOC) “SESM support for SPC topology”. The corresponding customer documentation should be used when it is available.

Basic VCAC Documentation

FN A00002730 (PLS FMDOC) - Basic VCAC. The corresponding customer documentation should be used when it is available.

94.4.3 Pre-requisites

1. All switch components must be upgraded to SN08 load line-up prior to network VCAC activation. Basic VCAC is supported over the upgrade from SN07 to SN08 load line-ups.
2. The VCAC SOC option will be active, as the switch is already running Basic VCAC. Refer to Basic VCAC documentation.
3. SPC should be installed and commissioned with SN08 load. Refer to SPC Provisioning Guide. Check for no DQoS connection alarms or other suspicious logs on SESM or SPC.
4. Basic VCAC topology must be frozen prior to start. No topology changes are allowed during the procedure. Selection of Network VCAC is switch wide. It is not possible to run part of the switch on Basic VCAC and part on Network VCAC. Please ensure that the provisioned topology will be sufficient for your needs for the whole duration of the procedure before proceeding. Refer to Basic VCAC Documentation for further guidance.
5. Topology details for basic VCAC need to be available to migration engineers. This information is likely to be available through customer network data. It is also available in the basic VCAC configuration in CS2M. Refer to Basic VCAC Documentation.
6. It is recommended that this procedure should be executed during a time when call processing is at a minimum.

94.4.4 Network VCAC Activation

1. Provision basic VCAC topology (from pre-requisite step 5) in SPC. Please refer to SPC Provisioning Guide.

NB: It is critical to ensure that the VCAC topology provisioning in the SPC matches the CS2M topology before Network VCAC is activated otherwise

access control will not function correctly. In SN08 this is not checked automatically and needs to be validated by the upgrade engineer.

2. Activate Network VCAC flag in CS2M. Please refer to the SESM Provisioning Guide for further details on this.

NB: When Network VCAC is activated, all new calls will trigger bandwidth management through the SPC. There is no transfer of current bandwidth status between Basic and Network VCAC. This means that the SPC will have no knowledge of existing calls set-up under basic VCAC. This may lead to temporary degradation of voice quality on some calls. As existing calls are cleared, potential problem will be removed.

3. Verify call processing to confirm network VCAC is functioning correctly. Check for any suspicious logs on SPC, GWC or CM. We suggest allowing the system to soak for some time to allow any potential errors to come to the surface.

4. Once you are fully satisfied that the system is functioning correctly, topology changes may be made. Note that the provisioning restrictions have changed between SN07 and SN08. Specifically, in SN08 it is possible to mix agent types (IAD, CICM, H323) behind a common link. **These changes will not survive a rollback correctly, so the topology freeze must extend long enough for the VCAC behavior to be thoroughly tested and soaked in.**

5. Ensure that all topology changes are entered identically on both CS2M and SPC databases. These must both be manually kept in sync going forwards, otherwise access control will not function correctly. Refer to both SESM and SPC Provisioning Guides.

94.4.5 Network VCAC activation without Basic VCAC

The pre-requisite steps 1, 2 and 3 will be complete. I.e. the switch has been upgraded, the VCAC SOC is enabled, the SPC is installed and configured.

1. Provision the required treatment datafill as described in this document. In the migration scenario this would have been present for Basic VCAC.

2. Activate Network VCAC flag in CS2M. Please refer to the SESM Provisioning Guide for further details on this.

3 Start configuring the topology on both SESM and the SPC. These must be manually kept in sync, otherwise access control will not function correctly. Refer to both SESM and SPC Provisioning Guides. Once active gateways are associated with the topology in SESM, confirm network VCAC is functioning correctly. Check for any suspicious logs on SPC, GWC or CM. We suggest allowing the system to soak for some time to allow any potential errors to come to the surface.

94.4.6 Network VCAC Rollback

This procedure describes how to abort the switch to Network VCAC, by rolling back to Basic VCAC. It should only be carried out while the topology database is frozen, i.e. up until step 4 of the activation procedure. If this is not the case, topology mismatches may occur, leading to basic VCAC functioning incorrectly.

1. Deactivate Network VCAC flag in CS2M. Please refer to the SESM Provisioning Guide.

NB: Once network VCAC is deactivated, bandwidth will be managed on the GWC. Bandwidth status will not be transferred from the SPC to the GWC. This may lead to temporary degradation of voice quality on some calls. As existing calls are cleared potential problem will be removed.

94.4.7 VCAC Deactivation

In the event of a serious VCAC malfunction, the VCAC SOC may be disabled. This will disable all VCAC functionality - Network and Basic VCAC. When this option is taken, no access control will be performed by the switch. The VCAC SOC option is described in the Basic VCAC Documentation.

94.5 Hardware Requirements or Dependencies

Network VCAC requires a Session Policy Controller installed and configured as per Act A00007393SPC.

94.6 Software Requirements or Dependencies

Standard SN08 CS2K software components are required.

94.7 Limitations and restrictions

The VCAC architecture has some provisioning limits that are enforced by the the provisioning system. These are:

1. There is a maximum of 5 network links between a GW and the Service Provider's core network.
2. VCAC only uses the negotiated values for a call. This means that fax and modem upspeeding to G711 from G729 will not be modelled. Similarly T.38 fax calls will not change the modelled bandwidth for the call.
3. There is a requirement that voice traffic is prioritised over the data traffic. Furthermore, VCAC does not model voice and non-SPC controlled data traffic on the same LBL. This has to be done by careful modeling of the logical network, as a part of the system engineering.
4. Interactions with codec negotiation. In a network configured to use G729 and the preferred codec and G711 as the default codec the originator offers a list of codecs to the terminator who chooses which one the call will use. Initially the NVCAC application assumes the worst case (G711) at the

originator until the negotiated SDP is returned by the terminator. However, this means that it is not always possible to get the expected number of G729 on a link. This is difficult to detect as it is difficult to guarantee that all calls will negotiate to G729.

94.8 Logs and Operational Measurements

No new logs or OMs are introduced by this feature.

94.9 Interactions

VCAC potentially affects any call. If there is insufficient resources for a call or call leg to complete then the call will be released, and the user directed to a treatment. Some specific service examples are described in the Service Interactions section below.

VCAC can deny call admission whenever the speech path changes, so the main scenarios are:

1. **Call Origination.** After the digits have been dialed and the CS 2000 attempts to establish a speech path prior to ringing/ringback VCAC can deny admission to the call. This is the main VCAC scenario.
2. **Call Hold.** The bearer path is dropped for a call placed on hold, whether as a call hold service or as a step in another service such as 3WC or consultation transfer. If other calls have consumed the available resources then an attempt to retrieve the held call will fail.
3. **Call Transfer.** The bearer path is changed after it has been set up. This can be caused by services such as call transfer, CFNA, 3WC. IN services use this functionality by connecting a call to announcements before routing to other destinations. This fails if there is a LBL in the new path without resources for the new call leg.
4. **Calls that ring before negotiating the speech path.** Examples of these service are non-pilot members for simring and pre-answer call waiting attempts. In these cases the application only calculates the bandwidth on answer, so the call will be denied then if there is no bandwidth.

On call denial VCAC will clear down the call that would overload the LBL. **Service failure handling will be on a best effort basis, i.e. there is no attempt to retry or change to a less demanding codec.** See below for more details.

Note: On trunk calls that support suspend/resume bandwidth is maintained for the duration of the suspend/resume timer. This means that some of the service behaviour described here will vary if some or all of the parties are trunks.

94.10 Service restrictions and limitations

Bearing in mind the best effort approach to services, some limitations and restrictions are summarised here.

94.10.1 Lawful Intercept (LI)

There are a number of restrictions for configuring LI:

1. The parties monitoring for the Law Enforcement Agency (LEA) must not be configured behind any LBLs. This is similar to the restriction for NAT traversal, that the parties monitoring for the LEA must not be configured behind any NAT device. If this is not followed then these LEA monitoring parties can ring but not get speech path.
2. C-tone may be interrupted for dedicated LI where a call leg is denied by VCAC. Similarly, there may be ringspash on the LEA monitoring parties for switched LI when a call leg is blocked by VCAC.
3. There is a transparency issue for cases where the subject parties are behind a common, full, LBL. In this case the two people can call each other if they are not subject to LI, but will be blocked if one of them is being monitored, as the call is extended to the LI replicator device. An extreme example is when both parties are on the same GW, and so would never be blocked, thus making LI monitoring very obvious. This can be solved by the Public Network Interception (PNI) feature which will prevent calls from being monitored unless the Law Enforcement Agency (LEA) chooses to take the risk of the monitoring action being discovered.

94.10.2 Emergency and other priority calls

There is no guarantee that any emergency or priority calls will get through. They are subject to the same VCAC process as any other call type. They are NOT given any extra precedence over any other voice traffic by the NVCAC application.

94.10.3 Examples of service behaviour

If there is sufficient bandwidth for a service to proceed the NVCAC application has no impact on it. If there is insufficient bandwidth then one or more call legs will not succeed and the service attempt will fail. This section provides some examples of common service failures and how they behave. This is NOT an exhaustive list of service. It is NOT an exhaustive list of ways in which each service can fail.

1. Three Way Call. This can be blocked at a number of points - when retrieving someone from hold, on contacting the second party and when the three members are being connected to the conference bridge. If the second party cannot be reached the controller hears NBLN treatment and can flash back to the first party. If one party cannot reach the conference bridge due to bandwidth restrictions then the controller receives 3 seconds

of NBLN treatment to alert them to the problem before being connected to the other party.

2. **Call Waiting.** Transferring to a waiting call will only apply NVCAC when the switch to the waiting call occurs. This can fail as there may not be sufficient bandwidth for the two parties to reach each other. In this case the waiting party hears ringing, then NBLN treatment and the called party hears 3 seconds of BUSY before being reconnected to their original call.
3. **Call Hold.** A party put on hold releases its bandwidth until a reconnect attempt is made. This reconnection can fail if other calls have consumed the bandwidth in the meantime. In this case the party on hold drops to dialtone and the retrieving party hears NBLN treatment.
4. **Call forward No Answer.** This can fail when the call is made to the first party or when the call is forwarded on to the second party. If the failure occurs on the connection to the second party then the originator will have heard several seconds of ringing before receiving the NBLN treatment.
5. **Music On Hold.** Music on hold is played when a party is put on hold. If there is insufficient bandwidth for the on hold part to reach the audio server then the held party will drop out of the service and hear dialtone.
6. **SIMRING.** SIMRING only reserves bandwidth to the pilot DN. If there is insufficient bandwidth to reach the pilot DN then ring splash is heard on the non-pilot members. If there is enough bandwidth to reach the pilot, but the call is answered on a non-pilot DN without enough bandwidth then the originator hears NBLN treatment followed by DISC treatment, the answering party drops back to dialtone.
7. **CICM EBS secondary DN services.** The CICM secondary DN service can maintain two bearer channels. This means that some service failures will not occur because the speech path is maintained and the bandwidth is not released. However, holding multiple bearer channels will exhaust the bandwidth on links faster.
8. **Meet-Me Conference.** The Meet-Me service applies a short ring tone to existing conferees when a party attempts to join, even if NVCAC actually blocks that party. The denied party hears NBLN treatment but existing conferees hear no indication that the joining attempt failed. If the NVCAC-denied party was first or second to dial into the Meet-Me bridge, the remaining party is disconnected as if the conference had ended normally. Calls to a Meet-Me bridge denied by NVCAC are recorded as answered but with no elapsed time (i.e. instant disconnect) for billing purposes.

This is a sample list of service behaviour when NVCAC denies calls. Other service scenarios will behave in similar ways.

94.11 Glossary

Term	Description
AMS	AudioCodes Media Server
CS2000	Communication Server 2000
GW	Gateway
GWC	Gateway Controller
LBL	Limited Bandwidth Link
LEA	Law Enforcement Agency
MB	Middlebox
MGCP	Media Gateway Control Protocol
MP	Media Proxy
NAT	Network Address Translator
QoS	Quality of Service
SPC	Session Policy Controller
UAS	Universal Audio Server
VCAC	Virtual Call Admission Control
VoIP	Voice over IP
VPN	Virtual Private Network

94.12 References

1. Session Policy Controller (FN) - <http://livelink-asiapac.us.nortel.com/asiapac/livelink.exe?func=ll&objId=1534787&objAction=browse&sort=nameRegards>
2. Basic VCAC on CS2K - DDOC A00002730 in PLS FMDOC
3. Network VCAC COPs Enhancements - DDOC A00007397 in PLS FMDOC
4. Network VCAC Maintenance & Upgrades - DDOC A00007399 in PLS FMDOC
5. Network VCAC Topology Provisioning (A00007242) - under Documents / SN08 on <http://ptm.us.nortel.com/>

95: A00007399 Functional description (FN)

95.1 Feature name

Network VCAC Maintenance and Upgrade

95.2 Description

Please refer to the base Network VCAC FN (also covering maintenance and upgrade aspects) document stored under A00007394.

95.3 Hardware Requirements or Dependencies

95.4 Software Requirements or Dependencies

95.5 Limitations and restrictions

95.6 Interactions

95.7 Glossary

Table 1

Term	Description

96: A00007404 Functional description (FN)

96.1 Feature name

IEMS Security Serialized Patching

96.2 Description

This feature ensures that only one IEMS security module component is restarted at a time with respect to patching. Specifically if a request is initiated from the NPM GUI, CLUI, or scheduler to restart all IEMS security module components, separate requests will be queued and executed serially.

To ensure the NPM server serializes IEMS security module restart requests for patching, a new platform type is implemented by this feature. The new platform type value is 'SCTY' and can be queried as part of report generation from the NPM GUI or CLUI.

Previous to SN08, the IEMS security application appeared as one device in the NPM GUI or CLUI (IEMSCSS); or 2 devices in a clustered configuration. With this activity, the security application is divided into 2 applications; IEMSCSS and IEMSCSS_DS. In a clustered configuration, there would be a total of 4 instances of the security applications; IEMSCSS and IEMSCSS_DS on the active machine and IEMSCSS and IEMSCSS_DS on the inactive machine.

The IEMSCSS_DS application in SN08 requires a restart to enable or disable patches regardless of whether it appears on the active or inactive machine in a clustered environment. The IEMSCSS_DS component is running on both machines in a clustered environment. It should be noted that one of the IEMSCSS_DS device names in an clustered environment that appears in the NPM GUI or CLUI will show up as 'inactive' even though it is providing service.

96.3 Hardware Requirements or Dependencies

None.

96.4 Software Requirements or Dependencies

None.

96.5 Limitations and restrictions

During upgrades into SN08 from older releases, a PSE that is upgraded to SN08 will not be able to send its devices or be available for patching to an NPM that is SN07 or older. This configuration and patching support is no change from the previous policy in SN07.

If patching is required to any components at a version of SN08 and the NPM has not been upgraded, the script utility called “PatchUpToDate” should be used to patch those components on a given machine.

96.6 Interactions

None.

96.7 Glossary

Table 1

Term	Description
None	

97: A00007415 Functional description (FN)

97.1 Feature name

Internodal Emergency Standalone (ESA) Element Manager

97.2 Description

Internodal ESA will provide the ability to make calls while in ESA between MG9K nodes. In doing so, the Telcos will also be provided the ability to provision a “Community of Interest” which defines which MG9K nodes can make ESA calls between one another. A community must have access to a LAN switch (e.g. Passport 15K or equivalent) in order for Internodal ESA calls to complete.

If an MG9K does not have access to a LAN switch, it will operate in the pre-SN08 manner of routing calls between VMGs within a single MG9K node. Also, although a Community of Interest is defined, each node must be in ESA for it to participate in the community. Nodes are not forced to enter ESA.

The current implementation of ESA only allows calls between Virtual Media Gateways (VMG) within the same MG9K node. This feature will expand ESA’s ability to make calls between a limited number of MG9K nodes termed a “Community of Interest”. However, as with previous ESA releases, calls can only be made between VMGs that are in ESA.

97.3 Hardware Requirements or Dependencies

This feature will apply to all supported hardware platforms, per SN08 succession server platform foundation software specification.

97.4 Software Requirements or Dependencies

This MG9K EM feature is dependent on the corresponding SN08 MG9K feature for internodal ESA - A00006894.

97.5 Limitations and restrictions

- Up to 32 communities of interest are supported
- Each community can contain up to 15 nodes.
- A given node can only belong in one community.

97.6 Interactions

N/A

97.7 Applicable Customer Facing Sections

Fault Management

Logs	___
Alarms	__X__
Configuration	
Data Schema	__X__
User Interface	__X__
Element Manager	__X__
Security	___
Service Order	___
Office Parameters	___
Accounting (Includes AMA billing)	___
Performance (Includes OMs)	___

97.8 Glossary

Table 1

Term	Description
ATM	Asynchronous Transfer Mode
RMON	Remote Network Monitoring
UAS	Unavailable Second
SSU	Synchronization Supply Units
SMON	Switched Network Monitoring
SES	Severely Errored Second
EM	Element Manager
COI	Community of Interest
ESA	Emergency Standalone
VMG	Virtual Media Gateway
PVR	Passport Virtual Router
MG9K	Media Gateway 9000

98: A00007416 Functional description (FN)

98.1 Feature name

BASE 'IRM IP Takeover Robustness' feature

98.2 Description

98.3 Hardware Requirements or Dependencies

98.4 Software Requirements or Dependencies

98.5 Limitations and restrictions

This feature does not robustify IP takeover for Ethernet IOPs because the scope of the firmware churn is only HIOP and HCMIC.

98.6 Interactions

98.7 Glossary

Table 1

Term	Description

99: A00007417 Functional description (FN)

99.1 Feature name

Ethernet link overload Control

99.2 Description

With the significant increase of the call processing power introduced by the XA-Core architecture, messaging resources including the bandwidth for the link and real-time, can be exhausted by the high call processing rate.

Without protection to the messaging resources, critical messages can be dropped due to the unavailable messaging resources.

The purpose of this activity is to provide a mechanism to prevent sustained over-utilization of Ethernet links and notify existing System Overload Control (SOC) which reacts by interacting with the peripherals to reduce the rate of incoming new originating calls.

99.3 Hardware Requirements or Dependencies

N/A

99.4 Software Requirements or Dependencies

Feature XA-Core IOCAP Monitoring toolset: A00006693 provides OMs of interest.

99.5 Limitations and restrictions

Ethernet link overload control is only applicable to XA-Core.

Peripherals must contain software which reacts to the core overload signal.

99.6 Interactions

This feature provides monitoring of the Ethernet messaging link. When the level of messaging through the Ethernet link is approaching the maximum capacity, it applies throttling through the System Overload Control (SOC) function.

99.7 Log

Table 1 New or modified logs

Log name	Log number	NEW/MOD/DELETED	System (SOS/UNIX)
CAP	101	MOD	SOS

99.8 Glossary

100: A00007424 Functional description (FN)

100.1 Feature name

Alarm Enhancements on SAM21

100.2 Introduction

This document covers the SAM21 SC software robustness on following areas:

- Alarming of locked IO cards
- Alarming of recovering IO cards
- Alarming of the connectivity loss of boot server
- Alarming of the loss of NFS mount

100.3 Alarming of Locked Application Card

100.3.1 Design Solution

On the SAM21 Shelf Controller, the Salus application is responsible for all IO OAM actions and alarms should failures be detected during an OAM action. Following the infrastructure of IO card alarming, this feature will add Alarm ID 56 - **underlyingResourceUnavailable** and Alarm Type 4 - **Processing Error** for each application card. The severity of the alarm is **minor**, this will have yellow color high-lighting on the card on the SAM21 Manager GUI.

When a card is locked successfully, this alarm will be raised against the card, a trap (Informs) will be sent to the SAM21 Manager with following data:

- PhysicalIndex - the slot number of the card seats in plus 33,
- AlarmID - 56
- TimeStamp - the time when the alarm is raised
- AlarmType - 4
- Severity - 1
- DetailedInfo - "This application card is unavailable"

Considering during upgrade and roll back scenario, Salus will not alarm locked application cards when the Shelf Controller is in the process of upgrade from pre-SN08 release to SN08 release or plus.

100.4 Alarming of Application Card being Recovered

100.4.1 Design Solution

Same as above, Salus will be used to alarm application card being auto-recovered.

When a card is being recovered by NSS_BOOT_AUDIT, it sends a message to Salus to indicate the start and finish of the recovery, Salus will raise a major alarm against the card and clear the alarm after the recovery is successful done.

The alarm is raised through a trap (Informs) with following data:

- PhysicalIndex - the slot number of the card seats in plus 33,
- AlarmID - 56
- TimeStamp - the time when the alarm is raised
- AlarmType - 4
- Severity - 2
- DetailedInfo - "This application card is unavailable and being recovered"

100.5 Alarming of Boot Server Unavailable

100.5.1 Design Solution

This is a straight-forward extension of the other forms of alarming the loss of network elements. Hubble will ping the Boot Server address and will keep Mama informed of its status. Mama will raise an alarm based on the severity of the issue. And will clear the alarm if Hubble reports that it can be reached.

100.6 Alarming of NFS Mounts down

100.6.1 Design Solution

Salus will be modified to check the mounts periodically. It will attempt to remount any mounts found to be down, and raise an alarm for any mounts that remain down after the check. Only the mounts for provisioned applications will be checked.

Salus will schedule a reminder with Chronos, so that Chronos will send a message to Salus to kick off the check every 10 minutes. When the NFS mounts down is detected, the interval will be decreased to 1 minutes.

The recover script is currently responsible for the mounting the directories on start-up. It will be modified so that it can be called to check the mounts. This will allow the knowledge of the mount points to remain in one place.

100.7 Glossary

Term	Description
CS2K	Communication Server 2000
cPCI	Compact Peripheral Component Interconnect
EM	Element Manager
GUI	Graphical User Interface
OAM	Operations, Administration, Maintenance
SAM	Service Application Module
SC	Shelf Controller
SDM	Succession Data Manager
GWC	Gateway Controller

101: A00007459 Functional description (FN)

The SBA and AFT applications are upgraded like other applications on CBM. Please refer to the A00007635 “CBM Upgrades” FN document.

101.1 Feature name

This document is a functional description for the A00007459 “SBA: Upgrade Support for CBM” feature.

101.2 Description

Please refer to the A00007635 “CBM Upgrades” FN document for a description.

Note: There will be 30 sec. service interruption during the swact. The SBA application will go into backup state till the swact is completed.

101.3 Hardware Requirements or Dependencies

Not applicable

101.4 Software Requirements or Dependencies

The patch is required for all SN07 CBM sites to be able to upgrade SBA in the future. The CR #Q00983279 is open to address it.

101.5 Limitations and restrictions

Please refer to the A00007635 “CBM Upgrades” FN document.

101.6 Interactions

The SBA upgrade process will require a number of pre-checks and post upgrade steps to be performed. These steps will be documented in the Upgrade section of the customer documentation.

This section describes only the SBA pre-checks.

101.6.1 Pre-upgrade checks

The pre-checks for the CBM upgrade will be performed before any software is upgraded.

- The SBA should have no alarms before attempting to perform the CBM upgrade. If an alarm does exist, the user has to investigate the alarm and clear it or contact the next level support.

- The user has to ensure adequate backup space is available on the Core as the upgrade procedure stops the Billing Application for approximately 30 sec. during the swact time.

101.6.2 Post upgrade steps

To ensure that the SBA is still in a healthy state before we perform the reboot and swact upgrade stages, the following checks have to be performed.

- The SBA should have no alarms before attempting to perform the CBM upgrade. If an alarm does exist, the user has to investigate the alarm and clear it or contact the next level support.
- It is recommended to deliver unprocessed billing files to a downstream destination. No more than one unprocessed billing file should remain on the system. The appropriate instructions on how to manually close billing files and send them downstream will be described in the customer documentation.

101.6.3 Pre-Cloning steps

These steps will be performed after the swact is completed and the Billing application is INSV and before cloning the upgraded system.

The following has to be verified:

- Billing is collecting records
- The status of each RTB stream

The appropriate instructions will be provided in the customer documentation.

101.6.4 Procedure to OFFL SBA prior to the swact

This procedure has to be performed only by the customers who have a billing stream that:

- uses File Format Type = DIRP and
- uses Stream Record Format = BC and
- validates the SENSOR_TYPE, SENSOR_ID, RECORD_OFFICE_TYPE, and RECORD_OFFICE_ID fields in the header and trailer records.

There is a possibility that SBA DIRP file format billing files for BC streams will have incorrect header/trailer field values after CBM is BSY/RTS during the swact.

The procedure on how to OFFL SBA prior to the swact and bring it in-service after will be described in the customer documentation.

101.7 Glossary

102: A00007460 Functional description (FN)

102.1 Feature name

Media Proxy Insertion for IP IWSPM/MG4K

102.2 Description

Synopsis

This feature expands on the Media Proxy insertion functionality introduced by A89007980 in SN06.1 and A00003452 in SN07. Media Proxy insertion support is provided for IWSPM/MG4K via the GWC. The IWSPM/MG4K is unaffected and remains unaware of the behavior occurring on the GWC.

Note: The IP MG4K project was canceled for SN08, so information in this feature regarding that project does not apply. However, the content of this feature applies equally for the IW SPM.

No additional provisioning is required beyond that stipulated in A00003452 in SN07.

Overview

The activity A00007460 encompasses Media Portal (MP) Insertion for the Internet Transparency solution for interworking calls between legacy peripherals and GateWays (GWs) via the Internet Protocol (IP) version of the InterWorking Spectrum Peripheral Module (IWSPM, or IW). It also covers identical scenarios in the IP version of the Succession Media Gateway 4000 (MG4K) for its trunk agents interworking with IP GWs. Much of the GateWayController (GWC) solution has already been implemented under separate activities, A00003452 and A89007980.

With activities A89007980 and A00003452, bearer media from a telco's IP GW is routed through a Media Portal (MP) if the far-end IP GW is not an internal IP address inside a telco's Captive Office (CO) address domain. That is, a Real Time Protocol (RTP) MP must be used if it is outside the core network - in the external public IP network and even possibly behind a Network Address Translator (NAT) in an Enterprise or Residential area network. An Internet Transparency solution was implemented on the GWCs in A89007980 to be able to insert a media portal in the bearer path in such calls. As a part of this solution, the GWC has the ability to insert a media portal in the bearer path if one is needed.

The intent of this is to provide the ability to insert a media portal in the bearer path of calls involving external IP GW and Session Initiation Protocol for Telecommunications (SIP) trunks (both SIP-T and SIP-NGSS) with bearer paths residing on the IWSPM, which interwork with ENET-based signalling

agents. The insertion of the MP will be provided by the peer GWC to the IW, without any new messaging or configuration of the IW.

102.3 Hardware Requirements or Dependencies

None.

102.4 Software Requirements or Dependencies

None.

102.5 Limitations and restrictions

None.

102.6 Interactions

None.

102.7 Glossary

Term	Description
Media Proxy	RTP Portal device.
GWC	Gateway Controller
IWSPM	Inter Working Spectrum Peripheral Module
MG4K	Media Gateway 4000

103: A00007464 Functional description (FN)

103.1 Feature name

SBA PacketCable Event Messaging

103.2 Description

SN08 PacketCable Solution requires support for two entirely new billing streams. These streams are Accounting (PCEM) and LI (PCES).

This SN08 Activity A00007464(SBA PacketCable Event Messaging) provides modifications to SBA functionality on the 3PC-core as well as CBM to ensure end-to-end billing data delivery for Accounting (PCEM) and LI (PCES) streams.

It should be noted that valid PacketCable Product configuration is 3PC-core connected to CBM. There are no requirements to support this activity on any other configurations such as Xacore, Brisc, or SDM. Consequently, testing will be concentrated on 3pc/cbm configuration. This activity will provide following functionalities:

- CBM-3PCcore: Provides End-to-end delivery of billing data for PCEM stream
- CBM/3PC-core: Provides End-to-end delivery of billing data for PCES stream
- CBM/3PC-core: Will provide PCEM throughput capacity of 225 KBHCA(10 events / call, 200 byte average event) as per 'SN08 PacketCable EM requirements for Billing'.
- CBM/3PC-core: Will provide PCES throughput capacity of 0.2 KBHCA(10 events/call, 200 bytes average event)
- CBM-3PCcore: Will provide latency for PCEM stream as per 'SN08 PacketCable EM requirements for Billing'. This feature will provide latency of 2.5 seconds from Event generation to SBA CBM disk.
- CBM-3PCcore: Will provide latency for PCES stream as per 'SN08 PacketCable EM requirements for Billing'. This feature will provide latency of 2.5 seconds from Event generation to IAA software .
- CBM: Configuration of PCEM stream from billmtc;confstrm;add level
- CBM: Configuration of PCES stream from billmtc;confstrm;add level
- CBM: query of PCEM stream from billmtc;confstrm;list level
- CBM: query of PCES stream from billmtc;confstrm;list level

- CBM: modification of already provisioned parameters for PCEM stream from billmtc;confstrm;change level. Note that modifications are not allowed if the stream is active.
- CBM: modification of already provisioned parameters for PCES stream from billmtc;confstrm;change level. Note that modifications are not allowed if the stream is active
- CBM: deactivation of PCEM stream from billmtc;confstrm;delete level
- CBM: deactivation of PCES stream from billmtc;confstrm;delete level
- 3PC-core: assignment of backup volumes for PCEM stream from mapci;mtc;appl;sdbil;addvol level
- 3PC-core: rejection of backup volumes configuration for PCES stream from mapci;mtc;appl;sdbil;addvol level
- 3PC-core: Activation of PCEM stream from mapci;mtc;appl;sdbil;post level
- 3PC-core: Activation of PCES stream from mapci;mtc;appl;sdbil;post level
- 3PC-core: query of PCEM stream from mapci;mtc;appl;sdbil;post pce;query level
- 3PC-core: query of PCES stream from mapci;mtc;appl;sdbil;post pces;query level
- 3PC-core: display banner for BKUP and REC subsystem for PCES stream will be set to offl at mapci;mtc;appl;sdbil;post pces level
- 3PC-core: deactivation of PCEM and PCES streams from mapci;mtc;appl;sdbil;post level

103.3 Hardware Requirements or Dependencies

Following hardware is required for PacketCable Event Messaging Solution:

- 2 x NTRX51GZ (Call Agent Blades with 1.5GBytes RAM)
- 2 x NTRX51GT (72GBytes STORM-IA disks)

103.4 Software Requirements or Dependencies

This activity is dependent on following activities for end-to-end delivery of PCEM and PCES billing streams from the core:

- **A00007196:** PacketCable Event Messaging. Allows successful datafill of CRSFMT and CRSMAP tables for PCES and PCEM streams
- **A00007465:** Integrated Accounting Application(IAA). Ensures PCEM , PCES event messages are delivered downstream.

103.5 Limitations and restrictions

- Filtered streams not supported for PacketCable streams PCEM and PCES.

- Some existing commands(such as query, closec, amadump, sendfile, and listfile) are modified for PacketCable streams. These commands are detailed in the Configuration Section (CN).

103.6 Interactions

None

103.7 Glossary

Term	Description
3PC	Third Party Core
CBM	Core Billing Manager
IAA	Integrated Accounting Application
LI	Legal Intercept
PCEM	PacketCable Event Messaging (ie. Accounting stream)
PCES	PacketCable Electronic Surveillance (ie. LI stream)
SBA	SDM Billing Application
SPS	Sterling PacketCable Software

104: A00007465 Functional description (FN)

104.1 Feature name

Integrated Accounting Application (IAA)

104.2 Description

This document covers the IAA Event Messaging and Legal Intercept processing functionality supported in the SN08 time frame. This functionality adds a packet cable transport mechanism to the Core Billing Manager 850 (CBM850) which is packet cable compliant.

Accounting and Legal Intercept Event Messages are received by the IAA from the SBA and Gateway Controllers (GWCs). When received, the messages do not contain the RADIUS header necessary to send the event messages to the down stream RKS pair or DF. When sending to a RKS pair, ftp or secure ftp can be used as a primary transport protocol.

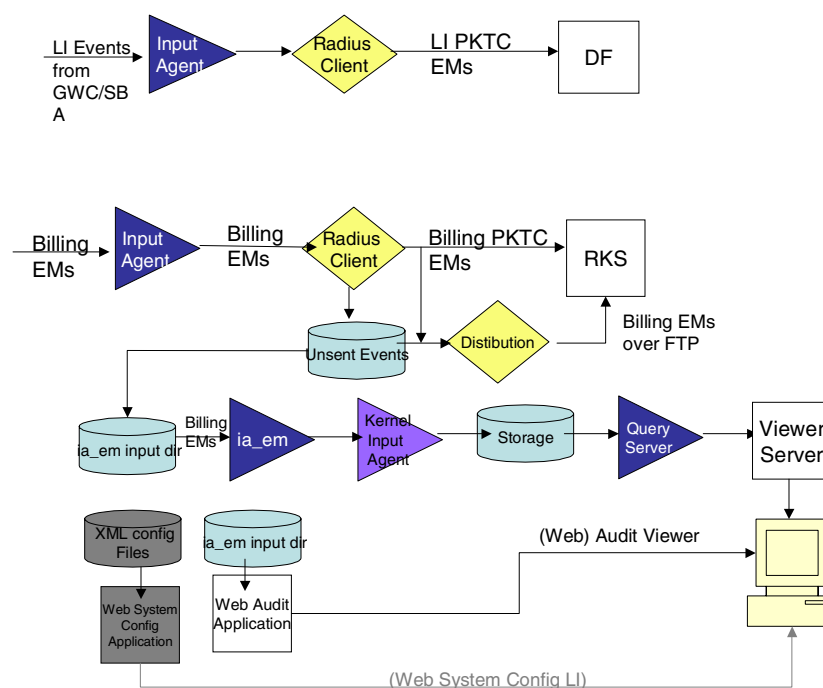
The accounting event messages will be reformatted to include a RADIUS header and a Sequence Number in the Event Message Header and then forwarded to a RKS pair. In the event that the accounting event messages cannot be delivered to the RKS, they are stored locally in the packet cable event message file format, and can be retrieved by the RKS or scheduled to be sent using the ftp or secure ftp protocol. In addition, the untransmittable accounting event messages are stored in the internal storage layer and made available to users via a record viewer web interface.

The legal intercept event messages are reformatted to include a RADIUS header and add a Sequence Number in the Event Message Header and then forwarded to a DF over a secure transport path. In the event the messages cannot be sent for any reason the events are dropped.

104.2.1 System Behavior

Accounting and Legal Intercept Event Messages will be received by the IAA application from the SBA (Supernode Billing Application) and GWCs (Gateway Controllers) via various interfaces.

There will be two SBA Input agents for processing primary and recovery files from the SBA. There will be a LI Collector module, which the SBA and different GWCs interface with, to transmit LI messages over UDP.



At the output side, there will be two Event Message Distribution Agents configured within the Accounting Server - one to handle LI messages and the other for Billing Accounting messages. These two instances will be identified by configuration as to what type of Event Messages each one handles.

The Billing/Accounting EMDA will send RADIUS messages to Record Keeping Server (RKS) pairs and the LI EMDA will send messages to one or more Delivery Function (DF) Servers.

The routing to various destinations will be done on the basis of the Channel ID field present in the LI and Billing Messages obtained from the SBA and GWCs. Each Channel ID will have corresponding to it (in a lookup table), a DF or RKS Pair to which the data needs to be sent to.

The accounting event messages will be reformatted to include a RADIUS header and add a Sequence Number in the Event Message Header and then forwarded to a RKS pair. In the event that the accounting event messages cannot be delivered to the RKS, they are stored locally and can be retrieved by the RKS or scheduled to be sent using the ftp or secure ftp protocol. In addition, the untransmittable accounting event messages are stored in the internal storage layer and made available to users via a record viewer web interface.

The legal intercept event messages are reformatted to include a RADIUS header and add a Sequence Number in the Event Message Header and then forwarded to a DF over a secure transport path. In the event the messages cannot be sent for any reason the events are dropped.

A FTP agent will take care of sending the data over FTP downstream to the RKS, if configured to do so.

A Web-based User Interface (and Command line tool) will allow configuration and ability to view untransmitted event messages.

104.2.2 Configuration

The configuration information used by the IAA is contained in various XML files. These files are found in the directory `/iaa/<xx>/data/config`. The items that can be configured by the user, using the web interface or command line tool (`iaa_config_cli`) can be found in the configuration section.

The configuration files that control the operation of the IAA modules can be found in `/iaa/<xx>/data/<modulename>/<modulename>.config`. This information is updated during the application installation and should not be modified by the end user. Below is an example of the xml configuration file for the emda module:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">

<!--
#
# FILE NAME
#   emda.config
#
# FILE CREATION
#   19 July'2004 By Ashwini Ravindra.
#
# FILE REVISION
#   $Id: emda_li.config,v 1.1.2.1 2004/08/06 10:21:36 vjohn Exp $
#
# FILE HISTORY
#   $Log: emda_li.config,v $
#   Revision 1.1.2.1 2004/08/06 10:21:36 vjohn
#   Initial checkin for EMDA
#
#
#
-->
<!--                                     -->
<!--                                     -->
<!-- Module           Event Message Distribution Agent           -->
<!--                                     -->
```

```

<!--      Start of configuration settings      -->

<config>

  <import file="common.xml">
    <section name="processTable">
      <param name="processID" value="302"/>
      <param name="processType" value="emda"/>
      <param name="processMgmtPort" value="6071"/>
    </section>

    <section name="urf"/>

    <section name="clientCom">
      <param name="clientId" value="401"/>
      <param name="clientUnixSocketPath" value="/tmp/kernel_1.sck"/>
      <param name="serverPort" value="5000"/>
    </section>

    <section name="serverCom">
      <param name="serverPort" value="7001"/>
      <param name="serverUnixSocketFile" value="/tmp/emda_li.sck"/>
    </section>

    <section name="miscSettings"/>

    <section name="log">
      <param name="logFileName" value="emda_li"/>
    </section>

    <section name="progressStorage"/>
    <section name="lightStorage"/>
    <section name="shmBuffer">
      <param name="shmPath" value="/shmpath/li_emda"/>
    </section>
    <section name="inputurf"/>
    <section name="io">
      <param name="outputMechanism" value="0"/>
      <param name="inputMechanism" value="0"/>
    </section>
  </import>
  <section name="EMDAMisc">
    <dir name="tablepath" value="$(RECO_HOME)"/>
    <bool name="useReferenceData" value="TRUE"/>
    <int name="numOfSeconds" value="10"/>
    <int name="DestinationType" value="0" />
    <int name="DistributionCapFactor" value="2"/>
    <int name="KeepVSAHeader" value="0"/>
    <int name="SenderThreadSleepTime" value="1000"/>
    <int name="MonitorThreadSleepTime" value="1000"/>
    <int name="ReceiverThreadSleepTime" value="1000"/>
  </section>

```

```

    <int name="FileWriterThreadSleepTime" value="1000"/>
    <int name="ShmFlushInterval" value="100"/>
</section>

<import file="global_parameters_list.config">
  <section name="GlobalParameters"/>
  <table name="GlobalParametersTable"/>
</import>
<import file="destination_streams_list.config">
  <section name="DestinationStreams"/>
  <table name="DestinationStreamsTable"/>
</import>

<table name="refDataSectionNames">
  <string column="refDataSectionName"/>
  <string column="tableSectionName"/>
  <row>
    <cell column="refDataSectionName" value="GlobalParameters"/>
    <cell column="tableSectionName" value="GlobalParameters"/>
  </row>
  <row>
    <cell column="refDataSectionName" value="DestinationStreams"/>
    <cell column="tableSectionName" value="DestinationStreams"/>
  </row>
</table>
</config>

```

104.2.3 Starting the IAA

The IAA modules are started and controlled by the SDM Application Manager (SAM). Upon startup the input agents bind to ports as defined in `/etc/services` to listen for LI event messages as well as messages from the SBA to indicate that data was written to a file.

104.2.4 Stopping the IAA

The IAA modules are stopped by the SDM Application Manager (SAM).

104.2.5 File Management

Temporary files used by the IAA modules are removed after they are no longer needed. Files created by the EMDA (if configured to send to the RKS via ftp or sftp or if they cannot send events to the downstream RKS in realtime) are moved to the `/iaa/<nn>/secondary` directory by the `fdsend` program. If the filesystem is full the oldest secondary (already transmitted) file or files will be removed to make room for the new file. It is anticipated that this filesystem will remain at 80 to 100 percent capacity.

The event messages that are not sent downstream are also stored in the IAA storage layer and made available to the end user for viewing via the web. This data is stored in the directory `/iaa/<nn>/kdb`. These files are removed by the

utility 'remove_aged_file'. When invoked it will take as parameters: the number of days old as a reference and the list of directories to search for old files.

104.2.6 Filesystems and Directories

Upon installation of the IAA the following filesystems and directories will be created to hold executables, libraries and data used and created by the application.

FileSystems:

```
/cbmdata/<slices>/iaa/data  
/cbmdata/<slices>/iaa/ftpout  
/cbmdata/<slices>/iaa/kdb  
/cbmdata/<slices>/iaa/config
```

Directories:

```
/opt/nortel/cbm/<xx>/iaa  
/opt/nortel/cbm/<xx>/iaa/bin  
/opt/nortel/cbm/<xx>/iaa/slib  
/opt/nortel/cbm/<xx>/iaa/webapps
```

104.3 Hardware Requirements or Dependencies

The IAA has the following requirements:

- SUN Netra 240
- 2GB of RAM dedicated for the IAA modules, for a system configuration of 4GB.

104.4 Software Requirements or Dependencies

SSPFS 3rd party Software Suite Version 08 with the following version dependencies:

- Apache Web Server 2.0.47 or above
- JRE 1.4.2_04 or above
- Apache Tomcat 4.1.24 or higher
- SBA
- jdom 1.0 beta 7 or higher
- dom4j 1.4
- saxon 6.4.3

104.5 Limitations and restrictions

Due to disk storage requirements only records not sent to the downstream RKS over the RADIUS protocol, will be viewable via the IAA record viewer

104.6 .Interactions

- Syslog daemon Server (Designer logs)
- Customer Logs
- State Changes

104.7 Applicable customer facing sections

Fault Management

Logs ___X___

Alarms ___X___

Configuration

Data Schema _____

User Interface ___X___

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) ___X___

104.8 Glossary

Table 1

Term	Description
DF	Delivery Function Server
GWC	Gateway Controllers
IAA	Integrated Accounting Application
LI	Legal Intercept
PC EM	Packet Cable Event Message
RKS	Record Keeping Server
SBA	Supernode Billing Application
XML	eXtensible Markup Language

105: A00007483 Functional description (FN)

105.1 Feature name

GR740 Secure using SSH

105.2 Description

The purpose of this feature is to provide a new scheme for securing the TCP/IP connections used for carrying GR-740¹ data between a CBM or SDM² and an OSS. This new scheme will ultimately replace the current DCE security scheme, but in the short term, both security schemes must co-exist. Hence, both the CBM and the OSS sides must support both schemes.

The connections shall be secured using the industry-standard SSH³ security scheme, which provides transparent 128-bit encryption (and decryption), data integrity, and user and node authentication. On the CBM-side, the SSH product to be used shall be OpenSSH⁴ version 3.8.

The connections between the CBM and the OSS will be established from the OSS-side using an SSH technique known as *local port forwarding*. Port forwarding allows forwarding of TCP/IP connections to a remote machine over an encrypted channel and allows those forwarded ports to be used securely by other TCP/IP-based applications. All data flowing through the forwarded port is automatically encrypted and authenticated. In this configuration, the OSS is the (local) client and the CBM is the (remote) server. Depending on the end office configuration, GR740 requires the setup of up to six connections from the OSS to the CBM, and for the purposes of this feature, each connection would have to be separately port-forwarded. The exact means of establishing the required port-forwarded connections is left to the discretion of each individual OSS vendor.

Local port forwarding can be accomplished using variants of the following basic command:

- `ssh -L loss_port:localhost:cbm_port cbm_ip_addr`

¹ And GR-746 data, as applicable to the office configuration.

² For the remainder of this document, CBM shall be used to refer to both CBM and SDM products, unless otherwise stated.

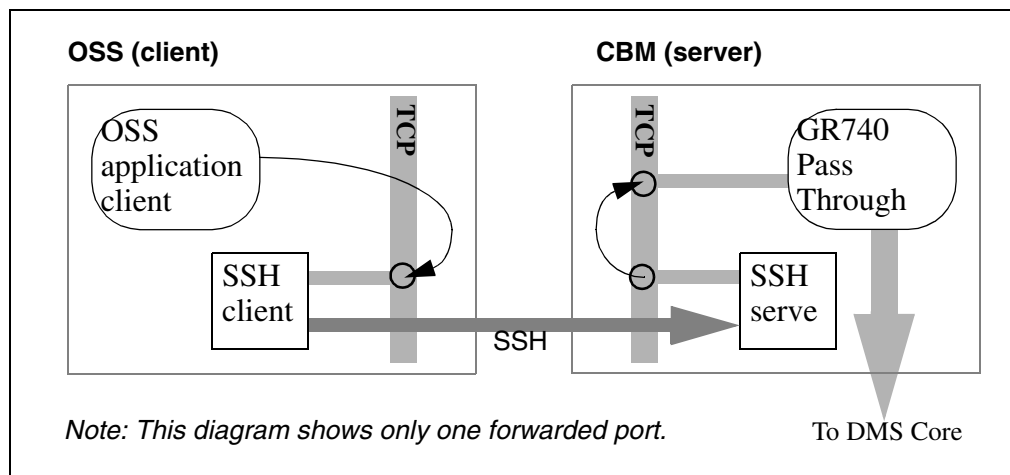
³For more information on SSH, please refer to any applicable published text such as “SSH, The Secure Shell: The Definitive Guide” by Barrett & Silverman (O’Reilly).

⁴For more information on OpenSSH, please visit <http://www.openssh.org>.

Where *cbm_port* is one of the six standard GR740 ports, i.e. 9550 - 9555, *oss_port* is any available port on the OSS node (as per vendor), and *cbm_ip_addr* is the IP or DNS address of the CBM node.

Connections to the remote server can be authenticated using user names and passwords or public/private key-pairs¹, at the OSS vendor's or customer's discretion. Public/private key-pairs particularly simplify login with only minimal extra effort required to initially configure the keys.

Figure 1 Local port forwarding in an OSS-CBM configuration



Since the connections have to be established by the OSS, it must also handle the detection and re-establishment of dropped connections. If a connection is lost, the OSS will be responsible for detecting the drop and re-connecting.

To help facilitate dropped connection detection, the ssh server daemon (i.e. *sshd*) on the CBM side has been configured for KeepAlive functionality, and thus any and all SSH connections to the CBM will implicitly use the KeepAlive feature. With KeepAlive set to 'yes' (default), the CBM will periodically transmit keepalive messages to the OSS; if no response is received within the timeout period, the connection is considered to be in error and the CBM will shut the connection down. The *sshd* KeepAlive interval is the generic TCP KeepAlive interval², which is already set to 2 minutes (120000ms) in the CBM and will not be changed. Please note that the CBM's TCP KeepAlive interval value of 2 minutes is significantly less than the default value of more than an hour for most Unix-based systems.

A similar KeepAlive feature is available for client-side SSH, and as such should be available on the OSS. As with the server (CBM) side KeepAlive, the OSS can send keepalive messages to the CBM; if no response is received

¹Following SSH upgrades on the OSS software, public/private key pairs will have to be regenerated.

²Parameter name: *tcp_keepalive_interval*

within the timeout period, the connection is considered to be in error and the OSS will shut the connection down. However, it is important to note that the SSH client KeepAlive setting and the OSS TCP KeepAlive interval are set as per each vendor's discretion. The vendor may also decide to implement a separate keepalive mechanism at the OSS application level.

On the CBM side, changes are generally limited to GR740 Pass Through configuration procedures. When configuring the GR740 Pass Through feature, the options presented to the user will depend on system configuration. During GR740 Pass Through configuration on CBMs and on non-DCE-provisioned SDMs, users will be presented with a menu consisting of two choices: *Non-secure*; and *Local (SSH) security*. For GR740PT configuration on SDMs which have the DCE installed and activated, users will first be asked if they want to enable DCE security for GR740PT. If they respond positively, then they will be prompted for the DCE userid and password. If the userid and password are valid, or if they answered 'No' to the original DCE security question, they will be presented with a menu listing 3 choices: *Non-secure*; *Local (SSH) security*; and *DCE security*.

By selecting the *Local (SSH) security* scheme, only SSH-secured external connections will be permitted to the GR740PT processes (and unsecured connections will not be permitted). This point implies that in order to access the GR740PT processes from another node (e.g. OSS), a port-forwarded SSH tunnel must first be established between the remote node and the CBM or SDM for each GR740PT port to which access is required. In *Local (SSH) security* mode, connections from within the CBM or SDM to the GR740PT processes (i.e. by local users already logged into the node) do not require an inter-nodal SSH tunnel.

If *DCE security* is chosen as the security scheme, then DCE security is established (as per previous software releases). Note that even if the user answered 'No' to the DCE security question asked prior to the displaying of the security options menu, *DCE security* can still be selected; the user will simply be prompted for the DCE userid and password at that point.

If the *Non-secure* option is chosen, unsecured connections originating from any node to GR740PT will be permitted (as per previous software releases), but SSH-secured external connections are also possible.

Note: The "authorized GR740 users only" requirement (A00007483 DID Project Requirement #10) described above for the SSH security mode has been deferred to SN09/CBM22. The deferral is being tracked via CR.Q00990244.

105.3 Hardware Requirements or Dependencies

None.

105.4 Software Requirements or Dependencies

This feature will depend on the SN08/SDM21 software load for the SDM and CBM products.

As this feature deals with the use of OpenSSH on the CBM and SDM products, there is also a dependency on OpenSSH 3.8. Any SSH-related functionality described as part of this feature must work with OpenSSH 3.8. The SSH product used by the individual OSS vendors must also function properly with OpenSSH 3.8.

The system for indicating authorized GR740 users will be the standard user authorization system for the CBM and SDM platforms. The standard authorization mechanism in SDM/CBM is based on user groups and is being modernized as part of activities A00007492SDM “User Group Administration -- 2324” and A00007489SDM “Integration Of SDM User Authentication With IEMS -- 2189” both delivered in this release (SN08). Conformance to the new authorization framework will allow GR740 user authentication and authorization to be centrally managed.

There are no explicit Core software dependencies; Core loads which support CBM08/SDM21 are the only pre-requisite.

105.5 Limitations and restrictions

If, when configuring GR740 on the CBM, the user chooses the non-secure or DCE options, then this feature will have no effect.

This feature is limited to providing a security option for GR740 connections TCP/IP only. No other types of connections or applications are supported/affected by feature A00007843, although SSH is available to all TCP connections and applications which use those connections.

105.6 Interactions

This feature will interact with the existing GR740 functionality on the CBM. The effects of the changes will be to provide a new means of securing GR740 TCP/IP connections between the OSS and the CBM. After initial configuration, any impacts of the changes should be transparent to the users.

105.7 Glossary

Table 1

Term	Description
CBM	Core & Billing Manager
DCE	Dispatcher Control Entry
OSS	Operations Support System
SDM	SuperNode Data Manager
SSH	Secure SHell

106: A00007489 Functional description (FN)

106.1 Feature name

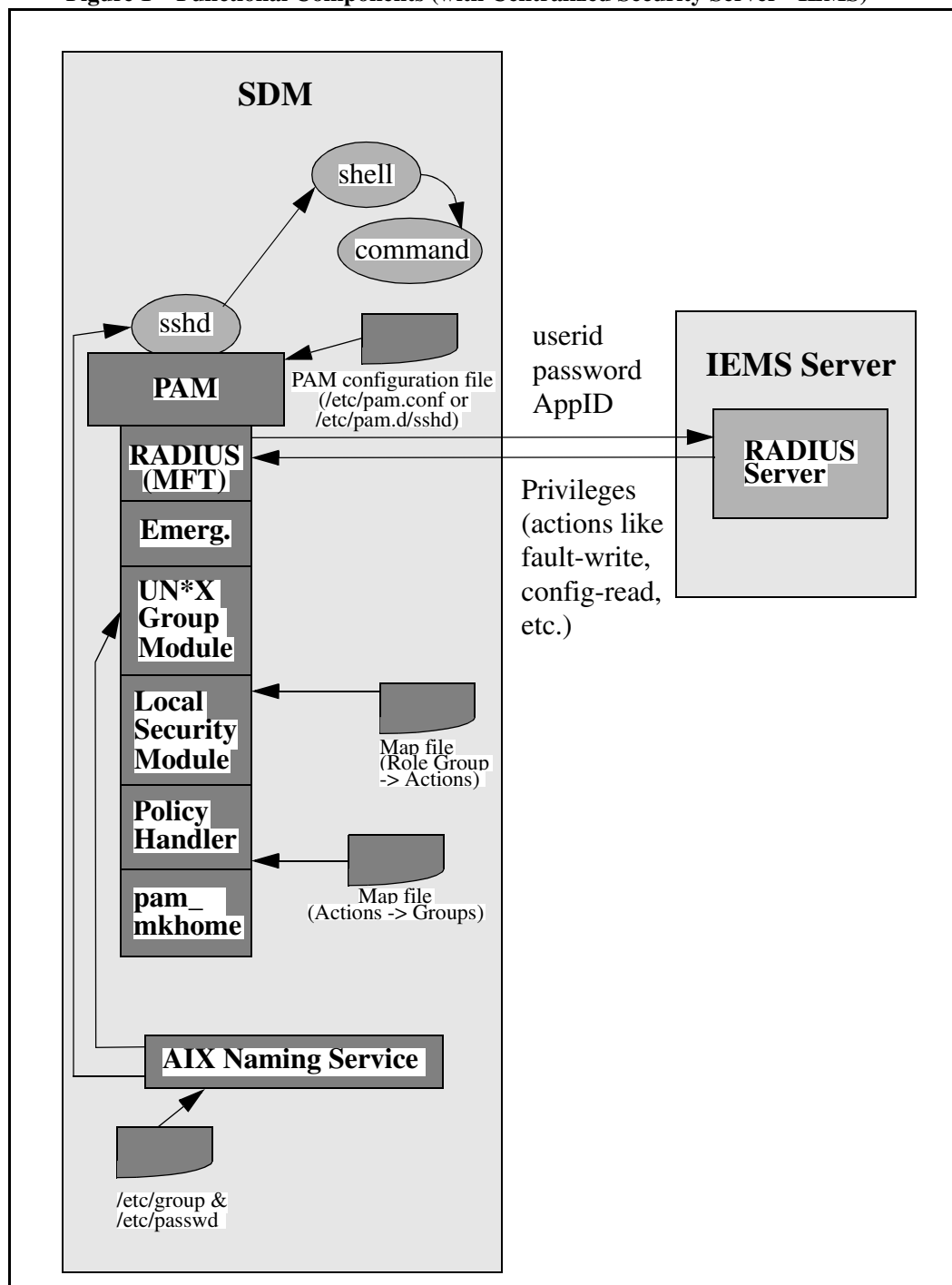
Integration of SuperNode Data Manager (SDM) User Authentication with the Integrated Element Manager System (IEMS)

106.2 Description

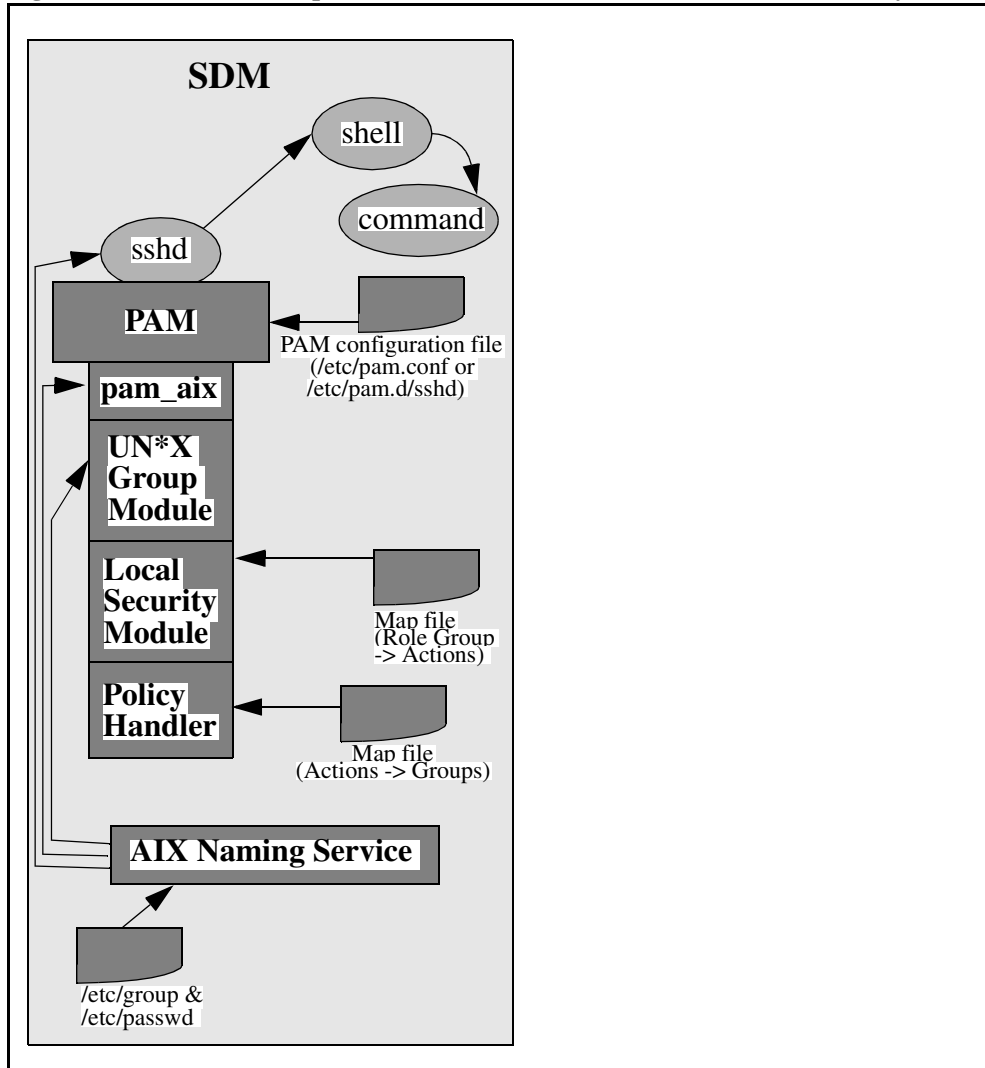
This feature is designed to support SDM integration with IEMS. It provides the following security functionality:

- Utilize the centralized security management of IEMS to provide Authentication, Authorization, Accounting functions.
- Support PAM on SDM to allow AAA via IEMS.
- Allow local emergency access when communication to IEMS is down.
- Support AAA through local security management when IEMS is not part of the SDM deployment.
- Enable access control based on user authorization.

The following two figures show the two deployment scenarios for user authentication/authorization.

Figure 1 Functional Components (with Centralized Security Server - IEMS)

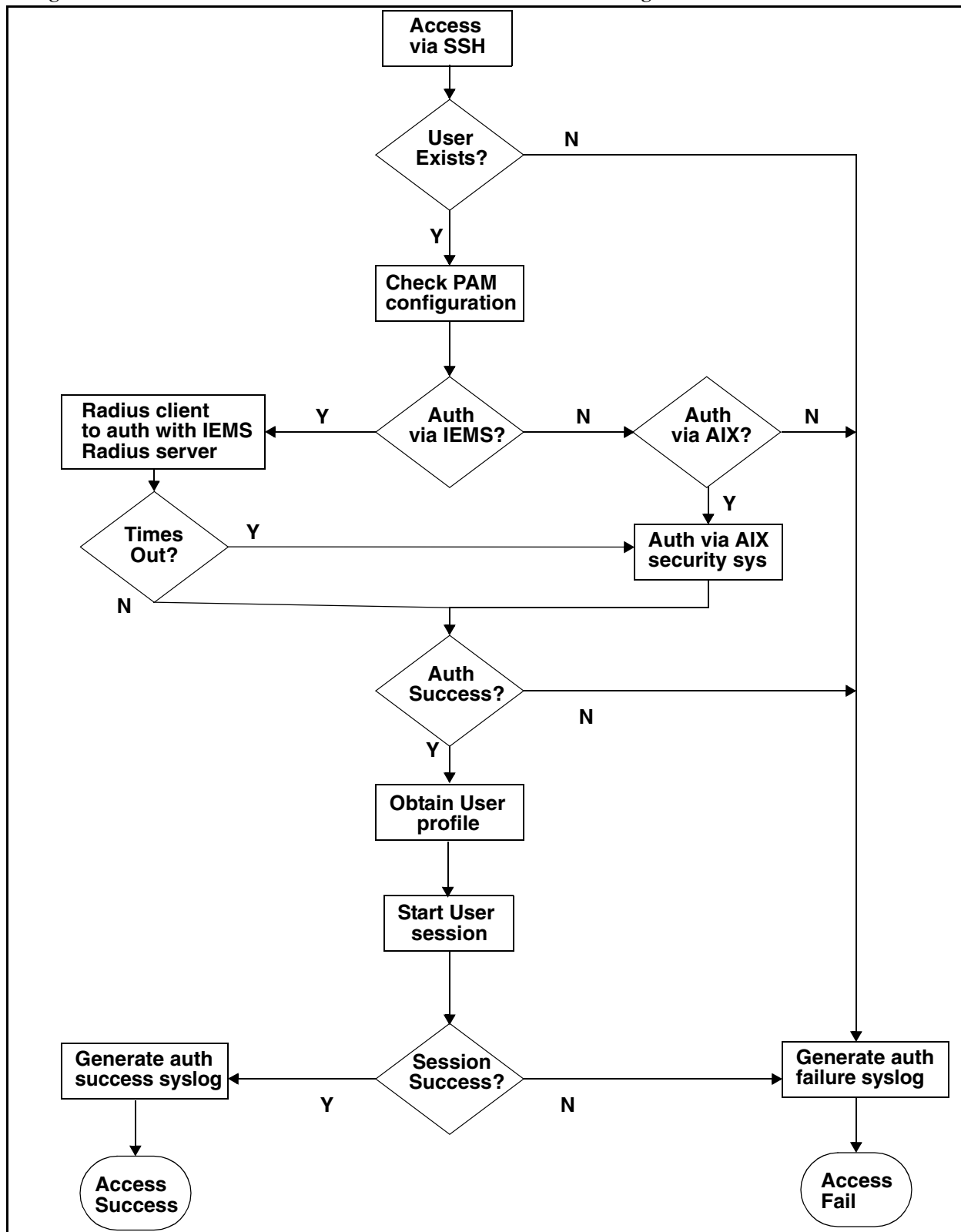
The above figure shows the users are authenticated remotely by a central security server (Centralized Authentication): SDM users are authenticated by a RADIUS server running on an IEMS server.

Figure 2 Functional Components (Standalone SDM without External Security Server)

The above figure shows users are authenticated locally on an SDM (Standalone SDM): There is no central security server. Users and their authentication/authorization information is stored locally in this case.

The following is a flow chart for user authentication and authorization through SSH.

Figure 3 Flow chart for user authentication and authorization through SSH



Emergency access is needed to address any system issue which impacts user authentication. Based on the different needs for emergency access, it is recommended you use local root user accounts for emergency access for both SDM deployment with IEMS and without IEMS.

The following is an example of emergency access:

- SSH demon is not available. No user will be able to access the system through SSH. The only way for a user to access the system in such a case is through console access with a local root account.

106.3 Hardware Requirements or Dependencies

No new hardware dependency is introduced in this feature for Standalone SDM deployment without a centralized security server.

For SDM deployment with the IEMS centralized security server, IEMS and its hardware dependencies are needed by this feature.

106.4 Software Requirements or Dependencies

No new software dependency is introduced in this feature for Standalone SDM deployment without a centralized security server.

For SDM deployment with the IEMS centralized security server, IEMS and its software dependencies are needed by this feature.

The following is the list of third party open source software that are used by this feature. The copyright notices and the acknowledgment for each software must be included in the documentation and/or other materials provided with the SDM product distribution.

- OpenSSL
- OpenSSH
- Linux-PAM
- pam-aix module

OpenSSL License

```
/* =====
 * Copyright (c) 1998-2001 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).
*
*/

```

Original SSLeay 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 routines 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.]
*/

```

OpenSSL Acknowledgment:

"This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)."

=====

OpenSSH License

```

* Copyright (c) 1999, 2000, 2001 Markus Friedl. All rights reserved.
* Copyright (c) 1999 Theo de Raadt. All rights reserved.
* Copyright (c) 1999 Niels Provos. All rights reserved.
* Copyright (c) 1999 Dug Song. All rights reserved.
* Copyright (c) 1999 Aaron Campbell. 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.
*
* THIS SOFTWARE IS PROVIDED BY THE AUTHOR "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 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.

```

```
=====
===
```

Linux-PAM Copyright

Redistribution and use in source and binary forms of Linux-PAM, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.
2. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU General Public License, in which case the provisions of the GNU GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential conflict between the GNU GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED "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(S) 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.

```
=====
===
```

pam-aix module License

```
/*
 * Copyright 2001 University of Illinois Board of Trustees
 * Copyright 2001 Mark D. Roth
 * All rights reserved.
 *
 * pam_aix.c - PAM module for legacy AIX authentication
 *
 * Mark D. Roth <roth@uiuc.edu>
 * Computing and Communications Services Office
 * University of Illinois at Urbana-Champaign
 */
```

106.5 Limitations and restrictions

- When an SDM user account is created on IEMS, the user account also needs to be added on each SDM via an SDM script/command (enableIEMSUser).

- User password expiry warning is only available on IEMS.
- When an SDM is changed from a standalone configuration to a centralized IEMS security server configuration, some of the exiting local user accounts on the standalone SDM need to be manually migrated to the IEMS server.
- Console/telnet login is only available for authorized user accounts that exist locally on a SDM. In addition, a user login through console/telnet will not get her/his role groups translated to command groups.
- A user can only su (change user) to a local user account. In addition, a user login through su will not get her/his role groups translated to command groups.
- SSH/SFTP login through a public key will not go through PAM authentication, as a result, an SSH/SFTP user login using a key will not get their command groups set based on the role groups she/he has, and the home directory will not be created automatically upon login. The administrator will have to set the command groups and create the home directory on every SDM for every user using key authentication.

106.6 Interactions

106.6.1 Changes to Network Connectivity Applications

The following table shows the impact of this feature on network connectivity applications.

Table 1 Network Connectivity Applications

Application	Current Release	SN08	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	Disable	Y	N
FTP	Enable	Disable	Y	N
Login	Enable	Disable	Y	N
Console access	Enable	Enable	N	N
su	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.

By default, a non-anonymous FTP will be disabled and an anonymous FTP will be enabled after an SDM is freshly installed with SN08 software. It is strongly recommended that the customers turn the anonymous FTP service OFF through sdmmtc for security purpose after the installation.

The Telnet service could be enabled or disabled during the fresh installation of an SDM. It is strongly recommended that the Telnet service be disabled. Customers are encouraged to use SSH instead of Telnet.

FTP and Telnet services will be kept as they were after an SDM is upgraded to SN08 software from a previous release. It is strongly recommended that the administrators on the customer sites change the configuration to turn these services OFF through sdmmtc.

When a network connectivity service is not integrated to work with a central security server, the service can only permit access to users who have accounts locally on an SDM.

106.7 Glossary

Table 2

Term	Description
AAA	Authentication, Authorization, Accounting
CBM	Core and Billing Manager
IEMS	Integrated Element Manager System
LDAP	Light-weight Directory Access Protocol
MFT	Management Framework Technology
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

107: A00007491 Functional description (FN)

107.1 Feature name

SuperNode Data Manager (SDM) File Integrity Audit.

107.2 Description

This feature monitors the files on the SDM and records file change events to log files. File change events will be logged to one of two log files, auditlog, and securitylog. File changes resulting from regular configuration changes will be recorded in the auditlog file. File changes which are abnormal, will be recorded in the securitylog file.

Examples of abnormal file changes would include:

- changes to executable files, not as a result of software delivery
- changes to configuration files, not done by the appropriate SDM configuration tools/commands.
- file changes by the root user.

Changes to files resulting from the application of an authenticated software delivery (patch or fileset) will not result in an audit or security log per file. One audit log will be created indicating the name of authenticated patch or package which was applied.

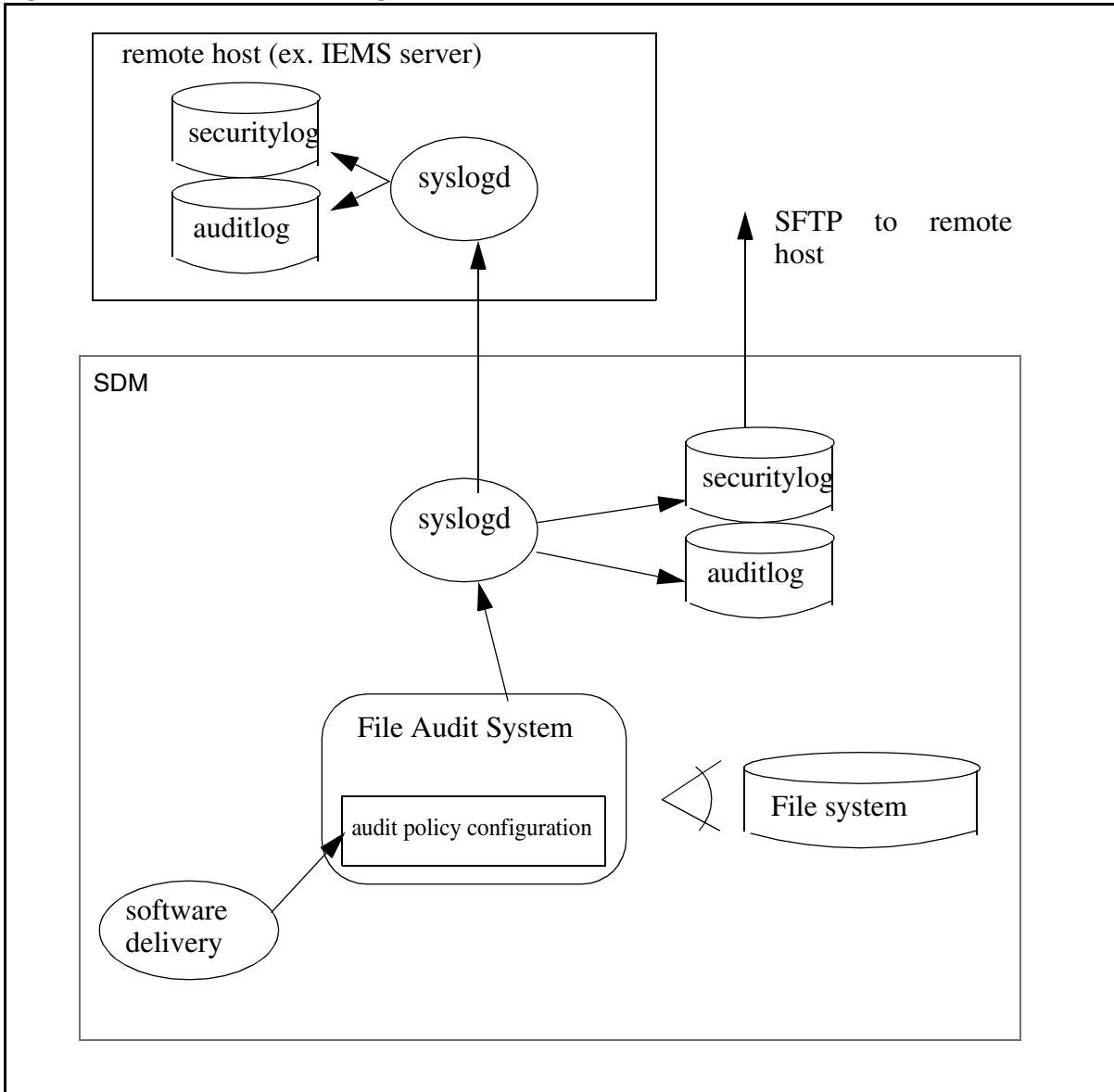
Each audit or security log will contain the following information:

- time of event
- event name (file change)
- login username of the person who changed the file
- complete file name, included the full path

The SDM file audit system utilizes the native AIX audit system, which is a part of the operating system. File change events are detected in real time, not as a result of a periodic comparison.

The audit and security log files will be rotated daily, and kept for one week. The disk storage space for the audit and security logs is monitored, and is alarmed if it exceeds a 70% full threshold. If desired, the files can be securely transferred to a remote host using SFTP (secure file transfer protocol).

In addition to the auditlog and security log files, the logs can also be forwarded in real time to a remote host which supports the UNIX syslog system.

Figure 1 Functional Behavior Diagram

107.3 Hardware Requirements or Dependencies

None.

107.4 Software Requirements or Dependencies

This feature will be distributed in the SN08 release.

107.5 Limitations and restrictions

The set files which are monitored are specified in the SDM software load. While this list will be updated as part of software delivery (patch etc.), there is

no tool provided to manually update the list of monitored files. It is not expected that the customer will add files to the SDM outside the application of authenticated Nortel software updates. Although it would be possible for a user with security administration privileges to change the audit system configuration by editing a configuration file with “vi”, the practice should not be encouraged.

The mechanism to send audit and security logs to a remote host in real-time (syslogd) does not encrypt the log stream, therefore it cannot be considered secure.

107.6 Interactions

This feature does not impact other SDM features.

107.7 Applicable customer facing sections

Fault Management

Logs __X__

Alarms __N/A__

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__

107.8 Glossary

Table 1

Term	Description
syslog	logging system present on UNIX platforms

108: A00007492 Functional description (FN)

108.1 Feature name

SDM User Group Improvements. This feature is part of the SDM21/SN08 release.

108.2 Description

A number of SDM 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 SDM maintenance procedures¹, except for procedures which require console access².

Currently there are only two authorization levels on the SDM: 1) the *root* user and 2) users belonging to the *maint* group. In SN08 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 in SN08, it will be possible to extend this feature in future releases and add additional groups.

The following table has a general summary of the SDM maintenance functions and the required authorization level.

Table: 1 Summary of Authorization Levels

Function	Root	emsadm	secadmin	maint
Initial system installation	*			
Application software install	*	*		
Application software upgrade	*	*	*	*
System upgrade	*			
User Administration (create users, add users to groups, etc.)	*		*	

¹Initial installation of an SDM will still require the use of the root account

²This restriction is documented in the companion feature A00007489. The new user groups are available via ssh access only and are not supported via the console or telnet.

Table: 1 Summary of Authorization Levels

Function	Root	emsadm	secadmin	maint
Application Configuration (effect out of service)	*	*		
Application Configuration (no service effect)	*	*	*	*
Application State Change	*	*	*	*
Data Access	*	*	*	*
view security logs	*		*	
Backup	*	*	*	*

This feature will extend the SDM 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 too
- create / remove users
- add/delete user to group.

Figure 1 Example Screen: SDM user administration

```

***      CON  512  NET  APPL  SYS  HW  CLI: SNM0
ISTb     .    ..   .   ISTb  ISTb  ISTb  Host: wcary2p3
          ..                               Fault Tolerant

User
0 Quit
2
3 PassThru  Role Groups          Users
4           maint                joe, bradly,...
5           secadm               Joe, patrick
6           emsadm               bradly, mark, brenda,...
7
8
9
10
11                      Role Groups: 1 to 3 of 3
12 Up
13 Down
14
15
16
17 Help
18 Refresh .
   root
Time 16:28 >

```

Figure 2 Example Screen: SDM user display

```

SDM      CON  512  NET  APPL  SYS  HW  CLI: SNM0
ISTb     .    ..    .    ISTb  ISTb  ISTb Host: hostname
                               Fault Tolerant
User
0 Quit
2
3 PassThru
4
5
6
7
8
9
10
11
12 Up
13 Down
14
15
16
17 Help
18 Refresh .
root
Time 16:28 >

```

Users	Groups
Bob	secadmin
Brad	secadmin, emsadm, maint
Brenda	emsadm, maint
joe	maint
mark	maint
patrick	maint

Users: 1 to 6 of 6

Table 2: SDM Command Authorization Summary

SDM Tool	Level	Commands	Description	Old auth. level	New auth. level
sdmmtc				maint	maint
	Mtc		Enter the maintenance level	maint	maint
	Mtc>Con		Enter the SDM connectivity status levels.	maint	maint
	Mtc>Con>DS512		Go to the DS512 connectivity level.	maint	maint
	Mtc>Con>DS512	Logs	Display the last DS512 event reported .	maint	maint
	Mtc>Con>DS512	Tst	Test the service DS512 link(s)	maint	maint
	Mtc>Con>DS512	Change	Change DS512 connectivity options	root	emsadm
	Mtc>Con>X25		Go to the X25 connectivity level.	main	maint

Table 2: SDM Command Authorization Summary

SDM Tool	Level	Commands	Description	Old auth. level	New auth. level
	Mtc>Con>X25	Logs	Display the last X.25 event reported	main	maint
	Mtc>Con>X25	Daemon	Control X.25 daemon.	root	emsadm
	Mtc>Con>Eth		Go to the Ethernet connectivity level.	maint	maint
	Mtc>Con>Eth	Logs	Display the last event reported on each of the Ethernet connection status indicators.	maint	maint
	Mtc>Con>Eth	Change	Change an ethernet interface.	root	emsadm
	Mtc>Con>Eth	Add	Add a new ethernet interface or monitored node.	root	emsadm
	Mtc>Con>Eth	Delete	Delete an ethernet interface or monitored node.	root	emsadm
	Mtc>Con>Eth	Period	Display or change the default ping period.	root	emsadm
	Mtc>Con>Eth	Failures	Display or change the max number of ping failures before the ethernet switches active domain.	root	emsadm
	Mtc>Con>Eth	Timeout	Display or change the max timeout before ping failure.	root	emsadm
	Mtc>Net		Enter the Network connectivity status level.	maint	maint
	Mtc>Net>Core		Go to the Core level.	maint	maint
	Mtc>Net>Core	Add	Add a communication path to the Core.	root	emsadm
	Mtc>Net>Core	Change	Change the values for the given communication path to the Core.	root	emsadm
	Mtc>Net>Core	Delete	Delete the given communication path to the Core.	root	emsadm
	Mtc>Net>Nodes		Go to the Nodes level.	maint	maint
	Mtc>Net>Nodes	Add	Add a node.	root	emsadm
	Mtc>Net>Nodes	Change	Change a node.	root	emsadm
	Mtc>Net>Nodes	Delete	Delete a node.	root	emsadm
	Mtc>Net>Nodes	Primary	Configure the primary node.	root	emsadm
	Mtc>Net>Nodes	Monitor	Toggle monitoring of a node.	root	emsadm

Table 2: SDM Command Authorization Summary

SDM Tool	Level	Commands	Description	Old auth. level	New auth. level
	Mtc>Net>DCE		Go to the DCE level.	maint	maint
	Mtc>Net>DCE	Add	Add DCE component(s)	root	emsadm
	Mtc>Net>DCE	Delete	Delete DCE components(s)	root	emsadm
	Mtc>Net>DCE	Logs	Display the last DCE event reported (if any).	root	emsadm
	Mtc>Net>NTP		Go to the NTP level.	maint	maint
	Mtc>Net>NTP	Query	Display the details of an NTP server.	maint	maint
	Mtc>Net>NTP	Logs	Display the last NTP event reported (if any).	maint	maint
	Mtc>Net>NTP	Add	Add NTP server(s) and peer(s)	root	emsadm
	Mtc>Net>NTP	Change	Change NTP server/peer.	root	emsadm
	Mtc>Net>NTP	Delete	Delete NTP server(s) and peer(s)	root	emsadm
	Mtc>Appl		Enter the software applications status level.	maint	maint
	Mtc>Appl	logs	Display the last event reported (if any) on each of the application status indicators.	maint	maint
	Mtc>Appl	Bsy	Busy an application.	maint	maint
	Mtc>Appl	RTS	Return an application to service.	maint	maint
	Mtc>Appl	OffL	Offline an application.	maint	maint
	Mtc>Sys		Enter the operating system software status level.	maint	maint
	Mtc>Sys>Storage		Enter the STORAGE system status level.	maint	maint
	Mtc>Sys>Storage	ESDAdd	Add the /swd/sdm/esd logical volume for upgrades from disk.	root	emsadm
	Mtc>Sys>Storage	ESDDel	Remove the /swd/sdm/esd logical volume and all its' contents.	root	emsadm
	Mtc>Sys>Storage	Add	Add new disks to the datavg volume group, OR add a new logical volume.	root	emsadm

Table 2: SDM Command Authorization Summary

SDM Tool	Level	Commands	Description	Old auth. level	New auth. level
	Mtc>Sys>Storage	Change	Change the alarm threshold for a system software status indicator, OR expand the size of an existing logical volume.	maint	maint
	Mtc>Sys>Backup Clear		Clears the Backup Status and alarm.	maint	maint
	Mtc>Sys>Audit Clear		Clears the System Audit Status and alarm.	maint	maint
	Mtc>Hw		Enter the hardware status level.	maint	maint
	Mtc>Hw	logs	Display the last event reported (if any) on each of the hardware status indicators.	maint	maint
	Mtc>Hw	Bsy	Busy a hardware device.	maint	maint
	Mtc>Hw	RTS	Return a hardware device to service.	maint	maint
	Mtc>Hw	Add	Add a new hardware module to the system.	root	emsadm
	Mtc>Hw	Delete	Delete a hardware module from the system.	root	emsadm
	Mtc>Hw	Upgrade	Upgrade an MFIO.	root	emsadm
	Mtc	Quit	Quit the current level or exit the SDM maintenance interface.	maint	maint
	Mtc	Bsy	Busy the SDM.	maint	maint
	Mtc	RTS	Return the SDM to service.	maint	maint
	Mtc	OffL	Offline the SDM.	maint	maint
	Mtc	QuerySDM	Query information about the SDM.	maint	maint
	Mtc	Locate	Determine location of SDM modules and devices	maint	maint
	Mtc	Help	Displays help for a single command or all valid	maint	maint
	Mtc	Refresh	Refresh the current screen.	maint	maint
	Admin		Enter the system administration level.	maint	maint
	Admin>User		Enter the user administration level.	maint	maint

Table 2: SDM Command Authorization Summary

SDM Tool	Level	Commands	Description	Old auth. level	New auth. level
	Admin>User>PassThru		Go to PassThru level.	maint	maint
	Admin>User>PassThru	Change	Change a PassThru user.	root	secadm
	Admin>User>PassThru	Add	Add a new PassThru user.	root	secadm
	Admin>User>PassThru	Delete	Delete a PassThru user.	root	secadm
	Admin>User	Add	Add a new maintenance class user id.	root	secadm
	Admin>User	Delete	Delete a maintenance class user id.	root	secadm
	Admin>User	Change	Change the password for the user specified.	root	secadm
	Admin>Backup		Enter the tape backup and restore level.	root	maint
	Admin>Restore		Begin a full system restore.	root	root
	Admin>SWIM		Enter the software inventory management level.	maint	maint
	Admin>SWIM>Apply		Enter the apply SDM software updates level.	root	emsadm
	Admin>SWIM>Apply	Reload	Reload the list of filesets from the current source.	root	emsadm
	Admin>SWIM>Apply	Source	Choose a source tape drive or directory from which to load filesets.	root	emsadm
	Admin>SWIM>Apply	Eject	Ejects the tape in the current tape drive or the given tape drive.	root	emsadm
	Admin>SWIM>Apply	Select	Selects a fileset.	root	emsadm
	Admin>SWIM>Apply	Apply	Apply filesets on this SDM.	root	emsadm
	Admin>SWIM>Apply	Upgrade	Upgrade all filesets to the latest versions available on the source.	root	emsadm
	Admin>SWIM>Apply	QueryTape	Query the SDM release information from the tape.	root	emsadm
	Admin>SWIM>Apply	Search	Search the list for the given text	root	emsadm

Table 2: SDM Command Authorization Summary

SDM Tool	Level	Commands	Description	Old auth. level	New auth. level
	Admin>SWIM>Apply	Filter	Toggle between showing the software description and the software fileset name.	root	emsadm
	Admin>SWIM>Apply	CD:	Change to the given directory.	root	emsadm
	Admin>SWIM>Apply	View	Toggle between showing the software description and the software fileset name.	root	emsadm
	Admin>SWIM>Details		Enter the software details level.	maint	maint
	Admin>SWIM>Details	Select	Selects a fileset.	maint	maint
	Admin>SWIM>Details	Remove	Remove software.	root	emsadm
	Admin>SWIM>Details	Search	Search the list for the given text	maint	maint
	Admin>SWIM>Details	Filter	Filter the list of software.	maint	maint
	Admin>SWIM>Details	View	Toggle between showing the software description and the software fileset name.	maint	maint
	Admin>SWIM>Fixes		Enter the software fixes level.	root	emsadm
	Admin>SWIM>Fixes	Reload	Reload the list of filesets from the current source.	root	emsadm
	Admin>SWIM>Fixes	Source	Choose a directory from which to load filesets.	root	emsadm
	Admin>SWIM>Fixes	Sched	Set up a scheduled time in which the Fix Auto Apply would execute.	root	emsadm
	Admin>SWIM>Fixes	Apply	Apply filesets on this SDM.	root	emsadm
	Admin>SWIM>Fixes	Filter	Filter the list of software.	root	emsadm
	Admin>SWIM>Fixes	View	Toggle between showing the software description and the software fileset name.	root	emsadm

Table 2: SDM Command Authorization Summary

SDM Tool	Level	Commands	Description	Old auth. level	New auth. level
	Admin>SWIM>Config		Enter the software configuration level.	maint	maint
	Admin>SWIM>Config	Select	Selects a fileset.	maint	maint
	Admin>SWIM>Config	Config	Configure filesets.	root	emsadm
	Admin>SWIM>Config	Filter	Filter the list of software.	maint	maint
	Admin>SWIM>Config	View	Toggle between showing the software description and the software fileset name.	maint	maint
	Admin>SWIM>Options		Enter the options level.	maint	maint
	Admin>SWIM>Options	Change	Change default values for SWIM.	root	emsadm
	Admin>SWIM>History		Enter the software history level.	maint	maint
	Admin>SWIM>History	ViewLog	View the log for the given history entry.	maint	maint
	Admin>SWIM>Query Tape		Select the tape drive you wish to query	maint	maint
	Admin>Access		Enter the Telnet access control level.	maint	maint
	Admin>Access	Change	Change SDM access settings	root	emsadm
	Admin>Time		Display & modify the date and time.	maint/ root	maint
	Admin>TimeZone		Adjust Daylight Savings Time values.	maint	maint
	Admin>TimeZone	Change	Change the Time Zone.	root	emsadm
sdmconfig	sdmconfig		Enter the system commissioning level.	maint	maint
	sdmconfig	Add	Add an entry for this commissioning step.	root	emsadm
	sdmconfig	Change	Change an entry or the commissioned values for the current commissioning step.	root	emsadm

Table 2: SDM Command Authorization Summary

SDM Tool	Level	Commands	Description	Old auth. level	New auth. level
	sdmconfig	Delete	Delete an entry for this commissioning step.	root	emsadm
	sdmconfig	Step	Jump to the given commissioning step number.	maint	maint
	sdmconfig	List	List all of the available commissioning steps.	maint	maint
	sdmconfig	Next	Go to the next commissioning step.	maint	maint
	sdmconfig	Prev	Go to the previous commissioning step.	maint	maint
	sdmconfig	Up	Scroll up through the list.	maint	maint
	sdmconfig	Down	Scroll down through the list.	maint	maint
	sdmconfig	LogQuery	Invoke the logquery tool to browse DMS logs.	maint	maint
billmtc			Enter billing maintenance level.	maint	maint
	CONFSTRM		Enters CONFSTRM level	maint	maint
	CONFSTRM	Add	Configures a new stream	maint	maint
	CONFSTRM	Change	Changes an existing stream configuration	maint	maint
	CONFSTRM	Delete	Deletes a stream	maint	maint
	CONFSTRM	List	Lists configuration of a (or all) stream(s)	maint	maint
	CONFSTRM	Act	Activates a filtered stream	maint	maint
	CONFSTRM	Deact	Deactivates a filtered stream	maint	maint
	CONFSTRM	Update	Updates a filtered stream's criteria.	maint	maint
	CONFSTRM	Start	Resume receiving records on a filtered stream.	maint	maint
	CONFSTRM	Stop	Stop receiving records on a filtered stream.	maint	maint
	APPL		Enters the APPL level	maint	maint
	APPL>AFT		Enters AFT level	maint	maint
	APPL>AFT>AFT-CONFIG		Enters AFT Session configuration level	maint	maint

Table 2: SDM Command Authorization Summary

SDM Tool	Level	Commands	Description	Old auth. level	New auth. level
	APPL>AFT>AFT-CONFIG	Add	Add AFT tuples to the MIB.	maint	maint
	APPL>AFT>AFT-CONFIG	Delete	Delete AFT tuples from the MIB.	maint	maint
	APPL>AFT>AFT-CONFIG	Change	Change number of retry attempts for a session.	maint	maint
	APPL>AFT>AFT-CONFIG	List	List AFT tuples in the MIB.	maint	maint
	APPL>AFT>	Query	Query info on file transfer lists for sessions.	maint	maint
	APPL>AFT>	Setfile	Set an override file, delete a file from the list.	maint	maint
	APPL>AFT>	Rsetfile	Reset a file from partial to pending.	maint	maint
	APPL>AFT>	AFTRESND	Enters AFT resend level	maint	maint
	APPL>AFT>	Start	Start an AFT session that was stopped.	maint	maint
	APPL>AFT>	Stop	Stop an AFT session file transfer.	maint	maint
	APPL>AFT>	Alarm	Query or cancel AFT session alarms.	maint	maint
	APPL>AFT>SFP		Enters SFP level	maint	maint
	APPL>AFT>SFP	Query	Queries the SFP status	maint	maint
	APPL>AFT>SFP	Act	Activates SFP	maint	maint
	APPL>AFT>SFP	Deact	De-activates SFP	maint	maint
	FILESYS		Enters FILESYS level	maint	maint
	FILESYS	Sendfile	Sends billing file(s) per stream to downstream	maint	maint
	FILESYS	Listfile	Lists stored billing file(s) per stream	maint	maint
	FILESYS	Closec	Closes currently open billing file(s) per stream	maint	maint
	SCHEDULE		Enters SCHEDULE level	maint	maint
	SCHEDULE	Add	Adds a tuple to the schedule	maint	maint
	SCHEDULE	Change	Changes a tuple in the schedule	maint	maint

Table 2: SDM Command Authorization Summary

SDM Tool	Level	Commands	Description	Old auth. level	New auth. level
	SCHEDULE	Delete	Deletes tuple(s) from the schedule	maint	maint
	SCHEDULE	List	Lists tuple(s) in the schedule	maint	maint
	SCHEDULE>RTB		Enters RTB level	maint	maint
	SCHEDULE>RTB	Rts	Returns RTB to service for a stream.	maint	maint
	SCHEDULE>RTB	Bsy	Busies RTB for a stream.	maint	maint
	SCHEDULE>RTB	Offl	Offlines RTB for a stream.	maint	maint
	SCHEDULE>RTB	Query	Queries the state of RTB for a stream.	maint	maint
	SCHEDULE>RTB	IPTest	Tests the IP address used by RTB for a stream.	maint	maint
	SCHEDULE>RTB	CONFRTB	Enters the RTB configuration level.	maint	maint
	TOOLS		Enters TOOLS level	maint	maint
	TOOLS	Amadump	Displays record information	maint	maint
	TAPE		Enters TAPE level	maint	maint
	TAPE	Write	Write billing files to DAT tape	maint	maint
	TAPE	List	List billings files on a DAT tape	maint	maint
	TAPE	Send	FTP billings files from a DAT tape	maint	maint
	billmtc	Set	Sets context	maint	maint
	billmtc	Query	Displays current state of streams	maint	maint
	billmtc	Clli	Displays core CLLI	maint	maint
	billmtc	Mib	Sets and gets MIB objects	maint	maint
	billmtc	Dispal	Displays all current SDM alarms	maint	maint
	billmtc	Displogs	Displays logs not yet sent to CM	maint	maint

108.3 Hardware Requirements or Dependencies

There are no hardware requirements for this feature.

108.4 Software Requirements or Dependencies

This feature is dependent on feature A00007489 (IEMS Integration).

108.5 Limitations and restrictions

No user interface is provided to create additional authorization levels.

108.6 Interactions

This feature will change the RMI for user creation.

108.7 Glossary

Term	Description
CBM	Core and Billing Manage
IEMS	Integrated Element Manager System
MS	Management System
NE	Network Element
NE/MS	NE or MS
RMI	Resource Manager Interface
SDM	Super Node Data Manager

109: A00007541 Functional description (FN)

109.1 Feature name

NGSS XML Framework

109.2 Description

Feature A00007541, NGSS XML Framework, was created to provide a generic XML processing environment on the NGSS. Specifically, this framework is expected to be used by the Session Policy Controller (SPC) component, however, this activity is meant to be general and useful for any NGSS application.

XML (<http://www.w3.org/TR/REC-xml/>), originally derived from SGML, is a very simple text-based way to represent structured data. Like SGML, it relies on markup tags to delimit content. To use XML data programmatically, several standard APIs have been developed. The first, defined by the W3 Commission at <http://www.w3.org/DOM>, is called the Document Object Model (DOM). The DOM allows the parsing of XML text into a tree-like structure, as well as the inverse, building XML documents from tree structures. The second standard API, Simple API for XML (SAX), was developed iteratively on internet mailing lists. Its definition is now hosted at <http://www.saxproject.org>. SAX is a lighter-weight API that uses a callback interface to allow its users to build their own structures from select XML text. The DOM, by contrast, parses an entire XML text into a tree.

The content of an XML document can be strictly defined using either a Document Type Declaration (DTD) or by an XML Schema (<http://www.w3.org/XML/Schema>). If either a DTD or a Schema exist for a given XML document, its content can be validated against the definition.

Any XML toolkit should support some version of the DOM and SAX APIs, as well as provide support for validating XML documents against DTDs and XML Schema definitions.

This activity will consist of choosing a third party XML toolkit that fits the needs of NGSS applications.

109.3 Hardware Requirements or Dependencies

This activity will introduce a new third-party software package to the NGSS platform. No new hardware dependencies are introduced.

109.4 Software Requirements or Dependencies

No new software dependencies are introduced by this activity.

109.5 Limitations and restrictions

This activity does not introduce any user-visible functionality. It provides a library that may be used by other applications -- those applications may have user visible functions.

109.6 Interactions

As stated above, this activity is introducing a completely new software library to the NGSS. This library, by itself, does not affect the end user.

109.7 Glossary

Table 1 Common Terms

Term	Description
XML	eXtensible Markup Language. http://www.w3.org/TR/REC-xml/
DOM	Document Object Model, http://www.w3.org/DOM
SAX	Simple API for XML. XML parsing API. http://www.saxproject.org
DTD	Document Type Definition. Defined in the XML specification
XML Schema	Alternative to DTD. http://www.w3.org/XML/Schema

111: A00007548 Functional description (FN)

111.1 Feature name

SN08 PacketCable Electronic Surveillance

111.2 Description

111.2.1 Background

CableLabs is a consortium of cable operators and cable equipment vendors that creates specifications for cable access VoIP. CableLabs' PacketCable project promotes vendor inter-operability. In order to provide a billing capability, PacketCable has defined a specification for an event reporting mechanism that is called "PacketCable Event Messaging" (PCEM). PCEM uses RADIUS accounting (RFC 2866) to deliver event messages to a record keeping server (RKS). Activity A00007196 (Packet Cable Event Messaging For Accounting SN08) provides an implementation of PCEM for the Succession Cable Solution.

PacketCable has also defined a specification for a lawful interception mechanism called "PacketCable Electronic Surveillance" (PCES). PCES and PCEM use an overlapping set of event messages, and use Radius accounting to send event messages.

This feature delivers a PacketCable-compliant Lawful Interception solution for the Call Server 2000 (CS2K) Cable VoIP Solution. It implements PacketCable surveillances, which consist of Call Data and if required Call Content for monitored calls.

This development activity is one component of Nortel's development effort to support "Packet Cable 1.5" compliance in the Succession Cable Solution.

This activity provides CMS PacketCable 1.5 compliance with PCES for PacketCable, specifically for the Lawful Interception component of event messaging CableLabs specification PKT-SP-EM-I10. The interface to the LEA is provided by the third-party DF component (as described below). The DF must be compliant to PacketCable specification PKT-SP-ESP-I03-040113.

111.2.2 Electronic Surveillance Implementation

Figure 1 illustrates PCES with respect to the components of the CS2K PacketCable solution. For PCES events which are detected by the CS2K, event notifications are sent to the Event Message Delivery Interface (EMDI), which sends PCES Event Messages (PCES EMs) to the DF, which in turn multicasts it to the LEA collection functions as required.

The CMTS sends PCES event messages directly to the DF. Call Content is sent directly to the DF by the Trunk GW and CMTS.

The EMDI (Event Messaging Delivery Interface) encapsulates the capability of formatting event messages with RADIUS headers and sending to the RKS (including retries). For this activity, the EMDI is provided by the IAA (Integrated Accounting Application) on the CBM. The IAA may also receive event messages from the GWC for ES (Electronic Surveillance).

The DF (Delivery Function) is third-party equipment provided by any DF vendor. The DF receives event messages from the EMDI, the CMTS, and the trunk gateway.

The PacketCable architecture refers to two network elements that are not labeled in Figure 1: the CMS and the MGC. The CMS, or call management server, is PacketCable's line solution. Nortel implements the CMS by using functionality in the CM and small-lines GWCs. The MGC, or media gateway controller (not to be confused with our GWC), is PacketCable's trunk solution. Nortel implements the MGC using the CM and trunk GWCs controlling TGCP trunk gateways.

USNBD is an existing CS2K Cable Solution lawful interception feature. PCES shares much functionality with USNBD, and in order to avoid duplication, the reader is referred to the USNBD NTPs for a description of certain functionality.

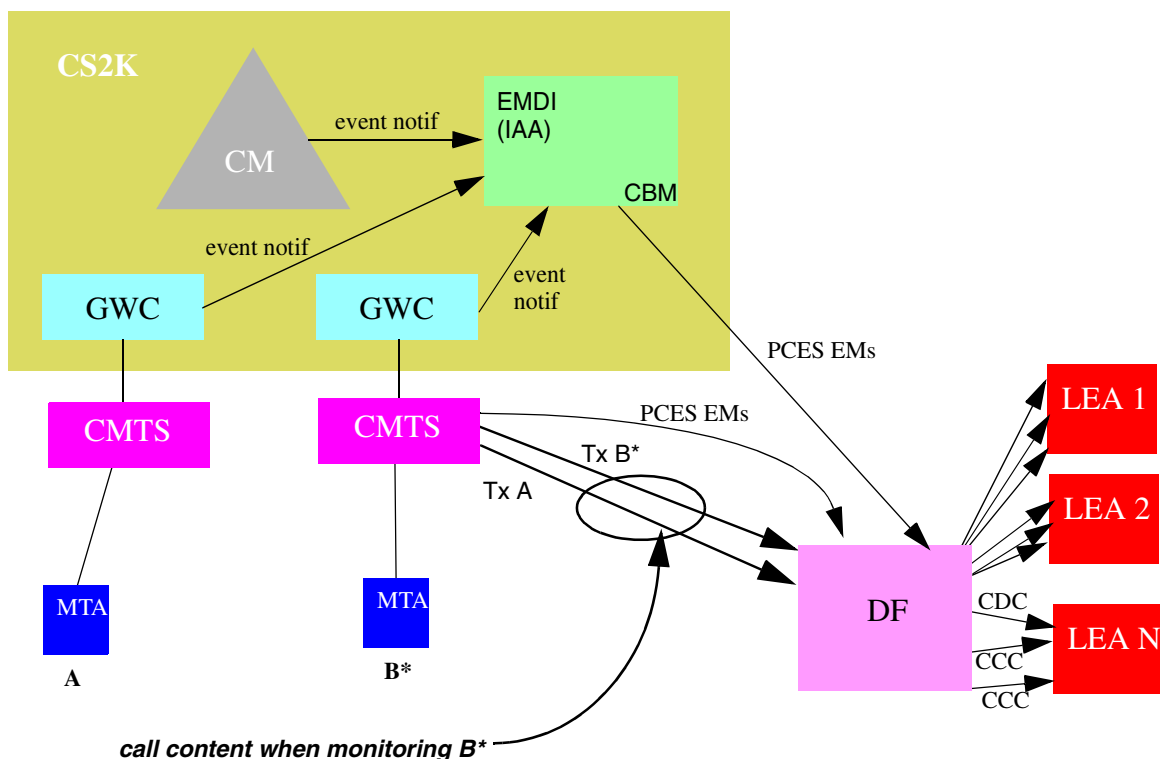
Table 1 Existing USNBD documentation

Number	Title
NN10264-709	Lawful Intercept
NN10190-113	Succession Performance Management: Operational Measurements Reference
NN10345-501	Configuration Management: Lawful Intercept Service
NN10300-100	IP Solutions Basics
NN10188-511	Communication Server 2000 Configuration Management

PCES has some common functionality with USNBD, and the existing USNBD documentation may be useful. ("Table 1 Existing USNBD documentation")

PCES cannot be used in the CM concurrently with USNBD, so the logs apply to the surveillance feature which is currently active in the CS2K. In order to avoid duplication, the reader is referred to the USNBD NTPs for a description of these logs.

Figure 1 PCES Architecture – subject monitoring



111.3 PCES call monitoring

111.3.1 Event Messages (call data)

Event Messages (PCES EMs) are generated at different points in the call and they contain information which can be used for surveillance purposes and for the purpose of interpreting call content. For example: a signaling_start event message contains the calling and called DNs.

Event messages are generated for each half call. Therefore, separate event messages are generated for the originating and terminating call halves.

111.3.1.1 Message Structure

Refer to the Packet Cable specification PKT-SP-EM-I10 for details regarding the individual components in the Packet Cable event messages.

111.3.1.2 Message Types

Table 2 PacketCable Event Messages

Name	Description
Signaling_Start	Start of signaling for originating or terminating half of the call
Signaling_Stop	End of signaling for originating or terminating half of the call
Database_Query	An inquiry into an external database; for example 800, LNP
QoS_Reserve*	Reservation of QoS bandwidth for originating or terminating half of the call
QoS_Commit*	Commitment of QoS bandwidth for originating or terminating half of the call
QoS_Release*	Release of QoS bandwidth for originating or terminating half of the call
Service_Activation	Indicates a subscriber has activated a service
Service_Instance	Indicates an occurrence of a service
Service_Deactivation	Indicates a subscriber has deactivated a service
Call_Answer	Indicates that all network resources have been allocated for originating or terminating half of the call
Media_Alive	Indicates if the call is still active (Not supported in SN08)
Call_Disconnect	Indicates that all network resources have been released for originating or terminating half of the call
Media_Report	Indicates a change in media session information. (PCES only)
Signal_Instance	Indicates an NCS signal sent from the subject or from the network. (PCES only)
Interconnect_Start	Start of network interconnect signaling (between PacketCable and PSTN) for originating or terminating half of the call
Interconnect_Stop	Stop of network interconnect signaling (between PacketCable and PSTN) for originating or terminating part of the call
Time_Change	Indicates time change on a network element.
*QOS_XXXX messages are generated by the CMTS and sent directly to the DF.	

111.3.2 Call Content

When a surveillance requires call content, the transmit of both agents in the connection is provided to Law Enforcement.

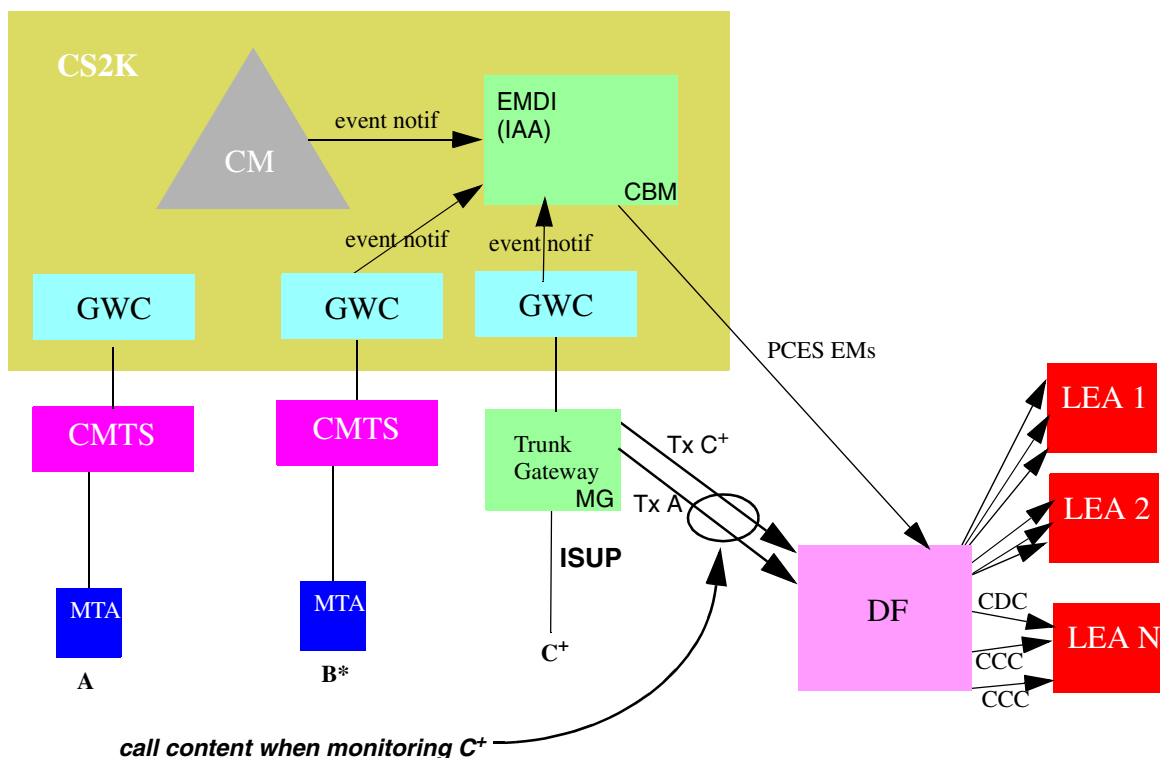
The call content (for both parties) is sent directly from the CMTS or MG to the DF. That is, if the subject B*, hosted on a CMTS, is talking to associate A, the

transmit paths of both the subject B^* and associate A are sent directly from the CMTS hosting B^* to the DF (as shown in Figure 1).

If the subject redirects a call on-net, the call content IAP will be the CMTS of the redirected-to party.

On the other hand, if the call is redirected by the subject to the PSTN and the replacement party (or *observed party*) is C^+ , hosted on a trunk MG, the content (or transmit paths) for C^+ and the associate (A) are sent directly from the MG to the DF. This only occurs when a call is redirected by the subject to the PSTN, so neither C^+ nor A is an actual subject. C^+ is a *monitored replacement party*, or MRP.¹ Figure 2 illustrates the case where A calls subject B^* who forwards the call off-net to C^+ , and the call content IAP is at the trunk MG.

Figure 2 PCES Architecture – MRP monitoring (subject redirects off-net)



Since content multicasting to multiple LEAs is done by the DF, PCES will provide a single call content stream if there is at least one PCES surveillance on an agent in a connection which requires call content.

¹A Monitored Replacement Party (MRP) is a party which replaces the subject through a redirection feature controlled by the subject. This could be caused by F calling subject A^* , and A^* either forwarding or transferring the call to C , which routes through the MG to the PSTN.

111.3.3 Multiple surveillances on a connection

PCES provides call content for a single agent in a connection. If a subject redirects a call to another subject, the resulting call will be monitored for only a single subject. The DF provides multicasting of the content and data to the appropriate LEA Collection Functions.

Consider the following example: Associate A calls subject B* which has call forwarding to subject C*. The resulting call is A – C⁺, where C⁺ is the terminating party.

If either B or C is subject to a call content surveillance, the resulting call will be monitored for content, regardless whether the other surveillance was data-only. Since at least one surveillance requires call content, the resulting call will be monitored for call content.

It is possible to configure a CS2K to support multiple DFs, and it is also possible to provision different surveillances to use different DFs. If B* and C* have surveillances provisioned to use different DFs, the resulting A – C⁺ call will be monitored to use C's DF.

In the future PacketCable architecture may require DFs to communicate with each other so that the surveillance data can be multicast by the DF not only to LEA Collection Functions, but also to other DFs (for example, B's). In the current release of the PacketCable architecture, the mechanisms to permit inter-DF communication are not yet specified. Therefore, it is recommended that only a single DF be provisioned for all surveillances on a CS2K.

If multiple DFs are configured on a CS2K, for purposes of redundancy, it is recommended that only one DF be used at any given time, and all surveillances be provisioned to use it.

111.4 Configuration

PCES requires PCEM to be configured and active, as described in the documentation for activity A00007196 (PacketCable Event Messaging for SN08). However, where PCEM requires an RKS to receive accounting event messages and forward them to billing systems, PCES requires a DF to Electronic Surveillance event messages and call content, and to forward them to LEA Collection Functions (CFs).

In addition to the PCEM configuration, PCES also requires

111.4.0.1 Add DF tuple entries

PCES requires one or more DFs to be provisioned on the CM.

```
> table pcementt
> add DF <df_index> DF <CDC_IP> <CDC_PORT> <CCC_IP> <CCC_PORT>
  <ASSOC_EMDI>
```

For example, to provision a DF using CDC address and port 47.135.41.107:4000, and CCC address and port 47.135.41.107:5000

```
> add DF 3    DF 47 135 41 107 4000 47 135 41 107 5000 0
```

In this example 0 is the index in Table PCEMENTT of the record for the EMDI which will be used to send the event messages to the DF.

111.5 Hardware requirements

The PCES solution requires a PacketCable 1.1 certified network (CMTS, Trunk GW, DF, MTAs).

111.6 Limitations and restrictions

There is no support for PCES and USNBD interworking. USNBD is a CS2K Lawful Interception application.

Either USNBD is the active LI application or PCES is the active LI application. Both cannot be active at the same time.

A maximum of 5 surveillances may be provisioned against a subject. However only a single surveillance can be activate on a subject at any time.

When there is a change to the Line Class Code (LCC) of a DN (*e.g.*, from POTS to RES or *vice versa*), if that DN is the subject of an active surveillance, the surveillance will be deleted. An inactive surveillance will not be deleted.

PCES surveillance will fail if the DF is either not in service or not properly configured on the CS2K.

DOCSIS requires that connections between two endpoints having the same IP address (and hence hosted on the same MTA) must not be routed to the CMTS. Therefore PCES does not provide call content for a connection between two lines on the same MTA. This is due to the fact that the voice stream for intra-MTA calls is locally routed and does not pass through the CMTS (the call content IAP).

111.7 Dependencies

The SOC state of USNBD must be set to ON for PCES SOC to be assigned state ON.

PacketCable Event Messaging (PCEM) must be active on the switch.

111.8 Logs (LG)

All the UNB 300 logs are generated by PCES as they are by USNBD, with the exception of UNB301 (CDC), UNB303 (CCR), and UNB306, which are not generated by PCES. Access to UNB logs is only provided to PCES users through LOGUTIL's OPENSECRET command (no password is required).

LOGUTIL
OPENSECRET UNB

USNBD log reports

- UNB300 - reports problems with USNBD shared resources used by PCES
- UNB302 - reports problems with USNBD processes used by PCES
- UNB304 - reports success and failure of surveillance activation and deactivation, and problems with surveillance activation.

The following is a sample surveillance activation log generated when a surveillance is activated.

```
COMIT_I07CU    UNB304 AUG20 14:15:53 3300 INFO
SURV ACT COMMAND SUCCESSFULLY PROCESSED
SURVEILLANCE HAS BEEN ACTIVATED
SIN: NYPD654
COMMAND ENTERED BY: USERJOE
```

When the line class code of a line changes, an active surveillance on the line will be removed. A UNB304 log will be generated as follows:

```
COMIT_I08AV    UNB304 NOV02 15:20:52 5100 INFO
SUBJECT HAS BEEN DELETED
SURVEILLANCE HAS BEEN DELETED
SIN: 9194303602
AGENCY:
SURV. DEFN.: DN 9194303602 9194303602 N Y N
```

- UNB305- reports problems that affect PCES administration data and reports all user creations and deletions
- UNB306 - Not used by PCES

111.9 Operational Measurements (OM)

Lawful Intercept OMs for group UNBCDC are not used by PCES.

Lawful Intercept OMs for group UNBMISC are used by PCES.

RELCPCY - Register RELCPCY counts the number of monitored calls for which monitoring was stopped because the monitoring capacity is exceeded.

RELNMON - Register RELNMON counts the number of calls for which monitoring was stopped because of non-monitorable features. **All features supported by the CS2K PacketCable solution are monitorable.**

UNBMCALL - Register UNBMCALL counts the number of calls monitored by USNBD. Register UNBMCALL determines the real-time impact monitored calls make on the CM.

111.10 Some differences between PCES and USNBD

111.10.1 Performance management

PCES differs from USNBD functionality described in NN10264-709 (I)SN07 Preliminary 01.01 September, 2004 Succession Performance Management Operational Measurements Reference.

The USNBD feature uses the registers in OM group CF3P to monitor usage of 3-way conference bridges used for combined call content resources (Combined CCRs). As PCES does not provide combined call content, this OM group is never incremented by PCES.

111.10.2 Private Network Interception

USNBD can be configured to provide Private Network Interception, as described in NN10190-113 (Lawful Intercept). PCES cannot be configured to provide call content for connections which reside behind a private NAT.

111.10.3 User classes

USNBD distinguishes between Regular users and Administrative users, who in addition to all Regular operations have the privilege to add and delete USNBD users. PCES does not have separate user classes, and any PCES user can add or delete PCES users.

111.10.4 Agency separation

PCES does not support agency separation. All PCES surveillances are visible to all PCES users.

111.10.5 Bearer Channel Tandeming

PCES does not perform call content interception using Bearer Channel Tandeming (BCT), hence all references to BCT and configuring a UAS for BCT do not apply.

111.10.6 Call Content delivery via CCRs

PCES does not deliver call content to the LEA. Instead, Call Content is delivered by the CMTS or MG to the DF, which forwards call content to the LEAs as required. Consequently there is no provisioning of CCCs, or CCRs for PCES, nor is there any associating CCRs with or disassociating CCRs from a surveillance.

USNBD supports a test call capability in order to test CCRs. Since PCES does not provide the call content delivery directly to the LEA, it does not have CCRs and does not have the capability to test CCR call setup.

111.10.7 Call Data delivery via CDCs

PCES does not deliver call data to the LEA. Instead, Call Data is delivered by the CMTS, and EMDI to the DF, which forwards call data to the LEAs as required. Consequently there is no provisioning of CDCs for PCES, nor is there any associating CDCs with or disassociating CDCs from a surveillance.

111.10.8 In-Band Digit Collection

A USNBD surveillance can be provisioned to provide in-band digit collection. PCES does not provide this capability. In the PacketCable architecture in-band digit collection can be provided by the DF. In order to allow the DF to perform in-band digit collection it is necessary to provide the DF with the call content by provisioning the PCES surveillance as data_content. A properly configured DF can then provide call content or call data to law enforcement as required.

111.10.9 In-band CCC_ID tagging

A USNBD surveillance can be provisioned to provide the CCC_ID tag in-band on the call content channel. PCES does not provide call content directly to the LEA. This functionality could be provided by the DF, but is not discussed in the PacketCable specifications.

111.10.10 Provisioning surveillance

NN10188-511 notes that lawful interception is provisioned on a line using the USNBD feature. This should also reflect that PacketCable-compliant Lawful Interception should be provisioned using PCES instead of USNBD.

111.11 Data schema (DS)

No existing tables are modified and no new tables are introduced by this feature. The DF IP address and port, and the CBM application IP address and port, should be entered in Table PCEMENTT prior to defining surveillances.

111.12 Office parameters (OP)

No new office parameters are introduced as part of this functionality.

111.13 Service orders (SO)

No changes to Service Orders are required by this feature.

111.14 Alarms (AL)

No new Alarms are introduced as part of this functionality.

111.15 Command interface (CI)

111.15.1 New/modified commands

This feature introduces a new CI which is used to provision PacketCable surveillances. Table 3 lists the set of PCES user commands.

Table 3 PCES Commands

CI Command	Description
>PCES	Enter the PacketCable Electronic Surveillance CI
>SURV ADD DN <10-digit DN>	Add a PCES surveillance by DN.
<Case ID>	The case ID is an arbitrary character string (up to 10 characters) which may be used for administrative purposes.
<SIN>	The SIN is an alphanumeric string Surveillance Identification Name (up to 10 digits) which is used to uniquely identify a surveillance, and must be unique across all surveillances.
<Monitor Type>	The Monitor Type specifies whether it is a data-only surveillance (data) or a data-plus-content surveillance (data_content).
<MRP>	The MRP field specifies whether Monitored Replacement Party functionality should be assigned to the surveillance. A Replacement Party is a party which the subject redirects his or her calls to, for example by Call Forwarding. The MRP field must be set to 'Y' since PacketCable 1.1 requires Replacement Parties to be monitored.
<Delivery Function Index>	The Delivery Function Index (or DF Index) is the index of the DF associated with the surveillance. This is the index which was assigned to the DF when it was entered in Table PCEMENTT.
>SURV DEL <sin>	Delete a PCES surveillance by SIN
>SURV LIST <option>; option = {all act inact dn sin}	List PCES surveillance(s)
>SURV ACT <sin>	Activate a PCES surveillance
>SURV DEACT <sin>	Deactivate a PCES surveillance
>USER ADD <user_id>	Define a new PCES user. The user_ID must already be defined as a valid login ID for the CS2K CM (e.g., using the PERMIT command)
>USER DEL <user_id>	Delete a PCES user
>USER LIST ALL	List all PCES users
>HELP <option>; option = {help surv quit user}	PCES CI help

111.15.2 Process of configuring PCES

1. Activate PCEM event messaging
2. SOC on PCES
3. Configure the EMDI in Table PCEMENTT
4. Bring the EMDI into service
5. Configure the DF in Table PCEMENTT

111.15.3 Process of setting up a PCES surveillance

1. Define the surveillance using the SURV ADD command

Example of adding a surveillance:

```
>surv add dn 9194303602 fbi sin123 data_content Y 4
```

Note that in PacketCable terminology the term Surveillance means call data only (data) and Intercept means call data plus call content (data_content).

2. Activate the surveillance using the SURV ACT command

Example of activating a surveillance:

```
>surv act sin123
```

No monitoring is provided for any calls the subject is involved in when the surveillance is activated. Monitoring of calls will begin after the subject line becomes idle.

111.15.4 Process of removing a PCES surveillance

1. Deactivate the surveillance using the SURV DEACT command

Example of deactivating a surveillance:

```
>surv deact sin123
```

Note that when a surveillance is deactivated, any monitored calls in progress will continue to be monitored until completion. The DF may provide the capability to terminate monitoring at any time.

2. Delete the surveillance using the SURV DEL command

Example of deleting a surveillance:

```
>surv del sin123
```

111.16 Operational measurements (OM)

No new OMs are introduced as part of this functionality.

OM group PCEM pegs success or failure for every PCEM event message generated by the CM. PCES event messages are PCEM messages that cause these registers to be incremented.

The register names and definitions are shown in Table 4 below.

Table 4 PCEM OM Group Register Definitions

PCEM Register Name	Definition
EMSENT	Event message successfully generated
EMFAIL	Failed to build event message.
EMSYSFL	System unable to send event message.

111.17 AMA/Billing information (AM)

PCES functionality requires the CS2K to be configured with PacketCable Event Messaging active. It does not require PacketCable event messaging Accounting to be active.

111.18 Software optionality control (SOC)

A new SOC code (NBD00005) has been implemented to support PCES and it has been added into the NBD SOC group.

NBD00005 requires NBD00003 (USNBD) to have SOC state ON. USNBD and PCES interworking is not supported and the two features cannot be used simultaneously on the same CS2K. Figure 5 lists the combinations of SOC codes that determine which application is active.

Table 5 PCES/USNBD SOC states combinations

NBD00003 USNBD SOC state	NBD00005 PCES SOC state	Active Application
OFF	OFF	-none-
ON	OFF	USNBD
ON	ON	PCES

111.19 Glossary

Table 6 Terminology

Term	Definition
BCT	Bearer Channel Tandeming
CBM	Core Billing Manager
CCR	Call Content Resource

Table 6 Terminology

Term	Definition
CDC	Call Data Channel
CF	Collection Function
CM	Computing Module
CMS	Call Management Server
CMTS	Cable Modem Termination System
CS2K	Call Server 2000
DF	Delivery Function
EM	Event Message
EMDI	Event Message Delivery Interface
EMS	Event Message Sender
GW	Gateway
GWC	Gateway Controller
IAP	Intercept Access Point
IAA	Integrated Accounting Application
LEA	Law Enforcement Agency
LNP	Local Number Portability
MGC	Media Gateway Controller
MRP	Monitored Replacement Party
MTA	Multimedia Terminal Adapter
PC	PacketCable
PCEM	PacketCable Event Messaging
PCES	PacketCable Electronic Surveillance
RKS	Record Keeping Server
SDM	Supernode Data Manager
SIN	Surveillance Identification Number
SOC	Software Optionality Control
TGCP	Trunking Gateway Control Protocol
USNBD	US Network Broadcast Delivery

Table 6 Terminology

Term	Definition
VoIP	Voice over IP

112: A00007564 Functional description (FN)

112.1 Feature name

SAM21 EM support for new hardware - MCPN905

112.2 Description

112.2.1 Feature Overview

This feature introduces two new components:

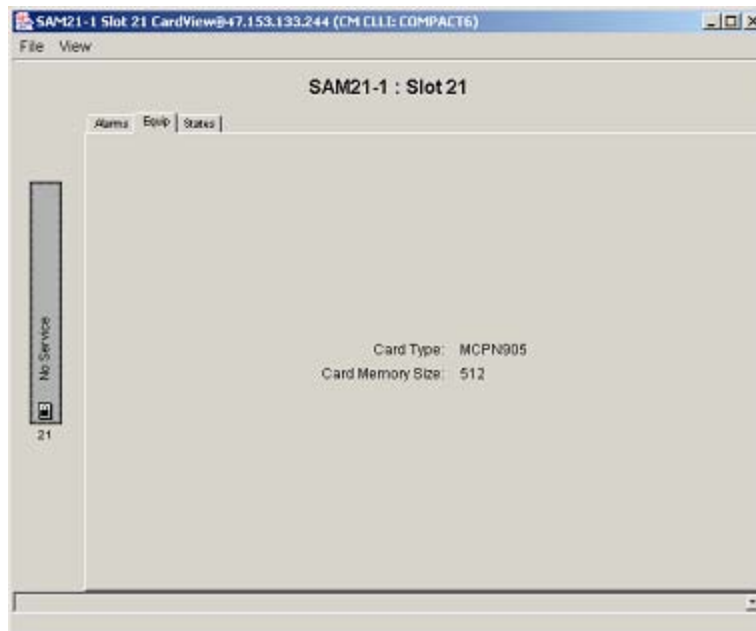
- Enable Supporting MCPN 905 card in SAM21 EM
- Enable provisioning of GWC and USPc service types on MCPN 905 card

112.2.2 Feature Functionality

MCPN 905 card currently support three functions, GWC and USPc, which are already supported by SAM21 EM. Their provisioning requirements for MCPN905 card are same as those for other cards. So the existing codes for all services are reused here, including provisioning panel, bootp entries, database storage, etc. However, to support a new card type, you must modify the hardware and memory requirements definition for the applications.

112.2.2.1 MCPN 905 card insertion support

When a MCPN 905 card insert into SAM21 shelf, the SAM21 EM will get the insertion trap, and show the card on the EM GUI. When opening the card view panel about this card, the card name will be displayed on the “Equip” panel.



112.2.2.2 MCPN 905 card service support

MCPN 905 card supports two type services, GWC and USPc. SAM21 EM should determine the services that can be assigned to the card according to the memory size. Below table shows the relation between the memory size and the service type.

Table 1 Memory requirements to enable GWC or USP service on MCPN 905 card

Memory on MCPN 905 Card	Is GWC Service Allowed (Yes/No)	Is USPc Service Allowed (Yes/No)
512M	Yes	Yes
1.5G	Yes	No

112.3 Hardware Requirements or Dependencies

This feature will support a new card model, MCPN 905, which supports USPc and GWC services.

112.4 Software Requirements or Dependencies

No new customer software or firmware dependencies are introduced in this feature.

112.5 Limitations and restrictions

No limitations or restrictions that is visible to any user are planned as part of this feature.

112.6 Interactions

- MCPN905 support in Shelf Controller DID A00007423
- MCPN905 support in Shelf Controller DSUM A00007423
- support MCPN905 card in SAM21EM DID A00007564

113: A00007571 Functional description (FN)

113.1 Feature name

MTP3b/SAAL/ATM BB-SS7 Protocol

113.2 Feature Synopsis

This feature enhances the existing ATM High Speed Link (ATM HSL) to fully support Broadband MTP3 (MTP3b) on the USP and allows it to operate in both ANSI and ITU markets using both T1 and E1 interfaces.

113.3 Feature Description

Prior to USP8.2, the ATM HSL on the USP consisted of ANSI T1 only and did not support the full 4K message size.

This feature provides the following enhancements to the USP's ATM HSL:

113.3.1 Support for up to 4K messages

This feature allows the USP to handle up to 4K sized messages. Support message flows for these large messages are:

- STP routed through MTP Level 3 from MTP3b to MTP3b link
- SCCP routed (using GTT) out an M3UA or MTP3b link

In order to support a 4K message, SCCP and M3UA are enhanced to fully support the LUDT and LUDTS message types. SCCP does not support Segmentation of LUDT messages. Any LUDT messages sent to SCCP will be routed out as LUDT messages if possible.

Due to current limits on the CORE, the USP will currently not send any messages larger than 1482 bytes through M3UA. This value is placed in the officeparm file. Any message destined to the core larger than this value result in an LUDTs being set to the originator.

This feature will also ensure that 1482 byte messages can be handled on the DMS up to the application i.e. MTP/SCCP/TCAP

The following table shows the impact that message size on the supported message rate of the ATM HSL.

Message Size	Cells	Messages/Second (0.8E)
25-36	1	1792
37-84	2	1490
85-132	3	1120

133-180	4	905
181-228	5	724
229-276	6	603
277-324	7	517
...	...	...
1381-1428	30	120
...	...	...
4069-4116	86	42

113.3.2 Support for ITU MTP3b

This feature implements ITU MTP3b (Q.2210) to compliment the existing ANSI version.

113.3.3 Support for both T1 and E1 physical interfaces

This feature allows the ATM High Speed links to use either the T1 or E1 physical interface. The interface choice is made upon provisioning of the ATM HSL card. If the physical interface value is changed, a re-boot of the card is required.

113.3.4 Support for 16 “SAAL” links per interface

The USP now supports up to 16 SS7 links provisioned on one ATMHSL link card. Each link must be provisioned with a different VPI and/or VCI. Each link provisioned on a given ATM HSL dynamically shares the available bandwidth of that card.

Through the support of these features, the USP has a fully capable MTP3b stack for use in all markets.

113.4 Hardware Information

No new hardware is introduced. MTP3b runs on existing NTST10BA and NTST81AA / NTST81BA.

113.5 GUI/CLI Information

A new field is added to the card provisioning screen and CLI command. This field is used to select whether the card is running with T1 or E1 interface. This field is available when the card is added or modified. A load of the card is required for any changes to take place.

113.6 OMs

No new OMs are created by this feature.

113.7 Logs, and Alarms

No new Logs are created by this feature.

113.8 Interactions

There are no interactions created by this feature.

113.9 Restrictions and Limitations

There are no restrictions introduced by this feature.

113.10 Definitions and Terms

ATM	Asynchronous Transfer Mode
CLI	Command Line Interface
GUI	Graphical User Interface
HSL	High Speed Link
MTP3	Message Transfer Part L3
MTP2	Message Transfer Part L2
OM	Operation Measurement
SCTP	Simple Control Transmission Protocol
SS7	Signaling System 7
USP	Universal Signaling Point

114: A00007572 Functional description (FN)

114.1 Feature name

M3UA RFC Peer to Peer Protocol

114.2 Feature Synopsis

This feature implements the M3UA Peer to Peer Protocol. This functionality allows the USP to function as IP Server Process (IPSP) using M3UA protocol. M3UA Peer to Peer allows the two end points to send and receive Payload, SS7 Network management and M3UA messages. This feature also allows the M3UA communicate with SS7 elements based on M3UA RFC standard. In 9.1 release, this functionality (IPSP) is only visible for SS7 connectivity.

114.3 References

MTP3 User Adaptation Layer (M3UA) RFC3332

MTP3. User Adaptation Implementers Guide Version 5

Stream Control Transmission Protocol (SCTP) Checksum Change RFC 3309

Stream Control Transmission Protocol (SCTP) Implementer Guide Version 10

USP8.1 M3UA RFC and Application Server Destination Support Functional Description.

114.4 Feature Description

This feature provides the support of M3UA Peer to Peer functionality based on M3UA RFC functionality on the SS7IPLINK card. To simplify, it is called as SS7M3UA

SS7M3UA allows the USP to communicate with the SS7 elements (such as IPSTP) using M3UA Peer to Peer messaging (IPSP) based on M3UA RFC standard.

This feature allows M3UA to be provisioned as a link set (can be viewed as 1+0 ASP model from the M3UA specification perspective) which can be mapped to combined link set to achieve load sharing and link set group to achieve alternate routing.

A M3UA link set can be mapped to more than one combined link sets and link set groups

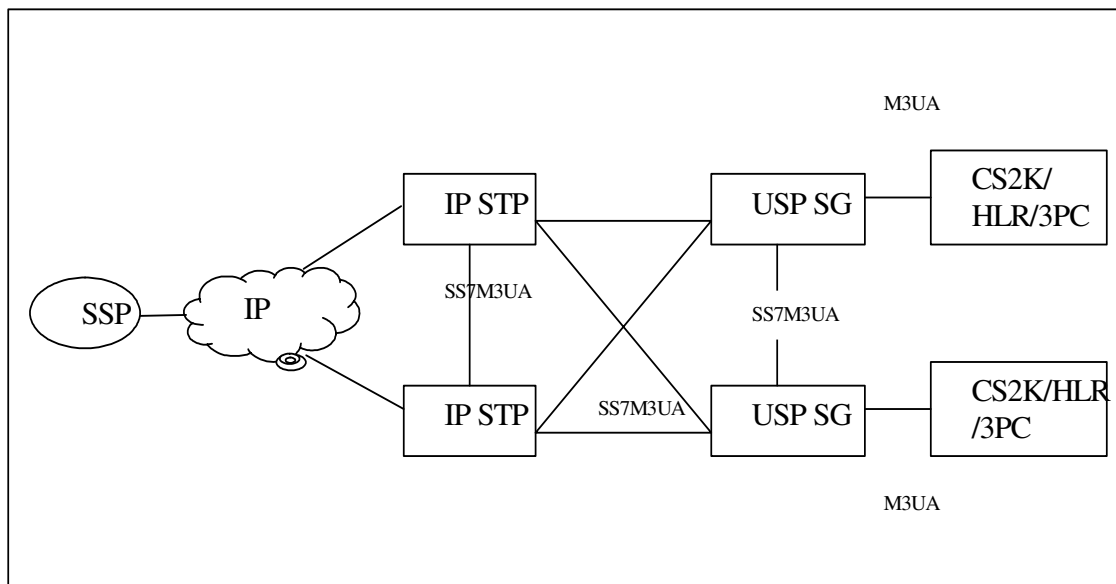
A M3UA link set will have up to 16 M3UA links and they are load shared

An SS7IPLink card can be provisioned up to 8 M3UA links provided only SS7M3UA links are used

Only M3UA links can be provisioned against the M3UA link set.

SS7 M3UA uses SCTP as transport protocol and it can be configured as either SCTP Client or SCTP Server. The USP supports RFC M3UA version RFC3332 and SCTP version RFC2960

The following diagram is an example of SS7M3UA in the network:



The SS7IPLINK card running M3UA peer to peer can handle approx 1792 messages/sec at 80% capacity or 2240 messages/sec in overload regardless of message size (equivalent to MTP2 based links running 25 bytes messages/sec at 0.8E).

114.5 Hardware Information

The M3UA protocol runs on NTST11BA and NTST11DA with NTST09AC TMs

114.6 GUI/CLI/Provisioning Information

114.6.1 Provisioning SS7M3UA link set

Existing MTP link set form is used to provision SS7M3UA link set. The new field “type-of-link-set” is added to indicate which type of link set is being used. The possible types of link set are **MTP**, **Virtual** and **M3UA-linkset**.

When a type of link set is chosen, the appropriate fields for that type are displayed.

Below is the link set form when M3UA-linkset is chosen. The field definitions are the same as the MTP link set except those explained below:

The M3UALinkset field indicates that the current link set is SS7M3UA link set

The **ipsp-type** can be provisioned as follow:

1. ipsp-se-Client (Single Exchange Client). Indicates the USP will start the M3UA connection (after SCTP is in-service) by sending ASP-UP. The ASP-UP is sent only once for the link set. The USP will not send ASP-UP for subsequent in-service M3UA links (SCTP associations) in the link set.
2. ipsp-se-Server (Single Exchange Server). Indicates the USP will wait for the other end to start M3UA connection (sending ASP-UP)

3. MTP link set CLI commands will be modified to include these changes for SS7M3UA link set.

114.6.2 Provisioning SS7M3UA link

The existing SS7IPLINK form will be used to provision the SS7M3UA link. The link-type used for M3UA link is still “ss7iplink”. The “protocol” field indicates the protocol used for the link. The possible protocols are M2PA, M2UA and M3UA.

For M3UA protocol, when M3UA link set is chosen, the “protocol” field will indicate M3UA and the local-port will be 2905.

Below is the SS7IPLINK form for “ss7iplink” with M3UA protocol is used. The definitions of the fields remain the same except for those explained below:

The screenshot shows a web-based form titled "mtp-link: v8.1.0" displayed in a "Layout Test Viewer" window. The form is organized into two primary columns: "Provisioning Data" on the left and "Operational Data" on the right. The "Provisioning Data" column contains fields for "link-type", "system-id", "linkset-name", "slc", "shelf", "slot", "protocol", "dest-ipaddress", "local-port", "remote-port", "sctp-operation-mode", "sctp-checksum", and "sctp-parms-index". The "Operational Data" column contains fields for "l3-link-status", "activation-state", "congestion", and "level-2-status". Above the form, there is a navigation bar with "File" and "View" menus, and a toolbar with icons for "New", "Add", "Modify", "Delete", "Activate", and "Deactivate". The status bar at the bottom of the window displays "Loading complete".

The **protocol** field indicates which protocol is being used. Possible protocols are M2UA, M2PA and M3UA.

The **local-port** for M3UA is always 2905 as defined in the M3UA RFC standard

sctp-operation-mode contains the following values:

1. M3uarfc/sctp-Client
2. M3uarfc/sctp-Server

Level-2-status field indicates the state of the corresponding sctp association and it will hold one of the following values:

- Out of Service: indicate that the M3UA link is being deactivated
- InitAlign : Indicates the link is activated and SCTP connection is being established
- In-service: Indicates SCTP is already in service

The current MTP link CLI commands will be modified to include SS7M3UA link

114.7 OMs

Current SS7 related OMs can be used for both SS7M3UA link and link set.

New OMs for M3UA related for SS7M3UA links will be created.

114.8 Logs, and Alarms

New SS7M3UA logs will be created.

114.9 Restrictions and Limitations

- The M3UA Peer to Peer functionality is available only on the SS7IPLINK card
- It is recommended that the same SS7IPLINK card should contains only SS7M3UA links
- M3UA link does not support Signaling Test message, therefore there will be no far end point code validated. It is required that the far end point code is entered correctly when provision the M3UA linkset
- M3UA does not support MTP restart.
- Change Over and Change Back are not supported in this release.
- M3UA congestion is not supported.
- LPO is not supported on M3UA link but M3UA link will be taken down when this occurs.

114.10 Definitions and Terms

CLI	Command Line Interface
GUI	Graphical User Interface
M3UA	MTP3 User Adaptation Layer
MTP3	Message Transfer Part L3
OM	Operational Measurement
SCTP	Stream Control Transmission Protocol
SS7	Signaling System 7
USP	Universal Signaling Point
SS7/M3UA	M3UA functionality on the SS7/IPLINK card to provide the communication between USP and SS7 side of the network.

115: A00007573 Functional description (FN)

115.1 Feature name

MTP3b/SAAL/ATM BB-SS7 Protocol

115.2 Feature Synopsis

This feature enhances the existing ATM High Speed Link (ATM HSL) to fully support Broadband MTP3 (MTP3b) on the USP and allows it to operate in both ANSI and ITU markets using both T1 and E1 interfaces.

115.3 Feature Description

Prior to USP8.2, the ATM HSL on the USP consisted of ANSI T1 only and did not support the full 4K message size.

This feature provides the following enhancements to the USP's ATM HSL:

115.3.1 Support for up to 4K messages

This feature allows the USP to handle up to 4K sized messages. Support message flows for these large messages are:

- STP routed through MTP Level 3 from MTP3b to MTP3b link
- SCCP routed (using GTT) out an M3UA or MTP3b link

In order to support a 4K message, SCCP and M3UA are enhanced to fully support the LUDT and LUDTS message types. SCCP does not support Segmentation of LUDT messages. Any LUDT messages sent to SCCP will be routed out as LUDT messages if possible.

Due to current limits on the CORE, the USP will currently not send any messages larger than 1482 bytes through M3UA. This value is placed in the officeparm file. Any message destined to the core larger than this value result in an LUDTs being set to the originator.

This feature will also ensure that 1482 byte messages can be handled on the DMS up to the application i.e. MTP/SCCP/TCAP.

The following table shows the impact that message size has on the supported message rate of the ATM HSL.

Table 1 Impact of message size on message rate

Message Size	Cells	Messages/Second (0.8E)
25-36	1	1792
37-84	2	1490
85-132		31120
133-180		4905
181-228		5724
229-276		6603
277-324	7	517
...	...	...
1381-1428	30	120
...	...	...
4069-4116	86	42

115.3.2 Support for ITU MTP3b

This feature implements ITU MTP3b (Q.2210) to compliment the existing ANSI version.

115.3.3 Support for both T1 and E1 physical interfaces

This feature allows the ATM High Speed links to use either the T1 or E1 physical interface. The interface choice is made upon provisioning of the ATM HSL card. If the physical interface value is changed, a re-boot of the card is required.

115.3.4 Support for 16 “SAAL” links per interface

The USP now supports up to 16 SS7 links provisioned on one ATMHSL link card. Each link must be provisioned with a different VPI and/or VCI. Each link provisioned on a given ATM HSL dynamically shares the available bandwidth of that card.

Through the support of these features, the USP has a fully capable MTP3b stack for use in all markets.

For a complete description of the ATM High Speed Link please see the SSR3.0 document “High Speed Link – Feature Description”

115.4 Hardware Information

No new hardware is introduced. MTP3b runs on existing NTST10BA and NTST81AA / NTST81BA.

115.5 GUI/CLI Information

A new field is added to the card provisioning screen and CLI command. This field is used to select whether the card is running with T1 or E1 interface. This field is available when the card is added or modified. A load of the card is required for any changes to take place.

115.6 OMs

No new OMs are created by this feature.

115.7 Logs, and Alarms

No new Logs are created by this feature.

115.8 Interactions

There are no interactions created by this feature.

115.9 Restrictions and Limitations

There are no restrictions introduced by this feature.

115.10 Definitions and Terms

ATM	Asynchronous Transfer Mode
CLI	Command Line Interface
GUI	Graphical User Interface
HSL	High Speed Link
MTP3	Message Transfer Part L3
MTP2	Message Transfer Part L2
OM	Operation Measurement
SCTP	Simple Control Transmission Protocol
SS7	Signaling System 7
USP	Universal Signaling Point

116: A00007576 Functional description (FN)

116.1 Feature name

Message Trace

116.2 Description

The purpose of this feature is to provide a message tracing tool built into the USP for monitoring and decoding SS7 messages. This feature introduces a new interface for monitoring incoming and outgoing messages, including M3UA, MTP3, SCCP and ISUP on a per-link or per-ASP path basis. In USP10, this functionality is offered in addition to the existing MSU Trace which is part of the gateway screening subsystem.

Previously, message tracing on the USP had to be done by configuring gateway screening criteria on a per-linkset basis. Defining a gateway screening rule for the purpose of debugging the network can be complex and may result in discarding messages unnecessarily.

This feature provides a message monitoring tool to capture messages on the signaling links. It can be used to filter messages at the M3UA, MTP, SCCP and/or ISUP levels. The tool is independent of gateway screening.

All ANSI and ITU MTP3, ANSI SCCP and ISUP messages are decoded in the MSU-trace on the GUI presented in a tree diagram as of USP8.1.0. This feature will add the support of M3UA message decode. Message decoding will be only done on the message types defined in the M3UA protocol. Any message type that is used by the other Sigtran Adaptation Layers, such as the provisioning messages to the Core, will be displayed in hexadecimal byte string.

If the tool is invoked from the Command Line Interface, no decode is provided; the message is captured and forwarded to the interface, but the data remains displayed in raw data format.

The tool provides two methods to define message tracing criteria.

First, the tool will allow filtering messages by providing byte string to match with, a given offset to the message, and the length of the given byte string.

Secondly, the tool will allow specific field/value matching as a filter.

The fields that may be used as filters are as follows:

- Originating Point Code

- Destination Point Code
- Network Indicator
- Message Priority
- MTP3 Network Management Message Types H0H1
- SCCP Message Types
- M3UA Message Types
- ISUP Message Types
- Affected Point Code in SCMG messages
- Affected Point Code in M3UA messages
- SCCP Subsystem Number
- SCCP Point Code
- SCCP GT Translation Type
- SCCP GT Nature of Address
- SCCP GT Addressing Information (dialed digits)
- SCMG Format Identifier
- ISUP Circuit Identification Code (new)
- ISUP IAM CdPN (dialed digits)

Only the following ISUP messages are fully decoded:

IAM, SAM, ACM, REL, SUS, RES

Other ISUP message types (BLO, CQM, CON, COT, etc.) may be traced by type, but the ISUP portion of the message is not decoded beyond the message type.

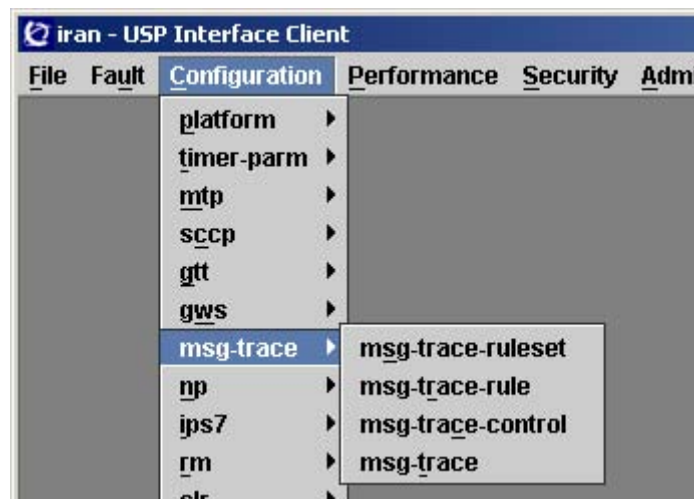
TCAP decode is not supported.

ITU14 country variants for Point Codes are supported. Partial Point Codes are not supported.

Four tables are introduced within the USP to allow for the provisioning of this screening.

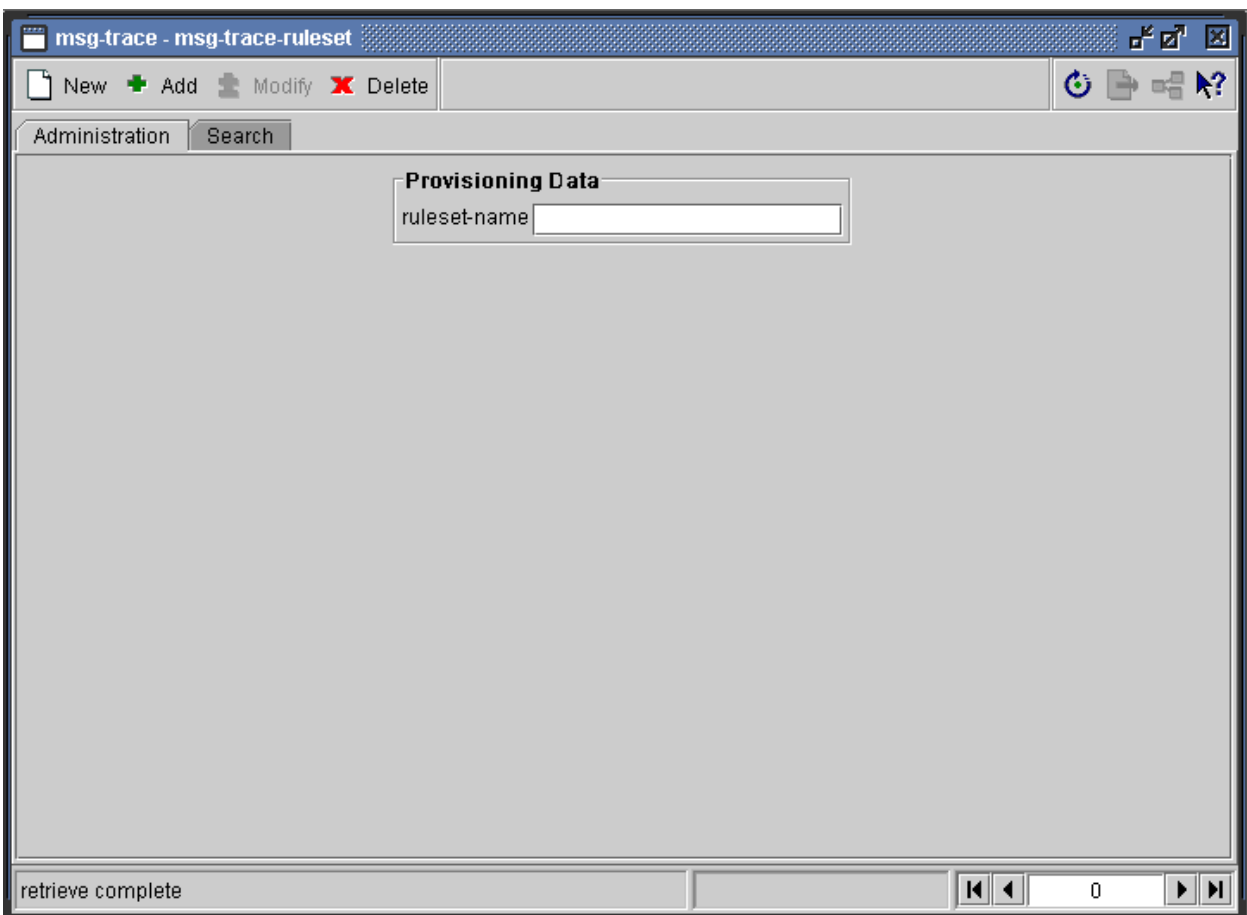
The following 5 figures give a view of how the msg-trace subsystem may be provisioned and used.

Figure 1 msg-trace Menu Items



This menu provides the launch point for provisioning and tracing of the data.

Figure 2 msg-trace-ruleset Screen Capture



Provisioning and maintenance of rulesets can be completed from this screen.

Figure 3 msg-trace-rule Screen Capture

The screenshot shows a web application window titled "msg-trace - msg-trace-rule". The interface includes a toolbar with "New", "Add", "Modify", and "Delete" buttons. Below the toolbar are tabs for "Administration" and "Search". The main content area is titled "Provisioning Data" and contains a form with the following fields:

ruleset-name	ansi1
rule-id	1
protocol	mtp3
match-type-selector	match-field
field-name	mtp3-opc
condition	equal
value	2-2-2
offset	
byte-string	

At the bottom of the window, there is a status bar showing "retrieve complete" and a pagination control with "0" and navigation arrows.

Provisioning and maintenance of rules against rulesets can be completed from this screen.

This screen allows for the creation of a set of rules which may be applied to any link/path using the Control table. The message will only be captured and forwarded to the GUI if all of the rules are satisfied.

Figure 4 msg-trace-control Screen Capture

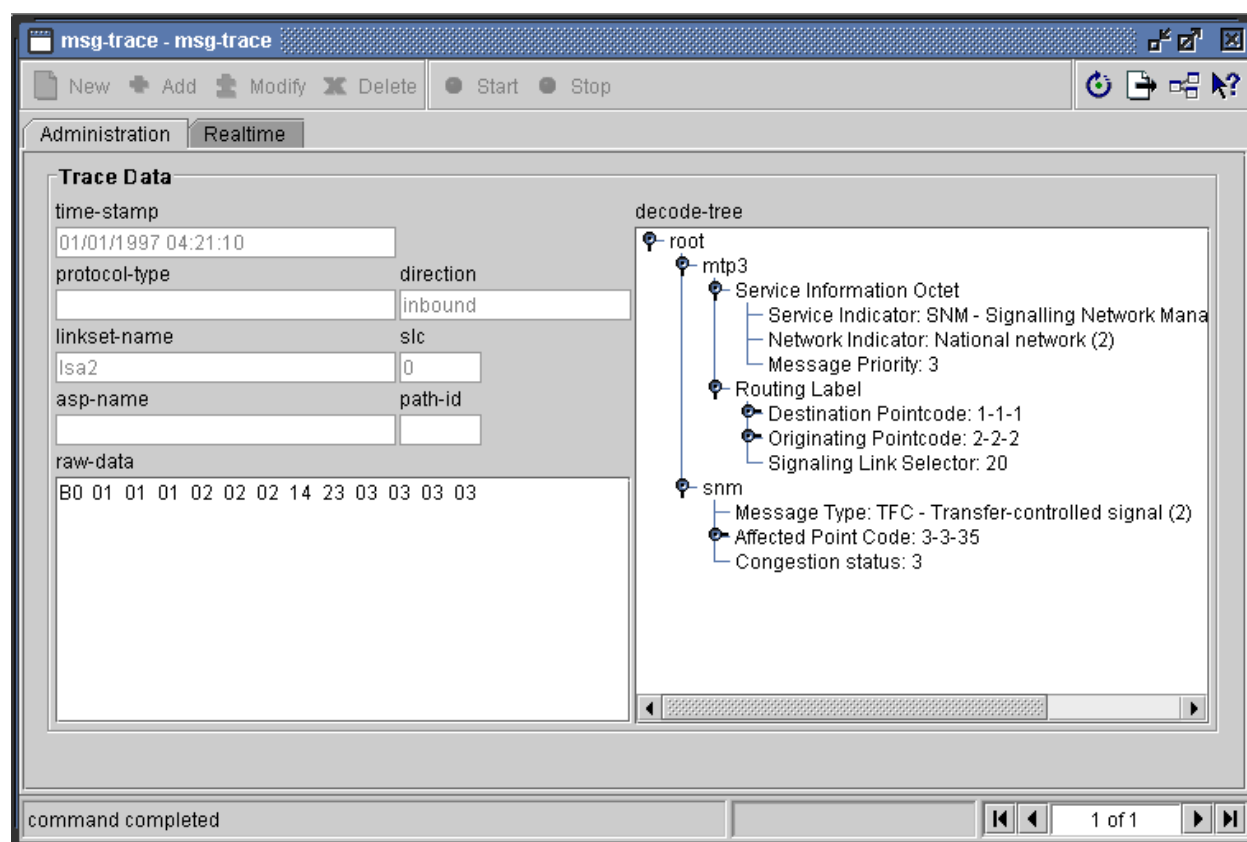
The screenshot shows a web application window titled "msg-trace - msg-trace-control". The interface includes a menu bar with "New", "Add", "Modify", and "Delete" options. Below the menu bar are tabs for "Administration" and "Search". The main content area displays a "Provisioning Data" form with the following fields:

trace-id	1
ss7-ips7	ss7
direction	both
ruleset-name	ansi1
linkset-name	lsa2
slc	0
asp-name	
path-id	

At the bottom of the window, there is a status bar showing "retrieve complete" and a pagination control with a "0" and navigation arrows.

Provisioning and maintenance of rulesets against links/paths can be completed from this screen.

Figure 5 msg-trace Screen Capture



This screen provides the realtime traceback of decoded messages passed in.

116.3 Hardware Requirements or Dependencies

There are no hardware requirements or dependencies associated with this feature.

116.4 Software Requirements or Dependencies

Message Trace is delivered as part of USP10.0.0.

116.5 Limitations and restrictions

Activation of the Message Trace functionality will impact the capacity of the link. The scope of the impact will vary depending on the rate of traffic and the types/size of the messages to be decoded. Message Trace should not be activated on links which are congested.

116.6 Interactions

This feature is compatible with all USP features as of USP10.0.0.

116.7 Glossary

Term	Description

117: A00007602 Functional description (FN)

117.1 Feature name

SDM Software Authenticity

117.2 Description

The intent of this feature is to add more security to the SDM software delivery (patches and ESD loads), and guarantee that the SDM deliverable sent to the field is authenticated by Nortel.

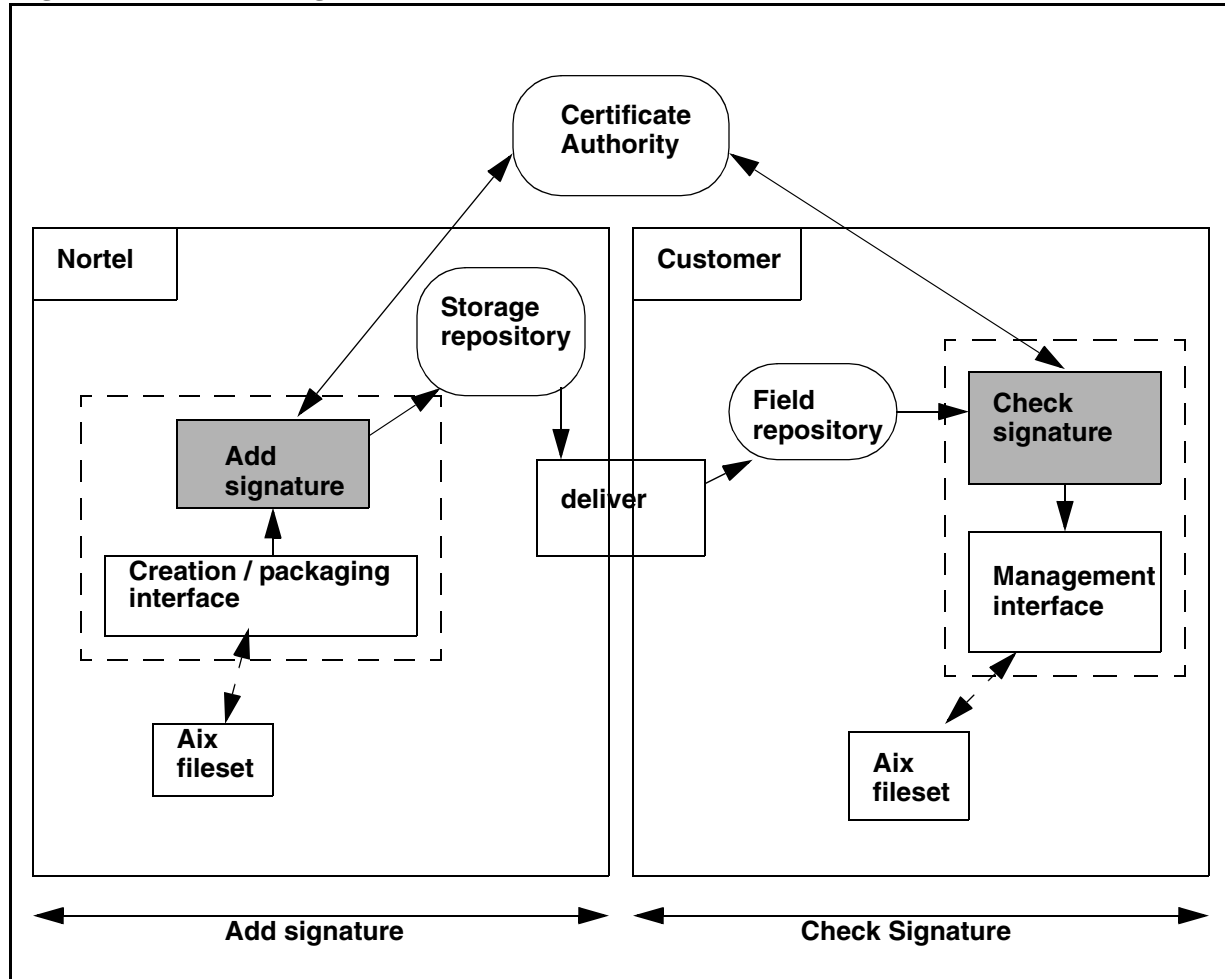
Without this authentication a third party could deliver rogue software to a customer and there would be no way of detecting it. This feature will implement a method of digitally signing any software created by the SDM development team. The SDM deliverable would then be signature checked prior to being applied on the customer system.

This FN document describes the new procedures for the following software delivery applications, using software authentication:

- Patch Apply: New alarms and security logs are created to reflect patch signature check failures. An alarm clearing mechanism is also available to manually clear alarms after detecting bad software. Please refer to section 117.6.1 “Patch Apply” on page 922 for the full details.
- ESD Load Upgrade: A signature check for the ESD load is done manually prior to the load upgrade. Descriptive messages are displayed to reflect software signature check failures. Please refer to section 117.6.2 “ESD load Upgrade” on page 928 for the full details.

In SN08, this feature is primarily concerned with Electronic Software Delivery (ESD) and does not provide a solution to authenticate physical media (i.e. tapes).

Figure 1 “Software Management Architecture” on page 921, provides a high level overview of the SDM software management architecture in SN08.

Figure 1 Software Management Architecture

117.3 Hardware Requirements or Dependencies

SDM system equipped with the SN08 hardware base line configuration.

117.4 Software Requirements or Dependencies

SDM system installed with the SN08 software.

117.5 Limitations and restrictions

- This feature supports software authentication only on the SDM platform in SN08, and does not support the CBM platform.
- The software authentication feature is not enabled on the SDM by default. In order to enable this functionality, the user needs to manually install the “SDM software Authentication services” package which will be part of the SDM SN08 load. Please refer to the SN08 SDM SW upgrade customer documentation (Upgrading the SDM - NN10059-461) for full details on how to install a SDM package.

- The software authentication functionality is only supported on patches and ESD loads, and does not support physical media (i.e. tapes). Applying software from physical media will succeed, but will not be authenticated.
- Customer documentation and release notes are not authenticated in SN08.
- Software loads that are serviced by the SDM's bootp server, packaged through RPM (Redhat Package Manager), will not be authenticated in SN08. These packages are:
 - MG9K0070 (MG9K)
 - GWCC0070 (NA-GWC)
 - GWCW0070 (INTL-GWC)
 - SAM20070 (SAM21)
 - 3PC00070 (3PC)

117.6 Interactions

117.6.1 Patch Apply

The patch apply procedure (customer documentation) in SN08 is exactly the same as in SN07. In SN08, all patches are digitally signed during packaging, and a signature check is applied on each patch prior to patch apply. This signature check procedure is completely transparent to the user.

Signature check failures are reported as follows:

- A new “SDM Patch Check Status” indicator is introduced under the “sdmmtc sys” level. This state will reflect “Failed”, once a single patch fails signature checking. Please refer to 117.6.1.1 “Minor alarm to reflect patch signature check failure” on page 923 for more details.
- A new minor alarm is generated under the “sdmmtc sys” level. Please refer to 117.6.1.1 “Minor alarm to reflect patch signature check failure” on page 923 for more details.
- New security logs are generated to report patch signature check failures and manual alarm clearing. Please refer to 117.6.1.3 “Security logs to reflect Patch signature check failure” on page 928 for more details.

All patches that fail signature checking will be moved to the following directory on the SDM:

```
/swd/sdm/fixes/rejected
```

A manual alarm clearing mechanism is provided to clear the alarm after detecting bad patches. Please refer to 117.6.1.2 “Manual alarm clearing” on page 925 for more details.

117.6.1.1 Minor alarm to reflect patch signature check failure

A new “SDM Patch Check Status” indicator is introduced under the “sdmmtc sys” level, to reflect the state of patch signature checking. By default this status indicator is set to “.” (in-service), to indicate that no patch failed through signature checking prior to patch apply. Figure 2 “SDM Patch Check Status indicator” on page 924 reflects the new patch check status indicator.

The user will receive no indication of successful patch checking/apply. Once a single patch fails signature checking, the “SDM Patch Check Status” indicator will reflect a “Failed” indication, and a minor alarm will be generated under the “sdmmtc sys” level. Figure 3 “Patch signature check failure indication” on page 925 reflects a failure with the patch signature checking.

A security log is generated to reflect the signature check failure (associated with the minor alarm). Please refer to 117.6.1.3 “Security logs to reflect Patch signature check failure” on page 928.

Note: Patches that fail signature checking will not be listed under “sdmmtc swim apply” level once the source command is invoked. The failed patches will be moved to the /swd/sdm/fixes/rejected directory. It is expected that the user detects the minor alarm, reads the security log, and checks the rejected directory for the failed patches.

Figure 2 SDM Patch Check Status indicator

SDM	CON	512	NET	APPL	SYS	HW	CLLI: SNM0
.	.	. .	.	.	.	.	Host: wcary2p3
		. .					Fault Tolerant
Sys							
0 Quit		SDM Storage State:	.				
2		SDM Backup Status:	.				
3		SDM Configuration State:	.				
4 Logs		SDM System Audit Status:	.				
5 Storage		SDM Patch Check Status:	.				
6		# Description				Current / Threshold	
7		1 CPU (run queue entries):				0 / 5	
8		2 Number of Processes:				81 / 250	
9		3 Number of Zombies:				0 / 3	
10		4 Number of Swap Queue Entries:				0 / 2	
11							
12							
13							
14 QuerySDM							
15 Locate							
16							
17 Help							
18 Refresh							
root							
Time 12:42							>

Figure 3 Patch signature check failure indication

SDM	CON	512	NET	APPL	SYS	HW	CLLI: SNM0
ISTb	.	..	.	.	ISTb	.	Host: wcary2p3
		..					Fault Tolerant
Sys							
0 Quit			SDM Storage State:	.			
2			SDM Backup Status:	.			
3			SDM Configuration State:	.			
4 Logs			SDM System Audit Status:	.			
5 Storage			SDM Patch Check Status: Failed				
6			# Description			Current / Threshold	
7			1 CPU (run queue entries):			0 / 5	
8			2 Number of Processes:			81 / 250	
9			3 Number of Zombies:			0 / 3	
10			4 Number of Swap Queue Entries:			0 / 2	
11							
12							
13							
14 QuerySDM							
15 Locate							
16							
17 Help							
18 Refresh							
root							
Time 12:42							>

117.6.1.2 Manual alarm clearing

A manual alarm clearing mechanism is provided to clear the minor alarm generated by the patch signature check failure. Once the failure is detected, the user can clear the minor alarm manually by executing the “patch clear” command from the “sdmmtc sys” level. Please refer to Figure 4 “Manual alarm clearing” on page 927 for the actual command invocation and system responses.

Once the alarm is manually cleared, the “SDM Patch Check Status” indicator is set to “.” as shown in Figure 2 “SDM Patch Check Status indicator” on page 924.

A security log is generated to reflect alarm clearing. Please refer to 117.6.1.3 “Security logs to reflect Patch signature check failure” on page 928 for the actual log generated.

Figure 4 Manual alarm clearing

```

SDM  CON  512  NET  APPL  SYS  HW  CLLI: SNM0
ISTb  .    . .    .    .    ISTb  .    Host: wcary2p3
                                     Fault Tolerant

Sys
0 Quit          SDM Storage State: .
2              SDM Backup Status: .
3              SDM Configuration State: .
4 Logs         SDM System Audit Status: .
5 Storage      SDM Patch Check Status: Failed
6              # Description                      Current / Threshold
7              1 CPU (run queue entries):          0 / 5
8              2 Number of Processes:              81 / 250
9              3 Number of Zombies:                 0 / 3
10             4 Number of Swap Queue Entries:      0 / 2
11
12
13
14 QuerySDM
15 Locate
16
17 Help
18 Refresh
  root
Time 12:42 > patch clear
=====
14 QuerySDM
15 Locate      This will clear the Patch Check status and alarm. Please insure
16             that the failed patch is removed from the system.
17 Help        Do you wish to proceed?
18 Refresh     Please confirm ("YES", "Y", "NO", or "N")
  root
Time 14:35 > y
=====
14 QuerySDM
15 Locate
16
17 Help
18 Refresh     Patch clear - Command complete.
  root
Time 14:36 >

```

117.6.1.3 Security logs to reflect Patch signature check failure

Security logs are generated to reflect patch signature check failure and alarm clearing. Examples of the security logs are shown in Figure 5 “Security logs” on page 928.

Figure 5 Security logs

Signature check failure:

Aug 24 14:58:02 wcary2p4 syslog: SDM337 MINOR TBL SDM Base Maintenance
Patch NT_SIM.tools-21.35.6.2.patch failed signature checking.

Alarm clearing:

Aug 24 15:05:32 wcary2p4 syslog: SDM637 NONE INFO SDM Base Maintenance
Patch check status is cleared by user.

117.6.2 ESD load Upgrade

An extra step is required to the ESD load upgrade procedure in SN08. A signature check is applied on all of the filesets included in the ESD load. A successful signature check is required on all of the filesets, for the ESD load to pass signature checking. If at least one fileset fails signature checking, the whole load must be rejected.

In summary, the following steps are required for an ESD load upgrade:

- Create a filesystem on the SDM (ex: /load), to hold the ESD load.
- Download the ESD load into the SDM (under the created filesystem).
- Extract the load (unzip/untar the load).
- Invoke signature checking (new step introduced in SN08). Please refer to 117.6.2.1 “ESD Load signature checking” on page 928 for full details.
- Upgrade the SDM to the new load, provided that a successful signature check is achieved.

Please refer to the SN08 SDM SW upgrade customer documentation (Upgrading the SDM - NN10059-461) for full details of the ESD load upgrade. This section will only address the new introduced ESD load signature checking step.

117.6.2.1 ESD Load signature checking

A new command “verifyload” is introduced in SN08 to perform a signature check on the ESD load. This command is packaged within the ESD load. Once the load is extracted on the SDM, the user is expected to invoke the

“verifyload” command manually from the command line before starting the upgrade.

No alarms and security logs are generated in case the ESD load fails signature checking. Instead, a message is displayed on the screen indicating the result of the signature check. It is the responsibility of the user to reject the load and contact “Nortel next level of support” in case of a signature check failure.

Figure 6 “ESD load signature check” on page 929 show the actual command to perform the signature check on ESD load, and the different expected return messages (success and failure). The “verifyload” command is located under the same directory as the ESD load (the filesystem that holds the load).

Figure 6 ESD load signature check

```
# ./verifyload
```

Checking the integrity of the load, please wait....

Successful return message:

Integrity and signature check completed successfully.
Please continue with the upgrade.

Failure return messages (could be either one of the following messages):

This load include missing packages.
Please contact your next level of support.

This load include zero size packages.
Please contact your next level of support.

This load failed signature checking.
Please contact your next level of support.

Signature check cannot not be completed.
Please contact your next level of support.

Integrity check failed, unknown failure.
Please contact your next level of support.

117.7 Glossary

Table 1

Term	Description
ESD load	Electronic Software Delivery load
SDM	SuperNode Data Manager
CBM	Core Billing Manager
ISTb	In Service Trouble
SW	Software

117.8 References

[1] Upgrading the SDM - NN10059-461

118: A00007635 Functional description (FN)

118.1 Feature name

CBM Upgrades

118.2 Description

The purpose of this feature is to provide a mechanism to upgrade the CBM 850 product from release CBM07 to release CBM08. The CBM 800 product is not being released for CBM08 and will not be discussed within this document.

The CBM upgrade procedure will involve the upgrade of the SSPFS platform and the upgrade of the CBM applications. The upgrade of the SSPFS platform will not be discussed within this document as it will be discussed within the “SSPFS Upgrades For SN08, A0000817” feature FN. It is important to note that the CBM upgrade procedure will be automatically initiated by the SSPFS platform upgrade.

Another important note is that the CBM07 applications will still reside on the CBM after a successfully completed upgrade. These applications will be dormant however. A separate procedure outside of the upgrade will allow the customer to remove “older” versions of software that are dormant on the system and will not be discussed within this document.

The CBM 850 product is a High Availability cluster made up of an active node and an inactive node. To ensure that the CBM will remain within an HA configuration, a separate boot environment (BE) on the inactive node is created in which the application upgrade will actually take place. This means that inactive node is still running the CBM07 release in standby mode. This process is actually performed using the Sun Solaris LiveUpgrade suite. The creation of this separate BE will be performed within the SSPFS platform upgrade procedure.

For CBMs in wireless market, the CBM Upgrade will automatically initiate the Wireless upgrade procedure after the required packages, value added packages and patches are applied to the system.

A successful CBM upgrade procedure is as follows:

Note: The creation of the separate boot environment and the upgrade of the operating system and other platform software within this separate environment would have been completed by the SSPFS platform upgrade. The CBM procedure starts when the platform upgrade initiates the CBM upgrade.

Note: Once the “clone” has been initiated at the end of a successful upgrade, NO fallback to CBM07 will be possible. In order to return the CBM to the CBM07 release, a restore or a fresh install would be required.

- Load the CBM08 software media (CDROM or ESD image file)
- Perform pre-upgrade checks
- Upgrade all CBM08 850 required packages
- Upgrade all value added CBM08 packages
- Apply patches, if any, for the CBM08 load
- Initiate Wireless Upgrade (if necessary)
- Perform post-upgrade checks
- Activate CBM08 load and reboot the CBM08 Inactive node (automatically done by SSFPS upgrade script)
- Perform SWACT from CBM07 node to the CBM08 node (manually initiated by the user)
- Clone the CBM08 node onto the CBM07 node (manually initiated by the user)

118.2.1 Logs

Upgrade logs for the CBM will be located within the /var/adm/ directory of the CBM07 environment in a file called cbm_upgrade_<from>_to_<to>.log where “from” and “to” are the release numbers involved. This log will be transferred to the CBM08 environment before the SWACT.

A customer log will be generated for any CBM upgrade failure. The log will identify the upgrade stage at which failure occurred, the upgrade log.

118.2.2 Failures

If a failure occurs during the upgrade, a message will be displayed to the user describing the failure and informing the user to contact next level support. The user will be provided a prompt to 1) Enter a maintenance shell where command could be executed in an attempt to correct the error. Exiting the maintenance shell will re-execute the step that failed. 2) Perform a fallback. This will send a signal back to the SSPFS upgrade for SSPFS to initiate a fallback. Both the Maintenance Shell and the Fallback have a yes/no user confirmation, answering no will re-execute the failed step.

118.2.2.1 Fallbacks

Fallbacks during the CBM upgrade would depend on which CBM load, 07 or 08, has been Activated on the inactive node at the time. A fallback will mean that the CBM inactive node will be put back into its original configuration of CBM07 inactive.

If a failure occurs before the “Activate CBM08 load and reboot the Inactive” step then,

- The user would have requested a fallback at a fallback prompt
- The CBM08 separate environment will be deleted

If a failure occurs after the “Activate CBM08 load and reboot the Inactive” upgrade step, but before the SWACT, then,

- The user would execute the SSPFS fallback command
- The CBM07 load will be “Activated” on the inactive node
- The Inactive node will be rebooted
- The CBM08 separate environment will be deleted

If a failure occurs after the SWACT from the CBM07 active node to the CBM08 inactive node then,

- The user would execute the SSPFS fallback command
- A SWACT is performed back to the CBM07 node
- The CBM07 load will be “Activated” on the inactive node
- The Inactive node will be rebooted
- The CBM08 separate environment will be deleted

118.3 Hardware Requirements or Dependencies

- CBM850 HA dual node Cluster hardware baseline
- HA Cluster must be fully in-service
- HA cluster must have no alarms

118.4 Software Requirements or Dependencies

- CBM must have a patch current CBM07 release.
- All CBM applications must not be in the Fail or Sysb state

118.5 Limitations and restrictions

- The CBM08 upgrades will not include the CBM800 product. Only the CBM850 HA configuration will be supported.
- The CBM08 media (CD or ESD) must have been delivered to the customer site prior to the commencement of the upgrade

- The ESD image must be located within the /swd/sdm directory.
- There is no upgrade support for single server CBM 850. A single server 850 must be converted into a dual node HA cluster configuration running CBM07 before being upgraded to CBM08.

118.6 Interactions

The CBM upgrade process involves the initial execution of the SSPFS platform upgrade procedure from which the CBM upgrade procedure will be automatically initiated.

118.6.1 Load the CBM08 software media (CDROM or ESD image file)

The CBM load is available on CDROM and via an ESD image (Electronic Software Delivery).

The user will be asked which media type they will be using (CDROM or ESD)

For CDROM, the user will be asked to place the CBM CD disk into the CDROM drive on the Inactive Node. The user will be prompted to “Start” the upgrade once the CDROM has been placed into the drive.

For ESD, the ESD image will be prepared for use and the CBM upgrade will be started automatically. The user will be notified if the ESD image has not been found in the proper location or if there is a problem extracting and preparing the ESD image for use.

In the event of any failure, the user will be prompted to

- 1) Enter a maintenance shell to suspend the upgrade and correct the failure,
- 2) perform a fallback to cancel the upgrade.

118.6.2 Perform Pre-upgrade checks

The prechecks for the CBM upgrade will be performed before any software is upgraded.

118.6.2.1 Examine CBM alarm and Node states

The CBM should have no major alarms before attempting to perform the CBM upgrade. If an alarm does exist, the user will be notified to contact next level support and is provided a prompt to 1) Suspend the upgrade and enter a maintenance shell to investigate the alarms, 2) perform a fallback to cancel the upgrade and 3) Continue with the upgrade, ignore the alarms.

118.6.2.2 Verify separate upgrade environment

If the separate boot environment does not exist the user will be notified that the separate boot environment does not exist and that the CBM upgrade cannot be executed.

The only way for a user to obtain this message would be if the cbm_setup upgrade script was being executed manually for an upgrade and the sspfs platform had not been performed.

118.6.2.3 Verify the CBM base directory

All CBM packages have what is called a BASE Directory or BASEDIR. The directory must exist before attempting to apply the CBM packages.

The platform upgrade will create this directory because there is a CBM package that gets applied during their upgrade procedure. In the event that the directory does not exist, it will be created automatically.

If the directory does not exist, the user will be notified that the CBM Base directory does not exist and that it will be created.

118.6.2.4 Examine installed software

In order to apply the common packages, a list of the applications that are currently installed within the separate boot environment is generated. This list is required for future steps of the upgrade.

In the event that the software list cannot be created, the user will be notified that there appears to be a problem with the separate boot environment and that the CBM upgrade cannot continue.

118.6.3 Upgrade all CBM08 850 required packages

Required packages are the core applications on the CBM that provide base and service level support.

In the event of a failure to apply any one of the packages the user will be notified of the failure, where the log can be obtained and that they should contact next level support and is provided a prompt to 1) Suspend the upgrade and enter a maintenance shell to correct the failure, 2) perform a fallback to cancel the upgrade.

118.6.4 Upgrade all value added CBM08 packages

Value added packages are applications that do not make up the required list of applications. The separate boot environment is examined for CBM07 applications. All CBM07 applications that exist within the separate environment and have not yet been upgraded to the CBM08 load are automatically “selected” and applied. A list of the “selected” packages is displayed and then the status of applying each package is displayed.

In the event the CBM does not have any “value added” packages, this step will not be executed.

The actual apply of the value added packages is performed using the command line version of the well known SDM/CBM SWIM application. The output of

the swim command line is the same as the output of the SWIM applications within the sdmmtc/cbmmtc interface.

Value added packages may have a “configuration” script that needs to be executed after installation. The scripts will prompt the user for information that will be used later on when the application is turned on or RTS’d.

In the event that there are configuration scripts to apply, the user will be notified that the scripts will be executed in which the user will be requested to press ‘return’ to start the execution of the scripts.

In the event of a failure to apply any one of the packages the user will be notified of the failure, where the log can be obtained and that they should contact next level support and is provided a prompt to

- 1) Suspend the upgrade and enter a maintenance shell to correct the failure,
- 2) perform a fallback to cancel the upgrade.

118.6.5 Apply patches, if any, for the CBM08 load

Once all the CBM08 packages have been applied into the separate boot environment, any patches that have been delivered with the CBM media are automatically applied, making the CBM08 load patch current.

The output of the patch apply is the same output as the current CBM patchctrl command.

In the event of a failure to apply any one of the patches the user will be notified of the failure, where the log can be obtained and that they should contact next level support and is provided a prompt to

- 1) Suspend the upgrade and enter a maintenance shell to correct the failure,
- 2) perform a fallback to cancel the upgrade.

118.6.6 Initiate Wireless Upgrade

For CBMs within the wireless market, there are additional packages that need to be upgrade. These packages reside on a different media that the CBM product.

If the CBM is a wireless CBM, the wireless upgrade start script will automatically be executed.

118.6.7 Perform post-upgrade checks

To ensure that the CBM is still in a healthy state before we perform the reboot and swact upgrade stages, the following checks will be performed.

The CBM should have no major alarms before attempting to perform reboot and swact portion of the upgrade. If an alarm does exists, the user will be notified to contact next level support to investigate the alarm and is provided a prompt to 1) Enter a maintenance shell to investigate the alarms, 2) perform

a fallback to cancel the upgrade and 3) Continue with the upgrade, ignore the alarms.

118.6.8 Activate CBM08 load and reboot the inactive node

The separate boot environment is automatically “activated” which prepares the system to have the CBM08 load upon a reboot. The activation and reboot of the inactive node is done by the SSPFS upgrade script once the CBM portion of the upgrade is successfully completed.

Note: Only the inactive node will be rebooted. The Active node running the CBM07 release will still be providing service.

118.6.9 Perform SWACT from CBM07 node to the CBM08 node

Since the CBM upgrade script is no longer running, this step will be a documented procedure. Within documentation, the user will be requested to log into the CBM07 active node as the root user once the CBM08 inactive node has successfully rebooted. For the command line on the CBM07 active node, the user will be documented to execute the “init 0” command to force a swact and prepare the CBM07 active node for the clone operation if the upgrade is successful.

Executing the “init 0” will make the CBM08 inactive node the CBM08 active node, meaning that the new CBM08 software is now running. The CBM07 node is now the inactive node.

This process would be described in more detail within the “SSPFS Upgrades For SN08, A0000817” feature FN.

118.6.10 Clone the CBM08 node onto the CBM07 node

If the CBM08 active node applications are all INSV and operational, the documentation will inform the user to initiate the “clone” sequence to change the CBM07 inactive node into a CBM08 inactive node.

This process would be described in more detail within the “SSPFS Upgrades For SN08, A0000817” feature FN.

Fallbacks are no longer possible once this stage of the upgrade is initiated. A restore from backup or a fresh install would be required to go back to the CBM HA cluster running the CBM07 load.

118.7 Glossary

Term	Description
BE	Boot Environment
SSPFS	Succession Server Platform Foundation Software
LiveUpgrade	Sun Solaris LiveUpgrade tool suite

119: A00007708 Functional description (FN)

119.1 Feature name

Unistim Security

119.2 Functional Description

119.2.1 Overview

In the 2.5 implementation of Unistim Security, once a terminal has been connected securely to a CICM it is tied to that particular CICM as the Fingerprint and Master keys pertain to those of the said CICM. Once in this state the client is not capable of connecting to a different CICM without manual intervention.

If a large number of terminals are required to transition from one CICM to another, this manual reset of terminals would be a daunting task. Thus this new automated procedure replaces the manual intervention.

119.2.2 Detail

The following section describes the process for moving a secured terminal from one CICM to another.

In order to move a secure terminal from one CICM to another the first step that is needed is to clear the associated security object from the terminal. There are three different methods of performing this process.

- Clearing Security Objects at an Enterprise level
- Clearing Security Objects at a Gateway level
- Clearing Security Objects at a Terminal level

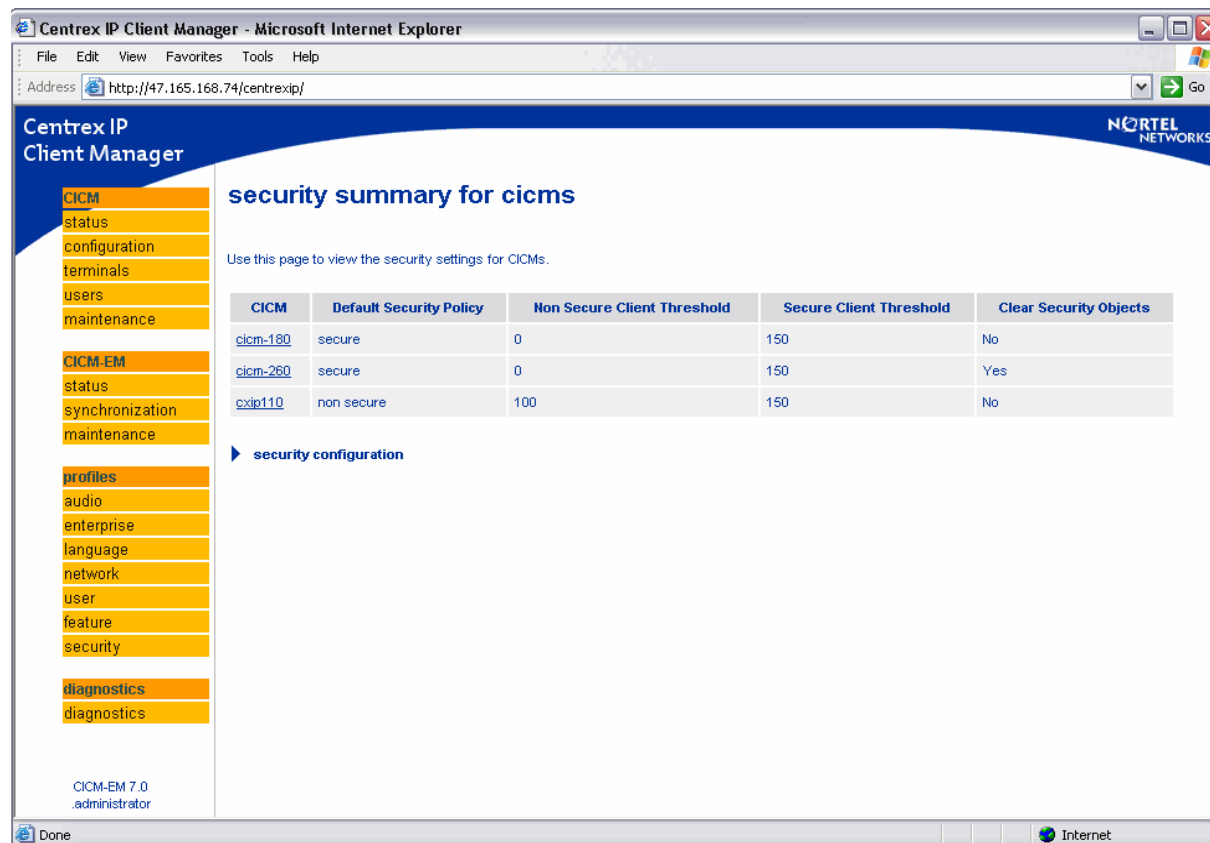
All clearing actions can be performed from the Security profile page (the link is found under the profile menu list on the left hand side of the CICM EM web page). The following diagram shows the Security profile page. This page provides the following capabilities:

- Managing RSA keys for a CICM
- Viewing Security Policies for CICMs
- Viewing Security Policies of Enterprises
- Viewing Clear Security Objects setting for terminals

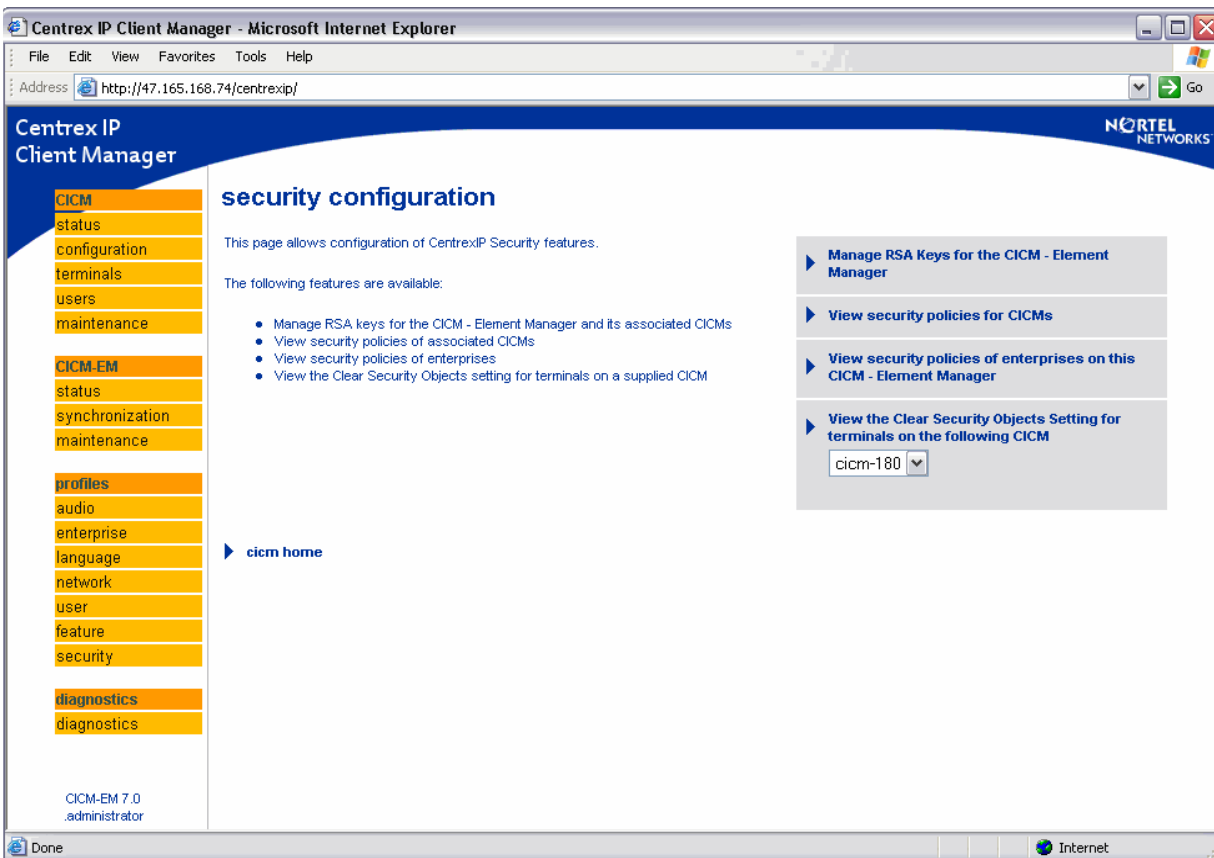
Note, that only the Clearing of Security objects will be discussed. For further information about Security profiles and RSA Key management refer to Ref 2.5

Unisim Security FN - found in clearcase in documents/ipcentrex/series2.5/features/unistimsecurity.

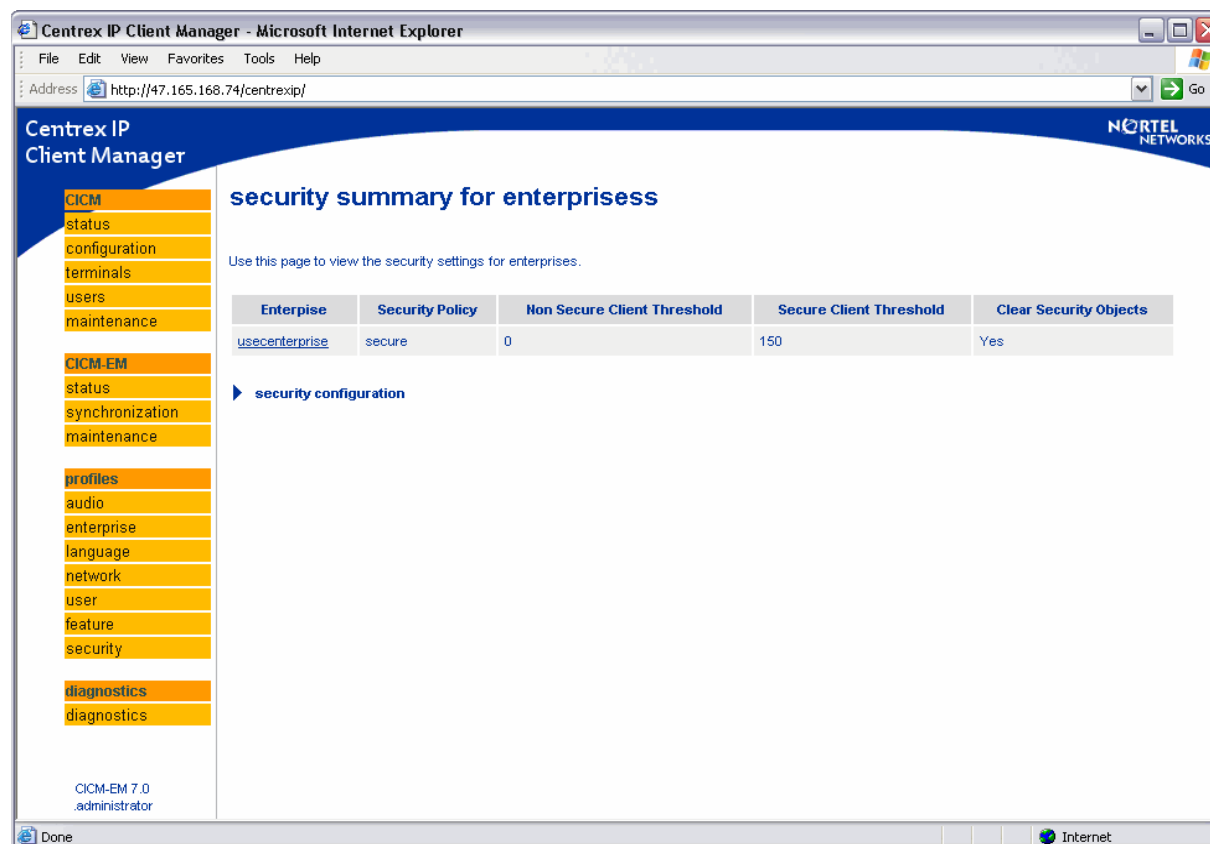
Figure 1 Security Profile



The following figure shows an example of what is displayed when the CICM EM is navigated to view the Security Policies for CICMs hosted by the CICM EM.

Figure 2 Security Policies for CICMs

The following figure shows an example of what is displayed when the CICM EM is navigated to view the Security Policies for Enterprises hosted by the CICM EM.

Figure 3 Security Policies for Enterprises

The following figure shows an example of what is displayed when the CICM EM is navigated to view the Clear Objects Settings for terminals. Note that the following can be accessed two different ways. The first is directly from the Security Profile page. The second is to perform a Terminal Audit as shown in 5. The link on the Security Profile page is just a short cut in performing the terminal audit.

Figure 4 Clear Security Objects settings for terminals

The screenshot shows the Centrex IP Client Manager web interface in a Microsoft Internet Explorer browser window. The address bar shows <http://47.165.168.74/centrexip/>. The page title is "Centrex IP Client Manager" and the Nortel Networks logo is in the top right corner.

The left sidebar contains a navigation menu with the following items:

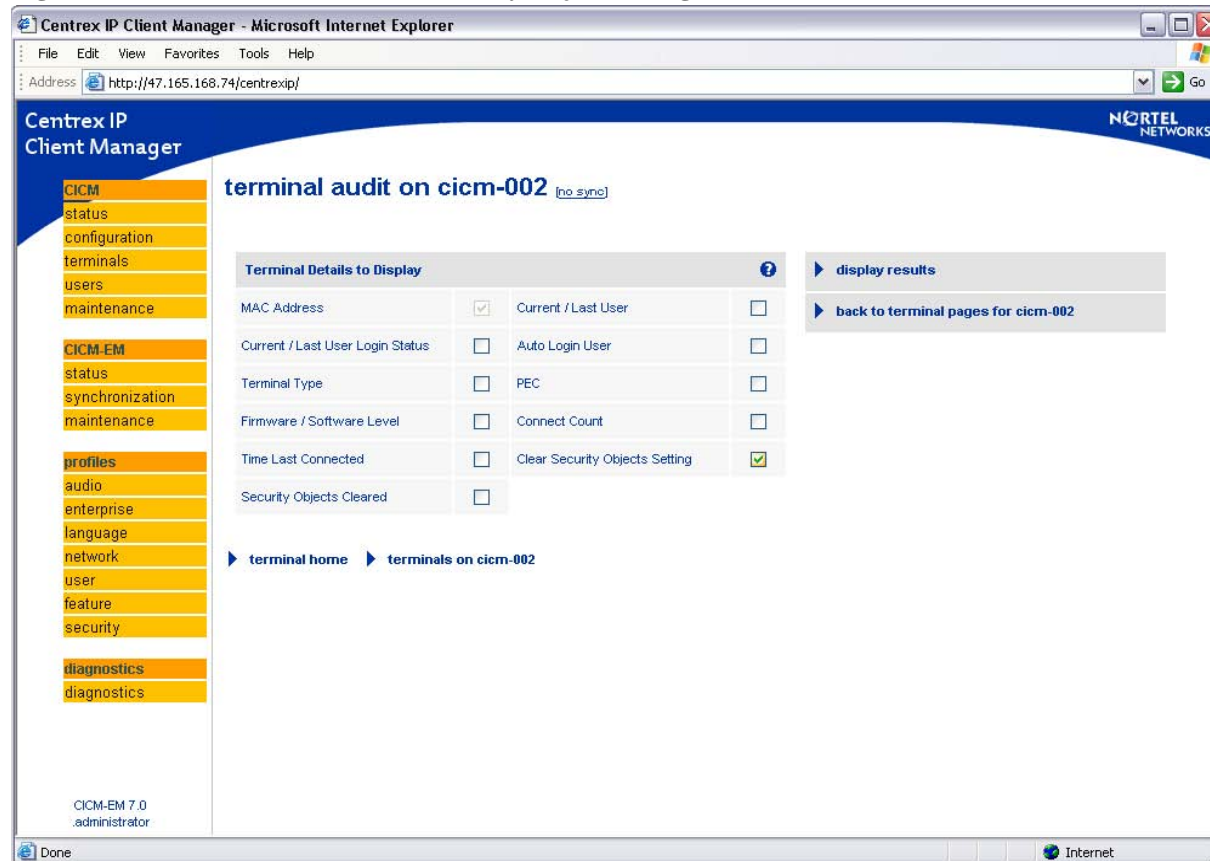
- CICM
 - status
 - configuration
 - terminals
 - users
 - maintenance
- CICM-EM
 - status
 - synchronization
 - maintenance
- profiles
 - audio
 - enterprise
 - language
 - network
 - user
 - feature
 - security
- diagnostics
 - diagnostics

The main content area is titled "terminal audit results on cicm-180". It contains a table with the following data:

MAC Address	Clear Security Objects
31-38-00-0A-E4-02-E3-B6	No
31-38-00-0A-E4-05-F1-FD	Yes
31-38-00-0A-E4-05-F1-FE	No
31-38-00-60-36-76-A8-88	No
31-38-00-60-36-DD-1B-0D	Yes

Below the table, there are navigation links: [terminal home](#) [terminals on cicm-180](#) [terminal audit on cicm-180](#).

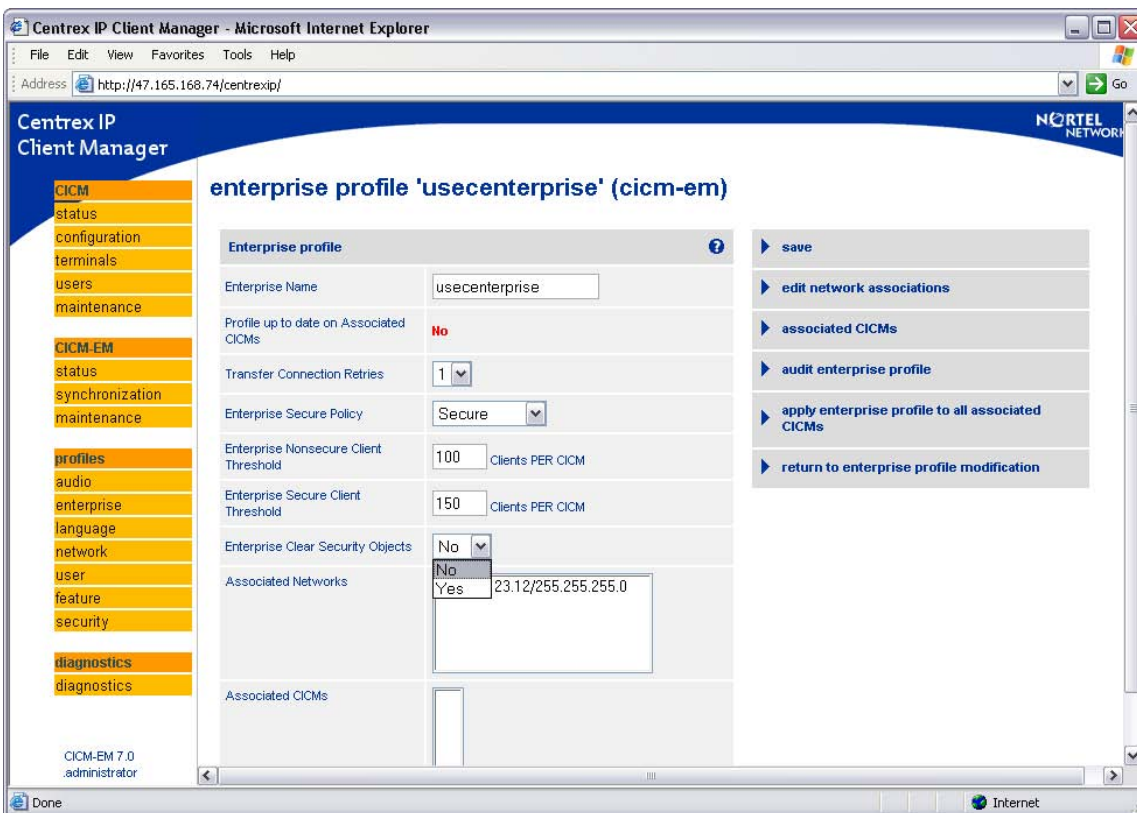
At the bottom left, it says "CICM-EM 7.0 administrator". At the bottom right, there is an "Internet" icon.

Figure 5 Terminal Audit for Clear Security Object Settings

119.2.3 Clearing Security Objects at a Enterprise level

This section describes how to change the Clear security objects setting at an Enterprise level. In order to change the Clear Security Objects setting the user must navigate the CICM EM web page to the Enterprise profile view as shown in 6. It is here that the user can then select the setting for the Clear Security Objects and click on the Save menu item on the right hand side. Note that for the setting to take effect the profile must be associated and applied to a CICM or set of CICMs.

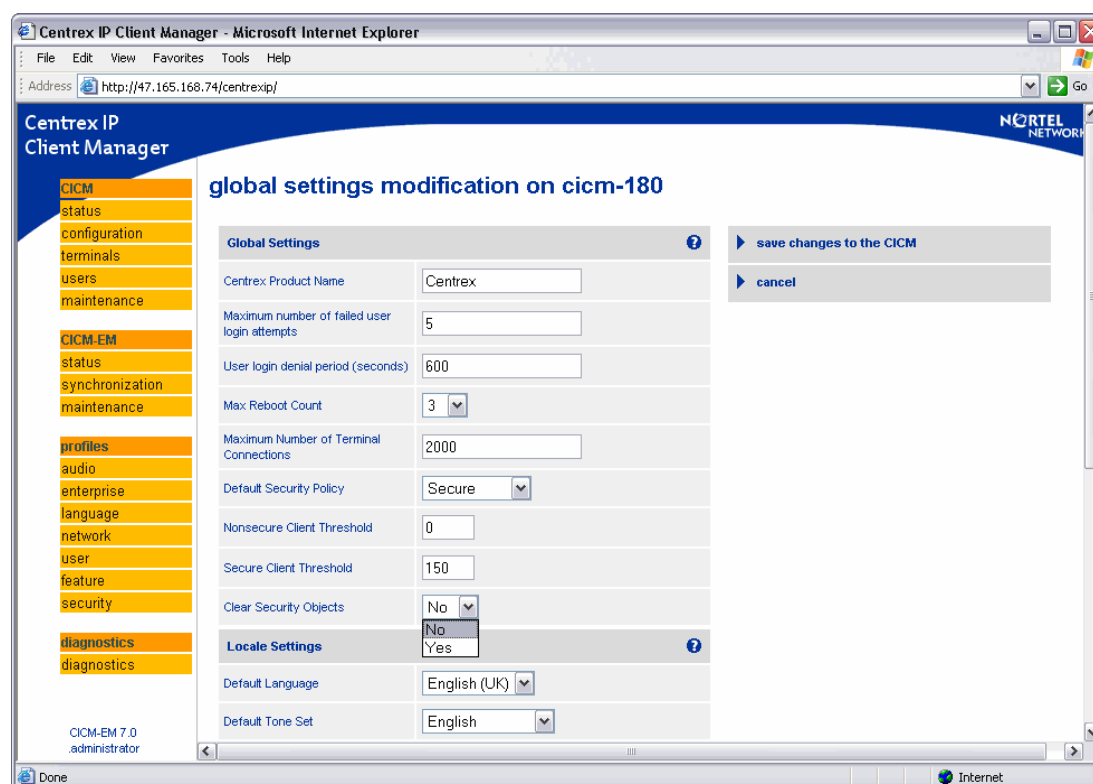
Figure 6 Clear Objects Setting for an Enterprise



119.2.4 Clearing Security Objects at a CICM level

This section describes how to change the Clear security objects setting at a Gateway (CICM) level. In order to change the Clear Security Objects setting the user must navigate the CICM EM web page to the global settings page for the particular CICM as shown in 7. It is here that the user can then select the setting for the Clear Security Objects and click on the Save menu item on the right hand side.

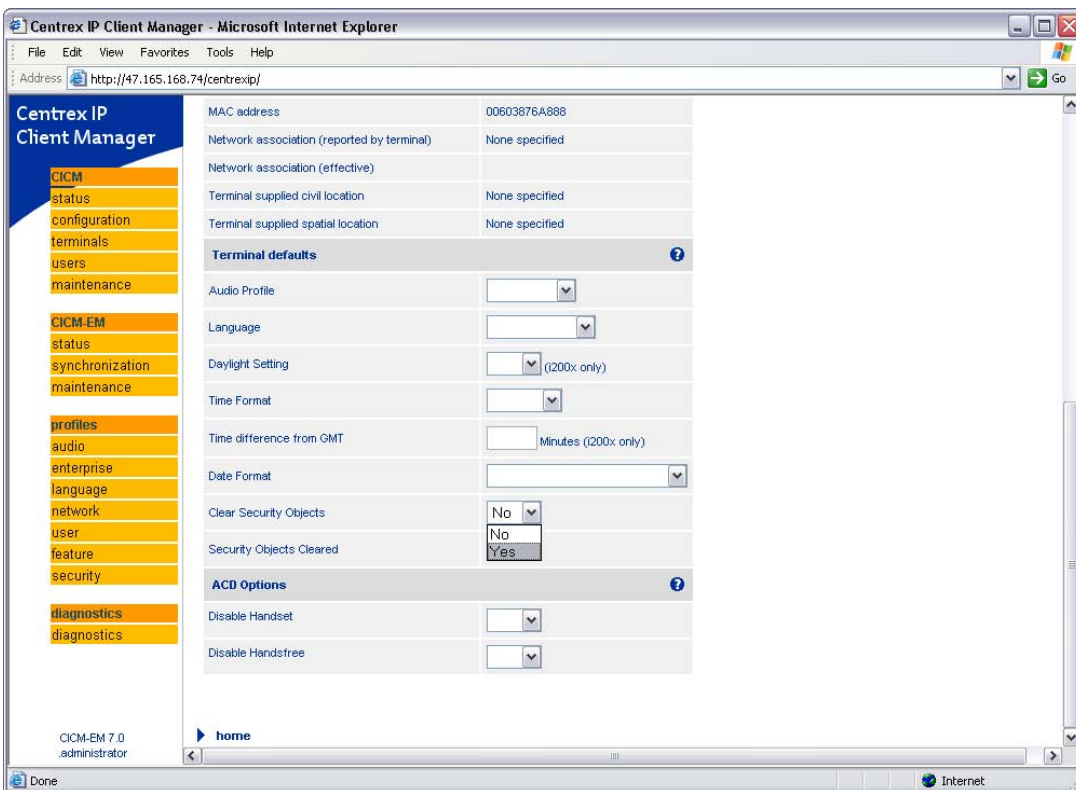
Figure 7 Clear Objects Setting for a Gateway



119.2.5 Clearing Security Objects at a Terminal level

This section describes how to change the Clear security objects setting at terminal level. In order to change the Clear Security Objects setting the user must navigate the CICM EM web page to the terminal settings page as shown in 8. It is here that the user can then select the setting for the Clear Security Objects and click on the Save menu item on the right hand side.

Figure 8 Clear Objects Setting for a Terminal



119.2.6 Clear Security Objects Setting Precedence

The following table illustrates the impact of setting the Clear Security Objects setting for each of the three aforementioned levels.

Table 1 Clear Security Objects Setting Precedence

Enterprise	Gateway	Terminal	Clear Objects	Comments
No	No	No	No	
No	No	Yes	Yes	Only the specific terminal will have objects cleared.
No	Yes	No	Yes	All terminals on the GW will have objects cleared.
No	Yes	Yes	Yes	
Yes	No	No	Yes	All terminals under the Enterprise will have objects cleared.
Yes	No	Yes	Yes	
Yes	Yes	No	Yes	
Yes	Yes	Yes	Yes	

119.2.7 Timing of the Clearing of Security Objects

When the Clear Security Object setting has been set to Yes (in any of the above cases) the results may not be seen immediately. Any clients connecting after the setting has been made will have the Security Objects Cleared post security

handshake. For clients already connected the changes could be seen up to 60 minutes after the setting has taken place.

Note: Depending upon implementation of how terminals are notified about the status of this setting the timing may change. This section will be updated once implementation details have been worked out.

119.2.8 Resulting Client Interactions

When the Security objects are cleared on a client the following will occur.

- The user will first be forced to logout. The transition to non secure mode will then be initiated.
- Once the transition has been completed successfully the user will be notified that the transition has been completed. Refer to Figure 9 i2001 transition completed9 and Figure 10 Softclient transition completed10 for the user notification.
- Once the security objects have been cleared the user should disconnect and reconfigure the server settings to connect to the new server.
- Once the client has been transitioned successfully the server will not respond to any Unistim messaging from that terminal, therefore any attempt to reconnect will eventually result in a timeout.
- The new server that the client connects to must allow for non secure connections. Once the terminal has connected to the new server, the server can then transition the new client into secure mode.

Figure 9 Figure 9 i2001 transition completed

Figure 10 Figure 10 Softclient transition completed



119.2.9 Failing to Transition the client

There are two steps in transitioning a client. The first is the clearing of the security objects. The second is the transitioning of the client from secure mode to non secure mode (setting of the action byte). There is a possibility of this transition failing i.e.) if one of the messages is lost or the client disconnects during the transition. The following table describes the symptoms of a failure and a resolution for the failure.

Table 2 Transition Failures

Table 2 Transition Failures

Clear Objects	Action byte	Symptoms	Resolution
Fail	Fail	The client will reconnect to the server and the transition will be attempted again.	No action is necessary. The server will attempt the transition once the security handshake has been completed
Fail	Pass	The client will be able to connect to servers in non secure mode. However it will fail to be transitioned into secure mode as the client will have an invalid fingerprint. This is assuming that the new server has a different fingerprint. If it is the same fingerprint then the secure transition will succeed.	A manual reset of the client is required.
Pass	Fail	The client will attempt to connect in secure mode. This however will fail. The authentication of the server will fail. CICM Logs stating that authentication failed will be generated. Clients will display that a security error has occurred.	A manual reset of the client is required.

119.2.10 Completing the Transition

There are two possible actions that may be performed to complete the transition. The first is to reset the “Security Object Cleared” setting for a terminal. The second is to clear the terminal records.

The following sections illustrate the two possible ways to complete the transition.

119.2.10.1 Resetting the Security Objects Cleared

When the “Security Objects Cleared” terminal setting is “yes” the terminal will not be able to connect to the hosting CICM. If it is desired to allow this terminal to reconnect this setting can be set to “No”. The following figures show how to perform the reset. The “Security Objects Cleared” setting for a terminal can be queried using the terminal audit page as show in 11. From there the terminal can be selected and the setting can be set to “No”.

Figure 11 Terminal Audit

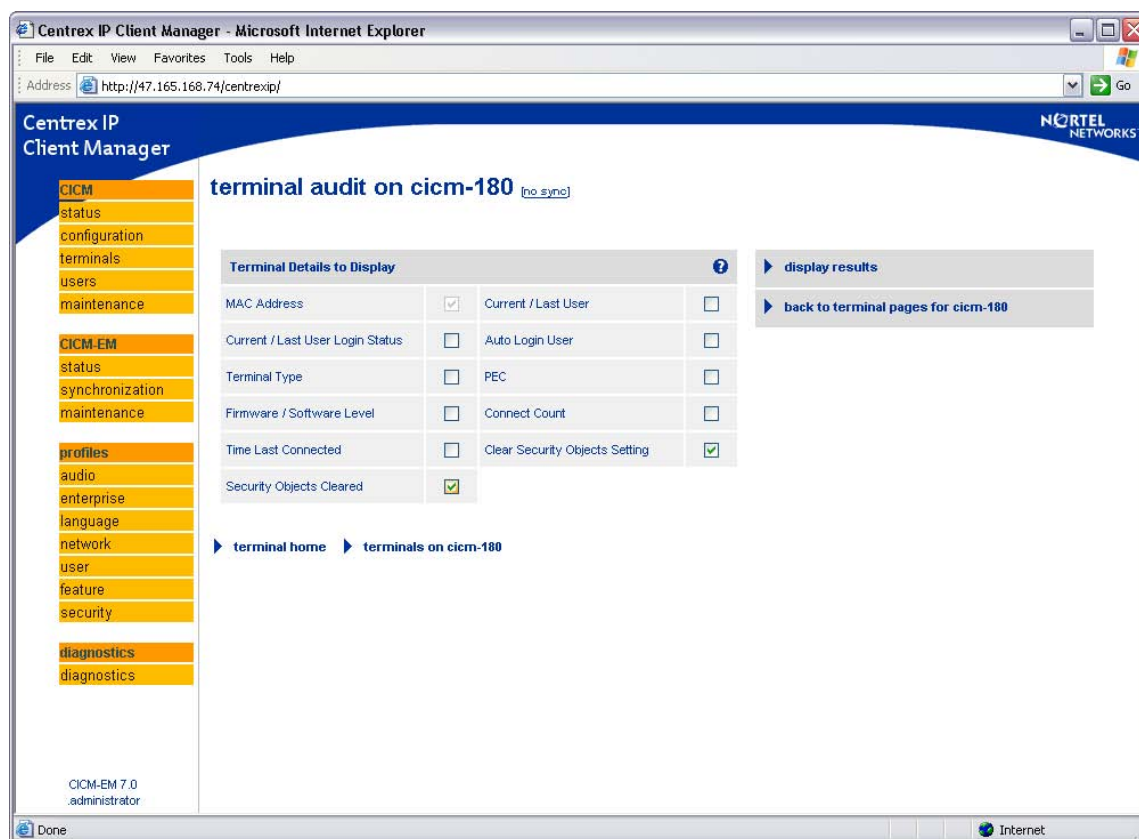


Figure 12 Terminal Audit Results

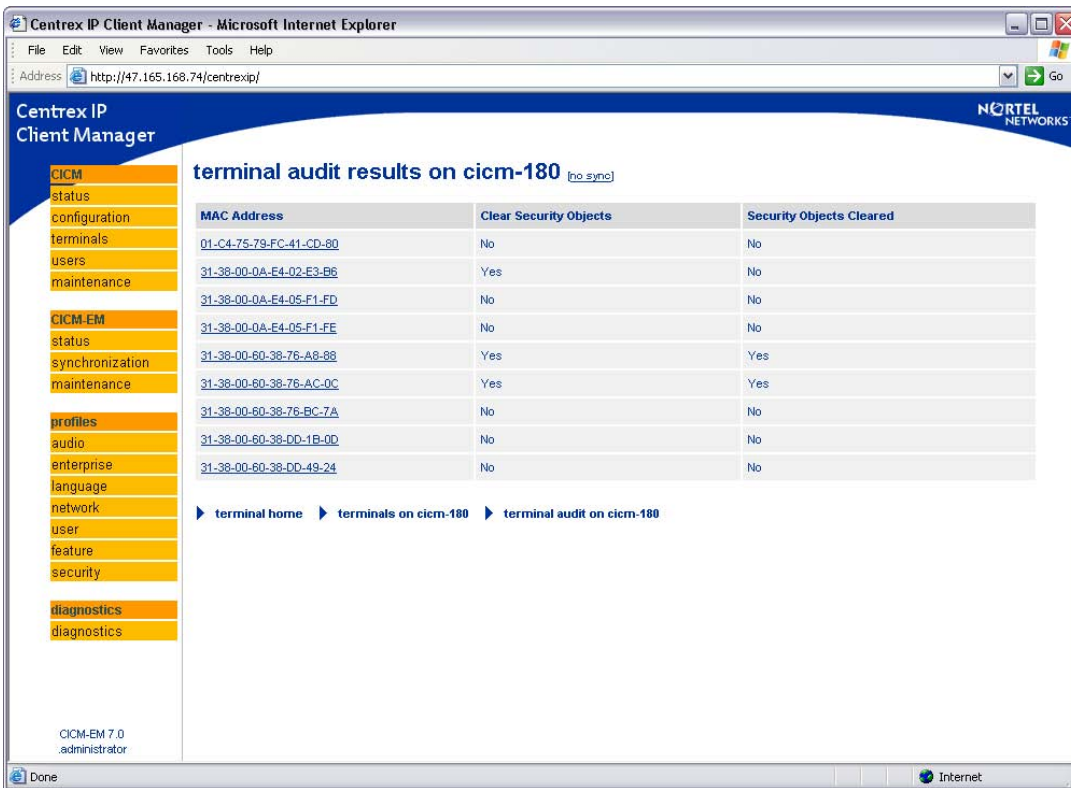
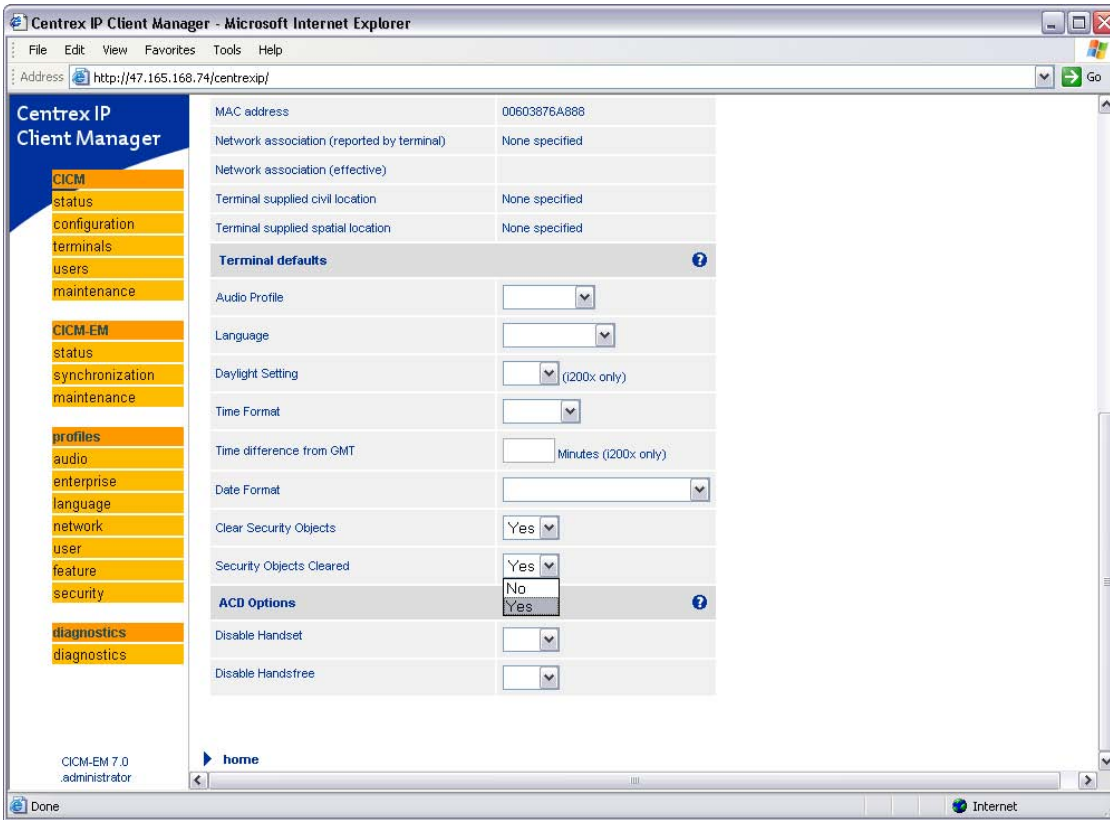


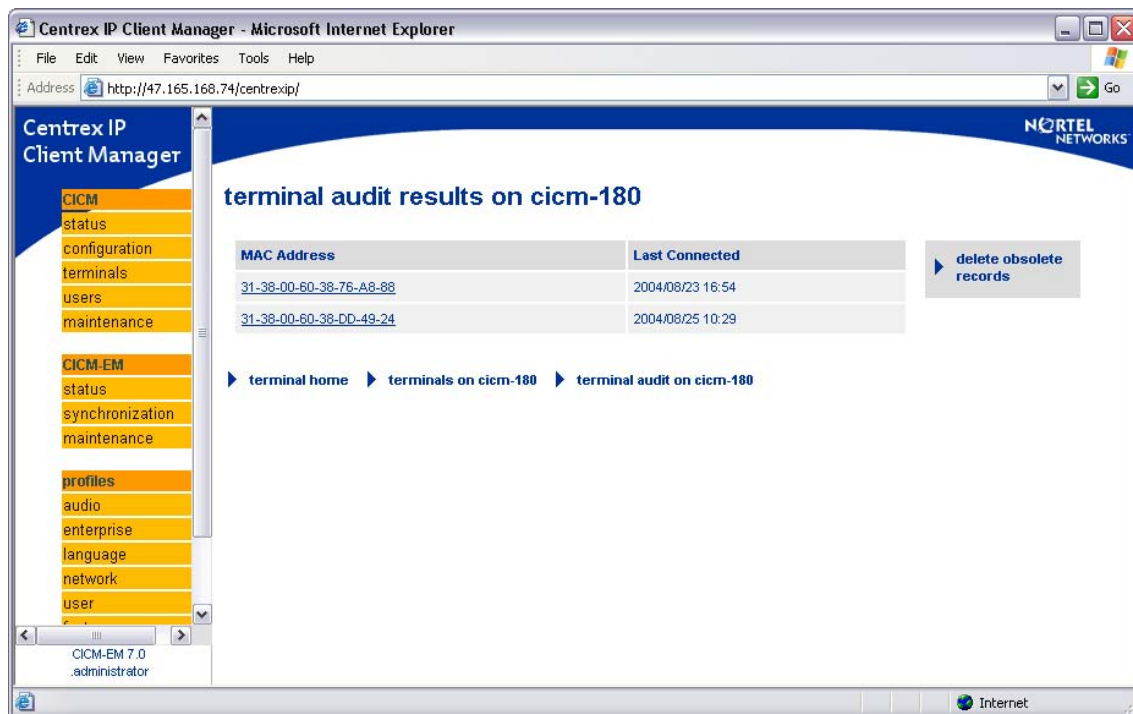
Figure 13 Resetting Terminal Objects Cleared



119.2.10.2 Clearing Terminal Records

Once the transition has been completed the terminal records can be removed. This can be done by selected the delete obsolete records from the terminal audit results web page shown in Figure 14, "Deleting Terminal Records". Note that this should only be done once the terminals have performed the transition and have been reconfigured to connect to the new server. If this deletion is done prior to the completion of the terminal transition, the terminal will be in a non recoverable state. The only means to correct this problem will to be manually reset the terminals.

Figure 14 Deleting Terminal Records



119.3 Logs (LG)

See Ref 2.5 Unisim Security FN - found in clearcase in documents/ipcentrex/series2.5/features/unistimsecurity for logs introduced by this feature.

119.4 Data schema (DS)

See Ref 2.5 Unisim Security FN - found in clearcase in documents/ipcentrex/series2.5/features/unistimsecurity for additional MIB entries introduced by this feature.

Table 3 MIB Entries

MIB name (registry key etc)	MIB version	Description
HKEY_LOCAL_MACHINE\SOFTWARE\Nortel Networks\CentrexIP International Gateway\7.2\terminal\<Terminal ID>\ClearSecurityObjects	7.2	Setting for the clearing of security objects at a terminal level. True or False.

HKEY_LOCAL_MACHINE\ SOFTWARE\Nortel Networks\ CentrexIP International Gateway\ 7.2\terminal\<Terminal ID>\SecurityObjectsCleared	7.2	Used to determine if the terminal has been instructed to clear the security objects.
HKEY_LOCAL_MACHINE\ SOFTWARE\Nortel Networks\ CentrexIP International Gateway\ 7.2\profile\enterprise\<enterprise ID>\ClearSecurityObjects	7.2	Setting for the clearing of security objects at an enterprise level. True or False.
HKEY_LOCAL_MACHINE\ SOFTWARE\Nortel Networks\ CentrexIP International Gateway\ 7.2\ClearSecurityObjects	7.2	Setting for the clearing of security objects at a gateway level. True or False.

119.5 Operating system parameters (OP)

None changed.

119.6 Alarms (AL)

This feature will introduce no new alarms.

119.7 New/modified filesystem directories (FS)

See Ref 2.5 Unisim Security FN - found in clearcase in documents/ipcentrex/series2.5/features/unistimsecurity for new directories introduced by this feature.

119.8 Command interface (CI)

There will be no modifications to the command interface.

119.9 Licensing

No new licensing requirements.

119.10 References

Ref 2.5 Unisim Security FN - found in clearcase in documents/ipcentrex/series2.5/features/unistimsecurity

120: A00007709 Functional description (FN)

120.1 Feature name

MCS CD Phase 2 Support.

120.2 Description

MCS Converged Desktop Phase 2 is a MCS feature that has a dependency on switch-based functionality in order to provide the presence-indication and call logging services for non-MCS (i.e., switch based) subscribers.

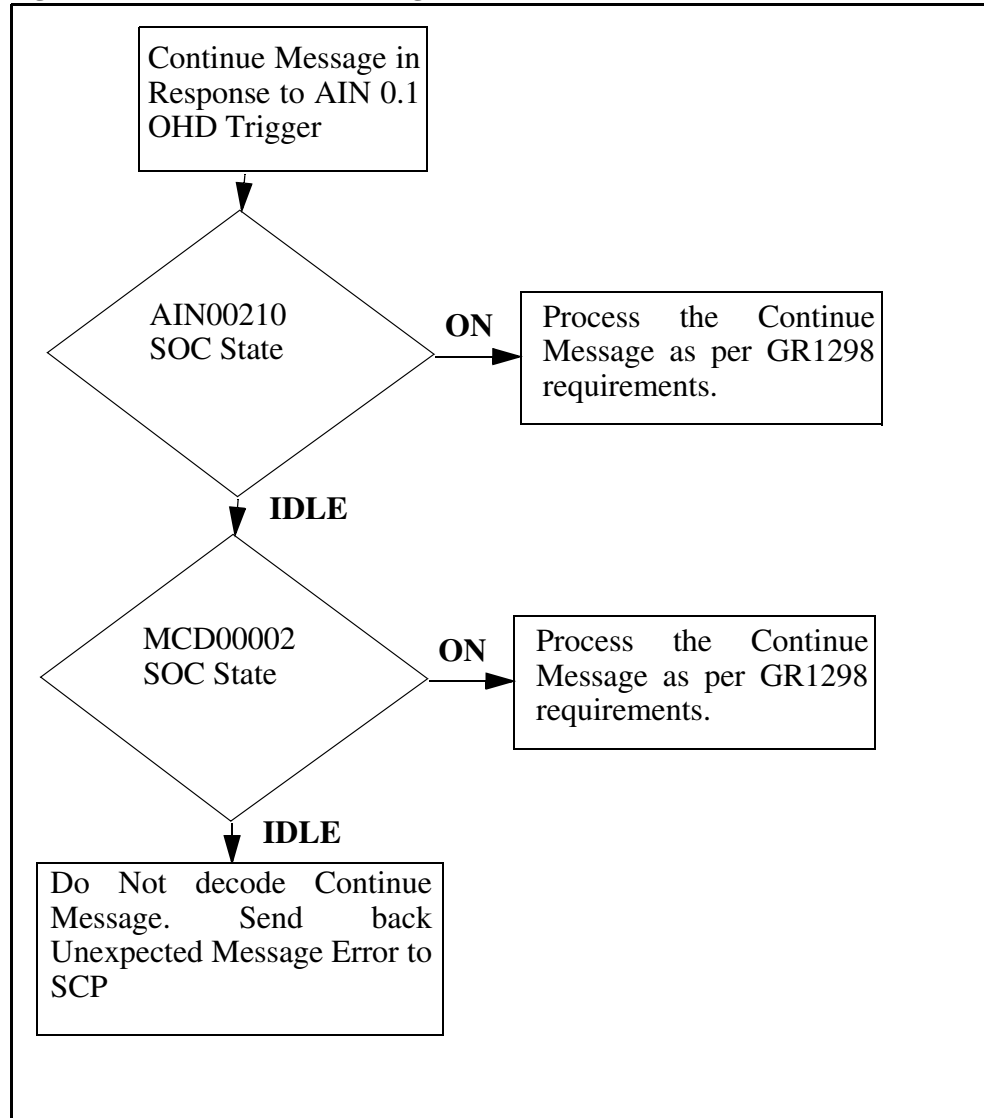
This switch based functionality is controlled by a new Software Order Code (SOC) MCD00002 in SN08. This new order code implemented by this activity replaces ACT patches SBB44 for SN04/SN06/SN07 releases and TWH36 for SN06/SN07 releases.

This feature, when enabled via the SOC MCD00002 along with AIN 0.1 (AIN Essentials) software, will enable the MCS Converged Desktop Phase 2 feature to operate correctly. It does so by adding incremental AIN support for CONTINUE response to the AIN 0.1 Off Hook Delay (OHD) trigger query message.

The SOC option MCD00002 is dependent on AIN Essentials software; order code AIN00006. It may only be enabled and used in conjunction with MCS Converged Desktop and is not supported for any other application.

When a MCS CD office with patch TWH36/SBB44 activated on SN06/SN07 upgrades to SN08 or a higher release, the SOC option MCD00002 will be automatically turned ON during ONP.

Please refer to figure 1 “Functional Behavior Diagram” on page 956 for an overview of how SOC MCD00002 and AIN00210 control the AIN Continue message functionality for the OHD trigger.

Figure 1 Functional Behavior Diagram**120.3 Hardware Requirements or Dependencies**

None.

120.4 Software Requirements or Dependencies

AIN Essentials.

120.5 Limitations and restrictions

None.

120.6 Interactions

No new AIN feature interactions are introduced by this feature.

120.7 Glossary

Table 1

Term	Description
AIN	Advanced Intelligent Network
CONT	Continue
SCP	Service Control Point
SOC	Software Optionality Control
SSP	Service Switching Point

121: A00007713 Functional description (FN)

121.1 Feature name

TOPS-IP Robustness

121.2 Description

The feature enhances the TOPS-IP product with the following:

- A TOPS615 information log indicating operator teams and number of positions in each team using voice auto-compression is created.
- The post command in the mapci;mtc;appl;topsip;topspos level is enhanced to create a post set of all in service IP positions with auto-compression on. The listset command displays the positions in the posted set. The info command in the mapci;mtc;appl;topsip;topspos level is enhanced to display the auto-compression status for the posted position.

121.2.1 Background

IP positions typically select the G.711 voice packet protocol as long as voice quality (latency, jitter, packet loss) is acceptable. When facilities are lost or data network equipment fails, and the available bandwidth is less than that required for IP positions, network performance degrades (that is, packet loss and jitter increase). IP positions detect the network quality degradation and will go into the voice auto-compression mode selecting the G.723 protocol on the next call. Once auto-compression is entered, the position remains in that mode for approximately four hours.

121.2.2 New Functionality

121.2.2.1 TOPS615 Log

The IP position sends an auto-compression message to TOPS to indicate the position has voice auto-compression turned on. When the position exits the auto-compression mode, an auto-compression message indicating off is sent.

The TOPS615 information log is generated indicating the operator teams and the number of positions in each team with auto-compression turned on. The log is generated if an auto-compression message has arrived during an approximate 5 minute audit period. It is also generated if an IP position with auto-compression turned on goes through a service affecting state change (i.e. bsy). Once auto-compression has been turned off for all positions, the log indicates no operator teams or positions have auto-compression on.

121.2.2.2 TOPSPOS MAP Post / Info Commands

The mapci;mtc;appl;topsip;topspos post command has parameter 'AC' added. When used, this parameter creates a post set of all in service IP positions with voice auto-compression turned on. The listset command is then used to display the position list.

The mapci;mtc;appl;topsip;topspos info command is enhanced to display the auto-compression status for the posted position.

121.3 Hardware Requirements or Dependencies

None

121.4 Software Requirements or Dependencies

- TOPS base functionality, SOC option OSB00101

121.5 Limitations and restrictions

- The auto-compression status of IP positions is not maintained during the One Night Process norestartswact. The auto-compression status is turned off for all IP positions after the norestartswact.
- If the auto-compression message indicating auto-compression has been turned off is lost, manual intervention (i.e. bsy) may be required to update the auto-compression status.
- If the auto-compression message indicating auto-compression has been turned on is lost, the auto-compression status in the switch is not updated to indicate an on status. In this event, the RAMP position may be utilized to verify the auto-compression status.
- The IP position software must be capable of sending the auto-compression message.

121.6 Interactions

TOPS-IP positions send TOPS an auto-compression message indicating if auto-compression is on or off.

121.7 Glossary

Table 1

Term	Description
IP	Internet Protocol
MAP	Maintenance and Administration Position
RAMP	Remote Access Maintenance Position

122: A00007717 Functional Description (FN)

122.1 Feature name

Health Monitor Logs

122.2 Logs

122.2.1 Radius Server Health Monitor (EMSS 313)

122.2.1.1 Format

Note 1: This log is sent directly to syslog via 'logger' UNIX utility.

Note 2: Replace all 'carriage returns' below with '^M' characters in code that generates the log.

May 10 18:03:56 host1 radsvrHealthMonitor.ksh[pid]: EMSS313 NONE INFO EMSS

Location: 191.1.1.1

Time: May 10 18:03:56

Category: processingErrorAlarm

Probable Cause: outOfService

Component Id: CLASS=SYS;SYSTYPE=SECMon;SECMonComp=RADSVR

Description: RADSVR is unhealthy, will restart if currently running.

122.2.1.2 Field Descriptions

Table 1 Field descriptions

Field	Value
Category	processingErrorAlarm
Severity	NONE
LogName	EMSS
LogNumber	313
EventType	INFO
Probable Cause	outOfService

122.2.1.3 Description / Explanation

This log is produced when ever the radius server health monitor detects the radius process is not functional.

122.2.1.4 Recovery Action

The health monitor will automatically try to restart the radius server if it is running already.

122.2.1.5 Additional information

Not applicable.

122.2.2 Identity Server Health Monitor (EMSS 314)

122.2.2.1 Format

Note 1: This log is sent directly to syslog via 'logger' UNIX utility.

Note 2: Replace all 'carriage returns' below with '^M' characters in code that generates the log.

May 10 18:03:56 host1 isHealthMonitor.ksh[pid]: EMSS314 NONE INFO EMSS

Location: 191.1.1.1

Time: May 10 18:03:56

Category: processingErrorAlarm

Probable Cause: outOfService

Component Id: CLASS=SYS;SYSTYPE=SECMon;SECMonComp=IS

Description: Identity Server (IS) is unhealthy, will restart if currently running.

122.2.2.2 Field Descriptions

Table 1 Field descriptions

Field	Value
Category	processingErrorAlarm
Severity	NONE
LogName	EMSS
LogNumber	314
EventType	INFO
Probable Cause	outOfService

122.2.2.3 Description / Explanation

This log is produced when ever the identity server health monitor detects the identity server process is not functional.

122.2.2.4 Recovery Action

The health monitor will automatically try to restart the identity server if it is running already.

122.2.2.5 Additional information

Not applicable.

122.2.3 PAM Login Servlet Health Monitor (EMSS 315)**122.2.3.1 Format**

Note 1: This log is sent directly to syslog via 'logger' UNIX utility.

Note 2: Replace all 'carriage returns' below with '^M' characters in code that generates the log.

May 10 18:03:56 host1 pamloginservletHealthMonitor.ksh[pid]: EMSS315
NONE INFO EMSS

Location: 191.1.1.1

Time: May 10 18:03:56 2004

Category: processingErrorAlarm

Probable Cause: outOfService

Component Id: CLASS=SYS;SYSTYPE=SECMon;SECMonComp=WEBSERVICES

Description: PAM login servlet is unhealthy, restarting WEBSERVICES.

122.2.3.2 Field Descriptions

Table 1 Field descriptions

Field	Value
Category	processingErrorAlarm
Severity	NONE
LogName	EMSS
LogNumber	315
EventType	INFO

Field	Value
Probable Cause	outOfService

122.2.3.3 Description / Explanation

This log is produced when ever the PAM login servlet health monitor detects the PAM login servlet is not functional.

122.2.3.4 Recovery Action

The health monitor will automatically try to restart WEBSERVICES via servman if it is running already.

122.2.3.5 Additional information

Not applicable.

123: A00007744 Functional description (FN)

123.1 Feature name

File Naming Convention for Nortel Carrier Grade Linux (NCGL)

123.2 Description

An updated file naming convention is to be put in place to provide several improvements over what is currently used. Current file names are hindering efforts to automate the build processes of the product groups that are utilizing NCGL software. Often files have to be manually renamed before they can be integrated into the product's build environments. In addition, tracking of different file versions is not well defined in the current practice.

The naming convention proposed in this document may be applied as required to any of the files provided by NCGL Loadbuild. This includes the API and CBE binary package files, source code archives, configuration files, and makefiles (including the ".in" product include files).

A special case is the naming of binary image files. The format of these files has already been decided upon by the NCGL Design and GNPS groups in order to facilitate patch management. At this time the strategy is to provide both the image files with their original names as well as a tarfile that does follow the new naming convention that contains the image. This way image files can be automatically distributed using the new name format, and yet retain the original version information expected by GNPS patching tools.

123.3 Hardware Requirements or Dependencies

No new hardware requirements are introduced by this feature.

123.4 Software Requirements or Dependencies

This feature will deliver a naming convention which will impact how the loadbuild group prepares files for each build. This will impact loadbuild's scripts and the way the NCGL software is organized within its software repository. Other than this there are no software requirements that impact the product software.

The format shown below proposes generating filenames by organizing each file's describing attributes into parts as follows:

```
{Product_prefix-}[Original_Name_and_Version][.NCGL_version_info]
{-Target_info}.[filetype_extension]
```

Fields in "{ }" are optional.

A note about the separators used: a dot (“.”) is used before the NCGL version information when it extends an existing original version code. If, however, the original package name did not include a version code, then a dash (“-”) will precede the NCGL version code.

A further refinement of this format is to remove the distinction between the original parts of the name as follows:

```
{Product_prefix-}[basename-][version_info]{-target_info}.[filetype_extension]
```

where `version_info` can then be broken down into:

```
[original_version][.NCGL_version_extension]
```

Note that if there is no original version code then the dot before the NCGL version part is dropped.

123.4.1 Original Name and Version information

The file’s **original_name_and_version** substring is intended to reflect whatever name the original provider assigned to the file. This is so that the original version information is retained which often proves useful in preventing confusion about the source of the file. Any revisions to the file by the NCGL team are reflected in the **NCGL_version_info** substring (see below).

As an example, typical original package filenames would be:

```
glib-2.4.0.tar.gz
```

```
glibc-2.3.2.tar.gz
```

The trailing “tar.gz” is actually considered the filetype extension, thus the original name and version substring would be “glib-2.4.0”. While the original name is typically an alphanumeric string, and the version code is a numeric code separated by dots, there is currently no universal convention which absolutely defines this pattern. This is not to say that attempts have not been made (see, for example, www.freestandards.org), but a universally accepted convention does not seem to have been adopted at this time.

Thus there are some risks in retaining the exact original name as in some cases they do not match conventions followed in the Linux open source community. There are reported problems with filenames that break version comparison utilities such as those used by RPM (the Red Hat Package Management system) and Gentoo’s Portage system. At this time such situations will need to be handled manually by a re-mapping of the name to something which works, or by manually managing the files within a build environment directory structure.

123.4.2 Product Prefix

This prefix allows distinction between files prepared for different platforms. This attribute group would likely benefit from being defined as a controlled set, with the following initial definition:

```
{srp, mpe280, mpe405, (none)}
```

This prefix may be empty for files that have no product specific content. (Note: The “devl” prefix was used to designate CBE or compiler host packages, but does not seem to be necessary for users other than the kernel development teams.)

Other prefix set entries are to be defined by the appropriate Release Engineering/Development/Product team.

123.4.3 Target Information

This attribute group provides information about the machine architecture of the intended target. It encompasses the target processor, format, and for cross compiled products information about the libraries used.

This information string can be broken down into sub-fields as follows:

```
[processor_id] - [format_id]
```

where **processor_id** is one of

```
{ppc, x86, mipsel, mips64el},
```

and **format_id** is one of

```
{n32, o32, n64, (none)}.
```

At this time only the Dolphin product files require this format_id. Files for other products will omit this sub-string.

For example, in the following filename the target information specifies that this package was built for the Mips processor, and the o32 library format:

```
gdbm-1.8.3.0.20040722-mipsel-o32.tar.gz
```

Refer to Appendix A for further examples in a mock-up sample directory listing.

123.4.4 NCGL Version Information

This is an indication of a version separate from that of the file’s original provider. It is specific to modifications made by the NCGL team.

For the near future, this substring is to be defined as **0.yywk.bb**. In this definition “yy” is the last 2 digits of the year, “wk” is the week number, and “bb” is a build number within that week.

The leading ‘0.’ is included to allow for future changes of the NCGL versioning scheme. If at a later time a new format for the NCGL is decided upon, then *removing* this leading zero will guarantee that those files moving to the latest format will always be considered newer than files with the previous format (assuming, of course, that the new format will not ever need to have a leading zero).

Refer to Appendix B for some proposed formats being considered for a future version of the NCGL version string.

123.4.5 File Type Extension

The file type extension describes a file format, such as whether the contents are text, binaries, if the file contents have been archived using **tar**, or compressed using **gzip** or **bzip2**.

The format of the extension should follow those in common usage by the Linux/Open Source community.

Typical type extensions:

txt

tar

gz

bz2

Note that it is common practice to string together all format types that apply to a file, separated by dots. For example, an archived and compressed file might have an extension of “tar.gz”. Also, in some cases the extension may be dropped if the name of the file already implies its contents (such as for Makefiles).

Enforcing a consistent use of file types would allow the use of default file openers.

123.5 File Category Details

To further describe how this naming convention will apply to the files, details of each file category is presented here. Following a brief description of each category are example filenames to demonstrate the convention.

123.5.1 CBE tarfiles

The Common Build Environment provides a consistent system in which to run a compiler used to build all NCGL deliverables (loads, kernel images).

Although the product groups may not elect to use the CBE, information about the build context (i.e. header files or other kernel interface descriptions) is sometimes required in order to successfully compile applications or modules (KLMs) for use with the NCGL kernels.

All the CBE packages are provided in the form of tarfiles, and the product groups take any that are needed.

- No product prefix code
- NCGL version info required
- Target information required

Examples:

Dolphin Old: devl-gdbm-1.8.3-mips.20040722-dolphin_apps-mips64-bin.tgz devl-gdbm-1.8.3.200740722-dolphin_apps-mips64-bin.tgz New: gdbm-1.8.3.0.0430.1-mipsel-o32.tar.gz gdbm-1.8.3.0.0430.1-x86.tar.gz
Neptune Old: devl-gcc-3.3.1.20040722-ppc-bin.tgz New: gcc-3.3.1.0.0430.1-ppc.tar.gz
BCM Old: cbe-ppc.tgz New: cbe-0.0430.1-ppc.tar.gz

123.5.2 API tarfiles

As with the CBE tarfiles, the NCGL API tarfiles are used to compile any application that requires knowledge about the kernel interfaces. Unlike the CBE, which is a separate system intended only to support the compiler, these APIs are a part of the NCGL product. Many of the API files have contents that are only a subset of the original packages as they do not need to provide source code, only header information.

- No product prefix code
- NCGL version info required
- Target information required

Examples:

Dolphin Old: devl-gdbm-1.8.3-mips.20040722-dolphin_apps-mips64-bin.tgz devl-gdbm-1.8.3.200740722-dolphin_apps-mips64-bin.tgz New: gdbm-1.8.3.0.0430.1-mipsel-o32.tar.gz gdbm-1.8.3.0.0430.1-x86.tar.gz
Neptune Old: external_gcc_v3_3_1.20040722-nep280-ppc-api.tgz internal_ee_v2_4_0.20040722-nep280-ppc-api.tgz New: gcc-3.3.1.0.0430.1-ppc.tar.gz ee-2.4.0.0.0430.1-ppc.tar.gz
BCM Old: bcm-devel-api.tgz New: bcm-devel-0.0430.1-ppc.tar.gz

123.5.3 Source (aka “Clearcase”) files

These files include things such as the NCGL kernel source, the kernel.config file used during build, makefiles, and the packing inclusion files (“.in” files).

- Product prefix code for kernel configuration only
- No target required
- NCGL version info required

Examples:

Dolphin Old: Makefile dolphin_apps_kernel.config_2004-07-22 ncgl_kernel_src_5.30.1.0.tar.gz New: Makefile-0.0430.1.tar srp-dolphin_apps_kernel.config-0.0430.1.txt ncgl_kernel_src-2.4.22.0.0430.1.tar.gz

Neptune Old: Makefile nep280_kernel.config_2004-07-22 ncgl_kernel_src_5.30.1.0.tar.gz New: Makefile-0.0430.1.tar mpe280-kernel.config-0.0430.1.txt ncgl_kernel_src-2.4.22.0.0430.1.tar.gz

BCM Old: 2.4.22_csc.bcm Makefile bcm-csc.in ncgl_kernel_src_5.30.1.0.tar.gz New: csc.bcm-2.4.22.0.0430.1.txt Makefile-0.0430.1.tar bcm-csc.in-0.0430.1.txt ncgl_kernel_src-2.4.22.0.0430.1.tar.gz

123.5.4 Image files

These files are the kernel images or load images (kernel + rootdisk) that are generated by the build.

As has been noted previously, the names of these files had already been set by the NCGL design and GNPS teams. The prefix of the filename (the product prefix) can be modified without impacting patching tools used by GNPS, but the name and version code that is currently in use must remain as is.

- Product prefix code required

Examples:

Dolphin Old: dolphin_initrd_zImage.initrd_5.30.1.0 New: srp-dolphin_initrd_zImage.initrd_5.30.1.0
Neptune Old: ncgl_nep280_vmlinux_5.30.1.0 ncgl_nep280_zImage.initrd_5.30.1.0 New: mpe280-vmlinux_5.30.1.0 mpe280-zImage.initrd_5.30.1.0

BCM Old: bcm-cscImage New: bcm-cscImage (no change)

123.5.5 Other Build Output files

In addition to the image files, each build generates supplemental debugging information from the build such as symbol maps. The contents of the ramdisk may also be bundled up in a binary package if the product does not use a combined kernel and disk image.

- Product prefix code is always required
- Target information required
- NCGL version info required

Examples:

Dolphin Old: mtcsym.tgz dolphin_apps_rootfs_tarfiles New: srp-mtcsym-0.0430.1-mipsel.tar.gz srp-dolphin_apps_rootfs_tarfiles-0.0430.1-mipsel.tar.gz
Neptune Old: mtcsym.tgz nep280_System.map nep280_ramdisk.image.gz nep280_rootfs_tarfiles.tgz New: mpe280-mtcsym-0.0430.1-ppc.tar.gz mpe280-System.map-0.0430.1-ppc.txt mpe280-ramdisk.image-0.0430.1-ppc.gz mpe280-rootfs_tarfiles-0.0430.1-ppc.tar.gz
BCM Old: rootdisk.image.gz New: rootdisk.image-0.0430.1-ppc.gz

123.5.6 Exceptions

Some of the files obtained from external sources do not follow a convenient naming convention. As stated earlier it is desirable to retain the original

provider's name and version, but what if the existing name does not follow the expected format?

Some options are presented below for consideration:

1. One alternative would be to simply rename any such files with unconventional names. However this means that renaming of all such files would have to continue as an ongoing effort.
2. Another possibility is the use of "Wrapper" packages, meaning that any existing files that have unconventional names would be tarred into a new package that does follow the naming convention.

For example:

```
gdb.5.2-6.tgz → package within
"gdb.5.2.6.0.0430.1-ppc.tar.gz"
```

While providing the wrapper packages would also require some ongoing effort, it seems this option might be more readily automated using a script. There is also some extra work required for the product groups who fetch these packages as they would first have to untar the wrapper, then install the contents are required. It is hoped that this is acceptable as the wrapper provides a filename re-mapping mechanism that should be easy to automate using scripts.

A related issue is the question of how to handle specific single files that have names which do not follow the naming convention. It may be desirable to bundle these single files up into packages for distribution purposes.

For example:

```
{Makefile, mtcsym.tgz, System.map, etc.} ->
"nep280-ncgl_build.0.0.1.0.0430.1-ppc.tar.gz"
```

It would be beneficial if the naming convention used for the package could specify that use of dashes and dots in the `Original_Name_and_Version` be strictly defined in order to make it easier to parse. Of course, the NCGL group has no control over the original naming of any files provided from external sources, but with wrapper packages some measure of control can be gained.

If an additional standard can be imposed by using a wrapper package, then the following convention is proposed for the "Wrapper_Name_and_Version":

```
[Package_name] - [Package_version]
```

In this convention no dashes or dots would be permitted within **Package_name**, and the **Package_version** will consist of a string of decimal digits separated by dots.

Thus valid wrapper names would be:

```
gdb-5.2.6
```

```
nice_new_3PC_package-1.0.0.0.0.0
```

Examples of invalid packages would be:

```
gdb.5.2-6
```

```
not-so-nice_new-3PC.package.1-0.b
```

123.6 Limitations and restrictions

No limitations or restrictions have been identified at this time.

123.7 Interactions

No interactions with other features have been identified at this time.

123.8 Glossary

Table 1

Term	Description
API	Application Program Interface
CBE	Common Build Environment
KLM	Kernel Loadable Module
NCGL	Nortel Carrier Grade Linux
TAR	A file archiving utility, “Tape ARchive”

123.9 Appendix A: Sample file listing

As a visualization aid, here are simulated listings of the NCGL software files under the proposed new naming convention.

The following file listing is based on the **ncgldlpn15ax_sp_80** build (week 30).

123.9.1 Listing 1: NCGL 5.0 Dolphin

```
dolphin_apps/
```

```
Makefile-0.0430.1.tar
```

```
srp-dolphin_apps_kernel.config-0.0430.1.txt
```

```
srp-dolphin_apps_rootfs_tarfiles-0.0430.1-mipsel-n32.tar.gz
```

```
srp-mtcsym-0.0430.1-mipsel.tar.gz
```

```
ncgl_kernel_src-2.4.22.0.0434.1.tar.gz
```

```
api_tar_files/
  gdb-5.2.6.0.0430.1-x86.tar (wrapper)
  ...
  ha_api-1.0.0.0430.1-x86.tar.gz

cbe_tar_files/
  alien-8.26.0.0430.1-x86.tar.gz
  ...
  gdbm-1.8.3.0.0430.1-mipsel.tar.gz
  gdbm-1.8.3.0.0430.1-x86.tar.gz
  ...

dolphin_apps_o32/
  Makefile-0.0430.1.tar
  srp-dolphin_apps_o32_kernel.config-0.0430.1.txt
  srp-dolphin_apps_o32_rootfs_tarfiles-0.0430.1-mipsel-o32.tar.gz
  ncgl_kernel_src-2.4.22.0.0430.1.tar.gz
  srp-postbld_o32_kernel_src-0.0430.1-mipsel-o32.tar.gz

dolphin_initrd/
  Makefile-0.0430.1.tar
  srp-dolphin_initrd_System_map-0.0430.1-mipsel-n32.txt
  srp-dolphin_initrd_kernel_config-0.0430.1.txt
  srp-dolphin_initrd_ramdisk_image-0.0430.1-mipsel-n32.gz
  srp-dolphin_initrd_rootfs_tarfiles-0.0430.1-mipsel-n32.tar.gz
  srp-dolphin_initrd_zImage.initrd-5.30.1.0
  ncgl_kernel_src-2.4.22.0.0430.1.tar.gz
  srp-postbld_initrd_kernel_src-0.0430.1-mipsel-n32.tar.gz
```

123.9.2 Listing 2: NCGL 5.0 Neptune

nep280@ppc ncglnp15ca:

```
api_tar_files/
  gcc-3.3.1.0.0430.1-ppc.tar.gz
  gdb-5.2.6.0.0430.1-ppc.tar
  glib-2.4.0.0.0430.1-ppc.tar.gz
  glibc-2.3.2.0.0430.1-ppc.tar.gz
  libtermcap-2.0.9.0.0430.1-ppc.tar.gz
```

```

libxml2-2.6.4.0.0430.1-ppc.tar.gz
ncurses-5.3.0.0430.1-ppc.tar.gz
ee-2.1.0.0430.1-ppc.tar.gz
ha_api-1.0.0.0430.1-ppc.tar.gz
ipaddr_api-1.0.0.0430.1-ppc.tar.gz
kbuild-2.4.22.0.0430.1-ppc.tar.gz
mercury-2.0.0.0430.1-ppc.tar.gz
ncgl_rpmdb-0.0430.1-ppc.tar.gz

cbe_tar_files/
  alien-8.26.0.0430.1-ppc.tar.gz
  ...
  zlib-1.1.4.0.0430.1-ppc.tar.gz

Makefile-0.0430.1.tar
mpe280-mtcsym-0.0430.1-ppc.tar.gz
ncgl_kernel_src-2.4.22.0.0430.1.tar.gz
mpe280-vmlinux-5.30.1.0
mpe280-zImage.initrd-5.30.1.0
mpe280-System_map-0.0430.1-ppc.txt
mpe280-kernel_config-0.0430.1.txt
mpe280-ramdisk_image-0.0430.1-ppc.gz
mpe280-rootfs_tarfiles-0.0430.1-ppc.tar.gz

```

123.9.3 Listing 3: NCGL 5.0 BCM

```

bcm-csc@ppc/:
csc_bcm-2.4.22.0.0430.1.txt
Makefile-0.0430.1.tar
bcm-csc_in-0.0430.1.txt
bcm-cscImage
bcm-devel_api-0.0430.1-ppc.tar.gz
cbe-0.0430.1-ppc.tar.gz
ncgl_kernel_src-2.4.22.0.0430.1.tar.gz
bcm-rootdisk_image-0.0430.1-ppc.gz

bcm-g4@ppc/:
g4_bcm-2.4.22.0.0430.1.txt

```

```
Makefile-0.0430.1.tar
bcm-devel-api-0.0430.1-ppc.tar.gz
bcm-g4-zImage
bcm-g4_in-0.0430.1.txt
cbe-0.0430.1-ppc.tar.gz
ncgl_kernel_src-2.4.22.0.0430.1.tar.gz
bcm-rootdisk_image-0.0430.1-ppc.gz
```

123.10 Appendix B: NCGL Modifier

A further proposed change is to eventually replace the current NCGL version extension with an **NCGL modifier** which describes a release version for the entire NCGL software layer. The exact definition of this modifier remains to be decided. If possible it would indicate when the contents of a given package have changed, and provide a way to track which versions of packages are included in a given release of the entire NCGL layer.

The current NCGL version code has a leading “0.” to identify the convention being used for the extension. This is sometimes referred to as the ***NCGL Modifier type code***. For future formats of this version extension, there are some options as to the usage of a leading NCGL Modifier type:

1. The type can be incremented each time the NCGL modifier format is changed.

For instance, if the NCGL version extension were to be changed to include the current release, then the file

```
glibc-2.4.0.0.0431.1-ppc.tar.gz
```

would become

```
glibc-2.4.0.1.060431.1-ppc.tar.gz
```

2. The modified type code can be dropped altogether if there is a strong indication that there will be no further need to change the NCGL version format again in the future. Thus, continuing the example from above, the filename might become

```
glibc-2.4.0.060431.1-ppc.tar.gz
```

which comparatively would be considered “newer” than the filename with the old format.

At the time of this writing the planned use of a leading type code remains an open issue.

123.10.1 Listing 4: Proposed NCGL Modifier format 1 (NCGL 06 format)

```
0.[yy][wk].[spin]
```

This format contains a version code where:

- field “yy” is the last two digits of the year,
- “wk” is the week number of the compile,
- “spin” is a design incremented version number (for builds within the same week).

For example, if the following package is intended for the NCGL 05 release:

```
gdb-5.2-6.0431.01.mips64el.tar.gz
```

Pros:

- Extends package’s/file’s existing version string with added information about the NCGL version on a weekly basis, with a provision for additional versions during each week.

Cons:

- Does not provide NCGL release information.

123.10.2 Listing 5: Proposed NCGL Modifier format 2

```
[NCGL_release].[yy][wk].[spin]
```

Using this format, a sample filename would be:

```
gdb-5.2-6.06.0431.01.mips64el.tar.gz
```

Pros:

- Extends the NCGL version information to include a clearly defined major release number (i.e. “06” for NCGL 06 and so on).
- This versioning information can help clarify NCGL release content as similar 3rd-Party package releases may be included across different NCGL releases.

Cons:

- Does not include any inter-release information (for example, for IT loads)

123.10.3 Listing 6: Proposed NCGL Modifier format 3

```
[NCGL_major_release].[NCGL_minor_release].[yy][wk].[spin]
```

The NCGL minor release version number allows specification of an inter-release milestone, such as for an IT, or a beta release.

The minor release number might map to a set of milestones as follows:

1 - 9: IT releases (IT1 through IT9, as required)

10: FC

11+: patch releases

Example:

`gdb-5.2-6.06.01.0431.01.mips64el.tar.gz`

Pros:

- With the addition of the minor release version, the filename clearly indicates the NCGL major release as well as an intermediate release.

Cons:

- (Subjective) The NCGL modifier string as a whole is getting rather long, and the definition of the minor release may be confusing.

- Mapping of the minor release number to milestones in this way is prone to problems in the future should milestone definitions change.

123.10.4 Listing 7: Proposed NCGL Modifier format 4

```
[NCGL_major_release].[NCGL_final_release].[NCGL_min  
or_release].[yy][wk].[spin]
```

The addition of a “final” release version would indicate that the file is part of a software load declared ready to ship to customers and is no longer undergoing development churn. The “NCGL_final_release” field is essentially a single bit, either “0” for a pre-release version, or “1” for a final version.

Using this format, a sample filename might be:

“Beta” (non-final) release:

`gdb-5.2-6.06.0.1.0431.01.mips64el.tar.gz`

Final release:

`gdb-5.2-6.06.1.15.0431.01.mips64el.tar.gz`

Pros:

- Clearly indicates the final release status of the file.

Cons:

- Unless really needed, tends to “clutter” the NCGL modifier.

124: A00007752 Functional description (FN)

124.1 Feature name

Universal Billing Correlation ID

124.2 Description

This activity will start the ground work for creating, storing and formatting a universal billing correlation id (UBCID). Currently the MCS generates its own BCID. The CS2K and GWC generate their own BCID for AMA/QOS correlation. With the various agents creating their own correlation id's it is impossible to correlate the various records which can be produced during a call. Future activity work will provide correlation of these records from end to end.

PacketCable event messaging defines a billing correlation id which is currently used for the cable solution, since this correlation id is an accepted standard we will use the format defined by PCEM for our UBCID. The UBCID will be formatted for the following billing types: Bellcore AMA format (BAF), UCS Flex CDR and AT&T CDR2BAF format. There are currently other activities which are creating billing correlation id's for MCS and NGSS, future activity work will attempt to merge all of these billing correlation id into one format.

124.3 Required Datafill Changes to activate this feature:

The following sections describe the datafill changes required to activate this feature for both the BC AMA format and CDR billing formats.

124.3.1 BC AMA: Table AMAOPTS

To allow the recording of the UBCID for BC format AMA a new option “**CORRID**” is introduced into table AMAOPTS. This is an ON/OFF option. When “**CORRID**” is set to “**ON**”, a module code 613 will be appended to the base billing record which requires the collection of the UBCID.

Table	Desc
AMAOPTS	New option CORRID is added to the AMAOPTS table to capture the UBCID for BC AMA format.

Sample datafill for table **AMAOPTS** (new field in bold).

OPTION

SCHEDULE

```

-----
CMCORIG          ON
CMCTERM          ON
COIN             ON
CORRID         ON
CRSEQNUM         OFF
CRT_BILLING      OFF

```

124.3.2 CDR: Table CDRTMPLT

To allow the capture and recording of the UBCID for CDR ,new parameter “**CORRID**” is added to the list of parameters which can be datafilled in table CDRTMPLT.

Table	Desc
CDRTMPLT	A new parameter for the FIELDS and REORIGCP subfields of table CDRTMPLT is added to record the UBCID for CDR

Sample datafill for table **CDRTMPLT** (new fields in bold):

NAME ACTIVE PRIMARY FIELDS REORIGCP

```

-----
CORRID_TMPLT Y N (SEQNUM) (CIC) (ORIGTIME) (ORIGDATE)
(ANSTYPE) (TIMECHNG) (ORIGAMPM) (INCINTL) (DISCTIME)
(DISCDATE) (ANISUFF) (DISCAMPM) (INCBILL) (FILL1) (CALLDUR)
(PINDIGS) (ANISP) (INFODIG) (BILLNUM) (ACCTCD) (CLGPTYNO)
(RLTCDR) (ACCTV) (UNIVACC) (DIALEDNO) (CALLEDNO)
(OUTPUTNO) (FILL4) (ORIGOPRT) (PREDIG) (CNPREDIG) (OPART)
(TPART) (QUEUED) (FILL3) (FILL3) (FILL4) (RTENO) (NETSEC)
(OPCHOICE) (COLLTIME) (ADIN) (LNPCHCK) (NUMWBCKT)
(WBCKTS) (FINSID) (BILLTYPE) (ORIGGRP) (DISCTYPE) (ORIGMEM)
(PASSTHRU) (TERMGRP) (PRESIND) (TERMMEM) (OSRASSOC)
(DIGDATA) (FINTKGRP) (TRAP) (COSOVE) (FINTKMEM) (SCPBILL)
(FILL3) (FILL3) (FILL3) (FILL2) (FILL3) (FILL2) (TRMTCD)
(COMPCODE) (CRID) (DNIS) (ORIGPVN) (TERMPVN) (ORIGLRN)
(PORTEDNO) (CAINCT) (ACG) (DNISNOA) (FILL1) (MLTCOSID)
(FILL4) (FILL1) (COSINDEX) (FILL2) (CARRSEL) (CORRID) (FILL8) $
$

```

124.4 Billing record layout and logs

124.4.1 BC format AMA - Module code 613

The option CORRID in table AMAOPTS triggers the additional module code 613 with context id 800xx for calls requiring the capture of the UBCID. The format of the module code 613 with the context id of 800xx is as follows:

- The context id 800xx is a 45 digit register.
- The first 8digits are the NTP timestamp.
- The next 5 digits is the Element_id.
- The next 8 digits is the Time Zone.
- The next 10 digits is the Event counter
- These 35 digits combine to make up the UBCID
- The remaining 12 digits are padded with zeroes and a 'C' delimiter.

Below is a sample of the module code 613 which will be appended to the base billing record.

Figure 1 Example of module code 613 With Context ID 800xx

MODULE CODE:	613C	GENERIC MOD: THREE DGT STR FMT
GENERIC CONTEXT ID:		
PARSE RULES	800xx	Universal Billing Corr ID
SIGNIFICANT DIGITS	31C	
GENERIC DIGIT STRING ONE:	132431017712391C	
GENERIC DIGIT STRING TWO:	345678123456781C	
GENERIC DIGIT STRING THREE:	100000000000000C	

124.4.2 CDR: New Field Description

The new data captured by this activity will be formatted into the CDR record using the following layout:

Field Name	Chars	CDR Field Description
CORRID	27	Contains the Universal billing correlation id.

Sample CDR Log (new fields in bold):

	RTPE_B115BH	CDR273 FEB04 21:44:14 4200 INFO CDR_CALL_ENTRY
250X15AY	CDR273 FEB09 13:44:20 0800 INFO CDR_CALL_ENTRY	

RECCD	F0	TEMPLID	016
ACTIDX	6	TOOLGEN	Y
USEEDIT	N	VARLNGTH	N
SEQNUM	00001	CIC	5676
ORIGTIME	34992	ORIGDATE	035
ANSTYPE	03	TIMECHNG	N
ORIGAMPM	1	INCINTL	N
DISCTIME	35052	DISCDATE	035
ANISUFF	1	DISCAMPM	1
INCBILL	1	CALLDUR	00013107
PINDIGS	6987	ANISP	5124599628
INFODIG	1	BILLNUM	50854321499779000001234
ACCTCD	802000012345	CLGPTYNO	214684552900000
RLTCDR	Y	ACCTV	3
UNIVACC	8007654321	DIALEDNO	508345214997799
CALLEDDNO	508543214997790	OUTPULNO	508345129479970
ORIGOPRT	501	PREDIG	1
CNPREDIG	1	OPART	511
TPART	31	QUEUED	Y
OPCHOICE	232	COLLTIME	060
ADIN	12	LNPCHECK	7
NUMWBCKT	16	WBCKTS	10000000 10000000 00000000
FINSID	111	BILLTYPE	35
ORIGGRP	0353	DISCTYPE	1
ORIGMEM	0101	PASSTHRU	2
TERMGRP	0355	PRESIND	1
TERMMEM	0101	OSRASSOC	N
DIGDATA	Y	FINTKGRP	09999
TRAP	N	COSOVE	Y
FINTKMEM	62843	SCPBILL	FE17700B
TRTMTCD	010	COMPCODE	3
CRID	684149400	DNIS	214684149400000
ORIGPVN	214684149400000	TERMPVN	214684466200000
ORIGLRN	2146841494	PORTEDNO	2146844662
CAINCT	1	ACG	Y
DNISNOA	103	MLTCOSID	0001
COSINDEX	0001	CARRSEL	02
CORRID	1324310177123913456781234567811		

124.5 Hardware Requirements or Dependencies

No special H/W requirements or dependencies.

124.6 Software Requirements or Dependencies

No special S/W requirements or dependencies.

124.7 Limitations and restrictions

This feature will not apply to MWC (MCI) or SSR (Sprint) loads.

124.8 Interactions

N/A

124.9 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)	__X__
Performance (includes operational measurements)	_N/A__

124.10 Glossary

Term	Description
BC AMA	Bellcore Automatic Message Accounting
CDR	Call Detail Recording
MCS	Multimedia Communications Server
NGSS	Next Generation Session Server
SBA	SuperNode Billing Application
SDM	SuperNode Data Manager
UBCID	Universal Billing Correlation ID
PCEM	Packet Cable Event Messaging

125: A00007785 Functional Description (FN)

125.1 Feature name

MFT Backend Security Services Integrating into IEMS

125.2 Introduction

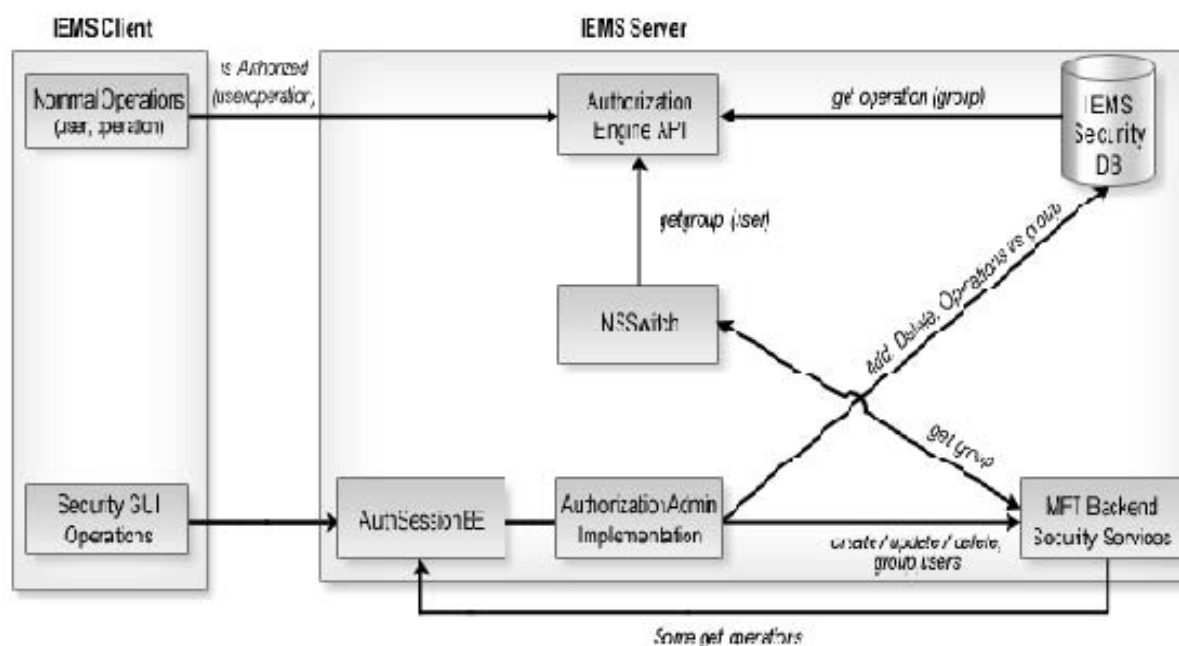
SN07 IEMS application maintains all the user and group related information in IEMS database. In SN08 the centralized Security Service is provided by MFT backend Security Services. The MFT backend Security Services will be maintaining all the user and group related information, **information that is stored in NSSwitch PASSWORD (including SHADOW) DB and GROUP DB.** This document covers the changes required for the integration of MFT backend Security Services into IEMS.

125.3 Acronyms Used

IEMS - Integrated Element Management System

MFTBSS - Management Framework Technologies Backend Security Services

125.4 Overview of MFTBSS Integration



In the above diagram the Security GUI related operations will be split into the following two types,

- create, update and delete users (or) groups
- add or delete operations for a group

The create, update and delete users (or) groups will be performed using MFT API's and add or delete operations for a group using our security framework. In the create group case, we have to first add the Group using MFT API's and if the group add success then we add the group related operations using our security framework. We assumed that, the MFT Backend server should be in the **High Availability** mode on a redundant IEMS cluster, **that is, if the local MFT Backend server's DB is not responding the MFT APIs will automatically fail over to use the other MFT Backend server's DB on the inactive unit.** In case of MFT API calls fails to respond, we will log the MFT failure information.

125.4.1 Location of IEMS Server logs:

/opt/nortel/iems/current/logs/secout*.txt.

Since IEMS Server has log rotation, the name of the file starts with secout.

Sample log would be as below.

“Problem in communicating with MFT Server.Unable to proceed SecurityAdmin operations.”

Similar error messages will be shown in the requesting client. Users will be able to use only the emergency user account, to login into IEMS without the MFT backend Security Services.

125.5 Changes

125.5.1 Client Side Changes

125.5.1.1 Changes in the Add User Wizard

In the second screen of the Add User Wizard, we can provide the account expiry as an absolute date field, whereas the earlier approach was to enter the number of days from the date of user creation. **Note that this account expiry GUI will be hidden until MFT provides the actual account expiry support.** The password expiry day field, 'The password expires every', now indicates how often (number of days) the user password will expire and not how soon the next password expiry will occur. The password expiry change will take effect after the next password expiry **or the next password change.**

In the Advanced Properties screen which is invoked by clicking on the “Advanced” button in the 3rd screen of Add User Wizard, the following fields are present during user addition.

Note: Starting SN08, all usernames must be 8 characters or less and must consist of lowercase letters or numeric digits only.

125.5.2 Additional User Attributes

- 1 UID: This will have the “AUTO GENERATED” since numerical uid's will be auto-generated for all users. This field will display a read-only UID value for already created accounts.
- 2 GID: The primary GID is given as a selectable drop down menu (ComboBox). The default primary GID selected will be “succssn” **for** all the users added during user addition. The administrator can change the primary Group name which is selected by default.
- 3 GECOS: Administrator can enter any information in this field, for example the actual full name of the user.
- 4 LoginShell: Administrator are given the following options to select for each user created. They are given below.

- no-access: Users created with this shell, do not have permission to invoke a shell in the system. No-access accounts are mainly for GUI-only user accounts. The actual value of LoginShell in this case is /usr/bin/nash.
 - restricted: Users created with this shell, has command line access to the systems. The actual value of LoginShell in this case is /usr/bin/rash.
- 5 Home Directory: The home directory for each user varies according to the Login Shell selected for each user.
- no-access: /export/home/tmp
 - restricted: /export/home/<username> The <username> is the login name of the created user.
- 6 MIN: This is the minimum number of days required between password changes. The default will be (0) days.
- 7 Password Expiry Date: This field is a read only field which will indicate the absolute date on which the current password for the user expires.
- 8 LastChange: This field show the absolute date on which the password was most recently changed.

Note: Account Expiry support is removed from IEMS Security Client GUI. This feature will be enabled after MFT Security Server provides support for Account Expiry

125.5.3 Add Group Wizard

In the group add wizard, the administrator has the provision to manually provide a GID for the newly created group. If a value is not provided in the GID field, IEMS will pick a value from the range **specified** in the configuration file.

125.5.3.1 Access permissions to IEMS Security Client GUI

Only members of the “secadm” group have access to IEMS Security Client GUI. This applies to JWS Client and the HTML Client. SN07 users who are present in emsadm group will be automatically be provisioned in secadm group in SN08 during the upgrade process.

Note: Starting SN08, all group names must be 8 characters or less and must consist of lowercase letters or numeric digits only.

125.6 Server Side Configurable parameters

125.6.1 User ID configuration:

The users in MFT BSS are identified by a unique numerical identifier which is generated by IEMS and MFT. This is achieved by providing a UID range in the following configuration file.

```
/opt/nortel/iems/current/conf/  
NmsProcessesBE.conf
```

The configurable user ID range is highlighted in bold.

```
#java com.adventnet.security.authentication.SecurityProcess  
PROCESS com.adventnet.security.authentication.SecurityProcess  
ARGS SecurityServerPort 7777 maximum_allowed_login_failed_count 0  
userIdRange 10001-12000 groupIdRange 12001-14000
```

The default UID range is 10001-12000.

The above can be changed by the user. When IEMS Server starts up, this value will be read by the IEMS Server. If a user changes the user id range, then IEMS Server must be restarted for the changes to take effect. During each useradd operation from the IEMS Security GUI, a value from the provided range will be automatically selected by IEMS Server and provided to MFT for the user. If the generated user id is exhausted, the user will receive a failure message indicating security database is full. The numerical UID for each user will be generated only by IEMS Server. It cannot be provided by the secadm user. The list of UID's which are freed up as a result of user deletions will be available for enumeration after the enumeration process reaches the upper bound and re-enters the lower bound for finding out free slots.

Note: At most 1000 user accounts can be provisioned and managed by IEMS Server. IEMS Server does not support more than 1000 user accounts.

125.6.2 Group ID configuration:

The groups in MFT Security Services are identified by a numerical group identifier. The range for the generated group identifier can be provided in the following configuration file in IEMS.

```
/opt/nortel/iems/current/conf/NmsProcessesBE.conf
```

The configurable group ID range is highlighted in bold.

```
#java com.adventnet.security.authentication.SecurityProcess
```

```
PROCESS com.adventnet.security.authentication.SecurityProcess
ARGS SecurityServerPort 7777 maximum_allowed_login_failed_count 0
userIdRange 10001-12000 groupIdRange 12001-14000
```

The default GID range can be changed by the user. When IEMS Server starts, this range is read by the IEMS Server. If a user changes the group Id range, then IEMS Server must be restarted for the changes to take effect. During each group add operation, IEMS Server picks up an identifier for the group which is added from the IEMS Security Client GUI from the provided range. If the range is exhausted, then the user will receive a failure message indicating group ID range is exhausted. The secadm user can provide a numerical GID.

125.6.3 Password Attributes Support.

The following are the attributes supported by MFT Backend Security Server.

- sp_max - Maximum number of days a password is valid. Password expiration is disabled if sp_max is set to -1. **It is settable on a per user basis.**
- sp_min - Minimum number of days required between password changes. The restriction is lifted if sp_min is set to 0. **It is settable on a per user basis.**
- sp_warn - Maximum number of days before the password expiry, the user will be warned. It is supported only as a global configuration, which means that warning value can be set only at the MFT Security Services level common for all users in MFT Security database. Please refer to MFT Security Services documentation on how to change this global parameter via an MFT-provided CLI interface.
- sp_expire - Absolute date (number of days since 1/1/1970) after which the account is disabled. **It is settable on a per user basis.** Account expiry is disabled if sp_expire is set to -1.

Note: sp_inact –Maximum number of days of inactivity allowed for a user. It is not supported by MFT Security Services.

125.7 Migration:

Security Data migration is actually performed in SN08 as a three-part operation. They are given below.

- 1 Data Extraction from IEMS database
- 2 Data Import into MFT Security Services
- 3 Data Clean up in the IEMS database

125.7.1 Data Extraction.

This step is performed as part of the installation process. After the installation of MFT & IEMS binaries, this script will be invoked. This will identify the list of users, groups, and the user group relationship. After identifying the information this process will export all the identified data as an XML file in the following location. The script will take the location of the export xml file as an argument. After successful data extraction, the data import will be called by the combo load script which will import data into MFT Security Services.

After the above step, IEMS will be started in the backward compatible mode, with all user and group information in the IEMS DB. During this time the IEMS Security Client cannot be started both in the JWS Client and the Web Client. After the stability of MFT Security Services is ensured, then the clean up script will be called

The following data will be exported to MFT Security Services.

125.7.1.1 List of Data to be exported.

- 1 User with only groups in IEMS DB
- 2 Users with only succssn group and Solaris groups
- 3 Users with IEMS groups and Solaris groups
- 4 Emergency user is NOT migrated
- 5 IEMS groups
- 6 Solaris groups (non-reserved) containing above listed users
- 7 Migration of user-group associations involving above listed users
- 8 Ability to login via IEMS central account during upgrade (07 backward compatibility mode)

When groups created in IEMS are exported, new GID's will be generated for each group exported to MFT Security Services. Each of the GID will be enumerated from the range provided from the configuration file given below.

```
/opt/nortel/iems/current/conf/NmsProcessessBE.conf
```

If any group ID is already present in MFT then user has to manually provision the GID for that group. Groups that are imported from Solaris, due to the user group relationship in IEMS, will have the same GID in the XML file which is exported by IEMS.

125.7.2 Notes

- 1 During data export process, all usernames/groupnames whose length (no of characters in username/groupname) exceeds 8 characters, will be dropped after generating a security log. Their corresponding user-->group relationship will also be dropped. After each drop a security log will be generated along with all the details of the user / group which are dropped. The admin user can take corrective measures with the input data from the logs.
- 2 During data export process all usernames/groupname will be changed to their corresponding lowercase characters. This change will be reflected in their corresponding user-->group relationship also.
- 3 During data export process all users who are present in emsadm group will be automatically be added to secadm group.
- 4 In SN08, a new authorization group, secadm, is introduced. Members of the secadm group can perform Security Administration functions such as:
 - Adding/Deleting/Users.
 - Adding/Deleting/Modifying Groups
 - Modifying user profiles
 - Modifying IEMS system security settings

125.8 Data Import into MFT Security Services.

After data is successfully exported from IEMS database and an XML file created as a result of successful export operation, the combo load script will invoke, the data import script provided by the MFT. Combo load script/MFT team will take care of importing the data successfully into MFT Server.

IEMS Server assumes that all data is successfully exported to MFT when the clean up script is called.

125.9 Data Clean up in the IEMS database

During data export all the above given users/groups/user-->group relationship present in the IEMS database is exported to the MFT Security Services through an XML file. After this step, the exported data will be redundant in IEMS database. So the clean up script is provided to clean up IEMS database of the redundant information. When this script is called, it will clean up the user, group & user group relationship except the emergency user account details from the IEMS database.

All the information given in the **(List of Data to be exported)** section will be cleaned up by the provided clean up script.

Note: IEMS Security Client GUI services will not be available when IEMS Server is started in the backward compatible mode. Existing IEMS users will be able to use IEMS Client GUI with the existing account and password information.

But the IEMS Security Client GUI cannot be invoked when the IEMS Server is running in the backward compatible [SN07] mode.

The following message will be shown to the user who invokes the IEMS Security Client when the server is running in backward compatible mode.

“IEMS is in Upgrade Mode. Cannot allow SecurityAdmin operations”

125.9.1 Emergency User Account:

IEMS Server provides its users with a special account called the emergency user account. This account has all administrative privileges for the IEMS Server, including security administration. The details of this account are maintained by the IEMS Server. When emergency user logs in and if MFT Security Server is available providing service, emergency user [iemsadm] will be able to use IEMS Security GUI interface. If MFT Security Services is not running, then if IEMS Security GUI is invoked, the error message provided by MFT will be displayed to the user.

UserName: iemsadm

Default Password : public

Since the details of this user account are maintained by IEMS Server, this account can be used when the MFT backend Security Service is not available. The administrator should not change the group association of this user. The password may be changed for this account.

125.9.2 Password Complexity:

When a user sets/changes his password, the following rules need to be followed. There are 4 class of characters that are allowed in a password. They are listed below.

- Lowercase characters
- Uppercase characters
- Numeric characters
- Special characters.

It is recommended that the password complexity rule requires 3 out of 4 of the above class of characters to be present in any password. The password complexity rules are configurable in the IEMS Server.

The provision for configuration is provided in a configuration file present in the following location.

`/opt/nortel/iems/current/defaultUserAttribute.prop`

In addition to the character set restrictions above, the password cannot be the same as the user name or the existing password, and must be at least 6 characters long by default and at most 256 characters long by default.

The following variables are used to configure the password complexity.

- `PASSWD_MIN_LENGTH=6`
- `PASSWD_MAX_LENGTH=256`
- `LOWERCASE_COUNT=1`
- `UPPERCASE_COUNT=1`
- `SPECIAL_CHAR_COUNT=0`
- `NUMBER_COUNT=1`
- `SPECIAL_CHARS=~!@#$%^&*()-_+=[]{}\\|;:'",<.>/?`

`PASSWD_MIN_LENGTH=6` - specifies that the password should have a minimum of 6 characters.

`PASSWD_MAX_LENGTH=256` - specifies that the password can have a maximum of 256 characters.

`LOWERCASE_COUNT=1` - specifies that the password should have atleast one lowercase character.

`UPPERCASE_COUNT=1` - specifies that the password should have atleast one uppercase character.

`SPECIAL_CHAR_COUNT=0` - specifies that password need not have a special character.

`NUMBER_COUNT=1` - specifies that the password should have atleast one of the numeric characters.

`SPECIAL_CHARS=~!@#$%^&*()-_+=[]{}\\|;:'",<.>/?`

When the password is scanned for special characters, each of the above characters is considered as a special character.

In the above sample the lowercase, uppercase & numeric characters are expected out of the 4(lowercase,uppercase,numeric & special characters).

Note: When one of these variables is changed the IEMS JWS Client should be restarted for the changes to take effect.

125.10 HTML Client Side:

Since HTML Client provides only minimal support for Security & User administration, Group, Operation provisioning is not provided in the HTML Client. In the HTML Client GUI the administrator will have the options given in Additional User Attributes section above in this document.

125.11 References

1. DID for 'MFT Backend security integration'

126: A00007786 Functional Description (FN)

126.1 Feature name

IEMS Configuration of RADIUS Secret

126.2 Introduction

This document provides an overview of configuring RADIUS secret through IEMS client. The IEMS currently provides provisioning of Network Elements, Element Managers, EMS Platforms, or EMS Applications in one step. Then provisioning of the RADIUS secrets through the CLI in a second step.

The SN08 IEMS will allow provisioning of RADIUS secrets directly through the IEMS in one step, eliminating the need of CLI for RADIUS secrets. IEMS will allow RADIUS secrets to be added, modified, and deleted from the Security Server. The RADIUS Server will be required to store all RADIUS device parameters, and they must be encrypted. No security data will be stored in the IEMS other than the default secrets.

This document also captures the different scenarios of Passport discovery along with the IP Address retrieve for RADIUS secret provisioning.

126.3 Acronyms Used

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

126.4 RADIUS Secret Provisioning

The RADIUS device parameters for each device are IP address, Type and RADIUS secret. In SN08, IEMS will provide the ability to provision RADIUS secrets directly from the IEMS GUI. All provisioning of RADIUS device parameters including add, modify and delete will be supported while the RADIUS Server is running. Provisioning of RADIUS secrets need to be added to the specific IEMS GUI for the platforms, Element Managers, and NEs that require RADIUS secrets.

The list of PAM-RADIUS clients and RADIUS clients are -

Security Client Type	Platform/EM/NE	RADIUS Device Type	IEMS Version	Comments
PAM-RADIUS	SSPFS Platform, except CBM	IEMS	SN07	Provision RADIUS secret for cluster IP and units.
PAM-RADIUS	SDM Platform	IEMS	SN08	
PAM-RADIUS	MDM Platform	IEMS	SN08	
PAM-RADIUS	Preside MDM Element Mgr	IEMS	SN08	Provision RADIUS secret for the server and client sets too.
PAM-RADIUS	CS2K Core Element Mgr (SDM Platform)	IEMS	SN08	
RADIUS	Passport/PVG	PASSPORT	SN08	
RADIUS	PP8600	PP8600	SN07	
RADIUS	MG9K	MG9K	SN08	
	CEM Element Mgr	-	-	It is part of the IEMS bundle. It runs on the security server and thus does not use PAM-RADIUS. Hence will not be supported for SN08.

RADIUS secrets cannot be provisioned for 6.2 devices. For devices that are newly integrated in SN08, the RADIUS secret cannot be provisioned for their SN07 version. Moreover, only IEMS users belonging to 'SECADM' group, can provision or view the RADIUS secrets. The default RADIUS secret must be encrypted via 3DES/DES and stored in IEMS. In case of RADIUS secret being exchanged between IEMS & MFT security server (add, update, retrieve), the secret will be in plaintext, unencrypted format.

126.5 Default RADIUS secret

IEMS will provide a GUI for an IEMS admin user to enter the default RADIUS secret for each type of RADIUS device. The various RADIUS device types supported for SN08 are IEMS, MG9k, Passport and PP8600. This screen will be launched from the Security Administration. Only IEMS users with SECADM privilege will have access to this screen.

The default RADIUS secret for each type will be undefined initially. The user will enter the default secret for each type through the GUI. When the value is entered, this RADIUS secret will be encrypted and stored in the IEMS database. It will then be displayed as default secret value for the RADIUS devices that are newly added, according to their type. The Admin user will

choose to use the default secret, change it or blank it out (remove it).

The following are the steps to be followed:

- The default RADIUS secret will be entered by the user, in the client GUI. The IEMS client will communicate the default RADIUS secret entered by the user for each type to the IEMS server.
- The IEMS server will store the default secret for each type in the Database in encrypted form.

126.6 Operations to be handled

The following operations are to be handled for the RADIUS secret:

126.6.1 Add An EMS/EMS Platform/NE

The Tools->Add platform/NE/EM screen has to be modified by including an attribute for the RADIUS secret. A check box will be provided for the attribute. The check box and the attribute should be shown only when the user selects version 7.0 or higher (and not when version 6.2 is selected). For devices that are newly integrated in SN08, the RADIUS secret attribute will not be applicable to their SN07 version. By default the check box will be enabled, indicating the device uses RADIUS authentication and thus a secret must be provided. IEMS should display the default unencrypted secret value, which the user can modify, if required or clear it. The secret should be displayed only for IEMS users with SECADM privilege.

- On enabling the check box, the secret value must be provided which will be added to the RADIUS server. If a secret value is not provided, IEMS will popup an error dialog indicating that a secret value should be provided for the device.
- On disabling the check box, IEMS will delete the RADIUS secret if it is already configured for the device.

When the RADIUS secret is set, add a tuple for the IP in the MFT database. IEMS client will send the request for Add operation to the IEMS server. The IEMS server will in turn execute the `configure_radius.sh` with the IP address, type and secret. The script will add the secret corresponding to the IP address in the MFT security server.

When a tuple is added for the IP address, IEMS will log the same in the security log. A sample security log entry for a successful add operation for user 'IEMSADM' is shown below –

E.g.: *IEMS class_security.ver01 STAT=SUCCESS SRC.USER=IEMSADM
EVNT.TYPE=Radius Parameters added for IP 192.168.4.3, device type IEMS*

The SSPFS Platform and PP8600 NE come under this category.

- **SSPFS Platform:** When manually adding a SSPFS platform with a version that supports RADIUS,
 - All three IP-addresses of a duplex SSPFS platform must be associated with the same RADIUS secret. The RADIUS configuration thus should be associated with the SSPFS cluster and not individual unit.
 - Adding the RADIUS secret for the cluster IP (in duplex case) automatically affects the two other UNIT-IP entries.
 - RADIUS configuration is not available to SSPFS units.

126.6.2 Adding Auto-discovered EMS Platforms/NEs

In the case of Auto-discovered *EMS* Platforms/NEs, IEMS will automatically interface with the Security server to provision the its RADIUS device parameters when the EM is added. The auto-discovered *EMS* Platforms/NEs that will be supported by this feature for SN08 are MDM Platform, SDM Platform, MG9k, PVG7k, PVG15k and PP15k.

When the EMS is added (whose version supports RADIUS secret)

- The RADIUS check-box will be enabled and the currently configured default RADIUS secret of this EMS device type is displayed.
- The user can optionally modify the default RADIUS secret or accept the default secret of this EMS device type
 - The secrets for its auto-discovered EMS Platforms will be automatically added using the same RADIUS secret specified for their EMS above and RADIUS configuration will be enabled for them, if either IEMS does not know the versions of the auto-discovered EMS Platforms or if their versions do support RADIUS
 - The secrets for its auto-discovered NEs will be automatically added using the current default RADIUS secret of the respective NE device type and RADIUS configuration will be enabled for them, if either IEMS does not know the versions of the auto-discovered NEs or if their versions do support RADIUS
- A requirement for this auto-provisioning to be done for auto-discovered EMS Platforms/NEs is that IEMS must be able to determine their IP addresses. If IEMS cannot determine the IP addresses of the discovered EMS Platforms/NEs, RADIUS secret configuration for them will not be done automatically at discovery. They will be manually provisioned when the IP addresses for the MDM client-server are provisioned
- If the version information is not available for the discovered EMS Platforms/NEs, IEMS should base the decision on the version of the EMS being added.

However, the same is not applicable for Passports/PVGs. There could be many IEMS servers that will have the MDM provisioned but only one will handle the authentication. Hence for an auto-discovered passport, the RADIUS parameters cannot be automatically added. For more details, refer Section 3.3.

When a tuple is added for the IP address in the security server, IEMS will log the same in the security log.

126.6.3 Update RADIUS Secrets

The PAM-RADIUS and RADIUS clients (platform/NE/EM) should contain a menu item called “Modify RADIUS secret” that will be used to update the RADIUS secret. For all RADIUS devices, their corresponding unencrypted RADIUS secret value should be fetched from security server and displayed in the RADIUS secret field. The ‘Modify RADIUS secret’ menu item should be shown only to IEMS users with SECADM privilege, when the user selects an EMS/EMS Platform/NE whose version supports RADIUS.

For objects (platform/NE/EMS) that support RADIUS, a check box will also be shown next to the RADIUS secret.

- It will be in DISABLED state if the MFT RADIUS server does not have a secret associated with the IP address of the client.
- Otherwise, the check box will be in ENABLED state with the current unencrypted secret shown.
- When the user wants to provision RADIUS secret for a device for which the secret is not yet provisioned, the check-box needs to be enabled first. It will display a warning message “Radius secret not configured for the device in Radius server, displaying the default value” and display the default Radius secret for the device type. When the user clicks modify, RADIUS secret will be provisioned for the device.

RADIUS secrets for all the EMS/EMS Platforms/NEs can be individually updated. The exception is when EMS and the underlying platform are associated with the same IP address, or when the different IP addresses may be associated with the same host. In this case updating the secret of one automatically affects the other.

When the user modifies the secret value:

- 1 Retrieve the secret value for the IP address from the security server.
- 2 If the secret value is set for a different type than the one existing in the MFT DB, display error. For example, if a secret already exists for the IP with type IEMS, the following will be the error message - “Error: RADIUS secret already existing for IP address 192.168.5.54, device type IEMS. Can not be set for a different type”.

- 3 If the check box is unselected in the GUI, the tuple should be removed from the database.
- 4 Else, a RADIUS secret must be provided and IEMS should update the secret value given in the field, in the security server.

When the RADIUS secret is updated for the IP address in the security server, IEMS will log the same in the security log. A sample log entry for a successful update operation for user IEMSADM is given below –

E.g.: *IEMS class_security.ver01 STAT=SUCCESS
SRC.USR=IEMSADM EVNT.TYPE=Radius Parameters updated for IP
192.168.5.54, device type PP8600*

126.6.4 Delete A RADIUS Device

When a RADIUS device (Platform/NE/EM) is deleted via the existing “Delete Object and Traces” menu item (on right click), check should be done if an entry exists for the IP address in the MFT DB. If it exists, the tuple corresponding to the IP address should be removed from the MFT DB. If the device is an EM (parent object), the entries corresponding to its NEs (children) should also be removed from the MFT DB. When a duplex SSPFS of version 7 or above is deleted, all three RADIUS entries must be removed. When the EMS is removed, all its auto-discovered EMS platforms or NEs and their RADIUS secrets should be removed automatically.

The delete operation for the IP address should also be logged by IEMS in the security log. A sample log entry for a failed delete operation for user IEMSADM is given below –

E.g.: *IEMS class_security.ver01 STAT=SUCCESS SRC.USR=IEMSADM
EVNT.TYPE=Radius Parameters deleted for IP 192.168.4.3, device type
IEMS*

126.6.5 Up-Versioning An EMS/EMS Platform/NE

When the user modifies the version of a non-RADIUS device to a higher version that supports RADIUS secret, using the “Managed Object Property” sheet available on right click of the object, the “Update Radius Secret” menu item of the device should be enabled (on right click).

- On invoking the menu item, the check-box for RADIUS secret will be in disabled state. To provision RADIUS secret for the device, the user should enable it. On enabling, it will display a warning message indicating that Radius secret not configured for the device and display the default RADIUS secret of the device type. The user can optionally modify the default RADIUS secret or accept the default secret of this device type.
- Specific rules for adding SSPFS Platform and auto-discovered EMS Platform/NE apply in the case of up-versioning a device. In particular,

- When a duplex SSPFS is up-versioned to version 7 or above, all three RADIUS entries must be added and RADIUS configuration enabled.
- In case of auto-discovered EMS platforms/NEs (except Passports/PVGs)
 - The secrets for its auto-discovered EMS Platforms will be automatically added using the same RADIUS secret specified for their EMS above and RADIUS configuration will be enabled for them, if either IEMS does not know the versions of the auto-discovered EMS Platforms or if their versions do support RADIUS
 - The secrets for its auto-discovered NEs will be automatically added using the current default RADIUS secret of the respective NE device type and RADIUS configuration will be enabled for them, if either IEMS does not know the versions of the auto-discovered NEs or if their versions do support RADIUS.
 - The secrets for auto-discovered Passports/PVGs will not be automatically added. The devices will be displayed in the 'Passport RADIUS Authentication' tool and need to be manually selected and configured for RADIUS secrets.

126.6.6 Down-Versioning An EMS/EMS Platform/NE

When the user modifies the version of a RADIUS device to a lower version that does not support RADIUS secret, using the “Managed Object Property” sheet available on right click of the object, the “Update Radius Secret” menu item of the device should be disabled (on right click). Also the RADIUS secret provisioned for the device should be removed automatically.

When a duplex SSPFS is down-versioned to version 6.2 or below, all three RADIUS entries must be deleted and RADIUS configuration disabled.

When MDM Mgr is down-versioned to version 7 or below, all MDM Platforms and Passports/PVGs that were auto-discovered through this MDM Mgr and were selected for authentication by this running IEMS security server will have their RADIUS secrets removed from this IEMS security server and RADIUS configuration disabled.

126.7 Centralized MDM/Passport Authentication

Since there can be many IEMS servers with the MDM provisioned and only one of IEMS servers manages different Passports/PVGs under the MDM manager, in order to enable only one to handle the authentication, the RADIUS parameters for the Passports/PVGs will not be added to the security server during auto-discovery. A centralized RADIUS authentication for Passports/PVGs will be supported in the IEMS GUI. A screen “Passport RADIUS Authentication”, which will display all discovered Passports for the MDM,

will be provided. This screen will be launched from IEMS client->Tools menu.

The passport devices will have an “authenticate” checkbox against each of them. The user will check all the Passports/PVGs that will be authenticated by the running IEMS security server. The RADIUS device parameters for all the checked Passports will be added to the security server. For all unchecked Passports, the RADIUS device parameters will be deleted from the Security Server.

The add and delete operations of RADIUS device parameters for Passports is feasible only if they are discovered with IP-Address. Before SN08, IEMS does not retrieve the IP-Address of the MDM auto-discovered Passports/PVGs. In SN08, the IP-Address of the Passports will be required for functionalities such as Passport Command Line launch and RADIUS secret provisioning.

The add and delete operations of RADIUS device parameters for Passports will be logged by the IEMS in the security log.

126.8 Passport Discovery

The different scenarios of the Passport discovery and the IP Address retrieve are as follows:

126.8.1 Retrieval of IP-Address

IEMS will use the following API to populate the IP-Address of the Passports/PVGs

- `_cmd: ACTION`
- `_obj_type: server`
- `_obj_id: serverId S GMDR`
- `_action_type: queryProperty`
- `_attr: compId NI EM *`
- `_attr: propName S NortelMomsProxyIPAddress`

A sample response message is given below -

```

_obj_class: server
_obj_id: serverId S FMDR_AESTEST@wcary3r6
_time: 2004 10 06 02 01 29
_attr: compId NI EM NEPALX
_attr: propName S NortelMomsProxyIPAddress
_attr: propValue S 47.138.180.194

_obj_class: server

```

```
_obj_id: serverId S FMDR_RTP@wcary3r6
_time: 2004 10 06 02 01 29
_attr: compId NI EM CAPEFEAR
_attr: propName S NortelMomsProxyIPAddress
_attr: propValue S 47.142.102.138
```

```
_obj_class: server
_obj_id: serverId S FMDR_RTP@wcary3r6
_time: 2004 10 06 02 01 29
_attr: compId NI EM CLEVELAND
_attr: propName S NortelMomsProxyIPAddress
_attr: propValue S 47.43.160.59
```

IEMS will parse the response to retrieve the IP-Address and assign it against the corresponding Passports.

126.8.2 Various Scenarios In Passport Discovery

- **Adding Passports:** Administrator or Craft person has to initiate the Resynchronization of Inventory manually in order to add the newly discovered Passport in the IEMS database.
- **When Passport name changes:** Administrator or Craft person has to initiate the Resynchronization of Inventory manually in order to update the new name of that Passport in the IEMS database.
- **When Passport IP-Address changes:** Administrator or Craft person has to initiate the Resynchronization of Inventory manually in order to update the new IP-Address of that Passport in the IEMS database.
- **When the Passport removed:** Administrator or Craft person has to initiate the Resynchronization of Inventory manually in order to remove that Passport from IEMS database.

126.9 Test Considerations

- Duplex IEMS servers are required running version 7.0 or greater.
- The different scenarios in Passport discovery should be captured while testing so that the Passports in the Network are always in sync with the IEMS Database.

126.10 Open Items

The IP-Address of MDM Platforms is not obtained. Provisioning of RADIUS secrets for MDM platforms can be done only if their IP-Address is obtained.

126.11 References

DID for Config RADIUS secret A00007786_-
_IEMS_Config_RADIUS_secret_(2061)_v2.pdf [Stephen Dreyer]

127: A00007790 Functional Description (FN)

127.1 Feature name

P-phone Expansion for CICM lines

127.2 Description

This feature will increase the number of Meridian Business Sets (such as M5216) which can be provisioned in Succession offices from the current limit of 31,743 to a new limit of 150,000. The same increase will apply to the number of add-on modules (such as M518 and M536) which can be assigned to these sets.

This activity will only impact the number of tuples which can be provisioned in table KSETINV. Other than that there are no customer visible changes to any of the Key-set provisioning tables nor is there any impact on Servord. There are also no customer visible changes to any of the functionality currently provided by Meridian Business Sets.

127.3 Hardware Requirements or Dependencies

Not applicable.

127.4 Software Requirements or Dependencies

None.

127.5 Limitations and restrictions

Although this feature is being done mainly to support Centrex IP clients which are provisioned as M5216 sets, the new limit will apply across all types of business sets which can be provisioned in table KSETINV.

It should also be noted that this feature does not increase the number of equivalent DN appearances (or virtual lines¹) which can be supported on these Business Sets. Please see Section 127.6, “Interactions”, on page 1007 for further details.

127.6 Interactions

Every P-phone provisioned in table KSETINV takes up one line card slot on the line peripheral (or node). In the case of IP Clients, the line peripheral is represented by a Logical Group that is provisioned in table LGRPINV.

¹One virtual lines is required for each DN appearance as well as services such as Call Waiting, Ring Again and certain programming features.

Each peripheral or Logical Group maps to a single node which can support up to 1024 lines. In addition, virtual nodes are required to support the DN appearances provisioned on Business Sets in table KSETLINE as well as certain features provisioned in table KSETFEAT. These virtual nodes can support up to 2050 equivalent DN appearances (or virtual lines). The number of virtual nodes required therefore depends on the configuration of the business sets.

As an example, 150 thousand IP Clients provisioned in table KSETINV would require at least 150 Logical Group nodes. Assuming an average of 4 equivalent DN appearances per Business Set, then an additional 300 virtual nodes would be required ($150K \times 4 = 300 \times 2K$).

Strictly from a node perspective these numbers can be supported without any additional development in the Core. Up to 1024 line peripherals (or Logical Groups) can be defined in an office of which up to 944 can be virtual. The 150 thousand IP Clients would therefore require 150 Logical Groups, leaving 874 nodes available for virtual lines.

127.7 Glossary

Term	Description
CICM	Centrex IP Client Manager
KSETINV	Key-set Inventory

128: A00007927 Functional Description (FN)

128.1 Feature name

SAM21 Enhancements from Bell Canada

128.2 Description

In SN07 and earlier, there is “Administrative State” in both SAM21 EM and GWC EM GUI. In SAM21 EM the “Administrative State” indicates the H/W state of a card, while in GWC EM it indicates the state of the application running on the card. However, if a user doesn’t understand what it means, he/she may feel confused.

In SN07 and earlier, when a NSS card (no matter it’s Unlocked/Enabled or Locked/Disabled) is pulled out and then inserted, it will come back in a Locked/Disabled state. The user needs to manually unlock it to bring it into service.

This document outlines the design scope and requirements of this feature that:

- Changes the label of “Administrative” to “Card Status” in every card view on SAM21 EM GUI (refer to figure 1 and figure 2).
- Changes the behavior of EM on pulling/inserting NSS card. If a Locked/Disabled NSS card is pulled, when it is re-inserted, the card will come back in Locked/Disabled status. However, if an Unlocked/Enabled NSS card is pulled, when it is re-inserted, SAM21 EM will automatically unlock this card.

Figure 1 Non-System Card View

The screenshot shows a web-based interface for managing a network card. The window title is "Lower Shelf-0 Slot 11 CardView@wnc0s0pc.us.nortel.com (CM CLI: UNF)". The interface has a "File View" menu and a "Storage Management" sidebar with a "11" button. The main content area is titled "Lower Shelf-0 : Slot 11" and contains tabs for "Alarms", "Equip", "States", "Diags", and "Provisioning". The "States" tab is active, showing the "OSI" section with the following status: "Card Status: Unlocked", "Operational: Enabled", and "Availability: None". There are "Lock" and "Unlock" buttons next to the "Operational" status. Below this is a "History" section with a large empty text area and "Save" and "Clear" buttons at the bottom.

Lower Shelf-0 Slot 11 CardView@wnc0s0pc.us.nortel.com (CM CLI: UNF)

File View

Lower Shelf-0 : Slot 11

Alarms Equip States Diags Provisioning

OSI

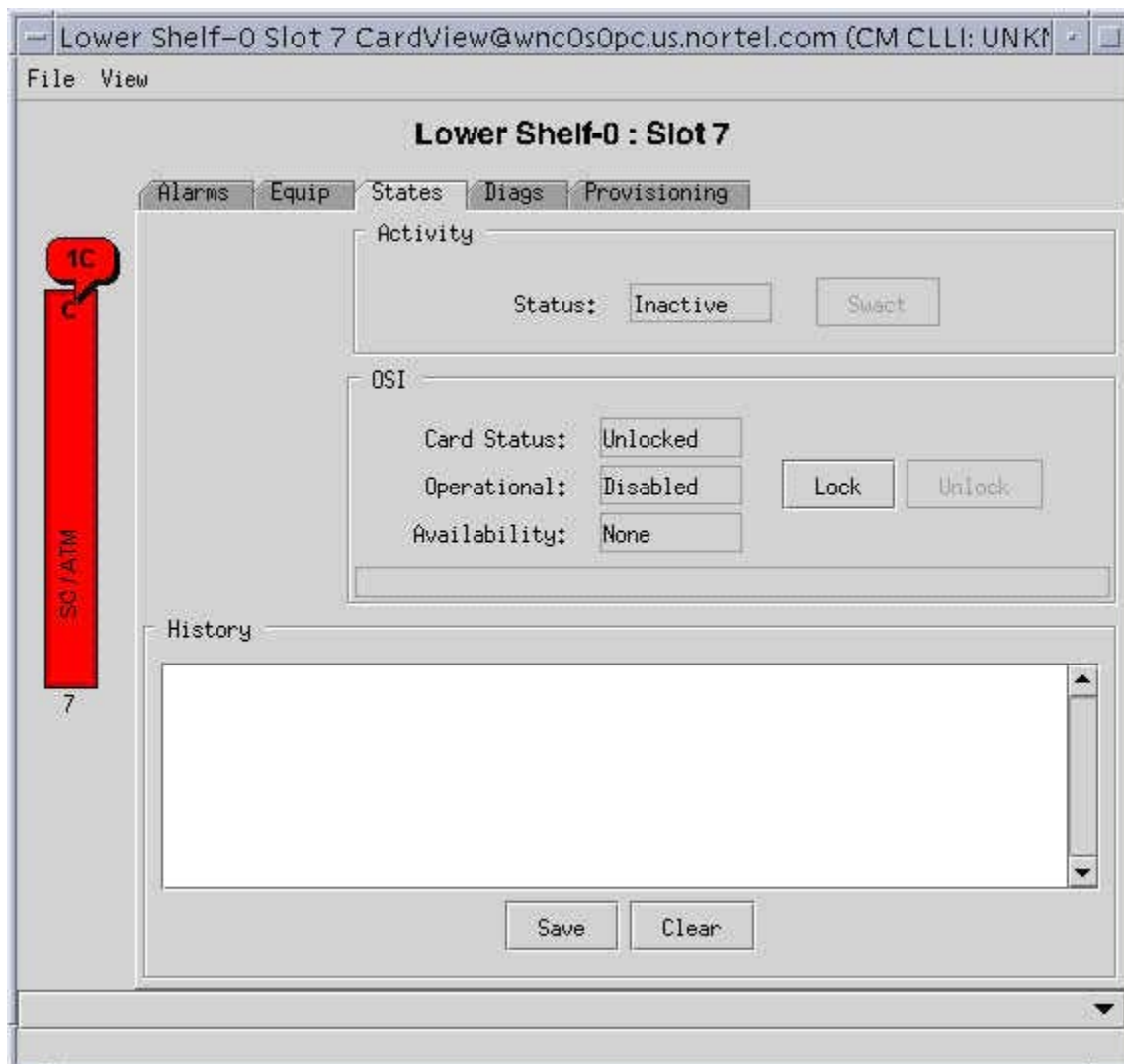
Card Status: Unlocked

Operational: Enabled Lock Unlock

Availability: None

History

Save Clear

Figure 2 Shelf Controller Card View

128.3 Checking the State Tab of card views on the SAM21 EM GUI

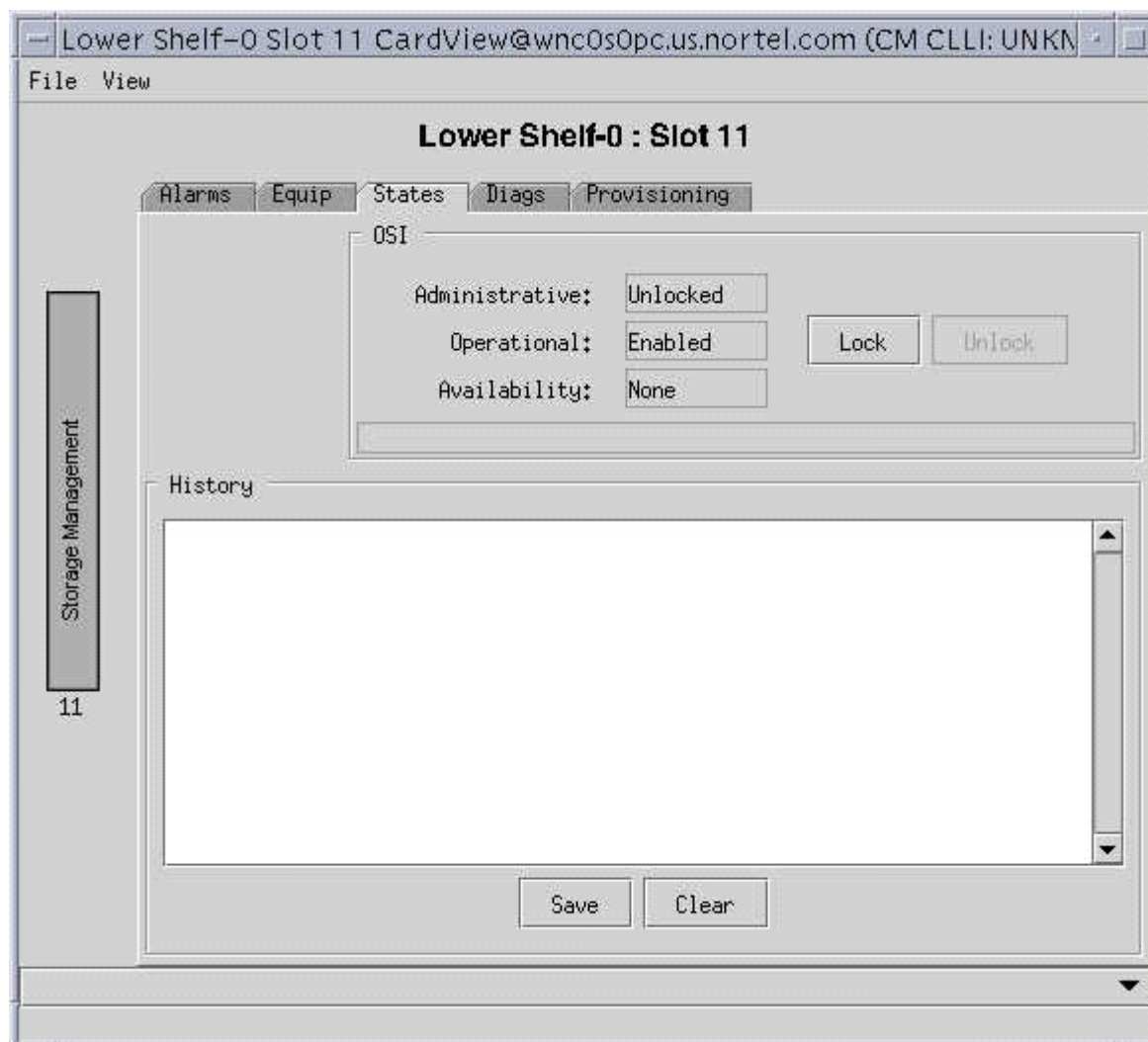
Use the following procedure to see changes in the state tab of every card view on the SAM21 EM GUI.

At your workstation

1. Launch your web browser.
2. Launch the SAM21 EM GUI via the common launch page: <http://{SSPFS serve IP or hostname}>.
3. Click on the Shelf icon to open the Shelf View.

4. Right click on a card (e.g. a STORM) to bring up the Card View.
5. Click the States tab on the Card View.

In SN07 or earlier, you will see a display as below:



In SN08, you will see a display as below:

The screenshot displays a web-based interface for managing a network device. The title bar indicates the connection is to 'Lower Shelf-0 Slot 11' via 'CardView@wnc0s0pc.us.nortel.com (CM CLI: UNF)'. The interface has a 'File View' menu and a main content area titled 'Lower Shelf-0 : Slot 11'. On the left, a vertical 'Storage Management' sidebar shows '11' selected. The main area contains tabs for 'Alarms', 'Equip', 'States', 'Diags', and 'Provisioning'. The 'States' tab is active, showing the 'OSI' section with fields for 'Card Status: Unlocked', 'Operational: Enabled', and 'Availability: None'. To the right of these fields are 'Lock' and 'Unlock' buttons. Below the OSI section is a 'History' section with a large empty text area and 'Save' and 'Clear' buttons at the bottom.

Lower Shelf-0 : Slot 11	
Alarms Equip States Diags Provisioning	
OSI	
Card Status:	Unlocked
Operational:	Enabled
Availability:	None
History	
[Empty History List]	
Save Clear	

You have completed this procedure.

129: A00007934 Functional description (FN)

129.1 Feature name

E800 Routing Enhancements

129.2 Introduction

Enhanced 800 (E800) is a U.S. service currently available in the DMS software. The E800 service provides the ability to route toll-free 8XX (e.g. 800) calls in a telecommunications network. The 8XX numbers must be mapped to a specific directory number and can be carried by either the Local Exchange Carrier (LEC) or a specific Inter-Exchange Carrier (IEC). When an 8XX call is originated, a database query is performed using the Transaction Capabilities Application Part (TCAP) layer of the Signaling System 7 (SS7) protocol. The database contains a mapping of 8XX numbers to routing directory numbers. Additionally, the database identifies the IEC to handle the call (when applicable). This information is returned in an E800 Response to the switch that initiated the query. The returned information is used by the switch for translations and routing.

Currently, the DMS100/CS2000 End Office (EO) switch provides two methods for translating an E800 Response:

1. Translate using the Standard Pretranslator (STDPRT) name of the originating subscriber.
2. Translate using the STDPRT name provisioned for option PRETRAN in table NSCDEFS. With this option, all E800 Response translations use a single STDPRT subtable.

With the first method, the STDPRT name of the originating subscriber is used when performing the E800 Response translation. However, this method may cause interaction issues with other datafill in the originating subscriber's STDPRT subtable. For example, if the STDPRT subtable contains datafill to route toll calls to treatment (i.e. toll denied), the E800 Response translation may route to treatment in error.

The second method was introduced as a provisioning alternative to avoid interactions with datafill in the originating subscriber's STDPRT subtable. With the second method, a single STDPRT name is provisioned via option PRETRAN in table NSCDEFS. This STDPRT name provides an *override* to the originator's STDPRT name and is used for translating all E800 Responses. However, with routing provided via a single STDPRT subtable, all E800 Response translations are limited to a single set of routes¹.

This activity provides additional flexibility for E800 Response translations by supporting *multiple* STDPRT names as an *override* to the originator's STDPRT name. With the support of multiple STDPRT names, a DMS100/CS2000 EO switch can be configured with multiple routes¹. This flexibility is provided with the introduction of the new option PRETRANMAP in table NSCDEFS and the introduction of the new table NSCPMAP. Table NSCPMAP provides a method to *override* or *map* the originating subscriber's STDPRT name with a new STDPRT name.

A new Software Optionality Control (SOC): NTS00030, "E800 Pretran Mapping" is created for this activity. This SOC has an RTU of A/P (Always Present), and it is always at the ON state. The new option PRETRANMAP, in table NSCDEFS, always takes precedence over the existing option PRETRAN since SOC NTS00030 is always set to ON.

129.3 Description

The combination of the new table NSCPMAP and the new option PRETRANMAP (in table NSCDEFS) provides the flexibility to support multiple STDPRT names for E800 Response translations.

Table NSCPMAP is introduced to provide a mapping from the originator's STDPRT name to a new STDPRT name for use by the E800 Response translation. By providing a mapping on a per originating subscriber's STDPRT name basis, E800 terminating routes can be (indirectly) configured on a per-originating subscriber basis.

The new option PRETRANMAP is added to table NSCDEFS as a provisioning trigger for activating a lookup in the new table NSCPMAP. In addition, the new option PRETRANMAP provides equivalent functionality to the existing NSCDEF's option PRETRAN. This is accomplished by adding fields CALLS and IGNORE² to option PRETRANMAP.

The following sections provide a detailed description for this new capability.

129.3.1 New Table NSCPMAP

The new table NSCPMAP provides the ability to override the originating subscriber's STDPRT name with a new STDPRT name for the E800 Response translation. Table NSCPMAP is accessed when the new option PRETRANMAP is provisioned in table NSCDEFS.

¹This restriction applies when the routing is performed from the STDPRT subtable. E800 calls that complete to the IEC are routed from the STDPRT subtable.

¹Applies when routing is performed from subtable STDPRT. E800 calls that complete to the IEC are routed from the STDPRT subtable.

²Existing option PRETRAN in table NSCDEFS consists of fields CALLS and IGNORE.

Refer to Table 1 on page 1016 for a description of the table NSCPMAP. The key field, **ORIGPTNM**, is the originating subscriber's STDPRT name. This STDPRT name is *mapped* to the new STDPRT name that is provisioned for field **MAPPTNM**. The *mapped* STDPRT name is used for the E800 Response translation. Note that neither key ORIGPTNM or field MAPPTNM can be provisioned with the nil pretranslator name - "NPRT". Table control will enforce this restriction.

Table 1 New Table NSCPMAP

Key & Field	Values	Comments
Key: ORIGPTNM	PRETRANSLATOR_NAME	The table key specifies the originating subscriber's STDPRT name.
Field: MAPPTNM	PRETRANSLATOR_NAME	This field specifies the new STDPRT name to be used for the E800 Response translation.

The functionality provided by table NSCPMAP is not activated until the option PRETRANMAP is provisioned in table NSCDEFS.

Following is a provisioning example for the new table NSCPMAP:

<u>TABLE: NSCPMAP</u>	
ORIGPTNM	MAPPTNM

P819	P800

129.3.2 New Option PRETRANMAP, Table NSCDEFS

To enable the functionality provided by this activity, the new option PRETRANMAP must be provisioned in table NSCDEFS. Option PRETRANMAP consists of three fields as shown in Table 2 on page 1017.

Table 2 Table NSCDEFS, New Option PRETRANMAP

New Option	Subfields	Comments
PRETRANMAP	DEFPREXLA	Specifies the default STDPRT name that is to be used if no entry is found in table NSCPMAP. When provisioned to NPRT and no entry is found in table NSCPMAP, the originating subscriber's STDPRT name is used. If the option PRETRAN already exists in table NSCDEFS, consideration should be given to provisioning option PRETRANMAP with the same <i>values</i> as the existing option PRETRAN. By provisioning the same <i>values</i> , the switch behavior is unchanged from option PRETRAN for those STDPRT names that are not provisioned in table NSCPMAP.
	CALLS {ALL, COIN}	Specifies whether ALL calls or only COIN calls should use this functionality.
	IGNORE {Y/N}	Specifies whether this option should be ignored for the AIN or LNP Response translation.

Option PRETRANMAP provides equivalent functionality to the existing option PRETRAN by supporting subfields CALLS and IGNORE. Additionally, a DEFPREXLA field is provided which specifies the default STDPRT name to be used in the event an entry is not found in table NSCPMAP. By provisioning a default STDPRT name, only exception cases need to be provisioned in table NSCPMAP.

An added capability provided by option PRETRANMAP is the ability to use the originator's STDPRT name, rather than a default STDPRT name, in the event an entry is not found in table NSCPMAP. This is accomplished by provisioning NPRT for subfield DEFPREXLA.

The following is a provisioning example for the new option PRETRANMAP in table NSCDEFS:

TABLE: NSCDEFS		
NSCCODE	TIMEOUT	OPTIONS

E800	3	(PRETRANMAP PDEF ALL N) \$

Existing Option PRETRAN Considerations:

- The new option PRETRANMAP can be configured to function identically to the existing option PRETRAN in table NSCDEFS. This is accomplished by provisioning option PRETRANMAP with the same values that are

provisioned for the existing option PRETRAN and by not adding STDPRT names in table NSCPMAP.

- If the existing option PRETRAN functionality is required with the exception of those STDPRT names provisioned in table NSCPMAP, the new option PRETRANMAP should be provisioned with the same values as the existing option PRETRAN. In this case, the new option PRETRANMAP will provide equivalent functionality to the existing option PRETRAN with the exception of those STDPRT names provisioned in table NSCPMAP.

129.3.3 New SOC NTS00030

SOC NTS00030, “E800 Pretran Mapping” is added by this activity. This SOC is always at the ON state and does not control the feature functionality. This SOC has an RTU of A/P (Always Present) and the state cannot be changed to IDLE.

Note SOC NTS00030 requires SOC NTS00005, “E800-US”.

The new option PRETRANMAP in table NSCDEFS controls both the call processing and Traver enhancements provided by this activity (refer to sections “Call Processing” on page 1019 and “Traver” on page 1022).

129.3.4 Recommended Provisioning Procedure for PRETRANMAP

The following provisioning procedure is recommended:

1. Add the required STDPRT name tuples to table NSCPMAP.
2. For the E800 service, add the new option PRETRANMAP in table NSCDEFS. Do not immediately remove option PRETRAN if it is currently provisioned. Once option PRETRANMAP is added, the new functionality is active and option PRETRAN is no longer referenced by the switch software.

If option PRETRAN is currently provisioned in table NSCDEFS, consideration should be given to provisioning option PRETRANMAP with the same *values* as existing option PRETRAN. By provisioning the same *values*, the switch behavior is unchanged from option PRETRAN for those STDPRT names that are not provisioned in table NSCPMAP.

To revert back to the functionality provided by the existing option PRETRAN, option PRETRANMAP should be removed from table NSCDEFS. Option PRETRAN (if previously provisioned) must still be present in table NSCDEFS to revert back.

Once the switch is properly configured to use option PRETRANMAP and table NSCPMAP, the existing option PRETRAN can optionally be removed from table NSCDEFS. Removal of option PRETRAN is not mandatory.

129.3.5 Call Processing

The DMS100/CS2000 EO call processing software is enhanced to use the new functionality provided by the option PRETRANMAP and table NSCPMAP. Figures 1, 2 and 3 provide flow charts of the enhanced call processing behavior. The call processing software enhancements are active only when option PRETRANMAP is provisioned in table NSCDEFS.

Note that figure 2 depicts the switch behavior when an E800 Query is performed on a call and a non-IEC routing number is returned from the E800 database. The E800 Response translation subsequently hits an AIN or LNP trigger resulting in a query to the AIN/LNP database. The IGNORE subfield for option PRETRANMAP specifies whether the AIN/LNP Response translation should ignore the PRETRANMAP option and use the originating subscriber's pretranslator.

Figure 1 E800 Response Translation

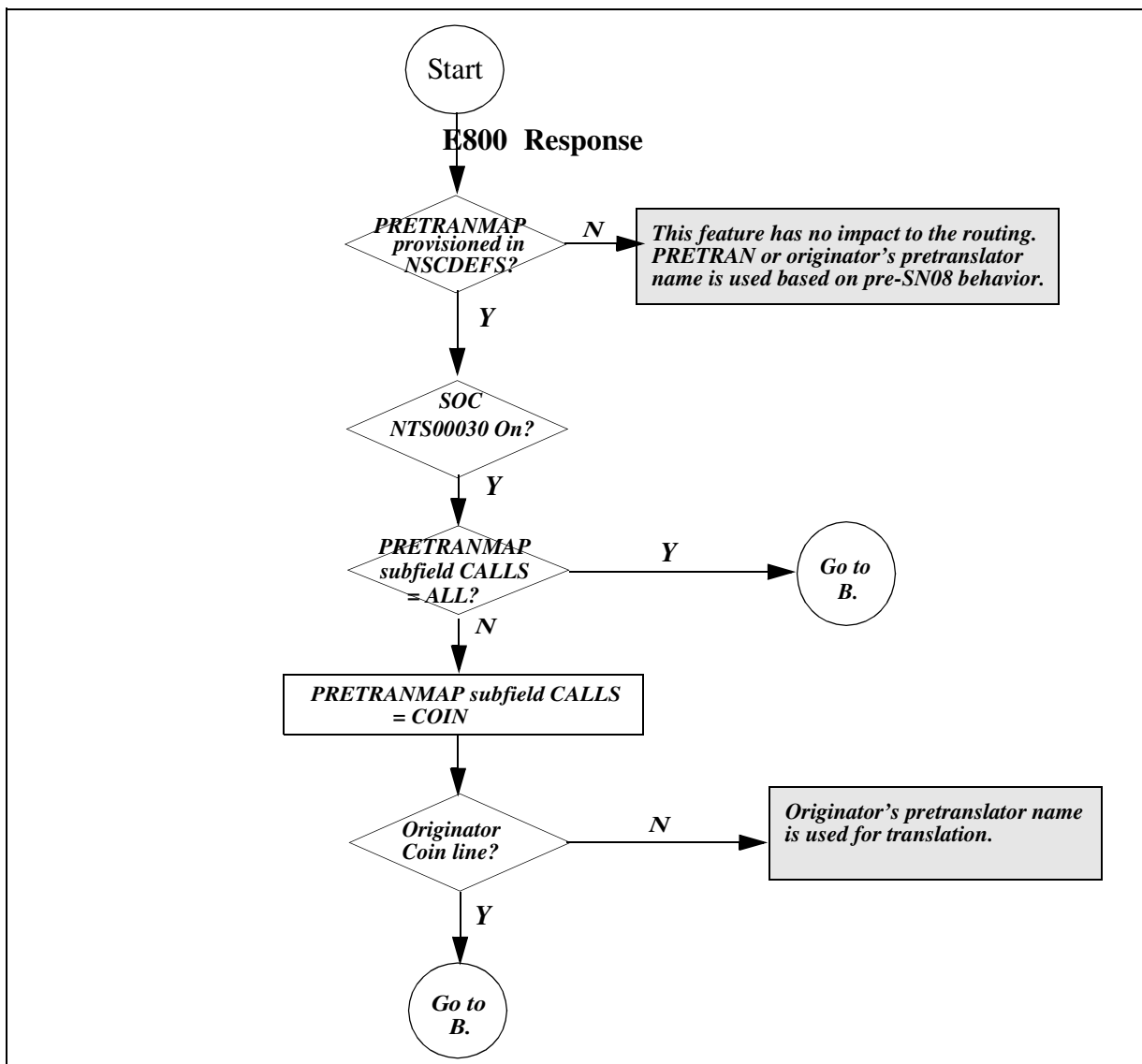


Figure 2 AIN/LNP Response Translation following an E800 Query

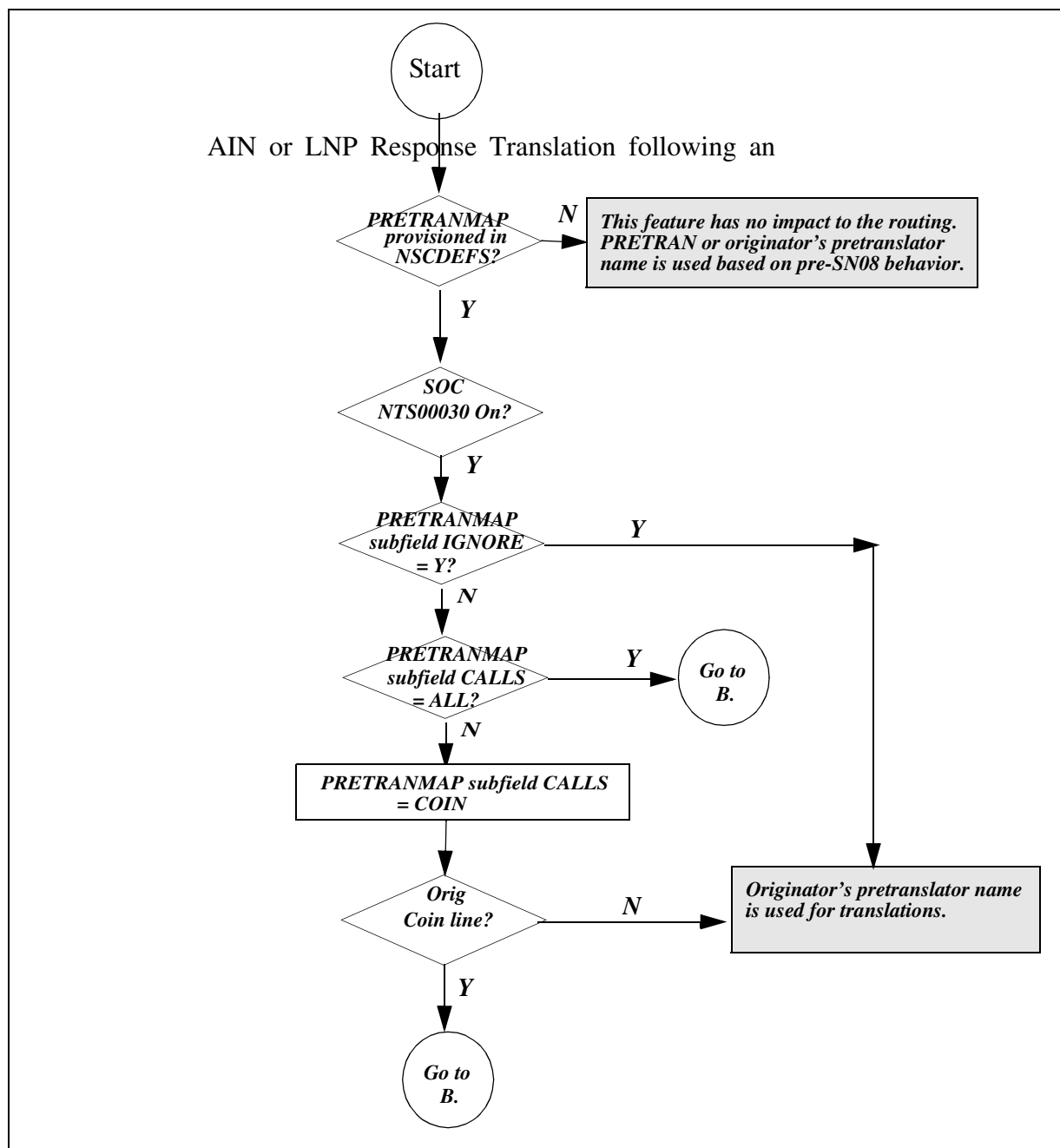
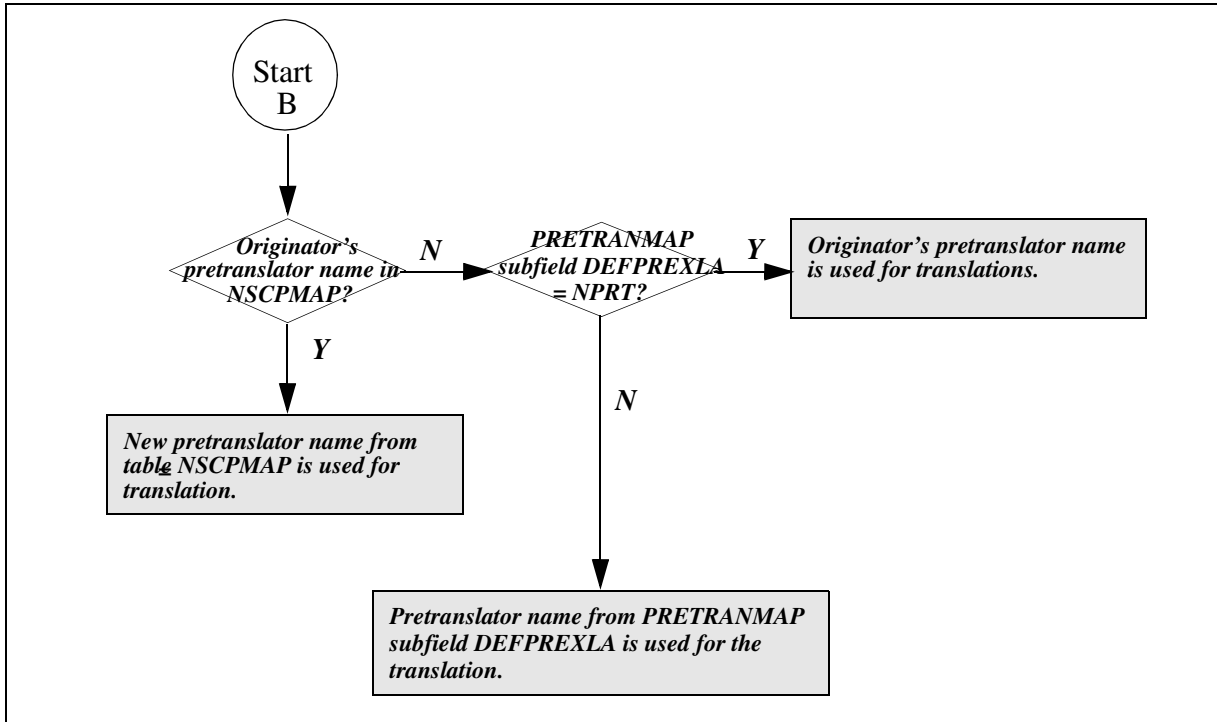


Figure 3 Response Translation - Part 2



129.3.6 Traver

The DMS100/CS2000 EO Traver software is enhanced to support the display of the new option PRETRANMAP in table NSCDEFS and to display the contents of the new table NSCPMAP. The existing “NSC” Traver command line option must be input in order to see the new Traver enhancements. The Traver enhancements are active only when option PRETRANMAP is provisioned in table NSCDEFS.

The following set of figures provide examples of the modified Traver output.

Figure 4 PRETRANMAP:CALLS set to ALL, entry in NSCPMAP

traver l 6215000 nsc 101022215198881111 b

```
TABLE LINEATTR
0 1FR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_0 L613_LATA1_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
613_P621_0 FR01 613 P621 TSPS Y RESGRP 0 2 $ $
TABLE RATEAREA
L613_LATA1_0 L613 NIL LATA1 $
TABLE DNATTRS
613 621 5000
(PUBLIC ( NAME SAM_SNEAD) $)$ $
TABLE DNGRPS
TUPLE NOT FOUND
TABLE LENFEAT
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP LNPOFFICE
TABLE NSCDEFS
E800 3 (4DGTIC ) (PRETRANMAP PDEF ALL Y) $
TABLE NSCPMAP
P621 P800
USING PRETRANSLATOR FROM TABLE NSCPMAP
TABLE STDPRTCT
P800 ( 1) ( 0) 4
. SUBTABLE STDPRT
. 1010222 1010222 EA DD 7 P PCAR CAR1 Y OFRT 700 8 25 N
. . TABLE OFRT
. . 700 S D ISUP2WATC
. . EXIT TABLE OFRT
. SUBTABLE AMAPRT
. KEY NOT FOUND
. DEFAULT VALUE IS: NONE OVRNONE N
TABLE STDPRTCT
PCAR ( 1) ( 0) 6
. SUBTABLE STDPRT
. 15 19 EA DD 1 T NA CAR1 N
. 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
. 519 519 FNPA 0
```

(traver for figure 2 continued)

TABLE FNPACONT

519 10 - (2) (0) (1) (0)

. SUBTABLE FNPACODE

. 888 888 3 Y

. SUBTABLE RTEREF

. . 3 N D ISUPIT 0 N N

. EXIT TABLE RTEREF

EXIT TABLE FNPACONT

LNP Info: Called DN is not resident.

LNP Info: HNPAA results are used.

TABLE LCASCRCN

613 L613 (56) OPTL N N Y

. SUBTABLE LCASCR

. TUPLE NOT FOUND. DEFAULT IS NON-LOCAL

TABLE PFXTREAT

TUPLE NOT FOUND. DEFAULT IS TO LEAVE XLA RESULT UNCHANGED

TABLE CLSVSCRC

KEY NOT FOUND

EA:Local override does not apply to this call.

TABLE LATA XLA

LATA1 51 INTER INTER STD

TABLE OCCINFO

CAR1 0222 TRANS Y Y Y Y Y N N Y Y Y Y LONG 0 FGRPD 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

Using Equal Access (EA) route OFRT 700 from Pretranslation

TABLE OFRT

700 S D ISUP2WATC

EXIT TABLE OFRT

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 ISUP2WATC 5198881111 ST

TREATMENT ROUTES. TREATMENT IS: GNCT

1 T120

Figure 5 PRETRANMAP:CALLS set to ALL, no entry in NSCPMAP, default in NSCDEFS

traver l 6215000 nsc 101022215198881111 b

```
TABLE LINEATTR
0 1FR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_0 L613_LATA1_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
613_P621_0 FR01 613 P621 TSPS Y RESGRP 0 2 $ $
TABLE RATEAREA
L613_LATA1_0 L613 NIL LATA1 $
TABLE DNATTRS
613 621 5000
(PUBLIC ( NAME SAM_SNEAD) $)$ $
TABLE DNGRPS
TUPLE NOT FOUND
TABLE LENFEAT
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP LNPOFFICE
TABLE NSCDEFS
E800 3 (4DGTCIC ) (PRETRANMAP PDEF ALL Y) $
TABLE NSCPMAP
TUPLE NOT FOUND
USING PRETRANSLATOR FROM TABLE NSCDEFS
TABLE STDPRTCT
PDEF ( 1 ) ( 0 ) 4
. SUBTABLE STDPRT
. 1010222 1010222 EA DD 7 P PCAR CAR1 Y OFRT 700 8 25 N
. . TABLE OFRT
. . 700 S D ISUP2WATC
. . EXIT TABLE OFRT
. SUBTABLE AMAPRT
. KEY NOT FOUND
. DEFAULT VALUE IS: NONE OVRNONE N
TABLE STDPRTCT
PCAR ( 1 ) ( 0 ) 6
. SUBTABLE STDPRT
. 15 19 EA DD 1 T NA CAR1 N
. 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
. 519 519 FNPA 0
```

(remainder of traver is the same as figure 2)

Figure 6 PRETRANMAP:CALLS set to ALL, no entry in NSCPMAP, NPRT in NSCDEFS

traver l 6215000 nsc 101022215198881111 b

```
TABLE LINEATTR
0 1FR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_0 L613_LATA1_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
613_P621_0 FR01 613 P621 TSPS Y RESGRP 0 2 $ $
TABLE RATEAREA
L613_LATA1_0 L613 NIL LATA1 $
TABLE DNATTRS
613 621 5000
(PUBLIC ( NAME SAM_SNEAD) )$ $
TABLE DNGRPS
TUPLE NOT FOUND
TABLE LENFEAT
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP LNPOFFICE
TABLE NSCDEFS
E800 3 (4DGTIC ) (PRETRANMAP NPRT ALL Y) $
TABLE NSCPMAP
TUPLE NOT FOUND
USING PRETRANSLATOR FROM TABLE XLAPLAN
TABLE STDPRTCT
P621 ( 1) ( 0) 4
. SUBTABLE STDPRT
. 1010222 1010222 EA DD 7 P PCAR CAR1 Y OFRT 700 8 25 N
. . TABLE OFRT
. . 700 S D ISUP2WATC
. . EXIT TABLE OFRT
. SUBTABLE AMAPRT
. KEY NOT FOUND
. DEFAULT VALUE IS: NONE OVRNONE N
TABLE STDPRTCT
PCAR ( 1) ( 0) 6
. SUBTABLE STDPRT
. 15 19 EA DD 1 T NA CAR1 N
. 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
. 519 519 FNPA 0
```

(remainder of traver is the same as figure 2)

129.4 Hardware Requirements or Dependencies

Not applicable.

129.5 Software Requirements or Dependencies

New SOC NTS00030, “E800 Pretran Mapping”, is added by this activity. NTS00030 requires existing SOC NTS00005 - “E800-US”.

129.6 Limitations and restrictions

The following limitations and restrictions apply:

- E800 is the only service supported by this activity.
The 800P and E008 services are not supported with option PRETRANMAP in table NSCDEFS¹. Table control restrictions are added to table NSCDEFS to prevent the PRETRANMAP option from being provisioned for a service other than E800.
- AIN Toll Free Service is not enhanced by this activity.
- Only the DMS100/CS2000 EO E800 software is enhanced by this activity. The DMS200 E800 software is not enhanced.
- NPRT (nil pretranslator name) cannot be provisioned in table NSCPMAP. Table control enforces this restriction.
- This feature does not support Attendant Consoles.
- The NSC option of TRAVER is not supported for PRI, PX, and MF/SS7 IBN trunks originating agents.
- The NSC option of TRAVER is not supported by AIN and LNP response translations.

129.7 Interactions

The following interactions apply:

- When the option PRETRANMAP is provisioned in table NSCDEFS, the existing option PRETRAN is no longer referenced by the switch software.
The existing option PRETRAN and the new option PRETRANMAP can co-exist in table NSCDEFS. This is permitted to support a transition from the existing option PRETRAN to the new option PRETRANMAP.
- If a redirection service (e.g. CFW) is encountered which results in an E800 Query and Response transaction, the STDPRT name of the redirecting agent is used to perform the lookup in table NSCPMAP.

¹Note the 800P and E008 services are currently not supported with the existing option PRETRAN in the table NSCDEFS.

- 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 the event AIN returns an 800 routing number resulting in a subsequent E800 TCAP Query, the interaction with the new option PRETRANMAP is dependent on whether the previous AIN translation specified a new pretranslator name or a new LINEATTR index:

If the previous AIN translation specified a new pretranslator name, the E800 response translation uses the originating subscriber's pretranslator¹. The new PRETRANMAP option is consistent with this behavior. If the option PRETRANMAP is provisioned, the originating subscriber's pretranslator is used to perform a lookup in table NSCPMAP.

If the previous AIN translation specified a new LINEATTR index, the E800 response translation uses the pretranslator name associated with the new LINEATTR². The new PRETRANMAP option is consistent with this behavior. If option PRETRANMAP is provisioned, the pretranslator associated with the new LINEATTR index is used to perform a lookup in table NSCPMAP.

AIN should not be configured to use a shared LINEATTR index for two (or more) groups of subscribers if the subsequent E800 translation requires a unique pretranslator for each group of subscribers. The mapping provided by table NSCPMAP uses the pretranslator name associated with the shared LINEATTR index. The shared LINEATTR index can only be mapped to a single pretranslator using table NSCPMAP.

129.8 Glossary

Table 3

Term	Description
800P	800 Plus
AIN	Advanced Intelligent Network
CFW	Call Forwarding
CS2000	Call Server 2000
DMS100	Digital Multiplex System 100
DMS200	Digital Multiplex System 200
E008	Enhanced 008
E800	Enhanced 800
EO	End Office

¹Applicable when neither the PRETRAN or PRETRANMAP option is used.

²Applicable when neither the PRETRAN or PRETRANMAP option is used.

Table 3

Term	Description
IEC	Inter-Exchange Carrier
LEC	Local Exchange Carrier
LNP	Local Number Portability
NPRT	Nil Pretranslator
SOC	Software Optionality Control
NSC	Number Services Code
SS7	Signaling System Number 7
STDPRT	Standard Pretranslator
TCAP	Transaction Capabilities Application Part

130: A00008045 Functional description (FN)

130.1 Feature name

CICM interoperability with SRG-500 for failover/recovery

130.2 Functional Overview

This feature implements the interoperability of CICM Gateway with SRG (Survivable Remote Gateway) in case of failover/recovery.

During normal mode of operation i20xx user will be connected to the CICM Gateway situated in the Main Office. This feature introduces a new option “Test Local Mode” which appears on the i20xx Etherset’s Diagnostics menu. On selection of this option, CICM will redirect the user to the SRG. When user connects to the SRG for the first time, it will be connected to the SRG until the set is manually provisioned as redirected set in the SRG. Once the set is provisioned as redirected set, SRG registers this set as a Redirected set.

In case of Network failure in-between Local office to the Main office, which might be due to the failure of the WAN link or the CICM Gateway is out of service, sets will reboot and will get connected to the SRG.

This is called Local Mode of operation with respect to the i20xx Ethersets.

While in Local Mode, Ethersets will be able to make call to any other IP client user registered to the SRG.

Without H.323, Calls coming from PSTN network connected to the SRG will **NOT** be able to reach those MODN connected to the SRG as redirected set if provisioned properly.

SRG will keep polling the status of the CICM Gateway regularly by sending NULL RUDP packets. As soon as the NULL RUDP packets are acknowledged by the CICM Gateway, SRG will redirect the Ethersets to the CICM.

In summary, Activity A00008045 provides the following functionalities to the users

- Users will be connected to the Main Office (as before) in normal scenario.
- During Network failure Users will be isolated from the Main Office but connected locally via SRG. Users will be able to contact other MODN connected to the same SRG.

- During Network failure calls coming from PSTN, a network connected with the SRG will be able to reach MODN Users via SRG.
- When User connects back to the CICM gateway, all the missed calls, messages and user settings will be restored.

130.3 Description

Users will be connected to the CICM Gateway situated in the Main Office. In case of connection failure to the CICM Gateway it will be temporarily registered with the SRG.

The following figures describe communication path during various possible modes of operation.

Figure 1 Normal Mode Control Path

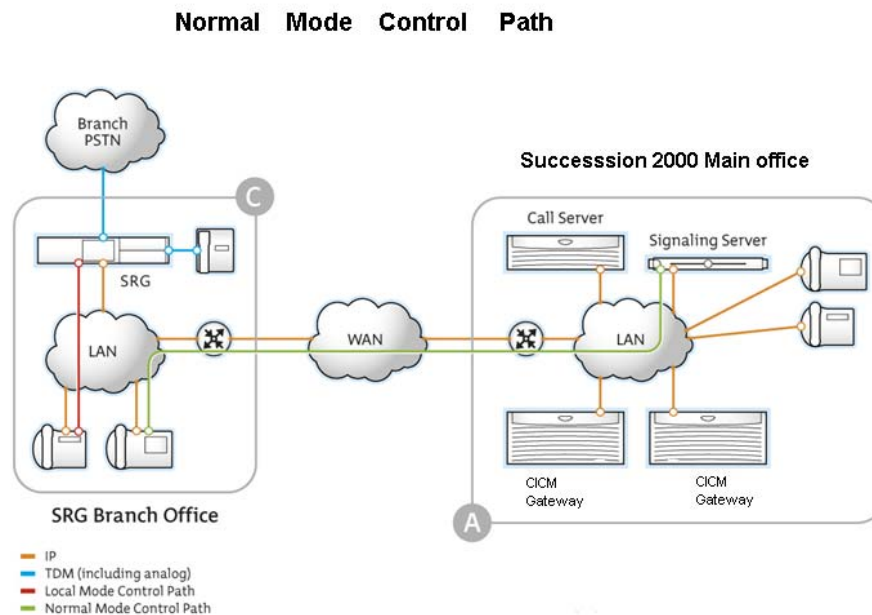


Figure 2 Local Mode Control Path (WAN failure)

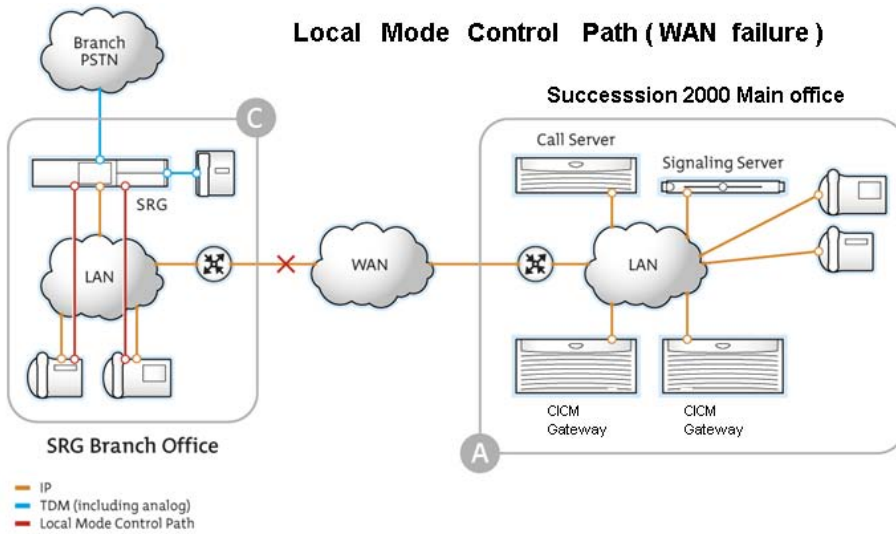
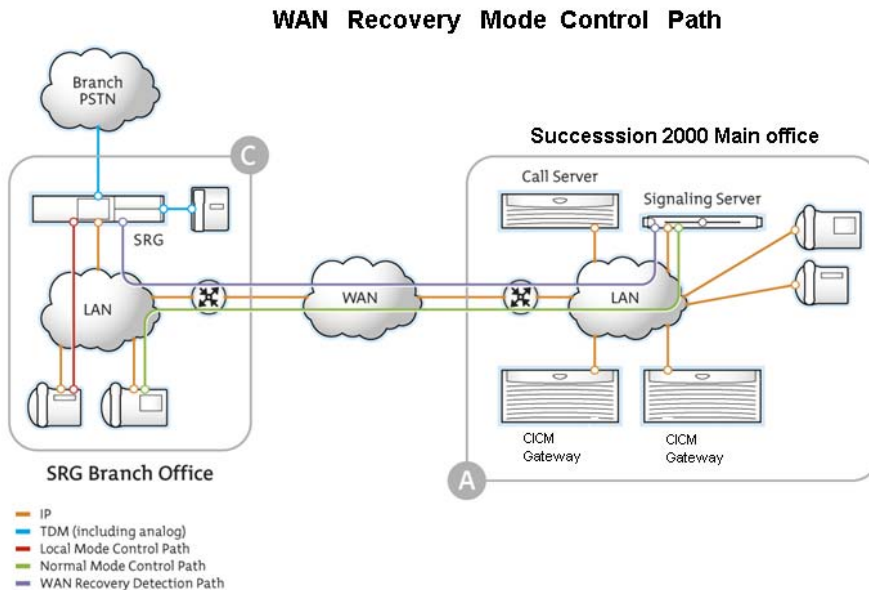


Figure 3 WAN Recovery Mode Control Path



SRG Branch Office is a part of the Succession 2000 Main Office Enterprise LAN. I20xx Ethersets will be located in the Local office (SRG branch office as in the figures). Ethersets will be connected to the Main Office via WAN link. S1 and S2 IP addresses of the i20xx Etherset have to be configured with the CICM and SRG client addresses respectively.

Normally, i20xx Ethersets will be connected to the Main office i.e. They will be connected to the CICM Gateway situated in the Main Office. In case of WAN failure, i20xx Ethersets will fail to connect to the S1 IP address and will get connected to the S2 IP address which is SRG's IP address. This is called Local mode of operation. While in Local mode i20xx Ethersets will be able to use various services provided by the SRG. For example, making calls to other i20xx Ethersets connected to the SRG. Details of the services provided by the SRG is referenced in the reference section of this document.

While in Local mode SRG will poll the CICM Gateway (at an interval of 3 seconds) to find out whether the Network connection between the SRG and the CICM Gateway is being restored. As soon as Network connection between the SRG and Main Office recovers, SRG will redirect the Ethersets to the CICM Gateway.

130.3.1 Normal Mode operation

In normal mode user is connected to the CICM gateway situated in the Main Office. Both CICM Gateway and the WAN link between the Main office and SRG are up and running.

Summary of the actions involved, in the Normal mode, are as follows.

- S1 configured with CICM IP Address (Action code = 6, for Security)
- S2 configured with SRG IP address (Action code = 1 Port = 7300).
- Sets initially register to CICM (on S1)
- CICM will have "local mode" option available to user/installer
- CICM will redirect sets to S2 (Non secure)
- SRG will boot sets for the first time
- Sets will be visible on SRG for provisioning and will remain on the SRG until provisioned as redirected sets
- Installer will manually redirect each set, specifying a Main Office DN, if desired, to support redirection of inbound calls to the set from the local PSTN connections on the SRG. The installer may leave the MO DN blank, and the set will still be redirected, but with no support for inbound calls from the SRG's local PSTN.
- Post installation, if the "Local Mode" feature is invoked on the CICM, the sets will be redirected back to SRG, where they will stay until either: the user presses the stop sign key or the configurable Test Local Mode timer times out.
- If S1 is initially not visible (because branch WAN is not yet connected), sets will boot on SRG on S2 and will stay there until provisioned as being redirected. Even if WAN is connected, sets will stay until provisioned as being redirected.

130.3.2 Local Mode Operation (WAN failure)

When the WAN link is down user will lose connection with the CICM Gateway. The set will reboot and try to connect to S1 address (which is the CICM address). After trying no of retry count configured with S1, Etherset will try to connect to the S2 address (which is of the SRG). Summary of the actions involved are as follows.

- The sets will time out on S1 (CICM Gateway IP address) and move to S2 (SRG IP address) where they will register with SRG.
- SRG will ping S1 with NULL RUDP packets at regular interval to find out whether it is up and running.
- User registered with the SRG will be able to call other users connected to the SRG and avail other services from the SRG.

130.3.3 WAN Recovery

As soon as WAN link is up, S1 (CICM Gateway) will respond to the NULL RUDP packets sent by SRG. SRG will redirect the set to S1. Set will go through a reboot and get connected to the CICM Gateway. Summary of the actions involved during WAN recovery are as follows.

- If S1 responds to the NULL RUDP ping two times, the set will be redirected back unless a hold off is in place
- The set will be held off from redirecting if
 - The set is busy on a call
 - The Test Local Mode timeout has not expired (this hold off is cancelled by the Stop key)

130.3.4 CICM Roaming and SRG interoperability

If the CICM Gateway, to which user is connected, is a part of an enterprise profile, User will have more than one CICM Gateway to connect to. All the available CICM Gateway will appear on the option menu. User can select any of the available CICM Gateway to connect to. Summary of possible actions involved due to CICM Roaming interoperability with SRG are as follows.

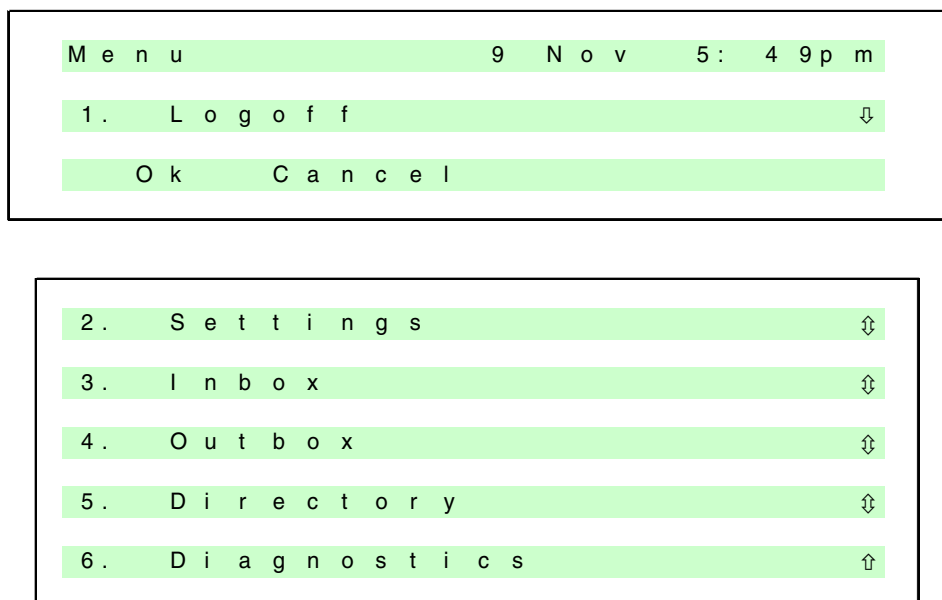
- If the user selects a different CICM from the list of available CICM's on the CICM Roaming User Interface, it gets redirected to the remote CICM via S3.
- If the Remote CICM is unresponsive, the set falls back to the Default CICM via S1, if the default is not available it obviously falls back to SRG on S2 where we monitor the CICM in S1 via NULL RUDP pings
- If the Remote CICM is responsive and the change is committed, the new CICM is programmed into S1, with no change to S2.

- If at this point the remote CICM becomes unreachable, the set will fall back to SRG on S2. SRG will NULL RUDP ping the CICM in S1, which is the new CICM. The original Default CICM is out of the picture.

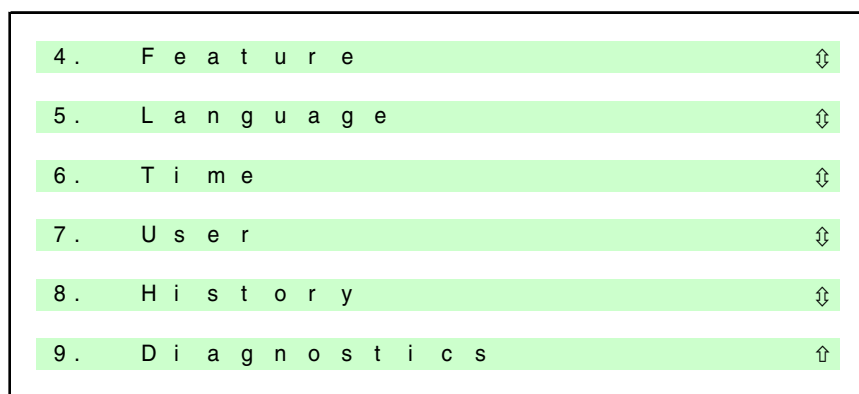
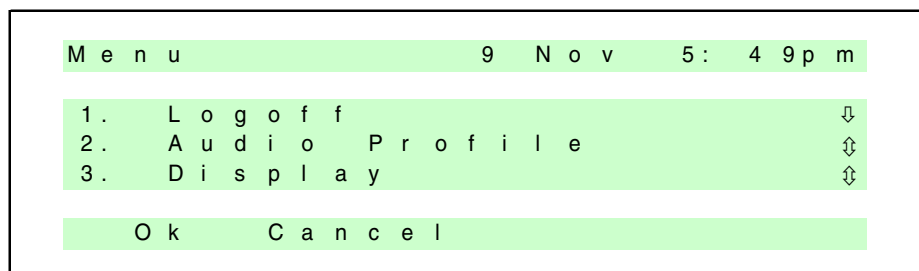
130.4 Provisioning

I20xx Ethersets will have “Test Local Mode” under diagnostics menu.

Figure 4 Menu Option: Diagnostics Menu Option on the IP Phone 2001



Menu Option 6: Diagnostics. This is available when the User Profile of User Overrides has the option Disable Diagnostics Menu set to No. Setting this option to Yes will remove this menu option

Figure 5 Menu Option: Diagnostics Menu Option on the IP Phone 2002 / 2004

Menu Option 9: Diagnostics. This is available when the User Profile of User Overrides has the option Disable Diagnostics Menu set to No. Setting this option to Yes will remove this menu option

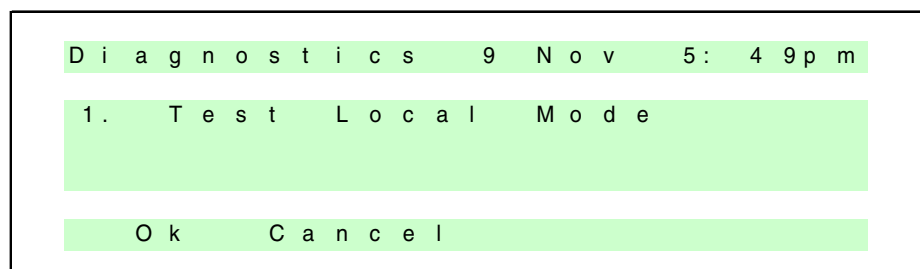
Figure 6 Diagnostics Menu: Test Local Mode

Figure 7 Diagnostics Menu: Test Local Mode confirmation

L o c a l M o d e	9 N o v	5 : 4 9 p m
A r e y o u s u r e		
Y e s	N o	H e l p

Figure 8 Diagnostics Menu: Test Local Mode Help

H e l p	9 N o v	5 : 4 9 p m
T e s t L o c a l M o d e .		
T r a n s f e r t h i s t e r m i n a l		
t o i t s S 2 a d d r e s s .		
O k		

Figure 9 Element Manager: Disable Diagnostics Menu option.

Prevent user logging out	☐ (IP Phone 20xx only)
Prevent user changing time settings	☐ (IP Phone 20xx only)
Disable Diagnostics Menu	☐ (IP Phone 20xx only)
Headset Confirmation Tone Configuration	☐
Headset Confirmation Tone Active	☐

This option is present on the User Profiles and User Override pages of the Element Manager, when set to Yes the diagnostics menu will not be present on the users main menu. Default for this parameter is No.

i20xx Ethersets have to be provisioned as follows.

- IP Set Configuration
 - S1 = CICM Gateway IP address, Action code = 6, Port 5000
 - S2 = SRG IP address, Action code = 1, Port 7300
- **System installation**
 - Ethersets initially register to CICM (on S1).
 - CICM will have “test local mode” option available to user/installer.
 - CICM will redirect sets to S2 (Non secure).
 - SRG will boot sets for the first time.
 - Sets will be visible on SRG for provisioning and will remain on the SRG until provisioned as redirected sets.
 - Installer will manually redirect each set, specifying a Main Office DN, if desired, to support redirection of inbound calls to the set from the local PSTN connections on the SRG. The installer may leave the MO DN blank, and the set will still be redirected, but with no support for inbound calls from the SRG's local PSTN.
 - Post installation, if the “Test Local Mode” feature is invoked on the CICM, the sets will be redirected back to SRG, where they will stay until either: the user presses the stop sign key or the configurable Test Local Mode timer times out.
 - If S1 is initially not visible (because branch WAN is not yet connected), sets will boot on SRG on S2 and will stay there until provisioned as being redirected. Even if WAN is connected, sets will stay until provisioned as being redirected.

When the set registers with the SRG for the very first time, it would stay in “Local Mode” until it is manually provisioned as “Redirected”. To provision the set as “Redirected” the following steps are to be followed.

1. Log in to the SRG Unified Manager by opening an IE browser and type `http://srgIPaddress`. **Userid:** admin **Password:** *****
2. Select “SRG” node under “Services”. On the right window panel “Summary”, “Main Office” and “IP Terminal Status” tabs will appear.
3. Select the “IP Terminal Status” tab. List of DN entries will appear on the window. Select the DN which appears on the i20xx Etherset while in Local mode.
4. To provision the set as redirected you have two options:

-
- Option 1: Redirect the Set without specifying a Main Office DN (MODN).
 - This is done by selecting the “Redirect Set” option from the configuration menu. The configuration menu is on the Main Horizontal Menu Bar on top of the screen.
 - SRG will start sending the RUDP pings (NULL PAYLOAD) to the CICM as soon as this option is selected.
 - Option 2: Specify a (Main Office DN) for the set.
 - This is done by selecting the “Modify Parameters” option from the configuration menu.
 - A dialog box will open up, with the empty MODN field. You can specify the MO DN which would be the DN of the set when registered at the CICM. This is required only if the SRG is equipped with PSTN trunks and you want calls from the local PSTN to be automatically forwarded to the DN specified in the MO DN field.

130.5 Hardware Requirements or Dependencies

BCM50 hardware and 5370/5385 CICM and 5370/5385 CICM-EM.

130.6 Firmware Requirements or Dependencies

Etherset Phase1 F/W 1.71 and above. Etherset Phase2 F/W 2.49 and above. BCM50 (SRG H/W) will be loaded with BCM50 plus the SRG500 patch software.

130.7 Software Requirements or Dependencies

Fully configured SRG500 running BCM50 plus SRG500 patch software. Fully configured CICM Gateway and Element manager.

This Activity is dependent on Active Call Failover feature (ACF) to be functional.

130.8 Limitations and restrictions

- SRG is a stand alone solution i.e. it does not communicate with the Call Server via H.323
- Currently it does not support m6350 softclient and i2033 etherset.
- Security is not available in local mode i.e. when User is connected to the SRG due to WAN failure.
- Currently there is no automatic configuration available for registering the redirected sets to the SRG. All the data have to be provisioned manually.

130.9 Glossary

Term	Description
ACF	Active Call Failover
BCM	Business Communication Manager
CICM	Centrex IP Client Manager
CICM-EM	CICM- Element Manager
MODN	Main Office Directory Number
MO	Main Office
LAN	Local Area Network
WAN	Wide Area Network
RUDP	Reliable User Datagram Protocol
SRG	Survivable Remote Gateway
PSTN	Public Switched Telephone Network

130.10 References

1. A00003953 Active Call Failover.

<http://pndinfo.europe.nortel.com/centrexip/ccdocs/documents/activities/A00003953/A00003953FN.doc>

2. SRG500 IPS.

131: A00008229 Functional description (FN)

131.1 Feature name

SN08: CICM i2033 IP Conference Terminal

131.2 Description

The i2033 is an IP Conference phone, the i2033 emulates the IP Phone 2001 introduced to the CICM in SN07. With the introduction of this conference phone we increase the number of terminals supported on the CICM and an audio conference phone will help provide an end-to-end IP network solution to our customers. Increasing numbers of enterprise and carrier customers are specifying IP audio conferencing phones as a requirement in RFI and RFP documents

The Nortel OEM Polycom, Inc. was selected as the vendor of choice to develop the 2033. Polycom controls the majority market share in the global audio conferencing market, and their products are known to provide superior performance and reliability

Figure 1 2033 top view



While 2033 emulates a low-end IP Phone 2001, there are some differences and unique characteristics that make this phone distinct. The main differences are:

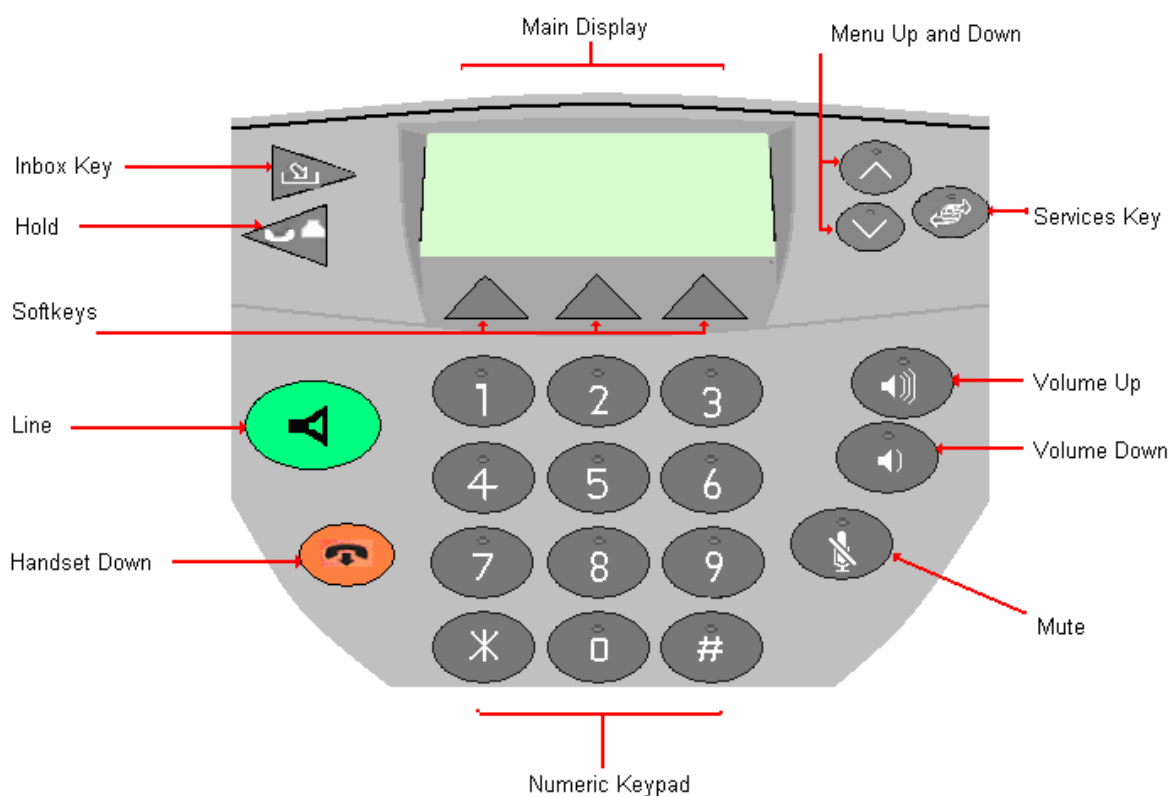
- 2033 is a handsfree unit.
- Lack of hookswitch on 2033.
- Presence of microphone.
- 3 softkeys instead of four.
- Mute button.

2033 is a Nortel-branded UNISTim IP conference unit based on the hardware of Polycom SoundStation IP unit. The firmware is sourced from an OEM and is unique for 2033.

131.2.1 Display

The 2033 LCD screen is identical to the IP Phone 2001 LCD screen.

Figure 2 2033 Function keys and screen



131.2.2 Generic Display Rules

The following rules have been devised for the i200x terminals and apply to the 2033 conference IP phone. These rules have been introduced to allow one

common interface across both terminal types and to help avoid issues with Language Translations on soft key strings.

1) All strings for menu options should be created with the following rules in mind:

- Recommended length 12 characters – strings meeting this condition will always be shown in full (both on the information lines and in the context field)
- Maximum length 20 character – strings above 12 characters in length and equal to or below 20 characters will be fully displayable in the information line but not in the context field. Long strings in the context field will be cropped off to 11 characters and terminated with an ellipsis to indicate they have been cropped.
- Strings above 20 characters to be shown:
- In the information lines will be cropped off to 19 characters and terminated with an ellipsis to indicate they have been cropped.
- In the context field will be cropped off to 11 characters and terminated with an ellipsis to indicate they have been cropped.

2) The Login Screen echoes entered digits to information line 0 rather than line 1. The username and passwords entered may be up to a maximum of 15 digits. If the username/password entered is longer than the field space left on the screen (i.e. if the “Username” string is 14 characters and 12 username digits are to be entered), the digits will be scrolled to the left and an ellipsis will be inserted to the left of the username to indicate this.

3) Bottom Soft key labels are set to a maximum of 5 characters with the exception of the last soft key on the screen which may use up to a maximum of 6 characters.

Figure 3 2033 Log-in display



4) Soft key labels are limited to a small generic subsection of the previously used soft keys (“Ok”, “Cancel”, “Clear”, “Bkspc”, “Menu”, “Help”, “Yes” and “No”).

5) Menu options are selected via a scrollable list (instead of being assigned to a soft key). Scrolling may be carried out using the up and down navigation. This allows menu options to be displayed in strings which may be up to a maximum of 20 displayable characters (see rule

This is advantageous for the following reasons:

- A greater area makes language translations easier.
- A more informative string may be displayed.

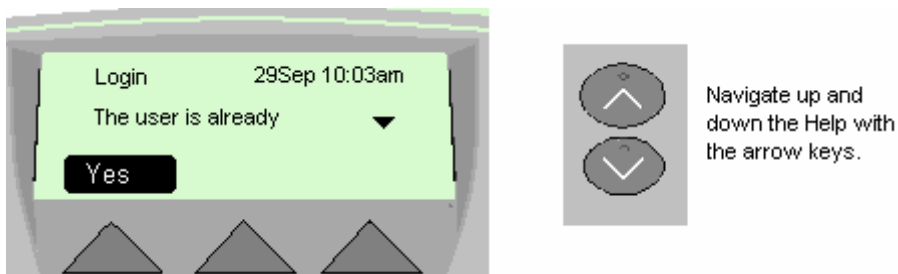
6) The position within a scrollable list is displayed to the far right hand side of the display. 1 character space is reserved to show scroll position.

7) All Menu Options in the scrollable list are numerically indexed with the shortcut key number assigned to that option, with the exception of the Inbox, Outbox and the Directory menu's. The numerical indexes will go from 1 – 9. Options above 9 will have no shortcut assigned/displayed next to the menu option.

8) A menu option may be selected by either highlighting the option (IP Phone 2004) or viewing the option (IP Phone 2002, IP Phone 2001, 2033) and selecting "Ok". Alternatively the appropriate shortcut key assigned to an option may be selected using the key pad. This will cause the user to jump straight into the menu option required without scrolling.

9) The Logout option is presented as the first option in the Menu Options List. This will avoid language translation issues on when using a soft key for the same operation.

10) All user prompts will be presented on Information line 0 on the display. The maximum length of a prompt is 23 characters. Prompts beyond 23 characters will be cropped down to 22 characters and an ellipsis will be presented as the 23rd character to indicate cropping has taken place. Further text to describe the prompt is viewable on a help screen which is accessed by selecting a "Help" soft key. The help screen presents text to the user by using scrolling pages. The help screen has a maximum number of 255 characters (due to the scrolling functionality). The recommended word size is 24 characters (words exceeding this limit will be word wrapped onto the next line of the display).

Figure 4 Override prompt**Figure 5 i2033 Override Help screen**

11) The Menu system is accessible by either selecting the “Menu” softkey or by selecting the “service” physical key. The IP Phone 2001 and 2033 terminal also provides feature activation via the “service” key when either CXR or 3WC is assigned on the core to one of the DN’s first 14 keys. (see Feature Interaction)

Figure 6 i2033 Service Key position

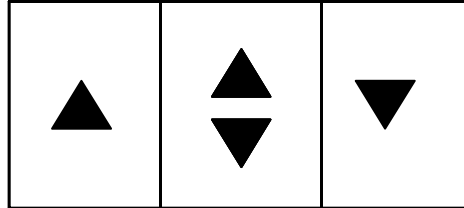
131.2.3 2033 Display Rules

The similarities between the IP Phone 2001 and 2033 terminals ensure that the display rules that are present on the IP Phone 2001 are also present on the 2033.

To show the information required to the user on a restricted display, the following list of rules have been devised.

- The Menu options are selected via a scrollable list.
- The relative position within the list is show to the far right of information line 0 via up and down arrows.

Figure 7 Example of navigation arrows



- Information line 1 is dedicated for the Soft keys.
- Time / Date is displayed on context line.

The 2033 has three LEDs that are always in an identical state. The following table shows the current implementation of the LED states:

State	IP Phone 2001 LEDs	2033 LEDs
Phone off hook	N/A	Solid Green
Mute	Mute LED Solid Red	Solid Red
Incoming call	Message Waiting LED Flashing Red	Flashing Green
Message Waiting	Message Waiting LED Solid Red	Flashing Red

131.2.4 Key Mappings

The following list includes the fixed keys on 2033. Keys are icon-only and similar to the corresponding keys on 200x IP phones.

- Numeric pad: 1-9, #, *.
- Volume Up
- Volume Down
- Mute
- Services
- Inbox (Messages)
- Hold
- Scroll Up
- Scroll Down
- Line (Speaker icon)
- Release
- Three soft keys

Similar to IP Phone 2001, the 2033 has no feature keys (soft labels) beside the LCD screen.

A configuration item in 2033 boot menu allows the user to choose two key mapping emulation modes: HF (Handsfree) and HS (Handset). In handsfree emulation mode the phone sends 'line' and 'release' key events. In handset emulation mode, pressing the 'line' key sends an 'off-hook' event and pressing the 'release' key sends an 'on-hook' key event. Because there is no toggle switch involved, it will be possible to send multiple off-hook (or on-hook) events; which is not possible in Nortel IP phones.

The CICM supports 2033 in handsfree mode (no hookswitch event) where the Line Key acts identical to programmable key 0 on 200x IP phones.

The 2033 has three keys assigned for context-dependent soft keys on the LCD screen. In the current IP Phone 2001 emulation mode, the 2033 supports four soft keys by using the third key as 'shift'. However for any future release of the call server that could distinguish between IP Phone 2001 and 2033, we recommend that the call server uses three soft keys only.

The IP Phone 2001 has no mute button, so the mute button on 2033 is local (no mute/unmute event is sent by the phone).

131.2.5 Audio and Tones

The 2033 is a handsfree phone with a single transducer. Currently, the phone supports G.711 A-law and Mu-law, and G.729A.

The 2033 supports stream-based and transducer-based tones and cadences, and programmable tones as specified in the UNISim specification document.

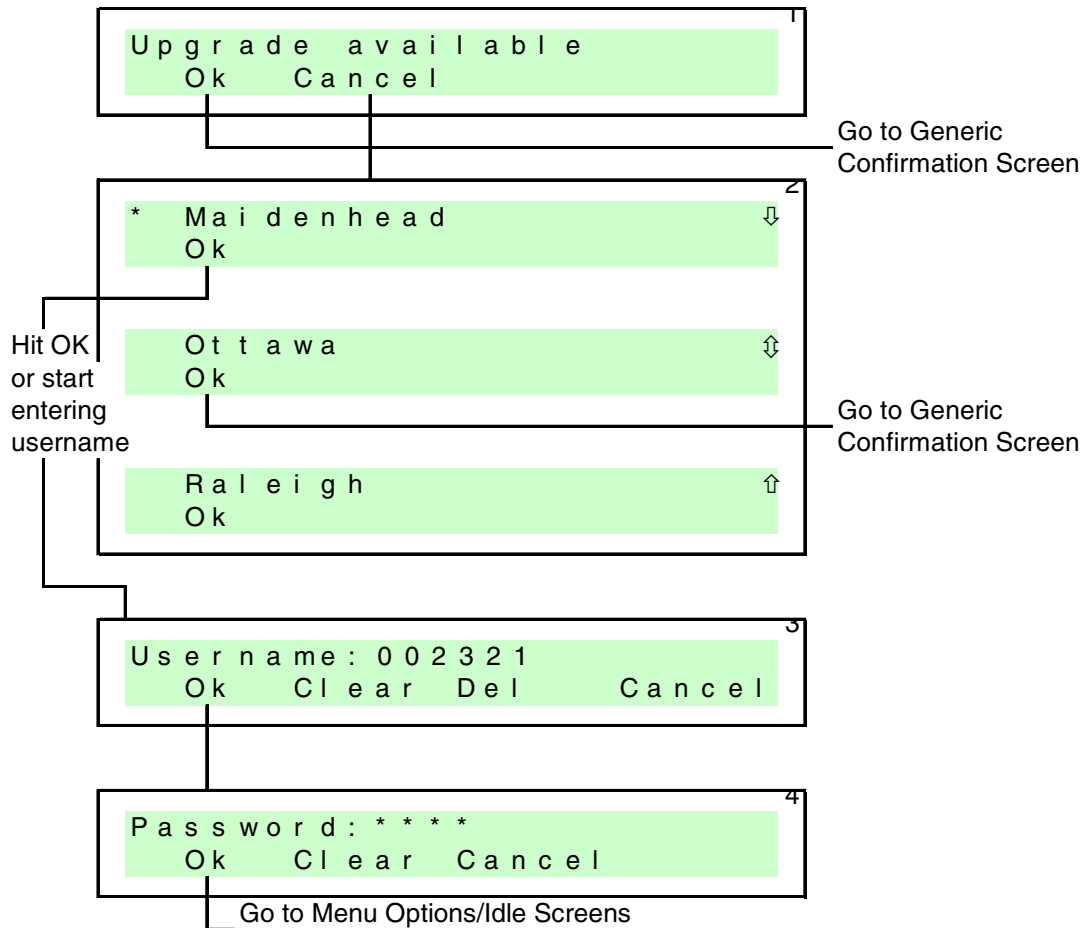
131.2.6 Menu Map

The following screen representations show what will be presented to the user when logging on to a gateway, and navigating the menu options of the 2033.

131.2.6.1 Login Screens

- 1 "Cancel" option is absent for "forced" upgrades. Menu not presented if no upgrade available.
 - 2 When the "active" server is shown (marked with a *), the user can start entering the username immediately or hit "Ok."
 - 7 "Centrex IP" is an *Enterprise* specific name, or (if one doesn't exist) the global Centrex Product Name.
 - 8 The logout function has moved into the menu (to remove the need for another soft key "verb"), other items in this menu are TBD.
- "Cancel"/"No" always returns to the previous menu (where one exists)
 "Ok" is always the first option, "Cancel" is always the last option
 "Help" buttons can be used to explain any ambiguities

I2002



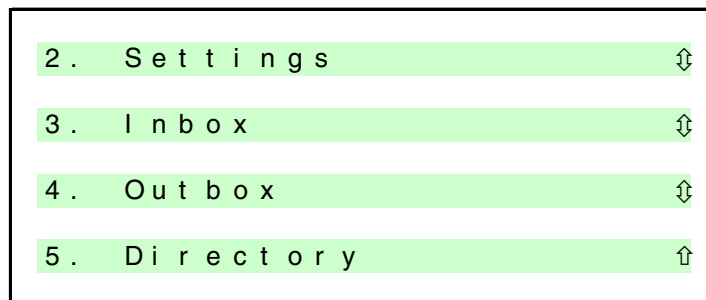
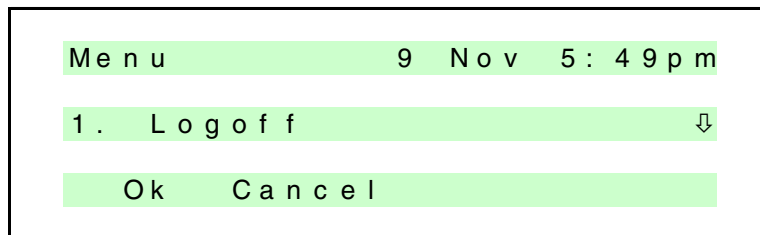
Screen 1 – Only shown if an upgrade is available / required.

Screen 2 – Selective Gateway Login feature

Screen 2 – A user can either hit “Ok” to accept a gateway to login to, they will then be presented with Screen 3 to login. Alternatively the user may start entering their username digits and this will also accept the currently selected gateway, go to Screen 3 and insert the digit(s) already entered.

Screen 3– If the username is too long for the display, the digits entered will scroll to the left, and an ellipsis will be shown to the left of the username to indicate this to the user.

131.2.6.2 Menu Option/Idle Screens



Menu Option 1: Logoff – a Generic confirmation screen is displayed.

Menu Option 2: Settings – launches the new 2033 settings menu.

Menu Option 3: Inbox – Launches the inbox, Inbox is also available via dedicated Inbox key.

Menu Option 4: Outbox – Launches the Outbox, the 2033 does not have a dedicated Outbox key and will only be able to access the Outbox via this menu system.

Menu Option 4:Directory – Launches the directory contact list, the 2033 does not have a dedicated Directory key and will only be able to launch the directory via this menu system.

131.2.6.3 Menu Option: Settings

Settings	9 Nov 5:49pm
1. Regional	↓
Ok	Cancel

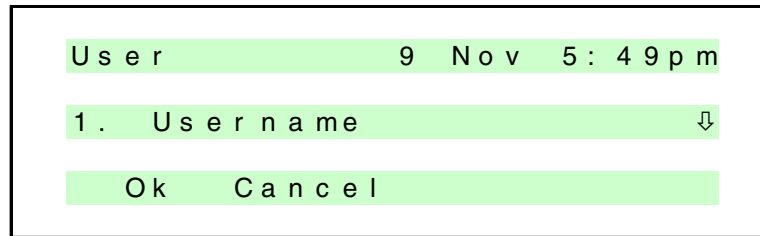
2. User	↕
3. Terminal	↕
4. Call	↑

131.2.6.4 Menu Option: Regional Settings

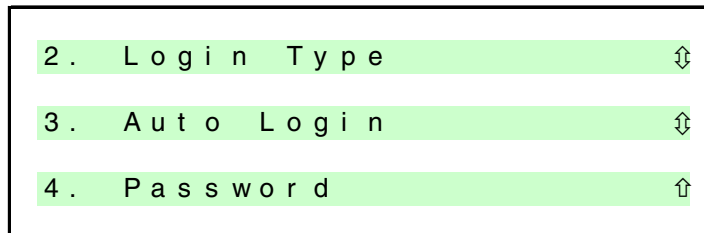
Regional	9 Nov 5:49pm
1. Language	↓
Ok	Cancel

2. Time	↕

131.2.6.5 Menu Option: User Settings

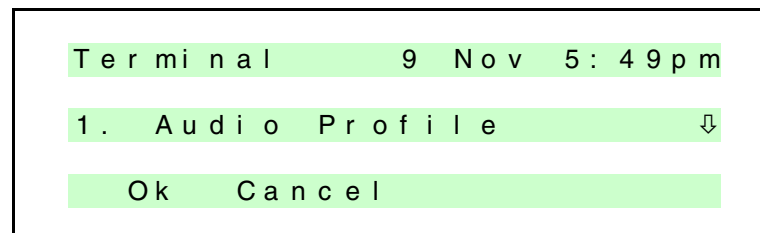


A screenshot of the 'User Settings' menu. At the top, the text 'User' is followed by the date and time '9 Nov 5:49 pm'. Below this is a list item '1. Username' with a downward arrow icon. At the bottom are two buttons: 'Ok' and 'Cancel'.

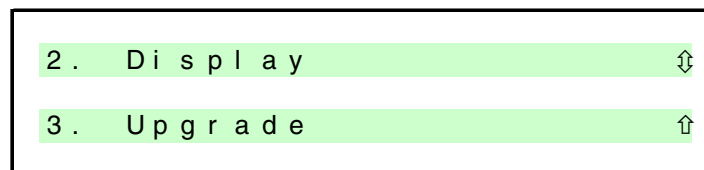


A screenshot showing the continuation of the 'User Settings' menu. It contains three list items: '2. Login Type' with a double-headed arrow icon, '3. Auto Login' with a double-headed arrow icon, and '4. Password' with an upward arrow icon.

131.2.6.6 Menu Option: Terminal Settings



A screenshot of the 'Terminal Settings' menu. At the top, the text 'Terminal' is followed by the date and time '9 Nov 5:49 pm'. Below this is a list item '1. Audio Profile' with a downward arrow icon. At the bottom are two buttons: 'Ok' and 'Cancel'.



A screenshot showing the continuation of the 'Terminal Settings' menu. It contains two list items: '2. Display' with a double-headed arrow icon and '3. Upgrade' with an upward arrow icon.

Terminal Settings Option 1: Launches the Audio Profile menu.

Terminal Settings Option 2: Launches the display Contrast screen

Terminal Settings Option 3: Launches the Upgrade confirmation menu, depending on if an upgrade is available or necessary.

131.2.6.7 Menu Option: Call Settings

Call 9 Nov 5:49pm

1. Feature ↓

Ok Cancel

2. History ↑

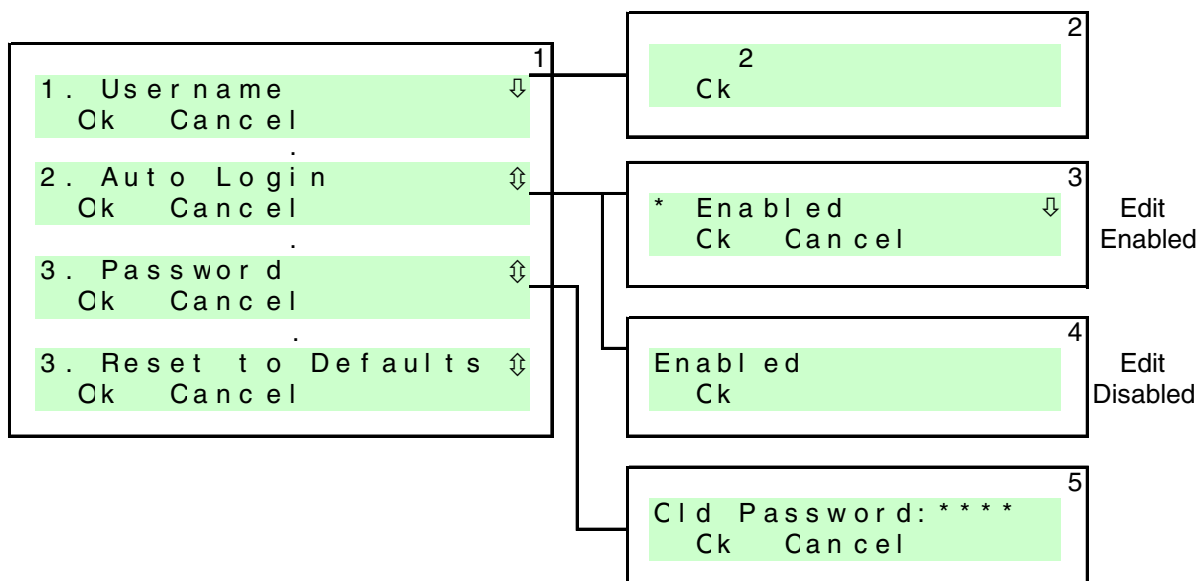
131.2.6.8 Display Contrast Screen

Contrast 9 Nov 5:49pm

< ■■■■■■■■ > 53%

Ok Cancel

131.2.6.9 User Information Screens

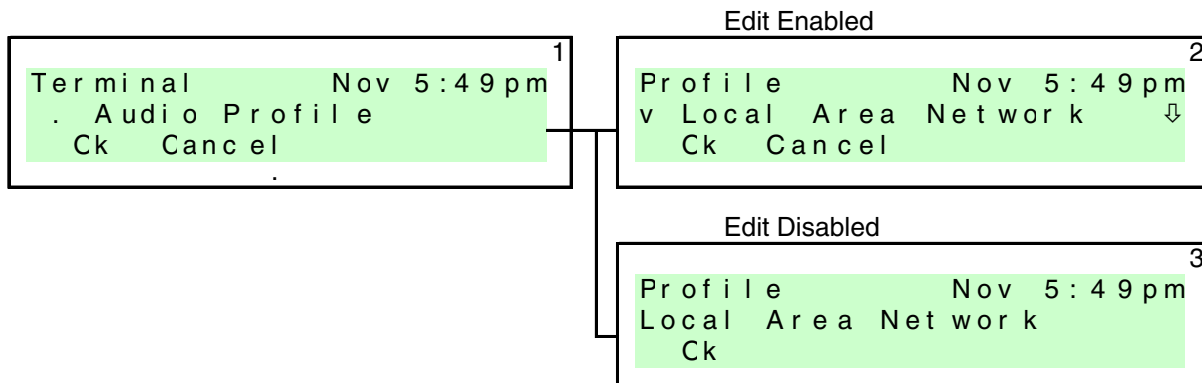


Screen 3 – The user has permission to edit their Auto Login functionality. The user may enable/disable the feature from this screen.

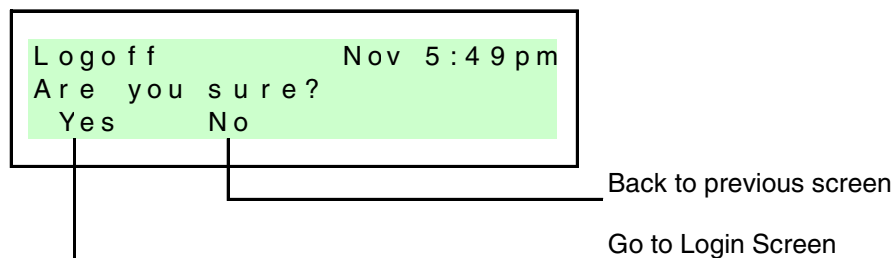
Screen 4 – The user has view permission to the Auto Login functionality. The user may only view what their current setting is.

Note: The permissions are configurable via the element manager in the user/user profile settings.

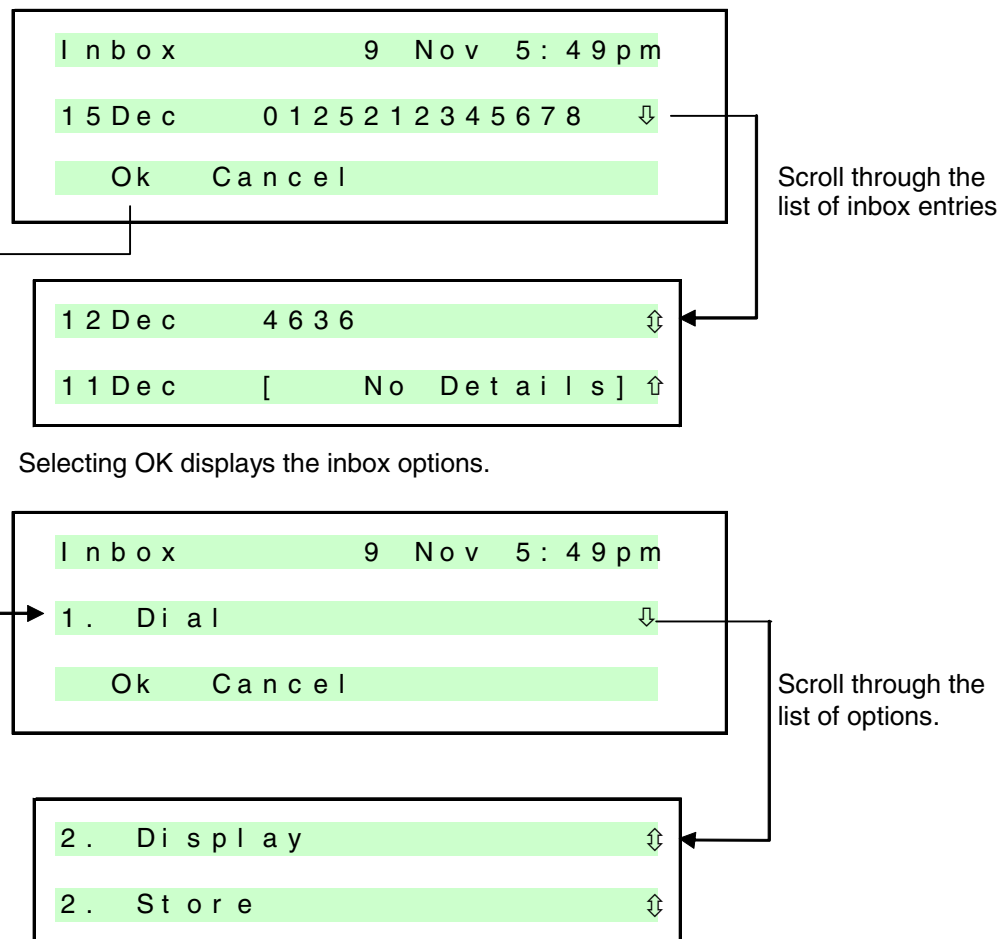
131.2.6.10 Audio Screens



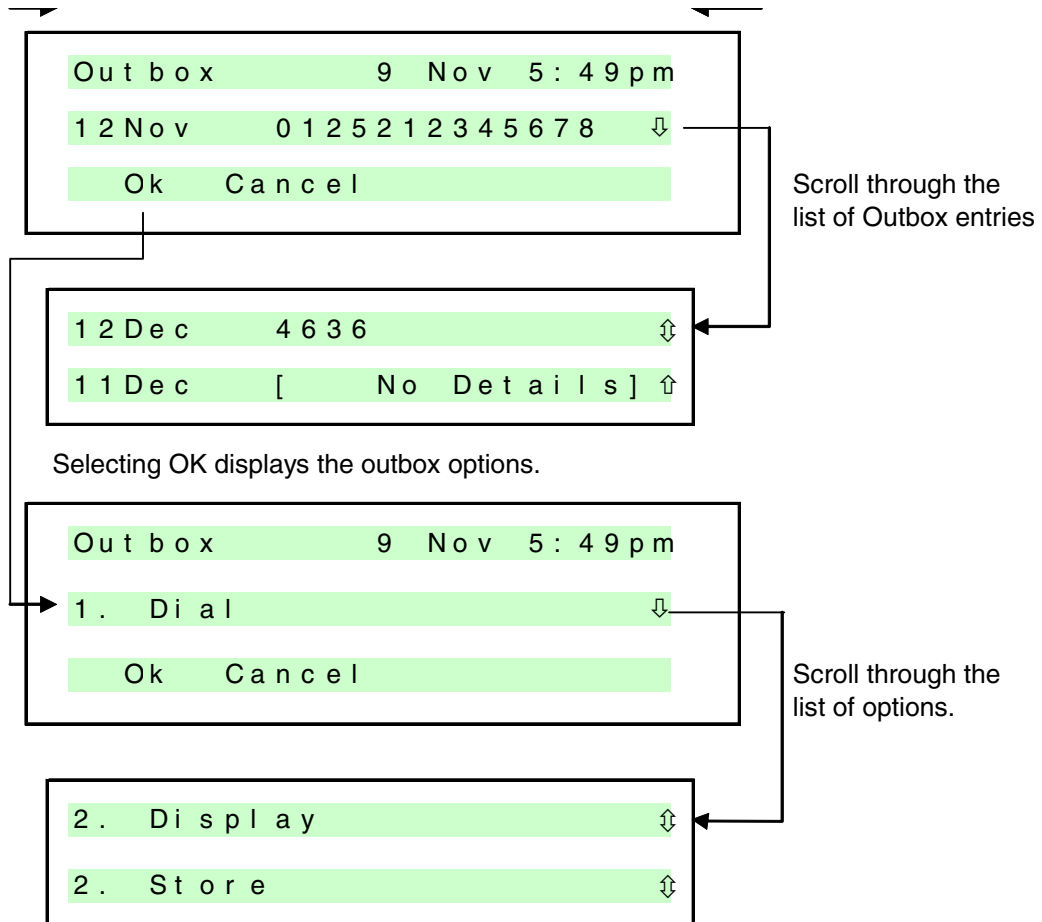
131.2.6.11 Generic Confirmation Screen



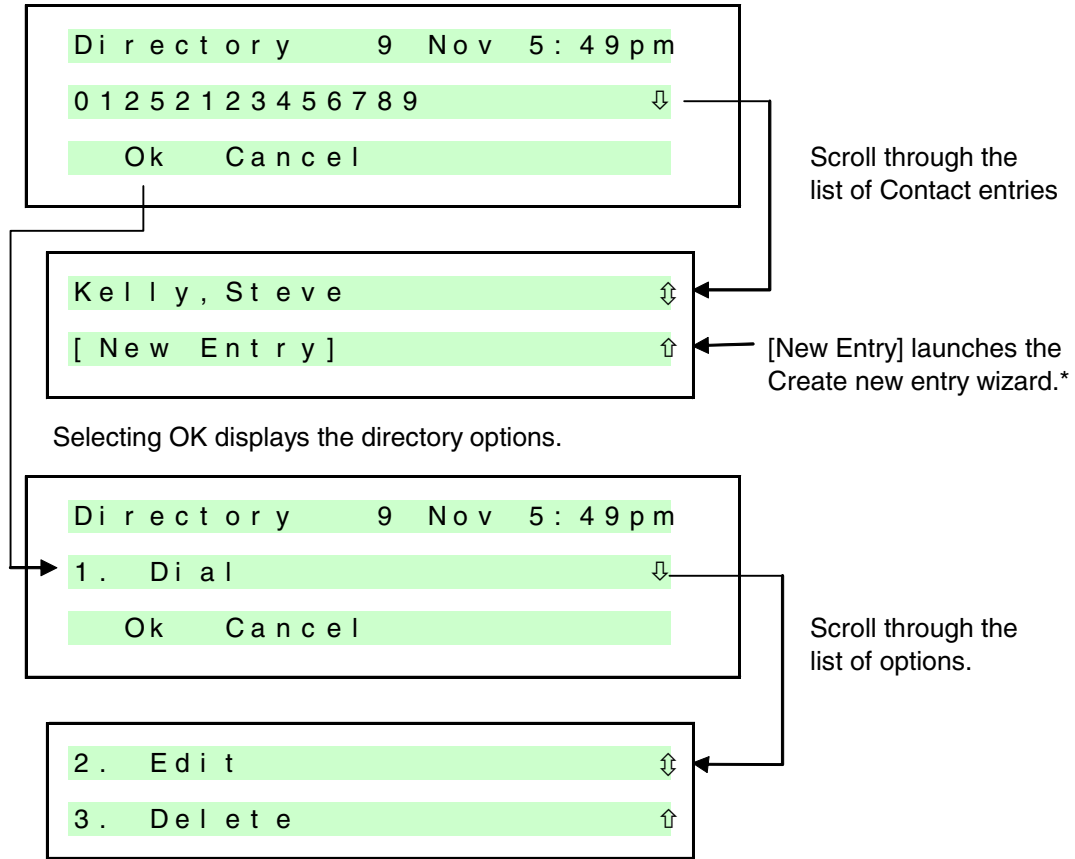
131.2.6.12 Inbox and submenu screens



131.2.6.13 Outbox and submenu screens

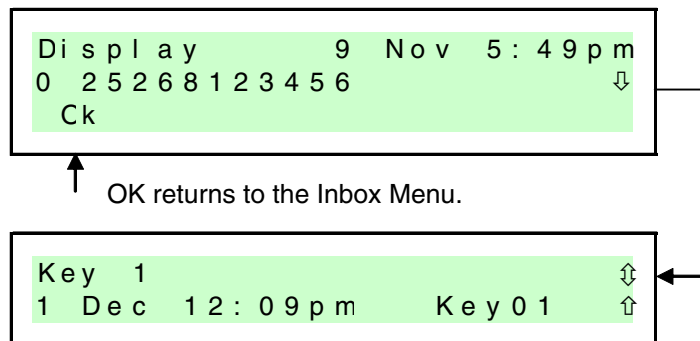


131.2.6.14 Directory display screens

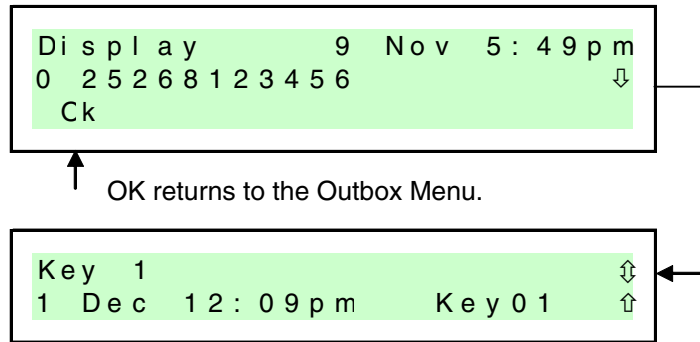


* The [New Entry] option may be ordered to feature at the top of the directory list, so upon entering the directory you will be presented with the first actual entry and press up to select [New Entry].

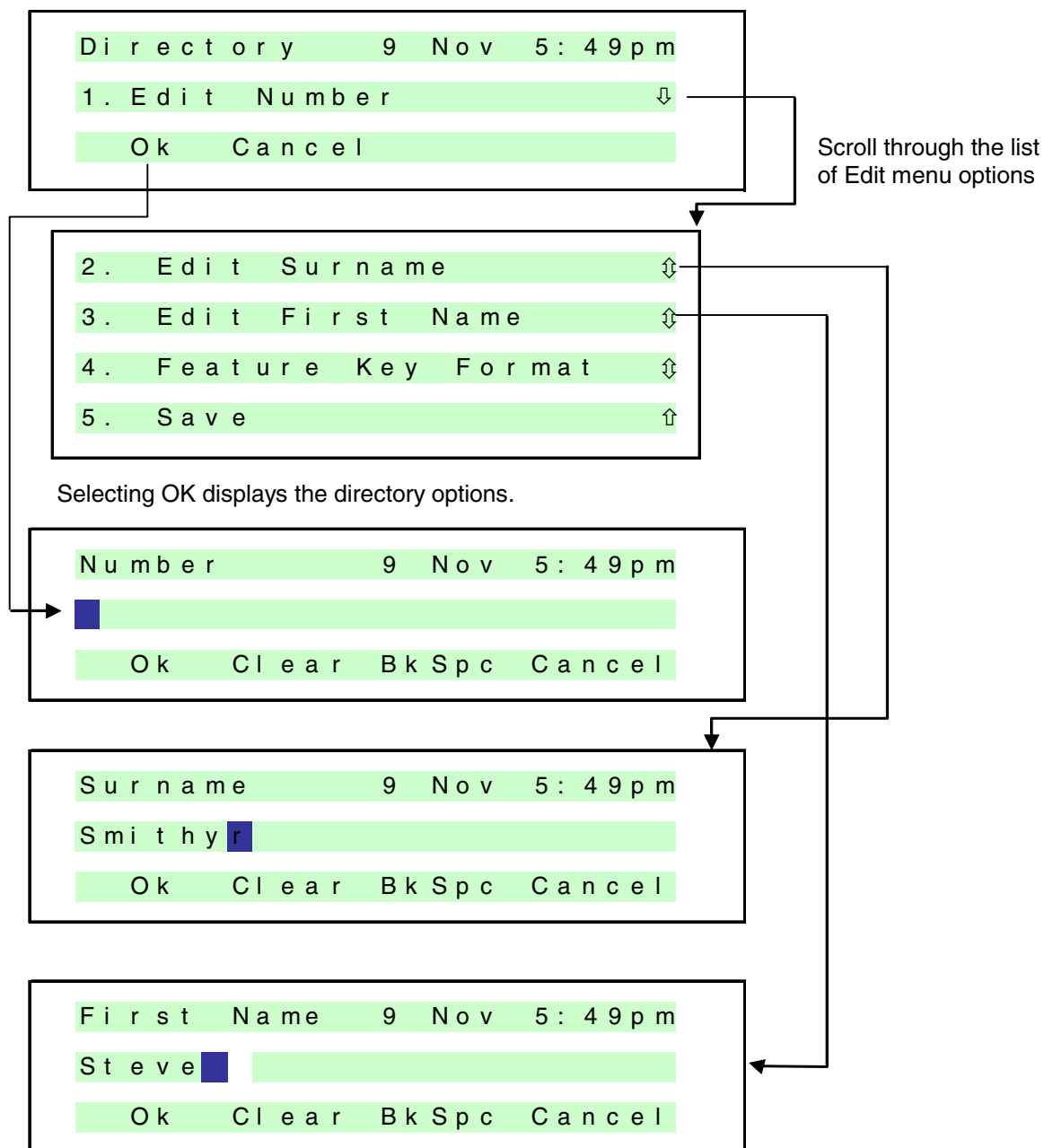
131.2.6.15 Inbox Display Screen



131.2.6.16 Outbox Display Screen

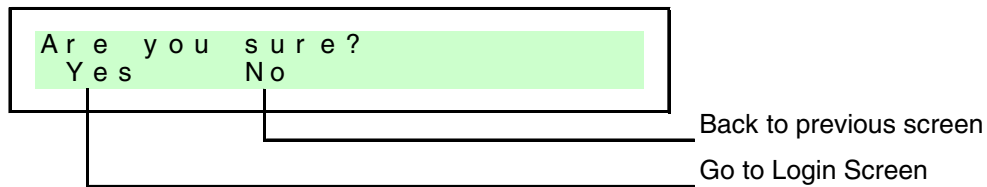


131.2.6.17 Directory Edit Screens



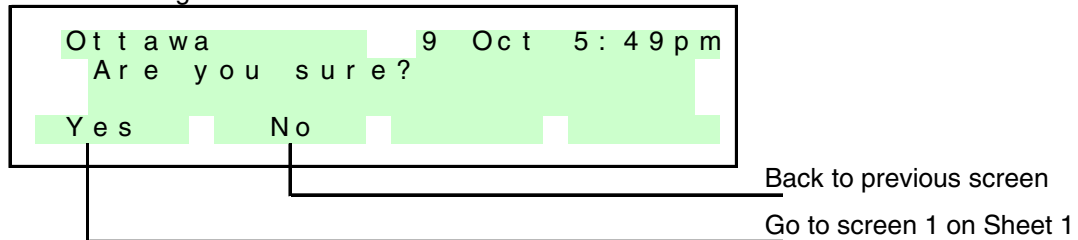
131.2.6.18 Time display screens

i2002

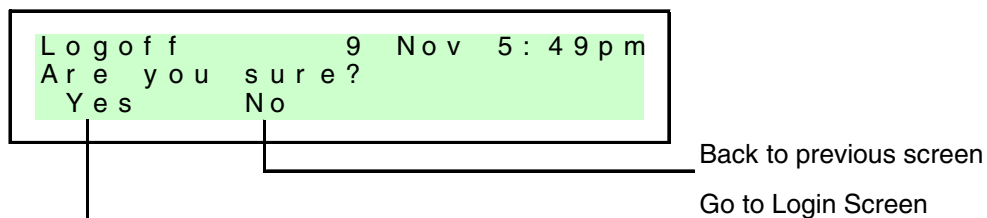
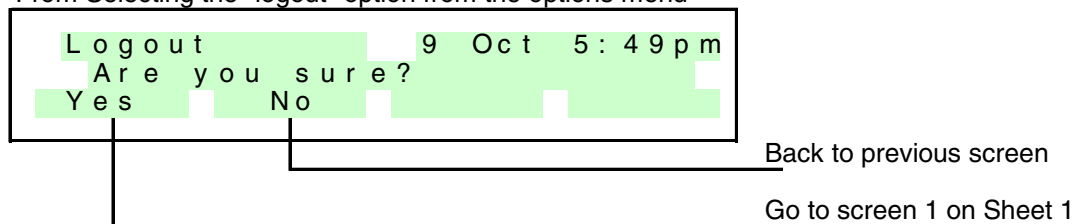


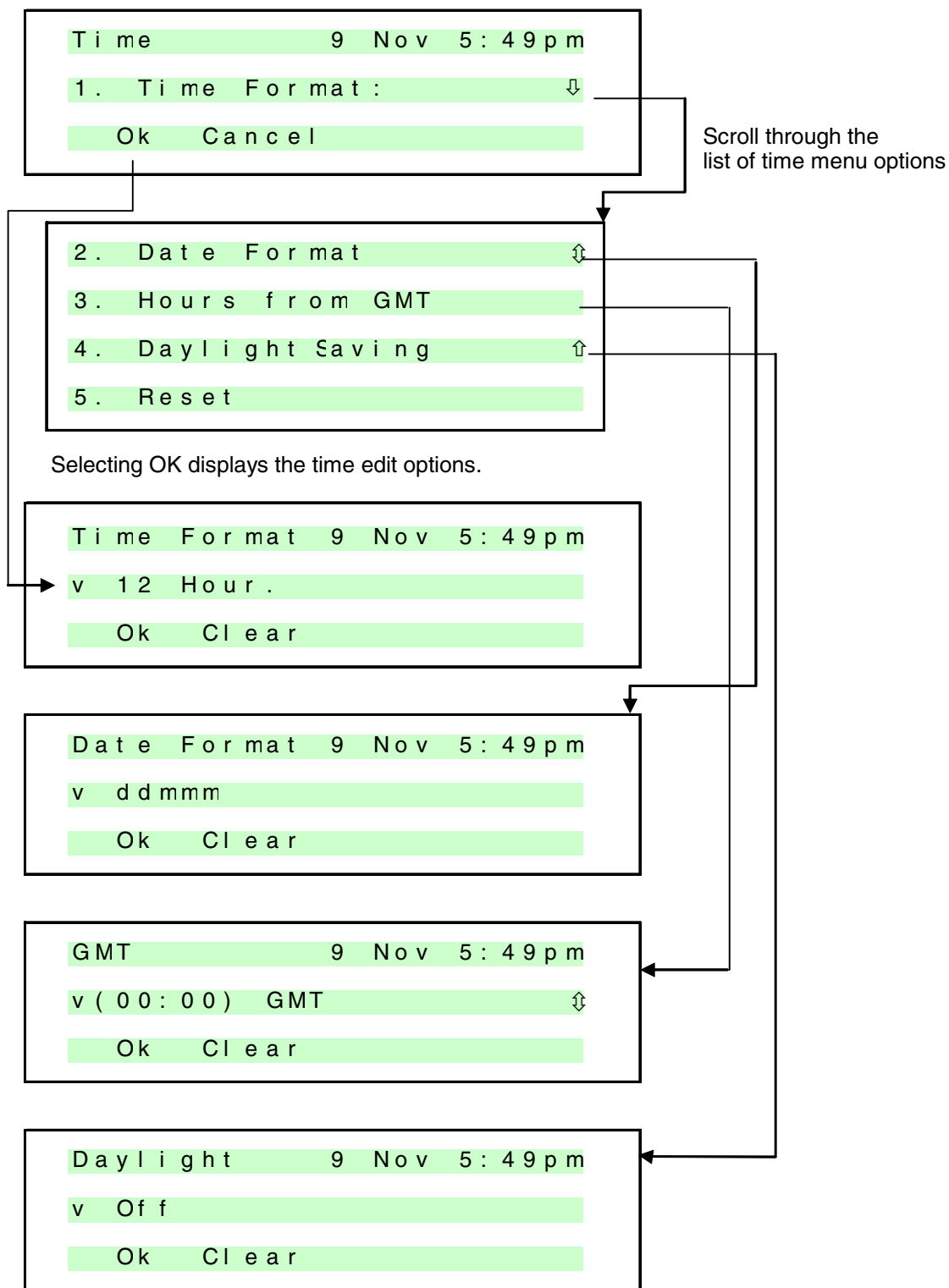
i2004

From selecting a new from the Server select menu



From Selecting the "logout" option from the options menu



131.2.6.19 Time display screens (continued)

131.2.6.20 Call History Screens

Call	9 Nov 5:49pm
1. Reset Inbox	↓
Ok	Cancel

2. Reset Outbox	↑

131.2.6.21 Missed Call Screen

Centrex	9 Nov 5:49pm
Missed Call(s)	
Menu	

131.2.6.22 Message waiting screen

Centrex	9 Nov 5:49pm
Message Waiting	
Menu	

131.2.7 Administration - Element Manager

The i2001, i2002 and i2004 ethersets have had a name change. New branding has eliminated the “i” at the beginning of the model number. All documentation and references to the IP Phones (Phase 2) should refer to “IP Phone 2001” “IP Phone 2002”, “IP Phone 2004”.

This feature will make changes to the internal referencing of terminals and to the naming of the terminals on the Element Manager, but to the system administrator the interface for accessing the 2033 will be the same as the existing interface for the 200x terminal.

Note, the name changes are not reflected in the following figures.

Figure 8 Configuration drop-down

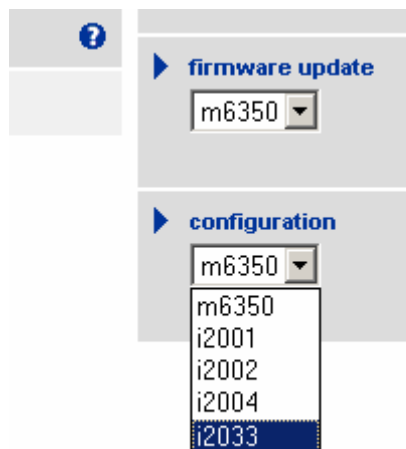
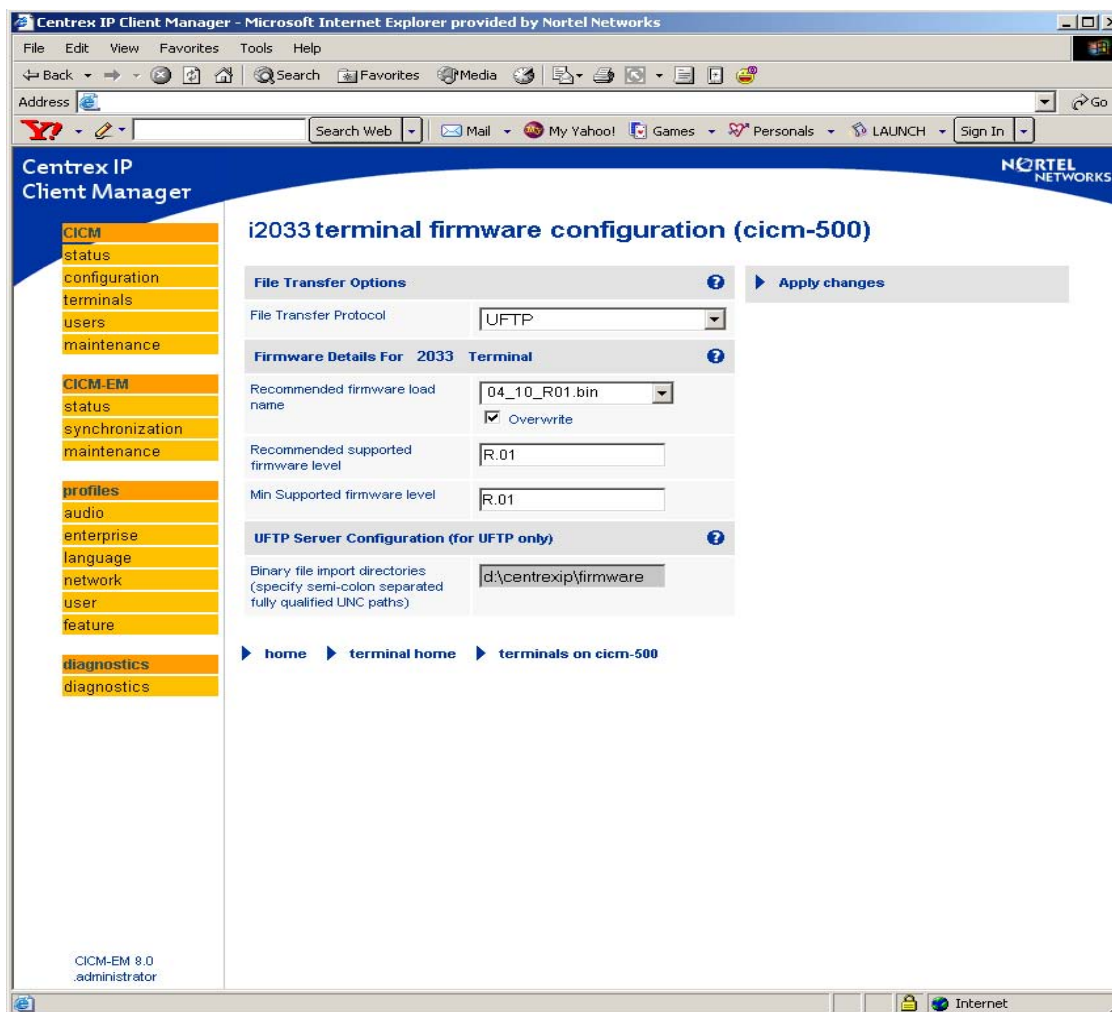


Figure 9 Screen capture of terminal firmware upgrade page



As seen in the preceding figure, the administration and configuration of the 2033 terminal will use the same pages which are already provided for the 200x terminals.

Figure 10 Screen capture of terminal configuration page

Centrex IP Client Manager - Microsoft Internet Explorer provided by Nortel Networks

File Edit View Favorites Tools Help

Address Search Web Mail My Yahoo! Games Personals LAUNCH Sign In

Centrex IP Client Manager **NORTEL NETWORKS**

i2033 terminal configuration (cicm-500) [no_sync]

Feature Key Attributes [?](#) [Apply changes](#)

Number of physical feature keys (on the main set)

Number of features available on the main set (pages of features are used if there are not enough physical feature keys)

Automatically hide features

Voice Parameters [?](#)

Default Audio Profile

Default Voice Codec

Secondary Voice Codec

RTP port number (must be an even number)

Default Volume Settings [?](#)

Prevent users modifying Default Volumes

Handset Transducer db (Decibels)

Handsfree Transducer db (Decibels)

[home](#) [terminal home](#) [terminals on cicm-500](#)

CICM-EM 8.0 .administrator

Done Internet

131.3 Hardware Requirements or Dependencies

2033 and SN08 CICM required.

131.4 Software Requirements or Dependencies

The 2033 will support standard TFTP or Nortel UFTP (UNISTim FTP) for firmware download. In case of UFTP, the call server must be able to recognize, store and upload 2033 firmware.

For the first release the 2033 emulates Nortel IP Phone 2001. It reports the same IT Type as IP Phone 2001 but with a unique release number (0x10) in order to avoid downloading the IP Phone 2001 firmware into 2033.

The firmware release at the time of this documents creation is 310S03, known restriction in this firmware include; no support for QoS, RFC2833 or BFI. KEM's is also irrelevant for this phone.

131.5 Limitations and restrictions

131.5.1 Joint Sessions

The 2033 will only be 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 i2033 will function in the same manner as the IP Phone 2004.

There will be no support for the 2033 to have a joint session with another i200x.

131.5.2 Unistim.

The 2033 will support the latest externally released UNISTim version (currently 2.6).

131.5.3 Networking

The 2033 provides a single 10/100 BaseT Ethernet port, and is able to force either 10 or 100BaseT operation through manual configuration in the boot menu. The phone does not currently support 802.3af Power-over-LAN.

The 2033 supports partial or full DHCP configuration.

The 2033 will default to port 5000 for signaling, but will be configurable by the TPS.

131.6 Interactions

131.6.1 Feature Interactions

The 2033, like the IP Phone 2001 has no feature keys. An alternative to drive features has been developed to provide the IP Phone 2001 and the 2033 with a limited set of features.

The "Services" key will provide access to a "Flash Hook", when pressed it will search through the list of features provisioned on the core for that specific DN. If 3WC (three way call) or CXR (call transfer) is provisioned on one of the first 14 keys then hitting the "Services" key action one of those features. The DMS-100 Family ABS MDC part 3 of 4 Translations Guide Volume 13 of 30 has

details of how 3WC and CXR can be used to drive access code features on sets that do not provide a flash hook.

To use any features through code access, the call must be active on a directory number (DN) or the Call Waiting (CWT) key/lamp. For the features that require flashes, the pressing of the Three-Way Calling/Call

Transfer (3WC/CXR) key generates the flash equivalent. An MBS must have a 3WC/CXR key for the use of many of the code accessed features. If only a CXR key is present, the end user cannot always flash. The type of call transfer and the type of line or trunks involved in the active call determines this action.

131.6.1.1 Unsupported Centrex features on the 2033:

Feature limitations of the 2033 can be defined as follows: any Centrex feature that cannot be assigned to key 1 (i.e. Primary DN key) of a line having a Line Class Code = M5216 cannot be supported on the 2033 set. In order to access a feature that cannot be provisioned on key 1, the 2033 set must be in a cooperative session with the m6350.

Features such as CCV, PRL, RAG (and others listed in section 2.6) that cannot be assigned to key 1 of an MBS line, either:

- do not have a corresponding access code or
- can be assigned to the set but on a key other than key 1. In this setup, the feature cannot always be activated/deactivated using the access code (as provisioned in table IBNXLA).

131.6.1.2 Use of the Services key on the 2033:

The “Services” key will default to activating the Menu when no 3WC or CXR features are provisioned. When 3WC or CXR is present, then the feature activation takes precedence.

131.6.1.3 Feature Interaction Issues on the 2033:

When 3WC or CXR features are assigned to one of the first 14 keys on the 2033 set in order to allow the Services key to act as a flash-hook and feature activation/deactivation codes (as provisioned in table IBNXLA) are dialed, there may be feature interaction issues between 3WC/CXR and the Centrex feature being accessed (as was observed for CPU).

131.6.2 Feature List

The following is a list of Centrex features to be tested with the 2033. Note this is not an exhaustive list. Attention must be given to the limitations and restrictions highlighted in section 2.5 when using these and other features with the 2033.

Feature Acronym	Feature Name	Access Code available	Stand Alone^a	Require Co-op with m6350	Comments
AUTODISP	Auto Display	No	Yes (if assigned to key 1)	No (if assigned to key 1)	Can assign to key 1 on 2033. If assigned to any other key (e.g. Secondary DN), 2033 must be in a cooperative session with m6350.
AUTODISP + CWT	Auto Display + Call Waiting	No	No (when both features in use)	Yes (when both features in use)	To utilize both these features, the 2033 must be in a cooperative session with the m6350 to access CWT key. Tested AUTODISP on key 1 and CWT on key 2 of 2033 set.
CCV	Call Covering	Yes	No	Yes	Requires 2033 in a cooperative session with m6350 to access CCV key (i.e. key other than key 1). CCV must be assigned to the secondary member of a MADN group. The primary MADN member must have EMW assigned. NTPs indicate CCV/EMW can also be activated/deactivated by using CRA (Call Request Activation) & CRR (Call Request Retrieval) access codes. With CCV assigned to key 2 (i.e. a key other than key 1), pressing the 3WC/CXR key or Services key and dialing the CRA access code, does not cause the EMW lamp to be turned on on the primary MADN. Suspect this will be a problem for any feature that cannot be assigned to key 1 of the 2033.
CCW	Cancel Call Waiting	Yes	Yes	No	CCW assigned to key 1 of 2033. Used IBNXLA access code 'CCW' to activate.
CFB	Call Forward Busy	Yes	Yes	No	CFB assigned to key 1 of 2033 Used IBNXLA access code 'CFBP' to activate and 'CFBC' to deactivate.
CFD	Call Forward Don't Answer	Yes	Yes	No	CFD assigned to key 1 of 2033. Used IBNXLA access code 'CFDP' to activate and 'CFDC' to deactivate.

CFDVT	Call Forward Don't Answer Variable Timing	No	Yes	No	'CFDVT 18 FIXRING' assigned to key 1 of 2033.

a. 'Stand alone' means the feature can be assigned to key 1 and a cooperative session is not required to activate the feature.

Feature Acronym	Feature Name	Access Code available	Stand Alone^a	Require Co-op with m6350	Comments
CFF	Call Forwarding Fixed	Yes	Yes	No	CFF assigned to key 1 of 2033. Used IBNXLA access code 'CFWP' to activate and 'CFWC' to deactivate.
CFI	Call Forwarding Intragroup	Yes	Yes	No	CFI assigned to key 1 of 2033. Used IBNXLA access code 'CFWP' to activate and 'CFWC' to deactivate.
CFRA	Call Forwarding Remote Access	Yes	Yes	No	CFRA assigned to key 1 of 2033. CFW, CFU, CFF, etc must also be assigned to the set on key 1. Used IBNXLA access code 'CFRA' to activate/deactivate.
CFU	Call Forward Universal	Yes	Yes	No	CFU assigned to key 1 of 2033. Used IBNXLA access code 'CFWP' to activate and 'CFWC' to deactivate.
CPU	Call Pickup	Yes	Yes (if 3WC/CXR also assigned to 2033)	No (if 3WC/CXR also assigned to 2033)	If CPU assigned to key 1 of 2033, must also assign 3WC/CXR to one of keys 2-14 to activate Services key. Used IBNXLA access code 'CPU' to activate. Basic Call Pickup scenarios work ok. Can put one call on-hold and pickup another by pressing Services key and dialing CPU access code, however, cannot switch between two calls. Instead, the first and second picked up calls are placed into conference. This appears to be a 3WC/CPU interaction issue (see NTP 297-8001-350 Vol.14 p.2-357 section 'Limitations and Restrictions').
CRA	Call Request Activation	Yes	Yes	No	CRA does not need to be assigned to a key. IBNXLA access code 'CRA' activates the feature. Tested in conjunction with MWT.

CWI	Call Waiting Intragroup	No	Yes	No	CWI assigned to key 1 on 2033. Used in conjunction with CWT.
CWT	Call Waiting	No	No	Yes	Requires 2033 in a cooperative session with m6350 to access CWT key (i.e. key other than key 1). May also need CWI assigned to key 1.
CXR	Call Transfer / Blind Transfer Recall	No	Yes	No	Can assign CXR to one of keys 2-14 on 2033 and use Services key to activate CXR. Can also use 2033 in cooperative session with m6350 to access CXR key.
DCBI	Directed Call Pickup Barge-In	Yes	Yes	No	DCBI assigned to key 1 of 2033. Used IBNXLA access code 'DCP' to activate.
DCBX	Directed Call Pickup Barge-In Exempt	Yes	Yes	No	DCBI assigned to key 1 of 2033 (Set A). DCBX on key 1 of 2033 (Set B). Used IBNXLA access code 'DCP' to activate DCBI.
DCPK	Directed Call Park	Yes	Yes (if 3WC/CXR also assigned to 2033)	No (if 3WC/CXR also assigned to 2033)	If DCPK is assigned to key 1, must also assign 3WC/CXR to one of keys 2-14 to activate Services key. 2033 can then press flash-hook (i.e. Services key) and dial the IBNXLA 'DPRKS' access code plus the DN of set at which the called party parks the call. If DCPK is assigned to a key other than key 1, 2033 must be in a cooperative session with m6350 to access DCPK key.

a. 'Stand alone' means the feature can be assigned to key 1 and a cooperative session is not required to activate the feature.

Feature Acronym	Feature Name	Access Code available	Stand Alone^a	Require Co-op with m6350	Comments
DCPU	Directed Call Pickup Non Barge-In	Yes	Yes	No	DCPU assigned to key 1 of 2033. Used IBNXLA access code 'DCP' to activate.
DISP	Display Called Number	No	Yes	No	DISP does not need to be assigned to a key (only needed when LCC=PSET).

DISP + HOLD	Display Called Number	No	Yes	No	Hold key functions properly on 2033.
DRCW	Distinctive Ringing/ Call Waiting	No	Yes	No	DRCW assigned to key 1 of 2033. Also need CWT on another key.
DRING	Distinctive Ringing Enhancements	No	Yes (if not used with GIC)	No (if not used with GIC)	DRING can be assigned to key 1 of 2033 but requires 2033 in a cooperative session with m6350 to access another key/feature (e.g. using DRING in combination with GIC where GIC is assigned to a key other than key 1).
EBO	Executive Busy Override	Yes	Yes (if 3WC/ CXR also assigned to 2033)	No (if 3WC/ CXR also assigned to 2033)	If EBO is assigned to key 1, must also assign 3WC/CXR to one of keys 2-14. Then the Services key can be used as a flash-hook and the IBNXLA 'EBO' access code dialed.
EBX	Executive Busy Override Exempt	No	Yes	No	IBNXLA access code exists for EBO - not required for EBX.
EMW	Executive Message Waiting	Yes	No	Yes	Cannot assign EMW to key 1. Requires 2033 in a cooperative session with m6350 to access EMW key (i.e. key other than key 1). If 2033 is not in cooperative session (and therefore cannot access EMW key), upon hearing ringing or busy tone on the 2033 set, instead of pressing the EMW key, the CRA code in IBNXLA can be dialed after pressing the 3WC/CXR key. This will turn on the EMW lamp on the called set. Similarly, if the EMW lamp is turned on on the 2033 set (can only tell this if in coop. session!), pressing the Services key and dialing the CRR code in IBNXLA, will dial the caller who activated the EMW lamp.
GIC	Group Intercom	No	No	Yes	Requires 2033 in a cooperative session with m6350 to access GIC key (i.e. key other than key 1).
LNR	Last Number Redial	Yes	Yes	No	LNR assigned to key 1 on 2033. Can press ## to activate LNR or dial IBNXLA 'LNR' access code.

LNRA	Last Number Redial Associated with Set	Yes	Yes (if not used with SDN)	No (if not used with SDN)	Can assign LNRA to key 1 on 2033 however requires 2033 in a cooperative session with m6350 to access a SDN. Note there is not a specific access code for LNRA in table IBNXL A. The access code for LNR can be used in this case.
LVM	Leave Message	No	No	Yes	Requires 2033 in a cooperative session with m6350 to access LVM key (i.e. key other than key 1).

a. 'Stand alone' means the feature can be assigned to key 1 and a cooperative session is not required to activate the feature.

Feature Acronym	Feature Name	Access Code available	Stand Alone^a	Require Co-op with m6350	Comments
MCH	Malicious Call Hold	Yes	Yes (if 3WC/CXR also assigned to 2033)	No (if 3WC/CXR also assigned to 2033)	If MCH is assigned to key 1, must also assign 3WC/CXR to one of keys 2-14 to activate Services key. This provides flash-hook so that IBNXL A 'MCH' access code can be dialed. If MCH is assigned to a key other than key 1, require 2033 in a cooperative session with m6350 to access MCH key.
MRF	MADN Ring Forward	No	Yes	No	Can assign MADN (SCA) and MRF to key 1 on 2033.
MSB	Make Set Busy	Yes	Yes	No	MSB assigned to key 1 of 2033. Used IBNXL A access code 'MSBA' to activate and 'MSBD' to deactivate.
MWIDC	Message Waiting Indication	No	No	Yes	Requires 2033 in a cooperative session with m6350 to access MWIDC key (i.e. key other than key 1).
MWQRY	Message Waiting Query	No	No	Yes	Requires 2033 in a cooperative session with m6350 to access MWQRY key (i.e. key other than key 1).

MWT	Message Waiting	Yes	Yes (if 3WC/CXR also assigned to 2033)	No (if 3WC/CXR also assigned to 2033)	MWT cannot be assigned to key 1, To access the MWT key (i.e. key other than key 1), the 2033 needs to be in a cooperative session with m6350. Alternatively, instead of pressing the MWT key, the CRA (Call Request Access) and CRR (Call Request Retrieval) access codes can be used. To leave a message, press the 3WC/CXR key or the Services key (if 3WC/CXR is assigned to one of keys 2-14) and the CRA code in IBNXLA. To retrieve a message, go off-hook and dial the CRR code in IBNXLA. Note: 'Message Waiting' appears on 2033 display when a message has been left.
NAME	Network Name Display	No	Yes	No	NAME assigned to key 1 on 2033.
PF	Power Features	Yes	Yes	No	PF assigned to key 1 on 2033. Used IBNXLA access code 'PF' to activate.
PRK	Call Park	Yes	Yes (if CXR also assigned to 2033)	No (if CXR also assigned to 2033)	If PRK is assigned to key 1, must also assign CXR to the set. If CXR is assigned to one of keys 2-14, then after pressing Services key (to activate flash-hook), the PRK access code (in IBNXLA) can be dialed to park the call. If CXR is assigned to a key other than 2-14, the 2033 must be in a cooperative session to access either the CXR or PRK key. If PRK is assigned to a key other than key 1, require 2033 in a cooperative session with m6350.

a. 'Stand alone' means the feature can be assigned to key 1 and a cooperative session is not required to activate the feature.

Feature Acronym	Feature Name	Access Code available	Stand Alone ^a	Require Co-op with m6350	Comments
PRL	Privacy Release	Yes	No	Yes	Requires 2033 in cooperative session with m6350 to access PRL key. While PRL cannot be assigned to key 1 (PDN key), it can be assigned to another key (e.g. key 2) and, without being in cooperative session, the 2033 can activate PRL by pressing the Services key (when 3WC is assigned to a key from 2-14) and then dialing the PRL access code (in IBNXLA). One issue noted with this setup was that an unexpected tone was heard when activating PRL for a second time. PRL activation did appear to work however. ^b
PRV	Privacy	Yes	No	Yes	Requires 2033 in cooperative session with m6350 to access PRV key. While PRV cannot be assigned to key 1 (PDN key), it can be assigned to another key (e.g. key 2) and, without being in a cooperative session, the 2033 can activate Privacy by pressing the Services key (when 3WC is assigned to a key from 2-14) and then dialing the PRV access code (in IBNXLA). Privacy did appear to be toggled by dialing the access code or by pressing the PRV key. ^c
QTD	Query Time and Date	No	No	Yes	Requires 2033 in a cooperative session with m6350 to access QTD key (i.e. key other than key 1).
RAG	Ring Again	Yes	No	Yes	Requires 2033 in a cooperative session with m6350 to access RAG key (i.e. key other than key 1). Cannot assign RAG to key 1 (DN key) therefore cannot activate RAG using flash-hook (obtained by adding 3WC to one of keys 2-14) via Services key and dialing RAG access code (in IBNXLA). No confirmation tone is received after dialing the access code. Cooperative session is currently the only supported configuration for the RAG feature.

a. 'Stand alone' means the feature can be assigned to key 1 and a cooperative session is not required to activate the feature.

- b. The unexpected tone is most likely a symptom of having PRL assigned to a key other than key 1 on the 2001 and trying to activate the feature using the IBNXLA access code. Attempting to use PRL with the 2001 outside a cooperative session is not recommended.
- c. Similar to the PRL feature, attempting to use PRV with the 2001 outside a cooperative session is not recommended.

1. Nortel Networks IP Audio Conference Phone 2033 Product Requirement Document, April 2004.
2. 2033 IP Conference Phone Product Specification Document (in preparation).

Feature Acronym	Feature Name	Access Code available	Stand Alone ^a	Require Co-op with m6350	Comments
REASDSP	Reason Display	No	Yes	No	REASDSP assigned to key 1 on 2033.
REASDSP + CFD	Reason Display + Call Forward Don't Answer	Yes	Yes	No	CFD assigned to key 1 of 2033. Used IBNXLA access code 'CFDP' to activate and 'CFDC' to deactivate.
SCL	Speed Calling Long	Yes	Yes (if assigned to key 1)	No (if assigned to key 1)	When SCL assigned to key 1 of 2033, can use IBNXLA access code 'SCPL' to program SCL. If SCL on a key other than 1, must use 2033 in a cooperative session with m6350.
SCS	Speed Calling Short	Yes	Yes (if assigned to key 1)	No (if assigned to key 1)	When SCS assigned to key 1 of 2033, can use IBNXLA access code 'SCPS' to program SCS. If SCS on a key other than key 1, must use 2033 in a cooperative session with m6350.
SCU	Speed Calling User	No	Yes	No	Do not need access code to activate SCU.
SUPPRESS	Suppress Line Identification	No	Yes	No	SUPPRESS assigned to key 1 on 2033.
TBO	Terminating Billing Option	No	Yes	No	TBO assigned to key 1 on 2033. AMA record displays correct Call Code (i.e. 800).
3WC	Three Way Conference	No	Yes	No	Can assign 3WC to one of keys 2-14 on 2033 and use Services key to activate 3WC. Can also use 2033 in cooperative session with m6350 to access 3WC key.

UCDLG	UCD Login	No	No	Yes	Requires 2033 in a cooperative session with m6350 to access UCDLG key.

a. 'Stand alone' means the feature can be assigned to key 1 and a cooperative session is not required to activate the feature.

2.1 Glossary

Term	Description

132: A00008338 Functional description (FN)

132.1 Feature name

QCA LOG/ALARM Consolidation

132.2 Description

This document covers the LOG/ALARM Consolidation for QoS Collector Application functionality supported in SN08 time frame.

It is the purpose of this activity is to remove the discrepancies in the existing Log report instances

It is intended that the logs generated by the QCA application running on the SESM fulfill certain requirements

Software: Each log name/number must have 1 consistent format

Software: Set and Clear logs must be unique to enable event correlation (For example if the Set and Clear use Location and Notification-ID tags the same Location and Notification-ID pair cannot be duplicated until after the log is cleared)

Software: all set logs with a severity need to have a clear logs with no severity. If the same log name/number is used for the clear must have the exact same format. (As per #1.). The clear log can have a different format it must be a different log name/number.

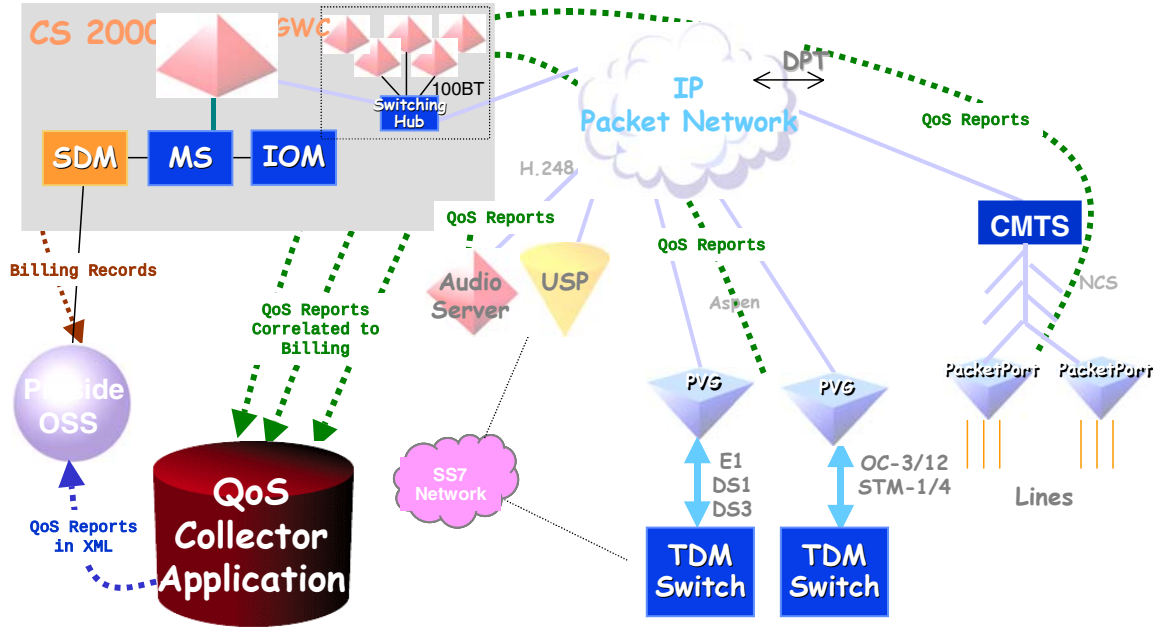
Software: The sequence number in log headers which is a tracking mechanism of lost logs must increment by 1. Downstream applications such as SDM Log Delivery Service and IEMS track this number and flag any lost log events (which is a bug/deficiency) to northbound OSSs.

Documentation: All QCA logs need to be documented in customers NTPs. Specifically, OSS Guide and Succession Log Reference Manual.

This is accomplished by ensuring

1. all instances of each log report number have the same consistent format.
2. Assigning new Log report number to achieve 1>
3. All Logs which have a severity of Critical/Major/Minor are required to have a corresponding Clear Log. All instances which had a severity but didn't have a detectable mechanism (from within QCA's scope) to generate a corresponding Clear Log have been changed to have a severity of None.

Figure 1 QoS Reporting in a VoIP Network



132.2.1 QCA customer logs

In addition to QCA Error IPDR Records the QCA raises alarms and events via the customer logging stream.

The QCA uses the logging API introduced by activity 89008996 “Log Reporting and Storage Mechanism for Managed Elements”.

Prior to this feature the QCA had 9 different Log report numbers (total instances = 62). After this feature it will have 11 different Log report numbers (total instances = 62)

All the QCA customer log instances have been listed in the table below.

The newly introduced logs and the modified log instances are in bold.

132.3 QCA Customer logs

Table 1 Service summary (initialization) warning logs

Event / Error	Report Number	Priority	Event Type	Message/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 Restore qca.properties file
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
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

Table 1 Service summary (initialization) warning logs

Event / Error	Report Number	Priority	Event Type	Message/Description	QCA Action	Customer Action
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	Message/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: <i>directory</i> as it is older than x days.	Directory removed	None

Table 1 Service summary (initialization) warning logs

Event / Error	Report Number	Priority	Event Type	Message/Description	QCA Action	Customer Action
File found in active directory when QCA started.	202	None	INIT	File Recovery: file <i>file name</i> 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.

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: <i>+reason</i> or QCA not started: Could not create File Handler: <i>+reason</i>	QCA not started	Rectify problem and re-start QCA.
Out of sequence QoS record received.	302	None	FLT	Out of Sequence QoS Record received. ' <i>MGC Type MGC number</i> ': sequence number = ' <i>record sequence number</i> ' previous sequence number = ' <i>last record sequence number</i> '	XML Error record generated.	None
Problem processing binary QoS record.	302	None	FLT	Problem processing binary QoS record: Sequence number = ' <i>record sequence number</i> ' Relevant MGC is mentioned in <i>Component ID</i> attribute of the log.	XML Error record generated. XML QoS Record not written to file.	None

Table 2 Trouble logs

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

Table 2 Trouble logs

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
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
The binary QoS Record header could not be processed.	305	None	FLT	Connection closed: Error while processing QoS record header: Client at, IP Address ' <i>client IP Address</i> '. Local Port ' <i>local port number</i> ' closed connection.	Connection to client closed	Investigate why client is sent QoS Record with faulty header Investigate why client is sent QoS Record with unsupported message type
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.

Table 2 Trouble logs

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
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.

Table 2 Trouble logs

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.

Table 2 Trouble logs

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
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.
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 <i>output</i> 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.

Table 2 Trouble logs

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
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	

I

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 ' <i>client IP Address</i> '. Local Port ' <i>local port number</i> ' 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

Table 3 Information and alarm clear logs

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
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
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."	QCA cannot be stopped	203
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.	QCA cannot be stopped	203

Table 3 Information and alarm clear logs

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: ComponentID: 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.	QCA cannot be stopped	203
QCA cannot be stopped	203	None	INIT	Location: <Hostname> Category: PROCESSINGERROR Cause: CONFIGERROR Time: ComponentID: 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.	QCA cannot be stopped	203
QCA cannot be stopped	203	None	INIT	Location: <Hostname> Category: PROCESSINGERROR Cause: CONFIGERROR Time: ComponentID: 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.	QCA cannot be stopped	203

Table 3 Information and alarm clear logs

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
Connection closed.	305	None	ERROR	Location: <Hostname> Category: COMMUNICATIONS Cause: COMMSUBFAIL Time: Specific Problem: MSGTYPEERROR Description: Client at, IP Address: closed connection.	Connection closed.	305
Connection closed.	305	None	INFO	Location: <Hostname> Category: COMMUNICATIONS Cause: COMMSUBFAIL Time: Specific Problem: CONNECTIONCLOSED Description: Client at, IP Address: closed connection.	Connection closed.	305
Connection closed.	305	None	ERROR	Location: <Hostname> Category: COMMUNICATIONS Cause: COMMSUBFAIL Time: Specific Problem: HEADERERROR. Description: Client at, IP Address: closed connection	Connection closed.	305
Connection closed.	305	None	INFO	Location: <Hostname> Category: COMMUNICATIONS Cause: COMMSUBFAIL Time: Specific Problem: CONNECTIONCLOSED. Description: Client at, IP Address: closed connection	Connection closed.	305
Connection closed.	305	None	INFO	Location: <Hostname> Category: COMMUNICATIONS Cause: COMMSUBFAIL Time: Specific Problem: nCONNECTIONCLOSED Description: Client at, IP Address: closed connection	Connection closed.	305

132.4 Glossary

Table 4

Term	Description
GW	Gateway
GWC	Gateway Controller
IP	Internet Protocol
QCA	QoS Collector Application
QoS	Quality of Service
SDM	SuperNode Data Manager
SESM	Succession Element and Subelement Manager
SLA	Service Level Agreement
SPM	Spectrum Peripheral Module
UTF	Universal Text Format
VoIP	Voice over IP
XML	eXtensible Markup Language

132.5 References.

1. A89007819 QoS Collector Application
2. Activity 89007781 - QoS Reporting: Provisioning
3. A00008338 DE
4. Activity 89008996 - Log Reporting and Storage Mechanism for Managed Elements

133: A00008350 Functional description (FN)

133.1 Feature name

Trunk group OM registers for establish bearer path failures

133.2 Description

This activity provides an enhancement to the per call failure handling in the CS2K Core by providing new OM registers. These registers will be pegged on a per-trunk group basis when the AUDT106 logs are generated. If throttling of logs is in effect resulting in suppression of AUDT106 logs, these OM registers will continue to be pegged to maintain an accurate count of the failures.

This activity addresses the following:

1. Creating new OM registers in the existing TRK/TRNK2, TRK2NET1/TRK2NET2 OM Groups
2. Pegging the new OM registers

OSS needs to be updated for these additional registers.

133.2.1 Creating new OM registers in the TRK/TRNK2 OM Groups

The AUDT106 log is generated when a call is forced down by the release of a trunk. Prior to this activity, customers relied on counting the number of AUDT106 logs in order to determine the impact to connecting offices (via trunks) of call failures.

This activity introduces a new register MIDFAIL at the end of the existing registers of the TRK OM group. This register will provide established bearer path failure counts on a per-trunk group basis.

OM Group Name	NEW, CHANGED or DELETED	Reason
TRK	Changed	A new register MIDFAIL is added

Another register MIDFAIL2 will be introduced in the TRNK2 OM group. This is the extension register of MIDFAIL.

OM Group Name	NEW, CHANGED or DELETED	Reason
TRNK2	Changed	A new register MIDFAIL2 is added

The snapshot after the addition is similar to that shown in Figure 1, "TRK OM Group".

Figure 1 TRK OM Group

TRK				
CLASS: ACTIVE				
START:2004/10/06 04:25:00 WED; STOP: 2004/10/06 04:25:33 WED;				
SLOWSAMPLES: 1 ; FASTSAMPLES: 3 ;				
KEY (COMMON_LANGUAGE_NAME)				
INFO (OM2TRKINFO)				
INCATOT	PRERTEAB	INFAIL	NATTMPT	
NOVFLATB	GLARE	OUTFAIL	DEFLDCA	
DREU	PREU	TRU	SBU	
MBU	OUTMTCHF	CONNECT	TANDEM	
AOF	ANF	TOTU	ANSWER	
INVAUTH	BLKCTRK	MAXBU	TRU2WIN	
NCTPASS	NCTFAIL	ACCCONG	NOANSWER	
NPQUERY	NPRESP	NPBDRTF	MIDFAIL	
51 DALI				
IC	0	0		
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
52 VTOA2WATC0				
2W	0	0		
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0

Figure 2 TRNK2 OM Group

```

TRNK2

CLASS: ACTIVE
START:2004/10/06 04:30:00 WED; STOP: 2004/10/06 04:34:07 WED;
SLOWSAMPLES:      3 ; FASTSAMPLES:      25 ;

      KEY (COMMON_LANGUAGE_NAME)
      INFO (OM2TRKINFO)
      INCATOT2    NATTMPT2    DEFLDCA2    TRU2
      SBU2       CONNECT2    TANDEM2     TOTU2
      ANSWER2    TRU2WIN2    MIDFAIL2

51 DALI
IC    0      0
      0      0      0      0
      0      0      0      0
      0      0      0      0

52 VTOA2WATC0
2W    0      0
      0      0      0      0
      0      0      0      0
      0      0      0      0

53 VER90
OG    0      0
      0      0      0      0
      0      0      0      0
      0      0      0      0

```

133.2.2 Creating new OM registers in the TRK2NET1/TRK2NET2 OM Groups

The OM groups TRK2NET1/TRK2NET2 were introduced as part of the Trimodal Logs and OM activity.

This activity introduces a new register MIDFAIL3 at the end of the existing registers of the TRK2NET1 OM group. This register will provide established bearer path failure counts on a per bearer network per-trunk group basis.

OM Group Name	NEW, CHANGED or DELETED	Reason
TRK2NET1	Changed	A new register MIDFAIL3 is added

Another register MIDFAIL4 will be introduced in the TRK2NET2 OM group.
This is the extension register of MIDFAIL3.

OM Group Name	NEW, CHANGED or DELETED	Reason
TRK2NET2	Changed	A new register MIDFAIL4 is added

Note: The OMSHOW command would display the OM groups and its fields. However the tuples of the TRK2NET1 OM group or any Trimodal OM groups are not displayed unless the MULTINET_DISPLAY_ACTIVE parameter in the table OFCVAR is set to 'Y'.

The snapshot after the addition is similar to that shown in Figure 3, "TRK2NET1 OM Group".


```
INFO (TRK2NET1_INFO)
INCAATT  PRERTEA1      NINFALL      NATMPT
NVFLATB  GLARE1       OUTFL      TRFCU
SBSYU    MBSYU        TRKNWBLK    CNCTAT
TNDMATT  ANIOFCFL     NANF      TOTBSYU
NANSWER  INVATHCD     MAXBSY    NACCCNG
NOANSWR  MIDFAIL3
```

1	TTT	NET	1	A1_P	100	OG	0	0
0				0		0		0
0				0		0		0
0				0		0		0
0				0		0		0
0				0		0		0
0				0				

Figure 4 TRK2NET2 OM Group

```

TRK2NET2

CLASS: ACTIVE
START:2004/10/06 04:35:00 WED; STOP: 2004/10/06 04:39:48 WED;
SLOWSAMPLES:          3 ; FASTSAMPLES:          29 ;

INFO (TRK2NET1_INFO)
INCAATT2      NATMPT2      TRFCU2      SBSYU2
CNCTAT2      TNDMAT2      TOTBSYU2    NANSWER2
MIDFAIL4

0
      TTT NET 0 ENET  100 OG      3      1
      0          0          0          0
      0          0          0          0
0

1
      TTT NET 1 A1_P  100 OG      0      0
      0          0          0          0
      0          0          0          0
0

2
      TTT NET 2 A1_S  100 OG      0      0
      0          0          0          0
      0          0          0          0
0

```

Note: The office parameter OFFICETYPE in table OFCSTD controls the generation of the registers for these OM Groups. These new registers will be included in all supported office types as defined for each of the OM groups.

133.2.3 Pegging the new OM register

The OM registers MIDFAIL and MIDFAIL3 will be pegged from the same location where the AUDT106 logs are generated irrespective of whether the throttle occurs or not.

133.3 Hardware Requirements or Dependencies

None

133.4 Software Requirements or Dependencies

None

133.5 Limitations and restrictions

None

133.6 Glossary

Term	Description
OM	Operational Measurements
CS2K	Call Server 2000

133.7 References

- A00003487 - Trimodal Provisioning, Logs and OMs.
- A00006777 - GWC Core LOGs for call failures.
- NTP 297-8021-814; North American DMS-100; Operational Measurements Reference Manual
- NN 10264-709; Succession Performance Management Operational Measurements Reference

134: A00008387 Functional description (FN)

134.1 Title

MG9KEM - GLC-32 AB Card Support

134.2 Description

This feature enhances the MG9KEM to provide the following capabilities:

- GLC-32 AB card (PEC NY53AB) support
Prior to this feature, MG9KEM and MG9K gateways only support the GLC-32 AA card (PEC NY53AA). With the combination of this feature and the matching SN08 gateway feature, both GLC cards, NY53AA and NY53AB are supported in SN08.
- Allowing bulk provisioning GLC card's line service types
This feature provides the capability for the user to bulk provision all the line circuits on a GLC card to the same service type. This option is only enabled when the card is deprovisioned.
- Card replacement support for GLC and WLC cards
With the combination of this feature and the matching SN08 gateway feature, card replacement between GLC AA and GLC AB cards and WLC and GLC cards can be performed without deprovisioning the card.

134.3 Hardware Requirements or Dependencies

This feature provides support for the NY53AB board with V2.1 or higher Infineon chipset.

134.4 Software Requirements or Dependencies

The capabilities provided by this feature require the SN08 gateway load.

134.5 Limitations and restrictions

1. SN08 gateway is required to support the NY53AB GLC card.
2. Once the NY53AB GLC card(s) are installed on a SN08 gateway, any gateway downgrade to pre-SN08 loads will render the NY53AB GLC card non-functional. The NY53AB GLC cards should be deprovisioned and removed prior to the downgrade attempt.
3. Since WLC card only supports the "potsLoopStart" line service type, when replacing a GLC card with a WLC, any EBS/pPhone or potsGroundStart lines on the GLC card MUST be decommissioned prior to the card replacement attempt; failed to do so will result in lost of service to these

lines. Once the GLC card is replaced with a WLC, all line circuits on the card will assume the line service type of “potsLoopStart”.

4. The WLC and GLC card replacement is only supported with the SN08 gateway.

134.1 Interactions

134.2 Glossary

Term	Description
GLC	Global Line Card
WLC	World Line Card

135: A00008431 Functional description (FN)

135.1 Title

System Mastership Support for CS 2000 - Compact Geographic Survivability Configuration

135.2 Description

This activity supports the Geographic Survivability configuration of the CS 2000 - Compact by modifying the mastership selection algorithm to obtain better performance during disaster scenarios.

The Geographic Survivability configuration splits the control components between 2 physically separate sites, using a highly available Optical transport system to connect the 2 sites.

In steady state, each of the components maintains communication with its mate in the other site, and they decide and negotiate activity between the two components using their existing mastership algorithm. This is the default behaviour when communications are up between the two sites, and maintains the current non-Geographic Survivability behavior when inter-building communications is present.

The enhanced mastership algorithm is used primarily in disaster scenarios, that is, when the communications between the buildings is lost, or either an entire site, or portions of it are down. The mastership algorithm detects what portions of the system are still active and reconfigures the system in an optimal mode to maintain services with the remaining inservice components.

The Geographic Survivability mastership algorithm spans the following components:

- CCA - Compact Call Agent - the master node in the algorithm
- GC - Gateway Controller
- USPc - Universal Signalling Point-Compact

Other components, while redundant, are not configured with components on both sites. These are:

- CMT & IEMS: both HA units configured on site A. Standby unit prepared on site B.
- CBM: both HA units configured on site B. Standby unit prepared on site A.
- Session Server and Policy Server: both units configured on single site

The SAM21 Manager GUI has a Geographic Survivability tab to allow configuration of the backup WAN path between the CS 2000 - Compact cards. Configuration of Call Agent interactions with the local ERS 8600 in each site is configured on each Call Agent blade using the setgeoconfig script tool.

The recommended CS-LAN router is the ERS 8600, dual processor version in each site. The CA is able to interact with the ERS 8600 in ring down scenarios, disabling OSPF on the inactive site, and thereby improving the call completion rate.

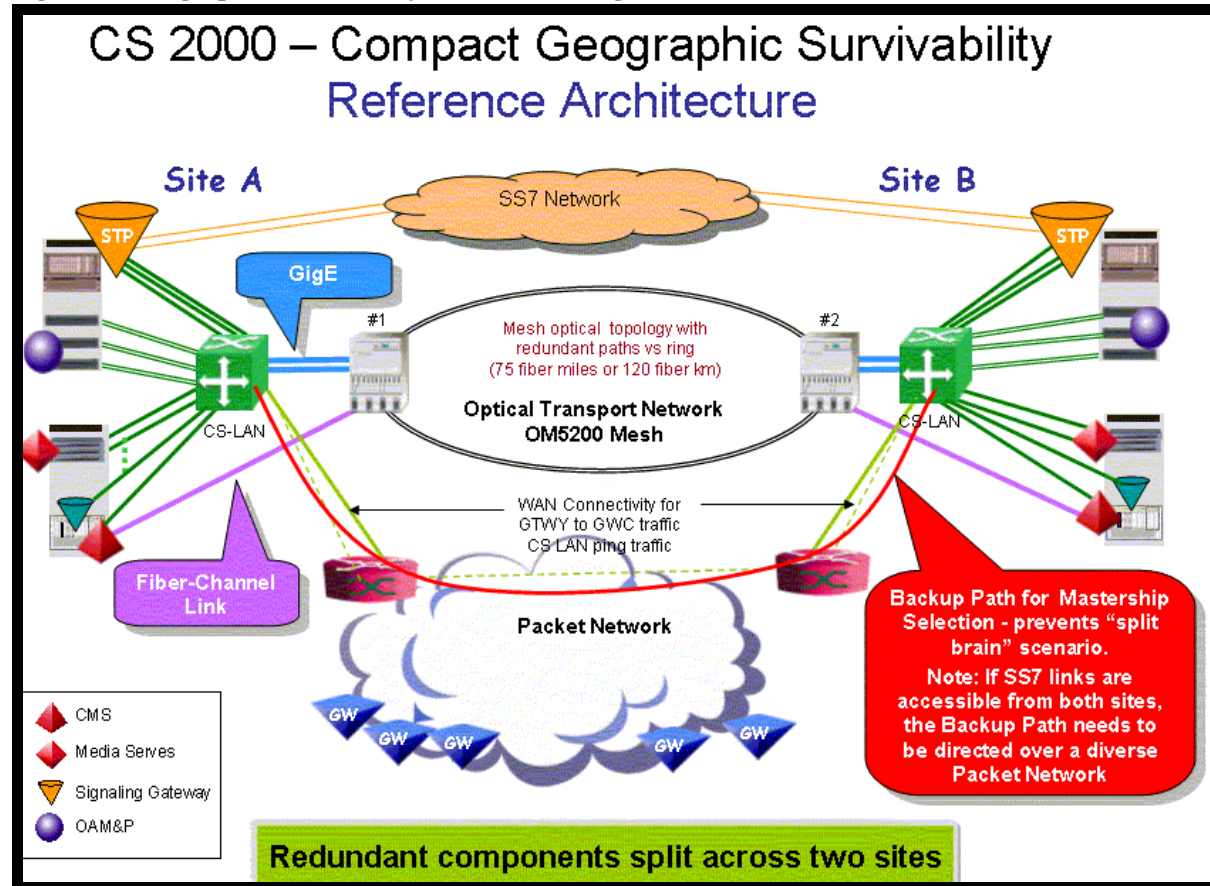
Other routers may be used, but the CA can only interact with the ERS 8600 to disable OSPF at this time.

135.2.1 Reference Configuration

The Geographic Survivability reference configuration consists of the principal core components split into 2 separate physical sites, which are connected via optical equipment. Although line gateways, trunk gateways and RTP Media Portals may be present at either of both of the CS 2000 - Compact Call Agent sites, they are not survivable in the event of a site disaster.

An example configuration is shown here for help in reviewing this document.

Figure 1 Geographic Survivability Reference Configuration



135.2.1.1 Key components of the Geographic Survivability configuration

- Main callp and oam control components split between two geographically separate sites (i.e. CA, GWCs, USPc, CICM).
- Highly survivable Optical connections (Ring or Mesh) between the two main control sites.
- Ethernet connectivity extended over the optical ring between the Ethernet Routing Switch 8600s in each site. CALLP and OAM subnets exist transparently between the two sites.
- Fiber Channel (FC) connectivity extended over Optical for the inter-Call Agent FC connection.
- IP WAN Gateway connections from each site. Configured separately from the optical ring.
- SS7 connectivity from each site to the SS7 network. Normally operates in load sharing mode.

- Backup path configured via WAN, separately from optical network for maximum redundancy.
- CMT/IEMS and CBM are configured in HA mode, with both units on the same site. For maximum OAM redundancy, the CMT/IEMSs and CBMs are configured on opposite sites. In case of a disaster scenario where one of the sites is unavailable for an extended period of time (days or more), additional hardware is pre-installed in each site which is recovered to a temporary CBM or CMT/IEMS via a manual recovery procedure.

It is important to note that not all components in the network are Geographically Survivable. The main core components are Geographically Survivable, but typically the access GWs are single units, and exist externally to both sites, close to the access point.

The core components in the Geographic Survivability configuration, categorized by type appear in the following table:

Table 1 Categorized core components

Type	Component	Geo Survivable	Comment
HA Pair (Act/Inact)	CCA	Yes	Master node in Geographic Survivability algorithm. Data sync across FC/Optical ring.
	GWC	Yes	Data sync across ring
	CICM	Yes	
	CBM	Recoverable on standby server	HA configured in site B. (Standby server configured in Site A)
	CMT/IEMS	Recoverable on standby server	HA configured in site A. (Standby server configured in Site B)
	SC	N/A	2 units control a specific shelf. Call Control shelves are geo-survivable as there is at least 1 shelf per site.
	Session Server	No	Not Geo Survivable in SN08. Configure both units in single site.
	Policy Server	No	Not Geo Survivable in SN08. Configure both units in single site.
Load Shared	USPc	Yes	Load shared. 1 unit in each site. Geo Survivable with single unit.
	MC	No	Load shared units in single site only. CS 2100 Hybrid solution only.
	MS2010	Yes	N units at each site, where N meets engineered requirements.
	Storm-IA	No	2 separate units, 1 per site.

135.2.2 Behaviour Overview during Failure scenarios

The goal of the Geographic Survivability algorithm is to detect and react to failure scenarios, to keep the maximum amount of equipment in service, during single or multiple fault scenarios.

To concentrate the majority of the decision making in a single place during failure scenarios, a master was chosen among the components (the CA). The master monitors multiple network connections, and has an additional backup link to its mate that are not available to the other components during optical ring failure.

Overall, the Geographic Survivability mastership algorithm works as follows:

- Algorithm spans both master (CA) and other components.
- Normal operations for master and other components: mates in contact with each other and negotiate activity and services between them.
 - This means that activity for the different components will generally be spread across both sites in normal operation.
- The master monitors several connections with its mate, and several connections with other components in order to determine the state of the overall system.
 - Mate to mate connections monitored are:
 - normal ethernet via ERS 8600 and optical,
 - backup FC link via optical (but not ERS 8600), and
 - backup WAN link via ERS 8600 and WAN, but not optical.
 - Master to network connections monitored are:
 - Master to local ethernet (ping local SC)
 - Master to local WAN edge
- Master uses WAN backup path separate from Optical link to negotiate activity if optical goes down. Only the master has access to this backup link.
- If no master mate connectivity present, master uses connection to WAN edge to determine whether to go/stay active or inactive. Assumes one or other of the locations is isolated.

This includes an assumption that the GWs (apart from those co-located in the bldg) are accessible via the WAN connection.
- When non-master mates lose connectivity with each other, they verify if they have connectivity to active master (CA). They follow the master activity during isolation.

- During isolation, one building will become active, the other inactive based on the master activity.
- The master to non-master communications rely on the non-master detecting loss of connectivity with the master node.

Summary of system behaviour during various failure scenarios.

Note: these scenarios do not include the OAMP configuration. The OAM&P configuration is described in more detail in section “135.2.6 OAM&P configuration” on page 1108.

Table 2 System Behaviour Summary

Scenario	Expected Behaviour
ERS 8600 failure in Bldg A.	All components lose mate connectivity via ethernet. CA also loses WAN backup connectivity. FC backup should remain up. Bldg B CA will remain active if already active. No outage. If Bldg B CA was not active, it will take activity within about 2 sec. SOS goes through WARM or COLD restart (about 30 secs). Bldg A CA will detect IST loss, but will not be able to disable OSPF since ERS 8600 down. Other components are expected to go active in Bldg B, following CA activity after losing mate connectivity. USPc in Bldg A detects isolation and takes down side A SS7 links.
Optical Frame failure in Bldg A	All components lose mate connectivity via ethernet. CA also loses FC backup connectivity. WAN backup should remain up. Active CA will remain active, but without sync. No outage. (Assume active is in Bldg A for remaining discussion). Bldg B CA will detect IST loss, and disable OSPF in bldg B. Other components are expected to go active in Bldg A, and inactive in Bldg B, follow CA activity after losing mate connectivity. USPc in Bldg B detects isolation from Active CA, and takes down Bldg B SS7 links.
Bldg A lost	All components in Bldg B lose mate connectivity. CA loses all mate connectivity including backups. CA loses sync. Bldg B CA will remain active if already active. No outage. If Bldg B CA was not active, it will take activity within about 2 sec. SOS goes through WARM or COLD restart (about 30 secs). Bldg A gone. Nothing happens there. SS7 network takes down links to site A. Other components are expected to go active in Bldg B, following CA activity after losing mate connectivity.

Table 2 System Behaviour Summary

Scenario	Expected Behaviour
CA card fails Bldg A (when active)	All components in both sites can still see their mates. No change required. CA in Bldg B (inact) detects loss of connectivity with mate. Detects local and WAN connectivity. Takes activity, performing SOS restart. Other components will experience disconnection with SOS for about 30 secs. (Normal restart behavior)
CA card fails Bldg A (when inactive)	All components in both sites can still see their mates. No change required. CA in Bldg B (act) detects loss of connectivity with mate. Detects local and WAN connectivity. Stays active. No switch of activity required. No restart required.
Recovery from Isolation Split Brain (Act/Act) scenario	During Recovery: Once CAs can talk to mate, they recognize that both are active. The one which was inactive previously backs down, leaving the other active. The fallout is to force unit 0 active, unit 1 inactive. Other components talk to their mates, negotiate activity and resume normal operations.

135.2.2.1 System impact of failure scenarios

Reacting to certain failure scenarios may cause a system impact. These are described below:

- When negotiating activity, the CA preference is always to remain on the same side, if this side supports activity.
- If failover of the CA is necessary, the CA switches activity in less than 2 secs, however there is a call processing interruption of approximately 30 seconds while the Callp Application performs a restart.
- If failover of other Callp nodes is necessary, they follow the CA within 2 secs.

135.2.2.2 Hybrid Configuration

In the CA Hybrid configuration, supported only in the Enterprise CS 2100 product, where the solution contains MC cards connected to Message Switches, supporting TDM peripherals, the MC cards and Message Switches are co-located in one of the principal Geographic Survivability sites. The behavior described above is modified in the following ways:

- During building isolation, when determining the appropriate master site, preference is given to the site containing the MC cards (assuming it is able to take activity). If necessary, activity is switched to this side during the activity negotiation.

135.2.3 Recovery Behaviour

A very important part of the algorithm is the recovery aspects. In general, the recovery portion of the algorithm works as follows:

- All components, regardless of their activity state, continually monitor connections with their mate, and with other network components that they normally communicate with. When connectivity is not present, they continue to monitor the connections, waiting for connectivity to return.
- All components negotiate activity and services when connectivity recovers, and resume normal operations.

135.2.3.1 System impact of recovery scenarios

In general, recovery scenarios have less system impact than failure scenarios. However, reacting to certain recovery scenarios may cause a system impact. These are described below:

- When negotiating activity, the CA preference is always to leave activity on the same side. When recovering to a full system configuration, activity remains on the same unit, without impact.
- If recovering from a split system where confusion was introduced into the system due to incorrect message routing, while the activity of the nodes will be resolved within a few seconds, it may take up to 15 mins before all call processing has completely recovered.

135.2.4 Geographic Survivability Mode Configuration

In SN08, it is necessary to configure Geographic Survivability mode as part of installation and commissioning of the new Geographic Survivability office.

- Configure the Backup path vlans and filtering on the CS-LAN.
- Configure the CCA access account, permissions etc on the ERS 8600.
- When configuring the CA cards in the EM GUI, fill in the Geographic Survivability portion of the panel, and include the IP addresses for the GEO WAN backup link.
- Use the setgeoconfig script tool to configure the interactions with the local ERS 8600, on each CA interface.

135.2.5 WAN backup path

An important component of the reliability of the Geographic Survivability algorithm is the WAN backup path configured to go via the WAN. This link has several important attributes:

- It is only used by the CA for mate to mate communication; not by any other network component.
- It is configured separately from the optical network, thus it provides an additional path which can stay up if the optical network completely fails.
- It routes packets via the external IP network, rather than over the Optical network.
- It is monitored continually, and alarmed if it goes down.

135.2.5.1 Backup Link Security

It is noted that:

- Information is exchanged over the IP network between the 2 CA units.
- The Call Agent IP addresses are visible on the external network.
- The messages are unencrypted and unauthenticated.
- Status/control information is exchanged over this link in certain conditions, which is used to determine CA activity.

The security risks are mitigated by the following:

- In normal operation, when the Optical ring is insv, only ping messages are exchanged over the IP network (no control information). This is used simply to monitor the state of the link.
- Status/Control messages are discarded if they arrive on the backup link, while the other links are still up. Only if the other links are down, are status/control messages from the mate used to decide on activity.
- ERS 8600 filters enabled to only allow packets to be received from the mate IP address, and on the single port used for mate communication.
- Msg Rate filtering is configured on the ERS 8600 to minimize the impact of a denial of service (DOS) attack on the CA IP addresses.

135.2.6 OAM&P configuration

The OAM components CMT, IEMS, CBM are in HA mode on one site with a standby server at the other site.

135.2.6.1 CBM accesibility

The CBM will be inaccessible during certain failure scenarios:

- Ethernet IST down (ring down) between sites, with site B core inactive (due to OSPF disable) when using ERS 8600 routers.
- Loss of site B

For various failure scenarios, the following table indicates the impacts to CBM applications for the duration of the condition (if the optical ring is down) or until restoration of the CBM applications on the standby server (if site B is lost).

Table 3 CBM functionality during fault conditions

CBM Application/Function	Description	CMT/IEMS Site A lost	CBM Site B lost	Ring down, Core on Site A	Ring down, Core on Site B
Fresh Install	Ultimate recovery mechanism, or to prep standby unit on site A. Needs to have both Core and CMT INSV/ Accessible to complete installation and commissioning.	NA	OK	OK	Cannot talk to Core to complete commissioning
Bootp server	Tells booting nodes where to tftp to obtain boot loads. Note: CMT is redundant bootp server.	OK	OK	OK	OK
Tftp server for boot loads	Supplies load to booting node, when unavailable from the element's flash memory.	CICM cannot boot	All CA, sc, gwc and audio servers cannot boot	Site B CICM cannot boot. Site A CA, sc, gwc and audio servers cannot boot	Site B CICM cannot boot. Site A CA, sc, gwc and audio servers cannot boot
Secure Terminal Access / Passthrough	Terminal access to the CBM server and passthrough capabilities through the CBM to the Core with standard SSH/ telnet clients	OK	Unavailable	Unavailable	OK
File Transfer Service	FTP Daemon for Core Access	OK	Unavailable	Unavailable	OK
FTP Proxy	Ability to FTP directly to Core from Client Machine	OK	Unavailable	Unavailable	OK
SSH Core Transfer	SSH File Transfer directly to Core from Client Machine	OK	Unavailable	Unavailable	OK

Table 3 CBM functionality during fault conditions

CBM Application/ Function	Description	CMT/IEMS Site A lost	CBM Site B lost	Ring down, Core on Site A	Ring down, Core on Site B
OM Access Service	Obtains OM from Core	OK	Unavailable	Unavailable	OK
Table Access Service	Provides Data Dictionary files to other CBM applications (OM, SBA etc.)	OK	Unavailable	Unavailable	OK
Generic Data Delivery	Obtains real time logs from Core	OK	Unavailable	Unavailable	OK
Log Delivery Service	Feeds real time Core and CBM logs to NOC for status and action.	OK	Unavailable	Unavailable	OK
SDM Billing Application	Reliable store and forward of Core billing records using FTP, supports real-time-delivery and stores data in DNS or DIRP files.	OK	Unavailable, new billing records backed up to Core for short term, unprocessed records on CBM lost.	Unavailable, billing records backed up to Core for short term	OK
Passport Log streamer	Consolidate ERS 8600 logs from the MDM EMS into the Log Delivery OSS feeds.	OK	Unavailable	Unavailable	OK
OSS and Application Svcs	The DMS Data Management System (DDMS) provides the Operation Support System Data Interface (OSSDI) interface for accessing DMS provisioning data. (Required by CMT)	OK	Unavailable	Unavailable	OK
DMS Maintenance Application	DMA provides an interface for line and trunk maintenance actions on the Core.	OK	Unavailable	Unavailable	OK
GR740 Pass Through	Provides TCP/IP GR-740 interface to the core for a network data collection operations system (NDC OS)	OK	Unavailable	Unavailable	OK

Table 3 CBM functionality during fault conditions

CBM Application/Function	Description	CMT/IEMS Site A lost	CBM Site B lost	Ring down, Core on Site A	Ring down, Core on Site B
Base Maintenance Interface	Provides a generic maintenance interface to receive notifications of states changes, query states and request maintenance actions of CM maintained components.	OK	Unavailable	Unavailable	OK
Lawful Intercept (International Market Only)	Provides detailed call information for law enforcement officials	OK	Unavailable	Unavailable	OK

135.2.6.2 Backup Access when CBM unavailable

When access via the CBM is unavailable due to failure conditions, the recommended method to connect to the Core or other nodes on either site is via telnet through the CS-LAN router.

- Telnet to the ERS 8600 can be used as a starting point. Once access is gained to the ERS 8600, access from there can be gained to the OAM and CallIP devices. Since the ERS 8600 supports multiple telnet sessions, access to multiple devices can be gained using this strategy.
 - Telnet to the IP of the ERS 8600.
 - Login as a user with r/w privileges
 - Telnet to the core or other node using the IP address of the node.
- This assumes that network connectivity is available between the NOC and site.
- To minimize the impacts of having OSPF disabled on the inactive site during certain failure scenarios, it is recommended to connect to the Circuitless IP for the CS-LAN router, which is outside the IPs used for OAMP access (and is not affected by OSPF disable).

135.2.6.3 CMT/IEMS accessibility

The CMT/IEMS will be inaccessible during certain failure scenarios:

- Ethernet IST down (ring down) between sites, with site A core inactive (due to OSPF disable) when using ERS 8600 routers.

- Loss of site A

When the CMT/IEMS is inaccessible the following services are retained:

- Call processing
- CBM functions for transfer of billing records, core logs and core OMs downstream and as the bootp load repository

The following CMT/IEMS resident services are unavailable:

- OA&M functions of the CS 2000 Management Tools and IEMS - GUI access, element management, alarms, non-core logs
- Access to the CS 2000 Compact Core Manager on the CBM (craft would be able to telnet to the CBM and from there access the Call Agent)

During an extended CMT/IEMS outage, the following recovery actions are recommended:

- Bring the standby Sun server(s) at Site B into service as the CMT and IEMS

Note: Requires manual intervention – roughly 2 to 3 hours once personnel are on site

The following is a detailed list of services which are not available during a period of CMT/IEMS inaccessibility:

- alarm reporting northbound
- alarm collection from NEs
- log collection from NEs
- log reporting northbound
- provisioning functions
- visibility to NEs (SC, GWC)
- GUI access (very similar to line above)
- maintenance actions on NEs (bsy/rts, lock/unlock etc)
- table access via the CBM
- QCA data collection
- OM collection
- OM push functions
- NTP services to NEs
- line maintenance function
- trunk maintenance functions
- proxy connections to Storm, USPC, Session Server (devices can not be accessed)

135.3 Hardware Requirements or Dependencies

Single ERS 8600 (dual processor) in each site, is the only router which supports interactions with the CA for OSPF disable. When the ERS 8600 is used, then an IST link must be configured across optical equipment between sites.

Enhanced GFSRM optical cards used for FC link between sites.

135.4 Software Requirements or Dependencies

SN08 loads for all components.

CMT/IEMS and CBM are HA versions.

135.5 Limitations and restrictions

This activity only addresses the mastership enhancements required for Geographic Survivability. It does not address other requirements of Geographic Survivability, including the optical requirements for syncing and communications over the distance required in the POR, or inservice upgrades from non-Geographic Survivability to Geographic Survivability configurations.

- In Hybrid configurations (with TDM equipment homed at 1 site), the TDM equipment is not Geo Survivable. Preference is given to the TDM side, only when either side can support callp. If necessary, a swact will be performed to the TDM side in order to allow callp on TDM side. Geographic Survivability Hybrid is supported only in Enterprise (CS2100) solutions.
- Due to the necessity for the CA to interact with the ERS 8600, this activity requires that there be only a single ERS 8600 per site, with IST links configured between sites. Dual ERS 8600s per site are not supported nor are SMLT links between sites. Enterprise upgrades from previous releases in Geographic Survivability configuration (which have dual ERS 8600s per site) require that the dual ERS 8600s be migrated to a single ERS 8600 per site.
- Other routers can be used for the CS-LAN, but the geographic survivability interactions with the call agent are only supported on the ERS 8600. If another router is used, the following limitations are in effect:
 - OSPF will not be disabled automatically on the inactive site when Ethernet connectivity is down between sites -- this will lead to additional call failures due to misdirected messages.
 - It may also lead to extended recovery times after the failure condition is removed.

- In cases of total communication loss between the two sites (i.e. all 3 master links), activity decision cannot be negotiated between the 2 call agents, and will be made based on connectivity check from each site to the WAN network.
 - While very unlikely, it could be possible to have an active/active (i.e. split brain) scenario, or an inactive/inactive scenario (no processing).
 - The WAN backup path was chosen as a method of mitigating the risk of the optical ring failure. The WAN connection check helps resolve activity when even the backup path is down.
- CS 2000 - Compact supports only a single time zone setting; if the two physical sites are in different time zones, then it is recommended to set the timezone to either GMT or the timezone of one of the sites.
- Session Server and Policy Server plans no mastership changes in SN08. Both Session Server and Policy Server units will be homed on 1 site.
- Geographic Survivability requires a WAN backup path configured separately from the Optical network for maximum redundancy.
 - dedicated vlan configured on each ERS 8600 for use by backup path only
 - vlans route via the WAN network, not over the optical ring
 - vlans are not disabled with OSPF disable
 - lack of connectivity is alarmed
- In general, the gateways and services node components of CS 2000 - Compact are single units, and not geographically survivable. Depending on where these nodes are located and how they are connected to the network impacts whether they survive any particular failure. Although the same nodes are supported in Geographic Survivability and non-Geographic Survivability config, there is no anticipated change in configuration or connection in the Geographic Survivability configuration.

135.6 Interactions

135.7 Applicable customer facing sections

Fault Management

Logs

___X__

Alarms

___X__

Configuration

Data Schema	__N/A__
User Interface	__X__
Element Management	__X__
Security	__N/A__
Service Order	__N/A__
Office Parameters	__N/A__
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	__N/A__

135.8 Glossary

Term	Description
CA or CCA	Compact / Call Agent
MC	Message Controller

136: A00008902 Corrective CAF excerpts

136.1 Feature name

Adding Category and Cause Values to SAM21 Alarm Logs in Syslog

136.2 Purpose

In the current SAM21 EM implementation, the EM generated syslogs for alarms do not contain values for category or probable cause. Also, the EM uses a field name 'Reason:' instead of 'Description:' to provide details about the alarm. Therefore, SAM21 EM alarms can't be correctly categorized by IEMS, nor can the Reason information be displayed in the IEMS message field. This CCAF will add the category and probable cause to the body of the SAM21 EM alarm logs. In addition, IEMS will put the contents of the Reason information from the log into its message field. These changes will make the SAM21 EM alarm logs consistent with other application fault logs when they are displayed by IEMS or sent northbound.

136.3 Problem symptoms

When the SAM21 reports an alarm, it does not contain the Description field or Classification type. Because of this the IEMS does not put any information in the MESSAGE FIELD seen in IEMS. It also does not have a Classification type so the IEMS throws it into the OTHER bucket instead of being classified as an EQUIPMENT failure.

The log sample like below:

```
Oct  7 11:59:28 wnc0s0pc SAM21EM:
_V2_~I=~H=wnc0s0pc~A=SAM21EM~S=0022~~ SCU356 CRIT
FLT Alarm Raised^M          Location: Upper Shelf
1:CSAM01-02:shelf 1:slot 9:card 1^M      Time:
Thu Oct 07 11:36:32 EDT 2004^M          Reason:  Shelf
Controller unavailable. Operating in Simplex.
```

```
Oct  7 11:59:28 wnc0s0pc SAM21EM:
_V2_~I=~H=wnc0s0pc~A=SAM21EM~S=0023~~ SCU356 CRIT
FLT Alarm Raised^M          Location: Upper Shelf
1:CSAM01-02:shelf 1:slot 7:card 1^M      Time:
Thu Oct 07 11:36:32 EDT 2004^M          Reason:  Mate
Shelf Controller unavailable. Operating in Simplex.
```

136.4 Description of problem

When the SAM21 reports an alarm, System log it into the customer log without the Description field or Classification type. Because of this the IEMS

does not put any information in the MESSAGE FIELD seen in IEMS. It also does not have a Classification type so the IEMS throws it into the OTHER bucket instead of being classified as an EQUIPMENT failure.

136.5 Description of fix

This feature plans to add two columns, category and cause, to each alarm entry in the SAM21 EM alarm log. The content of “category” column is the string mapping of AlarmType field value in the trap; and the content of “cause” is the string mapping of the Alarms AlarmID field value in the trap. There are four types of trap, mamaAlarmRaisedTrap, mamaShelfAlarmTrap, ScMissingAlarm and ATM alarm(s), will trigger the writing alarm log action. The ATM alarms don't use standard category and cause, so will be implemented differently.

The target log entry sample like below:

```
Oct  7 11:37:31 wnc0s0pc SAM21EM:
_V2_~I=~H=wnc0s0pc~A=SAM21EM~S=0053~~ SCU329 MAJOR
FLT Alarm Raised^M          Location: Upper Shelf
1:CSAM01-02:shelf 1:slot 7:card 1^M          Time:
Thu Oct 07 11:14:35 EDT 2004^M          Reason: Loss
of Communications: ISCS, Mate Ethernet, Serial
Connection^M          2 is down or unreachable^M
Category: communications^M          Cause:
performanceDegraded
```

```
Oct  7 11:38:25 wnc0s0pc SAM21EM:
_V2_~I=~H=wnc0s0pc~A=SAM21EM~S=0059~~ SCU356 N
ONE INFO Alarm Cleared^M          Location: Upper Shelf
1:CSAM01-02:shelf 1:slot
9:card 1^M          Time: Thu Oct 07 11:12:33 EDT
2004^M          Reason: Shel
f Controller unavailable. Operating in Simplex.^M
Category: equipment^M
Cause: underlyingResourceUnavailable
```

136.6 Example

Each alarm has an alarm ID (i.e. SCU310, IPOA301, etc.). System will divide the last 3 digits into 2 groups, the first digit stands for the alarm's category and the last two digits stands for the alarm's cause.

Using a mapping table, the digit can be transferred into some meaningful string, and then be added to the end of the alarm detail.

Use SCU310 alarm detail as an example. The current SCI310 alarm detail is as below:

```
OFC_NAME *** SCU310 JUL30 17:48:52 5000 FLT Alarm  
Raised
```

```
Location: sam21 1:CSAM01-02:shelf 1:slot 9:card 1
```

```
Time: Thu Jul 30 17:48:45 EST 2002
```

```
Reason: CPU load high. One Minute Load is 19.11
```

136.6.1 Actions to do:

1. We will divide the last digit of “SCU310” into two groups, “3” and “10”.
“3” stands for this alarm’s category; translate into “processingError” per the mapping table;

“10” stands for this alarm’s cause; translate into
“cpuCyclesLimitExceeded” per the mapping table.

2. Step 2 extends the two strings behind this alarm detail like below:

```
OFC_NAME *** SCU310 JUL30 17:48:52 5000 FLT Alarm  
Raised
```

```
Location: sam21 1:CSAM01-02:shelf 1:slot 9:card 1
```

```
Time: Thu Jul 30 17:48:45 EST 2002
```

```
Reason: CPU load high. One Minute Load is 19.11
```

```
Category: processingError
```

```
Cause: cpuCyclesLimitExceeded
```

Then we got the new version log detail entry. Other alarms detail will be updated in the similar way.

137: A00008907 Functional description (FN)

137.1 Title

CEM Log Key Changes for CEM Logs

137.2 Purpose

This corrective CAF is being created to churn in late requirements received while doing the ICAF A00007347, IEMS - CEM INTEGRATION INTO IEMS (POI 2050). The requirements concern a change of format for northbound events on the log feeds of IEMS, Integrated Element Management System, when used in conjunction with CEM, Core Element Manager. Also it addresses the functionality addition of addrep and delrep of logs from the SSPFS machine so the CEM will or will not process the logs.

137.3 Problem Symptoms

There are three main places the craft person will see differences with this corrective CAF.

1. The log in the IEMS GUI will be altered to CSEM 300, reflecting #2 immediately following.
2. The northbound feeds from IEMS will have new fields placed in them:
 - populate the logkey field with logname/number
 - populate the logname field with "CSEM"
 - populate the lognumber field with "300" for alarm sets and clears and "600" for info logs or unmapped logs
 - populate the eventtype field with "TBL" on raise and "INFO" on clear and "INFO" for unmapped logs
 - populate the eventlabel field with "Alarm set" on raise and "Alarm clear" on clear and "Log" for unmapped logs
 - populate the specificproblem field with the probable cause
 - populate the "bodytext" field with:
 - Equipment Id: <equipmentID>
 - Notification Id: <alarmindex>
 - Category: <category>
 - Cause: <probablecause>
 - Severity: <severity>

- Component Id: <componentid>

- Log Key: <logkey>

- Description:

- <mmessage>

each line should have eight leading blanks

3. The user can addrep/delrep logs that the CEM will receive from the CORE.

137.4 Description of Code Problem

137.4.1 Log Key

The different fields in the header must be modified with new variables listed in the previous section, and the new fields in the bodytext must be added.

137.4.2 Addrep/Delrep

The CEM Fault management solution filters out certain log types that come from the core but are not supported in CEM. The new requirement is to have a tool on the CEM Server by which the users will be able to add or delete logs that will be delivered to the CEM GUI from the core.

Two new processes – one as part of the SDM/CBM and one as part of the CEM Server has been introduced.

A script that runs on the SDM/CBM has been introduced.

The existing logNormalizer process on the CEM Server has been changed.

137.5 Description of Code Fix

137.5.1 Log Key changes:

The design was a printstring of the new fields listed above at the head of the body field. Then the data was written to the database as previously done.

137.5.2 Addrep/Delrep

137.5.2.1 CEM Server process:

A new process called llServer is introduced. This process collects input from the user on whether to add or drop logs. Also the log type and log number to add or drop is taken as input. The process connects to a listening socket on the SDM/CBM and the collected parameters are passed down in a message. On receiving the acknowledge message (success or failure of add or delete) from the SDM/CBM, the process writes the log type and number along with the format to a mapper.txt file. Based on the entry in the mapper file, the log is mapped into the CEM GUI.

137.5.2.2 SDM/CBM process:

A new process called llClient is introduced. This process opens a listening socket on a pre-defined port and waits for message from the server process. On receiving the message the desired operation of adding or dropping logs is performed with the help of a script (newly written). The script updates the cmlogs.config file part of the SDM/CBM base and restarts the logDelivery process.

137.6 Possible Design Side Effects**137.6.1 Log Key:**

none

137.6.2 Addrep/Delrep

The logDelivery process on the SDM base which interfaces with the core needs to be restarted for the change in log list (addition or deletion of logs) to take effect.

137.7 Testing Done

1. Make sure the llServer process is running on the SDM.
2. On the Server start the llClient process using the command –
./llClient -N<nickname of SDM> -o<addrep/delrep/addrep all> -l<logType> -n<logNumber>
3. On the CEM GUI make sure the new log shows up in the FM panel.

137.8 Related Documentation

<http://livelink.us.nortel.com/livelink/livelink.exe?func=ll&objId=6669363&objAction=browse&sort=name>
folders

[A00007302 - IEMS - CEM Integration](#)

[A00007304 - CEM I&C on IEMS](#)

[A00007347-IEMS - CEM Integration](#) and this document is in folder

[A00008907 - CEM Log Key Changes for CEM \(CCAF\)](#)

138: Q00720293 Functional Description (FN)

138.1 Feature name

Change in SWREL value

138.2 Description of change

Office parameter SITELABELINFO in table OFCVAR controls the SWREL (Software Release) value. The default value is derived from the actual product load of the switch, i.e. SNxx. Effective with SN07, the software release value is no longer NCSxx/UCSxx, but is now SNxx. The SWREL value is used in the Block Header record when writing CDR records to DIRP files. It is also passed to the SDM and CBM when using SBA billing.

The SWREL value is not transferred with an ONP as are the SITEID and SITELOC portions of SITELABELINFO. To check the value for a software load, use the IMAGENAME command. Once the ONP has completed, the customer may change the default SWREL value if desired.

139: Q00811611 Functional Description (FN)

139.1 Feature name

SSPFS – HA Support for user administration and passwords

139.2 Description

When a user is created, deleted, or modified on one node of a SSPFS HA cluster, the other node is not changed. This SN08 activity solves this problem by propagating the changes done to user accounts and groups on the active node to the inactive node. A synchronizing daemon is run on each node of the HA cluster to keep the login information in sync. No user intervention is needed. So, From SN08 onwards, the user accounts need not be created on both the active and inactive nodes.

139.3 Hardware Requirements or Dependencies

Not applicable

139.4 Software Requirements or Dependencies

Not applicable

139.5 Limitations and restrictions

This mechanism synchronizes the inactive node with the data on the active node. So, any changes to the user accounts or groups should be done only on the active node. Any changes done on the inactive node will be lost when the synchronizing mechanism overwrites them with the data from the active node.

139.6 Interactions

Not applicable

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
A00005562	MG9000 ITP/ABI Overload Controls
A00005646	IPSEC with MG9000 Element Manager
A00006893	TLS Support for NGSS
A000006901	Missing Patches
A000006979	Synchronized Backup Restore Manager
A000007000	GigE Network Interface
A000007071	SN08 3rd Party GW Interop Profiles
A00007074	GigE Link Maintenance
A00007102.AA11	Dual C-Side IP for GWC
A000007113	GWC External Interface Robustness
A00007213	MG9000 5/30 Minutes OMs
A00007243.AA09	Prevent Outage when CEM flash has not been erased
A00007270.AA13	Session Server Call Processing Overload Controls
A000007271.AA08	TOPS EOL for SN08
A00007304	SN08 CEM I & C on IEMS

A00007327.AA08	Media Proxy 5 and 30 minute Operational Measurements
A00007393	Session Policy Controller
A000007415	Internodal Emergency Standalone (ESA) Element Manager
A000007417.AA03	Ethernet link overload Control
A000007465.AA06	Integrated Accounting Application (IAA)
A000007489.AA13	Integration of SuperNode Data Manager (SDM) User Authentication with the Integrated Element Manager System (IEMS)
A000007713.AA02	TOPS-IP Robustness
A00008431.AA04	Support for CS2Kc Geo Survivability

1: A00005562 Fault Management (FM)

1.1 Document Name

MG9000 ITP/ABI Overload Controls

1.2 Fault management strategy

MG9000 when overload thresholds are crossed. The specific ITP or ABI with the fault is included in the alarm information. The overload faults will be displayed on the MG9000 Mgr Alarm Browsers, logged to the MG9000 Mgr CUST logs and forwarded to northbound OSS.

Individual connection denials due to overload are recorded in LINE 162 logs on the XA-Core.

1.3 Fault management tools and utilities

The existing MG9000 Mgr Alarm Browser will display any overload alarm conditions.

1.4 Logs

1.4.1 Explanation

Log Title: LINE162

Name: XA-Core INFO Log

Description: Backward Fabric Control Message received indicating call attempt denied due to MG9K Overload

Event type:Minor.

1.4.2 Example Format

RTP207AQ LINE162 JUL02 09:07:14 6100 INFO BACK_FCM

LG 09 0 00 00 DN 6195200900

Error: Connection denied due to GW Overload

1.4.3 Action

Log indicates GW is experiencing high traffic volume. Offload any maintenance or unnecessary call-processing.

1.5 Alarms

MG9K EM alarms are raised or cleared for various overload resource threshold crossing events. Also, a general overload alarm is raised if the system is declared to be in overload. Alarm types and formats are defined in the NORTEL-UEMG-PERFMON-MIB.

1.5.1 MG9KEM Alarm Format

Overload SNMP notifications contain the following information:

FaultType

- One of the fault types described in 3.4.2

AlarmSeverity

- Major or Critical

AlarmDescrip

- Short Description of fault type

Location

- frame/shelf/slot where fault occurred

RecentCpuAvg

- Last recorded CPU utilization datapoint

AlarmDefinition

- indicates alarm is set or cleared

AlarmEventTime

- timestamp

NotificationVal

- value of resource when threshold crossing recorded

1.5.2 Fault Types

1.5.2.1 ovldRsrcMonPduRateFault

Cause: Incoming AAL5 PDU rate threshold crossed

Severity: Major

Action: Information only - Verify traffic engineering.

1.5.2.2 ovldRsrcMonCbnMsgRateFault

Cause: Incoming Connection Broker message rate threshold crossed

Severity: Major

Action: Information only - Verify traffic engineering.

1.5.2.3 ovldRsrcMonConnQueueFault

Cause: Incoming Connection Broker queue delay threshold crossed

Severity: Major

Action: Information only - Verify traffic engineering.

1.5.2.4 ovldRsrcMonCpuUtilFault

Cause: Card CPU utilization threshold crossed

Severity: Major

Action: Information only - Verify traffic engineering.

1.5.2.5 ovldDetectionAlarm

Cause: System is actively denying connection requests.

Severity: Critical

Action: Offload any maintenance or unnecessary call-processing.

1.6 Related documentation

A00002007: MG9K EM Overload Controls FN

2: A00005646 Fault Management (FM)

2.1 Document Name

IPSEC with MG9000 Element Manager

2.2 Fault management strategy

The standard MG9k EM Fault Management strategy will apply to the faults for MG9kEM IPsec and Overload Controls. 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.

In support of the MG9K EM - MG9K IPsec connection, there will be new faults added to indicate threshold crossing and link issues.

For the MG9k EM Overload Controls feature there will not be any new faults added. However, existing faults for the DCC which indicate threshold crossing and overload detection will now also apply to the ITP and ABI.

2.3 Fault management tools and utilities

TBD (IPSEC)

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date, time, the NE Id, the generating resource information, the severity and the 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.

2.4 Logs

2.4.1 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 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

2.4.2 ITP/ABI Overload Controls.

The behavior for the logs for the ITP/ABI Overload Controls will be exactly the same as that implemented for the DCC Card in SN06.2. Please refer to the document titled Fault Management - MG9k EM Overload Controls (A00002007) for more details regarding these logs.

These are new alarms that will be generated by the MG9000.

- Unable to communicate with RADIUS Server
- Secure link Down w GWC
- Packet Discard (depends on the threshold set)
- Overload Controls. The alarms for the ABI and ITP Overload Controls are exactly same as those documented for the DCC Card in 6.2. The only difference being that these alarms will now also apply to the ABI & ITP Card as well as the DCC Card. Please refer to the document titled Fault Management - MG9k EM Overload Controls (A00002007) for more details regarding these alarms.

The following logs will be thresholds in the MG9000. When the threshold is crossed an alarm will be generated

1. Logging Event

- Sequence_Number_Overflow

-
- Life_Time_Expired, Type = SoftlHard
2. Security Policy Database
 - SAD_Discard_Policy:- Direction (in/outbound)
 - SAD_Lookup_Fail, info needed:- Direction (in/out bound):- Sub-info field invalid SPI, Replayed packet
 3. IKE
 - IKE_Main_Mode-Failed, Mismatched PSK
 - IKE_Quick_Mode-Failed, Proposal mismatch, NULL ESP & authentication = null, en/decryption failures
 - IKE_Packet Discarded, decryption errors, Auth errors
 4. IPsec Security Association
 - SA_Decryption_Error
 - SA_Authentication_Error

2.5 Related documentation

1. Fault Management - MG9kEM Overload Controls (A0002007) Bobby Robinson (SN06.2)

3: A00006893 Fault Management (FM)

3.1 Document Name

TLS Support for NGSS

3.2 Fault management strategy

The TLS security feature for the SIP Gateway application on the NGSS (Next Generation 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.

3.3 Fault management tools and utilities

This feature utilizes the current log and alarm display mechanisms in use by the NGSS. 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 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 - 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.

3.4 Logs

There are two logs associated with the certificate management (cert_mngt/cert_mgmt) tool:

- CRTM700 - New private key requested
- CRTM701 - Self signed certificate requested

All other logs and associated alarms will have the name start with SIPS (for SIP Security).

The following log events will be defined in this section:

- SIPS601 - A TLS authentication failure (error reason)
- SIPS305 - Initialization - TLS initialization critical logs
- SIPS605 - Initialization - TLS security initialization completed
- SIPS604 - Initialization - A TLS information log for the Local Certificate expiration date
- SIPS600 - TLS connection request dropped reason
- SIPS606 - TLS attempt to add trusted CA failed
- SIPS607 - TLS connection request failed

The following logs are associated with alarms:

- SIPS300 - TLS dropped number of requests over time
- SIPS301 - TLS failed certificate authentications over time
- SIPS302 - TLS Local certificate is expiring soon

3.4.1 CRTM700: New private key requested

3.4.1.1 Formats

3.4.1.1.1 Syslog

Following is the format of the log:

```
<Date> <Time> <DeviceName> cert_mgnt:CRTM700 <Severity>
<Type>CERT_MGNT<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>:
 - none/info: “^M User requested new private key.^M Existing key moved to /opt/base/share/ssl/server.key.<HHMM>_<DDMMYY>^M”

Example:

```
Nov 11 14:12:14 comit.ngss.unit0 cert_mgnt: CRTM700 NONE INFO CERT_MGNT ^M
User requested new private key.^M      Existing key moved to /opt/base/share/
ssl/server.key.1412_11112004^M
```

3.4.1.2 Explanation

During the execution of the cert_mgnt tool either option 1 or option 2, the user requested a new private key. The existing private key is backed up within the /opt/base/share/ssl. The new private key is placed in /opt/base/share/ssl/server.key

3.4.1.3 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>	NONE	Severity level of the log
<Type>	INFO	informational
<Log Message>	see bulleted list	Log message text.

3.4.1.4 Action

On an info log, no immediate action is required.

3.4.1.5 Associated Operational Measurements or Performance Measurements

Not applicable to this log.

3.4.1.6 Additional information

See tool output and TLS initialization logs to ensure that the new key and certificate was provisioned properly.

3.4.2 CRTM701: Self signed certificate requested

3.4.2.1 Formats

3.4.2.1.1 Syslog

Following is the format of the log:

```
<Date> <Time> <DeviceName> cert_mgnt:CRTM701 <Severity>
<Type>CERT_MGNT<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>:
 - none/info: “^M User accepted disclaimer for generating self-signed certificates^M”

Example:

```
Nov 12 09:54:50 comit.ngss.unit0 cert_mgnt: CRTM701 NONE INFO CERT_MGNT ^M
User accepted disclaimer for generating self-signed certificates^M
```

3.4.2.2 Explanation

During the execution of the cert_mgnt tool in option 1, the user selected to generate a self-signed certificate. Self-signed certificates carry a security risk because they are not signed by a trusted certificate authority and therefore cannot be authenticated by a certificate authority.

3.4.2.3 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>	NONE	Severity level of the log
<Type>	INFO	informational
<Log Message>	see bulleted list	Log message text.

3.4.2.4 Action

On an info log, no immediate action is required.

3.4.2.5 Associated Operational Measurements or Performance Measurements

Not applicable to this log.

3.4.2.6 Additional information

See tool output and TLS initialization logs to ensure that the new key and certificate was provisioned properly.

3.4.3 SIPS601 - A TLS authentication failure (error reason)

3.4.3.1 Formats

3.4.3.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> <process> SIPS601 <Severity> <Type> TLS
certificate common name: <Common Name>, reason: <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
- <process>: process class that raised the log (sipgwyappln:)
- <Severity>: The Severity of the log (MINOR).
- <Type>: The type of log (INFO)
- <Common Name>: The common name in the X.509 certificate that the remote side is presenting
- <Log Message>: “<message>”, where <message> is one of:
 - unable to get issuer certificate
 - unable to get certificate CRL
 - unable to decrypt certificate’s signature
 - unable to decrypt CRL’s signature
 - unable to decode issuer public key
 - certificate signature failure
 - CRL signature failure
 - certificate is not yet valid
 - CRL is not yet valid
 - certificate has expired
 - CRL has expired
 - format error in certificate’s notBefore field
 - format error in certificate’s notAfter field
 - format error in CRL’s lastUpdate field
 - format error in CRL’s nextUpdate field
 - out of memory

-
- self signed certificate
 - self signed certificate in certificate chain
 - unable to get local issuer certificate
 - unable to verify the first certificate
 - certificate chain too long
 - certificate revoked
 - invalid CA certificate
 - path length constraint exceeded
 - unsupported certificate purpose
 - certificate not trusted
 - certificate rejected
 - application verification failure
 - subject issuer mismatch
 - authority and subject key identifier mismatch
 - authority and issuer serial number mismatch
 - key usage does not include certificate signing
 - unable to get CRL issuer certificate
 - unhandled critical extension
 - key usage does not include CRL signing
 - unhandled critical CRL extension

Example:

```
Oct  8 16:36:56 comit.ngss.unit1 sipgwyappln: SIPS601 MINOR INFO TLS certificate
common name: 47.129.118.195, reason: self signed certificate
```

3.4.3.2 Explanation

The SIPS601 log is generated during authentication failure events. The INFO log indicates the reason for the authentication failures.

3.4.3.3 Field descriptions

Table 3: Field descriptions

Field	Value	Description
<DATE>	<Mon> <DD>	Current date when the log occurred.
<Time>	<HH>:<MM>:<SS>	Current time when the log occurred.

Table 3: Field descriptions

Field	Value	Description
<DeviceName>		Name of the session server.
<Severity>	MINOR	Severity level of the log
<Type>	INFO	informational
<Log Message>	see bulleted list	Log message text.

3.4.3.4 Action

On an info log, no immediate action is required.

3.4.3.5 Associated Operational Measurements or Performance Measurements

OM registers “TLS_CONNECTION_REQUESTS_FAILED” and “TLS_HANDSHAKE_AUTHENTICATION_FAILED” in group “SIPGW_TLS”

3.4.3.6 Additional information

An excessive amount of authentication failures may have associated alarms. Verify alarms and OMs

3.4.4 SIPS305: TLS Initialization logs**3.4.4.1 Formats****3.4.4.1.1 Syslog**

Following is the format of the log:

```
<Date> <Time> <DeviceName> sipgwyappln: SIPS305 <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 (CRIT).
- <Type>: The type of log (INIT)
- <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 Local Key and Cert do not match^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”

Example:

```
Feb  9 13:11:39 comit.ngss.unit1 sipgwyappln: SIPS305 CRIT INIT TLS ^M TLS
Failed to load Key^M
```

3.4.4.2 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.

3.4.4.3 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>	CRIT	Severity level of the log
<Type>	INIT	initialization log.
<Log Message>	see bulleted list	Log message text.

3.4.4.4 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_mngt tool). 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

3.4.4.5 Associated Operational Measurements or Performance Measurements

Not applicable to this log.

3.4.4.6 Additional information

Normally, the cert_mngt 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>).

3.4.5 SIPS605: TLS Initialization logs

3.4.5.1 Formats

3.4.5.1.1 Syslog

Following is the format of the log:

```
<Date> <Time> <DeviceName> sipgwyappln: SIPS605 <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>:
 - none/info: “^M TLS Security Enabled^M”

Example:

```
Oct  8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS605 NONE INFO TLS ^M      TLS
Security Enabled^M
```


3.4.5.2 Explanation

The SIPS605 log is generated during the initialization of the Call Processing application (i.e. during the unlock). This log indicates that TLS has been enabled. Expect a SIPS604 log along with this log.

3.4.5.3 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>	NONE	Severity level of the log
<Type>	INFO	informational.
<Log Message>	see bulleted list	Log message text.

3.4.5.4 Action

On an info log, no immediate action is required.

3.4.5.5 Associated Operational Measurements or Performance Measurements

Not applicable to this log.

3.4.5.6 Additional information

None.

3.4.6 SIPS604: TLS Initialization logs

3.4.6.1 Formats

3.4.6.1.1 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>:
 - none/info: “^M Local Certificate Expires: Year=<YYYY>, Month = <MM>, Day = <DD>^M”

Example:

```
Oct  8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS604 NONE INFO TLS ^M Local
Certificate Expires: Year=2005, Month = 10, Day = 8^M
```

3.4.6.2 Explanation

The SIPS604 log is generated during the initialization of the Call Processing application (i.e. during the unlock). This log indicates when the current local certificate will expire.

3.4.6.3 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>	NONE	Severity level of the log
<Type>	INFO	informational.
<Log Message>	see bulleted list	Log message text.

3.4.6.4 Action

On an info log, no immediate action is required.

3.4.6.5 Associated Operational Measurements or Performance Measurements

Not applicable to this log.

3.4.6.6 Additional information

None.

3.4.7 SIPS600 - TLS connection request dropped reason

3.4.7.1 Formats

3.4.7.1.1 Syslog

Following is the format of the log:

```
<Date> <Time> <DeviceName> sipgwyappln: SIPS600 MINOR INFO 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
- <Log Message>:
 - “^M Dropped TLS Handshake request, monitor OMs^M”
 - “^M Dropped TLS Handshake request, TLS is not enabled. ^M”
 -

Example:

```
Oct 8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS600 MINOR INFO TLS ^M Dropped
TLS Handshake request, monitor OMs^M
```

3.4.7.2 Explanation

The SIPS600 log is generated during the connection set up of the Call Processing application. When the ‘monitor OMs’ log comes out, ensure that the threshold levels set for connection throttling are reasonable for the size of the office. If the ‘TLS is not enabled’ message comes out, ensure that the initialization of the call processing application worked correctly.

3.4.7.3 Field descriptions

Table 7: 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.
<Log Message>	see bulleted list	Log message text.

3.4.7.4 Action

If the log comes out once or twice, it is likely a transient problem. Monitor the OM register “TLS_CONN_REQ_DROP” in group “SIPGW_TLS” and ensure that the event doesn’t continuously recur. If it does, check to ensure the threshold values for the TLS connections are set properly for the number of connections expected in the time period. If they are, check to ensure the integrity of the office LAN (as there might be an intruder on the network).

3.4.7.5 Associated Operational Measurements or Performance Measurements

TLS_CONNECTION_REQUESTS_DROPPED in OM group SIPGW_TLS

3.4.7.6 Additional information

None.

3.4.8 SIPS606 - TLS attempt to add trusted CA failed**3.4.8.1 Formats****3.4.8.1.1 Syslog**

Following is the format of the log:

```
<Date> <Time> <DeviceName> sipgwyappln: SIPS606 NONE INFO TLS  
^M Failed to add Trusted CA name <name>^M
```

Following are values/explanations of the variable values presented above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <name>: Unique name used to indicate which trusted certificate provisioned via the web interface is having trouble loading.

Example:

```
Oct  8 13:41:47 comit.ngss.unit1 sipgwyappln: SIPS606 NONE INFO TLS ^M      Failed  
to add Trusted CA name server^M
```

3.4.8.2 Explanation

The SIPS606 log is generated when there is a problem importing the trusted certificate provisioned via the web interface in the database.

3.4.8.3 Field descriptions

Table 8: 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.
<name>	Trusted certificate name from the database, Table SECURITYCONFIGCERTS, item SECURITYCERTNAME.	Unique name from the database.

3.4.8.4 Action

Since the certificate is not correct (i.e. it is unable to be loaded), try to re-provision the certificate (using a different name) or delete the certificate <name> and re-add it via the 'Add Remote Trusted Certificate' web interface.

3.4.8.5 Associated Operational Measurements or Performance Measurements

Not applicable to this log.

3.4.8.6 Additional information

If this log comes out, and then authentication logs come out, it is likely due to the failure to provision the trusted certificate for the remote server. Retrieve the remote servers' public self-signed certificate and add it to the database via the web interface.

3.4.9 SIPS607 - TLS Connection Request Failed

3.4.9.1 Formats

3.4.9.1.1 Syslog

Following is the format of the log:

```
<Date> <Time> <DeviceName> sipgwyappln: SIPS607 NONE INFO TLS
Connection Request Failed: Server: <Server Name>, IP Address: <IP
Address>
```

Following are values/explanations of the variable values presented above:

- <Date>: Current date

- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <Server Name>: The name of the remote certificate
- <IP Address>: The IP address of the remote server

Example:

```
Feb 16 09:53:44 comit.ngss.unit1 sipgwyappln: SIPS607 NONE INFO TLS Connection
Request Failed: Server: AURUM, IP Address: 47.129.118.195
```

3.4.9.2 Explanation

The SIPS607 log supplements the SIPS601 log. The SIPS607 is generated to provide details into which remote server is not able to connect with the local server.

3.4.9.3 Field descriptions

Table 9: 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.
<Server name>	Name of the remote server as it is provisioned in the Remote SIP Server web page. Table SIPSERVER, field: SERVERNAME where the corresponding field IPADDRESS1 matches the <IP Address> field in the SIPS607 log.	If this value is NULL, then there is no remote server name provisioned corresponding to the <IP Address>.
<IP Address>	IP address of the remote server that is unable to connect with the local server.	IP address of the remote server.

3.4.9.4 Action

No immediate action is required.

3.4.9.5 Associated Operational Measurements or Performance Measurements

OM registers “TLS_CONNECTION_REQUESTS_FAILED” in group “SIPGW_TLS”

3.4.9.6 Additional information

If the value of the server name is NULL, this log, together with the SIPS601 log indicates that the remote server is not provisioned locally.

If the value of the server name is not NULL, this log, together with the SIPS601 log, indicates the reason which remote server is not able to connect with the local server, and the reason why the remote server is not able to connect.

Verify provisioning of the remote server’s certificate on the remote side and on the local side.

If there is an excessive amount of SIPS601 and SIPS607 logs, monitor OMs and alarms.

3.4.10 SIPS300 - TLS dropped number of requests over time

3.4.10.1 Formats

3.4.10.1.1 Syslog

Following is the format of the log:

```
<Date> <Time> <DeviceName> alarmd: SIPS300 <Severity> TBL TLS
Dropped Connection Request NCGL=<DeviceName>;Unit=<Unit#>;SIPS
<alarmmessage>
```

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, MINOR, MAJOR, or CRIT).
- <Unit#>: The unit number assigned (either 0 or 1)
- <alarmmessage>: One of:
 - Dropped <number> Connections requests
 - Automatically cleared due to alarm generator process death
- <number>: The number of dropped requests.

Example:

Oct 6 20:19:53 comit.ngss.unit1 alarmd: SIPS300 MINOR TBL TLS Dropped Connection Request NCGL=comit.ngss.unit1;Unit=1;SIPS Dropped 10 Connections requests

3.4.10.2 Explanation

The SIPS300 log is generated during the alarming of dropped connection requests (due to either the threshold being crossed for throttling connections, or due to attempting to use TLS when TLS is not enabled). The severity of the alarm indicates the threshold that was crossed, 10 dropped connection requests in a minute for a MINOR, 50 dropped requests for a MAJOR, and 100 dropped requests (or more) for a critical. The alarm is raised for a minimum of 30 minutes.

3.4.10.3 Field descriptions

Table 10: 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>	NONE, MINOR, MAJOR or CRIT	Severity level of the log
<Unit#>	0 or 1	The unit number of the platform
<alarmmessage>	see bulleted list	Alarm log message text.
<number>	internally generated.	The number of dropped connections in the last time period (currently one minute).

3.4.10.4 Action

If the log comes out monitor the OM register “TLS_CONN_REQ_DROP” in group “SIPGW_TLS” and ensure that the event doesn’t continuously recur. If it does, check to ensure the threshold values for the TLS connections are set properly for the number of connections expected in the time period. If they are, check to ensure the integrity of the office LAN (as there might be an intruder on the network). The log/alarm will be raised at least 30 minutes, and if the problem has ceased, the clear alarm log will be generated.

3.4.10.5 Associated Operational Measurements or Performance Measurements

OM register “TLS_CONN_REQ_DROP” in group “SIPGW_TLS”

3.4.10.6 Additional information

See “SIPS600 - TLS connection request dropped reason” on page 1145.

3.4.11 SIPS301 - TLS failed certificate authentications over time

3.4.11.1 Formats

3.4.11.1.1 Syslog

Following is the format of the log:

```
<Date> <Time> <DeviceName> <process> SIPS301 <Severity> TBL TLS
Failed Authentication NCGL=<DeviceName>;Unit=<Unit#>;SIPS
<alarmmessage>
```

Following are values/explanations of the variable values presented above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <process>: process class that raised the log (either sipgwyappln: or alarmd:)
- <Severity>: The Severity of the log (NONE, MINOR, MAJOR or CRIT).
- <Unit#>: The Unit number.
- <alarmmessage>:
 - Failed <number> certificate authentications
 - <number>: The number of times this event occurred in the last minute before the alarm was raised.
 - Automatically cleared due to alarm generator process death

Example:

```
Feb  9 13:03:50 comit.ngss.unit1 alarmd: SIPS301 CRIT TBL  TLS Failed
Authentication NCGL=yin;Unit=0;SIPS Failed 28 certificate authentications
Feb  9 13:08:10 yin alarmd: SIPS301 NONE TBL  TLS Failed Authentication
NCGL=yin;Unit=0;SIPS Automatically cleared due to alarm generator process death
```

3.4.11.2 Explanation

The SIPS301 log is generated during authentication failure events. The alarmd process log indicates the level of trouble (CRIT indicates a very serious problem, MINOR may be transient or the beginning of a series of authentication failures).

3.4.11.3 Field descriptions

Table 11: 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>	NONE, MINOR, MAJOR, or CRIT	Severity level of the log
<Unit#>	0 or 1	The unit number of the platform
<number>	internally generated.	The number of dropped connections in the last time period (currently one minute).
<alarmmessage>	see bulleted list	Alarm log message text.
<Log Message>	see bulleted list	Log message text.

3.4.11.4 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). Alternatively contact the next level of support.

On an info log, no immediate action is required.

3.4.11.5 Associated Operational Measurements or Performance Measurements

OM registers “TLS_CONNECTION_REQUESTS_FAILED” and “TLS_HANDSHAKE_AUTHENTICATION_FAILED” in group “SIPGW_TLS”

3.4.11.6 Additional information

To determine the exact subject, use of the sp2ktrace tool would be warranted. This type of activity should be undertaken with the supervision of Nortel Technical Support.

3.4.12 SIPS302 - TLS Local certificate is expiring soon

3.4.12.1 Formats

3.4.12.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> alarmd: SIPS302 <Severity> TBL TLS

<Date> <Time> <DeviceName> alarmd: SIPS302 <Severity> TBL Local Certificate is Expiring Soon NCGL=<DeviceName>;Unit=<Unit#>;SIPS Local Certificate is Expiring Soon

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, MINOR, MAJOR or CRIT).

Example:

```
Oct  8 13:14:17 comit.ngss.unit0 alarmd: SIPS302 MINOR TBL  TLS Local Certificate
is Expiring Soon NCGL=comit.ngss.unit0;Unit=0;SIPS TLS Local Certificate is
Expiring Soon
```

3.4.12.2 Explanation

The SIPS302 log is generated as a result of the alarm process check to ensure the Local Server certificate continues to be valid. The expiration date contained in the certificate is checked on a daily basis, and when the expiration of the certificate will occur within 31 days (MINOR), 15 days (MAJOR), or 5 days (CRIT), the alarm is raised, with this log. For certificates that have already expired, the CRIT alarm and log is generated, and authentication failures will be output for any connections that are attempted.

3.4.12.3 Field descriptions

Table 12: 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>	NONE, MINOR, MAJOR or CRIT	Severity level of the log

3.4.12.4 Action

With the cert_mngt tool, create a new self-signed certificate (if using self-signed certificates) or generate a certificate signing request and then provision the result. Once this is done, lock/unlock the callp application (or perform a SWACT after locking/unlocking the inactive with the new certificate).

3.4.12.5 Associated Operational Measurements or Performance Measurements

Not applicable to this log.

3.4.12.6 Additional information

None.

3.5 Alarms

The following list of alarms will be provided:

- TLS connection request comes in above the connection throttle limit (and above the threshold for the alarm - the defined thresholds are: 10 for minor, 50 for major, and 100 for critical)
- TLS connection handshake failures (the thresholds are: 1 for minor, 2 for major, and 5 for critical)
- TLS local certificate expiration (expiry in 31 days or less - minor, 15 days or less - major, and 5 days or less - critical)

3.5.1 Connection Requests Dropped Alarm

3.5.1.1 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 13: IEMS Alarm GUI Field descriptions

Field	Value
Severity	NONE, MINOR, MAJOR, or CRIT
Category	<i>APC_Communications</i>
LogName	SIPS
LogNumber	300
EventType	TBL
EventLabel	TBL
ProbableCause	<i>thresholdCrossed</i>
SpecificProblem	TLS Dropped Connection Request
BodyText	Dropped <number> Connections requests<updatetext>

BodyText explanation: The BodyText entry for the log will contain “Dropped <number> Connections requests”. However, over time, other events may occur, and the alarm BodyText will be updated with “Dropped <number> Connections requests 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.

3.5.1.2 Explanation

Description: The SIPS300 log is generated during the alarming of dropped connection requests (due to either the threshold being crossed for throttling connections, or due to attempting to use TLS when TLS is not enabled). The severity of the alarm indicates the threshold that was crossed, 10 dropped connection requests in a minute for a MINOR, 50 dropped requests for a MAJOR, and 100 dropped requests (or more) for a critical. The alarm is raised for a minimum of 30 minutes. See also the SIPS600 log for an associated log.

Severity: Escalating severity, Minor for 10 or more connection requests dropped, Major for 50 or more requests dropped, and Critical for 100 or more connection requests dropped.

3.5.1.3 Action

If the alarm comes out monitor the OM register “TLS_CONN_REQ_DROP” in group “SIPGW_TLS” and ensure that the event doesn’t continuously recur. If it does, check to ensure the threshold values for the TLS connections are set properly for the number of connections expected in the time period. If they are, check to ensure the integrity of the office LAN (as there might be an intruder on the network). The log/alarm will be raised at least 30 minutes, and if the problem has ceased, the clear alarm log will be generated.

3.5.1.4 Corresponding Clear Log

Log Title: SIPS300 with severity NONE.

3.5.2 Connection Authentication Failures Alarm

3.5.2.1 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 14: IEMS Alarm GUI Field descriptions

Field	Value
Severity	NONE, MINOR, MAJOR, or CRIT
Category	<i>APC_Communications</i>
LogName	SIPS
LogNumber	301
EventType	TBL
EventLabel	TBL
ProbableCause	<i>authenticationFailure</i>
SpecificProblem	Too many authentication failures over time.
BodyText	Failed <number> certificate authentications<updatetext>

BodyText explanation: The BodyText entry for the log will contain “Failed <number> certificate authentications”. However, over time, other events may occur, and the alarm BodyText will be updated with “Failed <number> certificate authentications 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.

3.5.2.2 Explanation

Description: See “SIPS301 - TLS failed certificate authentications over time” on page 1151.

Severity: See “SIPS301 - TLS failed certificate authentications over time” on page 1151.

3.5.2.3 Action

See “SIPS301 - TLS failed certificate authentications over time” on page 1151.

3.5.2.4 Corresponding Clear Log

Log Title: SIPS301 with severity NONE.

3.5.3 Local Certificate Expiry Alarm

3.5.3.1 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 15: IEMS Alarm GUI Field descriptions

Field	Value
Severity	NONE, MINOR, MAJOR, or CRIT
Category	<i>APC_Communications</i>
LogName	SIPS
LogNumber	302
EventType	TBL
EventLabel	TBL
ProbableCause	<i>keyExpired</i>
SpecificProblem	Local certificate is about to expire (or has expired)
BodyText	TLS Local Certificate is Expiring Soon

3.5.3.2 Explanation

Description: See “SIPS302 - TLS Local certificate is expiring soon” on page 1153.

Severity: See “SIPS302 - TLS Local certificate is expiring soon” on page 1153.

3.5.3.3 Action

See “SIPS302 - TLS Local certificate is expiring soon” on page 1153.

3.5.3.4 Corresponding Clear Log

Log Title: SIPS302 with severity NONE.

3.6 Related documentation

n/a

4: A00006901 Fault Management (FM)

4.1 Document Name

Document Name: MissingPatches_FM.fm

4.2 Fault management strategy

This feature moves the PatchFile Receipt System access from the SSPFS TOOL into the Network Patch Manger (NPM). This feature also addresses the difference between R-status patches and V-status patches. The addition of this software into the NPM warrants the addition of three new alarms:

- REL_GEN_NOT_APP
- PFRSGETPATCH
- PFRSGENREPORT

4.3 Fault management strategy

No additional tools are implemented by this feature. Customer alarms for this feature are generated via the existing alarm software in the Network Patch Manager.

4.4 ALARMS

4.4.1 REL_GEN_NOT_APP Alarm

- **Alarm Format:**

** NPM360 SEP21 11:23:55 1100 INFO Alarm Raised

Alarm REL_GEN_NOT_APP has been raised.

Alarm Description: Released patches not applied.

- **Severity:** Major
- **Cause:** A patch that has a status of R has been validated but not applied.
- **Duration:** The alarm will continue to alarm until all the R status patches have been applied.
- **Action:** Apply all R status patches.

4.4.2 PFRSGENREPORT Alarm

- **Alarm Format:**

** NPM360 SEP21 11:23:55 1100 INFO Alarm Raised

Alarm PFRSGENREPORT has been raised.

Alarm Description: PFRS GENREPORT task has failed.

- **Severity:** Major
- **Cause:** PFRS GENREPORT failed to execute.
- **Duration:** The alarm will continue to alarm until the next successful execution of the PFRS GENREPORT task.
- **Action:** Fix the error and execute the task again.

4.4.3 PFRSGETPATCH

- **Alarm Format:**

** NPM360 SEP21 11:23:55 1100 INFO Alarm Raised

Alarm PFRSGETPATCH has been raised.

Alarm Description: PFRS GETPATCH task has failed.

- **Severity:** Major
- **Cause:** PFRS GETPATCH failed to execute.
- **Duration:** The alarm will continue to alarm until the next successful execution of the PFRS GETPATCH task.
- **Action:** Fix the error and execute the task again.

4.5 Related documentation

5: A00006979 Fault Management (FM)

5.1 Document Name

Synchronized Backup Restore Manager

5.2 Fault management strategy

Synchronized Backup Manager will generate two customer logs:

- BKM600 if a system backup completes successfully.
- BKM601 if a system backup fails.
- Synchronized Backup Manager will generate one security log if a user without the correct permissions attempts to invoke the Backup Manager.

5.3 Fault management tools and utilities

5.3.1 Faults, Alarms and Logs

Existing SSPFS customerlog and securitylog facilities.

5.4 Logs

Log Title/Log ID: BKM600

5.4.1 Formats

5.4.1.1 NTSTD

5.4.1.2 SCC2

5.4.1.3 Syslog

Aug 23 21:00:01 znc0s0j6.us.nortel.com BackupManager:
V2~I=~H=znc0s0j6~A=BackupManager~S=0206~~ BKM600 NONE
INFO System Backup Complete^M System backup 040830_134700
completed successfully.

5.4.1.4 SNMP

5.4.1.5 Integrated Element Manager GUI Fields

5.4.2 Explanation

Description: Generated when a system backup is completed successfully.

5.4.3 Field descriptions

None.

5.4.4 Action

None.

5.4.5 Associated Operational Measurements or Performance Measurements

None.

5.4.6 Additional information

Not applicable.

Log Title/Log ID: BKM601**5.4.7 Formats****5.4.7.1 NTSTD****5.4.7.2 SCC2****5.4.7.3 Syslog**

Aug 23 21:00:01 znc0s0j6.us.nortel.com BackupManager:
V2~I=~H=znc0s0j6~A=BackupManager~S=0206~~ BKM300 NONE
INFO System Backup Failure^M System backup failed. ^M Reason:
SESM not running.

5.4.7.4 SNMP**5.4.7.5 Integrated Element Manager GUI Fields****5.4.8 Explanation**

Description: Generated when a system backup fails.

5.4.9 Field descriptions**5.4.10 Action**

Correct problem in system based on failure reason. Once failure is corrected, re-attempt backup.

5.4.11 Associated Operational Measurements or Performance Measurements

None.

5.4.12 Additional information

Not applicable.

Log Title/Log ID: Backup Manager: class_security.ver01**5.4.13 Formats****5.4.13.1 Securitylog**

Aug 30 11:24:15 znc0s0jh Backup Manager: class_security.ver01
STAT=FAILED SRC.USR=fred EVNT.TYPE =Authentication

5.4.14 Explanation

Description: Generated when a user attempts to invoke the Backup Manager and does not have the correct permissions.

5.4.15 Field descriptions

None.

5.4.16 Action

None.

5.4.17 Associated Operational Measurements or Performance Measurements

None.

5.4.18 Additional information

Not applicable.

5.5 Alarms

None.

5.6 Related documentation

6: A00007000 Fault Management (FM)

6.1 Document Name

GigE Network Interface

6.2 Fault management strategy

The standard MG9K EM Fault management strategy will apply to the new faults raised by this feature. Alarms will be displayed by the MG9K EM alarms browser, logged in NT standard format to the SSPFS cust logs and forwarded to northbound OSS and IEMS

“A00007000 - GIGE network Interface” feature introduces new faults.

6.3 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.

6.4 Logs

6.4.1 Formats

The Log Delivery application for this feature generates logs in the Number 2 Switch Control Center (SCC2) format and the NT standard (STD) format.

The log type for GIGE alarms will be ‘GIGE’ and the log ids will start from 301.

6.4.1.1 NTSTD

- **LossOfSignal**

GIGE 301 *** AUG 31 06:14:43 3409 TBL MG9K NorGigeLinkFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 204
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:39:05 1970

Component Id: Port.frame0.shelf3.slot10.Gige.Link01
 Specific Problem:norGigeLinkFault - Description: Loss of Signal
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **RemoteFailureIndication**

GIGE 302 *** AUG 31 06:14:43 3410 TBL MG9K NorGigeLinkFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 205
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:39:05 1970
 Component Id: Port.frame0.shelf3.slot10.Gige.Link01
 Specific Problem:norGigeLinkFault - Description: Remote Failure

Indication

Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **TxF**

GIGE 303 *** AUG 31 06:14:43 3411 TBL MG9K NorGigeLinkFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 206
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:39:05 1970
 Component Id: Port.frame0.shelf3.slot10.Gige.Link01
 Specific Problem:norGigeLinkFault -
 Description: Transmit Failure on GIGE link
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **TEM**

GIGE 304 * AUG 31 06:14:43 3412 TBL MG9K NorGigeLinkFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 270
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:39:05 1970
 Component Id: Port.frame0.shelf3.slot10.Gige.Link01
 Specific Problem:norGigeLinkFault -
 Description: Temperature threshold exceeded
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **POW**

GIGE 305 * AUG 31 06:14:43 3413 TBL MG9K NorGigeLinkFault

Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 271
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:39:05 1970
 Component Id: Port.frame0.shelf3.slot10.Gige.Link01
 Specific Problem:norGigeLinkFault -
 Description: Low Power Indicated
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **RxSD**

GIGE 306 * AUG 31 06:14:43 3413 TBL MG9K NorGigeLinkFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 283
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:39:05 1970
 Component Id: Port.frame0.shelf3.slot10.Gige.Link01
 Specific Problem:norGigeLinkFault -
 Description: Receive Signal Degraded
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **RxEER**

GIGE 307 * AUG 31 06:14:43 3413 TBL MG9K NorGigeLinkFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 284
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:39:05 1970
 Component Id: Port.frame0.shelf3.slot10.Gige.Link01
 Specific Problem:norGigeLinkFault -
 Description: Receive Excessive Error Ratio.
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **TBC**

GIGE 308 * AUG 31 06:14:43 3414 TBL MG9K NorGigeLinkFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 272
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:39:05 1970

Component Id: Port.frame0.shelf3.slot10.Gige.Link01

Specific Problem:norGigeLinkFault

Description: Transmit Bias Current

Site Flr RPos Bay_id

FFFF FF FFFF MG9F FFF

- **LINT**

GIGE 309 ** AUG 31 06:14:43 3415 TBL MG9K NorGigeLinkFault

Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01

Notification Id: 273

State: not acknowledged

Category: Communication Alarm

Cause: Communications Subsystem Failure

Time: Jan 01 05:39:05 1970

Component Id: Port.frame0.shelf3.slot10.Gige.Link01

SpecificProblem:norGigeLinkFault-Description:LinkInitialization

Site Flr RPos Bay_id

FFFF FF FFFF MG9F FFF

- **OPT**

GIGE 310 *** AUG 31 06:14:43 3416 TBL MG9K NorGigeLinkFault

Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01

Notification Id: 274

State: not acknowledged

Category: Communication Alarm

Cause: Communications Subsystem Failure

Time: Jan 01 05:39:05 1970

Component Id: Port.frame0.shelf3.slot10.Gige.Link01

Specific Problem:norGigeLinkFault -

Description: Transmit Optical Power

Site Flr RPos Bay_id

FFFF FF FFFF MG9F FFF

- **OPR**

GIGE 311 * AUG 31 06:14:43 3417 TBL MG9K NorGigeLinkFault

Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01

Notification Id: 275

State: not acknowledged

Category: Communication Alarm

Cause: Communications Subsystem Failure

Time: Jan 01 05:39:05 1970

Component Id: Port.frame0.shelf3.slot10.Gige.Link01

Specific Problem:norGigeLinkFault -

Description: Receive Optical Power

Site Flr RPos Bay_id

FFFF FF FFFF MG9F FFF

- **GARP**

GIGE 312 ** AUG 31 06:14:43 3418 TBL MG9K NorGigeLinkFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 276
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:39:05 1970
 Component Id: Port.frame0.shelf3.slot10.Gige.Link01
 Specific Problem:norGigeLinkFault - Description: GARP failure
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **LKINT**

GIGE 313 ** AUG 31 06:14:43 3420 TBL MG9K NorGigeLinkFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 278
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:39:05 1970
 Component Id: Port.frame0.shelf3.slot10.Gige.Link01
 Specific Problem:norGigeLinkFault -
 Description: Link Initialization Failure
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **AUTONEG**

GIGE 314 ** AUG 31 06:14:43 3421 TBL MG9K NorGigeLinkFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 279
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:39:05 1970
 Component Id: Port.frame0.shelf3.slot10.Gige.Link01
 Specific Problem:norGigeLinkFault -
 Description: Auto negotiation Failure
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **NONPREFLINK**

GIGE 315 ** AUG 31 06:14:43 3422 TBL MG9K NorGigeLinkFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 280
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:39:05 1970

Component Id: Port.frame0.shelf3.slot10.Gige.Link01

Specific Problem:norGigeLinkFault -

Description: Non Preferred Link is active

Site Flr RPos Bay_id

FFFF FF FFFF MG9F FFF

- **LINK INVALID STATUS**

GIGE 315 ** AUG 31 06:14:43 3422 TBL MG9K NorGigeLinkFault

Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01

Notification Id: 280

State: not acknowledged

Category: Communication Alarm

Cause: Communications Subsystem Failure

Time: Jan 01 05:39:05 1970

Component Id: Port.frame0.shelf3.slot10.Gige.Link01

Specific Problem:norGigeLinkFault -

Description: The link status is invalid

Site Flr RPos Bay_id

FFFF FF FFFF MG9F FFF

- **Network Fault**

GIGE 315 ** AUG 31 06:14:43 3422 TBL MG9K NorGigeLinkFault

Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01

Notification Id: 280

State: not acknowledged

Category: Communication Alarm

Cause: Communications Subsystem Failure

Time: Jan 01 05:39:05 1970

Component Id: Port.frame0.shelf3.slot10.Gige.Link01

Specific Problem:norGigeNetworkFault -

Description: Network Fault

6.4.1.2 SCC2

- **Loss of Signal**

*** GIGE 301 5915 TBL MG9K NorGigeLineFault

Location: 406-c406-FrameFFF.Shelf3.Slot10.Link01

Notification Id: 300

State: not acknowledged

Category: Communication Alarm

Cause: Communications Subsystem Failure

Time: Jan 01 05:54:38 1970

Component Id: Port.frame0.shelf3.slot10.OC3.Link01

Specific Problem: NorGigeLinkFault Description: Loss Of Signal

Site Flr RPos Bay_id

FFFF FF FFFF MG9F FFF

- **Remote Failure Indication**

*** GIGE 302 5915 TBL MG9K NorGigeLineFault

Location: 406-c406-FrameFFF.Shelf3.Slot10.Link01
Notification Id: 301
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:54:38 1970
Component Id: Port.frame0.shelf3.slot10.OC3.Link01
Specific Problem: NorGigeLinkFault
Description: Remote Failure Indication
Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF

- **TXF**

*** GIGE 303 5915 TBL MG9K NorGigeLineFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Link01
Notification Id: 208
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:54:38 1970
Component Id: Port.frame0.shelf3.slot10.OC3.Link01
Specific Problem: NorGigeLinkFault
Description: Transmit Failure on GIGE Link
Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF

- **TEM**

*** GIGE 304 5915 TBL MG9K NorGigeLineFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Link01
Notification Id: 209
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:54:38 1970
Component Id: Port.frame0.shelf3.slot10.OC3.Link01
Specific Problem: NorGigeLinkFault
Description: Temperature threshold exceeded
Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF

- **POW**

*** GIGE 305 5915 TBL MG9K NorGigeLineFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Link01
Notification Id: 210
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:54:38 1970

Component Id: Port.frame0.shelf3.slot10.OC3.Link01
 Specific Problem: NorGigeLinkFault
 Description: Low Power indicated
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **RxSD**

*** GIGE 306 5915 TBL MG9K NorGigeLineFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Link01
 Notification Id: 210
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:54:38 1970
 Component Id: Port.frame0.shelf3.slot10.OC3.Link01
 Specific Problem: NorGigeLinkFault
 Description: Receive Signal Degraded
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **RxEED**

*** GIGE 307 5915 TBL MG9K NorGigeLineFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Link01
 Notification Id: 210
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:54:38 1970
 Component Id: Port.frame0.shelf3.slot10.OC3.Link01
 Specific Problem: NorGigeLinkFault
 Description: Receive Excessive error ratio
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **TBC**

*** GIGE 308 5915 TBL MG9K NorGigeLineFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 300
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:54:38 1970
 Component Id: Port.frame0.shelf3.slot10.OC3.Link01
 Specific Problem: NorGigeLinkFault
 Description: Transmit Bias Current
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **LINT**

*** GIGE 309 5915 TBL MG9K NorGigeLineFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
Notification Id: 300
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:54:38 1970
Component Id: Port.frame0.shelf3.slot10.OC3.Link01
Specific Problem: NorGigeLinkFault Description: Link Initialization
Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF

- **OPT**

*** GIGE 310 5915 TBL MG9K NorGigeLineFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
Notification Id: 300
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:54:38 1970
Component Id: Port.frame0.shelf3.slot10.OC3.Link01
Specific Problem: NorGigeLinkFault
Description: Transmit Optical Power
Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF

- **OPR**

*** GIGE 311 5915 TBL MG9K NorGigeLineFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
Notification Id: 300
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:54:38 1970
Component Id: Port.frame0.shelf3.slot10.OC3.Link01
Specific Problem: NorGigeLinkFault
Description: Receive Optical Power
Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF

- **GARP**

*** GIGE 312 5915 TBL MG9K NorGigeLineFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
Notification Id: 300
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:54:38 1970

Component Id: Port.frame0.shelf3.slot10.OC3.Link01
 Specific Problem: NorGigeLinkFault Description: GARP Failure
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **LKINT**

*** GIGE 313 5915 TBL MG9K NorGigeLineFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 300
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:54:38 1970
 Component Id: Port.frame0.shelf3.slot10.OC3.Link01
 Specific Problem: NorGigeLinkFault Description: Link Integrity Failure
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **AUTONEG**

*** GIGE 314 5915 TBL MG9K NorGigeLineFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 300
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:54:38 1970
 Component Id: Port.frame0.shelf3.slot10.OC3.Link01
 Specific Problem: NorGigeLinkFault
 Description: Auto negotiation Failure
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **NONPREFLINK**

*** GIGE 315 5915 TBL MG9K NorGigeLineFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
 Notification Id: 300
 State: not acknowledged
 Category: Communication Alarm
 Cause: Communications Subsystem Failure
 Time: Jan 01 05:54:38 1970
 Component Id: Port.frame0.shelf3.slot10.OC3.Link01
 Specific Problem: NorGigeLinkFault
 Description: Non Preferred link is active
 Site Flr RPos Bay_id
 FFFF FF FFFF MG9F FFF

- **LINK INVALID STATUS**

*** GIGE 315 5915 TBL MG9K NorGigeLineFault
 Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01

Notification Id: 300
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:54:38 1970
Component Id: Port.frame0.shelf3.slot10.OC3.Link01
Specific Problem: NorGigeLinkFault
Description: The Link Status is invalid
Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF

- **NETWORK FAULT**

*** GIGE 315 5915 TBL MG9K NorGigeLineFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Link01
Notification Id: 300
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:54:38 1970
Component Id: Port.frame0.shelf3.slot10.OC3.Link01
Specific Problem: NorGigeNetworkFault
Description: Network Fault
Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF

6.5 Alarms

The new alarms introduced in this feature are

1. LOS

- Alarm Format: - 301 LOS
- Associated alarm message - Loss of Signal
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an LOS with faultdefinition - clear is received.

2. RFI

- Alarm Format: - 302 RFI
- Associated alarm message - Remote Failure Indication
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an RFI with faultdefinition - clear is received.

3. TxF

- Alarm Format: - 303 TxF
- Associated alarm message - Transmit Failure
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an TxF with faultdefinition - clear is received.

4. TEM

- Alarm Format: - 304 TEM
- Associated alarm message - Temperature Threshold Exceeded
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an TEM with faultdefinition - clear is received.

5. POW

- Alarm Format: - 305 POW
- Associated alarm message - Low power indicated
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an POW with faultdefinition - clear is received.

6. RxSD

- Alarm Format: - 306 RxSD
- Associated alarm message - Receive Signal Degraded
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an POW with faultdefinition - clear is received.

7. RxEED

- Alarm Format: - 307 RxEED
- Associated alarm message - Receive Excessive Error Ratio
- Severity: Critical
- Cause: Network Problem

- Action: This alarm will be cleared when an RxEED with faultdefinition - clear is received.

8. TBC

- Alarm Format: - 308 TBC
- Associated alarm message - Transmit Bias Current
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an TBC with faultdefinition - clear is received.

9. LINT

- Alarm Format: - 309 LINT
- Associated alarm message - Link initialization
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an LINT with faultdefinition - clear is received.

10. OPT

- Alarm Format: - 310 OPT
- Associated alarm message - Transmit Optical Power
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an OPT with faultdefinition - clear is received.

11. OPR

- Alarm Format: - 311 OPR
- Associated alarm message - Receive Optical Power
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an OPR with faultdefinition - clear is received.

12. GARP

- Alarm Format: - 312 GARP
- Associated alarm message - GARP Failure
- Severity: Critical

-
- Cause: Network Problem
 - Action: This alarm will be cleared when an GARP with faultdefinition - clear is received.

13. LKINT

- Alarm Format: - 313 LKINT
- Associated alarm message - Link Integrity Failure
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an LKINT with faultdefinition - clear is received.

14. AUTONEG

- Alarm Format: - 314 AUTONEG
- Associated alarm message - Auto Negotiation Failure
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an AUTONEG with faultdefinition - clear is received.

15. NONPREFLINK

- Alarm Format: - 315 NONPREFLINK
- Associated alarm message - Non Preferred Link is active
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an NONPREFLINK with faultdefinition - clear is received.

16. LINKINVALIDSTATUS

- Alarm Format: - 316 LINKINVALIDSTATUS
- Associated alarm message - The link status is invalid
- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an NONPREFLINK with faultdefinition - clear is received.

17. NETWORK FAULT

- Alarm Format: - 317 NETWORK FAULT
- Associated alarm message - Network Fault

- Severity: Critical
- Cause: Network Problem
- Action: This alarm will be cleared when an NONPREFLINK with faultdefinition - clear is received.

6.6 Related documentation

NONE

7: A00007071 Fault Management (FM)

7.1 Document Name

SN08 3rd Party GW Interop Profiles

7.2 Fault management strategy

This activity is responsible for providing a flexible system that allows users to define Gateway (GW) profiles without making software updates. To this end, a certificate (XML document) polling strategy is being developed that will scan the SSPFS file system for new or removed certificates. With this strategy, the potential for error situations arise, and need to be handled without using an interactive interface. Therefore, this activity will amend the alarm system to include new alarms that are related to the importation and removal of certificates (profiles). The alarms are triggered from functionality included in the GWCEM part of the CMT.

The following conditions require amendments to the alarm system:

- Syntax errors are encountered when a new certificate is polled
- Field incompatibility problems are present when a new certificate is polled
- A certificate is deleted and GWs exist that are still using this profile

7.3 Fault management tools and utilities

There are two CMT alarm GUIs. One shows active alarms on the managed devices and the other shows the alarm history. This activity will update alarms associated with the GWCEM Network Element.

7.4 Alarms

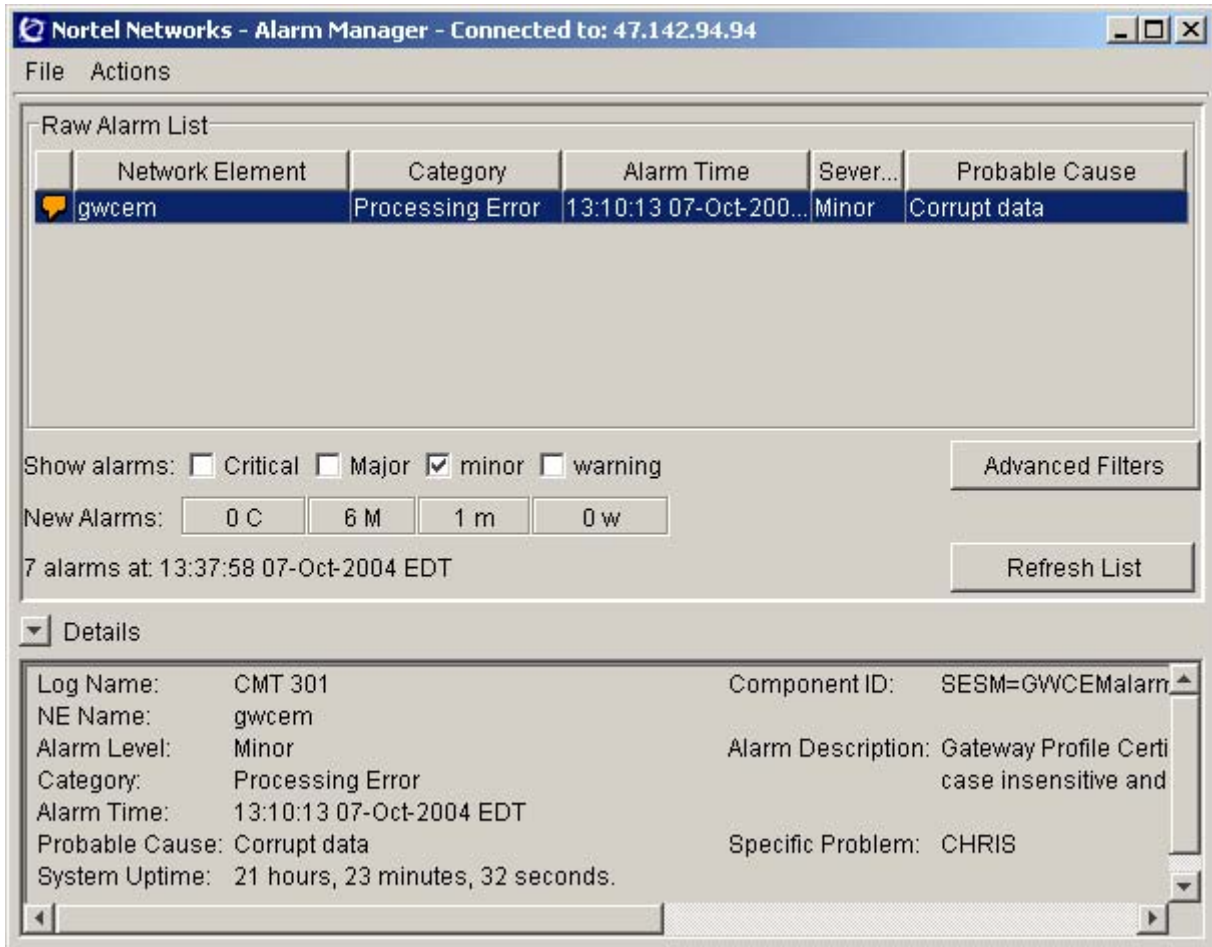
At least two new alarms will be introduced with the introduction of this feature. The following properties are included:

- Network Element: gwcem
- Category: Processing Error
- Severity: Minor
- Probable Cause: Certificate corruption
- Duration: Remains active until the alarm condition is cleared
- Action for new certificate: Replace the certificate with a new version without syntax or content problems
- Action for deleted certificate: Remove GWs that use the deleted certificate or replace deleted certificate
- Interfaces: This alarm is generated by the certificate poller on the CMT

7.4.1 GWCEM Certificate Alarms

An example of a GWCEM Certificate Alarm is listed below. This alarm is realized when an issue is discovered that is related to a problem with a Certificate or existing Profile.

Figure 1 Example of a GWCEM Certificate Alarm Body



7.4.1.1 Corrupt Certificate Alarm

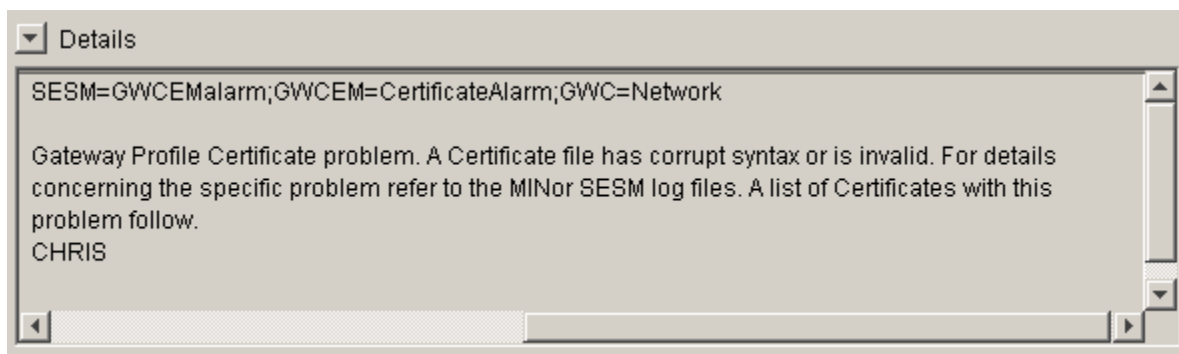
A Corrupt Certificate Alarm is realized when the syntax error is recognized in a Certificate. Certificate syntax must conform to rules enforced by the XML schema. This schema is located in the /opt/nortel/NTsesm/xsd/certificateIf directory and should be used as a guideline for certificate creation. If the rules for creating a certificate are violated then a Corrupt Alarm is raised.

In addition to syntax, some rules have been built into software that disallow combinations of some fields. In general, only blatantly incorrect combinations are tagged and it is the responsibility of the Certificate creator to define valid Certificates. However, some combinations will cause Corrupt Alarms to be generated.

7.4.1.1.1 Clearing a Corrupt Alarm

A Corrupt Alarm is cleared by updating the Certificate file so that the problem listed is no longer present. In addition, Certificate files that have not been successfully imported into the system can be removed without realizing additional alarms.

Figure 2 GWCEM Corrupt Certificate Alarm Detail



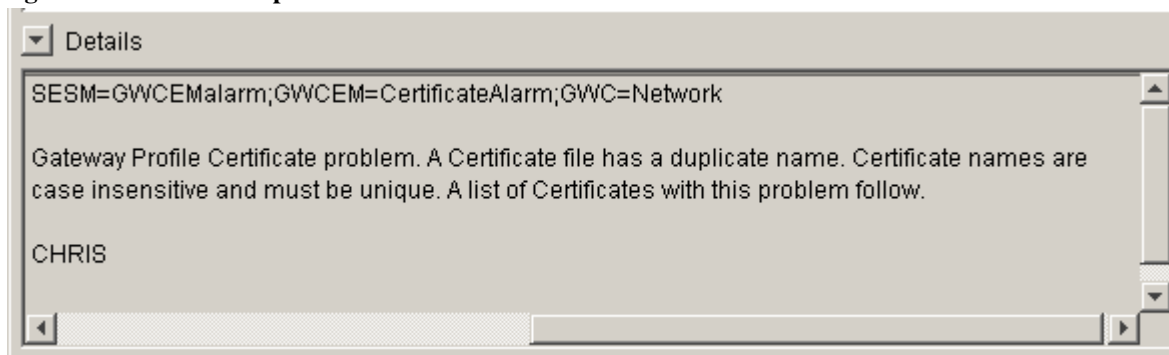
7.4.1.2 Duplicate Certificate Alarm

A Duplicate Certificate Alarm is realized when more than one Certificate with the same name is detected in the Nortel or Third Party certificate directories. Duplicating a certificate name is not allowed. Certificate names are case insensitive so the name XYZ.certificate is treated as a duplicate of the name xyz.certificate. In addition, duplicates span both the Nortel and the Third Party directories. Therefore, the XYZ.certificate can not co-exist in both the Nortel and Third Party directories.

7.4.1.2.1 Clearing a Duplicate Alarm

A Duplicate Alarm is cleared by simply removing the Certificate file that caused the duplication.

Figure 3 GWCEM Duplicate Certificate Alarm Detail



7.4.1.3 Delete Certificate Alarm

Third Party Certificates/Profiles can be removed from the system by removing the associated Certificate File. If a Certificate file is removed that has GWs

associated with it a Delete Alarm is raised. For this case, the corresponding profile is not removed from the system.

7.4.1.3.1 Clearing a Delete Alarm

A Delete Certificate Alarm is cleared by replacing the Certificate file. In addition, all of the GWs can be removed for the system that are associated with the Certificate and the alarm will be cleared. This action will also remove the Certificate.

Figure 4 GWCEM Delete Certificate Alarm



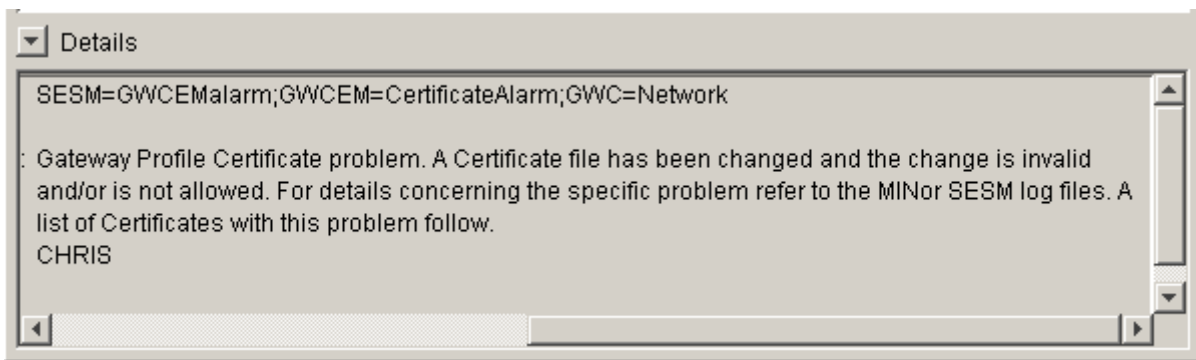
7.4.1.4 Certificate Changed Alarm

A Change Certificate Alarm is realized when an existing profile is changed and one or more of the fields that are changed are not allowed.

7.4.1.4.1 Clearing a Changed Alarm

A Changed Alarm is cleared by replacing the field that has been changed to the original value.

Figure 5 GWCEM Changed Certificate Alarm Detail



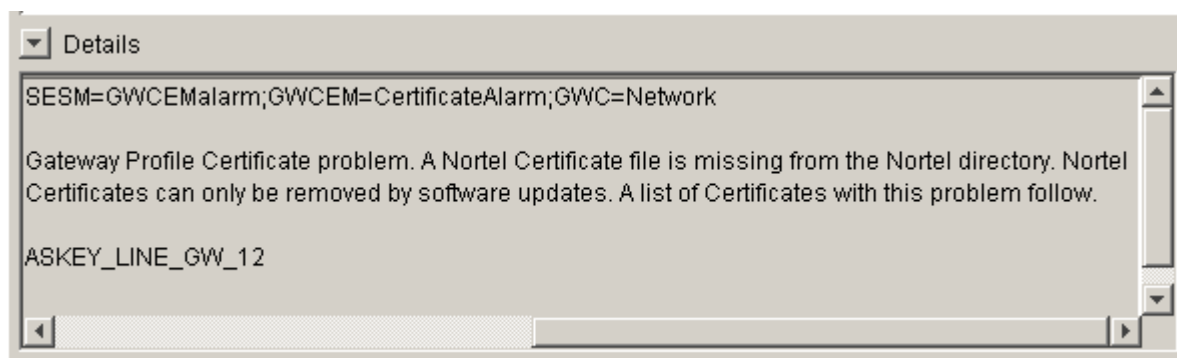
7.4.1.5 Missing Certificate Alarm

A Missing Certificate Alarm is realized when a Nortel Certificate has been removed from the Nortel directory or changed to a different name. Software updates are the only supported means to alter or remove Nortel Certificates.

7.4.1.5.1 Clearing a Missing Alarm

A Missing Alarm is cleared by replacing the Nortel Certificate that was removed.

Figure 6 GWCEM Missing Certificate Alarm Details



7.5 Logs

MI2 Logs are affected by this activity for two of the alarms listed above. Corrupt alarms and Changed alarms list additional detail when the Minor (MNR) alarms logging level is set. The alarms are raised when the syntax or settings of a certificate is incorrect. In addition, when an invalid change is made to a certificate one of these alarms may be realized. For these cases, addition information is listed with detailed information concerning the nature of the problem. An example of this condition follows:

```
04.10.07 13:55:25.903 MNR (EM) [Thread-25] *** CERTIFICATE
CORRUPT ALARM *** - Profile name = CISCO_2600
```

```
04.10.07 13:55:25.905 MNR (EM) [Thread-25] The problem is: Element type
"MxEndpoints" must be declared.
```

As previously mentioned, details concerning the “corrupt and changed” certificate alarms are listed in the CMT minor (MNR) log files. These files can be viewed at the following location “/opt/nortel/NTsesm/admin/logs/ptmdebuglog1.mi2.

Restricting the logs to list MNR and above logs only can be accomplished using the MI2Admin tool. This tool is located in the /opt/nortel/NTsesm/bin directory.

7.6 Related documentation

- <http://ptm->Documentation->SN06->AlarmLoggingDSUM.doc>
- <http://ptm->Documentation->SN08->Third Party Interop FN>
- <http://ptm->Documentation->SN08->Third Party Interop CN>

8: A00007074 Fault Management (FM)

8.1 Document Name

GigE Link Maintenance

8.1 Fault management strategy

Currently the GigE interfaces uses a 1+1 protection group redundancy model. A link is provisioned on each of the SGC cards into a protection group. When a service affecting fault is detected on the active link the SGC cards will be spared if possible to gain service on the other link. Crossovers are not supported so the link and card activity match.

8.2 Fault management tools and utilities

The EM and LCI provide an interface for viewing the faults currently and historically on an interface. Tools are provided fault isolation including traceroute. The link integrity test is available to provide information and isolation of faults both within the NE and the connected network.

8.3 Logs

Logs are generated for threshold crossings that occur and system errors. Logs are sent through the EM to the log stream. The log stream can then be monitored for craft to take appropriate action including contacting Nortel Networks for analysis.

The format is detailed in A00007000, GigE EM.

8.4 Alarms

The following alarms and recovery actions can occur:

Table 16: GigE alarms

Alarm	Severity	Description	System Action	Craft Action
LOS	Critical	Loss of signal	Spare	None
RFI	Critical	Remote fault indication	Spare	None
TXF	Critical	Transmit failure	Spare	None
AutoNeg	Critical	Autonegotiation failed	Spare	None

Table 16: GigE alarms

Alarm	Severity	Description	System Action	Craft Action
RxEER	Major	Receive excessive errors	Spare	None
LINT	Link Integrity	failure of one link to communicate	Spare if active link	None
LKINT	Major	external failure for link integrity	None	isolate fault hosting network
TEM	Minor	Temperature	None	replace card
POW	Minor	Power	None	replace card
RxSD	Minor	Receive signal degraded	None	isolate path introducing errors
TBC	Minor	Bias Current	None	replace card
OPT	Minor	Optical transmit	None	replace card
OPR	Minor	Optical receive	None	replace far end equipment
NONPRE-FLINK	Minor	active link is not the preferred link	None	isolate and recover fault on the preferred link

The format is detailed in A00007000, GigE EM.

8.5 Related documentation

Feature A00007000 FM.

9: A00007102 Fault Management (FM)

9.1 Document Name

Dual C-Side IP for GWC

9.2 Fault management strategy

No change.

9.3 Fault management tools and utilities

There are two CMT alarm GUIs. One shows active alarms on the managed devices and the other shows the alarm history. This activity will update alarms associated with the GWCEM.

9.4 Logs

An automatically generated customer log on raising an alarm will be provided. No other log will be implemented in this feature.

In this feature, the new alarm “No Available Call Server IP” will be added, a corresponding customer log when the alarm is raised/cleared will be automatically generated. The log file is “/var/log/customerlog”.

9.4.1 Formats

The **log header** will be organized as in the following format:

Report name: CMT

Report number:303

Priority:Critical

Event:TBL

Device ID:CMT

Label: Fault

Application name:CS2K Config Manager

The **log body** will be organized as in the following format:

<Location> <NotificationID> <State> <Category> <Cause> <Time>
<Component Id> <Specific Problem> <Description>

Please refer to Table 1, “Log Body Fields for STM 801 (Raise),” on page 1187 for log body field details.

9.4.1.1 NTSTD

9.4.1.2 SCC2

9.4.1.3 Syslog

Oct 6 11:03:31 wnc0s0r3 java[8665]:
 V2~I=CMT~H=wnc0s0r3~A=SESM~S=0014~~ CMT303 CRIT TBL
 CMT Fault^M Location: CS2K Config Manager^M NotificationID:
 5073690^M State: Raise^M Category: Environment^M Cause:
 Configuration or customization error^M Time: Oct 06 11:03:31 2004^M
 Component Id:
 SESM=Cs2kCfgMgr;Cs2kCfgMgr=NoAvailableCallServerIP^M Specific
 Problem: Communication problem between SESM and Core. Or Call S^M
 erver IP address was not properly filled in Core table <CMIPADDR/
 IPNETWR^M K>^M Description: Cannot get available Call Server
 IP address from Core.^M

9.4.1.4 SNMP

Table 1 Log Body Fields for STM 801 (Raise)

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Specific Problem:	Y	No available Call Agent IP address filled in Core table <TABLE NAME>	variable	variable text
Description:	Y	SESM can not get available Call Agent IP from Core, this information is necessary for every GWC.	variable	variable text detailing problem
Fabric	N			
Frame Location	N			

9.4.1.5 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).

Table 2

Field	Value
Category	Environment
Severity	Critical
LogName	CMT
LogNumber	303
EventType	TBL
EventLabel	Fault
ProbableCause	Configuration or customization error
SpecificProblem	Communication problem between SESM and Core. Or Call Agent IP address was not properly filled in Core table <CMIPADDR/IPNETWRK>
BodyText	Cannot get available Call Agent IP address from Core.

9.4.2 Explanation

:This log is automatically generated when the alarm “No Available Call Agent IP” is raised. It is a critical log, which indicates there is no available Call Agent IP address can be retrieved from Core. This problem will impacts all provisioned GWCs in the system.

9.4.3 Field descriptions

9.4.4 Action

Action is required to properly fill the Core table manually (table CMIPADDR on the Xa-Core or table IPNETWRK on the Compact Core).

9.4.5 Associated Operational Measurements or Performance Measurements

9.4.6 Additional information

9.5 Alarms

One new alarm “No Available Call Server IP” will be raised if the SESM cannot get any available C-Side IP address from the Core.

9.5.1 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:No Call Server IP was filled in the Core table <Table Name>.

Description:SESM cannot get available the Call Server IP address information from the Core. This information is necessary for every GWC.

9.5.2 Cause or condition

This scenario will happen if no C-Side IP address was filled in the table CMIPADDR on the XA-Core or table IPNETWRK on the Compact Core.

9.5.3 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

Field	Value
Severity	Critical
Category	Environment
LogName	CMT
LogNumber	303
EventType	TBL
EventLabel	Fault
ProbableCause	Configuration or customization error
SpecificProblem	Communication problem between SESM and the Core. Or Call Agent IP address was not properly filled in the Core table <CMIPADDR/IPNETWRK>
BodyText	Cannot get the available Call Agent IP address from the Core.

9.5.4 SNMP Northbound Alarm Event (Non-legacy logs only)

Not applicable for this feature.

9.5.5 Explanation

Description: SESM cannot get available Call Server IP information from the Core, this information is necessary for every GWC, the reason is that no Call Server IP information was filled in the Core table.

Severity: the severity level of this new alarm is Critical.

9.5.6 Action

Action is required to properly fill the Core table manually (table CMIPADDR on the Xa-Core or table IPNETWRK on the Compact Core). SESM will check the table periodically every 5 minutes. Once SESM can get at least one available Call Server IP address from the Core table, this alarm will be cleared.

9.5.7 Corresponding Clear Log

Log Title: CMT-303

9.5.7.1 Format

WNC0S0R3 CMT303 Oct 06 11:08:10 2004 0024 TBL

Location: CS2K Config Manager

Notification Id: 5073690

State: Cleared

Time: Oct 06 11:08:10 2004

9.5.7.2 NTSTD**9.5.7.3 SCC2****9.5.7.4 Syslog**

Oct 6 11:08:10 wnc0s0r3 java[8665]:

V2~I=CMT~H=wnc0s0r3~A=SESM~S=0024~~ CMT303 CRIT TBL

CMT Fault^M Location: CS2K Config Manager^M NotificationID:

5073690^M State: Clear^M Time: Oct 06 11:08:10 2004

9.5.7.5 SNMP

Not applicable for this feature.

9.6 Related documentation

10: A00007113 Fault Management (FM)

10.1 Document Name

GWC External Interface Robustness

10.2 Fault management strategy

The **GWC External Interface Robustness** feature provides improved fault management for existing Gateway Controller (GWC) components. The strategy for this feature is covered by two aspects: Collecting Operational Measurements (OMs) with error counters, and raising alarms based on the error counters.

10.3 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.

The SESM Alarm manager on the SSPFS is used to display the GWC alarms and log alarms history. Alarms can be filtered for display purposes, based on the alarm severity field.

The Operational Measurements will be collected by IEMS polling covered in feature ACTID A00007388.

10.4 Alarms

10.4.1 External Host Interface Signal Loss

Category: Communication

Description: External Communication Interface

Severity: Based on number of Elements involved and the number of elements with a signal loss collected with a 5 minute poll.

- Critical - Over 50% signal loss
- Major - Over 20 % signal loss
- Minor - Any signal loss

Cause: Signal Loss.

Interface or Specific Problem: This field provides the external host type.

- “Small GWs in Disabled State”

This alarm is based on the number of gateways that are out of service as compared to the number of gateways provisioned checked on a 5 minute polling period. Therefore, with very few gateways provisioned, few gateways out of service will have a more significant effect on call processing. Gateways are considered out of service when the heartbeat messages between the GWC and the gateway are lost.

Customer logs are sent as each small lines gateway goes out of service and when it comes back in service. The customer should you the alarm as an indication that there is a problem with the small lines gateways. It can use the new OM collected to see how many small lines gateways are out of service and then use the customer logs to identify the gateways that need attention.

- “USP SS7 paths disabled”

This alarm is based on the number of USP connections that are out of service as compared to the number of maximum paths of 2 checked on a 5 minute polling period. The link paths are considered out of service when the heartbeat messages between the GWC and the USP are lost.

The customer should you the alarm as an indication that there is a problem with the USP connections. A Major alarm is raised when both links are down while a minor alarm is raised if only one link is down. Since not all calls require SS7 signaling, this messaging path does not raise any critical alarms.

- “Peer connections failed during interval”

This alarm is based on the number of call setups failed as compared to the number of calls attempted in a 5 minute polling period. In this case as the number of calls is increased, the number of failed calls is not as significant for the alarm.

The customer should view this alarm as an indication of a problem with calls and look at the new Peer Communications OMs to see the number of calls failed over a longer period.

Action: Verify the Ethernet link to between the GWC and the remote host or Peer GWCs.

10.4.2 External Host Interface Configuration Error

Category: Quality of Service

Description: External Communication Interface

Severity: Non service effecting errors are warning alarms.

Cause: Configuration Or Customization Error.

Interface or Specific Problem: This field provides the external host type.

- “DNS failed GW discovery”

This alarm is based on the number of gateways that failed DNS lookup. This alarm is based on a 5 minute polling period. The new DNS OMs can be used to see the number of gateways that are not discovered and also the number of gateways that were discovered using RSIP. Note that RSIP discovery does not survive a Cold Swact on the GWC, which may result in long outages for the customer.

Action: Verify the DNS server entries for ever gateway.

10.4.3 External Host Interface Protocol Error

Category: Communication

Description: External Communication Interface

Severity: Based on service effecting.

- Major - effects some callp service.
- Minor - redundancy error.

Cause: Communications Protocol Error.

Interface or Specific Problem: This field provides the external host type.

- “USP SS7 path not Active”

This alarm is based on the number of USP connections that are not active but do have heartbeat messages checked on a 5 minute polling period. Therefore this is a protocol error with USP.

The customer should you the alarm as an indication that there is a problem with the USP connections. A Major alarm is raised when both links are not active while a minor alarm is raised if only one link is not active.

Action: Verify the USP configuration to the GWC.

10.5 Operational Measurements or Performance Measurements

Every new alarm in this feature will have associated measurements that will be reported using the performance MIB. The Specific problem field in the alarm is also the name of the metric that will be reported. The relationship between alarms and performance metrics are as follows:

The Alarm Category will be used as the Group in the performance metric.

- Measurement

- Communication
- Quality of Service

The alarm Interface or Specific Problem will be used as the name for the metric.

Table 1 Performance Measurements Metrics

name	Group	Source	Type
"Small GWs in Disabled State"	communication	multi	COUNTER_32
"Large GWs in Disabled State"	communication	multi	COUNTER_32
"Trunk GWs in Disabled State"	communication	multi	COUNTER_32
"Audio GWs in Disabled State"	communication	multi	COUNTER_32
"Total Gateways Provisioned"	measurement	multi	COUNTER_32
"DNS failed GW discovery"	quality of service	multi	COUNTER_32
"DNS good GW discovery"	measurement	multi	COUNTER_32
"RSIP used in GW discovery"	quality off service	multi	COUNTER_32
"Total DNS GWs to discover"	measurement	multi	COUNTER_32
"USP SS7 paths disabled"	communication	multi	COUNTER_32
"USP SS7 path not Active"	communication	multi	COUNTER_32
"Peer connections failed during interval"	communication	multi	COUNTER_32
"Peer connections completed during interval"	communication	multi	COUNTER_32
"Peer connections attempted during interval"	measurement	multi	COUNTER_32

11: A00007213 Fault Management (FM)

11.1 Document Name

MG9000 5/30 Minutes OMs

11.2 Fault management strategy

This feature uses the existing MG9KEM Fault management framework to raise and clear alarms.

11.3 Fault management tools and utilities

NA

11.4 Logs

11.4.1 Log Title/Log ID: OMC300

11.4.1.1 Formats

MSH10_I06BR *** OMC300 JUN20 15:29:20 4642 TBL OMDataCollectionFailed

Location: 1-RM9K

Notification Id:1000

State: not acknowledged

Category: Communication Alarm

Cause: Communications Subsystem Failure

Time: Jun 20 15:29:20 2003

Component Id: MG9k EM Comm Network

Specific Problem: OM data collection failed

Description:

Site Flr RPos Bay_id

FFFF FF FFF FFFF FFF

11.4.1.2 Explanation

Description: Log report OMC300 indicates that OM Collector failed to collect OM file from MG9K during a particular collection interval.

11.4.1.3 Field descriptions

Table 1: Field descriptions

Field	Value	Description
event type	TBL	Describes event type
event id	string	Log name. In this case, it is OMC300
Location	NE Number-NE Name	Gives a complete location of the originator
Notification Id	Alarm if	
State	string	Indicates state of alarm. Can be one of {not acknowledged, acknowledged, cleared}
Category	string	Indicates type of fault. In this case it is "Communication Alarm"
Cause	string	Cause of failure: In this case it is "Communications Subsystem Failure"
Time		Date/Time indicating when the condition occurred
Component Id	string	Indicates the type of equipment having the fault.
Specific Problem	string	Indicates the specific problem that caused the fault
Description	string	Provides specific text for the fault. In this case, it consists of Frame location information.

11.4.1.4 Action

Check the following

- whether MG9K is traffic overloaded.

11.4.1.5 Associated Operational Measurements or Performance Measurements

None

11.4.1.6 Additional information

Following is a list of reasons for the generation of the log report OMC300.

- MG9K is traffic overloaded
- Disk may be full. Hence, the OM Collector is not able to store the downloaded OM file.
- Gateway user id and password mentioned may be wrong
- OM file details mentioned in the SFTP request may be wrong

11.4.2 Log Title/Log ID: OMC300

11.4.2.1 Formats

MSH10_I06BE OMC300 APR23 08:50:10 5176 INFO OM Collection failed
Alarm Cleared

Location: 1-RM9K (Act)

Description: OM collection failed alarm cleared.

11.4.2.2 Explanation

Description: Log report OMC300 indicates that OM Collector could restart collecting OM file from MG9K, for which it had problem.

11.4.2.3 Field descriptions

Table 2: Field descriptions

Field	Value	Description
event type	INFO	Describes event type
event id	string	Log name. In this case, it is OMC300
Location	NE Number-NE Name	Gives a complete location of the originator
Description	string	Provides specific text for the fault

11.4.2.4 Action

This log report requires no action.

11.4.2.5 Associated Operational Measurements or Performance Measurements

None

11.4.2.6 Additional information

None

11.5 Alarms

11.5.1 Integrated Element Manager GUI Fields

Table 3: IEMS Alarm GUI Field descriptions

Field	Value
Severity	Minor
Category	Communication Alarm
LogName	OMC
LogNumber	300
EventType	TBL
EventLabel	TBD
ProbableCause	Communications Subsystem Failure
SpecificProblem	OM data collection failed
BodyText	Site Flr RPos Bay_id FFFF FF FFF FFFF FFF

11.5.2 SNMP Northbound Alarm Event (Non-legacy logs only)

NA (Alarm raised for this feature are EM specific)

11.5.3 Explanation

Description: OM Collector could not collect OM file for a particular NE for a particular collection interval. Severity: Minor

11.5.4 Action

Check the following

- whether MG9K is traffic overloaded.

11.5.5 Corresponding Clear Log

Log Title: **OMC300**

11.5.5.1 Format

MSH10_I06BE OMC300 APR23 08:50:10 5176 INFO OM Collection
failed Alarm Cleared
Location: 1-RM9K (Act)
Notification Id: 1000
State: Cleared

Description: OM collection failed alarm cleared.

11.5.5.2 NTSTD

MSH10_I06BE OMC300 APR23 08:50:10 5176 INFO

Location: 1-RM9K

Notification Id: 1000

State: Cleared

Time: APR23 08:50:10 2004

11.5.5.3 SCC2

19 OMC 300 5176 INFO

Location: 1-RM9K

Notification Id: 1000

State: Cleared

Time: APR23 08:50:10 2004

11.5.5.4 Syslog

Feb 24 19:19:43 wnc0s0pf IEMS:

V2~I=~H=wnc0s0pf~A=IEMS~S=0618~~ OMC300 NONE INFO ^M

Location: 47.166.56.10^M Notification Id: 13^M State: Cleared^M

Time: Jan 24 19:19:49 2004

11.5.5.5 SNMP

NA (since, these alarm are originated from EM)

11.6 Related documentation

[1] A00007213 FN

12: A00007243 Fault Management (FM)

12.1 Document Name

Prevent Outage when CEM flash has not been erased

12.2 Fault management strategy

Feature Name: A00007243 - *Prevent Outage when CEM flash has not been erased*, uses Logs to report MAC mismatches on a CEM CPK in MG4K SPM. MAC mismatch detects difference between the MAC address datafilled in table MNCKTPAK and the actual MAC address of the physical card.

Note that this feature is applicable only for the MG4K SPMs. No new Logs are introduced by this feature. Existing SPM313, NODE300 logs are modified to report the MAC mismatch. INM959 is modified to report the unexpected Snego reply on CEM.

12.3 Fault management tools and utilities

Not Applicable.

12.4 Logs: SPM313

Log Title/Log ID: SPM313

12.4.1 Formats

The Format for the SPM 313 log is as shown below in the example. This feature adds new Reason for the MAC address mismatch but format of the log is not changed.

Figure 1 SPM 313 log for MAC mismatch

```
<switch_name> ** SPM313 AUG07 03:31:07 9500 TBL Fault
SPM 5 CEM 1 : I Time: 03:31:07.525
Source: None State: Insv Type: None
Reason: CPK MAC address doesn't match prov.data.
Diagnostic: Autonomous fault detection
Comp:MCM RegAddr:0 Exp:0 Act:0
```

12.4.2 Explanation

Description: SPM313 log is generated, when TBL fault is detected. MAC mismatch is type of TBL fault, hence SPM313 will be generated when MAC mismatch is detected. SPM shows a Non-Critical fault. QueryPM flt reason

command can be used to query the faults on SPM. SPM313 is part of TBL event reporting. Log reason reports mismatch trouble on the CEM CPK.

SPM313 log shall be generated periodically till the MAC mismatch is corrected by craft by changing table MNCKTPAK datafill. It shall display the actual CEM MAC address.

12.4.3 Action

Craft has to check the TBL reason and take corrective action. In this case change the MAC datafill in table MNCKTPAK to match with that on the physical card. The steps to change MAC address in table MNCKTPAK are mentioned in NTP document - **NN10076-911 Title: MG4000 Fault Management.**

12.4.4 Associated Operational Measurements or Performance Measurements

None.

12.4.5 Additional information

None.

12.5 Alarms

Not Applicable.

12.6 Related documentation

- a. *NN10076-911 Title: MG4000 Fault Management Ver:6.2* (NTP document for replacing CEM card in MG4K node)

13: A00007270 Fault Management (FM)

13.1 Document Name

Session Server Call Processing Overload Controls

13.2 Fault management strategy

Not applicable.

13.3 Overload Controls Logs and Alarms

The following is a description of logs and alarms that are generated by the SIP Gateway Call Processing Application in regards to the Overload Controls Feature. These logs and Alarms can be viewed via the SIP Gateway Maintenance web browser interface on the Session Server - SIP Gateway application web page.

Note that these logs and alarms are only generated and reported on the SIP Gateway Application.

13.3.1 SIP Gateway Call Processing Application Logs

Following are the two customer logs that will be generated by this feature:

- SIPC310 - SIP CallP Overload Threshold Reached
- SIPC310 - SIP CallP Overload Cleared

13.3.1.1 SIPC310 SIP CallP Overload Threshold Reached

Log SIPC310 “SIP CallP Overload Threshold Reached” is associated with the generation of the Major alarm due to reaching a predefined threshold in call processing capacity

Log Title: SIP CallP

Name: SIPC310

Description: Overload Threshold Reached

Event Type: Trouble

FORMAT: For the SIPC310 log, the following are values/explanations of the variable values:

- alarmLevel = MAJ/MIN- Indicates a major alarm
- componentID = SIPC
- category = Communications
- description = Overload Threshold Reached

-
- probable cause = System overloaded
 - specific cause =
 - correlationIdList = None
 - neVendorSpecificInfo = None
 - technologySpecificInfo = None
 - reportName = SIPC
 - reportNum= 310
 - eventType = TBL
 - label = SIP CallP

ACTION: Monitor the network

13.3.1.2 SIPC310 SIP CallP Overload Cleared

Log SIPC310 “SIP CallP Overload Cleared” is generated when the SIP Gateway Application is no longer in Overload.

Log Title: SIP CallP

Name: SIPC310

Description: Overload Cleared

Event Type: Trouble

FORMAT: For the SIPC310 log, the following are values/explanations of the variable values:

- alarmLevel = None
- componentID = SIPC
- category = Communications
- description = Overload Threshold Cleared
- probable cause =
- specific cause =
- correlationIdList = None
- neVendorSpecificInfo = None
- technologySpecificInfo = None
- reportName = SIPC
- reportNum= 310
- eventType = TBL

- label = SIP CallP

ACTION: None

14: A00007271 Fault Management (FM)

14.1 Document Name

TOPS EOL for SN08

14.2 Fault management strategy

Not applicable.

14.3 Fault management tools and utilities

Not applicable.

14.4 Logs

Log Title/Log ID: TEOL100

The TEOL100 log was added in CSP12 and patched back to CSP09. This feature merely adds a potential new line to the existing log.

14.4.1 Format

If OSSAIN MIS is used during a week, a TEOL100 log will be generated at midnight the following Sunday with the “OSSAIN MIS” functionality listed (other functionalities may also be listed). For example:

TEOL100 mmmdd hh:mm:ss ssdd INFO TOPS End Of Life Notification
Use of functionality scheduled for removal:

Functionality Used	Scheduled Removal
-----	-----
OSSAIN MIS	SN10

14.4.2 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 TEOL100 log.

14.4.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
Functionality Used	OSSAIN MIS	This field identifies the functionality that is scheduled for removal yet is being used.
Scheduled Removal	SN10	This field identifies the release in which the functionality is scheduled to be removed.

14.4.4 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.

14.4.5 Associated Operational Measurements or Performance Measurements

Unchanged.

14.4.6 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 usage), nor does it indicate the number of times it was used.

14.5 Alarms

Not Applicable.

14.6 Related documentation

A59036888 - TOPS EOL Succession Baseline

15: A00007304 Fault Management (FM)

15.1 Document Name

SN08 CEM I & C on IEMS

15.2 Logs

15.2.1 CEM SAF Processes logs

CEM SAF (Store and Forward) Framework throws a number of logs depicting any Trouble or Information regarding CEM processes.

All these logs will fall under two categories:

TROUBLE log or INFO log.

TROUBLE log will be identified in the range TMN300~399

INFO log will be identified in the range TMN600~699

For example:

TMN600: Information only

TMN601: File IO info

TMN604: Application status

TMN630: Data Server OK

TMN302: System error

TMN301: Application error

TMN303: Communication error

TMN309: Data Server error

TMN311: Fatal error

Data Server process logs

The dmsDataServer process runs on the SDM/CBM, connects to call server node (core) and receives both the Performance and Configuration data through Base APIs (Table Access Service and OM Access Service). Depending on whether its operational measurements (OM) or configuration data, it forwards it to performance manager or configuration manager respectively.

The following warning/error/information messages are generated in custlog to reflect various problems. These messages can be seen in /var/adm/custlog file to find exact cause and fix.

1. Desc Msg: Could not read switch name

Fix Msg: Check state of switch

2. Desc Msg: Could not create tuple

Fix Msg: Check state of switch

3. Desc Msg: Could not read VRINV table

Fix Msg: Check state of switch

4. Desc Msg: Could not initialize OM Access

Fix Msg: Contact system administrator

5. Desc Msg: Could not initialize OM Access

Fix Msg: Contact system administrator

6. Desc Msg: Could not get keyinfo object, excluding group, <group>

Fix Msg: Check OM group for bad key/info type

7. Desc Msg: Could not get key, excluding group, <group>

Fix Msg: Check OM group for bad key type

8. Desc Msg: Could not get info, excluding group, <group>

Fix Msg: Check OM group for bad info type

9. Desc Msg: Could not register initialization timer

Fix Msg: Contact administrator

10. Desc Msg: Rejecting register request for excluded group: <group>

Fix Msg: Check group key/info for validity

11. Desc Msg: "Could not open listening connection

Fix Msg: Check /etc/services

12. Desc Msg: Could not open listening connection: <service name>

Fix Msg: Check services file

NLClient and NLServer logs

The operational measurements (OMs) are available on the CEM server for graphing, dashboard, thresholding, mass export and correlation. The CEM server gets all the performance data from SDM/CBM through NLServer and nlSafServer processes running on SDM/CBM. The nlClient process running on the IEMS server receives OM data from nlSafServer and NLServer, process it and forward it to the upstream processes. All these processes makes the handling of OM data easier and faster and offloads the load on CEM server in processing OM data.

The following warning/error/information messages in custlog will be generated by the NLServer and nlSafServer to reflect various problems. These messages can be seen in /var/adm/custlog file on the SDM/CBM to find exact cause and fix.

1. Desc Msg: Failed to register for connection to export Server at service <service name>

Fix Msg: Contact next level of support

2. Desc Msg: Failed to register for connection to Data Server at port <port number>

Fix Msg: Contact next level of support

3. Desc Msg: Failed to register for connection to Data Server at service <service name>

Fix Msg: Contact next level of support

4. Desc Msg: Failed to register for signals

Fix Msg: Contact next level of support

5. Desc Msg: Failed to send error

Fix Msg: Check SAFServer Process

6. Desc Msg: Communications not initialized

Fix Msg: Contact next level of support

7. Desc Msg: Input from unknown end point
Fix Msg: Contact next level of support
8. Desc Msg: Failed to send registration message to Data Server
Fix Msg: Check Data Server Process
9. Desc Msg: Failed to send deregistration message to Data Server
Fix Msg: Check Data Server Process
10. Desc Msg: Invalid Message from archive.
Fix Msg: Contact next level of support.
11. Desc Msg: store is disconnected:deregister the connection
Fix Msg: Check Archive Process
12. Desc Msg: Receive from Archive failed
Fix Msg: Contact next level of support
13. Desc Msg: Unreadable Data Server message type
Fix Msg: Contact next level of support
14. Desc Msg: Unreadable OM report
Fix Msg: Contact next level of support
15. Desc Msg: Failed to send correlation error data to Archive
Fix Msg: Check Archive Process
16. Desc Msg: OM Registration failed
Fix Msg: Contact next level of support
17. Desc Msg: Unreadable registration response
Fix Msg: Contact next level of support
18. Desc Msg: OM DeRegistration failed
Fix Msg: Contact next level of support
19. Desc Msg: Unreadable deregistration response from Data Server

-
- Fix Msg: Contact next level of support
20. Desc Msg: Failed to send CM info request to Data Server
- Fix Msg: Check Data Access Layer Process
21. Desc Msg: Failed to send deferred registration message to Data Server
- Fix Msg: Check Data Access Layer Process
22. Desc Msg: Failed to send re-registration message to Data Server
- Fix Msg: Check Data Access Layer Process
23. Desc Msg: Fatal status change
- Fix Msg: Check Data Access Layer Process
24. Desc Msg: Unreadable OM status received from Data Server
- Fix Msg: Contact next level of support
25. Desc Msg: Could not get GroupInfo
- Fix Msg: Contact next level of support
26. Desc Msg: Failed to send nlGrpInfoRsp data to Archive
- Fix Msg: Check Archive Process
27. Desc Msg: Unreadable CM info message from Data Server
- Fix Msg: Contact next level of support
28. Desc Msg: Could not open License File
- Fix Msg: Verify file existence and permission
29. Desc Msg: Unexpected message type from Data Server
- Fix Msg: Contact next level of support
30. Desc Msg: Lost connection to Data Server
- Fix Msg: Check Data Server Process
31. Desc Msg: Receive from Data Server failed
- Fix Msg: Contact next level of support
-

- 32. Desc Msg: Communications not initialized
 - Fix Msg: Contact next level of support
- 33. Desc Msg: Failed to send end_of_report msg to store
 - Fix Msg: Check Archive Process
- 34. Desc Msg: Connection from unknown end point
 - Fix Msg: Contact next level of support
- 35. Desc Msg: Switch name unknown
 - Fix Msg: Contact next level of support
- 36. Desc Msg: Arithmetic overflow in correlation <correlation name>
 - Fix Msg: Contact next level of support
- 37. Desc Msg: Failed to send OM data to Archive
 - Fix Msg: Check Archive Process
- 38. Desc Msg: Error while doing a send to the Agent, discard send queue
 - Fix Msg: Check Agent Process
- 39. Desc Msg: Port for the service <NLservice name> is not available.
 - Fix Msg: Please update /etc/services file & restart NLServer
- 40. Desc Msg: Failed to register for connection to export Server at service <service name>
 - Fix Msg: Contact next level of support
- 41. Desc Msg: Failed to register for connection to Data Server at port <port num>
 - Fix Msg: Contact next level of support
- 42. Desc Msg: Failed to register for connection to Data Server at service <service name>
 - Fix Msg: Contact next level of support

log Normalizer and logNormSAF Process logs

The fault data on being received from call server node (core) is processed by logNormalizer process running on CEM. The logNormSAF process (running on the SDM/CBM) stores and forward this data to the CEM server.

The logNormalizer process generates error/warning/information messages in custlog whenever there is a problem encountered due to improper configuration, improper log formats etc. These messages can be seen in /opt/nortel/logs/coreEMS/custlog file on the CEM server to find description and fix of the problem.

1. Desc Msg: Event file <EventFileName> was not found...logNormalizer exiting

Fix Msg: Check Path.

2. Desc Msg: Event delimiter cannot be more than one character long...logNormalizer exiting

Fix Msg: check event formatter file for the delimiter after a event name and use it

3. Desc Msg: Event file "<<EventFileName<<" is empty..logNormalizer exiting

Fix Msg: check path, file name and/or read write permission

4. Desc Msg: Event file "<<EventFileName<<" had errors...logNormalizer exiting

Fix Msg: please look at the event file to check errors

5. Desc Msg: Mapper file "<<MapperFileName<<" was not found...logNormalizer exiting

Fix Msg: check path, file name and/or read write permission

6. Desc Msg: Mapper delimiter cannot be more than one character long...logNormalizer exiting

Fix Msg: check mapper file for the delimiter after a log name and use it

7. Desc Msg: Mapper file "<<MapperFileName<<" is empty..logNormalizer exiting

Fix Msg: check path, file name and/or read write permission

8. Desc Msg: Mapper file "<<MapperFileName<<" has errors.."<<argv[0]<<" exiting

Fix Msg: please check the mapper file errors

9. Desc Msg: Mapping information parsing error for log "<<logName<<" empty information or wrong delimiter used

Fix Msg:

10. Desc Msg: output file "<<outputFileName<<" could not be opened

Fix Msg: No action possible

11. Desc Msg: lostLogFile "<<lostLogFileName<<" could not be opened

Fix Msg: Call Nortel Personal

12. Desc Msg: lostLogFile "<<outputFileName<<" is empty

Fix Msg: Call Nortel Personal

13. Desc Msg: lostLogFormat string is empty

Fix Msg: Call Nortel Personal

14. Desc Msg: lostLogTriggerSize is empty

Fix Msg: Call Nortel Personal

15. Desc Msg: lostLogVisibleMsg string is empty

Fix Msg: Call Nortel Personal

16. Desc Msg: lostLogVisLog string is empty

Fix Msg: Call Nortel Personal

17. Desc Msg: sdmLogList is empty

Fix Msg: Call Nortel Personal

18. Desc Msg: probeTimer string is empty

Fix Msg: No probe is assumed

19. Desc Msg: checkLen string is empty

Fix Msg: No checkLen is assumed

20. Desc Msg: No Lost Log Trigger message has been specified

Fix Msg: Call Nortel Personal

21. Desc Msg: Could not send events to agent. Agent removed from output list.

Fix Msg: No agents connected.. start an agent

22. Desc Msg: Unknown log format. No mapping will be done for input

Fix Msg: Contact Nortel Personal

15.3 References

Please refer to the following NTP document for more detailed format of the above logs:

411-8111-511.01.01 : GSM/UMTS VCN OAM Reference Manual

16: A00007327 Fault Management (FM)

16.1 Document Name

Media Proxy 5 and 30 minute Operational Measurements

16.2 Fault management strategy

The **Media Proxy 5 and 30 minute** OMs feature provides operational measurements for calls involving media proxies and alarms for lost communication with media proxies.

16.3 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 and controlled and maintained by the SESM alarm manager or IEMS.

The SESM Alarm manager on the SSPFS is used to display the GWC alarms and log alarms history. Alarms can be filtered for display purposes, based on the alarm severity field.

16.4 Alarms

16.4.1 Media Proxy Communications Failure

Category: Communication

Description: Media Proxy Communications Failure

Severity: Based on number of elements involved and the number of elements in a disabled state collected with a 5 minute poll.

- Critical - Over 50% of media proxies disabled
- Major - Over 20% of media proxies disabled
- Minor - Any media proxies disabled

Cause: Signal loss

This alarm is based on the number of media proxies that are out of service as compared to the number of media proxies provisioned checked on a 5 minute polling period. Media proxies are considered out of service when they fail to respond to messages sent from the GWC, and returned to service when the regular RSIP message is received by the GWC.

Alarms are raised as a media proxy goes out of service and cleared when it comes back in service. The customer should view the alarm as an indication

that there is a problem with the media proxy. The new OM collected can be used to see how many media proxies are out of service and then use the customer logs to identify the media proxies that need attention.

An OM “Number of media proxies currently provisioned” is also implemented to complement this alarm - see the Performance section of this feature.

17: A00007393 Fault Management (FM)

17.1 Document Name

Session Policy Controller

17.2 Fault Management Strategy

Alarm and Logging capabilities span the Session Policy Controller application and NGSS software platform. The SPC derives its Alarm and Logging functionality from the NGSS software platform and a majority of these key functions are provided by the capabilities of the underlying NGSS platform itself. Refer to the NGSS Fault Management documentation for more detail concerning NGSS logs and alarms.

Alarm notifications are sent to the IEMS NMS in the form of SNMP traps. The standard Nortel Alarm MIB is used for this purpose. Alarms notifications are also distributed to the web server and can be viewed from the Web GUI. Active alarms will be refreshed automatically every 45 seconds. Alarms cleared automatically when the issue that raised the alarm has been corrected. The audit alarm will reappear after a period of time if the problem is not corrected.

The SPC captures all system events in the customer log which can be viewed from the web GUI. The log files are automatically rotated so that the log file system is never filled through logging activity.

17.2.1 Audits

The Session Policy Controller is capable of initiating audit requests. Audits may be required for the following events:

- The SPC can audit the GWC to determine if a flow is invalid. The mechanism allows the SPC to query the status of suspect flows. There is a configurable timer on each flow; the default value is 60 minutes. If the timer for the flow expires, the flow is considered suspect. SPC then audits the suspect flow by exchanging messages over the signaling interface with the application server.
- Switch of Activity (SWACT) – when Session Policy Controller changes activity from one unit to another, it will initiate audits in order to assure that it has not lost critical information in the transfer.
- Change in Link State – if links to the Application Server are lost, the flow status audits described above should be sufficient to assure any transactions lost during the link outage are accounted for.

The results of the audits are logged.

17.3 Fault Management Tools and Utilities

The standard Nortel Alarm MIB is used to deliver alarm notification to the IEMS NMS.

All logs are stored locally on disk in custlog format. They can be viewed on the web GUI and transferred over the network to a log host. The logs use the SYSLOG utility in the NGSS base. File rotation will be based on the file size and file rotation timer. The file rotation time, maximum file size and file retention can be configured using the Logrotate utility. The Logs are sent automatically to IEMS.

17.4 SPC Alarms

17.4.1 SPC Application Server Signaling Communication Alarm

Alarm		Description	Corrective Action
APPSVR_SIGNALING_COMM_FAILURE		This alarm is generated for an Application Server Signaling interface communication failure	Check the application server status and the link to the application server
Category:	Communications		
Severity:	Major		
Cause:	Application Server Signaling Communication Failure		
Duration:	Until Application Server Signaling Communication is reestablished Or the alarm auto clear timer is expired.		

Raise and Cleared Alarm Report Parameters:

Report Parameter	Raise Alarm	Clear Alarm
alarmLevel	eAS_Major	eAS_Cleared
componentID	SPCP	
category	eAPC_Communications	
description	AppServer <i>IPAddress</i> Signaling Communication Failure	AppServer <i>IPAddress</i> Signaling Communication Recovered
probableCause	eAP_outOfService	
specificProblem	AppServer Signaling Communication Failure	
reportName	SPCP	
reportNum	301	
eventType	cTBL	
label	AppServer Signaling Communication Failure	AppServer Signaling Communication Recovered
notificationID	0	Raise alarm generated value

17.4.2 SPC No Database Connection Alarm

Alarm	Description	Corrective Action

SPC_NO_DB_CONNECTION		This alarm is generated when SPC lost database connection	Contact next level of support.
Category:	Communications		
Severity:	Critical		
Cause:	SPC lost database connection. This alarm is raised if SPC cannot establish a connection with the database during Policy Controller process initialization. The alarm should clear itself. At start-up, if Policy Controller process cannot establish a connection with the database it will restart itself and re-attempt the connection.		
Duration:	Until SPC database connection is reestablished		

Raise and Cleared Alarm Report Parameters:

Report Parameter	Raise Alarm	Clear Alarm
alarmLevel	eAS_Critical	eAS_Cleared
componentID	SPCP	
category	eAPC_Communications	
description	SPC Processing No Database Connection	SPC Processing Database Connection Established
probableCause	eAP_outOfService	
specificProblem	No Database Connection	
reportName	SPCP	
reportNum	302	
eventType	cTBL	
label	No Database Connection	Database Connection Established
notificationID	0	Raise alarm generated value

17.4.3 SPC Reservation Request Mass Failure Alarm

Alarm		Description	Corrective Action
REQUEST_MASS_FAILURE		This alarm is generated when Application server request failure ratio exceeds predefined threshold value <TBD>	Contact next level of support.
Category :	QualityOfService		
Severity:	Minor		
Cause:	Application server request failure ratio exceeds predefined threshold		
Duration:	Until Application server request failure ratio falls below predefined threshold		

Raise and Cleared Alarm Report Parameters:

Report Parameter	Raise Alarm	Clear Alarm
alarmLevel	eAS_Minor	eAS_Cleared
componentID	SPCP	
category	eAPC_QualityOfService	
description	CAC Request Failure Exceed Threshold	CAC Request Failure Below Threshold
probableCause	eAP_thresholdCrossed	

specificProblem	CAC Request Mass Failure	
reportName	SPCP	
reportNum	303	
eventType	cTBL	
label	CAC Request Mass Failure	
notificationID	0	Raise alarm generated value

17.4.4 SPC Endpoint Number Exceed Endpoint Block Size Alarm

Alarm		Description	Corrective Action
ENDPOINT_NUMBER_EXCEED_ENDPOINT_BLOCK_SIZE		This alarm is generated when SPC Endpoint Number Exceeds Endpoint Block Size	Get a new license to enlarge the endpoint number supported
Category:	QualityOfService		
Severity:	Critical		
Cause:	SPC Endpoint Number Exceeds Endpoint Block Size		
Duration:	Until SPC Endpoint Number falls below Endpoint Block Size or Endpoint Block Size is increased. A password is required to increase the Endpoint block size. The service provider has to contact Nortel customer support to get a new license		

Raise and Cleared Alarm Report Parameters:

Report Parameters	Raise Alarm	Clear Alarm
alarmLevel	eAS_Critical	eAS_Cleared
componentID	SPCP	
category	eAPC_QualityOfService	
description	Endpoint Number Exceed Endpoint Block Size	Endpoint Number Below Endpoint Block Size
probableCause	eAP_thresholdCrossed	
specificProblem	Endpoint Number Exceed Endpoint Block Size	
reportName	SPCP	
reportNum	304	
eventType	cTBL	
label	Exceed Endpoint Block Size	Exceed Endpoint Block Size Recovered
notificationID	0	Raise alarm generated value

17.4.5 SPC Endpoint Number Exceed Endpoint Block Warning Size Alarm

Alarm	Description	Corrective Action

ENDPOINT_NUMBER_EXCEED_ENDPOINT_BLOCK_WARNING_SIZE		This alarm is generated when SPC Endpoint Number Exceeds Endpoint Block Warning Size	Get a new license to enlarge the endpoint number supported
Category :	QualityOfService		
Severity:	Major		
Cause:	SPC Endpoint Number Exceeds Endpoint Block Warning Size		
Duration:	Until SPC Endpoint Number falls below Endpoint Block Warning Size		

Raise and Cleared Alarm Report Parameters:

Report Parameters	Raise Alarm	Clear Alarm
alarmLevel	eAS_Major	eAS_Cleared
componentID	SPCP	
category	eAPC_QualityOfService	
description	Endpoint Number Exceed Endpoint Block Warning Size	Endpoint Number Below Endpoint Block Warning Size
probableCause	eAP_thresholdCrossed	
specificProblem	Endpoint Number Exceed Endpoint Block Warning Size	
reportName	SPCP	
reportNum	305	
eventType	cTBL	
label	Exceed Endpoint Block Warning Size	Exceed Endpoint Block Warning Size Recovered
notificationID	0	Raise alarm generated value

17.4.6 Topology Manager No Database Connection Alarm

Alarm		Description	Corrective Action
TPM_NO_DB_CONNECTION		This alarm is generated when Topology Manager lost database connection.	Contact next level of support.
Category :	Communications		
Severity:	Critical		
Cause:	Topology Manager lost database connection. This alarm is raised if SPC cannot establish a connection with the database during Topology Manager process initialization or if the application fails to access the DB. The alarm should clear itself after the next topology change/update request is received. At start-up, if Topology Manager process cannot establish a connection with the database it will restart itself and re-attempt the connection.		
Duration:	Until Topology Manager database connection is reestablished		

Raise and Cleared Alarm Report Parameters:

Report Parameters	Raise Alarm	Clear Alarm
alarmLevel	eAS_Critical	eAS_Cleared
componentID	TPM	
category	eAPC_Communications	
description	Topology Manager No Database Connection	Topology Manager Database Connection Established
probableCause	eAP_outOfService	
specificProblem	No Database Connection	
reportName	TPM	
reportNum	301	
eventType	cTBL	
label	No Database Connection	Database Connection Established
notificationID	0	Raise alarm generated value

17.5 SPC Logs

Log Files are created to store the logs on the local disk in the custlog format. In addition to the SPC specific logs, NGSS Application Maintenance (NAM) logs 500, 300, 301, and 302 are generated during SPC operation. Refer to the NGSS Fault Management documentation for more information about those logs.

17.5.1 SPC Startup

17.5.1.1 Explanation

This log is generated when the SPC starts up.

17.5.1.2 Format

Report Name	SPCP
Report Num	501
Alarm Value	NONE
Event Type	INFO
LABEL	SPC Startup

17.5.1.3 Action

None

17.5.1.4 Associated Operational Measurements or Performance Measurements

None

17.5.2 SPC Shutdown

17.5.2.1 Explanation

This log is generated when the SPC shuts down

17.5.2.2 Format

Report Name	SPCP
Report Num	502
Alarm Value	NONE
Event Type	INFO
LABEL	SPC Shutdown

17.5.2.3 Action

None

17.5.2.4 Associated Operational Measurements or Performance Measurements

None

17.5.3 Audit Result**17.5.3.1 Explanation**

This log is generated when a Flow Status Audit is completed.

17.5.3.2 Format

Report Name	SPCP
Report Num	601
Alarm Value	NONE
Event Type	INFO
LABEL	Audit Result

17.5.3.3 Action

None

17.5.3.4 Associated Operational Measurements or Performance Measurements

None

17.5.4 CAC Request Denied**17.5.4.1 Explanation**

This log is generated when CAC request from Application server is denied.

17.5.4.2 Format

Report Name	SPCP
Report Num	602
Alarm Value	NONE
Event Type	INFO
LABEL	CAC Request Denied

17.5.4.3 Action

None

17.5.4.4 Associated Operational Measurements or Performance Measurements

The following OMs are pegged

- SPC Reservation Request or SPC Commit Request
- CAC Request on Network Segment

17.5.5 SPC Topology Change

17.5.5.1 Explanation

This log is generated when spc callp accepts a topology change.

17.5.5.2 Format

Report Name	SPCP
Report Num	603
Alarm Value	NONE
Event Type	INFO
LABEL	Topology Change

17.5.5.3 Action

None

17.5.5.4 Associated Operational Measurements or Performance Measurements

None

17.5.6 Topology Mismatch

17.5.6.1 Explanation

This log is generated when callP detects that the Ingress Id of the Network Segment sent in a GateSet message from the GWC is not present in the SPC database. This is an indication that there could be a topology mismatch between the SPC and GWC/SESM. A summary of the requested change is included in the free text portion of the report description field.

17.5.6.2 Format

Report Name	SPCP
Report Num	604
Alarm Value	NONE
Event Type	INFO
LABEL	Topology Mismatch

17.5.6.3 Action

None

17.5.6.4 Associated Operational Measurements or Performance Measurements

None

17.5.7 TPM Startup

17.5.7.1 Explanation

This log is generated when the Topology Manager starts up.

17.5.7.2 Format

Report Name	TPM
Report Num	501
Alarm Value	NONE
Event Type	INFO
LABEL	TopologyManager Startup

17.5.7.3 Action

None

17.5.7.4 Associated Operational Measurements or Performance Measurements

None

17.5.8 TPM Shutdown

17.5.8.1 Explanation

This log is generated when the Topology Manager shuts down

17.5.8.2 Format

Report Name	TPM
Report Num	502
Alarm Value	NONE
Event Type	INFO
LABEL	TopologyManager Shutdown

17.5.8.3 Action

None

17.5.8.4 Associated Operational Measurements or Performance Measurements

None

17.5.9 Topology Change

17.5.9.1 Explanation

This log is generated when topology manager accepts a topology change. A summary of the requested change is included in the free text portion of the report description field.

17.5.9.2 Format

Report Name	TPM
Report Num	601
Alarm Value	NONE
Event Type	INFO
LABEL	Topology Change

17.5.9.3 Action

None

17.5.9.4 Associated Operational Measurements or Performance Measurements

None

18: A00007415 Fault Management (FM)

18.1 Document Name

Internodal Emergency Standalone (ESA) Element Manager

18.2 Fault management strategy

The standard MG9k EM Fault Management strategy will apply to the faults for MG9kEM Internodal ESA. 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.

18.3 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, time, the NE Id, the generating resource information, the severity and the 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.

18.4 Logs and Alarms

Two new alarms (ESA304 (nnEsaCoiFault) and ESA312 (EM generated)) will be added. The new alarms will be displayed at the Alarm Browser at the subnet as well as the alarm browser for each corresponding network element. A log is also generated. Both are NE level alarms.

18.4.1 Explanation

18.4.1.1 ESA304 (nnEsaCoiFault)

Title: nnEsaCoiFault

Name: ESA

Description: This log is generated by the EM in response to a trap from the MG9000 (nnEsaCoiFault). The MG9000 sends this trap when it detects communication problems to other nodes in the same community of interest.

Severity: Major

Event type: ESA community of interest

18.4.1.2 ESA312 (Internodal Esa Provisioning Fault)

Title: Esa Provisioning Fault

Name: ESA

Description: This log is generated by the EM when a failure occurs whilst trying to provision internodal community of interest data for a given NE.

Severity: Major

Event type: Internodal ESA Provisioning failure

18.4.2 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 explained in the PLOA_SLOA_LOG_ALARMS DID.

18.4.2.1 ESA304 (nnESAFault)

***ESA304 Tue Jul 09 14:50:26 EDT 2005 TBL

NE Number: 8 NE Name: co8

State: not acknowledged

Type: Equipment

Cause: Equipment malfunction

Time: Jul 09 14:50:26:616 2005

Severity: Major

Description: Failed to ping members of community of interest

18.4.2.2 ESA312 (Esa Provisioning Failure)

***ESA312 Tue Jul 09 14:50:26 EDT 2005 TBL

NE Number: 8 NE Name: co8

State: not acknowledged

Type: Processing Error

Cause: Configuration Or Customization Error

Time: Jul 09 14:50:26:616 2005

Severity: Major

Description: Internodal ESA provisioning failure

18.4.3 Field descriptions

18.4.3.1 ESA304 (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 mmmdd hh:mm:ss zone yyyy
nnUemgAlarmSeverity	String	Major
Description	string	Failed to ping members of community of interest

18.4.3.2 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.

Table 2 Field descriptions ESA304

Field	Value	Description
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.
event type	TBL, INFO, etc	Trouble, Service Summary, State Change, Information, Threshold and Expert. TBL for this log.

Table 2 Field descriptions ESA304

Field	Value	Description
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 mmmdd hh:mm:ss zone yyyy
nnUemgAlarmSeverity	String	Major
Description	string	Internodal ESA provisioning failure

18.4.4 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.

18.4.5 Associated Operational Measurements or Performance Measurements

None.

18.5 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.

19: A00007417 Fault Management (FM)

19.1 Feature name

Ethernet link overload Control

19.2 Logs

Log Title/Log ID: CAP Capacity Data/ CAP101

19.2.1 Formats

Figure 1 Formats of log reports

```
<office name> CAP101 <date> <timestamp> INFO CAPACITY_DATA  
  
UTIL <n> ENGLEVEL <BELOW/ABOVE> CCOVRD <OFF/ON>IOOVRD <OFF/  
CMIC-ON/ETHR-ON/CMIC-ETHR-ON> PE_SC <YES/NO>
```

Figure 2 Sample log reports

```
VENUS21AO CAP101 SEP07 09:42:35 8700 INFO CAPACITY_DATA  
  
CATMP/HR 251881 SMS/HR 180 VLR_UPD/HR 331200 CAP 127%  
  
ENGBHCA 196972 CCOVRD ON IOOVRD ETHR PESC NO
```

19.2.2 Explanation

Description: This feature impacts the existing CAP101 log. Since this feature introduces the Ethernet overload control, the CMICOVLD field will be changed to IOOVRD. IOOVRD indicates the IO messaging link utilization status, including CMIC and Ethernet Link.

19.2.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
IOOVRD		Indicates the CMIC and Ethernet link overloading condition.
	OFF	When CMIC & ETHR are running under link capacity.
	CMIC	When CMIC link is over utilized.
	ETHR	When ETHR link is over utilized.
	CMIC-ETHR	When CMIC and ETHR links are over utilized.

19.2.4 Action

If the logs indicate IO link overload frequently, then it may suggest upgrading the IO capacity service hardware.

19.2.5 Associated Operational Measurements or Performance Measurements

IOCAP OM group has registers.

19.2.6 Additional information

Please refer A00006693 FN.

19.3 Related documentation

20: A00007465 Fault Management (FM)

20.1 Document Name

Integrated Accounting Application (IAA)

20.2 Fault management strategy

Faults and alarms generated by the IAA modules are sent to Customer logs using the API provided and defined in the Log Reporting Rules and Guidelines document. (IEMPG, AF01). The IAA modules will use Log Number SDM799 and SDM399 when generating messages viewable by the customer. Designer information is written to the designer logs using the syslog mechanism directly.

20.3 Fault management tools and utilities

As a result of using the API provided by Nortel, the customer logs, state changes and designer logs can be managed using the existing tools Nortel has in place.

20.4 Logs

The following new alarms and log ID are being added as part of the IAA feature

.

Table 1 IAA logs

LOG NAME	LOG NUMBER	NEW/MOD DELETED	SYSTEM (SOS/ UNIX)
IAA	341	NEW	UNIX
IAA	342	NEW	UNIX
IAA	343	NEW	UNIX
IAA	344	NEW	UNIX
IAA	345	NEW	UNIX
IAA	346	NEW	UNIX
IAA	347	NEW	UNIX
IAA	641	NEW	UNIX
IAA	646	NEW	UNIX
IAA	701	NEW	UNIX

20.4.1 Log Report - IAA341

Example:

CA108CD *** IAA341 APR08 14:50:47 3800 TBL IAA Module Initialization Failure

Module: <Module Name>

Reason: <Reason>

20.4.1.1 Overview

The IAA341 log is generated whenever an IAA module fails to initialize. The reason text field may contain one of the following strings:

- **“Error Loading URF Specification File”**

Cause: This log message is generated when the modules URF specification file is corrupted or missing.

Action: Verify the URF specification file for the module is in the correct location and is not corrupted. Otherwise contact next level of support.

- **“Error Initializing spathreaddata object”**

Cause: This log message is generated when the system resources are not available.

Action: Determine the cause of unavailable system resources and restart the application. Otherwise contact the next level of support.

- **“License check failed”**

Cause: This log message is generated if the software license, needed to run the IAA application, is missing.

Action: Verify the license file is in the correct directory and restart the application. Otherwise contact the next level of support.

- **“Cannot create socket, Port # %u”**

Cause: This log message is generated if the system resources are unavailable, or if another process is attached to the port number displayed in the alarm.

Action: Determine if another application is connected to the port number in question. Determine the cause of unavailable system resources and restart the application. Otherwise contact the next level of support.

- **“Shared Memory Initialization Failed”**

Cause: This log message is generated if the system resources are unavailable.

Action: Determine the cause of the unavailable system resources and restart the application. Otherwise contact the next level of support.

- **“Failed to flush shared memory queue to disk”**

Cause: This log message is generated, if the file system the module is attempting to write its shared memory queue to is full or the permissions are not correct.

Action: Verify that the files system has the correct permissions set and that there is space available on the filesystem. Otherwise contact the next level of support.

- **“Bad Parameters Passed at Startup”**

Cause: An invalid parameter was passed to the IAA module.

Action: Verify the startup script is passing correct parameters, and restart the application. Otherwise contact the next level of support.

20.4.2 Log Report - IAA342

Example:

```
CA108CD *** IAA342 APR08 14:50:47 3800 TBL IAA Module Interprocess Communication Failure
Module: <Module Name>
Reason: <Reason>
```

20.4.2.1 Overview

The IAA342 log is generated whenever an IAA module cannot communicate with other IAA modules. The reason text field may contain one of the following strings:

- **“Error Communicating to EMDA”**

Cause: This log message is generated when a module cannot communicate with the EMDA module.

Action: Verify that the EMDA modules is operational and listening to the correct port. Otherwise contact the next level of support.

20.4.3 Log Report - IAA343

Example:

```
CA108CD *** IAA343 APR08 14:50:47 3800 TBL IAA PCEM Processing Error
Module: <Module Name>
FileName: <Name of Bad file if Available>
Reason: <Reason>
```

20.4.3.1 Overview

The IAA343 log is generated when a PCEM processing error occurs. The reason text field may contain one of the following strings:

- **“Error Reading Input File”**

Cause: This log message is generated if there is a problem reading an input data file.

Action: Verify that the correct permissions are set on the file displayed in the alarm.

- **“Error Renaming or Accessing file”**

Cause: This log message is generated if the IAA module cannot access the specified file or rename it.

Action: Verify the correct permissions of the file and filesystem displayed in the log messages. Otherwise contact the next level of support.

- **“Error generating checksum”**

Cause: IAA module was unable to create the correct checksum.

Action: Verify that the input file is not corrupted. Otherwise contact the next level of support.

- **“Error writing to File”**

- **Cause:** This log message is generated if the IAA module cannot write to its output file.

- **Action:** Verify that the permissions on the file and filesystem are correct. Verify there is space available on the filesystem. Otherwise contact the next level of support.

- **“Failed to receive UDP messages”**

Cause: This log message is generated if the IAA application cannot receive UDP messages.

Action: Determine the cause of the unavailable system resources and restart the application. Otherwise contact the next level of support.

- **“Failed to flush shared memory queue to disk”**

Cause: This log message is generated if the file system, the module is attempting to write its shared memory queue to, is full or the permissions are not correct.

Action: Verify that the file system has the correct permissions set and that there is space available on the filesystem. Otherwise contact the next level of support.

20.4.4 Log Report - IAA344

Example:

CA108CD *** IAA344 APR08 14:50:47 3800 TBL IAA PCEM Audit Error

Module: <Module Name>

AuditName: <Name of Audit>

Reason: <Reason>

20.4.4.1 Overview

The IAA344 log is generated when an IAA module cannot create an audit entry. The reason text field may contain one of the following strings:

- **“Error Creating Audit”**

Cause: This log message is generated if there is a problem creating an audit entry.

Action: Verify that the correct permissions are set in the audit directory and that there is space on that filesystem.

20.4.5 Log Report - IAA345

Example:

CA108CD *** IAA345 APR08 14:50:47 3800 TBL IAA Module Configuration Error
 Module: <Module Name>
 Parameter: <Name of Parameter>
 Reason: <Reason>

20.4.5.1 Overview

The IAA345 log is generated when an IAA module detects a configuration problem. The reason text field may contain one of the following strings.

- **“Required Configuration parameter not found”**

Cause: This log message is generated if a required configuration value is not defined.

Action: Datafill the required configuration parameter.

- **“Received messages for Unknown Channel ID <%d>”**

Cause: This log message is generated if the IAA module receives a PCEM or PCES message for an unconfigured Channel ID.

Action: Datafill the Channel ID for the appropriate RKS pair or DF.

20.4.6 Log Report - IAA346

Example:

CA108CD *** IAA346 APR08 14:50:47 3800 TBL IAA Downstream Communication Error
 Module: <Module Name>
 Destination ID: <Name of Bad file if Available>
 Reason: <Reason>

20.4.6.1 Overview

The IAA346 log is generated when the IAA cannot communicate to the downstream RKS pair or DF. The reason text field may contain one of the following strings.

- **“Destination is down - Writing to file”**

Cause: This log message is generated if the downstream RKS pair is unreachable and the message is save to a file for transmission at a later time.

Action: The craftsperson should ascertain what was the cause of the problem and correct the problem. Once the connection to the RKS pair is re-established the IAA application will return to InSrv.

- **“DF: Destination is Down - Message dropped for ChannelID <%d>, Dropped Message Count <%d>”**

Cause: This log message is generated if the downstream DF is unreachable.

Action: The craftsperson should ascertain what was the cause of the problem and correct the problem. Once the connection to the DF is re-established the IAA application will return to InSrv.

- **“Cannot Connect to Primary RKS”**

Cause: The IAA cannot connect to the RKS when trying to ftp a file.

Action: The craftsperson should ascertain what was the cause of the problem and correct the problem. Once the connection to the RKS pair is re-established the IAA application will return to InSrv.

- **“Cannot place file on RKS”**

Cause: This log message is generated if the IAA cannot place the file on the RKS after the connection is made.

Action: The craftsperson should ascertain what was the cause of the problem and correct the problem. Once the connection to the RKS pair is re-established the IAA application will return to InSrv.

20.4.7 Log Report - IAA347

Example:

```
CA108CD *** IAA347 APR08 14:50:47 3800 TBL IAA Filesystem Management Error
Module: <Module Name>
Directory: <Directory Name>
Reason: <Reason>
```

20.4.7.1 Overview

The IAA347 log is generated when an IAA module detects a problem when trying to manage its filesystem storage. The reason text field may contain one of the following strings.

- **“Unable to move files to Secondary Directory”**

Cause: This log message is generated if the IAA module fdsend cannot move a file it successfully transferred to a RKS to a secondary directory.

Action: Verify permissions and space on filesystem.

20.4.8 Log Report - IAA641

Example:

```
CA108CD *** IAA641 APR08 14:50:47 3800 INFO IAA Module Startup
Module: <Module Name>
Reason: <Reason>
```

20.4.8.1 Overview

The IAA641 log is generated when an IAA module goes into service.

- **“IAA Module has been restarted”**

Cause: This log message is generated when an IAA module is successfully started.

Action: No Action is needed as this is purely for informational purposes.

20.4.9 Log Report - IAA646

Example:

CA108CD *** IAA646 APR08 14:50:47 3800 INFO IAA Communication Restored

Module: <Module Name>

Reason: <Reason>

20.4.9.1 Overview

The IAA646 log is generated when Communications between the IAA and the downstream RKS pair or DF has been restored.

- **“Communications has been re-established”**

Cause: This log message is generated when Communications between the IAA and the downstream RKS pair or DF has been restored.

Action: No Action is needed as this is purely for informational purposes.

20.4.10 Field Description

Field Name: Module

Field optionally: mandatory

Type: Alphanumeric

Size: Variable

Value(s): Variable

Descriptions: Identifies the module generating the log.

NTP table reference: Not applicable.

Field Name: Destination ID

Field optionally: mandatory

Type: Alphanumeric

Size: Variable

Value(s): Variable

Descriptions: Identifies the Destination the IAA is attempting to communicate to.

NTP table reference: Not applicable.

Field Name: Parameter

Field optionally: mandatory

Type: Alphanumeric

Size: Variable

Value(s): Variable

Descriptions: Identifies the Parameter that is not configured correctly.
NTP table reference: Not applicable.

Field Name: AuditName
Field optionally: mandatory
Type: Alphanumeric
Size: Variable
Value(s): Variable

Descriptions: Identifies the audit that the module is attempting to create.
NTP table reference: Not applicable.

Field Name: FileName
Field optionally: mandatory
Type: Alphanumeric
Size: Variable
Value(s): Variable
Descriptions: Identifies the file the IAA module is attempting to operate on.
NTP table reference: Not applicable.

Field Name: Reason
Field optionally: mandatory
Type: Alphanumeric
Size: Variable
Value(s): Variable
Descriptions: Provides an explanation of why the log was generated.
NTP table reference: Not applicable.

20.5 Alarms

20.5.1 Alarm - IAA701

Example:

```
CA108CD *** IAA701 APR08 14:50:47 3800 TBL IAA Data Corruption
Module: <Module Name>
Reason: <Reason>
```

20.5.1.1 Overview

The IAA701 log is generated when the data being process by the IAA is corrupted.

- **“Could not get EM Header in Message. Got %u at byte no %u. Channel ID= %u”**

Cause: This log message is generated when the EM messages being processed by the IAA is corrupted.

Action: Contact the next level of support.

20.5.2 Field Description

Field Name: Module

Field optionally: mandatory

Type: Alphanumeric

Size: Variable

Value(s): Variable

Descriptions: Identifies the module generating the log.

NTP table reference: Not applicable.

20.6 Related documentation

21: A00007489 Fault Management (FM)

21.1 Document Name

Integration of SuperNode Data Manager (SDM) User Authentication with the Integrated Element Manager System (IEMS)

21.2 Fault management strategy

The feature will log security events related to authentication and authorization. SDM Audit and Security Logs will be used by this feature to deliver the logs.

SDM Audit and Security Logs are generated and stored under /var/security/logs/ in auditlog and securitylog file. This feature only uses securitylog file to store its logs.

21.3 Fault management tools and utilities

21.3.1 Faults, Alarms and Logs

SDM Audit and Security Logs utilities will be used by this feature.

21.4 Logs

Authentication succeeded.

Log Title/Log ID: SN08 Authentication and Authorization Security Syslog.

21.4.1 Formats

Note: SDM Audit and Security Logs will be used for this feature.

21.4.1.1 NTSTD

Not applicable to this feature.

21.4.1.2 SCC2

Not applicable to this feature.

21.4.1.3 Syslog

The following is the format for the Authentication and Authorization Security log. It is based on Nortel OA&M Security IPT's Security Audit Logs Format Specification issue 1.1.

"date time" "host" "program[pid]:" class_security.ver02
"Message_tag"="Message_value" ...

The following is an example for the Authentication and Authorization Security log for a user login event.


```
Dec 10 09:04:29 wcary2p7 sshd[19464]: class_security.ver02
EVENT.TYPE="USER_ACT_Security_Login" DOC="PAM"
STAT="Success" DST="wcary2p7" DST.USER="jjsecu1"
SRC.OFFEND="47.129.112.162" HOST.TYPE="application"
SRC.USER="unknown" MESSAGE="pam_open_session: pam retval = 0
[Success]" MID="SDM_MID_defn.security.0010"
```

21.4.1.4 SNMP

Not applicable to this feature.

21.4.1.5 Integrated Element Manager GUI Fields

Not applicable to this feature.

21.4.2 Explanation

Description: The Authentication and Authorization Security Syslog is generated when a security event occurs on a SDM. They are created for information purposes.

21.4.3 Field descriptions

Table 1 Field descriptions

Field	Value	Description
Date time	e.g. Sep 17 15:42:40	Month, day and timestamp
host	e.g. wcary2p7	SDM system identifier
Program	sshd sdmmtc	The name of the SDM process which generated the log
PID	e.g. 19464	The process ID of the SDM process which generated the log
class_security.ver02	constant value	Message category
EVNT.TYP	USER_ACT_Security_Login USER_ACT_Security_Logout USER_ACT_Security_PAM	The type of the event
DOC	PAM RMI	Document field of the accessed resource
STAT	Success Failure	Status of the designed process
DST	e.g. wcary2p7	The address of the destination

Table 1 Field descriptions

Field	Value	Description
DST.USR	e.g. jjsecu1	User name or user id
SRC.OFFEND	e.g. 47.129.112.162	Address of the originating packet
HOST.TYPE	application	Device type
SRC.USR	e.g. unknown or jjsecu1	Login user name or user id (not effective user name or user id).
MESSAGE		Log message
		Note: The following is the log message's mapping to MID
	pam_open_session: pam retval = 0 [Success]	SDM_MID_defn.security.0010
	pam_close_session: pam retval = 25 [Please ignore underlying account module]	SDM_MID_defn.security.0011
	Naming Service was changed - Current: LOCAL New: LOCAL	SDM_MID_defn.security.0012
	PAM Authentication stack was changed - Current: LOCAL New: IEMS	SDM_MID_defn.security.0013
	Radius Server IP was set to: 47.135.214.67	SDM_MID_defn.security.0014
	Radius Port was set to: Default[1812]	SDM_MID_defn.security.0015
	Radius Secret was changed	SDM_MID_defn.security.0016
	User is not authorized for shell access	SDM_MID_defn.security.0017

Table 1 Field descriptions

Field	Value	Description
MID	SDM_MID_defn.security.0010	Message Identifier is a unique string to allow message text to change without affecting analysis tools
	SDM_MID_defn.security.0011	
	SDM_MID_defn.security.0012	
	SDM_MID_defn.security.0013	
	SDM_MID_defn.security.0014	
	SDM_MID_defn.security.0015	
	SDM_MID_defn.security.0016	
	SDM_MID_defn.security.0017	

21.4.4 Action

The Authentication and Authorization Security log for this feature is displayed for information purpose only. No further action is needed for handling these logs.

21.4.5 Associated Operational Measurements or Performance Measurements

Not applicable to this feature.

21.4.6 Additional information

Not applicable to this feature.

21.5 Alarms

Not applicable to this feature.

21.6 Related documentation

22: A00007713 Fault Management (FM)

22.1 Document Name

TOPS-IP Robustness

22.2 Fault management strategy

This feature does not change the fault management strategy for IP positions or for the TOPS product.

22.3 Fault management tools and utilities

Unchanged.

22.4 Logs

Log Title/Log ID: TOPS615

22.4.1 Format

The following are 2 examples:

Figure 1 TOPS615 Log With No IP Positions In Auto-Compression

TOPS615	mmdd	hh:mm:ss	ssdd	INFO	IP	Position	Auto	Compression
Operator	teams	reporting auto-compression in use:						
		Team Number			Number of Positions			
		-----			-----			
		N/A			0			

Figure 2 TOPS615 Log With IP Positions In Auto-Compression

TOPS615	mmdd	hh:mm:ss	ssdd	INFO	IP	Position	Auto	Compression
Operator	teams	reporting auto-compression in use:						
		Team Number			Number of Positions			
		-----			-----			
		1			5			
		6			975			
		30			1			

22.4.2 Explanation

Name: IP Position Auto Compression.

Description: The TOPS615 information log is generated indicating the operator teams and the number of positions in each team with auto-compression turned on. The log is generated if an auto-compression message has arrived during an approximate 5 minute audit period. It is also generated if an IP position with auto-compression turned on goes through a service

affecting state change (i.e. bsy). Once auto-compression has been turned off for all positions, the log indicates no operator teams or positions have auto-compression on.

22.4.3 Field descriptions

Table 1

Field	Value	Description
Team Number	1 - 30, N/A	This field indicates all of the team members that have IP operator positions reporting the use of voice auto-compression. The value will be 'N/A' if there are no positions in any team reporting auto-compression turned on.
Number of Positions	0 - 1023	This field indicates the total number of IP operator positions in each team reporting the use of voice auto-compression. The value will be zero if there are no positions in any team reporting auto-compression turned on.

22.4.4 Action

None required. If desired, the mapci;mtc;appl;topsip;topspos;post ac command may be used in the switch to determine the current auto-compression status of an IP position.

22.4.5 Alarms

Not Applicable.

22.4.6 Related documentation

Refer to 297-8403-906 TOPSIP User's Guide, for information about IP position fault management.

23: A00008431 Fault Management (FM)

23.1 Document Name

System Mastership Support for CS 2000 - Compact Geographic Survivability Configuration

23.2 Fault management strategy

The CS2000 - Compact in Geographic Survivability mode has extensions to the alarm strategy to support alarming additional connections monitored in Geographic Survivability mode. Specifically, the Call Agent (CA) monitors connectivity to its mate CA via the WAN backup path. Additionally, the CA monitors connectivity to the local wan edge router used to connect to the WAN. These additional connections are also described in existing connectivity logs, when in Geographic Survivability mode.

New logs in Geographic Survivability mode are used to show interactions with the local Ethernet Routing Switch 8600 (where used). OSPF is disabled on the CALLP and OAM vlans on the inactive call agent site in the case of optical and ethernet isolation between sites. Specifically, information logs are output as OSPF is enabled or disabled by the CA.

23.3 Fault management tools and utilities

No special fault management tools.

Alarms are available from the alarm command at the coremtc map level of the ccamtc map.

Logs are available from the logquery command at the coremtc map level of the ccamtc map.

23.4 New Logs CCA685 & CCA686

23.4.1 Explanation

Log Title: CCA685

Name: CCA Geo OSPF Disable

Description: The CCA disabled OSPF in the local ERS 8600.

Event type: Info

23.4.2 Explanation

Log Title: CCA686

Name: CCA Geo OSPF Enable

Description: The CCA enabled OSPF in the local ERS 8600.

Event type: Info

23.4.3 Format

CCA685 JAN11 12:38:05 INFO OSPF Disabled

Unit Number: 1, INACTIVE

Description: Open Shortest Path First routing protocol disabled on the local default gateway.

CCA686 JAN11 14:26:05 INFO OSPF Enabled

Unit Number: 0, ACTIVE

Description: Open Shortest Path First routing protocol enabled on the local default gateway.

23.4.4 Field descriptions

Table 1 Field descriptions

Field	Value	Description
Unit Number	0 or 1	The CCA unit number
Activity	ACTIVE or INACTIVE	The activity state of this unit

23.4.5 Action

No action required; this is an INFO only log.

For CCA685 - OSPF Disable log, this indicates that OSPF routing has been disabled on the local ERS 8600. This will only happen on the Inactive unit when the Ethernet connectivity or Optical Ring goes out of service between sites. This system action improves the ability of outside nodes to route to the remaining active call agent site.

23.4.6 Associated Operational Measurements or Performance Measurements

None

23.4.7 Additional information

None

23.5 Changed Logs CCA331 CCA335 CCA336 CCA631 CCA635 CCA636

These logs have an enhanced *Description* when in Geographic Survivability mode, giving details of the connection states being monitored. The description

format is the same for each of these logs, although the fields differ depending on the condition being logged.

When not in Geographic Survivability mode, the logs appear as documented previously.

The following sections describe the logs as seen in Geographic Survivability mode.

23.5.1 Explanation

Log Title: CCA331

Name: Mate Connectivity

Description: Indicates a connectivity problem with the mate CCA unit.

Event type: FLT

23.5.2 Explanation

Log Title: CCA631

Name: Mate Connectivity Restored

Description: Indicates connectivity problem with the mate CCA unit has been resolved.

Event type: INFO

23.5.3 Explanation

Log Title: CCA335

Name: Link Connectivity

Description: Indicates a link connectivity problem.

Event type: FLT

23.5.4 Explanation

Log Title: CCA635

Name: Link Connectivity Restored

Description: Indicates a link connectivity problem has been resolved.

Event type: INFO

23.5.5 Explanation

Log Title: CCA636

Name: Network Connectivity

Description: Indicates a connectivity problem with monitored network connections.

Event type: FLT

23.5.6 Explanation

Log Title: CCA336

Name: Network Connectivity Restored

Description: Indicates a network connectivity problem has been resolved.

Event type: INFO

23.5.7 Format

** CCA335 JAN24 11:23:32 FLT Link Connectivity

Unit Number: 0, INACTIVE

Description: Link0: INSV, mateCon: OK (opt: BAD, wan: OK),
netCon: OK (local: OK, wanEdge: OK); Link1:
INSV, mateCon: OK (opt: BAD, wan: OK), netCon:
OK (local: OK, wanEdge: OK); BLink: SYSB,
mateCon: BAD; FC: SYSB;

*** CCA331 JAN24 11:23:35 FLT Mate Connectivity

Unit Number: 0, INACTIVE

Description: Link0: INSV, mateCon: BAD (opt: BAD, wan: BAD),
netCon: OK (local: OK, wanEdge: OK); Link1:
INSV, mateCon: BAD (opt: BAD, wan: BAD),
netCon: OK (local: OK, wanEdge: OK); BLink:
SYSB, mateCon: BAD; FC: SYSB;

*** CCA336 JAN24 11:01:13 FLT Network Connectivity

Unit Number: 1, ACTIVE

Description: Link0: INSV, mateCon: BAD (opt: BAD, wan: BAD),
netCon: OK (local: OK, wanEdge: OK); Link1:
INSV, mateCon: BAD (opt: BAD, wan: BAD),
netCon: OK (local: OK, wanEdge: OK); BLink:
SYSB, mateCon: BAD; FC: SYSB;

CCA635 JAN12 14:38:03 INFO Link Connectivity Restored

Unit Number: 1, INACTIVE

Description: Link0: INSV, mateCon: OK (opt: OK, wan: OK),
netCon: OK (local: OK, wanEdge: OK); Link1:

INSV, mateCon: OK (opt: OK, wan: OK), netCon:
OK (local: OK, wanEdge: OK); BLink: INSV,
mateCon: OK; FC: INSV;

CCA631 JAN12 14:38:03 INFO Mate Connectivity Restored
Unit Number: 1, INACTIVE

Description: Link0: INSV, mateCon: OK (opt: OK, wan: OK),
netCon: OK (local: OK, wanEdge: OK); Link1:
INSV, mateCon: OK (opt: OK, wan: OK), netCon:
OK (local: OK, wanEdge: OK); BLink: INSV,
mateCon: OK; FC: INSV;

CCA636 JAN13 10:44:29 INFO Network Connectivity Restored
Unit Number: 0, ACTIVE

Description: Link0: INSV, mateCon: OK (opt: OK, wan: OK),
netCon: OK (local: OK, wanEdge: OK); Link1:
INSV, mateCon: OK (opt: OK, wan: OK), netCon:
OK (local: OK, wanEdge: OK); BLink: INSV,
mateCon: OK; FC: INSV;

23.5.8 Field descriptions

Table 2 Field descriptions

Field	Value	Description
Unit Number	0 or 1	The CCA unit number
Activity	ACTIVE or INACTIVE	The activity state of this unit
Description:		Description of Geo mode connection description follows:
Link0:	INSV or SYSB	State of Eth Link 0 connectivity to Router.
mateCon:	OK or BAD	Mate connectivity via Eth Link 0.
opt:	OK or BAD	Mate connectivity via Eth Link 0 and Ethernet via optical.
wan:	OK or BAD	Mate connectivity via Eth Link 0 and WAN.
netCon:	OK or BAD	Composite Network connectivity via Eth Link 0

Table 2 Field descriptions

Field	Value	Description
local:	OK or BAD	Network connectivity to local network (Shelf Controller) via Eth Link 0
wanEdge	OK or BAD	Network connectivity to local wan edge router.
Link1:	INSV or SYSB	State of Eth Link 1 connectivity to Router.
mateCon:	OK or BAD	Mate connectivity via Eth Link 1.
opt:	OK or BAD	Mate connectivity via Eth Link 1 and Ethernet via optical.
wan:	OK or BAD	Mate connectivity via Eth Link 1 and WAN.
netCon:	OK or BAD	Composite Network connectivity via Eth Link 1
local:	OK or BAD	Network connectivity to local network (Shelf Controller) via Eth Link 1
wanEdge	OK or BAD	Network connectivity to local wan edge router.
BLink:	INSV or SYSB	Backup Link state via Fiber Channel
mateCon:	OK or BAD	Mate connectivity via BLnk.
FC	INSV or SYSB	Fiber Channel (FC) state

23.5.9 Action

For CCA335, CCA331, CCA336 FLT logs:

- Use the description info in the logs, or in the corresponding CON alarm to determine the type of connectivity problem. Determine whether this is caused by a maintenance action underway, or by an actual network connectivity fault.
- If due to a network fault, attempt to isolate the connectivity problem.
- If due to a maintenance action, monitor the condition until the maintenance action is completed.

For CCA635, CCA631, CCA636 INFO logs:

- No action is required. These logs indicate a resolution of previously logged and alarmed connectivity problems.

23.5.10 Associated Operational Measurements or Performance Measurements

None

23.5.11 Additional information

These logs are associated with the CON alarm.

In normal (non-Geo) mode, these logs have a description like the following:

Description: Link0: INSV, mateCon: AVAIL, netCon: AVAIL;
Link1: INSV, mateCon: AVAIL, netCon: AVAIL;
BLink: INSV, mateCon: AVAIL; FC: INSV;

23.6 Alarms

23.6.1 CCA CON alarms

The description field of the LnkCon, MatCon and NetCon alarms describes the connectivity map for the monitored connections. In Geographic Survivability mode, the description is extended to show the enhanced connection monitoring. The description fields are identical to the corresponding logs described above.

The alarm severity varies with the number and types of connectivity problems.

Figure 1 shows an example of a MatCon and LnkCon alarms displayed on the CCA map, using the *alarm con* command.

Figure 1 Example Map showing MatCon and LnkCon alarms

CallAgent	SYS	CON	APPL	Unit: 1
.	.	MatCon	.	
		M		
CAMtc	CON alarms reported by CA unit 0:			
0 Quit	Alarm	Severity	Description	
2 Jam	LnkCon	major	Link0: INSV, mateCon: OK (opt: BAD, wan: OK),	
3 RelJam			netCon: OK (local: OK, wanEdge: OK);	
4 RExtst			Link1: INSV, mateCon: OK (opt: BAD, wan: OK),	
5 SwAct			netCon: OK (local: OK, wanEdge: OK);	
6			BLink: SYSB, mateCon: BAD;	
7			FC: SYSB;	
8				
9	MatCon	major	Link0: INSV, mateCon: OK (opt: BAD, wan: OK),	
10			netCon: OK (local: OK, wanEdge: OK);	
11			Link1: INSV, mateCon: OK (opt: BAD, wan: OK),	
12			netCon: OK (local: OK, wanEdge: OK);	
13 LogQuery			BLink: SYSB, mateCon: BAD;	
14 Alarm			FC: SYSB;	
15 QueryIP				

Figure 2 shows an example of a NetCon alarm displayed on the CCA map, using the *alarm con* command.

Figure 2 Example Map showing NetCon alarm

CallAgent	SYS	CON	APPL	Unit: 0
.	.	NetCon	.	
		M		
CAMtc	CON alarms reported by CA unit 0:			
0 Quit	Alarm	Severity	Description	
2 Jam	NetCon	major	Link0: INSV, mateCon: OK (opt: OK, wan: OK),	
3 RelJam			netCon: OK (local: OK, wanEdge: BAD);	
4 RExtst			Link1: INSV, mateCon: OK (opt: OK, wan: OK),	
5 SwAct			netCon: OK (local: OK, wanEdge: OK);	
6			BLink: INSV, mateCon: OK;	
7			FC: SYSB;	
8				

23.7 Related documentation

Configuration Management (CN)

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
A00005646	IPSEC on MG 9000 Element Manager
A00006226.AA06	NTPOLL: Restructuring and Table Control
A00006269	OSSGate Password No Echo
A00006347	Solaris 9 Introduction To SSPFS
A00006450	TL1 Line Test Interface for MG9K Lines
A00006570	CS2M Robustness enhancement - Moving SDM IP & CLI input to SSPFS
A00006693.AA08	XA-Core IO Capacity Monitoring Toolset
A00006731	Handle Flash on Exit
A00006780.AA23	Trimodal Call Server OAM & P Enhancements
A00006865	SN08 GIGE HAL Feature
A00006893.AA23	TLS Support for NGSS
A00006894.AA02	InterNodal Emergency Stand Alone (ESA) for MG9K
A00006901	Missing Patches
A00006979	Synchronized Backup Restore Manager

A00007000	GigE Network Interface
A00007071	SN08 3rd Party GW Interop Profiles
A00007072	3rd Party GW Interop Pre Provisioning
A00007074	GigE Link Maintenance
A00007102.AA11	Dual C-Side IP for GWC
A00007120.AA98	Packet Media Anchor for DPT
A00007213	MG9000 5/30 Minutes OMs
A00007243.AA09	Prevent Outage when CEM flash has not been erased
A00007250.AA12	ACDMIS Over TCP
A00007271.AA08	TOPS EOL for SN08
A00007277.AA04	LOGs Throttling
A00007293	VLAN for Gigabit Ethernet
A00007415	Internodal Emergency Standalone (ESA) Element Manager
A00007464.AA06	SBA Packet Cable Event Messaging
A00007465.AA06	Integrated Accounting Application (IAA)
A00007489.AA13	Integration of SuperNode Data Manager (SDM) User Authentication with the Integrated Element Manager System (IEMS)
A00007492.AA10	SDM User Group Improvements. This feature is part of the SDM21/SN08 release
A00007713.AA02	TOPS-IP Robustness
A00007790.AA08	P-phone Expansion for CICM Lines
A00007934.AA29	E800 Routing Enhancements
A00008387	GLC-32 AB Card Support
A00008431.AA04	Support for CS2Kc Geo Survivability

1: A00005646 Configuration (CN)

1.1 Feature name

IPSEC on MG 9000 Element Manager

1.2 Hardware and Software Requirements

SN08 or later software load for both the MG9000 and Element manager.

1.3 Initial Configuration

1.3.1 Security

From a high-level here are the steps to enable security on the OAM&P and call control links.

1. Load both MG9000 and MG9000 Element Manager with required software.
2. When commissioning the MG9000, thru the LCI, the craftsperson will enable security on the management link to the Element Manager.
3. The craftsperson will then use a web browser and connect to the MG9000 Element Manager server machine. (Not the Mid-Tier machine) After logging in, the craftsperson will enable security on communications with the MG9000 IP address.
4. Cold start from MG9000 or manual discovery from Element Manager.
5. This will complete securing the OAM&P link.
6. From SESM, enable security on the Gateway Controller.
7. From the SLOA GUI, provision a VMG. Enable security on the GW Controller Config tab.
8. This will complete securing the Call Control link.

1.3.1.1 MG9000

The LCI's IPSec and IKE security parameters must match the parameters provisioned through the SSPFS security servlet.

VMG IKE configuration parameters that are provisioned, via the Element Manager's SLOA GUI, must match the corresponding IKE parameters on the GWC.

1.3.1.2 MG9000 Element Manager

IPSec and IKE configuration parameters that are provisioned, via the SSPFS security servlet, must match the corresponding IPSec and IKE parameters on the MG9000, provisioned via the LCI.

1.3.2 MG9kEM SN008 Installation

If a user is upgrading from SN06.2 to SN008, the steps to upgrade are the same as they would be for SN06.2 to SN07.

If the user is upgrading from SN07 to SN008 - an additional step will be added to prompt the user to backup the table space for SN07.

As of SN008 the MG9kEM will continue to use the same tablespace as the previous release - with alters applied. Therefore in order to be able to roll back a MG9kEM release to SN07 from SN008 (if necessary)- the table space must be backed up prior to starting the SN008 MG9kEM.

1.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable

1.5 Upgrade Impact

1.5.1 Dump and Restore

If the user is upgrading from SN06.2 to SN008 - the steps for upgrade are the same as they would be for SN06.2 to SN07.

If the user is upgrading from SN07 to SN008, things change. As of SN008, we no longer will be running multiple versions of the EM. The EM will now use ONE tablespace from SN07 forward - with alters applied to support each new release. This means that the data from that tablespace for SN07 must be backed up prior to starting up the SN008 product. The script to backup the table space, mg9kem_db_backup.sh, and a mechanism to invoke this script will be provided.

If it is necessary to rollback to SN07, the use of the script mg9kem_db_restore.sh must be employed to restore the tablespace to its previous SN07 database schema and data set.

For SN07 to SN008 - no data export or import is necessary. The SN008 will attach to the existing SN07 tablespace and recover and use the network elements and data directly from that space.

1.5.2 Element Management Major Upgrade

If upgrading from SN06.2 directly to SN008, the data transition will be seamless to the user. The Element Manager will create the new tablespace for SN08 and will automatically import the SN06.2 data into the new tablespace.

If upgrading from SN07 to SN008, one modification to the way upgrades work is that the user is no longer required to move from one MG9kEM version to another if upgrading a MG9k from SN07 to SN008. The SN008 MG9kEM suite can handle discover and management of a MG9k Gateway running an SN07 load.

For SN07 to SN008, the steps will be install the SN008 package, backup the SN07 tablespace, start the SN008 MG9kEM. No data transfer steps are required.

One break in the way the MG9kEM can be run is that once SN008 has been started - the user cannot go back to using the SN07 Element Manager without restoring the previous database. It is not allowed to have SN07 MG9kEM and SN008 EM running at the same time, or to switch back and forth.

The Major upgrade from SN07 to SN008 is intended to be very similar in steps to that of a MR Upgrade.

1.5.3 Element Management MR Upgrade

The same steps as were done to support an SN07 MR Upgrade will apply to SN008.

1.6 Data schema (DS) (CM, MIBS, RDB)

The NORTEL-UEMG-PERFMON-MIB will be modified so the simple names of the items for Thresholds and Overload will be modified to no longer reference the DCC.

New Mib for the VMG provisioning of IP Sec: TBD

1.7 OSS Changes

In previous releases the northbound interfaces were required to change the prefix for their event channels and fault manager entries. In SN06.2 the prefix was Subnet_62. With SN07 the entry changed to Subnet_7.

As of SN08, there will NO LONGER be the need to change this prefix in the northbound interfaces. As of SN08 - the MG9kEM will henceforth use Subnet_7 as its prefix.

Example ORB entry changes:

SN06.2

EventChannel = "Subnet_62.ec.Oss"

FaultServiceManger = "Subnet_62.Service.FaultServiceManager"

SN07

EventChannel = "Subnet_7.ecc.Oss"

FaultServiceManager = "Subnet_7.Services.FaultServiceManager"

SN08

EventChannel = "**Subnet_7**.ecc.Oss"

FaultServiceManager = "**Subnet_7**.Services.FaultServiceManager"

The reason we can now do this is that SN07 and SN08 will NEVER be running at the same time. When SN08 is deployed - it will also use the same prefix (Subnet_7). This is because at any given time only ONE instance of these (SN07, SN08) - may be running on a server.

1.8 External Interface Changes

With SN07 the TL1 Adaptor for SN07 was required to change its connecting port to 2363. This port will not be required to change for SN08 and will remain at 2363.

In SN07, the EM's SNMP listening port was modified to be 8002. This will not change for SN08. The SNMP port will be 8002.

1.9 MG9000 Element Management

1.9.1 New/modified GUIs

From the current SLOA GUI, the craftsperson will be able to enable or disable IPSec and IKE on the call control channel from the MG9000's ITP to gateway controller.

The craftsperson will have the option of using Office Wide Defaults for the VMG security parameters. The defaults will be managed from, oddly enough, the current Office Wide Defaults GUI.

A new HTML security web page is available for the craftsperson to use to secure the MG9000 Element Manager server machine. Using the interface, secure communication with the MG9000 is possible.

In regards to the addition of ABI/ITP Overload Controls, the same Overload Threshold Pane that is now in existence for the DCC Cards will be applied to the ITP/ABI Cards. The user may access this via the existing Manage Thresholds functionality.

1.9.2 GUI information

1.9.2.1 GUI name: Office Wide Defaults

Office Wide Defaults

1.9.2.1.1 Functional description

This GUI will be used to define default security parameters that may be used during VMG provisioned. These parameters will be used in securing the call control link between the VMG and the gateway controller.

Added to the Office Wide Defaults GUI will be a section for Security. This section will have three parameters:

1. Security OFF, ON
2. IKE preshared key
3. IKE time to live

1.9.2.1.2 GUI usage and implications

Office Wide defaults should be assigned first before provisioning VMGs.

1.9.2.1.3 GUI fields

The following table lists the security fields for Office Wide Defaults GUI.

Table 1 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Security	New	No	OFF, ON	Default = OFF Indicates whether or not security is enabled.	TBD
IKE Preshare key	New	No	26 digit HEX string?	Preshared key used in the IKE establishment of a secure call control link.	TBD
IKE Time To Live	New	No	Non-negative integer	How long the currently established security session will last?	TBD

1.9.2.1.4 Usage example

The following example shows sample datafill for the Office Wide Defaults GUI:

Screenshot of the Office Wide Defaults GUI with IPSec parameters shown to be provided later.

1.9.2.1.5 GUI release history update

The following information was added:

Security section added to Office Wide Defaults GUI.

1.9.2.1.6 Supplementary information

None

1.9.2.1.7 CLUI Interface

Not applicable

1.9.2.2 GUI name: SLOA

Switched Line Services for MG9000

1.9.2.2.1 Functional description

This GUI will be used to define security parameters to be used in securing the call control link between the VMG and the gateway controller.

Added to the GW Controller Config tab will be a section for Security. This section will have three parameters:

1. Security OFF, ON or OfficeWide Default
2. IKE preshared key
3. IKE time to live

1.9.2.2.2 GUI usage and implications

GUIs must be used in the following sequence:

Optional: Office Wide defaults should be assigned first before provisioning VMGs.

1.9.2.2.3 GUI fields

The following table lists the security fields for SLOA GUI on the GW Controller Config tab.

Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Security	New	No	OFF, ON, Officewide Defaults	Default = OFF Indicates whether or not security is enabled. Option is to use the office wide defaults. If OfficeWide Defaults are selected the remaining fields are grayed out.	TBD
IKE Preshare key	New	No	26 digit HEX string?	Preshared key used in the IKE establishment of a secure call control link.	TBD
IKE Time To Live	New	No	Non-negative integer	How long the currently established security session will last?	TBD

1.9.2.2.4 Usage example

The following example shows sample datafill for the SLOA GUI:

Screenshot of SLOA GUI with IPSec parameters shown to be provided later.

1.9.2.2.5 GUI release history update

The following information was added:

Security section added to GW Controller Config tab.

1.9.2.2.6 Supplementary information

None

1.9.2.2.7 CLUI Interface

Not applicable

1.9.2.3 GUI name: SSPFS Security

SSPFS Security Interface

1.9.2.3.1 Functional description

This HTML webpage will be used to define security parameters to secure communications into and out from this SSPFS Machine. This includes MG9000 Element Manager to MG9000 OAM&P communications.

The craftsperson will be presented with a number of tables representing currently provisioned security parameters. Options to add and delete parameters are available. Adding parameters will be performed using HTML forms.

1.9.2.3.2 GUI usage and implications

Primary usage of this interface is to secure the OAM&P communications channel between the MG9000 and Element manager.

This interface provides for securing all 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.

1.9.2.3.3 GUI fields

The following table lists the security fields for SSPFS Security Interface.

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
TBD	TBD	TBD	TBD	TBD	TBD

1.9.2.3.4 Usage example

The following example shows sample datafill for the SSPFS Security Interface.:

Screenshot of the SSPFS Security Interface with IPSec parameters shown to be provided later.

1.9.2.3.5 GUI release history update

The following information was added:

Initial availability.

1.9.2.3.6 Supplementary information

None

1.9.2.3.7 CLUI Interface

Not applicable

1.10 Command interface changes

TBD

1.11 Security

1.11.1 Network configuration

No changes to the network are necessary to support the IPSec implementation.

1.11.2 Key management

1.11.2.1 VMG IKE Preshared key

VMG IKE preshared keys will be input by the user when provisioning a VMG. The key will be stored encrypted in the Oracle database. The will be sent the the MG9000 encrypted and stored in the MIB encrypted.

1.11.2.2 SSPFS IKE Preshared key

The SSPFS IKE preshared key be input by the user in the SSPFS Security Servlet. This key is secured by the use of secure http from the browser to the server. *Solaris stores all keys XXXXX.*

1.11.3 Protocol

IPSec is being used on the Solaris machine.

1.11.4 Authentication

Succession login will be used for SSPFS Security Servlet.

1.12 Configuration Walkthrough

1.12.1 OAM&P Security

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, thru the LCI, the craftsperson will enable security on the management link to the Element Manager.
3. The craftsperson will then use a web browser and connect to the MG9000 Element Manager server machine. (Not the Mid-Tier machine) After logging in, the craftsperson will enable security on communications with the MG9000 IP address.
4. Cold start from MG9000 or manual discovery from Element Manager.
5. This will complete securing the OAM&P link.

1.12.2 VMG Security

From a high-level here are the steps to enable security on the call control links.

1. From SESM, enable security on the Gateway Controller.

2. From the SLOA GUI, provision a VMG. Enable security on the GW Controller Config tab.
3. This will complete securing the Call Control link.

2: A00006226 Configuration (CN)

2.1 Feature name

NTPOLL: Restructuring and Table Control

2.2 Hardware and Software Requirements

2.3 Initial Configuration

2.4 Office/Subnet parameters (OP/SP) (CM & SESM)

2.5 Upgrade Considerations

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)
NTPOLL	New	New

2.6.2 Table/MIB/Remote Database Schema information

2.6.2.1 Name: NTPOLL

2.6.2.1.1 Functional description

Table NTPOLL is a new table which contains the steps (one per tuple) taken by the DMS polling system (administered by the POLL and POLLSCHD CI commands). This type of polling is existing functionality which gathers various information about the switch and stores the results in output files on either SFDEV or NTDEV. Previously, the user could not add, delete, or manipulate the polling steps as they were defined internally by the system at initialization time. This table allows the user that flexibility. Initially, the polling steps are still defined by the system. These system defined steps will be automatically entered into Table NTPOLL by the system. After that, the user is free to add, delete, or manipulate the polling steps. The system defines over 430 polling steps, so initially Table NTPOLL will have that many tuples.

2.6.2.1.2 Usage sequence and implications (CM Only)

Table NTPOLL has no dependencies on other tables.

2.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NTPOLL	0	1023	SEGSTOR and FREEMAPS are used to manage memory.

2.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for Table NTPOLL.

The following fields exist in all tuples.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
STEPNUM	new	n/a	{0..1023}	Step number. With the INSERT field, this is part of the key for the table. If there are n polling steps, STEPNUM will range from 0 to n-1. The step numbers in the table will be kept in order and consecutive by the system.
INSERT	new	n/a	{N, Y}	This bool is only meaningful and should only be set to Yes if the user wishes to add a new tuple between two existing tuples.
LONG	new	n/a	{N, Y}	A bool which tells the system if this step is part of a long format polling report.
SHORT	new	n/a	{N, Y}	A bool which tells the system if this step is part of a short format polling report.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
USAGE	new	n/a	{N, Y}	A bool which tells the system if this step is part of a usage format polling report.
MEMCALC	new	n/a	{N, Y}	A bool which tells the system if this step is part of a memcalc format polling report.
STPTYP	new	This field has a refinement for TABLE and a refinement for CMPLX.	{TABLE, CMPLX}	The step type, either table or complex. Table steps gather information from other DMS tables. Complex steps gather information from the switch by executing one or more CI commands.

The following fields apply when STPTYP=TABLE.

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
TABNAME	new	n/a	String (1 to 8 chars)	The name of the DMS table to gather information from.
TSOPER	new	Refinement if TSOPER = LIST	{COUNT, LIST}	Denotes whether to list tuples from, or count the tuples of the table denoted stored in the TABNAME field.

IF TSOPER = LIST

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LISTOP	new	Refinement if LISTOP = FIRST or LAST	{ALL, FIRST, LAST}	Determines whether all the tuples should be listed, or the FIRST or LAST n tuples (if FIRST or LAST, see the next field, HOWMANY).

IF LISTOP = FIRST or LISTOP = LAST

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
HOWMANY	new	n/a	unsigned INT	The number of tuples to be listed from the table should be entered here. If LISTOP = FIRST, the first HOWMANY tuples are listed, and if LISTOP = LAST, the last HOWMANY tuples are listed.

The following fields apply when STPTYP = CMPLX.

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CMPLXTYP	new	n/a	{INT, EXT}	INT denotes an "internal" complex step. These tuples can ONLY be datafilled by the system and not by the user. EXT denotes an "external" complex step, i.e. one that is defined by the user. When an internal complex step is executed, an internal procedure in the code is run. When an external complex step is executed, the exact string in the CMPLXNAME field is executed as if it was a CI command typed by the user.

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CMPLXNAME	new	n/a	String (1 to 40 chars)	This string denotes the name of the complex step. In the case of an internal complex step, it is merely a name denoting the step. In the case of an external complex step, it is the actual command that will run at polling time.

2.6.2.1.5 Datafill example

The following example shows sample datafill for table NTPOLL.

The following example shows about 20 sample tuples from Table NTPOLL. Four types of tuples are shown:

- Table step (list)
- Table step (count)
- Complex step (internal)
- Complex step (external)

NOTES:

(1) Note that in the CMXPLXNAME field (i.e. the string associated with complex steps), spaces are represented as underscores. Internally, these underscores are converted to spaces but since space is the field separator in table control, this is necessary to keep the whole CMPLXNAME in one field.

(2) The system keeps the steps in order and consecutive. If there are n steps in the polling, the table keys will always be numbered 0 to n-1.

25 N N Y N N CMPLX INT DMSMON_-_PMLOADS

26 N N Y N N CMPLX INT DMSMON_-_ASSESS

27 N Y Y N N CMPLX INT DMSMON_-_HIGHPARMS

28 N Y Y N N CMPLX INT DMSMON_-_HIGHCAP

29 N Y Y N N CMPLX INT DMSMON_-_MEMORY

30 N Y Y N N CMPLX INT DMSMON_-_DBLOCKS

31 N Y Y Y Y CMPLX INT Exit_DMSMON

32 N Y Y N N CMPLX INT Display_Office_Parms_Header

33 N Y Y N N TABLE OFCENG LIST ALL

34 N Y Y N N TABLE OFCOPT LIST ALL

35 N Y Y N N TABLE OFCSTD LIST ALL

36 N Y Y N N TABLE OFCVAR LIST ALL

37 N N N N Y CMPLX INT Display_MEMCALC_Office_Parms

38 N Y Y N Y TABLE OFCAUT LIST ALL

39 N Y Y N Y CMPLX INT Gathering_Table_Counts_Header

40 N Y Y N Y CMPLX EXT LOGUTIL

41 N Y Y N Y CMPLX EXT OPEN_SWER

42 N Y Y N Y CMPLX EXT QUIT

43 N Y N N Y TABLE EDRAMINV COUNT

44 N Y N N N TABLE E911PSAP COUNT

2.6.2.1.6 Table release history update

This is a new table in SN08/CSP21.

2.6.2.1.7 Supplementary information

N/A

2.6.2.1.8 Translation verification and other tools

N/A

2.7 Service Orders (SO) (CM & SESM)

2.8 Software optionality control (SOC)

2.9 Element Management

2.10 User interface changes

2.11 OSSGate Interface Changes

2.12 Security

2.13 Configuration Walkthrough

3: A00006269 Configuration (CN)

3.1 Feature name

OSSGate Password No Echo

3.1 Upgrade Impact

This activity is responsible for handling modifications to OSSGate login. By default the OSSGate login functionality will be same as in SN07 and to turn on the new functionality, the user has to manually turn on an option via SESM configuration.

Prior to the SN07 release, login to the OSSGate involved entering username and password in one line separated by space, and the password entered was visible on the telnet window. In SN08, the user has to manually configure to turn on the OSSGate Password Control option in the SESM's OSSGate configuration section. Once this option is turned on, when attempting to login to OSSGate, it will prompt for the username first and then the password and the password being entered will not be displayed to the screen.

The default value of this OSSGate Password Control option is off, meaning the OSSGate login will be similar to SN07. This is done to minimize the impact to OSS operations, since the new login prompts of OSSGate will require changes in OSS vendor software. With this approach, it gives the customer the flexibility to turn on OSSGate password control option, when they are ready with changes to OSS vendor software. There is no impact after upgrades other than this OSSGate Password Control option is now available in SESM's OSSGate configuration section and the user can turn it on (default is off).

3.2 Data schema (DS) (CM, MIBS, RDB)

N/A

3.3 Service Orders (SO) (CM & SESM)

N/A

3.4 Element Management

N/A

3.5 User Interface

3.5.1 OSSGate Login prompt changes

This section shows the new login prompt prompted by OSSGate. The other functionality of OSSGate does not change except for the login prompt changes.

The user has to manually turn on the OSSGate Password Control option in order for this login change to take affect, as it is turned off by default.

Shown below is the screen capture of logging into OSSGate from SESM box. (user input is shown in **blue**). The new login prompts are shown in **red**.

```
#telnet localhost 10023
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^['.
```

Enter User Name

```
> ptm
```

Enter Password

```
>
```

```
ptm logged in on 04/04/16 at 09:02:40.
```

```
*****
**                                     **
**          OSS Gateway              **
**                                     **
**    This is a PRIVATE Database.      **
**                                     **
**    All activity is subject to monitoring.  **
**                                     **
**    Any UNAUTHORIZED access or use is PROHIBITED  **
**    and may result in PROSECUTION.      **
**                                     **
*****
** WARNING: Different service types require  **
** different formats. Consult the OSSGate User's **
** Guide, NE1004-512, for detailed information **
** regarding command formats and usage rules.  **
** Failure to do so can cause a mismatch between **
** XACore and SESM data.                  **
*****

SN07 Build: Apr 13, 2004 7:28:37 PM
*****
```

```
>
```

3.5.2 OSSGate configuration

In this section, the screen output below shows the new OSSGate Password Control option which needs to be turned on to enable OSSGate to not echo

password to the screen. The new configuration option is available in SESM's OSSGate configuration section and is shown in **red**. The user input is shown in **blue**.

After logging into the SESM box as root,

```
#cd /opt/nortel/NTsesm/admin/bin
```

```
#./configure
```

SESM configuration

- 1 - SESM common configuration (IP addresses, Market, CM CLI)
- 2 - SESM database tools
- 3 - SESM related applications configuration (MG9K, LMM, CICM)
- 4 - SESM provisioning configuration
- 5 - SESM logging configuration (syslog, sesm debug log)
- 6 - view sesm configuration settings
- 7 - SESM refresh properties

X - exit

select - **4**

SESM Provisioning Configuration

- 1 - XML Trunk Provisioning configuration
- 2 - OSSGate Provisioning configuration
- 3 - Office Provisioning Type configuration

X - exit

select - **2**

SESM OSSGate Provisioning Configuration

Enter the Primary Port OSSGate will use for telnet connections (default: 10023):

Enter the Secondary Port OSSGate will use for telnet connections (default: 11023):

Enter the OSSGate Timeout period, in seconds (default: 600):

Do you wish to have OSSGate Port Forwarding on for SSH [y/n]: **n**

Do you wish to turn on/off OSSGate Password Control option
(when this option is turned on, OSSGate will not echo
password on screen when logging onto it) [default:off]: **on**

Updating the property files with changed values, please wait...

Reloading the changed property values into memory, please wait...

3.5.3 Login prompt change implications

Prior to the SN08 release, the user name and password was prompted in the same line. In this release, however, there are two main changes which impact clients of OSSGate. They are

1. Instead of looking for login prompt “Enter username and password”, clients should look for “Enter User Name” prompt from OSSGate first. Once it gets this, the user name should be sent to OSSGate. Ossgate will then send “Enter Password” prompt. After receiving this prompt, the password should be sent to OSSGate.
2. OSSGate sends telnet echo off byte sequence to clients (to tell telnet clients to not display password entered onto screen) after sending the “Enter Password” prompt. This echo off byte sequence is necessary to make telnet client software not echo a password typed on screen.

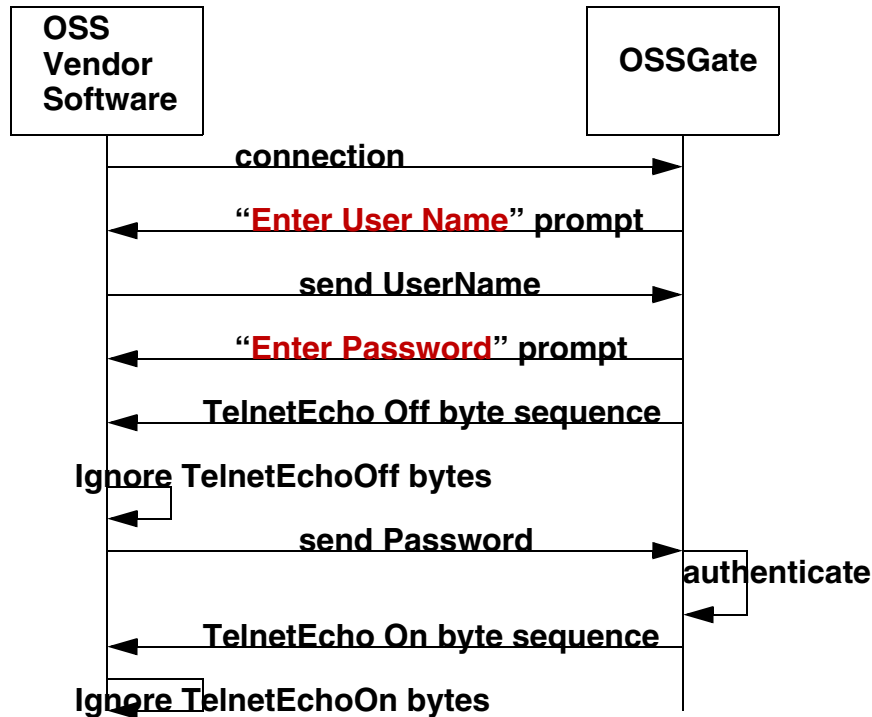
3.5.3.1 Impact to BPT tool

There are no external interface changes to BPT. Internally, BPT tool will handle the different prompts and will also strip telnet bytes and ignore them. But for users of BPT tool, there are no changes in the interface.

3.5.3.2 Impact to OSS vendor software

OSS software should be able to handle the new login prompts and also detect telnet bytes and strip these bytes and ignore them.

Shown in the Figure 1 below are the changes needed to be done to OSS vendor software to interact with OSSGate when the OSSGate password control option is enabled.

Figure 1 OSS Vendor software and its interaction with OSSGate

In the above figure, the new prompts are shown in dark red. The telnet bytes sent are explained below.

The Telnet Echo Off byte sequence are 3 bytes shown below

IAC WILL ECHO

IAC byte value is 255
 WILL byte value is 251
 ECHO byte value is 1

OSS software should look for these bytes and when received, just ignore them

The Telnet Echo On byte sequence are 3 bytes shown below

IAC WONT ECHO

IAC byte value is 255
 WONT byte value is 252
 ECHO byte value is 1

4: A00006347 Configuration (CN)

4.1 Feature name

Solaris 9 Introduction To SSPFS

4.2 IM Changes

It must be noted that for fresh installations of SN08 SSPFS, there will be a required change in the IM manuals. There are now three SSPFS disks instead of two.

Since there seems to not be a section for IM documentation, I will note the changes for the IM here.

There are new steps required to install the new disk 2. Following is a log of that portion of the installation:

Starting Web Start Launcher in Command Line Mode.

Please specify the media from which you will install Solaris 9 Software 2 of 2 (4/04 SPARC Platform Edition).

Alternatively, choose the selection for “Skip” to skip this disc and go on to the next one.

Media:

1. CD/DVD
2. Network File System
3. Skip

Media [1]: syslogd: line 24: WARNING: loghost could not be resolved

syslogd: /var/log/auditlog: No such file or directory
syslogd: /var/log/customerlog: No such file or directory
syslogd: /var/log/debuglog: No such file or directory
syslogd: /var/log/securitylog: No such file or directory
syslogd: /var/log/sspfslog: No such file or directory
syslogd: /var/log/upsuite: No such file or directory

May 27 12:40:34 nevada sendmail[515]: My unqualified host name (nevada) unknown;

sleeping for retry

Please insert the CD/DVD for Solaris 9 Software 2 of 2 (4/04 SPARC Platform Edition).

After you insert the disc, please press Enter.

Enter S to skip this disc and go on to the next one.
To select a different media, enter B to go Back.

[]

Reading Solaris 9 Software 2 of 2 (4/04 SPARC Platform Edition).... |

Launching installer for Solaris 9 Software 2 of 2 (4/04 SPARC Platform Edition). Please Wait...

Installing Solaris 9 packages (part 2)

| -1%-----25%-----50%-----75%-----100%|

Installation details:

Product	Result	More Info
1. Solaris 9 packages (part 2)	Installed	Available
2. Done		

Enter the number corresponding to the desired selection for more information, or enter 2 to continue [2]:

<Press Return to reboot the system> {"!" exits}
[]

In addition, you can find an installation guide at:

http://sspfs/SN07.1/SN07.1_InstallGuide.html

4.3 Hardware and Software Requirements

For the upgrade, the user must have fieldgrade Netra t1400s or N240s.

4.4 Initial Configuration

N/A

4.5 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

4.6 Upgrade Considerations

Until issues with DiskSuite and prototyping has been completed, the upgrade portion of this document cannot be completed.

4.7 Data schema (DS) (CM, MIBS, RDB)

N/A

4.8 Service Orders (SO) (CM & SESM)

N/A

4.9 Software optionality control (SOC)

N/A

4.10 Element Management

N/A

4.11 User interface changes

N/A

4.12 Security

N/A

4.13 Configuration Walkthrough

N/A

5: A00006450 Configuration (CN)

5.1 Feature name

TL1 Line Test Interface for MG9K Lines

Note: This feature impacts upgrades/downgrades only.

5.2 Hardware and Software Requirements

5.3 Initial Configuration

5.4 Office/Subnet parameters (OP/SP) (CM & SESM)

5.5 Upgrade Considerations

This feature introduces a dependency in the upgrade sequence of the Access Care system with the rest of the Succession components.

When upgrading **from** releases prior to SN07 **to** SN07 and greater, it is required that Access Care be upgraded **ONLY after the CMT, MG9K-EM and MG9K** upgrades are complete. Failing to do so will disable Line test capabilities between Access care and the MG9K.

5.5.1 Dump and Restore (CM)

N/A

5.5.2 Element Management Upgrade

There are no changes to the upgrade sequence for element managers.

5.5.3 Downgrade impact

If network downgrade is performed from a release higher than SN07 to a release lower than SN07, then Access Care **MUST** be downgraded **FIRST** to allow line test to function correctly.

5.6 Data schema (DS) (CM, MIBS, RDB)

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: A00006570 Configuration (CN)

6.1 Feature name

CS2M Robustness enhancement - Moving SDM IP & CLLI input to SSPFS

6.2 Hardware and Software Requirements

None.

6.3 Initial Configuration

None.

6.4 Office/Subnet parameters (OP/SP) (CM & SESM)

None.

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 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
pfrsScheduler	CHANGED	UnChanged

6.6.2 Table/MIB/Remote Database Schema information

6.6.2.1 NPM table: pfrsScheduler

6.6.2.1.1 Fields/OIDs

The following table lists fields/OIDs for pfrsScheduler.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
clli	Removed		VARCHAR(20)	Field clli is removed from this table. NPM transfers to use CM CLLI in /etc/profile

6.6.2.1.2 Table release history update

— Field “cli” removed from table pfrsScheduler

6.6.2.1.3 Supplementary information

None

6.6.2.1.4 Translation verification and other tools

pfrsScheduler does not use translation verification tools.

6.7 Service Orders (SO) (CM & SESM)

None.

6.7.1 Element Management

6.7.1.1 New/modified GUIs

Table 3 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
LMM	Changed

6.7.2 GUI information

6.7.2.1 GUI name: LMM

Line Maintenance Manager Graphical User Interface

6.7.2.1.1 Functional description

The LMM will be changed to let user input SDM IP instead of CM CLLI to transfer to another core server.

6.7.2.1.2 GUI usage and implications

Current datafill order unchanged.

6.7.2.1.3 GUI size

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
LMM	Unchanged	Unchanged	Unchanged
CS2M	Unchanged	Unchanged	Unchanged

6.7.2.1.4 Usage example: Set New CS CLLI

The following example shows sample datafill or menu selection for GUI

LMM:

Select “Set CS CLLI...” from LMM menu:

Line Maintenance Manager - Connected to: 47.153.133.245

Configure Preferences Actions Diagnostics Help

Re-Connect to LMM Server

Set CM CLI...

SDM/CBM IP: 47.153.132.177 CM CLI: JNANCICC01N

Exit

Post

SDM/CBM IP: 47.153.132.177
CM CLI : JNANCICC01N

Endpoint State
Communication Error

Gateway
Profile

Number	CLI	Line State

Clear All Refresh All < Prev

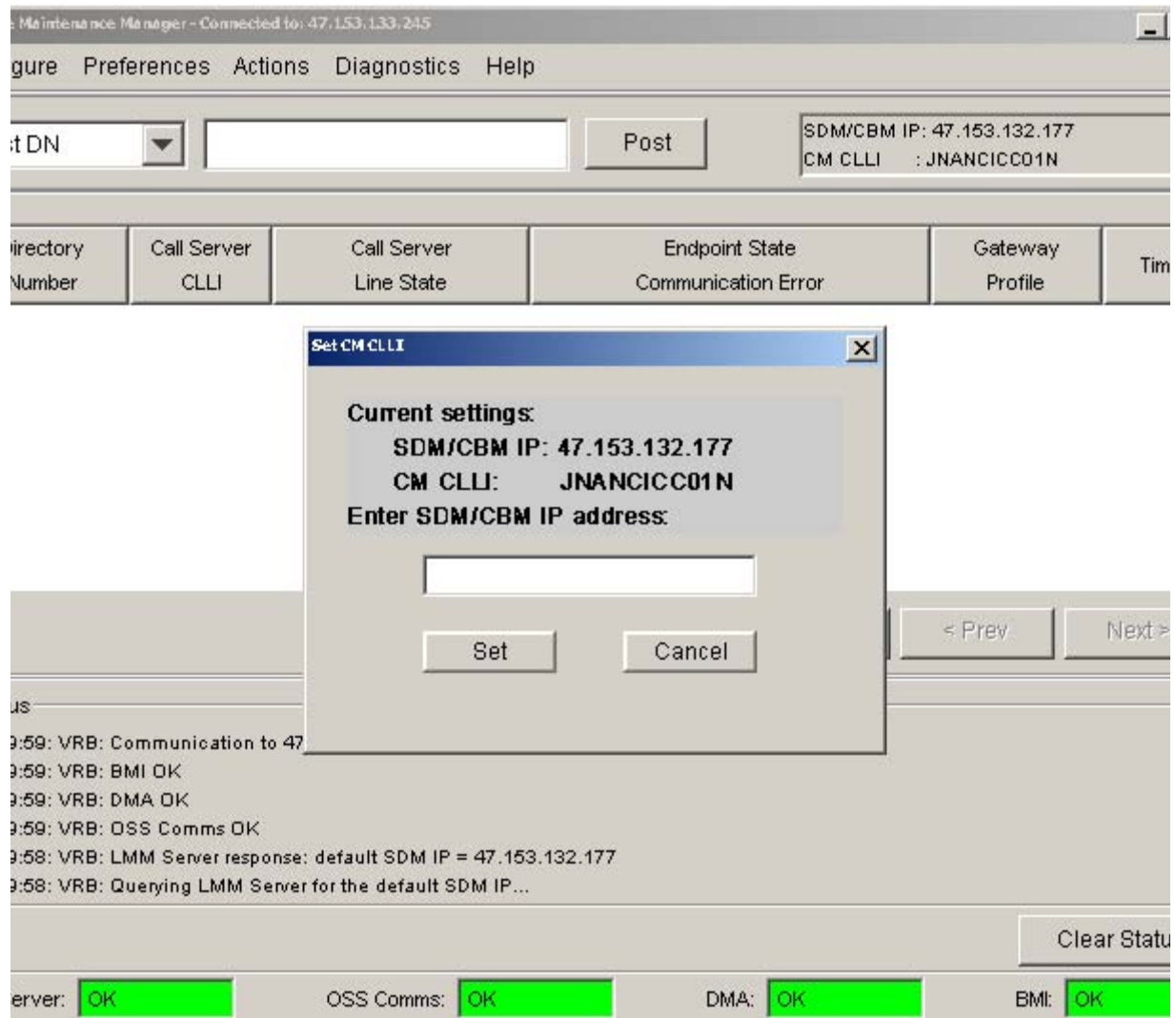
Status

11:39:59: VRB: Communication to 47.153.132.177: SUCCESSFUL
11:39:59: VRB: BMI OK
11:39:59: VRB: DMA OK
11:39:59: VRB: OSS Comms OK
11:39:58: VRB: LMM Server response: default SDM IP = 47.153.132.177
11:39:58: VRB: Querying LMM Server for the default SDM IP...

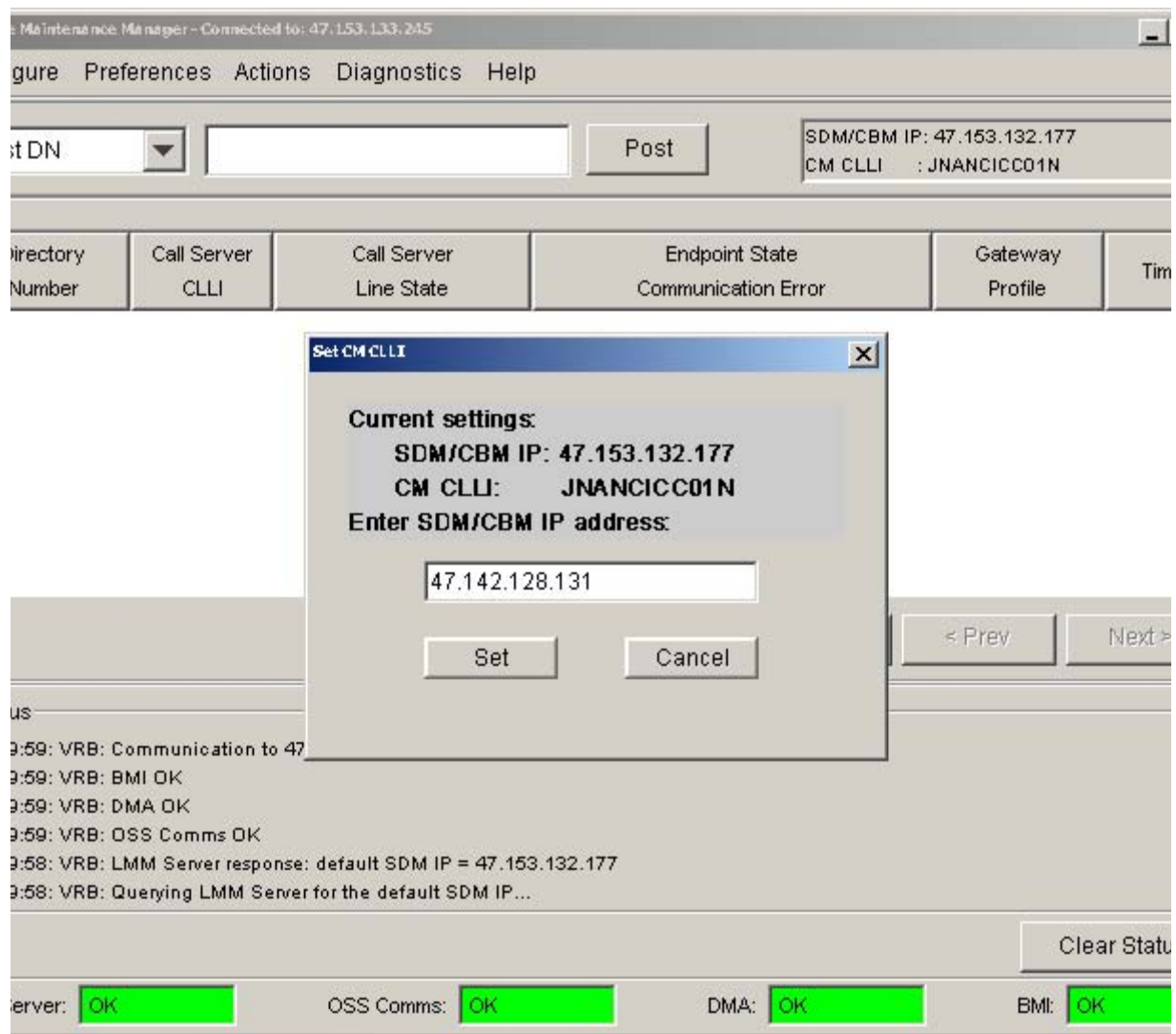
Cle

LMM Server: OK OSS Comms: OK DMA: OK BMI: O

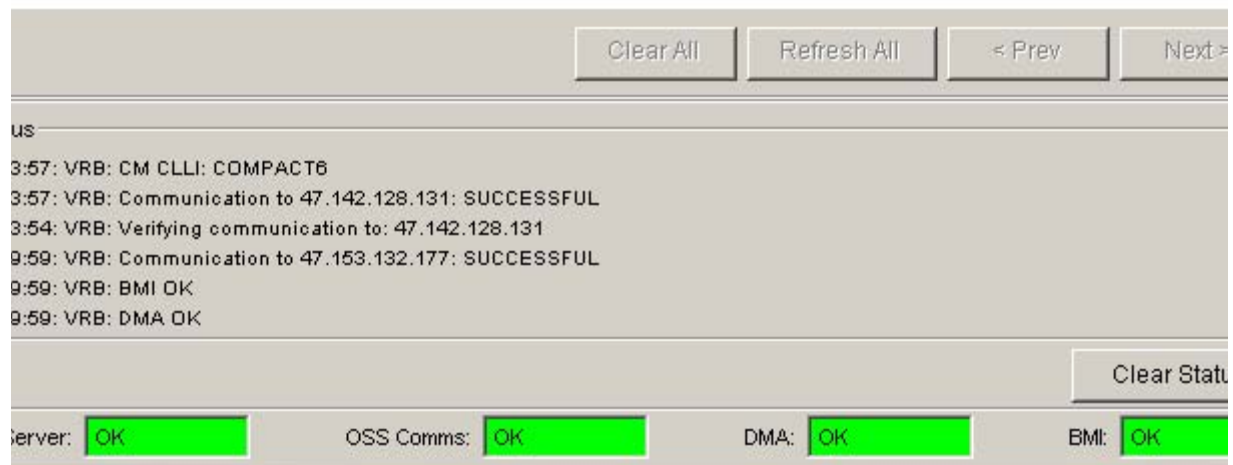
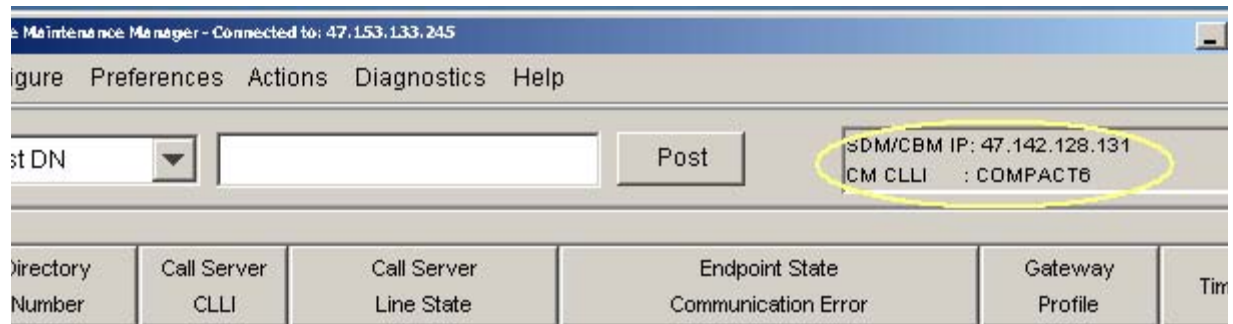
A dialog pops up to let user input SDM IP:



Input the SDM IP:



SDM IP is verified and the CM CLI is retrieved and set on client GUI.



6.7.2.1.5 GUI release history update

The following information was changed:

For the menu of “Set CS CLI“, it pops up a dialog to prompt user inputting SDM IP instead of CM CLI.

6.7.2.1.6 Context sensitive launching information

None.

6.7.2.1.7 Supplementary information

None.

6.7.2.2 GUI name: TMM

Trunk Maintenance Manager Graphical User Interface

6.7.2.2.1 Functional description

The TMM will be changed to let user input SDM IP instead of CM CLLI to transfer to another core server.

6.7.2.2.2 GUI usage and implications

Current datafill order unchanged.

6.7.2.2.3 GUI size

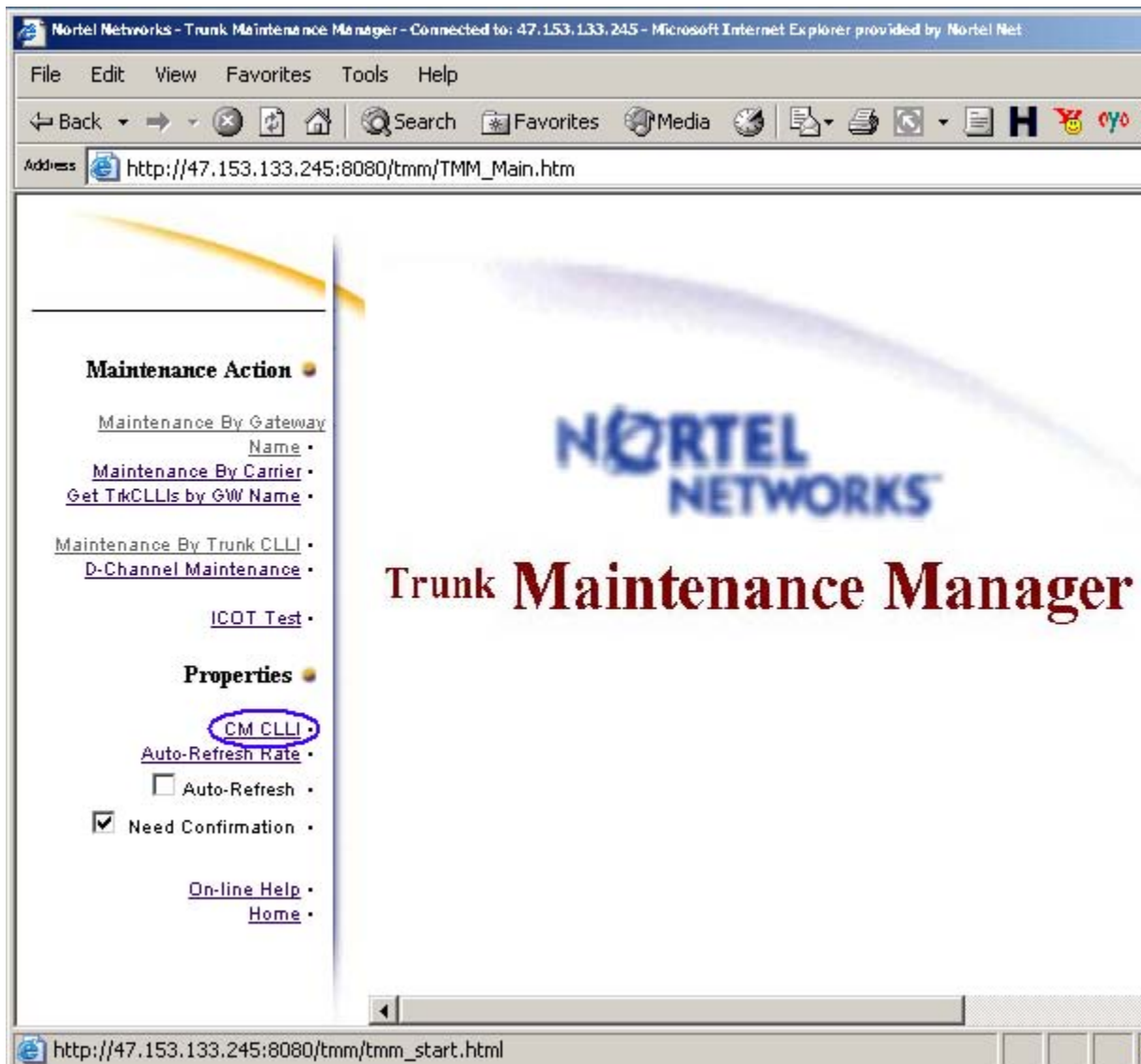
Table 5 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
TMM	Unchanged	Unchanged	Unchanged
CS2M	Unchanged	Unchanged	Unchanged

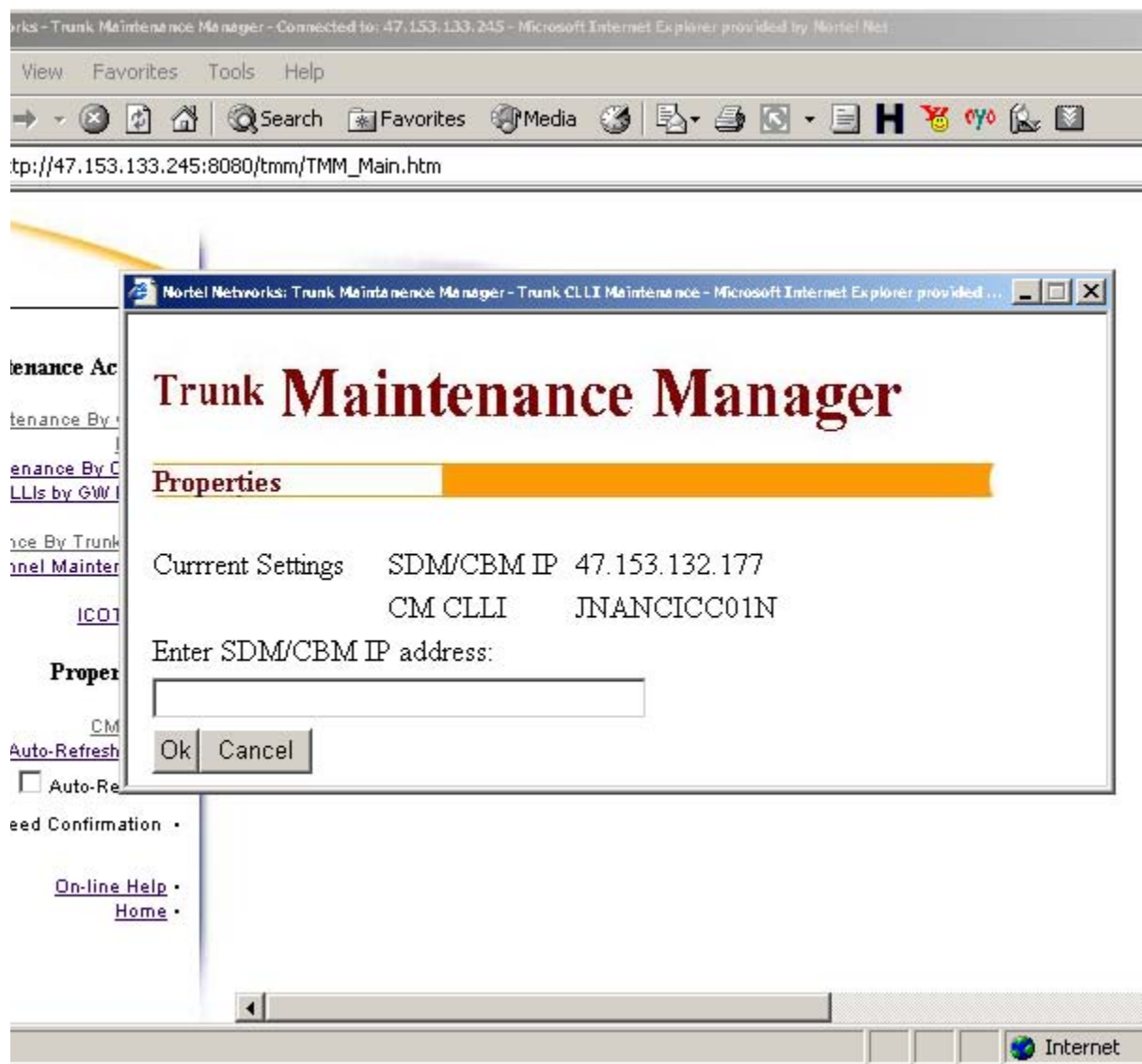
6.7.2.2.4 Usage example: Set New CM CLLI

The following example shows sample datafill or menu selection for GUI TMM:

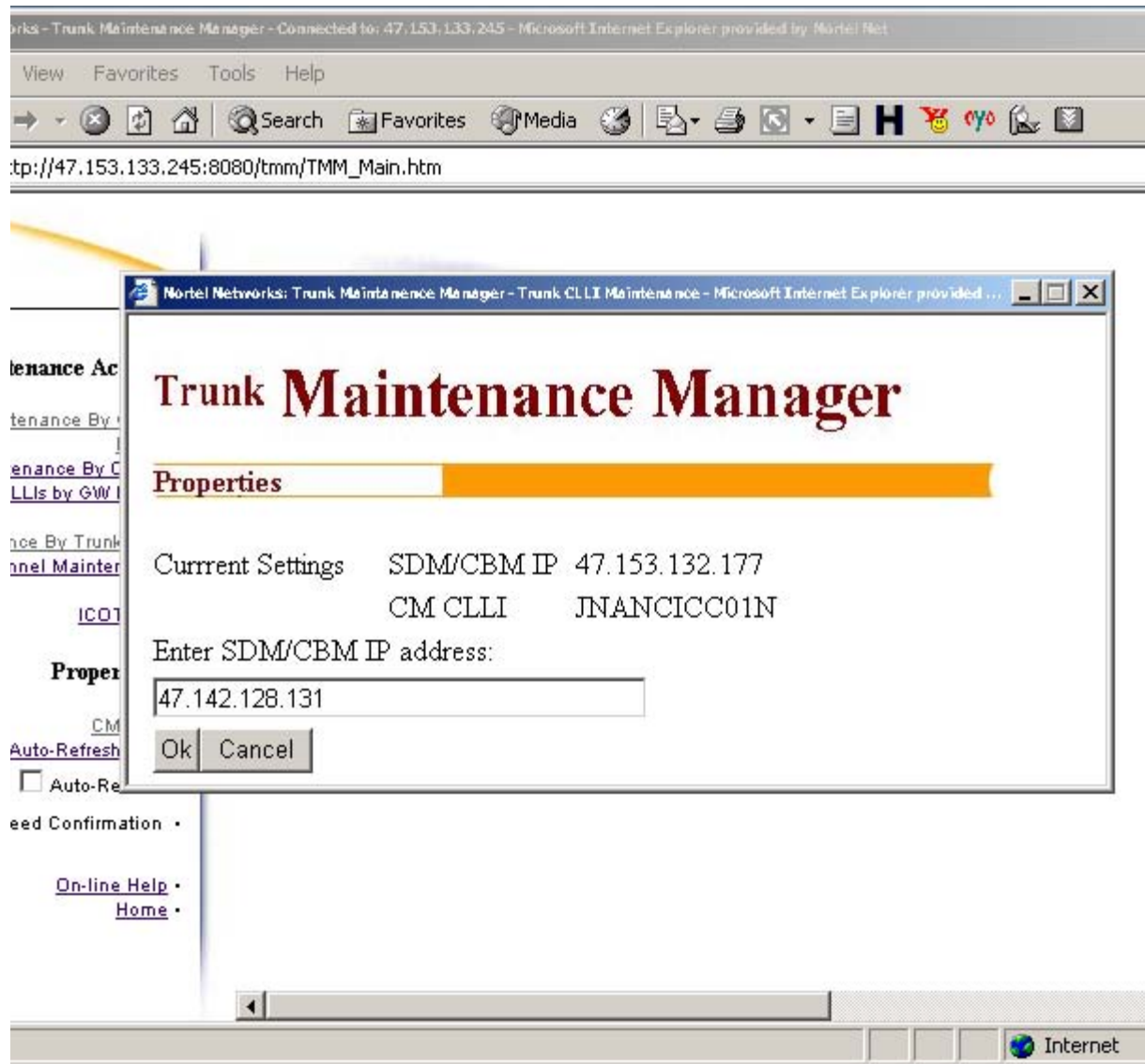
Click the “CM CLLI” from left menu:



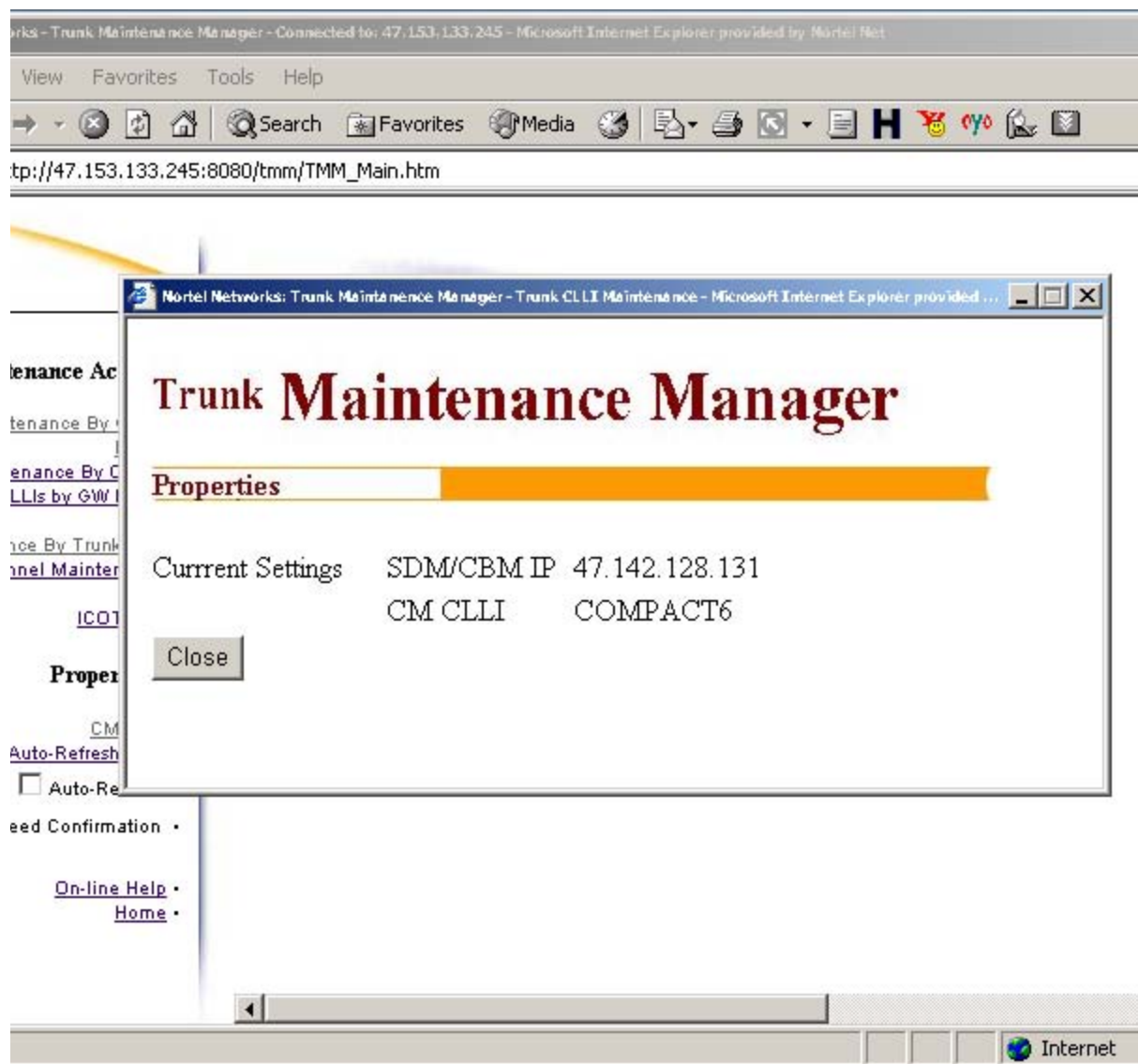
A dialog pops up to show the current settings. A input box which let user input SDM IP:



Input the SDM IP:



SDM IP is verified and the CM CLI is retrieved and set on client GUI.



6.7.2.2.5 GUI release history update

The following information was changed:

For the menu of “CM CLI”, it pops up a dialog to prompt user inputting SDM IP instead of CM CLI.

6.7.2.2.6 Context sensitive launching information

None.

6.7.2.2.7 Supplementary information

None.

6.8 User interface changes

6.8.1 SSPFS Installation Changes:

A step of SDM IP configuration is added to SSPFS installation for cs2kmt, cs2kaps, iemscs2k packages.

In this section, the screen output below shows the new step added in SSPFS installation process. The new step is shown in **blue**. The user input is shown in **red**.

Adding NTci (cs2kmt Profile Software Package 18 of 18)

Unzipping NTci From the Cdrom

.

Installing NTci Package

..

Done Installing NTci Package...

Executing server profile specific commands

Will the SDM IP be specific now? (y/n) **y**

Enter the ip address of the SDM [] **47.142.128.131**

Retrieving CM CLLI. Please wait a minute.....

SDM IP: 47.142.128.16

CM CLLI: COMPACT6

Enter "ok" to accept current settings **ok**

Please perform a logout and login so your
shell will pick up the SDM environment settings

SDM IP and CM CLLI is Successfully Configured

Unzipping DCE From The Cdrom

.....

6.8.2 SSPFS cli Tool Changes

SSPFS cli tool has some changes as below:

1. For cs2kmt, cs2kaps, iemscs2k packages, retrieve the CM CLLI while user configures the SDM IP in menu sdm_conf
2. Split the SDM IP configure and SDM User configure into two separate menus.
3. Binding the ddmsproxy to cli tool

In this section, the screen output below shows the cli tool changes in SSPFS. The new step is shown in blue. The modified menu is shown in magenta. The user input is shown in red.

6.8.2.1 sdm_conf

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 - 4

OAMP Application Configuration

- 1 - sdm_conf (Configure SDM IP Address)
- 2 - sdm_unconf (Unconfigure SDM IP Address)
- 3 - sdmuser_conf (Configure SDM User)
- 4 - sdmuser_unconf (Unconfigure SDM User)

-
- 5 - cmClli_rediscovery (Re-discovery the CM CLLI by SDM IP)
 - 6 - cmClli_conf (Configure CM_CLLI Address)
 - 7 - cmClli_unconf (Unconfigure CM_CLLI IP Address)
 - 8 - cm_conf (Configure CM IP Address)
 - 9 - cm_unconf (Unconfigure CM IP Address)

X - exit

select - 1

=== Executing "sdm_conf"

Enter the ip address of the SDM [] 47.142.92.26

Retrieving CM CLLI. Please wait a minute.....

SDM IP: 47.142.128.16
CM CLLI: COMPACT6

Enter "ok" to accept current settings ok

Please perform a logout and login so your
shell will pick up the SDM environment settings

SDM IP and CM CLLI is Successfully Configured

OAMP Application Configuration

- 1 - sdm_conf (Configure SDM IP Address)
- 2 - sdm_unconf (Unconfigure SDM IP Address)
- 3 - sdmuser_conf (Configure SDM User)
- 4 - sdmuser_unconf (Unconfigure SDM User)
- 5 - cmClli_rediscovery (Re-discovery the CM CLLI by SDM IP)
- 6 - cmClli_conf (Configure CM_CLLI Address)
- 7 - cmClli_unconf (Unconfigure CM_CLLI IP Address)
- 8 - cm_conf (Configure CM IP Address)
- 9 - cm_unconf (Unconfigure CM IP Address)

X - exit

select - x

6.8.2.2 sdmuser_conf

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 - 4

OAMP Application Configuration

- 1 - sdm_conf (Configure SDM IP Address)
- 2 - sdm_unconf (Unconfigure SDM IP Address)
- 3 - sdmuser_conf (Configure SDM User)
- 4 - sdmuser_unconf (Unconfigure SDM User)
- 5 - cmClli_rediscovery (Re-discovery the CM CLLI by SDM IP)
- 6 - cmClli_conf (Configure CM_CLLI Address)
- 7 - cmClli_unconf (Unconfigure CM_CLLI IP Address)
- 8 - cm_conf (Configure CM IP Address)
- 9 - cm_unconf (Unconfigure CM IP Address)

X - exit

select - 3

=== Executing "sdmuser_conf"

Enter the SDM user name for file management []swld

SDM User Name swld

Enter "ok" to accept current settings ok

Please ensure that you follow the SSPFS instructions
on setting up the SSH keys for SDM-SSPFS communications

In addition, please perform a logout and login so your
shell will pick up the SDM environment settings

SDM User Successfully Configured

=== "sdmuser_conf" completed successfully

OAMP Application Configuration

- 1 - sdm_conf (Configure SDM IP Address)
- 2 - sdm_unconf (Unconfigure SDM IP Address)
- 3 - sdmuser_conf (Configure SDM User)
- 4 - sdmuser_unconf (Unconfigure SDM User)
- 5 - cmClli_rediscovery (Re-discovery the CM CLLI by SDM IP)
- 6 - cmClli_conf (Configure CM_CLLI Address)
- 7 - cmClli_unconf (Unconfigure CM_CLLI IP Address)
- 8 - cm_conf (Configure CM IP Address)
- 9 - cm_unconf (Unconfigure CM IP Address)

X - exit

select - x

6.8.2.3 cmClli_rediscovery

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 - 4

OAMP Application Configuration

- 1 - sdm_conf (Configure SDM IP Address)
- 2 - sdm_unconf (Unconfigure SDM IP Address)
- 3 - sdmuser_conf (Configure SDM User)
- 4 - sdmuser_unconf (Unconfigure SDM User)
- 5 - cmClli_rediscovery (Re-discovery the CM CLLI by SDM IP)
- 6 - cmClli_conf (Configure CM_CLLI Address)
- 7 - cmClli_unconf (Unconfigure CM_CLLI IP Address)
- 8 - cm_conf (Configure CM IP Address)
- 9 - cm_unconf (Unconfigure CM IP Address)

X - exit

select - 5

=== Executing "cmClli_rediscovery "

Retrieve CM CLLI by SDM IP 47.142.92.26. Please wait a minute.....

CM CLLI old value: COMPACT5

CM CLLI new value: COMPACT5

CM CLLI does not changed. Please press any key to exit. <Enter>

=== "cmClli_rediscovery " completed successfully

OAMP Application Configuration

- 1 - sdm_conf (Configure SDM IP Address)
- 2 - sdm_unconf (Unconfigure SDM IP Address)
- 3 - sdmuser_conf (Configure SDM User)
- 4 - sdmuser_unconf (Unconfigure SDM User)
- 5 - cmClli_rediscovery (Re-discovery the CM CLLI by SDM IP)
- 6 - cmClli_conf (Configure CM_CLLI Address)
- 7 - cmClli_unconf (Unconfigure CM_CLLI IP Address)
- 8 - cm_conf (Configure CM IP Address)
- 9 - cm_unconf (Unconfigure CM IP Address)

X - exit

select - x

6.8.2.4 ddmsproxy menus:

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 - 17

Succession Element Configuration

1 - DDMSProxy Application Configuration

X - exit

select - 1

DDMSProxy Application Configuration

1 - ddmsproxy_query (Query the status of ddmsproxy service)

2 - ddmsproxy_stop (Stop the ddmsproxy service)

3 - ddmsproxy_start (Start up the ddmsproxy service)

X - exit

select - 1

=== Executing "ddmsproxy_query"

```
pmfadm -c ddmsproxyd -n 5 -t 60 /opt/nortel/ddmsproxy/bin/ddmsproxy.sh
    retries: 0
    owner: root
    pids: 9178 9180 9181
```

=== "ddmsproxy_query" completed successfully

DDMSProxy Application Configuration

1 - ddmsproxy_query (Query the status of ddmsproxy service)

2 - ddmsproxy_stop (Stop the ddmsproxy service)

3 - ddmsproxy_start (Start up the ddmsproxy service)

X - exit

select - 2

=== Executing "ddmsproxy_stop"

ddmsproxy service stopping

=== "ddmsproxy_stop" completed successfully

DDMSProxy Application Configuration

1 - ddmsproxy_query (Query the status of ddmsproxy service)

-
- 2 - ddmsproxy_stop (Stop the ddmsproxy service)
 - 3 - ddmsproxy_start (Start up the ddmsproxy service)

X - exit

select - 3
 === Executing "ddmsproxy_start"

ddmsproxy service starting

=== "ddmsproxy_start" completed successfully

DDMSProxy Application Configuration

- 1 - ddmsproxy_query (Query the status of ddmsproxy service)
- 2 - ddmsproxy_stop (Stop the ddmsproxy service)
- 3 - ddmsproxy_start (Start up the ddmsproxy service)

X - exit

select - x

6.8.3 SESM configure command changes

SESM command “configure” is changed to stop requiring user input SDM IP and CM CLLI. It reuses the SDM IP and CM CLLI from /etc/profile

configure

SESM configuration

- 1 - SESM common configuration (IP addresses, Market, CM CLLI)
- 2 - SESM database tools
- 3 - SESM related applications configuration (MG9K, LMM, CICM)
- 4 - SESM provisioning configuration
- 5 - SESM logging configuration (syslog, sesm debug log)
- 6 - view sesm configuration settings
- 7 - SESM refresh properties

X - exit

select - 1

SESM common configuration

SDM IP : 47.142.128.16
 CM CLLI : COMPACT5

Enter IP address of this machine (default: 47.153.133.245): <Enter>

SESM Market Selection

- 1 - International
- 2 - North American

Enter Market the SESM is to configured for: **2**

No mirroring performed as it is not necessary when NPM is on the local machine or cluster.

Setting address 47.153.146.200 in www/tmm.html

Setting address 47.153.146.200 in www/sesm.jnlp.template

Setting address 47.153.146.200 in www/lmm.jnlp.template

Setting address 47.153.146.200 in www/loginDialog.jnlp.template

Setting address 47.153.146.200 in www/config.js

Setting address 47.153.146.200 in settings

Setting communication host 47.153.146.200 in www/sesm.jnlp.template

Setting communication host 47.153.146.200 in www/lmm.jnlp.template

Setting communication host 47.153.146.200 in www/loginDialog.jnlp.template

Setting communication host 47.153.146.200 in www/config.js

Setting communication protocol http in www/sesm.jnlp.template

Setting communication protocol http in www/lmm.jnlp.template

Setting communication protocol http in www/loginDialog.jnlp.template

Setting communication protocol http in www/config.js

Setting communication port 8080 in www/sesm.jnlp.template

Setting communication port 8080 in www/lmm.jnlp.template

Setting communication port 8080 in www/loginDialog.jnlp.template

Setting communication port 8080 in www/config.js

Setting CM Host Name COMPACT5 in nv.sql

Setting CM Host Name COMPACT5 in nv_data.sql

SESM configuration

- 1 - SESM common configuration (IP addresses, Market, CM CLI)
- 2 - SESM database tools
- 3 - SESM related applications configuration (MG9K, LMM, CICM)
- 4 - SESM provisioning configuration
- 5 - SESM logging configuration (syslog, sesm debug log)
- 6 - view sesm configuration settings
- 7 - SESM refresh properties

X - exit

select - **x**

#

6.8.4 NPM command pfrsCli

NPM command pfrsCli stops requiring user to input CM CLI manually. It reuses the CM CLI in /etc/profile.

```
zsups231:/opt/nortel/NTnpm/bin> ./pfrscli
```

PFRS Configuration

- 1 - View
- 2 - Enable/Reconfigure
- 3 - Disable
- 4 - Patch retrieval (Now)
- 5 - Generate Report (Now)

X - exit

select - 2

Enter the hostname/IP of the patch file drop-off server [127.0.0.1]:47.153.146.200

220 ProFTPD 1.2.8 Server (Authorized Use Only) [zsups228]

Enter userid used to connect to the patch file drop-off server [ANONYMOUS]:maint

Enter password used to connect to the patch file drop-off server :maint

220 ProFTPD 1.2.8 Server (Authorized Use Only) [zsups228]

PFRS may not work if this user/passwd is used

Do you want to continue ? [n]:y

Enter time for patch retrieval cycle (hh:mm) [23:07]:10:00

Enter time for report generation cycle (hh:mm) [23:07]:10:00

Patch retrieval next cycle will be: 06-16-04 10:00

Report generation next cycle will be: 06-16-04 10:00

PFRS Configuration

- 1 - View
- 2 - Enable/Reconfigure
- 3 - Disable
- 4 - Patch retrieval (Now)
- 5 - Generate Report (Now)

X - exit

select - x

```
zsups231:/opt/nortel/NTnpm/bin>
```

6.9 OSSGate Interface Changes

None.

6.10 Security

None.

6.11 Configuration Walkthrough

Provisioning/configuring component software and services.

7: A00006693 Configuration (CN)

7.1 Feature name

XA-Core IO Capacity Monitoring Toolset

7.2 Hardware and Software Requirements

Not applicable.

7.3 Initial Configuration

Not applicable.

7.4 Office/Subnet parameters (OP/SP) (CM & SESM)

7.4.1 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	IO_WARNING_ THRESHOLD	NEW	XA-Core

7.4.2 Parameter information

7.4.2.1 IO_WARNING_THRESHOLD

IO_WARNING_THRESHOLD

7.4.2.1.1 Functional description

This parameter defines a utilization warning threshold for all IO service types (CMIC, ETHR, AMDI) in the system. The IOCAP monitoring toolset uses the value of this parameter to peg the IOTHRESH register of the IOCAP OM whenever the IO utilization level of any IO service has exceeded this threshold on the switch.

7.4.2.1.2 Provisioning rules

There is no formula for provisioning this office parameter. However, this office parameter should be set by the customer in such a manner that will allow sufficient advance warning time for their maintenance personnel to upgrade or reconfigure their IO devices in case the condition re-occurs often.

7.4.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
1	100	100

7.4.2.1.4 Activation

Any change activation for this office parameter is immediate.

7.4.2.1.5 Dependencies

Not applicable.

7.4.2.1.6 Consequences

If this office parameter is set low, the IOTHRESH register might be in pegged more often than necessary. If this office parameter is set high, the customer may not have enough advance notice to upgrade their IO configuration.

7.4.2.1.7 Verification

To verify, users can modify and display the value of IO_WARNING_THRESHOLD on table OFCENG via table control.

7.4.2.1.8 Memory requirements

No memory impact.

7.4.2.1.9 Parameter release history update

New office parameter in CSP20.

7.5 Upgrade Impact

Not applicable.

7.6 Data schema (DS) (CM, MIBS, RDB)

Not applicable.

7.7 Service Orders (SO) (CM & SESM)

Not applicable.

7.8 Software optionality control (SOC)

Not applicable.

7.9 Element Management

Not applicable.

7.10 Command interface changes

The following new directories will be provided in this feature.

7.10.1 Directory: CAPACITY

This existing CAPACITY MAPCI level will be modified to provide a new IOCAP MAPCI level in XA-Core only. The new IOCAP level will provide IO utilization and IO messaging throughput information for HCMIC and HIOP IO cards.

7.10.1.1 Directory description

This new IOCAP MAPCI level will be giving the IO utilization values and messaging throughput information for each IO service type (CMIC, ETHR and AMDI). The information on this new MAPCI level will be updated once every minute.

7.10.1.2 Accessing directory: CAPACITY

7.10.1.2.1 Access to directory or MAP level and return to CI

To access this directory, type:

> MAPCI; MTC; CAPACITY

To return to the CI environment, type:

> QUIT ALL

7.10.2 Command: IOCAP

This is a new command available under the CAPACITY MAPCI level in XA-Core only.

7.10.2.1 Command type: Listed MENU

7.10.2.2 Command target: XA-Core only

7.10.2.3 Command availability: RES

7.10.2.4 Command description

This new IOCAP MAPCI level will be giving the IO utilization values and messaging throughput information for each IO service type (CMIC, ETHR and AMDI). The information on this new MAPCI level will be updated once every minute.

7.10.2.5 Command syntax

Table 3 IOCAP command parameters and variables

Command	Parameters and variables
IOCAP	none
Parameters and variables	Description

7.10.2.6 Qualifications and warnings

Not applicable.

7.10.2.7 Responses

7.10.2.7.1 IOCAP response

Table 4 MAP outputs with associated meanings and actions

Command
Service: The type of IO service of the values shown on the same line is captured. Meaning: Possible IO service types are CMIC, ETHR and AMDI. System or user actions: Not applicable IOUTIL%: The average utilization of all active links in the system captured in the previous minute. Meaning: The value is given as a percent of total system and can take up to 3 digits. System or user actions: Not applicable TxMsg/s: The average number of transmitted messages captured in the last minute for this IO service type. Meaning: The unit is number of transmitted messages per second. System or user actions: Not applicable TxSize: The average size (in bytes) of all transmitted messages in the last minute. Meaning: The unit is in bytes. System or user actions: Not applicable RxMsg/s: The average number of received messages captured in the last minute for this IO service type. Meaning: The value unit is the number of received messages per second. System or user actions: Not applicable RxSize: The average size (in bytes) of all received messages in the last minute. Meaning: The unit is in bytes. System or user actions: Not applicable

This MAPCI level can be used for monitoring current IO throughput. Under normal condition, there is no response required from maintenance personnel. The descriptions of all fields displayed under this level are given above. These responses are seen in XA-core only.

7.10.2.8 Example

Table 5 Usage examples for IOCAP command

Description of task:	This new IOCAP MAPCI level will be giving the IO utilization values and messaging throughput information for each IO service type (CMIC, ETHR and AMDI). The information on this new MAPCI level will be updated once every minute.
Command:	MAPCI; MTC; CAPACITY; IOCAP
MAP response:	See example output below.

An example output of this new MAPCI level is given below.

IOCAP MAPCI Level

XACM	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
IOCAP									
0 Quit	CATMP/HR	UTIL	ENGCATMP	MAXCATMP	ENGLEVEL	CCOVRD	CMICOVRD	PESC	
2	120000	75	160000	200000	BELOW	OFF	OFF	NO	
3									
4	Service	IOUTIL%	TxMsg/s	TxSize	RxMsg/s	RxSize			
5									
6	AMDI	64	15324	107	13234	91			
7	CMIC	17	4102	202	1254	102			
8	ETHR	10	8967	123	3456	123			
9									
10	IOCAP:								
11									
12									
13									
14									
15									
16									
17									
18									
XMAP0									
Time 14:12 >									

7.10.3 Command: QUIT

This command will allow the user to exit IOCAP MAPCI level and to return to IOCAP higher MAPCI level (CAPACITY MAPCI level).

7.10.3.1 Command type: Listed MENU

This QUIT command is listed in IOCAP menu.

7.10.3.2 Command target: XA-Core only

This new IOCAP QUIT command is available in XA-Core only.

7.10.3.3 Command availability: RES

7.10.3.4 Command description

This command will allow the user to exit IOCAP MAPCI level and to return to IOCAP higher MAPCI level (CAPACITY MAPCI level).

7.10.3.5 Command syntax

Table 6 QUIT command parameters and variables

Command	Parameters and variables
QUIT	none

7.10.3.6 Qualifications and warnings

Not applicable.

7.10.3.7 Responses

7.10.3.7.1 QUIT

Table 7 MAP outputs with associated meanings and actions

Command
If QUIT is issued, the user will be returned to one MAPCI level higher than their current MAPCI level. If QUIT ALL is issued, the user will be returned to CI level. Meaning: Not applicable. System or user actions: Not applicable. Meaning: The IOCAP MAPCI level is exited and the user is returned to one MAPCI level higher or to CI level. System or user actions: Not applicable.

7.10.3.8 Example

Table 8 Usage examples for QUIT command

Description of task	Exit the IOCAP MAPCI level and return the user to CI level or one MAPCI level higher.
Command:	Example: QUIT ALL
MAP response:	Example: >

7.10.4 Directory: IOCAPCI

7.10.4.1 Directory description

This new IOCAPCI is provided to allow customers to display the IO utilization history data.

7.10.4.2 Accessing directory: IOCAPCI

7.10.4.2.1 Access to directory or MAP level and return to CI

To access this directory type:

> IOCAPCI

To return to CI environment, type:

> QUIT

7.10.5 Command: IOMAX

7.10.5.1 Command type: NON-MENU

7.10.5.2 Command target: XA-Core only

7.10.5.3 Command availability: RES

7.10.5.4 Command description

This command displays the hourly high watermark value captured for each IO service type (CMIC, ETHR or AMDI). The value is captured every hour of day for the last 31 days. The data survives all types of restarts (warm, cold and reload).

The date of the month will be in sequence. For every hour in the future (there is no data collected yet), a blank character will be displayed.

7.10.5.5 Command syntax

The command syntax for this command is as follows.

```
> q iomax
Display IO high watermark report.
Parms: <service> {CMIC,
                  ETHR,
                  ATM,
                  ALL}
```

Table 9 IOMAX command parameters and variables

Command	Parameters and variables
IOMAX	service
IOMAX	<Service> (CMIC, ETHR, AMDI, ALL)
Parameters and variables	Description
Service	Possible values are CMIC, ETHR, AMDI or ALL
CMIC	Displays only CMIC hourly max history data
ETHR	Displays only ETHR hourly max history data

Table 9 IOMAX command parameters and variables

Command	Parameters and variables
AMDI	Displays only AMDI hourly max history data
All	Displays all hourly.max history data for CMIC, ETHR, and AMDI.

7.10.5.6 Qualifications and warnings

Not applicable.

7.10.5.7 Responses**7.10.5.7.1 IOMAX response**

The following is the response if IOMAX CMIC is issued.

Table 10 MAP outputs with associated meanings and actions

Command
IOMAX CMIC: history data of CMIC hourly maximum utilization are displayed. Meaning: CMIC hourly maximum history data are displayed. System or user actions: Not applicable.
IOMAX ETHR: history data of ETHR hourly maximum utilization are displayed. Meaning: history data of ETHR hourly maximum utilization are displayed. System or user actions: Not applicable.
IOMAX AMDI: history data of AMDI hourly maximum utilization are displayed. Meaning: history data of AMDI hourly maximum utilization are displayed. System or user actions: Not applicable.
IOMAX ALL: history data of CMIC, ETHR, AMDI hourly maximum utilization are displayed. Meaning: history data of CMIC, ETHR, AMDI hourly maximum utilization are displayed. System or user actions: Not applicable.

7.10.5.8 Example**Table 11 Usage examples for IOMAX command**

Description of task	Display the history data of IO hourly max utilization.

Table 11 Usage examples for IOMAX command

Command: MAP response:	Example: IOMAX CMIC																										
	Example: Maximum CMIC Utilization																										
	Date	0	1	2	3	4	5	6	7	8	9	10	11	Hour		12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21			
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/29	8	7	8	10	8	9	7																				
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14			
Command: MAP response:	Example: IOMAX ETHR																										
	Example: Maximum ETHR Utilization																										
	Date	0	1	2	3	4	5	6	7	8	9	10	11	Hour		12	13	14	15	16	17	18	19	20	21	22	23
	2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21		
	2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/29	8	7	8	10	8	9	7																				
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14			
1/31	8	6	5	7	8	7	6	9	11	19	27																

Table 11 Usage examples for IOMAX command

Command: MAP response:	Example: IOMAX AMDI																										
	Example:																										
	Maximum AMDI Utilization																										
	Date	0	1	2	3	4	5	6	7	8	9	10	11	Hour		12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21		
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/29	8	7	8	10	8	9	7																				
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14			
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21			

Table 11 Usage examples for IOMAX command

Command: MAP response:	Example: IOMAX ALL																										
	Example: Maximum CMIC Utilization																										
	Date	0	1	2	3	4	5	6	7	8	9	10	11	Hour		12	13	14	15	16	17	18	19	20	21	22	23
	2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21		
	2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/29	8	7	8	10	8	9	7																			
	1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14		
	1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21		
	Maximum ETHR Utilization																										
	Date	0	1	2	3	4	5	6	7	8	9	10	11	Hour		12	13	14	15	16	17	18	19	20	21	22	23
	2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21		
	2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
	2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
	2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
	2/29	8	7	8	10	8	9	7																			
	1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14		
	1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21		

Table 11 Usage examples for IOMAX command

	Maximum AMDI Utilization																							
	Date	Hour																						
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8	7	8	10	8	9	7																	
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

7.10.6 Command: IOAVG**7.10.6.1 Command type: NON-MENU****7.10.6.2 Command target: XA-Core only****7.10.6.3 Command availability: RES****7.10.6.4 Command description**

This command displays the hourly average value captured for each IO service type (CMIC, ETHR or AMDI). The value is captured every hour of day for the last 31 days. The data survives all types of restarts (warm, cold and reload).

The date of the month will be in sequence. For every hour in the future (there is no data collected yet), a blank character will be displayed.

7.10.6.5 Command syntax

The command syntax for this command is as follows.

```
> q ioavg
Display IO average report.
Parms: <service> {CMIC,
                  ETHR,
                  ATM,
```

ALL}

Table 12 IOAVG command parameters and variables

Command	Parameters and variables
IOAVG	service
IOAVG	<Service> (CMIC, ETHR, AMDI, ALL)
Parameters and variables	Description
Service	Possible values are CMIC, ETHR, AMDI or ALL
CMIC	Displays only CMIC hourly average history data
ETHR	Displays only ETHR hourly average history data
AMDI	Displays only AMDI hourly average history data
All	Displays all hourly average history data for CMIC, ETHR, and AMDI.

7.10.6.6 Qualifications and warnings

Not applicable.

7.10.6.7 Responses**7.10.6.7.1 IOAVG response**

The following is the response if IOAVG CMIC is issued.

Table 13 MAP outputs with associated meanings and actions

Command
IOAVG CMIC: history data of CMIC hourly average utilization are displayed.
Meaning: CMIC hourly average history data are displayed.
System or user actions: Not applicable.
IOAVG ETHR: history data of ETHR hourly average utilization are displayed.
Meaning: history data of ETHR hourly average utilization are displayed.
System or user actions: Not applicable.
IOAVG AMDI: history data of AMDI hourly average utilization are displayed.
Meaning: history data of AMDI hourly average utilization are displayed.
System or user actions: Not applicable.

Table 13 MAP outputs with associated meanings and actions

Command
IOAVG ALL: history data of CMIC, ETHR, AMDI hourly average utilization are displayed.
Meaning: history data of CMIC, ETHR, AMDI hourly average utilization are displayed.
System or user actions: Not applicable.

7.10.6.8 Example

Table 14 Usage examples for IOAVG command

Description of task	Display the history data of IO hourly average utilization.																								
Command: MAP response:	Example: IOAVG CMIC																								
	Example: Average CMIC Utilization																								
	Hour																								
Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21	
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/29	8	7	8	10	8	9	7																		
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14	
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21	

Table 14 Usage examples for IOAVG command

Command: MAP response:	Example: IOAVG ETHR																									
	Example: Average ETHR Utilization																									
	Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	Hour	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21		
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/29	8	7	8	10	8	9	7																			
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14		
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21		

Command: MAP response:	Example: IOAVG AMDI																									
	Example: Average AMDI Utilization																									
	Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	Hour	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21		
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/29	8	7	8	10	8	9	7																			
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14		
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21		

Table 14 Usage examples for IOAVG command

Command: MAP response:	Example: IOAVG ALL																									
	Example: Average CMIC Utilization																									
	Hour																									
Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23		
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21		
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/29	8	7	8	10	8	9	7																			
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14		
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21		
	Average ETHR Utilization																									
	Hour																									
Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23		
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21		
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/29	8	7	8	10	8	9	7																			
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14		
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21		

Table 14 Usage examples for IOAVG command

	Average AMDI Utilization																							
	Date	Hour																						
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8	7	8	10	8	9	7																	
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

7.10.7 Command: DISP**7.10.7.1 Command type: NON-MENU****7.10.7.2 Command target: XA-Core only****7.10.7.3 Command availability: RES****7.10.7.4 Command description**

This DISP command displays the utilization and messaging throughput values of each IO service type of the last 60 minutes with option CURR (for example, when a command is issued at 2:35, displayed data is from 1:34 to 2:34) or previous full hour with option PREV (for example when a command is issued at 2:35, displayed data is from 1:00 to 2:00). This information survives all types of restarts (warm, cold and reload).

7.10.7.5 Command syntax

The command syntax for this command is as follows.

```
> q disp
Display table of IO utilization.
Parms: <when> {CURR,
               PREV}
       <service> {CMIC,
                  ETHR,
                  ATM,
                  ALL}
```

Table 15 DISP command parameters and variables

Command	Parameters and variables
DISP	<when> <service>
DISP	<when> (CURR, PREV)
	<service> (CMIC, ETHR, AMDI, ALL)
Parameters and variables	Description
When	Possible values are CURR or PREV
CURR	Displays the last 60 minutes utilization and messaging throughput of the specified IO service type
PREV	Displays the previous full hour utilization and messaging throughput of the specified IO service type
Service	Possible values are CMIC, ETHR, AMDI or ALL
CMIC	Displays only CMIC utilization and messaging throughput
ETHR	Displays only ETHR utilization and messaging throughput
AMDI	Displays only AMDI utilization and messaging throughput
ALL	Displays utilization and messaging throughput for CMIC, ETHR, and AMDI.

7.10.7.6 Qualifications and warnings

Not applicable.

7.10.7.7 Responses**7.10.7.7.1 DISP response**

The following is the response if DISP CURR CMIC is issued.

Table 16 MAP outputs with associated meanings and actions

Command
DISP CURR CMIC: last 60 minutes of CMIC utilization and messaging throughput are displayed.
Meaning: last 60 minutes data for CMIC utilization and messaging throughput are displayed.
System or user actions: Not applicable.
DISP CURR ETHR: last 60 minutes of ETHR utilization and messaging throughput are displayed.
Meaning: last 60 minutes of ETHR utilization and messaging throughput are displayed.
System or user actions: Not applicable.

Table 16 MAP outputs with associated meanings and actions

Command
DISP CURR AMDI: last 60 minutes of AMDI utilization and messaging throughput are displayed.
Meaning: last 60 minutes of AMDI utilization and messaging throughput are displayed.
System or user actions: Not applicable.
DISP CURR ALL: last 60 minutes of CMIC, ETHR, AMDI utilization are displayed.
Meaning: last 60 minutes of CMIC, ETHR, AMDI utilization are displayed.
System or user actions: Not applicable.

7.10.7.8 Example

Table 17 Usage examples for DISP command

Description of task	Display the last 60 minutes of IO utilization and messaging throughput.					
Command: MAP	Example: DISP CURR CMIC					
response:	Example:					
	Time	IOUTIL%	TxMsg/s	TxSize	RxMsg/s	RxSize
	16:17	45	23421	34	23421	34
	16:18	39	22119	31	21228	32
	16:19	38	21228	32	22119	31
	16:20	39	23421	31	21221	31
	. . .	. . .	. . .	. . .	. . .	. . .
	17:14	41	20023	32	20019	33
	17:15	39	21221	31	21228	32
	17:16	38	20019	33	23421	34
Command: MAP	Example: DISP CURR ETHR					
response:	Example:					
	Time	IOUTIL%	TxMsg/s	TxSize	RxMsg/s	RxSize
	16:17	45	23421	34	23421	34
	16:18	39	22119	31	21228	32
	16:19	38	21228	32	22119	31
	16:20	39	23421	31	21221	31
	. . .	. . .	. . .	. . .	. . .	. . .
	17:14	41	20023	32	20019	33
	17:15	39	21221	31	21228	32
	17:16	38	20019	33	23421	34
Command: MAP	Example: DISP CURR AMDI					
response:	Example:					
	Time	IOUTIL%	TxMsg/s	TxSize	RxMsg/s	RxSize
	16:17	45	23421	34	23421	34
	16:18	39	22119	31	21228	32
	16:19	38	21228	32	22119	31
	16:20	39	23421	31	21221	31
	. . .	. . .	. . .	. . .	. . .	. . .
	17:14	41	20023	32	20019	33
	17:15	39	21221	31	21228	32
	17:16	38	20019	33	23421	34

Table 17 Usage examples for DISP command

Command:	Example: DISP CURR ALL			
MAP	Example:			
response:	Time	CMICUTIL	ETHRUTIL	AMDIUTIL
	16:17	45	21	34
	16:18	39	19	31
	16:19	38	18	32
	16:20	39	21	31
				
	17:14	41	23	32
	17:15	39	21	31
	17:16	38	19	33

7.10.8 Command: STATUS**7.10.8.1 Command type: NON-MENU****7.10.8.2 Command target: XA-Core only****7.10.8.3 Command availability: RES****7.10.8.4 Command description**

This command displays all status information including current version of IOCAPCI tool, timestamp in terms of hour and minute, the current IO utilization values of all IO services (CMIC, ETHR, AMDI), the current value of the IO_WARNING_THRESHOLD office parm.

7.10.8.5 Command syntax

The command syntax for this command is as follows.

```
> q STATUS
Display current IOCAP status.
```

Table 18 STATUS command parameters and variables

Command	Parameters and variables
STATUS	no parameter

7.10.8.6 Qualifications and warnings

Not applicable.

7.10.8.7 Responses**7.10.8.7.1 STATUS response**

The following is the response if STATUS is issued.

Table 19 MAP outputs with associated meanings and actions

Command
STATUS: Status information such as IOCAPCI version, current utilizations and IO_WARNING_THRESHOLD office parm are displayed. Meaning: Status information such as IOCAPCI version, current utilizations and IO_WARNING_THRESHOLD office parm are displayed. System or user actions: Not applicable.

7.10.8.8 Example

Table 20 Usage examples for STATUS command

Description of task	Display status information such as IOCAPCI version, current utilizations and IO_WARNING_THRESHOLD office parm.
Command:	Example: DISP CURR CMIC
MAP	Example:
response:	<pre>> status IOCAP Version 1.0 Time CMICUTIL ETHRUTIL AMDIUTIL 17:16 32 29 15 IO_WARNING_THRESHOLD office parm is set to 100.</pre>

7.11 Security

Not applicable.

7.11.1 Network configuration

Not applicable.

7.11.2 Key management

Not applicable.

7.11.3 Protocol

Not applicable.

7.11.4 Authentication

Not applicable.

7.12 Configuration Walkthrough

Not applicable.

8: A00006731 Configuration (CN)

8.1 Feature name

Handle Flash on Exit

8.2 Hardware and Software Requirements

There is no hardware or software dependencies.

8.3 Upgrade Impact

No impact on upgrades.

8.4 Data schema (DS) (CM, MIBS, RDB)

8.4.1 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)
IBNLINES	changed	unchanged

8.4.2 Table/MIB/Remote Database Schema information

8.4.2.1 Name: IBNLINES

IBN Line Assignment Table

8.4.2.1.1 Functional description

Table IBNLINES contains the line assignments for each 500/2500 set assigned to an Integrated Business Network (IBN), Residential Enhanced Services (RES), and Multiple Appearance Directory Number (MADN) station number. This table also contains the line assignments for the IBN attendant consoles (AC).

8.4.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

8.4.2.1.3 Size

Unchanged.

8.4.2.1.4 Fields/OIDs

The following table lists fields/OIDs for IBNLINES.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RESULT	Changed	OPTLIST	EOF	Option List. Added EOF to OPTLIST as another line option. Enter EOF for Exit On Flash option.

8.4.2.1.5 Datafill example

The following example shows sample datafill for table IBNLINES.

```
>table ibnlines
>list
LEN DNNO RESULT
-----
HOST 00 0 00 01 0 DT STN IBN 6210201 350 819_P621_2 L819_NILLA_2 819 (EOF) $
```

8.4.2.1.6 Table release history update

ISN08 - Feature (A00006731) Handle Flash on Exit adds new OPTLIST option EOF.

8.5 Service Orders (SO) (CM & SESM)**8.5.1 Service order change details****8.5.1.1 LCC and options**

New line option, EOF, can only be assigned to LCC of IBN.

Option EOF is not compatible with the following options and features:

CHD, CNF, CWI, CWX, CWT, CXR, FXR, DCBX, HLD, LDSA, LDSO, LDSR, LDST, LNPTST, MPB, PCWT, PRK, 3WC, 3WCPUB, VOWDN.

8.5.2 New commands**8.5.2.1 How service order options are presented****8.5.2.1.1 Description**

The EOF option enables the subscriber on the assigned line to exit on flash.

8.5.2.1.2 Example

Figure 1 Example of the EOF option in prompt mode

```

SERVORD
SO:
>ado
SONUMBER:      NOW    4    1 14 PM
>
DN_OR_LEN:
>6137220110
OPTION:
>eof
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 4 1 14 PM 6137220110 ( EOF ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>Y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>Y

```

Figure 2 Example of the EOF option in no-prompt mode

```

SERVORD
SO:
>ado $ 6137220110 eof $ Y Y

```

8.5.2.1.3 Option prompts

Table 3 System prompts for EOF option

Prompt	Valid input	Description	Areas affected by prompt
OPTION	EOF	Assigns Exit On Flash feature to line	None

8.5.2.1.4 Line class code compatibility

Table 4 EOF compatibility to LCC

Line class code	Compatible?
IBN	Yes

8.5.2.1.5 Option prerequisites

EOF has no prerequisites

8.5.2.1.6 Notes

None.

8.5.2.1.7 Feature identification

Feature number: A00006731

9: A00006780 Configuration (CN)

9.1 Feature name

Trimodal Call Server OAM & P Enhancements

9.2 Hardware and Software Requirements

This functionality requires release SN08 or higher loads on the call server¹.

9.3 Office/Subnet parameters (OP/SP) (CM & SESM)

9.3.1 OSS_PROV_VERSION (New Parameter in table OFCVAR)

A new parameter OSS_PROV_VERSION is being added in table OFCVAR in SN07. This Parameter's value can be used by Features delivered on Core, which have an OSS Impact, to keep the feature functionality Switched ON/OFF on Switch Core till the time OSS software is upgraded to be in sync with feature code changes.

Currently the Line Query Command enhancements (Described in Section 12.9.1 of this document) being done as part of this feature, is being controlled using this table OFCVAR Parm.

Example of an OSS_PROV_VERSION tuple in OFCVAR:

.....	
.....	
OSR_FOR_IMT	N
OSR_FOR_ISUP	N
OSS_PROV_VERSION	SN07
OVLP_ID_TIME	3
.....	
.....	

9.3.1.0.1 Default value

Default value for OSS_PROV_VERSION is SN07.

For this feature, by default the code for the Line Query command enhancements listed under Section 12.9 of this document stays inert on the Trimodal Call Server. (The code stays inert if OSS_PROV_VERSION has a value of SN07)

¹Call Server in the Succession network.

This ensures that user needs to explicitly change the value from SN07 to any other value in permitted range of values, to get access to functionality provided by feature code which enhances Line Query Commands.

In the process, the Warning messages the user gets will ensure that the new functionality is enabled, only after upgrading the OSS software for switch.

9.3.1.0.2 Permitted range of values for new OFCVAR parameter

```
>cha
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
PARMVAL: SN07
>SN02
PARM VALUE IS WRONG TYPE
TYPE IS OSS_VERSION MULTIPLE WITH
      VER      {SN07,SN08,SN09,SN10,SN11,SN12,SN13,SN14,SN15,SN16,SN17}
TUPLE TO BE CHANGED:
                OSS_PROV_VERSION                SN02
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

9.3.1.0.3 Meaning of OSS_PROV_VERSION in SN08

ACT.A00006780(SN08 Trimodal OAMP Enhancements) uses the Office Parm OSS_PROV_VERSION.

- **OSS_PROV_VERSION = ‘SN07’**

Default value of SN07, means that the functionality provided by Line Query Command enhancements made under feature and described in Section 12.9 of this document is disabled

- **OSS_PROV_VERSION is anything greater than ‘SN07’ in permitted range**

If the Parameter has a any permitted value other than SN07 i.e. greater than SN07, then it means that the functionality provided by Line Query Command enhancements made under feature and described in Section 12.9 of this document is enabled.

User needs to ensure before setting value of parameter to anything permitted other than SN07, that the OSS software for switch is upgraded to be in sync with the Line Query Commands enhancements described in Section 12.9 of this document. User receives a Warning message to the same effect before he changes value from SN07 to any other permitted value.

9.3.1.0.4 Warning/Error Messages

- **If user enters a value outside of permitted range**

Change shall fail and user will get an error message as shown below. Also, user will be prompted to enter correct value with a Yes/No Prompt:

```
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
PARMVAL: SN08
>sn60
PARM VALUE IS WRONG TYPE
TYPE IS OSS_VERSION MULTIPLE WITH
      VER
{SN07, SN08, SN09, SN10, SN11, SN12, SN13, SN14, SN15, SN16, SN17}
TUPLE TO BE CHANGED:
      OSS_PROV_VERSION          SN60
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

- **If user tries to change parameter value from default value of SN07 to any other value within permitted range i.e. greater than SN07 but a permitted value:**

Change shall pass. User would get following Warning message, just before the Yes/No Prompt:

```
>pos OSS_PROV_VERSION
      OSS_PROV_VERSION          SN07
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
PARMVAL: SN07
>sn08
Changing from a lower to a higher version.
Check if the OSS Software has been upgraded to support
all OSS impacting feature enhancements contained
in the load corresponding to higher version.
Use QOSSVER tool to get list of OSS impacting features
in various loads.
TUPLE TO BE CHANGED:
      OSS_PROV_VERSION          SN08
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

- **If user tries to change parameter value from default value of SN07 to any other value within permitted range i.e. greater than SN07 but a value which is also greater than the current running load (SN08):**

the

Change shall fail. User would get following Warning messages, just before

Yes/No Prompt:

```
>pos OSS_PROV_VERSION
                                OSS_PROV_VERSION          SN07
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
PARMVAL: SN07
>sn09
ERROR: HIGHEST RELEASE ACTIVATED BY THIS PARM IS SN08
TUPLE TO BE CHANGED:
                                OSS_PROV_VERSION          SN09
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
ERROR: HIGHEST RELEASE ACTIVATED BY THIS PARM IS SN08
DATA CONSISTENCY ERROR
UNEXPECTED ERROR CONDITION
TUPLE TO BE CHANGED:
                                OSS_PROV_VERSION          SN09
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

- **If user tries to change the value from any valid value back to SN07, which is default value:**

Change shall pass. User will get a Warning message which is shown below, just before the Yes/No Prompt:

```
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
PARMVAL: SN08
>sn07
Changing from a higher to a lower version.
Some OSS impacting feature enhancements in
the load corresponding to higher version will stop
working after the change.
Check if the OSS Software needs to be downgraded
Use QOSSVER tool to get list of OSS impacting
features in various loads.
TUPLE TO BE CHANGED:
                                OSS_PROV_VERSION          SN08
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

9.4 Upgrade Considerations

9.4.0.1 OM Groups TRK2NET1 and TRK2NET2

In the event that the maximum numbers of OM tuples for OM groups TRK2NET1 and TRK2NET2 has been exceeded on the dump side, or will be exceeded on the restore side due to the tuple allocation enhancement provided by this feature, the tuples which are allocated are likely to be different between the two sides, due to the order in which they were allocated. On the ONP, the affected tables will restore in the order: BEARNETS, TRKGRP, OMKEYORD.

The OM tuples for TRK2NET1 and TRK2NET2 in table OMKEYORD are not transferred during the ONP since they are recreated by the transfer of tables BEARNETS and TRKGRP.

9.4.0.2 DISPLAY field of Tables BEARNETS and NETBRDGE

In SN08, the DISPLAY field of tables BEARNETS and NETBRDGE are required to be non-empty and unique for each Bearer Network (Table BEARNETS) and each Network Bridge CLI(NETBRDGE). Due to enforcement of these criteria, if these fields were not provisioned accordingly in the DUMP side datafill, a warning will be provided indicating that these values should be changed in the SN08 datafill to conform. The warning message will be recorded in the standard TRACE file on XACORE during the execution of TABXFR. Refer to section 12.8.8 for further details.

9.5 Data schema (DS) (CM, MIBS, RDB)

Not Applicable.

9.6 Service Orders (SO)

Not Applicable.

9.7 Software optionality control (SOC)

Not Applicable.

9.8 Element Management

Not Applicable.

9.9 User interface changes

9.9.1 Enhanced Line Query Commands commands

The sample datafill for the Table BEARNETS which is used as reference for the examples presented further below in “Sample BEARNETS table datafill” on page 1343:

Figure 1 Sample BEARNETS table datafill

```

TABLE: BEARNETS
<line length>: 76 columns can be output per line.
<pack mode>: Pack mode is ON.
<indent column>: Indented lines will begin in column 1.
<first column>: The first column of output is column 1.
TOP
NETIDX  BNETNAME                DISPLAY  FABRIC  OPTIONS
-----
NET 0    TDM_ENET                ENET     ENET     $
NET 1    AAL1_PRIMARY            A1_P     AAL1     (PKT_NETWORK_DEFAULT ) $
NET 2    AAL1_SECONDARY            A1_S     AAL1     $
NET 3    IP_PRIMARY                IP_P     IP        $
BOTTOM

```

9.9.1.1 QDN Command

9.9.1.1.1 Description

Line Query command QDN is used to display information about a Directory Number (DN).

Command is enhanced to display Bearer Network Information as part of the Command Output.

A new field **BEARER_NETWORK** is added to the Command Output.

The information printed in the BEARER_NETWORK FIELD is in the following format:-

BEARER_NETWORK: <FABRIC> <DISPLAY>

where,

- **DISPLAY:** Value datafilled in DISPLAY field of the table BEARNETS tuple, corresponding to the Bearer Network to which the DN belongs.
- **FABRIC:** Value datafilled in FABRIC field of the table BEARNETS tuple, corresponding to the Fabric of the Bearer Network to which the DN belongs.

Examples (Refer to the “Sample BEARNETS table datafill” on page 1343):

Figure 2 Enhanced QDN command output for a DN

```

CI>qdn 5207700
-----
DN:      5207700
TYPE: SINGLE PARTY LINE
SNPA: 214 SIG: DT LNATTIDX: 1
LINE EQUIPMENT NUMBER: SLOA 77 1 20 00
LINE CLASS CODE: 1FR
CARDCODE: RDTLSG GND: N PADGRP: PKLNL BNV: NL MNO: N
PM NODE NUMBER : 129
PM TERMINAL NUMBER : 913
BEARER NET: AAL1 A1_P
OPTIONS:
DGT
OFFICE OPTIONS:
U3WC AIN TIID SRA
-----

```

9.9.1.2 QLT Command

9.9.1.2.1 Description

Line Query command QLT is used to display information about a Logical Terminal ID(LTID).

Command is enhanced to display Bearer Network Information as part of the Command Output, if LTID is mapped to a LEN in table LTMAP.

A new field **BEARER NET** is added to the Command Output.

The information printed in the BEARER NET FIELD is in the following format:-

BEARER NET: <FABRIC> <DISPLAY>

where,

- **DISPLAY:** Value datafilled in DISPLAY field of the table BEARNETS tuple, corresponding to the Bearer Network to which the DN belongs.
- **FABRIC:** Value datafilled in FABRIC field of the table BEARNETS tuple, corresponding to the Fabric of the Bearer Network to which the DN belongs.

Examples (Refer to the“Sample BEARNETS table datafill” on page 1343):

Figure 3 Enhanced QLT command output for a LTID

```

>qlt isdn 194
-----
LTID: ISDN      194
SNPA: 416
DIRECTORY NUMBER: 4738073
LT GROUP NO: 0
LTCLASS: BRAFS  DEFAULT LOGICAL TERMINAL: N
EKTS: N  CACH: N
SLBRI: N
BEARER SERVICE ALLOWED: VOICE  VBD  CMD
CS: Y PS: N
ELN: N
VERSION: FUNCTIONAL ISSUE: 2
TSPID: 4164738073
LEN: HOST 01 1 11 22  TEI: DYNAMIC
BEARER NET: ENET ENET
CUSTGRP: MDC416 SUBGRP: 0 NCOS: 0 RING: Y
LINE CLASS CODE: ISDNKSET
MAXKEYS: 64
OPTIONS:
SFC
CUSTOMER GROUP OPTIONS:
AIN CDP CODE
OFFICE OPTIONS:
AIN TIID

  KEY      DN
  ---      --
    1      DN      4164738073

  KEY      FEATURE
  ---      -
    NONE
-----

```

9.9.1.3 QLEN Command

9.9.1.3.1 Description

Line Query command QLEN is used to display information about a Line Equipment Number (LEN).

Command is enhanced to display Bearer Network Information as part of the Command Output.

A new field **BEARER NET** is added to the Command Output.

The information printed in the BEARER NET FIELD is in the following format:-

BEARER NET: <FABRIC> <DISPLAY>

where,

- **DISPLAY:** Value datafilled in DISPLAY field of the table BEARNETS tuple, corresponding to the Bearer Network to which the LEN belongs.
- **FABRIC:** Value datafilled in FABRIC field of the table BEARNETS tuple, corresponding to the Fabric of the Bearer Network to which the LEN belongs.

Examples:

Figure 4 Enhanced QLEN command output for LEN

```

CI>qlen sloa 23 3 4 2
-----
LEN:      SLOA  23 3 04 02
TYPE: SINGLE PARTY LINE
SNPA: 613
DIRECTORY NUMBER:      7202342
LINE CLASS CODE:      1FR
IBN TYPE: STATION
CUSTGRP:      RES1      SUBGRP: 0  NCOS: 0
SIGNALLING TYPE: DIGITONE
LINE TREATMENT GROUP:      0
LINE ATTRIBUTE INDEX:      30
CARDCODE: RDTLSG  GND: N  PADGRP: PKLNL  BNV: NL  MNO: N
PM NODE NUMBER      :      118
PM TERMINAL NUMBER :      147
BEARER NET: IP IP_P
OPTIONS:
DGT
RES OPTIONS: NONE
OFFICE OPTIONS:
SRA

```

9.9.1.4 QDNWRK Command

Line Query Command QDNWRK displays information about a range of working lines using Directory Numbers, which meet the conditions specified by the query parameters passed to the command the user.

The command format is enhanced to include a mandatory query parameter called **BEARNETWORK**.

The range of DNs passed to command is refined such that the output includes DNs which belong to the Bearer Network passed as BEARNETWORK and which meet the specifications set by the values passed for the other command parameters

As mentioned earlier, BEARNETWORK Parm selects only DNs which are physically associated to a LEN, directly or indirectly (e.g. LTIDs which are MAPPED to a LEN in table LTMAP). This is because only if DN is associated/ attached to a LEN, can it be said that DN is part of a particular Bearer Network.

Table 1 New Mandatory Command Parameter “BEARNETWORK”

Parameter Name	Valid input	Description	Areas affected by prompt
BEARNETWORK	Range includes “ALL” and Character Strings datafilled in DISPLAY field of all table BEARNETS tuples: BNETDISP_RANGE{ENET, A1_P, A1_S, IP, ALL} Default value if no PARM is added is “ALL”, which means DNs corresponding to all Provisioned Bearer Networks is included in Query	A bearer network is entered for BEARNETWORK parameter of the command. A range of DNs and some other command parameters are also passed to the command. Command output includes DNs from the range which belong to the bearer network. The DNs also satisfy the command parameters other than BEARNETWORK	N/A

Figure 5 QDNWRK command format with new BEARNETWORK parameter

```

CI>help qdnwrk
COMMAND QDNWRK : QUERY WORKING DIRECTORY NUMBERS
COMMAND FORMAT :
QDNWRK <DIRECTORY NUMBER RANGE><BEARNETWORK><LCC><OPTION><SUMMARY OR DETAIL>

```

9.9.1.4.1 Examples:

- **QDNWRK SUMMARY output when default parameter “ALL” is passed for BEARNETWORK**

Prints SUMMARY output for DNs belonging to any Bearer Network datafilled in table BEARNETS, which satisfy the values passed in for the command parameters other than BEARNETWORK.

Figure 6 QDNWRK command SUMMARY output in Prompt Mode

```

CI>qdnwrk
DIRECTORY_NUMBER_RANGE: ALL
>
BEARNETWORK: ALL
>
AGENT OR LINE CLASS CODE: NLCC
>
OPTION:
>$
SUMMARY OR DETAIL: S
>s
COMMAND AS ENTERED
QDNWRK ALL  ALL NLCC $ ALL S
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
REPORT ON WORKING DIRECTORY NUMBERS
      LCC ALL                      OPTION ALL
      TOTAL COUNT OF WORKING DN:      135

```

Figure 7 QDNWRK SUMMARY command in No Prompt Mode (Same Output)

```

>QDNWRK ALL  ALL NLCC $  S
COMMAND AS ENTERED
QDNWRK ALL  ALL NLCC $ ALL S
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y

```

- **QDNWRK DETAIL output when default parameter “ALL” is passed for BEARNETWORK**

Prints DETAIL output for DNs belonging to any Bearer Network datafilled in table BEARNETS, which satisfy the values passed in for the command parameters other than BEARNETWORK.

Figure 8 QDNWRK command DETAIL output in Prompt Mode

```

CI>qdnwrk
DIRECTORY_NUMBER_RANGE: ALL
>
BEARNETWORK: ALL
>
AGENT OR LINE CLASS CODE: NLCC
>
OPTION:
>$
SUMMARY OR DETAIL: S
>d
COMMAND AS ENTERED
QDNWRK ALL  ALL NLCC $ ALL D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
REPORT ON WORKING DIRECTORY NUMBERS
  LCC ALL              OPTION ALL
-----
DN:      5207700
TYPE: SINGLE PARTY LINE
SNPA: 214  SIG: DT  LNATTIDX: 1
LINE EQUIPMENT NUMBER:  SLOA  77 1 20 00
LINE CLASS CODE:      1FR
CARDCODE:  RDTLSG  GND: N  PADGRP: PKLNL  BNV: NL MNO: N
PM NODE NUMBER      : 129
PM TERMINAL NUMBER  : 913
BEARER NET: AAL1 A1_P
OPTIONS:
DGT
OFFICE OPTIONS:
U3WC AIN TIID SRA
-----
. . .
DN:      6211002
TYPE: SINGLE PARTY LINE
SNPA: 613  SIG: DT  LNATTIDX: 407
LINE EQUIPMENT NUMBER:  HOST  01 1 00 01
LINE CLASS CODE:      1FR
CARDCODE:  6X17AC  GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER      : 90
PM TERMINAL NUMBER  : 2
BEARER NET: ENET ENET
OPTIONS:
DGT
OFFICE OPTIONS:
U3WC AIN TIID
TOTAL COUNT OF WORKING DN:      135

```

Figure 9 QDNWRK DETAIL command in No Prompt Mode (Same Output)

```

>QDNWRK ALL  ALL NLCC $  D
COMMAND AS ENTERED
QDNWRK ALL  ALL NLCC $ ALL D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y

```

- **QDNWRK SUMMARY output when a particular Bearer Network is passed for BEARNETWORK**

Prints SUMMARY output for DNs belonging to a particular Bearer Network datafilled in table BEARNETS entered for parameter BEARNETWORK, which satisfy the values passed in for the command parameters other than BEARNETWORK.

Figure 10 QDNWRK SUMMARY command output in Prompt Mode

```

CI>qdnwrk
DIRECTORY_NUMBER_RANGE: ALL
>
BEARNETWORK: ALL
> ENET
AGENT OR LINE CLASS CODE: NLCC
>
OPTION:
>$
SUMMARY OR DETAIL: S
>s
COMMAND AS ENTERED
QDNWRK ALL ENET NLCC $ ALL S
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
REPORT ON WORKING DIRECTORY NUMBERS
      LCC ALL                      OPTION ALL
      613621 : DN NOT IN HUNTMEM
.....
.....
TOTAL COUNT OF WORKING DN: 20

```

Figure 11 QDNWRK SUMMARY command in No Prompt Mode (Same Output)

```

>QDNWRK ALL ENET NLCC $ S
COMMAND AS ENTERED
QDNWRK ALL ENET NLCC $ ALL S
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y

```

- **QDNWRK DETAIL output when a particular Bearer Network is passed for BEARNETWORK**

Prints DETAIL output for DNs belonging to a particular Bearer Network datafilled in table BEARNETS entered for parameter BEARNETWORK, which satisfy the values passed in for the command parameters other than BEARNETWORK.

Figure 12 QDNWRK DETAIL command output in Prompt Mode

```

CI>qdnwrk
DIRECTORY_NUMBER_RANGE: ALL
>
BEARNETWORK: ALL
>ENET
AGENT OR LINE CLASS CODE: NLCC
>
OPTION:
>$
SUMMARY OR DETAIL: S
>d
COMMAND AS ENTERED
QDNWRK ALL ENET NLCC $ ALL D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
REPORT ON WORKING DIRECTORY NUMBERS
  LCC ALL              OPTION ALL
-----
DN:      6211001
TYPE: SINGLE PARTY LINE
SNPA: 613 SIG: DT      LNATTIDX: 406
LINE EQUIPMENT NUMBER: HOST  01 1 00 01
LINE CLASS CODE:      1FR
CARDCODE: 6X17AC GND: N  PADGRP: STDLN BNV: NL MNO: N
PM NODE NUMBER      :    90
PM TERMINAL NUMBER  :    1
BEARERNET: ENET ENET
OPTIONS:
DGT
OFFICE OPTIONS:
U3WC AIN TIID
-----
. . . .
DN:      6211005
TYPE: SINGLE PARTY LINE
SNPA: 613 SIG: DT      LNATTIDX: 407
LINE EQUIPMENT NUMBER: HOST  01 1 00 05
LINE CLASS CODE:      1FR
CARDCODE: 6X17AC GND: N  PADGRP: STDLN BNV: NL MNO: N
PM NODE NUMBER      :    90
PM TERMINAL NUMBER  :    5
BEARERNET: ENET ENET
OPTIONS:
DGT
OFFICE OPTIONS:
U3WC AIN TIID
TOTAL COUNT OF WORKING DN: 20

```

Figure 13 QDNWRK DETAIL command in No Prompt Mode (Same Output)

```

>QDNWRK ALL ENET NLCC $ D
COMMAND AS ENTERED
QDNWRK ALL ENET NLCC $ ALL D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y

```

9.9.1.4.2 Responses

Figure 14 BEARNETWORK entered is out of valid range

```

CI>qdnwrk
DIRECTORY_NUMBER_RANGE: ALL
>
BEARNETWORK: ALL
>jdhjd
  ***  ERROR  ***
JDHJD
|
TYPE OF BEARNETWORK IS BNETDISP_RANGE
BEARNETWORK: ALL
>BNETDISP_RANGE
  ***  ERROR  ***
BNETDISP_RANGE
|
TYPE OF BEARNETWORK IS BNETDISP_RANGE
TYPE IS BNETDISP_RANGE {ENET, A1_P, A1_S, IP, ALL}
BEARNETWORK: ALL
>A1_P ----->Valid value such that an entry is there in table BEARNETS
AGENT OR LINE CLASS CODE: NLCC
>

```

9.9.1.5 QLENWRK Command

Line Query command QLENWRK displays information about a range of working lines using Line Equipment Numbers (LENs), which meet the conditions specified by the query parameters passed to the command the user.

The command format is enhanced to include a mandatory query parameter called **BEARNETWORK**.

The range of LENs passed to command is refined such that: The output includes LENs which belong to the Bearer Network passed as BEARNETWORK and which meet the specifications set by the values passed for the other command parameters

Table 2 New Mandatory Command Parameter “BEARNETWORK”

Parameter Name	Valid input	Description	Areas affected by prompt
BEARNETWORK	Range includes “ALL” and Four Character Strings datafilled in DISPLAY field of all table BEARNETS tuples: BNETDISP_RANGE{ENET, A1_P, A1_S, IP, ALL} Default value if no PARM is added is “ALL”, which means LENSs corresponding to all Provisioned Bearer Networks is included in Query	A bearer network is entered for BEARNETWORK parameter of the command. A range of LENSs and some other command parameters are also passed to the command. Command output includes LENSs from the range which belong to the bearer network. The LENSs also satisfy the command parameters other than BEARNETWORK.	N/A

Figure 15 QLENWRK command format with new BEARNETWORK parameter

```

CI>q qlenwrk
COMMAND QLENWRK : QUERY WORKING LINE EQUIPMENT NUMBERS
COMMAND FORMAT :
QLENWRK <LINE MODULE RANGE><LINE DRAWER RANGE><BEARNETWORK><LCC OR
ACC><OPTION><SUMMARY OR DETAIL>

```

9.9.1.5.1 Examples:

- **QLENWRK SUMMARY output when default parameter “ALL” is passed for BEARNETWORK**

Prints SUMMARY output for LENSs which satisfy the values passed in for the command parameters other than BEARNETWORK, irrespective of which Bearer Network provisioned in table BEARNETS they belong to.

Figure 16 QLENWRK SUMMARY output in Prompt Mode

```

CI>qlenwrk
LINE_MODULE_RANGE: ALL
>
LINE_DRAWER_RANGE: ALL
>
BEARNETWORK: ALL
>
AGENT OR LINE CLASS CODE: NLCC
>
OPTION:
>$
SUMMARY OR DETAIL: S
>s
COMMAND AS ENTERED
QLENWRK ALL  ALL ALL NLCC $ S
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
SUMMARY OF WORKING LINE EQUIPMENT NUMBERS
DRAWERS ALL
LCC ALL          OPTION ALL
COUNT BY LINE DRAWERS
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
 32 33 34 35
LM : HOST 01 1   COUNT : 137
 16 18 16 17    0 0 0 0 17 20 17 16 0 0 0 0
          TOTAL:      137
. . . . .
DRAWER TOTALS:
 16 18 16 17    0 0 0 0 17 20 17 16 0 0 0 0

```

Figure 17 QLENWRK SUMMARY output in No Prompt Mode (Same Output)

```

>QLENWRK ALL  ALL ALL NLCC $ S
COMMAND AS ENTERED
QLENWRK ALL  ALL ALL NLCC $ S
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y

```

- **QLENWRK DETAIL output when default parameter “ALL” is passed for BEARNETWORK:**
Prints DETAIL output for LENS which satisfy the values passed in for the command parameters other than BEARNETWORK, irrespective of which Bearer Network provisioned in table BEARNETS they belong to.

Figure 18 QLENWRK DETAIL output in Prompt Mode

```

CI>qlenwrk
LINE_MODULE_RANGE: ALL
>
LINE_DRAWER_RANGE: ALL
>
BEARNETWORK: ALL
>
AGENT OR LINE CLASS CODE: NLCC
>
OPTION:
>$
SUMMARY OR DETAIL: S
>d
COMMAND AS ENTERED
QLENWRK ALL  ALL ALL NLCC $ ALL 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
      DRAWERS ALL
      LCC ALL              OPTION ALL
-----
LEN:      HOST 01 1 00 00
TYPE: SINGLE PARTY LINE
DN 6136211001 LCC      1FR      SIG DT LNATTIDX 407
CARDCODE: 6X17AA      GND: N   PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER      :      90
PM TERMINAL NUMBER  :      1
BEARERNET: ENET ENET
OPTIONS:
DGT
OFFICE OPTIONS:
U3WC AIN TIID
-----
.....
LEN:      SLOA 23 3 04 02
TYPE: SINGLE PARTY LINE
SNPA: 613
DIRECTORY NUMBER:      7202342
LINE CLASS CODE:      1FR
IBN TYPE: STATION
CUSTGRP:      RES1      SUBGRP: 0  NCOS: 0
SIGNALLING TYPE: DIGITONE
LINE TREATMENT GROUP:      0
LINE ATTRIBUTE INDEX:      30
CARDCODE: RDTLSG      GND: N   PADGRP: PKLNL  BNV: NL MNO: N
PM NODE NUMBER      :      118
PM TERMINAL NUMBER  :      147
BEARERNET: IP IP_P
OPTIONS:
DGT
RES OPTIONS: NONE
OFFICE OPTIONS:
SRA
-----
TOTAL:              137

```

Figure 19 QLENWRK DETAIL command in No Prompt Mode (Same Output)

```

>QLENWRK ALL  ALL ALL NLCC $ ALL D
COMMAND AS ENTERED
QLENWRK ALL  ALL ALL NLCC $ ALL D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y

```

- **QLENWRK SUMMARY** output when a particular Bearer Network is passed for BEARNETWORK:

Figure 20 QLENWRK SUMMARY command output in Prompt Mode

```

CI>qlenwrk
LINE_MODULE_RANGE: ALL
>
LINE_DRAWER_RANGE: ALL
>
BEARNETWORK: ALL
> ENET
AGENT OR LINE CLASS CODE: NLCC
>
OPTION:
>$
SUMMARY OR DETAIL: S
>s
COMMAND AS ENTERED
QLENWRK ALL  ALL NETO NLCC $ S
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
SUMMARY OF WORKING LINE EQUIPMENT NUMBERS
DRAWERS ALL
LCC ALL          OPTION ALL
COUNT BY LINE DRAWERS
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
 32 33 34 35
LM : HOST 01 1  COUNT : 20
8 4 4 4 0  0  0  0  0  0  0  0  0  0  0  0
      TOTAL:          137
. . . . .
DRAWER TOTALS:
8 4 4 4 0  0  0  0  0  0  0  0  0  0  0  0

```

Figure 21 QLENWRK SUMMARY command in No Prompt Mode (Same Output)

```

>QLENWRK ALL  ALL ENET NLCC $ S
COMMAND AS ENTERED
QLENWRK ALL  ALL ENET NLCC $ S
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y

```

- **QLENWRK DETAIL** output when a particular Bearer Network is passed for BEARNETWORK:
Prints DETAIL output for DNs in range, which belong to the Bearer Network passed in as BEARNETWORK parameter and comply with the values entered for the other command parameters.

Figure 22 QLENWRK DETAIL command in Prompt Mode

```

CI>qlenwrk
LINE_MODULE_RANGE: ALL
>
LINE_DRAWER_RANGE: ALL
>
BEARNETWORK: ALL
>ENET
AGENT OR LINE CLASS CODE: NLCC
>
OPTION:
>$
SUMMARY OR DETAIL: S
>d
COMMAND AS ENTERED
QLENWRK ALL ALL NET0 NLCC $ ALL 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
      DRAWERS ALL
      LCC ALL          OPTION ALL
-----
LEN:      HOST 01 1 00 00
TYPE: SINGLE PARTY LINE
DN 6136211001 LCC      1FR      SIG DT LNATTIDX 406
CARDCODE: 6X17AA      GND: N    PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER      :      90
PM TERMINAL NUMBER  :      1
BEARERNET: ENET ENET
OPTIONS:
DGT
OFFICE OPTIONS:
U3WC AIN TIID
-----
.....
LEN:      HOST 01 1 00 05
TYPE: SINGLE PARTY LINE
DN 6136211005 LCC      1FR      SIG DT LNATTIDX 407
CARDCODE: 6X17AA      GND: N    PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER      :      90
PM TERMINAL NUMBER  :      5
BEARERNET: ENET ENET
OPTIONS:
DGT
OFFICE OPTIONS:
U3WC AIN TIID
-----
TOTAL: 20

```

Figure 23 QLENWRK command in No Prompt Mode (Same Output)

```

>QLENWRK ALL ALL ENET NLCC $ ALL D
COMMAND AS ENTERED
QLENWRK ALL ALL ENET NLCC $ ALL D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y

```

9.9.1.5.2 Responses

Figure 24 BEARNETWORK out of valid range value

```

CI>qlenwrk
LINE_MODULE_RANGE: ALL
>
LINE_DRAWER_RANGE: ALL
>
BEARNETWORK: ALL
>jdhjd
*** ERROR ***
JDHJD
|
TYPE OF BEARNETWORK IS BNETDISP_RANGE
BEARNETWORK: ALL
>BNETDISP_RANGE
*** ERROR ***
BNETDISP_RANGE
|
TYPE OF BEARNETWORK IS BNETDISP_RANGE
TYPE IS BNETDISP_RANGE {ENET, A1_P, A1_S, IP, ALL}
BEARNETWORK: ALL
>A1_P
AGENT OR LINE CLASS CODE: NLCC
>

```

9.9.1.6 QHASU Command

Line Query command QHASU displays hardware assigned and software unassigned Line Equipment Numbers in a specified range. Enhance the command QHASU to allow querying by the Bearer Network.

The command format is enhanced to include a mandatory query parameter called **BEARNETWORK**.

The range of LENSs passed to command is refined such that: The output includes LENSs which belong to the Bearer Network passed as BEARNETWORK and which meet the specifications set by the values passed for the other command parameters

Table 3 New Mandatory Command Parameter “BEARNETWORK”

Parameter Name	Valid input	Description	Areas affected by prompt
BEARNETWORK	Range includes “ALL” and Four Character Strings datafilled in DISPLAY field of all table BEARNETS tuples: BNETDISP_RANGE{ENET, A1_P, A1_S, IP, ALL} Default value if no PARM is added is “ALL”, which means LENSs corresponding to all Provisioned Bearer Networks is included in Query	A bearer network is entered for BEARNETWORK parameter of the command. A range of LENSs and some other command parameters are also passed to the command. Command output includes LENSs from the range which belong to the bearer network. The LENSs also satisfy the command parameters other than BEARNETWORK	N/A

Figure 25 Enhanced QHASU command format

```
QHASU <LINE MODULE RANGE><LINE DRAWER RANGE><CARDTYPE><GND><BEARNETWORK><SUMMARY
OR DETAIL>
```

9.9.1.6.1 Examples:

- **QHASU SUMMARY output when default parameter “ALL” is passed for BEARNETWORK**

Prints SUMMARY output for LENS which satisfy the values passed in for the command parameters other than BEARNETWORK, irrespective of which Bearer Network provisioned in table BEARNETS they belong to.

Figure 26 QHASU command SUMMARY output in Prompt Mode

```
CI>qhasu
LINE_MODULE_RANGE: ALL
>
LINE_DRAWER_RANGE: ALL
>
BEARNETWORK: ALL
>
CARD CODE: NIL_CC
>
GND: N
>
SUMMARY OR DETAIL: S
>s
COMMAND AS ENTERED
QHASU ALL ALL ALL NIL_CC N S
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
SUMMARY OF HARDWARE ASSIGNED SOFTWARE UNASSIGNED LEN -- HASU
DRAWERS ALL
CARDTYPE ALL OPT ALL
COUNT BY LINE DRAWERS
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
32 33 34 35
LM : HOST 01 1 COUNT : 5
2 2 1 0 0 0 0 0 0 0 0 0 0 0 0 0
TOTAL: 5
. . . . .
DRAWER TOTALS:
2 2 1 0 0 0 0 0 0 0 0 0 0 0 0 0
```

Figure 27 QHASU SUMMARY command in No Prompt Mode (Same Pout

```
>QHASU ALL ALL NIL_CC N ENET S
COMMAND AS ENTERED
QHASU ALL ALL NIL_CC N ENET S
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
```

- **QHASU DETAIL output when default parameter “ALL” is passed for BEARNETWORK:**

Prints DETAIL output for LENS which satisfy the values passed in for the command parameters other than BEARNETWORK, irrespective of which Bearer Network provisioned in table BEARNETS they belong to.

Figure 28 QHASU command DETAIL output in Prompt Mode

```

CI>qhasu
LINE_MODULE_RANGE: ALL
>
LINE_DRAWER_RANGE: ALL
>
BEARNETWORK: ALL
>
CARD CODE: NIL_CC
>
GND: N
>
SUMMARY OR DETAIL: S
>d
COMMAND AS ENTERED
QHASU ALL ALL ALL NIL_CC N D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
HARDWARE ASSIGNED SOFTWARE UNASSIGNED LEN -- HASU
DRAWERS ALL
CARDTYPE ALL OPT ALL
LM COUNT LD COUNT LINE CARD SLOTS
HOST 01 1 5 0 2 3 18
1 2 18 19
2 1 13
TOTAL: 5

```

Figure 29 QHASU DETAIL command in No Prompt Mode (Same Output)

```

>QHASU ALL ALL NIL_CC N ALL D
COMMAND AS ENTERED
QHASU ALL ALL NIL_CC N ALL D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y

```

- **QHASU SUMMARY output when a particular Bearer Network is passed for BEARNETWORK:**

Prints SUMMARY output for LENS in the range, which belong to the Bearer Network passed in as BEARNETWORK parameter and comply with the values entered for the other command parameters.

Figure 30 QHASU command SUMMARY output in Prompt Mode

```

CI>qhasu
LINE_MODULE_RANGE: ALL
>
LINE_DRAWER_RANGE: ALL
>
BEARER_NETWORK: ALL
> ENET
CARD CODE: NIL_CC
>
GND: N
>
SUMMARY OR DETAIL: S
>s
COMMAND AS ENTERED
QHASU ALL ALL ENET NIL_CC N S
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
SUMMARY OF HARDWARE ASSIGNED SOFTWARE UNASSIGNED LEN -- HASU
DRAWERS ALL
CARDTYPE ALL OPT ALL
COUNT BY LINE DRAWERS
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
  16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
  32 33 34 35
LM : HOST 01 1 COUNT : 2
  2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
      TOTAL: 2
. . . . .
DRAWER TOTALS:
  2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

```

Figure 31 QHASU SUMMARY command in No Prompt Mode (Same Output)

```

>QHASU ALL ALL NIL_CC N ENET S
COMMAND AS ENTERED
QHASU ALL ALL NIL_CC N ENET S
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y

```

- **QHASU DETAIL output when a particular Bearer Network is passed for BEARNETWORK:**
Prints DETAIL output for LENS in range, which belong to the Bearer Network passed in as BEARNETWORK parameter and comply with the values entered for the other command parameters.

Figure 32 QHASU DETAIL output in Prompt Mode

```

CI>qhasu
LINE_MODULE_RANGE: ALL
>
LINE_DRAWER_RANGE: ALL
>
BEARER NETWORK: ENET
>ENET
CARD CODE: NIL_CC
>
GND: N
>
SUMMARY OR DETAIL: S
>d
COMMAND AS ENTERED
QHASU ALL  ALL  ENET NIL_CC N D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>Y
HARDWARE ASSIGNED SOFTWARE UNASSIGNED LEN -- HASU
      DRAWERS ALL
CARDTYPE ALL          OPT ALL
      LM  COUNT LD COUNT          LINE CARD SLOTS
HOST  01 1 2 0    2    3 18
      TOTAL:          0

```

Figure 33 QHASU DETAIL command in No Prompt Mode (Same Output)

```

>QHASU ALL  ALL  NIL_CC N ENET D
COMMAND AS ENTERED
QHASU ALL  ALL  NIL_CC N ENET D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>Y

```

9.9.1.6.2 Responses:

Figure 34 BEARNETWORK entered is out of valid range

```

CI>qhasu
LINE_MODULE_RANGE: ALL
>
LINE_DRAWER_RANGE: ALL
>
BEARNETWORK: ALL
>jdhjd
***  ERROR  ***
JDHJD
|
TYPE OF BEARNETWORK IS BNETDISP_RANGE
BEARER NETWORK: ALL
>BNETDISP_RANGE
***  ERROR  ***
BNETDISP_RANGE
|
TYPE OF BEARNETWORK IS BNETDISP_RANGE
TYPE IS BNETDISP_RANGE {ENET, A1_P, A1_S,  IP, ALL}
BEARNETWORK: ALL
>A1_P ----->Valid value such that an entry is there in table BEARNETS
AGENT OR LINE CLASS CODE: NLCC
>

```

9.9.1.7 QGRP Command

Line Query command QGRP queries information about Members belonging to Line Groups like CPU, SCU, QBS etc. and displays the information to the user.

The command output is enhanced to display against each Group member, the information about the Bearer Network to which the member belongs.

The enhanced output format for a Group member has bearer network information added as **<FABRIC> <DISPLAY>**:

where,

- **FABRIC:** Value datafilled in FABRIC field of the table BEARNETS tuple, corresponding to the Fabric of the Bearer Network to which the LEN belongs.
- **DISPLAY:** Value datafilled in DISPLAY field of the table BEARNETS tuple, corresponding to the Bearer Network to which the LEN belongs.

This enhancement holds true for the following command options of QGRP command only, as listed below:

QGRP CPU <LINE EQUIPMENT NUMBER>

QGRP QBS <LINE EQUIPMENT NUMBER> <KEY>

QGRP MDN <LINE EQUIPMENT NUMBER OR LOGICAL TERMINAL ID> <KEY>

QGRP MDN <DIRECTORY NUMBER>

QGRP MDN <DIRECTORY NUMBER> <BRIEF FULL OR CA <CALL APPEARANCE NUMBER>>

QGRP HNT <DIRECTORY NUMBER OR LINE EQUIPMENT NUMBER> <KEY>

QGRP HNT <DIRECTORY NUMBER OR LINE EQUIPMENT NUMBER>

QGRP BLF <DIRECTORY NUMBER>

For ISDN agents which are not attached to a LEN, the message 'UNATTACHED TO A LEN' is displayed.

9.9.1.7.1 Examples:

Figure 35 Enhanced QGRP command output for CPU Command Option

```
>qgrp cpu SLOA 23 3 08 07

CPU GROUP
-----

LINKLEN:      SLOA  23 3 08 07 KEY 1    BEARERNET: AAL1 A1_S      9097500036
               SLOA  23 3 08 07 KEY 8    BEARERNET: AAL1 A1_S
               SLOA  23 3 08 07 KEY 2    BEARERNET: AAL1 A1_S      9097500074

The number of members in the CPU  GROUP is 3.
```

Figure 36 Enhanced QGRP command output for QBS Command Option

```

>qgrp qbs HOST 00 0 08 05 2
LEN AND KEY NOT A MEMBER OF INTERCOM GROUP

QBS GROUP
-----

MONITORED LEN:  HOST  00 0 08 04      BEARER NET: ENET ENET
                  HOST  00 0 08 05 KEY 2  BEARER NET: ENET ENET

The number of members in the QBS GROUP is 1.

```

Figure 37 Enhanced QGRP command output for HNT Command Option

```

>qgrp hnt 9519111

DLH HUNT GROUP #9
-----

PILOT:          HOST  00 0 00 29 KEY 2      BEARER NET: ENET ENET DN      9099519111
                  SLOA  23 3 08 09 KEY 4      BEARER NET: AAL1 A1_S
                  CGA      105      KEY 11      BEARER NET: ENET ENET

HUNT options <TFO> apply to this HUNT GROUP.
The number of members in the HUNT GROUP is 3.

```

Figure 38 Enhanced QGRP command output for BLF Command Option

```

>qgrp blf 4731064
-----
THE LENS MONITORING THE INPUT DN VIA BLF ARE:

LEN                                KEY  TYPE              BEARER NET
.....
HOST  01 1 09 19                  2    GROUP_MONITOR  BEARER NET: ENET ENET
-----

```

Figure 39 Enhanced QGRP command output with Non-Attached ISDN Agents

```

>qgrp cpu HOST 00 0 08 01

CPU GROUP
-----

LINKLEN:          HOST  00 0 08 01 KEY 1      BEARER NET: ENET ENET      6137222008
                  FUNC      3      KEY 1      BEARER NET: AAL1 A1_P      6137223002
                  FUNC      27      KEY 1      UNATTACHED TO A LEN  6137223027

The number of members in the CPU GROUP is 3.

```

Figure 40 Enhanced QGRP command output for MDN Command Option

```

>qgrp mdn 4731064 brief

MDN GROUP
-----

HOST 01 1 09 19 KEY 1    BEARER NET: ENET ENET

There is no Primary member associated with this group.
Member HOST 01 1 09 19 has the following options :
CPU 0 HOST 01 1 09 19 1
CUSTOMER GROUP OPTIONS:
AIN CDPCODE
OFFICE OPTIONS:
AIN TIID

The number of members in the SCA MDN GROUP is 1.

>qgrp mdn 4731064 full

MDN GROUP
-----

HOST 01 1 09 19 KEY 1    BEARER NET: ENET ENET

There is no Primary member associated with this group.
Member HOST 01 1 09 19 has the following options :
CPU 0 HOST 01 1 09 19 1
CUSTOMER GROUP OPTIONS:
AIN CDPCODE
OFFICE OPTIONS:
AIN TIID

The number of members in the SCA MDN GROUP is 1.

>qgrp mdn 4731064 ca 4164731064

MDN GROUP
-----

HOST 01 1 09 19 KEY 1    BEARER NET: ENET ENET

There is no Primary member associated with this group.
Member HOST 01 1 09 19 has the following options :
CPU 0 HOST 01 1 09 19 1
CUSTOMER GROUP OPTIONS:
AIN CDPCODE
OFFICE OPTIONS:
AIN TIID

The number of members in the SCA MDN GROUP is 1.

>

```

```
>qgrp mdn 4731064
```

```
MDN GROUP
```

```
-----
```

```
HOST 01 1 09 19 KEY 1 BEARERNET: ENET ENET
```

There is no Primary member associated with this group.

Member HOST 01 1 09 19 has the following options :

CPU 0 HOST 01 1 09 19 1

CUSTOMER GROUP OPTIONS:

AIN CDPCODE

OFFICE OPTIONS:

AIN TIID

The number of members in the SCA MDN GROUP is 1.

```
>qgrp mdn HOST 01 1 09 19
```

```
KEY:
```

```
>1
```

```
LEN AND KEY NOT A MEMBER OF INTERCOM GROUP
```

```
MDN GROUP
```

```
-----
```

```
HOST 01 1 09 19 KEY 1 BEARERNET: ENET ENET
```

```
4164731064 : IS MDN DN
```

There is no Primary member associated with this group.

Member HOST 01 1 09 19 has the following options :

CPU 0 HOST 01 1 09 19 1

CUSTOMER GROUP OPTIONS:

AIN CDPCODE

OFFICE OPTIONS:

AIN TIID

The number of members in the SCA MDN GROUP is 1.

```
>qgrp mdn 4164731064
```

```
MDN GROUP
```

```
-----
```

```
HOST 01 1 09 19 KEY 1 BEARERNET: ENET ENET
```

There is no Primary member associated with this group.

Member HOST 01 1 09 19 has the following options :

CPU 0 HOST 01 1 09 19 1

CUSTOMER GROUP OPTIONS:

AIN CDPCODE

OFFICE OPTIONS:

AIN TIID

The number of members in the SCA MDN GROUP is 1.

```
>
```


9.9.1.8 QCUST

QCUST command displays all Line Equipment Numbers (LENs) corresponding to a Customer Group. The command output is enhanced to display the corresponding Bearer Network against each of the LENs.

The command output is enhanced such that the Bearer Network information for each LEN in a Customer Group is displayed against the LEN in the QCUST output.

A new Line of output (RECORD 22 i.e. We have “22” at start of LINE) showing **BEARERNET** field is introduced in the QCUST command output against each LEN.

The format of the new field BEARERNET is as follows:

22 BEARERNET: <FABRIC> <DISPLAY>

where,

- **DISPLAY**: Value datafilled in DISPLAY field of the table BEARNETS tuple, corresponding to the Bearer Network to which the LEN belongs.
- **FABRIC**: Value datafilled in FABRIC field of the table BEARNETS tuple, corresponding to the Fabric of the Bearer Network to which the LEN belongs.

These enhancements hold for the whole of the command menu applicable to QCUST command. The Command menu being:

```
COMMAND QCUST : QUERY CUSTOMER DATA
COMMAND FORMAT : QCUST <CUSTGRP> $
                  OR
                  QCUST LEN <LINE EQUIPMENT NUMBER/
                  LOGICAL TERMINAL IDENTIFIER>
                  OR
                  QCUST ALL
                  OR
                  QCUST OWNEDBY <CUSTNAME> INITIAL
                  OR
                  QCUST ALL <CUSTNAME> INCR
                  OR
                  QCUST ALL <CUSTNAME> DONE
```

9.9.1.8.1 Examples:

Figure 41 Enhanced QCUST command output

```

CI>qcust all
0 55 Y 4 Y N
99
18 ISDN
18 FUNC
.....
.....
18 BRI_TRAF
99
19 PUBLIC 0
19 PRIVATE 1
99
1 RDT1 45 0 00 13 M5316 NPDGP RDTEBS N
4 $
5 1 5200013 NT520 0 0 214 Y
22 BEARER NET: IP IP_P
99
.....
.....
99
17 FUNC 5 B BRAFS VOICE VBD CMD PVC FUNCTIONAL 2 DTEI TSPID 6137223003 $ Y RDT
1 24 0 00 94 $ N
1 FUNC 5 ISDNKSET NPDGP RDTISD N
4 60 $
5 1 7223003 THE_FAR_SIDE 0 0 613 Y
9 LNR SFC $
10 1 NAME PUBLIC YOMAMA
22 BEARER NET: AAL1 A1_P
The number of members in the HUNT GROUP is 4.

```

9.9.1.9 Restrictions & Special Cases

The Line Query Command Enhancements described in this Section **do not** apply to following:

- MTX DN/LENs
- Cellular DN/LENs
- Synonym DN/LENs
- Virtual DN
- Unassigned and free DN
- DN not associated to a LEN
- GSF DN/LENs

These Enhancements are aimed at the North American (NA) Markets. It is not supported for MSL loads and other non-NA loads

These enhancements become active only when value datafilled for table OFCVAR Parm OSS_PROV_VERSION is greater than SN07

The Enhancements to QLEN command do not hold true for LEN corresponding to Free slot i.e. without a Line Card physically present in slot, of the 2 Slots in a two slot Line Card

For QGRP Command Options enhanced, if a given DN is not attached to a LEN, in place of the “BEARER NET” field display, following will be displayed: “UNATTACHED TO A LEN”

For Offices with a JNET:-

- The BEARER NET field in enhanced command puts for QDN, QLEN, QCUST, QGRP (Options enhanced), QLT commands will be as follows:- “BEARER NET: JNET”
- The Displayed options list for BEARNETWORK Command Parm for QDNWRK, QLENWRK and QHASU commands will contain only “ALL”

9.9.2 Sample Datafills for PM MAP level and other MAP level enhancements described below

Figure 42 Sample BEARNETS table datafill

```
TABLE: BEARNETS
<line length>: 76 columns can be output per line.
<pack mode>: Pack mode is ON.
<indent column>: Indented lines will begin in column 1.
<first column>: The first column of output is column 1.
TOP
NETIDX  BNETNAME                DISPLAY  FABRIC  OPTIONS
-----
--
NET 0    TDM_ENET                ENET     ENET     $
NET 1    AAL1_PRIMARY             A1_P     AAL1     (PKT_NETWORK_DEFAULT) $
NET 2    AAL1_SECONDARY            A1_S     AAL1     $
NET 3    IP_PRIMARY                 IP_P     IP       $
NET 4    IP_SECONDARY               IP_S     IP       $
```

Figure 43 Sample NETBRDGE table datafill

```
TABLE: NETBRDGE
<line length>: 76 columns can be output per line.
<pack mode>: Pack mode is ON.
<indent column>: Indented lines will begin in column 1.
<first column>: The first column of output is column 1.
TOP
BRDGCLLI  BRDGTYPE  DISPLAY  BEARNETS
-----
ENET_TO_AAL1_PRI  CORE_BRDGE  E_AP     TDM_ENET  AAL1_PRIMARY
ENET_TO_AAL1_SEC  CORE_BRDGE  E_AS     TDM_ENET  AAL1_SECONDARY
```

9.9.3 Directory: PMLEVEL

This feature enhances a command in the PMLEVEL directory, but does not modify the directory itself.

9.9.3.1 Directory description

The commands in this directory help operating company personnel to operate and maintain the Peripheral Module (PM) at the node level.

9.9.3.2 Accessing directory: PMLEVEL Directory

9.9.3.2.1 Access to directory or MAP level and return to CI

To access the PMLEVEL level from the CI environment, type:

```
>MAPCI ; MTC ; PM ;
```

To return to the CI environment, type:

```
>QUIT ALL
```

9.9.4 Command: POST

9.9.4.1 Command type: Listed MENU

9.9.4.2 Command target: All

9.9.4.3 Command availability: RES

9.9.4.4 Command description

The POST command Displays the Peripheral Modules. This command is used to post the various Peripheral modules for Maintenance.

This feature introduces a new parameter PM BEARNETS. This parameter in POST command allows the craft to post all the PMs hosted on a given bearer network. The valid entries for this new parameter are the entries for the bearer network in the table BEARNETS.

The PMs can be posted by:

- Bearer network and PM type. The PM type allowed is limited to SPM type for this release.
- The PMs can be posted by Bearer network and PM type and the SPM node class type. The SPM node class types allowed is limited to SMG4 and IWDPT type of SPMs for this release.

Following is not supported (Description given further below, can be referred to for more details):

- The PMs being posted by Bearer network *and* PM type *and* the PM state.
- The PMs being posted by Bearer network *and* PM type *and* the PM alarm.

9.9.4.5 Command syntax

The command syntax is as shown in Figure 44.

Figure 44 PM POST command syntax

```

Post:Post specified PMs for maintenance
Parms: [<All PMs> {AllPMs}]
      [<PM Type>... {TM2 [<All> {All}]
                ....
                {SysB,
                ....
                InSv}}]
      [<PM Alarm>... {Minor,
                Major,
                Crit}]
      [<BN> {A1_P [<PM Type> {SPM [<SPM Type> {SMG4,
                DPT}}}}]
      A1_S [<PM Type> {SPM [<SPM Type> {SMG4,
                DPT}}}],
      IP_P [<PM Type> {SPM [<SPM Type> {SMG4,
                DPT}}}],
      IP_S [<PM Type> {SPM [<SPM Type> {SMG4,
                DPT}}}}]

```

Note: The Parms <PM Type> and the Parm <BN> cannot be used together.
E.g. POST SPM BN 0 is invalid command.

Figure 45 PM POST command parameters and variables

Command	Parameters and variables
POST	<pre> Parms: [<All PMs> {AllPMs}] [<PM Type>... {TM2 [<All> {All}] {SysB, ... InSv}}] [<PM Alarm>... {Minor, Major, Crit}] [<BN> {A1_P [<PM Type> {SPM [<SPM Type> {SMG4, DPT}}}}] A1_S [<PM Type> {SPM [<SPM Type> {SMG4, DPT}}}], IP_P [<PM Type> {SPM [<SPM Type> {SMG4, DPT}}}], IP_S [<PM Type> {SPM [<SPM Type> {SMG4, DPT}}}}] </pre>
Parameters and variables	Description
PM BEARNETS	Value datafilled in DISPLAY field of a table BEARNETS tuple corresponding to a Bearer network. This command posts all the PMs hosted on the corresponding bearer network. E.g. POST A1_P posts all the PMs which are on the Bearer network corresponding to the table BEARNETS tuple, which has the value A1_P datafilled in the DISPLAY field.

Figure 45 PM POST command parameters and variables

Command	Parameters and variables
PM Type	(optional) SPM [Currently only SPM is supported]. This command posts all the SPMs on the specified network.
Class	(optional) SPM node class. This command posts all the SPMs of the specified class and Bearer network data filled in the DMS Switch.
SMG4	Post all the SMG4 class SPM nodes hosted on the Switch
DPT	Post all the DPT class SPM nodes hosted on the Switch

9.9.4.6 Qualifications and warnings

No warnings are displayed.

9.9.4.7 Responses

Neither the POST command nor any of its options have required parameters; therefore, the user is never prompted for additional information when issuing any variant of the POST command.

9.9.4.7.1 POST <BN> response

The command and response for 'POST <BN>' is as shown in Table 4, "MAP outputs for POST <PM BEARNETS> with associated meanings and actions," on page 1373.

Table 4 MAP outputs for POST <PM BEARNETS> with associated meanings and actions

Command MAPCI;MTC;PM; POST <BN>
RESPONSE: All the PMs hosted on the bearer network corresponding to the table BEARNETS tuple whose DISPLAY field contains value specified as parameter, are posted. Meaning: The Parameter PM BEARNETS is the value datafilled in DISPLAY field of a table BEARNETS tuple corresponding to a Bearer Network. All the PMs hosted on the bearer network are posted as post-set at the MAP level. The MAP level is changed to the PM level of the first member in the post-set. The maintenance commands available off the specific PM MAP can be executed on this posted PM. System or user actions: N/A User actions: Menu/Non menu commands available off the specific PM MAP for maintenance can be executed.

9.9.4.7.2 POST <BN> response when an invalid entry for bearer network is given

The command and response for 'POST <BN>' is as shown in Table 5, "MAP outputs for POST <BN> with associated meanings and actions," on page 1374.

Table 5 MAP outputs for POST <BN> with associated meanings and actions

Command MAPCI;MTC;PM; POST BN NET
RESPONSE: "Either incorrect optional parameter(s) OR too many parameters. Failed to create Post set" MAP screen will remain at PM MAP. Meaning: The parameter given as bearer network [NET] is not a valid entry in the DISPLAY field of any table BEARNETS tuples. The valid entry for this is the contents of the DISPLAY field of a table BEARNETS tuple. So no PMs are posted for this command. User actions: The Craft has to give contents of DISPLAY field in any of the table BEARNETS tuples. Each tuple in table BEARNETS corresponds to a Bearer network.

9.9.4.7.3 POST <BN> <PM Type>

The command and response for 'POST <BN> <PM Type>' is as shown in Table 6, "MAP outputs for POST <BN> <PM Type> with associated meanings and actions," on page 1375. SPM is the only PM Type supported for this release.

Table 6 MAP outputs for POST <BN> <PM Type> with associated meanings and actions

Command MAPCI;MTC;PM; POST <BN> <PM Type> POST <BN> SPM
RESPONSE: All the SPMs hosted on the specified bearer network are posted. Meaning: The Parameter PM BEARNETS is the value datafilled in DISPLAY field of a table BEARNETS tuple corresponding to a Bearer Network. All the SPMs hosted on the specified bearer network are posted as post-set at the MAP level. The MAP level is changed to the SPM MAP level. The maintenance commands available off the SPM MAP can be executed on this posted SPM. System or user actions: N/A User actions: Menu/Non menu commands available off the specific SPM MAP for maintenance can be executed.

9.9.4.7.4 POST <BN> <PM Type>

The command and response for 'POST <BN> <PM Type>' when the PM Type is given as anything other than SPM is as shown in Table 7, "MAP outputs for POST <BN> <PM Type> with associated meanings and actions," on page 1376. SPM is the only PM Type supported for this release.

Table 7 MAP outputs for POST <BN> <PM Type> with associated meanings and actions

Command MAPCI;MTC;PM; POST <BN> SMA2
RESPONSE: “EITHER incorrect optional parameter(s) OR too many parameters. Failed to create Post set” Map screen will remain at PM MAP. Meaning: The parameter given as PM Type is not a valid entry. The only valid entry for this release is SPM. So no PMs are posted for this command. User actions: The PM Type has to given as SPM.

9.9.4.7.5 POST <BN> SPM SMG4

The command and response for ‘POST <BN> SPM SMG4’ is as shown in Table 8, “MAP outputs for POST <BN> SPM SMG4 with associated meanings and actions,” on page 1377. SMG4 and DPT are the only SPM class Types supported for this release.

Table 8 MAP outputs for POST <BN> SPM SMG4 with associated meanings and actions

Command MAPCI;MTC;PM; POST <BN> SPM SMG4
RESPONSE: All the SPMs of node class type as SMG4 hosted on the specified bearer network are posted. Meaning: The Parameter PM BEARNETS is the value datafilled in DISPLAY field of a table BEARNETS tuple corresponding to a Bearer Network. All the SMG4 SPMs hosted on the specified bearer network are posted as post-set at the MAP level. The MAP level is changed to the SPM MAP level. The maintenance commands available off the SPM MAP can be executed on this posted SPM. System or user actions: N/A User actions: Menu/Non menu commands available off the specific SPM MAP for maintenance can be executed.

9.9.4.7.6 POST <BN> SPM DPT

The command and response for 'POST <BN> SPM DPT' is as shown in Table 9, "MAP outputs for POST <BN>SPM DPT with associated meanings and actions," on page 1378. SMG4 and DPT are the only SPM class Types supported for this release.

Table 9 MAP outputs for POST <BN>SPM DPT with associated meanings and actions

Command MAPCI;MTC;PM; POST <BN> SPM DPT
RESPONSE: All the SPMs of node class type as DPT hosted on the specified bearer network are posted. Meaning: The Parameter PM BEARNETS is the value datafilled in DISPLAY field of a table BEARNETS tuple corresponding to a Bearer Network. All the DPT SPMs hosted on the specified bearer network are posted as post-set at the MAP level. The MAP level is changed to the SPM MAP level. The maintenance commands available off the SPM MAP can be executed on this posted SPM. System or user actions: N/A User actions: Menu/Non menu commands available off the specific SPM MAP for maintenance can be executed.

9.9.4.7.7 POST <BN> SPM <class>

The command and response for 'POST <BN> SPM <class>' where the entry for parameter class is other than SMG4 or DPT is as shown in Table 10, "MAP outputs for POST <BN> SPM <class> with associated meanings and actions," on page 1379. SMG4 and DPT are the only SPM class Types supported for this release.

Table 10 MAP outputs for POST <BN> SPM <class> with associated meanings and actions

Command MAPCI;MTC;PM; POST <BN> SPM IW
RESPONSE: “EITHER incorrect optional parameter(s) OR too many parameters. Failed to create Post set” MAP screen will remain at PM MAP. Meaning: The parameter given as SPM Node class Type is not a valid entry. The only valid entries for this parameter are SMG4 and DPT. So no PMs are posted for this command. User actions: The SPM Node class Type has to given as SMG4 or DPT.

9.9.4.8 Examples

Table 11 Examples for the POST command at PM MAP

Description of task	Post all the PMs hosted on an specified bearer network
Command: MAP response:	POST A1_P A post-set with of all the PMs which are hosted on the bearer network which has “A1_P” datafilled in table BEARNETS tuple is created.
Description of task	Post all the SPMs hosted on an specified bearer network
Command: MAP response:	POST A1_P SPM A post-set with of all the SPMs which are hosted on the bearer network which has “A1_P” datafilled in table BEARNETS tuple is created.
Description of task	Post all the SPM nodes by class SMG4 on specified bearer network
Command: MAP response:	POST A1_S SPM SMG4 A post-set with of all the SMG4 SPMs which are hosted on the bearer network which has “A1_S” datafilled in table BEARNETS tuple is created.
Description of task	Post all the SPM nodes by class DPT on specified bearer network

Command: MAP response:	POST A1_P SPM DPT A post-set with of all the DPT SPMs which are hosted on the bearer network which has "A1_P" datafilled in table BEARNETS tuple is created.

9.9.5 Command: POSTCLS

9.9.5.1 Command type: Hidden

9.9.5.2 Command target: All

9.9.5.3 Command availability: RES

9.9.5.4 Command description

This feature enhances an existing functionality POSTCLS at SPM level to post the PMTYPE by SPM node class type. This enables the craft to post the SPMs by the node class type (such as DMSCP, SMG4, IWDPT, IWB RG). The POST command, when posted by SPM node class type (E.g SMG4) creates a post set which contains all the SMG4 SPMs data filled in the DMS Switch.

9.9.5.5 Command syntax

The command syntax is as shown in Figure 46.

Figure 46 POSTCLS command Enhancements

```
POSTCLS: Post SPM by CLASS for maintenance.
Parms: <Class Type> {DMSCP,
                    IWB RG [<Netbrdge_clli>...{E_AP,E_AS}]
                    SMG4,
                    IWDPT}
```

Figure 47 POSTCLS command parameters and Variables

Command	Parameters and variables
POSTCLS	Parms: <Class Type> {DMSCP, IWB RG [<Netbrdge_clli>...{E_AP,E_AS}] SMG4, IWDPT}
Parameters and variables	Description
Class	(optional) SPM node class. This command posts all the SPMs of the specified class data filled in the DMS Switch.
DMSCP	Post all the DMSCP class SPM nodes hosted on the Switch
IWB RG	Post all the IWB RG class SPM nodes hosted on the Switch
IWB RG <NETBRDGE_DISPLAY>	(optional) Post all the IWB RG class SPM nodes hosted on the Switch which use the Netbrdge CLLI, corresponding to the table NETBRDGE tuple whose DISPLAY field has the specified value.
SMG4	Post all the SMG4 class SPM nodes hosted on the Switch

Command	Parameters and variables
IWDPT	Post all the IWDPT class SPM nodes hosted on the Switch

9.9.5.6 Qualifications and warnings

No warnings are displayed.

9.9.5.7 Responses

9.9.5.7.1 POSTCLS <class> response when class is specified is DMSCP

The command and response for 'POSTCLS DMSCP' is as shown in Table 12, "MAP outputs for POSTCLS <class> with associated meanings and actions," on page 1381.

Table 12 MAP outputs for POSTCLS <class> with associated meanings and actions

Command MAPCI;MTC;PM;POST SPM; POSTCLS DMSCP
RESPONSE: Map screen will be at SPMDIR. The DMSCP SPMs data filled in the DMS switch are posted on the SPM MAP. Meaning: All the SPMs of SPM node class type as DMSCP are posted as post-set at the SPM MAP level. All the maintenance commands available off a SPM MAP can be executed on this post-set. System or user actions: N/A User actions: Menu/Non menu commands available off the SPM MAP for maintenance can be executed.

9.9.5.7.2 POSTCLS <class> response when class is specified is SMG4

The command and response for 'POSTCLS SMG4' is as shown in Table 13, "MAP outputs for POSTCLS <class> with associated meanings and actions," on page 1382.

Table 13 MAP outputs for POSTCLS <class> with associated meanings and actions

Command MAPCI;MTC;PM;POST SPM; POSTCLS SMG4
RESPONSE: Map screen will be at SPMDIR. The SMG4 SPMs data filled in the DMS switch are posted on the SPM MAP. Meaning: All the SPMs of SPM node class type as SMG4 are posted as post-set at the SPM MAP level. All the maintenance commands available off a SPM MAP can be executed on this post-set. System or user actions: N/A User actions: Menu/Non menu commands available off the SPM MAP for maintenance can be executed.

9.9.5.7.3 POSTCLS <class> response when class is specified is IWDPT

The command and response for 'POSTCLS IWDPT' is as shown in Table 14, "MAP outputs for POSTCLS <class> with associated meanings and actions," on page 1383.

Table 14 MAP outputs for POSTCLS <class> with associated meanings and actions

Command MAPCI;MTC;PM;POST SPM; POSTCLS IWDPT
RESPONSE: MAP screen will be at SPMDIR. The IWDPT SPMs data filled in the DMS switch are posted on the SPM MAP. Meaning: All the SPMs of SPM node class type as IWDPT are posted as post-set at the SPM MAP level. All the maintenance commands available off a SPM MAP can be executed on this post-set. System or user actions: N/A User actions: Menu/Non menu commands available off the SPM MAP for maintenance can be executed.

9.9.5.7.4 POSTCLS <class> response when class is specified is IWBRG

The command and response for 'POSTCLS IW ALL' is as shown in Table 15, "MAP outputs for POSTCLS <class> with associated meanings and actions," on page 1384.

Table 15 MAP outputs for POSTCLS <class> with associated meanings and actions

Command MAPCI;MTC;PM;POST SPM; POSTCLS IWBRG
RESPONSE: Map screen will be at SPMDIR. All the IWBRG SPMs data filled in the DMS switch are posted on the SPM MAP. Meaning: All the SPMs of SPM node class type as IWBRG are posted as post-set at the SPM MAP level. All the maintenance commands available off a SPM MAP can be executed on this post-set. System or user actions: N/A User actions: Menu/Non menu commands available off the SPM MAP for maintenance can be executed.

9.9.5.7.5 POSTCLS <class> response when class is specified is IWBRG

The command and response for 'POSTCLS IWBRG <NETBRIDGE_DISPLAY>' is as shown in Table 16, "MAP outputs for POSTCLS <class> with associated meanings and actions," on page 1385.

Table 16 MAP outputs for POSTCLS <class> with associated meanings and actions

Command MAPCI;MTC;PM;POST SPM; POSTCLS IWRBG <NETBRDGE_DISPLAY>
RESPONSE: Map screen will be at SPMDIR. All the IWRBG SPMs data filled in table MNNODE, which use the Netbrdge CLLI in the DMS switch corresponding to the table NETBRDGE tuple having value specified for <NETBRDGE_DISPLAY> datafilled in the DISPLAY field, are posted on the SPM MAP. Meaning: The Parameter NETBRDGE_DISPLAY is the value data filled in the DISPLAY field of a table NETBRDGE tuple. All the SPMs of SPM node class type as IWRBG, which use the Netbrdge CLLI corresponding to the table NETBRDGE tuple, are posted as post-set at the SPM MAP level. The maintenance commands available off a SPM MAP can be executed on this post-set. System or user actions: N/A User actions: Menu/Non menu commands available off the SPM MAP for maintenance can be executed.

9.9.5.7.6 POSTCLS <class> response when specified class is not in the valid variables

The command and response for 'POSTCLS <class>' is as shown in Table 17, "MAP outputs for POSTCLS <class> with associated meanings and actions," on page 1386.

Table 17 MAP outputs for POSTCLS <class> with associated meanings and actions

Command MAPCI;MTC;PM;POSTCLS; POSTCLS SMG
RESPONSE: postcls smg Invalid symbol: <Class Type> {DMSCP, IWBRG [<Netbrdge_clli>...{E_AP,E_AS}], SMG4, IWDPT} Enter: <Class Type> Map screen will remain at PM MAP. Meaning: The parameter given as the node class type is invalid. So no PMs are posted for this command. User actions: The SPM node class type has to one of the types: DMSCP, SMG4, IWDPT, IWBRG.

9.9.5.7.7 POSTCLS IWBRG <NETBRDGE_DISPLAY> response when specified Netbrdge DISPLAY field value is not a valid entry in any table NETBRDGE Tuple

The command and response for 'POSTCLS IWBRG <NETBRDGE_DISPLAY>' is as shown in Table 18, "MAP outputs for POSTCLS IWBRG <NETBRDGE_DISPLAY> with associated meanings and actions," on page 1387.

Table 18 MAP outputs for POSTCLS IWBRG <NETBRDGE_DISPLAY> with associated meanings and actions

Command MAPCI;MTC;PM; POSTCLS IWBRG <NETBRDGE_DISPLAY>
RESPONSE: “EITHER incorrect optional parameter(s) OR too many parameters. Failed to create Post set” MAP screen will remain at PM MAP. Meaning: The parameter given as NETBRDGE_DISPLAY is invalid or not datafilled in DISPLAY field of any table NETBRDGE tuple. So no PMs are posted for this command. User actions: The NETBRDGE_DISPLAY has to be value data filled in DISPLAY field of a table NETBRDGE tuple.

9.9.5.8 Examples

Table 19 Examples for the POSTCLS command at SPM MAP level

Description of task	Post all the DMSCP SPM nodes
Command: MAP response:	POSTCLS DMSCP A post-set with of all the DMSCP SPMs is created.
Description of task	Post all the SMG4 SPM nodes
Command: MAP response:	POSTCLS SMG4 A post-set with of all the SMG4 SPMs is created.
Description of task	Post all the DPT SPM nodes
Command: MAP response:	POSTCLS IWDPT A post-set with of all the DPT SPMs is created.
Description of task	Post all the IW SPM nodes
Command: MAP response:	POSTCLS IWBRG A post-set with of all the IW SPMs is created.

Description of task	Post all the IW SPM nodes belonging to a Netbridge CLLI whose corresponding table NETBRDGE tuple's DISPLAY field contents are passed as parameter to the command.
Command: MAP response:	POSTCLS IWBRG E_AP A post-set with of all the IW SPMs using the NetBridge CLLI corresponding to the table NETBRDGE tuple whose DISPLAY field contains a value of "E_AP" is created.

9.9.6 Directory: TTP MAP

This feature enhances a command in the TTP MAP directory, but does not modify the directory itself.

9.9.6.1 Directory description

The commands in this directory helps operating company personnel to operate and maintain the trunks at the TTP MAP level.

9.9.6.2 Accessing directory: TTP

9.9.6.2.1 Access to directory or MAP level and return to CI

To access the TTP MAP level from the CI environment, type:

```
>MAPCI;MTC;TRKS;TTP;
```

To return to the CI environment, type:

```
>QUIT ALL
```

9.9.7 Command: POST

9.9.7.1 Command type: Listed MENU

9.9.7.2 Command target: All

9.9.7.3 Command availability: RES

9.9.7.4 Command description

The POST command Displays the trunk members. This command is used to post the various trunks for Maintenance.

This feature introduces a new parameter "BN" in the POST command to refine posted set of the trunks by a specified bearer network. This command can be used only on a already created post-set using any of the existing post commands. This enables the craft to use maintenance commands available at the TTP level on the trunk members of a specific bearer network.

9.9.7.5 Command syntax

The command syntax is as shown in "POST command at TTP MAP level with new parameters" on page 1389.

```

POST-- POST A NEW SET
Parms: [<SET TYPE> {T [<CLLI1> STRING
                        [<CNRI1> {0 TO 9999}}
                        [<....> STRING],
      G <CLLI> STRING
        [<CLNR> {0 TO 9999}]
        [<TO> {TO}]
        <CLNR> {0 TO 9999},
      ....
      WB <CLLI> STRING
        <CKTN> {0 TO 9999},
      BN [<ENET> STRING]
          [<A1_P> STRING]
          [<A1_S> STRING]
          [<IP_P> STRING]

```

Command	Parameters and variables
POST	Parms: BN [<ENET> STRING] [<A1_P> STRING] [<A1_S> STRING] [<IP_P> STRING] [<IP_S> STRING]]]
Parameters and variables	Description
BN	(optional) option to specify that the trunks are to be posted by bearer network.
BEARNETS_DISPLAY [STRING]	value datafilled in DISPLAY field of a table BEARNETS tuple

The command and response for ‘Post BN <BEARNETS_DISPLAY>’ is as shown in Table 20, “MAP outputs for POST BN <BEARNETS_DISPLAY> with associated meanings and actions,” on page 1390.

Table 20 MAP outputs for POST BN <BEARNETS_DISPLAY> with associated meanings and actions

Command MAPCI;MTC;TRKS;TTP;POST A IDL; POST BN <BEARNETS_DISPLAY>
RESPONSE: The trunk members in the given post-set hosted on the specified bearer network are posted on the TTP MAP. Meaning: All the trunks of a specified bearer network in the given post-set are posted at the TTP MAP level. All the maintenance commands available off a TTP MAP can be executed on this post-set. System or user actions: N/A User actions: Menu/Non menu commands available off the TTP MAP for maintenance can be executed.

9.9.7.5.2 POST BN <BEARNETS_DISPLAY> when bearer network entered is invalid

The command and response for ‘Post BN <BEARNETS_DISPLAY>’ when a invalid bearer network is as shown in Table 21, “MAP outputs for POST BN NET with associated meanings and actions,” on page 1391.

Table 21 MAP outputs for POST BN NET with associated meanings and actions

Command MAPCI;MTC;TRKS;TTP;POST A IDL; POST BN <INVALID BEARNETS_DISPLAY VALUE>
RESPONSE: “EITHER incorrect optional parameter(s) OR too many parameters.” PARM <no> INVALID POST -- Wrong number of parameters.” Meaning: The entry for the BEARNETS_DISPLAY is either not data filled in the DISPLAY field of any table BEARNETS tuples or is invalid. System or user actions: N/A User actions: Craft has to enter a valid value from the DISPLAY fields of any datafilled BEARNETS tuples.

9.9.7.5.3 Repetitive use of POST BN <BEARNETS_DISPLAY> is invalid

The command and response for ‘Post BN <BEARNETS_DISPLAY>’ when a invalid bearer network is as shown in Table 22, “MAP outputs for repetitive POST BN NET with associated meanings and actions,” on page 1392.

Table 22 MAP outputs for repetitive POST BN NET with associated meanings and actions

Command MAPCI;MTC;TRKS;TTP;POST G <TRUNK NAME>;POST BN BNET POST BN BNET
RESPONSE: “REPOST FOR NEW CONDITIONAL SELECTION” Meaning: Repetitive use of POST BN command is invalid. System or user actions: N/A User actions: Craft has to repost the Trunk to post the members of the new Bearer Network

9.9.7.5.4 POST BN <BEARNETS_DISPLAY> when no bearer network is entered

The command and response for ‘Post BN <BEARNETS_DISPLAY>’ when no bearer network is entered as shown in Table 23, “MAP outputs for POST BN with associated meanings and actions,” on page 1393.

Table 23 MAP outputs for POST BN with associated meanings and actions

Command MAPCI;MTC;TRKS;TTP;POST A IDL; POST BN
RESPONSE: “INVALID BEARER NETWORK ENTRY” Meaning: The selection of trunk members by bearer network is turned off. System or user actions: N/A User actions: Craft has to enter contents of the DISPLAY field in any of the table BEARNETS tuples, in the post BN command to activate it again.

Table 24 Examples for POST command at TTP MAP

Description of task	Select all the trunk members hosted on a bearer network in the given post-set. The value datafilled in DISPLAY field of corresponding table BEARNETS tuple being passed to the Command as parameter.
Command: MAP response:	POST BN A1_P Selects all trunk members of Bearer Network, the table BEARNETS tuple corresponding to which has a value of A1_P datafilled in the DISPLAY field.

9.9.8 New CI Tool called QOSSVER available to User on Core

A new CI tool QOSSVER is made available to user on the Nortel Switch Core. This tool helps list the CAF ACTIDs of Nortel features delivered in a load which has OSS impact.

9.9.8.1 Help Command for Tool

>q qossver

Displays list of Feature ACTIDs introduced in a load, which impact OSS. If no parameters are passed, the list displayed is for value of Parm OSS_PROV_VERSION in table OFCVAR.

Parms: [<LOAD RELEASE> {ALL,
SN07,
SN08,
SN09,
SN10,
SN11,
SN12,

```
SN13,
SN14,
SN15,
SN16,
SN17}]
```

9.9.8.2 Response message on passing an invalid Parm

```
>qossvr sn60
EITHER incorrect optional parameter(s) OR too many parameters.
QOSSVER -- Wrong number of parameters.
```

9.9.8.3 Output when “ALL” Parameter is passed to Tool

Tool lists CAF ACTIDs of all OSS impacting features delivered in all loads.

As stated earlier the ACTID of the features has to be entered against appropriate load, by the Nortel design team delivering the feature in the software database used by tool on Core, via feature code.

In case the software database used by tool, does not have any Feature ACTIDs entered for a load: There are no messages to the user to the effect that there are no OSS impacting features in a load.

A sample output in SN08 load (This feature's actid A00006780 has been entered in software database against SN08):

```
>qossvr all
OSS Impacting Features in SN08 are:
A00006780
```

9.9.8.4 Output when a valid load within permitted range is passed as Parm to QOSSVER:

- If there are one or more ACTIDs entered in database against load

```
>qossvr sn08
OSS Impacting Features in SN08 are:
A00006780
```

- If there are on ACTIDs entered in database against load

```
>qossvr sn09
No OSS Impacting Features in SN09
```

9.9.8.5 Output when no Parameter is passed to tool

Tool prints out ACTIDs entered in database against a load, which is same as load datafilled as value of table OFCVAR parm OSS_PROV_VERSION

Outputs when no Parameter is passed to QOSSVER

- If value of the OFCVAR Parm is SN07(No feature ACTIDs in database against SN07)

```
>qossvr
No OSS Impacting Features in SN07
```

- If value of the OFCVAR Parm is SN08(ACTID of this feature i.e. A00006780 is entered in database against SN08)

```
>qossvr
OSS Impacting Features in SN08 are:
```

A00006780

9.9.9 User Responses for Table Control Operations

9.9.9.1 Table BEARNETS

9.9.9.1.1 Tuple Addition Failure with Non-unique DISPLAY field

Attempting to add a tuple to table BEARNETS which includes a DISPLAY field value which is already used by an existing tuple in the table will be rejected as shown below.

Existing BEARNETS tuple

NETIDX	BNETNAME	DISPLAY	FABRIC	OPTIONS
NET 1	NET_AAL1	A1_P	AAL1	\$

```

>add net 4 NET_AAL2      A1_P      AAL1 $
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
DISPLAY field for a Bearer Network must be unique
TUPLE TO BE ADDED:
  NET 4                      NET_AAL3  A1_P  AAL1  $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

```

Note: Following are the Warning Messages provided to the user for a tuple in Table BEARNETS having a Non-Unique 'Display' field:

During TABXFR, the tuple will be transferred and the warning generated:

```

"DISPLAY fields in Table BEARNETS are not unique
Change the DISPLAY field values to be unique after RESTORE."

```

During TABAUDIT,

```

"DISPLAY fields in Table BEARNETS are not unique
Change the DISPLAY field values to be unique."

```

9.9.9.1.2 Tuple Change Failure with Non-unique DISPLAY field

Attempting to change a tuple to table BEARNETS which includes a DISPLAY field value which is already used by an existing tuple in the table will be rejected as shown below. Assume existing BEARNETS tuple as shown in 12.8.9.1.1.

```

>pos net 0
  NET 0                      TDM_ENET  ENET  ENET  $
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
BNETNAME: TDM_ENET
>
DISPLAY: ENET
>A1_P
FABRIC: ENET
>

```

```

OPTIONS:
>$
DISPLAY field for a Bearer Network must be unique
TUPLE TO BE CHANGED:
  NET 0          TDM_ENET    A1_P  ENET      $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

```

Note: Following are the Warning Messages provided to the user for a tuple in Table BEARNETS having a Non-Unique 'Display' field:

During TABXFR, the tuple will be transferred and the warning generated:

```

"DISPLAY fields in Table BEARNETS are not unique
Change the DISPLAY field values to be unique after RESTORE."

```

During TABAUDIT,

```

"DISPLAY fields in Table BEARNETS are not unique
Change the DISPLAY field values to be unique."

```

9.9.9.1.3 Tuple Addition Failure with Empty DISPLAY field

Attempting to add a tuple to table BEARNETS which includes an empty DISPLAY field value will be rejected as shown below.

```

>add net 7
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
BNETNAME:
>net_ip
DISPLAY:
>$
FABRIC:
>ip
OPTIONS:
>$
DISPLAY field value is not valid.
TUPLE TO BE ADDED:
  NET 7          NET_IP      $    IP      $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

```

Note: Following are the Warning Messages provided to the user for a tuple in Table BEARNETS having a Empty 'Display' field:

During TABXFR, the tuple will be transferred and the warning generated:

```

"DISPLAY fields of table BEARNETS tuples are empty
Change the DISPLAY field value to be non-empty after RESTORE."

```

During TABAUDIT,

```

"DISPLAY fields of table BEARNETS tuples are empty
Change the DISPLAY field value to be non-empty."

```

9.9.9.2 Table NETBRDGE

9.9.9.2.1 Tuple Addition Failure with Non-unique DISPLAY field

Attempting to add a tuple to table NETBRDGE which includes a DISPLAY field value which is already used by an existing tuple in the table will be rejected as shown below.

Existing NETBRDGE tuple:

BRDGCLLI	BRDGTYPE	DISPLAY	BEARNETS
ENET_TO_AAL1	CORE_BRDGE	E_A1	TDM_ENET NET_AAL1

```

--
>add ENET_TO_AAL3 CORE_BRDGE E_A1 TDM_ENET NET_AAL1
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
DISPLAY field for a Bridge Pool CLLI should be unique
TUPLE TO BE ADDED:
      ENET_TO_AAL3 CORE_BRDGE      E_A1 TDM_ENET NET_AAL1
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

Note: Following are the Warning Messages provided to the user for a tuple in Table NETBRDGE having a Non-Unique 'Display' field:

During TABXFR, the tuple will be transferred and the warning generated:
 "DISPLAY field of table NETBRDGE for a Bridge Pool CLLI is not unique
 Change the DISPLAY field value to be unique after RESTORE."
 During TABAUDIT,
 "DISPLAY field of table NETBRDGE for a Bridge Pool CLLI is not unique
 Change the DISPLAY field value to be unique."

9.9.9.2.2 Tuple Change Failure with Non-unique DISPLAY field

Attempting to change a tuple to table NETBRDGE which includes a DISPLAY field value which is already used by an existing tuple in the table will be rejected as shown below. Assume existing NETBRDGE tuple as shown in 12.8.9.2.1.

```

>pos ENET_TO_AAL2
      ENET_TO_AAL2 CORE_BRDGE      A2 TDM_ENET NET_AAL1
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
BRDGTYPE: CORE_BRDGE
>
DISPLAY: A2
>e_a1
BEARNETS: TDM_ENET NET_AAL1
>
DISPLAY field for a Bridge Pool CLLI should be unique
TUPLE TO BE CHANGED:
      ENET_TO_AAL2 CORE_BRDGE      E_A1 TDM_ENET NET_AAL1
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

Note: Following are the Warning Messages provided to the user for a tuple in Table NETBRDGE having a Non-Unique 'Display' field:

During TABXFR, the tuple will be transferred and the warning generated:
 "DISPLAY field of table NETBRDGE for a Bridge Pool CLLI is not unique
 Change the DISPLAY field value to be unique after RESTORE."
 During TABAUDIT,

“DISPLAY fields in Table NETBRDGE are not unique
Change the DISPLAY field values to be unique.”

9.9.9.2.3 Tuple Addition Failure with Empty DISPLAY field

Attempting to add a tuple to table NETBRDGE which includes an empty DISPLAY field value will be rejected as shown below.

```
>add enet_to_aal4
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
BRDGTTYPE:
>CORE_BRDGE
DISPLAY:
>$
BEARNETS:
>TDM_ENET NET_AAL1
DISPLAY field of NETBRDGE tuple cannot be empty
TUPLE TO BE ADDED:
      ENET_TO_AAL4 CORE_BRDGE          $ TDM_ENET NET_AAL1
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
```

Note: Following are the Warning Messages provided to the user for a tuple in Table NETBRDGE having a Empty 'Display' field:

During TABXFR, the tuple will be transferred and the warning generated:

“DISPLAY fields of table NETBRDGE tuples are empty
Change the DISPLAY field value to be non-empty after RESTORE.”

During TABAUDIT,

“DISPLAY fields of table NETBRDGE tuples are empty
Change the DISPLAY field value to be non-empty.”

9.9.9.2.4 Bridge Pool Creation Failure

If, when attempting to add a tuple to table NETBRDGE, the attempt to create a Bridge Pool fails, the tuple will be rejected. The following warning will be displayed to the user.

“Bridge Pool Creation Failed for CLI”

9.9.9.2.5 NETBRDGE Tuple Deletion Success

When a tuple from table NETBRDGE is deleted successfully, the following message will be displayed to the user.

“DELETING BRIDGE POOL OBJECT”

9.9.9.3 Table MNNODE

Bridge Pool Creation / Deletion no longer happens during addition / deletion of IW SPM(BRGD_ONLY)SPM Tuples in MNNODE table

The following message is no longer seen during deletion of MNNODE tuples for IW BRDG_ONLY SPMs:

“DELETING BRIDGE POOL OBJECT”

9.10 OSSGate Interface Changes

Functionality changes described in Section 9.9 of this Section, i.e. Enhancements to Line Query Commands. Functionality changes Turning ON/OFF is controlled using a newly introduced table OFCVAR Parm OSS_PROV_VERSION. The enhancements are effective only when this Office Parameter has a value greater than SN07.

9.11 Security

Not Applicable.

10: A00006865 Configuration (CN)

10.1 Feature name

SN08 GIGE HAL Feature

This document is intended for MG9000 customers as well as internal Nortel functional groups (design teams, test teams, etc).

This document will cover the functional description of the SN08 GIGE HAL (Hardware Abstraction Layer) feature, A00006865.

Please refer to A00006865 documentation for more information on the SN08 GIGE HAL feature.

10.2 Hardware and Software Requirements

This feature will provide HAL support for NTNY45FA (SuperCore GigE card).

10.3 Initial Configuration

This section is not applicable and the subsections are removed from the document.

10.4 Office/Subnet parameters (OP/SP) (CM & SESM)

This section is not applicable and the subsections are removed from the document.

10.5 Upgrade Considerations

This section is not applicable and the subsections are removed from the document.

10.6 Data schema (DS) (CM, MIBS, RDB)

This section is not applicable and the subsections are removed from the document.

10.7 Service Orders (SO) (CM & SESM)

This section is not applicable and the subsections are removed from the document.

10.8 Software optionality control (SOC)

This section is not applicable and the subsections are removed from the document.

10.9 User interface changes

This section is not applicable and the subsections are removed from the document.

10.10 OSSGate Interface Changes

This section is not applicable and the subsections are removed from the document.

10.11 Security

This section is not applicable and the subsections are removed from the document.

10.12 Configuration Walkthrough

This section is not applicable and the subsections are removed from the document.

11: A00006893 Configuration (CN)

11.1 Feature name

TLS Support for NGSS

11.1 Hardware and Software Requirements

Hardware/software required is a standard NGSS with a standard SN08 software load.

11.2 Initial Configuration

A standard SN07 load is the initial configuration for TLS-enabled NGSS.

11.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable. NGSS-only feature.

11.4 Upgrade Considerations

11.4.1 Dump and Restore (CM)

None.

11.4.2 Element Management Upgrade

Additional steps will be required to provision a new single certificate for the NGSS Sip application, Apache (NCGL), and Tomcat (NGSS). This tool must be executed manually.

11.4.3 Downgrade impact

None.

11.5 Data schema (DS) (CM, MIBS, RDB)

Not applicable.

11.6 Service Orders (SO) (CM & SESM)

Not applicable.

11.7 Software optionality control (SOC)

Not applicable. TLS will be standard on all SN08+ NGSS loads.

11.8 Element Management

11.8.1 New/modified GUIs

Table 12 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
NGSS Tomcat Web Server	Changed

11.8.2 GUI information

11.8.2.1 GUI: NGSS Tomcat Web Server

This GUI is an NGSS-specific management tool.

The changes made to this GUI consist of:

- The addition of a Security menu under the provisioning menu
- The addition of Security configuration parameters web page
- The addition of a Certificates menu
- The addition of the Display local server certificate web page
- The addition of the Display Trusted certificates web page
- The addition of the Add Trusted certificate web page

11.8.2.1.1 Functional description

Changes to the NGSS Tomcat GUI are as follows:

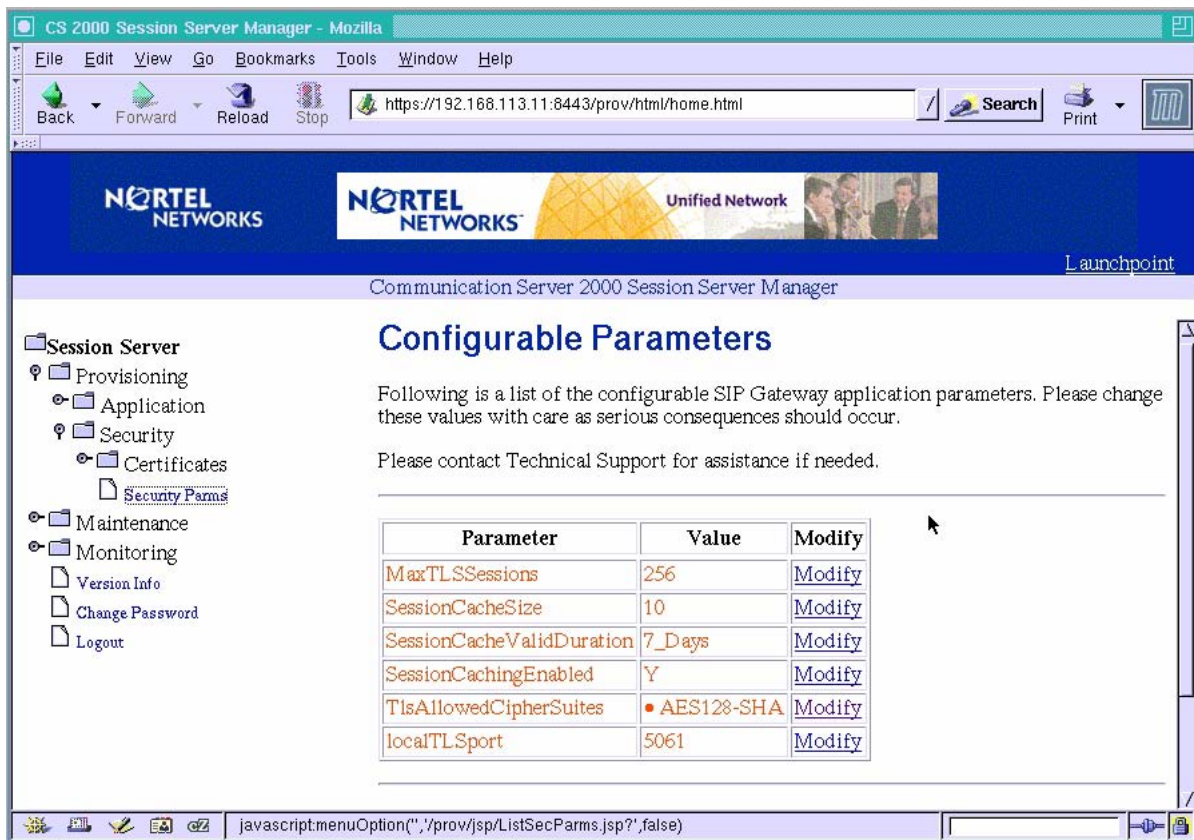
- A new “Security” subfolder has been added to the Provisioning folder of the Tomcat GUI.
- Under the “Security” subfolder a “Config Data” option has been added.
- Clicking on the “Security Params” option brings up the Security Params configuration page (see “Security Parameter Configuration Page” on page 1405).
- Under the “Security” subfolder, a new “Certificates” subfolder has been added.
- Under the “Certificates” subfolder, the “Server Certificate”, “Remote Trusted Certificate”, and “Add Remote Trusted Certificates” options have been added.
- Clicking on the “Server Certificate” option brings up the Display Local Server Certificate page.
- Clicking on the “Remote Trusted Certificates” option brings up the Certificates Provisioned page.
- Clicking on the “Add Remote Trusted Certificates” option brings up the Add Trusted Certificate page.

- Changes to the “Add Server” and “Modify Server” section of the SIP Gateway GUI allow for the provisioning of servers using the TLS protocol, in addition to the TCP and UDP protocols.

11.8.2.1.2 GUI usage and implications

The purpose of the new Security Parameter Configuration Page is to change the values of the customer-accessible security parameters. From the table listed in the figure below, customers can choose to alter any of the visible parameters.

Figure 1 Security Parameter Configuration Page



This can be done in the following way:

- Clicking on any parameter option brings up a change screen for that parameter (see Figure 2 “Sample Pull-down Menu for Parameter Provisioning” on page 1406, Figure 3 “Sample Text Input for Parameter Provisioning” on page 1407, and Figure 4 “Sample Checklist Input for Parameter Provisioning” on page 1408 below).
- Clicking on the “change” button on the change screen changes the value of that parameter in the NGSS SOLID database.

- Note that certain parameters (marked as Change Time = “CallP Restart” on the Configurable Parameters screen) require a restart of the NGSS CallP engine to effect the new parameter value.

A warning will be generated any time a security parameter is changed.

Figure 2 Sample Pull-down Menu for Parameter Provisioning

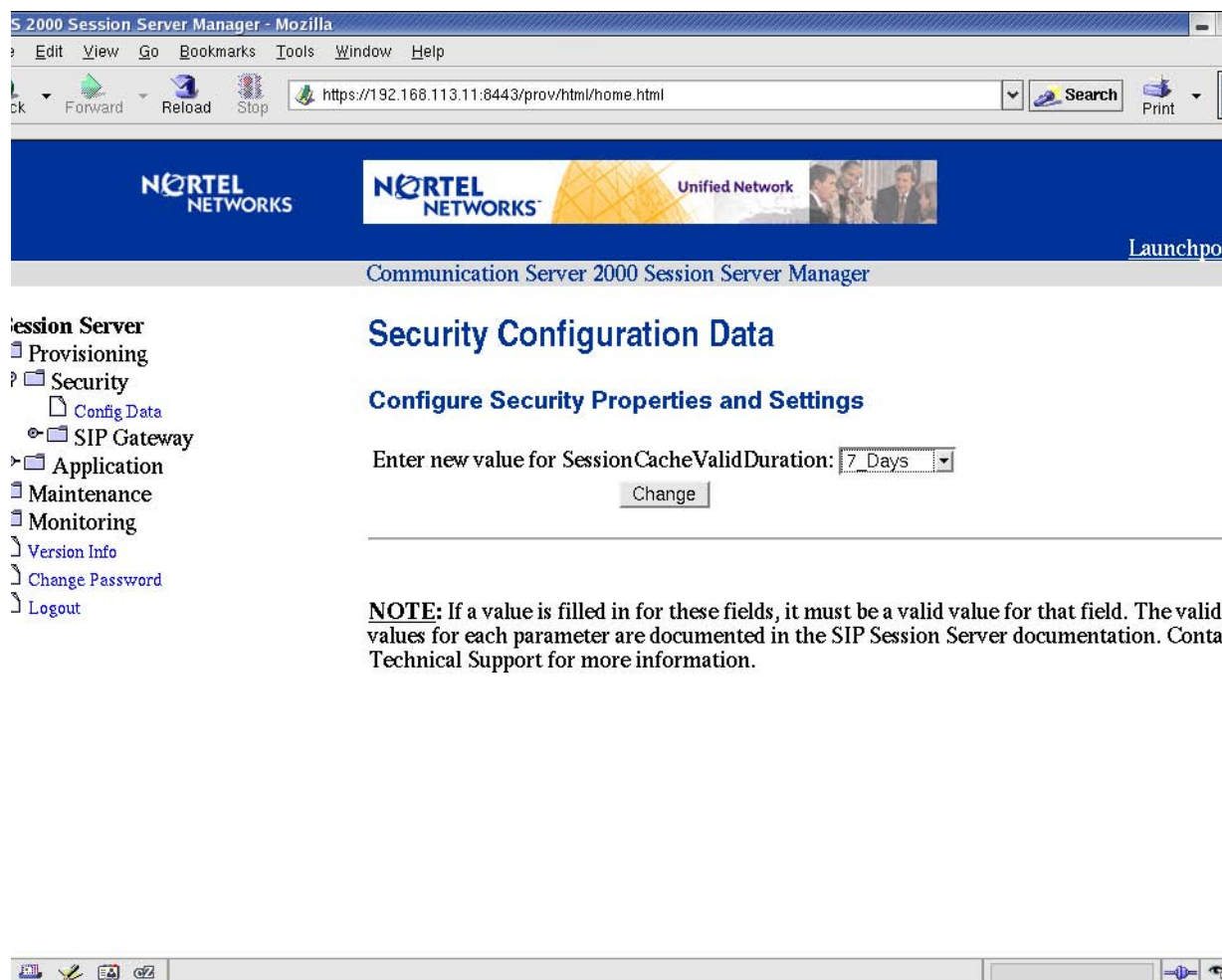


Figure 3 Sample Text Input for Parameter Provisioning

Session Server Manager - Mozilla

Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop <https://192.168.113.11:8443/prov/html/home.html> Search Print

NORTEL NETWORKS **NORTEL NETWORKS** Unified Network

Launchpage

Communication Server 2000 Session Server Manager

Session Server

- Provisioning
- Security
 - Config Data
 - SIP Gateway
- Application
- Maintenance
- Monitoring
- Version Info
- Change Password
- Logout

Security Configuration Data

Configure Security Properties and Settings

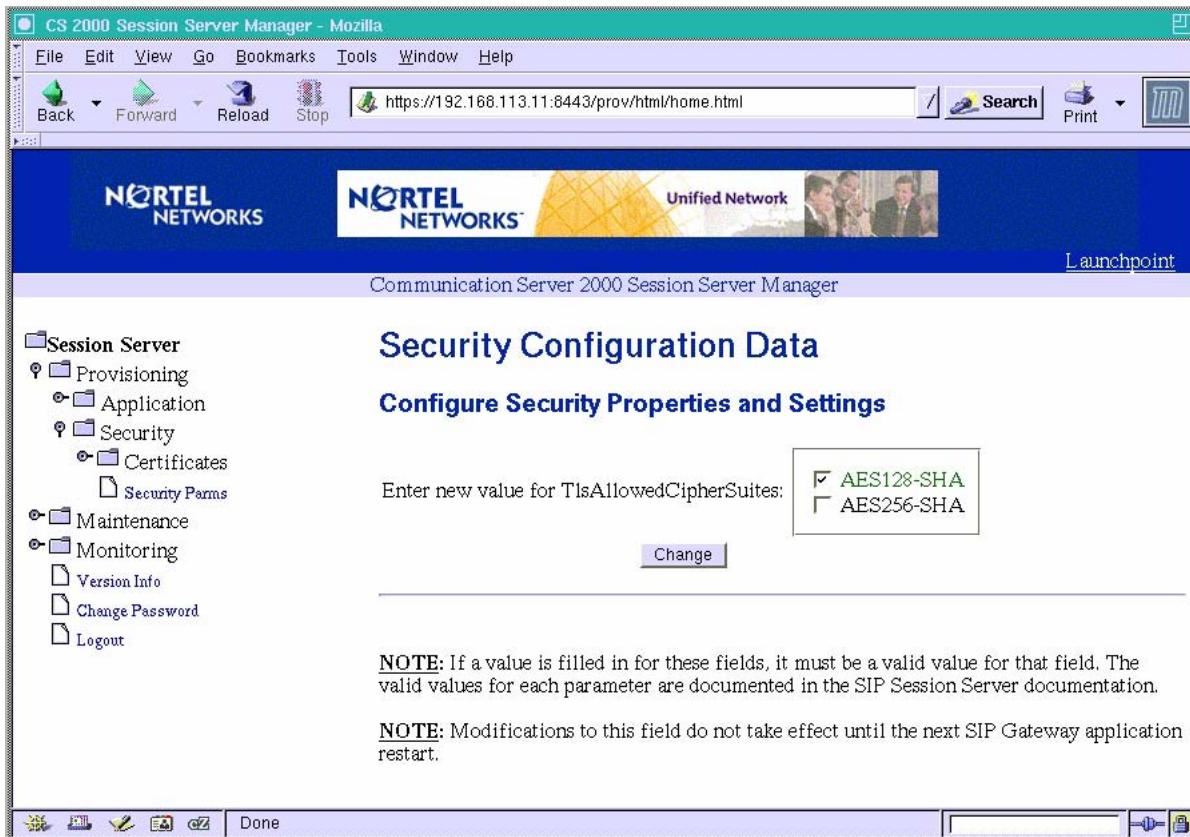
Enter new value for MaxTLSSessions:

NOTE: If a value is filled in for these fields, it must be a valid value for that field. The valid values for each parameter are documented in the SIP Session Server documentation. Contact Technical Support for more information.

NOTE: Modifications to this field do not take effect until the next SIP Gateway application restart.

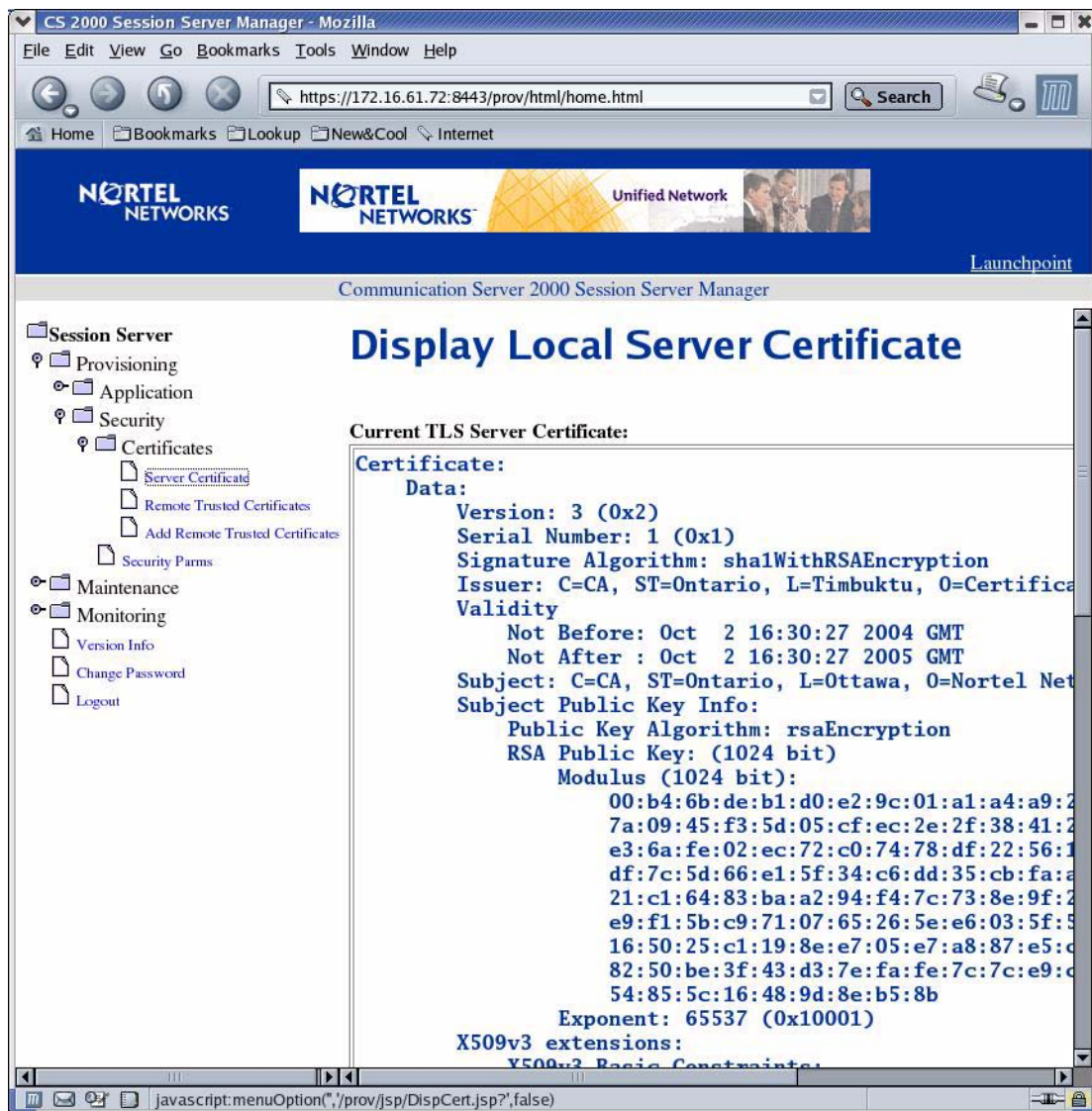
Done

This GUI has default values set for the parameters that will allow the NGSS to operate properly with no datafill operations after the upgrade. Customers can change these values as needed.

Figure 4 Sample Checklist Input for Parameter Provisioning.

The parameters on these pages materially affect the behavior of TLS CallP and NGSS security. Changes to them can cause problems for the NGSS up to and including an outage, and/or leaving NGSS signalling data open to capture and/or attack. It is advised that only knowledgeable customer or Nortel representatives recommend changes to these values.

The purpose of the Display local server certificate web page is to provide an interface to retrieve the local certificate and drop it into a remote server's trusted certificate list (in the case of self-signed certificates). From the "Security" submenu, then the "Certificates" submenu, click the "Display Certificate" option (see Figure 5 "Display local server certificate web page" on page 1409). Here, with a web page view to the Remote server, you could copy the certificate text as shown in the Display Certificate page, and paste it into the appropriate Remote Server's 'add trusted certificate' interface.

Figure 5 Display local server certificate web page

The purpose of the Display Trusted certificates web page is to provide an interface to view the current list of remote trusted certificates, and provide a way to remove them should the occasion arise. From the “Security” submenu, then the “Certificates” submenu, click the “Remote Trusted Certificates” option (see Figure 6 “Remote Trusted Certificates web page” on page 1410). Each name in the list is unique, and to remove an item from the list, select the “Delete” option, at which point the craftperson would be asked to confirm the deletion and the request would then take place. If the confirmation is not granted, no action is taken.

Figure 6 Remote Trusted Certificates web page

Certificates Provisioned

This is a list of configured trusted certificates.

Deleting these certificates will take effect on the next application restart. Please contact Technical Support for assistance if needed.

Certificate Name	Certificate PEM	Delete
certificate_server_1	<pre>-----BEGIN CERTIFICATE----- MIIDMTCAppqAwIBAgIBATANBgkqhkiG9wOBAQUFADBhMQswCQYDVQQGEwJDQTEQ MA4GA1UECBMHT250YXJpbzERMA8GA1UEBxMIYV1tYnVrdHUxHjAcBgNVBAoTFUN1 cnRpZmljYXR1IEF1dGhvcml0eTENMA8GA1UECxmETm9uZTAeFw0wNDEwMDI0NjMw MjdaFw0wNTEwMDI0NjMwMjdaMHAcCzAJBgNVBAYTAkNBMRAdBgYDVQKIEdwPbnRh cm1vMQ8wDQYDVQQHEwZp dHRhd2ExGDAwBgNVBAoTDO5vcnR1bCB0ZXRX3b3JrczEN MAsGA1UECxmETkdTUzEVMBMGA1UEAxMMMTcyLjE2LjYxLjcyMIGfMAOGCSqGSIb3 DQEBAAUAA4GNADCBiQKBgQCoA96x00KcAaGkqSyYb3oJRfNdBc/sLi84QSBvY+Nq /gLscsBOeN8iVhY2n998XWbhXzTG3TXL+qayZyHBZIO6opT0fHO0ny2W++nxw81x B2UmXuYDX1+ktRZQJcEZjucF56iH5cNiJjIjQvj9D0376/nx86ccIE1SFXBZInY61 iwIDAQABo4HpMIHmMakGALUdEwQCMaAwLAYJYIZIAyB4QgENBB8WU9wZ5TU0wg R2VuZXJhdGVkIEN1cnRpZmljYXR1MBOGA1UdDgQWBBTWXiqgr7d4Uo1MXX5Eqw5 oo3kSjCBiWYDVROjBIGDMIGAgBTL1FJssNnQD4ErOj//pQZ20wiVnaFlpGMwYTEL MAKGA1UEBhMCQOEExEDA0BgNVBAgTB09udGFyaW8xETAPBgNVBACTCFRpbWJ1a3R1 MR4wHAYDVQQKEwVZDZXJ0aWZpY2FOZSBBDXRob3JpdHkxDTALBgNVBAAsTBESvbmWC AQAwDQYJKoZIhvcNAQEFBQADgYEAREAha8cbYHDvgyeXajUemuA6G0yg13BpVjN QvBQnypv0DCvoSK10kB/LcqeHoyxsUJKQMeUf7H3jbbqWp4ot7n3/ha8vA+IA 21gOmEQkFpE5v2RzKZ39fCj/RP3QY5/jRmx5TaSt3C57ANziTWBqhNackvu8Ky 6MBDSiM= -----END CERTIFICATE-----</pre>	Delete

The purpose of the Add Trusted certificate web page is to provide an interface to add to the current list of Remote Server Certificates that are trusted. From the “Security” submenu, then the “Certificates” submenu, click the “Add Remote Trusted Certificate” option (see Figure 7 “Add Remote Trusted Certificate web page” on page 1411). When attempting to add a certificate to the list of trusted certificates, the name of the certificate must be unique, and the “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” lines must follow the example below. Instead of the word “CERTIFICATE”, the word “TRUSTED” could be used as well. Note that only PEM formatted (i.e. base64 encoded) certificates are acceptable.

Figure 7 Add Remote Trusted Certificate web page

File Edit View Go Bookmarks Tools Window Help

https://172.16.61.72:8443/prov/html/home.html Search

Home Bookmarks Lookup New&Cool Internet

NORTEL NETWORKS Unified Network Launchpoint

Communication Server 2000 Session Server Manager

Session Server

- Provisioning
- Application
- Security
 - Certificates**
 - Server Certificate
 - Remote Trusted Certificates
 - Add Remote Trusted Certificates
 - Security Params
- Maintenance
- Monitoring
 - Version Info
 - Change Password
 - Logout

Add Trusted Certificate

Certificate Name certificate_server_1

Certificate (in PEM)

```
-----BEGIN CERTIFICATE-----
MIIDMTCCApqgAwIBAgIBATANBgkqhkiG9wOBAQUFADBhMQswCQYDVQQGEwJDQTEQ
MA4GA1UECBMT250YXJpbzERMA8GA1UEBxMIVGltYnVrdHUXHjAcBgNVBAoTFUN1
cnRpZmljYXR1IEF1dGhvcml0eTENMA8GA1UECzMETm9uZTAeFw0wNDEwMDIxNjMw
MjdaFw0wNTEwMDIxNjMwMjdaMHAcCzAJBgNVBAYTAkNBMR4wDgYDVQQLIEwdPbnRh
cm1vMQ8wDQYDVQQHEwZPdHRhd2ExGDAWBgNVBAoTD05vcnRlbnCB0ZXR3b3JrczEN
MA8GA1UECzMETkdTUzEVMBMGA1UEAxMMMTcyLjE2LjYxLjcyMIGfMAOGCSqGSIb3
DQEBAAQAAAGNADCBiQKBgcQCoa96x0OKcAaGkqSyYb3oJRfNdBc/sLi84QSbvY+Nq
/gLscsBOeN8iVhY2n998XWbhXzTG3TXL+qayZyHBZIO6opTOfH00ny2W++nxW8lx
B2UmXuYDX1+ktRZQJcEZjucF56iH5cNiJlJQvj9D0376/nx86ccIE1SFXBZInY61
iwIDAQABo4HpMIHmMAkGA1UdEwQCMAAwLAYJYIZIAAYb4QgENBB8WHU9wZW5TU0wg
R2VuZXJhdGVkIENlcnRpZmljYXRlMBOGA1UdDgQWBBTWXiqgr7d4UoLMXX5Eqw5
oo3kSjCBiwyDVROjBIGDMIGAgBTL1FJssNnQD4ErOj//pQZ20wiVnaFlpGMwYTEL
MAkGA1UEBhMCQOEwEDAOBgNVBAGTB09udGFyaW8xETAPBgNVBACTCFRpbWJ1a3R1
MR4wHAYDVQQKEwVdZXJOaWZpY2FOZSBBDXR0b3JpdHkxDTALBgNVBAStBE5vbmWC
AQAwDQYJKoZIhvcNAQEFBQADgYEAkREAh8cbYHDvgYeXajUemuA6G0yg13BpVjN
QvBQqnyvpODCvoSK10kB/lcqeHoyxsUJKQMeUf7H3jbbqyTwp4ot7n3/hA8vA+IA
2IgOmEQuKbFpE5v2RzKZ39fCj/RP3QY5/jRmx5TaSt3C57ANziTWBqhNackvu8Ky
6MBDSiM=
-----END CERTIFICATE-----
```

Add

Done

The following figures demonstrate how to provision and/or modify a server so that it utilizes the TLS protocol rather than TCP or UDP.

Figure 8 "Adding a SIP Server using the TLS protocol." on page 1412 demonstrates how to add a SIP server using TLS protocol. The difference between this method and the new method is small: the user simply selects "TLS" in the protocol field beside the IP address in question to enable the use of TLS. Then complete and submit the datafill as required.

Figure 9 "Modifying a SIP server to use TLS protocol." on page 1413 demonstrates how to modify a SIP server to use the TLS protocol. The user chooses to modify the SIP server as is done normally. Using the drop-down menu of the protocol field next to the IP address in question, select "TLS". Then complete and submit the datafill changes as required.

Figure 8 Adding a SIP Server using the TLS protocol.

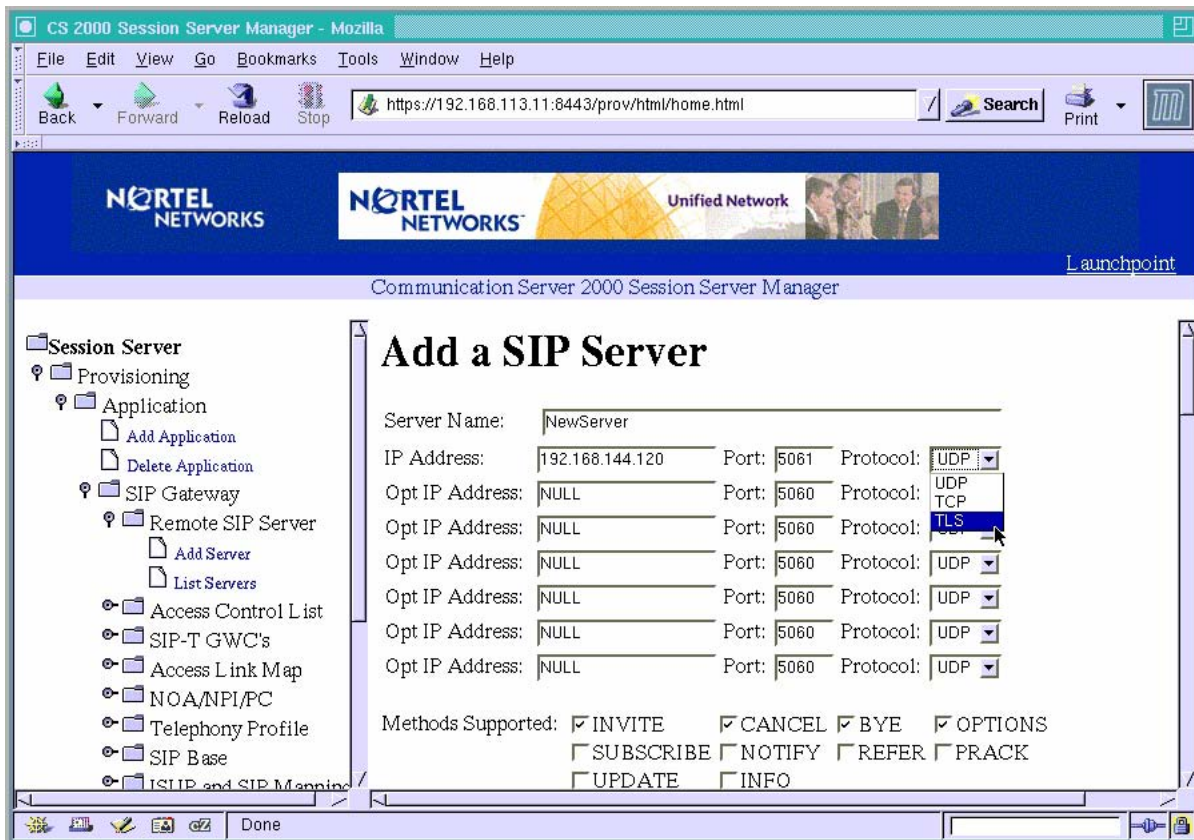
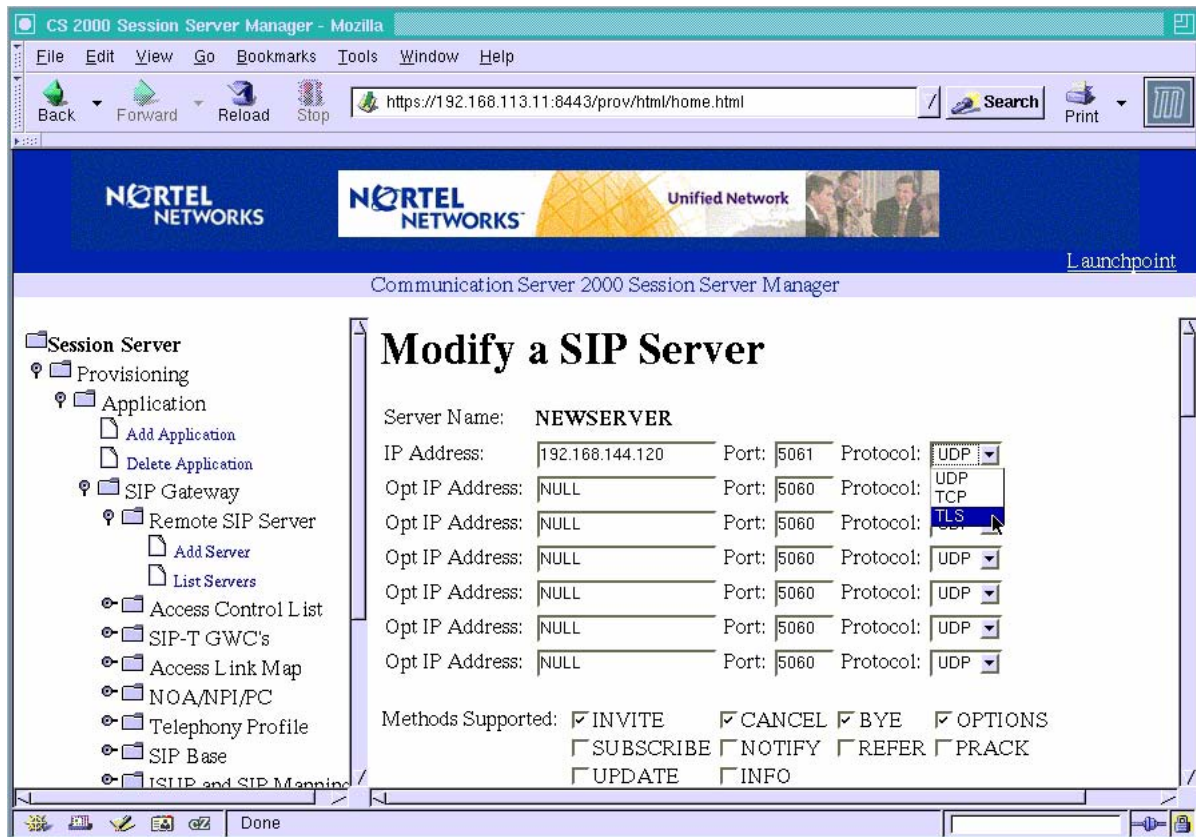


Figure 9 Modifying a SIP server to use TLS protocol.**11.8.2.1.3 GUI Fields**

The following table lists fields for the NGSS Tomcat Webserver Security Params GUI.

Table 13 Security Parameters in Tomcat WebServer

Parameter	maxTlsSessions	Type	Integer
Description	The Maximum number of TLS sessions allowed.	Default Value	256

Effect of Change	Changes the maximum number of TLS sessions allowed. Important: NGSS callp must be locked/suspended and unsus-pended/unlocked to activate changes made on the web page. Until the callp lock/suspend is performed, the displayed value will be inconsistent with the operational value.	Minimum= Maximum=	10 2048
Adverse Effects	Setting the value lower than the number of clients trying to connect will freeze some clients out. In SN08, the clients are peer servers to the NGSS, so this means remote servers will be denied a secure connection to the NGSS.		
Countering Adverse Effects	Set the value of the parameter as high as the maximum number of peer servers connected to this NGSS. The network should be engineered so that fewer than 2048 peer servers need to connect to a single NGSS at once.		
Parameter	SessionCacheEnabled	Type	Y/N
Description	Determines whether session caching is enabled or not.	Default Value	Y
Effect of Change	Enabling the session cache speeds up the performance of TLS connection requests for enabled clients. Note that, if few or no peer servers to the NGSS have session-caching enabled clients, then little or no performance increase will be observed for TLS connection requests. (Note that peer servers to the NGSS are considered clients when they initiate a connection request.) Important: NGSS callp must be locked/suspended and unsus-pended/unlocked to activate changes made on the web page. Until the callp lock/suspend is performed, the displayed value will be inconsistent with the operational value.		
Adverse Effects	Activating session caching will allocate memory for the session cache. See the SessionCacheSize parm for details.		
Countering Adverse Effects	See the SessionCacheSize parm for details.		
Parameter	SessionCacheSize	Type	Integer

Description	The size of the TLS session cache. The session cache increases system performance by allowing clients that support session caching to bypass the time-consuming TLS handshake procedure after one handshake is done.	Default Value	10
Effect of Change	A larger session cache speeds up the performance of TLS connection requests for enabled clients. Important: NGSS callp must be locked/suspended and unsuspended/unlocked to activate changes made on the web page. Until the callp lock/suspend is performed, the displayed value will be inconsistent with the operational value.	Allowed Values	10, 100, 1000
Adverse Effects	The largest session cache setting (1000) consumes 1 MB of memory on the NGSS.		
Countering Adverse Effects	In the event that 1MB of memory cannot be devoted to the session cache, memory can be reclaimed by reducing the size of the cache. This will reduce system performance if a relatively large number of clients were session-caching enabled. Remember to lock/suspend NGSS callp to enable the change.		
Parameter	SessionCacheValidDuration	Type	Time
Description	The duration for which sessions are stored in the session cache. The session data is expunged from the cache either 24 hours or 7 days from when it was first inserted into the cache. Important: NGSS callp must be locked/suspended and unsuspended/unlocked to activate changes made on the web page. Until the callp lock/suspend is performed, the displayed value will be inconsistent with the operational value.	Default Value	7_Days

Effect of Change	Every connecting client will be forced to do a full handshake on the first connection after its session is expunged from the cache. Changing this value changes the frequency with which this may happen. (Clients that typically stay connected for longer than 7 days will notice no difference.) Important: NGSS callp must be locked/suspended and unsus-pended/unlocked to activate changes made on the web page. Until the callp lock/suspend is performed, the displayed value will be inconsistent with the operational value.	Allowed Values	24_Hours; 7_Days
Adverse Effects	Systems that have large numbers of clients making frequent connection requests may notice performance issues on the 24_Hours setting. In SN08, this should be rare.		
Countering Adverse Effects	Increase the value of the SessionCacheValidDuration parameter to 7_Days, and lock/suspend NGSS callp to enable the change.		
Parameter	localTLSPort	Type	Integer
Description	The port number TLS uses on the local NGSS.	Default Value	5061
Effect of Change	Changes the port that TLS uses. Important: NGSS callp must be locked/suspended and unsus-pended/unlocked to activate changes made on the web page. Until the callp lock/suspend is performed, the displayed value will be inconsistent with the operational value.		
Adverse Effects	Remote clients or remote peer servers may require intervention to connect properly to TLS working under a changed port number.		
Countering Adverse Effects	Don't change the TLS port number unless absolutely necessary. 5061 is the default port number specified in the TLS standard (RFC 2246); we recommend that the TLS standard be followed.		
Parameter	TlsAllowedCipherSuites	Type	Checklist

Description	The cipher suites that TLS is allowed to use in secure communication.	Default Value	AES128-SHA
Effect of Change	Changes the set of ciphers that TLS is allowed to use. In SN08, only two ciphers are allowed; of those, AES128-SHA is mandatory. The NGSS will always accept TLS connections requested with the AES128-SHA cipher (providing, of course, that TLS is enabled in the first place). Important: NGSS callp must be locked/suspended and unsuspended/unlocked to activate changes made on the web page. Until the callp lock/suspend is performed, the displayed value will be inconsistent with the operational value.	Allowed Values	AES128-SHA; AES256-SHA
Adverse Effects	The only other choice available is AES256-SHA. This cipher uses larger (256-bit) keys. The user may notice a performance degradation with AES256-SHA allowed when compared to the default setting (AES128-SHA only).		
Countering Adverse Effects	If a performance degradation is attributable to allowing AES256-SHA ciphers in TLS connections, then uncheck AES256-SHA and lock/suspend NGSS callp to enable the change.		

11.8.2.1.4 Usage example

The following example shows sample datafill selection for the NGSS Tomcat Security Params Configuration Web Page. Please refer to the figures cited below for examples.

Example:

1. Customer enters the NGSS EM web page.
2. Customer enters the NGSS Tomcat CallP Application webpage.
3. Customer clicks on the Provisioning Tab on the Menu Frame (see “Security Parameter Configuration Page” on page 1405).
4. Customer clicks on the Security Tab.
5. Customer clicks on the Security Params link, which brings up the Security Configurable Parameters page.

6. Customer clicks on the “Modify” link beside the SessionCacheValid-Duration parameter. This brings up the Modify page for that parameter (see “Sample Pull-down Menu for Parameter Provisioning” on page 1406).
7. Customer chooses between one of three options on the pull-down menu.
8. Customer can press “Change” to accept their newly chosen value, or click on another link to abort the change operation.

11.8.2.1.5 GUI release history update

For the NGSS Tomcat Application Web Server GUI, the following was added in SN08 due to this feature:

- The Security Folder, under the Provisioning folder.
- The Security Params Config page, under the Security folder.
- The Individual Security Parm Change page, accessible via per-parameter links from the Security Params Config page.

Note: The parameters displayed on the pages above are derived from entries entered in to the SOLID SQL database at loadbuild time.

- The Certificates Folder, under the Security Folder.
- The Server Certificate page, accessible via the Certificates Folder.
- The Remove Trusted Certificates page, accessible via the Certificates Folder.
- The Add Remote Trusted Certificate page, accessible via the Certificates Folder.

11.8.2.1.6 Context sensitive launching information

This GUI is accessed from a series of links starting on the NGSS main web page. The normal instructions for launching the NGSS Application Web Server can be followed for the new web pages described herein.

11.8.2.1.7 Supplementary information

All of the parameters described above require a NGSS CallP Restart in order to have the value active in the CallP Application. These parameters are marked by an orange text color on the Security Parm Configuration page (see Figure 1 “Security Parameter Configuration Page” on page 1405), and also by a warning on the page where the parameter value is changed (see Figure 3 “Sample Text Input for Parameter Provisioning” on page 1407).

The act of removing a trusted certificate from the list of trusted certificates will not be reflected until a CallP Restart as well. However, adding to the list of trusted certificates via the “Add Remote Trusted Certificate” web page will take effect immediately (assuming the certificate presented passes the applicable checks).

11.8.3 CLI Interface

11.8.3.1 Certificate Management Tool (`cert_mngnt` or `cert_mgmt`)

The certificate management tool is a customer-visible tool that provides a common interface for provisioning certificates 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_mngnt` or `/sbin/cert_mgmt`, and is executable only by the root user. Since `/sbin` is in the path, `cert_mngnt` 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 craftsman would manually send the signing request to the Certificate Authority (CA) where it will be signed.
- Provision a trusted certificate (CAcertificate) and a CA-signed certificate produced from the signing request.

RSA encryption with SHA-1 only is supported by the three applications.

The tool makes permissions on private key files and the certificate keystore file to be read/write by the root user.

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 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: locate 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.

11.8.3.1.1 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.

11.8.3.1.2 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 SN08. 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.

11.8.3.1.3 Certificate and Key revocation

Not applicable.

11.8.3.1.4 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 10 "Choose a Certificate Type" on page 1423.
- 2 In order to proceed, the craftsperson must accept the disclaimer and the notice as indicated in:
 - Figure 11 "Disclaimer for Self-Signed Certificates (1 of 4)" on page 1424,
 - Figure 12 "Disclaimer for Self-Signed Certificates (2 of 4)" on page 1424,
 - Figure 13 "Disclaimer for Self-Signed Certificates (3 of 4)" on page 1425, and
 - Figure 14 "Disclaimer for Self-Signed Certificates (4 of 4)" on page 1426.

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 in Figure 12 "Disclaimer for Self-Signed Certificates (2 of 4)" on page 1424. 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 16 "Key Already Exists" on page 1428
 - If in Figure 16 "Key Already Exists" on page 1428, the craftsperson select 'n' that they do not want to proceed, then the tool prompts for key deletion in Figure 17 "Remove Existing Key" on page 1428.
 - If in Figure 16 "Key Already Exists" on page 1428, 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 17 “Remove Existing Key” on page 1428, 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 17 “Remove Existing Key” on page 1428, 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 18 “Expiry Days” on page 1429. 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 19 “Country Name” on page 1430, Figure 20 “State Name” on page 1431, Figure 21 “Locality Name” on page 1432. 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 22 “Organizational Name” on page 1433, and Figure 23 “Organizational Unit Name” on page 1434. These fields optional. Although they are optional, they help to identify the NGSS to a remote entity.
 - 8 In Figure 24 “Common Name” on page 1435, 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 25 “Email Address” on page 1436, the craftsperson identifies the optional e-mail 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 26 “Summary for Self Signed Certificates” on page 1437. 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
```


If this message is displayed, the tool was successful at creating the self-signed certificate.

Figure 10 Choose a Certificate Type

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
Stages      |
| X509 Certificate Setup
CertType    | -----
|
| Welcome to the X509 Certificate Setup tool.
|
| 1) Generate Self-Signed Certificate
|
| 2) Generate Certificate Signing Request
|
| 3) Validate Certificate Chain
|
|
| Option:
| [1]
| -----
| | Abort | | Next>>|
| -----
|
| This tool will help you to bring your SSL/TLS-based applicat
| into service
| Use the <TAB> key to move and select fields

```

Figure 11 Disclaimer for Self-Signed Certificates (1 of 4)

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved	
Stages	X509 Certificate Setup
CertType	
	PLEASE REVIEW THE FOLLOWING TERMS AND CONDITIONS REQUIRED FOR THE USE OF DIGITAL SELF-SIGNED CERTIFICATES. MOVE BETWEEN PAGES BY USING THE 'C' AND 'B' KEYS. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS BELOW, YOU ARE NOT AUTHORIZED TO USE A DIGITAL SELF-SIGNED CERTIFICATE. BY PRESSING 'Y' BELOW, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS BELOW Type (c) to continue

Figure 12 Disclaimer for Self-Signed Certificates (2 of 4)

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
Stages
-----
CertType
-----

LIMITATION OF LIABILITY: IN NO EVENT SHALL NORTEL OR
ANY OF ITS SUPPLIERS AND THEIR RESPECTIVE, EMPLOYEES,
OFFICERS, DIRECTORS AND AGENTS BE LIABLE FOR ANY
DIRECT, INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY,
RELIANCE, OR CONSEQUENTIAL DAMAGES OF ANY KIND,
INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF
BUSINESS OR BUSINESS OPPORTUNITIES, LOSS OF GOODWILL,
PROFITS OR DATA, BUSINESS INTERRUPTION, LOST SAVINGS
OR OTHER SIMILAR PECUNIARY LOSS, ARISING FROM OR IN
CONNECTION WITH THE USE, PERFORMANCE OR
NON-PERFORMANCE OF THE DIGITAL SELF-SIGNED
CERTIFICATE, WHETHER ARISING IN LAW OR EQUITY, ...

Type (c) to continue, or (b) to go back

```

Figure 14 Disclaimer for Self-Signed Certificates (4 of 4)

```
X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
Stages      |
            | X509 Certificate Setup
CertType    |-----
            |
            | (LIMITATION OF LIABILITY CON'T): ... ARISING FROM
            | CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT
            | (INCLUDING NEGLIGENCE) OR ANY OTHER THEORY OF
            | LIABILITY AND REGARDLESS OF WHETHER NORTEL OR ITS
            | SUPPLIERS WERE AWARE OF THE POSSIBILITY THEREOF.
            |
            | BY ENTERING 'Y', YOU AGREE TO BE BOUND BY THE TERMS
            | AND CONDITIONS JUST REVIEWED. IF YOU DO NOT AGREE TO
            | THE TERMS AND CONDITIONS JUST REVIEWED, ENTER 'N'
            | BELOW. IF YOU DO NOT ACCEPT THESE TERMS AND
            | CONDITIONS, YOU ARE NOT AUTHORIZED TO USE A DIGITAL
            | SELF-SIGNED CERTIFICATE.
            |
            | Please type yes (y) or no (n), or (b) to go back
```

Figure 15 Select Key Size

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
Pages |
CertType | Configure RSA modulus size
-----|-----
RSAModulus |
ExpiryDays | Please enter a RSA modulus size
CountryName | [1024]
State |
LocalityName |
OrgName |
OrgUnit |
CommonName |
EmailAddress |
Summary |

-----|-----
| <<Back | | Next>> |
-----|-----

| The RSA modulus size must be either 1024, 1536 or 2048 bits.
| Use '<' and '>' keys to move if left and right arrows don't wo

```

Figure 16 Key Already Exists

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
Stages      |
            | Configure RSA modulus size
-----
CertType    |
RSAModulus  |
ExpiryDays  |
CountryName |
State       | ----- Warning -----
LocalityName|
OrgName     | RSA Private key already exists.
OrgUnit     | Current Private key modulus is 1024.
CommonName  | The current RSA private key will be reused
EmailAddress| in the generation process
Summary     |
            | ----- Warning -----
            | Are you sure you want to reuse the current Private Key?
            |
            | Type yes (y) to reuse.
            | Type no (n) to generate a new RSA Private Key.
            |

```

Figure 17 Remove Existing Key

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
Stages      |
            | Configure RSA modulus size
-----
CertType    |
RSAModulus  |
ExpiryDays  |
CountryName |
State       | ----- Warning! -----
LocalityName|
OrgName     | RSA Private key is about to be deleted.
OrgUnit     |
CommonName  | ----- Warning! -----
EmailAddress|
Summary     | Are you sure you want to proceed?
            |
            | Please type yes (y) or no (n)
            |

```

Figure 18 Expiry Days

509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved

pages certType SAModulus serialNo countryName state localityName orgName orgUnit commonName mailAddress summary	Configure the certificate expiry days Please enter a expiry days value [7300] <<Back Next>> The value must be between 30 days and 7300 days. Use '<' and '>' keys to move if left and right arrows don't work

Figure 19 Country Name

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
ages          |
entType       | Configure the country name
SAModulus     |
expiryDays    |
countryName   | Please enter a country name (2 letter code) (optional)
state         | [US]
localityName  |
orgName       |
orgUnit       |
commonName    |
mailAddress   |
summary       |
              |
              | -----
              | | <<Back |
              | -----
              |
              | | Next>> |
              | -----
              | Use '<' and '>' keys to move if left and right arrows don't wo

```


Figure 20 State Name

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
ages
| Configure the state or province name
|-----
entType
SAModulus
xpiryDays
countryName
| Please enter a state/province name (optional)
|
| [State]
|
localityName
rgName
rgUnit
ommonName
mailAddress
ummary
|
|-----
| <<Back |
|-----
| Next>> |
|-----
| Use '<' and '>' keys to move if left and right arrows don't wo

```

Figure 21 Locality Name

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
ages          |
entType       | Configure the locality name
SAModulus     |
expiryDays    |
countryName   |
state         |
localityName   |
orgName       |
orgUnit       |
commonName    |
mailAddress   |
summary       |
              |
              | -----
              | | <<Back |
              | -----
              |
              | -----
              | | Next>> |
              | -----
              | Use '<' and '>' keys to move if left and right arrows don't wo

```

Figure 22 Organizational Name

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
ages          |
|             | Configure the organizational name
|             | -----
| certType    |
| SAModulus   |
| expiryDays  | Please enter a organizational name, e.g. company (optional)
| countryName |
| state       | [Organization Name]
| localityName|
| orgName     |
| orgUnit     |
| commonName  |
| mailAddress |
| summary     |
|             |
|             | -----
|             | | <<Back |
|             | -----
|             |
|             | | Next>> |
|             | -----
|             | Use '<' and '>' keys to move if left and right arrows don't wo

```

Figure 23 Organizational Unit Name

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
Pages |
CertType | Configure the organizational unit name (e.g. section)
-----
SAm modulus |
ExpiryDays | Please enter a organizational unit name (optional)
CountryName |
State | []
LocalityName |
OrgName |
OrgUnit |
CommonName |
EmailAddress |
Summary |

-----
| <<Back |
-----
| Next>>|
-----
Use '<' and '>' keys to move if left and right arrows don't work

```


Figure 25 Email Address

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
Pages |
entType |
SAModulus |
expiryDays |
countryName |
state |
localityName |
orgName |
orgUnit |
commonName |
mailAddress |
summary |
-----
Configure an email address
-----
Please enter an email address (optional)
[ ]

-----
| <<Back | | Next>> |
-----
Use '<' and '>' keys to move if left and right arrows don't wo

```

Figure 26 Summary for Self Signed Certificates

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserve
-----
Stages |
| Confirm the certificate information
-----
CertType |
RSAModulus |
ExpiryDays | Select 'Proceed' or 'Back' to make changes.
CountryName |
State | Modulus Size: 1024
LocalityName | Expiry Days: 7300
OrgName | Country Name: US
OrgUnit | State/Province: State
CommonName | Locality Name: City
EmailAddress | Org. Name: Organization Name
Summary | Org. Unit:
| Common Name: 10.66.18.72
| Email Address:
|
| -----
| | <<Back | | Proceed |
| -----
| This screen allows you to confirm that all of your
| settings are correct.

```

If the tool is successful in creating the self-signed certificate:

Server.crt will contain the local certificate

Server.key will contain the private key corresponding to the local certificate.

Trusted.crt will be an empty file if it did not already exist before the tool was run.

Certificate.keystore will contain the private key and local certificate.

Here is an example of the server. server.crt file respectively.

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: sha1WithRSAEncryption

Issuer: CN=10.66.18.72

Validity

Not Before: Nov 12 14:57:21 2004 GMT

(I)SN08 Release Change Reference Manual Standard 01.03 June 2005

kFrfmfKt/a4Z4HcjKrFiERAbA7DabZpw48aJDLsIaziwsyi/ie+v3olwk65hv/ZI
 gkg6dc4=
 -----END CERTIFICATE-----

11.8.3.1.5 Certificate Signing Request

- 1 In the case of a certificate signing request, the craftsperson selects option 2 in Figure 10 "Choose a Certificate Type" on page 1423.
- 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 12 "Disclaimer for Self-Signed Certificates (2 of 4)" on page 1424. 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 16 "Key Already Exists" on page 1428
 - If in Figure 16 "Key Already Exists" on page 1428, the craftsperson select 'n' that they do not want to proceed, then the tool prompts for key deletion in Figure 17 "Remove Existing Key" on page 1428.
 - If in Figure 16 "Key Already Exists" on page 1428, 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 17 "Remove Existing Key" on page 1428, 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.
- 4 The craftsperson selects a country, state, and city name in Figure 19 "Country Name" on page 1430, Figure 20 "State Name" on page 1431, Figure 21 "Locality Name" on page 1432. 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 22 "Organizational Name" on page 1433, and Figure 23 "Organizational Unit Name" on page 1434. These fields optional. Although they are optional, they help to identify the NGSS to a remote entity.

- 6 In Figure 24 "Common Name" on page 1435, 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 25 "Email Address" on page 1436, the craftsperson identifies the optional email address of the local contact. There is no validation of the email address.
- 8 In Figure 27 "Challenge Password" on page 1441, 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 28 "Certificate Signing Request Summary" on page 1441. Selecting "proceed" will generate the self signed certificate. The following message will be displayed on success.

Generating Certificate Signing Request

Creating Certificate Signing Request

Certificate Signing Request has been successfully generated

Changing permissions on key file

- 10 The certificate signing request 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 Validate the certificate chain in option 3 of the tool.

Figure 27 Challenge Password

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
Stages      |
            | Configure a challenge password
            |-----
CertType    |
RSA modulus  |
ExpiryDays  | Please enter a challenge password for this request
CountryName |
State       | [ ]
LocalityName|
OrgName      |
OrgUnit      |
CommonName   |
EmailAddress |
Passwd       |
Summary      |

            |-----
            | | <<Back |                               | Next>> |
            |-----
            | Use '<' and '>' keys to move if left and right arrows don't work

```

Figure 28 Certificate Signing Request Summary

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
Stages      |
            | Confirm the certificate request information
            |-----
CertType    |
RSA modulus  |
ExpiryDays  | Select 'Proceed' or 'Back' to make changes.
CountryName |
State       | Modulus Size: 2048
LocalityName| Expiry Days: 365
OrgName      | Country Name: US
OrgUnit      | State/Province: State
CommonName   | Locality Name: City
EmailAddress | Org. Name: Organization
Passwd       | Org. Unit:
Summary      | Common Name: 10.66.18.72
            | Email Address:
            | Passwd:
            |-----
            | | <<Back |                               | Proceed |
            |-----
            | This screen allows you to confirm that all of your
            | settings are correct.

```

11.8.3.1.6 Validate Certificate Chain

In this case, the craftsperson wishes to provision the CA-signed certificate from the signing request in option 2.

The same private key that was generated in option 2 must be the same private stored in /opt/base/share/ssl at this time. The tool will verify that the certificate provided as the user certificate matches the private key file server.key in /opt/base/share/ssl.

1 In Figure 30 "CA certificate - trusted certificate" on page 1448, the craftsperson supplies the full path and filename where the CA certificates can be found. The tool will not proceed unless the file exists. The root CA certificate and the chained certificate if applicable are added to this file. There are some guidelines as to the structure of this file.

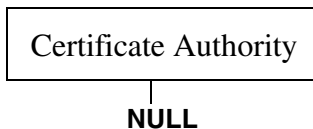
- Root CAs that do not correspond to the local server certificate are not placed in this file. They are added to the NGSS SIP application GUI under Add Trusted Certificates.
- Only the Root CA corresponding to the local certificate is placed in this file, followed by the CA chain. For example, if the local certificate is signed by one of the global public root CAs, then that root CA certificate is placed in this file.

Here is an example of the file which is provided. In this case, it is a chain composed of a root CA, followed by 3 (three) intermediate chain CA.

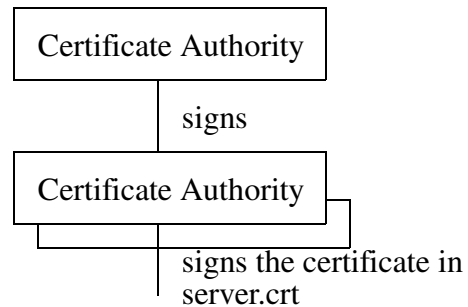
At the top of the file is certificate of the Certificate Authority (CA), followed by each intermediate chain CA, followed by that last CA which ultimately signed the local certificate.

Figure 29 Structure of trusted.crt file

Single Certificate Authority



Certificate Authority with intermediate CA (chain)



Certificate:
Data:

```

Version: 3 (0x2)
Serial Number: 0 (0x0)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=CA, ST=Ontario, L=Timbuktu, O=Nortel Networks, OU=Certificate Authority
Validity
    Not Before: Oct  8 01:14:48 2004 GMT
    Not After : Oct  8 01:14:48 2005 GMT
Subject: C=CA, ST=Ontario, L=Timbuktu, O=Nortel Networks, OU=Certificate Authority
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
        Modulus (1024 bit):
            00:bc:53:2a:bd:bf:36:87:36:5b:12:93:a7:55:84:
            1d:3b:75:0f:d9:de:d6:34:d3:51:8d:96:c6:41:c6:
            80:b3:08:18:e7:b1:e5:af:0a:00:1d:65:82:77:0a:
            ca:7d:74:00:79:85:d6:80:07:79:8d:ec:b0:e3:6e:
            8c:d0:a7:20:6f:c7:3b:df:09:83:93:36:9f:eb:67:
            c1:e2:ab:a5:ed:ab:3a:d8:97:ad:83:bf:8c:11:02:
            12:3b:dc:a9:82:0d:f3:45:d7:8a:ae:96:eb:17:26:
            3c:de:7a:cd:91:71:b9:56:c7:e7:0c:7a:5e:57:62:
            9c:d7:3e:41:82:c9:f3:34:1d
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Subject Key Identifier:
        90:20:BC:77:DD:64:50:D7:50:56:5D:C7:3F:EC:7A:32:21:0F:AE:F4
    X509v3 Authority Key Identifier:

keyid:90:20:BC:77:DD:64:50:D7:50:56:5D:C7:3F:EC:7A:32:21:0F:AE:F4
    DirName:/C=CA/ST=Ontario/L=Timbuktu/O=Nortel Networks/OU=Certificate Authority
    serial:00

X509v3 Basic Constraints:
    CA:TRUE
Signature Algorithm: md5WithRSAEncryption
33:65:6c:d0:0d:b8:7f:58:1c:33:1c:d2:4e:e3:19:2d:36:c3:
15:7f:b3:80:cb:22:2a:dc:eb:ba:84:50:24:7c:cc:07:49:62:
f5:2c:f9:bc:47:04:56:ea:bd:78:de:44:43:22:e2:1c:5f:fc:
17:91:80:70:f3:29:e2:74:46:8d:3d:ac:fa:63:f2:b4:ba:79:
d2:22:76:6c:2e:fb:e6:55:16:6f:db:27:5f:e3:ff:32:84:5a:
b7:a3:9c:c4:73:f9:72:c2:8b:6e:8d:4f:bf:d2:3f:b1:51:48:
b5:4e:27:b4:bb:80:4b:87:f9:e7:18:ba:63:20:ac:6d:25:c2:
74:1b

-----BEGIN CERTIFICATE-----
MIIDGDCCAoGgAwIBAgIBADANBgkqhkiG9w0BAQQFADBbMQswCQYDVQQGEwJDQTEQ
MA4GA1UECBMT250YXJpbzERMA8GA1UEBxMIVGltYnVrdHUXGDAWBgNVBAoTD05v
cnRlbCB0ZXR3b3JrczEeMBwGA1UECxMVQ2VydGhmaWNhdGUgQXV0aG9yaXR5MB4X
DTA0MTAwODAxMTQ0OFOxDTA1MTAwODAxMTQ0OFOwDELMAkGA1UEBhMCQ0ExEDAO

```

BgNVBAgTB09udGFyaW8xETAPBgNVBACTCFRpbWJ1a3R1MRgwFgYDVQQKEw9Ob3J0
 ZWwgTmV0d29ya3MxHjAcBgNVBASTFUNlcnRpZmljYXR1IEF1dGhvcml0eTCBnzAN
 BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAvmqvb82hzZbEpOnVYQd03UP2d7WNNNR
 jZbGQcaAswgY57HlrwoAHWWCdwrKfXQAEYXWgAd5jeyw426M0Kcgb8c73wmDkzaf
 62fB4qul7as62Jetg7+MEQISO9ypgg3zRdeKrpbrFyY83nrNkXG5VsfnDHpeV2Kc
 1z5BgsnzNB0CAwEAa0ByTCBxjAdBgNVHQ4EFgQUkCC8d91kUNdQV13HP+x6MiEP
 rvQwgZYGA1UdIwSBjjCBi4AUkCC8d91kUNdQV13HP+x6MiEPvShcKRuMGwxCzAJ
 BgNVBAYTAkNBMRAdGyYDVQZIEWdPbnRhcmlvMREwDwYDVQQHEWhUaW1idWt0dTEY
 MByGA1UEChMPTm9ydGVsIE5ldHdvcmZMR4wHAYDVQQLEExVDZlXJ0aWZpY2F0ZSBB
 dXR0b3JpdHmCAQAwDAYDVROTBABWAwEB/zANBgkqhkiG9w0BAQQFAAOBgQAZWzQ
 Dbh/WBwzHNJO4xktNsMVf7OAYyIq3Ou6hFAkfMwHswL1LPm8RwRW6r143kRDIuIc
 X/wXkYBw8ynidEaNPaz6Y/K0unnSInZsLvvmVRZv2ydf4/8yhFq3o5zEc/lywotu
 jU+/0j+xUUi1Tie0u4BLh/nngLpjIKxtJcJ0Gw==

-----END CERTIFICATE-----

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=CA, ST=Ontario, L=Timbuktu, O=Nortel Networks, OU=Certificate Authority

Validity

Not Before: Oct 8 01:19:20 2004 GMT

Not After : Oct 8 01:19:20 2005 GMT

Subject: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks, OU=Chain1, CN=Chain1

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:c5:d9:e9:4d:aa:87:56:ce:b0:ba:17:fb:fd:78:
 89:85:54:21:5b:2e:e8:71:e8:14:64:00:dd:b5:2e:
 0b:2a:e5:75:71:c2:42:17:29:e7:44:79:b0:2a:82:
 05:5b:92:c1:f3:5a:72:90:72:ee:ec:b1:77:39:cf:
 3c:c3:92:6a:6d:49:41:43:96:4c:e9:f6:3f:c3:3a:
 d9:79:11:ff:aa:74:ba:31:71:b3:0e:f0:f8:20:21:
 3c:76:5b:ad:6b:b6:27:2a:27:86:99:06:3a:1c:81:
 a5:ca:7c:68:36:cd:45:bd:2f:48:b0:5e:03:75:6e:
 35:95:42:60:3e:6e:f5:bc:35

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:TRUE

Signature Algorithm: sha1WithRSAEncryption

99:56:1b:2f:2f:b0:5f:4f:a5:7b:70:ce:6c:41:d3:36:20:2c:
 31:fb:61:df:81:58:81:4c:7f:30:a8:e1:d8:c7:97:0b:ad:19:
 21:19:79:ba:90:9f:3d:38:a0:66:6d:0a:6e:47:16:7f:4c:5b:
 7d:5b:bd:21:23:bc:15:27:e9:e5:f5:ec:6b:38:67:69:4e:86:
 82:a9:c0:f5:8a:c4:39:f7:98:89:ac:45:3f:a1:c9:47:26:9b:
 54:d2:d4:9d:d2:dd:c8:4f:58:cf:7c:57:d8:10:6d:d4:3e:3e:
 0a:12:1f:54:d7:f5:38:43:3d:f7:09:8e:33:b5:a1:80:00:14:

50:f0

-----BEGIN CERTIFICATE-----

MIICXjCCAcgAwIBAgIBATANBgkqhkiG9w0BAQUFADBQMswCQYDVQQGEwJDQTEQ
MA4GA1UECBMT250YXJpbzERMA8GA1UEBxMIVGltYnVrdHUxGDAWBgNVBAoTD05v
cnRlbCB0ZXR3b3JrczEeMBwGA1UECzMVQ2VydGhmaWNhdGUgQXV0aG9yaXR5MB4X
DTA0MTAwODAxMTkyMFoXDTA1MTAwODAxMTkyMFowbDELMAkGA1UEBhMCQ0ExEDAO
BgNVBAGTB09udGFyaW8xDzANBgNVBACTBk90dGF3YTEYMBYGA1UEChMPTm9ydGVs
IE5ldHdvcmtzMQ8wDQYDVQQLEwZDaGFpbjExDzANBgNVBAMTBkNoYWluMTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxdnpTaqHVs6wuhf7/XiJhVQhWy7ocegU
ZADdtS4LKuV1ccJCFynnRHmwKoIFW5LB81pykHLu7LF3Oc88w5JqbU1BQ5ZM6fY/
wzrZeRH/qnS6MXGzDvD4ICE8dluta7YnKieGmQY6HIGlynxoNs1FvS9IsF4DdW41
lUJgPm71vDUCAwEAAAMQMA4wDAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
gQCZVhsvL7BfT6V7cM5sQdM2ICwx+2HfgViBTH8wqOHYx5cLrRkhGXm6kJ89OKBm
bQpuRxZ/Tft9W70hI7wVJ+nl9exrOGdpToaCqcD1isQ595iJrEU/oclHJptU0tSd
0t3IT1jPffFYEG3UPj4KEh9U1/U4Qz33CY4ztaGAABRQ8A==

-----END CERTIFICATE-----

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 2 (0x2)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks, OU=Chain1,
CN=Chain1

Validity

Not Before: Oct 8 01:22:23 2004 GMT

Not After : Oct 8 01:22:23 2005 GMT

Subject: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks, OU=Chain2,
CN=Chain2

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:bf:8a:b7:44:9c:92:b5:fd:f0:e7:d3:1c:9d:65:
c4:e3:8c:cb:d3:60:a0:9d:bc:d7:87:15:d1:f0:68:
3c:71:be:2e:8d:2f:d0:7e:f6:95:2f:f3:89:b4:9b:
b6:c9:bd:52:62:8d:05:e3:71:3e:d5:c1:50:27:67:
01:f4:8b:7e:c9:6d:4e:a5:24:ff:d7:80:37:86:09:
8c:0a:8d:79:cc:b2:e6:9e:d8:7d:71:db:12:e6:84:
7e:2f:90:17:ca:84:87:9b:63:72:4a:28:d7:75:91:
f1:4f:c2:6b:5e:a7:d2:2b:01:60:f7:5f:35:dd:8e:
92:d7:b7:f5:a4:66:f6:af:21

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:TRUE

Signature Algorithm: sha1WithRSAEncryption

3c:0c:fa:58:1f:14:d3:3f:f1:cb:80:7b:8f:bb:f7:17:e5:18:
21:bd:a2:77:3e:ce:5d:4c:80:a8:3e:7e:a1:9c:fe:c8:6a:d0:
7d:67:45:b9:5a:a6:89:3a:2f:de:25:20:2f:ed:62:b5:06:8f:
dd:a1:85:aa:a2:a3:8d:a3:6d:4c:5e:ed:e8:35:f3:50:98:26:

99:38:1c:33:a3:99:0a:50:11:f8:0e:21:9d:fe:56:fb:ec:b9:
 55:ed:83:a7:b0:a4:26:82:7f:12:3b:35:9c:03:b9:40:02:3d:
 5c:d5:34:e2:ee:ff:91:58:9f:9d:cf:2e:91:35:9d:c8:5a:f1:
 19:59

-----BEGIN CERTIFICATE-----

MIICXjCCAcgAwIBAgIBAJANBgkqhkiG9w0BAQUFADBhMQswCQYDVQQGEwJDQTEQ
 MA4GA1UECBMT250YXJpbzEPMA0GA1UEBxMGT3R0YXdhMRgwFgYDVQQKEw9Ob3J0
 ZWwgTmV0d29ya3MxDzANBgNVBAsTBkNoYWluMTEPMA0GA1UEAxMQ2hhaW4xMB4X
 DTA0MTAwODAxMjIyM1oXDTA1MTAwODAxMjIyM1owbDELMAkGA1UEBhMCQ0ExEDAO
 BgNVBAGTB09udGFyaW8xZDZANBgNVBAcTBk90dGF3YTEYMBYGA1UEChMPTm9ydGVs
 IE5ldHdvcmtdzMQ8wDQYDVQQLLEwZDaGFpbiIxZDZANBgNVBAMTBkNoYWluMjCBnzAN
 BgkqhkiG9w0BAQEFAAOBjQAwYkCgYEA4q3RjYStf3w59McnWxE44zL02CgnbzX
 hxXR8Gg8cb4ujS/QfvaVL/OJtJu2yb1SYo0F43E+1cFQJ2cB9It+yW1OpST/14A3
 hgmMCo15zLLmth9cdsS5oR+L5AXyoSHm2NySijXdZHxT8JrXqfSKwFg91813Y6S
 17f1pGb2ryECAwEAAAMQMA4wDAYDVROTBAAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
 gQA8DPpYHxTTP/HLgHuPu/cX5RghvaJ3Ps5dTICoPn6hnp7IatB9Z0W5WqaJOi/e
 JSav7WK1Bo/doYWqoqONo21MXu3oNfnQmCaZOBwzo5kKUBH4DiGd/lb77L1V7YOn
 sKQmgn8SOzWca7lAAj1c1TTi7v+RWJ+dzy6RNZ3IWvEZWQ==

-----END CERTIFICATE-----

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 3 (0x3)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks, OU=Chain2,
 CN=Chain2

Validity

Not Before: Oct 8 01:24:40 2004 GMT

Not After : Oct 8 01:24:40 2005 GMT

Subject: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks, OU=Chain3,
 CN=Chain3

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:9e:10:4a:52:3a:e3:27:cc:0f:bb:70:a0:dc:66:
 df:27:47:17:54:4c:56:1e:f1:7c:6e:71:e6:b0:f1:
 7e:2d:a3:32:e0:c1:a4:50:5e:3a:cf:eb:09:ac:f5:
 00:f4:25:a5:ae:59:3d:b0:e5:02:af:ec:d8:b2:e5:
 c3:31:35:d0:d0:14:35:7d:c9:85:ef:fc:b3:c4:05:
 0b:06:b4:b9:67:53:4d:0b:e9:c8:f1:a0:44:ac:6f:
 27:4c:71:6f:be:31:63:12:21:4d:4b:a8:58:97:67:
 c0:e4:1f:bb:d2:fe:4d:d6:48:3c:19:c6:fb:db:2a:
 4e:1d:bf:f4:b4:41:23:69:c5

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:TRUE

Signature Algorithm: sha1WithRSAEncryption

bd:1b:08:a2:9f:af:f4:3e:3e:b6:72:e4:ca:ec:89:c5:fe:e4:


```

fd:99:b9:a4:31:b9:58:64:83:df:b5:8e:d3:97:89:c3:e8:0c:
96:0b:9d:c2:cc:81:b1:cd:78:17:13:ad:28:e8:ae:4d:2b:0e:
1b:b7:96:e2:74:65:23:02:5a:b1:e6:90:89:cf:9b:3c:c1:b5:
44:6f:ac:05:0d:d7:86:cc:eb:ce:ea:36:12:5a:3b:44:ac:f9:
0e:44:f5:c0:23:ff:55:1f:ef:1d:64:04:82:f2:7b:cc:22:25:
49:e4:a5:74:8c:9a:1d:22:5c:a7:7e:04:12:90:c9:88:d6:f4:
a2:b0
-----BEGIN CERTIFICATE-----
MIICXjCCAcegAwIBAgIBAzANBgkqhkiG9w0BAQUFADBQMqswCQYDVQQGEwJDQTEQ
MA4GA1UECBMHT250YXJpbzEPMA0GA1UEBxMGT3R0YXdhMRgwFgYDVQQKEw9Ob3J0
ZWwgTmV0d29ya3MxDzANBgNVBAsTBkNoYWluMjEPMA0GA1UEAxMGQ2hhaW4yMB4X
DTA0MTAwODAxMjQ0MFoXDTA1MTAwODAxMjQ0MFowbDELMAkGA1UEBhMCQ0ExEDAO
BgNVBAGTB09udGFyaW8xDzANBgNVBACTBk90dGF3YTEYMBYGA1UEChMPTm9ydGVs
IE5ldHdvcmtzMjQwDQYDVQQLLEwZDaGFpbjMxDzANBgNVBAMTBkNoYWluMzCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAAnhBKUjrjJ8wPu3Cg3GbfJ0cXVExWHvF8
bnHmsPF+LaMy4MGkUF46z+sJrPUA9CWlrlk9sOUCr+zYsuXDMTXQ0BQ1fcmF7/yz
xAULBrS5Z1NNC+nI8aBERG8nTHFvvjFjEiFNS6hYl2fA5B+70v5N1kg8Gcb72yp0
Hb/0tEEjacUCAwEAAMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
gQC9Gwiin6/0Pj62cutK7InF/ut9mbmkMblyZiPftY7Tl4nD6AyWC53CzIGxzXgX
E60o6K5NKw4bt5bidGUjAlqx5pCJz5s8wbVEb6wFDdeGzOvO6jYSWjtErPkORPXA
I/9VH+8dZASC8nvMIiVJ5KV0jJodIlynfgQSkMmI1vSisA==
-----END CERTIFICATE-----

```

It is recommended that this file be placed in a temporary directory such as /tmp/. When the tool validates the file, it will copy the file to /opt/base/share/ssl/trusted.crt. The file in /tmp can then be deleted once the tool completes successfully.

- 2 In Figure 31 "Server Certificate - CA signed certificate" on page 1449, the craftsperson supplies the full path and filename where the signed certificate can be found. The tool will not proceed unless the file exists. Only the local server/user certificate is placed in this file.

It is recommended that this file be placed in a temporary directory such as /tmp/. When the tool validates the file, it will copy the file to /opt/base/share/ssl/server.crt. The file in /tmp can then be deleted once the tool completes successfully.

- 3 In Figure 32 "Validation Summary" on page 1450, once the craftsperson has provisioned both files, then the tool validates the certificates chain and the trusted certificate files. Upon success, the tool will display the following lines:

```

Provisioning CA Certificate
Verifying certificate/key pair
server.crt: OK

```


Figure 31 Server Certificate - CA signed certificate

```
X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-----
Stages      |
CertType   | Configure the CA-signed certificate filename
CAFile     | -----
CAFile     |
CAFile     | Please enter the user certificate filename
CAFile     |
CAFile     | [/home/root/server.crt]
Summary    |
           |
           | -----
           | | <<Back |
           | -----
           |
           | -----
           | | Next>>| |
           | -----
           |
           | Use '<' and '>' keys to move if left and right arrows don't work
```

Figure 32 Validation Summary



11.8.3.1.7 New Installation

On a new installation, if there are no previous certificate files, then the craftsperson can initiate cert_mgnt without issues of retaining old keys or certificates. The key file, certificate files (server.crt for the certificate file, and trusted.crt for the CA certificate), and certificate.keystore are created by default in the /opt/base/share/ssl directory and it is recommended to leave the files in that location.

The cert_mgnt is run only on 1 unit of the NGSS, not on both. The files in /opt/base/share/ssl will have to be manually copied to the other NGSS host.

Cert_mgnt tool is executed after the base NCGL installation and before the NGSS InstallApps script. Although technically, the cert_mgnt tool can be run anytime, one of two actions must take place before any changes can take effect: 1) reboot machine, or 2) restart the Apache, Tomcat, and NGSS SIP application.

The craftsperson must also add the new certificate to the list of Remote Trusted Certificates on remote NGSS units.

11.8.3.1.8 Upgrade using existing certificate and key files

On an OS/application upgrade that will be using existing, the contents of /opt/base/share/ssl will have to be backed up to a safe storage (regular backups of this directory is recommended). Once the base OS upgrade is complete, then the contents of /opt/base/share/ssl are restored to the same directory. The NGSS application upgrade can then be executed. This will have to be done on both units.

When the 07 to 08 NCGL upgrade is complete, the use of certificates depends on whether the user wants to use certificates from 07.

In the case of re-using self-signed certificates, the files server.key, server.crt and certificate.keystore must be present in the /opt/base/share/ssl directory. The applications Apache, Tomcat, and Sipgwyappln should be either stopped/started, or the unit rebooted.

In the case of re-using CA signed certificates, run cert_mgnt to re-import the server.crt and trusted.crt and to create the certificate.keystore file. This is necessary if trusted.crt, server.crt, server.key, and certificate.keystore do not already exist.

If the user wants to use new certificates after upgrading to 08, the user can run cert_mgnt.

11.8.3.1.9 Existing installation with new certificates or keys

If the existing certificate has expired or the craftsperson wishes to use a new key, the cert_mgnt tool will have to be executed again. The resulting files will need to be copied to the other NGSS host.

A reboot will be required for the changes to take effect.

If a remote server has a new key and or certificate, it is important for the craftsperson to remove the old certificate from the list of Remote Trusted Certificates on remote NGSS units. See section 11.8.2 "GUI information" on page 1404.

The craftsperson must also add the new certificate to the list of Remote Trusted Certificates on remote NGSS units.

11.8.3.1.10 Expired Certificates or Certificate Revocation

There is no support for Certificate Revocation Lists in SN08. This is handled in the same manner as section 11.8.3.1.9 "Existing installation with new certificates or keys" on page 1451.

11.8.3.1.11 Copying certificate and key files to NGSS mate host

The cert_mgnt tool is executed only on 1 host of the NGSS, not both. The contents of /opt/base/share/ssl must be manually copied to the other NGSS

host. Please note that the key files and certificate files should be protected with proper root permissions only (this is done by the tool), and copied over using a secure copy protocol such as 'scp'.

11.8.3.1.12 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.

11.9 OSSGate Interface Changes

Not applicable.

11.10 Security

The primary intent of this feature is to provide security on the signalling paths between the NGSS and its peer servers.

11.10.1 Network configuration

Network configurations should not be changed as a result of this feature.

11.10.2 Key management

Key management will be done automatically as part of certificate management procedures. Keys will thus be managed internally by the NGSS web server and/or CLI tools. No customer interface dealing with keys will be implemented.

11.10.3 Protocol

This activity is not making changes to protocols that are used to manage security.

This activity *is* introducing the use of the TLS protocol for inter-nodal CallP signalling communications between the NGSS and its peer servers and IP phone clients.

11.10.4 Authentication

This activity eliminates the need for different certificates for the Apache and Tomcat webservers. The only change that is obvious for the user is that, when using self-signed or unsigned certificates, the user will have to approve the use of only one certificate instead of two as is currently done.

11.11 Configuration Walkthrough

See 11.8 "Element Management" on page 1404.

12: A00006894 Configuration (CN)

12.1 Feature name

InterNodal Emergency Stand Alone (ESA) for MG9K

12.2 Hardware and Software Requirements

This feature applies to all supported hardware platforms, per the SN08 Succession server platform foundation software specification. No new hardware is required. A MG9K node in a community must have access to a LAN Switch (i.e. Passport 15000 or equivalent) in order for InterNodal ESA calls to complete.

12.3 Initial Configuration

The inter-MG9000 communication will be provided by the Passport 15000 switch, using the Virtual Router capability to route the IP-based ESA traffic between MG9K gateways.

To deploy this feature in the field, the existing Passport 15000 switches must be configured to support it. This section covers the following:

- Details of the Passport 15000 software component provisioning.
- Engineering required to configure the Passports in the field.
- List of possible deployment scenarios.

12.4 Upgrade Considerations

For the InterNodal ESA feature using a Passport virtual router (PVR), it is expected that the Passport 15000 can be field upgraded to support inter-MG9000 communications.

For a MG9000 connected to Passport 16pOC3 FP cards without IP already enabled for in-band OAM, it can be a service impacting action to enable the PVR on the PP15K.

- Turning on IP reduces the card's ATM connection capacity such that only 14 ports can be supported. Fully populated cards would have to have some MG9000s migrated to other cards.

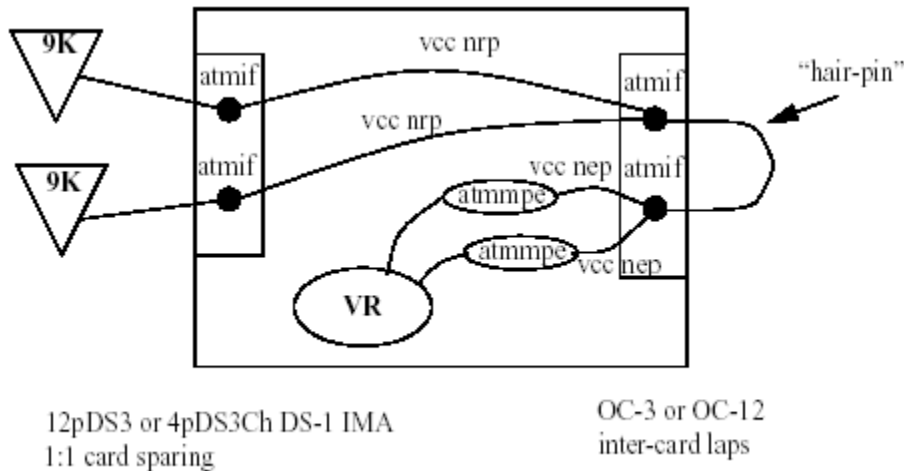
- atmif ca attributes on all ports on the FP need to be re-engineered from 3300 to 2100.
- Both of these changes (turning on IP and atmif ca) are “critical” changes - the former currently causes a dual-FP reboot.

Since an outage can not be allowed during an upgrade of existing field installations, the chosen solution is to put a hairpin on the shelf on a card that already supports IP, or can be IP enabled without service interruption (new hardware).

The MG9000 can have either a DS-1 IMA or an STS-1 interface which terminates on the Passport as a DS-3.

As IP is not supported on the 4pDS3ChIMA card, and carrier grade IP is not supported on the 12pDS3ATM FP card, these cards can only terminate the ATM layer, and an optical “hair-pin” must be used for IP forwarding.

Figure 1 Electrical interface hair-pin IP connectivity



This optical hair-pin can be deployed on a pair of cards deployed expressly for this purpose, or it can be deployed on spare ports of an optical pair with spare capacity. For instance, a pair of PQC12 4pOC12 FP cards with only two OC12 trunks will have enough spare ATM connection space and IP routing capacity to support over 100 MG9000 gateways for ESA traffic.

- A spare pair of ports on a card with available space can be used to deploy an IP hairpin that can do IP services.
- A new pair of cards (example: 4pOC3 FP) can be provisioned with an IP hairpin.

- **default:** the attribute value is customer defined and/or must be engineered depending on the switch or network configuration.
- **link:** an attribute that is a link to another component.

12.6.1 CP and Shelf Commissioning

The following components are to be created or changed when a Passport 15000 shelf is first being commissioned for InterNode ESA.

12.6.1.1 Software and Features

The following software packages and lpt for the CP are required. They are not configured by an NP template but as part of the Passport 15000 base IM24-9095.

Table 1 Software Component Provisionable Attributes

Attribute	Type	Value
Software		
avList	default	ip_CF01XXX, wanDte_CF01XXX <i>add if not already there</i>
Sw Lpt/CP		
featureList	set	ip, mvr <i>add if not already there</i>
Sw Lpt/ATM<n>		
featureList	set	ip, atmmpe <i>add if not already there</i>

12.6.1.2 Virtual Router

Table 2 Virtual Router component provisioning attributes

Attribute	Type	Value
VirtualRouter/ESA		
vpnMode	set	customer
vrp	set	lp/0
VirtualRouter/ESA Ip		
preConfigFwdPath	set	enabled
VirtualRouter/ESA Ip Static^a		
maxEcmpNextHops	set	1

Attribute	Type	Value
VirtualRouter/ESA Ip Static Route/<sub-net>^b nextHop/<next-hop-address>		
metric	set	1
VirtualRouter/ESA Ip Static DiscardRouteEntry/0.0.0.0,0.0.0.0,0		
discardRouteEntry	add	0.0.0.0,0.0.0.0

a. required to route traffic between Passport 15000 in the case where InterNode ESA groups span more than one Passport 15000.

b. <sub-net> is a triplet of the form <address>,<mask>,0

12.6.2 FP Cards

To carry the InterNodal ESA IP traffic, the FP cards that are directly connected to the MG9000 or supporting the hairpin connection for MG9000 connected to FP cards that cannot support IP traffic, the following FP level configuration changes must be made.

12.6.2.1 4pOC3SmIrATM

Table 3 4pOC3SmIrAtm Component Provisionable Attributes

Attribute Name	Type	Value
Lp Eng Ferc Pqc Ov		
ipRoutes	Set	4096

12.6.2.2 16pOC3SmIrAtm

Table 4 16pOC3SmIrAtm Component Provisionable Attributes

Attribute Name	Type	Value
Lp Eng Arc Ov		
connectionPoolCapacity	Default	<num>
protectedConnectionPoolCapacity	Default	29440 - <num>
Lp Eng Ferc Pqc Ov		
ipRoutes	Set	4096

12.6.2.3 4pOC12SmIrATM

Table 5 4pOC12SmIrAtm (NTHW86 only) Component Provisionable Attributes

Attribute Name	Type	Value
Lp Eng Ferc Pqc Ov		
ipRoutes	Set	4096

12.6.2.4 4pDS3ChAtm

No change to the FP configuration to add InterNodal ESA.

12.6.2.5 12pDS3Atm

No change to the FP configuration to add InterNodal ESA.

12.6.3 Interfaces

12.6.3.1 MG9000 OC-3 interface

The following component needs to be provisioned to support a InterNodal ESA IP MG9000 on a 1+1 OC-3 interfaces. Note that since MG9000 does not support ARP, there must be a static ARP entry provisioned into the Passport for each IP “host” on the MG9000.

Table 6 MG9000 OC-3 interface component configuration

Attribute Name	Type	Value
AtmIf Vcc/16.32 Nep		
applicationName	Set	AtmMpe/<n> Ac/1
AtmIf Vcc/16.32 vcd Tm		
atmServiceCategory	Set	rtVbr
txPacketWiseDiscard	Set	enabled
txTrafficDescriptorType	Set	6
txTrafficDescriptorParameters	Default	1 12000 2 6000 3 32
AtmMpe/<n>		
linkToProtocolPort	Link	Vr/ESA Pp/9K<n>_ESA
AtmMpe/<n> Ac/1		
atmConnection	Link	AtmIf/<n> Vcc/<vpi.vci> nep
Vr/ESA Pp/9K<n>_ESA		

Attribute Name	Type	Value
linkToMedia	Link	AtmMpe/<n>
Vr/ESA Pp/9K<n>_ESA ipport LogicalInterface/<ESA_IPaddr>		
netMask	Set	255.255.255.224
Vr/ESA Ip Arp Host/<ESA_IPaddr+m>,0^a		
pvc	Set	1

a. ARP entries must be provisioned for the 16 MG9000 ITP IP addresses

12.6.3.2 MG9000 DS-1 IMA interface

The following component needs to be provisioned to support MG9000 InterNodal ESA on a DS-1 IMA interface. This consists of a Vcc Network Relay Point (NRP) to a Hairpin ATM Interface.

Table 7 MG9000 DS-1 IMA interface Component Provisionable Attributes

Attribute Name	Type	Value
AtmIf Vcc/16.32 Nrp		
nextHop	Default	AtmIf/<HAI> Vcc/<vpi.vci> Nrp
AtmIf Vcc/16.32 Nrp Vcd Tm		
atmServiceCategory	Set	rtVbr
txPacketWiseDiscard	Set	enabled
txTrafficDescriptorType	Set	6
txTrafficDescriptorParameters	Default	1 950 2 380 3 32

12.6.3.3 MG9000 STS-1/DS3 interface

The following component needs to be provisioned to support MG9000 InterNodal ESA on a DS-3 interface This consists of a Vcc Network Relay Point (NRP) to a Hairpin ATM Interface.

Table 8 MG9000 STS-1/DS-3 interface Component Provisionable Attributes

Attribute Name	Type	Value
AtmIf Vcc/16/32 Nrp		
nextHop	Default	AtmIf/<HAI> Vcc/<vpi.vci> Nrp
AtmIf Vcc/16.32 Nrp Vcd Tm		
atmServiceCategory	Set	rtVbr

Table 8 MG9000 STS-1/DS-3 interface Component Provisionable Attributes

Attribute Name	Type	Value
txPacketWiseDiscard	Set	enabled
txTrafficDescriptorType	Set	6
txTrafficDescriptorParameters	Default	1 ?? 2 ?? 3 32

12.6.3.4 Hairpin ATM interface

Table 11, “Optical HII interface component configuration” documents all the components and attributes to be provisioned for the optical Hairpin ATM Interface (HAI) from scratch. Table 12, “MG9000 Vcc and Vr HII component configuration” covers the Vcc Nrp components required to support one MG9000. As a single hairpin interface can support many MG9000s, those components will typically be applied several times.

Table 9 Optical HAI interface component configuration

Attribute Name	Type	Value
Lp Sonet		
clockingSource	Set	module
vendor	Default	
commentText	Default	
Laps		
workingLine	Link	Lp/n Sonet/m
protectionLine	Link	Lp/n+1 Sonet/m
signalDegradeRatio	Default	-8
Laps Sts (OC-12 only)		
concatNumber	Set	12
Laps Sts AtmCell		
correctSingleBitHeaderErrors	Set	On
AtmIf		
interfaceName	Link	Laps/<n*100+m> Sts/0
remoteAtmInterfaceLabel	Default	EM/<remoteNodeName> ATMIF/<remote AtmIf instance>
oamSegmentBoundary	Set	No

Attribute Name	Type	Value
AtmIf ConnMap Ov (4pOC-12 only)		
numVccsForVpiZero	Set	16384
AtmIf Ca^a		
maxVccs	Set	3250/13000
maxAutoSelectedVciForVpiZero	Set	4095/16383
minAutoSelectedVciForVpiZero	Set	2048
maxVpcs	Set	0
maxVpts	Set	0
bandwidthPool	Set	1 100 2 0 3 0
AtmIf Ca rtVbr		
cdvt	Set	5000
usageParameterControl	Set	Disabled
AtmIf Ca nrtVbr		
cdvt	Set	5000
usageParameterControl	Set	Disabled

a. values are given for both OC-3 / OC-12

Table 10 MG9000 Vcc Nrp HAI component configuration.

Attribute Name	Type	Value
AtmIf Vcc/0.<vci> Nrp		
nextHop	Default	AtmIf/<MG> Vcc/16.32 Nrp
AtmIf Vcc/0.<vci> Nrp Vcd Tm		
atmServiceCategory	Set	rtVbr
txPacketWiseDiscard	Set	enabled
txTrafficDescriptorType	Set	6
txTrafficDescriptorParameters	Default	^a

a. values depend on whether the MG9000 is IMA or DS3

12.6.3.5 Hairpin IP interface

Table 11, “Optical HII interface component configuration” documents all the components and attributes to be provisioned for the optical Hairpin IP Interface (HII) from scratch. Table 12, “MG9000 Vcc and Vr HII component configuration” covers the Vcc, AtmMpe and Vr components required to support one MG9000. As a single hairpin can support many MG9000,s those components will typically be applied several times.

Table 11 Optical HII interface component configuration

Attribute Name	Type	Value
Lp Sonet		
clockingSource	Set	module
vendor	Default	
commentText	Default	
Laps		
workingLine	Link	Lp/n Sonet/m
protectionLine	Link	Lp/n+1 Sonet/m
signalDegradeRatio	Default	-8
Laps Sts (OC-12 only)		
concatNumber	Set	12
Laps Sts AtmCell		
correctSingleBitHeaderErrors	Set	On
AtmIf		
interfaceName	Link	Laps/<n*100+m> Sts/0
remoteAtmInterfaceLabel	Default	EM/<remoteNodeName> ATMIF/<remote AtmIf instance>
oamSegmentBoundary	Set	No
AtmIf ConnMap Ov (4pOC-12 only)		
numVccsForVpiZero	Set	16384
AtmIf Ca^a		
maxVccs	Set	3250/13000
maxAutoSelectedVciForVpiZero	Set	4095/16383

Attribute Name	Type	Value
minAutoSelectedVciForVpiZero	Set	2048
maxVpcs	Set	0
maxVpts	Set	0
bandwidthPool	Set	1 100 2 0 3 0
AtmIf Ca rtVbr		
cdvt	Set	5000
usageParameterControl	Set	Disabled
AtmIf Ca nrtVbr		
cdvt	Set	5000
usageParameterControl	Set	Disabled

a. values are given for both OC-3 / OC-12

Table 12 MG9000 Vcc and Vr HII component configuration

Attribute Name	Type	Value
AtmIf Vcc/0.<vci> Nep		
applicationName	Set	AtmMpe/<n> Ac/1
AtmIf Vcc/0.<vci> vcd Tm		
atmServiceCategory	Set	rtVbr
txPacketWiseDiscard	Set	enabled
txTrafficDescriptorType	Set	6
txTrafficDescriptorParameters	Default	^a
AtmMpe/<n>		
linkToProtocolPort	Link	Vr/ESA Pp/9K<n>_ESA
AtmMpe/<n> Ac/1		
atmConnection	Link	AtmIf/<n> Vcc/<vpi.vci> nep
Vr/ESA Pp/9K<n>_ESA		
linkToMedia	Link	AtmMpe/<n>
Vr/ESA Pp/9K<n>_ESA ippport LogicalInterface/<ESA_IPaddr>		

Attribute Name	Type	Value
netMask	Set	255.255.255.224
Vr/ESA Ip Arp Host/<ESA_IPAddr+m>,0^b		
AtmMpe/<n>		

a. values depend on whether the MG9000 is IMA or DS3

b. ARP entries must be provisioned for the 16 MG9000 ITP IP addresses

12.6.3.6 Passport to Passport interface

If an InterNodal ESA group spans more than one Passport 15000, then there needs to be at least one IP path among all the Passports over PNNI links.

Table 13 Passport to Passport interface component configuration

Attribute Name	Type	Value
AtmIf Vcc/0.33 Nep		
applicationName	Set	AtmMpe/<n> Ac/1
AtmIf Vcc/0.33 vcd Tm		
atmServiceCategory	Set	rtVbr
txTrafficDescriptorType	Set	6
txPacketWiseDiscard	Set	enabled
txTrafficDescriptorParameters	Default	1 12000 2 6000 3 32
AtmMpe/<n>		
linkToProtocolPort	Link	Vr/ESA Pp/<AtmIf>_ESA
AtmMpe/<n> Ac/1		
atmConnection	Link	AtmIf/<n> Vcc/0.33 nep
Vr/ESA Pp/PP<n>_ESA		
linkToMedia	Link	AtmMpe/<n>
Vr/ESA Pp/PP<n>_ESA ipport LogicalInterface/<PP_IPAddr>		
netMask	Default	255.255.255.252

13: A00006901 Configuration (CN)

13.1 Document Name

MissingPatches_CN.fm

13.2 Hardware and Software Requirements

This feature requires an SN08 Network Patch Manager (NPM) and the SN08 SSPFS platform.

13.3 Network Patch Manager Server

13.3.1 Initial Configuration

13.3.1.1 Upgrade

One of the functions of this feature is to save System and User defined information in the NPM database from one release to the next starting with SN08.

Therefore, the procedure for upgrades from an SN08 NPM and beyond retains the *user* and *system* defined information for tasks, set, alarms, reports and plans over an upgrade. If the user is upgrading from a pre-SN08 to SN08 the information in the database is un-initialized as it has always been.

If the user is going from SN07 to SN08 or above, the NPM now retains system and user defined data for tasks, sets, and plans.

If the user wishes to initialize the NPM database after the SN08 (and beyond) package has been installed; the user must exit the CLI tool after the NPM configuration and re-enter the CLI tool. The user must make their way back into the NPM configuration, only this time the user will choose “CreateDB”. Once this has finished executing, the NPM database will be initialized and all user defined data will be erased.

13.3.1.2 PFRS

In SN07 the configuration of PFRS was moved to the CLI tool. Although, the tool offered the user the ability to set up, and execute a PFRS GENREPORT and a PFRS GETPATCH either on demand or through a scheduler, the user needed to have root access to the SSPFS platform to utilize these commands.

This feature moves this information from the CLI tool into the NPM GUI and CLUI. Access for this functionality is the same as it is for all the other NPM maintenance commands; EMSADM.

The user may now set up the PFRS drop box information via a preferences window in the NPM GUI and via a preferences command in the NPM CLUI.

The user may also execute a PFRS GENREPORT and a PFRS GETPATCH on demand through the NPM by executing either one of two NPM system pre-defined tasks; PFRSGENREPORT and PFRSGETPATCH.

Both of these tasks are available in the Maintenance GUI panel or can be executed as part of the existing runtask command in NPM CLUI.

This feature also provides new functionality for the PFRS user. The user can now decide if they would like the NPM to “clean up” or delete patches from the drop box that have been transferred to the NPM after the PFRSGETPATCH task has been executed.

13.3.1.2.1 PFRS Scheduling

These two tasks can also be scheduled through the NPM Scheduler either via a user defined plan or via the provided NPM system plans; GETPATCH and GETREPORT. Although neither of the plans are defaulted to enabled; the default execution time for GETREPORT is at 9:00 am and the default execution time for GETPATCH is 11:00 pm.

It is recommended that the GETREPORT plan be scheduled to execute before the GETPATCH plan. Both plans should be executed before the NPM System plan.

13.3.1.3 Delete Reports

Delete Reports is a new NPM system defined task. This task is used to delete reports that have been created and left in the /data/npm/reports directory. Reports that are left in this directory are created when a user schedules reports to execute through the NPM Scheduler.

13.3.1.4 Automatic audit of MG9K and GWC devices after reload

This feature changes the 20 minute audit after an MG9K or GWC device reload to be immediately. This will provide immediate information back to the user/customer about the device load and if patches need to be re-applied.

13.4 Network Element Patch Manager GUI/CLUI

13.4.1 New/modified GUIs

The NPM GUI has been modified to include a new “View” button on specific NPM GUI panels and a new PatchFile Retrieval Preferences tab as part of the Preferences GUI. The following table will identify the names of each panel that has been modified as a result of this feature because of these specific items and others that will be described later in this document.

Table 1 New or modified GUIs

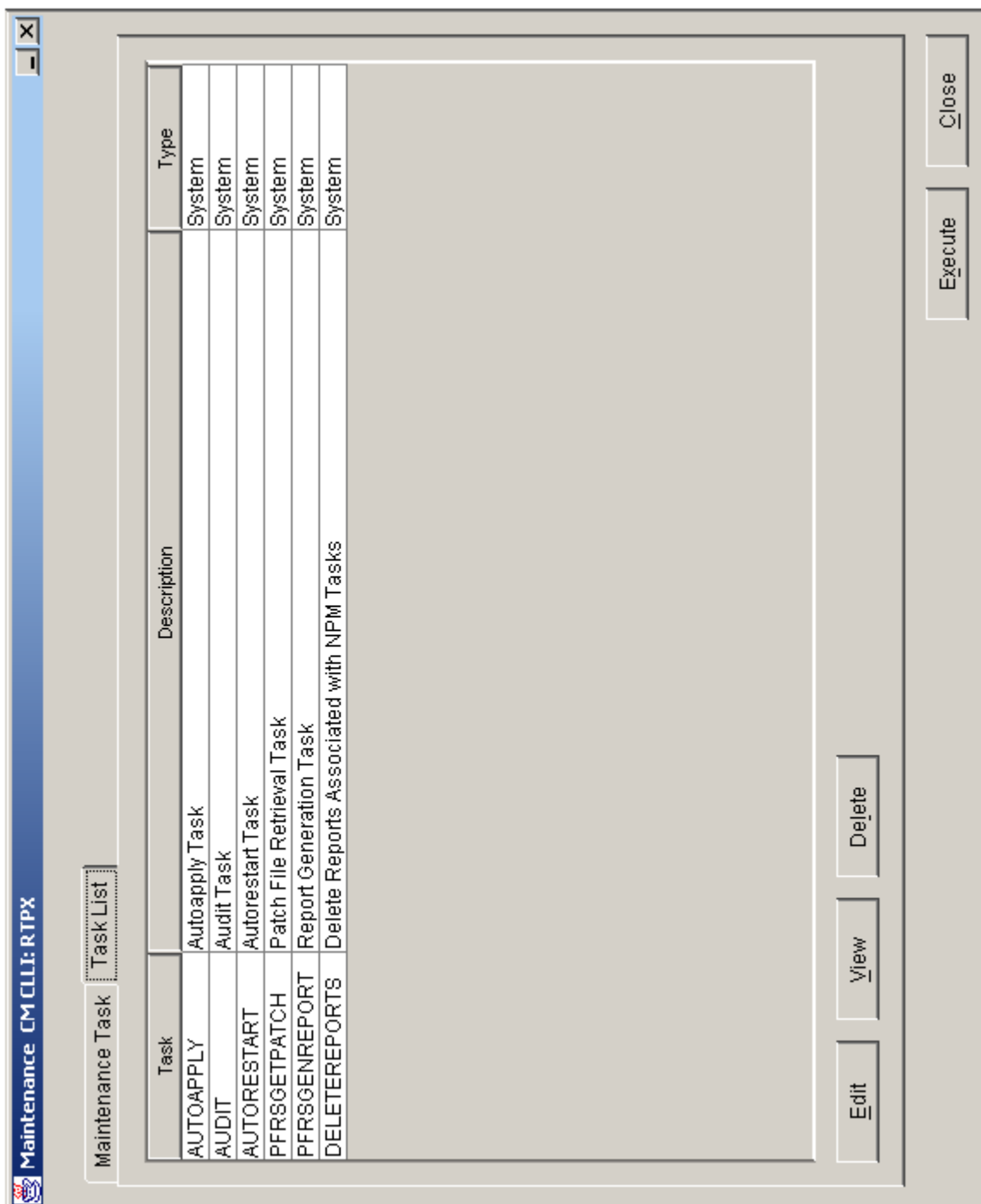
GUI name	NEW, CHANGED, or DELETED
Maintenance - Task List	CHANGED
Maintenance - Maintenance Task	CHANGED
Reports - Report List	CHANGED
Alarms - Alarm List	CHANGED
Plans - Plan List	CHANGED
Preferences - PatchFile Retrieval Preferences	NEW

13.4.2 GUI information

In addition to the GUI/CLUI items that have been added as a result of the NPM Server, this feature provides the following new features specific to the NPM GUI:

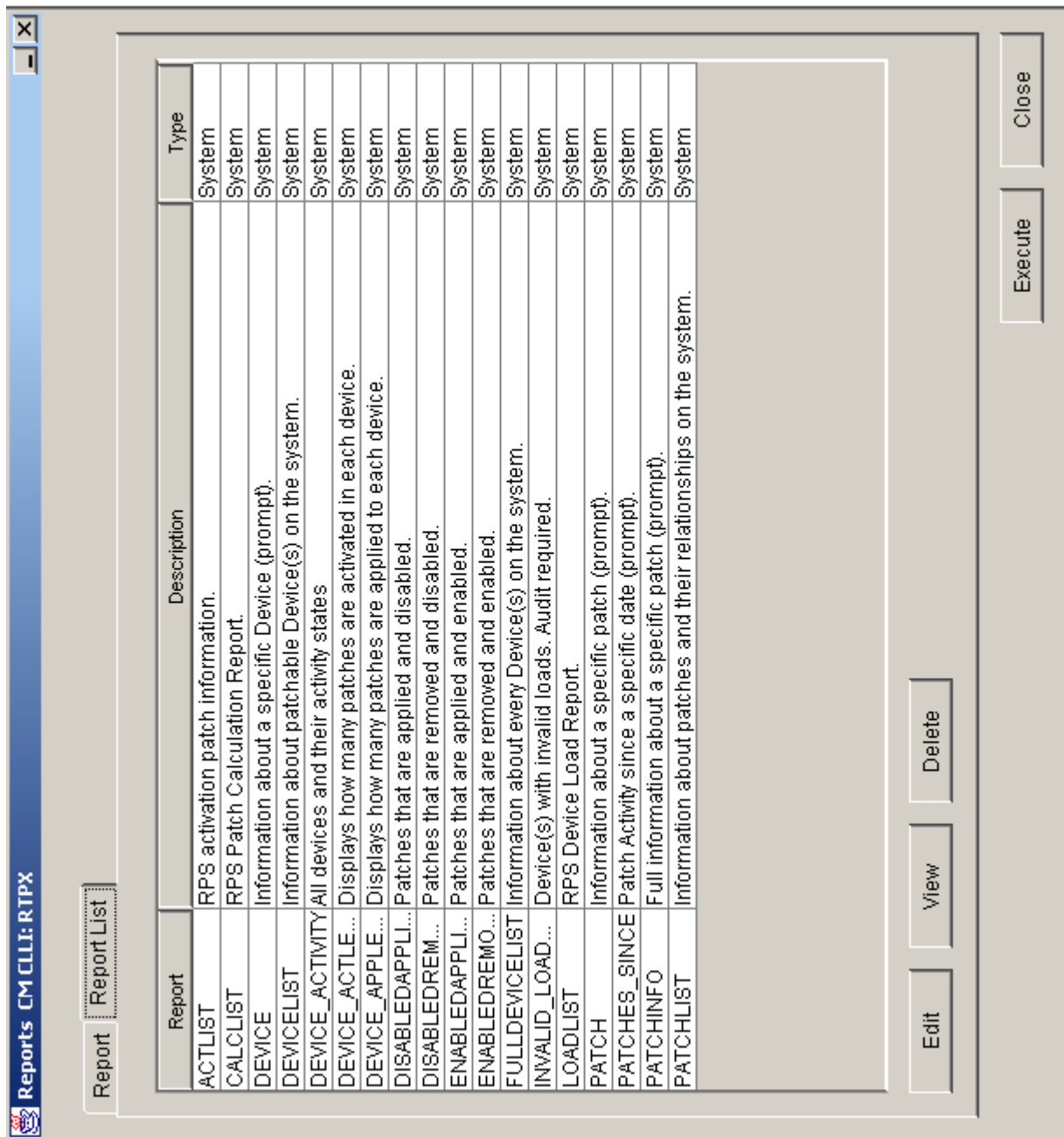
- System defined information in the NPM GUI can now only be viewed and cannot be edited.
- a new refine or filter button will be available which will allow the user to quickly determine which patch(es) are applicable to which device(s) and vice versa.
- a process monitor has been added which will provide a visual indicator to the user that a submitted request is in progress. This monitor will be specific to each instance of the NPM GUI and will not indicate activity of multiple GUIs.
- the CM CLI will appear on each NPM GUI window. This will provide clarification when the user is performing patching operations on multiple offices.

Figure 1 GUI name: Maintenance - Task List



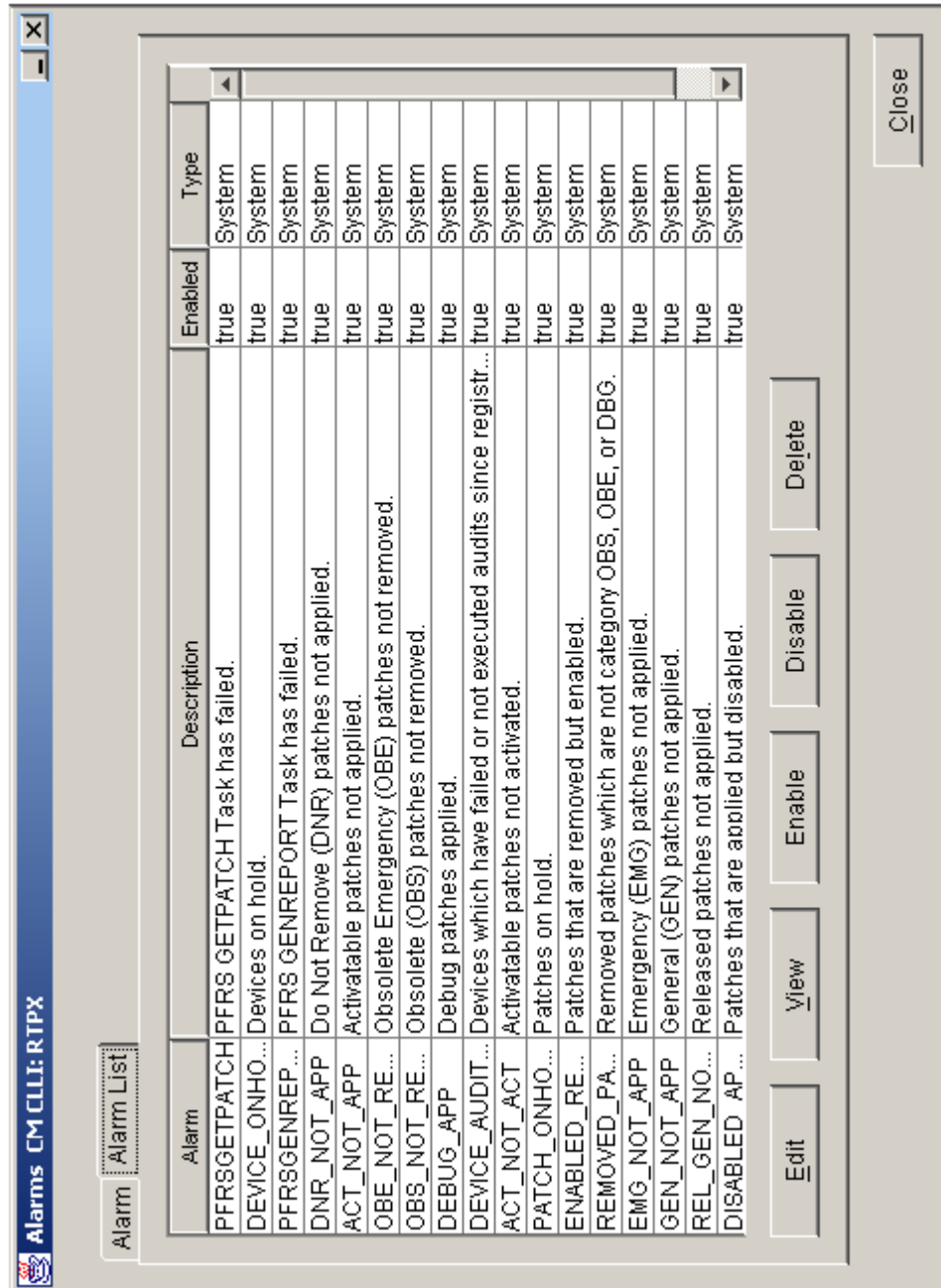
Notice the three new system defined tasks and the new “View” button on the bottom of the panel. System defined tasks can only be viewed.

Figure 2 GUI name: Reports - Reports List



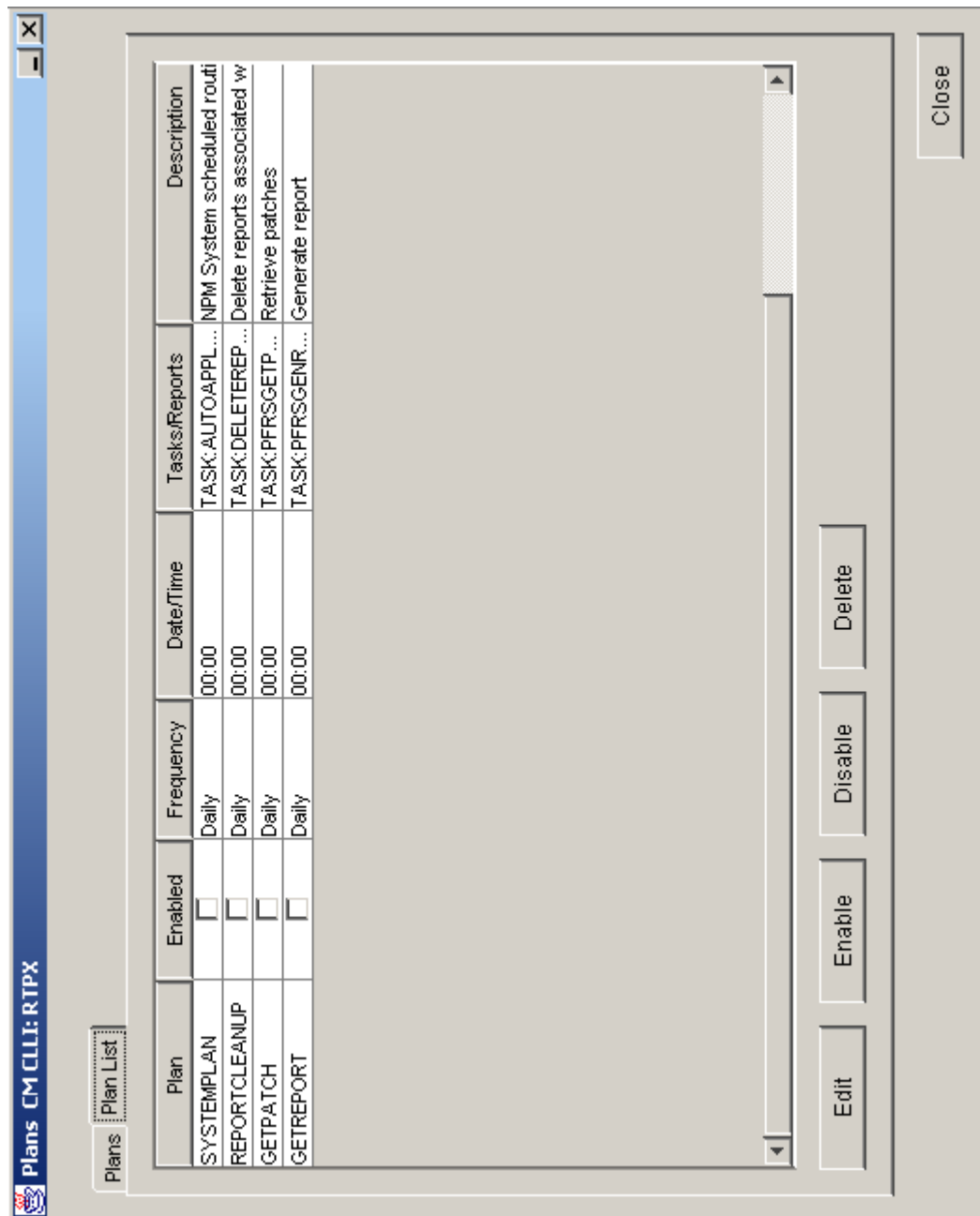
Notice the new “View” button on the bottom of the panel. System defined reports can only be viewed.

Figure 3 GUI name: Alarm - Alarm List

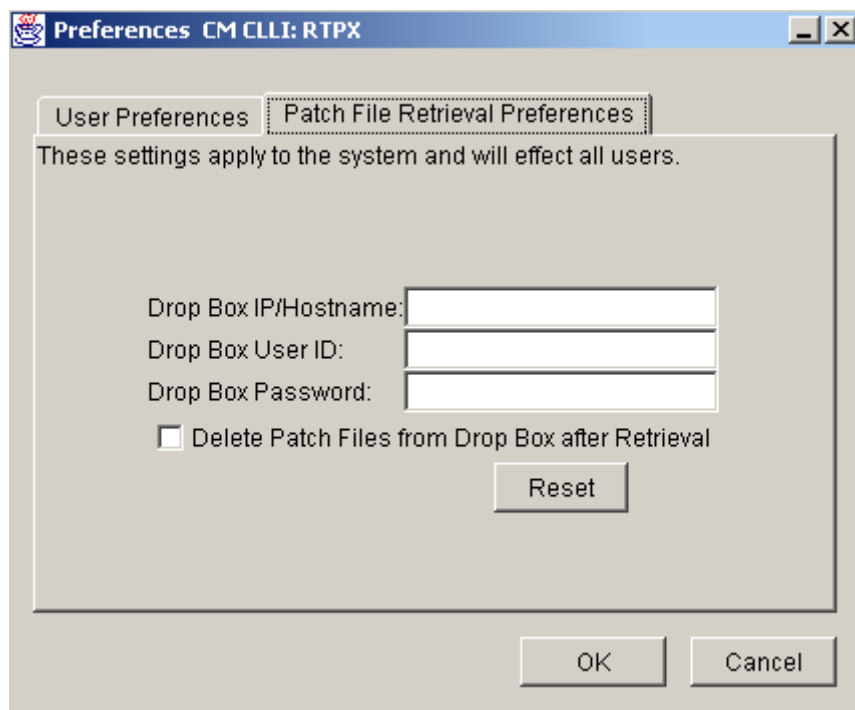


Notice the new “View” button on the bottom of the panel. System defined reports can only be viewed.

Figure 4 GUI name: Plan - Plan List



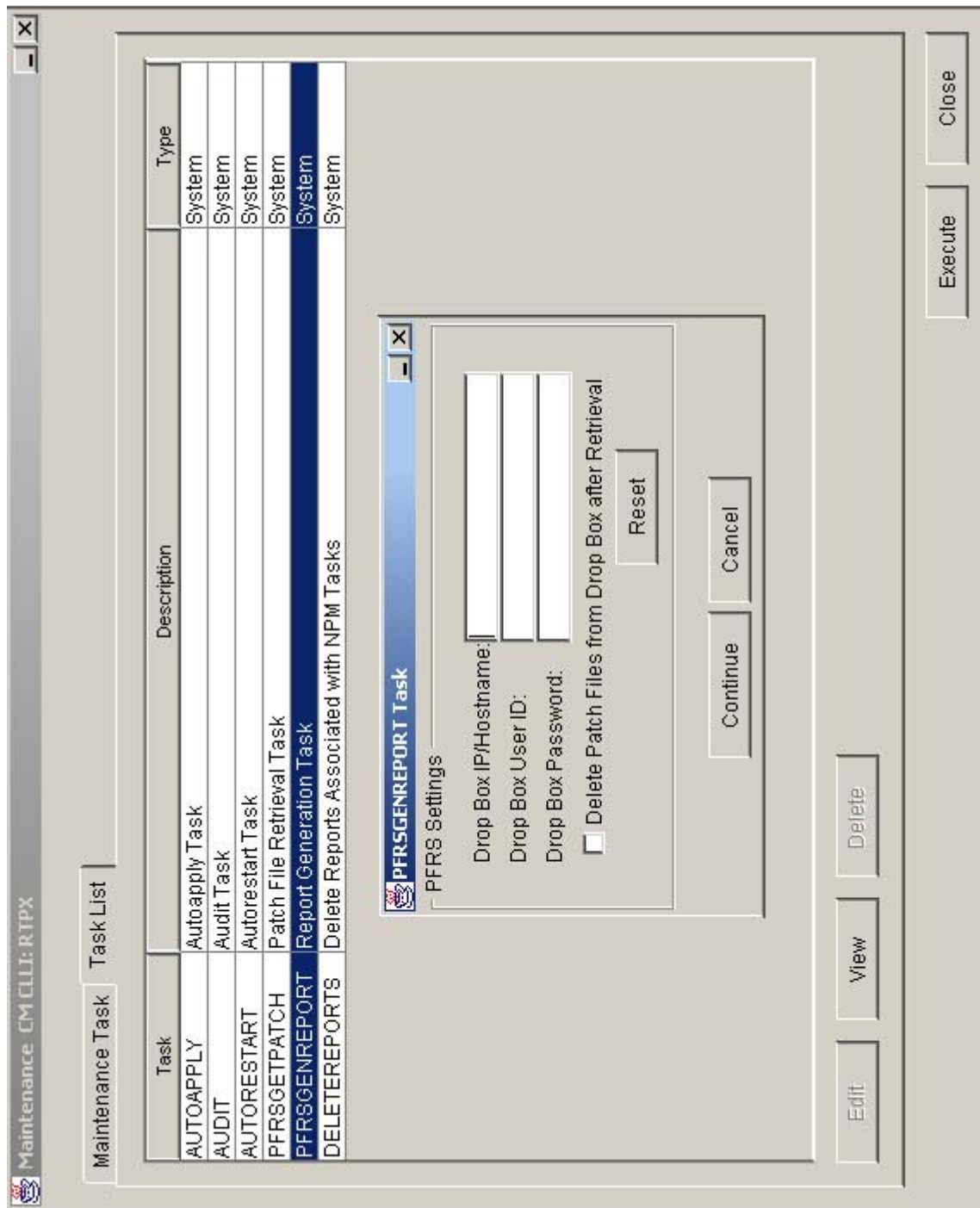
Notice the three new system defined plans that can be enabled and scheduled.

Figure 5 GUI name: Preferences - PatchFile Retrieval Preferences

This PatchFile Receipt Preference window allows the user to setup the drop off box information for the PatchFile Receipt System. The IP/Hostname, and user id will be verified and a warning message will be sent back to the user if the information cannot be verified. However, the information will still get put into and stored in the NPM database, since the user/customer may not have this remote drop off box configured at the time this information is input.

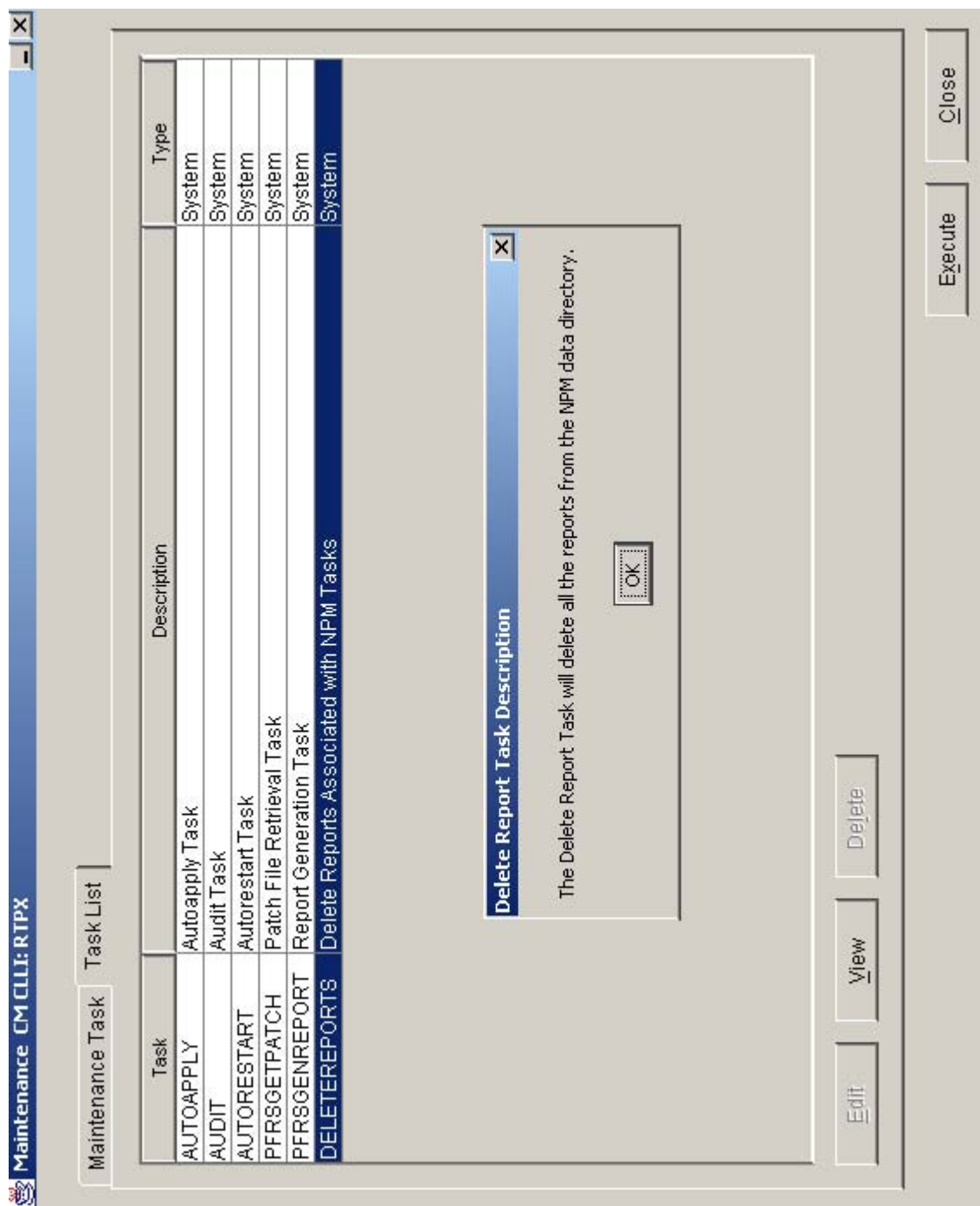
If the information is still incorrect at execution time of either PFRSGENREPORT or PFRSGETPATCH task, an error will occur and an alarm will be set. This information can also be set through the NPM CLUI and will execute in the same manner.

Figure 6 GUI name: PFRS TASK with preferences



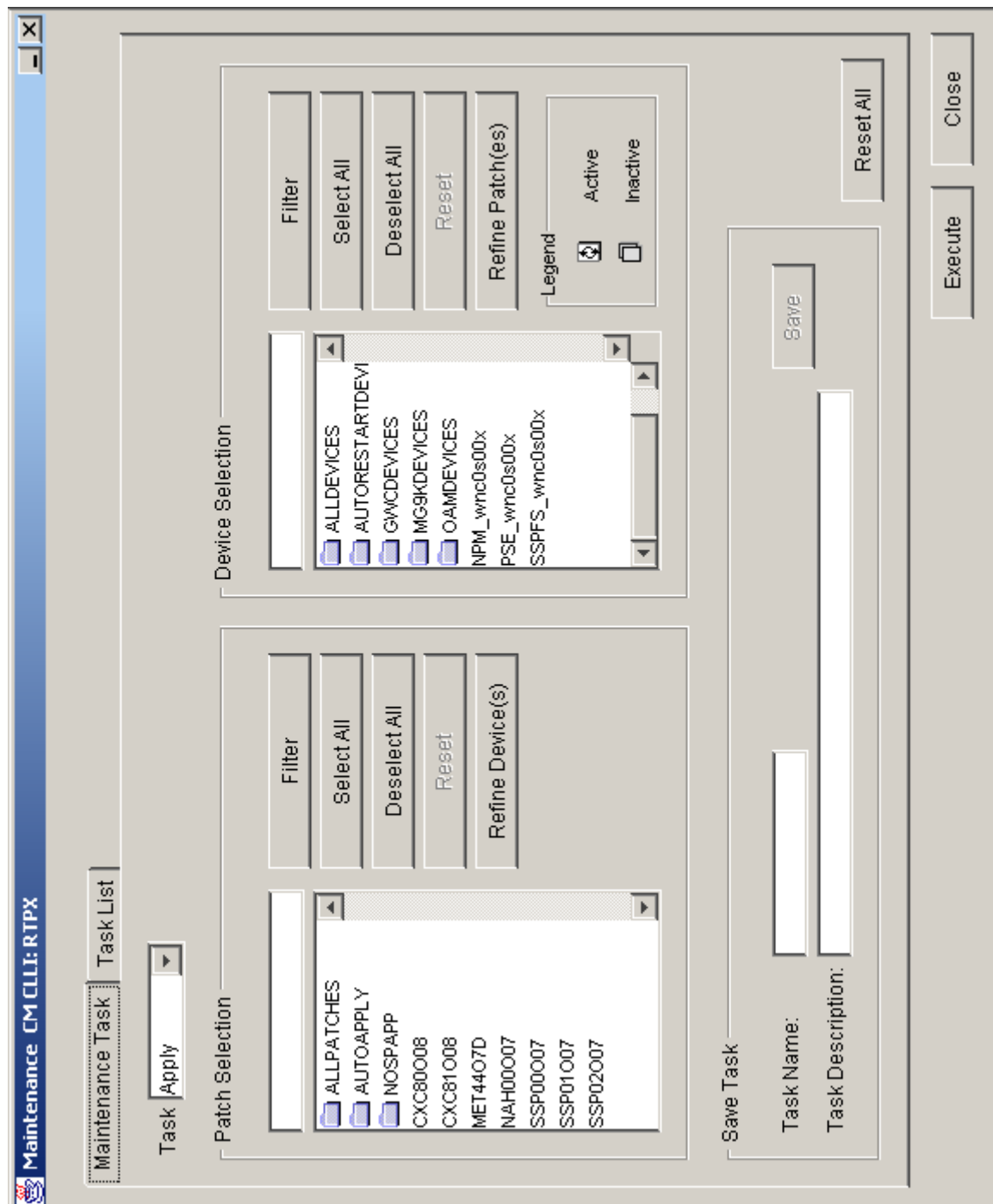
Notice the PFRS Preferences pop up window. This window is provided for each the PFRSGENREPORT and the PFRSGETPATCH task. This provides another option for the user to set up and execute either of these two tasks from the NPM GUI.

Figure 7 GUI name: Delete Task View



A new pop up window has been provided for tasks that do not contain either patches or devices. This pop up window provides the user a description of the task.

Figure 8 GUI name: Maintenance Task



Notice the new Refine Devices and Refine Patches buttons. These buttons narrow down either the devices or the patches for specific chosen patch or device.

13.4.3 CLUI Interface

The NPM CLUI provides the same functionality for the new PFRS access and task access as the GUI does. The following figures illustrate the commands in the NPM CLUI.

Figure 9 NPM CLUI Command Examples

```
npm>pfrsview
```

Retrieving PFRS settings...

Current PFRS Settings

IP address/Hostname : 47.142.164.252

Userid : FIELD

Delete Patches After Retrieval: N

```
npm>pfrsset 47.142.117.20 FIELD N
```

Enter password for drop box:

Setting PFRS preferences done

```
npm>qtask all
```

System retrieved...6

AUTOAPPLY: Autoapply Task (System Defined)

AUDIT: Audit Task (System Defined)

AUTORESTART: Autorestart Task (System Defined)

Figure 10 NPM CLUI Command Examples

npm>runtask PFRSGENREPORT

npm>

Reason : Passed

Detail : PFRS Gen Report was successful.

npm>pfrsset wnc0s00x FIELD N

Enter password for drop box:

Setting PFRS preferences done

14: A00006979 Configuration (CN)

14.1 Feature name

Synchronized Backup Restore Manager

14.2 Naming Conventions

Throughout this document, the backup restore functionality delivered under this feature will be referred to in 3 distinct ways:

Synchronous Backup Restore Manager (SBRM) refers specifically to the IEMS launched synchronized backup/restore software. The SRBM will control/synchronize the backup related activities across other components/devices which contain related backup software.

Device Backup Restore Manager (DBRM) refers specifically to the component/device level backup software which is controlled by the SBRM.

Backup Restore Manager is a generic term encompassing both SBRM and DBRM functionalities and in general simply refers to the software which is common to both.

14.3 Hardware and Software Requirements

Backup Restore Manager functionality requires that the appropriate software is resident and configured in all platforms which require synchronized imaging. The Backup Restore Manager software itself will be included in various platform software packages such as the SSPFS and SDM. SSPFS Backup Restore Manager functionality will be used for integration of Call Server Management Tools (CSMT), the Media Gateway 9000 Element Manager (MG9KEM), the Integrated Element Manager Server (IEMS), and the Core Billing Manager (CBM). The software on the SDM/CBM acts only to allow control of the XACore/3PC backup. No SDM/CBM data is backed up via the Backup Restore Manager software.

On the SDM, ensure the Java Runtime Environment (JRE) 1.3 package is installed. This package is not installed by default on the SDM. At the sdmmtc swim, level look for the following packages and install them in given order

First apply,

Java Runtime Environment Executables 1.3.0.0

Java Runtime Environment Libraries 1.3.0.0

Now, apply the following packages,

Java Runtime Environment Executables 1.3.0.15

Java Runtime Environment Libraries 1.3.0.15

14.4 Initial Configuration

1. Install Backup Restore Manager as part of the various platform software package installations (e.g. CSMT, IEMS, etc.).
2. Configure the Secure Shell (SSH) users and keys on the various platforms. See “14.9.2 Configuring SSH Between the Various Backup Restore Manager servers” on page 1487. Also, ensure the bkmgrusr is created on SDM platforms See “12.8.1.1”
3. Configure the automated Synchronous Backup Restore Manager scheduler if automated system backups are required. See “Automated Synchronous Backup Restore Manager service” on page 1495.
4. Configure the specific Backup Restore Manager installations, setting the appropriate properties for the Synchronous Backup Restore Manager which resides in IEMS and the individual component level Backup Restore Managers which reside in the other platforms (e.g. CSMT, SDM, etc.).
5. Configure the CM telnet users and Logical volume information on SDM/CBM machines. See “Configuring CM access information for Backup” on page 1502.

14.5 Upgrade Considerations

The centralized, Synchronous Backup Restore Manager functionality at IEMS will be blocked until the time that all affected components (CSMT, SDM, CBM, MG9KEM) are upgraded to SN08 load levels.

14.5.1 Dump and Restore (CM)

Not affected. Existing Dump and Restore will continue to function.

14.5.2 Element Management Upgrade

14.5.2.1 IEMS Database Table Spaces

In order to allow backup of only configuration data (as opposed to transient event and fault data) stored by IEMS, the Oracle database definitions are split into separate table spaces when IEMS is upgraded. A configuration table space and a runtime table space are created and existing tables are assigned to either space depending on the nature of the table data. Only the configuration table space is registered for backup.

14.5.3 Downgrade impact

None.

14.6 Element Management

14.6.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Request disallowed due to backup process.	NEW

14.6.2 GUI information

14.6.2.1 GUI name: IEMS System Backup Command Rejection Error Dialog

14.6.2.1.1 Functional description

IEMS will present the user with a general error dialog when the user attempts to perform actions which are incompatible with Synchronous Backup Restore Manager activity.

14.6.2.1.2 GUI usage and implications

No usage or implications for this GUI. It is simply an error response dialog.

14.6.2.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Backup Error	0	NA	NA

14.6.2.1.4 GUI fields

The following table lists fields for GUI or pull down menu Backup Error.

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Text Reason	NEW	NA	NA	User must accept error response.	NA

14.6.2.1.5 Usage example

The following example shows sample datafill or menu selection for GUI Backup Error:

14.6.2.1.6 GUI release history update

Not applicable.

14.6.2.1.7 Context sensitive launching information

Not applicable.

14.6.2.1.8 Supplementary information

GUI Screen shot example (many other actions can be rejected with a similar error dialog):



14.6.2.2 GUI name: <abbreviated name of GUI>

<long name of GUI>

14.6.2.2.1 Functional description

14.6.2.2.2 GUI usage and implications

14.6.2.2.3 GUI size

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory

14.6.2.2.4 GUI fields

The following table lists fields for GUI or pull down menu <abbreviated name of GUI>.

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

14.6.2.2.5 Usage example

The following example shows sample datafill or menu selection for GUI <abbreviated name of GUI>:

14.6.2.2.6 GUI release history update**14.6.2.2.7 Context sensitive launching information****14.6.2.2.8 Supplementary information****14.6.3 CLUI Interface**

The Synchronous Backup Restore Manager is invoked via a CLUI. The CLUI is started by IEMS. Once the user has entered the CLUI, only Synchronous Backup Restore Manager Commands are available to the user. The command prompt within the CLUI is “bkmgr>”. The following table shows the available commands and provides a brief description of each.

Table 6 Synchronous Backup Restore Manager Supported Commands

Command	Description
commands	Displays a list of commands available to the user.
help [command]	Displays help text. If the optional command name is omitted, help text for all commands will be displayed.
exit	Exits the Synchronous Backup Restore Manager CLUI.
quit	Exits the Synchronous Backup Restore Manager CLUI.
backup full	Performs all steps of a backup sequence. If a failure is encountered or an abort is issued, the backup stops at the completion of the current step in the backup sequence. Example: User issues the 'backup full' command. So the first thing the Synchronous Backup Restore Manager does is issue the command 'precheck' to all the Device Synchronous Backup Restore Managers on the supported nodes currently provisioned in IEMS. As the Device Backup Restore Managers are executing the precheck, the user issues the 'bkmgr abort'. AFTER the Device Backup Restore Managers are done with the prechecks it will stop the backup sequence and return all components to their initial states (e.g. startprov).

Table 6 Synchronous Backup Restore Manager Supported Commands

Command	Description
backup auto	Performs all steps of a backup sequence. Note: This is a “hidden” command only to be invoked by the Synchronous Backup Restore Manager scheduler. If a failure is encountered or an abort is issued, the backup stops at the completion of the current step in the backup sequence and the system will be restored to it's pre-backup state. This does not imply a 'rollback'. It simply means if the Device Backup Restore Managers have executed the 'stopprov' command the 'startprov' command will be issued to ensure provisioning can proceed.
backup abort	Aborts a backup after completion of the current step. Returns all applications to a startprov state if required.
query status	Display the status of the backup on a high level. Example: Backup in progress. Backup failed, etc.
query history	Display information about previous backups. Example: Last backup executed <date> <time> successful.
query inventory	Displays the components available for backup.
query backuplocation	Display the backup location of each component. All backups will be stored in a common file location. Example: /opt/nortel/backup/*
precheck	Perform basic sanity checks to ensure the system is in a state to perform a backup. Example: Check disk space and possibly subtending component (application) health
stopprov	Stops provisioning.
dumpdata	Backup the critical data.
startprov	Start provisioning (if stopped).
verify	Checks the validity of the backed up data. Example: Validate DB data.
activatenew	Marks the new backup data as the current backup. Example: Move current backup to permanent location.

All commands executed within the CLUI are synchronous commands. The command prompt will not be returned to the user until the requested command completes. Therefore, if the user wishes to perform an operation such as “query status” or “backup abort” while a command is executing, another CLUI instance must be started from IEMS, and the new command executed from the second CLUI instance.

Additionally, the Synchronous Backup Restore Manager allows only one backup related command to be running at a time. If a backup, or one of the commands that executes a backup step (precheck, stopprov, dumpdata, verify, startprov, activatenew), is invoked while a backup (or backup step) is in progress, the request will be rejected.

14.6.3.1 Execution of Backup Steps at Component Level

As the backup process, or steps of the backup process, are invoked from the CLUI, the Synchronous Backup Restore Manager distributes the commands to the various components/servers to be backed up. In rare instances, it may necessary to run various portions of the backup process on the individual components/servers themselves. This capability is provided, and is implemented as a CLUI interface as well.

This CLUI interface can be invoked by logging into the appropriate component via a Telnet session, and performing the following commands.

```
>cd /opt/nortel/bkresmgr/cbm  
>bkmgr
```

At this point, most of the commands listed in “ ” on page 1482 can be used. The commands NOT available when running at this component level are as follows.

- backup full
- backup auto
- backup abort

This capability should be used only in rare circumstances, and care should be taken to keep the Synchronous Backup Restore Manager and this Device Backup Restore Manager in sync.

14.7 OSSGate Interface Changes

14.7.1 OSSGate Changes

No existing Service Order formats or logic is affected by Backup Restore Manager. However, when Backup Restore Manager is executing a synchronized backup of CSMT, non-query OSSGate commands will be rejected with an error indicating that commands are disallowed during system backup. All modes (CI, XML, TL1) of OSSGate will support the error response. The error response will be formatted as follows:

“SERVICE ORDERS NOT ALLOWED. SYSTEM BACKUP IS IN PROGRESS. COMMANDS MAY BE REATTEMPTED FOLLOWING COMPLETION OF THE SYSTEM BACKUP.”

14.8 Security

14.8.1 Key management

SSH common key authorization based on user ID is used to screen activity between the various Backup Restore Managers. A common encrypted key is defined for the bkmgrusr user ID and distributed to all Backup Restore Manager platforms for the bkmgrusr user ID (see “Configuring the bkmgrusr user ID and Password for SSH Common Key Authorization” on page 1485 and “14.9.2 Configuring SSH Between the Various Backup Restore Manager servers” on page 1487)

14.8.2 Authentication

SSH common key authorization based on user ID is used to screen activity between the various Backup Restore Managers. A common encrypted key is defined for the bkmgrusr user ID and distributed to all Backup Restore Manager platforms for the bkmgrusr user ID (see “Configuring the bkmgrusr user ID and Password for SSH Common Key Authorization” on page 1485 and “14.9.2 Configuring SSH Between the Various Backup Restore Manager servers” on page 1487). The SSH connections between the IEMS based Synchronous Backup Restore Manager and the various Device Backup Restore Managers in the subtending application servers (CSMT, MG9KEM, etc.) are authenticated using this common key for the bkmgrusr user ID.

The launch of the Synchronous Backup Restore Manager from the IEMS GUI is authenticated using existing user based screening. Only users permitted to perform system level configuration changes will be allowed to launch the Synchronous Backup Restore Manager CLI from IEMS. Once launched, all commands (both query and non-query) are available. No further command level authentication is provided.

14.9 Configuration Walkthrough

14.9.1 Configuring the bkmgrusr user ID and Password for SSH Common Key Authorization

Before configuring SSH between the Backup Restore Manager servers the bkmgrusr user ID and password must be configured on all Backup Restore Manager Servers.

14.9.1.1 Configuring the bkmgrusr user ID and Password for SSH Common Key Authorization on SSPFS Based Platforms

On SSPFS based platforms, the bkmgrusr user ID is configured by default without a password. The bkmgrusr user ID password must be configured on all SSPFS based Backup Restore Manager servers using the Integrated EMS Central Security Server. Refer to section “Changing user password” in NN10336-611 Integrated EMS Security Administration.

Refer to section “Configuring the Integrated EMS central security server in the network” in NN10336-611 Integrated EMS Security Administration for configuring the Integrated EMS Central Security Server, and section “Configuring a central security client” in NN10336-611 Integrated EMS Security Administration for configuring an Integrated EMS Central Security client.

14.9.1.2 Configuring the bkmgrusr user ID and Password for SSH Common Key Authorization on SDM Based Platforms

On the SDM AIX platform, the bkmgrusr user ID and password needs to be configured in order for the SBRM to communicate with the DBRM.

1. Login to the DBRM (AIX/SDM box) by typing

>telnet <server> and pressing the Enter key. Where the server is the IP address or hostname of the SDM-AIX server where the Synchronous Backup Restore Manager is installed.

2. When prompted, login as root by entering root and password for root.
3. After login, create the user by typing

mkuser bkmgrusr

4. Now create the groups emsmtc, emsadm, emsrw by typing

mkgroup emsmtc

mkgroup emsadm

mkgroup emsrw

5. Now, make this user **bkmgrusr** belong to primary group **maint** and secondary group **emsmtc, emsadm, emsrw**

chuser pgrp=maint groups=emsmtc,emsadm,emsrw home=/home/bkmgrusr admin=true shell=/bin/ksh bkmgrusr

6. You can now confirm that the user bkmgrusr belongs to the groups maint, emsmtc, emsadm, emsrw by typing

groups bkmgrusr

and it will display the groups associated with this user.

7. Set the password for this user bkmgrusr by typing

passwd bkmgrusr

This new user is ‘locked out’ i.e. disabled until the password is set.

8. Logout as root and re login back to the AIX/SDM server as bkmgrusr. It would prompt the user to change password. After changing password the user would be logged in to the server. Go to the home directory if not already there

```
cd /home/bkmgrusr
```

```
mkdir .ssh
```

```
chmod 700 .ssh
```

14.9.2 Configuring SSH Between the Various Backup Restore Manager servers

1. Telnet to the IEMS server where the Synchronous Backup Restore Manager is installed by typing
> **telnet <server>** and pressing the Enter key. Where the server is the IP address or hostname of the IEMS server where the Synchronous Backup Restore Manager is installed.
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. If you are setting up SSH for the first time, or are changing the SSH keys follow the procedures outlined in “Generate SSH key and transfer to Device Backup Restore Manager server” on page 1487. If you need to transfer an existing SSH key to a new or existing DBRM follow the procedures outlined in “Transfer Existing SSH key to Device Backup Restore Manager server” on page 1492.

14.9.2.1 Generate SSH key and transfer to Device Backup Restore Manager server

1. Run the Backup Restore Manager configuration to setup SSH between the Synchronous Backup Restore Manager and various Device Backup Restore Managers:

- a. Change directory to the Backup Restore Manager configuration location and run the Backup Restore manager configuration:

```
$ cd /opt/bkresmgr/admin/bin
```

```
$ ./configure
```

Example response:

Backup Restore Manager Configuration

1 - Backup Restore Manager SSH Setup

2 - Automated Synchronous Backup Restore
Manager Service

X - exit

select - [X, 1-2]

- b. When prompted select 1 for Backup Restore Manager SSH Setup.

Example Response:

SSH Setup for Synchronous Backup Restore Manager

1 - Generate SSH key and transfer to Device
Backup Restore Manager servers

2 - Transfer existing SSH key to Device Backup
Restore Manager servers

X - exit

select - [X, 1-2]

- c. When prompted select 1 for Generate SSH key and transfer to Device
Backup Restore Manager servers.

Example Response:

Generate SSH key for Synchronous Backup Restore Manager and
transfer to Device Backup Restore Manager servers.

WARNING: Running this script will generate a new SSH key for the
bkmgrusr.

This new SSH key must be transferred to all existing and new Device
Backup Restore Manager servers.

Do you want to continue? [y/n]:

- d. When prompted, enter Y to continue.

Example response:

Generating SSH key for bkmgrusr.

Sun Microsystems Inc. SunOS 5.9 Generic May 2002

Generating public/private rsa key pair.

Enter file in which to save the key (/export/home/bkmgrusr/.ssh/
id_rsa):

- e. When prompted, press the Enter key to accept default location of key
file.

Example response:

Your identification has been saved in /export/home/bkmgrusr/.ssh/id_rsa.

Your public key has been saved in /export/home/bkmgrusr/.ssh/id_rsa.pub.

The key fingerprint is:

33:99:17:f0:ac:2a:3a:86:a9:d9:76:65:e6:70:4b:68
bkmgrusr@comp5iems

Synchronizing files IF clustered node

Transfer existing SSH key to Device Backup Restore Manager servers

WARNING: You must have the password for the bkmgrusr on the Device Backup Restore Manager server to transfer the SSH key.

Do you want to transfer the SSH key? [y/n]:

- f. When prompted, enter Y to transfer the SSH key.

Example response:

Setting up to transfer SSH key to DBRM server.

Enter hostname or IP address of DBRM server to transfer the SSH key to:

- g. When prompted, enter the DBRM server hostname or IP address.

Example response:

Platform type of DBRM server to transfer SSH key to:

1 - SSPFS

2 - SDM

Enter platform type of DBRM server to transfer SSH key to - [1-2]:

- h. When prompted, enter 1 if DBRM server is a SSPFS based server or 2 if DBRM server is a SDM based server.

Example response:

Sun Microsystems Inc. SunOS 5.9 Generic May 2002

The authenticity of host 'comp5iems (47.142.128.85)' can't be established.

RSA key fingerprint is
ff:eb:a8:87:14:d0:82:28:5c:43:70:5a:ab:af:e6:fd.

Are you sure you want to continue connecting (yes/no)?:

- i. When prompted, enter yes to continue connecting.

Example response:

Warning: Permanently added 'comp5iems,47.142.128.85' (RSA) to the list of known hosts.

Password:

- j. When prompted, enter the password for the bkmgrusr on the DBRM server.

Example response:

Transfer of SSH key to comp5iems complete.

- k. At this point, SSH will be set up for two alternate names of the server. Responses will vary depending on whether a server name or IP address was entered in the above steps, or if the server had been set up previously. Input may be required for either, both, or neither alternate name. The following examples provide one response requiring input, and one response that does not require input.

Example response:

```
Verifying SSH setup for  
'comp5iems.us.nortel.com'
```

```
The authenticity of host  
'comp5iems.us.nortel.com (47.142.128.85)' can't  
be established.
```

```
RSA key fingerprint is  
ff:eb:a8:87:14:d0:82:28:5c:43:70:5a:ab:af:e6:f  
d.
```

```
Are you sure you want to continue connecting  
(yes/no)?:
```

When prompted, enter yes.

```
Warning: Permanently added  
'comp5iems.us.nortel.com' (RSA) to the list of  
known hosts.
```

```
Successful
```

```
Verifying SSH setup for '47.142.128.85'
Successful
```

Is DBRM comp5iems a High Availability (HA) server? [y/n]:

2. If DBRM server is a HA server, enter Y. Otherwise enter N and proceed to Step 3.:

Note: You need to know the password for the root user on the NBRM server to complete the following steps.

- a. Synchronize the SSH data on the NBRM server:

Example response:

WARNING: On HA DBRM servers, SSH setup is not complete unless one of the following steps is performed.

- a) The HA DBRM server comp5iems is cloned.
- b) The SSH data on HA DBRM comp5iems is manually synched.

WARNING: Choosing this option requires the root password for comp5iems.

Do you want to manually synchronize the SSH data on DBRM comp5iems now [y/n]

- b. When prompted, enter Y to manually synchronize the SSH data:

Example response:

Password:

- c. When prompted, enter the password for the root user on the NBRM server.

Example response:

Synchronization of SSH data on DBRM comp5iems complete.

3. Repeat Step 1 f through 2 for each DBRM server.

Note: The SSH key must be transferred within the server it is created on. This is due to the configuration where both a SBRM and DBRM reside on the same server and use SSH to communicate within the server.

To transfer the SSH key within the server it is created on, simply enter the name (or IP address) of the server in step 1 g.

14.9.2.2 Transfer Existing SSH key to Device Backup Restore Manager server

1. Run the Backup Restore Manager configuration to setup SSH between the Synchronous Backup Restore Manager and various Device Backup Restore Managers:

- a. Change directory to the Backup Restore Manager configuration location and run the Backup Restore manager configuration:

```
$ cd /opt/bkresmgr/admin/bin
```

```
$ ./configure
```

Example response:

Backup Restore Manager Configuration

1 - Backup Restore Manager SSH Setup

2 - Automated Synchronous Backup Restore
Manager Service

X - exit

select - [X, 1-2]

- b. When prompted select 1 for Backup Restore Manager SSH Setup.

Example Response:

SSH Setup for Synchronous Backup Restore Manager

1 - Generate SSH key and transfer to Device
Backup Restore Manager servers

2 - Transfer existing SSH key to Device Backup
Restore Manager servers

X - exit

select - [X, 1-2]

- c. When prompted select 2 for Transfer existing SSH key to Device Backup Restore Manager servers.

Example Response:

Transfer existing SSH key to Device Backup Restore Manager servers

WARNING: You must have the password for the bkmgrusr on the Device Backup Restore Manager server to transfer the SSH key.

Do you want to transfer the SSH key? [y/n]:

-
- d. When prompted, enter Y to transfer the SSH key.

Example response:

Setting up to transfer SSH key to DBRM server.

Enter hostname or IP address of DBRM server to transfer the SSH key to:

- e. When prompted, enter the DBRM server hostname or IP address.

Example response:

Platform type of DBRM server to transfer SSH key to:

1 - SSPFS

2 - SDM

Enter platform type of DBRM server to transfer SSH key to - [1-2]:

- f. When prompted, enter 1 if DBRM server is a SSPFS based server or 2 if DBRM server is a SDM based server.

Example response:

Sun Microsystems Inc. SunOS 5.9 Generic May 2002

The authenticity of host 'comp5iems (47.142.128.85)' can't be established.

RSA key fingerprint is

ff:eb:a8:87:14:d0:82:28:5c:43:70:5a:ab:af:e6:fd.

Are you sure you want to continue connecting (yes/no)?:

- g. When prompted, enter yes to continue connecting.

Example response:

Warning: Permanently added 'comp5iems,47.142.128.85' (RSA) to the list of known hosts.

Password:

- h. When prompted, enter the password for the bkmgrusr on the DBRM server.

Example response:

Transfer of SSH key to comp5iems complete.

- i. At this point, SSH will be set up for two alternate names of the server. Responses will vary depending on whether a server name or IP address was entered in the above steps, or if the server had been set up previously. Input may be required for either, both, or neither alternate name. The following examples provide one response requiring input, and one response that does not require input.

Example response:

```
Verifying SSH setup for  
'comp5iems.us.nortel.com'
```

```
The authenticity of host  
'comp5iems.us.nortel.com (47.142.128.85)' can't  
be established.
```

```
RSA key fingerprint is  
ff:eb:a8:87:14:d0:82:28:5c:43:70:5a:ab:af:e6:f  
d.
```

```
Are you sure you want to continue connecting  
(yes/no)?:
```

When prompted, enter yes.

```
Warning: Permanently added  
'comp5iems.us.nortel.com' (RSA) to the list of  
known hosts.
```

```
Successful
```

```
Verifying SSH setup for '47.142.128.85'
```

```
Successful
```

Is DBRM comp5iems a High Availability (HA) server? [y/n]:

2. If DBRM server is a HA server, enter Y. Otherwise enter N and proceed to Step 3.:

Note: You need to know the password for the root user on the NBRM server to complete the following steps.

- a. Synchronize the SSH data on the NBRM server:

Example response:

WARNING: On HA DBRM servers, SSH setup is not complete unless one of the following steps is performed.

a) The HA DBRM server comp5iems is cloned.

b) The SSH data on HA DBRM comp5iems is manually synched.

WARNING: Choosing this option requires the root password for comp5iems.

Do you want to manually synchronize the SSH data on DBRM comp5iems now [y/n]

b. When prompted, enter Y to manually synchronize the SSH data:

Example response:

Password:

c. When prompted, enter the password for the root user on the NBRM server.

Example response:

Synchronization of SSH data on DBRM comp5iems complete.

3. You will be prompted to transfer the SSH key to another DBRM server. Enter Y to transfer SSH key to another DBRM server. Enter N if you do not want to transfer SSH key to another DBRM server. If you enter N you have completed the procedure.

Example response:

WARNING: You must have the password for the bkmgrusr on the Device Backup Restore Manager server to transfer the SSH key.

Do you want to transfer the SSH key to another DBRM server? [y/n]:

4. Repeat Step 1 d through 3 for each DBRM server you want to transfer the SSH key to.

14.9.3 Automated Synchronous Backup Restore Manager service

14.9.3.1 Configuring the Automated Synchronous Backup Restore Manager service

1. Telnet to the IEMS server where the Synchronous Backup Restore Manager is installed by typing
> **telnet <server>** and pressing the Enter key. Where the server is the IP address or hostname of the IEMS server where the Synchronous Backup Restore Manager is installed.
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. Run the Backup Restore Manager configuration. Change directory to the Backup Restore Manager configuration location and run the Backup Restore manager configuration:

```
$ cd /opt/bkresmgr/admin/bin
```

```
$ ./configure
```

Example response:

```
Backup Restore Manager Configuration
```

- 1 - Backup Restore Manager SSH Setup
- 2 - Automated Synchronous Backup Restore Manager Service
- X - exit

```
select - [X, 1-2]
```

6. When prompted select 2 for Automated Synchronous Backup Restore Manager Service.

Example Response:

```
Automated Synchronous Backup Restore Manager Service
```

- 1 - Configure Automated Synchronous Backup Restore Manager Service
- 2 - Start the Automated Synchronous Backup Restore Manager Service
- 3 - Stop the Automated Synchronous Backup Restore Manager Service
- 4 - View the Automated Synchronous Backup Restore Manager Service Configuration
- X - exit

```
select - [X, 1-4]
```

7. When prompted select 1 for Configure Automated Synchronous Backup Restore Manager Service.

Example Response:

```
Automated Synchronous Backup Restore Manager Service Configuration
```

```
Configuring the Automated Synchronous Backup Restore Manager Service does not START the service. Return to the previous menu and select
```

'Start the Automated Synchronous Backup Restore Manager Service' to start the service.

Day of week to run the Synchronous Backup Restore Manager:

This is day of the week the Synchronous Backup Restore Manager will execute a full backup.

- 1 - MONDAY
- 2 - TUESDAY
- 3 - WEDNESDAY
- 4 - THURSDAY
- 5 - FRIDAY
- 6 - SATURDAY
- 7 - SUNDAY

Enter day of week to run the Synchronous Backup Restore Manager (default: SUNDAY):

- 8.** When prompted enter the number corresponding to the day of the week.

Example Response:

Hour to run the Synchronous Backup Restore Manager based on 24 hour clock:

Example 1 is 1 AM, 12 is noon, and 24 is midnight.

This is the hour on the SATURDAY the Synchronous Backup Restore print Manager will execute a full backup.

Enter hour to run the Synchronous Backup Restore Manager (default: 24)

- 9.** When prompted enter a number corresponding to the time on the day of the week (based on a 24 hour clock).

Example Response:

Automated Synchronous Backup Restore Manager Service Configuration complete.

- 10.** You have completed this procedure. To start the Automated Synchronous Backup Restore Manager Service refer to.

14.9.3.2 Starting the Automated Synchronous Backup Restore Manager service

1. Telnet to the IEMS server where the Synchronous Backup Restore Manager is installed by typing
> **telnet <server>** and pressing the Enter key. Where the server is the IP address or hostname of the IEMS server where the Synchronous Backup Restore Manager is installed.
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. Run the Backup Restore Manager configuration. Change directory to the Backup Restore Manager configuration location and run the Backup Restore manager configuration:
\$ **cd /opt/bkresmgr/admin/bin**

\$ **./configure**

Example response:

Backup Restore Manager Configuration

- 1 - Backup Restore Manager SSH Setup
- 2 - Automated Synchronous Backup Restore Manager Service
- X - exit

select - [X, 1-2]

6. When prompted select 2 for Automated Synchronous Backup Restore Manager Service.

Example Response:

Automated Synchronous Backup Restore Manager Service

- 1 - Configure Automated Synchronous Backup Restore Manager Service
- 2 - Start the Automated Synchronous Backup Restore Manager Service
- 3 - Stop the Automated Synchronous Backup Restore Manager Service
- 4 - View the Automated Synchronous Backup Restore Manager Service Configuration
- X - exit

```
select - [X, 1-4]
```

7. When prompted select 2 for Start the Automated Synchronous Backup Restore Manager Service.

Example Response:

```
Start the Automated Synchronous Backup Restore
Manager Service
```

```
WARNING: Running this script will start the
Automated Synchronous Backup Restore Manager
Service
```

```
Starting the service does not initiate a backup
until the day and time configured.
```

```
Do you want to continue? - [y/n]:
```

8. When prompted enter Y to start the Automated Synchronous Backup Restore Manager Service.

Example Response:

```
Registering with SERVMAN.
```

```
Starting the Automated Synchronous Backup Restore
Manager Service.
```

```
Starting AUTO_BACKUP_MANAGER through servstart
AUTO_BACKUP_MANAGER Started
```

9. You have completed this procedure.

14.9.3.3 Stopping the Automated Synchronous Backup Restore Manager service

1. Telnet to the IEMS server where the Synchronous Backup Restore Manager is installed by typing
 > **telnet <server>** and pressing the Enter key. Where the server is the IP address or hostname of the IEMS server where the Synchronous Backup Restore Manager is installed.
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. Run the Backup Restore Manager configuration. Change directory to the Backup Restore Manager configuration location and run the Backup Restore manager configuration:

```
$ cd /opt/bkresmgr/admin/bin
```

```
$ ./configure
```

Example response:

```
Backup Restore Manager Configuration
```

```
1 - Backup Restore Manager SSH Setup
```

```
2 - Automated Synchronous Backup Restore  
    Manager Service
```

```
X - exit
```

```
select - [X, 1-2]
```

6. When prompted select 2 for Automated Synchronous Backup Restore Manager Service.

Example Response:

```
Automated Synchronous Backup Restore Manager  
Service
```

```
1 - Configure Automated Synchronous Backup Restore  
    Manager Service
```

```
2 - Start the Automated Synchronous Backup Restore  
    Manager Service
```

```
3 - Stop the Automated Synchronous Backup Restore  
    Manager Service
```

```
4 - View the Automated Synchronous Backup Restore  
    Manager Service Configuration
```

```
X - exit
```

```
select - [X, 1-4]
```

7. When prompted select 3 for Stop the Automated Synchronous Backup Restore Manager Service.

Example Response:

```
Stop the Automated Synchronous Backup Restore  
Manager Service
```

```
WARNING: Running this script will stop the  
Automated Synchronous Backup Restore Manager  
Service
```

Stopping the service does not abort a backup in progress.

Do you want to continue? - [y/n]:

8. When prompted enter Y to stop the Automated Synchronous Backup Restore Manager Service.

Example Response:

Stopping the Automated Synchronous Backup Restore Manager Service.

Stopping group using servstop
 AUTO_BACKUP_MANAGER Stopped

Deregistering with SERVMAN

9. You have completed this procedure.

14.9.3.4 Viewing the Automated Synchronous Backup Restore Manager service configuration

1. Telnet to the IEMS server where the Synchronous Backup Restore Manager is installed by typing
 > **telnet <server>** and pressing the Enter key. Where the server is the IP address or hostname of the IEMS server where the Synchronous Backup Restore Manager is installed.
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. Run the Backup Restore Manager configuration. Change directory to the Backup Restore Manager configuration location and run the Backup Restore manager configuration:
 \$ **cd /opt/bkresmgr/admin/bin**
 \$ **./configure**

Example response:

Backup Restore Manager Configuration

- 1 - Backup Restore Manager SSH Setup
- 2 - Automated Synchronous Backup Restore Manager Service

```
X - exit
select - [X, 1-2]
```

6. When prompted select 2 for Automated Synchronous Backup Restore Manager Service.

Example Response:

```
Automated Synchronous Backup Restore Manager
Service
```

```
1 - Configure Automated Synchronous Backup Restore
Manager Service
```

```
2 - Start the Automated Synchronous Backup Restore
Manager Service
```

```
3 - Stop the Automated Synchronous Backup Restore
Manager Service
```

```
4 - View the Automated Synchronous Backup Restore
Manager Service Configuration
```

```
X - exit
select - [X, 1-4]
```

7. When prompted select 4 for View the Automated Synchronous Backup Restore Manager Service Configuration.

Example Response:

```
The Automated Synchronous Backup Restore Manager
Service is running
```

```
Automated Synchronous Backup Restore Manager
Service Configuration Settings
```

```
Backup Enabled           : Y
Backup Day               : SATURDAY
Backup Hour              : 23
```

8. You have completed this procedure.

14.9.4 Configuring CM access information for Backup

Before the software can automatically back up image on CM, the user needs to configure information to access CM. This section covers the necessary steps which needs to be done, before CM backup will be successful when initiated through the Synchronous Backup Restore Manager. On the SDM (AIX), as

soon as the software is installed, this configuration script will be run automatically by SWIM. However on Core Billing Manager machine (Solaris), the user has to manually do the steps (1 - 6)

1. 1. telnet to Core Billing Manager machine, one of which would have been chosen in the network to interface with the CM by typing

```
#telnet <server>
```

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. cd to /opt/nortel/bkresmgr/cbm/scripts directory
6. Run the configure script by typing

```
#./bkmgr_config.sh and hit the <enter> key
```

This script will prompt the following information

- a. user name: This is the user name which will be used to login to CM to initiate image dump. The script restricts you to have user name of 16 characters. First permit this user on the CM before doing this configuration. See Section 12.12.2.1 Setting user id on CM
- b. password: This is the password for the user entered above. The script restricts you to have password of 16 characters. First permit this user on CM before doing this configuration. See Section 12.12.2.1 Setting user id on CM
- c. Logical Volume: This is the device in which the image dump will be stored. User should ensure that this device has enough space for backup
- d. CM type: The type of CM, whether it is Xacore or Compact. This information is needed so the software knows whether CM will have Message Switch load also.

Shown below is screen output running this configure script.

```
# ./bkmgr_config.sh
Backup Restore Manager Configuration
```

Enter the CM user name: bkuser

Enter the password for bkuser:

Enter the Logical volume where backup is to be stored: sd01image

Enter the type of CM 1.XA-Core 2. Compact [1/2]: 2

Please wait while storing configuration information...

14.9.4.1 Setting user id on CM

At the CI prompt on the switch

```
> permit <backup-user> <password> 4 10000 ENGLISH ALL
```

where,

<backup-user> is the user name for user which will be used by Backup Restore Manager to login

<password> is the password for the <backup-user>

4 is the priority

10000 is the stacksize

and language is ENGLISH

privilege is ALL

The type of operations done by this user are shown below

- i. Set dump_restore_in_progress field in ofcstd table
- ii. start image dump
- iii. should be able to run itocci command set
- iv. should be able to do diskut commands

Note 1: If Enhanced Password control is in effect on CM, the password should be atleast 6 characters long.

Note 2: If Enhanced Password control is in effect on CM, after the user is permitted on the switch, login to CM manually with this user first. The CM will prompt you to change the password at first login after being permitted. Change the password and then do the configuration on SDM/CBM with the user and the changed password. Backup Restore Manager software does not have ability to manage passwords. Hence, the customer needs to ensure that when the passwords expire and change on CM for this 'backup-user', CBM/SDM configuration should be re-run to ensure the Device Backup Restore Manager has password in sync with CM.

15: A00007000 Configuration (CN)

15.1 Feature name

GigE Network Interface

15.2 Hardware and Software Requirements

The MG9000 and MG9000 software load which supports GIGE should be available.

15.3 Initial Configuration

The MG9000 should be configured as GIGE from LCI. The EM user will be able to view the link details once the MG9000 is configured.

15.4 Upgrade Considerations

Since a new SCG card has been added to support this feature in SN08, there won't be any upgrade changes

15.5 Element Management

MG9000 Element manager will be used to manage the GigE MG9000.

The EM user will be able to view the GigE link configuration details, GigE alarms, PMs and OMs. The user will also be able to view and provision clock sync data, link protection data, VLAN related data for the GigE ports and links. Details are provided in the respective sections.

The audit on the administrative status of the GigE cards, links will be done if a mismatch is found. The data audit will be done if mismatch is found in any data provisioned from EM for clock sync, VLAN, thresholds and bandwidth. The MG9000 will be the master in all these cases.

15.5.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
GigECardView	NEW
GigEPortView	NEW
GigELinkProtection	NEW
BandWidthManager	NEW
VLAN	NEW
Performance Browser	CHANGED

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
LinkIntegrityView	NEW

15.5.2 GUI information

15.5.2.1 GUI name: GigeCardView

15.5.2.1.1 Functional description. Each SCG card has four ports. The card view can be opened from the shelf view. The card view shows totally four ilog graphics for the ports as shown in figure 1. Clicking on each of them opens the GigePortView.

Figure 1 Card View

MG9000 Actions

Card Attributes

CLEI Code:	VAC4SNPAAA
Card Description:	Nortel MG9k G
Hardware Version:	5 200249
Firmware Version:	06
Software Version:	08_0
Serial Number:	M40093570
Manufacturer:	Nortel Networks
PEC Code:	NTNY41AA

Status

Availability Status:	Dependency
Usage Status:	Idle
Standby Status:	Providing_Servi
Card Alarm Status:	None
Procedural Status:	Normal
Control Status:	

State

Administrative State:	Locked
Configuration State:	Offline
Operational State:	Disabled

Card

GigE Card Alarms

Critical:	0	Minor:	0
Major:	0	Warning:	0

15.5.2.2 GUI name: GigePortView

The GigePortView will be opened when the user double clicks on the SCG card's port icon in the card view. The port view displays port/link attributes and its provisioning information as shown in figures 2 & 3.

15.5.2.2.1 Functional description. The port/Link attributes are shown in 'Link Details' tab.

The 'Link Controls' tab allows the user to provision link information.

Once the WAN ports (active and inactive) are configured from the LCI, the EM user will be able to set any port as the inactive WAN port on the inactive GIGE card. To change the inactive port, the current WAN port should be offlined and the new port should be online. The port can be online in the 'Link Controls' tab.

If the user tries to change the inactive WAN port (i.e. online the new port) without changing the existing WAN port's configuration status to offline, an error message that 'the existing WAN port should be offlined' will be displayed to the user.

If the user tries to change the WAN port on the active card, an error message "The WAN port is active, port can not be changed" will be displayed to the user.

The user will be able to change administrative status and configuration status for the port. The EM user will not be able to change the administrative and configuration status of the active WAN port.

The loopback status is not modified in SN08 as loopback is not supported. The Tx RFI and Rx RFI will be 'ON' by default. When it is enabled, RFI alarms will be raised and receiving an RFI alarms will result in sparing activity. When the RFI is disabled the RFI alarms will not be sent to EM.

The user should specify no. of SES to 1 UAS. It will not be set by default. When the value is changed a warning message that the '<number> of SES set to one UAS' will be displayed to the user.

The Rx excessive error ratio and Rx signal degrade thresholds can be provisioned for each port.

Figure 2 Link details

The screenshot shows a software window titled "GigE Port: NE-16 Frame-0 Shelf-2 Slot-10 Port -0". The window has a menu bar with "MG9000" and "Actions". Below the menu bar are two tabs: "Link Details" (selected) and "Link Controls".

Port Attributes

Description:	Gigabit Ethernet Link
MAC Address:	00:60:38:63:34:63
Port Type:	Ethernet CSMA/CD
Optics Type:	0

Link Attributes

Link Type:	Primary NI
Auto-negotiation Mode:	Enabled
Auto-negotiation Status:	Other
Duplex:	Full Duplex
Speed in bps:	1000000
Pause Admin Mode:	Disabled
MTU Size:	1600

Local Advertised Values

Duplex:	44544
Speed in bps:	44544
Pause Admin Mode:	44544

Partner Advertised Values

Duplex:	0
Speed in bps:	0
Pause Admin Mode:	0

GigE Port Alarms

Critical:	0
Minor:	0

Figure 3 Link Controls information

GigE Port: NE-16 Frame-0 Shelf-2 Slot-10 Port -0

MG9000 Actions

Link Details | Link Controls

Status

Administrative status: LOCKED

Configuration status: OFFLINE

Operational status: Disabled

State

Loopback: No Loop

Tx RFI: Disable

Rx RFI: Disable

Bw/Link in bps: 1000000000

Soak Values

UAS Count: 10

SES Percent: 20

Threshold Crossings

Rx EER in percent: 21

Rx SD in percent: 10

Apply

GigE Port Alarms

Critical: 0 Minor: 0

15.5.2.2.2 GUI usage and implications

The portview should be opened from the GigE card view.

15.5.2.2.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GigePortView	1	8	

15.5.2.2.4 GUI fields

The GUI fields for the GigePortLinkView.

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
sDescription	New	-	-	Displays the port description	ifDesc
sPhyAddress	New	-	-	Physical address of the port	ifPhysAddress
iPortType	New	-	-	port type	ifType
iOpticsType	New	-	-	optics type	ifMAuTypeListBits
ilinkType	New			Specifies whether the link is network or subtending	nnGLinkConfigNiOrSubtending
iAutoNeg	New	-	-	autonegotiation variable	ifMauAutoNegAdminStatus
iDuplex	New	-	-		dot3StatsDuplexStatus
iSpeed	New	-	-		ifHighSpeed
iMtu	New	-	-		ifMtu
linkAttrFlowControl	New	-	-	Link attribute's flow control	?
pauseAdminMode	New	-	-	Link attribute's pause Tx	dot3PauseAdminMode
pauseRxOverride	New	-	-	Link attribute's pauseRxOverride	?
mtuSize	New	-	-	Mtu Size	ifMtuSize

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
passControl	New	-	-	Link attribute's pass control	?
locAdvDuplex	New	-	-	Local advertised duplex	ifMauAutoNegCapAdvertisedBits
locAdvSpeed	New	-	-	Local advertised speed values	ifMauAutoNegCapAdvertisedBits
locAdvPauseTx	New	-	-	Local advertised Pause Tx	ifMauAutoNegCapAdvertisedBits
locAdvPauseRx	New	-	-	Local advertised Pause Rx	ifMauAutoNegCapAdvertisedBits
parAdvDuplex	New	-	-	Partner advertised duplex	ifMauAutoNegRemoteFaultAdvertised
parAdvFlowControl	New	-	-	partner advertised flow control	ifMauAutoNegRemoteFaultAdvertised
parAdvSpeed	New	-	-	Partner advertised speed	ifMauAutoNegRemoteFaultAdvertised
linkAdminStatus	New	-	-	Admin state of the link	ifAdminStatus
linkConfigStatus	New	-	-	Configuration state of the link	nnGLinkConfigOnlineStatus
linkOperStatus	New	-	-	Operational state of the link	ifOperStatus
linkLaserStatus	New	-	-	Laser state of the link	nnGLinkConfigLaserStatus
loopbackState	New	-	-	tells whether the loopback is enabled	nnGLinkConfigLoopback
Tx RFI	New	-	-	Link State	nnGLinkConfigTxRfi
Rx RFI	New	-	-	Link State	nnGLinkConfigRxRfi
iUasCount	New	-	-	UAS count	nnGLinkSoakCountUAS
iSESPercent	New	-	-	no. of SES for 1 UAS	nnGLinkSoakPercentSES
RxEER	New	-	-		nnGLinkFaultConfigAlmDef

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
RxSD	New	-	-		nnGLinkFaultConfig AlmDef

15.5.2.3 GUI name: GigeLinkProtection

15.5.2.3.1 Functional description

The Link Protection Group should be enabled for the link protection to be enabled. The Link protection can be invoked from the shelfview. User will be able to specify the protection group number, protection group type, working (preferred) link and protected (non-preferred) link. In SN08, only one protection group of type 1:1 is supported. User can also enable/disable Link Reversion mode. When it is enabled, the working channel is always preferred. The system will swact to it when it is available again. The wait to revert time should be specified by the user. By default, the Wait to revert time is 600 sec. This option will be available only for the active and inactive WAN ports. To switch to the other link, the cards need to be swacted

Figure 4 .Link Protection Provisioning

GigE Protection Provisioning View

MG9000

Protection Group Number: 1 Select Group Number: 1 ▼

Protection Group Type: 1:1 ▼

Protection Mode: Revertive ▼

Wait To Revert in sec: 200

Create Group Delete Group Modify Group

Refresh Close

The Link protection status can be viewed for each link from GigELinkProtectionView from Actions submenu of GigePortView as shown in the figure following.

Figure 5 Link Protection status



15.5.2.3.2 GUI usage and implications

15.5.2.3.3 GUI size

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GigeProtection	1	2	
GigeProvisioning	1	1	

15.5.2.3.4 GUI fields

The GUI fields for the GigePortLinkView.

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
protGroupNumber	New	-	-	Protection Group Number	nnGLinkProtGrpType

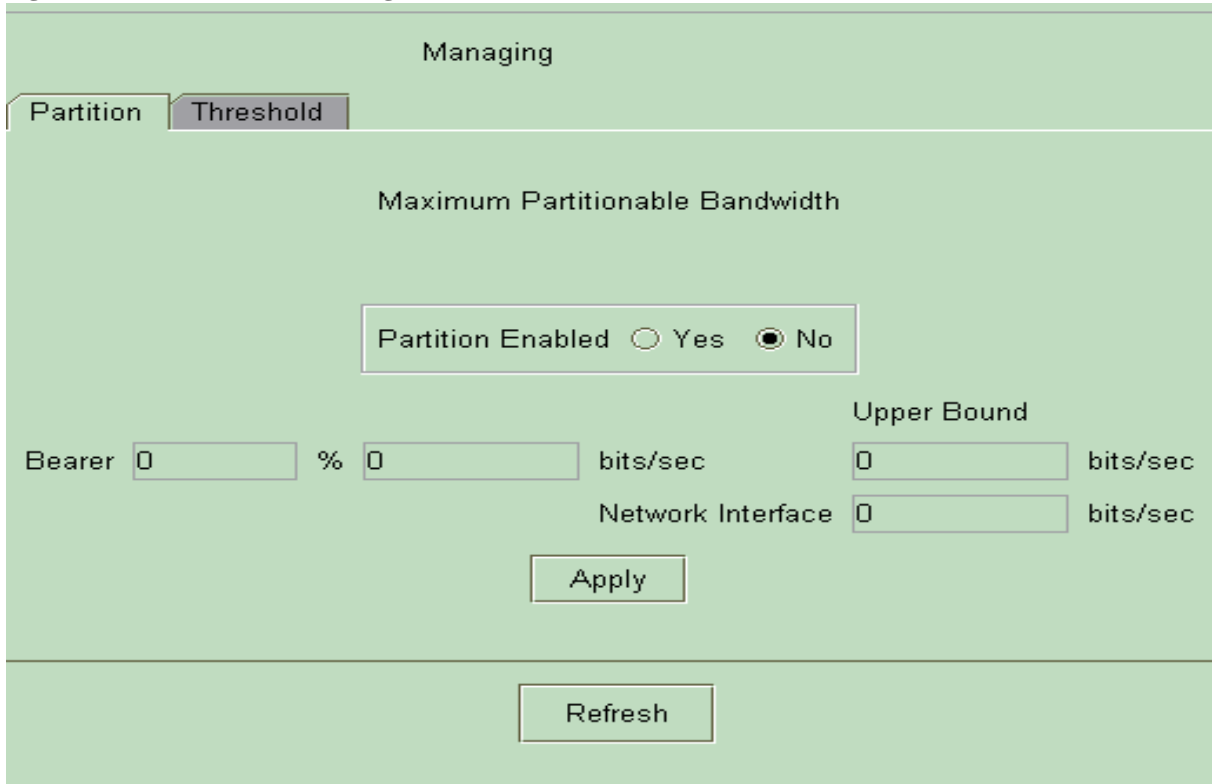
Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
protGroupType	New	-	-	protection group type	nnGLinkProtGrpType
protMode	New	-	-	Protection mode	nnGLinkProtGrpRevertive
waitToRevert	New	-	-	No.of seconds to revert	nnGLinkProtGrpWaitTime
prefLink	New			Preferred link	
nonPrefLink	New	-	-	Non preferred link	

15.5.2.4 GUI name: Bandwidth Manager

15.5.2.4.1 Functional description

In SN08, the Private lines and DSL services are not supported. The following network interface bandwidth data will be monitored: current ITP voice usage, current ABI voice usage and Overall network interface utilization. The data will be displayed in bits/second for GIGE systems. Bandwidth partitioning also will be supported in GIGE. The bandwidth manager panel can be viewed from the Services submenu. The bandwidth manager view will have following details

Figure 6 Bandwidth Partitioning View

The interface for the Bandwidth Partitioning View is displayed within a green-themed window titled "Managing". It features two tabs: "Partition" and "Threshold", with "Threshold" currently selected. The main content area is titled "Maximum Partitionable Bandwidth". Below this title, there is a section for "Partition Enabled" with two radio buttons: "Yes" and "No", where "No" is selected. Further down, there are three input fields for bandwidth settings: "Bearer" (set to 0), a percentage sign, another input field (set to 0), and "bits/sec"; "Upper Bound" (set to 0) and "bits/sec"; and "Network Interface" (set to 0) and "bits/sec". An "Apply" button is located below these fields. At the bottom of the window, there is a "Refresh" button.

Managing

Partition Threshold

Maximum Partitionable Bandwidth

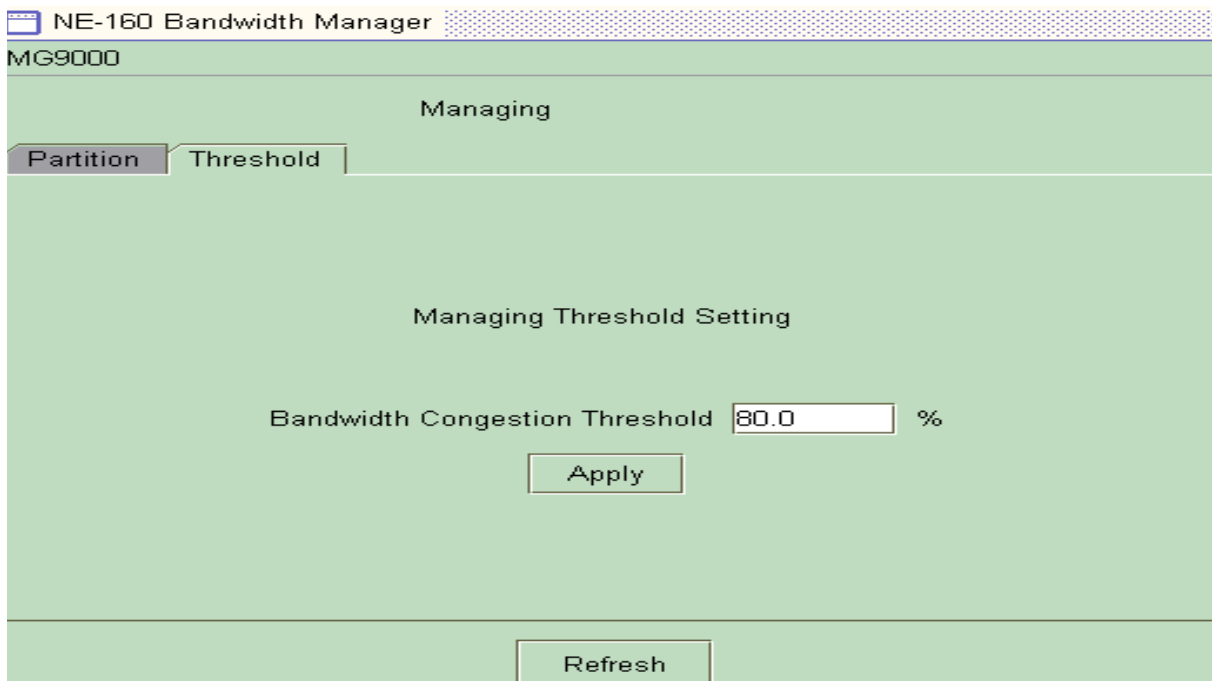
Partition Enabled ☐ Yes ☒ No

Bearer 0 % 0 bits/sec Upper Bound 0 bits/sec

Network Interface 0 bits/sec

Apply

Refresh

Figure 7 Bandwidth threshold managing

The interface for the Bandwidth threshold managing is displayed within a green-themed window titled "NE-160 Bandwidth Manager". Below the title bar, the text "MG9000" is visible. The main content area is titled "Managing" and contains two tabs: "Partition" and "Threshold", with "Threshold" currently selected. The section is titled "Managing Threshold Setting". It features a "Bandwidth Congestion Threshold" input field set to "80.0" followed by a percentage sign. An "Apply" button is located below this field. At the bottom of the window, there is a "Refresh" button.

NE-160 Bandwidth Manager

MG9000

Managing

Partition Threshold

Managing Threshold Setting

Bandwidth Congestion Threshold 80.0 %

Apply

Refresh

Figure 8 Bandwidth network Interface View

Network Interface Per Shelf Utilization

Currently Reserved Bandwidth

ITP Bearer 0 % 0 bits/sec

ABI Bearer 0 % 0 bits/sec

Total 0 % 0 bits/sec

Figure 9 Bandwidth reserved per shelf

Monitoring

Network Interface Per Shelf Utilization

Frame	Shelf	Bandwidth(%)	Bandwidth(bits/sec)
0	2	0	0

Close

Figure 10 Bandwidth utilization view

Monitoring

Network Interface Per Shelf Utilization

Network Interface Bandwidth Utilization

Mean Ingress Rate % bits/sec

Mean Egress Rate % hits/sec

Close

15.5.2.4.2 Bandwidth Manager IP solution

There is slight modification in bandwidth manager GUI for IP solution

Earlier the bandwidth manager GUI was same for both AAL1 and IP solutions. The existing GUI holds good for AAL1 solution. There are slight changes in IP solution bandwidth manager GUI. The changes are in Partition panel, Priority panel and the Network Interface panel.

Partition panel

There are 2 partitions, Bearer and DSL.

Each of the partition will have three fields percent, bandwidth in cps, and max value in cps (this is the upper bound).

When provisioning a partition percent, the corresponding bandwidth is calculated from the upper bound,

$$\text{i.e. } \% * \text{upperbound} = \text{partition bandwidth.}$$

Total partitionable and the interface capacity will be displayed. The total percent will not be displayed in this case.

Figure 11 Bandwidth manger partition panel for IP solution

Services Views Alarms

MG9000 Element 18

NE-18 Bandwidth Manager

MG9000

Managing

Partition Threshold Priority

Maximum Partitionable Bandwidth

Partition Enabled ☐ Yes ☒ No

Bearer % cells/sec

Guaranteed DSL % cells/sec

Total Partitionable

Network Interface

Upper Bound

Apply

Refresh

Priority Panel

PLOA holding priority data is removed. (as compared to AAL1 priority panel)

Network Interface Panel

PLOA data is removed from Network Interface tab (as compared to AAL1 Network Interface panel)

15.5.2.4.3 GUI usage and implications

15.5.2.4.4 GUI size

Table 6 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
BandwidthGige View	1	1	

Table 6 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory

15.5.2.5 GUI name: VLAN

15.5.2.5.1 Functional description

The user will be able to view the VLAN provisioning data from 'VLAN provisioning' view in the shelf view as shown in the figure. There are totally four VLAN IDs in SN08 release. The user will be able to change the priority and peak rate for VLANs. The VLAN details will be displayed as shown in the figure.

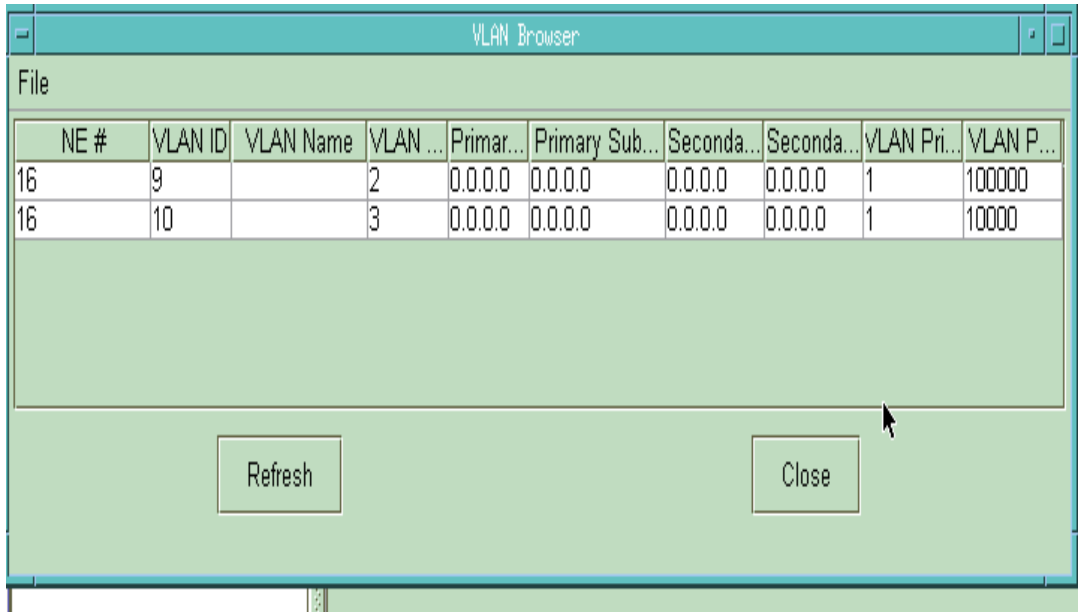
Figure 12 VLAN information

The screenshot displays the 'NE-160 Vlan Manager' window. The title bar includes a window icon, the text 'NE-160 Vlan Manager', and standard window control buttons (minimize, maximize, close). Below the title bar, the text 'MG9000' is visible. The main content area is titled 'Vlan Data' and contains a list of configuration parameters, each with a corresponding input field:

- VLAN_ID: 5
- VLAN_NAME: man9
- VLAN_TYPE: OAMP
- PRIORITY: 5
- PEAK_RATE: 900
- PRIM_SUBNET_ADDR: 0.0.0.0
- PRIM_SUBNET_MASK: 0.0.0.0
- SEC_SUBNET_ADD: 0.0.0.0
- SEC_SUBNET_MASK: 0.0.0.0

At the bottom of the window, there are three buttons: 'Refresh', 'Apply', and 'Close'.

Figure 13 Vlan browser



15.5.2.5.2 GUI usage and implications

15.5.2.5.3 GUI size

Table 7 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
VLAN	1	1	
VlanBrowserView	1	1	

15.5.2.5.4 GUI fields

The GUI fields for the VLAN View

Table 8 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
vlanId	New	-	-	Port Vlan id each port belongs to a VLAN	?
peakRate	New	-	-	Peak Rate for the VLAN id	nnGLinkVlanPeakRate

Table 8 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
priority	New	-	-	Priority of the VLAN	nnGLinkVlanUserPriority
Primary IP Address	New	-	-	Primary subnet address of the VLAN	nnGLinkVlanPrimarySubnetAddr
Primary Subnet Mask	New	-	-	Primary Subnet mask of the VLAN	nnGLinkVlanPrimarySubnetMask
Secondary IP Address	New	-	-	Secondary subnet address of the VLAN	nnGLinkVlanSecondarySubnetAddr

15.5.2.6 GUI name: Performance Browser

15.5.2.6.1 Functional description

The GigE feature introduces Generic OM, Ethernet OM, RMON and PM data. The SMON data related to VLAN is also displayed in the performance browser. The performance details are as shown in the following figures. The mib details are covered under PF section.

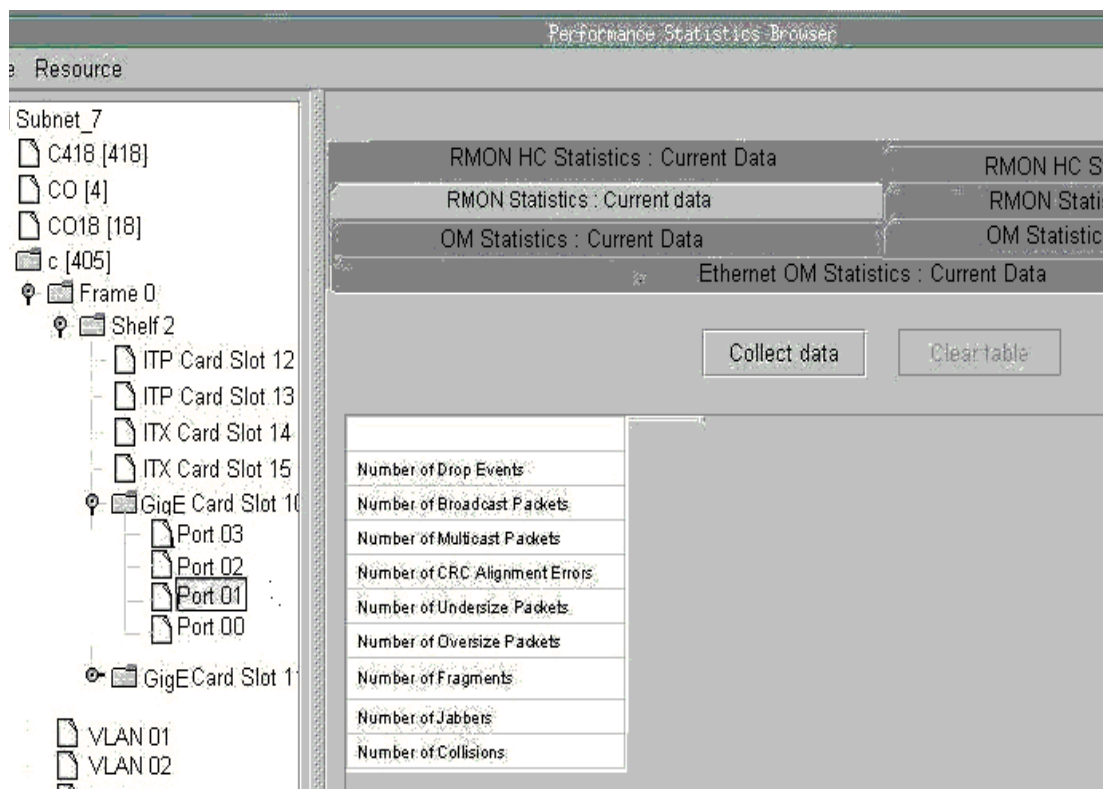
Figure 14 RMON data

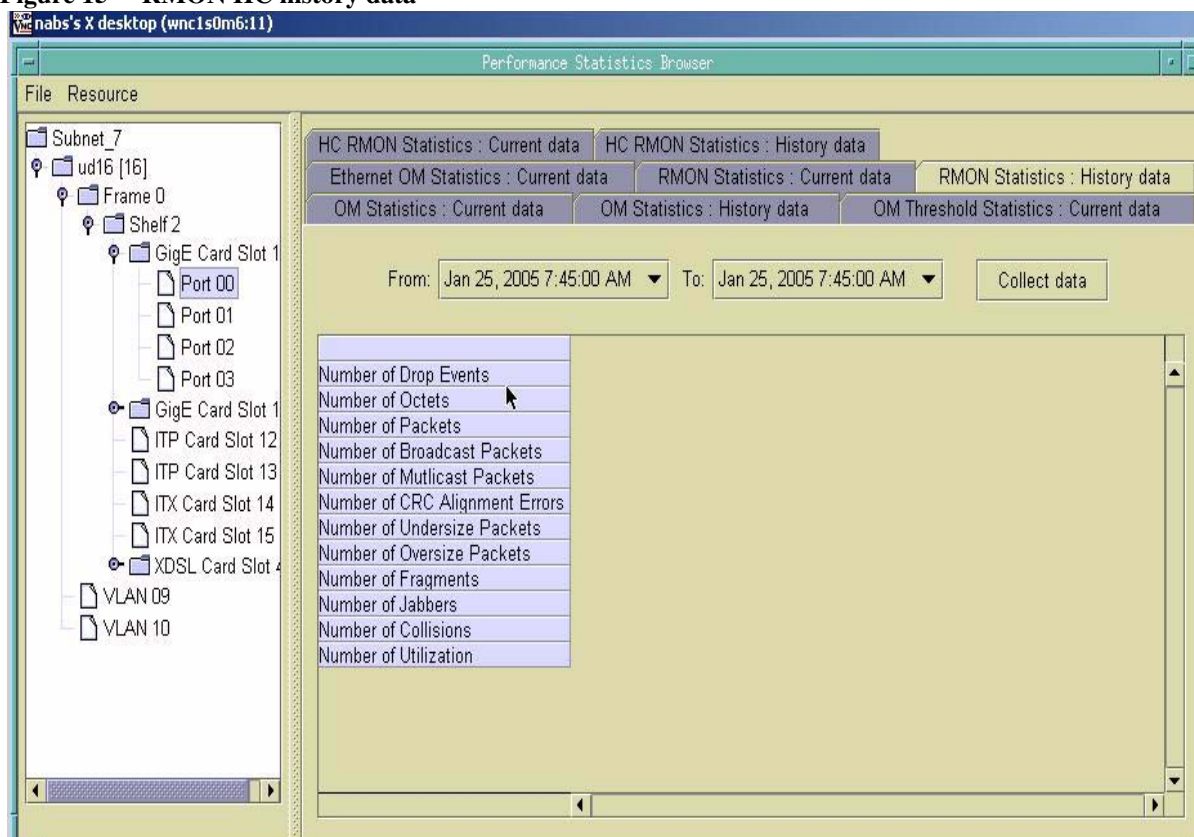
Figure 15 RMON HC history data

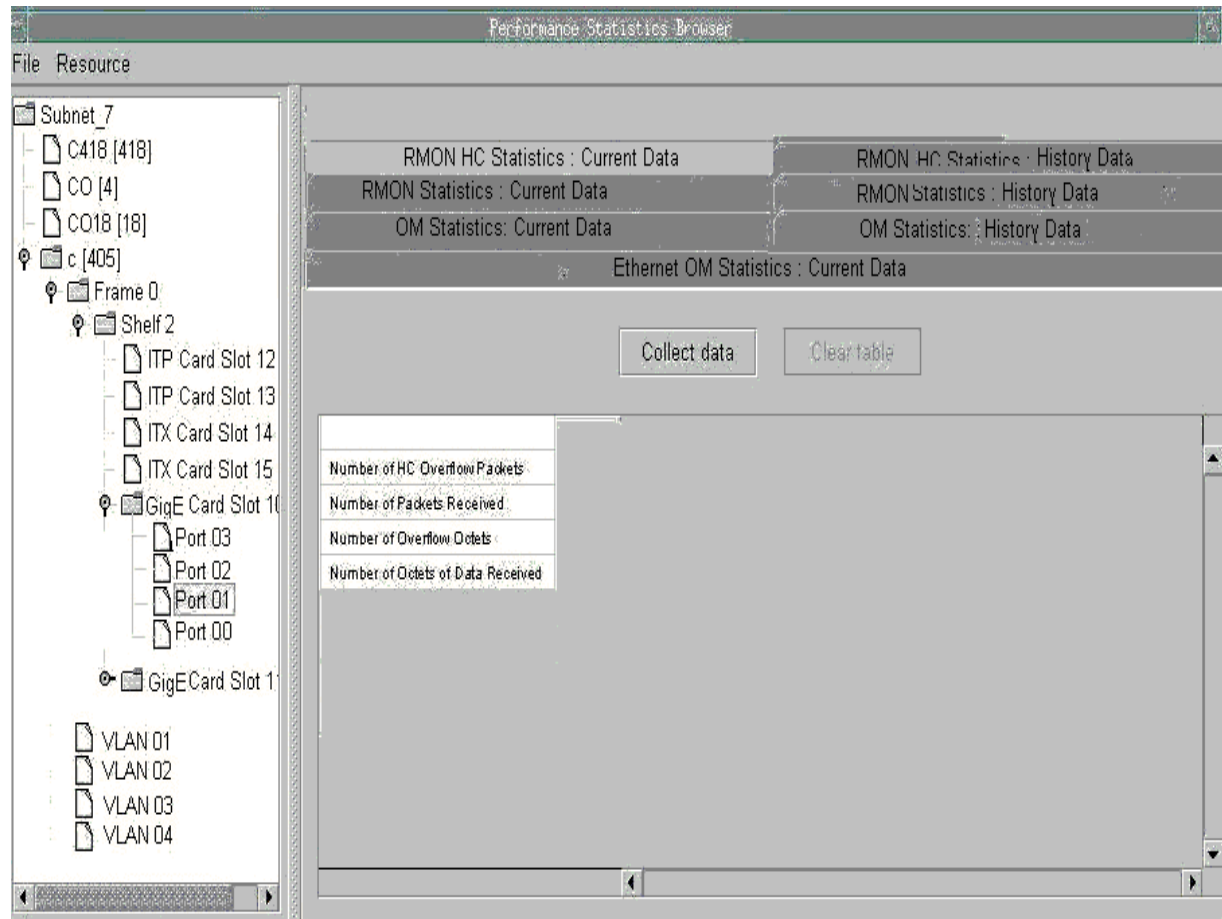
Figure 16 RMON HC current data

Figure 17 Ethernet OM Data

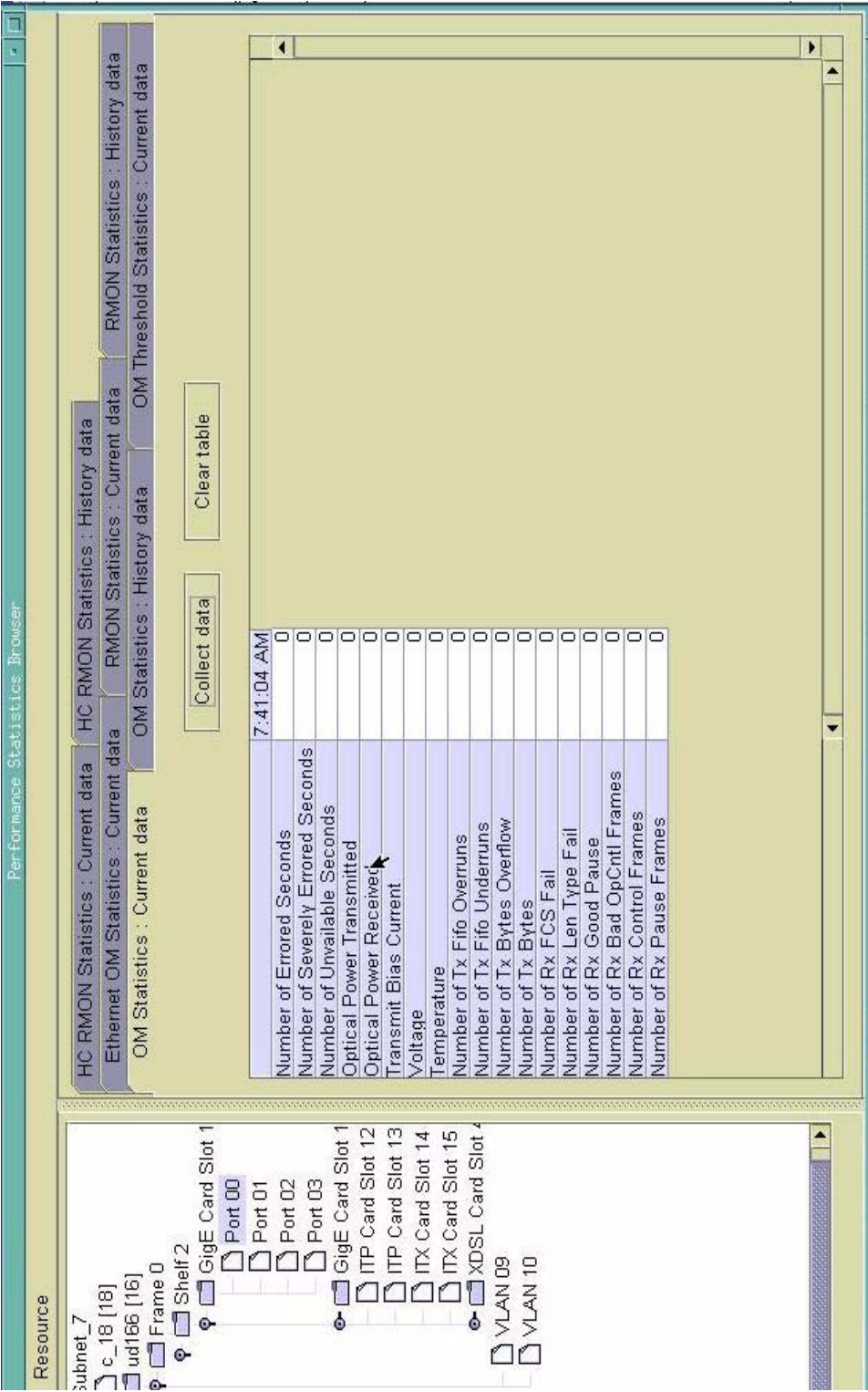


Figure 18 Generic OM/PM Data

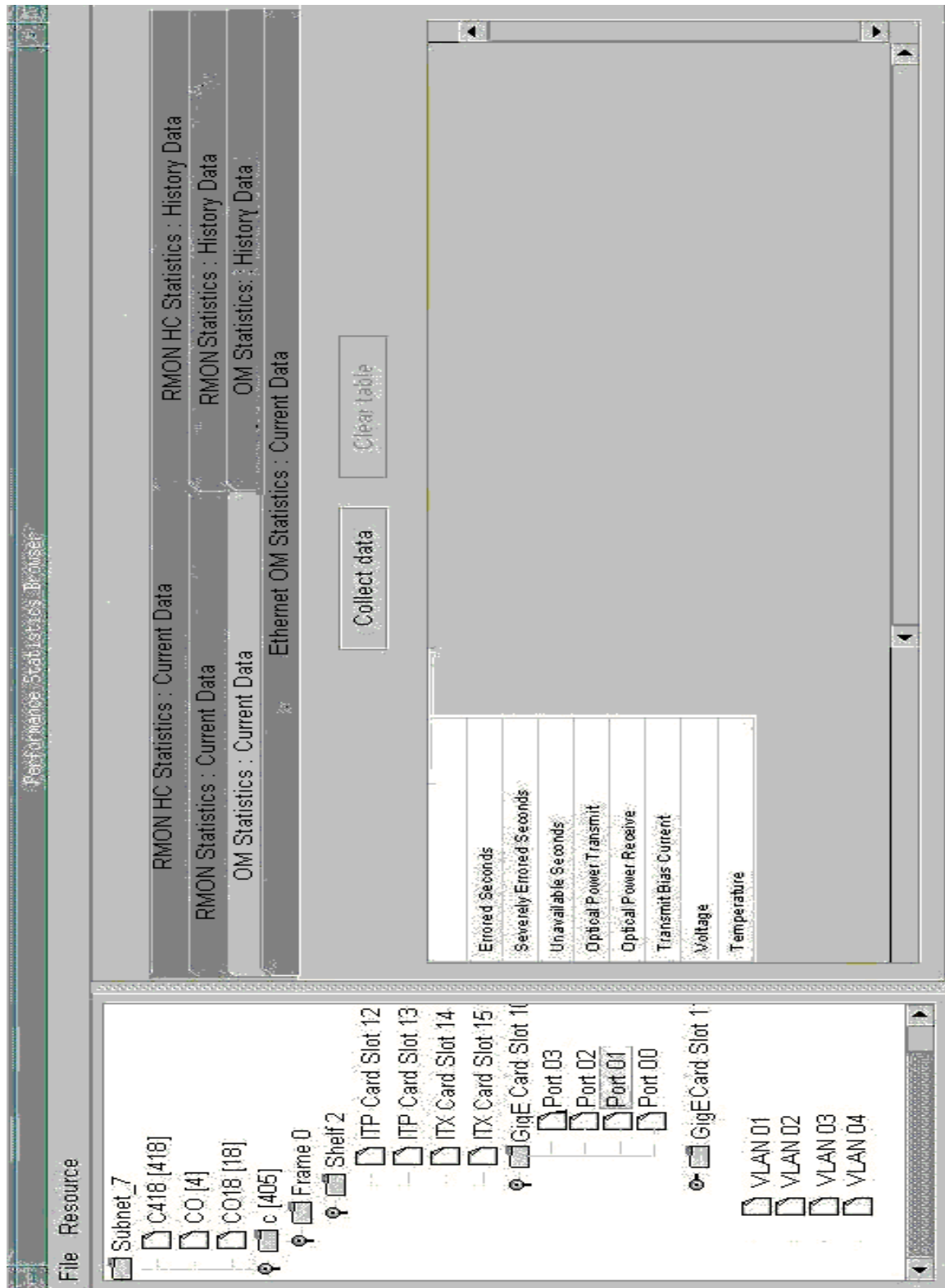


Figure 19 SMON VLAN Statistics

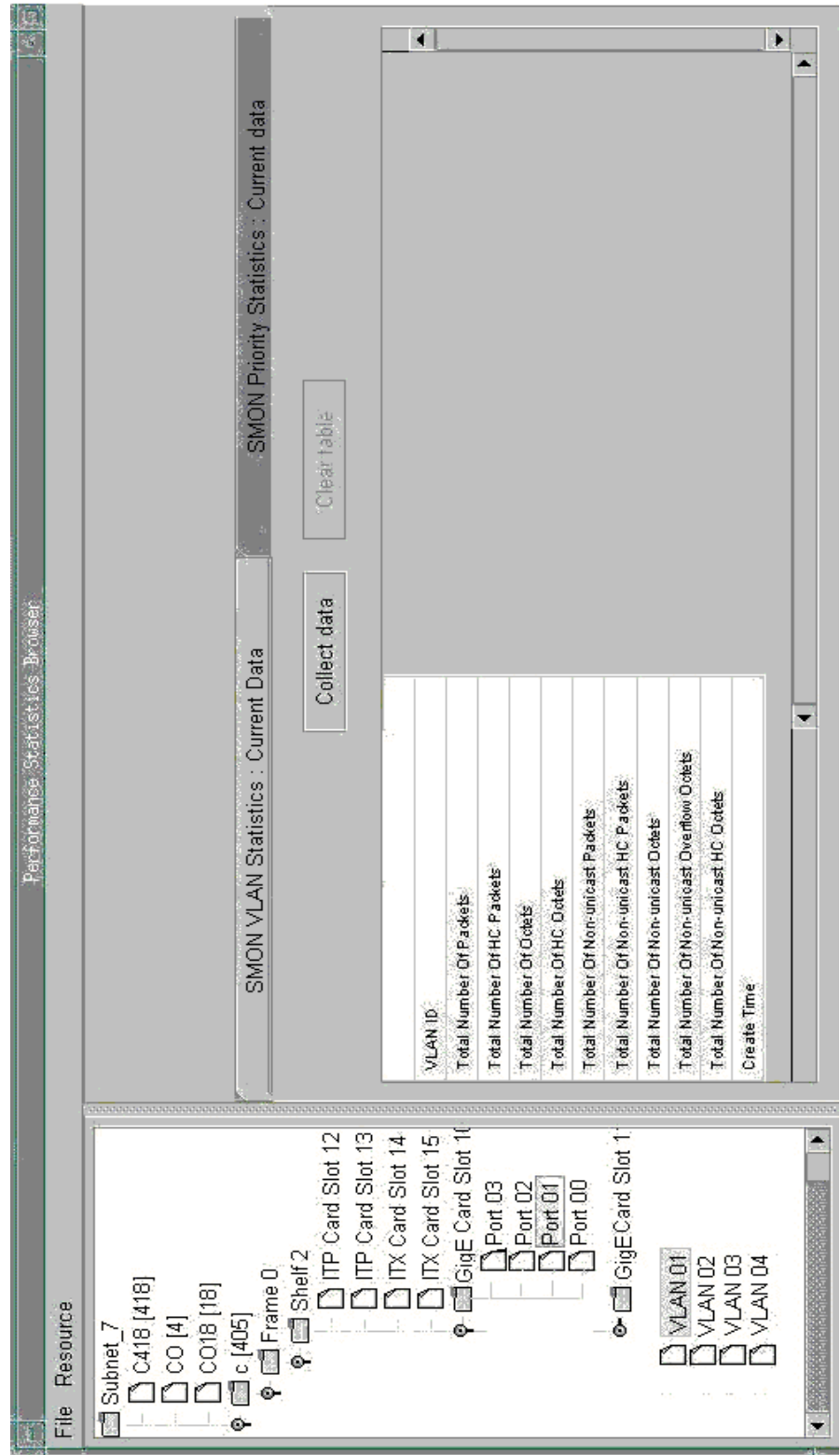


Table 9 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Performance Browser	1	1	

15.5.2.6.2 GUI fields

The GUI fields for the VLAN View.

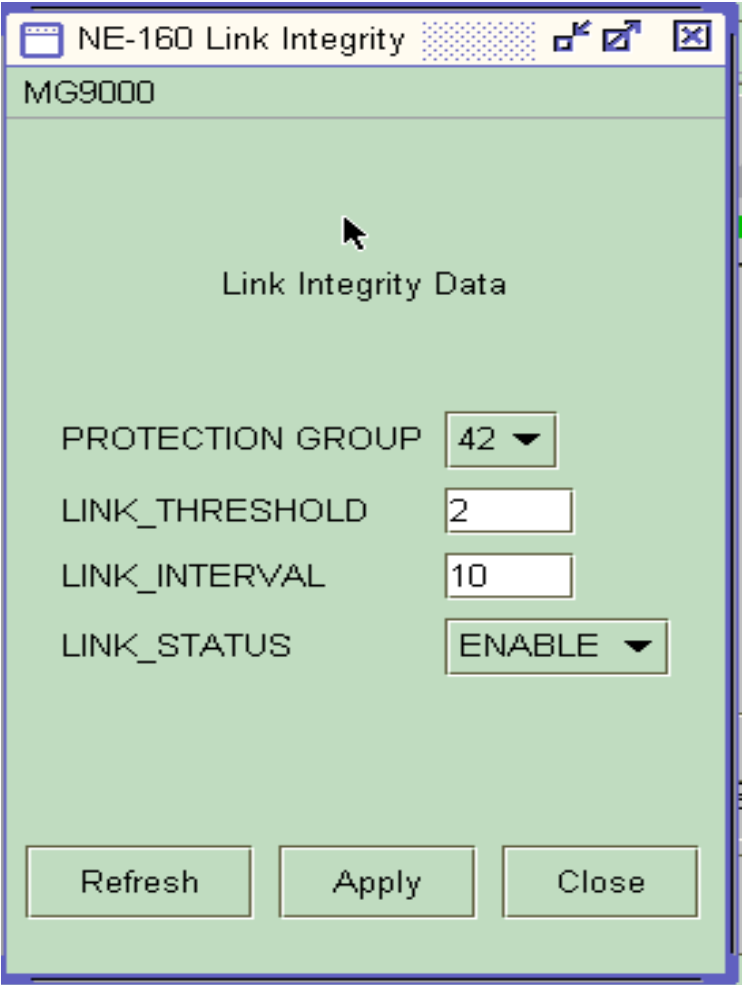
Table 10 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Generic OM -	New	-	-		IF-MIB (current and interval table)
Ethernet PM	New	-	-		dot3HCStatsTable (current and interval table)
Ethernet OM	New	-	-		dot3statEnrty (current and interval table)
SMON	New	-	-		smonPrioStatsTable, smonVlanIdStatsTable
RMON	New	-	-		etherHistoryTable, etherStatsTable

15.5.2.7 GUI name: Link Integrity**15.5.2.7.1 Functional description**

The Link Integrity test can be invoked from the shelfview Maintenance submenu 'Link Integrity View'. The link integrity test will be run on a protection group. The details as shown in the figure are displayed. The user should specify the threshold, and threshold interval. If the user does not specify any value, default values will be taken. The link integrity test can be enabled or disabled using integrity monitoring field in the Link Integrity Monitoring View. The test will run every interval specified in the view. If the threshold crosses, an Link Integrity alarm will be raised. If there are no protection groups created, it gives a message that "The Link protection information is provisioned yet".

Figure 20 Link Integrity view



15.5.2.7.2 GUI usage and implications

15.5.2.7.3 GUI size

Table 11 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
LinkIntegrity	1	1	

15.5.2.7.4 GUI fields

The GUI fields for the VLAN View

Table 12 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Protection Group	New	-	-	Protection Group	nnGLinkProtGrpNum
Integrity threshold	New	-	-	threshold	nnGLinkProtGrpIntegThreshold
Integrity Interval	New	-	-	Interval for the test to run	nnGLinkProtGrpIntegIntervalty
Integrity Monitoring	New	-	-	yes or no	nnGLinkProtGrpIntegEnable

16: A00007071 Configuration (CN)

16.1 Feature name

SN08 3rd Party GW Interop Profiles

16.2 Hardware and Software Requirements

The typical Succession hardware needs to be in place and functional prior to exercising the software provided by this feature. Some related specifics are:

Hardware requirements:

- CORE - available on the XACore (powerpc processor) or SuperNode (88k processor). Not available on the 68k processor or NT40 CNs.

Software requirements:

- CMT - SN08 release or later
- GWC - SN08 release or later
- CORE - SN08 release or later

16.3 Initial Configuration

As a provisioning component of the Succession program, much of this functionality performs as designed with the “typical” hardware being in place. The software loads mentioned above should be installed.

Once the hardware/software is installed and brought into service, the software for this feature is available. Now the ability to provision third party gateways is possible.

16.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

16.5 Upgrade Impact

16.5.1 Dump and Restore (CM)

CORE - No impact to DUMP and Restore mechanisms. This data is preserved via the existing TabXfr mechanism available to all Core Table Control tables.

16.5.2 Element Management Upgrade

This activity will affect CMT data profiles that were previously created prior to the SN08 release. Existing profiles have the potential to have multiple protocols assigned to the same profile. This activity will modify these profiles so that a separate and unique profile is listed for each protocol. This modification is performed during installation of the SN08 software and there is no requirement for users to take any action to realize these changes. The

following list of profiles are converted and list the new name and unique protocol assigned:

- NUERA_GX
 - NUERA_GX_ASPEN
 - NUERA_GX_MEGACO
- PVG_7K
 - PVG_7K_ASPEN
 - PVG_7K_MEGACO
- PVG15K
 - PVG15K_ASPEN
 - PVG15K_MEGACO
- PVG15K_1000
 - PVG15K_1000_ASPEN
 - PVG15K_1000_MEGACO
- PVG15K_PARTIAL
 - PVG15K_PARTIAL_ASPEN
 - PVG15K_PARTIAL_MEGACO
- PVG_VSP3
 - PVG_VSP3_ASPEN
 - PVG_VSP3_MEGACO
- PVG_APG_VSP3
 - PVG_APG_VSP3_ASPEN
 - PVG_APG_VSP3_MEGACO
- PVG_APG
 - PVG_APG_ASPEN
 - PVG_APG_MEGACO

16.5.3 Downgrade impact

CORE - From the Core's perspective, there exists two scenarios:

1. Using the existing AbortSwact mechanism, only valid while the Core is still in split mode but after the Swact.

If 3rd party gateways were not provisioned, then no problems using the AbortSwact mechanism. However, if 3rd party gateways were provisioned, then the preswact check for the AbortSwact procedure will fail because new Lgrp nodes have been provision on the “new side” which

does not exist on the “old side”. To correct this condition the user is required to match up the “old” and “new” sides. This can be accomplished one of two ways:

- a. delete any newly provisioned 3rd party gateways on the “new side”
 - b. add these 3rd party gateways to the “old side”
2. Sync-ing the Core - assuming the Core is still in split mode and a Swact has not occurred.

This is the simpler case, no new provisioning of 3rd party gateways have occurred due to the fact the Swact has not occurred. So just sync the switch. There is no impact for this case.

CMT - Downgrades of the CMT are accomplished by reinstalling the desired release of software and importing the Oracle data base data that was saved against that version. This activity has not affected current downgrade procedures.

16.6 Data schema (DS) (CM, MIBS, RDB)

16.6.1 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)
LGRPINV	Changed	Unchanged

16.6.2 Table LGRPINV Database Schema information

16.6.2.1 Name: LGRPINV

Long table name: Logical GRoup INventory

16.6.2.1.1 Functional description

Table LGRPINV is where Logical Groups (Lgrps) are provisioned. Generally speaking Logical Groups are the Cores representation of gateway line concentrating devices (gateway LCDs).

This feature will provide:

- new value for existing field GRPTYPE
- the new optional field, GTWYKEY, will be visible not provisionable.

16.6.2.1.2 Usage sequence and implications (CM Only)

No change to the current datafill sequence, this is Table LGRPINV:

- must be datafilled after table SERVRINV. Table SERVRINV is where the gateway controllers are provisioned.
- must be datafilled prior to table LNINV. Table LNINV is where LENs for this Lgrp are provisioned.

16.6.2.1.3 Size

No change in the maximum number of tuples for table LGRPINV

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LGRPINV	0	1000	Memory is automatically allocated in increments of 20 LCDs at a time up to 1000.

16.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for LGRPINV.

Table 3 Table field descriptions for LGRPINV

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GRPTYPE	Changed	Added new value to existing field	GRPTYPE	This field specifies the type of Logical group: {S,M,C, LL_3rdpty }
LGRPOPTS	Changed	Added new refinement, GTWYKEY - identifies the hosting gateway	GTWY_TY PE	This field specifies the type of gateway: {NLGW,ABI,CICM,GW,ITP,PVG,UAS}
			GTWY_NO	This field specifies a unique gateway of a certain gateway type: Integer {0 TO 9999}

16.6.2.1.5 Datafill example

The following example illustrates the prompting sequence for the new value for GRPTYPE and new GTWYKEY option in table LGRPINV.

Figure 1 Prompting sequence for GRPTYPE and option Gateway Key

```

>table lgrpinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LGRPINV
>add cary 1 0 gwc 1
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
GRPTYPE:
>LL_3RDPTY
LGRPOPTS:
>gtwykey
GTWY_TYPE:
>ITP
GTWY_NO:
>2
LGRPOPTS:
>$

```

Figure 2 on page 1536 shows the changes to the GRPTYPE and LGRPOPTS fields with field ranges.

Figure 2 Range Values for new GRPTYPE and optional Gateway Key

```

>table lgrpinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LGRPINV
>ran 3
3 GRPTYPE          LGRP_TYPE
TYPE IS LGRP_TYPE {S,M,C, LL_3RDPTY}
>
>ran LGRPOPTS
4 LGRPOPTS          LGRPINV_OPT_ATTR_VECTOR
TYPE IS LGRPINV_OPT_ATTR_VECTOR VECTOR OF UP TO 3 MULTIPLES WITH
LGRPOPTS           {MTSTAPT,LGRPLOC,GTWYKEY} REFINEMENTS:
{MTSTAPT}           MULTIPLE WITH
SITE_NAME           TABLE OF 4 CHAR'S
VERT_INFO           VECTOR OF UP TO 8 MULTIPLES WITH
VERT_NO             {0 TO 1023}
MTAPTNO             {0 TO 48}
{LGRPLOC}           MULTIPLE WITH
FRAME_TYPE          FRAME_NAME
FLOOR_POSITION      {0 TO 99}
ROW_POSITION        ROW_POS
FRAME_POSITION      {0 TO 99}
SHELF_POSITION      {0 TO 77}
{GTWYKEY}           MULTIPLE WITH
GTWY_TYPE          {NLGW,ABI,CICM,GW,ITP,PVG,UAS}
GTWY_NO           {0-1023}

```

Figure 3 on page 1537 provides a view of a successfully added tuple with the new GRPTYPE field and optional Gateway data.

Figure 3 Sample LGRPINV Tuple with new GRPTYPE and option Gateway Key

```

>table lgrpinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LGRPINV
pos lg 1 0
GRPNO SRVRNAME GRPTYPE LGRPOPTS
-----
CARY 01 0 GWC 1 LL_3RDPTY GTWYKEY ITP 2 $

```

16.6.2.1.6 Table release history update

SN08 Feature A00007071:

Modified field: LGRPOPTS

- adding a new GTWYKEY refinement. For more information see “Table field descriptions for LGRPINV” on page 1535.

16.6.2.1.7 Supplementary information

Limitations:

- The new optional field, GTWYKEY, is only visible not provisionable in SN08.

16.6.2.1.8 Translation verification and other tools

Table LGRPINV does not impact translations. Therefore TABAUDIT is the tool used to verify the contents of table LGRPINV. The following Figure 4 on page 1538 shows the output from TABAUDIT when it is used to verify Table LGRPINV.

Figure 4 Sample Tabaudit output for Verifying LGRPINV Table Datafill

```

>tabaudit
TABAUDIT:
>include lgrpinv

>execute
-----
|          TABAUDIT STATUS          |
-----

The following tables are included:
table LGRPINV (300)

The following tables are excluded:
  From table VERSIONS (0)           to table SERVINV (90).
  From table MGCINV (92)           to table IPINV (299).
  From table X75INFO (301)        to table INWATNPA (1426).

Please confirm ("YES", "Y", "NO", or "N"):
>yes
Creating TABAUDIT summaryfile: SUMMARY$MAP on SFDEV.
Starting DMS data verification ...
Table LGRPINV: New table control.
  Completed tuple checking.
  SUMMARY: Tbl LGRPINV: tuples checked 26, passed 26, failed 0.
Data verification is completed.

```

16.7 Service Orders (SO) (CM & SESM)

N/A

16.8 Software optionality control (SOC)

N/A

16.9 Element Management

16.9.1 New/modified GUIs

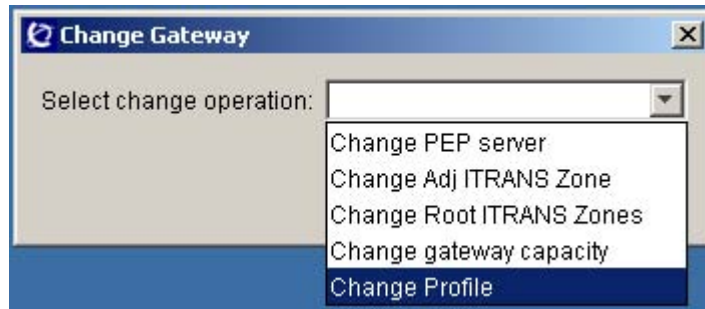
Table 4 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Change GW	Changed

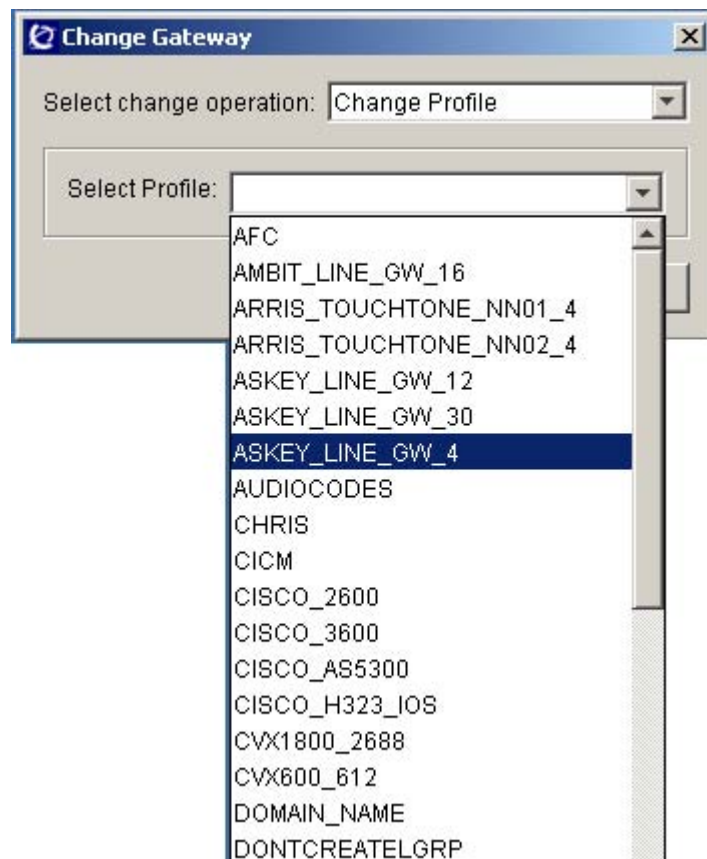
16.9.2 GUI information

This activity updates the Change Gateway GUI with a new item in the “pick” list as shown below.

16.9.2.1 GUI name: Change Gateway (Profile)



16.9.2.2 GUI name: Change Gateway (Profile) expansion



16.9.2.2.1 Functional description

The Change GW dialog is displayed by selecting one or more GWs when in the Provisioning/Gateways Panel of the CMT GUI. This activity adds the "Change gateway profile" item to the pick list of changeable attributes.

Changing a GW from one profile to another is not an operation that is supported for all of the certificate fields, and some fields can only be changed under certain conditions (e.g., you cannot reduce the maximum number of endpoints below the number of endpoints already allocated to the Gateway). A pre-condition for being able to change a GWs profile is that the Compatible Profiles field is set for the profile being changed to. In other words, if you are changing a GW from profile A to profile B, the profile B's "Compatible Profiles" field must have profile A in its list.

Changing a GW to a different profile is a potentially risky operation. Interop personnel should test thoroughly prior to creating a Certificate with the Compatible Profiles field set to a profile other than itself. While some error checking is performed, it is the responsibility of the Certificate creator to make the final decisions concerning if one profile is truly compatible with another.

The user has the ability to change (with limitations) a profile assigned to a Gateway with the following attributes having different values:

- Maximum Endpoints
- Supported Protocol
- Reserve Terminal Mandatory
- Display Physical Location
- Compatible Profiles
- Gateway Name Format
- Endpoint Name Format

16.9.2.2.2 GUI usage and implications

The Change GW Profiles transaction should be used when a user wants to move a GW from one profile to another. Note that this is the supported method for changing profiles. In contrast, changing the certificate file to realize profile changes is not supported.

16.10 User Interface

16.10.1 Defining GW Profiles Using XML Schema's and Certificates

A profile is the method used by the Nortel Succession products to describe certain behaviors of a GW. With the introduction of this activity, two categories of profiles are defined for use by customers; Nortel profiles and Third Party profiles. Both categories use certificate files to describe their attributes. As previously mentioned, a certificate is an XML document used to uniquely describe all of the behaviors of one profile. Certificate files are made available to the system by existence in the certificate directories. The name given to the certificate file is the unique identifier for the profile. For example, a certificate file named "UAS.certificate" defines that a UAS profile exists. Using the "certificate" extension is mandatory for all profiles. Details concerning the certificate directories are described in subsequent sections of this document.

The Nortel defined certificates are built into CMT software and are automatically populated in the "Nortel" certificate directory. These profiles are not user modifiable. Because these profiles are built into the Nortel CMT package, they are immediately available for use when the CMT is upgraded to the SN08 release. Availability means that the profile is selectable from the CMT Associate GW GUI and as a profile field value when using the OSSGate Associate GW interface.

Third party certificates are defined and created by Nortel Interop personnel. These profiles are flexible within the bounds of predefined fields and values. In other words, the current set of behaviors is made available to users by defining an XML document, referred to as a "Certificate", that dictate the features that are appropriate for the GW in question. In subsequent sections of this document, these fields and values are described in detail.

16.10.1.1 Profile Field Definitions and Values

The following list of GW attributes are made available in the SN08 release and are user definable. Some attributes are obvious concerning their impact, and others, less so. A detailed description of each attribute is provided in the following sections. Where applicable, a GUI capture of the fields affected is listed.

- Maximum Endpoints
- Category
- EndpointType
- GenerateLGRP
- ResvTermMandatory
- ChangeIPAvailable

- DispPhyLocation
- InventroyRole
- InventoryType
- SupportedProtocol
- GWCPProfileNumber
- EPIDGenDesc
- ServiceTypeList
- CompatibleGWProfile
- BearerFormatList
- GatewayNameFormatList
- EndpointNameFormatList

Note: For some of the field descriptions below datafill values are listed. These values are included as an aid to understanding and may not accurately reflect actual allowed values. For specifics concerning acceptable field values refer to the schema definition where the CMT application is installed at directory location /opt/nortel/NTsesm/xsd/certificateif.

16.10.1.1.1 MaxEndpoints Field

The maximum endpoints field is used to limit the number of EPs that can be assigned to a GW. For most GWs, this field is used as the default value if the user chooses to omit this value. If a user tries to populate more EPs then this field is set for on a GW, then software restrictions will kick in and disallow the operation.

16.10.1.1.2 Category Field The category field is a field that dictates endpoint lookup algorithms used in the GWC device. Different endpoint lookup algorithms are used for efficiency. Four categories are available:

- small - This category should be used for GWs with small capacities, 31 or less is suggested.
- large - This category should be used for GWs with large capacities, more than 31 endpoints is suggested.
- audio - This category is a special purpose category used with audio GWs. These GWs use pools of endpoints.
- APG - This is another special purpose category used for APG GWs. It uses virtual TID space that have unique mapping.

Although datafill for this field is defined as enumerated types, these types are mapped to integers and stored with the representation listed below in the

database. The following list of mappings is provided for informational purposes only and is subject to change.

Table 5 Category Mappings

Element Value	Database Value
large	1
small	2
audio	3
APG	4

16.10.1.1.3 Endpoint Type Field

The Endpoint Type field determines how endpoints are managed within succession products. This field affects the ability of a GW to pre-provision endpoints and alters where and when endpoints are provisioned. For the CMT product, some settings auto populate endpoints within the database, and subsequently send these endpoints to the GWC. For the XaCore, this field manages which value, “S”, “M”, “C” or the newly introduced “LL_3RDPTY” that is datafilled in LGRPTYPE field of LGRPINV table. For a detailed discussion concerning this field, refer to the Data Schema section of this document.

Although datafill for this field is defined as enumerated types, these types are mapped to integers and stored with the representation listed below in the database. The following list of mappings is provided for informational purposes only and is subject to change.

Table 6 EndpointType Mappings

Element Value	Database Value	Comments
managedLens	1	Line GWs with managed LGRPs
ue9000Lens	2	UE9000 GW unique processing
cicmLens	3	CICM GW unique processing
carrierTrksGwcNN	4	Trunks, no LGRPs
carrierTrksSubNN	5	Trunks, no LGRPs
nocarrierTrkGwcNN	6	H.323 GWs
asynchronousBridgingInterface	7	ABI
thirdPartyLens	8	Large Line Third Party unique processing

16.10.1.1.4 Generate LGRP Field

The LGRP Generation field is included to dictate whether a new LGRP is created when a GW with the profile in question is associated. This field is applicable to Nortel and Third Party line GWs that allow the system to manage TID allocation. This ability has been added with the introduction of this feature. For example, pre-SN08 small line GWs with a category of small would only allocate a new LGRP when an existing LGRP was not available with capacity for the new GW that was being added. Category large profiles would always add a new LGRP upon GW creation. This functionality is altered in SN08 so that the decision of whether a new LGRP is created or not is dictated by this newly introduced field, "LGRP Generation". Indicating "true" for this field means that a GW that is added will cause a new LGRP to be created. "false", indicates to use existing LGRPs if one exists that still has capacity. Indicating that a new LGRP is created should be taken with caution due to the limited number of LCD nodes available on the XaCore. For a discussion of XaCore LCD nodes, refer to the NTPs.

16.10.1.1.5 Reserved Terminations Mandatory Field

This certificate field is used to dictate the behavior concerning the Associate GW "reserved terminations" value. If this field is left blank in the client, then server behavior is to default this value to the maximum reserved termination value defined in certificate field value "Maximum Endpoints". For some GWs, it is mandatory that the customer specify this value. In other words, setting the Reserved Terminations Mandatory field to "true" in the certificate forces the user to specify a reserved terminations client value and the system default will not be used. This is enforced by not turning the OK button on at the GUI and by rejecting the command if the OSSGate Associate GW Maximum Termination field is not included. Currently, only GW's using the H.323 protocol use this restriction and this certificate field is typically be set to "false" for all other GW types.

Figure 5 GUI fields affected by Rsvd Terms Mandatory Field

16.10.1.1.6 Change IP Available Field

This certificate field is used to dictate the behavior concerning the “pick” list for the GUI operation change GW. If this certificate element is set to “false”, then the “Change gateway IP address” pick is removed from the list of changeable attributes. As of SN08, only H.323 GWs support the change GW IP functionality.

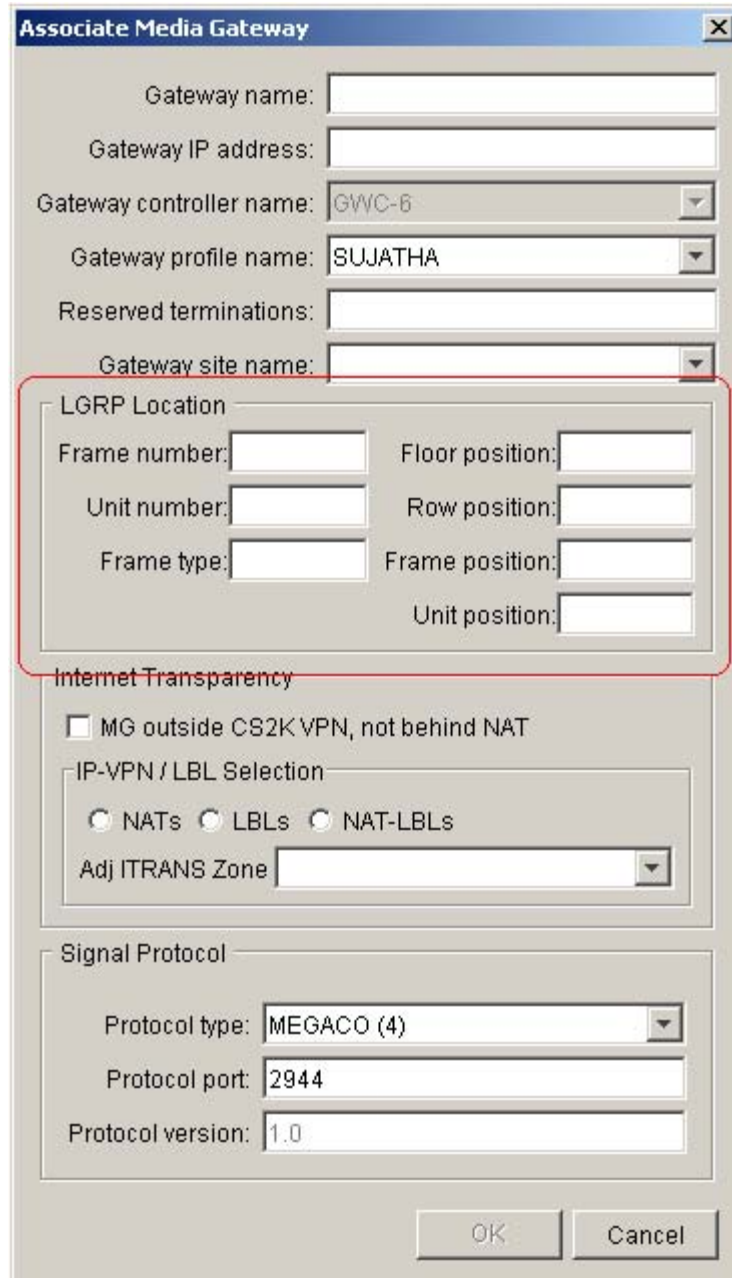
Figure 6 Change Gateway IP Pick Affected

16.10.1.1.7 Display Physical Location

The Display Physical Location field is used to indicate that additional fields should be datafilled in the Associate Media Gateway GUI. These fields are

used to populate specific LGRP and LEN information. Currently, these fields are unique to the Third Party Large Line and CICM profiles only. For a detailed discussion concerning this topic, refer to SN08 activity Third Party Gateway Provisioning (A00007072).

Figure 7 Associate Media Gateway Dialog



The image shows a Windows-style dialog box titled "Associate Media Gateway". It contains several input fields and sections. A red rectangle highlights the "LGRP Location" section, which includes fields for Frame number, Floor position, Unit number, Row position, Frame type, Frame position, and Unit position. Below this is the "Internet Transparency" section with a checkbox for "MG outside CS2K VPN, not behind NAT", a radio button group for "IP-VPN / LBL Selection" (NATs, LBLs, NAT-LBLs), and a dropdown for "Adj ITRANS Zone". The "Signal Protocol" section at the bottom has dropdowns for "Protocol type" (set to MEGACO (4)), "Protocol port" (set to 2944), and "Protocol version" (set to 1.0). "OK" and "Cancel" buttons are at the bottom right.

Field	Value
Gateway name:	
Gateway IP address:	
Gateway controller name:	GWC-6
Gateway profile name:	SUJATHA
Reserved terminations:	
Gateway site name:	
LGRP Location	
Frame number:	
Floor position:	
Unit number:	
Row position:	
Frame type:	
Frame position:	
Unit position:	
Internet Transparency	
MG outside CS2K VPN, not behind NAT	☐
IP-VPN / LBL Selection	☐ NATs ☐ LBLs ☐ NAT-LBLs
Adj ITRANS Zone	
Signal Protocol	
Protocol type:	MEGACO (4)
Protocol port:	2944
Protocol version:	1.0

16.10.1.1.8 Inventory Role Field

The Inventory Role field dictates the expected use of the GW. Currently, only the “Media GW” role has been defined, but, other uses may be defined for future deliveries.

16.10.1.1.9 Inventory Type Field

The inventory type field is similar to the Endpoint Type field in that it affects how endpoints are provisioned. Unique behavior is associated with the different values available. This behavior affects generation of LGRPs for lines or trunk behaviors for trunks. The following list is available for datafill in SN08.

Table 7 Datafill Values for Inventory Type Field

DEFINED VALUES
Large Trunk Gateway
H.323 Gateway
Audio Server
Large Line Gateway
Small Line Gateway
Audio Server
CICM
UE9000MG
Third Party

16.10.1.1.10 Maximum Endpoints Field

As the name implies, the Maximum Endpoint field is a field that dictates the maximum number of endpoints that can be added to a GW. In theory, this field should be less than or equal to the maximum number of endpoints that can be assigned to the GWC it is intended to be provisioned for. Because the profile type for the GWC assignment is not know, range error checking for this field is not performed and it is the responsibility of the certificate creator to assign this field with an appropriate value. For example, if this field is assigned the value of 2000, and the GWC that will use it can only support 1000 endpoints, an error condition would be realized if the user datafilled 2000 in the “reserved terminations” field for the Associate GW operation. This is because the GWCs capacity is overrun. In some situations, this may be deemed appropriate if the GWs capacity is truly 2000. The user has the option of associating the GW with a reserved capacity of less than the value assigned to this certificate field. The screen captures below show the affected fields.

Figure 8 Associate Media GW Reserved Terminations

Associate Media Gateway

Gateway name:

Gateway IP address:

Gateway controller name:

Gateway profile name:

Reserved terminations:

Signal Protocol

Protocol type:

Protocol port:

Protocol version:

OK Cancel

Figure 9 H.323 GWC Profile Port Capacity

Profile

Current: H.323_NA

Capability	Capacity	Units
Large Gateways	300	gateways
IP Security	NA	NA
H.323	1032	ports

16.10.1.1.11 Supported Protocol Field

As the name implies, the supported profile field is used to define the protocol associated with this profile. Prior to SN08, multiple protocols were available within a profile. This functionality has been altered so that a profile and protocol has a 1 to 1 correspondence. If a GW supports multiple protocols, then a unique certificate should be created for each protocol supported. Profiles that supported multiple protocols prior to the SN08 release have been modified to conform to this behavior. For example, the PVG_7K profile has been expanded in the SN08 release and is listed as PVG_7K_ASPEN and PVG_7K_MEGACO.

Although datafile for this field is defined as enumerated types, these types are mapped to integers and stored with the representation listed below in the database. The following list of mappings is provided for informational purposes only and is subject to change.

Table 8 Protocol Mappings

Element Value	Database Value
NCS_PROTOCOL	1
ASPEN	2
DSM-CC	3
MEGACO	4
MGCP	5
TGCP	6
H.323	11

16.10.1.1.12 GWC Profile Number Field

The GWC Profile Number field is a field used in the GWC device that dictates the behavior of the GWC. The number sent to the GWC is associated with a unique series of flags in the GWC. These flags instruct the GWC on specific actions to use in the GWC device. For any 3rd party certificate creation, one of the “spare” profiles created for this activity should be used. For details concerning which number should be used, please contact GWC Persistent Data architects and designers.

The following table shows the range of “spare” profile numbers.

Table 9 Profile numbers and reference gateways

Profile numbers	Reference gateways
100 - 124	Arris MTA
125 - 149	Motorola MTA
150 - 174	Generic MTA
175 - 224	IAD
225 - 249	UE9000
250 - 274	CentrexIP Client Manager
275 - 299	MG9000
300 - 324	ABI
325 - 349	PVG
350 - 374	CVX
375 - 399	AudioCodes PRI
400 - 424	Upgrade PVG
425 - 449	Nuera trunking GW
450 - 474	TGCP
475 - 499	Nortel BCM
500 - 524	Nortel Meridian 1
525 - 549	CISCO 2600 / 3600 / AS5300
550 - 574	Nortel Westell
575 - 599	H.323 proxy gateway

16.10.1.1.13 EPID Generation Field

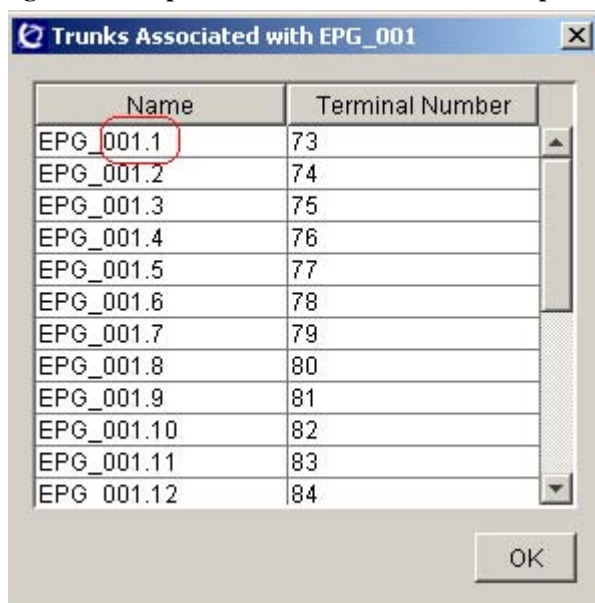
The EPID Generation field is used to describe the behaviors of endpoint groups that are expanded. It dictates properties such as using a “.” or “/” as naming delimiters and other attributes as listed in the table below. An example of H.323 expansion is listed below in the screen shot. This example uses the auto1 expansion. With this expansion, a “.” is used for the delimiter, the numbering starts at 1, and it is not “0” padded.

Table 10 EndpointDesc Mappings

Element Value	Delimiter	Channel Start	Pad Supported
manual		1	N

Table 10 EndpointDesc Mappings

Element Value	Delimiter	Channel Start	Pad Supported
auto1	.	1	N
auto2	.	1	Y
auto3	/	1	N
auto4	/	1	Y
auto5	/	0	N
auto6	/	0	Y
auto7	.	0	N
auto8	.	0	Y

Figure 10 Expansion of a H.323 Carrier Group Using auto01

16.10.1.1.14 Service Type Field

The Service Type field dictates the capabilities of the GW. Some GWs may have multiple capabilities within this list and can be assigned several values. For instance, some gateways have middle box “ITRANS” or “DQOS” abilities in addition to being a “line” GW.

The following table lists the current set of defined Service Type values that can be assigned. Although datafile for this field is defined as enumerated types,

these types are mapped to integers and stored with the representation listed below in the database. The following list of mappings is provided for informational purposes only and is subject to change.

Table 11 ServiceType Mappings

Element Value	Database Value
line	0
trunk	1
audio	2
APG	3
DQOS	4
ITRANS	5
H323	6
ITRANS_ROAM	7

16.10.1.1.15 Compatible Gateway Profile

The compatible GW profile field describes which profiles are compatible with this profile. This field should be set to the name of the profile being defined at a minimum.

16.10.1.1.16 Bearer Fabric Field

The bearer fabric field is an optional field used to dictate the type of network used by GW. Two ATM versions, AAL1 and AAL2, are available and an IP version too. For more information concerning specifics of this field, refer to the Tri-modal provisioning (A00003487) documentation.

16.10.1.1.17 Gateway Name Format Field

The data within this tag is used to define the syntax for the name of the Gateway associated with this certificate/profile. Gateway association/addition will be rejected if the gateway name does not conform to this definition. See section ***NameFormatsType Schema*** for a more complete description of the sub-tags which make up this syntax definition.

16.10.1.1.18 Endpoint Name Format Field

The data within this tag is used to define the syntax for the name of the Endpoints added to a gateway associated with this certificate/profile. No endpoints will be allowed to be created which do not conform to this definition. See section ***NameFormatsType Schema*** for a more complete description of the sub-tags which make up this syntax definition.

16.10.1.2 XML Schema Definitions for Certificates

16.10.1.2.1 Base Certificate Schema

The base certificate schema is used to define a profile. Many of the fields are mandatory, but, a few are optional as indicated by the “minOccurs=”0” terminology. These fields allow users to define a profile’s certificate as described in this document.

```
<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="GenerateLGRP" type="stringBoolean" />
      <xsd:element name="ResvTermMandatory" type="stringBoolean" />
      <xsd:element name="ChangeIPAavailable" type="stringBoolean" />
      <xsd:element name="DispPhyLocation" type="stringBoolean" />
      <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="GatewayNameFormatList" type="nameFormatsType" />
      <xsd:element name="EndpointNameFormatList" type="nameFormatsType" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

</xsd:schema>
```

16.10.1.2.2 CertificateTypes Schema

The Certificate Types Schema is used in conjunction with the certificate schema listed above and defines allowable values for the base certificates values. Typically, an enumerated list of values is listed. However, some elements has ranges of values that can be used or allow a free form string value.

```
<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="250" />
  </xsd:restriction>
</xsd:simpleType>
```

```
</xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="profileNameType">
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="1" />
    <xsd:maxLength value="32" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="stringBoolean">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="true"/>
    <xsd:enumeration value="false"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="maxEndpointsType">
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="0" />
    <xsd:maxInclusive value="4094" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="serviceTypeListType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="line"/>
    <xsd:enumeration value="trunk"/>
    <xsd:enumeration value="audio"/>
    <xsd:enumeration value="APG"/>
    <xsd:enumeration value="DQOS"/>
    <xsd:enumeration value="ITRANS"/>
    <xsd:enumeration value="H323"/>
    <xsd:enumeration value="ITRANS_ROAM"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="categoryType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="niltype"/>
    <xsd:enumeration value="LARGE"/>
    <xsd:enumeration value="SMALL"/>
    <xsd:enumeration value="AUDIO"/>
    <xsd:enumeration value="APG"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="inventoryRoleType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="Media Gateway"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="inventoryTypeType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="Large Trunk Gateway"/>
    <xsd:enumeration value="H.323 Gateway"/>
    <xsd:enumeration value="Audio Server"/>
    <xsd:enumeration value="Large Line Gateway"/>
    <xsd:enumeration value="Small Line Gateway"/>
    <xsd:enumeration value="Audio Server"/>
    <xsd:enumeration value="CICM"/>
    <xsd:enumeration value="UE9000MG"/>
    <xsd:enumeration value="Third Party"/>
  </xsd:restriction>
</xsd:simpleType>
```

```

    </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="EPIDGenDescType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="manual" />
    <xsd:enumeration value="auto1" />
    <xsd:enumeration value="auto2" />
    <xsd:enumeration value="auto3" />
    <xsd:enumeration value="auto4" />
    <xsd:enumeration value="auto5" />
    <xsd:enumeration value="auto6" />
    <xsd:enumeration value="auto7" />
    <xsd:enumeration value="auto8" />
  </xsd:restriction>
</xsd:simpleType>

<!-- PVG to Aspen is currently the only supported profile change -->
<xsd:simpleType name="compatibleGWProfileListType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:complexType name="supportedProtocolType">
  <xsd:sequence>
    <xsd:element name="protocolName" type="protocolType" />
    <xsd:element name="version" type="xsd:decimal" />
  </xsd:sequence>
</xsd:complexType>

<xsd:simpleType name="protocolType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="none" />
    <xsd:enumeration value="ncsprotocol" />
    <xsd:enumeration value="aspen" />
    <xsd:enumeration value="dsmcc" />
    <xsd:enumeration value="megaco" />
    <xsd:enumeration value="mgcp" />
    <xsd:enumeration value="tgcp" />
    <xsd:enumeration value="sipbcpt" />
    <xsd:enumeration value="h323" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="endpointTypeType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="niltype" />
    <xsd:enumeration value="managedLens" />
    <xsd:enumeration value="ue9000Lens" />
    <xsd:enumeration value="cicmLens" />
    <xsd:enumeration value="carrierTrksGwcNN" />
    <xsd:enumeration value="carrierTrksSubNN" />
    <xsd:enumeration value="nocarrierTrkGwcNN" />
    <xsd:enumeration value="thirdPartyLens" />
    <xsd:enumeration value="asynchronousBridgingInterface" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="marketRestrictionListType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="NA" />
    <xsd:enumeration value="International" />
  </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:schema>

```

16.10.1.2.3 NameFormatsType Schema

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema" version="1.0" xml:lang="en" >

<!-- ***** -->
<!-- * Name Format XSD Definition -->
<!-- ***** -->
<xsd:complexType name="nameFormatsType">
  <xsd:sequence>
    <xsd:element name="nameFormat" minOccurs="0" maxOccurs="70">
      <xsd:complexType>
        <xsd:all>
          <xsd:element name="appDataList" type="appDataListType" minOccurs="0"/>
          <xsd:element name="name" type="xsd:token" minOccurs="1"/>
          <xsd:element name="minLength" type="xsd:nonNegativeInteger" minOccurs="0"/>
          <xsd:element name="maxLength" type="xsd:nonNegativeInteger" minOccurs="0"/>
          <xsd:element name="delimiters" type="xsd:string" minOccurs="0"/>
          <xsd:element name="forceDelimiterOrder" type="xsd:string" minOccurs="0"/>
          <xsd:element name="template" type="xsd:string" minOccurs="0"/>
          <xsd:element name="pattern" type="xsd:string" minOccurs="0"/>
          <xsd:element name="minTokens" type="xsd:nonNegativeInteger" minOccurs="0"/>
          <xsd:element name="maxTokens" type="xsd:nonNegativeInteger" minOccurs="0"/>
          <xsd:element name="enabled" type="xsd:boolean" minOccurs="0"/>
          <xsd:element name="tokenFormats" type="tokenFormatsType" minOccurs="0"/>
        </xsd:all>
        <xsd:attribute name="formatKey" type="xsd:token" use="required"/>
        <xsd:attribute name="applyToPattern" type="xsd:string" use="optional"/>
        <xsd:attribute name="enabled" type="xsd:boolean" use="optional"/>
      </xsd:complexType>
    </xsd:element>
  </xsd:sequence>
  <xsd:attribute name="enabled" type="xsd:boolean" use="optional"/>
</xsd:complexType>

<!-- ***** -->
<!-- * Define tokenFormatType -->
<!-- ***** -->
<xsd:complexType name="tokenFormatsType">
  <xsd:sequence>
    <xsd:element name="tokenFormat" minOccurs="0" maxOccurs="40">
      <xsd:complexType>
        <xsd:all>
          <xsd:element name="name" type="xsd:token" minOccurs="0"/>
          <xsd:element name="type" type="tokenType" minOccurs="0"/>
          <xsd:element name="template" type="xsd:string" minOccurs="0"/>
          <xsd:element name="minLength" type="xsd:nonNegativeInteger" minOccurs="0"/>
          <xsd:element name="maxLength" type="xsd:nonNegativeInteger" minOccurs="0"/>
          <xsd:element name="values" type="xsd:string" minOccurs="0"/>
          <xsd:element name="minValue" type="xsd:nonNegativeInteger" minOccurs="0"/>
          <xsd:element name="maxValue" type="xsd:nonNegativeInteger" minOccurs="0"/>
          <xsd:element name="pattern" type="xsd:string" minOccurs="0"/>
        </xsd:all>
      </xsd:complexType>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>

```

```

        <xsd:element name="zeroPadding" type="zeroPaddingType" minOccurs="0"/>
        <xsd:element name="validRanges" type="xsd:string" minOccurs="0"/>
        <xsd:element name="invalidRanges" type="xsd:string" minOccurs="0"/>
        <xsd:element name="case" type="caseType" minOccurs="0"/>
    </xsd:all>
    <xsd:attribute name="tokenKey" type="xsd:token" use="required" />
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>

<!-- ***** -->
<!-- * Define tokenFormatType -->
<!-- ***** -->
<xsd:simpleType name="tokenType">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="alphanumeric" />
        <xsd:enumeration value="alpha" />
        <xsd:enumeration value="alphanumericrequiredalpha" />
        <xsd:enumeration value="numeric" />
    </xsd:restriction>
</xsd:simpleType>

<!-- ***** -->
<!-- * Define appDataListType -->
<!-- ***** -->
<xsd:complexType name="appDataListType">
    <xsd:sequence>
        <xsd:element name="appData" type="appDataType" maxOccurs="40"/>
    </xsd:sequence>
</xsd:complexType>

<!-- ***** -->
<!-- * Define appDataType -->
<!-- ***** -->
<xsd:complexType name="appDataType" >
    <xsd:attribute name="name" type="xsd:token" use="required" />
    <xsd:attribute name="value" type="xsd:string" use="optional" />
    <xsd:attribute name="type" type="xsd:token" use="optional" />
</xsd:complexType>

<!-- ***** -->
<!-- * Define caseType -->
<!-- ***** -->
<xsd:simpleType name="caseType">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="upper" />
        <xsd:enumeration value="lower" />
        <xsd:enumeration value="mixed" />
    </xsd:restriction>
</xsd:simpleType>

<!-- ***** -->
<!-- * Define zeroPaddingType -->
<!-- ***** -->
<xsd:simpleType name="zeroPaddingType">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="allow" />
        <xsd:enumeration value="disallow" />
        <xsd:enumeration value="force" />
    </xsd:restriction>
</xsd:simpleType>

```

```

<!-- ***** -->
<!-- * Tag Definitions -->
<!-- ***** -->
<!-- * The string "none" can be used for any non-numeric tag value to cause -->
<!-- * it to be ignored. Leaving the tag out entirely yields the same result. -->
<!-- * -->
<!-- * <nameFormats> Start of the naming format description. There will -->
<!-- * be one <nameFormat> for each name format definition. -->
<!-- * -->
<!-- * <nameFormat formatKey=name applyToPattern=pattern> -->
<!-- * Start of a naming format. Will be -->
<!-- * referenced by formatKey (which is mandatory). -->
<!-- * -->
<!-- * The applyToPattern attribute is optional -->
<!-- * and can be used to restrict this format check to -->
<!-- * only those names which match the pattern. In other -->
<!-- * words, if used, and the name matches the pattern, -->
<!-- * then the rest of the rules which follow must also -->
<!-- * be successful. However, if used, and the name does -->
<!-- * NOT match the pattern, then the name is not checked -->
<!-- * and a successful match is always declared for this -->
<!-- * formatKey. -->
<!-- * -->
<!-- * To put this another way, if the name does not match -->
<!-- * the pattern, the "enabled" tag is dynamically set to -->
<!-- * false. -->
<!-- * -->
<!-- * The definition of "pattern" is defined in the Java -->
<!-- * class Pattern. -->
<!-- * -->
<!-- * <name> descriptive name for this format; optional -->
<!-- * -->
<!-- * <enabled> true - checking enabled for this format -->
<!-- * false - checking disabled -->
<!-- * optional- default is disabled -->
<!-- * -->
<!-- * <minLength> minimum overall length of the name; optional -->
<!-- * -->
<!-- * <maxLength> maximum overall length of the name; optional -->
<!-- * -->
<!-- * <delimiters> string containing all recognized name delimiters; -->
<!-- * if more than 1 potential delimiter, include 1 -->
<!-- * instance of delimiter for each position it should -->
<!-- * hold, e.g. _._._ matches A_B.C.D_E; -->
<!-- * space - the space character will be used as the -->
<!-- * delimiter value; -->
<!-- * -->
<!-- * <forceDelimiterOrder> -->
<!-- * -->
<!-- * true - when multiple delimiters are specified (see -->
<!-- * <delimiters> tag above), requires that they -->
<!-- * appear in the order listed. -->
<!-- * false - does not require multiply listed delimiters -->
<!-- * to appear in order within the string. -->
<!-- * optional, default = false; -->
<!-- * -->
<!-- * <forceDelimiterOrder> -->
<!-- * -->
<!-- * true - when multiple delimiters are specified (see -->
<!-- * <delimiters> tag above), requires that they -->
<!-- * appear in the order listed. -->
<!-- * false - does not require multiply listed delimiters -->
<!-- * to appear in order within the string. -->
<!-- * optional, default = false; -->
<!-- * -->
<!-- * <minTokens> minimum number of tokens; optional -->
<!-- * -->
<!-- * <maxTokens> maximum number of tokens; optional -->
<!-- * -->
<!-- * <template> template showing how name should look-used for -->

```

```

<!-- *                error reporting only; optional                -->
<!-- *                -->
<!-- *    <pattern>        can be used to define a names properties, including -->
<!-- *                    delimiters, number of alpha/numeric characters, etc. -->
<!-- *                    Refer to the Pattern class in the JavaDocs for more -->
<!-- *                    details on its syntax; optional                -->
<!-- *                -->
<!-- *    <appData name= value= type= >                -->
<!-- *                    As many optional appData tags can be included -->
<!-- *                    as desired. This data is stored with the -->
<!-- *                    format and can be retrieved by an application. -->
<!-- *                    The appData has not effect on the parsing. -->
<!-- *                    -->
<!-- *                    When an application does a name format check -->
<!-- *                    against a token key, all matching formats will -->
<!-- *                    include the appData, which can be retrieved by -->
<!-- *                    the application. See NameFormat.getAppData() -->
<!-- *                    for more details. The usage of the appData -->
<!-- *                    data is strictly application driven. Below are -->
<!-- *                    is an example of a current usage. -->
<!-- *                    -->
<!-- *                    This case is setting the default port capacity for -->
<!-- *                    a carrier whose name matches the format and is -->
<!-- *                    North American to 31. -->
<!-- *                    <appData name="CapacityDefault" -->
<!-- *                        value="31" -->
<!-- *                        type="NA"/> -->
<!-- *                    -->
<!-- *    <tokenFormats>    Start of the token descriptions. There will be one -->
<!-- *                    set of <tokenFormat> for each token in the name. -->
<!-- *                    The name will be parsed into tokens using the -->
<!-- *                    <delimiters> tag, then checked for format against -->
<!-- *                    these blocks. Order is significant, as the tokens -->
<!-- *                    are expected to be checked in the same order as -->
<!-- *                    they are defined here. -->
<!-- *                    -->
<!-- *    <tokenFormat tokenKey=name>                -->
<!-- *                    One of these blocks exist for each token. -->
<!-- *                    -->
<!-- *                    <name>                descriptive name for this token (optional) -->
<!-- *                    -->
<!-- *                    <type>                type of token (optional): -->
<!-- *                    numeric - must be an integer -->
<!-- *                    alphanumeric - must contain letters, -->
<!-- *                    digits, or combinations of either; -->
<!-- *                    alpha - must contain only letters; -->
<!-- *                    alphanumericrequiredalpha - -->
<!-- *                    must contain letters and may -->
<!-- *                    contain numbers. Use of this -->
<!-- *                    type will exclude validation by -->
<!-- *                    by values or by pattern -->
<!-- *                    -->
<!-- *                    <minValue>            int containing minimum numeric value of token -->
<!-- *                    (optional) -->
<!-- *                    -->
<!-- *                    <maxValue>            int containing maximum numeric value of -->
<!-- *                    token (optional) -->
<!-- *                    -->
<!-- *                    <validRanges>        list of ranges considered valid for the -->
<!-- *                    token; part of type based processing (optional) -->
<!-- *                    Example: <validRanges>0-2,4-5</validRanges> -->
<!-- *                    -->
<!-- *                    <invalidRanges>list of ranges considered invalid for the -->
<!-- *                    token; part of type based processing (optional) -->
<!-- *                    -->
<!-- *                    <zeroPadding>        determines how to enforce 0 padding within a -->
<!-- *                    numeric value (optional). -->
<!-- *                    -->
<!-- *                    allow - allow 0 padding in the number, but do -->
<!-- *                    not force it. Essentially a "don't -->
<!-- *                    care." This is the default. -->
<!-- *                    disallow - prevents numbers from starting with a -->

```

```

<!-- *                                0.                                -->
<!-- *                                force - require numbers to be left-padded with -->
<!-- *                                0s. The pad size is dependent on the -->
<!-- *                                number of digits in the specified -->
<!-- *                                <maxValue>. If maxValue is not -->
<!-- *                                provided, then this option is treated -->
<!-- *                                as "allow".                                -->
<!-- *                                -->
<!-- *                                <case> the case for the token; -->
<!-- *                                e.g., upper, lower, mixed (default) (optional) -->
<!-- *                                -->
<!-- *                                <minLength> minimum length (optional) -->
<!-- *                                -->
<!-- *                                <maxLength> maximum length (optional) -->
<!-- *                                -->
<!-- *                                <template> template showing how token should look; -->
<!-- *                                No validation is performed against the -->
<!-- *                                template. It is used only for error reporting -->
<!-- *                                -->
<!-- *                                <values> list of valid string values; Use of the -->
<!-- *                                values property will exclude validation of -->
<!-- *                                the token by type or by pattern (optional) -->
<!-- *                                -->
<!-- *                                <pattern> can be used to define a tokens properties, -->
<!-- *                                including delimiters, number of alpha/numeric -->
<!-- *                                characters, etc. Refer to the Pattern class -->
<!-- *                                in the JavaDocs for more info on its use; -->
<!-- *                                Use of the pattern property will result in -->
<!-- *                                pattern checking ONLY. Individual token -->
<!-- *                                checking by type or by values will not be -->
<!-- *                                performed (optional) -->
<!-- ***** -->
</xsd:schema>

```

16.10.1.3 Directories Used for Certificates and Schema's

Placing a certificate in the Third Party directory listed below is how a profile is imported into the CMT software. Every 5 minutes, a polling cycle starts and scans these directories for changes. If a new file is found, its contents are verified for correctness and if verification passes, the profile is imported into the system. In addition, profiles can be removed from the system by removing certificates from this directory. Error conditions such as malformed certificates are reported as alarms. For more information on error conditions, refer to the "FM" document which accompanies this documentation.

The Nortel Certificates directory is auto datafilled by profiles that are included in customer delivered software. Users should never put a certificate directly in this directory. Nortel/Interop personnel should use the Third Party directory while working with the certificate file until a production version is ready. For updates or additions to Nortel certificates directory, Clear Case modifications are required. Appropriate Nortel personnel should be contacted for detailed information concerning building the final version of a newly defined certificate into customer deliverable software.

16.10.1.3.1 Certificate Directories The directories listed below hold the certificate files (XML documents) The Third Party directory is polled every 5 minutes for changes:

- /opt/nortel/NTsesm/properties/certificates/NortelCertificates
- /opt/nortel/NTsesm/properties/certificates/ThirdPartyCertificates

The following list shows certificates that are available in the /opt/nortel/NTsesm/properties/certificates/ThirdPartyCertificates as of the SN08 release. When building new certificates, these files can be used as a reference for understanding profile attributes.

Figure 11 SN08 Nortel Defined Certificates in the NortelCertificates Directories



16.10.1.4 Schema Directories

The following directory holds the schema files that are used as the template to define certificates. Three files are made available. The base “certificate” file defines the fields that define a certificate. The certificateTypes file holds the data values that should be used for the majority of the fields. And the nameFormats file which holds the Endpoint and Gateway naming conventions which should be used for these fields.

- /opt/nortel/NTsesm/xsd/certificateif

16.10.2 Changed OSSGate Commands

In SN08, each Profile is defined with a unique Protocol and no longer supports multiple Protocols. With this change, the Change GW command has been updated to remove the Change Protocol command and now supports Change Profile only. Other restrictions may apply.

16.10.2.1 Change MG Schema

The following text lists the schema definition for the Change GW Profile command. This existing command has been updated to include a new “choice” of “mgProfile”. Because the field is defined within the choice block, the user must choose between changing the Reserved Terminations, IP information, or newly added Profile and is not allowed to change multiple attributes at the same time.

```
<!-- ***** -->
<!-- * Define changeMG Method Parameters -->
<!-- ***** -->
<xsd:complexType name="changeMGMethodType">
  <xsd:all>
    <xsd:element name="Parameters" type="changeMGParamsType" />
  </xsd:all>
  <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
</xsd:complexType>
<xsd:complexType name="changeMGParamsType">
  <xsd:sequence>
    <xsd:sequence>
      <xsd:element name="mgUIName" type="NoSpaceNameType" />
    </xsd:sequence>
    <xsd:choice >
      <xsd:element name="reservedTerminations" type="ReservedTerminationsType" />
      <xsd:element name="mgProfile" type="NoSpaceNameType" />
    </xsd:sequence>
    <xsd:element name="mgIpAddr" type="IPAddressType" minOccurs="0" />
    <xsd:element name="mgProtocolPort" type="IpPortType" minOccurs="0" />
  </xsd:sequence>
</xsd:choice>
</xsd:sequence>
</xsd:complexType>
</xsd:schema>
```

16.10.2.2 Change MG Document

The following XML document definition shows a GW that is being changed to the “ARRIS_TOUCHTONE_NN03_4” profile definition. In order for this command to work, this profile must have been previously defined and imported into the CMT software.

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <changeMG usn="1" version="1.0" >
        <Parameters>
          <mgUIName>MG1</mgUIName>
          <mgProfile>ARRIS_TOUCHTONE_NN03_4</mgProfile>
        </Parameters>
      </changeMG>
```

```

</Methods>
</Command>
</CommandList>

```

16.10.3 New OSSGate Commands

This activity introduces two new commands that can be issued via the OSSGate interface. These commands allow users to retrieve information that is associated with profiles.

16.10.3.1 Get Certificate List

The getCertificateList command is a newly introduced XML command for the SN08 release. Unlike the GUI interface, which provides a pull down menu of defined profiles, the user must know the specific name of a profile in order to associate a GW to the system. This command is included as a means to retrieve profiles that have been imported into CMT software. Valid profile names are returned in a list and can be used with the associate GW command.

16.10.3.2 Get Certificate List Schema

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  version="1.0"
  xml:lang="en" >

  <xsd:include schemaLocation="../certificateossif/certificatecommon.xsd" />

  <!-- ***** _
  -->
  <!-- * Define GWCCConfiguration getCertificateList Method Parameters -->
  <!-- ***** _
  -->
  <xsd:complexType name="getCertificateDataMethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="getCertificateDataType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>

  <xsd:complexType name="getCertificateDataType">
    <xsd:sequence>
      <xsd:element name="CertificateName" type="NoSpaceNameType" />
    </xsd:sequence>
  </xsd:complexType>

</xsd:schema>

```

16.10.3.2.1 Get Certificate List Document

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
  <Command>
    <Interface>CertificateOSSIf</Interface>
    <Methods>
      <getCertificateList usn="1" version="1.0">
        <Parameters>
          </Parameters>
        </getCertificateList>
      </Methods>
    </Command>
  </CommandList>

```

```

        </Command>
    </CommandList>

```

16.10.3.3 Get Certificate List Result Set

The Get Certificate List command returns a list of profile names that can be used to provision a GW using the associate GW OSSGate command.

```

<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>CertificateOSSIf</Interface>
    <Methods>
      <getCertificateList usn="1" version="1.0"><ReturnCode value="13.0"
text="Successful result" /><certificate>ARRIS_TOUCHTONE_NN01_4</certificate>
<certificate>ARRIS_TOUCHTONE_NN02_4</certificate>
<certificate>ASKEY_LINE_GW_12</certificate>
<certificate>ASKEY_LINE_GW_30</certificate>
<certificate>ASKEY_LINE_GW_4</certificate>
<certificate>AUDIOCODES</certificate><certificate>CICM</certificate>
<certificate>CISCO_2600</certificate><certificate>CISCO_3600</certificate>
<certificate>CISCO_AS5300</certificate><certificate>CISCO_H323_IOS</certificate>
<certificate>CVX1800_2688</certificate><certificate>CVX600_612</certificate>
<certificate>DOMAIN_NAME</certificate><certificate>H323_PROXY</certificate>
<certificate>MEDIATRIX_LINE_GW_24</certificate>
<certificate>MEDIATRIX_LINE_GW_4</certificate>
<certificate>MGCP_LINE_GW_1</certificate>
<certificate>MOTOROLAMTA_1</certificate>
<certificate>MOTOROLAMTA_2</certificate>
<certificate>MOTOROLAMTA_4</certificate>
<certificate>NORTEL_BCM</certificate>
<certificate>NUERA_GX_ASPEN</certificate>
<certificate>NUERA_GX_MEGACO</certificate>
<certificate>PVG15K_1000_ASPEN</certificate>
<certificate>PVG15K_1000_MEGACO</certificate>
<certificate>PVG15K_ASPEN</certificate>
<certificate>PVG15K_MEGACO</certificate>
<certificate>PVG15K_PARTIAL_ASPEN</certificate><certificate>AFC</certificate>
<certificate>PVG15K_PARTIAL_MEGACO</certificate>
<certificate>AMBIT_LINE_GW_16</certificate>
<certificate>PVG7K_ASPEN</certificate>
<certificate>PVG7K_MEGACO</certificate>
<certificate>PVG_APG_ASPEN</certificate>
<certificate>PVG_APG_MEGACO</certificate>
<certificate>PVG_APG_VSP3_ASPEN</certificate>
<certificate>PVG_APG_VSP3_MEGACO</certificate>
<certificate>PVG_VSP3_ASPEN</certificate>
<certificate>PVG_VSP3_MEGACO</certificate>
<certificate>SN06_CICM</certificate><certificate>SUCCESSION_1000</certificate>
<certificate>TGCP</certificate><certificate>TOUCHTONE_NN01_1</certificate>
<certificate>TOUCHTONE_NN01_2</certificate>
<certificate>TOUCHTONE_NN01_3</certificate>
<certificate>TOUCHTONE_NN01_4</certificate><certificate>UAS</certificate>
<certificate>UE9000MG</certificate><certificate>UE9000MG_ABI</certificate>
<certificate>UE9000MG_ABI_IP</certificate>
<certificate>UE9000MG_IP</certificate><certificate>WESTELL</certificate>
</Methods>
    </Response>
  </Response>

```

```
</CommandList>
```

16.10.3.4 Get Certificate Data OSSGate Command

In addition to the list of profiles, this activity introduces the ability to list the Certificate that was used to generate a profile. This Certificate can be used to understand datafill options when creating a new GW.

16.10.3.4.1 Get Certificate Data Schema

```
<xsd:include schemaLocation="../certificateossif/certificatecommon.xsd" />

<!--
*****
-->
<!-- * Define GWCCConfiguration getCertificateData Method Parameters -->
<!--
*****
-->

<xsd:complexType name="getCertificateListMethodType">
  <xsd:all>
    <xsd:element name="Parameters" type="getCertificateListType" minOccurs="0" />
  </xsd:all>
  <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
</xsd:complexType>

<xsd:complexType name="getCertificateListType">
  <xsd:sequence>
    <xsd:element name="List" type="xsd:string" minOccurs="0" />
  </xsd:sequence>
</xsd:complexType>

</xsd:schema>
```

16.10.3.4.2 Get Certificate Data Document

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
  <Command>
    <Interface>CertificateOSSIf</Interface>
    <Methods>
      <getCertificateData usn="1" version="1.0">
        <Parameters>
          <CertificateName>CISCO_2600</CertificateName>
        </Parameters>
      </getCertificateData>
    </Methods>
  </Command>
</CommandList>
```

16.10.3.5 Get Certificate Data Result Set

The Get Certificate Data command returns the Certificate used to generate a profile.

```
<?xml version='1.0'?>
<CommandList>
```

```

    <Response>
      <Interface>CertificateOSSIf</Interface>
      <Methods>
        <getCertificateData usn="1" version="1.0"><ReturnCode value="13.0" text="Successful
result" /><certificate> <MaxEndpoints>1032</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>63</GWCProfileNumber>
        <EPIDGenDesc>auto1</EPIDGenDesc>
        <ServiceTypeList>H323</ServiceTypeList>
        <ServiceTypeList>ITRANS</ServiceTypeList>
        <CompatibleGWProfileList>CISCO_2600</CompatibleGWProfileList>

    <GatewayNameFormatList>
      <nameFormat formatKey="GATEWAY.H323" enabled="true" applyToPattern=".*">
        <name>H323 Gateway</name>
        <delimiters>`</delimiters>
        <maxTokens>1</maxTokens>
        <tokenFormats>
          <tokenFormat tokenKey="GW">
            <name>Name</name>
            <pattern><![CDATA[^[^"'<>=]*]]></pattern>
          </tokenFormat>
        </tokenFormats>
      </nameFormat>
      <nameFormat formatKey="GATEWAY.ALL" enabled="true" applyToPattern=".*">
        <name>Generic For All Gateways</name>
        <template>gatewayName</template>
        <maxLength>32</maxLength>
        <minLength>1</minLength>
        <delimiters>none</delimiters>
        <tokenFormats>
          <tokenFormat tokenKey="GW">
            <pattern><![CDATA[^[^"'<>=,;]*]]></pattern>
            <name>Name</name>
          </tokenFormat>
        </tokenFormats>
      </nameFormat>
    </GatewayNameFormatList>

    <EndpointNameFormatList>
      <nameFormat formatKey="CARRIER.H323.EPG" enabled="true" applyToPattern=".*">
        <name>EPG</name>
        <template><![CDATA[EPG_<nnn>]]></template>
        <maxTokens>2</maxTokens>
        <minTokens>2</minTokens>
        <delimiters>_</delimiters>
        <maxLength>7</maxLength>
        <minLength>7</minLength>
        <appDataList>

```

```

    <appData name="CARRIERTYPEORPROTOCOLALLOWED" value="H323"
type="NONE" />
    <appData name="CAPACITYDEFAULT" value="32" type="INTL" />
    <appData name="CAPACITYDEFAULT" value="24" type="NA" />
  </appDataList>
  <tokenFormats>
    <tokenFormat tokenKey="TYPE">
      <name>Type</name>
      <template>EPG</template>
      <type>alphanumeric</type>
      <values>EPG</values>
    </tokenFormat>
    <tokenFormat tokenKey="NUMBER">
      <min Value>0</min Value>
      <max Value>999</max Value>
      <name>Number</name>
      <type>numeric</type>
      <template><![CDATA[<nnn>]]></template>
    </tokenFormat>
  </tokenFormats>
  </nameFormat>
</EndpointNameFormatList>

</certificate></getCertificateData>    </Methods>
</Response>
</CommandList>

```

16.11 Security

N/A

16.12 Configuration Walkthrough

16.12.1 Certificate Creation

A certificate is created with the goal of creating a new profile. The following procedure should be used:

1. Understand schema field values by reading field descriptions in this document. Also, existing certificates listed in the appendix of this document and also available in the Nortel certificate directory, give examples of how the certificate fields are being used for other profiles.
2. Use a plain vanilla editor (i.e., UNIX vi) that will not put hidden formatting characters into the file. Or, using any editor, save the file as “text” making sure that hidden characters such as ^Ms are not put in document.
3. Create a XML document (a Certificate) with the desired behaviors of the new profile making sure to name the file with the “.certificate” extension.

Note: Certificate names are case insensitive. The convention is to use uppercase when creating Certificates, however, mixed case name are recognized. Mixed case names are converted to upper case when imported into the system.

Note: Duplicate Certificate names are not allowed and do not consider case. In other words, XYZ.certificate and xyz.certificate are regarded by software as the same name and would cause a duplicate alarm. This restriction applies to both the Nortel and Third Party directories and spans both directories. For example, if the XYZ.certificate is present in the Nortel directory and also in the Third Party directory a duplicate alarm would be raised.

16.12.2 Importing a Profile into the System

In order to use a newly created certificate, the certificate must be imported into the CMT system. System importation is an automatic process as listed below.

Note: Only 3rd Party Interopt certificates are imported into CMT software. Nortel Defined certificates are included in the software that is delivered in the released product.

1. Put the certificate created from the process listed above in the following directory: /opt/nortel/NTsesm/properties/certificate/ThirdPartyCertificates
2. A polling cycle occurs every 5 minutes and automatically reads in any new certificates placed in this directory.
3. If a problem is encountered with the certificate, an alarm is raised. In order to clear the alarm, the contents of the certificate should be altered as listed in the alarm, and the file should be reloaded. When the polling cycle runs again, the file is once again scanned into the system if the alarm condition is remedied.

Note: Details concerning the “corrupt and changed” certificate alarms are listed in the CMT minor (MNR) log files. These files can be viewed at the following location “/opt/nortel/NTsesm/admin/logs/ptmdebuglog1.mi2.

Note: Restricting the logs to list MNR and above logs only can be accomplished using the MI2Admin tool. This tool is located in the /opt/nortel/NTsesm/bin directory.

4. A certificate that is successfully imported into the system gives the following capabilities:
 - The profile is listed in the Associate GW GUI profile combo box
 - The profile is available as a provisioning parameter for the OSSGate Associate GW profile field

16.12.3 Changing the Profile Assigned to a GW

The following procedure should be used when a user wants to change the profile assigned to a GW. Note that, certificates should never be manipulated directly to change a profile. The following attributes can be changed: endpoint and gateway format, reserved terminations, mandatory reserved flag, physical

location flag, service type, compatible profile, maximum endpoints, and protocol.

1. Create a new profile with the changed Administrative attributes
2. or, have an existing profile available with differences in Administrative attributes only
3. Select the GW to be changed from the Provisioning/Gateways panel and push the “change” button
4. Select the profile that the GW is to be changed to and select OK
5. or, issue the OSSGate Change GW command with the new profile

16.12.4 Removing a Profile

It may be desirable for a user to remove a profile from the system. One reason for doing this is to reduce the clutter for obsolete profiles or to remove the ability to assign one of these profiles to a GW mistakenly. The following procedure should be used to accomplish this.

1. Remove all GWs that have the profile in question assigned to them
2. or, change the GWs with the profile to a different profile as listed above
3. Remove the certificate from the /opt/nortelNTsesm/properties/certificates/ThirdParty Directory
4. Wait up to 5 minutes for the certificate directory to be polled and the certificate is remove automatically

Note: If a certificate is removed that has GWs assigned to it, an alarm is raised and will not clear until all GWs with the deleted certificate are removed or the certificate is put back in the certificates directory. For more information on this topic, refer to the FM document that accompanies this documentation.

16.12.5 3rd Party Certificate Distribution

A profiles certificate is a text file that can be transferred like any other file. Once a certificate has been created, distribution of the file to customers can be performed using any file transfer program such as FTP. Theoretically, the file can be recreated at the customer site, but, it is recommended that the original certificate is sent to the customer by a file transfer program to avoid inadvertent syntax errors. Important: caution should be used so that hidden or formatting characters are not introduced into Certificate files. For example, editors such as Microsoft Notepad introduce a ^M character.

16.13 Appendix

16.13.1 Converted Profile Nortel Certificates

Following is a few samples of Nortel provided certificates that are available at creation of this document. While every attempt has been made to insure completeness and accuracy of these certificates, the content may be incomplete or obsolete. These definitions are provided here for illustration purposes only. For the released list of certificates, please refer to /opt/nortel/NTsesm/properties/certificates/NortelCertificates directory.

16.13.1.1 ASCII_LINE_GW_30

```
<?xml version="1.0" encoding="UTF-8" ?>

<certificate>

  <MaxEndpoints>30</MaxEndpoints>
  <Category>SMALL</Category>
  <EndpointType>managedLens</EndpointType>
  <GenerateLGRP>false</GenerateLGRP>
  <ResvTermMandatory>false</ResvTermMandatory>
  <ChangeIPAvailable>false</ChangeIPAvailable>
  <DispPhyLocation>false</DispPhyLocation>
  <InventoryType>Small Line Gateway</InventoryType>
  <InventoryRole>Media Gateway</InventoryRole>
  <SupportedProtocol>
    <protocolName>mgecp</protocolName>
    <version>1.0</version>
  </SupportedProtocol>
  <GWCPProfileNumber>49</GWCPProfileNumber>
  <EPIDGenDesc>manual</EPIDGenDesc>
  <ServiceTypeList>line</ServiceTypeList>
  <ServiceTypeList>ITRANS</ServiceTypeList>
  <CompatibleGWProfileList>ASKEY_LINE_GW_30</CompatibleGWProfileList>

  <GatewayNameFormatList>
    <nameFormat formatKey="GATEWAY.UE511" enabled="true">
      <delimiters>.</delimiters>
      <minLength>1</minLength>
      <maxLength>32</maxLength>
      <minTokens>1</minTokens>
      <maxTokens>16</maxTokens>
      <name>IAD Gateway</name>
      <template>
        <![CDATA[<name segment>[.<name segment>. ... <name segment>] up to 16 segments
(e.g. MyGate05.com, AA-BB-CC, a12345)]]>
      </template>
      <tokenFormats>
        <tokenFormat tokenKey="NAME">
          <name>Name</name>
          <template><![CDATA[<name segment - must start with letter>]]></template>
          <pattern><![CDATA[^[a-zA-Z][a-zA-Z0-9-]*]]></pattern>
        </tokenFormat>
        <tokenFormat tokenKey="DOMAIN">
          <name>Domain</name>
          <template><![CDATA[<domain>]]></template>
          <pattern><![CDATA[[a-zA-Z0-9-]*]]></pattern>
        </tokenFormat>
      </tokenFormats>
    </nameFormat>
  </GatewayNameFormatList>

```

[illegible]

```

        <tokenFormat tokenKey="DOMAIN">
            <name>Domain</name>
            <template><![CDATA[<domain>]]></template>
            <pattern><![CDATA[[a-zA-Z0-9-]*]]></pattern>
        </tokenFormat>
        <tokenFormat tokenKey="DOMAIN">
            <name>Domain</name>
            <template><![CDATA[<domain>]]></template>
            <pattern><![CDATA[[a-zA-Z0-9-]*]]></pattern>
        </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>
        <tokenFormat tokenKey="GW">
            <name>Name</name>
            <pattern><![CDATA[[^"'"<=>.,;]*]]></pattern>
        </tokenFormat>
    </tokenFormats>
</nameFormat>
</GatewayNameFormatList>
<EndpointNameFormatList>
<nameFormat formatKey="LINE.SMALL">
    <maxTokens>2</maxTokens>
    <template><![CDATA[aaln/<nnnn>]]></template>
    <delimiters>/</delimiters>
    <minLength>6</minLength>
    <minTokens>2</minTokens>
    <name>Small Line</name>
    <enabled>true</enabled>
    <maxLength>9</maxLength>
    <tokenFormats>
        <tokenFormat tokenKey="PREFIX">
            <name>Prefix</name>
            <values>aaln</values>
            <template>aaln</template>
            <maxLength>4</maxLength>
            <minLength>4</minLength>
            <type>alphanumeric</type>
        </tokenFormat>
        <tokenFormat tokenKey="LINENUM">
            <maxValue>4095</maxValue>
            <name>Line Number</name>
            <type>numeric</type>
            <template><![CDATA[<nnnn>]]></template>
            <minValue>0</minValue>
        </tokenFormat>
    </tokenFormats>
</nameFormat>
</EndpointNameFormatList>
</certificate>

```

16.13.1.2 CISCO_2600

```

<?xml version="1.0" encoding="UTF-8" ?>

<certificate>

  <MaxEndpoints>1032</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>63</GWCProfileNumber>
  <EPIDGenDesc>auto1</EPIDGenDesc>
  <ServiceTypeList>H323</ServiceTypeList>
  <ServiceTypeList>ITRANS</ServiceTypeList>
  <CompatibleGWProfileList>CISCO_2600</CompatibleGWProfileList>

  <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>
        <tokenFormat tokenKey="GW">
          <name>Name</name>
          <pattern><![CDATA[[^"'"<>=,;]*]></pattern>
        </tokenFormat>
      </tokenFormats>
    </nameFormat>
  </GatewayNameFormatList>

  <EndpointNameFormatList>
    <nameFormat formatKey="CARRIER.H323.EPG">
      <appDataList>
        <appData name="CapacityDefault" value="24" type="NA" />
        <appData name="CapacityDefault" value="32" type="INTL" />
        <appData name="CarrierTypeOrProtocolAllowed" value="H323" />
      </appDataList>
      <template><![CDATA[EPG_<nnn>]]></template>
      <name>EPG</name>
      <maxLength>7</maxLength>
      <minLength>7</minLength>
    </nameFormat>
  </EndpointNameFormatList>

```

```

    <maxTokens>2</maxTokens>
    <enabled>true</enabled>
    <minTokens>2</minTokens>
    <delimiters>_</delimiters>
    <tokenFormats>
      <tokenFormat tokenKey="TYPE">
        <values>EPG</values>
        <name>Type</name>
        <type>alphanumeric</type>
        <template>EPG</template>
      </tokenFormat>
      <tokenFormat tokenKey="NUMBER">
        <max Value>999</max Value>
        <name>Number</name>
        <type>numeric</type>
        <template><![CDATA[<nnn>]]></template>
        <min Value>0</min Value>
      </tokenFormat>
    </tokenFormats>
  </nameFormat>
</EndpointNameFormatList>

</certificate>

```

16.13.1.3 PVG_APG_ASPEN

```

<?xml version="1.0" encoding="UTF-8" ?>

<certificate>

  <MaxEndpoints>1120</MaxEndpoints>
  <Category>APG</Category>
  <EndpointType>carrierTrksGwcNN</EndpointType>
  <GenerateLGRP>false</GenerateLGRP>
  <ResvTermMandatory>false</ResvTermMandatory>
  <ChangeIPAvailable>false</ChangeIPAvailable>
  <DispPhyLocation>false</DispPhyLocation>
  <InventoryType>Large Trunk Gateway</InventoryType>
  <InventoryRole>Media Gateway</InventoryRole>
  <SupportedProtocol>
    <protocolName>aspen</protocolName>
    <version>2.1</version>
  </SupportedProtocol>
  <GWCPProfileNumber>46</GWCPProfileNumber>
  <EPIDGenDesc>auto1</EPIDGenDesc>
  <ServiceTypeList>APG</ServiceTypeList>
  <CompatibleGWProfileList>PVG_APG_ASPEN</CompatibleGWProfileList>

  <GatewayNameFormatList>
    <nameFormat formatKey="GATEWAY.PVG">
      <name>PVG Gateway</name>
      <delimiters>none</delimiters>
      <enabled>true</enabled>
      <maxTokens>1</maxTokens>
      <tokenFormats>
        <tokenFormat tokenKey="GW">
          <name>Pvg</name>
          <case>upper</case>
          <type>alphanumeric</type>

```

```

        </tokenFormat>
      </tokenFormats>
    </nameFormat>
    <nameFormat formatKey="GATEWAY.ALL">
      <template>gatewayName</template>
      <delimiters>none</delimiters>
      <name>Generic For All Gateways</name>
      <enabled>true</enabled>
      <tokenFormats>
        <tokenFormat tokenKey="GW">
          <name>Name</name>
          <pattern><![CDATA[[^"'<>=,;]*]]></pattern>
        </tokenFormat>
      </tokenFormats>
    </nameFormat>
  </GatewayNameFormatList>

  <EndpointNameFormatList>
    <nameFormat formatKey="CARRIER.ASPEN.DS1" applyToPattern="^DS1.*">
      <appDataList>
        <appData name="CapacityDefault" value="24" type="*" />
        <appData name="CarrierTypeOrProtocolAllowed" value="ISUP" />
        <appData name="CarrierTypeOrProtocolAllowed" value="PRI" />
      </appDataList>
      <maxLength>6</maxLength>
      <template><![CDATA[DS1_<nn>]]></template>
      <minLength>5</minLength>
      <maxTokens>2</maxTokens>
      <delimiters>_</delimiters>
      <name>DS1</name>
      <minTokens>2</minTokens>
      <enabled>true</enabled>
      <tokenFormats>
        <tokenFormat tokenKey="TYPE">
          <name>Type</name>
          <type>alphanumeric</type>
          <values>DS1</values>
          <template>DS1</template>
        </tokenFormat>
        <tokenFormat tokenKey="NUMBER">
          <template><![CDATA[<nn>]]></template>
          <minValue>0</minValue>
          <maxValue>99</maxValue>
          <name>Number</name>
          <type>numeric</type>
        </tokenFormat>
      </tokenFormats>
    </nameFormat>
    <nameFormat formatKey="CARRIER.ASPEN.DS3" applyToPattern="^DS3.*">
      <appDataList>
        <appData name="CapacityDefault" value="24" type="*" />
        <appData name="CarrierTypeOrProtocolAllowed" value="ISUP" />
        <appData name="CarrierTypeOrProtocolAllowed" value="PRI" />
      </appDataList>
      <delimiters>_</delimiters>
      <name>DS3</name>
      <template><![CDATA[DS3_<nnn>.<dd>]]></template>
      <maxLength>10</maxLength>
      <minLength>7</minLength>
      <enabled>true</enabled>
      <maxTokens>3</maxTokens>

```

```

<minTokens>3</minTokens>
<tokenFormats>
  <tokenFormat tokenKey="TYPE">
    <values>DS3</values>
    <name>Type</name>
    <type>alphanumeric</type>
    <template>DS3</template>
  </tokenFormat>
  <tokenFormat tokenKey="LPSLOT">
    <template><![CDATA[<nnn>]]></template>
    <minValue>0</minValue>
    <maxValue>999</maxValue>
    <name>LP Slot and Port</name>
    <type>numeric</type>
  </tokenFormat>
  <tokenFormat tokenKey="DS1NUMBER">
    <minValue>0</minValue>
    <maxValue>99</maxValue>
    <name>DS 1 Number</name>
    <type>numeric</type>
    <template><![CDATA[<dd>]]></template>
  </tokenFormat>
</tokenFormats>
</nameFormat>
<nameFormat formatKey="CARRIER.ASPEN.E1" applyToPattern="^E1.*">
  <appDataList>
    <appData name="CapacityDefault" value="31" type="*" />
    <appData name="CarrierTypeOrProtocolAllowed" value="*" />
  </appDataList>
  <name>E1</name>
  <delimiters>_</delimiters>
  <enabled>true</enabled>
  <maxLength>7</maxLength>
  <minLength>6</minLength>
  <maxTokens>2</maxTokens>
  <template><![CDATA[E1_<nnnn>]]></template>
  <minTokens>2</minTokens>
  <tokenFormats>
    <tokenFormat tokenKey="TYPE">
      <type>alphanumeric</type>
      <values>E1</values>
      <template>E1</template>
      <name>Type</name>
    </tokenFormat>
    <tokenFormat tokenKey="LPE1">
      <zeroPadding>disallow</zeroPadding>
      <template><![CDATA[<nnnn>]]></template>
      <name>LP Slot and E1 Number</name>
      <type>numeric</type>
      <minValue>0</minValue>
      <maxValue>9999</maxValue>
    </tokenFormat>
  </tokenFormats>
</nameFormat>
<nameFormat formatKey="CARRIER.ASPEN.STM" applyToPattern="^SM_.*_412_.*">
  <appDataList>
    <appData name="CapacityDefault" value="31" type="*" />
    <appData name="CarrierTypeOrProtocolAllowed" value="ISUP" />
    <appData name="CarrierTypeOrProtocolAllowed" value="PRI" />
  </appDataList>
  <maxLength>18</maxLength>

```

```

<maxTokens>4</maxTokens>
<template><![CDATA[SM_<lp><pp><r>_412_<aa><t><u><v>]]></template>
<minLength>17</minLength>
<minTokens>4</minTokens>
<name>STM</name>
<delimiters>_</delimiters>
<enabled>true</enabled>
<tokenFormats>
  <tokenFormat tokenKey="TYPE">
    <template>SM</template>
    <name>Type</name>
    <type>alphanumeric</type>
    <values>SM</values>
  </tokenFormat>
  <tokenFormat tokenKey="LPPOINT">
    <name>LP / Port / Level</name>
    <type>numeric</type>
    <template><![CDATA[<lp><pp><r>]]></template>
    <minValue>1000</minValue>
    <maxValue>15999</maxValue>
  </tokenFormat>
  <tokenFormat tokenKey="MUX">
    <template>412</template>
    <name>Mux Type VC4VC12</name>
    <values>412</values>
    <type>alphanumeric</type>
  </tokenFormat>
  <tokenFormat tokenKey="AUGTUG">
    <template><![CDATA[<aa><t><u><v>]]></template>
    <minValue>1000</minValue>
    <maxValue>99999</maxValue>
    <name>AUG / VC4-TUG3 / TUG2-TUG3 / TU</name>
    <type>numeric</type>
  </tokenFormat>
</tokenFormats>
</nameFormat>
<nameFormat formatKey="CARRIER.ASPEN.STS" applyToPattern="^SS_.*_VT15_.*">
  <appDataList>
    <appData name="CapacityDefault" value="24" type="*" />
    <appData name="CarrierTypeOrProtocolAllowed" value="ISUP" />
    <appData name="CarrierTypeOrProtocolAllowed" value="PRI" />
  </appDataList>
  <name>SS</name>
  <maxTokens>4</maxTokens>
  <minLength>17</minLength>
  <minTokens>4</minTokens>
  <enabled>true</enabled>
  <template><![CDATA[SS_<lp><pp><r>_VT15_<ss><t><v>]]></template>
  <maxLength>18</maxLength>
  <delimiters>_</delimiters>
  <tokenFormats>
    <tokenFormat tokenKey="TYPE">
      <name>Type</name>
      <template>SS</template>
      <type>alphanumeric</type>
      <values>SS</values>
    </tokenFormat>
    <tokenFormat tokenKey="LPPOINT">
      <maxValue>15999</maxValue>
      <name>LP / Port / Level</name>
      <type>numeric</type>

```

```

        <template><![CDATA[<lp><pp><r>]]></template>
        <min Value>1000</min Value>
    </tokenFormat>
    <tokenFormat tokenKey="MUX">
        <template>VT15</template>
        <values>VT15</values>
        <name>Mux Type VT15</name>
        <type>alphanumeric</type>
    </tokenFormat>
    <tokenFormat tokenKey="TUG">
        <name>STS-1 / TUG3 / VT</name>
        <type>numeric</type>
        <template><![CDATA[<ss><t><v>]]></template>
        <max Value>9999</max Value>
        <min Value>100</min Value>
    </tokenFormat>
</tokenFormats>
</nameFormat>
<nameFormat formatKey="CARRIER.ASPEN.ALL">
    <name>Generic Name Check for APSEN Protocol</name>
    <delimiters>none</delimiters>
    <enabled>true</enabled>
</tokenFormats>
    <tokenFormat tokenKey="NAMEPREFIX">
        <template>DS1 or DS3 or E1 or SM or SS</template>
        <name>Generic Name Prefix</name>
        <pattern>^DS1.*|^DS3.*|^E1.*|^SM.*|^SS.*</pattern>
    </tokenFormat>
</tokenFormats>
</nameFormat>
</EndpointNameFormatList>

</certificate>

```

16.13.1.4 UE9000MG

```

<?xml version="1.0" encoding="UTF-8" ?>

<certificate>

    <MaxEndpoints>512</MaxEndpoints>
    <Category>LARGE</Category>
    <EndpointType>ue9000Lens</EndpointType>
    <GenerateLGRP>true</GenerateLGRP>
    <ResvTermMandatory>>false</ResvTermMandatory>
    <ChangeIPAvailable>>false</ChangeIPAvailable>
    <DispPhyLocation>>false</DispPhyLocation>
    <InventoryType>UE9000MG</InventoryType>
    <InventoryRole>Media Gateway</InventoryRole>
    <SupportedProtocol>
        <protocolName>megaco</protocolName>
        <version>1.0</version>
    </SupportedProtocol>
    <GWCPProfileNumber>50</GWCPProfileNumber>
    <EPIDGenDesc>auto6</EPIDGenDesc>
    <ServiceTypeList>line</ServiceTypeList>
    <CompatibleGWProfileList>UE9000MG</CompatibleGWProfileList>
    <BearerFabricList>AAL1</BearerFabricList>

    <GatewayNameFormatList>

```

```

<nameFormat formatKey="GATEWAY.UE9000MG">
  <minLength>8</minLength>
  <enabled>true</enabled>
  <maxTokens>3</maxTokens>
  <name>UE9000MG Gateway</name>
  <minTokens>3</minTokens>
  <delimiters>-</delimiters>
  <template>
    <![CDATA[<sitename=1-4char+officeframe=000-511>-<logicalframe=0-7>-<shelf=0-
3>]]>
  </template>
  <maxLength>11</maxLength>
  <tokenFormats>
    <tokenFormat tokenKey="SITEOFFICEFRAME">
      <type>alphanumeric</type>
      <template><![CDATA[<sitename=1-4char+officeframe=000-511>]]></template>
      <maxLength>7</maxLength>
      <minLength>4</minLength>
      <name>Site Name / Office Frame Number</name>
    </tokenFormat>
    <tokenFormat tokenKey="LOGICALFRAME">
      <name>Logical Frame Number</name>
      <template><![CDATA[<logicalframe=0-7>]]></template>
      <maxValue>7</maxValue>
      <type>numeric</type>
      <minValue>0</minValue>
    </tokenFormat>
    <tokenFormat tokenKey="SHELF">
      <template><![CDATA[<shelf=0-3>]]></template>
      <name>Shelf Number</name>
      <minValue>0</minValue>
      <maxValue>3</maxValue>
      <type>numeric</type>
    </tokenFormat>
  </tokenFormats>
</nameFormat>
<nameFormat formatKey="GATEWAY.ALL">
  <template>gatewayName</template>
  <delimiters>none</delimiters>
  <name>Generic For All Gateways</name>
  <enabled>true</enabled>
  <tokenFormats>
    <tokenFormat tokenKey="GW">
      <name>Name</name>
      <pattern><![CDATA[[^"'"<>=,;]*]]></pattern>
    </tokenFormat>
  </tokenFormats>
</nameFormat>
</GatewayNameFormatList>

<EndpointNameFormatList>
<nameFormat formatKey="LINE.UE9000MG" applyToPattern="^tp/.*/.*">
  <enabled>true</enabled>
  <template>
    <![CDATA[tp/<slot=02-21,0-padded>/<circuit=00-31,0-padded>]]>
  </template>
  <delimiters>/</delimiters>
  <maxLength>8</maxLength>
  <name>UE9000MG Line</name>
  <minLength>8</minLength>
  <maxTokens>3</maxTokens>

```

```

    <minTokens>3</minTokens>
    <tokenFormats>
      <tokenFormat tokenKey="PREFIX">
        <name>Prefix</name>
        <template>tp</template>
        <type>alphanumeric</type>
        <values>tp</values>
      </tokenFormat>
      <tokenFormat tokenKey="SLOT">
        <type>numeric</type>
        <template><![CDATA[<slot=02-21,0-padded>]]></template>
        <minValue>2</minValue>
        <maxValue>21</maxValue>
        <name>Slot Number</name>
      </tokenFormat>
      <tokenFormat tokenKey="CIRCUIT">
        <maxValue>31</maxValue>
        <name>Circuit Number</name>
        <type>numeric</type>
        <template><![CDATA[<circuit=00-31,0-padded>]]></template>
        <minValue>0</minValue>
      </tokenFormat>
    </tokenFormats>
  </nameFormat>
  <nameFormat formatKey="LINEGROUP.UE9000MG" enabled="true"
applyToPattern="^tp\d*$">
    <maxLength>5</maxLength>
    <minLength>5</minLength>
    <maxTokens>2</maxTokens>
    <delimiters></delimiters>
    <minTokens>2</minTokens>
    <name>UE9000MG Line</name>
    <template>
      <![CDATA[tp<slot=02-21,0-padded>]]>
    </template>
    <tokenFormats>
      <tokenFormat tokenKey="PREFIX">
        <values>tp</values>
        <template>tp</template>
        <name>Prefix</name>
        <type>alpha</type>
      </tokenFormat>
      <tokenFormat tokenKey="SLOT">
        <maxValue>21</maxValue>
        <name>Slot Number</name>
        <type>numeric</type>
        <template><![CDATA[<slot=02-21,0-padded>]]></template>
        <minValue>2</minValue>
      </tokenFormat>
    </tokenFormats>
  </nameFormat>
  <nameFormat formatKey="UE9000MG.ALL">
    <delimiters>none</delimiters>
    <name>Generic Name Check for UE9000MG</name>
    <enabled>true</enabled>
    <pattern>^tp/.*/.*|^tp\d*$</pattern>
    <template>
      <![CDATA[tp<slot=02-21,0-padded> OR tp<slot=02-21,0-padded><circuit=00-31,0-
padded>]]>
    </template>
  </nameFormat>

```

```
</EndpointNameFormatList>  
</certificate>
```

17: A00007072 Configuration (CN)

17.1 Feature name

3rd Party GW Interop Pre Provisioning

17.2 Hardware and Software Requirements

SN08 base loads will be required across all the components of this solution to effectively use this feature.

17.3 Initial Configuration

Not applicable.

Note: A third party GW must have been successfully associated with its GWC using appropriate GW profile, before attempting the end-point provisioning. This feature makes use of this pre-condition to facilitate end-point provisioning of such a GW.

17.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

Note: This feature leverages a previously defined gateway profile for third party large line gateways.

17.4.1 New/modified office/subnet parameters

Not applicable.

17.4.2 Parameter information

Not applicable.

17.4.2.0.1 Memory requirements

No memory impact.

17.5 Upgrade Impact

17.5.1 Dump and Restore

Not applicable.

17.5.2 Element Management Upgrade

Conversion of existing third party large line GW data to SN08 format is not supported. To leverage any of the capabilities delivered by this feature, the existing GW and the associated end-points and the Service must be removed and re-added in SN08. Both new and old format data will be allowed to co-exist in SN08, however the existing GW and the end-points will be managed in the same format as defined in the previous release.

Due to a dependency of this feature on the GW Profile Feature, A00007071, the capabilities provided by this feature can not be fully utilized until all the components of the OAMP are at the base 08 load line up. There is a dependency on the new LGRPTYPE in the 08 CS2K Core that will be used by the third party GW nodes in the Core. The GWC devices are required to be on the 08 release as well to support spare profiles. Please refer to the A00007071 feature documentation for additional details regarding this dependency.

17.6 Data schema (DS) (CM, MIBS, RDB)

17.6.1 New/modified tables, MIBs, or Database Schema

Not Applicable.

17.7 Gateway and End-point Name Mapping to Logical Group and Line Equipment Number (LEN)

The logical group name is derived from the GW SITE, the frame number and the unit number. The end-point name is user defined and its associated LEN has absolutely no bearing on the end-point name. The LEN is derived from the logical group name and the user specified circuit number. The following sections clarify this relationship with an example.

17.7.0.0.1 GW

<GWNAME>, e.g. "MyGW"

17.7.0.0.2 Logical Group

<SITE> <FFF> <U>, e.g. "CARY 142 0"

where:

<SITE> = SITE name chosen at gateway provisioning time. Matching gateway name to SITE name is not an enforced rule, however it is suggested that a third party GW SITE name be defined in the CS2K Core and that all third party gateway provisioning utilize the "third party GW" SITE name.

<FFF> = Frame number that is specified during the third party GW provisioning. This number can range between 0 - 511

<U> = Unit number that is specified during the third party GW provisioning. This number can range from 0 - 9.

17.7.0.0.3 End-point

The end-point name is flexible. The format of the name is defined during the GW profile creation time and enforced during the GW provisioning time. The name is completely user defined. The name can include any physical location data of the hardware. The end-point name can be up to 32 characters long with no spaces in between.

17.7.0.0.4 LEN Format

<SITE> <FFF> <U> <TT> <tt>, e.g. "CARY 142 0 10 13"
where:

<SITE>, <FFF>, <U>, <TT>, and <tt> are as defined in the above sections.

The following summarizes the correlation between a GW, its end-points and the associated LENs:

- One third party "GW" mapped to one logical group in the CS2K Core.
- 1023 terminations are supported per logical group.
- 1 terminal number is reserved in the CS2K Core for maintenance/messaging.

Table 1 GW, LGRP, End-point, TN and LEN Relationship

GW Name (User Input)	Profile	LGRP Name	End-point (User Input)	Circuit Number (User Input)	LEN
MyGW.ext.net	PRF_1	CARY 100 5	ext/100/5/1/1	0	EXT 100 5 00 00
MyGW.ext.net	PRF_1	CARY 100 5	ext/100/5/1/2	2	EXT 100 5 00 01
:		:	:	:	:
:		:	:	:	:
MyGW2.ext.net	PRF_2	EXT2 200 8	ext2-ep-last	1022	EXT2 200 8 10 22

Terminal number 0 is reserved in the CS2K Core for the maintenance/messaging terminal on the node.

LEN is generated using the following formula:

(LGRPName) (CN/100) (CN%100) where CN => Circuit Number

The last 2 parts of LEN are 0 padded to keep the value to 2 digits similar to the other LENs.

17.8 Service Orders (SO) (CM & SESM)

Not applicable.

17.9 Software optionality control (SOC)

Not applicable.

17.10 Element Management

17.10.1 New/modified GUIs

The CS2000 Management Tools GUI is modified by this feature. Specifically the ‘Associate Media Gateway’ dialog box will be altered to support provisioning of the frame and unit numbers and the LGRPLOC information as part of LGRPOPTS (LGRP OPTions)

A third party GW will be associated with its GWC using an appropriate gateway profile. The profile must have been defined before associating the GW. When the third party GW profile is selected on the “Associate Media Gateway” GUI, the new fields for taking the input for the frame and unit numbers along with the other LGRPLOC fields will be displayed.

Table 2 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
AssocMG	CHANGED

17.10.2 GUI information

17.10.2.1 GUI name: AssocMG

“Associate Media Gateway”

17.10.2.1.1 Functional description

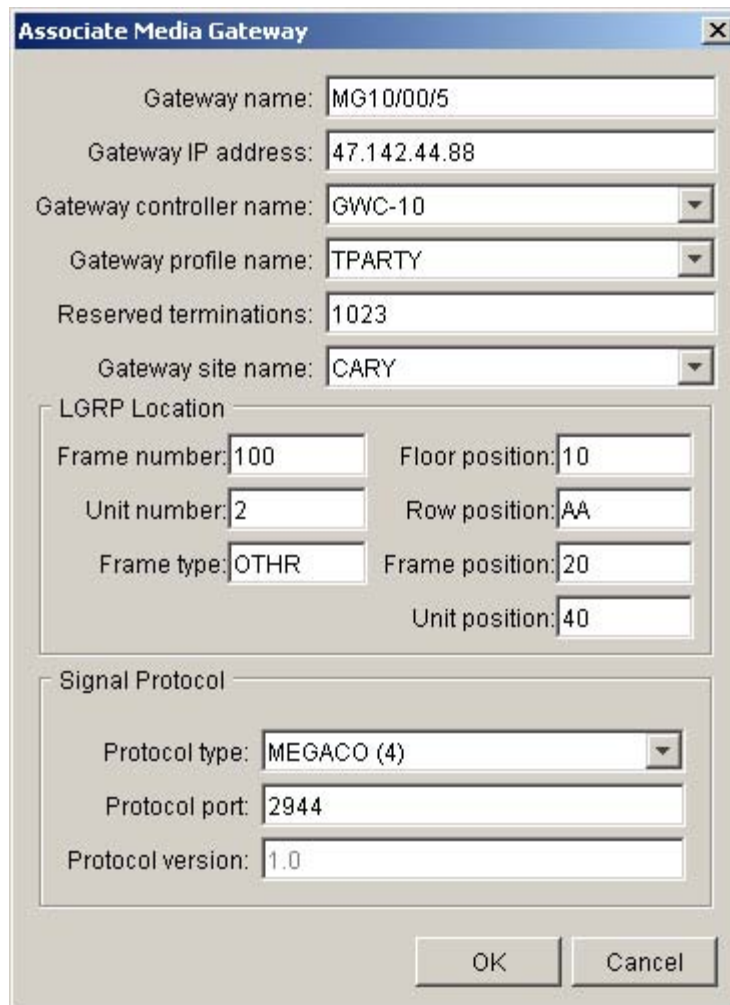
The existing “Associate Media Gateway” GUI prompts the user for profile specific information based on the profile selection. For the third party gateways, there are additional parameters required to be gathered along with the SITE name. The new fields are for gathering the frame number, the unit number and the LGRP OPTION data. These new fields will be populated in the GUI based on the query of a specific field in the GW profile definition.

17.10.2.1.2 GUI usage and implications

A sample GUI for associating a third party GW is included below. Please note that the “Frame number” and “Unit number” fields are mandatory. The other 5 fields constitute the LGRPLOC field as defined in the LGRPINV table schema in the Core.

These five fields are optional fields, but if need to be specified, all the five fields must be specified, otherwise it will be considered an invalid input.

Note: The LGRPLOC part of the GUI is also applicable to the CICM GW profile. Only difference is that the “Frame number” and “Unit number” fields are not allowed to be input by the user during the “Associate GW” operation. This part of the GUI is mainly useful for entering the LGRPLOC data if required. Same rule applies in regards to a valid input for these five fields as explained above.



The image shows a Windows-style dialog box titled "Associate Media Gateway". It contains several input fields and dropdown menus for configuring a media gateway. The fields are organized into sections: Gateway information, LGRP Location, and Signal Protocol. At the bottom are "OK" and "Cancel" buttons.

Field	Value
Gateway name	MG10/00/5
Gateway IP address	47.142.44.88
Gateway controller name	GWC-10
Gateway profile name	TPARTY
Reserved terminations	1023
Gateway site name	CARY
LGRP Location	
Frame number	100
Unit number	2
Frame type	OTHR
Floor position	10
Row position	AA
Frame position	20
Unit position	40
Signal Protocol	
Protocol type	MEGACO (4)
Protocol port	2944
Protocol version	1.0

17.10.2.1.3 GUI size

Not applicable.

17.10.2.1.4 GUI fields

The following new fields are introduced as part of provisioning a third party gateway to successfully create a node in the CS2K core for the GW being added.

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Frame number	New	Not applicable	User Input	Frame Number	Not applicable
Unit number	New	Not applicable	User Input	Unit Number	Not applicable
Frame Type	New	Not applicable	User Input	Frame Type	Not applicable
Floor Position	New	Not applicable	User Input	Floor Position	Not applicable
Row Position	New	Not applicable	User Input	Row Position	Not applicable
Frame Position	New	Not applicable	User Input	Frame Position	Not applicable
Unit Position	New	Not applicable	User Input	Frame Position	Not applicable

17.10.2.1.5 Usage example

The “Associate Media Gateway” GUI will be used as before but with these additional fields for the third party GW profile, as explained in the above sections.

17.10.2.1.6 GUI release history update

Not applicable.

17.10.2.1.7 Supplementary information

NONE.

17.10.3 CLUI Interface

There are 3 sub-sections in this component. One of them is the XML interface for providing the end-point provisioning and the other component includes the Batch Provisioning Tool (BPT) enhancements to support bulk provisioning of end-points. These are discussed in detail in the following sections:

17.10.3.1 XML interface for GW provisioning:

The XML interface for Associate MG XML command in Nodes Provisioning facilitates provisioning the LGRPLOC information including the frame and the unit number data in the input XMLs for this command.

Please see later sections for the corresponding schema definitions (XSDs) and the XML document templates.

17.10.3.2 XML interface for end-point provisioning:

The end-point pre-provisioning is achieved by using XML from the OSSGATE interface similar to Nodes Provisioning.

The following are the supported XML commands:

1. addLineEndpoint
2. delLineEndpoint
3. queryLineEndpoint
4. queryAllLineEndpoints

The above mentioned XML commands are the OSS interfaces supported by this feature. A brief description of each one of these interfaces, including input parameters and possible output parameters are listed below.

A brief description of the common parameters used across these different commands:

- **mgUIName** - Fully qualified gateway name. This can be 1 - 32 characters long. TYPE *string*.
- **endpointName** - Name of the end-point that is being provisioned. This can be 1 - 32 characters long. TYPE *string*.
- **circuitNumber** - Number to associate the terminal with. The range of this value is 0 - 1022. TYPE *unsignedShort*
- **cardCode** - String that defines the card code associated with the card. TYPE *string*. Optional parameter. The default is RDL SG.
- **padGroup** - String that defines the pad group. TYPE *string*. Optional parameter. The default is PKLNL.
- **ground** - String that defines the ground property. TYPE *string*. Values can be “N” or “Y”. Optional parameter. The default is “N”.
- **version** - The version refers to the version of the method or operation - e.g., the AddSubscriber operation may have version 1.0 and 2.0, where version 1.0 takes parameters X and Y and version 2.0 takes parms X, Y, and Z. TYPE *decimal*.
- **usn** - Unique Sequence Number. This parameter is introduced to facilitate sending multiple XML commands in one file. This parameter value will be used to match the responses with the requests. TYPE *integer*.
- **RC** - Return Code. A numeric value indicating the result of the attempted operation (see Table 2, above for range and definitions of each possible value). TYPE *short*.
- **MsgTxt** - Appropriate text that describes the result of the operation. TYPE *string*.

Individual XML document structure for each of the end-point provisioning commands is described in the following sections:

addLineEndpoint - Interface/Method that adds a specified end-point to the SESM database and allocates a LEN to the corresponding terminal in CS2K Core.

- Input data:
 - usn
 - version
 - mgUIName
 - endpointName
 - cardCode - Default: RDTEBS
 - padGroup - Default: STDLN
 - ground - Default: N
- Output data:
 - usn (value should be the same as the input)
 - version (value should be the same as the input)
 - RC - Return Code
 - MsgTxt - Text data detailing specific results of the operation in terms of success or failure of the operation and possible indication of failure reason incase of a failure.

delLineEndpoint - Interface/Method that deletes a specified end-point from the SESM database and de-allocates LEN from the corresponding terminal in CS2K Core.

Pre-condition: Service on the end-point must be un-assigned before attempting this operation.

- Input data:
 - usn
 - version
 - mgUIName
 - endpointName
- OR
- To delete a bunch of end-points with a specified range of circuit numbers,
- circuitNumberBegin

-
- circuitNumberEnd

OR

To delete ALL the end-points on this GW

- ALL

- Output data:

- usn (value should be the same as the input)
- version (value should be the same as the input)
- RC - Return Code
- MsgTxt - Text data detailing specific results of the operation in terms of success or failure of the operation and possible indication of failure reason incase of a failure.

queryLineEndpoint - Interface/Method that queries a specific end-point data on this gateway.

The end-point data will be enclosed within the <Row> tags similar to the output of the other nodes XML operations.

- Input data:

- usn
- version
- mgUIName
- endpointName

- Output data:

- usn (value should be the same as the input)
- version (value should be the same as the input)
- usn (value should be the same as the input)
- version (value should be the same as the input)
- mgUIName
- endpointName
- CircuitNumber
- cardCode
- padGroup
- status
- ground
- status

- tid
- LEN
- RC - Return Code
- MsgTxt - Text data detailing specific results of the operation in terms of success or failure of the operation and possible indication of failure reason incase of a failure.

queryAllLineEndpoints - Interface/Method that queries all the end-points on this gateway.

The end-point data for each of the end-points will be enclosed within the <Row> tags similar to the output of the other nodes XML operations.

- Input data:
 - usn
 - version
 - mgUIName
- Output data:
 - usn (value should be the same as the input)
 - version (value should be the same as the input)
 - mgUIName
 - endpointName
 - CircuitNumber
 - cardCode
 - padGroup
 - status
 - ground
 - status
 - tid
 - LEN
 - RC - Return Code
 - MsgTxt - Text data detailing specific results of the operation in terms of success or failure of the operation and possible indication of failure reason incase of a failure.

17.10.3.2.1 XML - Example Commands and Responses

Introduction:

The end-point pre-provisioning capability is provided using the OSSGate interface with XML documents. This application takes XML based command files as input and returns XML formatted response messages. (See www.w3.org for more information on XML.)

OSSGate accepts client connections and forwards incoming XML input to the pre-provisioning application. The XML commands are parsed, processed, and the appropriate response is returned to the client.

The following format is the general file format for a valid XML input file:

Table 4 XML File Format

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <someMethod usn="1" version="1.0">
        <Parameters>
          <fieldName>somevalue</fieldName>
          <fieldName>somevalue</fieldName>
        </Parameters>
      </someMethod>
      <someMethod usn="2" version="1.0">
        <Parameters>
          <fieldName>somevalue</fieldName>
          <fieldName>somevalue</fieldName>
        </Parameters>
      </someMethod></Methods>
    </Command>
  </CommandList>
```

Response to XML commands are returned in XML formatted response documents. The following format is the general file format for a valid XML response file:

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Response>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <someMethod usn="1" version="1.0">
        <ReturnData>
          <fieldName>somevalue</fieldName>
          <RC>somevalue</RC>
          <MsgTxt>somevalue</MsgTxt>
        </ReturnData>
      </someMethod>
    </Methods>
  </Response>
</CommandList>
```

Few important guidelines for valid XML documents are:

- For every open tag there must be a close tag.
- Every attribute value must be quoted, either with single or double quotes, but they must be consistent.
- No attribute name may appear more than once in a single element.
- Elements must be nested (closed) properly.
- Only one root element is allowed.
- XML is case-sensitive.
- The document must be conforming to the rules defined in the XML schema file (XSD file). Please see later sections towards the end of this document for details on the individual XSD documents.

17.10.3.2.2 Examples of the pre-provisioning XMLs

The following are few examples of the end-point pre-provisioning commands for each operation supported by this activity. The XML messages in these examples are formatted for the ease of understanding.

addLineEndpoint Command:

Example of an **addLineEndpoint** XML request:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <addLineEndpoint usn="1" version="1.0">
        <Parameters>
          <mgUIName>MYMG000-0-1</mgUIName>
          <endpointName>aaln/1/2</endpointName>
          <circuitNumber>1</circuitNumber>
          <cardCode>RDTLSG</cardCode>
          <padGroup>PKLNL</padGroup>
        </Parameters>
      </addLineEndpoint>
    </Methods>
  </Command>
</CommandList>
```

delLineEndpoint XML Command:

Example of a **delLineEndpoint** XML request:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <delLineEndpoint usn="1" version="1.0">
        <Parameters>
          <mgUIName>MYMG000-0-1</mgUIName>
          <endpointName>aaln/1/2</endpointName>
        </Parameters>
      </delLineEndpoint>
    </Methods>
  </Command>
</CommandList>
```

Example of a **delLineEndpoint** request for deleting **a range** of end-points (with circuit numbers ranging from 2 - 10 with limits inclusive) of this gateway:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <delLineEndpoint usn="1" version="1.0">
        <Parameters>
          <mgUIName>MYMG000-0-1</mgUIName>
          <circuitNumberBegin>2</circuitNumberBegin>
          <circuitNumberEnd>10</circuitNumberEnd>
        </Parameters>
      </delLineEndpoint>
    </Methods>
  </Command>
</CommandList>
```

Example of a **delLineEndpoint** request for deleting **ALL** the end-point of this gateway:

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <delLineEndpoint usn="1" version="1.0">
        <Parameters>
          <mgUIName>MYMG000-0-1</mgUIName>
        </Parameters>
      </delLineEndpoint>
    </Methods>
  </Command>
</CommandList>

```

queryLineEndpoint XML Command:

Example of a **queryLineEndpoint** XML request:

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <queryLineEndpoint usn="1" version="1.0">
        <Parameters>
          <mgUIName>MYMG000-0-1</mgUIName>
          <endpointName>aaln/1/2</endpointName>
        </Parameters>
      </queryLineEndpoint>
    </Methods>
  </Command>
</CommandList>

```

Example of a **qryAllLineEndpoints** request for querying **ALL** the end-point of this gateway:

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <queryAllLineEndpoints usn="1" version="1.0">
        <Parameters>
          <mgUIName>MYMG000-0-1</mgUIName>
        </Parameters>
      </queryAllLineEndpoints>
    </Methods>
  </Command>
</CommandList>

```

Examples of Response XMLs:

addLineEndpoint Response with 4 commands:

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
<Response>
<Interface>cs2kCfgMgrIf</Interface>
<Methods>
  <addLineEndpoint usn="1" version="1.0">
    <ReturnData>
      <RC>18</RC>
      <MsgTxt>The MG service type is not supported by the GWC.</MsgTxt>
    </ReturnData>
  </addLineEndpoint>
  <addLineEndpoint usn="2" version="1.0">
    <ReturnData>
      <RC>18</RC>
      <MsgTxt>The MG service type is not supported by the GWC.</MsgTxt>
    </ReturnData>
  </addLineEndpoint>
  <addLineEndpoint usn="3" version="1.0">
    <ReturnData>
      <RC>18</RC>
      <MsgTxt>The MG service type is not supported by the GWC.</MsgTxt>
    </ReturnData>
  </addLineEndpoint>
  <addLineEndpoint usn="4" version="1.0">
    <ReturnData>
      <RC>18</RC>
      <MsgTxt>The MG service type is not supported by the GWC.</MsgTxt>
    </ReturnData>
  </addLineEndpoint>
</Methods>
</Response>
</CommandList>

```

delLineEndpoint XML Response:

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
<Response>
<Interface>cs2kCfgMgrIf</Interface>
<Methods>
  <delLineEndpoint usn="1" version="1.0">
    <ReturnData>
      <RC>18</RC>
      <MsgTxt>Delete Failed </MsgTxt>
    </ReturnData>
  </delLineEndpoint>
</Methods>
</Response>
</CommandList>

```

queryLineEndpoint XML Response:

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
<Response>
<Interface>cs2kCfgMgrIf</Interface>
<Methods>
  <queryLineEndpoint usn="1" version="1.0">
    <ReturnData>
      <mgUIName>myMG.usa.net</mgUIName>
      <Row>
        <endpointName>first/ep</endpointName>
        <circuitNumber>1010</circuitNumber>
        <cardCode>RDTLSG</cardCode>
        <padGroup>PKLNL</padGroup>
        <ground>N</ground>
        <status>HASU</status>
        <tid>1011</tid>
        <LEN>CARY 111 2 10 10</LEN>
      </Row>
      <RC>0</RC>
      <MsgTxt>Query Single Endpoint Successful</MsgTxt>
    </ReturnData>
  </queryLineEndpoint>
</Methods>
</Response>
</CommandList>

```

queryAllLineEndpoints XML Response:


```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
<Response>
<Interface>cs2kCfgMgrIf</Interface>
<Methods>
<queryAllLineEndpoints usn="1" version="1.0">
<ReturnData>
  <mgUIName>thirdParty.us.com</mgUIName>
  <Row>
    <endpointName>first/ep</endpointName>
    <circuitNumber>1010</circuitNumber>
    <cardCode>RDTLSG</cardCode>
    <padGroup>PKLNL</padGroup>
    <ground>N</ground>
    <status>HASU</status>
    <tid>1011</tid>
    <LEN>CARY 111 2 10 10</LEN>
  </Row>
  <Row>
    <endpointName>second/ep</endpointName>
    <circuitNumber>1011</circuitNumber>
    <cardCode>RDTLSG</cardCode>
    <padGroup>PKLNL</padGroup>
    <ground>Y</ground>
    <status>WORKING</status>
    <tid>1012</tid>
    <LEN>CARY 111 2 10 10</LEN>
  </Row>
  <RC>0</RC>
  <MsgTxt>Query endpoints operation successful</MsgTxt>
</ReturnData>
</queryAllLineEndpoints>
</Methods>
</Response>
</CommandList>

```

assocmg XML Command:

Example of a **assocmg** XML request:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <assocMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>MyGW.ext.net</mgUIName>
          <mgProfileName>THIRD_PARTY</mgProfileName>
          <mgIpAddr>47.171.3.44</mgIpAddr>
          <mgProtocolPort>2427</mgProtocolPort>
          <gwcUIName>GWC-2</gwcUIName>
          <lgrpLocation>
            <frameType>ABCD</frameType>
            <frameNumber>5</frameNumber>
            <unitNumber>8</unitNumber>
            <floorPosition>10</floorPosition>
            <rowPosition>SS</rowPosition>
            <framePosition>44</framePosition>
          </lgrpLocation>
        </Parameters>
      </assocMG>
    </Methods>
  </Command>
</CommandList>
```

17.10.3.2.3 XML Schema Language (XSD)

XML Schemas validate each incoming XML request and ensure that the instance document follows the required content model and the parameters are valid before sending the provisioning request down to the Server.

addLineEndpoint.xsd:

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  version="1.0"
  xml:lang="en" >

  <!-- ***** -->
  <!-- * Define Method Parameters -->
  <!-- ***** -->
  <xsd:complexType name="addLineEndpointMethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="addLineEndpointParamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addLineEndpointParamsType">
    <xsd:sequence>
      <xsd:element name="mgUIName" type="NoSpaceNameType" />
      <xsd:element name="endpointName" type="NoSpaceNameType" />
      <xsd:element name="circuitNumber" type="CircuitNumberType" minOccurs="0" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
```

```

        <xsd:element name="cardCode" type="xsd:token" default="RDTLSG"
minOccurs="0" />
        <xsd:element name="padGroup" type="xsd:token" default="PKLNL"
minOccurs="0" />
        <xsd:element name="ground" type="xsd:string" default="N"
minOccurs="0" />
    </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

delLineEndpoint.xsd

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
            xml:lang="en" >

    <!-- ***** -->
    <!-- * Define Method Parameters -->
    <!-- ***** -->
    <xsd:complexType name="delLineEndpointMethodType">
        <xsd:all>
            <xsd:element name="Parameters" type="delLineEndpointParamsType" />
        </xsd:all>
        <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
    </xsd:complexType>
    <xsd:complexType name="delLineEndpointParamsType">
        <xsd:sequence>
            <xsd:element name="mgUIName" type="NoSpaceNameType" />
            <xsd:choice minOccurs="0">
                <xsd:element name="endpointName" type="NoSpaceNameType" />
                <xsd:sequence>
                    <xsd:element name="circuitNumberBegin" type="CircuitNumberType" />
                    <xsd:element name="circuitNumberEnd" type="CircuitNumberType" />
                </xsd:sequence>
            </xsd:choice>
        </xsd:sequence>
    </xsd:complexType>
</xsd:schema>

```

queryLineEndpoint.xsd

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            version="1.0"
            xml:lang="en" >

    <!-- ***** -->
    <!-- * Define Method Parameters -->
    <!-- ***** -->
    <xsd:complexType name="queryLineEndpointMethodType">
        <xsd:all>
            <xsd:element name="Parameters" type="queryLineEndpointParamsType" />
        </xsd:all>
        <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
    </xsd:complexType>

```

```

</xsd:complexType>
<xsd:complexType name="queryLineEndpointParamsType">
  <xsd:sequence>
    <xsd:element name="mgUIName" type="NoSpaceNameType" />
    <xsd:element name="endpointName" type="NoSpaceNameType" />
  </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

queryAllLineEndpoints.xsd

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  version="1.0"
  xml:lang="en" >

  <!-- ***** -->
  <!-- * Define Method Parameters -->
  <!-- ***** -->
  <xsd:complexType name="queryAllLineEndpointsMethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="queryAllLineEndpointsParamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="queryAllLineEndpointsParamsType">
    <xsd:sequence>
      <xsd:element name="mgUIName" type="NoSpaceNameType" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

```

assomg.xsd:

```

<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:sequence>
  </xsd:complexType>
  <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="lgrpLocation" type="LGRPLocationType" minOccurs="0"
/>
    <xsd:choice minOccurs="0">
        <xsd:element name="pepServerName" 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:sequence>
</xsd:complexType>
</xsd:schema>

```

cs2cfgbase.xsd:

Note: Only updates are shown here, the previous content will be left unchanged.

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    version="1.0"
    xml:lang="en" >
    <xsd:include schemaLocation="snbase.xsd"/>
    <xsd:include schemaLocation="assocmg.xsd"/>
    <xsd:include schemaLocation="addLineEndpoint.xsd"/>
    <xsd:include schemaLocation="delLineEndpoint.xsd"/>
    <xsd:include schemaLocation="queryLineEndpoint.xsd"/>
    <xsd:include schemaLocation="queryAllLineEndpoints.xsd"/>

<!--
*****
***** -->
<!-- ** Define Parser Convention Required elements -->
<!-- ** These are CommandList (root element), Comand, Interface, Methods -->
<!--
*****
***** -->
    <xsd:element name="CommandList" >
        <xsd:complexType >
            <xsd:sequence>
                <xsd:element name="Command" type="CommandType" />
            </xsd:sequence>
        </xsd:complexType >
    </xsd:element>

    <!-- Define CommandType -->
    <xsd:complexType name="CommandType">
        <xsd:sequence>
            <xsd:element name="Interface" type="cs2kCfgMgrIfType"/>
            <xsd:element name="Methods" type="cs2kCfgMgrIfMethodsType" />
        </xsd:sequence>
    </xsd:complexType>

```

```

<!--
*****
***** -->
<!-- ** Define cs2kCfgMgrIfType -->
<!--
*****
***** -->

    <!-- cs2kCfgMgrIfType -->
    <xsd:simpleType name="cs2kCfgMgrIfType">
        <xsd:restriction base="xsd:token">
            <xsd:enumeration value="cs2kCfgMgrIf" />
        </xsd:restriction>
    </xsd:simpleType>

    <!-- ***** -->
    <!-- * Define interface cs2kCfgMgrIfMethods -->
    <!-- ***** -->
    <xsd:complexType name="cs2kCfgMgrIfMethodsType">
        <xsd:choice minOccurs="1" maxOccurs="unbounded">
            <xsd:element name="assocMG" type="assocMGMethodType" />

            <xsd:element name="addLineEndpoint" type="addLineEndpointMethodType" /
> <!-- NEW -->
            <xsd:element name="delLineEndpoint" type="delLineEndpointMethodType" /
> <!-- NEW -->
            <xsd:element name="queryLineEndpoint" type="queryLineEndpointMethodType"
/> <!-- NEW -->
            <xsd:element name="queryAllLineEndpoints"
type="queryAllLineEndpointsMethodType" /> <!-- NEW -->

        </xsd:choice>
    </xsd:complexType>

    <!--
*****
***** -->
    <!-- * Define FrameNumberType -->
    <!--
*****
***** -->
    <xsd:simpleType name="FrameNumberType">
        <xsd:restriction base="xsd:unsignedShort">
            <xsd:minInclusive value="0" />
            <xsd:maxInclusive value="511" />
        </xsd:restriction>
    </xsd:simpleType>

    <!--
*****
***** -->
    <!-- * Define UnitNumberType -->
    <!--
*****
***** -->
    <xsd:simpleType name="UnitNumberType">
        <xsd:restriction base="xsd:unsignedShort">
            <xsd:minInclusive value="0" />
            <xsd:maxInclusive value="9" />

```

```

    </xsd:restriction>
</xsd:simpleType>

<!--
*****
***** -->
    <!-- * Define CircuitNumberType -->
*****
***** -->
    <!--
*****
***** -->
    <xsd:simpleType name="CircuitNumberType">
        <xsd:restriction base="xsd:unsignedShort">
            <xsd:minInclusive value="0" />
            <xsd:maxInclusive value="1022" />
        </xsd:restriction>
    </xsd:simpleType>

    <!-- *****
-->
    <!-- * Define LGRPLocType-->
    <!-- *****
-->
<xsd:complexType name="LGRPLocationType">
    <xsd:all>
        <xsd:element name="frameType" type="xsd:string" minOccurs="0"/>
        <xsd:element name="frameNumber" type="FrameNumberType"/>
        <xsd:element name="unitNumber" type="UnitNumberType" />
        <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:all>
</xsd:complexType>

</xsd:schema>

```

17.10.3.3 Batch Provisioning Tool (bpt):

The SESM application, 'bpt', is a command line tool that provides an ability to perform bulk provisioning. Enhancements to this tool include new menu options to facilitate end-point bulk provisioning and a new option to facilitate converting query end-point operation output into add end-point operation input.

In addition, the 'bpt' help text will be updated to include the new enhancements. The 'bpt' menus are enhanced as follows:

```
=====
```

Batch Provisioning Tool (BPT V1.0)

```
=====
```

Username:ptm

Password:

Login in progress...

You are currently logged in as: ptm

=====

Main Menu:

=====

- (1) Execute Batch File
- (2) Display Output
- (3) Display Logs
- (4) Delete Output or Log Files
- (h) Help
- (x) Exit

Selection: [1/2/3/4/h/x:1] 1

=====

Provisioning Input Entry Menu:

=====

Coming from this menu:

- (1) *Lines*
- (2) *ADSL*
- (3) ***Line Endpoints***
- (4) *Go to shell prompt*
- (r) *Return to the main menu.*
- (x) *Exit BPT.*

Selection: [1/2/3/4/r/x:1] 3

=====

Line Endpoints Sub-Menu:

=====

(1) Line Endpoints

(2) Export queryLineEndpoints Output

(b) Back to the previous menu

(r) Return to the main menu

(x) Exit BPT.

Selection: [1/2/b/r/x:1] 1

Which mode would you like to have the log file on? Critical/Verbose/Major/Minor [c/v/ma/mi:c]:c

Please enter the input file name :

For the “export” command (option 4 on the ‘Provisioning Input Entry Menu’), the generated output xml file name will be auto generated and (in a format for addLineEndpoint XML command) will be available on the SESM Server at the following location:

/opt/nortel/NTsesm/tools/bpt/output/export

The line endpoints menu will be integrated into the other menus of bpt for managing the output files and the log files. For ex, following are the output snapshots:

For output file management:

=====

Main Menu:

=====

- (1) Execute Batch File
- (2) Display Output
- (3) Display Logs
- (4) Delete Output or Log Files
- (h) Help

- (x) Exit

Selection: [1/2/3/4/h/x:1] 2

=====

Display Output Menu:

=====

Coming from this menu: output

- (1) Lines
- (2) ADSL
- (3) Line Endpoints**
- (4) Go to shell prompt
- (r) Return to the main menu.
- (x) Exit BPT.

Selection: [1/2/3/4/r/x:1] 3

=====

Line Endpoints Sub-Menu:

=====

- (1) Line Endpoints
- (2) Export queryLineEndpoints Output
- (b) Back to the previous menu
- (r) Return to the main menu
- (x) Exit BPT.

Selection: [1/2/b/r/x:1] 1

The following files are listed in the output directory:

test.xml

Please enter the file name (or press 'Enter' to go to the previous menu):

For Log file management:

=====

Main Menu:

=====

- (1) Execute Batch File
- (2) Display Output
- (3) Display Logs
- (4) Delete Output or Log Files

(h) Help

(x) Exit

Selection: [1/2/3/4/h/x:1] 3

=====

Display Log File Menu:

=====

(1) Lines

(2) ADSL

(3) Line Endpoints

(4) Go to shell prompt

(r) Return to the main menu.

(x) Exit BPT.

Selection: [1/2/3/4/r/x:1] 3

For deleting output or log files:

=====

Main Menu:

=====

(1) Execute Batch File

(2) Display Output

(3) Display Logs

(4) Delete Output or Log Files

(h) Help

(x) Exit

Selection: [1/2/3/4/h/x:1] 4

=====

Delete Files Menu:

=====

Coming from this menu: del

(1) Lines

(2) ADSL

(3) Line Endpoints

(4) Go to shell prompt

(r) Return to the main menu.

(x) Exit BPT.

Selection: [1/2/3/4/r/x:1] 3

Going to show Line EP Sub-menu

The input parm is dollar 1: del

=====

Line Endpoints Sub-Menu:

=====

- (1) Line Endpoints
- (2) Export queryLineEndpoints Output
- (b) Back to the previous menu
- (r) Return to the main menu
- (x) Exit BPT.

Selection: [1/2/b/r/x:1]

17.11 Command interface changes

Not applicable.

17.12 Security

Authorization is supported based on the user privileges similar to other Nodes related operations. All the end-point pre-provisioning XML commands are allowed to be performed *only if the logged in user is successfully authorized for that particular operation*. Each operation requires a level of authorization and the user has to belong to a specific group that has the required access rights or to a higher group in the hierarchy of the defined groups.

Here is the mapping of each of the XML command to the required permissions:

addLineEndpoint=nortel.mgc.iprov

delLineEndpoint=nortel.mgc.iprov

qryLineEndpoint=nortel.mgc.ro

All the successful authorization attempts will be logged to the audit log located in /var/log directory on the SESM server.

All the authorization failures will be logged to the security log located in /var/log directory on the SESM server.

17.12.1 Network configuration

Not applicable.

17.12.2 Key management

Not applicable.

17.12.3 Protocol

Not applicable.

17.12.4 Authentication

Not impacted. Same authentication to log-in to the SESM GUI is applicable.

17.13 Configuration Walkthrough

The general order of provisioning is as follows:

- Provision table SITE in CS2K Core. SITE values for third party gateways should be restricted for use for this type of gateways.
- Provision table PADDDATA in CS2K Core (PKLNL and PKNIL entries).
- Provision the third party gateway in SESM (autocreates LGRPINV entry).
- Configure the gateway at its EM, if needed.
- Pre-provision the GW end-points from OSSGATE (autocreates LNINV entry)
- Execute SERVORD+ commands via OSSGate (service is assigned to LENS in LNINV).

18: A00007074 Configuration (CN)

18.1 Feature name

GigE Link Maintenance

18.2 Hardware and Software Requirements

Not Applicable.

18.3 Initial Configuration

Not Applicable

18.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable

18.5 Upgrade Considerations

Not Applicable

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)
ifEntry table	Changed	Changed
ifMauEntry	New	New
ifJackEntry	New	New
ifMauAutoNegEntry	New	New
dot3Stats	New	New
dot3HCStatsEntry	New	New
dot3PauseEntry	New	New
EtherStatsEntry	New	New
MediaIndependentEntry	New	New
EtherStatsHighCapacityEntry	New	New
EtherHistoryEntry	New	New
EtherHistoryHighCapacityEntry	New	New
nnGLinkConfigTable	New	New

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
nnGLinkFaultConfigTable	New	New
nnGLinkThresholdTable	New	New
nnGLinkSoakTable	New	New
nnGLinkProtGroupTable	New	New
nnGLinkOmCurrTable	New	New
nnGLinkOmIntervTable	New	New

18.6.2 Table/MIB/Remote Database Schema information

18.6.2.1 Name: ifEntry table

18.6.2.1.1 Functional description

A list of interface entries. The number of entries is given by the value of ifNumber. This table has been modified to allow for Gige specific values. See RFC2863 for details.

18.6.2.1.2 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ifEntry	8	8	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.1.3 Fields/OIDs

The following table lists fields/OIDs for ifEntry Table.

Table 3 Table field descriptions

Field	Default	Read/Write Access	Size	Note
ifDesc	“Nortel-pec-frame-shelf-slot-port-gige”	Read	DisplayString	

Table 3 Table field descriptions

Field	Default	Read/Write Access	Size	Note
ifType	ethernetCsmacd	Read	IANAifType	
ifMtu	1600	Read	Integer32	
ifSpeed	1000000000 bps	Read	Gauge32	
ifPhysAddress	“mac address”	Read	PhysAddress	
ifAdmin	Down	Read/Write	Integer	
ifOper	notPresent	Read	Integer	
ifLastChange	0	Read	Timeticks	
ifName	“protgroup-slot-port”	Read		
ifLinkUpDownTrapEnable	enabled	Read/Write	Integer	
ifHighSpeed	1000	Read	Gauge32	
ifConnectorPresent	true	Read	Truth value	

18.6.2.2 Name: ifMauEntry table**18.6.2.2.1 Functional description**

Table of descriptive and status information about MAU(s) attached to an interface. See RFC3636 for details

18.6.2.2.2 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ifMauEntry	8	8	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.2.3 Fields/OIDs

The following table lists fields/OIDs for ifMauEntry Table.

Table 5 Table field descriptions

Field	Default	Read/Write Access	Size	Note
ifMauIfIndex	ifindex from rfc 2863	read	InterfaceIndex	
ifMauIndex	0	read	ifMauIndex	
ifMauType	unknownMauType	read	AutonomousType	
ifMauStatus	Shutdown or unknown	read	INTEGER	
ifMauMediaAvailable		read	INTEGER	
ifMauMediaAvailableStateExits		read	Counter32	
ifMauJabberState	noJabber	read	INTEGER	
ifMauJabberingStateEnters	0	read	Counter32	
ifMauDefaultType		Read-write	AutonomousType	
ifMauAutoNegSupported	true	read	TruthValue	
ifMauTypeListBits		read	BITS	2
ifMauHCFALSECarriers			Counter64	1

Note 1) Unknown whether the hardware can support this counter

Note 2) bits b1000baseXFD(22),b1000baseLXFD(24),b1000baseSXF(26), and b1000baseCXFD(28) will be set.

18.6.2.3 Name: ifJackEntry table

18.6.2.3.1 Functional description

Information about the external jacks attached to MAUs attached to an interface. See RFC3636 for details

18.6.2.3.2 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ifJackEntry	8	8	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.3.3 Fields/OIDs

The following table lists fields/OIDs for **ifJackEntry** Table.

Table 7 Table field descriptions

Field	Default	Read/Write Access	Size	Note
ifJackIndex	ifIndex	Not-accessible	Integer32	
ifJackType	0	read	JackType	1
ifMauHCFALSECarriers			Counter64	1

Note 1) if unsupported jack type raise fault and don't allow link to unlock

18.6.2.4 Name: IfMauAutoNegEntry table

18.6.2.4.1 Functional description

Configuration and status objects for the auto-negotiation function of MAUs attached to interfaces. The ifMauAutoNegTable applies to systems in which auto-negotiation is supported on one or more MAUs attached to interfaces. Note that if auto-negotiation is present and enabled, the ifMauType object reflects the result of the auto-negotiation function." See RFC3636 for details

18.6.2.4.2 Size

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IfMauAutoNegEntry	8	8	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.4.3 Fields/OIDs

The following table lists fields/OIDs for **IfMauAutoNegEntry** Table.

Table 9 Table field descriptions

Field	Default	Read/Write Access	Size	Note
ifMauAutoNegAdminStatus	enabled	Read-write	INTEGER	
ifMauAutoNegRemoteSignaling	notdetected	read	INTEGER	
ifMauAutoNegConfig	configuring	read	INTEGER	
ifMauAutoNegRestart	norestart	Read-write	INTEGER	
ifMauAutoNegCapabilityBits		read	BITS	1
ifMauAutoNegCapAdvertisedBits		Read-write	BITS	1
ifMauAutoNegCapReceiveDBits	0	read	BITS	
ifMauAutoNegRemoteFaultAdvertised	offline	Read-write	INTEGER	
ifMauAutoNegRemoteFaultReceived	noerror	read	INTEGER	

Note 1) bits

bfdxPause(8),bfdxAPause(9),bfdxSPause(10),bfdxBPause(11),bfdxbaseXFD(13) will be set

18.6.2.5 Name: dot3stats table

18.6.2.5.1 Functional description

Configuration and status objects for the Dot3 stats function of each interface.
See RFC3635 for details

18.6.2.5.2 Size

Table 10 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
dot3stats	8	8	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.5.3 Fields/OIDs

The following table lists fields/OIDs for dot3stats Table.

Table 1: RFC3635 dot3stats table

ifdot3StatsEntryField	Default Value	Read/Write Access	size
dot3StatsIndex	ifIndex	read	InterfaceIndex
dot3StatsSingleCollisionFrames	0	read	Counter32
dot3StatsMultipleCollisionFrames	0	read	Counter32
dot3StatsSQETestErrors	0	read	Counter32
dot3StatsDeferredTransmissions	0	read	Counter32
dot3StatsLateCollisions	0	read	Counter32
dot3StatsExcessiveCollisions	0	read	Counter32
dot3StatsCarrierSenseErrors	0	read	Counter32
dot3StatsDuplexStatus	fullDuplex	read	INTEGER
dot3StatsRateControlAbility	true	read	TruthValue
dot3StatsRateControlStatus	unknown	read	INTEGER
dot3HCStatsAlignmentErrors	0	read	Counter64
dot3HCStatsFCSErrors	0	read	Counter64
dot3HCStatsInternalMacTransmitErrors	0	read	Counter64
dot3HCStatsFrameTooLongs	0	read	Counter64
dot3HCStatsInternalMacReceiveErrors	0	read	Counter64
dot3HCStatsSymbolErrors	0	read	Counter64

18.6.2.6 Name: dot3pauseentry Table

18.6.2.6.1 Functional description

Configuration and status objects for the Dot3 pause function of each interface. See RFC3635 for details

18.6.2.6.2 Size

Table 11 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
dot3pauseentry	8	8	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.6.3 Fields/OIDs

The following table lists fields/OIDs for dot3PauseEntry Table.

Table 2: RFC3635 dot3PauseEntry table

ifdot3PauseEntryField	Default Value	Read/Write Access	size
dot3PauseAdminMode	enabledXmitAndRcv	Read-write	INTEGER
dot3PauseOperMode	enabledXmitAndRcv	read	INTEGER
dot3InPauseFrames	0	read	Counter32
dot3OutPauseFrames	0	read	Counter32
dot3HCInPauseFrames	0	read	Counter64
dot3HCOutPauseFrames	0	read	Counter64

indexed by ifIndex

18.6.2.7 Name: Etherstatsentry Table

18.6.2.7.1 Functional description

Configuration and status objects for the ethernet statistics function of each interface. See RFC2819 for details

18.6.2.7.2 Size**Table 12 Table size**

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
etherstatsentry	8	8	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.7.3 Fields/OIDs

The following table lists fields/OIDs for EtherStatsEntry Table.

Table 3: RFC 2819 EtherStatsEntry

Attribute	Default	Access	Type	Note
etherStatsIndex	IF index	Read	Integer32	
etherStatsDataSource	0	Read	OBJECT IDENTIFIER	
etherStatsDropEvents	0	Read	Counter32	
etherStatsBroadcastPkts	0	Read	Counter32	
etherStatsMulticastPkts	0	Read	Counter32	
etherStatsCRCAlignErrors	0	Read	Counter32	
etherStatsUndersizePkts	0	Read	Counter32	
etherStatsOversizePkts	0	Read	Counter32	
etherStatsFragments	0	Read	Counter32	
etherStatsJabbers	0	Read	Counter32	1
etherStatsCollisions	0	Read	Counter32	1
etherStatsOwner	“Frame,shelf,slot,port”	Read	OwnerString	
etherStatsStatus	invalid	Read	EntryStatus	

Note 1: Not collected, always zero

18.6.2.8 Name: MediaIndependentEntry Table**18.6.2.8.1 Functional description**

Configuration and status objects for the Media Independent statistics function of each interface. See RFC3273 for details

18.6.2.8.2 Size

Table 13 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MediaIndependentEntry	8	8	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.8.3 Fields/OIDs

The following table lists fields/OIDs for MediaIndependentEntry Table.

Table 4: RFC 3273 MediaIndependentEntry

Attribute	Default	Access	Type
mediaIndependentIndex	IF index	Read	Integer32
mediaIndependentDataSource	ifIndex.y where y is one of our port ifindexs	Read	OBJECT IDENTIFIER
mediaIndependentDropEvents	0	Read	Counter32
mediaIndependentDroppedFrames	0	Read	Counter32
mediaIndependentInOverflowPkts	0	Read	Counter32
mediaIndependentInHighCapacityPkts	0	Read	Counter64
mediaIndependentOutOverflowPkts	0	Read	Counter32
mediaIndependentOutHighCapacityPkts	0	Read	Counter64
mediaIndependentInOverflowOctets	0	Read	Counter32
mediaIndependentInHighCapacityOctets	0	Read	Counter64
mediaIndependentOutOverflowOctets	0	Read	Counter32
mediaIndependentOutHighCapacityOctets	0	Read	Counter64
mediaIndependentInNUCastOverflowPkts	0	Read	Counter32
mediaIndependentInNUCastHighCapacityPkts	0	Read	Counter64
mediaIndependentOutNUCastOverflowPkts	0	Read	Counter32
mediaIndependentOutNUCastHighCapacityPkts	0	Read	Counter64
mediaIndependentInErrors	0	Read	Counter32
mediaIndependentOutErrors	0	Read	Counter32
mediaIndependentInputSpeed	1000000	Read	Gauge32
mediaIndependentOutputSpeed	1000000	Read	Gauge32
mediaIndependentDuplexMode	fullduplex(2)	Read	INTEGER
mediaIndependentDuplexChanges	0	Read	Counter32
mediaIndependentDuplexLastChange	0	Read	TimeStamp
mediaIndependentOwner	"Frame,shelf,slot,port"	Read	OwnerString
mediaIndependentStatus	???	Read	RowStatus

18.6.2.9 Name: EtherStatshighCapacityEntry Table**18.6.2.9.1 Functional description**

Configuration and status objects for the Ethernet high capacity statistics function of each interface. See RFC3273 for details

18.6.2.9.2 Size**Table 14 Table size**

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
EtherStatshighCapacityEntry	8	8	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.9.3 Fields/OIDs

The following table lists fields/OIDs for EtherStatshighCapacity Table.

Table 5: RFC 3273 EtherStatshighCapacityEntry

Attribute	Default	Access	Type	Note
etherStatsHighCapacityOverflowPkts	0	Read	Counter32	
etherStatsHighCapacityPkts	0	Read	Counter64	
etherStatsHighCapacityOverflowOctets	0	Read	Counter32	
etherStatsHighCapacityOctets	0	Read	Counter64	
etherStatsHighCapacityOverflowPkts64Octets	0	Read	Counter32	1
etherStatsHighCapacityPkts64Octets	0	Read	Counter64	1
etherStatsHighCapacityOverflowPkts65to127Octets	0	Read	Counter32	1
etherStatsHighCapacityPkts65to127Octets	0	Read	Counter64	1
etherStatsHighCapacityOverflowPkts128to255Octets	0	Read	Counter32	1
etherStatsHighCapacityPkts128to255Octets	0	Read	Counter64	1
etherStatsHighCapacityOverflowPkts256to511Octets	0	Read	Counter32	1
etherStatsHighCapacityPkts256to511Octets	0	Read	Counter64	1
etherStatsHighCapacityOverflowPkts512to1023Octets	0	Read	Counter32	1
etherStatsHighCapacityPkts512to1023Octets	0	Read	Counter64	1
etherStatsHighCapacityOverflowPkts1024to1518Octets	0	Read	Counter32	1
etherStatsHighCapacityPkts1024to1518Octets	0	Read	Counter64	1

indexed by ifIndex

Note 1: Not collected, always zero

18.6.2.10 Name: EtherHistoryEntry Table

18.6.2.10.1 Functional description

Configuration and status objects for the Ethernet historical statistics function of each interface. See RFC2819 for details

18.6.2.10.2 Size

Table 15 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
EtherHistoryEntry	8	8	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.10.3 Fields/OIDs

The following table lists fields/OIDs for EtherHistoryEntry Table.

Table 6: RFC 2819 EtherHistoryEntry

Attribute	Default	Access	Type	Note
etherStatsIndex	IF index	Read	Integer32	
etherHistorySampleIndex	0	Read	Integer32	
etherHistoryIntervalStart	0	Read	TimeTicks	
etherHistoryDropEvents	0	Read	Counter32	
etherHistoryBroadcastPkts	0	Read	Counter32	
etherHistoryMulticastPkts	0	Read	Counter32	
etherHistoryCRCAlignErrors	0	Read	Counter32	
etherHistoryUndersizePkts	0	Read	Counter32	
etherHistoryOversizePkts	0	Read	Counter32	
etherHistoryFragments	0	Read	Counter32	
etherHistoryJabbers	0	Read	Counter32	1
etherHistoryCollisions	0	Read	Counter32	1
etherHistoryUtilization	0	Read	Integer32	

Note 1: Not collected, always zero

18.6.2.11 Name: EtherHistoryHighCapacityEntry Table

18.6.2.11.1 Functional description

Configuration and status objects for the Ethernet High Capacity historical statistics function of each interface. See RFC2819 for details

18.6.2.11.2 Size

Table 16 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
EtherHistoryHighCapacityEntry	8	8	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.11.3 Fields/OIDs

The following table lists fields/OIDs for EtherHistoryHighCapacityEntry Table.

Table 7: RFC 3273 EtherHistoryHighCapacityEntry

Attribute	Default	Access	Type	Note
etherHistoryHighCapacityOverflowPkts	0	Read	Integer32	
etherHistoryHighCapacityPkts	0	Read	CounterBasedGauge64	
etherHistoryHighCapacityOverflowOctets	0	Read	Gauge32	

etherHistoryHighCapacityOctets	0	Read	CounterBasedGauge64	

indexed by etherStatsIndex and etherHistorySampleIndex

18.6.2.12 Name: nnGLinkConfigTable table

18.6.2.12.1 Functional description

The GiGE Link Config Table contains management information for each GigE Link. Allows the Manager to config and Manage these links. There is one entry per GigE Link (port). See NORTEL-UEMG-GIGE-MIB for details. It can be found at <http://triweb/smg500/mibDir/mibList.html>

18.6.2.12.2 Size

Table 17 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
nnGLinkConfigTable	8	8	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.12.3 Fields/OIDs

The following table lists fields/OIDs for nnGLinkConfigTable Table.

Table 18 Table field descriptions

Field	Default	Read/Write Access	Size	Note
nnGLinkConfigIfIndex	ifIndex	Not-accessible	Integer32	
nnGLinkConfigWorkOrProt	notUsed	Read-write	INTEGER	
nnGLinkConfigNiOrSubte nding	notUsed	Read-write	INTEGER	
nnGLinkProtGrpNum	nullprtgrp=0	Read-write	Unsigned32	
nnGLinkConfigTxRfi	enabled	Read-write	INTEGER	
nnGLinkConfigRxRfi	enabled	Read-write	INTEGER	

Table 18 Table field descriptions

Field	Default	Read/Write Access	Size	Note
nnGLinkConfigIfPromMode	notPromMode	Read-write	INTEGER	
nnGLinkConfigIfMtu	1600	Read	Integer32	
nnGLinkConfigLoopBack	noLoop	Read-write	INTEGER	
nnGLinkConfigStatusCurrent	0	Read	INTEGER	
nnGLinkConfigPriority	1	Read-write	Integer32	
nnGLinkConfigOnlineStatus	offLine	Read-write	INTEGER	
nnGLinkConfigLaserStatus	off	Read	INTEGER	
nnGlinkForce	false	Read-write	INTEGER	new
nnGlinkBandWidth	1000?	Read-write	INTEGER	new 1

Note 1) In megabits to 2 decimal points, i.e. 1.67????

18.6.2.13 Name: nnGLinkFaultConfigTable

18.6.2.13.1 Functional description

The Fault Config Table maps Faults/Alarms to desired Severity. It allows manager to modify the alarmSeverity and to shutdown notification of these alarms, on each interface and for each Fault/Alarm type. There is one entry in this table for each Link and FaultType Pair, indexed by the ifIndex of the Link, and FaultType. See NORTEL-UEMG-GIGE-MIB for details. It can be found at <http://triweb/smg500/mibDir/mibList.html>. In SN08 this table will be filled in with defaults only as the Element Manager will have interface to change them.

18.6.2.13.2 Size

Table 19 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
nnGLinkFaultConfigTable	8x16	8x16	Memory is automatically allocated for 8 GigE interfaces and 16 fault types.

18.6.2.13.3 Fields/OIDs

The following table lists fields/OIDs for nnGLinkFaultConfigTable.

Table 20 Table field descriptions

Field	Default	Read/Write Access	Size	Note
nnGLinkFaultConfigType		na	NnGLinkFaultType	
nnGLinkFaultConfigNotify		Read-write	INTEGER	1
nnGLinkFaultConfigSeverity		Read-write	INTEGER	1
nnGLinkFaultConfigSoak		Read-write	INTEGER	1
nnGLinkFaultConfigAlmDef		Read-write	INTEGER	1

Note 1) defaults are dependent of fault type.

18.6.2.14 Name: nnGLinkThresholdTable

18.6.2.14.1 Functional description

The Threshold Table allows the Manager to configure Performance Thresholds for which the Agent will generate a Threshold Notifications when the performance Counter (Type) is crossed. There is one entry in this table for each Link / Threshold Counter Type pair (doubly indexed) default ratios:

Type	ShortPeriod Crossing	LongPeriod Crossing
ES	5 %	5 %

SES	5 %	5 %
UAS	1 %	1 %

See NORTEL-UEMG-GIGE-MIB for details. It can be found at <http://triweb/smg500/mibDir/mibList.html>.

18.6.2.14.2 Size

Table 21 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
nnGLinkThresholdTable	8x3	8x3	Memory is automatically allocated for 8 GigE interfaces and 3 Threshold types.

18.6.2.14.3 Fields/OIDs

The following table lists fields/OIDs for nnGLinkThresholdTable.

Table 22 Table field descriptions

Field	Default	Read/Write Access	Size	Note
nnGLinkThreshType		na	NnGLinkThresholdType	
nnGLinkThreshShortPeriod		Read	Unsigned32	
nnGLinkThreshShortRatio		Read-write	NnGLinkPercent	1
nnGLinkThreshLongPeriod		Read	Unsigned32	
nnGLinkThreshLongRatio		Read-write	NnGLinkPercent	1
nnGLinkThreshNotify	notify	Read-write	NnGLinkPercent	

Note 1) defaults are dependent of threshold type.

18.6.2.15 Name: nnGLinkSoakTable

18.6.2.15.1 Functional description

The Soak Table allows the Manager to configure Performance Counter soak times/values. There is one entry in this table for each GigE Link. The GR 253, GR 474 defines the standard soak times for performance counters but since certain customer networks run at different network quality levels where such networks require the soak times to be configurable so that management stations do not get flooded with PM threshold crossings.

See NORTEL-UEMG-GIGE-MIB for details. It can be found at <http://triweb/smg500/mibDir/mibList.html>.

18.6.2.15.2 Size

Table 23 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
nnGLinkSoakTable	8	8x3	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.15.3 Fields/OIDs

The following table lists fields/OIDs for nnGLinkSoakTable.

Table 24 Table field descriptions

Field	Default	Read/Write Access	Size	Note
nnGLinkSoakCountUAS		Read-write	Unsigned32	
nnGLinkSoakPercentSES		Read-write	Unsigned32	

18.6.2.16 Name: nnGLinkProtGroupTable

18.6.2.16.1 Functional description

The GigE Protection Group Table manages the Link Protection Group Configuration. There is one entry in this table for each protection Group, typically 1 per MG9k. This is a Manager Create Table.

See NORTEL-UEMG-GIGE-MIB for details. It can be found at <http://triweb/smg500/mibDir/mibList.html>.

18.6.2.16.2 Size**Table 25 Table size**

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
nnGLinkProtGroupTable	0	8	only 1 in sn08

18.6.2.16.3 Fields/OIDs

The following table lists fields/OIDs for nnGLinkProtGroupTable.

Table 26 Table field descriptions

Field	Default	Read/Write Access	Size	Note
nnGLinkProtGrpNumber		Read-create	Unsigned32	
nnGLinkProtGrpRevertive		Read-create	INTEGER	
nnGLinkProtGrpType		Read-create	INTEGER	
nnGLinkProtGrpWaitTime		Read-create	Unsigned32	
nnGLinkProtGrpIntegThreshold		Read-create	Unsigned32	
nnGLinkProtGrpIntegInterval		Read-create	Unsigned32	
nnGLinkProtGrpIntegEnable		Read-create	INTEGER	
nnGLinkProtGrpStatus		read-only	INTEGER	
nnGLinkProtGrpLastChg		read-only	TimeStamp	new
nnGLinkProtGrpRowStatus		Read-create	RowStatus	

18.6.2.17 Name: nnGLinkOmCurrTable

18.6.2.17.1 Functional description

The GigE Link OM Table contains Operational Measurements per Link, there is one entry per Link

See NORTEL-UEMG-GIGE-MIB for details. It can be found at <http://triweb/smg500/mibDir/mibList.html>.

Table 27 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
nnGLinkOmCurrTable	8	8	Memory is automatically allocated for 8 GigE interfaces.

18.6.2.17.2 Fields/OIDs

The following table lists fields/OIDs for nnGLinkOmCurrTable.

Table 28 Table field descriptions

Field	Default	Read/Write Access	Size	Note
nnGLinkCurrESs		read-only	Unsigned32	
nnGLinkCurrSESSs		read-only	Unsigned32	
nnGLinkCurrUASs		read-only	Unsigned32	
nnGLinkCurrOPT		read-only	Unsigned32	
nnGLinkCurrOPR		read-only	Unsigned32	
nnGLinkCurrTBC		read-only	Unsigned32	
nnGLinkCurrVCC		read-only	Unsigned32	
nnGLinkCurrTEMP		read-only	Unsigned32	
txFifoOverruns		read-only	Unsigned64	new
txFifoUnderruns		read-only	Unsigned64	new

Table 28 Table field descriptions

Field	Default	Read/Write Access	Size	Note
txBytesOverFlow		read-only	Unsigned32	new
txBytes		read-only	Unsigned64	new
rxFcsFail		read-only	Unsigned64	new
rxLenTypeFail		read-only	Unsigned64	new
rxGoodPause		read-only	Unsigned64	new
rxBadOpcodeCntlFrames		read-only	Unsigned64	new
rxControlFrames		read-only	Unsigned64	new
txPauseFrames		read-only	Unsigned64	new

18.6.2.18 Name: nnGLinkOmIntervTable**18.6.2.18.1 Functional description**

The GigE Link OM Table contains Operational Measurements per Link, there is one entry per Link, 96 interval entries per Link.

See NORTEL-UEMG-GIGE-MIB for details. It can be found at <http://triweb/smg500/mibDir/mibList.html>.

Table 29 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
nnGLinkOmIntervTable	8x96	8x96	Memory is automatically allocated for 8 GigE interfaces by 96 intervals.

18.6.2.18.2 Fields/OIDs

The following table lists fields/OIDs for nnGLinkOmCurrTable.

Table 30 Table field descriptions

Field	Default	Read/Write Access	Size	Note
nnGLinkInterval				
nnGLinkIntervESs		read-only	Unsigned32	
nnGLinkIntervSESs		read-only	Unsigned32	
nnGLinkIntervUASs		read-only	Unsigned32	
nnGLinkIntervOPT		read-only	Unsigned32	
nnGLinkCurrOPR		read-only	Unsigned32	
nnGLinkintervTBC		read-only	Unsigned32	
nnGLinkintervVCC		read-only	Unsigned32	
nnGLinkIntervTEMP		read-only	Unsigned32	
txFifoOverruns		read-only	Unsigned64	new
txFifoUnderruns		read-only	Unsigned64	new
txBytesOverFlow		read-only	Unsigned32	new
txBytes		read-only	Unsigned64	new
rxFcsFail		read-only	Unsigned64	new
rxLenTypeFail		read-only	Unsigned64	new
rxGoodPause		read-only	Unsigned64	new
rxBadOpcodeCntlFrames		read-only	Unsigned64	new
rxControlFrames		read-only	Unsigned64	new
txPauseFrames		read-only	Unsigned64	new

18.7 Service Orders (SO) (CM & SESM)

Not Applicable

18.8 Software optionality control (SOC)

Not Applicable

18.9 Element Management

Detailed in the documentation for A00007000.

18.10 User interface changes

Detailed in the documentation for A00007000.

18.11 OSSGate Interface Changes

Not Applicable

18.12 Security

Not Applicable

18.13 Configuration Walkthrough

Detailed in the documentation for A00007000.

19: A00007102 Configuration (CN)

19.1 Feature name

Dual C-Side IP for GWC

19.2 Hardware and Software Requirements

This feature makes changes to the Gateway Controller Element Manager GUI.

19.3 Initial Configuration

Launch the Gateway Controller Element Manager.

19.4 Office/Subnet parameters (OP/SP) (CM & SESM)

No parm changes.

19.5 Upgrade Considerations

None

19.6 Data schema (DS) (CM, MIBS, RDB)

19.6.1 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)
INVENTORY.ROLES	Changed	Old
INVENTORY.ELEMENTTYPE	Changed	Old
INVENTORY.ELEMENT	Changed	Old

19.6.1.1 SESM Table INVENTORY.ROLES

19.6.1.1.1 Functional description

At the SESM server, this table defines all element roles. In order to support the new element “C-Side IP address” storage in the Inventory database, a new role will be added into this table.

19.6.1.1.2 Fields

No structure changes on this table.

19.6.1.1.3 Datafill example

The new role will be defined as in the following datafill.

Table 2 INVENTORY.ROLES: New pre-defined role

NAME	TYPE	DESCRIPTION
CSIP	IP address	Core c-side IP address

19.6.1.2 SESM Table INVENTORY.ROLES

19.6.1.2.1 Functional description

At the SESM server, this table defines all element types. In order to support the new element “C-Side IP address” storage in the Inventory database, a new type will be added into this table.

19.6.1.2.2 Fields

No structure changes on this table.

19.6.1.2.3 Datafill example

The new role will be defined as in the following datafill.

Table 3 INVENTORY.ELEMENTTYPE: New pre-defined element type

NAME	TYPE	CATEGORY
IP address	IP address	Logical

19.6.1.3 SESM Table INVENTORY.ELEMENT

19.6.1.3.1 Functional description

This table will be used to store the new element “C-Side IP address” retrieved from the Core. Up to two CSIPs will be stored in this table, the element name should be “CSIP-0” and “CSIP-1”.

19.6.1.3.2 Fields

No structure changes on this table.

19.6.1.3.3 Datafill example

The new element will be filled as in the following sample.

Table 4 INVENTORY.ELEMENTTYPE: Usage sample for CSIP storage

ELEMENTID	PARENTID	ROLE	TYPE	IP ADDRESS	EMID	LAUNCH HURL	OWNER RID
CSIP-0	COMPACT5	CSIP	IP address	47.142.128.24	-	-	XaCore
CSIP-1	COMPACT5	CSIP	IP address	47.142.128.25	-	-	XaCore

Note:

- Element ID will be filled with the format “CSIP-<nn>”, where <nn> is a valid number starting from 0. Every CSIP record will use a unique number.
- PARENTID will be filled as the current configured CM CLLI.
- EMID and LAUNCHURL will be filled as blank as they are not required for the CSIP record.
- OWNER ID will always be filled as “XaCore”.

19.7 Service Orders (SO) (CM & SESM)

None

19.8 Software optionality control (SOC)

None

19.9 Element Management

19.9.1 New/modified GUIs

Table 5 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
GWC Network Display	Changed
GWC Display	Changed
Add Gwc Node Interface	Changed

19.9.2 GUI information

The first screen GWC Network Display has been modified to accommodate the C-Side IP addresses, which have been shifted here in respect of the requirement to have C-Side IP common to the entire network rather than to individual GWCs. The first snapshot is of the GWC Network Display Panel:

Figure 1 GWC Network Display Panel

The screenshot displays the GWC Network Display Panel, which is divided into several sections:

- Device Types:** A tree view on the left showing 'Device Types' with sub-items 'APS', 'Gateway Controller', and 'UAS'. 'Gateway Controller' is selected.
- Contents of Gateway Controller:** A section with 'Directory' and 'Find' tabs. Below them is a text input field and a 'Go To' button. Underneath, it lists 'Gateway Controllers:' with 'GWC-163'.
- Network Configuration:** A section with three tabs: 'Network Codec Profile', 'DQoS Configuration', and 'VCAC Resource Usage'. The 'Network Codec Profile' tab is active, showing a table with one entry: 'IP Profile 1' with 'IP' as the Bearer Network Type, 'G.711-a law' as the Codec Selection, '10 ms' as the Packetization Rate, and 'Disabled' as the status. Below the table is a scrollable list area with 'Add...', 'Delete', and 'Change' buttons.
- Network Devices:** A section with six tabs: 'PEP Servers', 'Media Proxies', 'IP-VPNs (Virtual NATs)', 'Limited BW Links (LBL)', 'QoS Collectors', and 'Location Recipients'. The 'IP-VPNs (Virtual NATs)' tab is active, showing an empty table with columns: 'Name', 'IP Address', 'Type', 'Max Conn', and 'Protocol Version'. Below the table are 'Add...', 'Delete', and 'Change' buttons.
- General Network Settings:** A section at the bottom with two columns of settings. The left column includes 'GWC default domain name: <not configured>', 'Call Agent id: <not configured>', and 'Auto Imaging: disabled' with a 'Change...' button. The right column includes 'Call Agent IP Address 0: 172.16.17.5' and 'Call Agent IP Address 1: 172.16.17.5'.

At the bottom left, there are '< Prev' and 'Next >' buttons, and a status bar indicating 'Last update: Sep 20, 2004 4:35 PM'.

Once the first requirement is met, we need to eliminate the redundancy of having the Message Router IP Address at every GWC Display Panel. To achieve this we remove the Message Router IP Address at the GWC Display Level. This is how the GWC Display Panel looks after it has been modified:

Figure 2 Figure. 2 Removal of Message Router IP Address from GWC Display Panel

Management Tools - 172.16.17.5 (CM CLI: INDIA1LAB)

Configuration Maintenance Windows Help

es

Gateway Controller

Unit 0: 172.16.16.26

Unit 1: 172.16.16.27

Maintenance Provisioning

Controller Gateways Lines Carriers Media Proxies QoS Collectors IPsec

IP Addresses _____ Element Manager _____

Active: 172.16.16.24 IP address: 172.16.17.5

Inactive: 172.16.16.25 SNMP port: 161

Unit 0: 172.16.16.26 Trap port: 162

Unit 1: 172.16.16.27

Profile _____ XA-Core _____

Current: SMALL_LINEINTL Change...

Node number: 45

Capability	Capacity	Units
Lines	6400	ports
Dynamic Quality of...	20	connections
Small Gateways	6400	gateways
IP Security	NA	NA
Kerberos	NA	NA

Exec Lineup	
POTSEX	POT
KSETEX	KEY

General Settings _____

☐ Enable Location Identification rep

Bearer Network and Codec Profile _____

Bearer network: <none>

Bearer fabric type: IP

Codec Profile: Network_Default_Profile Change...

Go To

Next >

Also since the provisioning has been changed to auto-provisioning, the need for manual provisioning does not arise. Hence we need to modify the 'Add GWC Interface' where we insert the Message Router IP Address. We remove the Message Router IP Address from this Panel. The screen after this modification will look as below:

Figure 3 Figure 3 Removal of Message Router IP Address from Add GWC Node

Add Gateway Controller

Gateway controller name: GWC-

Gateway controller active IP address:

GWC Profile Information

Gateway controller profiles:

Tone data:

Term Type	Exec Data

Capability	Capacity

GWC Bearer Networks and Codec Profile Information

Bearer networks:

GWC codec profile:

OK Cancel

19.9.2.1 GUI name: GND Panel

GWC Network Display Panel

19.9.2.1.1 Functional description

This panel is used for representing the attributes that are across the network of the GWCs rather than each GWC. The GUI can be invoked through the CMT Application. Once we invoke the application we get the CS2000 Management Tools Screen. On this screen we will find a Folder GUI with 'Device Types' written alongside it. Under this we will find 'Gateway Controller'. On clicking the 'Gateway Controller', we get a page which has a section called 'General Network Settings'. Under this we find our required information 'Call Agent IP Addresses'.

19.9.2.1.2 GUI usage and implications

N/A.

19.9.2.1.3 GUI size

Table 6 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
G N D Panel	N/A	N/A	N/A.

19.9.2.1.4 GUI fields

Table 7 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
<i>coreIPAddressText1</i>	New	---	String	Default = Null	
<i>coreIPAddressText2</i>	New	---	String	Default = Null	

19.9.2.1.5 Usage example

N/A

19.9.2.1.6 GUI release history update

The C-Side IP addresses were added to the GWC Network Display Screen. Hence we get a Network common view of the C-Side IP addresses.

19.9.2.1.7 Context sensitive launching information

N/A

19.9.2.1.8 Supplementary information

N/A.

19.9.2.2 GUI name: G D Panel

GWC Display Panel

19.9.2.2.1 Functional description This panel is used for representing the attributes corresponding to each GWC, i.e. each panel represents a GWC in the Network. We remove the Core IP address as we have settled for the Call Agent IP address on a Network level rather than on a GWC level. The GUI can be invoked through the CMT application. Once we invoke the application we get the CS2000 Management Tools screen. On this screen we will find a folder GUI with 'Device Types' written alongside it. Under this we will find 'Gateway Controller'. On clicking the 'Gateway Controller', we get a 'Gateway Controllers' display. Under this will be displayed the list of all GWCs in the network. On clicking on any one of the list, we get the GWC display for that listed GWC. We get 2 tabbed panes to select, the first is 'Maintenance' and the second is 'Provisioning'. Take 'Provisioning' and in that take the next pane 'Controller', here we remove the display for the Message Router IP address and end up having only 'IP address' and 'Element Manager'.

19.9.2.2.2 GUI usage and implications

N/A.

19.9.2.2.3 GUI size

Table 8 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
G D Panel	N/A	N/A	N/A.

19.9.2.2.4 GUI fields

No new fields added or changed.

19.9.2.2.5 Usage example

N/A.

19.9.2.2.6 GUI release history update

The GWC Display panel has been changed by the Removal of the 'Message Router IP address' from the panel.

19.9.2.2.7 Context sensitive launching information

N/A.

19.9.2.2.8 Supplementary information

N/A.

19.9.2.3 GUI name: Add GWC Node Interface Panel

19.9.2.3.1 Functional description

We have moved from the Manual Provisioning of the GWC Message Router IP address to the Auto Provisioning of the C-Side IP address. The GUI can be

invoked through the CMT application. Once we invoke the application we get the CS2000 Management Tools screen. Here on the toolbar we get a Configuration button and when we click the button a drop down menu is obtained. On the drop down menu we have an option of 'Add GWC Node'. When we click on this option we get a Add GWC Node interface. Here we have modified the interface, so as to avoid manually setting the Message Router IP address.

19.9.2.3.2 GUI usage and implications

N/A.

19.9.2.3.3 GUI size

Table 9 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Add GWC Node I/f's	N/A	N/A	N/A.

19.9.2.3.4 GUI fields

No new fields added or changed.

19.9.2.3.5 Usage example

The following interface is used when we need to add a new GWC to the network. In the CMT application we go to the Configuration--> Add GWC Node interface. Here in this interface we can add a new GWC.

19.9.2.3.6 GUI release history update

The modification we have made here is that we have removed the Message Router IP address from this interface, so that we avoid manually provisioning the C-Side IP address.

19.9.2.3.7 Context sensitive launching information

N/A.

19.9.2.3.8 Supplementary information

N/A.

19.9.3 CLUI Interface

The CLUI interface is modified such that the Call Agent IP Addresses are displayed on a Per-Gwc basis.

Note: Currently CLUI does not support the Network level interface. All existing interfaces focus on the per GWC level. This will make it inconsistent between CLUI and GUI (GUI now only supports the Call Agent IP Address on a Network level). Since we do not extend CLUI support to the customer, these inconsistencies are acceptable at this moment.

19.10 User interface changes

None

19.11 OSSGate Interface Changes

19.11.1 XML Command Changes

- a** Add GWC: the new XML command change is that during adding a GWC. Here we need to forgo the need to pass the Message Router IP address and Message Router port.
- b** Query GWC: the other is when we get a response for a Query for the GWC. Here the response is changed so that Message Router IP address and Message Router port are not displayed.

19.11.1.1 Command XML

- a** Add GWC: here we need to remove the XML reference to the Message Router IP address and the Message Router port. The red indicates the lines that will be removed.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<CommandList >
<Command>
<Interface>cs2kCfgMgrIf</Interface>
<Methods>
<addGWCtoCS usn="1" version="1.0">
<Parameters>
<csUIName>COMPACT5</csUIName>
<gwcUIName>GWC-0</gwcUIName>
<profileName>TRUNKNA</profileName>
<gwcActvIp>47.142.128.36</gwcActvIp>
<gwcSnmpPort>161</gwcSnmpPort>
<msgRouterIp>47.142.128.24</msgRouterIp>
<msgRouterIpPort>4684</msgRouterIpPort>
</Parameters>
</addGWCtoCS>
</Methods>
</Command>
</CommandList>
```

- b** Query GWC: no changes in the Query GWC Command.

Table 10 XML Command Tag Descriptions

tag name	description of valid values
N/A	
N/A	

19.11.1.2 Response XML

- a** Add GWC: no changes on the response side for Add GWC.
- b** Query GWC: The display here will not have the Message Router IP address and Message Router port. The red indicates that those lines will not be displayed.

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
<Response>
  <Interface>cs2kCfgMgrIf</Interface>
  <Methods>
    <queryGWC usn="1" version="1.0">
      <ReturnData>
        <Row>
          <gwcUList>GWC-3</gwcUList>
          <gwclpList>47.142.128.52</gwclpList>
          <callServerId>COMPACT5</callServerId>
          <nodeName>GWC 3</nodeName>
          <typeList>2</typeList>
          <typeList>8</typeList>
          <typeList>15</typeList>
          <xacNodeNumber>24</xacNodeNumber>
          <actvIpAddress>47.142.128.52</actvIpAddress>
          <snmpPort>161</snmpPort>
          <mktTones>NORTHAM</mktTones>
          <termTypes>ABTRK</termTypes>
          <termTypes>AB250</termTypes>
          <termTypes>PRAB</termTypes>
          <pmExecs>GWCEX</pmExecs>
          <pmExecs>GWC250</pmExecs>
          <pmExecs>UTR250</pmExecs>
          <capacity>4094</capacity>
          <externalIP>NOT_YET_SUPPORTED</externalIP>
          <externalPort>0</externalPort>
          <msgRtrIP>47.142.128.24</msgRtrIP>
          <msgRtrPort>4684</msgRtrPort>
          <bearerNetworkName>IP</bearerNetworkName>
          <bearerFabricType>IP</bearerFabricType>
          <codecProfileName>IP_default</codecProfileName>
        </Row>
        <RC>0</RC>
        <MsgTxt>Query of a Single GWC was successful</MsgTxt>
      </ReturnData>
    </queryGWC>
  </Methods>
</Response>
</CommandList>
```

19.11.2 Additional OSSGate Changes

N/A.

19.12 Security

None

19.13 Configuration Walkthrough

20: A00007120 Configuration (CN)

20.1 Feature name

Packet Media Anchor for DPT

20.2 Hardware and Software Requirements

20.2.1 Required Hardware

- Audiocodes Media Server (AMS) for IP

20.2.2 Required Software

- SNO8

20.3 Initial Configuration

- Identify the maximum number of anchored calls to support
- Provision the a Packet Media Anchor tuple in table SRVSINV with the maximum number of simultaneous calls to support
- In the GWC element manager:
 - Verify the gateway profile of each AMS is set to “AMS.”
 - Provision a new Network Codec Profile that supports only G.711 for voice calls
 - Change the Codec Profile the AMS GWC uses to be the profile defined above.
- In the AMS element manager provision
 - Three (3) BCT resources for each anchored call. (3 * the maximum number of simultaneous anchored calls)
 - One (1) Audio resource for each anchored call
- Cold SWACT the ACC GWC or Re-initialize all the AMS gateways

20.4 Upgrade Considerations

20.4.1 Dump and Restore (CM)

A new option is added in table SERVSINV. There is no impact on the Dump and Restore process.

20.4.2 Element Management Upgrade

No impact.

20.4.3 Downgrade impact

No impact.

20.5 Data schema (DS) (CM, MIBS, RDB)

20.5.1 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)
SERVSINV	CHANGED	UNCHANGED

20.5.2 Table Database Schema information

20.5.2.1 Name: SERVSINV

GWC Services Inventory

20.5.2.1.1 Functional description

Table SERVSINV lists the services associated with a Gateway Controller. Examples of the supported services are:

- Conferencing
- Announcements
- Lawful intercept
- SIPT and BICC Dynamic Packet Trunking

In SNO8 the new Packet Media Anchor service is added to this list of services provisioned in the table.

20.5.2.1.2 Usage sequence and implications (CM Only)

The table must be datafilled in the following sequence:

- SERVRINV
- SERVSINV

20.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVSINV	0	256	Protected

20.5.2.1.4 Fields/OIDs The following table lists the changed fields for table SERVSINV.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTIONS	Changed		See refinement (table 4)	Options. New PKTMA_MAX_CALLS option may be entered in this field.

OPTION = PKTMA_MAX_CALLS

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTIONS	new		PKTMA_MAX_CALLS	Used to control the number of Packet Media Anchor calls. This field contains subfield PKTMA_MAX_CALLS .
		PKTMA_MAX_CALLS	1 to 1000	Anchor calls. Defines the number of supported anchored calls on the audio server. Enter value between 1 to 1000.

20.5.2.1.5 Datafill example

The following example shows a sample datafill for table SERVSINV. Table 5 shows an example of datafill prior to provisioning the PKTMA_MAX_CALLS option. Table 6 shows an example of the provisioning changes when the PKTMA_MAX_CALLS option is added.

Table 5 Table SERVSINV Datafill without the PKTMA_MAX_CALLS Option

TABLE: SERVSINV									
>LIST ALL									
TOP									
	SRVSNAME		SRVRNAME	NUMTERMS					OPTIONS
	AUD	4	GWC	20	4095	(3PORT 30)	(6PORT 30)	(ANNC 300)	\$
	DPT	6	GWC	15	2048			(SIPT)	\$
	BCT	4	GWC	20	1024			(ALTTERMS 90)	\$
BOTTOM									

Table 6 Table SERVSINV Datafill with the PKTMA_MAX_CALLS Option

TABLE: SERVSINV									
>LIST ALL									
TOP									
	SRVSNAME		SRVRNAME	NUMTERMS					OPTIONS
	AUD	4	GWC	20	4095	(3PORT 30)	(6PORT 30)	(ANNC 600)	\$
	DPT	6	GWC	15	2048			(SIPT)	\$
	BCT	4	GWC	20	1024			(ALTTERMS 90)	\$
	BCT	5	GWC	20	4095			(PKTMA_MAX_CALLS 300)	\$
BOTTOM									

20.5.2.1.6 Table release history update

The PKTMA_MAX_CALLS option was added in SN08.

20.5.2.1.7 Supplementary information

- A GWC may support a maximum of one BCT node for Lawful Intercept (ALTTERMS) and one BCT node for the Packet Media Anchor (PKTMA_MAX_CALLS). Multiple appearances of either option, on a single GWC, is not permitted.
- The PKTMA_MAX_CALLS option ranges from 0 to 1000 for future expansion. The functional limit per GWC is 480 PKTMA calls. This limitation is determined with the following calculation:
 - $(30 \text{ PKTMA calls per AMS}) * (16 \text{ AMS gateways per GWC}) = 480 \text{ PKTMA calls per GWC.}$
- The Audio Server must be configured to support three BCT resources and one announcement resource per call. Using the example above, the Audio Server should be configured with:
 - 990 BCT resources: $(3 * \text{PKTMA\_MAX\_CALLS}) + \text{ALTTERMS}$
 - 600 ANNC resources: $(\text{Orig. ANNC value}) + (\text{PKTMA\_MAX\_CALLS})$
- Changes to the PKTMA_MAX_CALLS parameter require the AMS gateways to be re-initialized for the parameter to take affect.
- The PKTMA option can be provisioned on a GWC that does not have audio resources provisioned in table SERVSINV; however, the AMS must be provisioned with the following resources to support the PKTMA functionality.
 - Announcement resources
 - BCT resources
 - Voice Prompt file
 - Call Progress Tone file
 - Pre Recorded Tones file
- In the GWC element manager, the profile of the AMS must be set to "AMS," and not "UAS." This enables functionality on the AMS necessary to support the PKTMA application.

20.5.2.1.8 Translation verification and other tools

Not Applicable.

20.6 Software optionality control (SOC)

Not Applicable.

Table 7 SOC

SOC option name:	
SOC option title:	Yes/No
SOC option control type:	<state/usage/combined>
New SOC option?	<Yes/No>
SOC option order code	<order code>
Option defined in DRU:	<DRU>
Affected products:	<PCL(s)>

20.7 User interface changes**20.7.1 Directory: GWC****20.7.1.1 Directory description**

Posts the GWC peripherals and provides commands for viewing the status of GWC peripherals. No maintenance actions, such as BSY and RTS, can be performed from this MAP level.

20.7.1.2 Accessing directory: GWC**20.7.1.2.1 Access to directory or MAP level and return to CI**

>MAPCI;MTC;PM;POST GWC ALL

>QUIT ALL

20.7.2 Command: QUIT**20.7.2.1 Command type: Listed MENU****20.7.2.2 Command target: All****20.7.2.3 Command availability: RES****20.7.2.4 Command description**

Exits the GWC level and returns the user to a previous MAP level or to the CI prompt.

20.7.2.5 Command syntax

Table 8 QUIT command parameters and variables

Command	Parameters and variables
QUIT	<nlevels incrname ALL>
Parameters and variables	Description
nlevels	Exits the specified number of levels
incrname	Exits the specified increment
All	Returns to the CI prompt

20.7.2.6 Qualifications and warnings

None.

20.7.2.7 Example Commands

>MAPCI;MTC;PM;POST GWC ALL

- Enters the GWC MAP level and places all GWC type peripherals in the posted set.

>QUIT

- Returns to the PM MAP level

>QUIT All

- Returns to the CI level

20.7.3 Command: POST

20.7.3.1 Command type: Listed MENU

20.7.3.2 Command target: All

20.7.3.3 Command availability: RES

20.7.3.4 Command description

Used to post a specific GWC, or a set of GWC type peripherals.

20.7.3.5 Command syntax

Table 9 POST command parameters and variables

Command	Parameters and variables
POST	[<All> {All}] [<PMNo>.... {0 TO 2047}] [<PMTType>...{ GWC [<All> {All}] [<PMNo>... {0 TO 255}] }] [<state>... {SysB, ManB, OffL, CBsy, ISTb, InSv}] [<Alarm>... {Minor, Major, Crit}]
Parameters and variables	Description
ALL	Posts all GWC type peripherals
PMNo	Posts a specific GWC using the PM Number
PMTType	Posts all GWC type peripherals or a specific GWC
State	Posts all GWC peripherals in the specified state
Alarm	Posts all GWC peripherals in the specified state

20.7.3.6 Qualifications and warnings

None.

20.7.3.7 Example Commands

>MAPCI;MTC;PM;POST GWC ALL

- Enters the GWC MAP level and places all GWC type peripherals in the posted set.

>POST 2

- Displays GWC 2 and modifies the posted set to contain only GWC 2.

>POST MANB

1. Changes the posted set to contain GWC peripherals in the MANB state.

20.7.4 Command: LISTSET

20.7.4.1 Command type: Listed MENU

20.7.4.2 Command target: All

20.7.4.3 Command availability: RES

20.7.4.4 Command description

Lists the peripherals in the current posted set.

20.7.4.5 Command syntax

Table 10 LISTSET command parameters and variables

Command	Parameters and variables
LISTSET	noparm <ALL> <PMType>
Parameters and variables	Description
noparm	Displays a list of the peripherals in the current posted set
All	Displays details about the posted set: total number of peripherals posted and the number of different PM types
PMType	Displays a list of the specified PM type peripherals in the posted set

20.7.4.6 Qualifications and warnings

None.

20.7.4.7 Example Commands

>LISTSET

- Displays a concise list of the peripherals in the posted set

>LISTSET ALL

- Displays a summary of the number of peripherals and the number of different types of peripherals in the posted set.

>POST GWC

- Displays the list of GWC peripherals in the posted set.

20.7.5 Command: DISP

20.7.5.1 Command type: Listed MENU

20.7.5.2 Command target: All

20.7.5.3 Command availability: RES

20.7.5.4 Command description

Display all PMs in the specified PM state.

20.7.5.5 Command syntax

Table 11 DISP command parameters and variables

Command	Parameters and variables
DISP	<Option> {STATE <state> {SysB, ManB, OffL, CBsy, ISTb, InSv}, DIAGHIST} [<PM Type> {TM2,..., GWC}]
Parameters and variables	Description
STATE	Display the PMs in a specific state
DIAGHIST	Display the diagnostic history of all PMs
PM Type	Specify the state, or diagnostic history, for all PMs of a specific PM type.

20.7.5.6 Qualifications and warnings

- The DIAGHIST option of this command is not valid for GWC type peripherals.

20.7.5.7 Example Commands

>DISP STATE MANB

- Displays a concise list of the peripherals in the MANB state

>DISP STATE MANB GWC

- Displays a concise list of all GWC type peripherals in the MANB state.

20.7.6 Command: NEXT

20.7.6.1 Command type: Listed MENU

20.7.6.2 Command target: All

20.7.6.3 Command availability: RES

20.7.6.4 Command description

Step to the next PM in post set or to the first PM of the next PM type in post set

20.7.6.5 Command syntax

Table 12 NEXT command parameters and variables

Command	Parameters and variables
NEXT	[<PM TYPE> {PMTYPE}]

Table 12 NEXT command parameters and variables

Command	Parameters and variables
Parameters and variables	Description
PMTYPE	Optional parameter for stepping to the next PM type.

20.7.6.6 Qualifications and warnings

None.

20.7.6.7 Example Commands

>NEXT

- Steps to the next PM in the post set

>NEXT PMTYPE

- Steps to the next PM type in the post set

20.7.7 Command: LISTRES**20.7.7.1 Command type: Listed MENU****20.7.7.2 Command target: All****20.7.7.3 Command availability: RES****20.7.7.4 Command description**

Displays information related resources associated with the Gateway Controller (GWC). The command is only valid for Audio Server GWCs. The resources presented are:

- Announcements
- Conferencing
- Lawful Intercept
- Packet Media Anchor

For each resource type, the following data is displayed:

- Maximum number of provisioned resources in table SERVSINV (MaxPorts)
- Number of in-service resources (InsvPorts)
- Number of resources involved in a call (CPBports)
- Number of busy resources (BsyPorts)

The LISTRES command provides a snapshot of the resource usage, the MAP display is not updated dynamically. The command must be re-entered to update the display.

20.7.7.5 Command syntax

Table 13 LISTRES command parameters and variables

Command	Parameters and variables
LISTRES	None.
Parameters and variables	Description

20.7.7.6 Qualifications and warnings

- The command is only valid for Audio Server GWC type peripherals.

20.7.7.7 Example Commands

>LISTRES

- Displays the resource information.

20.7.7.8 Example MAPCI Screen

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	.	NODLOG	Istb	1 SPM	.	SYSB	48C..	.	SDM
M				*C*		*C*	*C*		
GWC				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		11	1	42	8	7	60
2 Post_		GWC		3	0	0	0	0	15
3 Listset									
4 Listres		GWC	20 InSv						
5		Unit0:	Act ISTb						
6		Unit1:	Inact SysB						
7		Listres							
8				MaxPorts	InsvPorts	BsyPorts	CPBports	ResType	
9				-----	-----	-----	-----	-----	
10		Conf3		30	30	0	0	CONF	
11 Disp_		Conf6		30	30	0	0	CONF	
12 Next		Announcements		300	50	0	0	ANNC	
13		Lawful Intercept		90	8	0	0	BCT	
14 QueryPM		PKT Media Anchor		90	0	0	0	BCT	
15									
16									
17									
18									

20.7.8 Command: QUERYPM

20.7.8.1 Command type: Listed MENU

20.7.8.2 Command target: All

20.7.8.3 Command availability: RES

20.7.8.4 Command description

Presents general information about the posted GWC, including:

- The load name for each unit
- The active unit IP address
- In-service trouble reasons

20.7.8.5 Command syntax

Table 14 LISTRES command parameters and variables

Command	Parameters and variables
QUERYPM	[<option> {FLT, CNTRS, FILES, CONFIG, DIAGHIST, ABICNN}]
Parameters and variables	Description
none	Displays general information about the posted GWC
FLT	Displays in-service trouble reasons for the GWC
CNTRS	Not supported for GWC type peripherals
FILES	Not supported for GWC type peripherals
CONFIG	Not supported for GWC type peripherals
DIAGHIST	Not supported for GWC type peripherals
ABICNN	Not supported for GWC type peripherals

20.7.8.6 Qualifications and warnings

- GWC Type peripherals only support the “FLT” option.

20.7.8.7 Example Commands

>QUERYPM

- Displays general information regarding the posted GWC

>QUERYPM FLT

- Displays in-service trouble reasons for the posted GWC

20.8 Configuration Walkthrough

- Identify the maximum number of anchored calls to support
- Provision the a Dynamic Packet Trunk Media Anchor tuple in table SRVSINV with the maximum number of simultaneous calls to support
- In the GWC element manager:
 - Verify the gateway profile of each AMS on the GWC is set to “AMS.” (See note 2 below).

-
- Provision a new Network Codec Profile that supports only G.711 for voice calls
 - Change the Codec Profile the AMS GWC uses to be the profile defined above.
 - In the AMS element manager provision
 - Three (3) BCT resources for each anchored call. (3 * the maximum number of simultaneous anchored calls)
 - One (1) Audio resource for each anchored call
 - Cold SWACT the ACC GWC or Re-initialize all the AMS gateways
 - Use the LISTRES command to verify resource allocation. All discrepancies between the provisioned resources (MaxPorts) and in-service resources (InsvPorts) should be investigated. Differences may be caused by
 - Provisioning errors in the gateway element manager
 - Provisioning errors in table SERVSINV
 - Gateways not registered with the GWC

Notes:

1. Ensure each AMS is configured with the following files to support the PKTMA functionality.
 - Voice Prompt file
 - Call Progress Tones file
 - Pre Recorded Tones file
2. When converting an existing AMS to support the PKTMA functionality, the AMS must be disassociated from the GWC in the GWC element manager and re-associated using the new AMS profile. Standard maintenance procedures should be followed to perform this action as it will result in a call processing outage on the gateway.

21: A00007213 Configuration (CN)

21.1 Feature name

MG9000 5/30 Minutes OMs

21.2 Hardware and Software Requirements

None

21.3 Initial Configuration

NA

21.4 Office/Subnet parameters (OP/SP) (CM & SESM)

NA

21.5 Upgrade Considerations

21.5.1 Element Management Upgrade

21.5.1.1 Element Management Upgrade from SN07 to SN08

Here are the steps to upgrade MG9K Manager software from SN07 to SN08.

1. Stop SN07 OM Collector (Refer to note #1 in this section).
2. Uninstall SN07 OM Collector package
3. Install SN08 EM package (Note that, user is not allowed to install SN08 EM server package if SN07.x OMC package exists)
4. Install SNO8 OMC.
5. Start SN08 MG9KEM

All the MG9Ks in a subnet are configured with same collection intervals. SN07 MG9K support 15 minutes Collection interval. Hence, Collection interval is not allowed to be set to anything other than 15 minutes until all MG9Ks are upgraded to SN08.

Note #1: SN07 OMC keeps CSV files in /data/oms/1. If SN08OMC is also configured to keep CSV files in /data/oms/1, then we will have problem if SN07 OMC is also left running, since both would try to write CSV file into the same directory. To avoid this problem, step #1 shall be performed before step #5.

21.4.2.2 Element Management Upgrade from SN06.x to SN08

Here are the steps to upgrade MG9K Manager software from SN06/SN06.2 to SN08.

1. Start SN08 MG9KEM
2. Consider one SN06.x NE at a time. Before performing step #3, delete the NE from SN06.2 OMC (Refer to note #1 and #2)
3. When the NE is upgraded to SN08 software, enable OM collection for SN06.2 NEs in SN08 MG9KEM.
4. Repeat step #2 and #3 for each NE.

Note #1: The reason for performing step #2 after step #1 is as follows. After step #1, older NEs would be upgraded to SN08. If there are more older NEs, then this would take relatively more time. If we remove all the NEs from SN06.x OMC immediately after step #1, then we would lose OM data for the period wherein older NEs are upgraded to SN08.

Note #2: The reason for performing step #2 before step #3 is as follows. SN08 NE support SFTP and SN06.2 OMC supports only FTP. If NE still exists in SN06.2 OMC even after NE is upgraded to SN08 (i.e., step #3), then data collection would fail.

21.4.2 Downgrade impact

21.4.2.1 Element Management Upgrade from SN08 to SN07/SN06.x

When collection interval is 5/30 minutes, if a NE is downgraded to older release, then disable OM collection for the downgraded NE. With this, OMC does not collect data for the downgraded NE. The reason is that, downgraded NE can not collect at 5/30 minutes.

21.5 Data schema (DS) (CM, MIBS, RDB)

21.5.1 New/modified tables, MIBs, or Database Schema

Table 4 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
OFFICE_WIDE_DEFAULTS	Changed	Unchanged

21.5.2 Table/MIB/Remote Database Schema information

21.5.2.1 Name: OFFICE_WIDE_DEFAULTS

Office wide defaults Database table.

21.5.2.1.1 Functional description

One more entry is made in this existing database table to store Collection intervals.

Impact on existing functionality of enabling/disabling of OM collection:

When OM Collection is enabled or disabled for a NE through GUI, the database variable OMCSTATUS in the database table NODE_ATTRIBUTES will be set to enabled.

While a pre SN08 NE is discovered, current collection interval (which is configured at EM) will be checked. If it is 5/30 minutes, the database variable OMCSTATUS will be set to disabled. In turn, OM collection will be disabled from next collection cycle.

Impact on discovery of NE:

While a SN08 NE is discovered, current collection interval (which is configured at EM) will be pushed to the NE. In case the push fails, discovery would still continue. The mismatch will be rectified when NE is audited next time.

21.5.2.1.2 Usage sequence and implications (CM Only)

None

21.5.2.1.3 Size

Table 5 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
OFFICE_WIDE_DEFAULTS	Same as current table size	One more entry than current table size.	Memory requirement is less than 1 KB.

21.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for OFFICE_WIDE_DEFAULTS

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DFLT_NAME	Changed	NA	New value "Collection_Interval" is added	
DFLT_SUBSYSTEM	Changed	NA	OMC	

Table 6 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DFLT_VALUE	Changed	NA	Default value is "15 Minutes"	

21.5.2.1.5 Datafill example

None

21.5.2.1.6 Table release history update

One more entry is made in the table OFFICE_WIDE_DEFAULTS, to store the Collection intervals. This entry is made either during major release upgrade or during SN08 MR upgrade.

21.5.2.1.7 Supplementary information

The Collection interval value stored in the table OFFICE_WIDE_DEFAULTS is applicable for all the NEs present in the subnet.

21.5.2.1.8 Translation verification and other tools

None

21.6 Service Orders (SO) (CM & SESM)

NA

21.7 Software optionality control (SOC)

NA

21.8 Element Management**21.8.1 New/modified GUIs****Table 7 New or modified GUIs**

GUI name	NEW, CHANGED, or DELETED
Configure Collection Interval	New
Performance Statistics Browser	Changed

21.8.2 GUI information

21.8.2.1 GUI name: Configure Collection Interval

21.8.2.1.1 Functional description

This new GUI is introduced under the submenu option MG9KEM Subnet view ->Performance. This GUI allows users to configure Sample and Summary intervals uniformly for all SN08 MG9Ks in a Subnet. If there are no MG9Ks in a subnet, the configured collection interval will just be stored in database.

Sample and Summary intervals are specified in terms of minutes. In SN08, the user is allowed to select following combinations of Sample and Summary intervals.

- Sample interval of 5 minutes and Summary interval of 30 minutes. This is shown as “5/30 minutes” in the GUI.
- Sample interval of 15 minutes and no Summary interval. This is shown as “15 minutes” in the GUI.

If Collection intervals are not configured from the GUI “Configure Collection Interval”, they will have the default value “15 minutes”.

Impact on existing functionality of enabling/disabling of OM collection:

OM collection can be enabled for a MG9K through the “OMCollection” check box provided in the existing GUIs, “MG900 Provisioning”, “NE Properties”. Refer to A00003531 CN for more details. In association with this existing capability of enabling OM collection, the GUI “Configure Collection Interval” affects OM collection as follows.

- When OMC is running, if OM collection is enabled for a MG9K, OMC will start collecting OM data at the Collection intervals.
- If collection interval is 5/30 minutes, the OMC checkbox is disabled for pre-SN08 NEs.

Impact on working of OMC and Performance Browser:

Whenever Collection intervals are changed, Performance browser and OM Collector behave as follows.

- OM Collector will start collecting OMs at new collection intervals, starting from next collection interval.
- After Collection interval is changed, if User tries to collect performance data, Performance browser will collect OMs at new Sample collection interval.

21.8.2.1.2 GUI usage and implications

None

21.8.2.1.3 GUI size

Table 8 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Configure Collection Interval	1	1	TBD

21.8.2.1.4 GUI fields

The following table lists fields for GUI “Configure Collection Interval”.

Table 9 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Collection Interval	New	None	5/30 minutes 15 minutes	- A value “5/30 minutes” specifies Sample and summary collection intervals of 5 and 30 minutes respectively. - A value “15 minutes” specifies Sample and summary collection intervals of 15 minutes and none respectively. - Default value is “15 minutes”.	<u>MIB name:</u> NORTEL-UEMG-BASE.mib <u>Table name:</u> None <u>Attributes:</u> nnUemgOMStandardInterval and nnUemgOMExtendedIntervalMulti.

The following paragraphs explain about the option/s shown in this field, during different scenarios.

Scenarios wherein there is mix of NEs:

If either undiscovered or pre-SN08 NE exists along with SN08 NE(s), then only currently configured collection interval will be shown. This is explained with below examples.

Example #1:

Step 1/ Let say just one or more SN08 NEs exist and collection interval is set to X minutes (15 or 5/30).

Options shown are; 15 and 5/30 minutes

Step 2/ A new NE is added and is not discovered.

Note: EM can not make out the NE version of a discovered NE. So. EM will it consider this as a “mix NEs” scenario.

Options shown are; X minutes, the current configured collection interval.

Step 3/ The new NE is discovered and is pre-sn08.

Options shown are; X minutes, the current configured collection interval.

Example #2:

Step 1/ Let say just one or more pre-SN08 NEs exist and collection interval is set to X minutes (15 or 5/30).

Options shown are; 15 and 5/30 minutes

Step 2/ A new NE is added and is not discovered.

Options shown are; X minutes, the current configured collection interval.

Step 3/ The new NE is discovered and is sn08.

Options shown are; X minutes, the current configured collection interval.

Difference between example #1 and example #2 is that, example #1 had sn08 first and got added with pre-sn08 NE later. Example #2 had pre-sn08 first and got added with sn08 NE later.

Scenarios wherein there is no mix of NEs;

Case #1: Subnet has only sn08 NEs:

Options shown are; both the options

Case #2: Subnet has only undiscovered NEs:

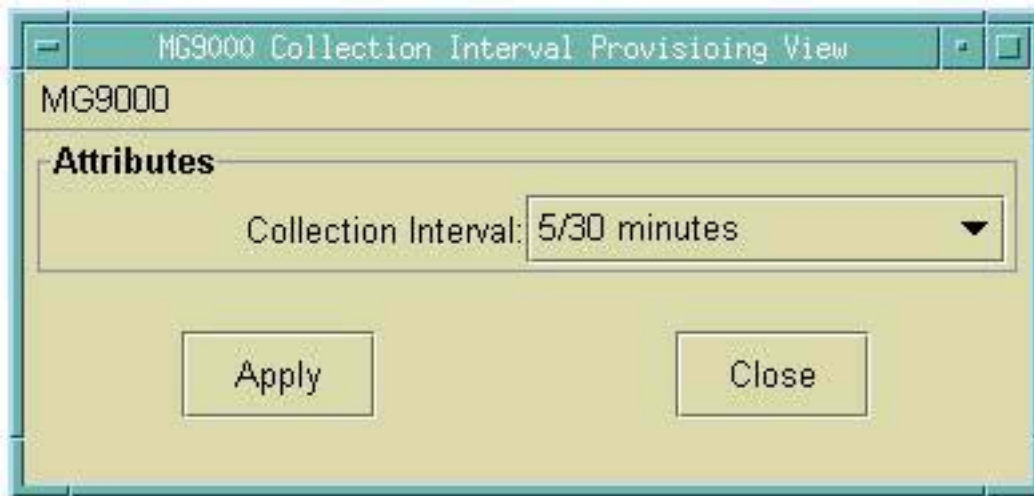
Options shown are; both the options

Case #3: Subnet has only pre-sn08 NEs:

Options shown are; only 15 min

21.8.2.1.5 Usage example

The following example shows the GUI “Configure Collection Intervals“, when the value “5/30 minutes” is selected.



21.8.2.1.6 GUI release history update

A new GUI “Configure Collection Interval” is introduced in order to configure Sample and Summary intervals uniformly for all the MG9Ks in a Subnet.

21.8.2.1.7 Context sensitive launching information

None

21.8.2.1.8 Supplementary information

When MG9KEM changes Collection interval, any data collected by OM Collector and/or Performance browser till the end of current collection interval after MG9KEM changes collection intervals, may not be accurate. Following paragraphs explains the reason for this.

Example #1:

Let us consider that, MG9KEM changes the collection intervals say from 15 to 5/30 minutes, at 9:06 AM. In this scenario, MG9KEM and OM Collector will switch over starting from next collection interval time as explained below.

- OM Collector will collect new Sample interval (i.e, 5 min in this example) starting from 9:10 AM and Summary interval starting from 9:30 AM.

- Performance browser will changeover immediately. i.e, it will show Collection time period in terms of new Sample collection interval.

However, MG9K changes over to new collection interval at end of current collection interval (i.e., at 9:15 AM in the scenario explained above). Also, MG9K flushes its history performance data at 9:15 AM.

Because of this behavior difference between MG9K and MG9KEM PM components (i.e., performance browser and OM Collector), any data collected by OM Collector and/or Performance browser till and including 9:15 AM, may not be accurate.

Example #2:

Let us consider that, MG9KEM changes the collection intervals say from 5/30 to 15 minutes, at 9:06 AM. In this scenario, MG9KEM and OM Collector will switch over starting from next collection interval time as explained below.

- OM Collector will collect new Sample interval (i.e, 15 min in this example) starting from 9:15 AM.

- Performance browser will changeover immediately. i.e, it will show Collection time period in terms of new Sample collection interval.

However, MG9K changes over to new collection interval at end of current collection interval (i.e., at 9:10 AM in the scenario explained above). Also, MG9K flushes its history performance data at 9:10 AM.

Because of this behavior difference between MG9K and MG9KEM PM components (i.e., performance browser and OM Collector), any data collected by OM Collector and/or Performance browser till and including 9:15 AM, may not be accurate.

21.8.2.2 GUI name: Performance Statistics Browser

21.8.2.2.1 Functional description

Two date range fields “From” and “To” are shown on Performance browser. Today, these two fields show date either in steps of 15 minutes or in steps of 1 day. Apart from 15 minutes and 1 day, in SN08, these two fields show date in steps of 5 minutes also.

21.8.2.2.2 GUI usage and implications

None

21.8.2.2.3 GUI size

Table 10 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Performance Statistics Browser	1	One per GUI workstation	No change

21.8.2.2.4 GUI fields

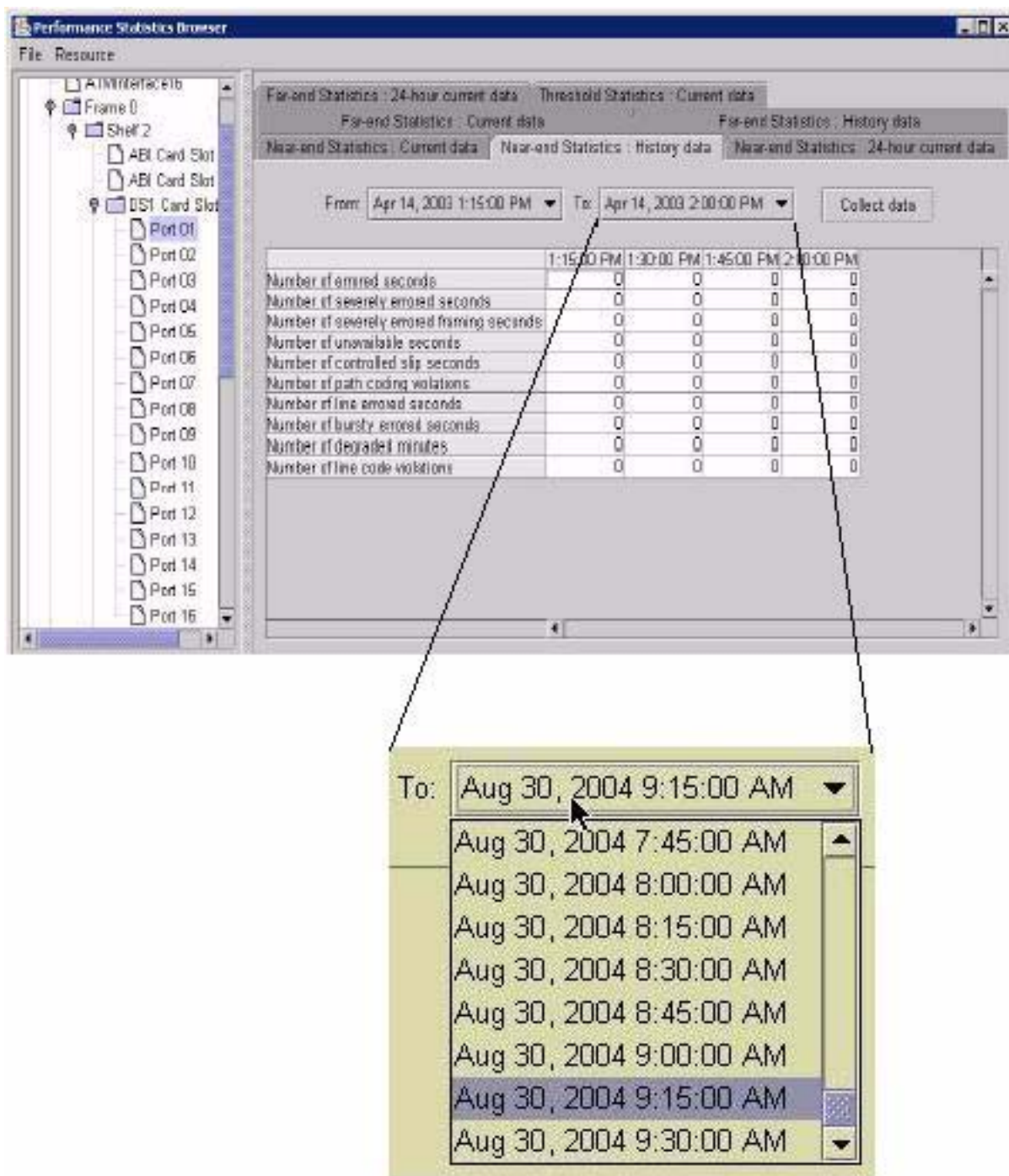
The following table lists fields for GUI “Configure Collection Intervals”.

Table 11 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
From	Changed	NA	Data ranges are based on Sample interval	Date range shown corresponds to last 96 sample intervals. Size of each interval is equal to the Sample interval.	None
To	Changed	NA	Data ranges are based on Sample interval	Date range shown corresponds to 96 sample intervals. Size of each interval is equal to the Sample interval.	None

21.8.2.2.5 Usage example

The following example shows the GUI “Configure Collection Interval“, when the value “15 minutes” is selected.



21.8.2.2.6 GUI release history update

The date range fields present in Performance browser are based on the sample interval.

21.8.2.2.7 Context sensitive launching information

None

21.8.2.2.8 Supplementary information

None

21.8.3 CLUI Interface

NA

21.9 User interface changes

NA

21.10 OSSGate Interface Changes

None

21.11 Security

NA

21.11.1 Authentication

The new GUI “**Configure Collection Interval**” has an authorization level of “emsrw”.

21.12 Configuration Walkthrough

None

21.13 Reference

[1] A00007213 FN

[2] A00007107 FN

[3] A00003531 CN

22: A00007243 Configuration (CN)

22.1 Feature name

Prevent Outage when CEM flash has not been erased

22.2 Hardware and Software Requirements

The functionality requires SN08 on the core with MG4K21 on MG4K nodes.

22.3 Initial Configuration

Not Applicable.

22.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable

22.5 Upgrade Considerations

Not Applicable

22.6 Data schema (DS) (CM, MIBS, RDB)

Not Applicable

22.7 Service Orders (SO) (CM & SESM)

Not Applicable

22.8 Element Management

Not Applicable

22.9 User interface changes

22.9.1 Directory: SPMDIR

This feature changes a command response in the SPMDIR directory, but does not modify the directory itself.

22.9.1.1 Directory description

The commands in this directory help operating company personnel to operate and maintain the Spectrum Peripheral Module (SPM) at the node level.

22.9.1.2 Accessing directory:

22.9.1.2.1 Access to directory or MAP level and return to CI

To access the SPMDIR level from the CI environment, type:

>MAPCI;MTC;PM;POST SPM <node_no>

or

>MAPCI;MTC;PM;POST SPM <SPMNo> (0 to max.spm_no.)

or
 >MAPCI;MTC;PM;POST SPM all
 This is an example of entering the command:
 >MAPCI;MTC;PM;POST SPM 0

To return to the CI environment, type:
 >QUIT ALL

or
 >QUIT MAPCI

22.9.2 Command: QueryPM

22.9.2.1 Command type: Listed MENU

22.9.2.2 Command target: All

22.9.2.3 Command availability: RES

22.9.2.4 Command description

The QueryPM command displays miscellaneous information about the SPM, such as the shelf number, slot number, unit number, state and activity status for all the datafilled modules (such as CEM, DSP, VSP, OC3, ATM, SYNCRM, IEM, STM or DLC). This command applies to DMS Call Processing (DMSCP), Inter-working (IW) and Media Gateway 4000 (MG4K) class variants but enhancement is specific to MG4K nodes.

The QueryPM command has an optional parameter, OPTION to display the fault and load information of the currently posted SPM and all its devices. The OPTION parameter has two possible values: FLT and FILES. The optional parameter REASON for the FLT option value displays the reasons for the ISTB/SYSB state of the Resource Modules (RMs) of the posted SPM.

22.9.2.5 Command syntax

The command syntax is as shown below.

Figure 1 SPM QueryPM command syntax

```
QueryPM: Display miscellaneous information about the PM.
Parms: [<OPTION> {FLT [<REASON> {REASON}]}
        [<POSTSET> {All}},
        FILES}]
```

Table 1 QueryPM command parameters and variables

Command	Parameters and variables
QueryPM	[<OPTION> {FLT [<REASON> {REASON}] [<POSTSET> {All}], FILES}]
Parameters and variables	Description
FLT	Fault (optional). This command provides a list of devices, on the posted SPM, that are currently reporting a fault (FLT) condition.
FLT REASON	Fault Reason (optional). This command provides the reasons for the ISTB/SYSB state of the devices on the posted SPM.
FLT ALL	Fault All (optional). This command provides a list of devices, on all the posted SPMs that are currently reporting a fault condition regardless of the SPM currently displayed on the MAP.
FLT REASON ALL	Fault Reason All (optional). This command provides the reasons for the ISTB/SYSB states of devices, on all the posted SPMs regardless of the SPM currently displayed on the MAP.
FILES	Files (optional). This command displays the default load names and the currently running loads in all devices on the posted SPM. It also displays the Flash Loader's load file for each device that supports Flash Loader functionality. Additionally, it displays the image file for each device on the posted SPM.

22.9.2.6 Qualifications and warnings

No warnings are displayed.

22.9.2.7 Responses

Neither the QueryPM command nor any of its options have required parameters; therefore, the user is never prompted for additional information when issuing any variant of the QueryPM command.

In all cases, the QueryPM options either output the data requested or output a message stating that the data are unavailable.

The following is enhanced response for the provided by this activity for MG4K nodes.

22.9.2.7.1 QUERYPM FLT REASON request response - when unit/device state is ISTB/SYSB

Table 2 MAP outputs with associated meanings and actions

Command >MAPCI;MTC;PM; POST SPM <SPMNo> >QUERYPM FLT REASON
CEM 0 ISTb NonCritical faults: Board: CPK MAC address doesn't match prov.data. [SPM313]. Meaning: The response means that MAC address of the CEM card does not match the datafill in table MNCKTPAK for that CEM card. This new response has been added to QUERYPM FLT REASON command and is only for the CEM card of MG4K variant of the SPM. System actions: N/A User actions: Change the datafill in table MNCKTPAK to match the MAC address of the physical CEM card.

22.9.2.8 Example

Table 3 Usage examples for QueryPM flt reason command

Description of task	Querying Flt reason on an SPM/s.
Command: MAP response:	QueryPM flt reason Board: CPK MAC doesn't match prov.data. [SPM313]. It shows that MAC datafill mismatch between physical card and MNCKTPAK datafill. Craft has to change the datafilled MAC to match MAC on physical card. Check SPM 313 log for more details.

22.9.3 Directory: CEMDIR

This feature changes a command response in the CEMDIR directory, but does not modify the directory itself.

22.9.3.1 Directory description

The commands in this directory help operating company personnel to operate and maintain the CEM at the node level.

22.9.3.2 Accessing directory:

22.9.3.2.1 Access to directory or MAP level and return to CI

To access the CEMDIR level from the CI environment, type:

```
>MAPCI;MTC;PM;POST SPM <node_no>;SELECT CEM <CEMNo>
```

This is an example of entering the command:

```
>MAPCI;MTC;PM;POST SPM 0; select cem 0
```

To return to the CI environment, type:

```
>QUIT ALL
```

or

```
>QUIT MAPCI
```

22.9.4 Command: RTS

22.9.4.1 Command type: Listed MENU

22.9.4.2 Command target: All

22.9.4.3 Command availability: RES

22.9.4.4 Command description

RTS command tries bring an MANB CEM running S/W to INSV state. RTS is available at the CEM MAP level. This command applies to DMS Call Processing (DMSCP), Inter-working (IW) and Media Gateway 4000 (MG4K) class variants.

22.9.4.5 Command syntax

The command syntax is as shown below.

Figure 2 RTS command syntax

```
RTS: Return the selected CEM to Service.
    ALL option applies to all the selected CEMs (one or both).
Parms: [<All> {ALL}]
        [<Force> {FORCE}]
        [<Prompt> {NOPROMPT}]
        [<Options> {NOWAIT,
                    NOREPLY}]
```

Table 4 RTS command parameters and variables

Command	Parameters and variables
RTS	<pre>[<All> {ALL}] [<Force> {FORCE}] [<Prompt> {NOPROMPT}] [<Options> {NOWAIT, NOREPLY}]</pre>
Parameters and variables	Description
ALL	The ALL option will attempt to bring all the both CEMs of SPM to INSV state from a MANB (manual busy) state.
FORCE	Indicates that user wishes to override warnings, if any, during RTS.
NOPROMPT	Indicates that user does not wish any Yes/No prompting messages to be displayed. Response to prompts defaults to "Yes".
NOWAIT	Indicates that user does not wish to wait for the command response.
NOREPLY	Indicates that user does not desire a response from the map on execution of the command.

22.9.4.6 Qualifications and warnings

No warnings are displayed.

22.9.4.7 Responses

If RTS fails change CEM to INSV/ISTb state then on the MAP it displays reason for failure of the RTS command but enhancement is specific to MG4K nodes.

The following is enhanced response for the provided by this activity for MG4K nodes.

22.9.4.7.1 RTS request response - when unit/device state is MANB

Table 5 MAP outputs with associated meanings and actions

Command >MAPCI;MTC;PM; POST SPM <SPMNo>;SELECT CEM <CEMNo> >RTS
Request has been submitted. Command completed. The state is now ISTb. CPK MAC address doesn't match prov.data. Please update table MNCKTPAK to match physical MAC address. Meaning: Mismatch between MAC datafilled and actual MAC on the card. Change the datafill in MNCKTPAK to match the MAC address of the physical CEM card. System actions: N/A User actions: Change the datafill in table MNCKTPAK to match the MAC address of the physical CEM card.

22.9.4.8 Example

Table 6 Usage examples for RTS command

Description of task	Change CEM state to INSV from MANB.
Command: MAP response:	RTS CPK MAC address doesn't match prov.data. Please update table MNCKTPAK to match physical MAC address. Indicates that MAC mismatch exists between physical card MAC and MNCKTPAK datafill. Craft has to update MAC datafill in table MNCKTPAK so that it matches with the physical MAC.

22.10 OSSGate Interface Changes

Not Applicable

22.11 Security

Not Applicable

22.12 Configuration Walkthrough

Not Applicable

23: A00007250 Configuration (CN)

23.1 Feature name

ACDMIS Over TCP

23.2 Hardware and Software Requirements

This feature will use the existing TLI interface to provide connectivity between the DMS-100/CS2K and a DSP. The DMS -100/CS2K is provided with Local Area Network (LAN) connectivity by an Ethernet Interface Unit (EIU) or in the case of a CS2KCompact, the 3PC card. The basic ACD software package is needed to use this feature.

23.3 Initial Configuration

The configuration for this feature is detailed in the DS section of this document.

23.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

23.5 Upgrade Considerations

23.5.1 Dump and Restore (CM)

No manual action is required. A reformat Procedure will be used as the software solution.

ONP reformat procedures will be written to default the LNKSEL field of table ACDMISPL to X25 as required. Transport datafill changes from X25 to TCP/IP or TCP/IP to X25 may require the ACDMIS link to be brought down and may require datafill changes to existing X25 related tables.

23.5.2 Element Management Upgrade

N/A

23.5.3 Downgrade impact

N/A

23.6 Data schema (DS) (CM, MIBS, RDB)

23.6.1 New/modified tables, MIBs, or Database Schema

The existing ACDMISPL table will be modified to define the relationship between the ACDMIS pool and the transport type, X.25 or TCP/IP. This feature will introduce a new field named LNKSEL to the ACDMISPL table. The new LNKSEL field will be datafillable with either X25 or TCP with the TCP designation having additional refinements of an IP address that refers to

the remote DSP, an Alternative IP address for the remote DSP, a UserID and a Password. The newly created LNKSEL field will serve a dual purpose of defining which remote IP addresses are allowed access to the DMS-100/CS2K as well as defining the relationship between the pool and session link. Impacted tables are listed below in Table 1

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
ACDMISPL	CHANGED	UNCHANGED

23.6.1.1 Fields/OIDs

The following table lists fields/OIDs for ACDMISPL

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
POOL		n/a		ACD Pool Name
PASSWORD		n/a		Pool Password
PROTOCOL		n/a		ACD MIS Protocol Version
OUTEVENT		n/a	10 to 200	Message Buffers
BUNDLING		n/a	Y or N	Message Bundling
LNKSEL	NEW	n/a	X25 or TCP	Indicates whether this pool will use a X25 or TCP transport.
X25	NEW	n/a	n/a	If X25 is chosen no additional refinements are needed as existing X25 tables and datafill are used.
TCP	NEW	IP_ADDR	IP Address	If TCP is chosen an additional refinement is required to indicate the remote systems IP Address.
	NEW	ALT_IP_ADDR	IP Address	Refinement to allow an alternative or “back-up” IP Address for the remote system.
	NEW	USER_ID	Alphanumeric >=5 and <= 8 Characters	Mandatory refinement which will be used to verify the Userid field of the nosLogon message.
	NEW	LOGIN_PASSW D	Alphanumeric >=5 and <=16 Characters	Mandatory refinement which will be used to verify the Password field of the nosLogon message.

23.6.1.2 Datafill example

- **ACDMISPL Datafill Example for TCP Transport**

```
POOL:
>ACDPOOL
PASSWORD:
>PASSWD1
PROTOCOL:
>BCS35
OUTEVENT: 200
>110
BUNDLING:
>N
LNKSEL:
>TCP
IP_ADDR:
>47 245 5 2
ALT_IP_ADDR:
>47 246 6 3
USER_ID:
>USER2
LOGIN_PASSWD:
>PASS2

TUPLE TO BE ADDED:
ACDPOOL PASSWD1 BCS35 110 N TCP 47 245 5 2 47 246 6 3 USER2
PASS2
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

- **ACDMISPL Datafill Example for X25 Transport**

```
POOL:
>ACDPOOL
PASSWORD:
>PASSWD1
PROTOCOL:
>BCS35
OUTEVENT: 200
>110
BUNDLING:
>N
LNKSEL:
>X25
```

TUPLE TO BE ADDED:
 ACDPOOL PASSWD1 BCS35 110 N X25
 ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

- **Example of ACDMISPL table**

TABLE: ACDMISPL

POOL PASS	PROTOCOLOUTEVENTBUND	LNKSEL

POOL01POOL01	BCS43	110NX25
POOL02POOL02	BCS43	110N
TCP 47 245 5 247 246 6 3	USER2 PASS2	

23.6.1.3 Supplementary information

The alternative IP Address (ALT_IP_ADDR) refinement for TCP in table ACDMISPL is mandatory. If no alternative IP Address is available, the ALT_IP_ADDR field should be datafilled with the same IP Address used for the IP_ADDR field.

Any changes to existing tuples in the ACDMISPL table will require the ACD MIS LINK to be brought down if there is an active session on the Pool/tuple being changed. If there is not an active session on the Pool/tuple being changed, then changes are allowed.

In addition to the above restriction, changes in the LNKSEL field from TCP to X25 will require the standard X25 datafill that has always been used when establishing a ACD MIS X.25 Link, which will involve changes/additions to table datafill in table MPCLINK.

23.6.1.4 Translation verification and other tools

N/A

23.7 Service Orders (SO) (CM & SESM)

There are no SERVORD impacts for this feature.

23.8 Software optionality control (SOC)

There is no SOC interaction with this feature.

23.9 Element Management

Not applicable

23.10 User interface changes

Not applicable

23.11 OSSGate Interface Changes

Not applicable

23.12 Security

Not applicable

23.13 Configuration Walkthrough

Not applicable

24: A00007271 Configuration (CN)

24.1 Feature name

TOPS EOL for SN08

24.2 Hardware and Software Requirements

None.

24.3 Initial Configuration

Not applicable.

24.4 Office Parameters

None.

24.5 Upgrade Considerations

24.5.1 Dump and Restore

This section documents the behavior of certain tables over an ONP from a pre-SN08 load to an SN08 load (or higher).

24.5.1.0.1 Table TMSOCDL

All tuples datafilled in table TMSOCDL will be dropped.

24.5.1.0.2 Table OCGRP

All tuples datafilled in table OCGRP as LAPD (indicating ETMS) will be dropped.

24.5.1.0.3 Table VLMEM

All tuples datafilled in table VLMEM which reference a LAPD tuple in OCGRP will be dropped.

24.5.1.0.4 Table OCHOST

A tuple datafilled in table OCHOST which references a LAPD tuple in OCGRP will halt the table transfer.

24.5.1.0.5 Table OCHOSTQ

All tuples datafilled in table OCHOSTQ which reference a LAPD tuple in OCGRP will halt the table transfer.

24.5.1.0.6 Table TQMSFCQA

All tuples datafilled in table TQMSFCQA as SA (in the ASSTAREA field) will halt the table transfer.

24.5.1.0.7 Table TOPSPOS

All tuples datafilled in table TOPSPOS as TMS (indicating ETMS) will be dropped.

24.5.1.0.8 Table PARSMBR

All tuples datafilled in table PARSMBR which reference a TMS tuple in TOPSPOS will be dropped.

24.5.2 Element Management Upgrade

Not applicable.

24.5.3 Downgrade impact

None.

24.6 Data Schema

24.6.1 New/modified tables

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/or DELETED/	Table Control (NEW/OLD/ UNCHANGED)
ARUIBMRT	DELETED	N/A
DUAQOPT	DELETED	N/A
DQMODEM	DELETED	N/A
HOBICDEV	DELETED	N/A
OPRDAT	DELETED	N/A
SAQSIZE	DELETED	N/A
TOPSPARM	CHANGED	UNCHANGED
VSNOPT	CHANGED	UNCHANGED
VROPT	CHANGED	UNCHANGED
OCGRP	CHANGED	UNCHANGED
TOPSPOS	CHANGED	UNCHANGED
OCHOSTQ	CHANGED	UNCHANGED
TQMSFCQA	CHANGED	UNCHANGED
TMSOCDL	CHANGED	UNCHANGED

24.6.2 Table information

The following tables have been deleted as of SN07:

-
- ARUIBMRT
 - DUAQOPT
 - DQMODEM
 - HOBICDEV

The following tables have been deleted as of SN08:

- OPRDAT
- SAQSIZE

24.6.2.1 Name: TOPSPARM

The following parms have been removed as of SN07, and cannot be re-added:

- LANG_ERROR_SCREEN_DISPLAY
- ADAS_ENABLE

24.6.2.2 Name: VSNOPT

The following parms have been removed as of SN07, and cannot be re-added:

- OPR_0PLUS_3RD_DISPLAY
- OPR_0PLUS_COL_DISPLAY
- OPR_0PLUS_3RDCON_DISPLAY
- OPR_0PLUS_CLDCON_DISPLAY

24.6.2.3 Name: VROPT

The following parms have been removed as of SN07, and cannot be re-added:

- DA_BP_HOTEL_ROOM_REQUIRED

The following parms have been removed as of SN08, and cannot be re-added:

- TOPSACD_DASERV_INSTANCE
- TOPSACD_INTCserv_INSTANCE

24.6.2.4 Name: OCGRP

All tuples with a DLSEL (within the DLOVRLAY field) of LAPD will be removed as of SN08, and cannot be re-added.

24.6.2.5 Name: TOPSPOS

All tuples with a DATATYPE (within the DATAPATH field) of TMS will be removed as of SN08, and cannot be re-added.

24.6.2.6 Name: OCHOSTQ

As of SN08, all tuples which have a REROUTESEL of Y will have VLTHROTL removed from their REASONS set (if it is present), and cannot be re-added. If a REASONS set contains only VLTHROTL, then the

REROUTESEL will be set to N and the ALTHOST will be removed.
VLTHROTL cannot be re-added to a REASONS set.

24.6.2.7 Name: TQMSFCQA

All tuples with an ASSTTYPE (within the ASSTAREA field) of SA cannot be added as of SN08.

24.6.2.8 Name: TMSOCDL

All tuples will be removed as of SN08, and cannot be re-added.

24.7 Service Orders

Not applicable.

24.8 Software optionality control (SOC)

Not applicable.

24.9 Element Management

Not applicable.

24.10 User interface changes

Not applicable.

24.11 OSSGate Interface Changes

Not applicable.

24.12 Security

Not applicable.

24.13 Configuration Walkthrough

Not applicable.

25: A00007277 Configuration (CN)

25.1 Feature name

LOGs Throttling

25.2 Hardware and Software Requirements

See section 13.5 for Table (Data Schema0.

25.3 Initial Configuration

25.4 Office/Subnet parameters (OP/SP) (CM & SESM)

25.5 Upgrade Impact

25.6 Data schema (DS) (CM, MIBS, RDB)

25.6.1 New/modified tables, MIBs, or Database Schema

The requirement of this feature is to use of datafill table for throttling logs.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
LOGTHROT	New	OLD

Customer can throttle the log report by specifying the time unit and threshold value.

There is also a requirement to throttle the DLOG when it is specified by the customer. By default throttled logs will go to DLOG, unless it is specified by the user.

Only core logs will be throttled.

Desired behavior of this feature is to implement the throttling mechanism for LOG Devices and DLOGs. New throttling functionality will allow customer to specify on Time Units and Thresholds per Report Name (REPNAME) through a Table LOGTHROT.

LOGs Throttling functionality is implemented only for XA-Core (PowerPC) platform. Table LOGTHROT is not implemented for 68K and 88K platform.

25.6.2 Table/MIB/Remote Database Schema information

25.6.2.1 Name: <abbreviated name of table, MIB, or Database if applicable> LOGTHROT

25.6.2.1.1 Functional description

The following information for each report name (REPNAME) appears in table LOGTHROT:

“the threshold that specifies which messages the terminal prints or displays

“the time, in minutes, when the register count associated with a threshold report resets to 0 (zero)

“if a log needs to be throttled in DISK LOG (DLOG)

For any log name that does not appear in table LOGTHROT, the values in fields THRESHOLD and TUNITS are 0.

Table LOGCLASS allows a maximum of 100 different time units (TUNITS).

If the field THRESHOLD is 0 (print all reports), field TUNITS must be 0 or <0.

The following office parameters can affect the production of the log reports:

“LOG_CENTRAL_BUFFER_SIZE in table OFCVAR

“LOG_DEVICE_BUFFER_SIZE in table OFCVAR

“LOG_CENTRAL_POLLING_MILLI_SECOND in table OFCSTD

“SYSLOG_ACCESS in table OFCVAR

Refer to the Input/Output System Reference Manual, 297-1001-129 for additional information on log systems.

25.6.2.1.2 Usage sequence and implications (CM Only)

You do not need to enter data in other tables before you enter data in table LOGTHROT.

25.6.2.1.3 Size

The system automatically allocates memory for a maximum of 512 tuples.

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LOGTHROT	0	512	Memory is automatically allocated for 512 tuples.

25.6.2.1.4 Fields/OIDs

The following table lists fields for TABLE LOGTHROT:

1- REPNAME

2- THRESHOLD

3- TUNITS

4- DLOG

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
REPNAME	New		see subfields	Report name. This field contains subfields
		LOGNAME	alphabetical (up to 4)	Log name. Enter the log name. Refer to the Log Report Reference Manual for a list of log names in the logs system.
		REPNUM	000 to 999 or -1	Report number. Enter the report number. If all report numbers are necessary, enter -1.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
THRSHOLD	New		0 to 255	Threshold. Enter the number to specify which messages the system prints or displays. Enter 0 to generate all messages. If threshold is 1 to 255, logs will be throttled as per defined threshold value.
TUNITS	New		-32768 to 32767	Time units. Enter the time, in minutes, when the register count associated with a threshold report resets to 0. This table allows a maximum of 100 unique TUNITS. Enter 0 or a negative value to generate all reports. Enter 0 or a negative value (<0) if TUNITS = 0 if a reset is not necessary.
DLOG	New		Y or N	Disk Log. Enter Y (yes) if DLOGs need to be throttled. Enter N (no) if DLOGs do not need to be throttled.

25.6.2.1.5 Datafill example

Sample datafill for table LOGTHROT appears in the following example.

Figure 1

TABLE LOGTHROT:			
REPNAME	THRSHOLD	TUNITS	DLOG

TRK 113	5	1	N

25.6.2.1.6 Table release history update

25.6.2.1.7 Supplementary information

Same tuple cannot be existed in both the tables LOGSCLASS and LOGTHROT at the same time. If an Tuple exists in Table LOGCLASS and user want to add the same tuple in table LOGTHROT following warning will be appear on the screen:

INFO: ENTRY EXIST IN TABLE LOGCLASS.

PLEASE REMOVE THE ENTRY FROM LOGCLASS FIRST.

INCONSISTENT DATA

And vice versa:

INFO: ENTRY EXIST IN TABLE LOGTHROT.

PLEASE REMOVE THE ENTRY FROM LOGTHROT FIRST.

INCONSISTENT DATA

25.6.2.1.8 Translation verification other tools

LOGTHROT does not use translation verification tools.

25.7 Service Orders (SO) (CM & SESM)

25.8 Software optionality control (SOC)

25.9 Element Management

25.10 Command interface changes

25.11 Security

25.12 Configuration Walkthrough

26: A00007293 Configuration (CN)

26.1 Feature name

VLAN for Gigabit Ethernet

26.2 Data schema (DS) (CM, MIBS, RDB)

26.2.1 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)
nnGLinkVlanTable	NEW	n/a

26.2.2 Table/MIB/Remote Database Schema information

26.2.2.1 Name: nnGLinkVlanTable

26.2.2.1.1 Functional description

MIB table nnGLinkVlanTable is used to create, modify, and delete VLANs on the MG9K. There is one entry for each VLAN. The table is indexed by a unique VLAN ID defined by the user.

26.2.2.1.2 Fields/OIDs

The following table lists fields/OIDs for an entry in the nnGLinkVlanTable.

Table 2 VLAN Entry

Field	Type	Description
nnGLinkVlanId	INTEGER	Index into the VLAN table.
nnGLinkVlanName	SnmpAdminString	20 character string
nnGLinkVlanType	INTEGER	byPort or byIpSubnet; in SN08 all VLANs are byIpSubnet.

Field	Type	Description
nnGLinkVlanPortMember1	InterfaceIndexOrZero	IfIndex of a port associated with this VLAN. A value of 0 indicates no port association with this member.
nnGLinkVlanPortMember2	InterfaceIndexOrZero	
nnGLinkVlanPortMember3	InterfaceIndexOrZero	
nnGLinkVlanPortMember4	InterfaceIndexOrZero	
nnGLinkVlanPortMember5	InterfaceIndexOrZero	
nnGLinkVlanPortMember6	InterfaceIndexOrZero	
nnGLinkVlanPortMember7	InterfaceIndexOrZero	
nnGLinkVlanPortMember8	InterfaceIndexOrZero	
nnGLinkVlanPrimarySubnetAddr	IpAddress	The SCG IP address for this VLAN.
nnGLinkVlanPrimarySubnetMask	IpAddress	Corresponding primary subnet mask for the primary IP address.
nnGLinkVlanSecondarySubnetAddr	IpAddress	This is provided for extensibility purposes.
nnGLinkVlanSecondarySubnetMask	IpAddress	This is provided for extensibility purposes.
nnGLinkVlanUserPriority	INTEGER	Specified VLAN priority as defined in 802.1 Q; range is 0 - 7.
nnGLinkVlanPeakRate	Unsigned32	Peak rate at which the packets on this VLAN will be sent to the destination port.
nnGLinkVlanRowStatus	RowStatus	

27: A00007415 Configuration (CN)

27.1 Feature name

Internodal Emergency Standalone (ESA) Element Manager

27.2 Hardware and Software Requirements

SN08 or later software load for both the MG9000 and Element manager.
Passport Virtual Router (PVR).

27.3 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 the call server. Prior to SN08 only intra-nodal ESA was supported. With the introduction 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 will function. 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 the community is established.

The customer should first determine how the nodes will be grouped together into communities. In addition each MG will need to be configured with a new ESA IP address. This IP address should be chosen from an available IP address from the call control subnet (the same subnet used for VMG configuration). No “default” communities are provided so each community must be manually configured 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.

27.4 Upgrade Considerations

None

27.4.1 Dump and Restore (CM)

27.4.2 Element Management Upgrade

27.4.3 Downgrade impact

Prior to SN08 intra-nodal ESA was not supported. Therefore if an MG9K is in a community and is downgraded to SN07 from SN08 an error message will be generated and the user will not be able to downgrade until the node is removed from its community.

27.5 Data schema (DS) (CM, MIBS, RDB)

27.5.1 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)
nnCommunityOfInterest	NEW mib	

27.5.2 Table/MIB/Remote Database Schema information

27.6 Element Management

27.6.1 New/modified GUIs

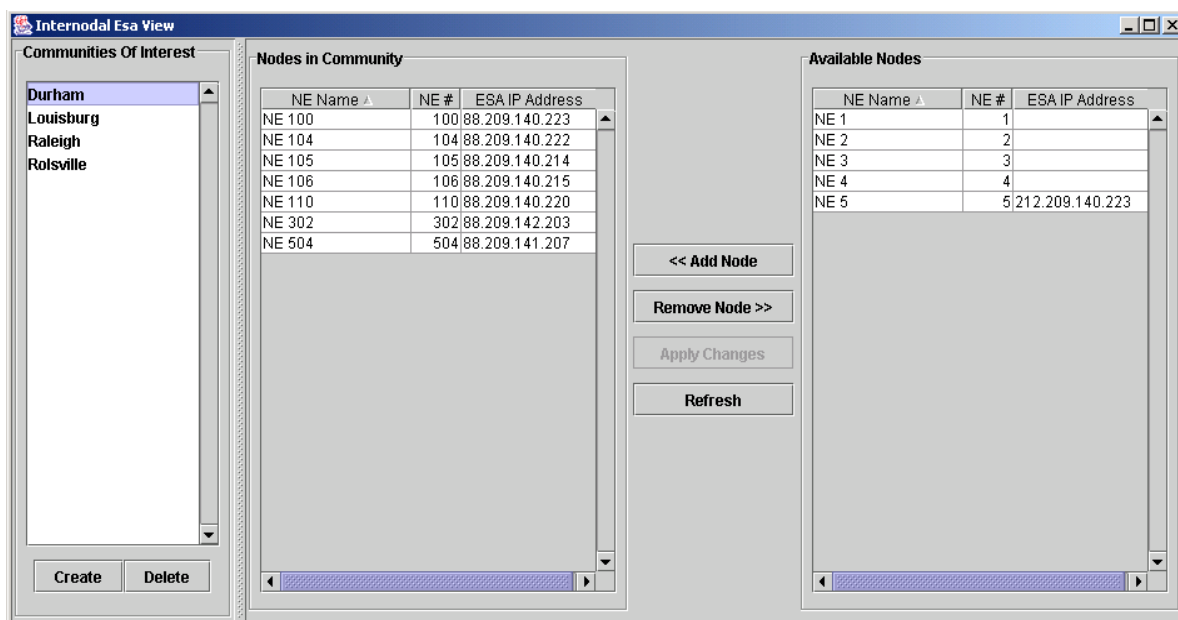
Table 2 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Internodal ESA Configuration	NEW

27.6.2 GUI information

The new GUI will allow the customer to configure communities of interest. A screenshot is provided below for reference only - the screen is subject to change.

Figure 1 Community Of Interest Configuration GUI



27.6.2.1 GUI name: COI Configuration

Community of Interest Configuration

27.6.2.1.1 Functional description

The purpose of the COI Configuration GUI is to allow the customer to manage Internodal ESA Communities of Interest. The GUI is accessed from the main subnet view window under the “Configuration” menu item. The GUI layout contains three main list windows.

The Communities Of Interest List contains a list of all currently defined communities. When you click on an item in this list the “Nodes In Community” list changes. The number of communities is limited to 32.

The “Nodes In Community” list displays all the nodes that are currently in the selected community of interest. The number of nodes in a community is limited to 15.

The “Available Nodes” list displays all nodes that are available to be added to a community (they do not currently belong to a community). Only nodes that are ESA enabled will be displayed in this list.

The Create and Delete buttons allow the user to create and delete COI names. COI names are limited to 20 characters and can only contain the characters ‘a’ - ‘z’, ‘A’ - ‘Z’, and underscore.

The Add Node button allows the user to add nodes from the available list to the COI node list. Before a node is added the ESA IP address must be set.

The Delete Node button allows the user to remove nodes from the selected community. The currently selected node in the “Nodes In Community” list will be removed from the list and it will appear in the “Available Nodes” list.

IP Address field. The ESA IP Address field in the “Nodes in Community” list and “Available Nodes” list is editable. The other fields in the lists are not editable. The IP Address field must be configured before a node is added to the community. When the user presses enter or clicks in another window or button, the IP address will be validated and saved in the database. The IP address must be “well-formed” and unique in the system.

The Apply Changes button allows the user to apply changes to the Community. The button is disabled until there are changes to commit. When the user makes changes to a community the button is disabled. If the user tries to leave the GUI or click on another community name, the user will be prompted to save or discard changes.

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 “Reconfigure” button on the GUI. The “Reconfigure” button will cause the currently selected COI data to be sent to all affected nodes.

The Refresh button allows the user to completely refresh the GUI with data from the database.

27.6.2.1.2 GUI usage and implications

The GUIs must be configured in the following sequence. This sequence is for adding a new community of interest.

1. Configure MG9K nodes to support ESA, configuring VMGs, etc.

2. Bring up the COI Configuration GUI.
3. Click the Create button to create a new COI name.
4. In the “Available Nodes” list, select a node to be added to the community.
5. Set the ESA IP address of the node and press enter.
6. Click the Add Node button.
7. Repeat until all desired nodes are added to the community.
8. Press the Apply Changes button.

A NE cannot be deleted if it is in a community of interest. An error message will be generated if the user attempts to delete an NE that is configured in a community.

27.6.2.1.3 GUI size

Table 3 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
COI Configuration	0	1	fixed memory allocation.

27.6.2.1.4 GUI fields

The following table lists fields for GUI or pull down menu <abbreviated name of GUI>.

Table 4 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
ESA IP Address	New	no	Valid, Unique IP Address	The initial value is blank. The field must be filled in before a node is added to a community.	
COI Name	New	no	Community of Interest Name. Up to 20 characters (a-z, A-Z, and underscore). COI names not case sensitive. So “COI1” and “coil” cannot co-exist.		

27.6.2.1.5 Usage example

The following example shows sample datafill or menu selection for GUI <abbreviated name of GUI>:

See above image.

27.6.2.1.6 GUI release history update

27.6.2.1.7 Context sensitive launching information

27.6.2.1.8 Supplementary information

27.6.3 CLUI Interface

27.7 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” communities 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 both the MG9K and MG9KEM with required software.
2. Launch the MG9K Element Manager from a web browser.
3. Select Configure Internodal ESA from the main menu.
4. Set the ESA IP address of the nodes that are being placed into communities.
5. Create a new community of interest.
6. Add desired nodes to the community of interest.
7. Click Apply Changes button.
8. 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 “Reconfigure” button on the GUI. The “Reconfigure” button will cause the currently selected COI data to be sent to all affected nodes.

28: A00007464 Configuration (CN)

28.1 Feature name

SBA Packet Cable Event Messaging

28.2 Hardware and Software Requirements

This feature is dependent on actid A00007196 (SBA PacketCable Event Messaging). Namely, it assumes successful datafill of CRSFMT and CRMAP tables for PCEM and PCES PacketCable streams.

TABLE: CRSFMT

KEY	FORMAT	DATADUMP	CDRSRCH	ALARMS	TIMERDMP	TIMERVAL
NIL	NTFMT	N	NIL_FM	N	N	0
AMA	BCFMT	N	NIL_FM	N	N	0
PCEM	PCEMFMT	N	NIL_FM	N	N	0
PCES	PCESFMT	N	NIL_FM	N	N	0

TABLE: CRSMAP

KEY	STREAM

CAMA	AMA
LAMA	AMA
TOPS	AMA
PCEM	PCEM
PCES	PCES

28.3 Initial Configuration

This activity spans across switch core (3pc, xacore, brisc) and the CBM (Core Billing Manager).

Following is recommended:

- On CBM:
 - PacketCable Accounting stream (PCEM) must be configured for 6 hours of IAA (Integrated Accounting Application) downtime. This amounts to a logical volume requirement of 8Gbytes for SBA.
 - PCEM stream must be configured so that it grows to maximum possible size 20Mbytes. i.e. File closure based on max number of bytes.

28.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Entire section is not applicable

28.5 Upgrade Considerations

28.5.1 Dump and Restore (CM)

Although new field (EXPEDITE) is introduced in table SDMBILL, the upgrade scenario is handled through the reformat proc. This proc., on upgrade to CSP21(SN08), will convert old tuple appropriately.

28.5.2 Element Management Upgrade

Not applicable

28.5.3 Downgrade impact

None.

28.6 Data schema (DS) (CM, MIBS, RDB)

28.6.1 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)
SDMBILL	CHANGED	UNCHANGED

28.6.2 Table/MIB/Remote Database Schema information

28.6.2.1 Name: SDMBILL (SDM Billing Table)

This table is modified to include one additional field named EXPEDITE.

28.6.2.1.1 Functional description

- Extra field named EXPEDITE is introduced in table SDMBILL
- PacketCable streams PCEM and PCES needs to provide PacketCable Event Messages as per 'SN08 PacketCable EM requirements for Billing' specifications. This is accomplished through new EXPEDITE field. This field will be set to Y for PCEM and PCES streams, and set to N for legacy streams such as AMA, OCC, SMDR
- Table SDMBILL is dependent on table CRSFMT. If an entry is added to CRSFMT table, corresponding entry will be created in SDMBILL through table dependency proc.
- for each entry in SDMBILL table, corresponding stream is visible in mapci;mtc;appl;sdmbil;post level. Stream can be configured/activated/deactivated from this level
- If an entry is deleted from CRSFMT table, corresponding entry will be deleted from SDMBILL table through table dependency proc.

- EXPEDITE field in software controlled and is not editable

28.6.2.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill table SDMBILL in any specific order

28.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SDMBILL	1	15	No additional memory impact

28.6.2.1.4 Fields/OIDs

NA

28.6.2.1.5 Datafill example

The following example shows sample datafill for table SDMBILL

```

TABLE: SDMBILL
SDMBKEY SDMBACT SDMBSTAT  EXPEDITE  VOLUMES
-----
--
      NIL      OFF      Off      N      $
      AMA      ON      InSv      N      (F02LAMA1) (F17LAMA1)$
      PCEM    OFF    Off      Y      (F02LPCEM1) (F17LPCEM1)$

```

28.6.2.1.6 Table release history update

Added field EXPEDITE to provide delivery of PacketCable Event Messages (billing data) to CBM.

28.6.2.1.7 Supplementary information

None

28.6.2.1.8 Translation verification and other tools

SDMBILL does not use translation verification tools.

28.7 Service Orders (SO) (CM & SESM)

Entire section is not applicable

28.8 Software optionality control (SOC)

Not applicable

28.9 Element Management

28.9.1 CLUI Interface

No new commands are introduced by this activity. Behavior of addvol command has changed for PacketCable Electronic Surveillance (PCES) steam. See “Configuration Walkthrough” on page 1711.

28.10 User interface changes

No new commands are introduced by this activity. Behavior of addvol command has changed for PacketCable Electronic Surveillance (PCES) steam. See “Configuration Walkthrough” on page 1711.

28.11 OSSGate Interface Changes

Entire section is not applicable

28.12 Security

Entire section is not applicable

28.13 Configuration Walkthrough

28.13.1 Provisioning of PacketCable Accounting stream (PCEM)

- core: create Accounting stream (PCEM) by datafilling CRSFMT table

TABLE: CRSFMT

KEY	FORMAT	DATADUMP	CDRSRCH	ALARMS	TIMERDMP	TIMERVAL

NIL	NTFMT	N	NIL_FM	N	N	0
PCEM	PCEMFMT	N	NIL_FM	N	N	0

- core: Due to CRSFMT / SDBBILL table dependency, creation of PCEM entry in CRSFMT creates following entry in table SDBBILL

TABLE: SDBBILL

SDBKEY	SDBACT	SDBSTAT	EXPEDITE	VOLUMES

NIL	OFF	Off	N	\$
AMA	ON	InSv	N	(F02LAMA1) (F17LAMA1)\$
PCEM	OFF	off	Y	\$

- core: assign backup volumes to Accounting stream PCEM. This is done by issuing mapci;mtc;appl;sdbbil;addvol pcem f02lpcem1 f17lpcem1

TABLE: SDBBILL

SDBKEY	SDBACT	SDBSTAT	EXPEDITED	VOLUMES

NIL	OFF	Off	N	\$

AMA	ON	InSv	N	(F02LAMA1)	(F17LAMA1)\$
PCEM	OFF	Off	Y	(F02LPCEM1)	(F17LPCEM1)\$

- core: map calldata type PCEM to accounting stream PCEM by datafilling CRSMAP table

```
TABLE: CRSMAP
KEY      STREAM
-----
CAMA     AMA
LAMA     AMA
TOPS     AMA
PCEM    PCEM
```

- cbm: configure PCEM billing stream using billmtc;confstrm;add command

example:

```
Stream Name [] { } : pcem
Is this a Filter Stream [NO] {NO YES } : no
Stream Record Format [] {SMDR BC CDR300 CDR250 PCEM PCES } : pcem
File Format Type [] {LW } : lw
Please specify the logical Volume [/cbmdata/00/billing/pcem] { } : /cbmdata/00/billing/pcem
Do you want Files closed based on time [NO] {NO YES } : no
Number of records per day [0] { } : 0
Maximum Number of records per file [500000] {10000 - 500000} : 500000
Maximum Number of bytes per file [20000000] {1000000 - 20000000} : 20000000
```

```
Stream Name -> PCEM
Is this a Filter Stream -> NO
Stream Record Format -> PCEM
File Format Type -> LW
Logical Volume Name -> /cbmdata/00/billing/pcem
Do you want Files closed based on time -> NO
Number of records per day -> 0
Average record size -> 80
Maximum Number of records per file -> 500000
Maximum Number of bytes per file -> 20000000
Commit ? [Save] {Save Edit Abort} : save
Saving stream
Configuration of Stream PCEM is now complete
```

- cbm: modify logical volume of already configured pcm stream (from billmtc;confstrm;change map level) while stream is still inactive

example:

Stream Name [] {} : pcem
 Stream Record Format [PCEM] {SMDR BC CDR300 CDR250 PCEM PCES } : pcem
 File Format Type [LW] {LW } : lw
 Please specify the logical Volume [/cbmdata/00/billing/pcem] {} :
 /cbmdata/00/billing/acct
 Do you want Files closed based on time [NO] {NO YES } : no
 Number of records per day [0] {} : 0
 Maximum Number of records per file [500000] {10000 - 500000} : 500000
 Maximum Number of bytes per file [20000000] {1000000 - 20000000} : 20000000

Stream Name -> PCEM
 Is this a Filter Stream -> NO
 Stream Record Format -> PCEM
 File Format Type -> LW
 Logical Volume Name -> /cbmdata/00/billing/acct
 Do you want Files closed based on time -> NO
 Number of records per day -> 0
 Average record size -> 80
 Maximum Number of records per file -> 500000
 Maximum Number of bytes per file -> 20000000
 Commit ? [Save] {Save Edit Abort} : save
 Saving stream
 Configuration of Stream PCEM is now complete

- cbm: query PCEM from billmtc;confstrm;list map level) while stream is inactive

example:

Stream Name [] {} : pcem

Displaying stream(s) PCEM

Stream Name -> PCEM

Stream Running status -> NO

Is this a Filter Stream -> NO

Stream Record Format -> PCEM

File Format Type -> LW

Logical Volume Name -> /cbmdata/00/billing/acct

Do you want Files closed based on time -> NO

Maximum Number of records per file -> 500000

Maximum Number of bytes per file -> 20000000

- core: activate PCEM billing stream by issuing command
“mapci;mtc;appl;sdbil;post pcem;sdbctrl pcem on”
- cbm: query PCEM from billmtc;confstrm;list map level) while stream is active

example:

Stream Name [] {} : pcem

Displaying stream(s) PCEM

Stream Name -> PCEM

Stream Running status -> YES

Is this a Filter Stream -> NO

Stream Record Format -> PCEM

File Format Type -> LW

Logical Volume Name -> /cbmdata/00/billing/pcem

Do you want Files closed based on time -> NO

Maximum Number of records per file -> 10000

Maximum Number of bytes per file -> 1000000

- cbm: modify ‘File closure criteria’ of already configured pcem stream
(from billmtc;confstrm;change map level) while stream is active

example:

Stream Name [] {} : pcem
 Do you want Files closed based on time [NO] {NO YES } : yes
 File Closure time limit [10080] {5 - 10080} : 5
 Number of records per day [0] {} : 0
 Maximum Number of records per file [500000] {10000 - 500000} : 500000
 Maximum Number of bytes per file [20000000] {1000000 - 20000000} : 20000000

Stream Name -> PCEM
 Stream Running status -> YES
 Is this a Filter Stream -> NO
 Stream Record Format -> PCEM
 File Format Type -> LW
 Logical Volume Name -> /cbmdata/00/billing/pcem
 Do you want Files closed based on time -> YES
 File Closure time limit -> 5
 Number of records per day -> 0
 Average record size -> 80
 Maximum Number of records per file -> 500000
 Maximum Number of bytes per file -> 20000000

- core: display of pcam map level (mapci;mtc;appl;sdbil;post pcam

	IOD	PM	CCS	Lns	Trks	Ext	APPL
ITOC	4LIU7	4	RS	.	132C..	1Crit	.
	C	*C*	*C*		*C*	*C*	
POST	OAMAP	ATMFW	SDM	SPMCP	SWMTC	SDMBIL	
PKT	TOPSIP						
0 Quit	.	.	.	.	.	.	.
2 Post_							
3 Addvol_							
4 Remvol_	PCEM :	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 POST:
15
16
17 Audit
18
D
Time 19:59 >

- cbm: query command

example:

query pcam

PCEM:

PrimarySubStream: InSv
Number of Records in Open Files: 100
ClosedNotSent Files Available: 59
Records within the ClosedNotSent files: 7244059
Date of Last File Sent:
Tue Oct 19 11:25:16 2004

- cbm: amadump command

example:

amadump pcam

Error: pcam record format is not supported.

- cbm: sendfile command

example:

sendfile pcam

Sendfile does not support the LW format.

- cbm: listfile command

example:

```
U.20041019.111713.01071.PCEM.P
  Date: Tue Oct 19 11:17:13 2004 Recs: 122527 Size: 15622128 CNS
U.20041019.112213.01072.PCEM.P
  Date: Tue Oct 19 11:22:13 2004 Recs: 122801 Size: 15657016 CNS
U.20041019.112713.01073.PCEM.P
  Date: Tue Oct 19 11:27:13 2004 Recs: 122675 Size: 15640904
```

- cbm: closec command

example:

```
# closec pcm
```

```
No open files found
```

- cbm: attempt to create filter stream for already configured PCEM stream

```
Stream Name [] {} : emf
Is this a Filter Stream [NO] {NO YES } : YES
Associated Stream Name [] {} : pcm
```

Error: PCEM is a packet cable stream and cannot be specified as an associated stream.

28.13.2 Provisioning of PacketCable LI stream (PCES)

- core: create LI stream (PCES) by datafilling CRSFMT table

TABLE: CRSFMT

KEY	FORMAT	DATADUMP	CDRSRCH	ALARMS	TIMERDMP	TIMerval
NIL	NTFMT	N	NIL_FM	N	N	0
PCES	PCESFMT	N	NIL_FM	N	N	0

- core: Due to CRSFMT / SDMBILL table dependency, creation of PCES entry in CRSFMT creates following entry in table SDMBILL

TABLE: SDMBILL

SDMBKEY	SDMBACT	SDMBSTAT	EXPEDITE	VOLUMES	
NIL	OFF	Off	N	\$	
AMA	ON	InSv	N	(F02LAMA1)	(F17LAMA1)\$
PCES	OFF	Off	Y	\$	

- core: Note that backup volumes are not required for PCES stream. In fact, mapci;mtc;appl;sdbil;addvol pces f02lpces f17lpces command will alert user with 'backup volumes cannot be configured for PCES stream'.
- core: map calldata type PCES to LI stream PCES by datafilling CRSMAP table

TABLE: CRSMAP

KEY	STREAM
CAMA	AMA
LAMA	AMA
TOPS	AMA
PCES	PCES

- cbm: configure PCES billing stream using billmtc;confstrm;add command

example:

Stream Name [] {} : pces

Is this a Filter Stream [NO] {NO YES } : no

Stream Record Format [] {SMDR BC CDR300 CDR250 PCEM PCES } : pces

Stream Name -> NPES

Is this a Filter Stream -> NO

Stream Record Format -> PCES

Commit ? [Save] {Save Edit Abort} : save

Saving stream

Configuration of Stream PCES is now complete

- cbm: query PCES from billmtc;confstrm;list map level when stream is inactive

example:

Stream Name [] {} : pces

Displaying stream(s) PCES

Stream Name -> PCES

Stream Running status -> NO

Is this a Filter Stream -> NO

Stream Record Format -> PCES

- core: activate PCES billing stream by issuing command
“mapci;mtc;appl;sdbil;post pces;sdbctrl pces on”
- cbm: query PCES from billmtc;confstrm;list map level when stream is active

example:

Stream Name [] {} : pces

Displaying stream(s) PCES

Stream Name -> PCES

Stream Running status -> YES

Is this a Filter Stream -> NO

Stream Record Format -> PCES

- cbm: attempt to modify already configured pces stream (from billmtc;confstrm;change map level) while stream is active. Note that no changes are allowed.

example:

Stream Name [] {} : pces

Stream Name -> PCES

Stream Running status -> YES

Is this a Filter Stream -> NO

Stream Record Format -> PCES

Commit ? [Save] {Save Edit Abort} :

Commit ? [Save] {Save Edit Abort} :

Saving stream

Configuration of Stream PCES is now complete

- cbm: attempt to create filter stream for already configured PCES stream

Stream Name [] {} : esf

Is this a Filter Stream [NO] {NO YES } : YES

Associated Stream Name [] {} : pces

Error: PCES is a packet cable stream and cannot be specified
as an associated stream.

- core: display of pcam map level (mapci;mtc;appl;sdmbil;post pces

	IOD	PM	CCS	Ln	Trks	Ext	APPL
ITOC	4LIU7	4	RS	.	132C..	1Crit	.
	C	*C*	*C*		*C*	*C*	
POST	OAMAP	ATMFW	SDM	SPMCP	SWMTc	SDMBIL	
PKT	TOPSIP						
0 Quit	.	.	.	.	.	.	.
2 Post_							
3 Addvol_							
4 Remvol_	PCES :	InSv	Pri:	InSv	Rec:	Offl	
5			Bkup:	Offl	Comm:	InSv	
6 TST							
7 Bsy							
8 RTS							
9 Conf_							
10							
11 DispAL							
12							
13 Status							
14 Query	POST:						
15							
16							
17 Audit							
18							
D							

Time 19:59 >

- cbm: amadump command

example:

amadump pces

Error: pces record format is not supported.

- cbm: sendfile command

example:

sendfile pces

No file formats supported for PCES stream.

- cbm: listfile command

example:

listfile pces

Error: No file formats supported for PCES stream

- cbm: closec command

example:

closec pces

No open files found

28.14 Recommended SBA configuration

This activity spans across switch core (3pc, xacore, brisc) and the CBM (Core Billing Manager).

Following is recommended:

- On CBM:
 - PacketCable Accounting stream (PCEM) must be configured for 6 hours of IAA (Integrated Accounting Application) downtime. This amounts to a logical volume requirement of 8Gbytes for SBA.
 - PCEM stream must be configured so that it grows to maximum possible size 20Mbytes. i.e. File closure based on max number of bytes.

29: A00007465 Configuration (CN)

29.1 Feature name

Integrated Accounting Application (IAA)

29.2 Hardware and Software Requirements

The IAA has the following hardware requirements:

- SUN Netra 240
- 2GB of RAM dedicated for the IAA modules, for a system configuration of 4GB.

The IAA has the following software requirements:

- SSPFS 3rd party Software Suite Version 08 with the following version dependencies:
- Apache Web Server 2.0.47 or above
- JRE 1.4.2_04 or above
- Apache Tomcat 4.1.24 or higher
- SBA
- jdom 1.0 beta 7 or higher
- dom4j 1.4
- saxon 6.4.3

29.3 Initial Configuration

Following the installation of the IAA modules the following items must be configured:

- RKS pair
- DF
- Distribution Schedule
- Global System parameters

29.4 Upgrade Considerations

This is the first installation of this application, there are no upgrade considerations for this release. The software is designed and packaged such that two or more versions can reside on the same platform, this allows the system to be upgraded without interruption of service. Tools will be provided to migrate the configuration of previous release to the latest release, beginning with SN09.

29.4.1 Patching

Fixes required to an existing IAA application will be delivered in the form of a solaris patch. The patch will follow the conventions set forth in the CBM Designer's Guide.

29.4.2 Dump and Restore (CM)

For SN08 the ability to backup the current configuration to a removable storage media is supported. This configuration information can be used to populate the configuration of a second instance on the same system or on a second system.

Beginning with SN09 a migration tool will be supplied to take an existing configuration and use the information to populate the configuration of the new version. Once the new release is loaded on the system the command "migrate_configuration -p<prev_rel> -c<current_rel>" is used to move the previous release's configuration information to the new release's configuration.

29.4.3 Downgrade impact

Providing that the old software has not been removed, the old software only needs to be re-registered with SAM, by issuing the \$BASEDIR/bin/appctrl -i command.

29.5 Element Management

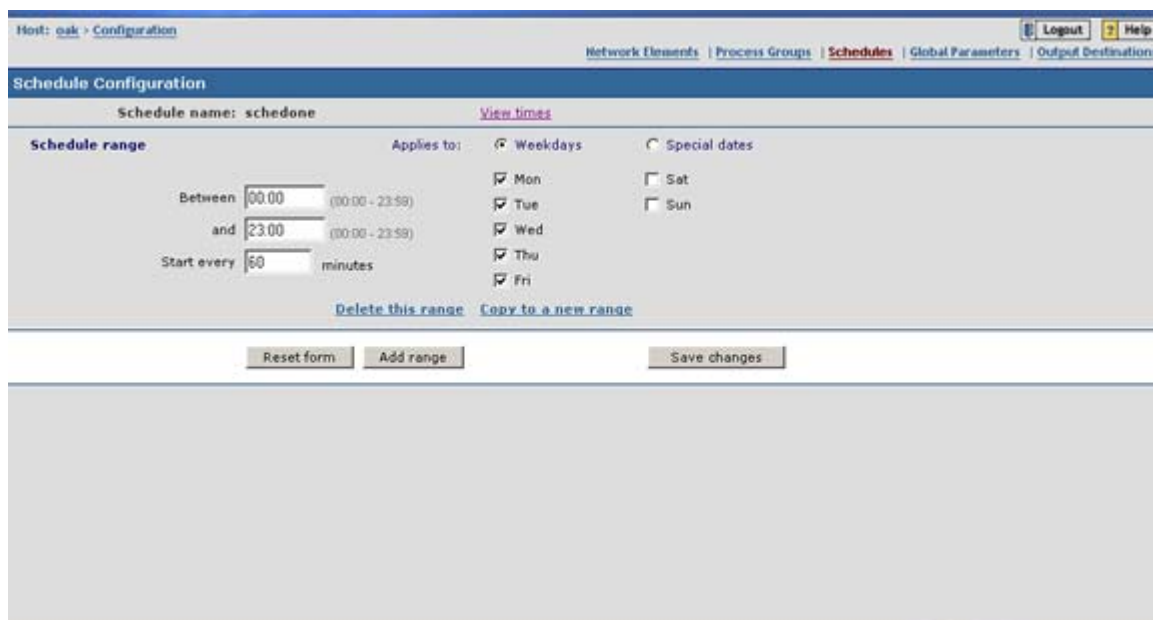
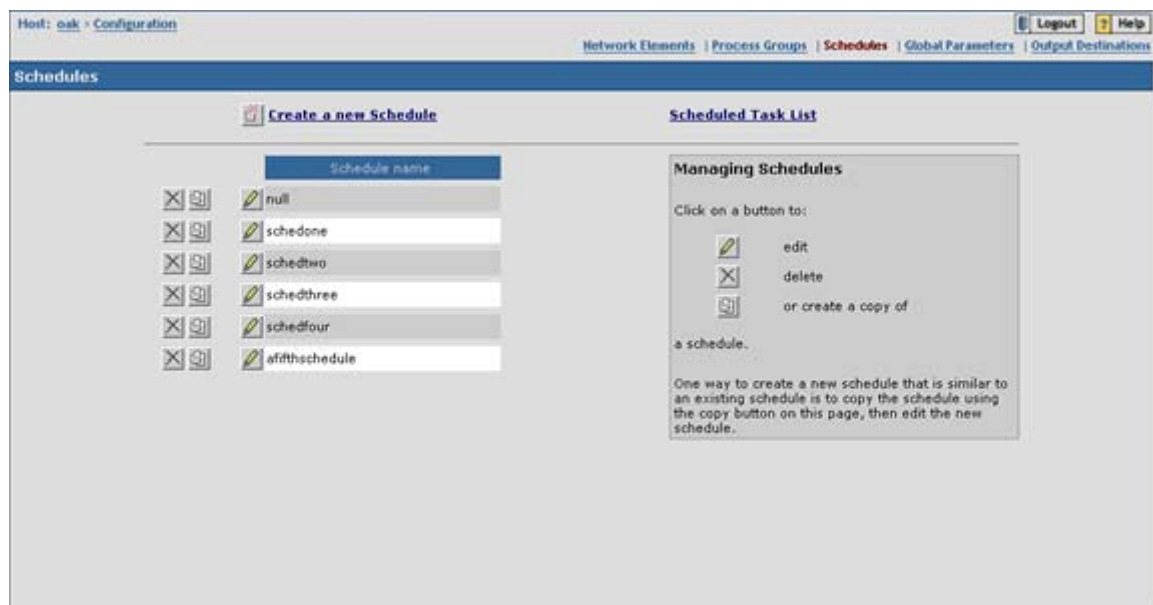
Configuration changes for the IAA modules can be done via a Web interface or via a command line program. On-line help is available from each web page, by selecting the help button at the top of each page.

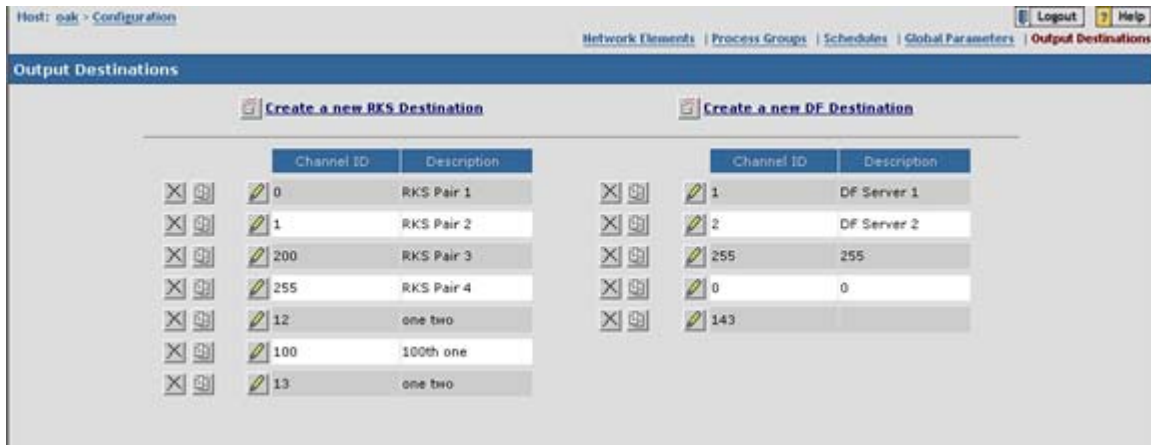
29.5.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
RKS Output Destination	NEW
DF Output Destination	NEW
Global System Parameters	NEW

29.5.2 GUI information





29.5.2.1 GUI name: RKSOD

RKS Output Destination

29.5.2.1.1 Functional description

This GUI is used to configure the downstream RKS pairs to which the EMDA sends event messages as well as the protocol to use.

Example:

The screenshot shows the 'RKS Output Destination Configuration' window. At the top, there's a navigation bar with 'Network Elements', 'Process Scripts', 'Schedules', 'Global Parameters', and 'Output Destinations'. The main area is divided into sections. The first section is for 'Channel ID: 200' with a 'Description' of 'P2P File 2' and 'Destination Type: RKS'. Below this, there are fields for 'FTP Direction' (Inbound/Outbound), 'Maximum File Length' (10 MB), 'Maximum File Open Time' (10 minutes), 'File Priority' (2), and 'Schedule' (null). The 'FTP Mode' is set to 'FTP' with a 'Secure FTP' checkbox. The 'Security Protocol' is set to 'None' with a 'SPSec' checkbox. The 'Primary RKS' section includes fields for 'IP Address' (191.40.37.172), 'FTP Port' (21), 'Server username' (ksuser1), 'Server password', and 'Destination Directory' (\\191.40.37.172\incoming\bin). The 'Secondary RKS' section has similar fields for 'IP Address' (191.40.37.172), 'FTP Port' (21), 'Server username' (ksuser2), 'Server password', and 'Destination Directory' (\\191.40.37.172\incoming\sec). At the bottom, there are fields for 'Retry Limit' (3), 'Retry Interval' (3), 'Messages in Batch' (5), 'Batch Interval' (3), and 'Shared Secret' (0000000000000000). 'Reset form' and 'Save changes' buttons are at the bottom right.

29.5.2.1.2 GUI usage and implications

The Schedule GUI must be datafilled prior to datafill of this GUI.

29.5.2.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
RKSOD	1	1	N/A

29.5.2.1.4 GUI fields

On-line help is available on this web page which defines the meanings of each field contained on the page.

Table 3 Output Destination Streams

Parameter	Description/ List of values	Data Format	Validation	Max Value	Max Field Size	Default Value
Channel Id	1 byte field	integer	required	255		

Table 3 Output Destination Streams

Parameter	Description/ List of values	Data Format	Validation	Max Value	Max Field Size	Default Value
Destination Type	0 - DF 1 - RKS	integer	required		1	
Description	Free Form Text	alphanumeric	optional		32	
DF Collector / Primary RKS IP	IP address	alphanumeric	required		15	
DF Collector / Primary RKS Radius Port		positive integer	required	65535		
Primary RKS FTP Port		positive integer	required if RKS (note 1)	65535		21
Primary RKS FTP Username		alphanumeric	required if RKS (note 1)		32	
Primary RKS FTP Password		alphanumeric [not displayed]	required if RKS (note 1)		32	
Primary RKS Destination Directory		alphanumeric	Optional (Note 1)		512	
Secondary RKS IP	IP address		required if RKS		15	
Secondary RKS Radius Port		positive integer	required if RKS	65535		
Secondary RKS FTP Port		positive integer	optional (note 1)	65535		21
Secondary RKS FTP Username		alphanumeric	optional (note 1)		32	
Secondary RKS FTP Password		alphanumeric [not displayed]	optional (note 1)		32	
Secondary RKS Destination Directory		alphanumeric	Optional (note 1)		512	
Retry Limit	Number of retries	integer	required	9		3
Retry Interval	in seconds	positive integer	required	9		1

Table 3 Output Destination Streams

Parameter	Description/ List of values	Data Format	Validation	Max Value	Max Field Size	Default Value
Batch Interval	in seconds	positive integer	required	30		2
Messages in Batch	Number of messages	positive integer > 1	required	10		5
Shared Secret		alphanumeric	required		32	00000000 00000000
Security Protocol	0 - None 1 - IPSec	Integer	required	1		1 - IPSec
FTP Inbound / Outbound	0 - Outbound (Push) 1 - Inbound (Pull)	integer	required	1		
FTP Schedule	List of Configured Schedules	alphanumeric	only if FTP Outbound			
FTP Mode	0 - FTP 1 - Secure FTP	integer	only if FTP Outbound	1		sFTP
Max. File Length	size of file in bytes, kB, MB	positive integer	required		3	2 MB
Max. Open Time	time in minutes	positive integer	required	120		60
File Priority	1, 2, 3, 4	positive integer	required	4		1 - lowest

Notes

(1) Only if sending mode is set to FTP

29.5.2.2 GUI name: DFOD

DF Output Destination

29.5.2.2.1 Functional description

This GUI is used to configure the downstream DF which the EMDA sends LI event messages as well as the protocol to use.

Example:

Host: oak > Configuration Logout Help

Network Elements | Process Groups | Schedules | Global Parameters | **Output Destinations**

DF Output Destination Configuration

Channel ID: 2 Destination Type: DF

Description: DF Server 2

IP Address: 212.12.34.169 RADIUS Port: 21

Retry Limit: 3 Retry Interval: 3

Shared Secret: 0000000000000000

Reset form Save changes

29.5.2.2.2 GUI usage and implications

No other datafill is required prior to datafill of this GUI.

29.5.2.2.3 GUI size

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
DFOD	1	1	N/A

29.5.2.2.4 GUI fields

On-line help is available on this web page which defines the meanings of each field contained on the page.

Table 5 Output Destination Streams

Parameter	Description / List of values	Data Format	Validation	Max Value	Max Field Size	Default Value
Channel Id	1 byte field	integer	required		255	
Channel Type	0 - DF 1 - RKS	integer	required		3	
Description	Free Form Text	alphanumeric	optional		32	
DF Collector / Primary RKS IP	IP address	alphanumeric	required		16	
DF Collector / Primary RKS Radius Port		positive integer	required	65535		21
Retry Limit	Number of retries	integer	required	9		3
Retry Interval	in seconds	positive integer	required	9		1

Table 5 Output Destination Streams

Parameter	Description / List of values	Data Format	Validation	Max Value	Max Field Size	Default Value
Shared Secret		alphanumeric	required		32	00000000 00000000

29.5.2.3 GUI name: GSP

Global System Parameters.

29.5.2.3.1 Functional description

This GUI is used to configure the NE providing the Accounting messages.

Example:

The screenshot shows a web-based configuration interface titled 'Global Parameters'. It contains several input fields and controls:

- Packet Cable Element ID:** A text box containing 'asasa'.
- Format Version:** A dropdown menu currently showing 'PacketCable Multimedia'.
- Time Zone Daylight Savings Time:** A checkbox that is currently unchecked.
- Time Zone UTC Offset (h:mm:ss):** A dropdown menu with a small input box next to it.
- Accounting Message Sending Mode:** A dropdown menu currently showing 'FTP'.
- Event Message File Path:** A text box containing '/cbndata/00/meddata/outgoing/ftpdata/sending'.
- Buttons:** 'Reset form' and 'Save changes' buttons are located at the bottom of the form.

29.5.2.3.2 GUI usage and implications

No other datafill is required prior to datafill of this GUI.

29.5.2.3.3 GUI size**Table 6 New or modified GUIs**

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GSP	1	1	N/A

29.5.2.3.4 GUI fields

On-line help is available on this web page which defines the meanings of each field contained on the page.

Table 7 Packet Cable Global Parameters

Parameter	Description / List of Values	Data Format	Validation Description	Max. Value	Max Field Size	Default Value
Element ID	5 digit unique Network Element ID	integer	required	99999		
Format Version	1 - PktCbl 1.0 2 - PktCbl 1.1 3 - PktCbl Multimedia	positive integer	required	3		1
TimeZone DST	0 - Standard 1 - DST	integer	required	1		
TimeZone UTC Offset	+/- HHMMSS	alphanumeric	required		10	
Sending Mode for Accounting Messages	0 - RADIUS Realtime 1 - RADIUS Batch 2 - FTP	integer	required		1	0
EM File Path	Unix File Path	Printable ASCII Characters Only	required		256	0

29.6 User interface changes

29.6.1 Command: `iaa_config_cli`

29.6.1.1 Command type: NON-MENU

29.6.1.2 Command target: CBM

29.6.1.3 Command availability: RES

29.6.1.4 Command description

This command is used to provide the user with a means to configure the IAA modules from the command line.

At any point during the execution of this command changes can be saved to the active configuration. If the users decide they do not want to save any changes made they can abort the program and leave the configuration unchanged.

29.6.1.5 Command syntax

From the command line a user in the maint group may execute this command to configure the IAA application.

Table 8 <CommandName> command parameters and variables

Command	Parameters and variables
iaa_config	None (displays a menu)

1. From the main menu the user can select to configure Global system parameters or Output Destinations, which includes DFS or RKS pairs.

```
=====
Main Menu                                     Page 1 of 1
=====

1. Global Parameters
2. Output Destinations

=====
[S]ave      e[X]it      [N]extPage      [P]revPage      [Q]uit
Select: █
```

2. From the Global Parameter Screen the user can change any of the Global Parameters as described in section 29.5.2.3. The Daylight Savings field (DST) is used to populate the DST field in the Packet Cable file header when events are ftped to the RKS.

```

=====
Global Parameters                                     Page 1 of 1
=====
1. Element ID [00001]
2. Packet Cable Format Version [1]
3. Enable Daylight Saving [0]
4. UTC Offset [+000000]
5. Sending Mode [0]
* 6. Base EM File Path [/cbmdata/00/iaa/ftpout/]
7. EM File Path [ ]

Note: * Fields are not Editable
=====
[S]ave      [R]eturn    [N]extPage   [P]revPage   [Q]uit
Select: █

```

3. From the Output Destinations screen, Delivery Function or Record Keeping Server Destination configuration screens can be selected.

```

Status: None
=====
Output Destinations                                     Page 1 of 1
=====
1. Delivery Function Destinations
2. Record Keeping Server Destinations

=====
[S]ave      [R]eturn    [N]extPage   [P]revPage   [Q]uit
Select: █

```

4. From the Record Keeping Server screen the user can list the existing RKS destinations, create a new destination, copy an existing destination to a new destination, edit, view or delete an existing destination.

```

=====
Record Keeping Server Destinations                               Page 1 of 1
=====

1. List
2. New
3. Copy
4. Edit
5. View
6. Delete

=====
[Slave]      [R]eturn      [N]extPage    [P]revPage    [Q]uit
Select: █

```

5. From the new or edit selections, items described in section 29.5.2.1 can be configured.

```

Status: None
=====
RKS Destination Parameters                                     Page 1 of 3
=====

1. Channel ID           [ ]
2. Description           [ ]
3. Primary IP Address   [ ]
4. Primary RADIUS Port  [ ]
5. Secondary IP Address [ ]
6. Secondary RADIUS Port [ ]
7. Retry Limit          [3]
8. Retry Interval       [3]
9. Shared Secret        [0000000000000000]
10. Batch Interval      [3]
11. Messages In Batch   [5]

=====
[A]dd      [R]eturn      [N]extPage    [P]revPage    [Q]uit
Select: █

```

6. When the Delivery Function selection is made from the Output Destinations menu, the user is presented with the following screen. From the Delivery Function Server screen the user can list the existing DF destinations, create a new destination, copy an existing destination to a new destination, edit, view or delete an existing destination


```

Status: None
=====
                Delivery Function Destinations                Page 1 of 1
=====

1. List
2. New
3. Copy
4. Edit
5. View
6. Delete

=====
[S]ave      [R]eturn    [N]extPage    [P]revPage    [Q]uit
Select: █

```

7. From the new or edit selections, items described in section 29.5.2.2 can be configured.

```

=====
                DF Destination Parameters                Page 1 of 1
=====

1. Channel ID                [ ]
2. Description                [ ]
3. IP Address                 [ ]
4. RADIUS Port                [ ]
5. Retry Limit                [3]
6. Retry Interval             [3]
7. Shared Secret              [0000000000000000]

=====
[A]dd      [R]eturn    [N]extPage    [P]revPage    [Q]uit
Select: █

```

29.6.1.6 Qualifications and warnings

Incorrect configuration of the system could result in lost event messages.

29.6.1.7 Responses

The program prompts the user through a menu for information to configure the IAA modules.

Host: oak > Tools Logout Help

[Application Status](#) | [Viewers](#) | [View config files](#) | [SNMP Graphs](#) | [User Logins](#) | [System Administration](#) | [System Logs](#)

Event Viewer -- Settings BCID Subquery report View report

1 Query Start

Start Date: 9/9/2004 Start Time: 00:00:00

2 Query End

End Date: 9/9/2004 End Time: 23:59:59

3 Maximum Matches

Max Matches: 10

NOTE! For best performance, limit the number of matches to display.

4 Build Search Criteria

Channel ID		
Filename		
Originating Number		
Terminating Number		
Element ID		
BCID		

This field not for use with BCID Subquery report.

View report

Host: oak > Tools Logout Help

[Application Status](#) | [Viewers](#) | [View config files](#) | [SNMP Graphs](#) | [User Logins](#) | [System Administration](#) | [System Logs](#)

Event Viewer -- Results

Report Created: Sep 9, 2004 6:45:10 PM

Date/Time Filter: Sep 8, 2004 12:00:00 AM - Sep 9, 2004 11:59:59 PM

Search Criteria: Event Message Type != NULL

	Processing Time	Originating Number	Terminating Number	Event Message	Element ID	Event Time
+	09/09/2004 14:54:16			CallAnswer	12345	20021114163757.805
+	09/09/2004 14:54:16			CallAnswer	12345	20021114163757.815
+	09/09/2004 14:54:16			CallDisconnect	12345	20021114163801.987
+	09/09/2004 14:54:16			SignalingStop	12345	20021114163801.987
+	09/09/2004 14:54:16			SignalingStop	12345	20021114163802.114

[illegible]

29.7 Security

Accounting messages are sent to the downstream RKS pairs via the RADIUS protocol or using ftp or secure ftp. When using RADIUS or regular ftp, IPsec can be used as the underlying security protocol if configured. When using sftp, IPsec is optional.

Legal Intercept messages are sent to the downstream DF over an IPSec connection. Should the connection to the downstream DF become unavailable the LI messages will be discarded after the configured number of retry attempts have been exhausted, this will result in lost LI messages. LI messages will not be viewable in the web based event viewer nor will they be stored on disk while being processed by the IAA.

Access to the web interface, which can be used to configure the IAA application as well as for viewing events that have not been sent to the downstream RKS pair because of communications errors, is controlled via a login page. The user is prompted for their userid and password before access to the web interface is granted. The authentication method ties into the same one used for users to gain local access to the system. The web interface can be configured to use SSL if required.

29.7.1 Network configuration

29.7.2 IPSec needs to be configured between the CBM and the downstream RKS pair or DF server. This is handled by the SSPSF, the IAA makes use of this feature.**Key management**

Once configured, key management is handled at the SSPSF level, the IAA makes use of this feature.

29.7.3 Protocol

IPSec is utilized by the IAA to send real-time events to the downstream RKS pair or DF server. SFTP can be used to send files to the RKS pair if the IAA is configured to do so.

29.7.4 Authentication

Access to the Web interface is controlled by the Java JAAS unix authentication method, which uses the same userid and password used to gain CLI access to the CBM. When a user attempts to log in to the Web interface, they must enter their userid and password which allows them access to the system. The user must also be in the maint group to gain access to the configuration and record viewing screens available via the web interface.

29.8 Configuration Walkthrough

Once installed the users is required to configure the IAA Global System Parameters, the desired DF(s) to which LI event messages will be delivered and the desired RKS pair(s) to which Accounting event messages will be delivered.

29.8.1 Creating Logical Volumes for use by the IAA

The following logical volumes are required before the installation of the IAA software.

1. `makelv /cbmdata/00/iaa/config 512`
2. `makelv /cbmdata/00/iaa/data 5120`
3. `makelv /cbmdata/00/iaa/ftpout 8192`
4. `makelv /cbmdata/00/iaa/kdb 17408`

29.8.2 Configure RKS Output Destination

1. On the Main User Interface, click on Configuration -> Output Destinations.
2. Click on Create a new RKS Destination
3. The RKS Output Destination Configuration user interface will appear, as below:

Host: [redwood](#) > [Configuration](#) [Global Parameters](#) | [Output D](#)

RKS Output Destination Configuration

Channel ID: Destination Type: RKS
Description:

FTP Direction: ☐ Inbound ☒ Outbound
Maximum File Length: MB
Maximum File Open Time: minutes
File Priority:
Schedule:
FTP Mode: ☒ FTP ☐ Secure FTP
Security Protocol: ☒ None ☐ IPsec

Primary RKS
IP Address: RADIUS Port:
FTP Port:
Server username: Server password:
Destination Directory:

Secondary RKS
IP Address: RADIUS Port:
FTP Port:
Server username: Server password:
Destination Directory:

Retry Limit: Retry Interval:
Messages in Batch: Batch Interval:
Shared Secret:

4. Enter the requested information such as Channel ID, Description, FTP Direction, Primary IP Address and Primary RADIUS Port.
5. If values other than the defaults are desired, enter them for the Maximum File Length, Maximum File Open Time, File Priority, Retry Limit, Retry Interval, Messages in Batch, Batch Interval, and Shared Secret
6. If selecting the FTP Direction as Outbound, select a Schedule, FTP Mode and the Security Protocol. Also, enter information for the Primary and Secondary FTP Port, Server username, Server password and Destination Directory if desired.
7. Click on Save Changes.

29.8.3 Configure DF Output Destination

1. On the Main User Interface, click on Configuration -> Output Destinations
2. Click on Create a new DF Destination

3. The DF Output Destination Configuration user interface will appear, as below:

The screenshot displays the 'DF Output Destination Configuration' page within the Nortel Networks Integrated Accounting Application. The page header includes the application name and navigation links like 'Reports', 'Tools', and 'Configuration'. The main content area contains several input fields: 'Channel ID', 'Description', 'IP Address', 'RADIUS Port', 'Retry Limit' (set to 3), 'Retry Interval' (set to 3), and 'Shared Secret' (a long alphanumeric string). At the bottom, there are two buttons: 'Reset form' and 'Save changes'.

4. Enter the requested information such as Channel ID, Description, IP Address and RADIUS Port
5. If values other than the defaults are desired, enter them for the Retry Limit, Retry Interval and Shared Secret
6. Click on Save Changes

29.8.4 Sending or Retrieving Files from the IAA

Accounting messages that are stored in files due to communication failures are automatically ftped to the RKS when communications to the destination are restored. In the event there is a need to retrieve the files before communications are restored, the following procedures can be used.

29.8.4.1 Manually sending files from the IAA

1. Login into the IAA.
2. Go to the file staging directory (`cd /iaadata/ftpout/<channelID>`), where `channelID` is the channel ID of the destination, 1 to 255.
3. Transfer the file to the remote system. (`ftp remote host`).
4. Place the files on the remote host using the `ftp put` command.

29.8.4.2 Manually retrieving a files from the IAA

1. From the remote host ftp into the IAA.

2. Go to the file staging directory (cd /iaadata/ftpout/<channelID>), where channelID is the channel ID of the destination, 1 to 255.
3. Using the ftp get command retrieve the requested file.
4. After the file is retrieved, copy the file to the secondary directory so that it is not sent downstream one the communication link is re-established. (cp <filename> ../secondary/<ChannelID>).

29.8.5 Steps to Configure IPSec between the IAA and a remote RKS or DF

The following steps define the procedures to configure the IAA to communicate with a RKS, DF or GWC over a IPSec connection. The remote system must be configured in a similar fashion to allow for successful communications. The configuration files which need to be modified are found in the following directories:

Directory	File
/etc/inet	ipsecinit.conf (If this file does not exist copy /etc/inet/ipsecinit.sample to /etc/inet/ipsecinit.conf)
/etc/inet/ike	config (If this file does not exist copy /etc/inet/ike/config.sample to /etc/inet/ike/config)
/etc/inet/secret	ike.preshared
/etc/inet/secret	ipseckeys (If this file does not exist copy /etc/inet/secret/ipseckeys.sample to /etc/inet/secret/ipseckeys)

1. Edit the /etc/inet/ipsecinit.conf file to add an entry similar to the following: (note this is all on one line)

Sending host:

```
{ raddr 172.19.160.58 rport 1704 laddr 172.19.160.170 ulp udp dir both }
ipsec { encr_algs 3des encr_auth_algs sha1 auth_algs sha1 sa shared }
```

Receiving host:

```
{ raddr 172.19.160.170 laddr 172.19.160.58 lport 1704 ulp udp dir both } ipsec
{ encr_algs 3des encr_auth_algs sha1 auth_algs sha1 sa shared }
```

Where:

raddr is the ip address of the remote system

rport is the port number of the remote system

laddr is the ip address of the local system (if a cluster it is the cluster IP)

lport is the port number of the local system

2. Edit the /etc/inet/ike/config file so that the following values are set as described below. This only needs to be done for the first IPSec connection.

```
## Global parameters
#
## Phase 1 transform defaults
p1_lifetime_secs 604800
p1_nonce_len 40
#
## Defaults that individual rules can override.
p1_xform
{ auth_method preshared oakley_group 1 auth_alg sha encr_alg 3des }
p2_pfs 0
```

3. Also edit the `/etc/inet/ike/config` file to add an entry for each remote host as required, similar to the one below:

On the Sending Host:

```
{ label "cluster1-sundev3"
  local_addr 172.19.160.170
  remote_addr 172.19.160.58
  p1_xform
  { auth_method preshared oakley_group 1 auth_alg sha1 encr_alg 3des p1_lifetime_secs
604800 }
  p2_pfs 2
}
```

On the Receiving Host:

```
{ label "cluster1-sundev3"
  local_addr 172.19.160.58
  remote_addr 172.19.160.170
  p1_xform
  { auth_method preshared oakley_group 1 auth_alg sha1 encr_alg 3des p1_lifetime_secs
604800 }
  p2_pfs 2
}
```

Where:

label is any unique name

remote_addr is the ip address of the remote system.

local_addr is the ip address of the local host.

4. Edit the `/etc/inet/secret/ike.preshared` file to add an entry for each remote host as required, similar to the one below:

On the Sending Host:

```
{ localidtype IP
  localid 172.19.160.170
  remoteidtype IP
  remoteid 172.19.160.58
  key f1d8ab6cf3bf5f1232e1cea8cf4657e09a63b5b6b575dc3a
}
```

On the Receiving Host:

```
{ localidtype IP
  localid 172.19.160.58
  remoteidtype IP
  remoteid 172.19.160.170
  key f1d8ab6cf3bf5f1232e1cea8cf4657e09a63b5b6b575dc3a
}
```

Where:

label is any unique name

remoteid is the ip address of the remote system.

localid is the ip address of the local host.

key is a hex string.

5. After the changes to the files are made execute the following to start IpSec with the desired configuration:

```
pkill in.iked
  /usr/lib/inet/in.iked
ipseckey -f /etc/inet/secret/ipseckey
ipseccnf -a /etc/inet/ipsecinit.conf
```

6. To verify the data is encrypted:
on the receiving host:

```
snoop -v host 172.19.160.170

.
.
.
AH:  ----- Authentication Header -----
AH:
```

```

AH:  Next header = 50 (ESP)
AH:  AH length = 4 (24 bytes)
AH:  <Reserved field = 0x0>
AH:  SPI = 0xad42fdc1
AH:  Replay = 54745
AH:  ICV = 98d75a36720c3398cf18e35b
AH:
ESP:  ----- Encapsulating Security Payload -----
ESP:
ESP:  SPI = 0x70498dd0
ESP:  Replay = 54745
ESP:      ....ENCRYPTED DATA....

```

OR

```
snoop -x 0 host 172.19.160.170
```

```

Using device /dev/eri (promiscuous mode)
cluster1 -> sundev3   ESP SPI=0x70498dd0 Replay=56870

```

```

0: 0003 ba5c 454b 0000 bb71 f34e 0800 4500    ... \EK...q.N..E.
16: 0128 adcc 4000 ff33 33ca ac13 a0aa ac13    . (...@...33.....
32: a03a 3204 0000 ad42 fdc1 0000 de26 e34f    .:2....B.....&.O
48: 1672 0a50 c928 93f8 8246 7049 8dd0 0000    .r.P.(.ø.FpI....
64: de26 40ab 17fa 4bcb 9704 55a2 2c85 1bfa    .&@...úK...U.,...ú
80: 84f6 813e b7d2 75ec 5f0a 7894 0d40 0aae    ...>...u...x...@..
96: 7be6 8e93 629b 6f3b cfca 97cd b278 53bb    {...b.o;.....xS.
112: daed 33f8 bae1 3768 a171 7ef4 fcb9 6255    ..3ø..7h.q~...bU
128: 3904 bb38 73e5 d5b4 e5e0 5d11 bfee 1bbb    9..8s.....].....
144: d339 4d44 8a5f ee79 2093 9bdf 690b bcb3    .9MD...y ...i...
160: 19b2 321c 77dd 3d13 1dd3 64af 5bdc cbc5    ..2.w.=...d.[...
176: 4012 05ab a6e7 abe5 e508 9629 fedc 0876    @.....)p...v
192: 823e 1817 59eb 6109 8c41 4fa9 56b8 7a25    .>...Y.a..AO.V.z%
208: 9646 2e45 5a98 8521 3fe0 b914 a356 f074    .F.EZ...!?...V.t
224: 1450 35dc 5742 ada2 5e87 ee43 0180 1f99    .P5.WB...^..C....
240: 85ba abe0 7153 bee8 98ae d90c 3055 e413    ....qS.....0U..

```

```

256: a0df 5b03 be9e 0e8a 05b9 6da0 8ad6 4f6d    ..[.....m...Om
272: f670 eaf6 64b7 704a 567d 8e1a 89f3 87a3    .p..d.pJV}.....
288: f964 b542 7676 d089 89a0 a0b2 6d6f 7cac    ùd.Bvv.....mo|.
304: 0c4f c8e8 e675                                .O...u

```

29.8.6 Backing Up and Restoring Configuration Data

29.8.6.1 Backup Configuration Data

Configuration data can be backed up to any removable device by using the following commands:

1. Busy the IAA application modules, (IAA Accounting Event Message Processing, IAA Accounting Event Message Viewing, and IAA LI Event Message Processing).
2. Go to the configuration directory, (cd /iaadata/config).
3. Write the data to a removable media device, (tar cvf /dev/[device name] *).
4. Restart the IAA application modules.

29.8.6.2 Restoring Configuration Data

Configuration data can be restored from any removable device by using the following commands:

1. Busy the IAA application modules, (IAA Accounting Event Message Processing, IAA Accounting Event Message Viewing, and IAA LI Event Message Processing).
2. Go to the configuration directory, (cd /iaadata/config).
3. Extract the data from the removable media device, (tar xvf /dev/[device name] *).
4. Restart the IAA application modules.

29.8.7 Changing File Aging Parameters for the IAA

Processed and temporary files used by the IAA are removed from the system by programs run from the user maint's crontab file. This time a file resides on the system can be changed using the following procedures.

29.8.7.1 Record Viewing

Events which have not been delivered to the destination because of communication problems are made available for viewing for 1 day. On slower volume installations this can be set for a longer value by changing the following entry in the crontab file for the user maint.

```

30 0 * * * /usr/bin/ksh -c ". ./profile.iaa ; [ -x
/opt/nortel/cbm/21/iaa/bin/remove_aged ] && /opt/
nortel/cbm/21/iaa/bin/remove_aged -d -a 1 -i /

```

```
cbmdata/00/iaa/data/etc/remove_dirs.include -x /  
cbmdata/00/iaa/data/etc/remove_dirs.exclude"
```

1. As the user root edit the crontab file for the maint user, (crontab -e maint).
2. Change the “-a1” to “-a X”.
3. Save the crontab file.

29.8.7.2 Temporary Files

Files that are used to process events are stored on the system for a period of 5 days. This can be set to a different value by changing the following entry in the crontab file for the user maint.

```
0 1 * * * /usr/bin/ksh -c ". ./profile.iaa ; [ -x /  
opt/nortel/cbm/21/iaa/bin/remove_aged ] && /opt/  
nortel/cbm/21/iaa/bin/remove_aged -a 5 -i /cbmdata/  
00/iaa/data/etc/remove_aged.include -x /cbmdata/00/  
iaa/data/etc/remove_aged.exclude"
```

1. As the user root edit the crontab file for the maint user, (crontab -e maint).
2. Change the “-a5” to “-a X”.
3. Save the crontab file.

29.8.7.3 Temporary Files

Audit files are stored on the system for a period of 30 days. This can be set to a different value by changing the following entry in the crontab file for the user maint.

```
0 2 * * * /usr/bin/ksh -c ". ./profile.iaa ; [ -x /  
opt/nortel/cbm/21/iaa/bin/remove_aged ] && /opt/  
nortel/cbm/21/iaa/bin/remove_aged -a 30 -i /cbmdata/  
00/iaa/data/etc/remove_audits.include -x /cbmdata/  
00/iaa/data/etc/remove_audits.exclude"
```

1. As the user root edit the crontab file for the maint user, (crontab -e maint).
2. Change the “-a30” to “-a X”.
3. Save the crontab file.

30: A00007489 Configuration (CN)

30.1 Feature name

Integration of SuperNode Data Manager (SDM) User Authentication with the Integrated Element Manager System (IEMS)

30.2 Hardware and Software Requirements

SN08 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 the SDM before feature configuration can take place.

For SDM deployment with the IEMS centralized security server, IEMS and its hardware and software dependencies need to be available and configured.

30.3 Initial Configuration

- No hardware initial configuration for this feature.
- The initial software configuration for this feature uses the local security server (i.e. native AIX security system) for authentication and authorization. No user input is needed for initialization.

30.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable to this feature.

30.5 Upgrade Considerations

30.5.1 Dump and Restore (CM)

Not applicable to this feature.

30.5.2 Element Management Upgrade

No impact on the Element Management Upgrade when a SDM is deployed without an external security server.

When a SDM is deployed with the IEMS centralized security server in SN08, the SDM is changed from using the Pre-SN08 local security system to the external security server. 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.

The following are the steps for migrating SDM local user accounts to IEMS:

- Login to a SDM and determine which SDM user accounts need to be exported to IEMS. e.g. Local SDM root account should not be exported to IEMS.
- Obtain the list of the user accounts which need to be migrated to the central server for every SDM.
- For each account which needs to be migrated to the central server:
 1. Create the account on IEMS security server manually
 2. On each SDM as a user allowed to perform “security” action:
 - a. Remove the user account using sdmmtc
 - b. Run the command enableIEMSUser¹ for this user account

30.5.3 Downgrade impact

No impact on downgrade if the SDM feature installation is aborted.

30.6 Data schema (DS) (CM, MIBS, RDB)

Not applicable to this feature.

30.7 Service Orders (SO) (CM & SESM)

Not applicable to this feature.

30.8 Software optionality control (SOC)

Not applicable to this feature.

30.9 Element Management

Not applicable to this feature.

30.10 User interface changes

30.10.1 Directory: sdmmtc;SDMConfig or sdmmtc;Admin;SecuConf

SDM Config level menu will not be changed by this feature. It will be used to commission the feature software.

A new SecuConf level is created under Admin level for the SDM security services configuration.

30.10.2 Command: Step in SDMConfig or Change in SecuConf

Step command from the SDM Config level menu will not be changed by this feature. It will be used to commission the feature.

Change command is provided under SecuConf level for changing the SDM security configuration.

¹See “New command: enableIEMSUser” on page 1755.

30.10.2.1 Security Services Configuration

A new configuration screen will be presented for selecting security servers for this feature.

Table 1 Security Services Configuration prompts and options

Configuration prompts	Options
Change Authentication Naming Service	LOCAL
Please choose one of the following available option(s) on the system. More option(s) will be available if the corresponding fileset(s) is (are) applied. (1) LOCAL:	Note: Options that may available in the future - SAML, LDAP.
Change Authentication PAM Stack	LOCAL, IEMS
Please choose one of the following available option(s) on the system. More option(s) will be available if the corresponding fileset(s) is (are) applied. (1) IEMS (2) LOCAL:	Note: Options that may available in the future - LDAP.
Enter the IP Address of the External Radius Server: ^a	User Response Enter the IP address of the external Radius server.
Do you want to enter the port number instead of using default?	User Response
Please confirm (“YES”, “Y”, “NO”, or “N”): ^b	
Enter the Port Number of the External Radius Server: ^c	User Response Enter the shared port number of the external Radius server.
Enter the Radius Shared Secret: ^d	User Response Enter the Radius shared secret of the external Radius server.
The Radius Server to be configured:	User Response
IP address: 1.2.3.4	
Port number: 1234	
Do you wish to proceed?	
Please confirm (“YES”, “Y”, “NO”, or “N”): ^e	

a. Available only when IEMS is selected for Auth PAM Stack.

b. Available only when IEMS is selected for Auth PAM Stack.

c. Available only when IEMS is selected for Auth PAM Stack.

d. Available only when IEMS is selected for Auth PAM Stack.

e. Available only when IEMS is selected for Auth PAM Stack.

30.10.2.2 Example

The following are the example screens for configuring the local authentication naming service with the local authentication PAM module. Please note this is the default security servers setting. Therefore, the customers do not need to invoke SDM Config level for the default setup.

```

SDM      CON NET  APPL  SYS  HW  CLI: NONE
ISTb     .  SysB .  ISTb  .  Host: wcary2p7
M        M        Fault Tolerant

SDMConfig
0 Quit
2 Add     # Commissioning Step      Status / Value
3 Change  7 Network Security        Commissioned
4 Delete  8 Ethernet Connectivity    Commissioned
5         9 DS512 Connectivity       Uncommissioned
6 Next    10 X25 Connectivity         Uncommissioned
7 Prev    11 Gateway IP Address      47.135.213.1
8         12 Core Communication Path Commissioned
9 List    13 Network Nodes            Commissioned
10 Step   14 Edge Node Monitoring     Uncommissioned
11        15 Network Time Protocol    Commissioned
12 Up     16 DCE                      Uncommissioned
13 Down   17 PassThru Users           Commissioned
14        18 Security Services      Commissioned
15        Commissioning Steps: 7 to 18 of 18
16
17 Help
18 Refresh
root
Time 15:13 > Step 18

SDM      CON NET  APPL  SYS  HW  CLI: NONE
ISTb     .  SysB .  ISTb  .  Host: wcary2p7
M        M        Fault Tolerant

SDMConfig
0 Quit
2 Add     1 Authentication Naming Service: LOCAL
3 Change
4 Delete  2 Authentication PAM Stack: LOCAL
5
6 Next    3 Remote Security Log Destination: -
7 Prev
8         4 Remote Audit Log Destination: -
9 List
10 Step
11
12 Up
13 Down   Security Services
14        Use the Change command to change the existing security service
15        configuration.
16
17 Help   Type Next to continue with the next commissioning step, Prev to go
18 Refresh back, or List to display a list of available commissioning steps.
root
Time 15:16 > Change 1

SDM      CON NET  APPL  SYS  HW  CLI: NONE
ISTb     .  SysB .  ISTb  .  Host: wcary2p7
M        M        Fault Tolerant

```



```

SDMConfig
0 Quit
2 Add    1 Authentication Naming Service: LOCAL
3 Change
4 Delete  2 Authentication PAM Stack: LOCAL
5
6 Next    3 Remote Security Log Destination: -
7 Prev
8         4 Remote Audit Log Destination: -
9 List
10 Step
11
12 Up
13 Down
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) LOCAL :
root
Time 15:18 >1

```

```

      SDM    CON  NET  APPL  SYS  HW  CLI: NONE
      ISTb   .   SysB .   ISTb .   Host: wcary2p7
      M       M               Fault Tolerant
SDMConfig
0 Quit
2 Add    1 Authentication Naming Service: LOCAL
3 Change
4 Delete  2 Authentication PAM Stack: LOCAL
5
6 Next    3 Remote Security Log Destination: -
7 Prev
8         4 Remote Audit Log Destination: -
9 List
10 Step
11
12 Up
13 Down
14
15        Change Authentication Naming Service
16        You have chosen the same option as the existing configuration. Do
17 Help    you really want to continue?
18 Refresh Please confirm ("YES", "Y", "NO", or "N"):
root
Time 15:19 >y

```

```

      SDM    CON  NET  APPL  SYS  HW  CLI: NONE
      ISTb   .   SysB .   ISTb .   Host: wcary2p7
      M       M               Fault Tolerant
SDMConfig
0 Quit
2 Add    1 Authentication Naming Service: LOCAL
3 Change
4 Delete  2 Authentication PAM Stack: LOCAL
5
6 Next    3 Remote Security Log Destination: -
7 Prev
8         4 Remote Audit Log Destination: -
9 List
10 Step
11
12 Up
13 Down
14

```

```

15
16
17 Help
18 Refresh Change 1 - Command complete.
root
Time 15:22 >

```

The following are the example screens from the Admin SecuConf level for configuring the authentication PAM stack with the IEMS Radius authentication PAM module. The IEMS Radius PAM module option will only be shown if the IEMS Radius client software for this feature is installed on the SDM. Radius server address, port number and secret need to be entered by the users for this configuration.

```

SDM   CON NET  APPL SYS  HW  CLI: 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  CLI: 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 2

```

SDM   CON  NET  APPL  SYS  HW  CLI: 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 PAM Stack
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) IEMS (2) LOCAL :
jjsecu1
Time 15:38 >1

```

```

SDM   CON  NET  APPL  SYS  HW  CLI: 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 PAM Stack - IEMS
17 Help
18 Refresh Enter the IP Address of the External Radius Server:
jjsecu1
Time 15:40 >47.1.2.3

```

```

SDM   CON  NET  APPL  SYS  HW  CLI: 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 PAM Stack - IEMS
17 Help   Do you want to enter the port number instead of using default?
18 Refresh Please confirm ("YES", "Y", "NO", or "N"):
jjsecu1
Time 15:41 >y

```

```

SDM   CON  NET  APPL  SYS  HW  CLI: 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 PAM Stack - IEMS
17 Help
18 Refresh Enter the Port Number of the External Radius Server:
jjsecu1
Time 15:43 >1234

```

```

SDM   CON  NET  APPL  SYS  HW  CLI: 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 PAM Stack - IEMS
17 Help
18 Refresh Enter the Radius Shared Secret:
jjsecu1
Time 15:45 >****1

```

¹Stars will be shown in SN08 but will not be shown in future releases.

```

SDM      CON NET  APPL SYS  HW  CLI: NONE
ISTb     .  SysB .  ISTb .  Host: wcary2p7
M        M                      Fault Tolerant
SecuConf
0 Quit
2
3
4
5
6
7
8
9
10
11      Change Authentication PAM Stack - IEMS
12
13      The Radius Server to be configured:
14      IP address: 47.1.2.3
15      Port number: 1234
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  CLI: 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: IEMS
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 >

```

30.10.3 New command: enableIEMSUser

A new command, enableIEMSUser, is added so that the administrator can allow an IEMS user to logon to an SDM.

The synopsis of the command is:

```
enableIEMSUser <username> <uid> <gid> <shell>
```

Where:

<username> is the IEMS user name (login)

<uid> is the UID of the IEMS user

<gid> is the integer ID or character-string name of the primary group of the IEMS User

<shell> is the login shell for this IEMS user. It could be either rash or fash

30.10.3.1 Example

The following is the example command line to allow IEMS user “john” to logon to SDM:

```
enableIEMSUser john 10001 usr fash
```

30.10.4 New command: disableIEMSUser

A new command, disableIEMSUser, is added so the administrator can disallow an IEMS user to logon to an SDM.

The synopsis of the command is:

```
disableIEMSUser <username>
```

Where:

<username> is the IEMS user name (login)

30.10.4.1 Example

The following is the example command line to disallow IEMS user “john” to logon to SDM:

```
disableIEMSUser john
```

30.11 OSSGate Interface Changes

Not applicable to this feature.

30.12 Security

The feature will change user authentication and authorization for SDM.

30.12.1 Network configuration

n/a

30.12.2 Key management

n/a

30.12.3 Protocol

n/a

30.12.4 Authentication

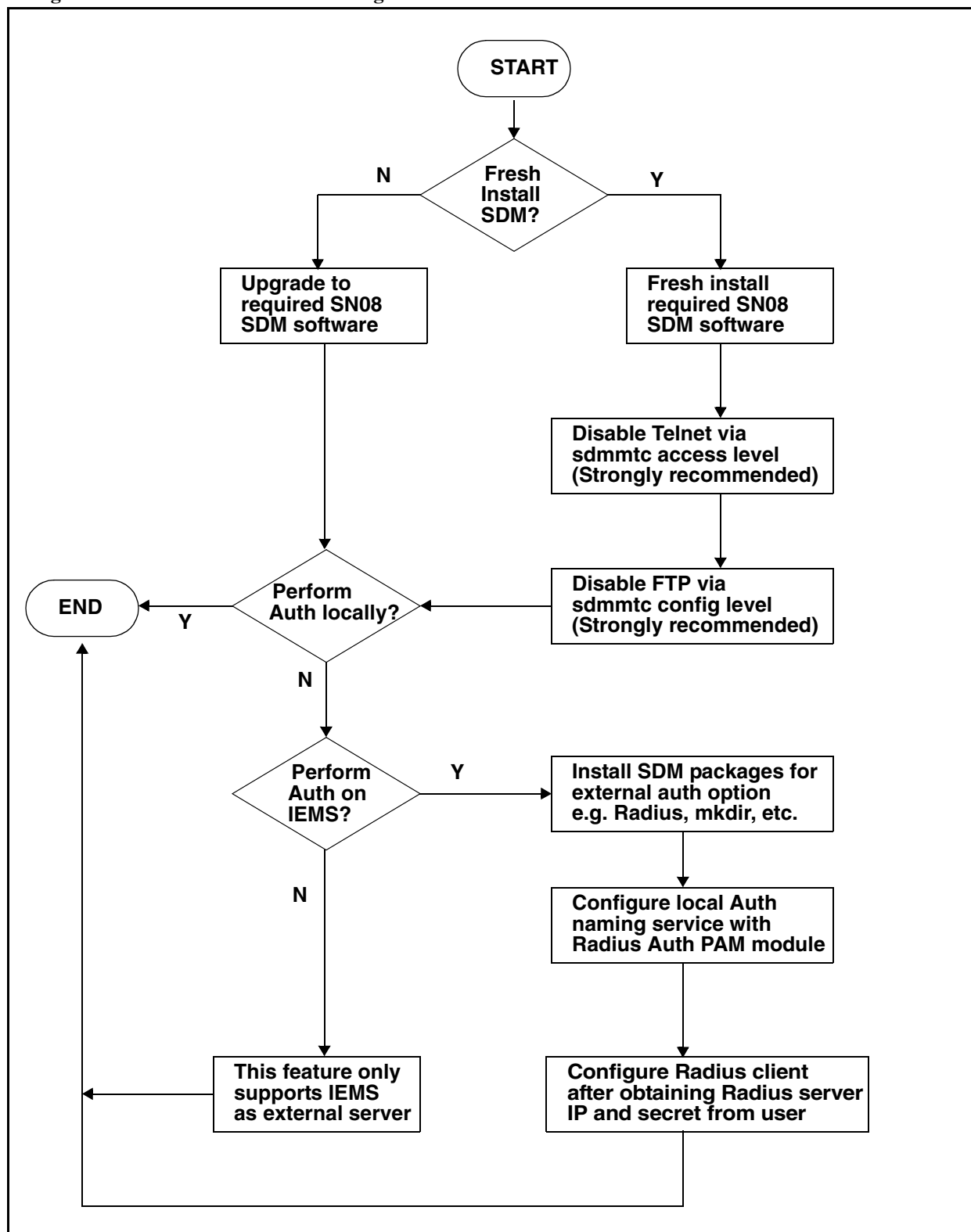
When a SDM is deployed without an external security server, user authentication and authorization will be performed locally on the SDM.

When a SDM is deployed with an external security server like IEMS, user authentication and authorization will be performed through IEMS via Radius protocol.

30.13 Configuration Walkthrough

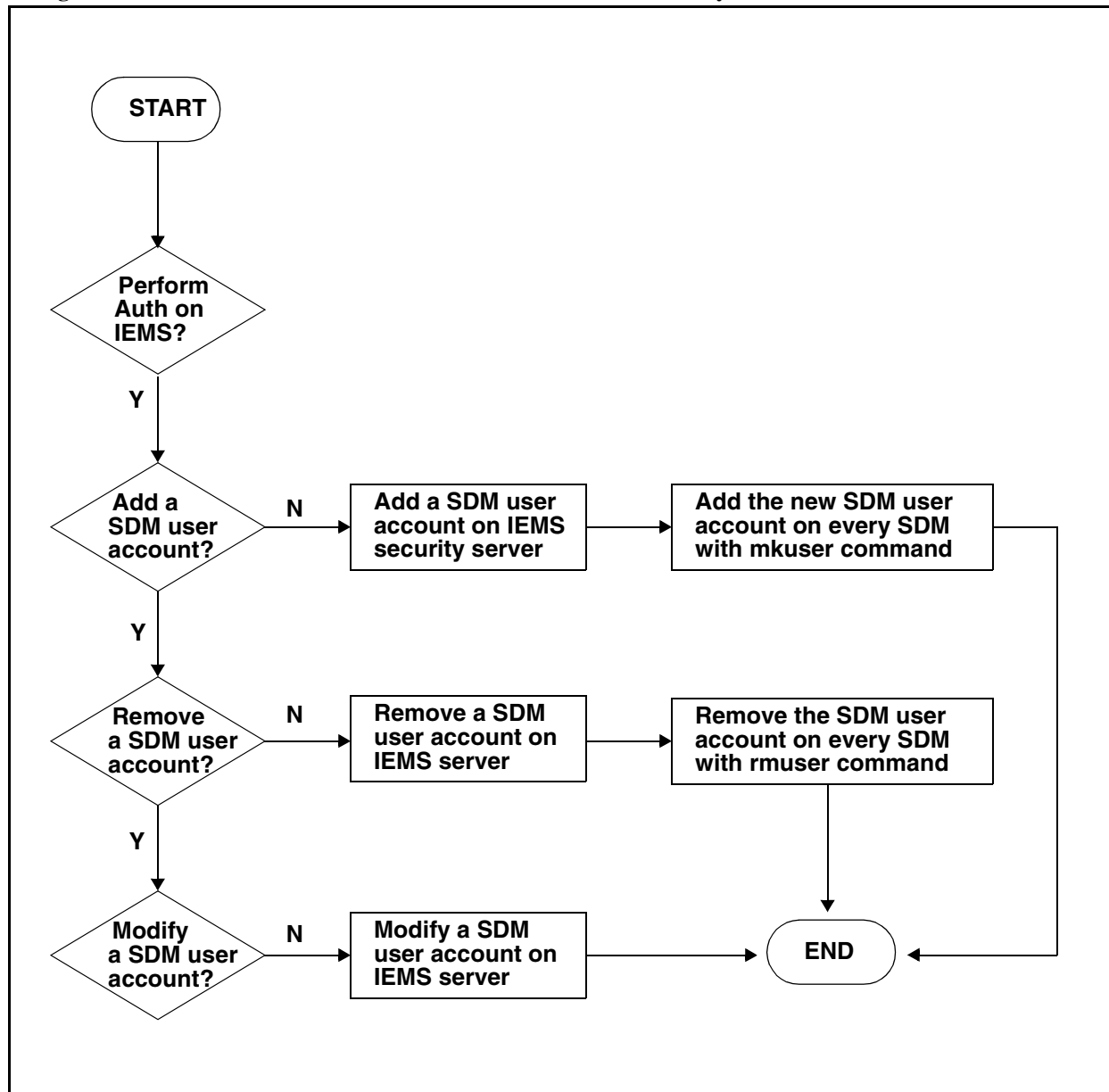
The following figure shows the configuration steps for this feature.

Figure 1 Flow chart for feature configuration

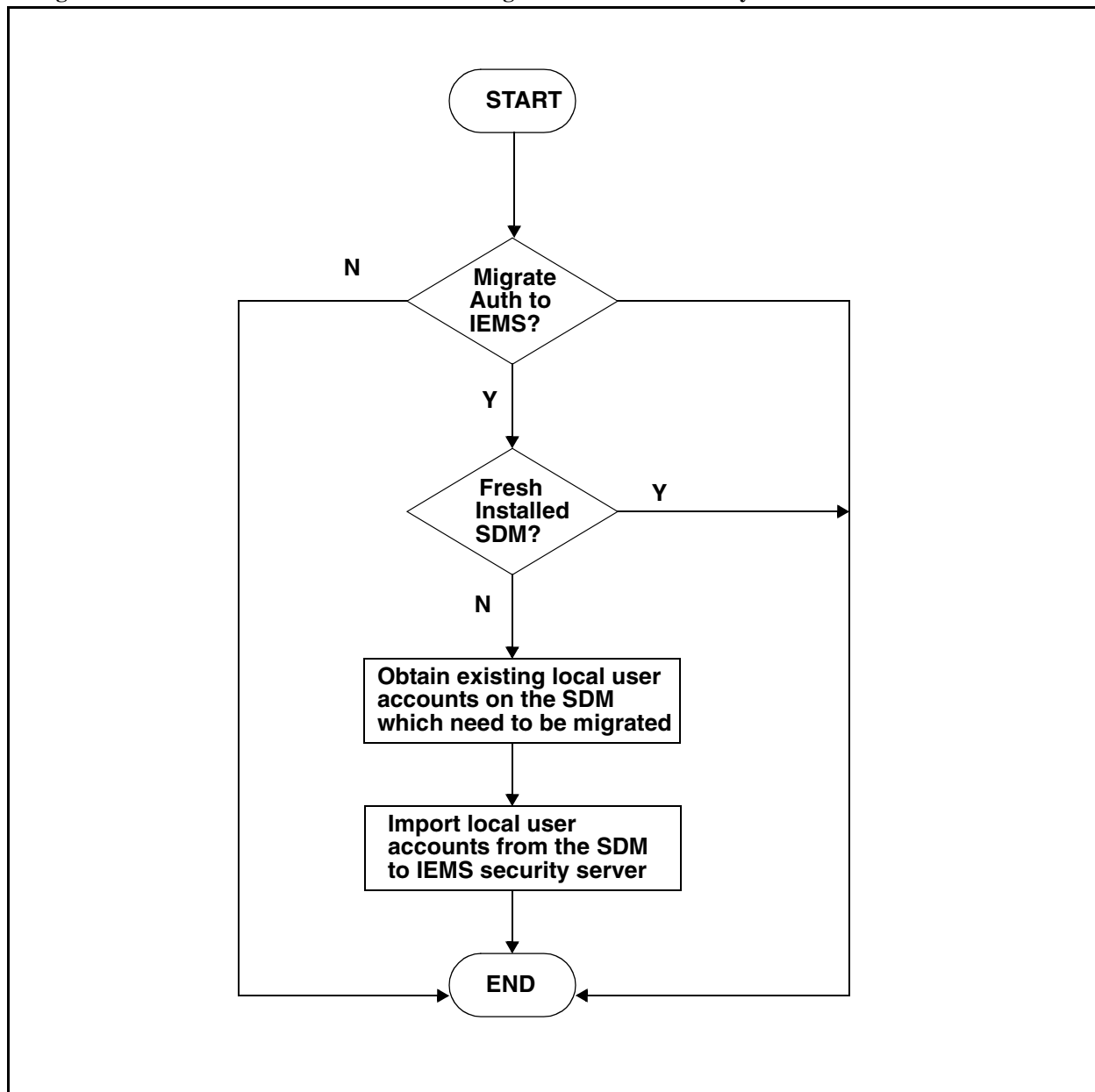


The following figure shows the user account administration steps for this feature when deployed with IEMS as the external security server.

Figure 2 Flow chart for user account admin with IEMS as security server



The following figure shows the steps for migrating SDM local user accounts on an existing system to the IEMS security server. These steps are needed to support central authentication and authorization.

Figure 3 Flow chart for local user account migration to IEMS security server

31: A00007492 Configuration (CN)

31.1 Feature name

Integration of SuperNode Data Manager (SDM) User Authentication with the Integrated Element Manager System (IEMS)

31.2 Hardware and Software Requirements

31.3 Initial Configuration

31.4 Office/Subnet parameters (OP/SP) (CM & SESM)

31.5 Upgrade Considerations

31.6 Data schema (DS) (CM, MIBS, RDB)

31.7 Service Orders (SO) (CM & SESM)

31.8 Software optionality control (SOC)

31.9 Element Management

31.10 User interface changes

31.10.1 Directory: <SDM user level>

31.10.1.1 Directory description

The user level of the SDM user interface has been changed. New commands have been added. “Dispusr” enables the operator to display all the users on the system or information about a specific user. “Dispgrp” allows the operator to display all the role groups, the user in a specific role group and the actions that a specific role group can do. The add and change commands of the user interface have also been changed. These commands now prompt the user for each piece of information needed to create a user. The information asked for include primary groups, groups, shell and password.

31.10.1.2 Accessing directory: <sdmmtc; user>

Access to directory or MAP level and return to CI

The user level of the SDMMTC is accessed the same as before.

```
>sdmmtc
```

```
>user
```

31.10.2 Command: <Dispgrp>

31.10.2.1 Command type: < Listed MENU>

31.10.2.2 Command target: <SDM>

31.10.2.3 Command availability: <ALL>

31.10.2.4 Command description

Enables the operator to display all the role groups on the system or the users in a specific user or the activities that a specific role group can perform.

31.10.2.5 Command syntax

Table 1 <CommandName> command parameters and variables

Command	Parameters and variables
dispusr	all
	group
	group act
Parameters and variables	Description
All	Displays all role groups defined on the system. The role group name is displayed along with what users belong to that group.
Group	Displays the users that belong to the specified group.
Group Act	Displays the actions the specified group is allowed to perform.

31.10.2.6 Qualifications and warnings

Only role groups can be displayed.

31.10.2.7 Responses

31.10.2.7.1 <errors>

Table 2 MAP outputs with associated meanings and actions

Command
dispgrp junk Cannot execute command. Only Role groups can be displayed. Meaning: This happens when the group specified is not a role group. System or user actions: User should type a group that is a role group. This command with no parameters or with “all” will display all the role groups.
dispusr maint junk Command failed. The third parameter can only be ACT. Meaning: The third parameter must be the reserved word “ACT”. System or user actions: User should type “act” as the third parameter.
dispusr junk junk junk DispUsr junk junk - EITHER incorrect optional parameter(s) OR too many parameters. Meaning: This happens when too many parameters are given. System or user actions: User should type a group that is a role group. This command with no parameters or with “all” will display all the role groups.

31.10.2.8 Examples

Figure 1 Example Screen: SDM user dispgrp all

```

SDM      CON  512  NET  APPL  SYS  HW  CLI: SNM0
ISTb     .    ..    .    ISTb  ISTb  ISTb  Host: hostname
                               Fault Tolerant
User
0 Quit
2
3 PassThru 1 emsadm  dvsE,bn_ems,dvsE2,dvsE3,bnemsadm,jean
4          2 maint   dvsS3,maint,ftp,anonymou,limaint,dvsM,dvs...
5          3 secuadm  dvsS2,dvsS3,dvsS,bn_sec,jean
6
6          Role Groups: 1 to 3 of 3
7
8
9
10 Dispgrp
11 DispUsr
12 Up
13 Down
14
15
16
17 Help
18 Refresh .
root
Time 16:28 >

```

Figure 2 Example Screen: SDM user display

```

SDM      CON  512  NET  APPL  SYS  HW  CLI: SNM0
ISTb     .    ..    .    ISTb  ISTb  ISTb Host: hostname
                               Fault Tolerant
User
0 Quit
2      maint Users
3 PassThru  1 bob
4           2 fred
5           3 maint
6           4 dvsM
7           5 dvsM2
8
9
10 Dispgrp
11 Dispusr
12 Up
13 Down
14
15
16
17 Help
18 Refresh .
  root
Time 16:28 >

```

Lines: 1 to 5 of 5

Figure 3 Example Screen: SDM user display

SDM	CON	512	NET	APPL	SYS	HW	CLLI: SNM0
ISTb	.	..	.	ISTb	ISTb	ISTb	Host: hostname
	..						Fault Tolerant
User							
0 Quit							
2							
3 PassThru							
4							
5							
6							
7							
8							
9							
10 Dispgrp							
11 Dispusr							
12 Up							
13 Down							
14							
15							
16							
17 Help							
18 Refresh							
root							
Time 16:28							
>							

Table 3 Usage examples for DispUsr command

Description of task:	
Description of task	Display all role group
Command:	dispgrp all
MAP response:	display of all role groups (see figure 3)
Description of task	Display a specific role group
Command:	dispgrp maint
MAP response:	display all the users in the specified group (see figure 4)
Description of task	Display a specific role group's actions
Command:	dispusr secuadm act
MAP response:	display of the actions the specified group can perform (see figure 5)

31.10.3 Command: <Dispusr>

31.10.3.1 Command type: <NON-MENU, Listed MENU, Unlisted MENU>

31.10.3.2 Command target: <SDM>

31.10.3.3 Command availability: <ALL>

31.10.3.4 Command description

Enables the operator to display all the users on the system or information about a specific user.

31.10.3.5 Command syntax

Table 4 <CommandName> command parameters and variables

Command	Parameters and variables
dispusr	All User
Parameters and variables	Description
All	Displays all users defined on the system that belong to one of the role groups. The user name is displayed along with what groups it is a part of.
User	Displays the primary groups, groups, home directory and shell for the user specified.

31.10.3.6 Qualifications and warnings

Only users that are a members or a role group may be displayed.

31.10.3.7 Responses

31.10.3.7.1 <errors>

Table 5 MAP outputs with associated meanings and actions

Command
dispusr junk
Command failed. User junk does not exist.
Meaning: This happens when a user name does not exist
System or user actions: User should type a user that is in a role group. This command with no parameters or with “all” will display all users in role groups.

Table 5 MAP outputs with associated meanings and actions

Command
dispusr root
Command failed. User root is not a role group user.
Meaning: This happens when the user is not in a role group.
System or user actions: User should type a user that is in a role group. This command with no parameters or with “all” will display all users in role groups.
dispusr junk junk
DispUsr junk junk - EITHER incorrect optional parameter(s) OR too many parameters.
Meaning: This happens when too many parameters are given.
System or user actions: User should type a user that is in a role group. This command with no parameters or with “all” will display all users in role groups.

31.10.3.8 Examples

Figure 4 Example Screen: SDM user display

SDM	CON	512	NET	APPL	SYS	HW	CLLI: SNM0
ISTb	.	..	.	ISTb	ISTb	ISTb	Host: hostname
	..						Fault Tolerant
User							
0 Quit							
2							
3 PassThru							
4							
5							
6							
7							
8							
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							>

Figure 5 Example Screen: SDM user display

SDM	CON	512	NET	APPL	SYS	HW	CLLI: SNM0
ISTb	.	..	.	ISTb	ISTb	ISTb	Host: hostname
	..						Fault Tolerant
User							
0 Quit							
2		<u>maint</u>					
3 PassThru	pgrp		maint				
4	groups						
5			maint				
6	home		/home/maint				
7	shell		/bin/rash				
8							Lines: 1 to 5 of 5
9							
10 Dispgrp							
11 Dispusr							
12 Up							
13 Down							
14							
15							
16							
17 Help							
18 Refresh	.						
root							
Time 16:28							>

Table 6 Usage examples for DispUsr command

Description of task:	
Description of task	Display all role group users
Command:	dispusr all
MAP response:	display of all users (see figure 6)
Description of task	Display a specific role group user
Command:	dispusr maint
MAP response:	display of the user's information (see figure 7)

31.10.4 Command: <Add>**31.10.5 Command type: < Unlisted MENU>****31.10.6 Command target: <SDM>****31.10.7 Command availability: <Secuadm users>****31.10.8 Command description**

Enables the operator to create a new user.

31.10.8.1 Command syntax**Table 7 <CommandName> command parameters and variables**

Command	Parameters and variables
add	User
Parameters and variables	Description
User	Add a user with the name that was specified.
Pgrp	Set the primary group to the value specified. Allowed values are maint, emsadm or secuadm.
Groups	Add the group list for this user. Allowed values are maint, emsadm and secuadm. One or more groups may be added. List them separated by blanks or commas
Shell	Set the shell of the user. Allowed values are rash for a restricted shell, fash for a full shell and nash for no shell.
password	Set the password for the user.

31.10.8.2 Qualifications and warnings

None.

31.10.8.3 Responses

31.10.8.3.1 <errors>

Table 8 MAP outputs with associated meanings and actions

Command
add maint Command failed. User 'maint' already exists. Meaning: This happens when a user name is already in use System or user actions: User should type a different name
add toobigname Cannot execute command. USERID cannot exceed 8 characters. Meaning: This happens when the user name is greater than 8 characters. System or user actions: User should type a user name less than or equal to 8 characters long.
add or add junk junk EITHER incorrect optional parameter(s) OR too many parameters. Meaning: This happens when too many or not enough parameters are given. System or user actions: User should type a user name.
add User - Primary Group Enter the new Primary Group for user bn_ems: [maint] >junk Group 'junk' is not a Role Group. Meaning: This happens when a non role group is entered System or user actions: User should type a valid role group (maint, emsadm or secuadm) or type enter to accept the default.

Table 8 MAP outputs with associated meanings and actions

Command
add User - Groups Enter the new Group List for user bn_ems: [maint] >junk Group 'junk' is not a Role Group. Type list of role groups separated by commas. Meaning: This happens when a non role group is entered System or user actions: User should type a valid role group (maint, emsadm or secuadm) or type enter to accept the default. add User - Shell Enter the new Shell for user bn_ems: [rash] >junk 'junk' is not a valid shell. Allowed values are 'rash', 'fash' or 'nash'. Meaning: This happens when a non-valid shell is typed. System or user actions: User should type a valid shell (rash, fash or nash) or type enter to accept the default. add User - Change Password? Do you wish to change the password for user bn_ems? Please confirm ("YES", "Y", "NO", or "N"): >jmaybe Invalid input: Please try again. Meaning: Allowed answers are yes or no. System or user actions: User must reply yes or no.

31.10.8.4 Examples

Figure 6 Example Screen: SDM user display

```

SDM      CON  512  NET  APPL  SYS  HW  CLI: SNM0
ISTb     .    ..   .    ISTb  ISTb  ISTb  Host: hostname
                        Fault Tolerant
User
0 Quit
2          Role Group  Users
3 PassThru  1 emsadm  bn_ems
4           2 maint   maint,ftp,anonymou,limaint
5           3 secuadm No users defined in this group
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 - Primary Group
18 Refresh Enter the new Primary Group for user bn_sec: [maint]
root
Time 16:28 >

```

Figure 7 Example Screen: SDM user display

```

SDM      CON  512  NET  APPL  SYS  HW  CLI: SNM0
ISTb     .    ..    .    ISTb  ISTb  ISTb  Host: hostname
                               Fault Tolerant
User
0 Quit
2          Role Group  Users
3 PassThru  1 emsadm   bn_ems
4           2 maint    maint,ftp,anonymou,limaint
5           3 secuadm  No users defined in this group
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 - Groups
18 Refresh Enter the new Group List for user bn_sec: [maint]
root
Time 16:28 >

```


Figure 8 Example Screen: SDM user display

```

SDM      CON  512  NET  APPL  SYS  HW  CLI: SNM0
ISTb     .    ..    .    ISTb  ISTb  ISTb  Host: hostname
                        Fault Tolerant
User
0 Quit
2          Role Group  Users
3 PassThru  1 emsadm  bn_ems
4           2 maint   maint,ftp,anonymou,limaint
5           3 secuadm No users defined in this group
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 - Shell
18 Refresh Enter the new Shell for user bn_sec: [rash]
    root
Time 16:28 >

```

Figure 9 Example Screen: SDM user display

SDM	CON	512	NET	APPL	SYS	HW	CLLI: SNM0
ISTb	.	..	.	ISTb	ISTb	ISTb	Host: hostname
	..						Fault Tolerant
User							
0 Quit							
2							
3 PassThru							
4							
5							
6							
7							
8							
9							
10 Dispgrp							
11 DispUsr							
12 Up							
13 Down							
14							
15							
16							
17 Help							
18 Refresh							
root							
Time 16:28							

31.10.9 Command: <Change>**31.10.9.1 Command type: < Unlisted MENU>****31.10.9.2 Command target: <SDM>****31.10.9.3 Command availability: <Secuadm users>****31.10.9.4 Command description**

Enables the operator to change an existing user.

31.10.9.5 Command syntax**Table 9 <CommandName> command parameters and variables**

Command	Parameters and variables
Change	User
Parameters and variables	Description

Table 9 <CommandName> command parameters and variables

Command	Parameters and variables
User	change a user with the name that was specified.
Pgrp	change the primary group to the value specified. Allowed values are maint, emsadm or secuadm.
Groups	change the group list for this user. Allowed values are maint, emsadm and secuadm. One or more groups may be added. List them separated by blanks or commas
Shell	change the shell of the user. Allowed values are rash for a restricted shell, fash for a full shell and nash for no shell.
password	Change the password for the user.

31.10.9.6 Qualifications and warnings

None.

31.10.9.7 Responses**31.10.9.7.1 <errors>****Table 10 MAP outputs with associated meanings and actions**

Command
change junk
Command failed. 3004-687 User “junk” does not exist.
Meaning: This happens when a user name does not exist.
System or user actions: User should type a user that already has been created.
change toobigname
Cannot execute command. USERID cannot exceed 8 characters.
Meaning: This happens when the user name is greater than 8 characters.
System or user actions: User should type a user name less than or equal to 8 characters long.
change junk junk
EITHER incorrect optional parameter(s) OR too many parameters.
Meaning: This happens when too many or not enough parameters are given.
System or user actions: User should type a user name.

Table 10 MAP outputs with associated meanings and actions

Command
change User - Primary Group Enter the new Primary Group for user bn_ems: [maint] >junk Group 'junk' is not a Role Group. Meaning: This happens when a non role group is entered System or user actions: User should type a valid role group (maint, emsadm or secuadm) or type enter to accept the default. change User - Groups Enter the new Group List for user bn_ems: [maint] >junk Group 'junk' is not a Role Group. Type list of role groups separated by commas. Meaning: This happens when a non role group is entered System or user actions: User should type a valid role group (maint, emsadm or secuadm) or type enter to accept the default. change User - Shell Enter the new Shell for user bn_ems: [rash] >junk 'junk' is not a valid shell. Allowed values are 'rash', 'fash' or 'nash'. Meaning: This happens when a non-valid shell is typed. System or user actions: User should type a valid shell (rash, fash or nash) or type enter to accept the default.

Table 10 MAP outputs with associated meanings and actions

Command
change User - Change Password?
Do you wish to change the password for user bn_ems?
Please confirm ("YES", "Y", "NO", or "N"):
>jmaybe
Invalid input: Please try again.
Meaning: Allowed answers are yes or no.
System or user actions: User must reply yes or no.

31.10.9.8 Examples

Figure 10 Example Screen: SDM user display

SDM	CON	512	NET	APPL	SYS	HW	CLLI: SNM0
ISTb	.	..	.	ISTb	ISTb	ISTb	Host: hostname
	..						Fault Tolerant
User							
0 Quit							
2							
3 PassThru							
4							
5							
6							
7							
8							
9							
10 Dispgrp							
11 DispUsr							
12 Up							
13 Down							
14							
15							
16							
17 Help							
18 Refresh							
root							
Time 16:28							
>							

Figure 11 Example Screen: SDM user display

```

SDM      CON  512  NET  APPL  SYS  HW  CLI: SNM0
ISTb     .    ..    .    ISTb  ISTb  ISTb  Host: hostname
                               Fault Tolerant
User
0 Quit
2          Role Group  Users
3 PassThru  1 emsadm  bn_ems
4           2 maint   maint,ftp,anonymou,limaint
5           3 secuadm No users defined in this group
6                                     Role Groups: 1 to 3 of 3
7
8
9
10 Dispgrp
11 DispUsr
12 Up
13 Down
14
15
16
17 Help    Change User - Groups
18 Refresh Enter the new Group List for user bn_sec: [maint]
root
Time 16:28 >

```

Figure 12 Example Screen: SDM user display

```

SDM      CON  512  NET  APPL  SYS  HW  CLI: SNM0
ISTb     .    ..    .    ISTb  ISTb  ISTb  Host: hostname
                        Fault Tolerant
User
0 Quit
2          Role Group  Users
3 PassThru  1 emsadm bn_ems
4           2 maint   maint,ftp,anonymou,limaint
5           3 secuadm No users defined in this group
6                                     Role Groups: 1 to 3 of 3
7
8
9
10 Dispgrp
11 DispUsr
12 Up
13 Down
14
15
16
17 Help    Change User - Shell
18 Refresh Enter the new Shell for user bn_sec: [rash]
root
Time 16:28 >

```

Figure 13 Example Screen: SDM user display

```

SDM      CON  512  NET  APPL  SYS  HW  CLI: SNM0
ISTb     .    ..    .    ISTb  ISTb  ISTb  Host: hostname
                        Fault Tolerant
User
0 Quit
2
3 PassThru   Role Group  Users
4             1 emsadm   bn_ems
5             2 maint    maint,ftp,anonymou,limaint
6             3 secuadm  No users defined in this group
7                                     Role Groups: 1 to 3 of 3
8
9
10 Dispgrp
11 DispUsr
12 Up
13 Down
14
15
16           Add User - Change Password?
17 Help      Do you wish to change the password for user bn_sec?
18 Refresh   Please confirm ("YES", "Y", "NO", or "N"):
root
Time 16:28 >

```

Change can also be typed with no parameters. In this case the command can be run by any user and the user is only allowed to change their own password.

31.11 OSSGate Interface Changes

31.12 Security

31.13 Configuration Walkthrough

32: A00007713 Configuration (CN)

32.1 Feature name

TOPS-IP Robustness

32.2 Hardware and Software Requirements

None

32.3 Initial Configuration

Not applicable.

32.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

32.5 Upgrade Considerations

None

32.6 Data schema (DS) (CM, MIBS, RDB)

Not applicable.

32.7 Service Orders (SO) (CM & SESM)

Not applicable.

32.8 Software optionality control (SOC)

Not applicable.

32.9 Element Management

Not applicable.

32.10 User interface changes

32.10.1 Directory: Mapci;mtc;appl;topsip;topspos

32.10.1.1 Directory description

The mapci;mtc;appl;topsip;topspos level is used to perform maintenance activities on IP operator positions. Information related to posted IP positions is also available at this level.

32.10.1.2 Accessing directory: Mapci;mtc;appl;topsip;topspos

32.10.1.2.1 Access to directory or MAP level and return to CI To access the topspos level:

> mapci;mtc;appl;topsip;topspos

32.10.2 Command: Post

32.10.2.1 Command type: Listed MENU

32.10.2.2 Command target: All

32.10.2.3 Command availability: RES

32.10.2.4 Command description

The post command has parameter 'AC' added. When used, this parameter creates a post set of all in service IP positions with voice auto-compression turned on. The listset command is then used to display the position list.

32.10.2.5 Command syntax

Table 1 Post command parameters and variables

Command	Parameters and variables
Post	Parms: <ippos_Selector> {P [<POSNO>... {0 TO 9999}}, S <STATE> {OFFL, MANB, URES CRES, IDL, CPB, CPD, SYSB, INI}, PM <PMTYPE> {DTC} <DTCNO> {0 TO 254}, C <COMID> {0 TO 1023}, R<STARTPOS>{0TO9999} <ENDPOS> {0 TO 9999}, AC, ALL}
AC Parameter	The AC parameter is used to post all in service IP positions with auto-compression turned on.

32.10.2.6 Qualifications and warnings

32.10.2.7 Responses

Table 2 MAP outputs with associated meanings and actions

Response To Post Command With AC Parameter - Positions Found
Size of Post Set: 2
Meaning: There were 2 IP positions found with auto-compression turned on.
System or user actions:
No user action required.

Table 3 MAP outputs with associated meanings and actions

Response To Post Command With AC Parameter - No Positions Found
No IP positions found with auto-compression turned on.
Meaning: The switch is not aware of any in service IP positions with auto-compression turned on.
System or user actions:
No user action required.

32.10.2.8 Example

Table 4 Usage examples for Post command

Description of task:	Post a set of all in service IP positions with auto-compression turned on.
Command:	mapci;mtc;appl;topsip;topspos;post ac
MAP response:	Size of Post Set: 1
Command:	MAP mapci;mtc;appl;topsip;topspos;listset
response:	POS 1800 DTC 15 COMID 15 Idl
Command:	MAP mapci;mtc;appl;topsip;topspos;post ac
response:	No IP positions found with auto-compression turned on.

Table 5 Usage examples for Info Command

Description of task:	Display auto-compression status of the posted IP position.

Table 5 Usage examples for Info Command

Command:	MAP	mapci;mtc;appl;topsip;topspost;post p1800;info
response:		Last Known Position IP Address: 96.92.8.1 XPM IP Address: 95.92.9.100 VoiceTrunk:None Operator:None Alarm Conditions: None Auto Compression: ON SysB Reason: None

32.11 OSSGate Interface Changes

Not Applicable.

32.12 Security

Not Applicable.

32.13 Configuration Walkthrough

Not Applicable.

33: A00007790 Configuration (CN)

33.1 Feature name

P-phone Expansion for CICM Lines

33.2 Hardware and Software Requirements

Not applicable.

33.3 Initial Configuration

Not applicable.

33.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

33.5 Upgrade Considerations

Not applicable.

33.6 Data schema (DS) (CM, MIBS, RDB)

33.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHAN GED)
KSETINV	changed	new

33.6.2 Table/MIB/Remote Database Schema information

33.6.2.1 Name: KSETINV

Business Set and Data Unit Inventory Table

33.6.2.1.1 Functional description

No change.

33.6.2.1.2 Usage sequence and implications (CM Only)

No change.

33.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
KSETINV	0	150,000	Memory is automatically allocated for this table.

33.6.2.1.4 Fields/OIDs

33.6.2.1.5 Datafill example

33.6.2.1.6 Table release history update

The maximum table size is increased from 31,743 to 150,000.

33.6.2.1.7 Supplementary information

33.6.2.1.8 Translation verification and other tools

33.7 Service Orders (SO) (CM & SESM)

Not applicable.

33.8 Software optionality control (SOC)

Not applicable.

33.9 Element Management

Not applicable.

33.10 User interface changes

Not applicable.

33.11 OSSGate Interface Changes

Not applicable.

33.12 Security

Not applicable.

33.13 Configuration Walkthrough

34: A00007934 Configuration (CN)

34.1 Feature name

E800 Routing Enhancements

34.2 Hardware and Software Requirements

Not applicable.

34.3 Initial Configuration

Not applicable.

34.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

34.5 Upgrade Considerations

None.

34.6 Data schema (DS) (CM, MIBS, RDB)

34.6.1 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)
NSCDEFS	Changed	New
NSCPMAP	New	New

34.6.2 Table/MIB/Remote Database Schema information

34.6.2.1 Name: NSCDEFS

Number Service Code Database Response Time-outs table

34.6.2.1.1 Functional description

The new option PRETRANMAP is added to table NSCDEFS. The option PRETRANMAP, in combination with table NSCPMAP, provides the ability to override the originator's standard pretranslator name for the E800 response translation.

When option PRETRANMAP is provisioned for the E800 service in table NSCDEFS, table NSCPMAP is accessed to map the originator's standard pretranslator name to a new pretranslator name for use by the E800 response translation.

Option PRETRANMAP is compatible only with the service E800 in table NSCDEFS.

This functionality provided by option PRETRANMAP requires SOC NTS00030. However, SOC NTS00030 has an RTU of A/P (Always Present), and it is always at the ON state. Therefore, only option PRETRANMAP in table NSCDEFS controls both the call processing and traver enhancements provided by this activity.

34.6.2.1.2 Usage sequence and implications (CM Only)

The current datafill order for table NSCDEFS is unchanged.

34.6.2.1.3 Size

The size of table NSCDEFS is unchanged.

34.6.2.1.4 Fields/OIDs

Table 2 lists the impacted fields/OIDs for table NSCDEFS.

Table 2 Table field descriptions - NSCDEFS

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTION	Changed	Refinement	PRETRANMAP refinement is added	Adding new option, PRETRANslator MAPping

Table lists the subfields for option PRETRANMAP in table NSCDEFS:

Table 3 Table field descriptions - Option PRETRANMAP

New Option	Subfield or refinement	Entry	Explanation and action
PRETRANMAP	subfield	DEFPREXLA PRETRANSLATOR_NAME	Specifies the default STDPRT name that is to be used if no entry is found in table NSCPMAP. When provisioned to NPRT and no entry is found in table NSCPMAP, the originating subscriber's STDPRT name is used. If option PRETRAN already exists in table NSCDEFS, consideration should be given to provisioning option PRETRANMAP with the same values as existing option PRETRAN. By provisioning the same values, the switch behavior is unchanged from option PRETRAN for those STDPRT names that are not provisioned in table NSCPMAP.

Table 3 Table field descriptions - Option PRETRANMAP

New Option	Subfield or refinement	Entry	Explanation and action
		CALLS {ALL, COIN}	Specifies whether ALL calls or only COIN calls should use this functionality.
		IGNORE {Y/N}	Specifies whether this option should be ignored for the AIN/LNP Response translation.

34.6.2.1.5 Datafill example

The following example shows a sample datafill for option PRETRANMAP in table NSCDEFS.

TABLE: NSCDEFS		
NSCCODE	TIMEOUT	OPTIONS

--		

34.6.2.1.6 Table release history update

Option PRETRANMAP is added for the E800 service in table NSCDEFS.

34.6.2.1.7 Supplementary information

None.

34.6.2.1.8 Translation verification and other tools

The following example shows the output from Traver when it is used to verify table NSCDEFS.

traver l 6215000 nsc 101022215198881111 b

TABLE LINEATTR

0 1FR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_0 L613_LATA1_0 \$
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE

TABLE XLAPLAN

613_P621_0 FR01 613 P621 TSPS Y RESGRP 0 2 \$ \$

TABLE RATEAREA

L613_LATA1_0 L613 NIL LATA1 \$

TABLE DNATTRS

613 621 5000

(PUBLIC (NAME SAM_SNEAD) \$)\$ \$

TABLE DNGRPS

TUPLE NOT FOUND

TABLE LENFEAT

TUPLE NOT FOUND

TABLE OFCVAR

AIN_OFFICE_TRIGGRP LNPOFFICE

TABLE NSCDEFS

E800 3 (4DGTIC) (PRETRANMAP PDEF ALL Y) \$

TABLE NSCPMAP

P621 P800

USING PRETRANSLATOR FROM TABLE NSCPMAP

TABLE STDPRTCT

P800 (1) (0) 4

. SUBTABLE STDPRT

. 1010222 1010222 EA DD 7 P PCAR CAR1 Y OFRT 700 8 25 N

. . TABLE OFRT

. . 700 S D ISUP2WATC

. . EXIT TABLE OFRT

. SUBTABLE AMAPRT

. KEY NOT FOUND

. DEFAULT VALUE IS: NONE OVRNONE N

TABLE STDPRTCT

PCAR (1) (0) 6

. SUBTABLE STDPRT

. 15 19 EA DD 1 T NA CAR1 N

. SUBTABLE AMAPRT

. KEY NOT FOUND

. DEFAULT VALUE IS: NONE OVRNONE N

TABLE HPCPATTN

TUPLE NOT FOUND

TABLE HNPACONT

```

TABLE FNPACONT
519 10 - ( 2 ) ( 0 ) ( 1 ) ( 0 )
. SUBTABLE FNPACODE
. 888 888 3 Y
. SUBTABLE RTEREF
. . 3 N D ISUPIT 0 N N
. EXIT TABLE RTEREF
EXIT TABLE FNPACONT
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
TUPLE NOT FOUND. DEFAULT IS TO LEAVE XLA RESULT UNCHANGED
TABLE CLSVSCRC
KEY NOT FOUND
EA:Local override does not apply to this call.
TABLE LATA XLA
LATA1 51 INTER INTER STD
TABLE OCCINFO
CAR1 0222 TRANS Y Y Y Y Y N N Y Y Y Y LONG 0 FGRPD 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
Using Equal Access (EA) route    OFRT 700 from Pretranslation
TABLE OFRT
700 S D ISUP2WATC
EXIT TABLE OFRT
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 +++

```

34.6.2.2 Name: NSCPMAP

Number Services Code Pretranslator MAPping

34.6.2.2.1 Functional description

The new table NSCPMAP is added. Table NSCPMAP, in combination with option PRETRANMAP in table NSCDEFS, provides the ability to override the originator's standard pretranslator name for the E800 response translation.

When option PRETRANMAP is provisioned for the E800 service in table NSCDEFS, table NSCPMAP is accessed to map the originator's standard pretranslator name to a new pretranslator name for use by the E800 response translation. The originator's standard pretranslator name is used as the index into table NSCPMAP. The new standard pretranslator name to be used by the E800 response translation is retrieved from field MAPPTNM.

The nil pretranslator name, NPRT, is not permitted to be datafilled in table NSCPMAP.

The functionality provided by table NSCPMAP requires SOC NTS00030. However, SOC NTS00030 has an RTU of A/P (Always Present), and it is always at ON state.

34.6.2.2.2 Usage sequence and implications (CM Only)

It is recommended that when initially configuring the switch, table NSCPMAP should be provisioned prior to adding option PRETRANMAP in table NSCDEFS for the E800 service. Once the switch has been completely configured, new entries can be added to, changed in or deleted from table NSCPMAP at any time. The switch does not enforce a provisioning sequence.

34.6.2.2.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NSCPMAP	0	4095	4 Kwords of static data store

34.6.2.2.4 Fields/OIDs

The following table lists the impacted fields/OIDs for table NSCPMAP.

Table 5 Table field descriptions

Field	New or Changed	Entry	Explanation and action
ORIGPTNM	new	PRETRANSLATOR_NAME	The table key specifies the originating subscriber's STDPRT name.

Table 5 Table field descriptions

Field	New or Changed	Entry	Explanation and action
MAPPTNM	new	PRETRANSLATOR_NAME	This field specifies the new STDPRT name to be used for the E800 response translation.

34.6.2.2.5 Datafill example

The following example shows sample datafill for table NSCPMAP.

<u>TABLE: NSCPMAP</u>	
ORIGPTNM	MAPPTNM

P613	P800

34.6.2.2.6 Table release history update

The new table NSCPMAP is created.

34.6.2.2.7 Supplementary information

None.

34.6.2.2.8 Translation verification and other tools

The following example shows the output from Traver when it is used to verify table NSCPMAP.

traver l 6215000 nsc 101022215198881111 b

TABLE LINEATTR

0 1FR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_0 L613_LATA1_0 \$
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE

TABLE XLAPLAN

613_P621_0 FR01 613 P621 TSPS Y RESGRP 0 2 \$ \$

TABLE RATEAREA

L613_LATA1_0 L613 NIL LATA1 \$

TABLE DNATTRS

613 621 5000

(PUBLIC (NAME SAM_SNEAD) \$)\$ \$

TABLE DNGRPS

TUPLE NOT FOUND

TABLE LENFEAT

TUPLE NOT FOUND

TABLE OFCVAR

AIN_OFFICE_TRIGGRP LNPOFFICE

TABLE NSCDEFS

E800 3 (4DGTIC) (PRETRANMAP PDEF ALL Y) \$

TABLE NSCPMAP

P621 P800

USING PRETRANSLATOR FROM TABLE NSCPMAP

TABLE STDPRTCT

P800 (1) (0) 4

. SUBTABLE STDPRT

. 1010222 1010222 EA DD 7 P PCAR CAR1 Y OFRT 700 8 25 N

. . TABLE OFRT

. . 700 S D ISUP2WATC

. . EXIT TABLE OFRT

. SUBTABLE AMAPRT

. KEY NOT FOUND

. DEFAULT VALUE IS: NONE OVRNONE N

TABLE STDPRTCT

PCAR (1) (0) 6

. SUBTABLE STDPRT

. 15 19 EA DD 1 T NA CAR1 N

. SUBTABLE AMAPRT

. KEY NOT FOUND

. DEFAULT VALUE IS: NONE OVRNONE N

TABLE HPCPATTN

TUPLE NOT FOUND

TABLE HNPACONT

```

TABLE FNPACONT
519 10 - ( 2 ) ( 0 ) ( 1 ) ( 0 )
. SUBTABLE FNPACODE
. 888 888 3 Y
. SUBTABLE RTEREF
. . 3 N D ISUPIT 0 N N
. EXIT TABLE RTEREF
EXIT TABLE FNPACONT
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
TUPLE NOT FOUND. DEFAULT IS TO LEAVE XLA RESULT UNCHANGED
TABLE CLSVSCRC
KEY NOT FOUND
EA:Local override does not apply to this call.
TABLE LATA XLA
LATA1 51 INTER INTER STD
TABLE OCCINFO
CAR1 0222 TRANS Y Y Y Y Y N N Y Y Y Y LONG 0 FGRPD 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
Using Equal Access (EA) route    OFRT 700 from Pretranslation
TABLE OFRT
700 S D ISUP2WATC
EXIT TABLE OFRT
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 +++

```

34.7 Service Orders (SO) (CM & SESM)

Not applicable.

34.8 Software optionality control (SOC)

Table 6 SOC

SOC option name:	E800 Pretran Mapping
SOC option title:	Yes
SOC option control type:	State
New SOC option?	Yes
SOC option order code	NTS00030
Option defined in DRU:	CNA
Affected products:	SN08

34.9 Element Management

Not applicable.

34.10 User interface changes

Not applicable.

34.11 OSSGate Interface Changes

Not applicable.

34.12 Security

Not applicable.

34.13 Configuration Walkthrough

Recommended Provisioning Procedure for PRETRANMAP:

The following provisioning procedure is recommended:

- Add the required STDPRT name tuples to table NSCPMAP.
- For the E800 service, add the new option PRETRANMAP in table NSCDEFS. Do not immediately remove option PRETRAN if it is currently provisioned. Once option PRETRANMAP is added, the new functionality is active and option PRETRAN is no longer referenced by the switch software.

If option PRETRAN is currently provisioned in table NSCDEFS, consideration should be given to provisioning option PRETRANMAP with the same *values* as existing option PRETRAN. By provisioning the

same *values*, the switch behavior is unchanged from option PRETRAN for those STDPRT names that are not provisioned in table NSCPMAP.

To revert back to the functionality provided by the existing option PRETRAN, option PRETRANMAP should be removed from table NSCDEFS. Option PRETRAN (if previously provisioned) must still be present in table NSCDEFS to revert back.

Once the switch is properly configured to use option PRETRANMAP and table NSCPMAP, the existing option PRETRAN can optionally be removed from table NSCDEFS. Removal of option PRETRAN is not mandatory.

35: A00008387 Configuration (CN)

35.1 Feature name

GLC-32 AB Card Support

35.1 Hardware and Software Requirements

Standard Media Gateway 9000 Element Manager (MG9000 EM) configuration.

35.2 Initial Configuration

Standard Media Gateway 9000 Element Manager (MG9000 EM) configuration.

35.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

35.4 Upgrade Considerations

35.4.1 Dump and Restore (CM)

35.4.2 Element Management Upgrade

35.4.3 Downgrade impact

SN08 gateway is required to support the NY53AB GLC card. Once the NY53AB GLC card(s) are installed on a SN08 gateway, any gateway downgrade to pre-SN08 loads will render the NY53AB GLC card non-functional. The NY53AB GLC cards should be deprovisioned and removed prior to the downgrade attempt.

SN06.2 gateway loads do not support pPhone and potsGroundStart line service types for GLC cards. When downgrading to the SN06.2 gateway load, if pPhone and postGroundStart lines are provisioned on the GLC cards, they will have to be deprovisioned prior to the downgrade attempt.

The WLC and GLC card replacement is only supported with the SN08 gateway.

35.5 Data schema (DS) (CM, MIBS, RDB)

N/A

35.6 Service Orders (SO) (CM & SESM)

N/A

35.7 Software optionality control (SOC)

N/A

35.8 Element Management

35.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
LineCoefficientView	changed
BulkProvSvceTypesView	new

35.8.2 GUI information

35.8.2.1 GUI name: LineCoefficientView

35.8.2.1.1 Functional description

This is an existing view that shows the Line Coefficients available for the GLC circuits.

35.8.2.1.2 GUI usage and implications

This is an existing view that shows the Line Coefficients available for the GLC circuits. This GUI is updated to display the Line Coefficient information in a table format. The usage for this GUI has not changed.

35.8.2.1.3 GUI fields

Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Name	changed			Name of the Coefficient	
Index	changed			Coefficient Index	
PEC	new			GLC Card PEC (NY53AA or NY53AB)	
Country Info	new			Country the coefficient is intended for	
CRAM	new			cRAM info from the GLC card	
Vinetic Ver.	new			Vinetic version from the GLC card	
Loop Info	new			loop status	
Metering	new			with or without Metering	
Svc Type	new			service type the coefficient is for	

Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Default	new			is or is not the default coefficient for the country	

35.8.2.1.4 Usage example

From the GLC Card View pulldown menu, select “Coefficient Table Manager...” to launch the GUI.

Here is an example of the GUI:

Name	Index	PEC	Country Info	CRAM	Vinetic Ver.	Loop Info	Metering	Svc Type	Default
PPHONE_LL	90	NY53AA	Global	0	0x2484	LongLoop	false	pPhone	true
PPHONE_LL_LV	91	NY53AA	Global	0	0x2484	LongLoopLowVoltage	false	pPhone	false
POTS_SL	1	NY53AA	NorthAmerica	0	0x2484	ShortLoop	false	pots	true
POTS_LL_LV	13	NY53AA	NorthAmerica	0	0x2484	LongLoopLowVoltage	false	pots	false
POTS_LL	2	NY53AA	NorthAmerica	0	0x2484	LongLoop	false	pots	false
POTS_SL	10	NY53AA	Russia	0	0x2484	ShortLoop	false	pots	true
POTS_LL	11	NY53AA	Russia	0	0x2484	LongLoop	false	pots	false
POTS_LL_LV	12	NY53AA	Russia	0	0x2484	LongLoopLowVoltage	false	pots	false
POTS_SL	3	NY53AA	Spain	0	0x2484	ShortLoop	false	pots	true
POTS_LL	5	NY53AA	Spain	0	0x2484	LongLoop	false	pots	false
POTS_LL_WM	14	NY53AA	Spain	0	0x2484	LongLoopLowVoltage	true	pots	false
POTS_LL_WM	6	NY53AA	Spain	0	0x2484	LongLoop	true	pots	false
POTS_SL_WM	4	NY53AA	Spain	0	0x2484	ShortLoop	true	pots	false
POTS_SL	7	NY53AA	Mexico	0	0x2484	ShortLoop	false	pots	true
POTS_LL	8	NY53AA	Mexico	0	0x2484	LongLoop	false	pots	false
POTS_LL_LV	9	NY53AA	Mexico	0	0x2484	LongLoopLowVoltage	false	pots	false
PPHONE_LL	95	NY53AB	Global	0	0x1490	LongLoop	false	pPhone	true
PPHONE_LL_LV	96	NY53AB	Global	0	0x1490	LongLoopLowVoltage	false	pPhone	false
POTS_SL	31	NY53AB	NorthAmerica	0	0x1490	ShortLoop	false	pots	true
POTS_LL	32	NY53AB	NorthAmerica	0	0x1490	LongLoop	false	pots	false
POTS_LL_LV	33	NY53AB	NorthAmerica	0	0x1490	LongLoopLowVoltage	false	pots	false
POTS_SL	50	NY53AB	Russia	0	0x1490	ShortLoop	false	pots	true
POTS_LL	51	NY53AB	Russia	0	0x1490	LongLoop	false	pots	false
POTS_LL_LV	52	NY53AB	Russia	0	0x1490	LongLoopLowVoltage	false	pots	false

35.8.2.1.5 GUI release history update

35.8.2.1.6 Context sensitive launching information

This GUI is only accessible through the GLC Card View pulldown menu.

35.8.2.1.7 Supplementary information

35.8.3 GUI information

35.8.3.1 GUI name: BulkProvSvceTypesView

35.8.3.1.1 Functional description

This is a new view. This view can be used to bulk provision all the line circuits on a GLC card to the same service type.

35.8.3.1.2 GUI usage and implications

This view can be used to bulk provision all the line circuits on a GLC card to the same service type. This GUI is only enabled when the card is deprovisioned.

35.8.3.1.3 GUI fields

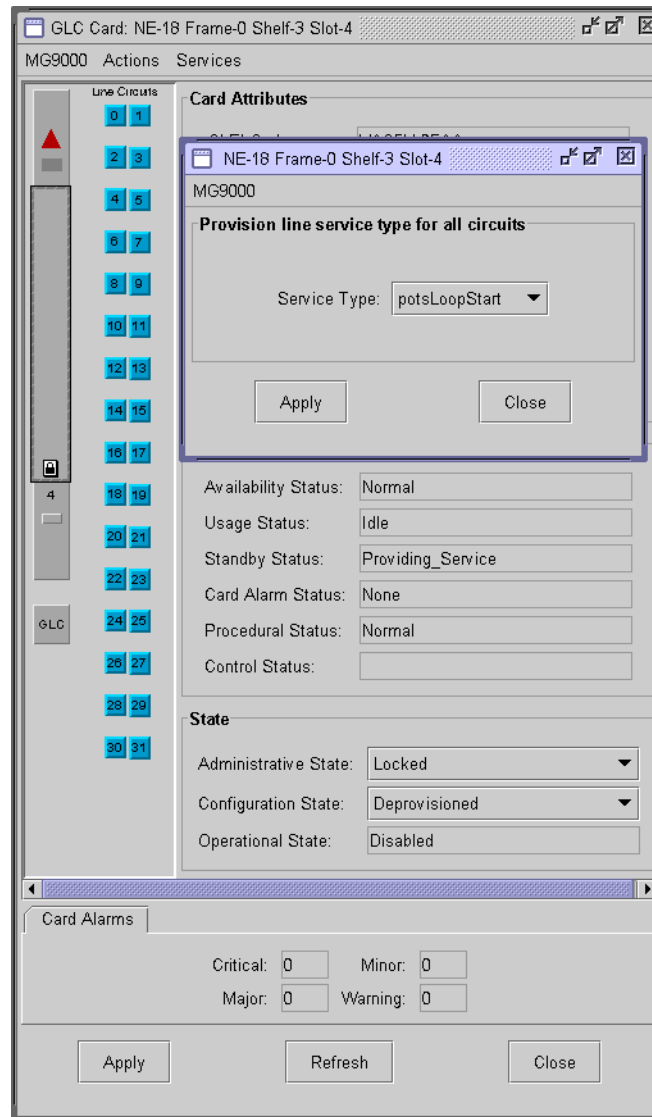
Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Service Type	new			This is a selection field, the options are: potsLoopStart, pPhone or potsGroundStart	

35.8.3.1.4 Usage example

From the GLC Card View, offline and deprovision the card. Once the card is deprovisioned, select “Provision Bulk Line Service Types...” from the card’s pulldown menu to launch the GUI. Select the desired service type from the new GUI then press “Apply” to provision this service type for all the circuits on the card.

Here is an example of the GUI:



35.8.3.1.5 GUI release history update

35.8.3.1.6 Context sensitive launching information

This GUI is only accessible through the GLC Card View pulldown menu when the card is deprovisioned.

35.8.3.1.7 Supplementary information

35.8.4 CLUI Interface

35.9 User interface changes

N/A

35.10 OSSGate Interface Changes

N/A

35.11 Security

Only users in the *emsmtc*, *emsrw* or *emsadm* groups are authorized to bulk provision the GLC card's line service types.

35.12 Configuration Walkthrough

36: A00008431 Configuration (CN)

36.1 Feature name

System Mastership Support for CS 2000 - Compact Geographic Survivability Configuration

36.2 Hardware and Software Requirements

36.3 Initial Configuration

36.4 Office/Subnet parameters (OP/SP) (CM & SESM)

36.5 Upgrade Impact

36.5.1 Dump and Restore

No dump/restore impact.

36.5.2 Element Management Upgrade

No element management upgrade impact?

36.6 Data schema (DS) (CM, MIBS, RDB)

No data schema changes.

36.7 Service Orders (SO) (CM & SESM)

No service order changes.

36.8 Software optionality control (SOC)

Not applicable.

36.9 Element Management

36.9.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
SAM21 EM 3PC provisioning Panel	Changed

36.9.2 GUI information

36.9.2.1 GUI name: SAM21 EM 3PC Provisioning Panel SAM21 EM 3PC Provisioning Panel

36.9.2.1.1 Functional description

This panel is for provisioning 3PC card through SAM21 EM GUI. In this feature, a new sub panel for provisioning GR backup WAN IP addresses is added to the existing 3PC provisioning panel (refer to figure 6).

Figure 1 SAM21Manager Call Agent Provisioning Panel

The screenshot shows the 'OTT4 CA-1 : Slot 6' provisioning panel. The 'Provisioning' tab is selected. The 'General' section contains fields for IP (10.72.17.22), Gateway IP (10.72.16.1), Subnet Mask (255.255.240.0), FW Version (RM03-2.4), MAC Address (0001AF12AFA0), and MAC 2 (0001AF12AF9F). The 'NTP' section has Primary NTP (47.135.43.193) and Secondary NTP (47.135.43.196). The 'Load Info' section includes Server IP (47.135.43.193), Path (/3pc), Load (ncgl_cca_image_7.02.1.0), and a 'Get Load Files' button. The 'Geographical Survivable' section has a checked 'enable' checkbox. The 'Backup Path' section contains GEO UNIT 0 IP (10.72.0.12) and Mask (255.255.255.248), and GEO UNIT 1 IP (10.72.0.20) and Mask (255.255.255.248). Red circles highlight the 'Provisioning' tab, the 'Geographical Survivable' tab, and the GEO UNIT 0 and 1 IP address fields.

36.9.2.1.2 GUI usage and implications

Current datafill order unchanged.

36.9.2.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
SAM21EM 3PC provisioning Panel	0	1 per card view	Memory is automatically allocated

36.9.2.1.4 GUI fields

The following table lists fields for the GR backup WAN IP addresses configuration panel which is newly added to existing SAM21 EM 3PC provisioning panel.

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Enable	New	0	0	Check this box to enable Geographical Survivable WAN IP addresses configuration	
GEO UNIT 0 IP	New	0	0	The IP address for the GEO UNIT 0 Backup path IP for CA 0. The address specified here is the network ip +4. The last octet of this IP address must be 4 less than a base multiple of 8 address.	
GEO UNIT 1 IP	New	0	0	The IP address for the GEO UNIT 1 Backup path IP for CA 1. The address specified here is the network ip +4. The last octet of this IP address must be 4 less than a base multiple of 8 address.	

36.9.2.1.5 Usage example

The following example shows sample datafill for GR backup WAN IP addresses configuration panel:

Enable: true

GEO UNIT 0 IP: 47.142.114.84

GEO UNIT 1 IP: 47.142.114.44

36.9.2.1.6 GUI release history update

N/A

36.9.2.1.7 Supplementary information

N/A

36.9.2.1.8 CLUI Interface

N/A

36.10 Command interface changes

N/A

36.11 Security

N/A

36.12 Configuration Walkthrough

During the CS 2000 - Compact Geographic Survivability Configuration mode, it is necessary to perform specific configuration for Geo Survivability at various phases of the commissioning and setup of the office.

36.12.1 During Planning:

Ensure that the following additional configuration information is identified. Additional details are found in the System Engineering Bulletins.

- CA Backup Link VLANs and IP addresses. 2 separate 8 IP address ranges are required to setup packet routing via the IP network. These values are be configured in the GUI when configuring the CA cards. Both VLANs are configured with a subnet max of 255.255.255.248.

Table 4 Example Backup Path IP addresses

IP	Comment
192.168.0.0 (base + offset 0)	Network ID - base address for vlan
192.168.0.1 (base + offset 1)	Used by CA to access the local ERS 8600
192.168.0.2 (base + offset 2)	port 0 (localwan0 or matewan0)
192.168.0.3 (base + offset 3)	port 1 (localwan1 or matewan1)
192.168.0.4 (base + offset 4)	backup path provisioned value (localwan or matewan)
192.168.0.5 (base + offset 5)	reserved
192.168.0.6 (base + offset 6)	reserved
192.168.0.7 (base + offset 7)	broadcast

- To enable the setgeoconfig script to automatically identify the CallP and OAM vlans, the following naming convention for CallP and OAMP VLANs is required. Additional details are found in the System Engineering Bulletins.
 - The OAMP VLAN name must start with the string “OAMP”.

- All CallIP VLAN names must start with the string “CallIP”, except for the Private-CallIP VLAN.

36.12.2 During CS-LAN configuration:

- Create 1 backup path vlan on each of the CS LAN routers. Additional details are found in the System Engineering Bulletins.
 - Create Backup_path_subnet VLAN by IPSubnet
 - Remove all ports from the backup_path_subnet except the two physical ports from the CA
 - Create a IP Traffic filter-set to allow traffic to/from the backup_path_subnet's only
 - Setup routing to ensure the backup path always routes through the core network, and not over the IST.
- If the CS LAN router is an ERS 8600, create a user acct and access policy for the CA access:
 - Enabling rlogin server
 - config bootconfig flags rlogind true
 - configuring and enabling an access policy.
 - # Create 3PC access policy on the ERS8600
 - config sys access-policy enable true
 - config sys access-policy policy 2 create
 - config sys access-policy policy 2 accesslevel rwa
 - config sys access-policy policy 2 host <CA IP address>
 - config sys access-policy policy 2 name "3PC-script"
 - config sys access-policy policy 2 username "root"
 - config sys access-policy policy 2 service rlogin enable

36.12.3 During CA GUI configuration:

In the CA GUI for each blade:

- Check the Enable check box in the Geographic Survivable section of the CA GUI.
- Enter the Unit0 and Unit1 Backup Link IPs as determined during planning.

Figure 2 Backup Path provisioning

OTT4 CA-1 Slot 6

Alarms Equip States Diags **Provisioning**

General

IP: 10.72.17.22 Gateway IP: 10.72.16.1

Subnet Mask: 255.255.240.0 FW Version: RM03-2.4

MAC Address: 0001AF12AFA0 MAC 2: 0001AF12AF9F

NTP

Primary NTP: 47.135.43.193 Secondary NTP: 47.135.43.196

Load Info

Server IP: 47.135.43.193

Path: /3pc

Load: ncgl_cca_image_7.02.1.0 Get Load Files

☒ FW Flash Enable

Geographical Survivable

Geographical CS 2000 Compact

☒ Enable

Backup Path:

GEO UNIT 0 IP: 10.72.0.12 Mask: 255.255.255.248

GEO UNIT 1 IP: 10.72.0.20 Mask: 255.255.255.248

36.12.4 During CA setup:

Once the CA blades have been booted and brought inservice, use the setgeoconfig.sh script tool to configure the local router actions with the CA:

36.12.4.1 Configuration with ERS 8600 router

- As root user, invoke the setgeoconfig.sh script tool to begin the configuration:

Figure 3 setgeoconfig.sh script invocation

```
[root@10.73.17.19 root]# cd /usr/admin_bin/
[root@10.73.17.19 admin_bin]# ./setgeoconfig.sh
```

- Enter the ERS 8600 configuration mode, and enter the 8600 userid created for CA access.

Figure 4 ERS 8600 configuration mode and userid

```
*****
3PC-P8600 Passport Interaction configuration
*****
```

Note : Current value are put in [] at prompts
Type new value or press enter for default

```
-----
Does this Geographic Redundant (RC)
Configuration of the CS2Kc use p8600
```

```
Type yes or no
P8600_used => [] : yes
```

```
-----
Type in Passport P8600 User ID
P8600_USER => [] : rwa
-----
```

- The script then validates connectivity to the ERS 8600, then connects to the ERS 8600 and retrieve a list of CallP and OAMP vlans. Confirm each vlan which will be configured to be part of the set to have OSPF disabled during certain failure scenarios. The script prompts for each vlan in turn.

Figure 5 ERS 8600 configuration of CallP and OAMP vlans

Configuring CallP & OAMP VLANs to monitor

```
-----
The following CallP & OAMP are configured on passport
```

5	CallP Private	byPort	1	none	N/A	N/A
6	CallP Carrier	byPort	1	none	N/A	N/A
7	CallP Public	byPort	1	none	N/A	N/A
8	OAMP	byPort	1	none	N/A	N/A

```
-----
Do you want to include VLAN name:id [CallP:5]
Response => [y] :
```

```
Do you want to include VLAN name:id [CallP:6]
Response => [y] :
```

```
Do you want to include VLAN name:id [CallP:7]
Response => [y] :
```

```
Do you want to include VLAN name:id [OAMP:8]
Response => [y] :
```

- The script summarizes the configuration data and exits. To correct any errors or change configuration data at another time, rerun the setgeoconfig.sh script.

Figure 6 ERS 8600 configuration data summary

```
-----
The config data for GEO scripts are as follows
Note : Run setgeoconfig.sh to modify any data
-----
```

```
P8600_used=yes
CMD=rsh
Passport_IP=10.73.0.9
P8600_USER=rwa

typeset -a WAN
WAN_Array_Size=1
WAN[0]=192.168.101.114
WAN_ALL='192.168.101.114'
typeset -a VLAN
VLAN[0]=5
VLAN[1]=6
VLAN[2]=7
VLAN[3]=8
VLAN_Array_Size=4
-----
```

```
[root@10.73.17.19 admin_bin]#
```

36.12.4.2 Configuration with non-ERS 8600 router

If the CS-LAN is not using ERS 8600 routers, this is also configured using the setgeoconfig.sh script tool.

- Invoke the setgeoconfig.sh script tool to begin the configuration:

Figure 7 setgeoconfig.sh script invocation

```
[root@10.73.17.19 root]# cd /usr/admin_bin/
[root@10.73.17.19 admin_bin]# ./setgeoconfig.sh
```

- Configure non-ERS 8600 mode.

Figure 8 non-ERS 8600 configuration mode

```

*****
3PC-P8600 Passport Interaction configuration
*****

Note : Current value are put in [] at prompts
      Type new value or press enter for default

-----
Does this Geographic Redundant (RC)
Configuration of the CS2Kc use p8600

Type yes or no
P8600_used => [yes] : no
-----

```

- Configure WAN edge IP to monitor. First configure the number of wan edge IPs to monitor (default 1), then the IPs to monitor. The script tests that the IPs are reachable by ping.

Figure 9 non-ERS 8600 Wan edge configuration

```

Configure WAN Edge IP
How many Wan Edge IP address required

WAN_Array_Size => [1] : 1

Read Wan edge IP address
WAN[0] => [192.168.101.114] : 192.168.101.114
-----
Pinging IP address 192.168.101.114
PING 192.168.101.114 (192.168.101.114) 56(84) bytes of data.
...

```

- The script summarizes the configuration data and exits. To correct any errors or change configuration data at another time, rerun the setgeoconfig.sh script.

Figure 10 non-ERS 8600 configuration data summary

```

The config data for GEO scripts are as follows
Note : Run setgeoconfig.sh to modify any data
-----
P8600_used=no
typeset -a WAN
WAN_Array_Size=1
WAN[0]=192.168.101.114
-----
[root@10.73.17.19 admin_bin]#

```


Performance Management (PF)

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
A00004741.AA05	Enabling TRKGRP OM ON GEM and SUPPORT NOD-AL OMS
A00005562	MG9000 ITP/ABI Overload Controls
A00006693.AA08	XA-Core IO Capacity Monitoring Toolset
A00006780.AA23	Trimodal Call Server OAM & P Enhancements
A00007000	GigE Network Interface
A00007074	GigE Link Maintenance
A00007120.AA98	Packet Media Anchor for DPT
A00007213	MG9000 5/30 Minutes OMs
A00007270.AA13	Session Server Call Processing Overload Controls
A00007271.AA08	TOPS EOL for SN08
A00007293	VLAN for Gigabit Ethernet
A00007327.AA08	Media Proxy 5 and 30 minute Operational Measurements
A00007393	Session Policy Controller
A00007465.AA06	Integrated Accounting Application (IAA)
A00008350.AA04	Trunk group OM registers for establish bearer path failures

1: A00004741 Performance (PF)

1.1 Feature name

Enabling TRKGRP OM ON GEM and SUPPORT NODAL OMS

1.2 Performance management strategy

This capability provides statistics which are necessary for Link Bandwidth Engineering and to determine the network usage and transmission errors.

1.3 Performance management tools and utilities

This feature provides Nodal Based Operational Measurements for MG4K-IP and IW-IP nodes.

Two new Nodal Based OM groups added by this activity are:

- MNGEMLNK - Statistics for Nodal Gigabit Ethernet Link usage.
- MNGEMTRF - Statistics for Nodal traffic usage and transmission errors.

To view the MNGEMLNK and MNGEMTRF, use the OMSHOW CI command as follows:

```
>OMSHOW MNGEMLNK ACTIVE
```

```
>OMSHOW MNGEMTRF ACTIVE
```

1.4 Performance Measurements (PM), Operational Measurements (OM), and stats

New Nodal Based OM groups added by this activity are:

- MNGEMLNK
- MNGEMTRF

1.4.1 PM, OM, and stats format

Component: MG4K-IP Node, IW-IP node

Performance Measurement Name: MNGEMLNK

Performance Measurement Description:

This OM group provides the statistics related to the Gigabit Ethernet Link connected to a particular MG4K-IP/ IW-IP node. This information will be used for Gigabit Ethernet Link bandwidth Engineering.

History: Created in SN08

Component: MG4K-IP Node, IW-IP node

Performance Measurement Name: MNGEMTRF

Performance Measurement Description:

This OM group provides the usage statistics related to bearer traffic on the MG4K-IP and IW-IP nodes. These information will be used to identify the Nodal traffic usage in the network.

History: Created in SN08

1.4.2 OM Group - MNGEMLNK**1.4.2.1 OM description**

OM Group MNGEMLNK

Multiservice Node Gigabit Ethernet Module Link Bandwidth Engineering

The purpose of this OM group is to provide Gigabit Ethernet Link usage statistics to assist with network bandwidth Engineering.

In this OM group, the pegs include:

- The number of packets/octets transmitted/received on the Gigabit Ethernet Link connected to a MG4K-IP/IW-IP node.
- The number of packets/octets transmitted/received with different types of error.

The Gigabit Ethernet Module (GEM) hardware is a Resource Module of MG4K-IP/IW-IP node. The GEM provides a 1 Gigabit/sec Ethernet network interface that will support up to 2016 DS0 voice channels over an IP based packet network.

1.4.2.2 Release history update

OM group MNGEMLNK is new in SN08

1.4.2.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 1 MNGEMLNK OM group display

```

>omshow mngemlnk active

MNGEMLNK

CLASS: ACTIVE
START:2004/07/08 06:30:00 THU; STOP: 2004/07/08 06:34:44 THU;
SLOWSAMPLES:      3 ; FASTSAMPLES:      28 ;

      INFO (MNMGPIP_BASED_OMINFO)
      TXOCT      TXOCT2      RXOCT      RXOCT2
      TXPKT      TXPKT2      RXPKT      RXPKT2
      TXEROCT    TXEROCT2    RXEROCT    RXEROCT2
      TXERPKT    RXERPKT    CRCERPKT    UNDERPKT
      OVERPKT    SHORTPKT    LONGPKT

2
  IW  2  SPM_2
        0          0          0          0
        0          0          0          0
        0          0          0          0
        0          0          0          0
        0          0          0

3
  SMG4 3  SPM_3
        0          0          0          0
        0          0          0          0
        0          0          0          0
        0          0          0          0
        0          0          0

```

1.4.2.4 Group structure

OM group provides one tuple for each MG4K-IP and IW-IP node.

Key field: SPM PM Number, a number in the range 0 - 85

Info field: SPM PM Number, a number in the range 0 - 85

1.4.2.5 Associated OM groups

None

1.4.2.6 Associated functional groups

None

1.4.2.7 Associated functionality codes

None

1.4.2.8 OM group registers logic flow chart

The Gigabit Ethernet Link usage statistics are available in GigMAC chip of the GEM RM. This information is used for incrementing the OM Registers for that MG4K-IP/IW-IP node.

1.4.2.9 Register - TXOCT, TXOCT2

1.4.2.9.1 Register description

Register TXOCT (Transmitted Octets) provides count for total number of bytes transmitted on a Gigabit Ethernet Link connected to a particular MG4K-IP/IW-IP node. Register TXOCT2 is an extension register for TXOCT.

The count is represented in Kilo Bytes (Scaled by factor of 1024).

1.4.2.9.2 Register TXOCT release history update

Register TXOCT is new in SN08.

1.4.2.9.3 Associated registers

None

1.4.2.9.4 Associated logs

None

1.4.2.10 Register - RXOCT, RXOCT2

1.4.2.10.1 Register description

Register RXOCT (Received Octets) provides count for total number of bytes received on a GigE Link connected to a particular MG4K-IP/IW-IP node. Register RXOCT2 is an extension register for RXOCT.

The count is represented in Kilo Bytes (Scaled by factor of 1024).

1.4.2.10.2 Register RXOCT release history update

Register RXOCT is new in SN08.

1.4.2.10.3 Associated registers

None

1.4.2.10.4 Associated logs

None

1.4.2.11 Register - TXPKT, TXPKT2

1.4.2.11.1 Register description

Register TXPKT (Transmitted Packets) provides count for total number of packets transmitted on a GigE Link connected to a particular MG4K-IP/IW-IP node. Register TXPKT2 is an extension register for TXPKT.

The count is represented in Kilo Packets (Scaled by factor of 1000).

1.4.2.11.2 Register TXPKT release history update

Register TXPKT is new in SN08.

1.4.2.11.3 Associated registers

None

1.4.2.11.4 Associated logs

None

1.4.2.12 Register - RXPKT, RXPKT2**1.4.2.12.1 Register description**

Register RXPKT (Received Packets) provides count for total number of packets received on a GigE Link connected to a particular MG4K-IP/IW-IP node. Register RXPKT2 is an extension register for RXPKT.

The count is represented in Kilo Packets (Scaled by factor of 1000).

1.4.2.12.2 Register RXPKT release history update

Register RXPKT is new in SN08.

1.4.2.12.3 Associated registers

None

1.4.2.12.4 Associated logs

None

1.4.2.13 Register - TXEROCT, TXEROCT2**1.4.2.13.1 Register description**

Register TXEROCT (Transmitted Error Octets) provides count for total number of bytes transmitted in errored packets on a GigE Link connected to a particular MG4K-IP/IW-IP node. Register TXEROCT2 is an extension register for TXEROCT.

1.4.2.13.2 Register TXEROCT release history update

Register TXEROCT is new in SN08.

1.4.2.13.3 Associated registers

None

1.4.2.13.4 Associated logs

None

1.4.2.14 Register - RXEROCT, RXEROCT2**1.4.2.14.1 Register description**

Register RXEROCT (Received Error Octets) provides count for total number of bytes received in errored packets on a GigE Link connected to a particular MG4K-IP/IW-IP node. Register RXEROCT2 is an extension register for RXEROCT.

1.4.2.14.2 Register RXEROCT release history update

Register RXEROCT is new in SN08.

1.4.2.14.3 Associated registers

None

1.4.2.14.4 Associated logs

None

1.4.2.15 Register - TXERPKT**1.4.2.15.1 Register description**

Register TXERPKT (Transmitted Error Packets) provides count for total number of errored packets transmitted on a GigE Link connected to a particular MG4K-IP/IW-IP node.

1.4.2.15.2 Register TXERPKT release history update

Register TXERPKT is new in SN08.

1.4.2.15.3 Associated registers

None

1.4.2.15.4 Associated logs

None

1.4.2.16 Register - RXERPKT**1.4.2.16.1 Register description**

Register RXERPKT (Received Error Packets) provides count for total number of errored packets received on a GigE Link connected to a particular MG4K-IP/IW-IP node.

1.4.2.16.2 Register RXERPKT release history update

Register RXERPKT is new in SN08.

1.4.2.16.3 Associated registers

None

1.4.2.16.4 Associated logs

None

1.4.2.17 Register - CRCERPKT**1.4.2.17.1 Register description**

Register CRCERPKT (Cyclic Redundancy Check Error Packets) provides count for total number of packets received with Cyclic Redundancy Check (CRC) errors on a GigElink connected to a particular MG4K-IP/IW-IP node.

1.4.2.17.2 Register CRCERPKT release history update

Register CRCERPKT is new in SN08.

1.4.2.17.3 Associated registers

None

1.4.2.17.4 Associated logs

None

1.4.2.18 Register - UNDERPKT**1.4.2.18.1 Register description**

Register UNDERPKT (Undersize Packets) provides count for total number of undersize packets received on a Gige Link connected to a particular MG4K-IP/IW-IP node.

Undersize packet is one with less than 64 bytes.

1.4.2.18.2 Register UNDERPKT release history update

Register UNDERPKT is new in SN08.

1.4.2.18.3 Associated registers

None

1.4.2.18.4 Associated logs

None

1.4.2.19 Register - OVERPKT**1.4.2.19.1 Register description**

Register OVERPKT (Oversize Packets) provides count for total number of oversize packets received on a Gige Link connected to a particular MG4K-IP/IW-IP node.

Oversize Packet is one with more than 1518 bytes.

1.4.2.19.2 Register OVERPKT release history update

Register OVERPKT is new in SN08.

1.4.2.19.3 Associated registers

None

1.4.2.19.4 Associated logs

None

1.4.2.20 Register - SHORTPKT**1.4.2.20.1 Register description**

Register SHORTPKT (Short Packets) provides count for total number of short packets (aka fragments) received, on a GigE Link connected to a particular MG4K-IP/IW-IP node.

Short Packet is one with less than 64 bytes and CRC error or alignment error.

1.4.2.20.2 Register SHORTPKT release history update

Register SHORTPKT is new in SN08.

1.4.2.20.3 Associated registers

None

1.4.2.20.4 Associated logs

None

1.4.2.21 Register - LONGPKT

1.4.2.21.1 Register description

Register LONGPKT (Long Packets) provides count for total number of long packets (aka jabber) received on a GigE Link connected to a particular MG4K-IP/IW-IP node.

Long Packet is one with more than 1518 bytes and CRC error or alignment error.

1.4.2.21.2 Register LONGPKT release history update

Register LONGPKT is new in SN08.

1.4.2.21.3 Associated registers

None

1.4.2.21.4 Associated logs

None

1.4.3 OM Group - MNGEMTRF

1.4.3.1 OM description

OM Group MNGEMTRF

Multiservice Node Gigabit Ethernet Module Traffic Engineering

The purpose of this OM group is to provide statistics of Nodal traffic usage.

In this OM group, the pegs include:

- The number of RTP packets transmitted/received for bearer traffic.
- The number packets transmitted/received for different types connections used for bearer traffic.

1.4.3.2 Release history update

OM group MNGEMTRF is new in SN08

1.4.3.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 2 MNGEMTRF OM Group Display

```
>omshow mngemtrf active

MNGEMTRF

CLASS: ACTIVE
START:2004/07/08 06:40:00 THU; STOP: 2004/07/08 06:44:59 THU;
SLOWSAMPLES:      3 ; FASTSAMPLES:      30 ;

INFO (MNMGP_IP_BASED_OMINFO)
  TOTCONN  G711MUCN  G711ACN  G729CN
  CCDCN    T38CN    VBDCN    RF2833CN
  TXRTPPK  TXRTPPK2 RXRTPPK  RXRTPPK2
  TXG711PK TXG711P2  RXG711PK RXG711P2
  TXG729PK TXG729P2  RXG729PK RXG729P2
  TXCCDPK  RXCCDPK  TXT38PK  RXT38PK
  TXVBDPK  RXVBDPK  SLSUPCN

2
  IW  2  SPM_2
      0      0      0      0
      0      0      0      0
      0      0      0      0
      0      0      0      0
      0      0      0      0
      0      0      0      0
      0      0      0      0

3
  SMG4 3  SPM_3
      0      0      0      0
      0      0      0      0
      0      0      0      0
      0      0      0      0
      0      0      0      0
      0      0      0      0
      0      0      0      0
```

1.4.3.4 Group structure

OM group provides one tuple for each MG4K-IP and IW-IP node.

Key field: SPM PM Number, a number in the range 0 - 85

Info field: SPM PM Number, a number in the range 0 - 85

1.4.3.5 Associated OM groups

None

1.4.3.6 Associated functional groups

None

1.4.3.7 Associated functionality codes

None

1.4.3.8 OM group registers logic flow chart

The registers in this group are incremented by the statistics collected at the end of each connection used for a call.

1.4.3.9 Register - TOTCONN**1.4.3.9.1 Register description**

Register TOTCONN (Total Connections) provides count for total number connections handled by a particular MG4K-IP/IW-IP node.

1.4.3.9.2 Register TOTCONN release history update

Register TOTCONN is new in SN08.

1.4.3.9.3 Associated registers

None

1.4.3.9.4 Associated logs

None

1.4.3.10 Register - G711MUCN**1.4.3.10.1 Register description**

Register G711MUCN (G.711 MuLaw Connections) provides count for total number of G.711 MuLaw codec connections handled by a particular MG4K-IP/IW-IP node.

The MG4K-IP/IW-IP uses industry standard G.711 codec as a default codec for Mu-law and A-law at 10 and 20 milliseconds, to encode and decode TDM to and from packets transmitted via RTP over UDP over IP.

ITU-T G.711 is a standard to represent 8 bit compressed pulse code modulation (PCM) samples for signals of voice frequencies, sampled at the rate of 8000 samples/second. G.711 encoder will create a 64 Kbps bitstream. This standard has two forms, A-Law and μ -Law.

1.4.3.10.2 Register G711MUCN release history update

Register G711MUCN is new in SN08.

1.4.3.10.3 Associated registers

None

1.4.3.10.4 Associated logs

None

1.4.3.11 Register - G711ACN

1.4.3.11.1 Register description

Register G711ACN (G.711 A-Law Connections) provides count for total number of G.711 A-Law codec connections handled by a particular MG4K-IP/IW-IP node.

1.4.3.11.2 Register G711ACN release history update

Register G711ACN is new in SN08.

1.4.3.11.3 Associated registers

None

1.4.3.11.4 Associated logs

None

1.4.3.12 Register - G729CN

1.4.3.12.1 Register description

Register G729CN (G.729 Connections) provides count for total number of G.729 connections handled by a particular MG4K-IP/IW-IP node.

1.4.3.12.2 Register G729CN release history update

Register G729CN is new in SN08.

1.4.3.12.3 Associated registers

None

1.4.3.12.4 Associated logs

None

1.4.3.13 Register - CCDCN

1.4.3.13.1 Register description

Register CCDCN (Clear Channel Data Connections) provides count for total number of 64K Clear Channel Data (CCD) Connections handled by a particular MG4K-IP/IW-IP node.

Clear Channel Data (CCD) calls are raw data streams instead of digitized 8KHz audio.

1.4.3.13.2 Register CCDCN release history update

Register CCDCN is new in SN08.

1.4.3.13.3 Associated registers

None

1.4.3.13.4 Associated logs

None

1.4.3.14 Register - T38CN**1.4.3.14.1 Register description**

Register T38CN (T.38 Connections) provides count for total number of T.38 connections handled by a particular MG4K-IP/IW-IP node.

T.38 Protocol is used to transmit fax calls over the IP network.

1.4.3.14.2 Register T38CN release history update

Register T38CN is new in SN08.

1.4.3.14.3 Associated registers

None

1.4.3.14.4 Associated logs

None

1.4.3.15 Register - VBDCN**1.4.3.15.1 Register description**

Register VBDCN (Voice Band Data Connections) provides count for total number of Voice Band Data (VBD) Connections handled by a particular MG4K-IP/IW-IP node.

VBD will allow pass-through of inband data over established voice channels for packet networks.

1.4.3.15.2 Register VBDCN release history update

Register VBDCN is new in SN08.

1.4.3.15.3 Associated registers

None

1.4.3.15.4 Associated logs

None

1.4.3.16 Register - RF2833CN**1.4.3.16.1 Register description**

Register RF2833CN (RFC2833 Connections) provides count for total number of RFC2833 connections handled by a particular MG4K-IP/IW-IP node.

The RFC2833 is used for tone transmission in all codec types. The speech compression can greatly impair the ability of downstream systems to recognize in-band DTMF tones. RFC2833 provides solution for this problem.

The special RTP data packets will be transmitted instead of generating the tones at the ingress gateway. These RTP packets will instruct the downstream gateway to generate the appropriate tones.

1.4.3.16.2 Register RF2833CN release history update

Register RF2833CN is new in SN08.

1.4.3.16.3 Associated registers

None

1.4.3.16.4 Associated logs

None

1.4.3.17 Register - TXRTPPK, TXRTPPK2

1.4.3.17.1 Register description

Register TXRTPPK (Transmitted RTP Packets) provides count for total number of RTP packets transmitted from a MG4K-IP/IW-IP node. Register TXRTPPK2 is an extension register for TXRTPPK.

1.4.3.17.2 Register TXRTPPK release history update

Register TXRTPPK is new in SN08.

1.4.3.17.3 Associated registers

None

1.4.3.17.4 Associated logs

None

1.4.3.18 Register - RXRTPPK, RXRTPPK2

1.4.3.18.1 Register description

Register RXRTPPK (Received RTP Packets) provides count for total number of RTP packets received for a MG4K-IP/IW-IP node. Register RXRTPPK2 is an extension register for RXRTPPK.

1.4.3.18.2 Register RXRTPPK release history update

Register RXRTPPK is new in SN08.

1.4.3.18.3 Associated registers

None

1.4.3.18.4 Associated logs

None

1.4.3.19 Register - TXG711PK, TXG711P2

1.4.3.19.1 Register description

Register TXG711PK (Transmitted G.711 Connection Packets) provides count for total number of RTP packets transmitted for G.711 connections handled by a particular MG4K-IP/IW-IP node. Register TXG711P2 is an extension register for TXG711PK.

1.4.3.19.2 Register TXG711PK release history update

Register TXG711PK is new in SN08.

1.4.3.19.3 Associated registers

None

1.4.3.19.4 Associated logs

None

1.4.3.20 Register - RXG711PK, RXG711P2

1.4.3.20.1 Register description

Register RXG711PK (Received G.711 Connection Packets) provides count for total number of RTP packets received for G.711 connections handled by a particular MG4K-IP/IW-IP node. Register RXG711P2 is an extension register for RXG711PK.

1.4.3.20.2 Register RXG711PK release history update

Register RXG711PK is new in SN08.

1.4.3.20.3 Associated registers

None

1.4.3.20.4 Associated logs

None

1.4.3.21 Register - TXG729PK, TXG729P2

1.4.3.21.1 Register description

Register TXG729PK (Transmitted G.729 Connection Packets) provides count for total number of RTP packets transmitted for G.729 connections handled by a particular MG4K-IP/IW-IP node. Register TXG729P2 is an extension register for TXG729PK.

1.4.3.21.2 Register TXG729PK release history update

Register TXG729PK is new in SN08.

1.4.3.21.3 Associated registers

None

1.4.3.21.4 Associated logs

None

1.4.3.22 Register - RXG729PK, RXG729P2

1.4.3.22.1 Register description

Register RXG729PK (Received G.729 Connection Packets) provides count for total number of RTP packets received for G.729 connections handled by a particular MG4K-IP/IW-IP node. Register RXG729P2 is an extension register for RXG729PK.

1.4.3.22.2 Register RXG729PK release history update

Register RXG729PK is new in SN08.

1.4.3.22.3 Associated registers

None

1.4.3.22.4 Associated logs

None

1.4.3.23 Register - TXCCDPK

1.4.3.23.1 Register description

Register TXCCDPK (Transmitted Clear Channel Data Connection Packets) provides count for total number of RTP packets transmitted for Clear Channel Data connections handled by a particular MG4K-IP/IW-IP node.

1.4.3.23.2 Register TXCCDPK release history update

Register TXCCDPK is new in SN08.

1.4.3.23.3 Associated registers

None

1.4.3.23.4 Associated logs

None

1.4.3.24 Register - RXCCDPK

1.4.3.24.1 Register description

Register RXCCDPK (Received Clear Channel Data Connection Packets) provides count for total number of RTP packets received for Clear Channel Data connections handled by a particular MG4K-IP/IW-IP node.

1.4.3.24.2 Register RXCCDPK release history update

Register RXCCDPK is new in SN08.

1.4.3.24.3 Associated registers

None

1.4.3.24.4 Associated logs

None

1.4.3.25 Register - TXT38PK**1.4.3.25.1 Register description**

Register TXT38PK (Transmitted T38 Connection packets) provides count for total number of packets transmitted for T.38 connections handled by a particular MG4K-IP/IW-IP node.

1.4.3.25.2 Register TXT38PK release history update

Register TXT38PK is new in SN08.

1.4.3.25.3 Associated registers

None

1.4.3.25.4 Associated logs

None

1.4.3.26 Register - RXT38PK**1.4.3.26.1 Register description**

Register RXT38PK (Received T.38 Connection Packets) provides count for total number of packets received for T.38 connections handled by a particular MG4K-IP/IW-IP node.

1.4.3.26.2 Register RXT38PK release history update

Register RXT38PK is new in SN08.

1.4.3.26.3 Associated registers

None

1.4.3.26.4 Associated logs

None

1.4.3.27 Register - TXVBDPK**1.4.3.27.1 Register description**

Register TXVBDPK (Transmitted Voice Band Data Connection Packets) provides count for total number of packets transmitted for Voice Band Data connections handled by a particular MG4K-IP/IW-IP node.

1.4.3.27.2 Register TXVBDPK release history update

Register TXVBDPK is new in SN08.

1.4.3.27.3 Associated registers

None

1.4.3.27.4 Associated logs

None

1.4.3.28 Register - RXVBDPK

1.4.3.28.1 Register description

Register RXVBDPK (Received VBD Connection Packets) provides count for total number of packets received for Voice Band Data connections handled by a particular MG4K-IP/IW-IP node.

1.4.3.28.2 Register RXVBDPK release history update

Register RXVBDPK is new in SN08.

1.4.3.28.3 Associated registers

None

1.4.3.28.4 Associated logs

None

1.4.3.29 Register - SLSUPCN

1.4.3.29.1 Register description

Register SLSUPCN (Silence Suppression Connections) provides count for total number of Silence Suppression connections handled by a particular MG4K-IP/IW-IP node.

As much as 50% of human speech consists of silence resulting from pauses between words or breaks in the conversation. Most of the codecs, such as G.723 recognize silence via a Voice Activity Detector (VAD), and transmit small Silence Descriptor (SID) packets instead of empty voice packets. Since true silence is unnatural, many receiving codecs generate background comfort noise (CNG) based on level and spectral information passed in the Silence Descriptor Packets

1.4.3.29.2 Register SLSUPCN release history update

Register SLSUPCN is new in SN08.

1.4.3.29.3 Associated registers

None

1.4.3.29.4 Associated logs

None

2: A00005562 Performance (PF)

2.1 Feature name

MG9000 ITP/ABI Overload Controls

2.2 Performance management strategy

The MG9K EM provides access to the resource datapoints used to evaluate system performance in reference to overload controls. At a high level, the operational measurements (OMs) are statistics that are collected real time on a specific resource and then saved for later viewing. This information may be used to evaluate network performance or identify resource imbalance. These statistics will be available in 15 minute chunks for a period of 24 hours. This is a total of 96 15 minute chunks. The element manager retrieves the next chunk of statistics as it becomes available. Given the definition above, the element manager would retrieve statistics from the resource every 15 minutes. This frequency is currently not a configurable parameter. It is defined by the gateway.

The OMs for a specific resource can be displayed through the MG 9000 Manager's Performance Statistics Browser GUI. In addition, the Performance Collector Formatter application collects OMs and stores them for OSS retrieval.

2.3 Performance management tools and utilities

Access to the OMs is provided using the Performance Statistics Browser on the MG9K EM. The left frame of the browser will display the performance resources within an EM, arranged in a tree format. Selecting a resource in the left frame will cause its operational measurements to be displayed in the right frame. Null performance resources may be defined to group "real" resources together. These null resources will not have operational measurements associated with them.

2.4 Performance Measurements (PM), Operational Measurements (OM), and stats

PMs for the MG9000 Mgr Overload Controls feature are listed below. The "Alarms and OMs" portion of the FN for this feature describes the OMs in detail.

- nnPmOvldRscIntervPduRatePeak
- nnPmOvldRscIntervPduRateAvg
- nnPmOvldRscIntervCbvMsgRPeak
- nnPmOvldRscIntervCbvMsgRAvg:

- nnPmOvldRscIntervConQDelPeak
- nnPmOvldRscIntervConQDelAvg
- nnPmOvldRscIntervCpuUtilPeak
- nnPmOvldRscIntervCpuUtilAvg
- nnPmOvldConnDenyIntervCount

2.4.1 PM, OM, and stats format

Component: MG9000 Overload Controls

MIB name: The SNMP based OMs listed above are from the NORTELUEMG-PERFMON-MIB.

Element Manager Screen Name: The PM Browser.

Table 1 MG9000 Overload Controls PM/OM Stats

PM Name/MIB Object Name	MibSyntax	Measurement Units
nnPmOvldRscInterval	INTEGER	N/A
nnPmOvldRscIntervPduRatePeak	INTEGER32	PDU/sec
nnPmOvldRscIntervPduRateAvg	INTEGER32	PDU/sec
nnPmOvldRscIntervCbvMsgRPeak	nnPerfMonHundreths	Msgs/sec
nnPmOvldRscIntervCbvMsgRAvg	nnPerfMonHundreths	Msgs/sec
nnPmOvldRscIntervConQDelPeak	nnPerfMonHundreths	Milliseconds
nnPmOvldRscIntervConQDelAvg	nnPerfMonHundreths	Milliseconds
nnPmOvldRscIntervCpuUtilPeak	nnPerfMonPercent	Percent Utilization
nnPmOvldRscIntervCpuUtilAvg	nnPerfMonPercent	Percent Utilization
nnPmOvldConnDenyInterval	INTEGER	N/A
nnPmOvldConnDenyIntervCount	INTEGER32	Total Count

2.5 Related documentation

A00002007: MG9K EM Overload Controls FN

3: A00006693 Performance (PF)

3.1 Feature name

XA-Core IO Capacity Monitoring Toolset

3.2 Performance management strategy

3.3 Performance management tools and utilities

The new OM group can be displayed and collected via OMSHOW interface regularly by Telcos to monitor system IO throughput.

3.4 Performance Measurements (PM), Operational Measurements (OM), and stats

This feature will provide a new OM group IOCAP.

3.4.1 PM, OM, and stats format

3.4.2 OM Group template (applies only to DMS)

New OM group IOCAP provides information on IO capacity such as utilization and utilization high watermark and IO throughput information on a per IO service type (CMIC, ETHR and AMDI).

3.4.2.1 OM description

OM group IOCAP provides one tuple per IO service type available in the office. Possible IO service types are CMIC, ETHR and AMDI.

Key field: IO_SERVICE.

Info field: none.

3.4.2.2 Release history update

The OM group is being created in CSP21 and will be patched backed to CSP20.

3.4.2.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 1 OM Group Display

IO_SERVICE	IOUTIL	IOHWM	TXMSGPS	TXSIZE	RXMSGPS
RXSIZE	IOTHRESH				

3.4.2.4 Group structure

OM group provides one tuple for each IO service type. There are 3 possible IO service types (CMIC, ETHR, AMDI).

Key field: IO_SERVICE indicates the IO service type the information is captured. Possible IO service types are CMIC, ETHR, and AMDI. The service type is displayed as a 4 character string (CMIC, ETHR, AMDI).

Info field: None.

3.4.2.5 Associated OM groups

Not applicable.

3.4.2.6 Associated functional groups

The following functional groups are associated with OM group: none

3.4.2.7 OM group registers logic flow chart

Not applicable.

3.4.3 Register (applies only to DMS)

IOHWM

3.4.3.1 Register description

IOHWM is a high watermark register holding the highest utilization value of the specified IO service type over the OM transfer period.

3.4.3.2 Register release history update

The register is being created in CSP21 and patched back to CSP20.

3.4.3.3 Associated registers

None.

3.4.3.4 Associated logs

None.

3.4.4 Register (applies only to DMS)

IOTHRESH

3.4.4.1 Register description

IOTHRESH is a peg register holding the number of one minute intervals in the transfer period the IO utilization has exceeded the value of the IO_WARNING_THRESHOLD office parm.

3.4.4.2 Register release history update

The register is being created in CSP21 and patched back to CSP20.

3.4.4.3 Associated registers

None.

3.4.4.4 Associated logs

None.

3.4.5 Register (applies only to DMS)

IOUTIL

3.4.5.1 Register description

IOUTIL is a usage register holding the average utilization value of the specified IO service type. This value is accumulated every minute and the average is calculated for every OM transfer period.

3.4.5.2 Register release history update

The register is being created in CSP21 and patched back to CSP20.

3.4.5.3 Associated registers

None.

3.4.5.4 Associated logs

None.

3.4.6 Register (applies only to DMS)

RXMSGPS

3.4.6.1 Register description

RXMSGPS is a usage register holding the average total system number of received messages of the specified IO service type. This value is accumulated every minute and the average is calculated for every OM transfer period. The unit is the number of messages per second.

3.4.6.2 Register release history update

The register is being created in CSP21 and patched back to CSP20.

3.4.6.3 Associated registers

None.

3.4.6.4 Associated logs

None.

3.4.7 Register (applies only to DMS)

RXSIZE

3.4.7.1 Register description

RXSIZE is a usage register holding the average incoming message size of the specified IO service type. This value is accumulated every minute and the average is calculated for every OM transfer period. The message size unit is in bytes.

3.4.7.2 Register release history update

The register is being created in CSP21 and patched back to CSP20.

3.4.7.3 Associated registers

None.

3.4.7.4 Associated logs

None.

3.4.8 Register (applies only to DMS)

TXMSGPS

3.4.8.1 Register description

TXMSGPS is a usage register holding the average total number of outgoing messages of the specified IO service type. This value is accumulated once every minute and the average is calculated for every OM transfer period. The unit is in number of messages per second.

3.4.8.2 Register release history update

The register is being created in CSP21 and patched back to CSP20.

3.4.8.3 Associated registers

None.

3.4.8.4 Associated logs

None.

3.4.9 Register (applies only to DMS)

TXSIZE

3.4.9.1 Register description

TXSIZE is a usage register holding the value of average size of outgoing messages of the specified IO service type. This value is accumulated once every minute and the average is calculated for every transfer period. The value unit is in bytes.

3.4.9.2 Register release history update

The register is being created in CSP21 and patched back to CSP20.

3.4.9.3 Associated registers

None.

3.4.9.4 Associated logs

None.

4: A00006780 Performance (PF)

4.1 Feature name

Trimodal Call Server OAM & P Enhancements

4.2 Performance management strategy

TRK2NET2 and TRK2NET1 OM tuples are allocated for all bearer networks provisioned in table BEARNETS, for each Trunk Group datafilled in table TRKGRP, i.e. even if there are no Trunk Members datafilled in table TRKMEM against the Trunk Group in a bearer network.

By allocating OM tuples for each bearer network of each trunk group, attempts to use a trunk group member of a particular bearer network fabric not provisioned for that trunk group will be pegged. This is done to assist in evaluating provisioning and engineering in a Trimodal Call Server environment.

4.3 Performance management tools and utilities

The TRK2NET2 and TRK2NET1 OM tuples can be seen by executing the following commands, when the value of table OFCVAR field MULTINET_DISPLAY_ACTIVE is set to Y:

- CI>omshow TRK2NET1 ACTIVE
- CI>omshow TRK2NET2 ACTIVE

4.4 Performance Measurements (PM), Operational Measurements (OM), and stats

The following is a list of the enhanced OM groups for the SN08 Trimodal Call Server feature A00006780:

- TRK2NET1
- TRK2NET2

4.4.1 PM, OM, and stats format

4.4.1.1 TRK2NET1

Component: Trunks

Performance Measurement Name: TRK2NET1

Description: TRK2NET1 OM Group provides information for per trunk group traffic analysis per bearer network. The OM group is modeled after group TRK. The TRK2NET1 OM group provides information on trunk traffic for each trunk group. The registers in TRK2NET1 count the following:

-
- routing attempts
 - seizure attempts
 - seize failures
 - total trunk use
 - busy state use

History:

This OM was created in SN07 under Feature ACT.A00003487.

The OM tuples creation/deletion mechanism for this OM Group is enhanced in SN08, under feature ACT.A00006780.

4.4.1.2 TRK2NET2

Component: Trunks

Performance Measurement Name: TRK2NET2

Description: TRK2NET2 OM Group provides information for per trunk group traffic analysis per bearer network. It contains extension registers for registers found in OM Group TRK2NET1.

History:

This OM was created in SN07 under Feature ACT.A00003487.

The OM tuples creation/deletion mechanism for this OM Group is enhanced in SN08, under feature ACT.A00006780.

4.4.2 TRK2NET1 OM Group

4.4.2.1 OM description

TRK2NET1 OM Group provides information for per trunk group traffic analysis per bearer network. The OM group is modeled after group TRK. The TRK2NET1 OM group provides information on trunk traffic for each trunk group. The registers in TRK2NET1 count the following:

- routing attempts
- seizure attempts
- seize failures
- total trunk use
- busy state use

The OM groups OFZ and OTS provide office-wide traffic summaries for trunks. The OM groups OFZ2NET1 and OFZ2NET2 provide office-wide per bearer network traffic summaries for trunks.

4.4.2.2 Release history update

4.4.2.2.1 Enhancement in Release SN07

TRK2NET1 OM group is new in SN07.

The addition of this new TRK2NET1 OM group is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to 'Y', then the tuples of the new TRK2NET1 OM group are displayed. If the parameter is set to 'N', then the tuples of the TRK2NET1 OM group are not displayed. The tuples of this OM group are created when the office parameter MULTINET_DISPLAY_ACTIVE is set to Y for the first time.

4.4.2.2.2 Enhancement in Release SN08

In SN07, the tuples for TRK2NET1 OM Groups are allocated only for the bearer networks of the trunk group members datafilled in table TRKMEM.

In SN08, TRK2NET1 OM tuples are allocated for all bearer networks provisioned in table BEARNETS, for each Trunk Group datafill in table TRKGRP i.e. even if there are no Trunk Members against the Trunk Group in a bearer network

- When a bearer network is datafilled in table BEARNETS, a TRK2NET1 OM tuple is added for every Trunk Group datafilled in table TRKGRP.
- When a bearer network is deleted from table BEARNETS, all corresponding TRK2NET1 OM tuples are deleted. This functionality is delivered in SN07.
- When a Trunk Group is added in table TRKGRP, a TRK2NET1 OM tuple is added for every bearer network datafilled in table BEARNETS.
- When a Trunk Group is deleted from table TRKGRP, all corresponding TRK2NET1 OM tuples are deleted.
- TRK2NET1 OM tuple creation and deletion does not happen during tuple addition/deletion in tables TRKOPTS and TRKMEM.
- The TRK2NET1 OM group is ignored by table OMKEYORD.

4.4.3 TRK2NET2 OM Group

4.4.3.1 OM description

TRK2NET2 OM Group provides information for per trunk group traffic analysis per bearer network. It contains extension registers for registers found in the OM Group TRK2NET1.

4.4.3.2 Release history update

4.4.3.2.1 Enhancements in Release SN07

TRK2NET2 OM group is new in SN07.

The addition of this new TRK2NET2 OM group is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to 'Y', then the new TRK2NET2 OM group is displayed. If the parameter is set to 'N', then the TRK2NET2 OM group is not displayed.

4.4.3.2.2 Enhancements in Release SN08

In SN07, the tuples for TRK2NET2 OM Groups are allocated only for the bearer networks of the trunk group members data filled in table TRKMEM.

In SN08, TRK2NET2 OM tuples are allocated for all bearer networks provisioned in table BEARNETS, for each Trunk Group datafill in table TRKGRP i.e. even if there are no Trunk Members against the Trunk Group in a bearer network

- When a bearer network is datafilled in table BEARNETS, a TRK2NET2 OM tuple is added for every Trunk Group datafilled in table TRKGRP.
- When a bearer network is deleted from table BEARNETS, all corresponding TRK2NET2 OM tuples are deleted. This functionality is delivered in SN07.
- When a Trunk Group is added in table TRKGRP, a TRK2NET2 OM tuple is added for every bearer network datafilled in table BEARNETS.
- When a Trunk Group is deleted from table TRKGRP, all corresponding TRK2NET2 OM tuples are deleted.
- TRK2NET2 OM tuple creation and deletion does not happen during tuple addition/deletion in tables TRKOPTS and TRKMEM.
- The TRK2NET1 OM group is ignored by table OMKEYORD.

4.4.4 Special Scenarios(SN08 Enhancement)

- Before associating TRK2NET2 and TRK2NET1 OM tuples against a bearer network (when a table BEARNETS tuple is added) or associating TRK2NET2 and TRK2NET1 OM tuples against a Trunk Group (when adding a table TRKGRP tuple):
 - A check is made in the software to check if there is space left to be able to associate the required number of OM tuples (refer to Limitation Section in FN)
 - If the above check fails i.e. there is not enough space left, then not even a single TRK2NET2 or TRK2NET1 OM tuple is associated with the bearer network or Trunk Group (as the case may be)
 - An appropriate Warning is given to the user (refer to Limitation Section of the FN document). This tells the user how much space is needed and how much of the space is actually available.

-
- This gives the user an option of freeing up required space, given that the user knows the requirement. The user can free up space as per his/her discretion, by deleting table BEARNETS or TRKGRP tuples.
 - The SN08 Enhancement gives the user an option of doing a NIL Change on the BEARNETS or TRKGRP tuple (during the addition of which the user faced the OM tuple space availability issue). This particular enhancement causes the Feature code to re-attempt trying to associate the required number of TRK2NET2/TRK2NET1 OM tuples against the bearer network or Trunk Group (as the case maybe). This re-attempt would succeed, if the user has freed up space by deleting TRKGRP or BEARNETS tuples before attempting the NIL Change.
 - NIL Change operation on a tuple means trying a REPLACE command on the tuple with none of the fields of TUPLE having a changed value.
 - Note: The above enhancement in software of re-attempting the association of the OM tuples, is run even if it is a normal tuple CHANGE operation and not a NIL Change operation only.
 - When an ONP is done from a SN07 or SN08 load (without feature code) to a SN08 load (with feature code): then the TRK2NET2 and TRK2NET1 OM tuples found associated with bearer networks and Trunk Groups *will be different* from those associated on the DUMP side. *In some cases, TRK2NET2/TRK2NET1 OM tuples existing on the DUMP side for a bearer network and Trunk Group, will be found missing after TABXFR on the RESTORE side.*
 - An example is:-
 - When we have 5 bearer networks provisioned on the DUMP side and 4000 Trunk Groups datafilled in the TRKGRP.
 - Without the feature code, we have TRK2NET2/TRK2NET1 OM tuples associated with each of the bearer networks *only* for those Trunk Groups (say there are 4000 Trunk Groups) which have Members physically belonging to a bearer network. Due to this, the Max OM tuple limit per OM Group is not hit.
 - Now when TABXFR of table BEARNETS happens to load with the feature code: when the first 4 BEARNETS tuples are TABXFRed, $4 * 4000 = 16000$ (Max OM tuple limit per OM Group) is reached for TRK2NET2 and TRK2NET1 OM Groups.
 - When the 5th table BEARNETS tuple is TABXFRed, the feature code detects that there is no space to associate even a single TRK2NET2/TRK2NET1 OM tuple against the bearer network. Hence on the RESTORE side, not even a single TRK2NET2/TRK2NET1 OM tuple exists for the bearer network corresponding to the 5th table BEARNETS tuple.

-
- Table OMKEYORD will ignore the TRK2NET1 and TRK2NET2 OM groups during an ONP. This means that table OMKEYORD cannot be used to reorder the TRK2NET1 and TRK2NET2 tuples for EADAS. This will also help with limiting the impact of the restore time due to the number of tuples which are created.
 - During ONP, the HOLE tuples from the OM groups TRK2NET1 and TRK2NET2 are not transferred to the Table OMKEYORD. TRK2NET1 and TRK2NET2 related OMKEYORD tuples are ignored.

5: A00007000 Performance (PF)

5.1 Feature name

GigE Network Interface

5.2 Performance management strategy

This follows the existing MG9K EM performance strategy where in the data is collected 15 or 5/30 minutes for 96 intervals.

5.3 Performance management tools and utilities

The performance data can be viewed from Performance browser.

5.4 Performance Measurements (PM), Operational Measurements (OM), and stats

5.4.1 OM Statistics

The new OM performance parameters introduced in this feature are

5.4.1.1 Errored Seconds

Component: OM Statistics

Performance measurement name: Errored Seconds

The Performance measurement description: counter associated with Errored Seconds

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.2 Severely Errored Seconds

Component: OM Statistics

Performance measurement name: Severely Errored Seconds

Performance measurement description: The counter associated with SES

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.3 Unavailable seconds

Component: OM Statistics

Performance measurement name: Unavailable Seconds

Performance measurement description: The counter associated with UAS

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.4 Optical Power Transmit

Component: OM Statistics

Performance measurement name:Optical Power Transmit

Performance measurement description: The counter associated with Optical Power Transmit

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.5 Optical Power Receive

Component: OM Statistics

Performance measurement name:Optical Power Receive

Performance measurement description: The counter associated with Optical Power Receive

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.6 Transmit Bias Current

Component: OM Statistics

Performance measurement name:Transmit Bias Current

Performance measurement description: The counter associated with Transmit Bias Current

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.7 Temperature

Component: OM Statistics

Performance measurement name:Temperature

Performance measurement description: The counter associated with Temperature

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.8 Voltage

Component: Generic OM

Performance measurement name: Voltage

Performance measurement description: The counter associated with Voltage

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.9 nnGLinkCurrTxFifoOverruns

Component: Generic OM

Performance measurement name: Number of Tx Fifo Overruns

Performance measurement description: The counter associated with Number of Tx Fifo Overruns

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.10 nnGLinkCurrTxFifoUnderruns

Component: Generic OM

Performance measurement name: Number of Tx Fife Underruns

Performance measurement description: The counter associated with Number of Tx Fifo Underruns

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.11 nnGLinkCurrTxBytesOverflow

Component: Generic OM

Performance measurement name: Number of Tx Bytes OverFlow

Performance measurement description: The counter associated with Number of Tx bytes overflow

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.12 nnGLinkCurrTxBytes

Component: Generic OM

Performance measurement name: Number of Tx Bytes

Performance measurement description: The counter associated with Number of Tx bytes

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.13 nnGLinkCurrRxFcsFail

Component: Generic OM

Performance measurement name: Number of Rx FCS Fails

Performance measurement description: The counter associated with Number of Rx fails

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.14 nnGLinkCurrRxFcsFail

Component: Generic OM

Performance measurement name: Number of Rx FCS Fails

Performance measurement description: The counter associated with Number of Rx fails

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.15 nnGLinkCurrRxLenTypeFail

Component: Generic OM

Performance measurement name: Number of Rx Len type fail

Performance measurement description: The counter associated with Number of Len type fails

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.16 nnGLinkCurrRxGoodPause

Component: Generic OM

Performance measurement name: Number of Rx Good Pause

Performance measurement description: The counter associated with Number of Rx good pause

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.17 nnGLinkCurrRxGoodPause

Component: Generic OM

Performance measurement name: Number of Rx Good Pause

Performance measurement description: The counter associated with Number of Rx good pause

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.18 nnGLinkCurrRxBadOpCntlFrames

Component: Generic OM

Performance measurement name: Number of Rx bad op cantle frames

Performance measurement description: The counter associated with Number of Rx bad OpCntl frames

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.1.19 nnGLinkCurrRxPauseFrames

Component: Generic OM

Performance measurement name: Number of Rx control frames

Performance measurement description: The counter associated with Number of Rx control frames

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - OM Statistics

5.4.2 Ethernet OM

5.4.2.1 AlignErr

Component: Ethernet OM

Performance measurement name: Number of Alignment Errors

Performance measurement description: The counter associated with AlignErr

Collection Interval: NA

Element Manager Screen Name: GIGE Card/Port xx - Ethernet OM Statistics

5.4.2.2 FcsErr

Component: FcsErr

Performance measurement name: Number of FCS Errors

Performance measurement description: The counter associated with FcsErr

Collection Interval: NA

Element Manager Screen Name: GIGE Card/Port xx - Ethernet OM Statistics

5.4.2.3 Internalmacrxerr

Component: Ethernet OM

Performance measurement name: Number of Internal MAC Receive Errors

Performance measurement description: The counter associated with Internalmacrxerr

Collection Interval: NA

Element Manager Screen Name: GIGE Card/Port xx - Ethernet OM Statistics

5.4.2.4 Frtoolongs

Component: Ethernet OM

Performance measurement name: Number of Frame Too Longs

Performance measurement description: The counter associated with Frtoolongs

Collection Interval: NA

Element Manager Screen Name: GIGE Card/Port xx - Ethernet OM Statistics

5.4.2.5 Internalmactxerr

Component: Ethernet OM

Performance measurement name: Number of Internal MAC TX Errors

Performance measurement description: The counter associated with Internalmactxerr

Collection Interval: NA

Element Manager Screen Name: GIGE Card/Port xx - Ethernet OM Statistics

5.4.2.6 Symbolerr

Component: Ethernet OM

Performance measurement name: Number of Symbol Errors

Performance measurement description: The counter associated with Symbolerr

Collection Interval: NA

Element Manager Screen Name: GIGE Card/Port xx - Ethernet OM Statistics

5.4.2.7 Inpausefr

Component: Ethernet OM

Performance measurement name: Number of Inpause Frames

Performance measurement description: The counter associated with Inpausefr

Collection Interval: NA

Element Manager Screen Name: GIGE Card/Port xx - Ethernet OM Statistics

5.4.2.8 Outpausefr

Component: Ethernet OM

Performance measurement name: Number of Outpause Frames

Performance measurement description: The counter associated with Outpausefr

Element Manager Screen Name: MG9kEM Performance Browser

Collection Interval: NA

Element Manager Screen Name: GIGE Card/Port xx - Ethernet OM Statistic

5.4.3 RMON Data

5.4.3.1 etherStatsDropEvents

Component: RMON

Performance measurement name: Number of Drop Events

Performance measurement description: The current data associated with etherStatsDropEvents

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON Statistics

5.4.3.2 etherStatsBroadcastPkts

Component: RMON

Performance measurement name: Number of Broadcast Packets

Performance measurement description: The counter data associated with etherStatsBroadcastPkts

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON Statistics

5.4.3.3 etherStatsMulticastPkts

Component: RMON

Performance measurement name: Number of Multicast Packets

Performance measurement description: The counter associated with etherStatsMulticastPkts

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON Statistics

5.4.3.4 etherStatsCRCAlignErrors

Component: RMON

Performance measurement name: Number of CRC Alignment Errors

Performance measurement description: The counter associated with etherStatsCRCAlignErrors

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON Statistics

5.4.3.5 etherStatsUndersizePkts

Component: RMON

Performance measurement name: Number of Undersize Packets

Performance measurement description: The counter associated with etherStatsUndersizePkts

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON Statistics

5.4.3.6 etherStatsOversizePkts

Component: RMON

Performance measurement name: Number of Oversize Packets

Performance measurement description: The counter associated with etherStatsOversizePkts

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON Statistics

5.4.3.7 etherStatsFragments

Component: RMON

Performance measurement name: Number of Fragments

Performance measurement description: The counter associated with etherStatsFragments

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON Statistics

5.4.3.8 etherStatsJabbers

Component: RMON

Performance measurement name: Number of Jabbers

Performance measurement description: The counter associated with etherStatsJabbers

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON Statistics

5.4.3.9 etherStatsCollisions

Component: RMON

Performance measurement name: Number of Collisions

Performance measurement description: The counter associated with etherStatsCollisions

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON Statistics

5.4.4 RMON HC Statistics

5.4.4.1 HC Overflow Packets

Component: RMON HC

Performance measurement name: Number of HC overflow packets

Performance measurement description: The counter associated with HC Overflow Packets

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON HC Statistics

5.4.4.2 Packets Received

Component: RMON HC

Performance measurement name: Number of packets received

Performance measurement description: The counter associated with number of packets received

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON HC Statistics

5.4.4.3 Overflow octets

Component: RMON HC

Performance measurement name: Number of overflow octets

Performance measurement description: The counter associated with HC number of Overflow octets

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON HC Statistics

5.4.4.4 Octets of data received

Component: RMON HC

Performance measurement name: Number of octets of data received

Performance measurement description: The counter associated with number of octets of data received.

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON HC Statistics

5.4.4.5 etherHistoryOctets

Component: RMON HC

Performance measurement name: Number of ether history octets

Performance measurement description: The counter associated with number of ether history octets received.

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON HC History Statistics

5.4.4.6 etherHistoryPkts

Component: RMON HC

Performance measurement name: Number of ether history packets

Performance measurement description: The counter associated with number of ether history packets received.

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON HC History Statistics

5.4.4.7 etherHistoryUtilization

Component: RMON HC

Performance measurement name: Number of ether history utilization

Performance measurement description: The counter associated with number of history utilization received.

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: GIGE Card/Port xx - RMON HC History Statistics

5.4.5 SMON Statistics

5.4.5.1 VLAN ID

Component: SMONVlanStats

Performance measurement name: VLAN ID

Performance measurement description: The VLAN ID

Element Manager Screen Name: VLANxx/SMONVLANStatistics

5.4.5.2 Total number Packets

Component: SMONVlanStats

Performance measurement name: Total number Packets

Performance measurement description: The counter associated with Total number Packets

Element Manager Screen Name: VLANxx/SMONVLANStatistics

5.4.5.3 Total Number of HC Packets

Component: SMONVlanStats

Performance measurement name: Total Number of HC Packets

Performance measurement description: The counter associated with Total Number of HC Packets

Element Manager Screen Name: VLANxx/SMONVLANStatistics

5.4.5.4 Create Time

Component: SMONVlanStats

Performance measurement name: Create time

Performance measurement description: create time

Element Manager Screen Name: VLANxx/SMONVLANStatistics

5.4.5.5 Total Number of Octets

Component: SMONVlanStats

Performance measurement name:Total Number of Octets

Performance measurement description: The counter associated with Total Number of Octets

Element Manager Screen Name: VLANxx/SMONVLANStatistics

5.4.5.6 Total Number of HC Octets

Component: SMONVlanStats

Performance measurement name:Total Number of HC Octets

Performance measurement description: The counter associated with Total Number of HC Octets

Element Manager Screen Name: VLANxx/SMONVLANStatistics

5.4.5.7 Total number of non unicast packets

Component: SMONVlanStats

Performance measurement name:Total number of non unicast packets

Performance measurement description: The counter associated with Total number of non unicast packets

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: VLANxx/SMONVLANStatistics

5.4.5.8 Total number of non unicast HC octets

Component: SMONVlanStats

Performance measurement name:Total number of non unicast HC octets

Performance measurement description: The counter associated with Total number of non unicast HC octets

Element Manager Screen Name: VLANxx/SMONVLANStatistics

5.4.5.9 Total number of non unicast octet

Component: SMONVlanStats

Performance measurement name: Total number of non unicast octet

Performance measurement description: The counter associated with Total number of non unicast octet

Element Manager Screen Name: VLANxx/SMONVLANStatistics

Total number of non unicast over flow octet

Total number of non unicast over flow octet

5.4.5.10 Total Number of Non Unicast Over Flow Octet

Component: SMONVlanStats

Performance measurement name: Total number of non unicast over flow octet

Performance measurement description: The counter associated with Total number of non unicast over flow octet

Collection Interval: 15 or 5/30 mins

Element Manager Screen Name: VLANxx/SMONVLANStatistics

5.4.5.11 Total number of non unicast HC octet

Component: SMONVlanStats

Performance measurement name: Total number of non unicast HC octet

Performance measurement description: The counter associated with Total number of non unicast HC octet

Element Manager Screen Name: VLANxx/SMONVLAN Statistics

5.4.6 SMON Priority Statistics**5.4.6.1 Total number of packets**

Component: SMON Priority Statistics

Performance measurement name: Total number of packets

Performance measurement description: It displays the total number of packets

Element Manager Screen Name: VLANxx/SMON Priority Statistics

5.4.6.2 Total number of overflow packets

Component: SMON Priority Statistics

Performance measurement name: Total number of packets

Performance measurement description: It displays the total number of overflow packets

Element Manager Screen Name: VLANxx/SMON Priority

5.4.6.3 Total number of HC packets

Component: SMON Priority Statistics

Performance measurement name: Total number of HC packets

Performance measurement description: It displays the total number of HC packets

Element Manager Screen Name: VLANxx/SMON Priority Statistics

5.4.6.4 Total number of octets

Component: SMON Priority Statistics

Performance measurement name: Total number of octets

Performance measurement description: It displays the total number of octets

Element Manager Screen Name: VLANxx/SMON Priority Statistics

5.4.6.5 Total number of overflow octets

Component: SMON Priority Statistics

Performance measurement name: Total number of octets

Performance measurement description: It displays the total number of overflow octets

Element Manager Screen Name: VLANxx/SMON Priority Statistics

5.4.6.6 Total number of HC octets

Component: SMON Priority Statistics

Performance measurement name: Total number of HC octets

Performance measurement description: It displays the total number of HC octets

Element Manager Screen Name: VLANxx/SMON Priority Statistics

6: A00007074 Performance (PF)

6.1 Feature name

GigE Link Maintenance

6.2 Performance management strategy

Performance for each of the GigE links will be monitored using OM counts. These counts will be provided through the OM collector.

6.3 Performance management tools and utilities

OM will be available from the EM and OM collector stream. Details of the EM can be found in the documentation for A00007000.

6.4 Performance Measurements (PM), Operational Measurements (OM), and stats

The following table indicates the OMs that will be collected, their correlation in the MIBs and the hardware register they are being pulled from.

6.4.1 PM, OM, and stats format

Table 1: OM collector table

From Table	Field	size	Hardware counter
EtherHistoryEntry	etherHistoryDropEvents	Counter32	rxFifoOverruns
EtherHistoryEntry	etherHistoryBroadcastPkts	Counter32	?
EtherHistoryEntry	etherHistoryMulticastPkts	Counter32	?
EtherHistoryEntry	etherHistoryCRCAAlignErrors	Counter32	?
EtherHistoryEntry	etherHistoryUndersizePkts	Counter32	rxUndersize
EtherHistoryEntry	etherHistoryOversizePkts	Counter32	rxOversize
EtherHistoryEntry	etherHistoryFragments	Counter32	rxFragmented
EtherHistoryHighCapacityEntry	etherHistoryHighCapacityOverflowPkts	Integer32	rxFrames

EtherHistoryHighCapacityEntry	etherHistoryHighCapacityPkts	Integer64	rxFrames
EtherHistoryHighCapacityEntry	etherHistoryHighCapacityOverflowOctets	Integer32	rxBytes
EtherHistoryHighCapacityEntry	etherHistoryHighCapacityOctets	Integer64	rxBytes
nnGLinkOmCurrenTable	txFifoOverruns	Integer32	txFifoOverruns
nnGLinkOmCurrenTable	txFifoUnderruns	Integer32	txFifoUnderruns
nnGLinkOmCurrenTable	txBytesOverFlow	Integer32	txBytesOverFlow
nnGLinkOmCurrenTable	txBytes	Integer64	txBytes
nnGLinkOmCurrenTable	rxFcsFail	Integer32	rxFcsFail
nnGLinkOmCurrenTable	rxLenTypeFail	Integer32	rxLenTypeFail
nnGLinkOmCurrenTable	rxGoodPause	Integer32	rxGoodPause
nnGLinkOmCurrenTable	rxBadOpcodeCntlFrames	Integer32	rxBadOpcodeCntlFrames
nnGLinkOmCurrenTable	rxControlFrames	Integer32	rxControlFrames
nnGLinkOmCurrenTable	txPauseFrames	Integer32	txPauseFrames

6.4.2 Performance File (CSV, SSV, XML) Format

Detailed in the documentation for the OM collector feature.

6.4.3 OM Group template (applies only to DMS)

Not Applicable

6.4.4 Register (applies only to DMS)

Not Applicable

7: A00007120 Performance (PF)

7.1 Feature name

Packet Media Anchor for DPT

7.2 Performance management strategy

The Packet Media Anchor (PKTMA) performance management provides the customer a means to monitor the PKTMA resources. To assist the customer with network engineering, the system monitors:

- Anchored call attempts
- Failed anchored call attempts
- Maximum anchored call attempts (High Water Mark)

A new XPKT340 log will be introduced for reporting a variety of Gateway, Gateway Controller, and PKTMA resource problems. The infrastructure for such logs will be constructed.

7.3 Performance management tools and utilities

When a Packet Media Anchor is provisioned in table SERVSINV, the PKTMA Operational Measurement group can be used to monitor the anchor resource usage. To view the group data the OMSHOW CI command may be used.

Example: OMSHOW PKTMA ACTIVE

7.4 Performance Measurements (PM), Operational Measurements (OM), and stats

PKTMA presents usage counts for Dynamic Packet Trunk Anchor resources.

7.4.1 PM, OM, and stats format

Performance Measurement Name: PKTMA

Performance Measurement Description: Presents usage counts on a GWC basis

Performance Registers: PMAREQST, PMAFLNR, PMAHWM

History: Created in SN08/GWC11

7.4.2 OM Group template (applies only to DMS)

7.4.2.1 OM description

PKTMA

Packet Media Anchor

7.4.2.2 Release history update

The OM group is new in SN08.

7.4.2.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 1 OM Group Display

PMAREQST PMAFLNRPMAHWM

7.4.2.4 Group structure

OM group provides 1 tuple for each GWC provisioned with PKTMA resources.

Key field: Integer.

The PKTMA anchor number derived from datafill order

Info field: PKTMA_OM_INFO

Presents the GWC number and the maximum number of anchored calls supported by the GWC resources.

Example:

1 GWC 20 125

7.4.2.5 Associated OM groups

None.

7.4.2.6 Associated functional groups

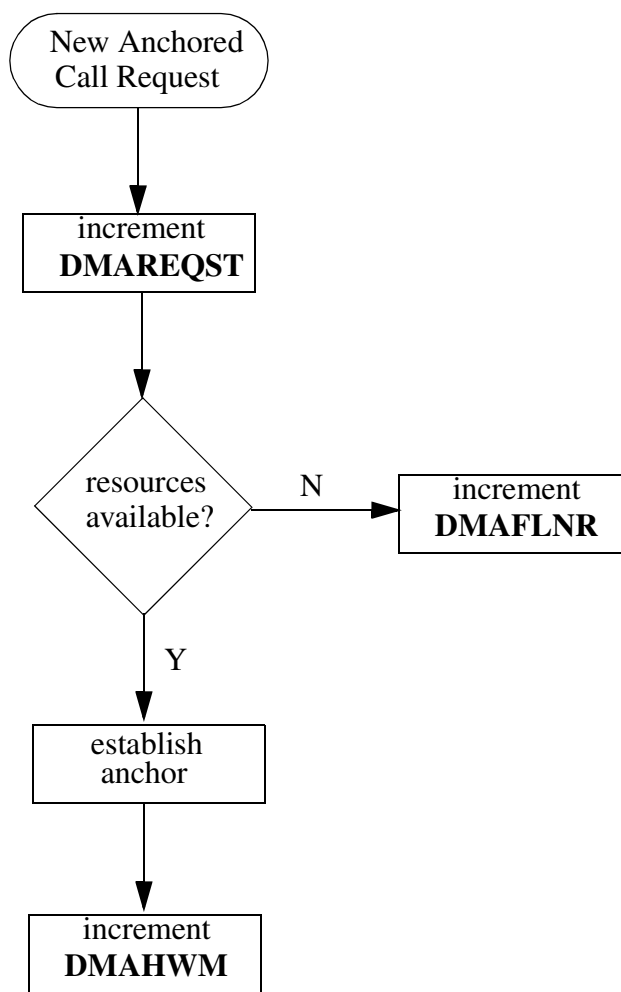
The following functional groups are associated with OM group: None.

7.4.2.7 Associated functionality codes

Table 1 Functionality codes associated with OM group

Functionality	Code
NA	
NA	

7.4.2.8 OM group registers logic flow chart



7.4.3 Register (applies only to DMS)

7.4.3.1 PMAREQST Register description

Register PMAREQST:

PMAREQST is a peg register to indicate the number of anchored call attempts.

7.4.3.2 Register release history update

New in SN08

7.4.3.3 Associated registers

None.

7.4.3.4 Associated logs

None.

7.4.3.5 PMAFLNR Register description

Register PMAFLNR

PMAFLNR is a peg register to indicate the number of failed anchored call attempts due to the unavailability of resources.

7.4.3.6 Register release history update

New in SN08

7.4.3.7 Associated registers

None.

7.4.3.8 Associated logs

XPKT340 log will be generated for failed anchor attempts.

7.4.3.9 PMAHWM Register description

Register PMAHWM

PMAHWM is a high water mark register to indicate the maximum number of simultaneous anchored calls.

7.4.3.10 Register release history update

New in SN08

7.4.3.11 Associated registers

None.

7.4.3.12 Associated logs

None.

7.5 New XPKT340 log.

The infra-structure to generate an XPKT340 log will be added for SN08.

7.6 Log format

An example of such a log is shown in Table 2 on page 1867.

Table 2 example XPKT340 log

RTP7 XPKT340 FEB01 11:44:12 7100 INFO PKTMA Call Failure	
Location: DPT 3	
Type: GWC	
Orig Agent: GRP	BICCINTRA1
Orig Node: DPT 3	
Term Agent: GRP	BICCINTRA2
Term Node: SPM 4	
Called Number:	9686930
CallID: 28705228	
Cause: Number 20 - No PKTMA Resources	
0000 0000 0000 0000 0300 0000 1400 0000 0000 000	
0000 0000 0000 EE5E 0000 0000 0000 0000 1C1C 1C1C	

The anticipated type of logs to be output, along with the information pertaining to them is shown in the following table. Note all messages will display hex debug information. The Debug Info field in the table lists information detailed in a more readable format from the hex data, which is displayed prior to the hex display.

Table 3 XPKT340 Log Detail

Cause	Output String on CM	Debug Info
16	Audio operation failure	IP address, signal ID, phrase ID. example specific data: Cause: Number 16 - Audio Operation Failure IP Address: 47.142.134.147 Signal ID: 51 Phrase ID: 999
17	Gateway Exception	IP address, GWC exception value, protocol error code, signal ID. example specific data: Cause: Number 17 - Gateway Exception IP Address: 47.142.134.147 Gateway Exception Value: 11 Protocol Error Code: 0 Signal ID: 0
18	No Conf Resources	None
19	No Annc resources	None

Cause	Output String on CM	Debug Info
20	No PKTMA Resources	None
21	Max Anchored Calls	None

Note: When a signal ID or phrase ID is output, only one ID is provided, so in the cases where more than one signal or phrase has been requested, the first one in the request is provided. Typically only one signal is required in a request. There are times when more than one phrase is requested in a single request, but the phrases are usually very unique so that providing the first of the phrase segments indicates which announcement phrase list has been requested and subsequently resulted in an audio failure.

7.7 Log management

When a error cause is logged which indicates an exception at the audio server, the craftsperson should check the error code (associated protocol specifications are used to determine the error cause meaning) to determine the possible mismatch. For errors indicating an unsupported request, the craftsperson should check the audio server for appropriate signal and audio provisioning.

When a GW cause is logged which indicates a missing phrase from the audio server, the craftsperson should check the announcement datafill at the call server (Table ANNAUDID, Table ANNPHLST) for the announcement phrases which contain the flagged segment ID, and these segments must be compared against those supported on the audio server. Then action must be taken by the craftsperson to either change the call server datafill to use audio segments that are supported on the audio server, or the desired audio segments must be incorporated on the audio server.

When an resource unavailable cause is logged, the craftsperson should compare the call server audio datafill (table SERVSINV) against the provisioned port data on the audio server to determine if this information matches and if the provisioned port size is large enough to provide the announcement and conferencing support needed for the office.

8: A00007213 Performance (PF)

8.1 Feature name

MG9000 5/30 Minutes OMs

8.2 Performance management strategy

In SN08, OM Collector is integrated with MG9KEM server. So, OM Collector is started, stopped and configured along with MG9KEM server.

Today, there is considerable latency between the time OM data is generated at GW and the time it is available at north-bound interfaces of MG9KEM. In order to reduce this latency, OM Collector sends a CORBA notification when it generates CSV files. It also sends a CORBA notification when it fails to generate CSV files. Note that, these notification are raised one per MG9K per collection interval.

OM Collector raise a minor alarm when it fail to collect OM file from MG9K and clears the alarm when it could again collect OM file from MG9K. Note that these alarms are generated one per MG9K per collection interval.

8.3 Performance management tools and utilities

Following are the two configurations which are related to OM data.

- Enabling/disabling OM collection for a MG9K: OM collection can be enabled for a MG9K through a check box provided in the existing GUIs, “MG900 Provisioning”, “NE Properties”. OM collector collects OM data for a MG9K, if OM collection is enabled. Refer to A00003531 CN for more details.
- Configuration of Collection intervals: This is done through the GUI “Configure Collection Interval”.

When OMC is running, if OM collection is enabled for a MG9K, OMC will start collecting OM data at the Collection intervals.

Impact of “Configuration of Collection Interval”:

Whenever Collection intervals are changed, Performance browser and OM Collector behave as follows.

- OM Collector will start collecting OMs at new collection intervals, starting from next collection interval.
- After Collection interval is changed, if User tries to collect performance data, Performance browser will collect OMs at new Sample collection interval.

When MG9KEM changes Collection interval, any data collected by OM Collector and/or Performance browser till the end of current collection interval after MG9KEM changes collection intervals, may not be accurate. Refer to section 12.4.2.1.8 in A00007213 CN for more details.

8.3.1 OM Collector configuration scripts

OM Collector is integrated with MG9KEM server. So, OM Collector is started, stopped and configured along with MG9KEM server. Following is CLUI changes;

- The scripts which were present under the directory /opt/nortel/omcltr_07/bin/ are no more available in SN08. Instead, user need to use the scripts available under the directory /opt/nortel/mg9ksrv_08/bin for the same purpose.
- Directory for CSV file is configurable. It can be configured through one of the scripts, “/opt/nortel/mg9ksrv_08/bin/mg9kconfig.sh”, “/opt/nortel/mg9ksrv_08/bin/mg9ksrv config”. Note that, the default CSV collection directory /data/oms/1 is registered for rotation. However, OMC does not do this registration. If CSV collection directory is configured to directory other than /data/oms/1, User of OMC has to register the CSV collection directory for rotation. In SN08, this capability is intended to be used for designer testing.

8.4 Performance Measurements (PM), Operational Measurements (OM), and stats

8.4.1 PM, OM, and stats format

In SN08, following information elements are changed,

- Collection Interval: Periodic collection interval may be configured to a combination of Sample and Summary intervals. In SN08, “5/30 Minutes” and “15 Minutes” are supported.
- OSS delivery (and interface) or Local only: OM Collector sends appropriate CORBA notification whenever it succeeds or fails to generate CSV file
- OSS Collection Interval: As and when CSV file is generated, OM Collector sends a CORBA notification. OSS can use appropriate mechanism to collect CSV file as and when it receives this notification.
- File Name: Directory wherein CSV are generated, are configurable in SN08.

8.4.2 Performance File (CSV, SSV, XML) Format

There is no change in SN08.

8.4.3 OM Group template (applies only to DMS)

NA

9: A00007270 Performance (PF)

9.1 Feature name

Session Server Call Processing Overload Controls

9.2 Performance management strategy

New Operational Measurement Register is added under this activity and is pegged to generate the performance history.

9.3 Performance management tools and utilities

The OMSHOW command will be used to display the OM statistics on the Session Server.

9.4 Performance Measurements (PM), Operational Measurements (OM), and stats

This activity adds a new register (OVRD_CALLS_REJECTED) to the SIPGW_CALLP om group in order to track the number of incoming calls that are rejected due to SIP Callp being in overload.

9.4.1 OM Group SIPGW_CALLP

9.4.1.1 OM Description

SIPGW_CALLP OM Group is used to track the performance statistics of the SIP Gateway Callp Application on the Session Server.

9.4.1.2 Release history update

In this release a new Register (OVRD_CALLS_REJECTED) is added to this OM Group.

9.4.1.3 Registers

SIPGWY_CALLP OM group registers display on the MAP terminal as follows:

OMGROUP: SIPGW_CALLP

TUPLE KEY: 1 TUPLE KEY NAME: SIP_TO_NGSS

Register Name	Value
IC_CALL_ATTEMPTS	0

OG_CALL_ATTEMPTS	0
CALLS_ABANDONED	0
CALLS_ANSWERED	0
CALLS_REJECTED	0
CALLS_REDIRECTED	0
OVRLD_CALLS_REJECTED	0

9.4.1.4 Associated OM groups

None

9.4.1.5 Associated functional groups

None

9.4.1.6 Associated functionality codes

Not Applicable

9.4.1.7 OM group registers logic flow chart

When the SIP Gateway Application Callp is deemed to be in overload, all incoming INVITE requests are rejected and the OVRLD_CALLS_REJECTED register is pegged.

9.4.2 Register OVRLD_CALLS_REJECTED

This register represents how many incoming INVITE requests have been rejected due to the SIP Gateway Callp being in Overload.

9.4.2.1 Register release history update

New in this release

9.4.2.2 Associated registers

None

9.4.2.3 Associated logs

SIPC310 MAJOR TBL SIP Callp NCGL=RTP7-UNIT1;Unit=1;SIPC
Overload Threshold Reached

10: A00007271 Performance (PF)

10.1 Feature name

TOPS EOL for SN08

10.2 Performance management strategy

Not applicable.

10.3 Performance management tools and utilities

Not applicable.

10.4 Performance Measurements (PM), Operational Measurements (OM), and stats

10.4.1 OM groups removed

The following TOPS OM groups have been removed as of SN07:

- DUAQ
- DUAQMOD

The following TOPS OM groups have been removed as of SN08:

- TOPSPSZ

10.4.2 OM group TOPSALT changed

The ALTVL register has been removed from the TOPSALT OM group as of SN08. The ALTDEF, ALTOFL, ALTDL, and ALTTOT registers are unchanged, although the ALTTOT register will now appear on the same line as the others.

Previously, a tuple was displayed within the OM group TOPSALT if and only if the corresponding call queue was datafilled in table OCHOSTQ. As of SN08, a tuple is displayed within TOPSALT if and only if the corresponding call queue is datafilled in OCHOSTQ **with a REROUTESEL (within the RRDATA field) of Y**. Tuples with a REROUTESEL of N do not specify an alternate host, and hence cannot generate a peg in TOPSALT for that call queue.

10.4.3 OM group TOPSOC changed

The OCMCCS register has been removed from the TOPSOC OM group as of SN08. The OCINI and OCQABN registers are unchanged.

11: A00007293 Performance (PF)

11.1 Feature name

VLAN for Gigabit Ethernet

11.2 Performance management strategy

The MG9K Element Manager provides access to per VLAN statistics. The statistics may be queried for there current value or on a historical basis. This data may be used to identify high traffic periods or used for troubleshooting purposes to verify packet transmission/reception during a specific time period.

11.3 Performance management tools and utilities

Access to the OMs is provided using the Performance Statistics Browser on the MG9K EM.

11.4 Performance Measurements (PM), Operational Measurements (OM), and stats

New OMs available on a per VLAN basis are listed below. These may be obtained from the SMON MIB table smonVlanIdStatsTable.

- smonVlanIdStatsTotalPkts - total incoming packets
- smonVlanIdStatsTotalHCPkts - total outgoing packets
- smonVlanIdStatsTotalOctets - total incoming octets
- smonVlanIdStatsTotalHCOctets - total outgoing octets

11.4.1 PM, OM, and stats format

Table 1 VLAN OMs

Field	Syntax	Unit
smonVlanIdStatsTotalPkts	Counter32	Total Count
smonVlanIdStatsTotalHCPkts	Counter32	Total Count
smonVlanIdStatsTotalOctets	Counter32	Total Count
smonVlanIdStatsTotalHCOctets	Counter32	Total Count

12: A00007327 Performance (PF)

12.1 Feature name

Media Proxy 5 and 30 minute Operational Measurements

12.2 Performance management strategy

The **Media Proxy 5 and 30 minute** OMs feature provides operational measurements for calls involving media proxies and alarms for lost communication with media proxies.

12.3 Performance management tools and utilities

The scope of this feature in perspective to performance management is to provide a method of reporting information to the end-user; all tools and utilities for the analysis and handling procedures and controlled and maintained by the IEMS.

The Operational Measurements will be collected by IEMS polling covered in feature ACTID A00007388.

12.4 Performance Measurements (PM), Operational Measurements (OM), and stats

12.4.1 Number of provisioned Media Proxies

Description: The number of currently provisioned media proxies on the GWC.

Behavior: Simply counts the number of currently provisioned media proxies on the GWC each 5 minute period. This OM is intended to complement the “number of media proxies disabled” alarm described in **optfm**.

12.4.2 Media Proxy 5 minute successful calls

Description: The number of calls that were successfully setup using this Media Proxy on this GWC in the last 5 minute OM period.

Behavior: Each time a successful call is setup involving a given Media Proxy, the specific count for that Media Proxy is incremented. At every 5 minute polling period, the count is reported and then reset to 0 to begin counting for the next period.

12.4.3 Media Proxy 30 minute successful calls

Description: The number of calls that were successfully setup using this Media Proxy on this GWC in the last 30 minute period.

Behavior: Same as 14.3.2 except reported/reset only every sixth 5 minute period (i.e. 30 minute period).

12.4.4 Media Proxy 5 minute failed calls

Description: The number of failed attempts to setup a call using this Media Proxy on this GWC in the last 5 minute OM period.

Behavior: Each time an attempt to setup a call on a given Media Proxy fails, the specific count for that Media Proxy is incremented. At every 5 minute polling period, the count is reported and then reset to 0 to begin counting for the next period.

12.4.5 Media Proxy 30 minute failed calls

Description: The number of failed attempts to setup a call using this Media Proxy on this GWC in the last 30 minute period.

Behavior: Same as 14.3.4 except reported/reset only every sixth 5 minute period (i.e. 30 minute period).

12.4.6 GWC 5 minute successful calls

Description: The number of calls that were successfully setup using any available Media Proxy on this GWC in the last 5 minute OM period.

Behavior: Each time a successful call is setup involving any Media Proxy, the count for the whole GWC incremented. At every 5 minute polling period, the count is reported and then reset to 0 to begin counting for the next period.

12.4.7 GWC 30 minute successful calls

Description: The number of calls that were successfully setup using any available Media Proxy on this GWC in the last 30 minute period.

Behavior: Same as 14.3.7 except reported/reset only every sixth 5 minute period (i.e. 30 minute period).

12.4.8 GWC 5 minute failed calls

Description: The number of failed attempts to setup a call on any available Media Proxy on this GWC in the last 5 minute OM period.

Behavior: Each time an attempt to setup a call involving any Media Proxy fails, the count for the whole GWC is incremented. A failure in this case is deemed to be a call where a media proxy is required and media proxy resources

have been requested but subsequently ends for any reason before media proxy resources are successfully allocated.

At every 5 minute polling period, the count is reported and then reset to 0 to begin counting for the next period.

12.4.9 GWC 30 minute failed calls

Description: The number of failed attempts to setup a call on any available Media Proxy on this GWC in the last 30 minute period.

Behavior: Same as 14.3.8 except reported/reset only every sixth 5 minute period (i.e. 30 minute period).

12.4.10 Important Notes

If a call fails to setup on a media proxy attempted by the GWC, it may still succeed on another media proxy. In this case, a failure will still be logged against the failing media proxy, but the call itself will be counted as successful for the GWC.

If there are no media proxies in service when one is required, a fail will be counted against the whole GWC, but not against any individual media proxy.

For the above two reasons, the total number of failed calls for the GWC will not always be equal to the sum of failed calls on all its media proxies.

12.4.11 Limitations

If a media proxy is de-provisioned, its operational measurements for the current 5 minute and 30 minute periods are lost.

13: A00007393 Performance (PF)

13.1 Feature name

Session Policy Controller

The SPC application has its own set of performance measurement although it relies on the NGSS base platform for some of its OM facilities.

13.1 Performance Management Strategy

The SPC has two types of OMs: Static and Per-Instance. Static OMs are performance measurements in the traditional sense where the counter/gauge is created when the application starts and exists for the duration of the SPC application. Per-Instance OMs are dynamic performance measurements that are captured for semi-permanent objects such as network nodes or endpoints. The number of per-instance OMs can vary. There can be up to 5000 network nodes.

13.2 Performance Management Tools and Utilities

The SPC uses the common OM Framework provided by the NGSS platform for all OM functions. The OMs can be retrieved via FTP for off-board processing. The OMSHOW utility can be used to view from the NGSS platform.

In NGSS OM subsystem, the OM system stores the OM data to CSV files. It generates 5Min files and 15~30Min files for all OMs. The 5Min files would be kept for 30 minutes and the 15~30Min files kept for 24 hours.

NGSS platform provides ftp access to the stored OM data. These files can be periodically FTP'ed to the IEMS and viewed.

15 or 30 minutes data are stored in
/opt/apps/ngsspm/stdhist

5 minutes data would be stored in
/opt/apps/ngsspm/trafhist

OM files would be named like NGSS. OMs. QoS. 2004. 5. 25_10. 15_CDT. csv

13.3 Performance Measurements (PM), Operational Measurements (OM), and Stats

13.3.1 SPC Reservation Request

This OM group records reservation request events on the SPC signaling interface

OM Item	Peg Event
IC_RESERVATION_REQUESTS	When SPC receives a incoming reservation request
RESERVATION_REQUESTS_SUCCESS	When SPC sends a reservation success response
RESERVATION_REQUESTS_FAILURE	When SPC sends a reservation failure response because resource is unavailable
RESERVATION_REQUESTS_ERROR	When SPC sends a reservation error response because the request has a incorrect context

13.3.2 SPC Commit Request

This OM group records commit request events on the SPC signaling interface

OM Item	Peg Event
IC_COMMIT_REQUESTS	When SPC receives a incoming commit request
COMMIT_REQUESTS_SUCCESS	When SPC sends a commit success response
COMMIT_REQUESTS_FAILURE	When SPC sends a commit failure response because resource is unavailable
COMMIT_REQUESTS_ERROR	When SPC sends a commit error response because the request has a incorrect context

13.3.3 SPC Deletion Request

This OM group records deletion request events on the SPC signaling interface

OM Item	Peg Event
IC_DELETION_REQUESTS	When SPC receives a incoming deletion request
DELETION_REQUESTS_SUCCESS	When SPC sends a deletion success response
DELETION_REQUESTS_ERROR	When SPC sends a deletion error response because the request has a incorrect context

13.3.4 SPC CallP

This OM group records SPC Callp OMs.

OM Item	Peg Event
NUM_HalfCall_Attempts	When SPC receives a half call attempts
NUM_HalfCall_Success	When SPC successfully sets up a half call

13.3.5 Topology Update

This OM group records topology update events in the topology manager

OM Item	Peg Event
IC_PROV_TOPO_UPDATE	When TPM receives a incoming topology update transaction from Web Prov
IC_PROV_TOPO_UPDATE_FAILURE	When a incoming topology update transaction from Web Prov is failed
IC_OSS_TOPO_UPDATE	When TPM receives a incoming topology update transaction from OSS
IC_OSS_TOPO_UPDATE_FAILURE	When a incoming topology update transaction from OSS is failed

13.3.6 CAC Request on Network Segment

This is a Per-Instance OM. This group records CAC requests to each network segment

OM Item	Peg Event
CAC_REQUESTS	When SPC sends CAC request to certain network segment
CAC_REQUESTS_SUCCESS	When CAC request to certain network segment succeeds.
CAC_REQUESTS_FAILURE	When CAC request to certain network segment fails.

13.4 Command User Interface

13.4.1 Web GUI

A web-based GUI interface is used to display the Session Policy Controller Element Manager. The Web-based graphical user tools are provided to allow the customer to define and configure topology elements and also supports SPC configuration and management. The web interface is used to perform both provisioning and maintenance activities.

13.4.2 Supported Browsers

The following operating systems are supported:

- Win2K, Win2003, Windows XP based operating system
- Solaris version 2.8, 2.9, 2.10

Supported web browsers include:

- Internet Explorer 6.0 SP1+
- Netscape 6.2.3+ with exception of Netscape 7.0

13.4.3 OSS

The SPC supports an OSS interface for topology provisioning and maintenance. The OSS interfaces are programmed to process XML command requests as service orders are sent. Separate commands are required for multiple operations. For example, in order to add multiple Network Segments, an XML command request would be needed for each Network Segment.

See the following section for security aspects of using OSS via IEMS.

The SPC XML command schema is published separately.

13.5 Security

13.5.1 Access

The SPC web GUI pages follow the same security model as other NGSS based applications. There are some privileges which can be assigned to specific craftpersons. For example, some craftsperson may only have read-only privilege, and someone with administrator privileges can write and modify the SPC configuration.

The UID/Password is used to determine the user access level, and privileges are based on user access level. The authentication of user is done during the login process. For each topology configuration command, the access privilege is checked and based on the user group. If the user does not have sufficient privilege to execute a command, an error message "Insufficient Security Privileges to perform this action" is returned as part of the response.

The SPC reuses the same set of access groups as other NGSS based applications for configuration, provisioning, and maintenance commands. The access group levels would be as follows:

- mgcadm
- mgcrw
- mgcprov
- mgcmte
- mgcro

13.5.2 CSLAN

The SPC is deployed on the CSLAN. The signaling between the CS2000-GWC and SPC takes place on a subnet of the CSLAN.

The SPC provisioning web client can be launched from IEMS. The OSS operator can log into the SPC via IEMS/SSPFS's

13.5.3 Overload Controls

The SPC provides a uniform topology provisioning interface for OSS and SPC Web GUI. This interface is responsible for creating server sockets, listening ports, setting up a new connection when a client (OSS or GUI) is connected, authenticating users, and receiving client (OSS or GUI) requests. Since the management interface can process multiple connections at the same time, the SPC implements a delayed IP address holder function to prevent any one user from abusing these connections.

For example if a user setup many connections, and once those connections are established, ignores them, closes connections, and repeatedly sets up new connections, this could waste much CPU time and other resources, and even block other applications running in the same machine.

The SPC Delayed IP Holder function detects this type of activity. If a user sets up a connection and does nothing but immediately closes connection, the client's IP address will be recorded and any connections from that IP address are rejected until the delay-time for that IP address has expired. The delay timer is configurable and default value is 10 seconds

13.5.4 Platform security

The Session Policy Controller derives Security functionality from the NGSS software platform.

In SN08, the platform provides:

- User login and password authentication
- Web based security user access via HTTPS
- Secure shell environment (SSH)

13.6 SOC and Keycoding

The SPC revenue model is based on the number of Endpoints in use on the SPC. A usage control function is used to restrict the number of Endpoint that the service provider can use.

The endpoint usage is purchased in blocks of 5000. The Endpoint block size is maximum number of end points allowed to be in use on the SPC. The endpoint block size allotment is configurable from the GUI, and its provisioning protected by set of passwords. Changes to this endpoint block size require the craftsman to enter a password. The password protection or software license key functions as a SOC. So for example, if the endpoint block size was 5000, there would be 20 passwords for each increment in block size up to 100,000. In effect every increase in block size is protected by a specific password.

OMs are used to track the number of endpoint in use over 14 days. When the endpoint count passed a threshold (a percentage of endpoint block size), alarms are raised, and the event logged. After the endpoint count exceeded the maximum endpoint block size, call attempts to additional endpoints are denied. Subsequent calls to new endpoints continue to be denied until the endpoint block size is increased. A password is required to increase the Endpoint block size. The service provider has to contact Nortel customer support to get the password.

13.7 References

13.7.1 Specifications

COPS-Dqos Specification

13.7.2 Internal Documents

NGSS Fault Management guide

IEMS Configuration guide

OSSgate Users guide

14: A00007465 Performance (PF)

14.1 Feature name

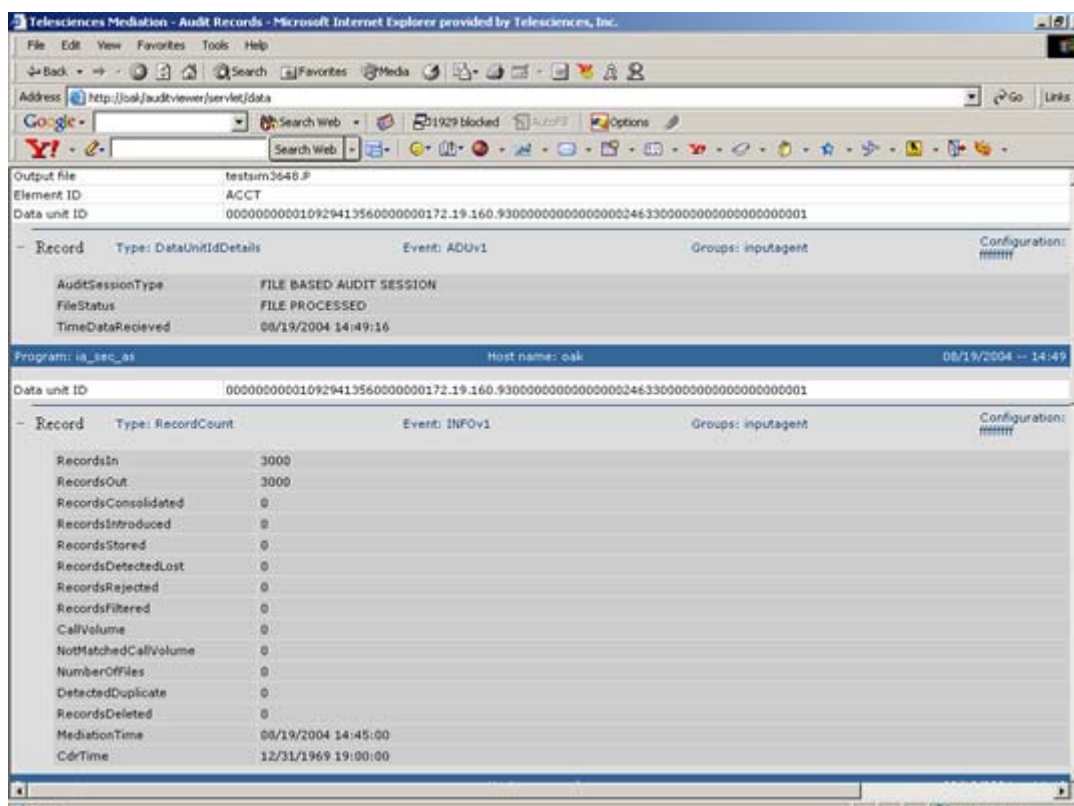
Integrated Accounting Application (IAA)

14.2 Performance management strategy

Auditing information is available for each module delivered as part of the IAA which processes Accounting and Legal Intercept Event Messages. In the case of Legal Intercept Event Messages auditing can be disabled by changing the the LI Collector's configuration file. The purpose of the auditing is to provide the end user with a summary of the number of records received and the number of records sent downstream. This serves as a way for the end user to verify that no events were lost during processing. Audits are created in 15 minute intervals by each module, with the exception of the SBA Input agents which create audit entries per file processed.

14.3 Performance management tools and utilities

The audits created by the IAA modules are stored in XML files on the system and are viewable via the Web Interface provided. Each module will audit the number of records in and out of the process for each 15 minute interval, with the exception of the SBA Input agents which create audit entries per file processed. In addition to these two counts the EMDA will also provide audits for the number of records which retries were attempted and the number of records written to a file.



14.4 Performance Measurements (PM), Operational Measurements (OM), and stats

Each module will provide the following OMs:

- Records In
- Records Out
- Channel Type (EMDA Module Only)
- Channel ID (EMDA Module Only)
- Events Sent (EMDA Module Only)
- Acknowledgements Received (EMDA Module Only)
- Events Retransmitted (EMDA Module only)
- Events Written to File (EMDA Module only)
- Events Rejected (EMDA Module Only)
- Last Event Message Header Sequence Number (EMDA Module Only)

14.4.1 PM, OM, and stats format

The OM stats (audits) are stored in an XML file, an example of which is shown below:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<!DOCTYPE applicationinfo SYSTEM "file:/telesci/application_home/./config/caching.dtd">
<applicationinfo applicationname="oak" hostname="oak" processid="24675"
programname="ia_pri_as" type="ST5000" version="1.0.0.0">

  <session datehex="1093034797" datestring="08/20/2004 16:46:37" id="Session4">
    <category name="AUDITS"/>
    <appdataunit appspecname="" create="FALSE" datasourcename=""
dataunitid="000000000010930347960000000172.19.160.930000000000000000
24675000000000000000000001">
      <tableinfo infoid="InfoId4">
        <tabletype name="RecordCount"/>
        <event name="INFOv1"/>
        <grouplist>
          <group name="inputagent"/>
        </grouplist>
        <configuration id="ffffff"/>
        <fieldlist>
          <field length="10" name="RecordsIn" show="TRUE" type="INTEGER" value="5"/>
          <field length="10" name="RecordsOut" show="TRUE" type="INTEGER" value="5"/>
          <field length="10" name="RecordsConsolidated" show="TRUE" type="INTEGER" value="0"/>
          <field length="10" name="RecordsIntroduced" show="TRUE" type="INTEGER" value="0"/>
          <field length="10" name="RecordsStored" show="TRUE" type="INTEGER" value="0"/>
          <field length="10" name="RecordsDetectedLost" show="TRUE" type="INTEGER" value="0"/>
          <field length="10" name="RecordsRejected" show="TRUE" type="INTEGER" value="0"/>
          <field length="10" name="RecordsFiltered" show="TRUE" type="INTEGER" value="0"/>
          <field length="10" name="CallVolume" show="TRUE" type="INTEGER" value="0"/>
          <field length="10" name="NotMatchedCallVolume" show="TRUE" type="INTEGER" value="0"/>
          <field length="10" name="NumberOfFiles" show="TRUE" type="INTEGER" value="0"/>
          <field length="10" name="CallDuration" show="FALSE" type="INTEGER" value="0"/>
          <field length="10" name="NotMatchedCallDuration" show="FALSE" type="INTEGER"
value="0"/>
          <field length="10" name="DetectedDuplicate" show="TRUE" type="INTEGER" value="0"/>
          <field length="10" name="RecordsDeleted" show="TRUE" type="INTEGER" value="0"/>
          <field length="20" name="MediationTime" show="TRUE" type="DATE-STANDARD"
value="08/20/2004 16:45:00"/>
          <field length="20" name="CdrTime" show="TRUE" type="DATE-STANDARD" value="12/31/
1969 19:00:00"/>
        </fieldlist>
      </tableinfo>
    </appdataunit>
  </session>
</applicationinfo>
```

15: A00008350 Performance (PF)

15.1 Feature name

Trunk group OM registers for establish bearer path failures

15.2 Performance management strategy

15.2.1 Purpose

This activity provides an enhancement to the per call failure handling in the CS2K Core by providing new OM registers. These registers will be pegged when the AUDT106¹ logs are generated irrespective of whether the log throttle occurs or not.

This activity addresses the following:

- Creating new OM registers in the existing TRK/TRNK2, TRK2NET1/TRK2NET2 OM Groups
- Pegging the new OM registers

OSS needs to be updated for these additional registers. Customers, field support and design must have a means of knowing the number of established bearer path failures. Prior to this activity, customers relied on counting the number of AUDT106 logs in order to determine the impact to connecting offices (via trunks) of call failures. As part of this activity, new OM registers will be provided which gives the exact count of the established bearer path failures. If throttling of logs is in effect resulting in suppression of AUDT106 logs, these OM registers will continue to be pegged to maintain an accurate count of the failures.

15.3 Performance management tools and utilities

PM information in general can be accessed with the following tool:

DMS OM system (i.e. OMSHOW command)

- This command can be used as follows on the CI prompt:

CI> OMSHOW <OM_GROUP> ACTIVE

This will display the registers of specified OM group for which the statistics are being gathered.

CI> OMSHOW <OM_GROUP> HOLDING

This will display the registers of specified OM group with the contents of the previous collection period.

¹The AUDT106 log is generated when a call is forced down by the release of a trunk.

15.4 Performance Measurements (PM), Operational Measurements (OM), and stats

15.4.1 Operational Measurements (OM)

This activity introduces four new registers in the existing OM groups:

- MIDFAIL in TRK OM group
- MIDFAIL2 in TRNK2 OM group
- MIDFAIL3 in TRK2NET1 OM group
- MIDFAIL4 in TRK2NET2 OM group

Note: The office parameter OFFICETYPE in table OFCSTD controls the generation of the registers for these OM Groups. These new registers will be included in all supported office types as defined for each of the OM groups.

15.4.2 Performance File (CSV, SSV, XML) Format

None

15.4.3 OM description

15.4.3.1 TRK OM Group

15.4.3.1.1 New OM register MIDFAIL in TRK OM Group

A new register MIDFAIL is introduced in the OM group TRK. This register gives the count of the established bearer path failures on a per trunk group basis. It gets pegged whenever AUDT106 logs are generated.

Table 1 TRK OM group

OM Group Name	New/Modified	Changes
TRK	Modified	New register MIDFAIL is introduced.

OM group registers display on the MAP terminal as follows:

(I)SN08 Release Change Reference Manual Standard 01.03 June 2005

15.4.3.5 Associated functionality codes

None

15.4.3.6 OM group registers logic flow chart

None

15.4.3.7 Associated logs

AUDT106

15.4.3.8 TRNK2 OM Group**15.4.3.8.1 New OM register MIDFAIL2 in TRNK2 OM Group**

A new register MIDFAIL2 is introduced in the OM group TRNK2. This register is the extension register of MIDFAIL. It gets pegged only when its associated register (MIDFAIL) overflows the maximum value.

Table 2 TRNK2 OM group

OM Group Name	New/Modified	Changes
TRNK2	Modified	New register MIDFAIL2 is introduced.

OM group registers display on the MAP terminal as follows:

Figure 2 TRNK2 OM Group

TRNK2					
CLASS: ACTIVE					
START:2004/10/06 04:30:00 WED; STOP: 2004/10/06 04:34:07 WED;					
SLOWSAMPLES: 3 ; FASTSAMPLES: 25 ;					
KEY (COMMON_LANGUAGE_NAME)					
INFO (OM2TRKINFO)					
INCATOT2		NATTMPT2	DEFLDCA2	TRU2	
SBU2		CONNECT2	TANDEM2	TOTU2	
ANSWER2		TRU2WIN2	MIDFAIL2		
51 DALI					
IC 0		0	0	0	0
		0	0	0	0
		0	0	0	
52 VTOA2WATC0					
2W 0		0	0	0	0
		0	0	0	0
		0	0	0	
53 VER90					
OG 0		0	0	0	0
		0	0	0	0
		0	0	0	

15.4.3.8.2 Release history update

The new MIDFAIL2 OM register is introduced in SN08 by the activity A00008350.

15.4.3.8.3 Associated OM groups

TRK2NET2_MIDFAIL4 and TRK_MIDFAIL are associated registers since MIDFAIL2 is the extension register of MIDFAIL.

15.4.3.8.4 Associated functional groups

Unchanged by this activity.

15.4.3.8.5 Associated functionality codes

None

15.4.3.8.6 OM group registers logic flow chart

None

15.4.3.8.7 Associated logs

None.

15.4.3.9 TRK2NET1 OM Group**15.4.3.9.1 New OM register MIDFAIL3 in the TRK2NET1 OM Group**

A new register MIDFAIL3 is introduced in the OM group TRK2NET1. This register gives the count of the established bearer path failures on a per bearer network per trunk group basis. It gets pegged whenever AUDT106 logs are generated.

Table 3 TRK2NET1 OM group

OM Group Name	New/Modified	Changes
TRK2NET1	Modified	New register MIDFAIL3 is introduced.

The OM group registers display on the MAP terminal as follows:

Figure 3 TRK2NET1 OM group

TRK2NET1

CLASS: ACTIVE

START:2004/10/06 04:35:00 WED; STOP: 2004/10/06 04:36:37 WED;

SLOWSAMPLES: 1 ; FASTSAMPLES: 10 ;

INFO (TRK2NET1_INFO)

INCAATT	PRERTEA1	NINFAIL	NATMPT
NVFLATB	GLARE1	OUTFL	TRFCU
SBSYU	MBSYU	TRKNWBLK	CNCTAT
TNDMATT	ANIOFCFL	NANF	TOTBSYU
NANSWER	INVATHCD	MAXBSY	NACCCNG
NOANSWR	MIDFAIL3		

0

TTT	NET	0	ENET	100	OG	3	1
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0
0			0		0		0

15.4.3.9.2 Release history update

The new MIDFAIL3 OM register is introduced in SN08 by the activity A00008350.

15.4.3.9.3 Associated OM groups

TRK_MIDFAIL and TRK2NET2_MIDFAIL4 are associated registers and MIDFAIL4 is the extension register.

15.4.3.9.4 Associated functional groups

Unchanged by this activity.

15.4.3.9.5 Associated functionality codes

None

15.4.3.9.6 OM group registers logic flow chart

None

15.4.3.9.7 Associated logs

AUDT106.

15.4.3.10 TRK2NET2 OM Group**15.4.3.10.1 New OM register MIDFAIL4 in the TRK2NET2 OM Group**

A new register MIDFAIL4 is introduced in the OM group TRK2NET2. This register is the extension register of MIDFAIL4. It gets pegged only when its associated register (MIDFAIL3) overflows the maximum value.

Table 4 TRK2NET2 OM group

OM Group Name	New/Modified	Changes
TRK2NET2	Modified	New register MIDFAIL4 is introduced.

OM group registers display on the MAP terminal as follows:

Figure 4 TRK2NET2 OM Group

```

TRK2NET2

CLASS: ACTIVE
START:2004/10/06 04:35:00 WED; STOP: 2004/10/06 04:39:48 WED;
SLOWSAMPLES:          3 ; FASTSAMPLES:          29 ;

INFO (TRK2NET1_INFO)
INCAATT2      NATMPT2      TRFCU2      SBSYU2
CNCTAT2      TNDMAT2      TOTBSYU2    NANSWER2
MIDFAIL4

0
      TTT NET 0 ENET  100 OG      3      1
0              0              0      0
0              0              0      0
0

1
      TTT NET 1 A1_P  100 OG      0      0
0              0              0      0
0              0              0      0
0

2
      TTT NET 2 A1_S  100 OG      0      0
0              0              0      0
0              0              0      0
0

```

15.4.3.10.2 Release history update

The new MIDFAIL4 OM register is introduced in SN08 by the activity A00008350.

15.4.3.10.3 Associated OM groups

TRNK2_MIDFAIL2 and TRK2NET1_MIDFAIL3 are associated registers since MIDFAIL4 is the extension register of MIDFAIL3.

15.4.3.10.4 Associated functional groups

Unchanged by this activity.

15.4.3.10.5 Associated functionality codes

None

15.4.3.10.6 OM group registers logic flow chart

None

15.4.3.10.7 Associated logs

None.

15.5 References

- A00003487 - Trimodal Provisioning, Logs and OMs.
- A00006777 - GWC Core LOGs for call failures.
- NTP 297-8021-814; North American DMS-100; Operational Measurements Reference Manual
- NN 10264-709; Succession Performance Management Operational Measurements Reference

Publication history-International

June 2005

Version 01.02 Standard release for (I)SN08, International. Multiple features have been updated since the preliminary release, and the following feature has been added:

- A00007790, P-phone expansion for CICM lines

January 2005

Version 01.01 Preliminary release for (I)SN08.

Table of Contents, International Features

RelDoc Introduction	1
(I) SN08 Feature Subset Cross Reference Tables: International Features	5
Feature to Functional Group Cross Reference	5
Functional Group to Feature Impacts Cross Reference	7
Functional Descriptions (FN) List	11
A00005315 Functional description (FN)	15
A00005822 Functional description (FN)	38
A00005932 Functional description (FN)	72
A00005962 Functional description (FN)	77
A00005980 Functional description (FN)	81
A00005981 Functional description (FN)	104
A00006064 Functional description (FN)	108
A00006271 Functional description (FN)	116
A00006387 Functional description (FN)	126
A00006406 Functional description (FN)	137
A00006407 Functional description (FN)	141
A00006636 Functional description (FN)	167
A00006660 Functional description (FN)	190
A00006661 Functional description (FN)	206
A00006662 Functional description (FN)	214
A00006666 Functional description (FN)	232
A00006708 Functional description (FN)	238
A00006728 Functional description (FN)	255
A00006730 Functional description (FN)	262
A00006731 Functional description (FN)	291
A00006980 Functional description (FN)	294
A00007038 Functional description (FN)	303
A00007040 Functional description (FN)	308
A00007146 Functional description (FN)	311
A00007242 Functional description (FN)	315
A00007255 Functional description (FN)	346
A00007329 Functional description (FN)	356
A00007349 Functional description (FN)	372
A00007380 Functional description (FN)	382
A00007383 Functional description (FN)	386
A00007405 Functional description (FN)	392

A00007440 Functional description (FN)	458
A00007749 Functional description (FN)	464
A00007793 Functional description (FN)	474
A00007794 Functional description (FN)	502
A00007796 Functional description (FN)	517
A00007807 Functional description (FN)	533
A00007864 Functional description (FN)	550
Configuration Management (CN) List	573
A00005315 Configuration (CN)	575
A00005962 Configuration (CN).....	588
A00005980 Configuration (CN).....	592
A00005981 Configuration (CN)	596
A00006064 Configuration (CN)	599
A00006387 Configuration (CN)	601
A00006407 Configuration (CN)	605
A00006636 Configuration (CN)	618
A00006660 Configuration (CN).....	620
A00006661 Configuration (CN).....	623
A00006662 Configuration (CN).....	638
A00006731 Configuration (CN).....	641
A00006980 Configuration (CN).....	644
A00007255 Configuration (CN).....	647
A00007349 Configuration (CN).....	652
A00007383 Configuration (CN).....	657
A00007749 Configuration (CN).....	663
A00007793 Configuration (CN).....	673
A00007807 Configuration (CN	) 680

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.

(I)SN08 Feature Subset Cross Reference Tables:

International Features

Feature to Functional Group Cross Reference

Table 1 shows 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, please refer to the FN sections.

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release (Functional Group)
Note: Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.		
A000005315.AA05	Calling Number Delivery for PRI, ISUP & CS-1	WT21
A000005822.AA10	AOC Support over H.323	GC08
A000005932.AA06	Removing Loopback Trunks in CEPT DISA calls for Remote Feature Activation	WT21, Core21
A000005962.AA06	CLIR Removal For Centrex Intragroup Calls	WT21, Core21
A000005980.AA10	GSP IN CONNECT Operation Enhancement to support RouteList Parameter	WT21, Core21
A000005981.AA09	GSP IN InitDP Operation Enhancement to support POE (Path Of Entry) Parameter	WT21
A000006064.AA12	DNSCRN Disable CCR Screening	WT21

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release (Functional Group)
A000006271.AA10	CEPT Act/Deact and Interrogation for ETSI BRI CFK, CFB/CFD K	WT21, Core21
A000006387.AA08	Support of SUSpend/RESume over ETSI ISUP QFT (QSIG Feature Transparency)	WT21
A000006406.AA09	ETSI ISUP(V1/V2 base) to J-PRI(V1/V2) UII NAK	WT21
A000006407.AA07	China ISUP Enhancement	WT21, Core21
A000006636.AA10	First ITX on Answer	WT21, XPM21
A000006660.AA09	DDRM Node Definition and Provisioning	WT21, Core21
A000006661.AA10	DDRM Node Maintenance	WT21, Core21
A000006662.AA08	DDRM Line Definition and Line Maintenance	WT21, Core21
A000006666.AA07	DDRM XPM Support and Monitoring	XPM21
A000006708.AA13	Metering on Israeli ISUP for IDDD calls	WT21
A000006728.AA05	USPc Japan NTT Protocol Support	WT21, Core21, GC08
A000006730.AA28	French NAOC on Succession CS2K	WT21, GC08
A000006731.AA08	Handle Flash on Exit	Core21
A000006980.AA10	AMA Module Code 130 Flexibility	WT21
A000007038.AA22	Intl R2 CAS Framework - Flexible Digit Map support	GC08
A000007040.AA17	Intl R2 CAS Framework - Error handling support	GC08
A000007146.AA14	CM Audits and Carrier grade for Intl. FDCP CAS on CS2K	GC08, Core21
A00007255.AA07	Dial Plan Enhancement for ETSI MWI TCAP	WT21, Core21
A00007329.AA13	International H.323 2CLI (Calling Line Identity) Support	WT21, Core21, GC08
A00007349.AA13	CPC Screening support for FDCP Trunks	WT21
A00007380.AA07	INTL H.323 GW interworking to IWSPM for DTMF Relay and T.38	GC08

Table 1 Feature to Functional Group Cross Reference

Featid	Title	Stream and release (Functional Group)
A00007383.AA11	DNH (Directory Number Hunting) enhancements: pilot DN charge and display	WT21, Core21
A00007405.AB01	Intl CAS - Korean R2 support	GC08
A00007440.AA06	ConnectToResource and PlayAnnouncement during Alert	WT21
A00007749.AA06	MG9000 ABI Support for LGCO, LGCOi	Core21
A00007790.AA08	P-phone expansion for CICM lines	WT21, Core21
A00007793.AA22	IN: SCF Id, Correlation Id and QoR Base LNP Support (DACOM)	WT21
A00007794.AA10	IN Collect Call Support (DACOM)	WT21
A00007796.AA20	Color-ring Feature (DACOM)	WT21
A00007807.AA16	Base ETSI ISUP V2 support for Dacom IN	WT21, GC08
A00007864.AA14	Pakistan ISUP tandeming on CS2Kc	WT21, GC08

Functional Group to Feature Impacts Cross Reference

Table 2 is organized alphabetically by functional group. Within each group, the features are listed numerically. 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 1 Functional Group to Feature Impacts Cross Reference

Functional Group (Functional Group)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
<i>Note:</i> Core is comprised of CCM, CNA, CSP, MSH, SHR, and UCS streams.						
WT21	A000005315.AA05	Y		Y		
GC08	A000005822.AA10	Y				
WT21, Core21	A000005932.AA06	Y				
WT21, Core21	A000005962.AA06	Y		Y		
WT21, Core21	A000005980.AA10	Y		Y		
WT21	A000005981.AA09	Y		Y		
WT21	A000006064.AA12	Y		Y		
WT21, Core21	A000006271.AA10	Y				
WT21	A000006387.AA08	Y		Y		
WT21	A000006406.AA09	Y				
WT21, Core21	A000006407.AA07	Y		Y		
WT21, XPM21	A000006636.AA10	Y		Y		
WT21, Core21	A000006660.AA09	Y		Y		
WT21, Core21	A000006661.AA10	Y		Y		
WT21, Core21	A000006662.AA08	Y		Y		
XPM21	A000006666.AA07	Y				
WT21	A000006708.AA13	Y				
WT21, Core21, GC08	A000006728.AA05	Y				
WT21, GC08	A000006730.AA28	Y				
Core21	A000006731.AA08	Y		Y		
WT21	A000006980.AA10	Y		Y		

Table 1 Functional Group to Feature Impacts Cross Reference

Functional Group (Functional Group)	Featid	FN	FM (Logs)	CN (DS, SOC)	ACC (AMA)	PF (OMS)
GC08	A000007038.AA22	Y				
GC08	A000007040.AA17	Y				
GC08, Core21	A000007146.AA14	Y				
WT21	A00007255.AA07	Y		Y		
WT21, Core21, GC08	A00007329.AA13	Y				
WT21	A00007349.AA13	Y		Y		
GC08	A00007380.AA07	Y				
WT21, Core21	A00007383.AA11	Y		Y		
GC08	A00007405.AB01	Y				
WT21	A00007440.AA06	Y				
Core21	A00007749.AA06	Y		Y		
WT21, Core21	A00007790.AA08	Y				
Core21	A00007793.AA22	Y		Y		
WT21	A00007794.AA10	Y				
WT21	A00007796.AA20	Y				
WT21, GC08	A00007807.AA16	Y		Y		
WT21, GC08	A00007864.AA14	Y				

Functional Descriptions (FN) List

Introduction

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

Featid	Title
A000005315.AA05	Calling Number Delivery for PRI, ISUP & CS-1
A000005822.AA10	AOC Support over H.323
A000005932.AA06	Removing Loopback Trunks in CEPT DISA calls for Remote Feature Activation
A000005962.AA06	CLIR Removal For Centrex Intragroup Calls
A000005980.AA10	GSP IN CONNECT Operation Enhancement to support RouteList Parameter
A000005981.AA09	GSP IN InitDP Operation Enhancement to support POE (Path Of Entry) Parameter
A000006064.AA12	DNSCRN Disable CCR Screening
A000006271.AA10	CEPT Act/Deact and Interrogation for ETSI BRI CFK, CFB/CFD K
A000006387.AA08	Support of SUSpend/RESume over ETSI ISUP QFT (QSIG Feature Transparency)
A000006406.AA09	ETSI ISUP(V1/V2 base) to J-PRI(V1/V2) UII NAK
A000006407.AA07	China ISUP Enhancement
A000006636.AA10	First ITX on Answer
A000006660.AA09	DDRM Node Definition and Provisioning
A000006661.AA10	DDRM Node Maintenance

A000006662.AA08	DDRM Line Definition and Line Maintenance
A000006666.AA07	DDRM XPM Support and Monitoring
A000006708.AA13	Metering on Israeli ISUP for IDDD calls
A000006728.AA05	USPc Japan NTT Protocol Support
A000006730.AA28	French NAOC on Succession CS2K
A000006731.AA08	Handle Flash on Exit
A000006980.AA10	AMA Module Code 130 Flexibility
A000007038.AA22	Intl R2 CAS Framework - Flexible Digit Map support
A000007040.AA17	Intl R2 CAS Framework - Error handling support
A000007146.AA14	CM Audits and Carrier grade for Intl. FDCP CAS on CS2K
A00007242	SESM Support of SPC Topology
A00007255.AA07	Dial Plan Enhancement for ETSI MWI TCAP
A00007329.AA13	International H.323 2CLI (Calling Line Identity) Support
A00007349.AA13	CPC Screening support for FDCP Trunks
A00007380.AA07	INTL H.323 GW interworking to IWSPM for DTMF Relay and T.38
A00007383.AA11	DNH (Directory Number Hunting) enhancements: pilot DN charge and display
A00007405.AB01	Intl CAS - Korean R2 support
A00007440.AA06	ConnectToResource and PlayAnnouncement during Alert
A00007749.AA06	MG9000 ABI Support for LGCO, LGCOi
A00007790.AA08	P-phone expansion for CICM lines
A00007793.AA22	IN: SCF Id, Correlation Id and QoR Base LNP Support (DACOM)
A00007794.AA10	IN Collect Call Support (DACOM)
A00007796.AA20	Color-ring Feature (DACOM)

A00007807.AA16	Base ETSI ISUP V2 support for Dacom IN
A00007864.AA14	Pakistan ISUP tandeming on CS2Kc

1: A00005315 Functional description (FN)

1.1 Feature name

Calling Number Delivery for PRI, ISUP & CS-1

This feature implements a specific calling party PI, NI mapping and calling party number manipulation from originating to terminating ISUP/PRI/CS-1 trunk groups, and a new CLI delivery logic according to PI value for specific market of HongKong is enhanced to support terminating ISUP trunk groups. This feature is implemented for GSPISN08 combo load.

For call originating from any agents of IDA-M/R, HK ISUP, ANSI ISUP, ETSI ISUP V1/V2, IDA-P(HK PRI), ANSI PRI or CS-1 and terminating to HK ISUP, ANSI ISUP, ETSI ISUP V1/V2, ANSI PRI, ETSI PRI, IDA-P(HK PRI) and CS-1 trunk, this feature implements the special mapping plan to set the PI, NI field and modify calling party number of outgoing calling party according to the length of incoming CLI, prefixes, PI and NI. Furthermore, this feature also changes the existing CLI delivery logic for the ISUP outgoing trunk.

1.2 Description

Below is the mapping requirement deployed in the Hong Kong (HK) market (table 1).

Table 1 ¹PI and NI Mapping Table

Originating agent				Terminating agent				
				ISUP		CS-1		PRI
				PI	NI	PI	NI	PI
IDA-M/R	00	-	8-10 Digit, Non 77	00	0	00	0	00
	01	-	8-10 Digit, Non 77	01	0	01	0	01
	10	-	8-10 Digit, Non 77	00	1	10	0	10
	X	-	8-10 Digit, 77	00	1	10	0	10

ISUP	00	0	10 Digit, Non 77	00	0	00	0	00
	01	0	10 Digit, Non 77	01	0	01	0	01
	10	0	10 Digit, Non 77	00	1	10	0	10
	11	0	10 Digit, Non 77	00	1	10	1	10
	00	1	10 Digit, Non 77	00	1	10	1	10
	01	1	10 Digit, Non 77	00	1	10	1	10
	10	1	10 Digit, Non 77	00	1	10	1	10
	11	1	10 Digit, Non 77	00	1	10	1	10
	X	X	10 Digit, 77	00	1	10	1	10
PRI	00	-	10 Digit, Non 77	00	0	00	0	00
	01	-	10 Digit, Non 77	01	0	01	0	01
	10	-	10 Digit, Non 77	00	1	10	0	10
	11	-	10 Digit, Non 77	00	1	10	1	10
CS-1	00	0	10 Digit, Non 77	00	0	-	-	00
	01	0	10 Digit, Non 77	01	0	-	-	01
	10	0	10 Digit, Non 77	00	1	-	-	10
	11	0	10 Digit, Non 77	00	1	-	-	10
	00	1	10 Digit, Non 77	00	1	-	-	10
	01	1	10 Digit, Non 77	00	1	-	-	10
	10	1	10 Digit, Non 77	00	1	-	-	10
	11	1	10 Digit, Non 77	00	1	-	-	10
	X	X	10 Digit, 77	00	1	-	-	10

The following table shows the interworkings of the two agencies which are supported in this feature.

Table 2 Supported Interworkings for MMP

Terminator Originators	ANSI ISUP	ETSI ISUP V1/V2	HK ISUP	ANSI PRI	HK PRI (CR13)	CS-1	ETSI PRI
ANSI ISUP	Y	Y	Y	Y	Y	Y	Y
ETSI ISUP V1/V2 (no variants)	Y	Y	Y	Y	Y	Y	Y
Hong Kong ISUP (CR14/CR15)	Y	Y	Y	Y	Y	Y	Y
ANSI PRI	Y	Y	Y	Y	Y	Y	N
Hong Kong PRI (CR13)	Y	Y	Y	Y	Y	Y	Y
CS-1	Y	Y	Y	Y	Y	N	Y
ETSI PRI	Y	Y	Y	N	Y	Y	Y

Notes: "Y " denotes supported interworkings; "N" denotes not supported interworkings.

Table 3 Supported Interworkings for GSP

Terminator Originators	ANSI ISUP	ETSI ISUP V1/V2	HK ISUP	ANSI PRI	HK PRI (CR13)	CS-1	ETSI PRI
IDA-M/R(CR11/CR12)	Y	Y	Y	Y	Y	N	Y
ANSI ISUP	Y	Y	Y	Y	Y	Y	Y
ETSI ISUP V1/V2 (no variants)	Y	Y	Y	Y	Y	Y	Y
Hong Kong ISUP (CR14/CR15)	Y	Y	Y	Y	Y	Y	Y
ANSI PRI	Y	Y	Y	Y	Y	Y	N
Hong Kong PRI (CR13)	Y	Y	Y	Y	Y	Y	Y
CS-1	Y	Y	Y	Y	Y	N	Y
ETSI PRI	Y	Y	Y	N	Y	Y	Y

Notes: "Y " denotes supported interworkings; "N" denotes not supported interworkings.

For any ISUP related function, only trunk type IBNT(IBNTI, IBNT0, IBNT2) is supported for MMP ISUP and trunk type AXXESS is supported for GSP ISUP.

1.2.1 Datafillable PI, NI Mapping and calling party number manipulation

This feature provides a datafillable outgoing calling party PI, NI mapping and calling party number manipulation functionality for the interworkings specified in 2.

The following tables are introduced in feature 59040499 to make the PI mapping rules datafillable for outgoing PRI trunks:

- CGPNBLDR (Calling Party Number Builder)
- CGBLDADD (Address-Type Screening)
- CGBLDDGL (Digit-Length Screening)
- CGBLDDIG (Digit Screening)
- CGBLDNI (NI Screening)
- CGBLDPI (PI Screening)

In this feature, all the tables above are changed to support calling party number manipulation. Also, outgoing ISUP trunks and CS-1 agents are supported. For outgoing ISUP trunks, the screening is also triggered from CGPNBLDR option in table TRKOPTS like outgoing PRI trunk; for outgoing CS-1 agent, the screening is triggered from CGNBD_IN option in table TRKOPTS.

A new table CGBLDSIN is introduced in this feature to enhance the screening mechanism so that incoming agent can be judged:

- CGBLDSIN (SMALLINT Screening)

The CGPNBLDR table acts as the main table for this feature, which is accessed from table TRKOPTS. The CGPNBLDR processing procedures are accessed the corresponding screening tables based on the datafill to decide how to map the PI.

1.2.1.1 Table CGPNBLDR

The format of table CGPNBLDR is shown in below. Only the new options introduced by this feature are listed, other options please refer to A59040499.

Table 4 Format of Table CGPNBLDR

Field	Option	Range of Values	Description
CGNBDKEY		String of up to 20 characters	alphanumeric (1 to 20 characters)

Table 4 Format of Table CGPNBLDR

Field	Option	Range of Values	Description
CBOPTION	IC_VAR_SCRN:		Allows the operator to screen the variables that are datafilled in table VARDEF. This option currently only supports to screen the small integer (0-255) type variables. The value of the variable can be set for the incoming trunk using the SETVAR SMALLINT option in table CALLCNTL or one of its screening tables. The table CGBLDSIN is accessed to find if the match can be found for a given CGPNBLDR Index, variable and its value. If screening fails, the CGPNBLDR process can be terminated or continued based on the datafill of field CONTINUE. <i>Please note that if a variable is not assigned to the incoming trunk, the screening returns failed result by default.</i>
	Variable Type	{SMALLINT, DIGITS}	
	Variable Name	String of up to 8 characters	
	CONTINUE	Y or N	

Table 4 Format of Table CGPNBLDR

Field	Option	Range of Values	Description
	CND_GOTO: CONDITION NEWBDKEY	{IC_INAP} String of up to 20 characters(a new CGPNBLDR index)	Allows the operator to change the CGPNBLDR index when the incoming call accords with the condition. Currently, only incoming IN call will be checked
	DIGMAN: DMI	0 to 32767	Allows the operator to change the CLI. And the field DMI is indexed to the table DIGMAN which is used to manipulate the CLI digits.
	ENHANCED_DIG SCRN: DMI	0 to 32767	Indicates the digits of the address to be screen, this option is associated with table CGBLDDIG. And the field DMI is indexed to the table DIGMAN which is used to manipulate the CLI digits temporarily before entering the table CGBLDDIG. The manipulation can only be seen when processing in CGBLDDIG, it can not take effect to the real CLI after returning from CGBLDDIG.

Figure 1 Sample datafill - Table CGPNBLDR

```

TABLE: CGPNBLDR
CGNBDKEY CBOPTION
-----
SCRN_CHOSEN_IC_ADDR
(CND_GOTO IC_INAP SCRIN_IN_IC_ADDR ) (IC_ADDR_SCRN (ADDRTYPE) (DIGLEN) $)
(DIGMAN 8) (ENHANCED_DIGSCRN 4)
(IC_VAR_SCRN (SMALLINT IC_VAR) Y) $

```

1.2.1.2 Table CGBLDADD

Table CGBLDADD allows the operator to identify the type of the incoming address.

Table 5 Format of Table CGBLDADD

Field	Range of Values	Description
CGNADDRK: CGNBDKEY ADDRTYPE	String of up to 20 characters One of {CLI, RDN, CHARGE, PN, CONTRACTOR, GENERIC_NO}	The key is composed of two subfields.
NEWBDKEY	String of up to 20 characters	A new CGPNBLDR Index.
CBOPTION	CGPNBLDR Options: SETPI, SETNI, DIGMAN	New option DIGMAN is added to perform calling party number manipulation.

Below shows a datafill sample of table CGBLDADD.

Figure 2 Datafill example of Table CGBLDADD

```
TABLE: CGBLDADD
CGNADDRK NEWBDKEY CBOPTION
-----
SCRN_IC_ADDR CLI SCRNIC_CGPN (DIGMAN 10) $
```

1.2.1.3 Table CGBLDDGL

Table CGBLDDGL allows the operator to screen the length of digits of the incoming address. The format of CGBLDDGL is shown in below table.

Table 6 Format of Table CGBLDDGL

Field	Range of Values	Description
CGNDGLK: CGNBDKEY DIGLEN	String of up to 20 characters {0-30}	The key is composed of two subfields.
NEWBDKEY	String of up to 20 characters	A new CGPNBLDR Index
CBOPTION	CGPNBLDR Options: SETPI, SETNI, DIGMAN	New option DIGMAN is added to perform calling party number manipulation.

Below shows a datafill example of table CGBLDDGL.

Figure 3 Datafill example of Table CGBLDDGL

```
TABLE: CGBLDDGL
CGNDGLK NEWBDKEY CBOPTION
-----
SCRN_IC_CGPN 8  SCRN_RETURN  $
SCRN_IC_CGPN 9  SCRN_RETURN (SETPI ALLOWED) $
SCRN_IC_CGPN 10 IC_CGPN_LENGTH_10 (DIGMAN 10) $
```

1.2.1.4 Table CGBLDDIG

Table CGBLDDIG allows the operator to screen the digits of incoming address which is chosen to map into the outgoing CGPN.

The format of this table is shown in below table.

Table 7 Format of Table CGBLDDIG

Field	Range of Values	Description
CGNDGKEY:		The key is composed of 3 subfields.
CGNBDKEY	String of up to 20 characters	
FROMDIGS	1-15 digits	
TODIGS	1-15 digits	
NEWBDKEY	String of up to 20 characters	A new CGPNBLDR Index
CBOPTION	CGPNBLDR Options: SETPI, SETNI, DIGMAN	New option DIGMAN is added to perform calling party number manipulation.

Below shows a datafill example of table CGBLDDIG.

Figure 4 Datafill example of Table CGBLDDIG

```
TABLE: CGBLDDIG
CGNDGKEY NEWBDKEY CBOPTION
-----
BASE 77 77 SCR_N_RETURN (SETPI NOT_AVAIL) $
BASE 88 88 PREFIX_88 (DIGMAN 10) $
```

1.2.1.5 Table CGBLDNI

Table CGBLDNI allows the operator to screen the NI of the incoming address (a default value 0=complete is use instead, if this field is missing) which is chosen to map into the outgoing CGPN.

Table 8 Format of Table CGBLDNI

Field	Range of Values	Description
CGNNIKEY:		The key is composed of two subfields.
CGNBDKEY	String of up to 20 characters	
NI	One of {COMPLETE, INCOMPLETE}	
NEWBDKEY	String of up to 20 characters	A new CGPNBLDR Index
CBOPTION	CGPN Builder Options: SETPI, SETNI, DIGMAN	New option DIGMAN is added to perform calling party number manipulation.

Below is a datafill example table CGBLDNI.

Figure 5 Datafill example of Table CGBLDNI

```
TABLE: CGBLDNI
CGNNIKEY NEWBDKEY CBOPTION
-----
SCRN_IC_CGPN COMPLETE NI_0 (DIGMAN 10) $
SCRN_IC_CGPN INCOMPLETE NI_1 (SETPI NO_AVAIL) $
```

1.2.1.6 Table CGBLDPI

Table CGBLDPI allows the operator to screen the PI of the incoming address which is chosen to map into the outgoing CGPN.

Table 9 Format of Table CGBLDPI

Field	Range of Values	Description
CGNPIKEY: CGNBDKEY PI	String of up to 20 characters One of {ALLOWED, RESTRICTED, NOT_AVAIL, SPARE}	The key is composed of two subfields.
NEWBDKEY	String of up to 20 characters	A new CGPNBLDR Index
CBOPTION	CGPNBLDR Options: SETPI, SETNI, DIGMAN	New option DIGMAN is added to perform calling party number manipulation.

Below is a datafill example of table CGBLDPI.

Figure 6 Datafill example of Table CGBLDPI

```
TABLE: CGBLDPI
CGNPIKEY NEWBDKEY CBOPTION
-----
SCRN_IC_CGPN ALLOWED PI_00 (SETPI ALLOWED) (DIGMAN
10) $
SCRN_IC_CGPN NOT_AVAIL PI_10 (SETPI NOT_AVAIL) $
```

1.2.1.7 Table CGBLDSIN

The new introduced table CGBLDSIN allows the operator to screen the variable and its value assigned to the incoming trunk.

Table 10 Format of Table CGBLDSIN

Field	Range of Values	Description
SINTVAR: SINTVAR CGNBDKEY VALUE	Variable name (1-8 characters) from table VARDEF String of up to 20 characters {0 TO 255}	The key is composed of three subfields.
NEWBDKEY	String of up to 20 characters	A new CGPNBLDR Index

Table 10 Format of Table CGBLDSIN

Field	Range of Values	Description
CBOPTION	CGPNBLDR Options: SETPI, SETNI, DIGMAN	Allows setting of the PI, NI and CLI value of the outgoing CGPN as performed in table CGPNBLDR.

Table CGBLDSIN must be datafilled after table TRKOPTS for outgoing trunks.

Below is a datafill example of table **CGBLDSIN**.

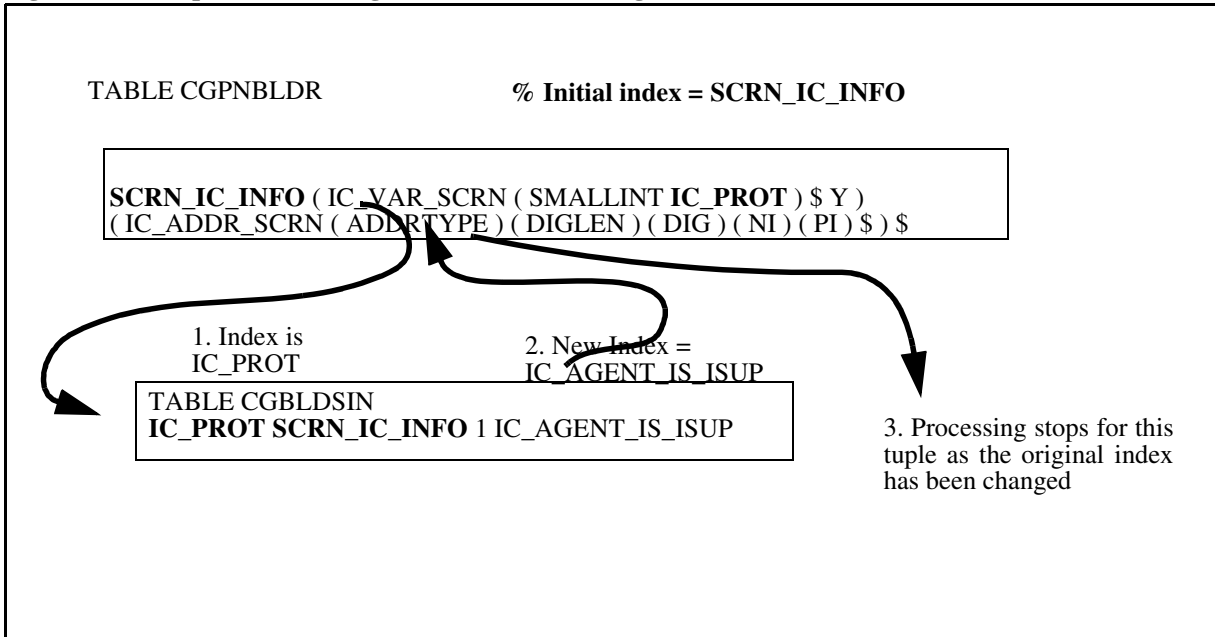
Figure 7 Datafill example of Table CGBLDSIN

```
TABLE: CGBLDSIN
SINTVAR CGNBDKEY VALUE NEWBDKEY CBOPTION
-----
IC_PROT SCRN_IC_PROT 1 IC_AGENT_IS_ISUP (SETPI SPARE) (SETNI INCOMPLETE) $
IC_PROT SCRN_IC_PROT 2 IC_AGENT_IS_PRI (SETPI NOT_AVAIL) $
```

1.2.1.8 CGPNBLDR Processing

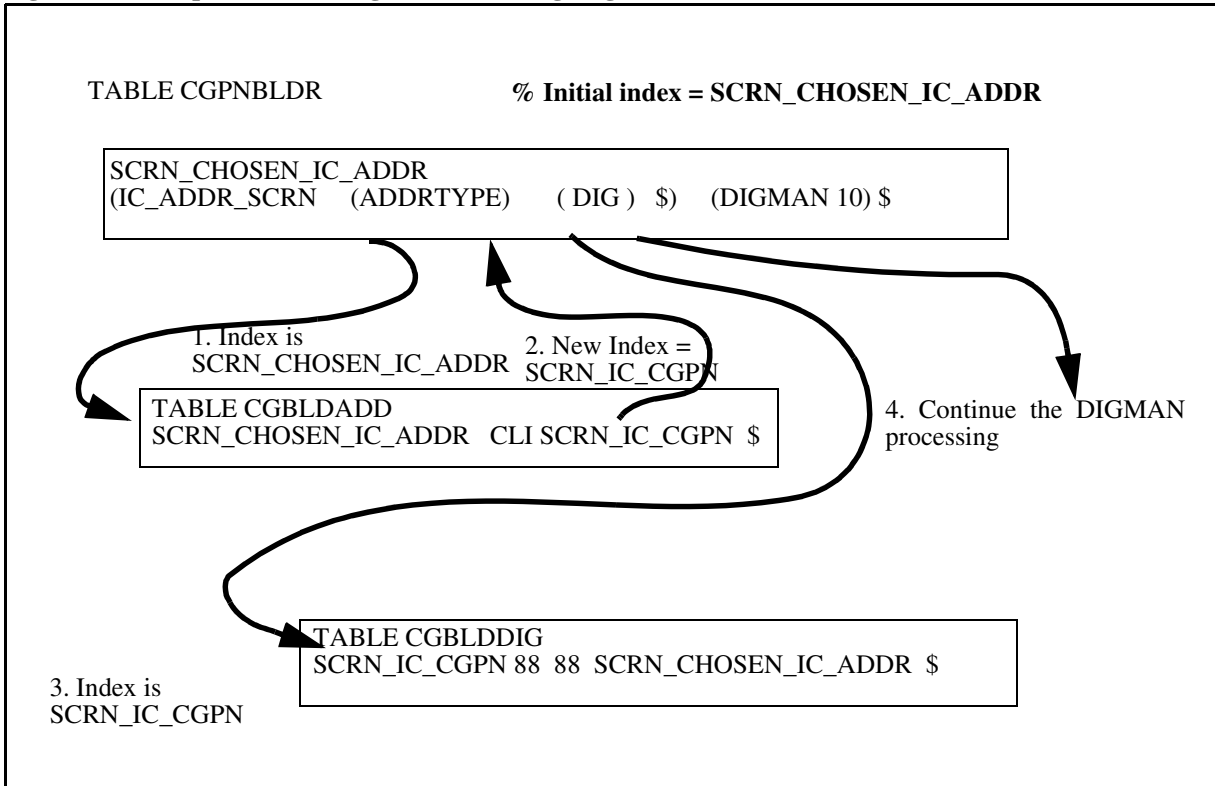
The CGPNBLDR mechanism is a recursive structure, which uses the initial CGPNBLDR index specified in table TRKOPTS to start the manipulation process.

Each option datafilled on the initial tuple in table CGPNBLDR is processed in turn. If any of the IC_ADDR_SCRN or IC_VAR_SCRN options are datafilled, call processing continues to the appropriate screening table using the same index it had in CGPNBLDR. If the CGPNBLDR index is updated via this screening table, CGPNBLDR will use the updated value to re-index this table when processing of the current option is complete. If processing of the current option is not complete, the updated CGPNBLDR index will be used to access any subsequent incoming address screening tables. This process is illustrated in the following example diagrams.

Figure 8 Example 1: Processing exits after index change

In this example the CGPNBLDR index is updated in table CGBLDSIN and the index into CGPNBLDR is re-evaluated after the first “IC_VAR_SCRN” option. Processing continues directly to the next CGPNBLDR tuple (IC_AGENT_IS_ISUP).

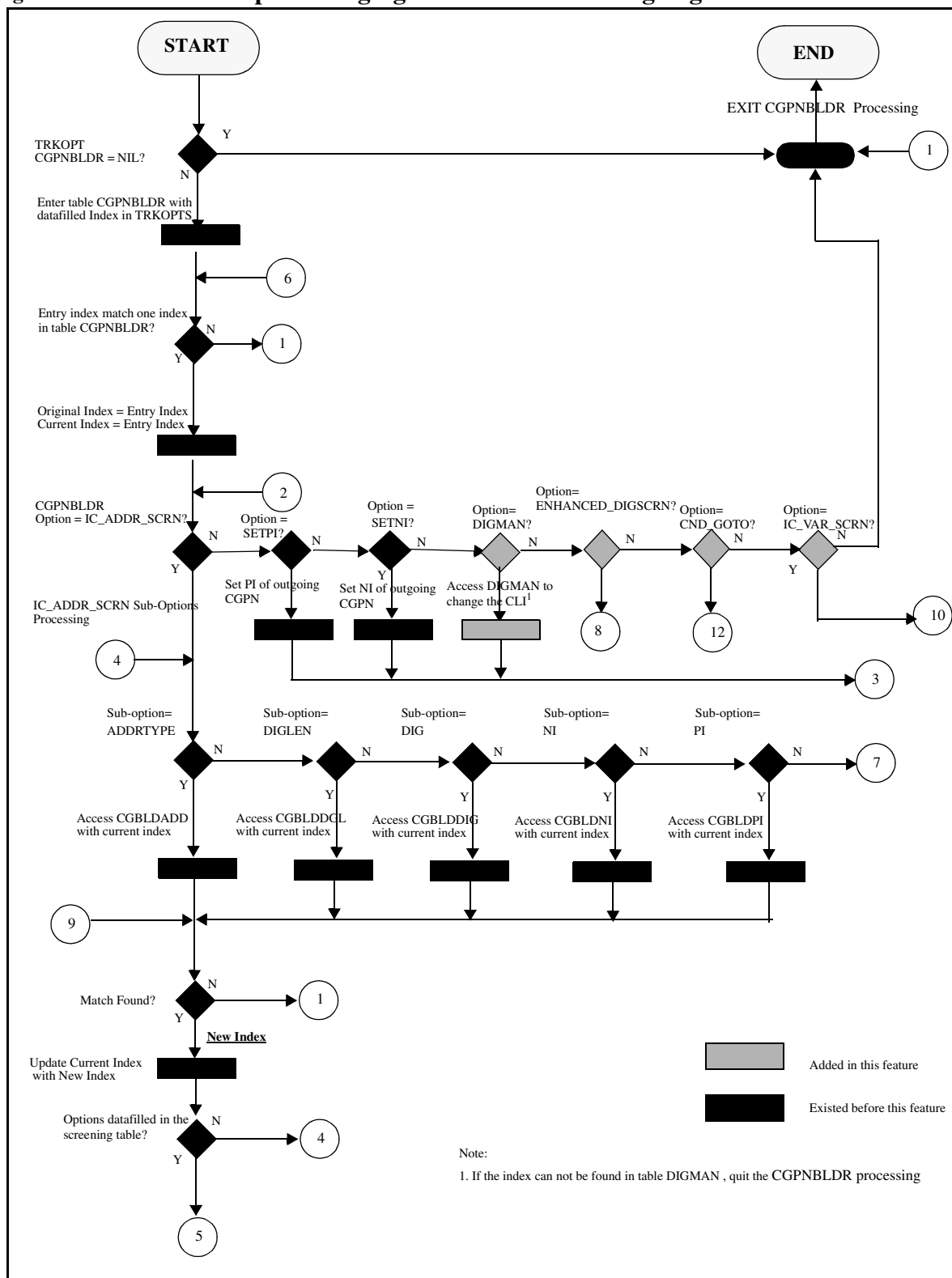
Figure 9 Example 2: Processing continues using original index

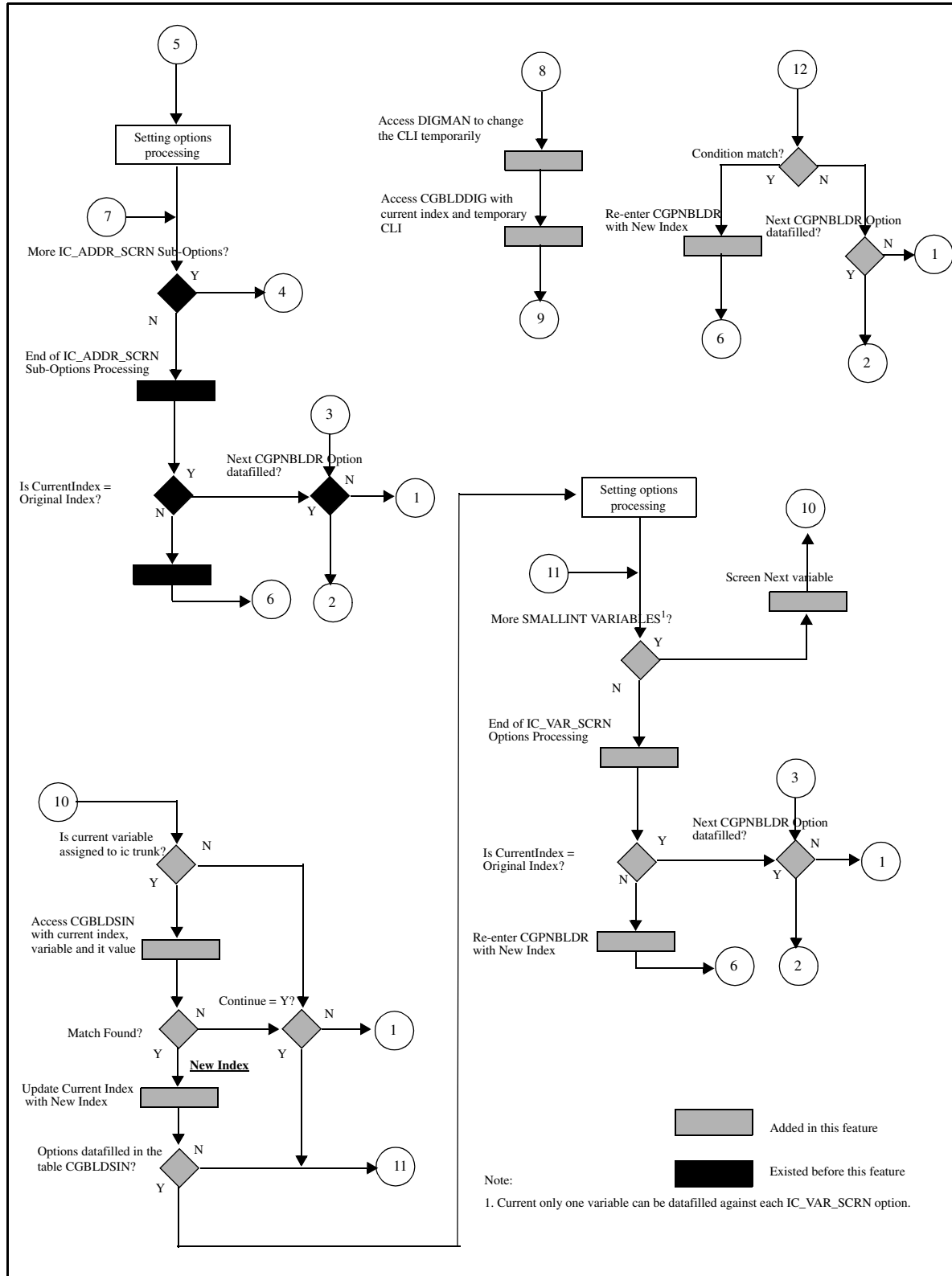


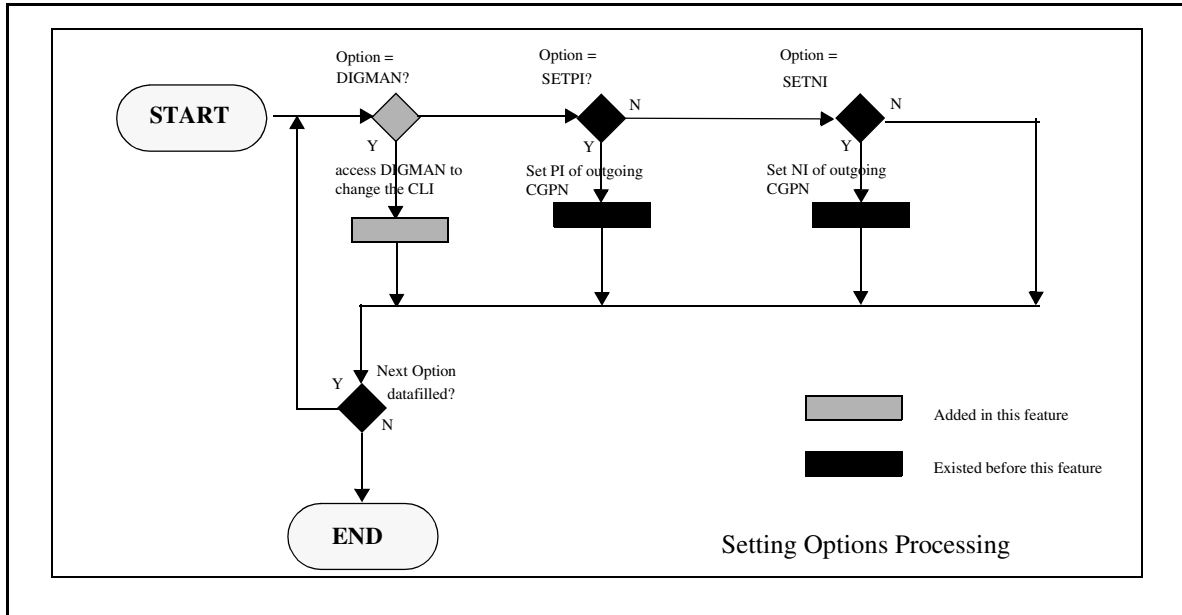
In this example even though the CGPNBLDR index is altered in CGBLDADD it is reset to “SCR_N_CHOSEN_IC_ADDR” in table CGBLDDIG, so the next option (DIGMAN 10) is processed.

Below is the CGPNBLDR processing figure for PRI and ISUP outgoing trunk:

Figure 10 CGPNBLDR processing figure for PRI/ISUP outgoing trunk







1.2.1.9 Datafill example for a particular PI mapping plan (Access from option CGPNBLDR, apply to terminating PRI trunk)

Refer to a PI mapping example requirement: if the incoming agent is ISUP trunk, then mapping PI=00; otherwise, adopting the mapping plan shown in Table 10 below.

Table 11 PI Mapping Example for terminating PRI trunk

Originating non ISUP trunk			Terminating ISUP or PRI trunk
PI	NI	10-digit CLI's Prefix	PI
11	0	Non 77	10

Here is the datafill implementation:

For the all incoming ISUP trunks

```

+-----+
TABLE VARDEF
-----
IC_PROT

+-----+
TABLE CALLCNTL
-----
SET_IC_PROT_ISUP (SETVAR SMALLINT IC_PROT 1) $

```

%% Note: This example prescribes the value 1 stands for ISUP protocol

```
+-----+
TABLE TRKOPTS
-----
<ISUP TRUNK CLLI> CCNTLIDX CCNTLIDX SET_IC_PROT_ISUP
```

For the outgoing PRI trunks

```
+-----+
TABLE TRKOPTS
-----
<PRI or ISUP TRUNK CLLI> CGPNBLDR CGPNBLDR SCRN_IC_INFO
+-----+
TABLE DIGMAN
-----
10 (CL BEG) (REM 2) $
+-----+
TABLE CGPNBLDR
-----
SCRN_IC_INFO (IC_VAR_SCRN (SMALLINT IC_PROT) Y)
(IC_ADDR_SCRN (ADDRTYPE) (DIGLEN) (DIG) (NI) (PI) $) $
IC_AGENT_IS_ISUP (SETPI ALLOWED) (DIGMAN 10) $
```

```
+-----+
TABLE CGBLDSIN
-----
IC_PROT SCRN_IC_INFO 1 IC_AGENT_IS_ISUP $
```

%% Note: According to assumption before, if the incoming agent is ISUP trunk, then the variable IC_PROT will be set to 1.

```
+-----+
TABLE CGBLDADD
-----
SCRN_IC_INFO CLI SCRN_IC_CGPN $ $
+-----+
TABLE CGBLDDGL
-----
SCRN_IC_CGPN 10 CLI_LENGTH_10 $
+-----+
TABLE CGBLDDIG
-----
CLI_LENGTH_10 0 76 CLI_PREFIX_NON_77 $
CLI_LENGTH_10 78 9 CLI_PREFIX_NON_77 $
```

```
+-----+
TABLE CGBLDNI
-----
CLI_PREFIX_NON_77 COMPLETE NI_0 $
+-----+
TABLE CGBLDPI
-----
NI_0 SPARE SCRN_RETURN (SETPI NOT_AVAIL) $
```

Below is the processing steps, suppose the incoming CGPN (CLI=88123456, PI=11 and NI=0) is chosen to outpulse into outgoing CGPN:

In case of ISUP -> PRI

1. Screen table TRKOPTS, get entry index from CGPNBLDR option: "SCRN_IC_INFO".
2. Screen table CGPNBLDR using the index, find the tuple.
3. Screen the tuple of table CGPNBLDR, option "IC_VAR_SCRN" is datafilled, get the first variable "IC_PROT".
4. Screen the table CGBLDSIN using the index "SCRN_IC_INFO", because the incoming is ISUP trunk, then the new index "IC_AGENT_IS_ISUP" is set and return to table CGPNBLDR.
5. The tuple with index "IC_AGENT_IS_ISUP" in table CGPNBLDR sets the PI=00.
6. Get the DIGMAN index "10", go to table DIGMAN, find the tuple whose index is 10, and delete the first 2 digits in CLI

In case of incoming Non-ISUP -> PRI

1. Screen table TRKOPTS, get entry index from CGPNBLDR option: "SCRN_IC_INFO".
2. Screen table CGPNBLDR using the index, find the tuple.
3. Screen the tuple of CGPNBLDR, option "IC_VAR_SCRN" is datafilled, get the first variable "IC_PROT".
4. Screen the table CGBLDSIN using the index "SCRN_IC_INFO", because the incoming is Non-ISUP trunk, the screening of table CGBLDSIN is failed, the process will return to table CGPNBLDR with original index, the processing will be continued with next option in the same tuple because the field "CONTINUE" of option "IC_VAR_SCRN" is set to Y.
5. The next option is "IC_ADDR_SCRN", get the first sub-option "ADDRTYPE".
6. Screen the corresponding table CGBLDADD using the index "SCRN_IC_INFO", because the address type to be outputted into outgoing CGPN is CLI, find the tuple and get new index "SCRN_IC_CGPN".
7. Go back to the tuple of CGPNBLDR, next sub-option is "DIGLEN".
8. Screen the corresponding table CGBLDDGL using new current index "SCRN_IC_CGPN", because length of CLI is 10, find the tuple and get new index "CLI_LENGTH_10".
9. Go back to the tuple of CGPNBLDR, next sub-option is "DIG".
10. Screen the corresponding table CGBLDDIG using new current index "CLI_LENGTH_10", because DIG prefix is '88', find the tuple and get new index "CLI_PREFIX_NON_77".

11. Go back to the tuple of CGPNBLDR, next sub-option is “NI”.
12. Screen the corresponding table CGBLDNI using new current index “CLI_PREFIX_NON_77”, because NI is ‘COMPLETE’, find the tuple and get new index “NI_0”.
13. Go back to the tuple of CGPNBLDR, next sub-option is “PI”.
14. Screen the corresponding table CGBLDPI using new current index “NI_0”, because PI is ‘SPARE’, find the tuple, set PI according to the option in the tuple, and get new index “SCRN_RETURN”.
15. Go back to the tuple of CGPNBLDR, end of sub-option is met. The index is changed, so will continue using new index “SCRN_RETURN”.
16. Tuple “SCRN_RETURN” is not found in table CGPNBLDR, so the processing is stopped.

1.2.1.10 Datafill example for a particular PI mapping plan (Access from option CGNBD_IN, apply to trunks invoke INAP service - CS-1 agent equivalent)

For outgoing CS-1 agent, CGPNBLDR process is triggered from CGNBD_IN option in table TRKOPTS. Refer to a PI mapping example requirement (Table 11 below) for CS-1 agent.

Table 12 PI Mapping Example for CS-1 agent

Originating ISUP trunk invokes INAP service			Terminating CS-1 agent
PI	NI	10-digit CLI's Prefix	PI
11	0	Non 77	10

Here is the datafill implementation:

```

+-----+
TABLE TRKOPTS
-----
<ISUP Trunk CLLI> CGNBD_IN CGNBD_IN SCR_N_IC_ADDR

+-----+
TABLE CGPNBLDR
-----
SCR_N_IC_ADDR
(IC_ADDR_SCRN (ADDRTYPE) (DIGLEN) (DIG) (NI) (PI) $) $

+-----+
TABLE CGBLDADD
-----
SCR_N_IC_ADDR CLI SCR_N_IC_CGPN $ $

+-----+
TABLE CGBLDDGL
-----
SCR_N_IC_CGPN 10 CLI_LENGTH_10 $ $

```

```

+-----+
TABLE CGBLDDIG
-----
CLI_LENGTH_10 0 76 CLI_PREFIX_NON_77 $
CLI_LENGTH_10 78 9 CLI_PREFIX_NON_77 $
+-----+

TABLE CGBLDNI
-----
CLI_PREFIX_NON_77 COMPLETE NI_0 $
+-----+

TABLE CGBLDPI
-----
NI_0 SPARE SCRN_RETURN (SETPI NOT_AVAIL) $
+-----+

```

Below is the processing steps, suppose the incoming CGPN (CLI=88123456, PI=11 and NI=0) is chosen to outpulse into outgoing CGPN of InitialDP message:

1. Screen table TRKOPTS, get entry index from CGNBD_IN option: "SCRN_IC_ADDR".
2. Screen table CGPNBLDR using the index, find the tuple.
3. Other steps refer to the previous example in the case of incoming non-ISUP trunk.

1.2.2 New CLI Delivery Logic Supported by outgoing ISUP trunk

Prior to this feature, the field CLIDELV in table TRKOPTS has three options:

- If CLIDELV is set to 'Y', CLI will be delivered.
- If CLIDELV is set to 'N', CLI will not be delivered.
- If CLIDELV is set to 'SCRN_PI', CLI will be delivered unless the PI is set to 'Presentation Restricted'.

In feature 59040499, a new CLI delivery logic is implemented for PRI outgoing trunk. For CLIDELV=SCRN_PI, the delivery logic is changed to:

- The CLI will only be delivered when the PI is '00', i.e. 'Allowed'.
- If the PI is '01' (Restricted), '10' (Not available) or '11' (Spare), no CLI digits will be delivered but the PI will be delivered.

The modified CLI delivery logic is illustrated in 13.

Table 13 CLI Delivery Logic for ISUP/PRI outgoing trunk

PI of outgoing CGPN	CLIDELV		
	Y	SCRN_PI	N
00	CLI = Y , PI = Y	CLI =Y, PI = Y	no CGN IE
01	CLI = Y, PI = Y	CLI = N, PI = Y	no CGN IE
10	CLI = Y, PI = Y	CLI = N, PI = Y	no CGN IE
11	CLI = Y, PI = Y	CLI = N, PI = Y	no CGN IE

Note: In Table 12, “CLI = Y” denotes sending CLI digits, “CLI = N” denotes not sending CLI digits, “PI = Y” denotes sending Presentation Indicator and “no CGN IE” denotes no Calling Party Number Information Element will be contained in the outgoing PRI SETUP message , or no Calling Party Number Parameter will be contained in the outgoing ISUP IAM message.

The new CLI delivery activation or deactivation is controlled by an option CLIDLVPI in table TRKOPTS on a per trunk group basis.

Moreover, if we select only option CLIDELV=SCRN_PI without CLIDLVPI option, no CGN IE at the result of CLI's PI = 01 by CGPNBLDR should be applied.

This feature enhances the CLI delivery logic also to support the ISUP trunk.

1.3 Hardware Requirements or Dependencies

N/A.

1.4 Software Requirements or Dependencies

N/A.

1.5 Limitations and restrictions

If want to activate the option "CGPNBLDR" for the PI and NI mapping on MMP, the operator has to datafill option CLIOUTP first in table TRKOPTS against the same terminating trunk. The option CLIOUTP was introduced in feature A59023300 "CLI Delivery Control".

According to current implementation, PI of '11' could not be outputted to terminating PRI agent. If the PI mapping result is '11', a PI of '01' will be outputted to the outgoing PRI agent as currently implemented.

On MMP side, for originating ETSI PRI, the PI may be changed before entering the PI mapping functionality. For details, Please refer to PRI Screening Enhancements (Functional Group ISD00006). If no ISD00006 related datafill is filled, PI=00,01,10 are changed to 00 before entering the PI mapping functionality of this feature.

1.6 Interactions

The existing outgoing calling party PI Mapping and CLI delivery logic are modified according to the requirements of this feature when this feature is activated.

When table DEFNUM is datafilled and chosen to be outpulsed, the mapping is based on the default number datafilled.

For the new CLI delivery logic, the PI may be changed and the CLI may be set according to the changed PI before entering the PI mapping functionality.

1. On MMP side, when the incoming is ISUP/PRI trunk, the outgoing is HK ISUP(CR14/CR15) trunk:
 when the PI in the incoming IAM is 11, it is mapped to 01 before entering the new CLI delivery logic;
 when the PI in the incoming IAM is 10, the CLI would be not available.
2. On MMP side, when the incoming is ISUP trunk, the outgoing is ANSI ISUP trunk:
 when the PI in the incoming IAM is 10/11, it is mapped to 01 before entering the new CLI delivery logic.
3. Currently, on MMP side, in the Calling Party Number of the CONNECT message from SCP, only PI='00' and '01' are supported.

1.7 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

Performance (includes operational measurements)N/A

Realtime N/A

Engineering Information N/A

1.8 Glossary

Term	Description
CGPN	CallinG Party Number
CLI	Calling Line Identification
CS-1	Capability Set 1
DMS-MMP	DMS switch with MMP software load
IE	Information Element
ISUP	ISDN User Part
NI	Number Incomplete Indicator
PI	Presentation Indicator
PRI	Primary Rate Interface

1.9 Reference

1. A59040499 Calling Number Delivery Enhancement for ISDN PRI - MMP
2. A59039145 Calling Number Delivery Enhancement for ISDN PRI - GSP
3. A59039152 Default 10 digits CLI for IDA-M/R trunk

2: A00005822 Functional description (FN)

2.1 Feature name

AOC Support over H.323

2.2 Description

2.2.1 Summary

Advice of Charge (AOC) gives the CS2000 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

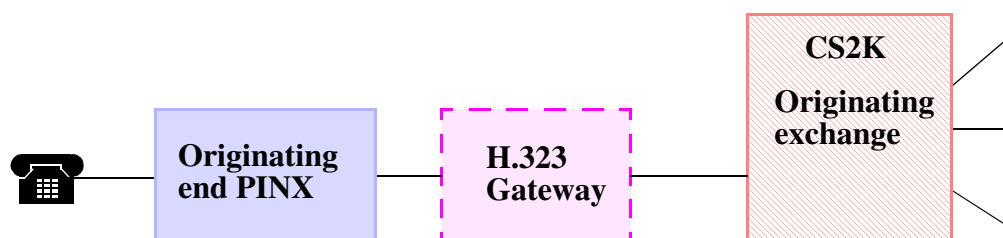
This activity, A00005822, addresses two AOC services: **AOC-D** and **AOC-E**. These services are deployed for originating agents connected to the CS2000 over H.323. For the AOC calculation, the CS2K node has to be configured to determine and apply the tariffs (nodal configuration or combined CGP/CDP, see also Figure 1, on page 38 and Figure 3, on page 42)

The actual activity reuses the AOC on QSIG solution implemented by Nortel with the activities AF7344 [35], A59024423 [36], A590038835 [37] and provides the support for QSIG originating agents.

The overall solution will include a 3rd party H.323 gateway capable of delivering AOC information to BRI subscribers in different national variants, for example in France

- EURO-NUMERIS (VN4, VN6)
- EURO-NUMERIS+ .

Figure 1 AOC over H.323 (functional overview)



2.3 Background information

2.3.1 Charging Information at Call Set-up time (AOC-S)

When the *AOC-S* supplementary service is activated, the network shall provide the user with call charging information at call establishment. In addition, the network shall inform the served user if a change in charging rates takes place during the call.

The network shall provide the charging information during call establishment or at the latest at call connection. When there is a change in charging rate during the call, the network shall send information about the new charging rate to the served user.

2.3.2 Charging Information During the Call (AOC-D)

When the *AOC-D* supplementary service is activated, the network shall provide the user with call charging information during the active phase of a call. The network shall provide the charging information and transfer it to the user in an appropriate message. The supplied charging information shall be provided as a cumulative charge incurred so far for the call.

When the call is released, the network shall send the user the recorded charges for the call in one of the call control messages clearing the call.

If the network has determined that the call is free of charge, the network shall send the user a free-of-charge indication. The network shall not send any further charging information during the call. When the call is released, the network shall send the free-of-charge indication in a call control message clearing the call.

2.3.3 Charging Information at the End of the Call (AOC-E)

When the *AOC-E* supplementary service is activated, the network shall provide the user with call charging information indicating the recorded charges when the call is released. The network shall send the user the charging information in one of the call control messages clearing the call.

2.3.4 Indication of Charge [télétaxe]

This term is used in France in order to describe the supplementary service which informs the user of the charges which have been attributed during the active phase of a call. With other words, it is another term for *AOC-D*. Please refer to chapter “2.3.2 Charging Information During the Call (AOC-D)” on page 39.

2.3.5 Total Cost

This term is used in France in order to describe the supplementary service which informs the user of the call charges when the call is released. It is another term for *AOC-E*. Please refer to chapter “2.3.3 Charging Information at the End of the Call (AOC-E)” on page 39.

2.3.6 Charging Units

In this variant of AOC, the AOC charging information is presented to the terminal in form of a pulse count. The subscriber or terminal has to know the amount and currency equivalent to one pulse in order to calculate the cost of a call.

2.3.7 Currency Units

In this variant of AOC, the AOC charging information is presented to the terminal in form of amount and currency.

2.3.8 Functional Protocol

The functional protocol is based on the use of the Facility information element and the FACILITY message, as well as of other specific functional messages specified in clause 7 of Recommendation Q.932.

This protocol is functional in the sense that it requires the knowledge of the related supplementary service by the user equipment supporting it. This facilitates user equipment operation without human intervention by defining semantics for the protocol elements which user equipment can process on its own.

The protocol is symmetrical and is applicable to both basic and primary rate interfaces.

The key characteristic of the functional protocol is that it may operate end-to-end as contrasted with the Keypad Protocol that is local in nature.

2.3.9 Keypad Stimulus Protocol

The Keypad protocol is a stimulus protocol providing a means of transferring a sequence of IA5-characters from the user to the network to control supplementary services and indicating network responses to the user. The Keypad protocol is based on the use of the Keypad facility and Display information elements. The Keypad facility information element may be included in the SETUP and INFORMATION messages. The Display information element may be included in any message sent by the network to the user according to Recommendation Q.931.

The Keypad protocol is a stimulus protocol in the sense that it does not require any knowledge about the invoked supplementary service by the user equipment. It may be used in any state of a call and in association with a call for supplementary service invocation. Whatever digits dialled by the user are sent, as such, in a Keypad IE to the network. The keypad facility codes used for the invocation of individual supplementary services are network dependent.

The protocol is applicable to both basic and primary rate interfaces.

In general, the keypad protocol has only a local significance.

2.3.10 AOC on request

In this variant of AOC, charging information is not sent for every call that the user originates but only for calls where the subscriber explicitly requests AOC information by adding a respective Facility Information Element (FAC IE) into the Q.931 SETUP message.

2.3.11 NAOC

Network **Advice Of Charge** (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 a charge message over the network (**CDP** and **CGP** on different exchanges¹) or passed internally to the CGP interface (**CGP** and **CDP** on the same exchange²).

¹This is the case where the originating network does not keep any tariff information for the selected carrier

²This is the case where the originating network has included the tariff information for the selected carrier in its local database

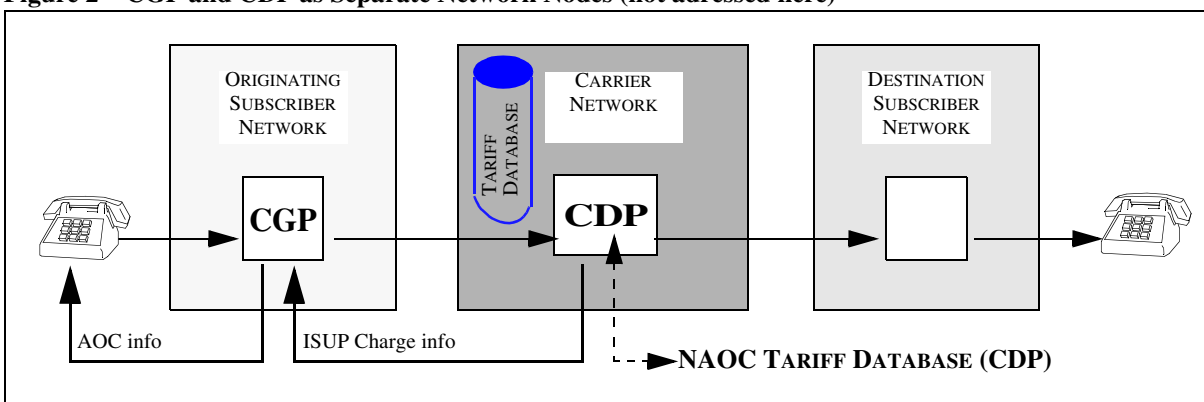
2. **CGP** - The **Charge Generation Point** is an exchange where the received charging information is converted into a format that is delivered to the subscriber.

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.

Based on these types of network nodes, there are two scenarios which have been considered for **NAOC**:

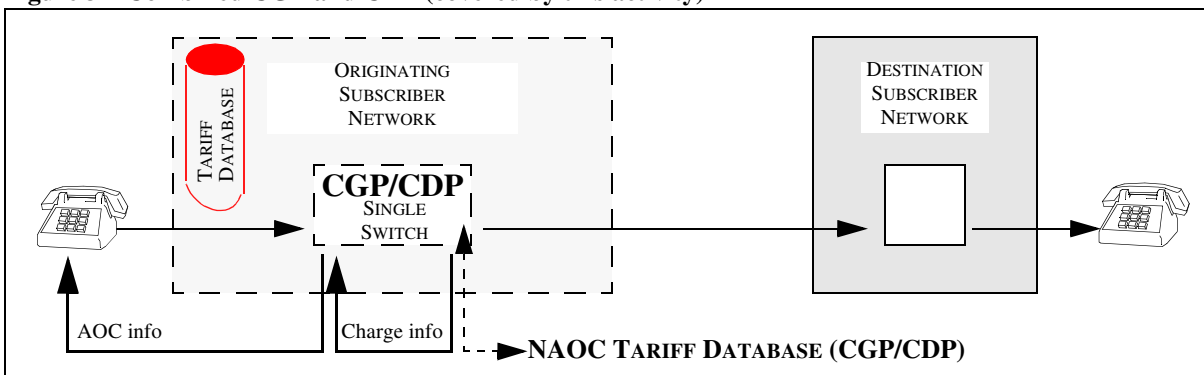
- **CDP** and **CGP** are located in different networks, so that the **CDP** has to send the tariff information over the network boundaries to the **CGP**. Please refer to Figure 2. This scenario will not be addressed by the current activity

Figure 2 CGP and CDP as Separate Network Nodes (not addressed here)



- **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 3. This is the valid scenario which will be addressed by the current activity.

Figure 3 Combined CGP and CDP (covered by this activity)



The decision whether a call has to be tariffed by the originating exchange (combined CGP/CDP functionality) or by another exchange located in an intermediate network (CDP tariffing) is made on a **per call basis**, based on the translations information datafilled at the originating exchange. This ensures that the network structure is dynamic.

2.3.12 NAOC Interworking

A brief overview of the supported agent interworkings is given below. The combinations of supported interworkings are listed in “ ” on page 43. Only the agents marked green and with “X” are being supported. Other agents supported by AOC on QSIG which are not being covered by this activity are marked yellow and “N/A”

Figure 4 Agent interworking for the current feature

Platform	Originator	Terminating agents										
		H323 agents	IBN lines	ETSI PRI	QSIG (95)	ETSI ISUP V1	ETSI ISUP V2/N2+	SIP-T	SSURN2 (FTUP)	SPIROU	UK ISUP	ANSI ISUP
CS2K	H323	X							N/A			

2.3.12.1 NAOC functionality

The NAOC framework provides support for the following functionality:

- **Support for multiple carriers/resellers.**
Up to 16 carriers and 204 resellers can be handled by one CS2000 node;
- **Enhanced Call Translations**
The NAOC tariff determination process is initiated through new translation options cont/rte.
- **Tariffing based on zoning information**
Zoning is supported for
 - local calls,
 - national calls,
 - international calls, and
 - service (special destination) calls i.e. calls to premium rate services, non-geographical numbers, mobile subscribers etc.
- **Tariffing based on Type of Day / Time of Day System.**

Up to 30 tariff changeovers (TCOs) and several datafillable day types are supported per CS2000 node. The CS2000 provides the ability to specify the zones that are applicable to each individual changeover time.

- **Tariffing support for Discounts.**

The Discount System is supported independently for each Carrier Identification Code (CIC) based carrier and simple reseller. Up to 511 discount levels can be assigned. Partial discounts can be given for service numbers

- **Enhanced Tariff tables.**

Supported independently for each CIC based carrier and simple reseller. Supported tariff definitions include:

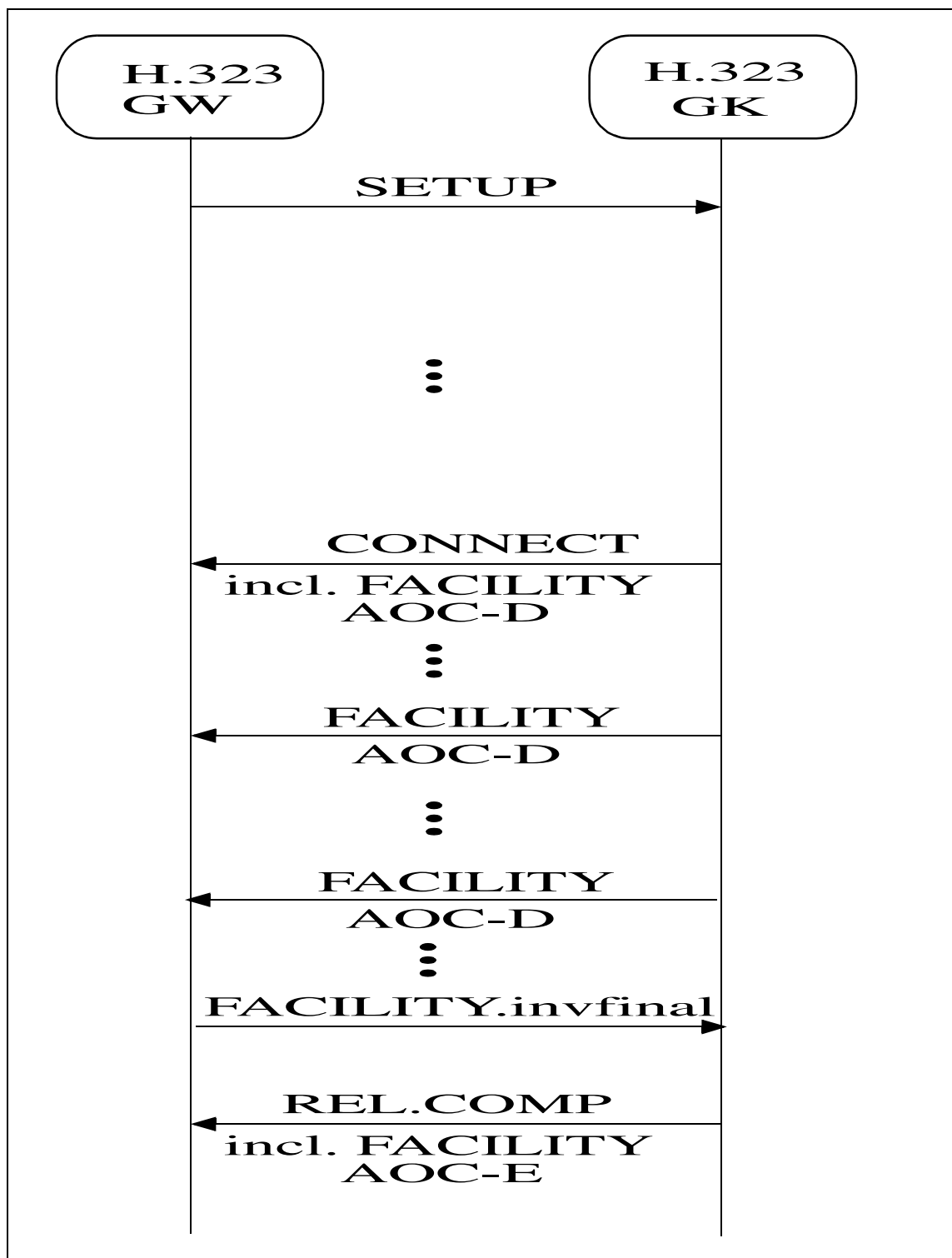
- Block tariffing. This is simply a call setup charge, or a fixed amount to be applied at the beginning of a call.
- Combination tariffing. This is a call setup charge along with a time dependent charge. A time dependant charge is an amount (in the Euro currency) to be applied on a per second basis.
- Minimum communication charge. This is a call setup charge along with a “zero” first sub-tariff charge. In other words, the first sub-tariff is set to zero and there is a call setup charge. In this manner, regardless if the first tariff expires or not, the call will be charged at the minimum amount.

2.4 Feature description

2.4.1 Introduction

AOC is provided for ISDN agents connected via H.323 interface. From a CS2000 point of view, this interface is seen as a QSIG trunk. All related AOC messages are sent as Q.931 Facility Information Elements, generated at the QSIG/H.323 interface and tunneled in H.225[Q.931] messages to the H.323 gateway. At the gateway, the information is unpacked and applied to the originating ISDN agents. Figure 5, on page 45 provides a high level view on the CS2000 architecture with regards to QSIG/H.323.

Figure 6 High Level AOC message flow on a combined CGP/CDP



2.4.2 AOC Control

The AOC functionality can be controlled/provisioned via 3 components:

- Trunk group (customer) basis, through table **TRKOPTS**,
- GWC basis, through table **SERVRINV**.
- Call Server basis, via **SOC** (Software Optionality Control) by using the codes **NETK0024**, **NSUP0020**, **NSUP0023**, **PBXT0011**, **PBXT0018**

H323QSIG trunks datafilled in table **TRKOPTS** can have a option called **AOC**. This option has several fields:

1. **AOCD**, to enable/disable the “AOC During call (AOC-D)” functionality. If set to Y, Facility messages are sent to provide the PBX subscriber with the charge unit count on a regular basis during a call.
2. **AOCE**, to enable/disable the “AOC End of call (AOC-E)” functionality. If set to Y, the final charge unit count is sent at the end of the call in a standard call control message during the disconnect phase.
3. **DSCNT**, to specify the discount class number to which the customer belongs
4. **AOCREL** to enable/disable releasing a call if AOC is not available, i.e.the datafill on both CS2K and GW is not complete. Emergency calls and Priority calls are not released although this flag is set.

Note: For H.323QSIG, AOCREL has to be set to **N**, otherwise a GW misconfiguration might cause calls to be released.

5. **AOCCHGOV** to enable/disable tariff and discount changeover during time of day changeover. This flag also controls if changes in the tariff tables apply directly to active calls.
6. **PROTOCOL** to choose the AOC protocol. If set to **KEYPAD**, the AOC information will be sent in the national defined **KEYPAD** protocol to the user, if set to **FUNCTIONAL** the Functional protocol will be used instead.

Note: For H.323QSIG, PROTOCOL has to be set to **FUNCTIONAL**.

7. **UNITS** to choose which units shall be used to send the charging information. If set to **CURRENCY**, the charging information will be given in currency units of the specific market, if set to **CHARGING** charging units will be used.

Note: For H323QSIG, UNITS have to be set to **CHARGING**.

8. **REQUEST** to choose if AOC is only invoked if it is explicitly requested by the user in the SETUP message (REQUEST = ‘Y’) or if it is invoked for every call (REQUEST = ‘N’).

Note: For H.323QSIG, REQUEST has to be set to ‘Y’.

2.4.3 Message Protocols

The AOC is specified by ETSI standards. Three type of AOC is defined :

- **AOC-S** : Advice of Charge at the beginning of the call. The main goal is to advise the user about how the communication will be charged. Specified in ETS 300 178 [1].
- **AOC-D** : Advice of Charge during a call. Information about the cost (units or currency) is delivered continuously during the call. Specified in ETS 300 179 [2].
- **AOC-E** : Advice of Charge at the end of the call. Information about the total cost of the communication is delivered during the disconnection. Specified in ETS 300 180 [3].

The signalling protocol used for the AOC is defined in ETS 300 182 [4].

For the purpose of this activity, the AOC information is mapped to H.323 / H.225 call signalling messages [5], using the Q.931 Facility Information Element [6] to carry charging requests and charging information.

The AOC Q.931 Facility Information Element is supported in the messages shown in the table below. The codeset change is done using a Q.931 Locking Shift information element.

Table 1 Messages which can contain a Q.931 Advice Of Charge IE

MESSAGE TYPE	DIRECTION	COMMENTS
SETUP	user -> network	may be used to carry AOC-D and / or AOC-E invoke APDUs
FACILITY	user -> network	may be used to carry AOC-D and / or AOC-E invoke APDUs
FACILITY	network -> user	used to carry AOC-D (aocInterim) information
FACILITY	network -> user	also used to carry returnError and returnResult APDUs
CONNECT	network -> user	used to carry AOC-D returnError APDUs, reporting 'Service not Available' or 'supplementary Service Interaction Not Allowed'
RELEASE COMPLETE	network -> user	may be used for AOC-E (aocFinal) information

If no charge is available for a call (datafill error or CS2000 resource problem) no indication is sent to the user. The call is released depending on the AOCREL parameter (if AOCREL is TRUE), the Q.931 RELEASE COMPLETE message contains no AOC information.

2.4.4 AOC Requests

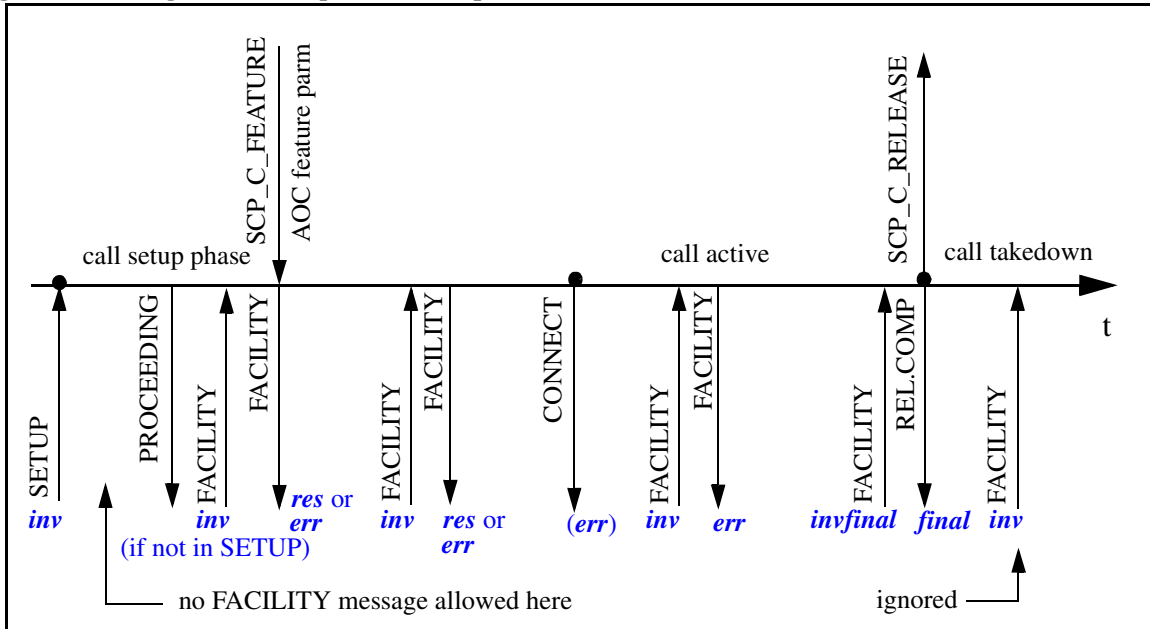
AOC requests from the originating H.323 gateway can be received in Facility IEs included in either SETUP or FACILITY messages. An AOC request in turn is a ROSE Invoke APDU with one of the operations defined for AOC in ISO 15049/ECMA-211 [10] and ISO 15050/ECMA-212 [11].

Figure 7 on page 50 shows the per-call sequence of AOC requests and responses on a relative time scale, as supported by this activity. The H.323 Gatekeeper should be imagined as being on the time axis. Messages above the time axis are from/to the CS2000 Core, and messages below the time axis are from/to the originating H.323 gateway.

Table 2 AOC APDU types

Request	Definition
<i>inv</i>	invoke APDU requesting AOC-D
<i>res</i>	returnResult APDU reporting positive acknowledgement for an AOC-D request
<i>err</i>	returnError APDU reporting negative acknowledgement for an AOC-D request (with error values 'notAvailable' or 'supplementaryServiceInteraction NotAllowed')
<i>invfinal</i>	invoke APDU requesting AOC-E
<i>final</i>	invoke APDU reporting AOC-E final charge
	Bullets on the time axis delineate call phases. Only messages relevant for AOC request handling are shown.

Figure 7 Timings of AOC requests and responses



- An **inv** APDU may be sent in either SETUP or FACILITY message, but not in both.
- An **inv** APDU in a FACILITY message may be sent after PROCEEDING and before CONNECT. Instead of PROCEEDING there may be a SETUP ACK message right before the (internal) SCP_C_FEATURE message.
- An **err** APDU in the CONNECT message will only be sent if an **inv** APDU was previously received, but AOC service is not provisioned in table TRKOPTS.
- An **inv** APDU received after CONNECT and before RELEASE will be replied with an **err** APDU in FACILITY (*supplementary Service Interaction Not Allowed*).
- An **inv** APDU received after RELEASE COMPLETE will be discarded by the CS2000 without reply.
- An **invfinal** APDU MAY be sent in a FACILITY message up to the beginning of the call takedown phase. Please note that H323 QSIG does support a special forward clearing procedure for AOC calls: the originating gateway may send getFinalCharge.inv in a FACILITY message which triggers a call release initiated by the CS2000.

2.4.5 Charge Information Messages

The AOC charging information will be transported in a Facility Information Element as part of the FACILITY and RELEASE COMPLETE messages as defined in ISO 15049/ECMA-211 [10] and ISO 15050/ECMA-212 [11].

The format of the AOC currency units messages for both AOC-D and AOC-E will be as defined in ISO 15049/ECMA-211 [10] and ISO 15050/ECMA-212 [11]. If the originating GW offers AOC information in the ETSI format (ETS 300 179 [2] and ETS 300 180 [3]) it would have to translate the ECMA encoded messages into ETSI format.

The following figures show the H.225[Q.931] (H.225 with embedded Q.931) message sequence charts relevant for the AOC functional protocol implementation of this activity.

Figure 8 depicts a message sequence typical for AOC-D where the originator takes down the call (Clear Forward).

Figure 8 AOC-D message sequence (Clear Forward)

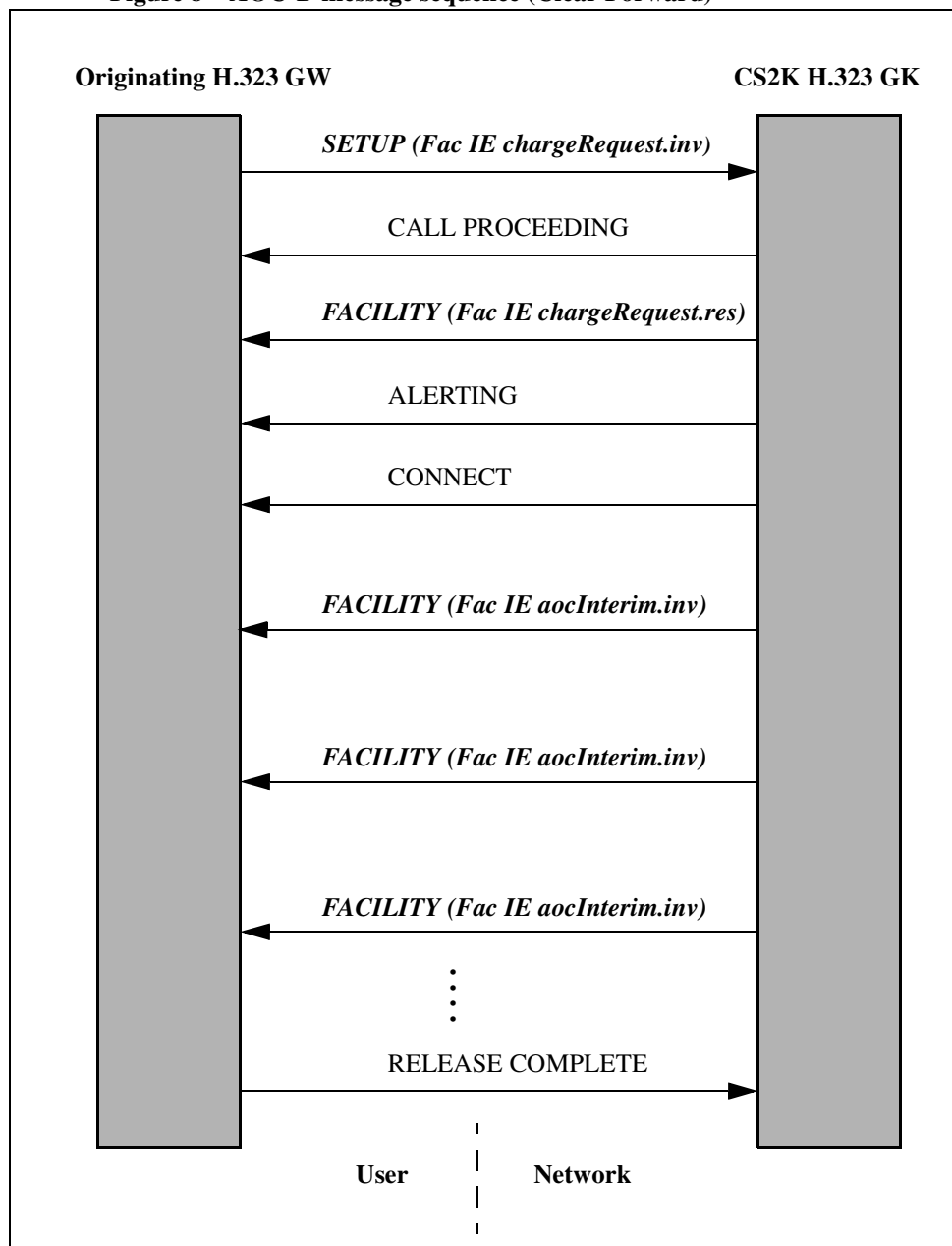
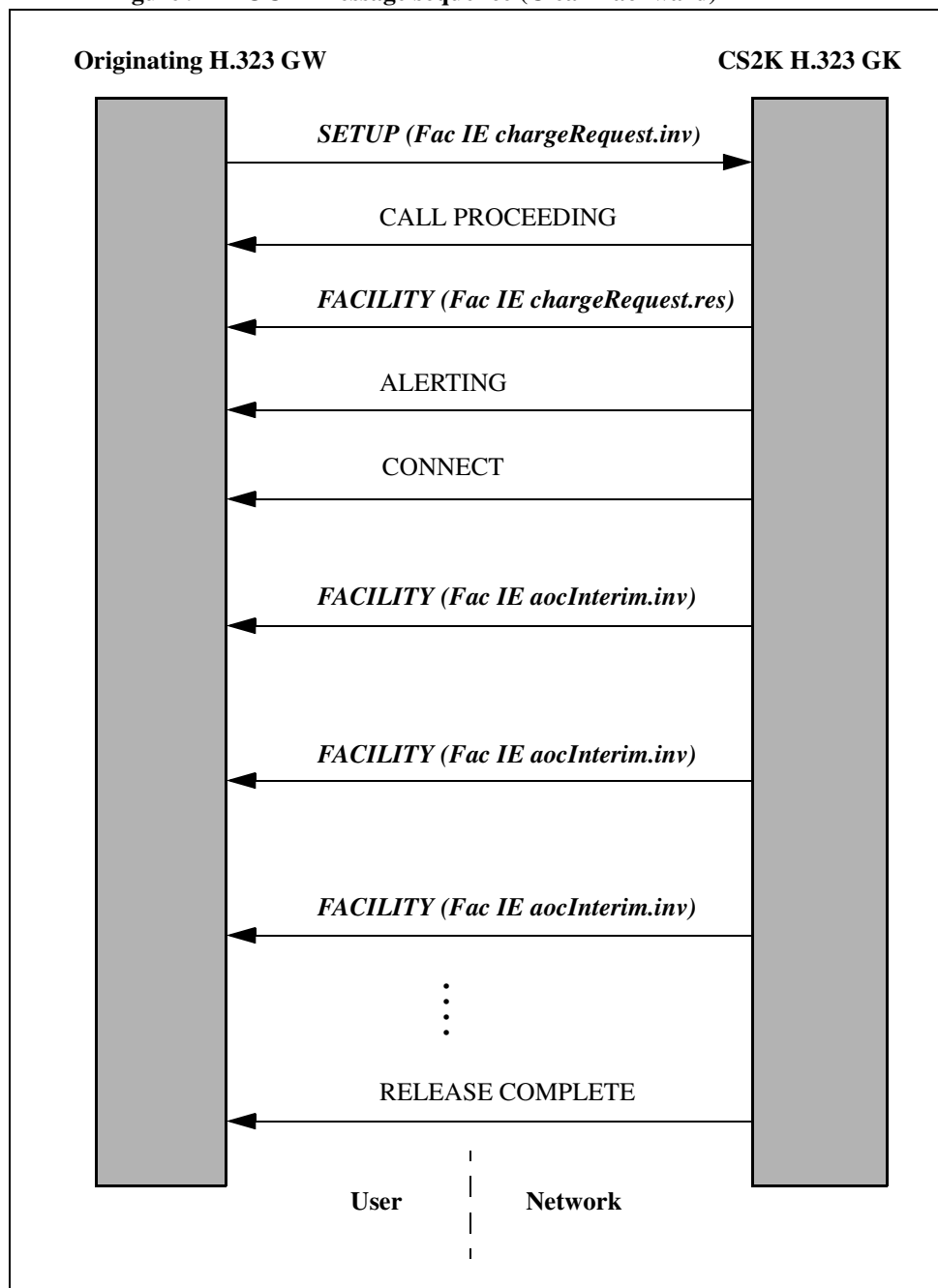


Figure 9 depicts a message sequence typical for AOC-D where the terminator takes down the call (Clear Backward).

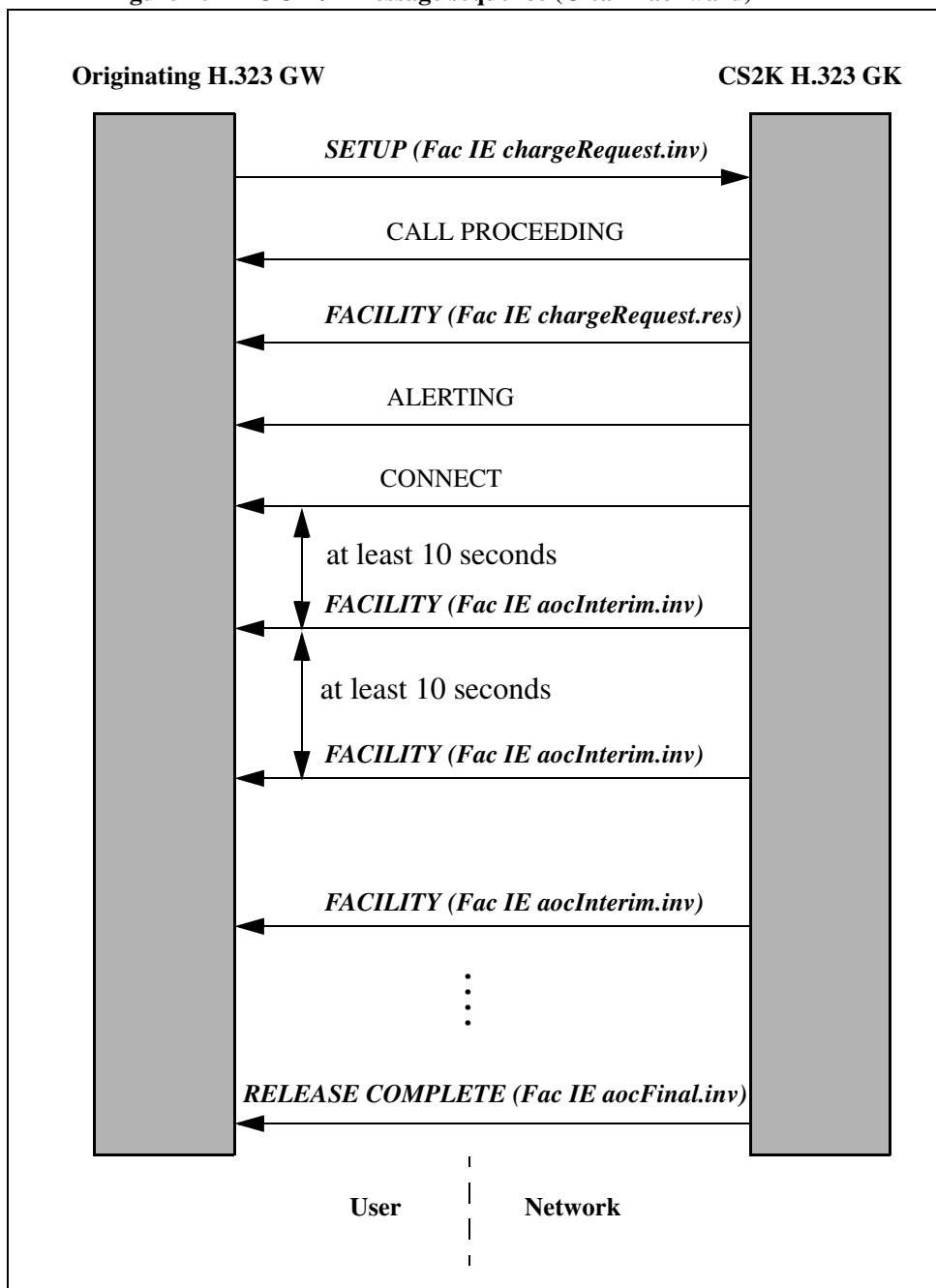
Figure 9 AOC-D message sequence (Clear Backward)



The following figures show the H.225[Q.931] message sequence charts for delivering **both** AOC-D **and** AOC-E information, considering two call takedown scenarios.

Figure 10 depicts a typical AOC message sequence where both AOC-D and AOC-E are activated at call setup time.

Figure 10 AOC-D/E message sequence (Clear Backward)



For the format of the FACILITY message please refer to H.225 [5] and Q.931 [6].

For the format of the AOC Facility IE, please refer to ISO 15049/ECMA-211 [10] and ISO 15050/ECMA-212 [11].

The encoding used for sending the charge units in the AOC Facility IE is ASN.1 and is done according to ITU-T Recommendations [12] - [19].

If a call is free of charge, this is indicated by sending an indication “*free of charge*”.

In case of AOC-D the “*free of charge*” indication is sent twice, after CONNECT and at the end of the call.

In case of AOC-E the “*free of charge*” indication is sent once at the end of the call. Sending of “*free of charge*” as a response to an AOC request is not supported. Note that this does not lead to a non-compliance to ETS 300 179 [2] and ETS 300 180 [3].

2.5 Hardware Requirements or Dependencies

An appropriate H.323 GW from a 3rd party vendor being able to convert Facility messages from ECMA format ISO 15049/ECMA-211 [10] and ISO 15050/ECMA-212 [11] into ETSI format ETS 300 179 [2] and ETS 300 180 [3] is needed.

2.6 Software Requirements or Dependencies

This feature requires the following features to be activated by SOC:

- **NETK0024** Network AOC Tariff
- NSUP0020 NAOC/PCA Supp Svcs
- NSUP0023 PCA SW Metering Support for Billing
- PBXT0011 ETSI PRI Info
- PBXT0018 QSIG AOC

NAOC tariff information is required, since this feature reuses the NAOC framework. If no NAOC information is provided, the payment ceiling counter cannot be updated for that call. NAOC datafill including the NAOC tables and translation options have to be set up in an appropriate way. Please refer to [1] - [7] for additional information.

2.7 Restrictions/Limitations

2.7.1 Interactions

Interactions with terminators other than the following are *not* supported:

-
- ETSI ISUP V1
 - ETSI ISUP V2
 - ETSI PRI
 - QSIG
 - IBN
 - BRI
 - V5.2 IBN

2.7.2 Restrictions/Limitations

Only some few new limitations or restrictions are introduced by the current activity:

1. Sending of AOC charge information as **currency** units is not supported for H.323 QSIG trunks yet.
2. AOC calculation based on the **charging interval** introduced with A00002625 [39] is not supported
3. A delta may exist between the number of charge units saved in the AMA record by the CM feature A00002638 [38] controlled by SOC NSUP0023 and the number of charge units provided by the AOC metering counter in the GWC. This is due to charge interval based calculation done in the CM.
4. The GWC calculation of the AOC does not influence or change AMA records extension introduced with A00002638 [38]. There are no direct interactions between the AMA billing system and the AOC functionality in the GWC.
5. AOC on H.323 QSIG is only supported for **bearer calls**. AOC on H.323 QSIG for non-bearer calls is not supported. Facility IEs with AOC operations for these calls are transparently passed through the CS2000.

The enumeration below lists all known restrictions, which have been introduced by the previous activities AF7344 [35], A59024423 [36], A590038835 [37], A59020791 [33]

6. **AOC-S** (AOC at call setup) is not supported.
7. Provisioning of AOC can only be per trunk group and per GWC. AOC request is always on a per call basis.
8. Out of the supported AOC modes, only those will be delivered which are requested and provisioned at the same time.
9. Only connection-oriented charging information is transmitted to the user (charges for supplementary services are not included).

10. 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. If the AOCREL boolean is set in table ***TRKOPTS***, the call is released, otherwise it is not released.
11. 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.
12. 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.
13. 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.
14. Basic Service discounts are not supported on H.323 QSIG because there is no formal definition of Basic Service for H.323 QSIG, 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 QSIG.
15. 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
16. The SESM interface for table ***SERVRINV*** does not support the AOC option. This option has to be manually added to the table ***SERVRINV***.
17. 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).
18. Interactions with supplementary services other than those specified in the QSIG AOC standards will not be handled.
 - a. any '***aocComplete***' request at Call Transfer will be rejected with a ReturnError APDU with error code '***supplementaryServiceInteractionNotAllowed***';
 - b. any '***aocDivChargeReq***' will be ignored but not passed along towards the terminator.
19. The currency name can only consist of up to 10 capital letters (no lower case and blanks supported).
20. Currency name changes affect calls in progress as well as new calls.
21. It is possible to define only 16 currency names and 16 currency units conversion factor per Call Server.

-
22. A conversion factor change does not affect calls in progress; it only affects calls established after the change.
 23. A dummy sourceEntityAddress = 0 will be coded in the NFE of outpulsed Facility IEs, because PINX are not supported by QSIG GF.
 24. 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.
 25. 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.
 26. 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.
 27. 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 $\geq$ 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.
 28. Table *TRKOPTS*, AOC option, AOCREL = Yes datafill does not have an effect in the following situations (calls are not released):
 - a. 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.
 - b. 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.
 29. 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.
-

30. AOC tariff determination is supported only for the combined CGP/CDP scenario. Support for the French NAO trunk metering functionality (ITX/TAX messages) is not part of this activity. The translations table **xxHEAD** / **xxCODE** will therefor have to use the keyword (**NAOC** xxxx)

31. The following restrictions already exist for the NAO trunk tariff database

- only 220 operators (16 carrier and 204 reseller) are available per CS2000 node
- a pool of up to 64K tariffs is available for all operators (carriers and resellers) on a single CS2000 node
- every carrier can adress up to 1022 zones and up to 1022 tariffs. Zones cannot be shared between incompatible zone classes
- a pool of up to 30 TCOs is available for all operators (carrier and reseller) on a single CS2000 node. TCOs can be shared between operators
- zoning for international calls is not available on a reseller basis
- only 10,000 ONDCs can be used for zoning national calls
- only 511 discounts are available per single CS2000 node
- all exceptions have to be zoned as SERVICE calls
- up to 4 million SERVICE DNs can be datafilled in table SERVZONE

2.8 Glossary

Term	Description
AOC	Advice of Charge
BRI	Basic Rate interface
CDN	Called Party Directory Number
CDP	Charge Determination Point
CGN	Calling Party Directory Number
CGP	Charge Generation Point
CS	Carrier Selection
CS2000	Communication Server 2000
CS2K	Communication Server 2000
ELN	Essential Line
ETSI	European Telecommunication Standard Institute
IAM	Initial Address Message
IBN	Integrated Business Network
IP	Internet Protocol
ISUP	Integrated Services Digital Network User Part
LNP	Local Number Portability
MMP	Multi Market Platform
NAOC	Network Advice of Charge
PINX	Private Integrated Services Network Exchange
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
UXLA	Universal Translations
XLA	Translations

2.9 References

REF #	Description of Reference
[1]	<i>ETS 300 178 - ISDN; Advice of Charge: charging information at call set-up time supplementary service, Service description, October 1992</i>
[2]	<i>ETS 300 179 - ISDN; Advice of Charge: charging information during the call supplementary service, Service description, October 1992</i>
[3]	<i>ETS 300 180 - ISDN; Advice of Charge: charging information at the end of the call supplementary service, Service description, October 1992</i>
[4]	<i>ETS 300 182 - ISDN; Advice of Charge supplementary service, DSS-1 protocol, April 1993</i>
[5]	<i>ITU-T H.225.0 - Call signalling protocols and media stream packetization for packet-based multimedia communication systems (2000)</i>
[6]	<i>ITU-T Q.931 - ISDN user-network interface layer 3 specification for basic call control</i>
[7]	<i>ITU-T Q.932 - Generic procedures for the control of ISDN supplementary services</i>
[8]	<i>ISO/IEC 11572 / ECMA-142 and ISO/IEC 11574 / ECMA-143 - QSIG Basic Call</i>
[9]	<i>ISO/IEC 11582 / ECMA-165 - QSIG Generic functional protocol</i>
[10]	<i>ISO/IEC 15049 / ECMA-211 - QSIG Advice of Charge - Specification, Functional Model and Information Flows</i>
[11]	<i>ISO/IEC 15050 / ECMA-212 - QSIG Advice of Charge - Interexchange Signalling</i>
[12]	<i>ITU-T X.680 Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation (1997)</i>
[13]	<i>ITU-T X.681 Information technology - Abstract Syntax Notation One (ASN.1): Information object specification (1997)</i>
[14]	<i>ITU-T X.682 Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification (1997)</i>
[15]	<i>ITU-T X.683 Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications (1997)</i>
[16]	<i>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)</i>

-
- [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] *PRIARHLD - Legacy PRI Rearchitecture - Phase 1A; PLS FMDOC*
 - [26] *ELO001 - Euro ISDN Advice of Charge SIM; PLS FMDOC*
 - [27] *ND0035 - AOC for NLOs SIM; PLS FMDOC*
 - [28] *CSE P22-30A; Call Control for ISDN Interfacing Protocol D, Layer 3 (for interfaces S and T)*
 - [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 - NAOX 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*

2.10 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)_____

Figure 12 Overview of the NAOC and PCA development

Type	Stream	ACTID	Description of Reference
N A O C	MMP12	59007987	<i>ETSI ISUP - Network AOC (CDP+CGP), Issue AA25, PLS FMDOC module: network_aoc_etsi_isup.</i>
		59008229	<i>ETSI ISUP - Network AOC Tariff And Time Of Day Switchover (CDP), Issue AA67, PLS FMDOC module: naoc_etsi_isup_tariff_db_tco.</i>
		59007780	<i>Network AOC CGP Function, Issue AA18, PLS FMDOC module: A59007780.</i>
	MMP13	59012308	<i>ETSI ISUP Network AOC - analog enhancement, Issue AA15, PLS FMDOC module A59012308 (TDM onlly)</i>
		59012315	<i>ETSI ISUP Network AOC - V5.2 enhancement, Issue AA02, PLS FMDOC module A59012315</i>
		59013775	<i>Network AOC: Integrated CGP and CDP, Issue AA27, PLS FMDOC module: A59013775.</i>
	ISNH03	59032878	<i>NAOC on PRI, Issue AA05, PLS FMDOC module: A59032878.</i>
P C A	SN04	59034497	<i>Payment ceiling for Succession Intl. Cable IP, Issue AA32, PLS FMDOC module: A59034497.</i>
	SN05	59039121	<i>NAOC and PCA Feature Interworkings with 3WC, CFx, CXR and HOLD, Issue AA30, PLS FMDOC module: A59039121.</i>

NAOC	SN06	89007454	<i>NAOC German Regulatory Enhancements, Issue AA17, PLS FMDOC module: A89007454.</i>
PCA		89007461	<i>Payment Ceiling Regulatory Enhancements, Issue AA40, PLS FMDOC module: A89007461.</i>
NAOC	SN06.2	A00001927	<i>Line Hardware Metering, Issue AA03, PLS FMDOC module: A00001927.</i>
		A00002938	<i>Full Line HW Metering / Billing Compliance, Issue AA12, PLS FMDOC, module: A00002625.</i>
	SN07	A00002625	<i>Full Line HW Metering / Billing Compliance, Issue AA12, PLS FMDOC, module: A00002625.</i>
		A00002637	<i>NAOC Trunk Metering Enhancements, Issue AA02, PLS FMDOC module: A00002637.</i>
		A00002909	<i>Telekom ISUP (T-ISUP), Issue AA24, PLS FMDOC module A00002909</i>
		A00004933	<i>Indian ISUP Charging, Issue AA02, PLS FMDOC module A00004933</i>
		A00002638	<i>PCA SW Metering Billing Compliance, Issue AA14, PLS FMDOC module A00002638</i>
		S00002638	<i>Software Metering support for Billing, Issue AA02, PLS FMDOC module S00002638</i>
PCA			
NAOC & PCA			

2.11 Annex A: Facility Information Elements

This annex provides typical, albeit not normative, examples of Facility Information Elements the CS2000 H.323 Gatekeeper is able to generate and. The structure of AOC information carried in H.225[Q.931] Facility Information Elements (FIEs) is as follows.

I. Examples of upstream AOC FIEs (taken from automated STEP test cases)

```
#define AOC_D_CHR_REQ  "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 03"
#define AOC_E_CHR_REQ  "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 04"
#define AOC_DE_CHR_REQ "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 05"
#define GET_FINAL_CHR  "9F AA 06 80 01 00 82 01 00 8B 01 01 A1 08 02 01 06 02 01 3C 05 00"

#
# NFE |Interpr | chgreg
#define AOC_D_CHR_REQ  "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 03"
#define AOC_E_CHR_REQ  "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 04"
#define AOC_DE_CHR_REQ "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 05"
#define GET_FINAL_CHR  "9F AA 06 80 01 00 82 01 00 8B 01 01 A1 08 02 01 06 02 01 3C 05 00"
```

```

#define AOC_D_CHR_REQ  "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 03"
#define AOC_E_CHR_REQ  "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 04"
#define AOC_DE_CHR_REQ "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 05"
#define GET_FINAL_CHR  "9F AA 06 80 01 00 82 01 00 8B 01 01 A1 08 02 01 06 02 01 3C 05 00"
#                          |           NFE                      |Interpr | getFinalChg

#define AOC_D_CHR_REQ  "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 03"
#define AOC_E_CHR_REQ  "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 04"
#define AOC_DE_CHR_REQ "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 05"
#define GET_FINAL_CHR  "9F AA 06 80 01 00 82 01 00 8B 01 01 A1 08 02 01 06 02 01 3C 05 00"

#define AOC_D_CHR_REQ  "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 03"
#define AOC_E_CHR_REQ  "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 04"
#define AOC_DE_CHR_REQ "9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30
05 30 03 0A 01 05"
#define GET_FINAL_CHR  "9F AA 06 80 01 00 82 01 00 8B 01 01 A1 08 02 01 06 02 01 3C 05 00"

```

II. Examples of upstream and downstream AOC FIEs (taken from STEP traces)

```

up      SETUP      1c 1b 9f aa 06 80 01 00 82 01 00 8b 01 02 a1 0d 02 01 05 02 01 3b 30
05 30 03 0a 01 05

down    FACILITY   1c 1d 9f aa 0b 80 01 01 a1 03 80 01 30 82 01 00 a2 0d 02 01 05 30 08
02 01 3b 30 03 0a 01 05

up      FACILITY   1c 1b 9f aa 06 80 01 00 82 01 00 8b 01 02 a1 0d 02 01 05 02 01 3b
30 05 30 03 0a 01 03

down    FACILITY   1c 1d 9f aa 0b 80 01 01 a1 03 80 01 30 82 01 00 a2 0d 02 01 05 30
08 02 01 3b 30 03 0a 01 03

down    FACILITY   1c 31 9f aa 0b 80 01 01 a1 03 80 01 30 82 01 00 8b 01 00 a1 1e 02
01 01 02 01 3e 30 16 30 14 a1 12 81 08 43 48 41 52 47 49 4e 47 a2 06 81 01 4b 82 01 03

down    FACILITY   1c 32 9f aa 0b 80 01 01 a1 03 80 01 30 82 01 00 8b 01 00 a1 1f 02
01 02 02 01 3e 30 17 30 15 a1 13 81 08 43 48 41 52 47 49 4e 47 a2 07 81 02 00 81 82 01 03

down    FACILITY   1c 32 9f aa 0b 80 01 01 a1 03 80 01 30 82 01 00 8b 01 00 a1 1f 02
01 03 02 01 3e 30 17 30 15 a1 13 81 08 43 48 41 52 47 49 4e 47 a2 07 81 02 00 8b 82 01 03

down    FACILITY   1c 32 9f aa 0b 80 01 01 a1 03 80 01 30 82 01 00 8b 01 00 a1 1f 02
01 04 02 01 3e 30 17 30 15 a1 13 81 08 43 48 41 52 47 49 4e 47 a2 07 81 02 00 8e 82 01 03

down    FACILITY   1c 32 9f aa 0b 80 01 01 a1 03 80 01 30 82 01 00 8b 01 00 a1 1f 02
01 05 02 01 3e 30 17 30 15 a1 13 81 08 43 48 41 52 47 49 4e 47 a2 07 81 02 00 91 82 01 03

down    FACILITY   1c 31 9f aa 0b 80 01 01 a1 03 80 01 30 82 01 00 8b 01 00 a1 1e 02
01 06 02 01 3e 30 16 30 14 a1 12 81 08 43 48 41 52 47 49 4e 47 a2 06 81 01 0f 82 01 04

down    FACILITY   1c 32 9f aa 0b 80 01 01 a1 03 80 01 30 82 01 00 8b 01 00 a1 1f 02
01 07 02 01 3e 30 17 30 15 a1 13 81 08 43 48 41 52 47 49 4e 47 a2 07 81 02 00 9b 82 01 03

```

```

down    FACILITY    1c 31 9f aa 0b 80 01 01 a1 03 80 01 30 82 01 00 8b 01 00 a1 1e 02
01 08 02 01 3e 30 16 30 14 a1 12 81 08 43 48 41 52 47 49 4e 47 a2 06 81 01 10 82 01 04

down    FACILITY    1c 32 9f aa 0b 80 01 01 a1 03 80 01 30 82 01 00 8b 01 00 a1 1f 02
01 09 02 01 3e 30 17 30 15 a1 13 81 08 43 48 41 52 47 49 4e 47 a2 07 81 02 00 a5 82 01 03

down    DISCONNECT 1c 32 9f aa 0b 80 01 01 a1 03 80 01 30 82 01 00 8b 01 00 a1 1f 02
01 0a 02 01 3d 30 17 30 15 a1 13 81 08 43 48 41 52 47 49 4e 47 a2 07 81 02 00 a8 82 01 03

up      SETUP      1c 1b 9f aa 06 80 01 00 82 01 00 8b 01 02 a1 0d 02 01 05 02 01 3b 30
05 30 03 0a 01 05

down    FACILITY    1c 16 9f aa 0b 80 01 01 a1 03 80 01 30 82 01 00 a3 06 02 01 05 02 01 03

```

III. AOC FIEs, decomposed

1) Upstream AOC_D_CHR_REQ - Advice Of Charge During Call Charge Request

```

1C 1B 9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30 05 30 03 0A 01 03
1C 1B
 9F          # Protocol Profile = Networking Extensions
AA 06       # Network Facility Extensions
 80 01 00    # Source Entity = endPINX(0)
 82 01 00    # Destination Entity = endPINX(0)
8B 01 02    # Interpretation APDU = rejectAnyUnrecognisedInvokePdu(2)
A1 0D       # Rose Invoke APDU
 02 01 05    # Invoke Id = 5
 02 01 3B    # Invoke Opcode = ChargeRequest
 30 05       # ChargeRequestArg = Sequence of
 30 03       # AdviceModeCombinations = Sequence of
 0A 01 03    # 03 = Interim = Advice Of Charge During Call

```

2) Upstream AOC_E_CHR_REQ - Advice Of Charge At End of Call Charge Request

```

1C 1B 9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30 05 30 03 0A 01 04
1C 1B
 9F          # Protocol Profile = Networking Extensions
AA 06       # Network Facility Extensions
 80 01 00    # Source Entity = endPINX(0)
 82 01 00    # Destination Entity = endPINX(0)
8B 01 02    # Interpretation APDU = rejectAnyUnrecognisedInvokePdu(2)
A1 0D       # Rose Invoke APDU
 02 01 05    # Invoke Id = 5
 02 01 3B    # Invoke Opcode = ChargeRequest
 30 05       # ChargeRequestArg = Sequence of
 30 03       # AdviceModeCombinations = Sequence of
 0A 01 04    # 04 = Final = Advice Of Charge At End of Call

```

3) Upstream AOC_DE_CHR_REQ - Advice Of Charge During and End Of Call Charge Request

```

1C 1B 9F AA 06 80 01 00 82 01 00 8B 01 02 A1 0D 02 01 05 02 01 3B 30 05 30 03 0A 01 05
1C 1B
 9F          # Protocol Profile = Networking Extensions
AA 06       # Network Facility Extensions
 80 01 00    # Source Entity = endPINX(0)
 82 01 00    # Destination Entity = endPINX(0)
8B 01 02    # Interpretation APDU = rejectAnyUnrecognisedInvokePdu(2)
A1 0D       # Rose Invoke APDU
 02 01 05    # Invoke Id = 5
 02 01 3B    # Invoke Opcode = ChargeRequest
 30 05       # ChargeRequestArg = Sequence of

```



```

    30 03      # AdviceModeCombinations = Sequence of
    0A 01 05   # 05 = interimFinal = Advice Of Charge During and End Of Call

```

4) Upstream GET_FINAL_CHR - Advice of Charge Get Final Charge Request

```

1C 16 9F AA 06 80 01 00 82 01 00 8B 01 01 A1 08 02 01 06 02 01 3C 05 00
1C 16
  9F      # Protocol Profile = Networking Extensions
  AA 06   # Network Facility Extensions
    80 01 00 # Source Entity = endPINX(0)
    82 01 00 # Destination Entity = endPINX(0)
  8B 01 01 # Interpretation APDU = clearCallIfAnyInvokePduNotRecognised(1)
  A1 08   # Rose Invoke APDU
    02 01 06 # Invoke Id = 6
    02 01 3C # Invoke Opcode = getFinalCharge
    05 00   # DummyArg = none

```

5) Downstream FACILITY (Charge Request ReturnResult APDU)

```

1C 1D 9F AA 0B 80 01 01 A1 03 80 01 30 82 01 00 A2 0D 02 01 07 30 08 02 01 3B 30
03 0A 01 03
1C 1D
  9F      # Protocol Profile = Networking Extensions
  AA 0B   # Network Facility Extensions
    80 01 01 # Source Entity = anyTypeOfPINX(1)
  A1 03 80 01 30 # sourceEntityAddress = dummy source entity address of '0'
    82 01 00 # Destination Entity = endPINX(0)
    A2 0D   # Rose ReturnResultPDU
    02 01 07 # Invoke Id = 7
  30 08   # Sequence of
    02 01 3B # Invoke Opcode = ChargeRequest
    30 03   # Sequence of
    0A 01 03 # Advice Of Charge During Call

1C 1D 9F AA 0B 80 01 01 A1 03 80 01 30 82 01 00 A2 0D 02 01 08 30 08 02 01 3B 30
03 0A 01 05
1C 1D
  9F      # Protocol Profile = Networking Extensions
  AA 0B   # Network Facility Extensions
    80 01 01 # Source Entity = anyTypeOfPINX(1)
  A1 03 80 01 30 # sourceEntityAddress = dummy source entity address of '0'
    82 01 00 # Destination Entity = endPINX(0)
    A2 0D   # Rose ReturnResultPDU
    02 01 08 # Invoke Id = 8
  30 08   # Sequence of
    02 01 3B # Invoke Opcode = ChargeRequest
    30 03   # Sequence of
    0A 01 05 # Advice Of Charge During and at End Of Call

```

6) Downstream FACILITY (Charge Request ReturnError APDU)

```

1C 16 9F AA 0B 80 01 01 A1 03 80 01 30 82 01 00 A3 06 02 01 09 02 01 03
1C 16
  9F      # Protocol Profile = Networking Extensions
  AA 0B   # Network Facility Extensions
    80 01 01 # Source Entity = anyTypeOfPINX(1)
  A1 03 80 01 30 # sourceEntityAddress = dummy source entity address of '0'
    82 01 00 # Destination Entity = endPINX(0)
    A3 06   # Rose ReturnErrorPDU
    02 01 09 # Invoke Id = 9
    02 01 03 # error code = 03 = notAvailable

```

7) Downstream FACILITY (Charge Request ReturnError APDU)

```

1C 16 9F AA 0B 80 01 01 A1 03 80 01 30 82 01 00 A3 06 02 01 09 02 01 0a
1C 16
  9F          # Protocol Profile = Networking Extensions
  AA 0B       # Network Facility Extensions
80 01 01      # Source Entity = anyTypeOfPINX(1)
A1 03 80 01 30 # sourceEntityAddress = dummy source entity address of '0'
82 01 00      # Destination Entity = endPINX(0)
  A3 06       # Rose ReturnErrorPDU
02 01 09      # Invoke Id = 9
02 01 0a      # error code = 0a = supplServiceInteractionNotAllowed

8) Downstream FACILITY (Charge Request Reject APDU)

1C 16 9F AA 0B 80 01 01 A1 03 80 01 30 82 01 00 A3 06 02 01 0a 80 01 02
1C 16
  9F          # Protocol Profile = Networking Extensions
  AA 0B       # Network Facility Extensions
80 01 01      # Source Entity = anyTypeOfPINX(1)
A1 03 80 01 30 # sourceEntityAddress = dummy source entity address of '0'
82 01 00      # Destination Entity = endPINX(0)
  A4 06       # Rose ReturnErrorPDU
02 01 0a      # Invoke Id = 10
80 01 02      # general problem, badly structured APDU

9) Downstream FACILITY (Charge Request Reject APDU)

1C 16 9F AA 0B 80 01 01 A1 03 80 01 30 82 01 00 A3 06 02 01 0b 80 01 02
1C 16
  9F          # Protocol Profile = Networking Extensions
  AA 0B       # Network Facility Extensions
80 01 01      # Source Entity = anyTypeOfPINX(1)
A1 03 80 01 30 # sourceEntityAddress = dummy source entity address of '0'
82 01 00      # Destination Entity = endPINX(0)
  A4 06       # Rose ReturnErrorPDU
02 01 0b      # Invoke Id = 11
81 01 02      # invoke problem, mistyped argument

10) Downstream FACILITY (Intermediate Charge Amount)

1C 31 9F AA 0B 80 01 01 A1 03 80 01 30 82 01 00 8B 01 00 A1 1E 02 01 01 02 01 3E
30 16 30 14 A1 12 81 08 43 48 41 52 47 49 4E 47 A2 06 81 01 4B 82 01 03
1C 31
  9F          # Protocol Profile = Networking Extensions
  AA 0B       # Network Facility Extensions
80 01 01      # Source Entity = anyTypeOfPINX(1)
A1 03 80 01 30 # sourceEntityAddress = dummy source entity address of '0'
82 01 00      # Destination Entity = endPINX(0)
  8B 01 00    # Interpretation APDU = discardAnyUnrecognisedInvokePdu(0)
  A1 1E       # Rose Invoke APDU
02 01 01      # Invoke Id = 1
02 01 3E      # Invoke Opcode = AocInterim
30 16         # AocInterimArg = Sequence of
  30 14       # interimCharge = specificCurrency = Sequence of
  A1 12       # recordedCurrency =
  81 08       # rCurrency = Currency = IA4string
    43 48 41 52
    47 49 4E 47 # CHARGING
  A2 06       # rAmount =
    81 01 4B   # currencyAmount = INTEGER = 75
    82 01 03   # multiplier = enum = 03 = one

11) Downstream FACILITY (Intermediate Charge Amount)

```

```

1C 32 9F AA 0B 80 01 01 A1 03 80 01 30 82 01 00 8B 01 00 A1 1F 02 01 02 02 01 3E
30 17 30 15 A1 13 81 08 43 48 41 52 47 49 4E 47 A2 07 81 02 00 81 82 01 03
1C 32
  9F                                # Protocol Profile = Networking Extensions
  AA 0B
80 01 01
A1 03 80 01 30
82 01 00
  8B 01 00
  A1 1F                                # Rose Invoke APDU
02 01 02                                # Invoke Id = 2
02 01 3E                                # Invoke Opcode = AocInterim
30 17                                # AocInterimArg = Sequence of
  30 15                                # interimCharge = specificCurrency = Sequence of
  A1 13                                # recordedCurrency =
  81 08                                # rCurrency = Currency = IA4string
    43 48 41 52
    47 49 4E 47                        # CHARGING
  A2 07                                # rAmount =
    81 02 00 81                        # currencyAmount = INTEGER = 127
    82 01 03                        # multiplier = enum = 03 = one

12) Downstream FACILITY (Intermediate Charge Amount)

1C 31 9F AA 0B 80 01 01 A1 03 80 01 30 82 01 00 8B 01 00 A1 1E 02 01 06 02 01 3E
30 16 30 14 A1 12 81 08 43 48 41 52 47 49 4E 47 A2 06 81 01 0F 82 01 04
1C 31
  9F                                # Protocol Profile = Networking Extensions
  AA 0B                                # Network Facility Extensions
80 01 01
A1 03 80 01 30
82 01 00
  8B 01 00                                # Interpretation APDU = discardAnyUnrecognisedInvokePdu(0)
  A1 1E                                # Rose Invoke APDU
02 01 06                                # Invoke Id = 6
02 01 3E                                # Invoke Opcode = AocInterim
30 16                                # AocInterimArg = Sequence of
  30 14                                # interimCharge = specificCurrency = Sequence of
  A1 12                                # recordedCurrency =
  81 08                                # rCurrency = Currency = IA4string
    43 48 41 52
    47 49 4E 47                        # CHARGING
  A2 06                                # rAmount =
    81 01 0F                        # currencyAmount = INTEGER = 15
    82 01 04                        # multiplier = enum = 04 = ten

13) Downstream FACILITY (Intermediate Charge Amount)

1C 31 9F AA 0B 80 01 01 A1 03 80 01 30 82 01 00 8B 01 00 A1 1E 02 01 08 02 01 3E
30 16 30 14 A1 12 81 08 43 48 41 52 47 49 4E 47 A2 06 81 01 10 82 01 04
1C 31
  9F                                # Protocol Profile = Networking Extensions
  AA 0B                                # Network Facility Extensions
80 01 01
A1 03 80 01 30
82 01 00
  8B 01 00                                # Interpretation APDU = discardAnyUnrecognisedInvokePdu(0)
  A1 1E                                # Rose Invoke APDU
02 01 08                                # Invoke Id = 8
02 01 3E                                # Invoke Opcode = AocInterim
30 16                                # AocInterimArg = Sequence of
  30 14                                # interimCharge = specificCurrency = Sequence of
  A1 12                                # recordedCurrency =
  81 08                                # rCurrency = Currency = IA4string
    43 48 41 52
    47 49 4E 47                        # CHARGING

```

```

A2 06          # rAmount =
  81 01 10     # currencyAmount = INTEGER = 16
  82 01 04     # multiplier = enum = 04 = ten

```

14) Downstream RELEASE COMPLETE (Final Charge Amount)

```

1C 32 9F AA 0B 80 01 01 A1 03 80 01 30 82 01 00 8B 01 00 A1 1F 02 01 0A 02 01 3D
30 17 30 15 A1 13 81 08 43 48 41 52 47 49 4E 47 A2 07 81 02 00 A8 82 01 03
1C 32
  9F          # Protocol Profile = Networking Extensions
  AA 0BA      # Network Facility Extensions
80 01 01
A1 03 80 01 30
82 01 00
  8B 01 00    # Interpretation APDU = discardAnyUnrecognisedInvokePdu(0)
  A1 1F        # Rose Invoke APDU
02 01 0A      # Invoke Id = 10
02 01 3D      # Invoke Opcode = AocFinal
30 17         # AocFinalArg = Sequence of
  30 15        # finalCharge = specificCurrency = Sequence of
  A1 13        # recordedCurrency =
  81 08        # rCurrency = Currency = IA4string
    43 48 41 52
    47 49 4E 47
A2 07         # CHARGING
  81 02 00 A8  # rAmount =
  82 01 03     # currencyAmount = INTEGER = 168
              # multiplier = enum = 03 = one

```

15) Downstream RELEASE COMPLETE (Final Charge Amount - chargeNotAvailable)

```

1C 1D 9F AA 0B 80 01 01 A1 03 80 01 30 82 01 00 8B 01 00 A1 1F 02 01 0A 02 01 3D
30 02 80 00
1C 1D
  9F          # Protocol Profile = Networking Extensions
  AA 0BA      # Network Facility Extensions
80 01 01
A1 03 80 01 30
82 01 00
  8B 01 00    # Interpretation APDU = discardAnyUnrecognisedInvokePdu(0)
  A1 1F        # Rose Invoke APDU
02 01 0A      # Invoke Id = 10
02 01 3D      # Invoke Opcode = AocFinal
30 02         # AocFinalArg = Sequence of
  80 00        # finalCharge = chargeNotAvailable = NULL

```

16) Downstream RELEASE COMPLETE (Final Charge Amount - freeOfCharge)

```

1C 1D 9F AA 0B 80 01 01 A1 03 80 01 30 82 01 00 8B 01 00 A1 1F 02 01 0A 02 01 3D
30 02 80 00
1C 1D
  9F          # Protocol Profile = Networking Extensions
  AA 0BA      # Network Facility Extensions
80 01 01
A1 03 80 01 30
82 01 00
  8B 01 00    # Interpretation APDU = discardAnyUnrecognisedInvokePdu(0)
  A1 1F        # Rose Invoke APDU
02 01 0A      # Invoke Id = 10
02 01 3D      # Invoke Opcode = AocFinal
30 02         # AocFinalArg = Sequence of
  81 00        # finalCharge = freeOfCharge = NULL

```

3: A00005932 Functional description (FN)

3.1 Feature name

Removing Loopback Trunks in CEPT DISA calls for Remote Feature Activation

3.2 Description

3.2.1 Introduction

This feature enhances the digit collection in DISA features which are CEPT Call Forwarding Remote Access (CFRA) and CEPT Remote Access (CEPTR). In existing functionality, digit collection is performed via loopback CAS trunks for all originating agents although they have capability to use UTR; that means, following kinds of originating agents below, loopback trunk is inserted between the agent and DISA feature by default:

- ISDN BRI lines
- ETSI ISUP trunks
- ETSI PRI trunks

This feature changes this behaviour, and provides flexibility in digit collection as in following hierarchical order.

- 1 collect digits via UTR if possible
- 2 collect digits via DTMF receiver (for PRI agents only)
- 3 collect digits via LOOPBACK trunk

This feature provides the possibility not to use superfluous loopback equipment and optimize the digit collection for mentioned agents on CEPT markets; when the user of CFRA/CEPTR feature will need to send digits for remote call activation, UTR or DTMF receivers (on MTMs) will be used for it. If both of them are not available, loopback trunk will be inserted as in existing functionality.

Note: Note: Throughout this document, “originating agent” refers to the originating agent of the call in the switch where DISA feature is located on.

3.2.2 General Considerations

This feature is applicable for only CEPT features related with DISA framework, and provides the algorithm as explained below.

- a. Firstly, digit collection via UTR is tried to perform if it's already available.

- b. Secondly, if UTR is not available for originating agent, digit collection via DTMF receiver on MTMs is tried to perform. (for PRI agents only)
- c. Thirdly, if both of them are not available, digit collection is performed via LOOPBACK trunks.

The following table illustrates the originating agents versus supported digit collection types.

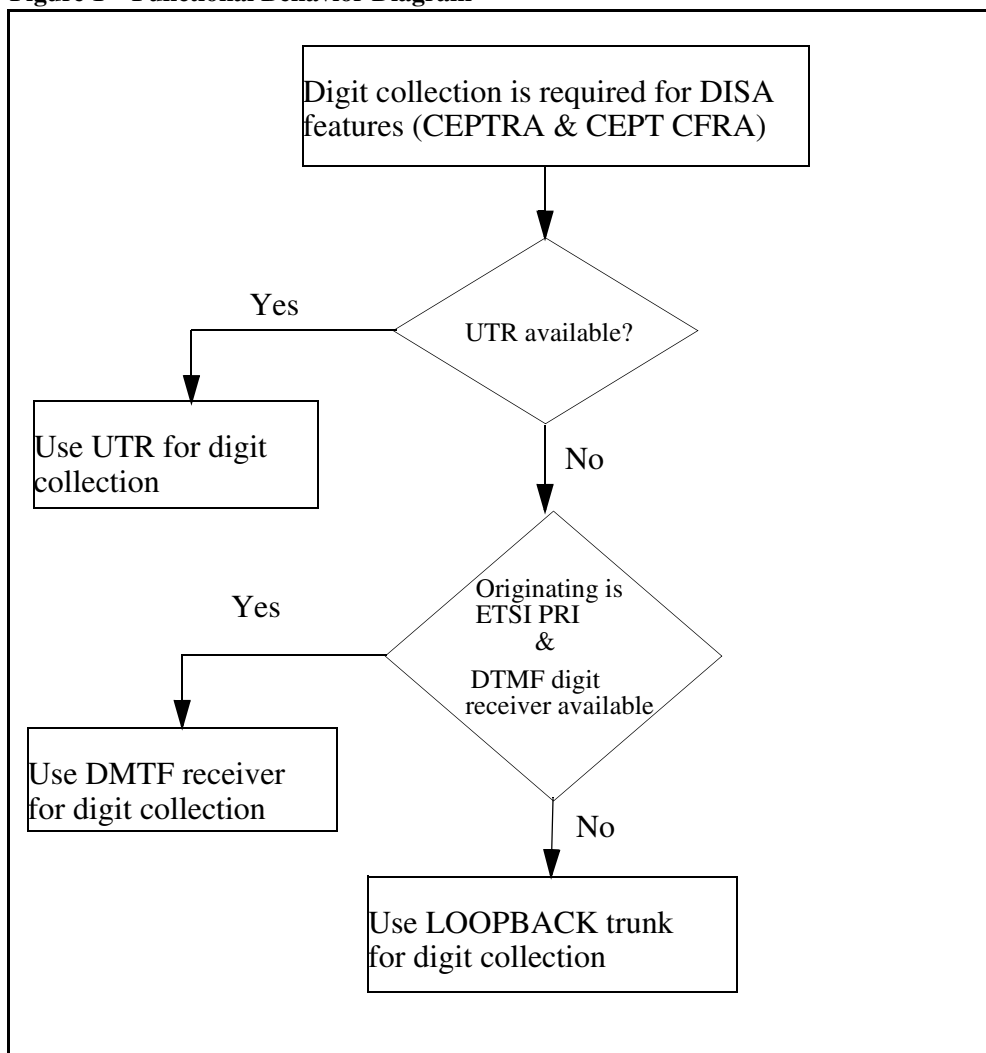
Table 1 Supported digit collection types versus originating agents

Originating Agents	Digit collection type		
	via UTR	via DTMF digit receiver	via LOOPBACK trunks
ETSI ISUP	X		X
ETSI PRI	X	X	X
R1 (NTLS01, 02, 09), R2 (Base)	X		
ETSI BRI lines	X		X
IBN/EBS lines	X		

X abbreviates this type of digit collection is supported on that agent.

As seen from Table 1, Digit collection via DTMF digit receiver cards is supported for only ETSI PRI trunks on which digit collection can be performed by UTR or Loopback trunks also.

Algorithm of choosing of which digit collection type used is simple. UTR has the first priority, DTMF digit receiver has the second, whereas loopback trunk has the last priority. The functional behavior diagram is as shown below.

Figure 1 Functional Behavior Diagram

3.3 Hardware Requirements or Dependencies

The RCVRDGT pool will be used as DTMF digit receiver in this activity, and digit receiver cards (2X48xx, where xx refers to "AB, BA, CC") should be located in MTMs.

Table RECEIVER should be provisioned as illustrated in Figure 2 below for using DTMF digit receiver in DISA calls. In order to be in service, each RCVRDGT must be taken in service by **"bsy;rts"** using the **"mapci;mtc;trks;ttp"** level.

Figure 2 DTMF digit receiver provisioning

TABLE: RECEIVER						
>lis all						
TOP						
	RCVRKEY	RCVRTYPE	TMTYPE	TMNO	TMCKTNO	
CARDCODE						

RCVRDGT	0	D	MTM	0	6	2X48CC
RCVRDGT	1	D	MTM	0	7	2X48CC
BOTTOM						

3.4 Software Requirements or Dependencies

N/A

3.5 Limitations and restrictions

In case of originating agent is ETSI PRI agent, Dial Tone is applied to the subscriber instead of SDT where it requires.

3.6 Interactions

N/A

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)_____

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.

3.8 Glossary

Table 2

Term	Description
BRI	Basic Rate Interface
CAS	Channel Associated Signaling
CEPT	Counsel for European Postal and Telecommunications
DISA	Direct Inward System Access
DTMF	Dual-Tone Multifrequency
DTM	Digital Trunk Module
EBS	Electronic Business Set
ETSI	European Telecommunications Standards Institute
IBN	International Business Network
ISDN	Integrated Services Digital Network
MTM	Maintenance Trunk Module
SDT	Special Dial Tone
UTR	Universal Tone Receiver

4: A00005962 Functional description (FN)

4.1 Feature name

CLIR Removal For Centrex Intragroup Calls

4.2 Description

4.2.1 Introduction

Calling Number Delivery Blocking Overriding (CNDBO) feature gives the customer the ability to get the calling number on his CPE even it is restricted at the originating site. This option is provisioned either customer group basis or assigned to a line via servord.

On this activity, the functionality on customer group basis is enhanced according to the requirements of Turk Telekom. A new subfield is added to customer group option CNDBO in this aim. When CNDBO is assigned to a customer group, according to the value of this subfield, first it will be determined if the option will be valid on all calls arriving to subscribers on that customer group or it will be valid only for calls where the originator and the terminator are both on this customer group.

CNDBO is a SOC option with code BPRD0001. This SOC must be ON in order to this feature be available at the office. Both nodal and network CNDBO options are activated via this SOC instead of RES00100 and RES00101.

4.2.2 New subfield CNDBOTYPE

The CNDBO customer group option is provisioned at table CUSTSTN. On current implementation, the option has no subfields. It either exists or not.

A subfield is added to the option called CNDBOYPE. It has two values:

- **ALL:** When the subfield has the value ALL, the option will be valid for all calls terminating on a subscriber at this customer group. In other words, current implementation will be valid on this choice.
- **INTRAONLY:** When the subfield has value INTRAONLY, then the CNDBO option will be valid only on calls where the originator and the terminator are both on this customer group. Calls arriving to the subscribers at this customer group from other agents, will not be affected.

Figure 1 Example of table CUSTSTN datafill

```

CI:
>table custstn
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: CUSTSTN
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
CUSTNAME:
>custyas
OPTNAME:
>cndbo
OPTION:
>cndbo
CNDBOTYPE:
>intraonly
TUPLE TO BE ADDED:
      CUSTYAS      CNDBO                      CNDBO INTRAONLY
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE

```

After ONP from a previous load to the ISN08 load, the suboption CNDBOTYPE will have the value ALL.

All trunks are not capable of carrying the customer group information. Here is an example which this information is carried: MBG trunks.

The NETCGID value for the customer group datafilled at table CUSTNTWK is used for this aim. The netinfo parameter can be seen at IAM as an optional information. Also the BGID and BGXLA parameters must be entered for corresponding customer group in BGDATA table for the MBG trunk over ANSI ISUP network. The BGID value for customer group is used for carrying customer group information via MBG trunks.

Figure 2 Example for BGDATA table datafill

BGID BGXLA OPTIONS

LOCAL 1111 (212 242 7 212) \$ (DSR) (CUSTGRP CENTREX Y 9 Y 0 60) \$

Figure 3 Example for netinfo parameter carried at MBG trunk

```

CCS7 MESSAGE TYPE: ISUP_IAM
.....

OPTIONAL PART: CALLING PARTY :
                EVEN_ODD_IND:          EVEN_NUM_NIBBLES
                NATURE_OF_ADD :         UNIQUE_NATIONAL_SIG_NUMBER
                ADDR_PREP_RESTRICTED_IND : PRESENTATION_ALLOWED
                NUMBERING_PLAN :         ISDN_TELEPHONY_NUM_PLAN
                SCREENING_IND :          NETWORK_PROVIDED
                ADDRESS_INFORMATION = 1027835479

NETWORK_INFO_PARM :
PARTY_SEL_CODE :      NETINFO_CALLING_PARTY
EXTERNAL_NETID :      0
EXTERNAL_NETCGID:     8
NETNCOS :             0

```

The External_Netcgid parameter is used to compare the calling and called party customer groups.

4.3 Hardware Requirements or Dependencies

No hardware dependency.

4.4 Software Requirements or Dependencies

None.

4.5 Limitations and restrictions

All limitations and restrictions of CNDBO feature are valid.

When INRAONLY is datafilled as subfield, for calls over trunks, the customer group information is not always carried. So, the option will be available only for calls made over trunks which netinfo information is carried through (for example MBG).

4.6 Interactions

Please refer to the interactions of basic CNDBO feature.

4.7 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)_____

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.

4.8 Glossary

Table 1

Term	Description
CND	Calling Number Delivery
CNDBO	Calling Line Delivery blocking Overriding
MGB	Meridian Business Group
CLIR	Calling Line Identity Restriction
CPE	Customer Premises Equipment
ONP	One Night Process

4.9 Recommended Reading/References

- AJ1494 - Calling Number Delivery Blocking Overriding
- AG0781 - Calling Number Delivery
- AG0778 - Calling Number Delivery Blocking
- AG1155 - Calling Number Delivery Blocking

5: A00005980 Functional description (FN)

5.1 Feature name

GSP IN CONNECT Operation Enhancement to support RouteList Parameter

5.2 Description

This feature enhances the Global Services Platform Intelligent Networks (GSP IN) service to handle the optional RouteList information received in an INAP CONNECT operation, and also implements Table RTELMAP.

5.2.1 Functional overview

This functionality covers the following developments for GSP IN:

- Enable the receiving of the RouteList parm in INAP CONNECT; with the RouteList parm containing from 1 up to 16 BusinessLineIDs
- Develop Table RTELMAP, in which the customer will be able to define, for each used BusinessLineID, the OVR Table and the Index in that OVR Table that will be used in routing.
- Validate each received BusinessLineID against Table RTELMAP datafill, and store all the valid (datafilled) BusinessLineIDs until the INAP dialogue terminates.
- Starting with the first Business Line ID, enable the routing according to the OVR Table and Index for that BusinessLineID; and then, if the routes for this BusinessLineID are exhausted without success, enabling the routing with the next BusinessLineID; until all of the BusinessLineIDs provided in the INAP CONNECT RouteList parm, and also datafilled in Table RTELMAP, are exhausted.
- If all the BusinessLineIDs in the Route List are exhausted without successful routing (Please refer to “Figure 3 RouteList parm interaction at EDP-4” on page 89. For more information see “Routing” on page 85.):
 - If an RRBCSME (EDP-4R: Route Select Failure - Interrupted) has been received before CONNECT:
 - Enable the reporting of ERBCSM (EDP4 / RSF: Route Select Failure) to the SCP.
 - Wait for a new instruction from the SCP
 - If an RRBCSME (EDP-4R) has *not* been received before CONNECT:
 - Not report ERBCSM (EDP-4) to the SCP
 - Enable normal clearing of the INAP dialogue
 - Let DMS-GSP apply GNCT treatment

- Enhance EINTRACE tool to support the new RouteList parm in INAP CONNECT. Please refer to Section “5.5.4.1 EINTRACE Enhancement” on page 91.
- Enhance GTRAVER to prompt whether a RouteList parameter is received in CONNECT, and if so to ask for a BusinessLineID, and to display the routes and outpulsed digits after CONNECT based on such a BusinessLineID. Please refer to Section “5.5.4.2 GTRAVER Enhancement” on page 92.
- Provide OVR Table Provisioning to prevent deletion of tuples that have already been datafilled in Table RTELMAP against at least one BusinessLineID, and to give a warning for a change of such tuples.
- Set Billing CDR record(s) correctly, according to current behaviour.
- Perform appropriate Error Processing, Treatment Setting, and clearing of calls, when irregular conditions arise such as, but not limited to:

No valid BusinessLineID in a RouteList parameter, incorrect Header and/or Parameter length(s) for the RouteList parm and/or the BusinessLineID sub-parameter, RouteList parameter received in a CONNECT for a TDP-2 received call, etc.

5.2.2 Feature description

The following sections describe in detail the concepts and provisioning for the different development components.

5.2.2.1 INAP Connect RouteList parm

INAP CONNECT operation requests the DMS-GSP switch to route a call to a specific destination.

Before this feature, the DMS-GSP switch supported and used the following parameters to be received in CONNECT and to be used to enter translations for routing:

- DestinationRoutingAddress
Mandatory.
- CutAndPaste

The SCP uses this parameter to instruct the DMS-GSP switch to delete (cut) a specified number of leading digits from the Called Party Number and to paste the digits that the SCP supplied in the DestinationRoutingAddress. Optional.

With this functionality, the DMS-GSP switch will also support the receiving of the following parameter in CONNECT, to be used in routing:

- **RouteList**

Contains a sequence of 1 to 3 Octet Strings. The 2nd and the 3rd Octet Strings are not used; but the 1st Octet String contains 1 to 16 Business Line IDs (indices). Each Business Line ID is mapped by the DMS-GSP to an index in table RTELMAP, which will contain the associated OVR Table ID and Index to be used in routing. Optional.

Each BusinessLineID represents an alternative International Carrier, who routes the call to the destination country. The BusinessLineIDs given in the RouteList parameter should be sent by the SCP in the order of most desirability in terms of Least Cost Routing. For each BusinessLineID, the subsequent OVR Table and Index contains a list of alternative routes, which are associated with that carrier, and should also be datafilled in the order of least cost.

5.2.2.2 RouteList parameter format

The DMS-GSP definition for the RouteList parameter in an INAP CONNECT operation is based on the Q.1218 (Ref 1 Q.1218: ITU-T Interface Recommendation for CS-1R (10/95)), as follows:

```
connect OPERATION
  ARGUMENT
    SEQUENCE {
      ...
      routeList [7] IMPLICIT SEQUENCE SIZE (1..3) OF
        OCTET STRING (SIZE (minRouteListLength..maxRouteListLength))
        OPTIONAL,
      ...
    }
```

The 1st octet string is defined as follows:

```
SEQUENCE SIZE(1..16) OF {
  BusinessLineID OCTET STRING SIZE (2)
}
```

This means, in the received INAP CONNECT RouteList parm's 1st Octet String Data, we expect to find a minimum of 1 BusinessLineID, and up to 16 BusinessLineIDs, each of 2 Bytes long Data. Hence, the maximum expected octet string size for the RouteList Octet String 1 using the above 1..16 sequence is 16 * 2 Bytes (per BusinessLineID sub-parameter) = 32 bytes.

The 2 Bytes per BusinessLineID sub-parameter comes from:

- 1 Byte [for BusinessLineID Octet String Tag of #04]
- 1 Byte [for BusinessLineID Data Length of 2 = #02]
- 2 Bytes [for BusinessLineID Data itself]

The BusinessLineID is an index that takes a value in the range {0 TO 65535}. Each BusinessLineID is checked on receipt whether it is datafilled in Table RTELMAP; and is stored as a valid BusinessLineID only if it is datafilled in Table RTELMAP.

If the RouteList parm has some problem in Header or Data length(s) or if there are 0 BusinessLineIDs in a RouteList parm, appropriate Error Handling will be performed (Please see Section “5.5.1 Logs (LG)” on page 90).

Each octet string of the RouteList parameter is implemented as a RouteListOctetString sub-parameter, with tag number of #04 for the Octet String, of Universal tag class, and as a Constructor of BusinessLineID sub-parameters (Refer to Section “5.5.4.1 EINTRACE Enhancement” on page 91 for an example of an EINTRACE output with a HEX dump of an INAP CONNECT operation containing a RouteList parameter).

The 2nd and 3rd octet strings of the RouteList parm are not used. In case DMS-SSP receives any data in the 2nd and 3rd Octet Strings:

- if the data in the 2nd or 3rd Octet Strings is structured in the same manner as the 1st Octet String (in terms of BusinessLineIDs of 2 BYTES data), the Octet Strings will be received successfully but their data will be ignored.
- if the data in the 2nd or 3rd Octet Strings is not structured in the same manner as the 1st Octet String (in terms of BusinessLineIDs of 2 BYTES data), the call will go through Error Handling and will be cleared, due to problem in received parameter.

5.2.2.3 Table RTELMAP

A new Table RTELMAP is defined to be utilized for mapping from the BusinessLineIDs provided in the INAP CONNECT RouteList parm to the desired OVR Tables and Indices to be used in routing. Up to 65536 tuples can be datafilled in Table RTELMAP.

Table 1, “RTELMAP Field Descriptions,” on page 84 describes the fields in table RTELMAP.

Table 1 RTELMAP Field Descriptions

FIELD NAME	DESCRIPTION	RANGE
BLINEID	This is the key field. It corresponds to the BusinessLineID received from the SCP.	{0..65535}

FIELD NAME	DESCRIPTION	RANGE
TABID	OVR Table Identifier.	OVR0 - OVR89
KEY	OVR Table Index in the identified OVR Table above.	{0..1023}

For more information on Table RTELMAP datafill, please refer to Section “5.5.2.1 New/modified table list” on page 90.

5.2.2.3.1 Mapping BusinessLineIDs to Physical Route Lists

BusinessLineIDs provided in the RouteList parameter are mapped to physical route lists in the new table RTELMAP.

The technician must define the required OVR route list by entering data into an OVR table at a specific OVR index (e.g. table **OVR4** position **243**). Enter this OVR index against the associated BusinessLineID value in table RTELMAP.

5.2.2.4 Processing the Connect Operation with Route List parm

This section describes how the Connect operation, containing a RouteList parm, is processed on the DMS-GSP SSP switch. At the end of the section, several flow charts show the service logic of this operation.

Call processing with RouteList parm in Connect

If the RouteList parameter is present in the Connect operation, then call processing resumes at PIC_4 (Routing & Alerting).

If the CutAndPaste parameter is present, the number of most significant digits specified in this parameter are removed from the Called Party Number, and the digits in the DRA parameter are appended onto the beginning. If the CutAndPaste parameter is not present, the DRA is used to overwrite the Called Party Number.

When the RouteList parm is present, the IN Pretranslator Name is reset to NPRT (No Pretranslation), and this overrides the IN_PRTNM in Table OFCVAR. The translation after INAP CONNECT is started through the BusinessLineID at Table RTELMAP, and the associated OVR Table and Index, and DRA digits are only used from this point on in the translations, either to be outputted as Called Number digits to the found routes in the OVR Table, or to enter translations starting from the OVR Table entry.

Routing

For routing, each BusinessLineID element in the RouteList parameter is taken sequentially, mapped to an OVR Table and Index using table RTELMAP, and input to the DMS-GSP switch routing system. If the route list contained in the given OVR Table and Index is exhausted without successful seizure of an

outgoing trunk, the DMS-GSP switch tries to route the call using the OVR Table and Index mapped from the next BusinessLineID element in the RouteList parameter.

If all BusinessLineIDs given in the RouteList parm are exhausted:

- if EDP-4R is not armed, the INAP dialogue is cleared normally, and the DMS-GSP switch is instructed to apply the appropriate treatment.
- if EDP-4R is armed, the DMS-GSP sends an RRBCSME (EDP4/RSF) operation to the SCP and the call suspends without any treatment.

Please refer to “Figure 3 RouteList parm interaction at EDP-4” on page 89.

Note:

Processing of the RouteList parameter is only supported by the DMS-GSP SSP switch for TDP-3 triggered INAP dialogues. If the RouteList operation is received for TDP-2 triggered dialogues, treatment FNAL (Feature Not Allowed) is applied to the call.

The following flow charts show how the Connect operation is processed on the DMS-GSP switch for TDP-2 and TDP-3 triggered dialogues, respectively.

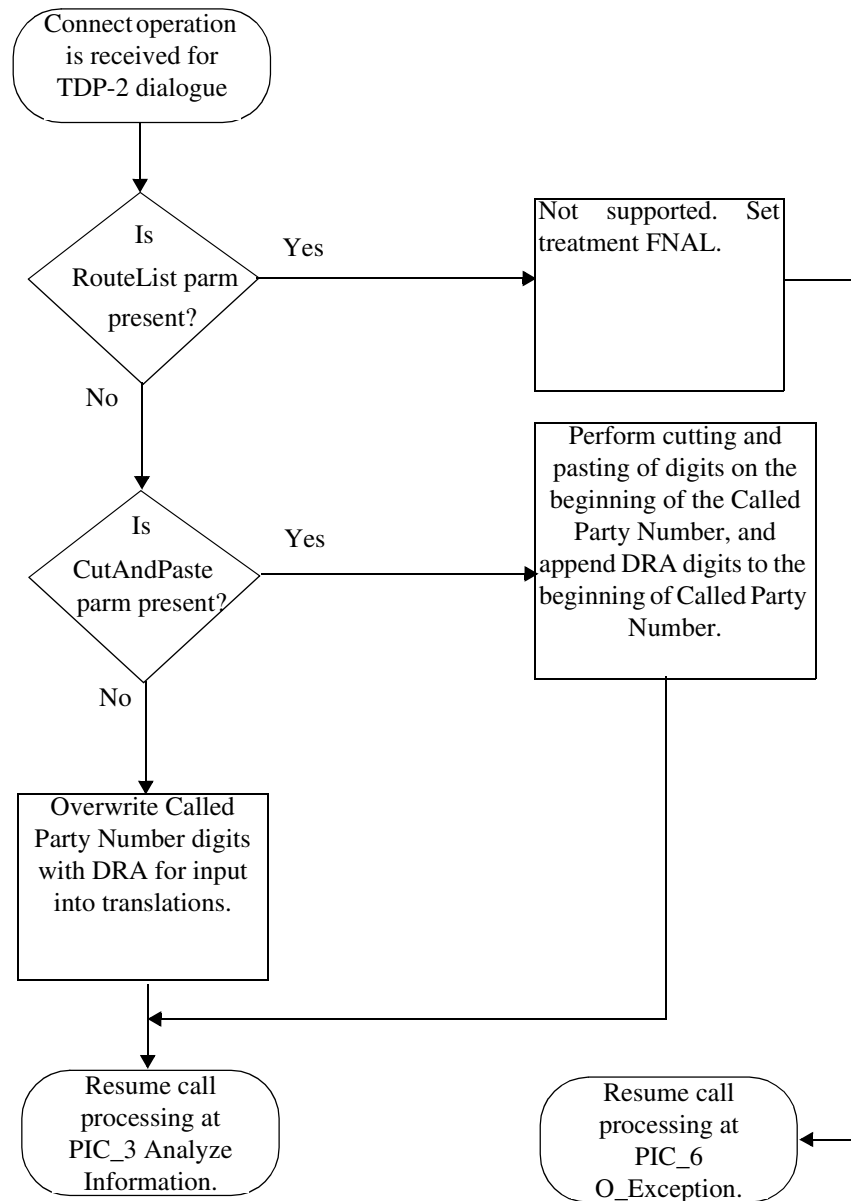
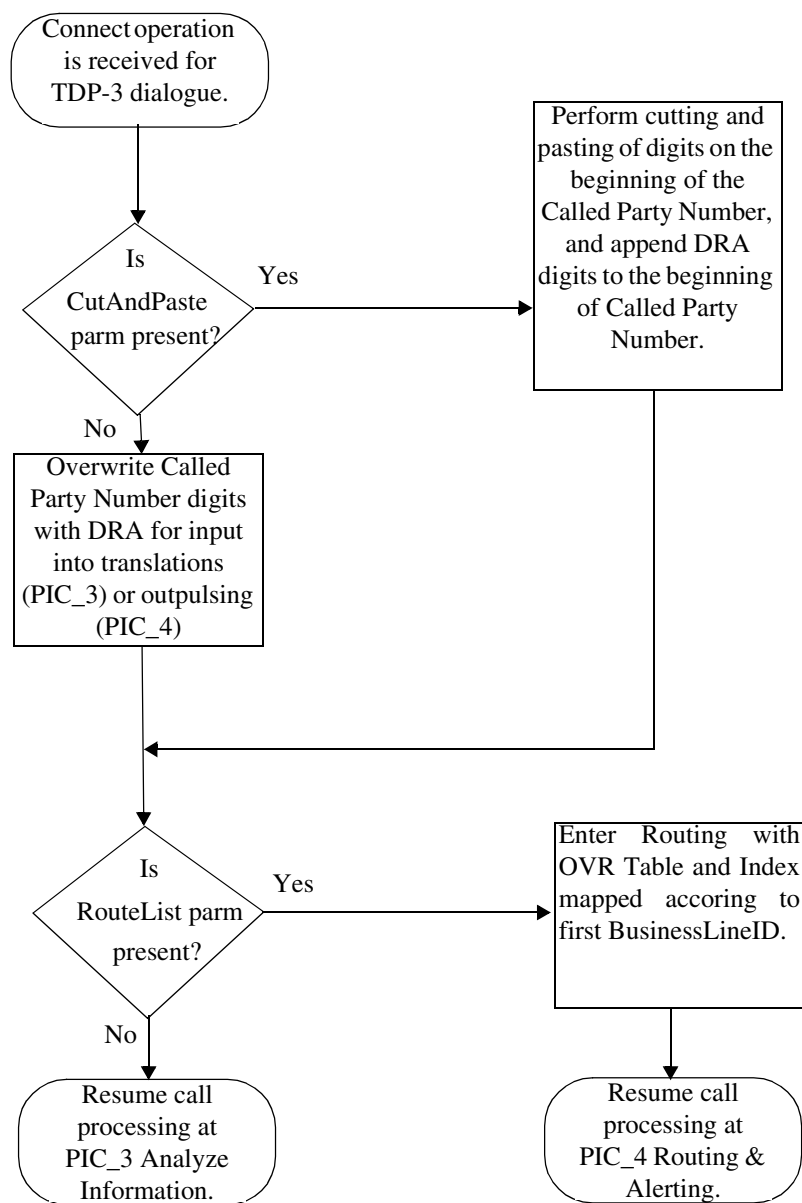
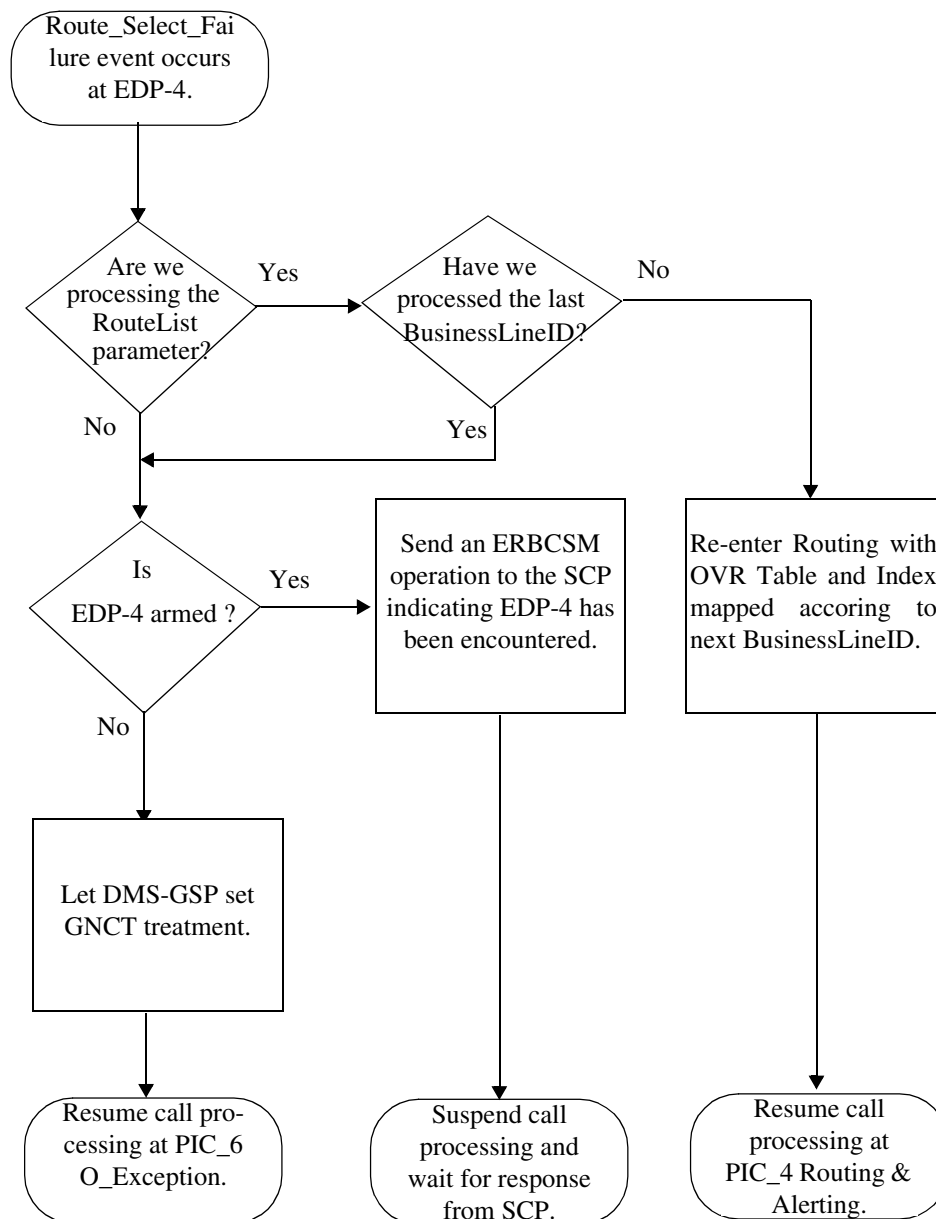
Figure 1 Connect Operation for TDP-2 triggered INAP dialogues

Figure 2 Connect Operation for TDP-3 triggered INAP dialogues

The following flow chart shows the affect that the RouteList parm processing has on processing the Route Select Failure (RSF) event at EDP-4.

Figure 3 RouteList parm interaction at EDP-4



Billing

The new GSP IN Routing State Machine based on RouteList parameter has been designed such that IN Billing will proceed as it used to do before. When an INAP Connect is received with a RouteList parm, Billing will be performed as usual, based on the following conditions:

- If routing according to a BusinessLineID is successful, its Billing CDR record will be processed as a successfully routed call as it is performed at present,
- If routing according to a BusinessLineID fails, its Billing CDR will be processed as a RSF (EDP4) scenario as it is performed at present, with the DEST_NUM field set according to the Destination Routing Address and Cut&Paste parameters (see “Figure 2 Connect Operation for TDP-3 triggered INAP dialogues” on page 88.), and after the probable manipulation of the OVR Route, if such a digit manipulation exists in the given OVR Route for the BusinessLineID.

5.3 Hardware Requirements or Dependencies

N/A

5.4 Software Requirements or Dependencies

N/A

5.5 Supplementary information

5.5.1 Logs (LG)

A new Trouble Description has been defined for RouteList parameter-related troubles that may require a GIN301 Log. This new Trouble Description is:

‘Error whilst processing RouteList parameter’

A new Reason Description has been defined for the GIN301 Log to be printed in the case when none of the BusinessLineIDs provided in the RouteList parameter are datafilled in Table RTELMAP. This new Reason Description is:

‘No Valid (datafilled) Business Line ID in RouteList Parm’

5.5.2 Data schema (DS)

5.5.2.1 New/modified table list

Table Name	New, Changed or deleted	Table Control
RTELMAP	New	New

Table RTELMAP maps logical BusinessLineID route IDs provided in a RouteList parameter received from the SCP in an INAP Connect operation, to DMS-GSP switch outgoing OVR indexes, for routing.

Example datafill for Table RTELMAP:

TABLE: RTELMAP

>

>lis all

TOP

BUSINESSLINEID

0 OVR74 44

16 OVR6 7

315 OVR4 371

4426 OVR4 6

37354 OVR74 24

65535 OVR6 373

BOTTOM

>

5.5.3 Service orders (SO)

N/A

5.5.4 Man machine interface (MM)

5.5.4.1 EINTRACE Enhancement

The EINTRACE tool has been enhanced to display RouteList parm and its contents if it is received in an INAP CONNECT operation. Below is an example EINTRACE output as such:

```
21:07:54 TCAP MESSAGE                      Tid :    2
=====
65 73 48 04 00 00 00 03 49 04 00 00 01 00 6C 65
A1 63 02 01 03 02 01 14 30 5B A0 06 04 04 83 13
87 03 83 01 04 A7 4E 24 40 04 02 34 75 04 02 78
90 04 02 24 53 04 02 12 34 04 02 00 00 04 02 04
44 04 02 FF FF 04 02 01 11 04 02 D6 C7 04 02 00
03 04 02 00 01 04 02 00 0D 04 02 00 16 04 02 00
1E 04 02 01 01 04 02 56 78 24 04 04 02 06 13 24
04 04 02 F4 01
=====
```

```

Type of Package : 65 = CONTINUE
Originating TRID : 00 00 00 03
Destination TRID : 00 00 01 00
Component Type : A1 = INVOKE
Invoke ID : 03
Operation : 14 = CONNECT
Destination Routing Address
  Called Party Number
    Odd/Even Indicator : 1 = ODD
    Nature Of Address : 03 = NATIONAL (SIGNIFICANT) NUMBER
    INN Indicator : 0 = ROUTING TO INTERNAL NETWORK NUMBER ALLOWED
    Numbering Plan Indicator : 01 = ISDN (TELEPHONY) NUMBERING PLAN (E164)
    Digits : 87 03 = 783
Cut And Paste : 04 = 4
Route List
  Route List Octet String 1
    BusinessLineID 1 : 13429
    BusinessLineID 2 : 30864
    BusinessLineID 3 : 9299
    BusinessLineID 4 : 4660
    BusinessLineID 5 : 0
    BusinessLineID 6 : 1092
    BusinessLineID 7 : 65535
    BusinessLineID 8 : 273
    BusinessLineID 9 : 54983
    BusinessLineID 10 : 3
    BusinessLineID 11 : 1
    BusinessLineID 12 : 13
    BusinessLineID 13 : 22
    BusinessLineID 14 : 30
    BusinessLineID 15 : 257
    BusinessLineID 16 : 22136
  Route List Octet String 2
    *** RouteList Octet String 2 NOT DECODED ***
  Route List Octet String 3
    *** RouteList Octet String 3 NOT DECODED ***

```

5.5.4.2 GTRAVER Enhancement

The GTRAVER tool has been enhanced to prompt to enter a BusinessLineID if expected from SCP, subsequently printing the routing steps based on that BusinessLineID, if received in an INAP CONNECT RouteList parameter. The outplused digits to an outgoing trunk are also printed as usual, although they are not used to enter translations after the INAP CONNECT if there is a RouteList parameter. If no BusinessLineID is entered, GTRAVER resumes translations with the DRA digits, assuming no BusinessLineID is expected from the SCP.

The following are some examples of various scenarios:

```

>GTRAVER TR GM2WEISV2BA 0500 T
TABLE TRKGRP
GM2WEISV2BA AXXESS 0 NPDGP NCIT 2W NPRT MIDL 16 7 16 16 4 5

```

```

4 ALERTING NIL_COSGRP 0 103 NONE 0 0 NIL_CUST 1 Y Y NODEF
NO_OVERRIDE VOICE_DATA Y Q764 N 1 0 0 0 N N NIL NIL ISUP $ 45
STD N Y NIL 0 N
TABLE ISUPATTR
45 EISUPV2 NIL THRH 0 Y NATL N 0 N N UNEQ 2WN7 NONE CIC N
NOVERI N N NIL FILTER 0
TABLE INTRK
GM2WEISV2BA PINAR
TABLE OFCVAR
IN_OFFICE_TRIGGRP NIL
INAP TDP-2 (Info Collected): no subscribed trigger.
TABLE INTRK
GM2WEISV2BA PINAR
TABLE GTRIGGRP
PINAR INFOANAL
. GENTRIG (CDPN PINAR)$ NIL
Trigger INAP GENTRIG is applicable to individual trunk.
. . TABLE GTRIGDIG
. . PINAR 0500 GINDCT CALLED (SERVKEY 4) (SERVINFO_INDEX 4)
$
. . . TABLE GSERVIN
. . . 4 (INITDP_INFO Y N N N N N N) $
. . . TABLE C7GTTTYPE
. . . GINDCT CCITT7 3 NATL E164 $
. . . TABLE C7GTT
. . . GINDCT 0500 0500 PCSSN (DCT2KRTESET GIN 0) $ SSN
INAP TDP-3 (Info Analyzed): trigger criteria met.
Select the INAP Operation expected from the SCP:
1- Connect
2- Continue
>1
Enter NOA and Destination Number expected in Connect operation:
>3
Next par is: <DEST DIGITS> STRING
Enter: <DEST DIGITS>
>7835453
Enter a BusinessLineID {0-65535} if expected from SCP in RouteList,
else press Return:

```

```

>416
Translating with BusinessLineID: 416
Pretranslating with Pretranslator: NPRT
Translating with STS 103 and CUSTNAME NIL_CUST
TABLE RTELMAP
416 OVR4 16
TABLE OVR4
. 16 S A GM2WEISV2BA
The Outpulsed Number is : 6067835452
.GBL GRX PINARX N N N 416
TABLE DIGEDIT
  416 (CL BEG) (REM 3)
EXIT TABLE DIGEDIT
. . TABLE CALLCNTL
. . PINARX (PRTNM PINAR) (STS 103) (CUSTNAME NIL_CUST) $
.CND NRR SK 0
.S A GM2WFTUPBA
The Outpulsed Number is : 7835452
.GBL GRX CLICNTL_NOSCRN_BL_CLI N N N 8965
TABLE DIGEDIT
  8965 (CL BEG) (INC 600)
EXIT TABLE DIGEDIT
. . TABLE CALLCNTL
. . CLICNTL_NOSCRN_BL_CLI (CLICNTL NOSCRN_BL_CLI) $
.T OVR89 65
TABLE POECRTE
TUPLE NOT FOUND
. . TABLE OVR89
. .65 S A GM2WFTUPBA
The Outpulsed Number is : 6007835452
. . EXIT TABLE OVR89
TABLE STDPRTCT
PINAR ( 1 ) ( 0 ) 3
. SUBTABLE STDPRT
. 6 9 CT OFFNET PX 1 24 0 416 NAT
Translating with STS 103 and CUSTNAME NIL_CUST
TABLE PXTRAN
103 NIL_CUST PXOFF PXON PXOFF PXIP

```

TABLE PXHEAD**PXOFF DFLT CONT (XLT FA FAOFF)\$ DFOP \$ NOCON STD****THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 6007835452****TABLE PXCODE****PXOFF 600 600 RTE (PF 3) (DEST 606) (CLASS NATL) (LNET NAT)
(MZONE 1)\$****TABLE: PXRTE****KEY:PXOFF 606****. S GM2WEISV2BA****The Outpulsed Number is : 7835452****EXIT TABLE PXRTE**

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>GTRAVER TR GM2WEISV2BA 0800 T

TABLE TRKGRP**GM2WEISV2BA AXCESS 0 NPDGP NCIT 2W NPRT MIDL 16 7 16 16 4
5 4 ALERTING****NIL_COSGRP 0 103 NONE 0 0 NIL_CUST 1 Y Y NODEF
NO_OVERRIDE VOICE_DATA Y Q764****N 1 0 0 0 N N NIL ISUP \$ 45 STD N Y NIL 0 N****TABLE ISUPATTR****45 EISUPV2 NIL THRH 0 Y NATL N 0 N N UNEQ 2WN7 NONE CIC N
NOVERI N N NIL FILTER****0****TABLE INTRK****GM2WEISV2BA PINAR****TABLE OFCVAR****IN_OFFICE_TRIGGRP NIL****INAP TDP-2 (Info Collected): no subscribed trigger.****TABLE INTRK****GM2WEISV2BA PINAR****TABLE GTRIGGRP****PINAR INFOANAL****. GENTRIG (CDPN PINAR)\$ NIL****Trigger INAP GENTRIG is applicable to individual trunk.****. . TABLE GTRIGDIG**

.. PINAR 0800 GINDCT CALLED (SERVKEY 2209) (SERVINFO_INDEX 2209) \$

. . . TABLE GSERVIN

. . . 2209 (INITDP_INFO Y N N N N N N Y) \$

. . . TABLE C7GTTTYPE

. . . GINDCT CCITT7 3 NATL E164 \$

. . . TABLE C7GTT

. . . GINDCT 0800 0800 PCSSN (ISTEPRSET2 SS108 2) \$ SSN

INAP TDP-3 (Info Analyzed): trigger criteria met.

The Called Party NOA sent to the SCP is: 2 (Unknown)

The Called Party Number sent to the SCP is: 0800

Select the INAP Operation expected from the SCP:

1- Connect

2- Continue

>1

Enter NOA and Destination Number expected in Connect operation:

>4

Next par is: <DEST DIGITS> STRING

Enter: <DEST DIGITS>

>6067835452

Enter a BusinessLineID {0-65535} if expected from SCP in RouteList, else press Return:

>

No RouteList-BusinessLineID expected from SCP.

Translating only with DRA.

TABLE OFCVAR

IN_PRTNM NPRT

Pretranslating with Original Pretranslator: NPRT

Translating with STS 103 and CUSTNAME NIL_CUST

TABLE PXTRAN

103 NIL_CUST PXOFF PXON PXOFF PXIP

TABLE PXHEAD

PXOFF DFLT CONT (XLT FA FAOFF)\$ DFOP \$ NOCON STD

THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 6067835452

TABLE PXCODE

PXOFF 606 606 RTE (PF 3) (DEST 606) (CLASS NATL) (LNET NAT) (MZONE 1)\$

TABLE POECRTE

TUPLE NOT FOUND

TABLE: PXRTE

KEY:PXOFF 606

. S GM2WEISV2BA

The Outpulsed Number is : 7835452

EXIT TABLE PXRTE

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>GTRAVER TR GM2WEISV2BA 0800 T

TABLE TRKGRP

GM2WEISV2BA AXCESS 0 NPDGP NCIT 2W NPRT MIDL 16 7 16 16 4
5 4 ALERTING

NIL_COSGRP 0 103 NONE 0 0 NIL_CUST 1 Y Y NODEF
NO_OVERRIDE VOICE_DATA Y Q764

N 1 0 0 0 N N NIL NIL ISUP \$ 45 STD N Y NIL 0 N

TABLE ISUPATTR

45 EISUPV2 NIL THRH 0 Y NATL N 0 N N UNEQ 2WN7 NONE CIC N
NOVERI N N NIL FILTER

0

TABLE INTRK

GM2WEISV2BA PINAR

TABLE OFCVAR

IN_OFFICE_TRIGGRP NIL

INAP TDP-2 (Info Collected): no subscribed trigger.

TABLE INTRK

GM2WEISV2BA PINAR

TABLE GTRIGGRP

PINAR **INFOANAL**

. GENTRIG (CDPN PINAR)\$ NIL

Trigger INAP GENTRIG is applicable to individual trunk.

. . TABLE GTRIGDIG

. . PINAR 0800 GINDCT CALLED (SERVKEY 2209) (SERVINFO_INDEX
2209) \$

. . . TABLE GSERVINF

. . . 2209 (INITDP_INFO Y N N N N N N Y) \$

. . . TABLE C7GTTYPE

```

. . . GINDCT CCITT7 3 NATL E164 $
. . . TABLE C7GTT
. . . GINDCT 0800 0800 PCSSN (ISTEPRTSET2 SS108 2) $ SSN
INAP TDP-3 (Info Analyzed): trigger criteria met.
The Called Party NOA sent to the SCP is: 2 (Unknown)
The Called Party Number sent to the SCP is: 0800
Select the INAP Operation expected from the SCP:
1- Connect
2- Continue
>1
Enter NOA and Destination Number expected in Connect operation:
>3
Next par is: <DEST DIGITS> STRING
Enter: <DEST DIGITS>
>6067835452
Enter a BusinessLineID {0-65535} if expected from SCP in RouteList,
else press Return:
>2474
Translating with BusinessLineID: 2474
Pretranslating with Pretranslator: NPRT
Translating with STS 103 and CUSTNAME NIL_CUST
TABLE RTELMAP
TUPLE NOT FOUND
TABLE TMTCNTL
AXXESS ( 0)
. SUBTABLE TREAT
KEY NOT FOUND
DEFAULT OFFTREAT IS USED
TABLE TMTCNTL
OFFTREAT ( 223)
. SUBTABLE TREAT
. AINF Y S 120T0

+++ TRAVER: SUCCESSFUL CALL TRACE +++

```

```

>GTRAVR TR GM2WEISV1BA 0800 T
TABLE TRKGRP
GM2WEISV1BA AXXESS 0 NPDGP NCIT 2W NPRT MIDL 16 7 16 16 4
5 4 ALERTING
  NIL_COSGRP 0 103 NONE 0 0 NIL_CUST 1 Y Y NODEF
NO_OVERRIDE VOICE_DATA Y Q764
  N 1 0 0 0 N N NIL NIL ISUP $ 44 STD N Y NIL 0 N
TABLE ISUPATTR
44 EISUPV1 NATIONAL NOVERI NIL THRH 0 Y Y N 0 N N UNEQ 2WN7
NONE CIC N NOVERI N
  N NIL FILTER 0
TABLE INTRK
GM2WEISV1BA PINAR1
TABLE GTRIGGRP
PINAR1 INFOCOL
  . GENTRIG ( SPC PINAR)$ NIL
Trigger INAP GENTRIG is applicable to individual trunk.
  . . TABLE GTRIGDIG
  . . PINAR 0800 GINDCT CALLED (SERVKEY 2209) (SERVINFO_INDEX
2209) $
  . . . TABLE GSERVINF
  . . . 2209 (INITDP_INFO Y N N N N N N Y) $
  . . . TABLE C7GTTYPE
  . . . GINDCT CCITT7 3 NATL E164 $
  . . . TABLE C7GTT
  . . . GINDCT 0800 0800 PCSSN (ISTEPRTSET2 SS108 2) $ SSN
INAP TDP-2 (Info Collected): trigger criteria met.
The Called Party NOA sent to the SCP is:  2 (Unknown)
The Called Party Number sent to the SCP is: 0800
Select the INAP Operation expected from the SCP:
1- Connect
2- Continue
>1
Enter NOA and Destination Number expected in Connect operation:
>10
Next par is: <DEST DIGITS> STRING
Enter: <DEST DIGITS>

```

>6017835452

**Enter a BusinessLineID {0-65535} if expected from SCP in RouteList,
else press Return:**

>345

Translating with BusinessLineID: 345

Pretranslating with Pretranslator: NPRT

Translating with STS 103 and CUSTNAME NIL_CUST

**Routing with a BusinessLineID is not allowed for TDP-2 triggered
calls.**

TABLE TMTCNTL

AXXESS (0)

. SUBTABLE TREAT

KEY NOT FOUND

DEFAULT OFFTREAT IS USED

TABLE TMTCNTL

OFFTREAT (223)

. SUBTABLE TREAT

. FNAL Y S 120T0

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>GTRAVER TR GM2WEISV1BA 0800 T

TABLE TRKGRP

GM2WEISV1BA AXXESS 0 NPDGP NCIT 2W NPRT MIDL 16 7 16 16 4
5 4 ALERTING

NIL_COSGRP 0 103 NONE 0 0 NIL_CUST 1 Y Y NODEF
NO_OVERRIDE VOICE_DATA Y Q764

N 1 0 0 0 N N NIL ISUP \$ 44 STD N Y NIL 0 N

TABLE ISUPATTR

44 EISUPV1 NATIONAL NOVERI NIL THRH 0 Y Y N 0 N N UNEQ 2WN7
NONE CIC N NOVERI N

N NIL FILTER 0

TABLE INTRK
 GM2WEISV1BA PINAR1
 TABLE GTRIGGRP
 PINAR1 INFOCOL
 . GENTRIG (SPC PINAR)\$ NIL
 Trigger INAP GENTRIG is applicable to individual trunk.
 . . TABLE GTRIGDIG
 . . PINAR 0800 GINDCT CALLED (SERVKEY 2209) (SERVINFO_INDEX
 2209) \$
 . . . TABLE GSERVINF
 . . . 2209 (INITDP_INFO Y N N N N N N Y) \$
 . . . TABLE C7GTTTYPE
 . . . GINDCT CCITT7 3 NATL E164 \$
 . . . TABLE C7GTT
 . . . GINDCT 0800 0800 PCSSN (ISTEPRSET2 SS108 2) \$ SSN
 INAP TDP-2 (Info Collected): trigger criteria met.
 The Called Party NOA sent to the SCP is: 2 (Unknown)
 The Called Party Number sent to the SCP is: 0800
 Select the INAP Operation expected from the SCP:
 1- Connect
 2- Continue
 >1
 Enter NOA and Destination Number expected in Connect operation:
 >3
 Next par is: <DEST DIGITS> STRING
 Enter: <DEST DIGITS>
 >6017835452
**Enter a BusinessLineID {0-65535} if expected from SCP in RouteList,
 else press Return:**
 >
No RouteList-BusinessLineID expected from SCP.
Translating only with DRA.
 TABLE OFCVAR
 IN_PRTNM NPRT
 Pretranslating with Original Pretranslator: NPRT
 Translating with STS 103 and CUSTNAME NIL_CUST
 TABLE PXTRAN
 103 NIL_CUST PXOFF PXON PXOFF PXIP

```

TABLE PXHEAD
PXOFF DFLT CONT ( XLT FA FAOFF)$ DFOP $ NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 6017835452
TABLE PXCODE
PXOFF 601 601 RTE ( PF 3) ( DEST 601) ( CLASS NATL) ( LNET NAT)
( MZONE 1)$
TABLE POECRTE
TUPLE NOT FOUND
TABLE: PXRTE
KEY:PXOFF 601
. S GM2WEISV1BA
The Outpulsed Number is : 7835452
EXIT TABLE PXRTE

+++ TRAVER: SUCCESSFUL CALL TRACE +++

```

5.5.5 Operational measurements (OM)

N/A

5.6 Limitations and restrictions

1. This feature is supported for:
 - all incoming GSP trunks for which IN triggering at TDP3 is supported,
 - and for all outgoing GSP trunks for which routing after INAP CONNECT is supported while there is still an active INAP dialogue involved in the call
2. Processing of the RouteList parameter in the Connect operation is only supported for TDP-3 triggered INAP dialogues.
3. The RouteList parameter in the received Connect operation can contain a minimum of 1 and maximum of 16 BusinessLineIDs.
4. The routing is subject to the limitation of ACM_Timeout at the originating exchange. Note that although it is possible to retry routing with up to 16 BusinessLineIDs, if the routing takes longer than the ACM_Timeout, the call will clear before finding a successful route, even if all of the routes associated with all the BusinessLineIDs have not been tried yet.
5. The supported range of BusinessLineID values is 0 to 65535.
6. Up to 65536 tuples can be datafilled in Table RTELMAP.

7. When datafilling Table RTELMAP, it is verified whether the OVR table ID and Index is datafilled. Furthermore, when removing a tuple from an OVR Table, it is also checked whether this OVR Table and the Index for the to-be- changed/deleted tuple is datafilled in Table RTELMAP. If it is datafilled in Table RTELMAP, the deletion of the given tuple from the OVR table is not allowed until all present datafills in Table RTELMAP are removed, but a change is allowed with a Warning message printed to notify the operator that this OVR tuple is datafilled in Table RTELMAP.
8. This feature has been patched back to GSPISN04 and GSPISN07; however the patched feature allows for an OVR Table ID & Key to be changed/ deleted even if it is datafilled in Table RTELMAP. Care must be taken not to have any deleted OVR Table ID and Key still datafilled in Table RTELMAP before an ONP Table Transfer from GSPISN04 to GSPISN08 / higher load, or GSPISN07 to GSPISN08 / higher load. Otherwise, an error of the following nature will be observed:

Did not add temporary ovrt tuple

OVr Table and Index tuple must exist.

ERROR: Failed to restore - 32300 OVR5 109

If it has been forgotten, either the missing OVR Table ID & Key must be datafilled or the associated Table RTELMAP tuple(s) must be deleted in the FROM load, and the ONP Table Transfer can be resumed.

9. Restrictions apply to DRA digit manipulation when the Connect operation RouteList parameter is in use. For more information see “Call processing with RouteList parm in Connect” on page 85.
10. GTRAVR has been enhanced to print the routing based on *only* one BusinessLineID at a time, and *not* for all the 1 to 16 BusinessLineIDs that may be received in a RouteList parameter at once.

5.7 Interactions

N/A

5.8 Glossary

- CS-1R Capability Set version 1 Revised
- DMS Digital Multiplexing Systems
- DRA Destination Routing Address
- EDP Event Detection Point
- ERBCSM Event Report BCSM
- GAME Generic AIN Messaging Environment

- GSP Global Services Platform
- IN Intelligent Network
- INAP Intelligent Network Application Part
- ITU International Telecommunication Union
- OVR Overseas Route Tables
- PIC Point In Call
- RRBCSME Request Report BCSM Event
- RSF Route Select Failure
- SCP Service Control Point
- SSP Service Switching Point
- TCAP Transaction Capabilities Application Part
- TDP Trigger Detection Point

5.9 References

- 1 Q.1218: ITU-T Interface Recommendation for CS-1R (10/95)
- 2 AX0944: “DMS-300 switch CS-1R INAP Phase 1”

6: A00005981 Functional description (FN)

6.1 Feature name

GSP IN InitDP Operation Enhancement to support POE (Path Of Entry) Parameter.

6.2 Description

This activity enhances GSP IN to incorporate and send Path Of Entry (POE) information to the SCP in the InitialDP Operation.

The following requirements are implemented:

- Table GSERVINF optionality is provided for Path Of Entry (POE) information to be built into the InitialDP.
- The Path of Entry information (POECGRP and POECIDX) is built as a Path Of Entry (POE) parameter and passed into the InitialDP message if:
 - i. PATH_OF_ENTRY field of INITDP_INFO option in table GSERVINF is set to Y and
 - ii. The POE information is datafilled in table TRKGRP or both in tables TRKGRP and CALLCNTL. (Please see References 1 and 2 in section “References” on page 108 for POE information datafill).
- EINTRACE tool is enhanced for InitDP POE parameter printing.

6.2.1 Table GSERVINF datafill for Path Of Entry Parameter

In order to provide optionality for the Path Of Entry parameter, this activity includes a new field named PATH_OF_ENTRY under INITDP_OPTION of table GSERVINF. If it is desired to send the Path Of Entry parameter in the InitDP message, this new PATH_OF_ENTRY field should be set to Y and other POE datafills (in table(s) TRKGRP/CALLCNTL) should be complete. Table 1 on page 105 shows an example GSERVINF tuple with PATH_OF_ENTRY datafill.

Table 1 Example GSERVINF tuple with Path_Of_Entry Datafill

TABLE: GSERVINF

```

>pos 2209
2209 (INITDP_INFO N N N N N N N N) $
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
OPTION: INITDP_INFO
>
CALLING_PN: N
>
BEARER_CAPABILITY: N
>
FORWARD_CALL_INDICATOR: N
>
ORIG_CALLED_NUMBER: N
>
REDIRECTING_NUMBER: N
>
IN_BUSINESS_GROUP: N
>
REDIRECTION_INFORMATION: N
>
PATH_OF_ENTRY: N
>
OPTION:
>

```

6.2.2 Path Of Entry Parameter Format

The DMS-GSP definition for the Path Of Entry parameter in an InitialDP operation is as follows:

initialDP OPERATION

ARGUMENT

SEQUENCE {

PathOfEntry[] IMPLICIT OCTET STRING (SIZE (1..32)) OPTIONAL,

...

}

Here:

- the first 2 BYTES = 16 BITS of Path Of Entry parameter will be used for POE Group ID {0..2047}
- the 3rd BYTE of Path Of Entry parameter will be used for POE index {0..255}
- the 4th BYTE is reserved for future use.

Below is an INITDP Operation containing Path Of Entry parameter.

Figure 1 Example of printed POE parameter in EINTRACE

```
=====
62 34 48 04 00 00 2A 00 6C 2C A1 2A 02 01 00 02
01 00 30 22 80 02 08 A1 82 07 03 10 79 56 20 21
43 83 06 01 13 87 53 54 02 85 01 00 9C 01 03 9F
1F 04 00 01 23 00
=====
Type of Package : 62 = BEGIN
Originating TRID : 00 00 2A 00
Component Type : A1 = INVOKE
Invoke ID : 00
Operation : 00 = INITIAL DP
Service Key : 08 A1 = 2209
Called Party Number
  Odd/Even Indicator : 0 = EVEN
  Nature Of Address : 03 = NATIONAL (SIGNIFICANT) NUMBER
  INN Indicator : 0 = ROUTING TO INTERNAL NETWORK NUMBER ALLOWED
  Numbering Plan Indicator : 01 = ISDN (TELEPHONY) NUMBERING PLAN (E164)
  Digits : 79 56 20 21 43 = 9765021234
Calling Party Number
  Odd/Even Indicator : 0 = EVEN
  Nature Of Address : 01 = SUBSCRIBER NUMBER
  NI Indicator : 0 = COMPLETE
  Numbering Plan Indicator : 01 = ISDN (TELEPHONY) NUMBERING PLAN (E164)
  Presentation Restriction : 00 = PRESENTATION ALLOWED
  Screening Indicator : 03 = NETWORK PROVIDED
  Digits : 87 53 54 02 = 78354520
Calling Partys Category : 00 = UNKNOWN AT THIS TIME
Event Type BCSM : 03 = ANALYZED INFORMATION
Path Of Entry:
  Poe Group : 0001 = POECGRP_P
  Poe Index : 23 = 35
```

Note: EINTRACE tool is enhanced so that it will be capable of printing the Path Of Entry parameter in the InitialDP Operation.

6.3 Hardware Requirements or Dependencies

N/A

6.4 Software Requirements or Dependencies

This development covers GSP IN only.

6.5 Limitations and restrictions

- The functionality explained in this FN document works for TDP-3 triggered IN calls only. For a TDP-2 triggered IN call, if Path Of Entry field of INITDP_INFO option in table GSERVINP is set to Y and the POE information is datafilled in table(s) TRKGRP or both in TRKGRP and CALLCNTL , Path Of Entry Group will be NIL and Path of Entry index will be 0 in the INITDP operation.

6.6 Glossary

Table 2

POE	Path Of Entry
INITDP	Initial Detection Point
SCP	Service Control Point
GSP	Global Services Platform

6.7 References

- A60006660: Path of Entry screening on the DMS GSP
- A60008617: DMS-GSP Routing Engine.
- A59028840: Least Cost Routing

7: A00006064 Functional description (FN)

7.1 Feature name

DNSCRN Disable CCR Screening

7.2 Description

The purpose of this activity is to disable CCR (Cumulative Charge Restriction) screening in Universal Translations Tables under certain circumstances. In current behavior, CCR screening for Third Party Billed Calls occurs for called party number datafilled with THIRDPY or V3PTYBIL option with FEATINFO VALIDATE selector.

With this functionality, CCR screening for Third Party Billed Calls should not occur for called number datafilled THIRDPY option with FEATINFO VALIDATE selector.

Feature AU2351 implements functionality of CCR DN screening call restriction attribute and uses DN screening base functionality provided by activity AR0100. This new feature involves flexibility of CCR screening for Third Party Billed Calls and uses Cumulative Charge Restriction (CCR) provided by activity AU2351.

The activity is optional with a SOC option. When state of SOC is ON, feature becomes active, otherwise system behaves as it was before this functionality.

The feature is implemented in ISN08.

7.2.1 Background:

CCR attribute is introduced in feature AU2351 for CCR call screening functionality, which is used to indicate when subscribers have exceeded their cumulative charge limit. CCR attribute is to be used to block calls in order to prevent fraudulent charges and route them to an appropriate treatment, as datafilled in table OPTTREAT, once subscribers have exceeded their cumulative charge limit.

A subscriber's cumulative charge limit is determined by the operating company in their downstream billing process. When the downstream billing process determines that a subscriber's cumulative charge limit has been exceed, table DNSCRN can be datafilled with the new CCR attribute against the subscriber's DN.

For enabling CCR screening, once CCR attribute is datafilled in table DNSCRN for a subscriber and then call screening is setup in Universal Translations using the FEATINFO VALIDATE selector with the SUBSCRN option, and the CHKCCR field for a subscriber type datafilled to Y, so that CCR screening becomes enable, and the call is blocked, routed to treatment. In this scenario call fails since CCR screening fails.

Figure 1 describes datafill example of DNSCRN and PXCODE (Universal Translation Table) table for CCR screening. In this figure 1, CHKCCR field in PXCODE table must be Y to do CCR screening for each subscriber types (General, Payphone, Mobile, Personal). Subscriber type CCR screening fails because, CHKCCR is set to Y and CCR attribute is datafilled in table DNSCRN against the subscriber DN (1027835453).

In figure 1, the tuple in table PXCODE does the following:

- Use the calling party number for screening purposes
- Allow all subscribers (General, Payphone, Mobile, Personal)
- Check for only CCR attribute in table DNSCRN
- If screening passed would continue, with remaining digits, into table PXCODE using PTTXLA translation name

FEATINFO VALIDATE CCR screening on the calling party number (by default) or called party number (using the CALLED option) is controlled by the CHKCCR field for each of the subscriber types of General, Payphone, mobile and Personal.

Figure 1 Datafill Example of DNSCRN and PXCODE Tables for CCR Screening

```
TABLE: DNSCRN
>pos 1027835453
1027835453 (CCR) $

>TABLE PXCODE
>pos pttla 111 111
PTTXLA 111 111 FEATINFO VALIDATE (SUBSCRN (GENERAL N N N Y)
(PAYPHONE N N N Y) (MOBILE N N N Y) (PERSONAL N N N Y) $) $ 0 2
24 PX PTTXLA
```

Order of precedence for FEATINFO VALIDATE Subscriber type screening with CCR is Unpaid attribute, CCR attribute, Blckcall attribute respectively. In figure 2, the assumption is that the DN belongs to a General subscriber type, and the CHKUNPD, CHKBLKCL and CHKCCR fields for a GENERAL subscriber type are datafilled to 'Y'.

Figure 2 Order of Precedence for FEATINFO VALIDATE Subscriber Type Screening with CCR

DNSCRN Entry		OPTTREAT Screening Event			
1027835455	(UNPAID)	(BLCKCALL)	(CCR)	\$	
VLD_GEN_UNPAID_DN_SCRN					
1027835455	(UNPAID) (CCR)	\$			VLD_GEN_UNPAID_DN_
1027835455	(BLCKCALL) (CCR)	\$			VLD_GEN_CCR_DN_SC
1027835455	(CCR)	\$			VLD_GEN_CCR_DN_SC
Note: CCR is added to the end of existing no data attributes in table DNSCRN and it will always appear at the end.					

In feature AU2351 Third Party Billed calls are screened for CCR against the THDPTYDN (Third Party DN) of THIRPTY attribute in table DNSCRN.

THIRDPTY attribute is used for doing automatic Third Party Billing. When this attribute is specified a Third Party Billing number must also be entered. Figure 3 describes datafill examples of tables that enable CCR screening for Third Party Billed Calls with feature AU2351. Assumption here is that the DN belongs to a general subscriber type and CHKCCR field for a general subscriber type is datafilled to Y.

Third Party Billing DN Screening is done in addition to subscriber type screening, and is not part of subscriber type screening.

Figure 3 General Subscriber Failing Third Party DN CCR Screening

```

TABLE: PXCODE
>pos pttvla 111 111
PTTVLA 111 111 FEATINFO VALIDATE
(SUBSCRN (GENERAL N N N Y) $) (THIRDPTY) $ 0 2 24 PX PTTVLA
    For calling party DN 1027835452;
TABLE: DNSCRN
>pos 1027835453 ----->Third Party Billing DN
1027835453 (CCR) $

>pos 1027835452 ----->This DN is calling number
1027835452 (THIRDPTY 1027835453) $

```

Note: Third Party DN is 1027835453.

In figure 3, if a call is made by subscriber who's DN is 1027835452 and who is identified as a GENERAL subscriber, then with the above translations the call will be routed to the treatment. Subscriber Type CCR Screening passes because, CHKCCR field is set to Y for GENERAL subscribers, but the CCR attribute is not datafilled in table DNSCRN against the subscriber DN (1027835452). Third Party CCR Screening fails because, the THIRDPTY attribute in PXCODE triggers the Third party DN to be screened for the CCR attribute in table DNSCRN. As a result of the CCR attribute being datafilled against the Third Party DN (1027835453), screening fails.

7.2.2 Functional Description

With this new functionality, CCR screening part is skipped whenever the THIRDPTY option is datafilled in the FEATINFO VALIDATE selector of Universal Translation tables and DNSCRN table. So that Third Party Billed call screening for Third Party DN in table DNSCRN is only done for the UNPAID DN call restriction attribute

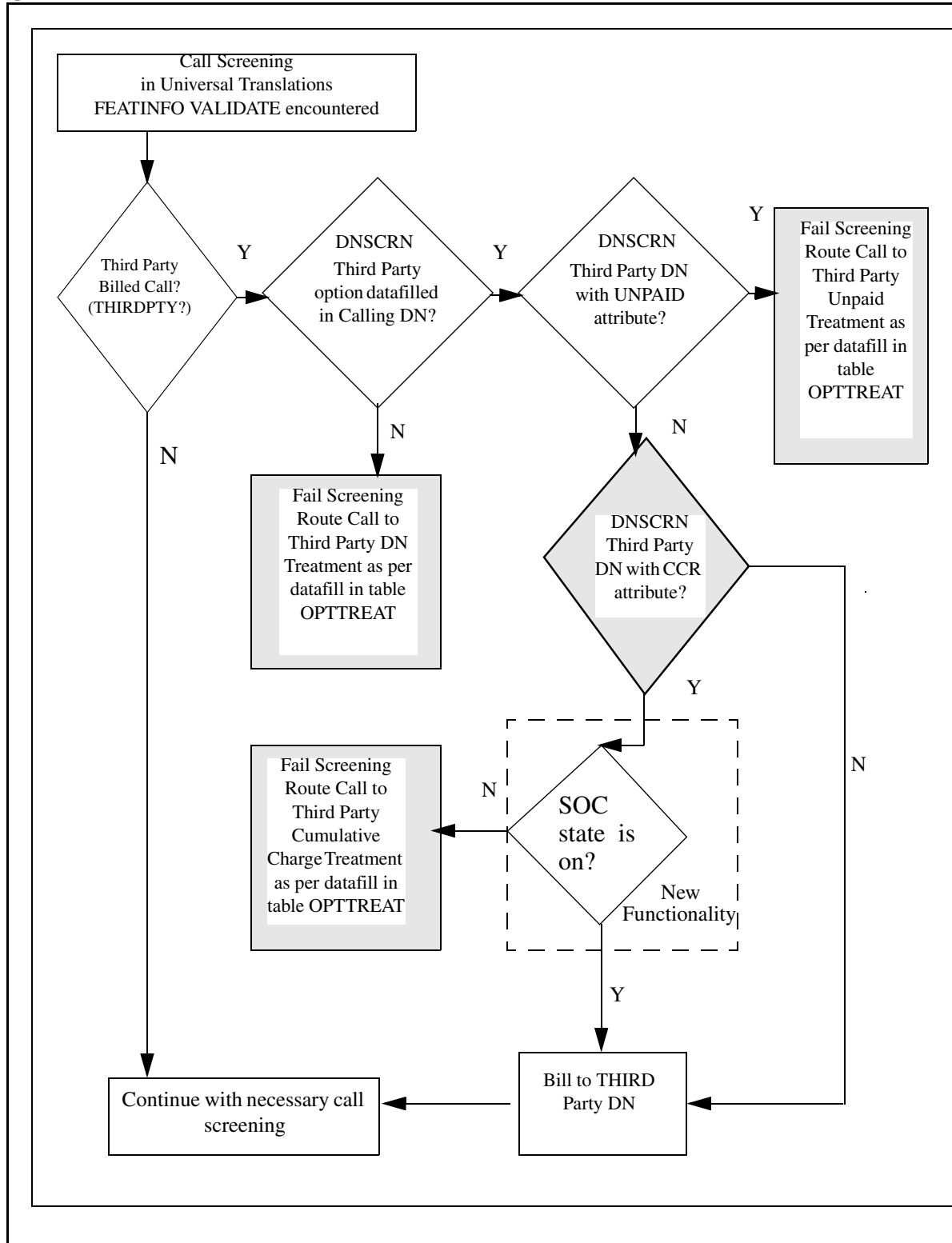
Desired Behavior of the activity can be summarized as follows;

When a call goes through Universal Translations and hits the FEATINFO VALIDATE selector the following is what occurs:

- Subscriber type screening is done. This is same with functionality in feature AU2351. FEATINFO VALIDATE CCR screening on the Calling Party number (by default) or Called Party number (using called option) is controlled by the CHKCCR field for each of the subscriber type of GENERAL, PAYPHONE, MOBILE and PERSONAL.

-
- When the THIRDPTY option is present in Universal Translations, table DNSCRN is checked for datafill of the THIRDPTY attribute for the subscriber DN
 - If the THIRDPTY attribute in DNSCRN is datafilled against the subscriber DN, then table DNSCRN is checked for datafill of the UNPAID attribute against the Third Party DN
 - If the UNPAID attribute is datafilled against the Third Party DN then the calls fails call screening as before
 - If the UNPAID attribute is not datafilled, but the CCR attribute is datafilled against the Third Party DN, and If SOC option state is ON, CCR functionality is skipped, billing record is updated and then call continues translation.
 - If the UNPAID attribute is not datafilled, but the CCR attribute is datafilled against the Third Party DN, and If SOC option state is OFF, translation continues same with functionality in feature AU2351. In other words, the call is routed to the treatment datafilled in table OPTTREAT against the screening event VLD_THRDPTY_BILLNUM_CCR.
 - If the UNPAID and CCR attribute is not datafilled, translation continues.

Figure 4 describes the flow of FEATINFO VALIDATE third party call screening with changes made by this feature for CCR screening.

Figure 4 Flow of THIRD PARTY CALL SCREENING with This Feature

7.3 Hardware Requirements or Dependencies

None

7.4 Software Requirements or Dependencies

SOC option XLAS0056 'CCR Screen Enh' must be ON for activation of this feature.

7.5 Limitations and restrictions

CCR screening for Third Party Billed Calls can be enabled/disabled by of this feature.

The following JI-ISUP interworkings are supported as in RS section of activity 59017299:

JI-ISUP <==> JI-ISUP

JI-ISUP <==> ANSI7+

JI-ISUP <==> ETSI ISUP V2

JI-ISUP <==> NCC ISUP

JI-ISUP <==> Japan T1 CAS (R1)

JI-ISUP <==> Japan PRI (INS1500)

JI-ISUP <==> IBN Line

7.6 Interactions

N/A

7.7 Applicable customer facing sections

Fault Management

Logs N/A

Alarms N/A

Configuration

N/A

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

7.8 Glossary

Table 1

Term	Description
CCR	Cumulative Charge Restriction

7.9 References

- AU2351 - Cumulative Charge Restriction
- RS section of FN document of activity 59017299- JI-ISUP
- Spec RFF 368
- AR0101 - Call Screening Applications

8: A00006271 Functional description (FN)

8.1 Feature name

CEPT Act/Deact and Interrogation for ETSI BRI CFK, CFB/CFD K

8.2 Description

8.2.1 Background

Activation, deactivation and interrogation of CFB (Call Forwarding Busy), CFD (Call Forwarding Don't Answer) and CFU (Call Forwarding Unconditional) features based on the CEPT Dialing Sequence has been already implemented per loop (or a chosen DN keylist) (for more information, please refer to [1] (A59034125 "ISDN BRI CEPT Call Forwarding" in PLS FMDOC).

CFx and CFx per Key are administration assigned features but the subscriber as well as the administrator has the ability of activating, deactivating and interrogating the feature.

This activity is only interested in the activation, deactivation and interrogation of the previously assigned CFx per Key option based on CEPT Dialing Sequence and neither interested in the provisioning of the CFx per Key option nor the existing CFx per Key activation, deactivation and interrogation code (for more information, please refer to [2] A59028702 "Support of CFx for Multiple DN's for ETSI BRI" in PLS FMDOC).

8.2.1.1 Existing CFB and CFD Types

There are 4 types of CFB and CFD:

- N (Normal) - "Forwarded to DN" is specified during assignment of feature, and forwarding capability is immediately activated and remains activated.
- F (Fixed) - "Forwarded to DN" is specified during assignment of feature, but forwarding capability is activated and deactivated by the user from the set to which the feature is assigned.
- P (Programmable) - Similar to F type, but upon activation, user from set also specifies forwarded to DN. No "Forwarded to DN" is specified during assignment of the feature.
- K (Programmable per Key) - For every DN in the KEYLIST, a new tuple is created in table CFX (for the other types of CFB and CFD, a common tuple is created for all the DN's in the keylist). This means that each DN might have its own data.

The CFB and CFD call forwarding features are assignable only to KEY 1 of an ISDN BRI set. Those DN Keys which receive the functionality of such an assignment are specified in a KEYLIST.

8.2.1.2 Existing CFK Feature

The CFK (Call Forwarding per Key) feature can be assigned to KEY 1 or to any vacant key on a set. Again, those DN Keys which receive the functionality of such an assignment are specified in a KEYLIST. For CFK, the user can program a separate “Forwarded to DN” to each key specified in the KEYLIST.

This activity is only interested in CFK option and the K (Programmable per Key) type of the CFB and CFD options.

8.2.2 Feature Overview

This document describes the Functional Description of the ETSI BRI activity A00006271 “CEPT Act/Deact and Interrogation for ETSI BRI CFK, CFB/CFD K” in ISN08.

This feature is needed to make available the activation, deactivation and interrogation of CFB per Key (Call Forwarding Busy per Key), CFD per Key (Call Forwarding Don’t Answer per Key) and CFK (Call Forwarding Unconditional per Key) features based on the CEPT Dialing Sequence.

In this document, CFD is used instead of ETSI CFD or CFNR (Call Forwarding No Reply). With the existing implementation, CFD is used in Servord and in provisioning tables, and CFNR is invisible to the crafts person. Therefore, only CFD is used in this document to mean CFNR.

In this document, “MSN A” is used to define the DN which is assigned to ISDN BRI set or IBN set by configuring the TA’s (Terminal Adaptor) port as the first DN by subscriber and can be different from the primary DN (Key 1) provisioned at the exchange.

The following abbreviations are used in describing the activation, deactivation and interrogation control procedures of ETSI BRI CFK per Key in CEPT Dialing Sequence:

LH: Lift Handset, RH: Replace on Hook, DT: Dial Tone, ACK: Acknowledge Tone, NACK: Negative ACKnowledge Tone, AC: Access Code, DN: Directory Number, *: Dialing Star, #: Dialing Octotorphe.

According to Turk Telecom tender, the feature CFx per Key is enhanced to function on ETSI BRI lines by using CEPT Dialing Sequence.

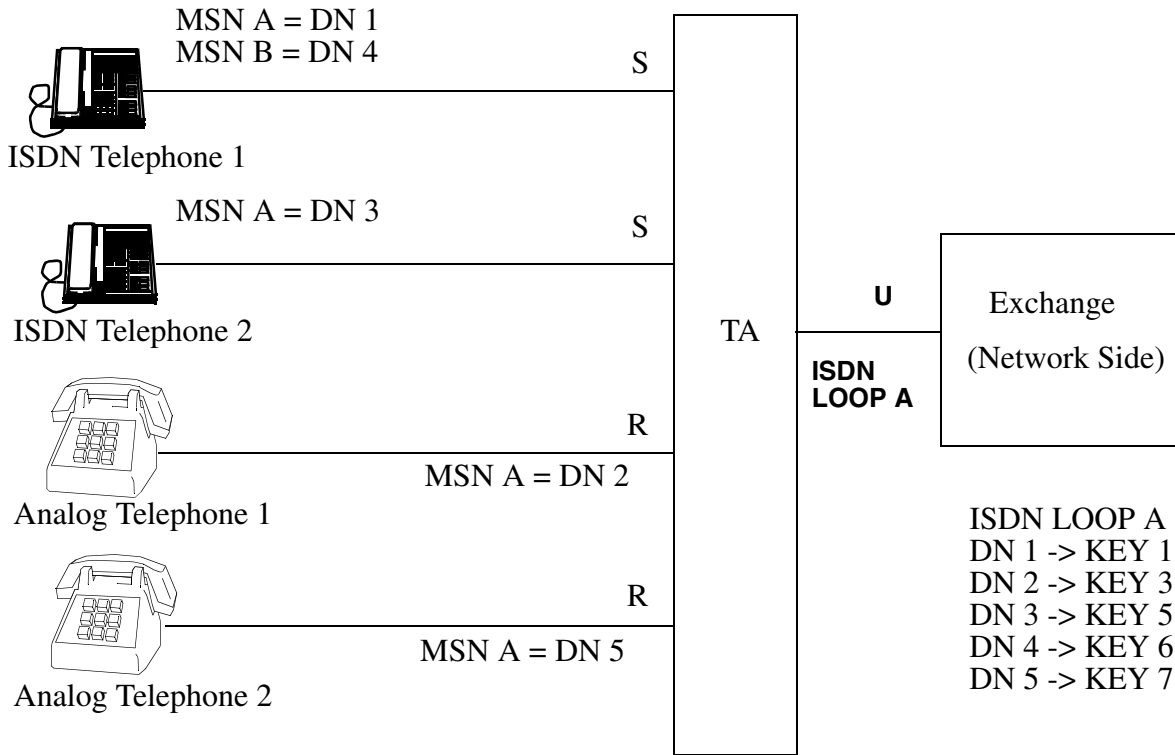
Although, subscriber can activate and deactivate a CFx per Key option by using ISDN BRI Set's menu options and keys (for more information, please refer to [2] A59028702 "Support of CFx for Multiple DN's for ETSI BRI" in PLS FMDOC), if there is an "Analog Telephone" on the loop which is connected to the ISDN loop over TA (Terminal Adaptor), user has no chance to use menu options and keys. So, this activity supplies CEPT dialing ability to the "Analog Telephone" user which is connected to the ISDN loop over TA (and also to the ISDN BRI user) to activate, deactivate and interrogate a CFx per Key option.

While explaining the desired behavior, refer to the example configuration in Figure. It is supposed that DN1, DN2, DN3, DN4 and DN5 of the "ISDN loop A" have CFx per Key options. If a subscriber has the configuration like Figure 1, subscriber might:

- a. Activate, deactivate or interrogate the CFx per Key option assigned to DN 1 by using "ISDN Telephone 1" (subscriber might activate, deactivate or interrogate a CFx per Key option assigned to DN of the MSN A of the ISDN BRI terminal which is used to dial CEPT sequence).
- b. Activate, deactivate or interrogate the CFx per Key option assigned to DN 4 by using "ISDN Telephone 1" (subscriber might activate, deactivate or interrogate a CFx per Key option assigned to DN of the MSN X (an MSN of the ISDN BRI set different than MSN A) of the ISDN BRI terminal which is used to dial CEPT sequence).
- c. Activate, deactivate or interrogate the CFx per Key option assigned to DN 3 by using "ISDN Telephone 1" (subscriber might activate, deactivate or interrogate a CFx per Key option assigned to DN of the MSN A of the other ISDN BRI terminal on the same ISDN loop).
- d. Activate, deactivate or interrogate the CFx per Key option assigned to DN 2 by using "Analog Telephone 1" (subscriber might activate, deactivate or interrogate a CFx per Key option assigned to DN of the MSN A of an Analog Telephone by dialing from that Analog Telephone which is connected to the ISDN loop over a TA).
- e. Activate, deactivate or interrogate the CFx per Key option assigned to DN 5 by using "Analog Telephone 1" (subscriber might activate, deactivate or interrogate a CFx per Key option assigned to DN of the MSN A of the other Analog Telephone on the same ISDN loop by dialing from another Analog Telephone on the same loop which is connected to the ISDN loop over a TA).
- f. Activate, deactivate or interrogate the CFx per Key option assigned to DN 3 by using "Analog Telephone 1" (subscriber might activate, deactivate or interrogate a CFx per Key option assigned to DN of the MSN A of an ISDN BRI terminal on the same ISDN loop by dialing

from an Analog Telephone on the same loop which is connected to the ISDN loop over a TA).

Figure 1 Sample Configuration of an ISDN loop



TA : Terminal Adaptor

8.2.2.1 Activating CFx per Key Option

1. If subscriber wants to activate:

a CFx per Key option assigned to DN of the MSN A of the ISDN BRI terminal which is used to dial CEPT sequence (item “a” of Section 8.2.2),

or

a CFx per Key option assigned to DN of the MSN A of an Analog Telephone by dialing from that Analog Telephone which is connected to the ISDN loop over a TA (item “d” of Section 8.2.2);

LH DT * AC * Forwarded to DN # ACK RH

The ETSI BRI Call Forward per Key option becomes active immediately after execution of this sequence. DN entered must be a translatable number, that means “Forwarded to DN” is validated.

Any incomplete activation sequence will result in NACK:

LH DT * AC * invalid-dialing-sequence NACK RH

The implementation of this behavior for the CFB per Key and CFD per Key options is already available in the existing code (if CFB per Key or CFD per Key options are assigned to MSN A of an ISDN BRI terminal which is used to dial CEPT sequence or assigned to DN of the MSN A of an Analog Telephone by dialing from that Analog Telephone which is connected to the ISDN loop over a TA, it already works). **This activity only implements this functionality for the CFK option.**

2. If subscriber wants to activate,

a CFx per Key option assigned to DN of the MSN X (an MSN of a terminal different than MSN A) of that terminal which is used to dial CEPT sequence (item “b” of Section 8.2.2),

or

a CFx per Key option assigned to DN of the MSN A of the other ISDN BRI terminal on the same ISDN loop (item “c” of Section 8.2.2),

or

a CFx per Key option assigned to DN of the MSN A of an Analog Telephone on the same ISDN loop by dialing from another Analog Telephone on the same loop which is connected to the ISDN loop over a TA (item “e” of Section 8.2.2),

or

a CFx per Key option assigned to DN of the MSN A of an ISDN BRI terminal on the same ISDN loop by dialing from an Analog Telephone on the same loop which is connected to the ISDN loop over a TA (item “f” of Section 8.2.2);

LH DT * AC * Forwarded to DN * DN of MSN X # ACK RH

The ETSI BRI Call Forward per Key option becomes active immediately after execution of this sequence. DN entered must be translatable number, that means Call Forwarded to DN is validated.

Any incomplete activation sequence will result in NACK:

LH DT * AC * invalid-dialing-sequence NACK RH

8.2.2.2 Deactivating CFx per Key Option

1. If subscriber wants to deactivate;

a CFx per Key option assigned to DN of the MSN A of the ISDN BRI terminal which is used to dial CEPT sequence (item “a” of Section 8.2.2),

or

a CFx per Key option assigned to DN of the MSN A of an Analog Telephone by dialing from that Analog Telephone which is connected to the ISDN loop over a TA (item “d” of Section 8.2.2);

LH DT # AC # ACK RH

The ETSI BRI Call Forward per Key option becomes deactive immediately after execution of this sequence.

The implementation of this behavior for the CFB per Key and CFD per Key options are already available in the existing code (if CFB per Key or CFD per Key options are assigned to MSN A of an ISDN BRI terminal which is used to dial CEPT sequence or assigned to DN of the MSN A of an Analog Telephone by dialing from that Analog Telephone which is connected to the ISDN loop over a TA, it already works). **This activity only implements this functionality for the CFK option.**

2. If subscriber wants to deactivate;

a CFx per Key option assigned to DN of the MSN X (an MSN of a terminal different than MSN A) of that terminal which is used to dial CEPT sequence (item “b” of Section 8.2.2),

or

a CFx per Key option assigned to DN of the MSN A of the other ISDN BRI terminal on the same ISDN loop (items “c” of Section 8.2.2),

or

a CFx per Key option assigned to DN of the MSN A of an Analog Telephone on the same ISDN loop by dialing from another Analog Telephone on the same loop which is connected to the ISDN loop over a TA (item “e” of Section 8.2.2),

or

a CFx per Key option assigned to DN of the MSN A of an ISDN BRI terminal on the same ISDN loop by dialing from an Analog Telephone on the same loop which is connected to the ISDN loop over a TA (item “f” of Section 8.2.2);

LH DT # AC * DN of MSN X # ACK RH

The ETSI BRI Call Forward per Key option becomes active immediately after execution of this sequence.

Any incomplete activation sequence will result in NACK:

LH DT * AC * invalid-dialing-sequence NACK RH

8.2.2.3 Interrogating CFx per Key Option

1. If subscriber wants to interrogate a “Forwarded to DN” of;
 - a CFx per Key option assigned to DN of the MSN A of the ISDN BRI terminal which is used to dial CEPT sequence (item “a” of Section 8.2.2),
 - or
 - a CFx per Key option assigned to DN of the MSN A of an Analog Telephone by dialing from that Analog Telephone which is connected to the ISDN loop over a TA (item “d” of Section 8.2.2);
 - if DN is equivalent to the DN stored,

LH DT *# AC * Forwarded to DN # ACK RH

if DN stored does not match the DN entered

LH DT *# AC * Forwarded to DN # NACK RH

The implementation of this behavior for the CFB per Key and CFD per Key options are already available in the existing code (if CFB per Key or CFD per Key options are assigned to MSN A of an ISDN BRI terminal which is used to dial CEPT sequence or assigned to DN of the MSN A of an Analog Telephone by dialing from that Analog Telephone which is connected to the ISDN loop over a TA, it already works). **This activity only implements this functionality for the CFK option.**

2. If subscriber wants to interrogate a “Forwarded to DN” of;
 - a CFx per Key option assigned to DN of the MSN X (an MSN of a terminal different than MSN A) of that terminal which is used to dial CEPT sequence (item “b” of Section 8.2.2),
 - or
 - a CFx per Key option assigned to DN of the MSN A of the other ISDN BRI terminal on the same ISDN loop (item “c” of Section 8.2.2),
 - or
 - a CFx per Key option assigned to DN of the MSN A of an Analog Telephone on the same ISDN loop by dialing from another Analog Telephone on the same loop which is connected to the ISDN loop over a TA (item “e” of Section 8.2.2),
 - or
 - a CFx per Key option assigned to DN of the MSN A of an ISDN BRI terminal on the same ISDN loop by dialing from an Analog Telephone on the same loop which is connected to the ISDN loop over a TA (item “f” of Section 8.2.2);

if DN is equivalent to the DN stored,

LH DT *# AC * Forwarded to DN * DN of MSN X # ACK RH

if DN stored does not match the DN entered

LH DT *# AC * Forwarded to DN * DN of MSN X # NACK RH

8.3 Hardware Requirements or Dependencies

N/A

8.4 Software Requirements or Dependencies

N/A

8.5 Limitations and restrictions

- Maximum number of digits for Forwarded-to-DN is 30.
- Restrictions for the maximum number of digits for DN-of -MSNX are as follows:
 - i. SNPA + OFC CODE + STN CODE $\leq$ 15
 - ii. OFC CODE + STN CODE $\leq$ 14
 - iii. STN CODE $\leq$ 8
 - iv. OFC CODE $\leq$ 7
- If dialed Forwarded-to-DN contains a DN which is available at the same office as the subscriber and if subscriber dials extra digits after the valid Forwarded-to-DN by following the restriction of the maximum number of digits for Forwarded-to-DN, extra digits are removed and the rest of the translatable digits are stored as Forwarded-to-DN.
- Since DN-of-MSNX must be a DN which is available ISDN loop of the subscriber (at the same office), if subscriber dials extra digits after the valid DN-of-MSNX by following the restriction of the maximum number of digits for DN-of-MSNX, it is acceptable.
- This activity is not supported for the Centrex offices.
- CEPT Act/Deact and Interrogation are not supported via Keypad Facility Messages.
- This activity is not affected from the "Flexible Digit Analysis". Although this activity uses "Flexible Digit Analysis" until collecting first three digits (until translation finding the feature), digit collection part of the FPE does not use "Flexible Digit Collection".
- If CEPT dialing sequence is not finished with octothorpe (#), after a time interval, a time-out message and a "last digit" message are received. When this message is received, it is evaluated as an error and a NACK (negative acknowledgement) tone is given to the user.

This time interval can vary for different CEPT dialing sequences (for example; according to number of digits dialed, between overlap and enblock dialing and between NDGT and STDCOLL digit collection types defined in NCOS table). Some of the test results for the available office settings (DGCOLNM: NDGT) are as follows:

	<u>ENBLOCK</u>	<u>OVERLAP</u>
*14*7831023	40s	10s
*14	40s	40s
#14	40s	40s
14	40s	10s
*14*7831023*7831093	40s	5s

8.6 Interactions

This activity follows the existing feature interaction rules. Existing interactions remain unchanged:

If RESL option types OTR and ORR are datafilled, Call Forward Deactivation and Interrogation are allowed. However, Activation of Call Forward is not allowed. If RESL option type TRR is datafilled, Call Forward Activation, Deactivation and Interrogation are allowed.

If OCB is active at the same DN, Call Forward Activation is not allowed according to restriction class of OCB. On the other hand, Deactivation and Interrogation are allowed to be programmed.

8.7 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

8.8 Glossary

Table 1

Term	Definition
BRI	Basic Rate Interface
WT	World Trade
CEPT	Conference of European Postal and Telecommunications
CFNR	Call Forward No Reply
CFB	Call Forward Busy
CFD	Call Forward Don't Answer
CFU	Call Forward Unconditional
CFx	Call Forward
TA	Terminal Adaptor
DN	Directory Number
MSN	Multiple Subscriber Number
AC	Access Code
ETSI	European Telecommunications Standard Institute
FPE	Feature Process Environment
KEYSET	Key telephone set

8.9 Recommended Reading/References

- A59034125 “ISDN BRI CEPT Call Forwarding”
- A59028702 “Support of CFx for Multiple DNs for ETSI BRI” in PLS FMDOC
- ETS 300 199, 200, 201, 202 Chapter 6.1
- AD9698 “CFB/CFD Per Key Destination” in PLS FMDOC

9: A00006387 Functional description (FN)

9.1 Feature name

Support of SUSpend/RESume over ETSI ISUP QFT (QSIG Feature Transparency)

9.2 Description

9.2.1 Purpose

The goal of the work covered by this activity is to provide new functionality to generate network initiated SUSpend/RESume messages over ETSI ISUP QFT (QSIG Feature Transparency) in response to on-hook/off-hook indications (respectively) from an analogue called party (IBN line).

Note: Throughout this document, the phrase “ETSI ISUP” is by implication referring to “ETSI ISUP V2 and ETSI ISUP V3”.

Note that it is assumed that the reader is familiar with the following specifications:

- ITU-T recommendations Q.761-Q.764
- ITU-T recommendation Q.767 D.2.5
- ETSI ISUP version 2+ APM/QSIG Feature Transparency

9.2.2 Background information

The current implementation of ETSI ISUP QFT mechanism does not support the generation of ISUP SUSpend message when an analogue line goes on-hook. The same applies to the generation of RESume message when a suspend message had previously been sent and the analogue called party goes off-hook. This feature enhances the DMS software to allow SUS/RES generation over ETSI ISUP QFT for public calls.

9.2.3 Functional description

By enabling the feature via datafilling the QFT_SUS_RES_SUPPORT parameter in table ISERVOPT the generation of the SUS/RES messages will be supported over ETSI ISUP QFT.

9.2.4 Feature Operation

This activity provides control of SUS/RES generation support over ETSI ISUP QFT to Line calls by introducing a new service option QFT_SUS_RES_SUPPORT of type Y or N in table ISERVOPT.

When service option QFT_SUS_RES_SUPPORT in table ISERVOPT is datafilled and assigned to Y, SUS/RES messages are generated for ETSI ISUP QFT to Line calls when the terminating Line goes on-hook and off-hook respectively.

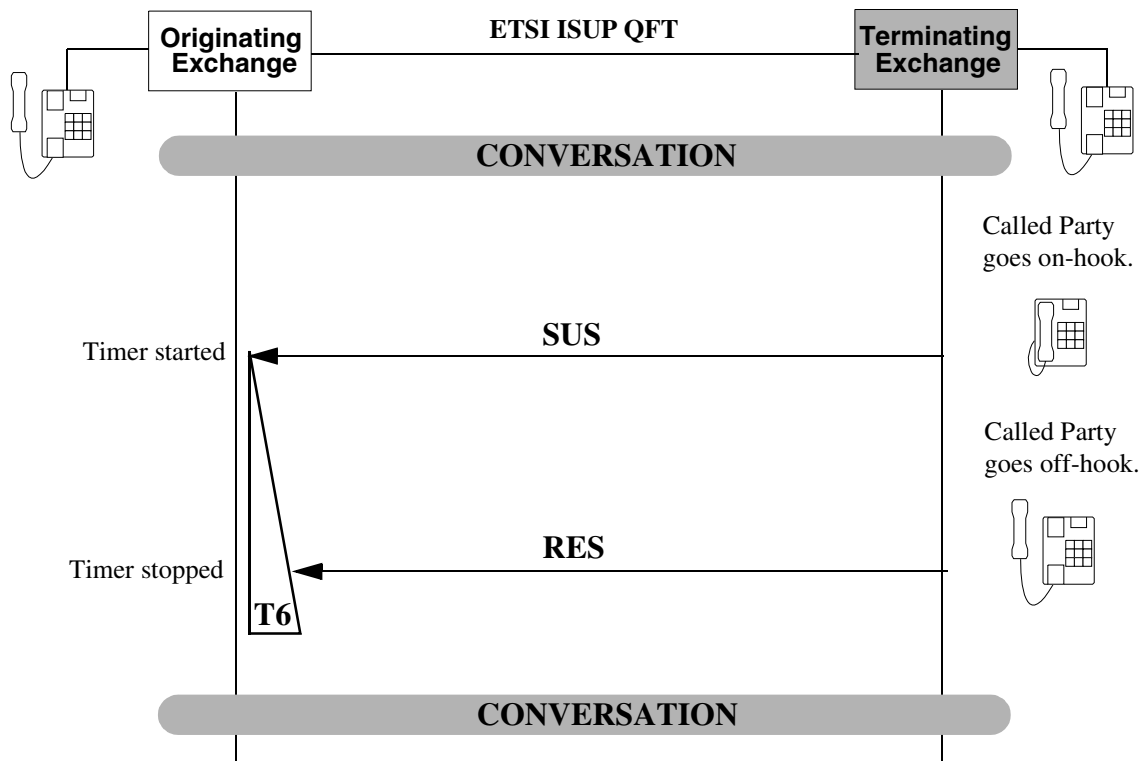
When service option QFT_SUS_RES_SUPPORT in table ISERVOPT is datafilled and assigned to N, ETSI ISUP QFT to Line call behavior remains unchanged and when the terminating Line goes on-hook the call is released immediately.

When service option QFT_SUS_RES_SUPPORT in table ISERVOPT is not datafilled, ETSI ISUP QFT to Line call behavior remains unchanged and when the terminating Line goes on-hook the call is released immediately.

The diagrams below show the desired behavior when the feature is activated.

9.2.4.1 Actions at the Originating and Terminating exchanges

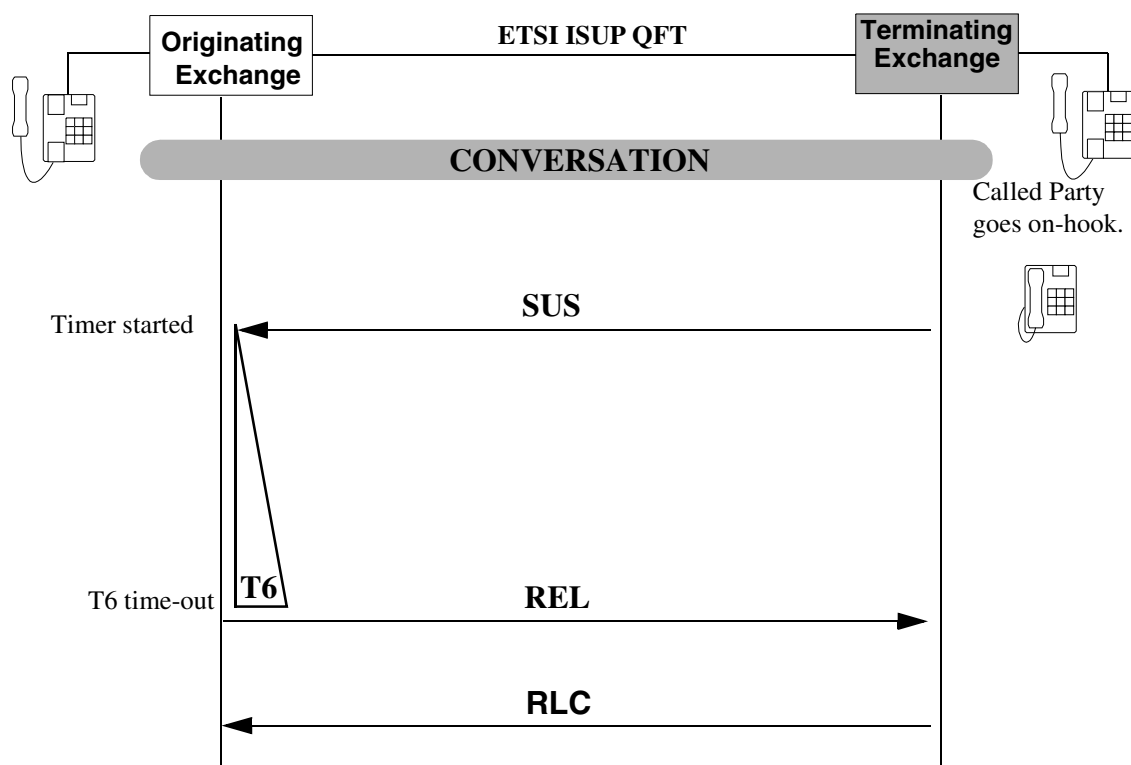
Figure 1 Resume before Re-answer time-out



At the terminating exchange, on receipt of an on-hook indication from the analogue called party, send a network Suspend message to the preceding exchange. On detection of the off-hook indication, the network Resume message is sent to the preceding exchange.

At the originating exchange on receipt of the network Suspend message, start the suspend timer T6. On receipt of the network Resume message, stop the timer T6 and continue with the call.

Figure 2 Re-answer timer expires.



On suspend timer (T6) expiry, a REL message with cause 102 (Recovery On Timer Expiry) is sent from the originating exchange. The call is released.

9.2.4.2 Actions at the interworking (Protocol X <-> ETSI ISUP QFT call) exchange

Figure 3 T6 Timer starting at Interworking (controlling) exchange

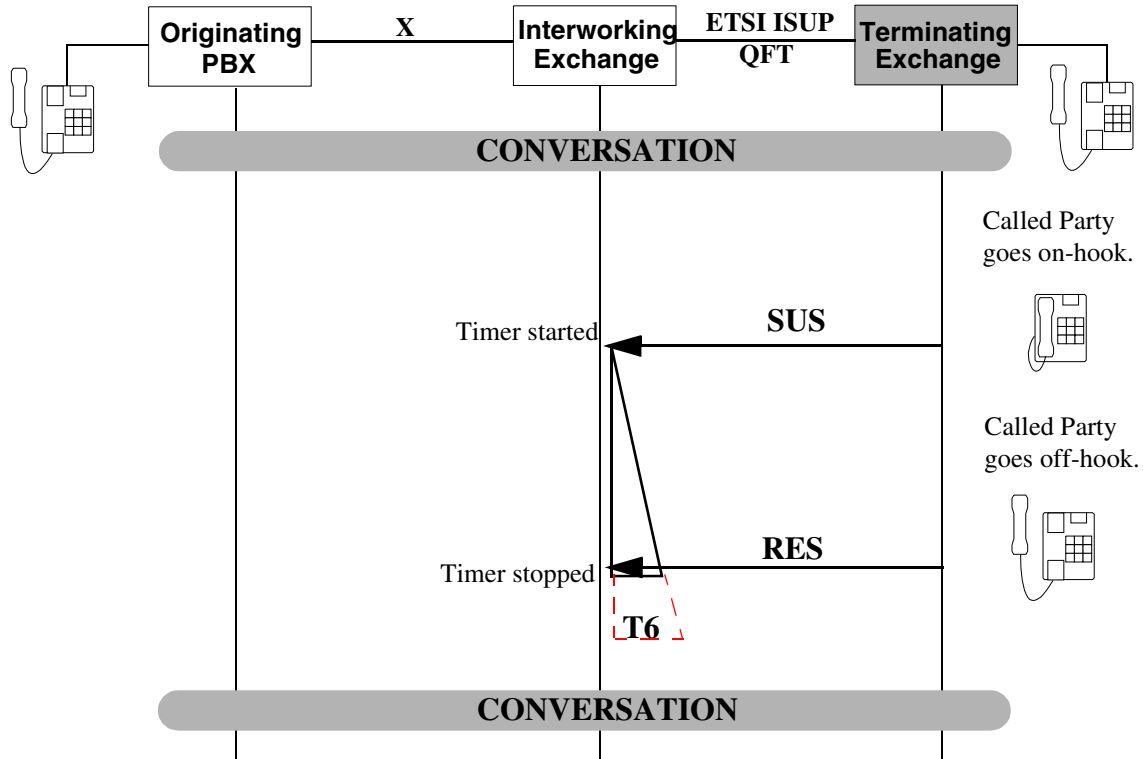


Figure 3 shows the message sequence for interworking to protocols (X) which neither support clear back indication nor suspend message (e.g.: QSIG/ PRI). The interworking exchange acts as the controlling exchange by running the timer T6.

Figure 4 T6 timer starting at the originating (controlling) exchange

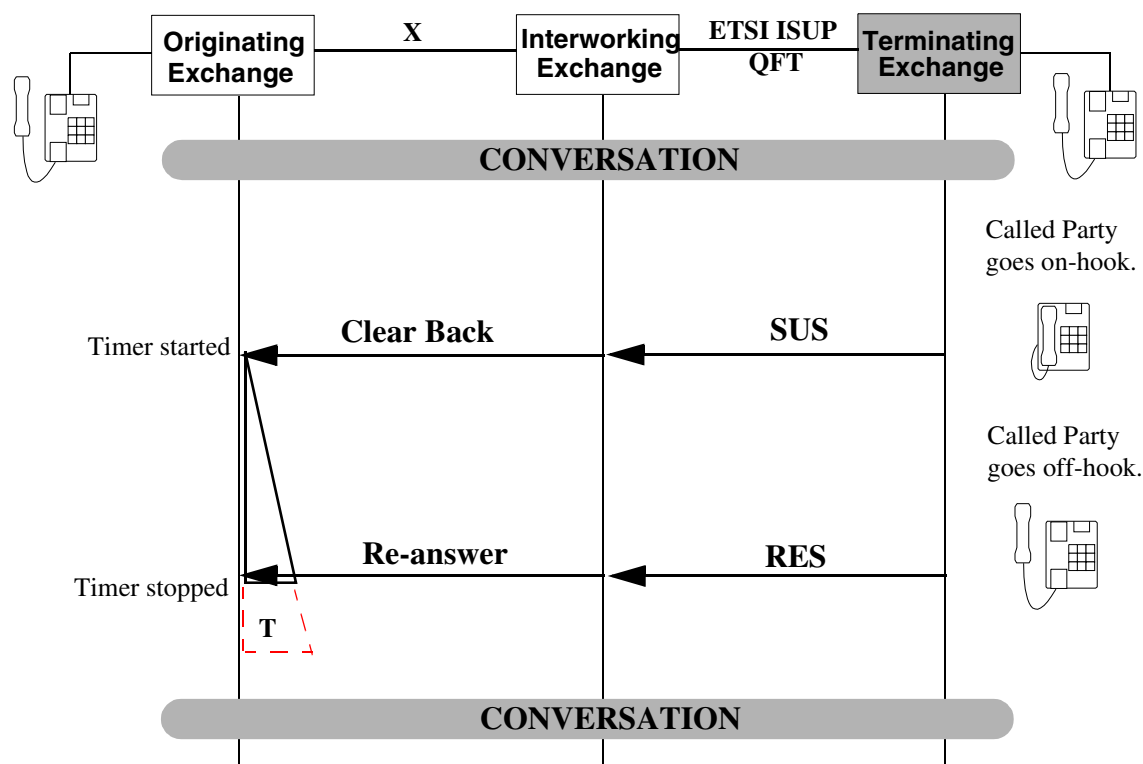


Figure 4 shows the re-answer timer(T) and the message sequence when interworking with protocol (X) which supports clear back indication (e.g.: BTUP/ R2/ R1). The originating exchange acts as the controlling exchange and starts the re-answer timer.

Figure 5 T6 time-out at interworking (controlling) exchange

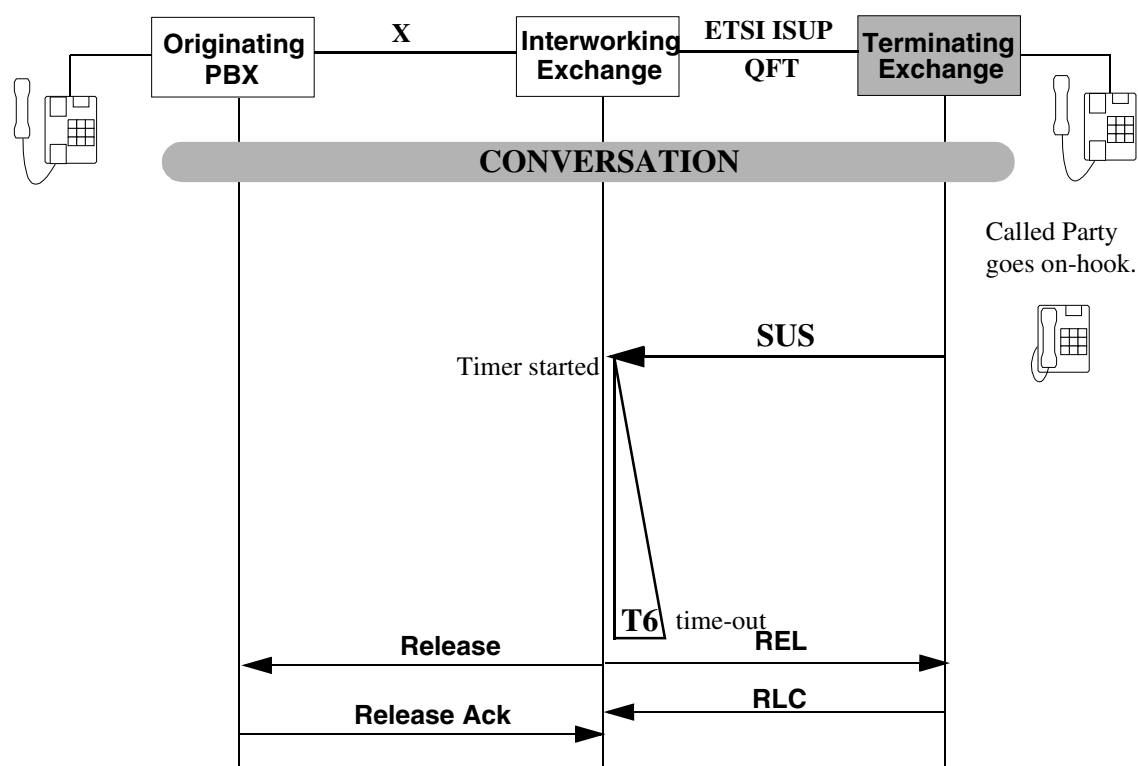


Figure 5 shows the Suspend timer T6 expiry at the interworking (controlling) exchange. This is governed by the fact that protocol X is not supporting clear back or re-answer indications (e.g.: QSIG/ PRI).

Figure 6 T6 timer interrupted by a REL message

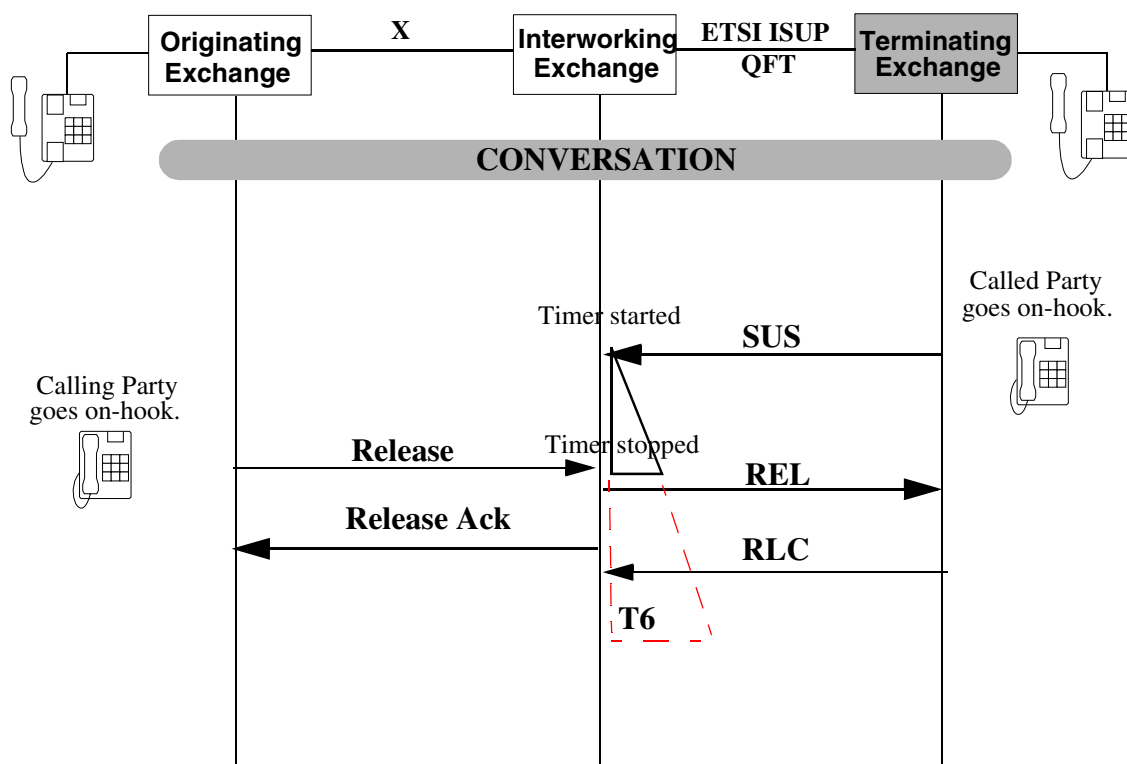
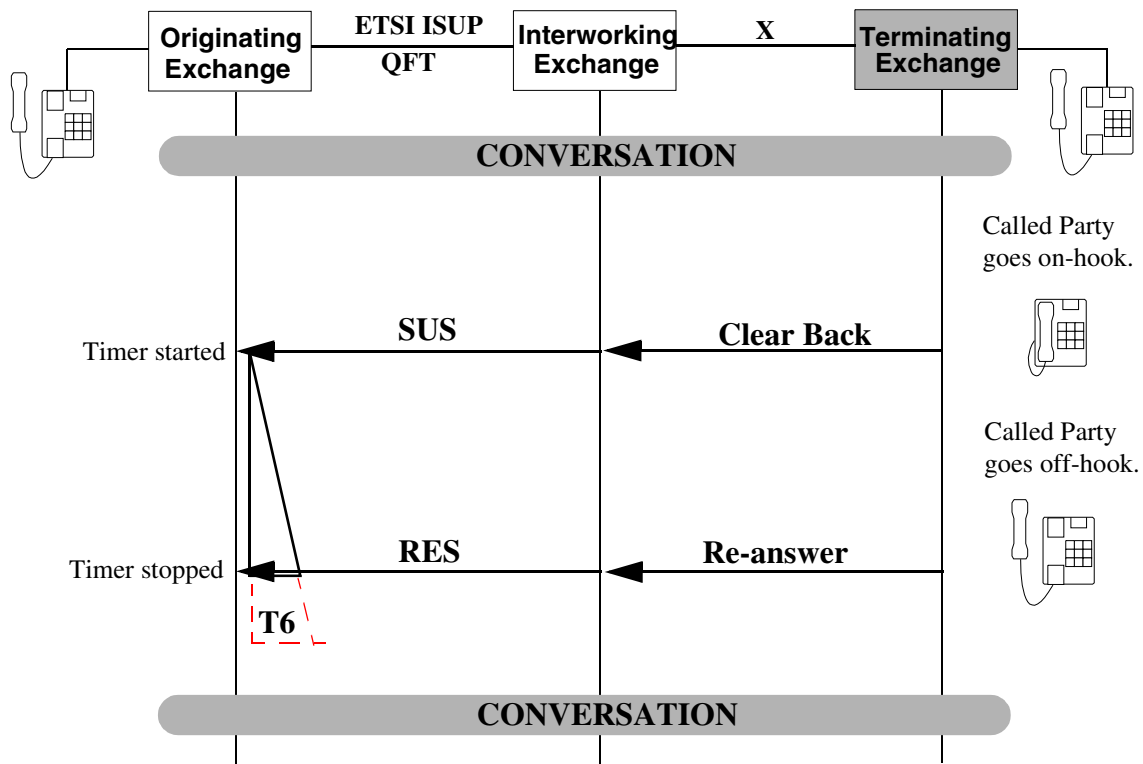


Figure 6 shows the result of a REL message being received while the timer T6 is running. The timer is stopped and the call is released.

Figure 7 Interworking Exchange.Suspend/Resume (network) message generation

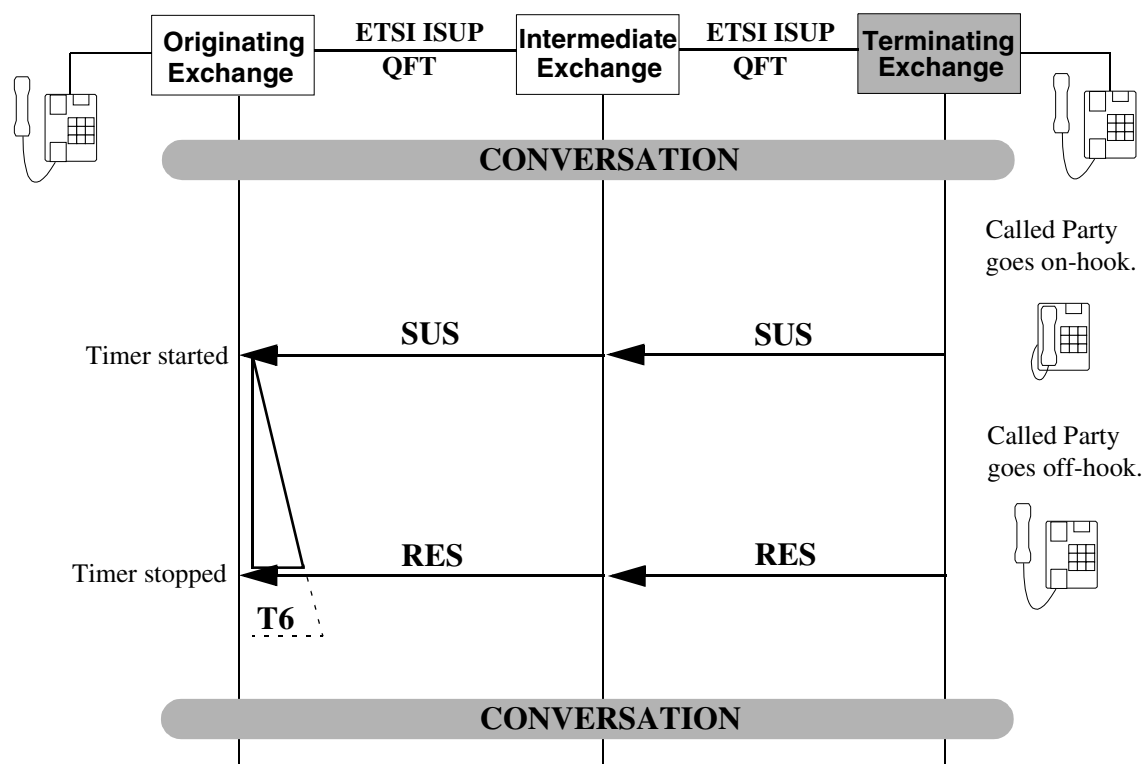


At the interworking exchange on receipt of the clear back indication from protocol (X) (e.g.: BTUP/ R2/ R1), send the suspend message to the preceding exchange. On receipt of the Re-answer indication, send a resume (network) message to the preceding exchange.

9.2.4.3 Actions at the Intermediate (Tandem-ETSI ISUP QFT to ETSI ISUP QFT call) exchange

At the intermediate exchange on receipt of the suspend/resume (network) message, the message is sent to the preceding exchange.

Figure 8 Network SUS/RES at Intermediate exchange



9.2.5 Activation

Feature activation is done by datafilling the service option QFT_SUS_RES_SUPPORT in table ISERVOPT and assigning to Y.

Please find the sample datafill below:

TABLE: ISERVOPT

>lis

SOPTSKEY SOPTSVAR

QFT_SUS_RES_SUPPORT QFT_SUS_RES_SUPPORT Y

9.3 Hardware Requirements or Dependencies

No changes due to this feature.

9.4 Software Requirements or Dependencies

The new functionality provided by this activity is being implemented using the existing interfaces. As such, no new software dependencies are being introduced.

This functionality requires release SN08 or higher loads.

9.5 Limitations and restrictions

This activity supports only analogue called parties (IBN line-host, remote and V5.2) as ETSI ISUP does. SUS/RES generation is not supported for ACD, UCD agents, BRI lines and PPhones.

9.6 Patch Availability

The activity is implemented in SN08 and patched back to SN04.

9.7 Interactions

Networked Centrex Services supported over ETSI ISUP QFT are in the scope of this activity.

Please refer to Chapter 14 (APM Feature Transparency) in ISN06 (TDM) Product Description (Issue ISN06TDM.4) document for the list of Networked Centrex Services supported over ETSI ISUP QFT.

9.8 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)___N/A___

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.

9.9 Glossary

Table 1

Term	Explanation
QFT	QSIG Feature Transparency
REL	ISUP Release Message
RES	ISUP Resume Message
RLC	ISUP Release Complete Message
SUS	ISUP Suspend Message

9.10 References

1. AJ4986 ETSI ISUP V2 Support for QFT (QSIG Feature Transparency) on the DMS100E
2. AU3360 ETSI ISUP (Q764) SUSpend/RESume Compliance
3. ISN06 (TDM) Product Description (Issue ISN06TDM.4)
4. ETSI ISUP version 2+ APM Feature Transparency DMS/CS2000 (Version: PRE 4.0)
5. ETSI ISUP version 2+ Q.SIG Feature Transparency DMS-MMP/CS2000 (Version: AUT 3.2)
6. AJ4356 QSIG Basic Call for the DMS-100 Phase 1
7. A59039741 Network Wide Calling Name Display (CNAMD over QFT)
8. ITU Q.767 D.2.5 and ITU Q.764 2.4 specifications

10: A00006406 Functional description (FN)

10.1 Feature name

ETSI ISUP(V1/V2 base) to J-PRI(V1/V2) UUI NAK

Platform: ISN08

10.2 Description

On CS2KC, there are two versions of Japan PRI(J-PRI): J-PRI V1 complies with the version 1 of INS1500 specification (Refer to 2.9 reference 3); J-PRI V2 complies with the version 5 of INS1500 specification.

Note: In table LTDEF, J-PRI V1 is datafilled as INSPRI V1; J-PRI V2 is datafilled as INSPRI V2.

Currently in ETSI ISUP(V1/V2 base) to J-PRI(V1/V2) interworkings, if an UUI parameter is included in the incoming ISUP IAM message, the UUI parameter is discarded and no acknowledgement is sent back.

In this feature, if an UUI parameter is included in the ETSI ISUP IAM message, an UUI negative acknowledgement will be sent out in the first backward ISUP message to indicate that UUI is not supported by J-PRI.

According to ITU-T Q767 Recommendation, parameter User-to-User Indicators with default value #81 is used as the negative acknowledgement. (Shown in Table 1)

Table 1 User-to-User Indicators (#81)

ETSI ISUP User-to-User Indicators optional parameter	
(Applies to message: ACM)	Bits
<u>Type</u>	<u>A</u>
Response	1
<u>Service 1</u> (If Bit A = 1)	<u>CB</u>
no information	00
<u>Service 2</u> (If Bit A = 1)	<u>ED</u>
no information	00
<u>Service 3</u> (If Bit A = 1)	<u>GF</u>
no information	00
<u>Network Discard Indicators</u>	<u>H</u>
UUI discarded by Network	1

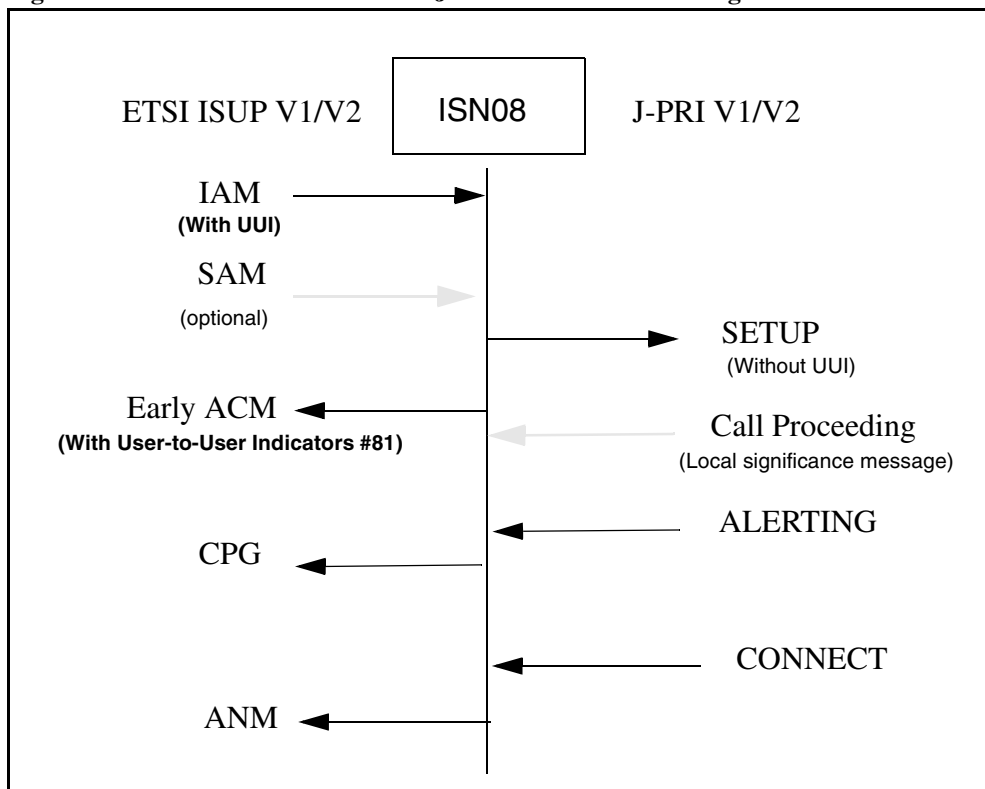
10.2.1 UUI negative acknowledgement in the normal call scenario

For ETSI ISUP(V1/V2 base) to J-PRI(V1/V2) successful normal call scenario, the first backward ISUP message is always early ACM¹.

With this feature, if an UUI parameter is included in the ETSI ISUP IAM message, the UUI negative acknowledgement (an optional parameter “User-to-User Indicators” with default value #81) is added into this early ACM.

The call flow for ETSI ISUP V1/V2 base to J-PRI V1/V2 interworking when an UUI parameter is included in the ETSI ISUP IAM is shown in Figure 1.

Figure 1 ETSI ISUP V1/V2 base To J-PRI V1/V2 Interworking



10.3 Hardware Requirements or Dependencies

N/A

10.4 Software Requirements or Dependencies

N/A

¹J-PRI does not support OVERLAP outpulsing and an early ACM message is always sent back to the ISUP side when the digits are completely collected under ETSI ISUP V1/V2 base -> J-PRI V1/V2 interworkings

10.5 Limitations and restrictions

1. UUI NAK in the scenario that incoming ETSI ISUP(V1/V2 base) call is forwarded to J-PRI(V1/V2) is not supported in this feature because of the logic of call forward handling. If UUI is included in incoming ISUP IAM and the call is forwarded by a non-ISDN line to PRI trunk, the UUI parameter is discarded in the call forward process. So when sending out ACM or CPG after the call forwarding, information that whether there is UUI parameter originally can not be got.

10.6 Interactions

N/A

10.7 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

10.8 Glossary

Table 2

Term	Description
ACM	Address Complete Message
ANM	Answer Message
CFB	Call Forward Busy
CFD	Call Forward Don't Answer
CFU	Call Forward Unconditional

Table 2

Term	Description
IAM	Initial Address Message
INS1500	Information Network System 1500
J-PRI	Japan PRI
NAK	Negative Acknowledgement
UUI	User-to-User Information

10.9 Reference

1. PRSDOC BX18840 - ANSI7+ to INS1500 interworking enhancement to support Q.767 in DMS-300
2. ITU-T Recommendation Q.767
3. NTT Technical Reference INSNet Service Interface Volume 3

11: A00006407 Functional description (FN)

11.1 Feature name

China ISUP Enhancement

Platform: ISN08

11.2 Description

11.2.1 Background

YD/T 1157-2001 “The Transfer of Calling Party Number between Operators” [reference 1] is released by China MII. In this specification, calling party number format is revised against the former China MII spec YDN038-1997 and YDN038.1-1999.

The existing China ISUP (CISUP) implementation originally complies with YDN038 and YDN038.1. This activity enhances it to comply with the following new specification on calling party number format in YD/T 1157.

1. YD/T1157 6.1.1 For originating local switch (line->trunk), the calling party number (CGPN) should be a local number, regardless whether it is a local call or a toll call.
2. YD/T1157 6.1.1 For local tandem switch (trunk->trunk), CGPN should be tandemmed unchanged, regardless whether it is a local call or a toll call.
3. YD/T 1157 6.1.2 For originating toll switch (trunk->trunk), CGPN should be changed from local number format to national significant number format with ‘0’ toll-prefix (‘0’+ area code + local number).
4. YD/T 1157 6.1.2 For toll tandem switch (trunk->trunk) and terminating toll switch (trunk->trunk), CGPN should be tandemmed unchanged.
5. YD/T 1157 8.1.1 If call forward (A->B->C) occurs among the same local network, i.e. A, B, C have the same area code, CGPN should be A’s local number, the original called number (OCN) should be B’s local number.
6. YD/T 1157 8.1.2 If call forward to toll number (A->B->C) occurs between different local networks, i.e. A and B have the same area code, while C has different area code from A and B, CGPN and OCN should be transferred as below:
 - For originating local switch, CGPN and OCN should be a local number.
 - For local tandem switch, CGPN and OCN should be tandemmed unchanged.
 - For originating toll switch, CGPN should be a national significant number with ‘0’ toll-prefix, OCN should be a national significant number without ‘0’ toll-prefix.

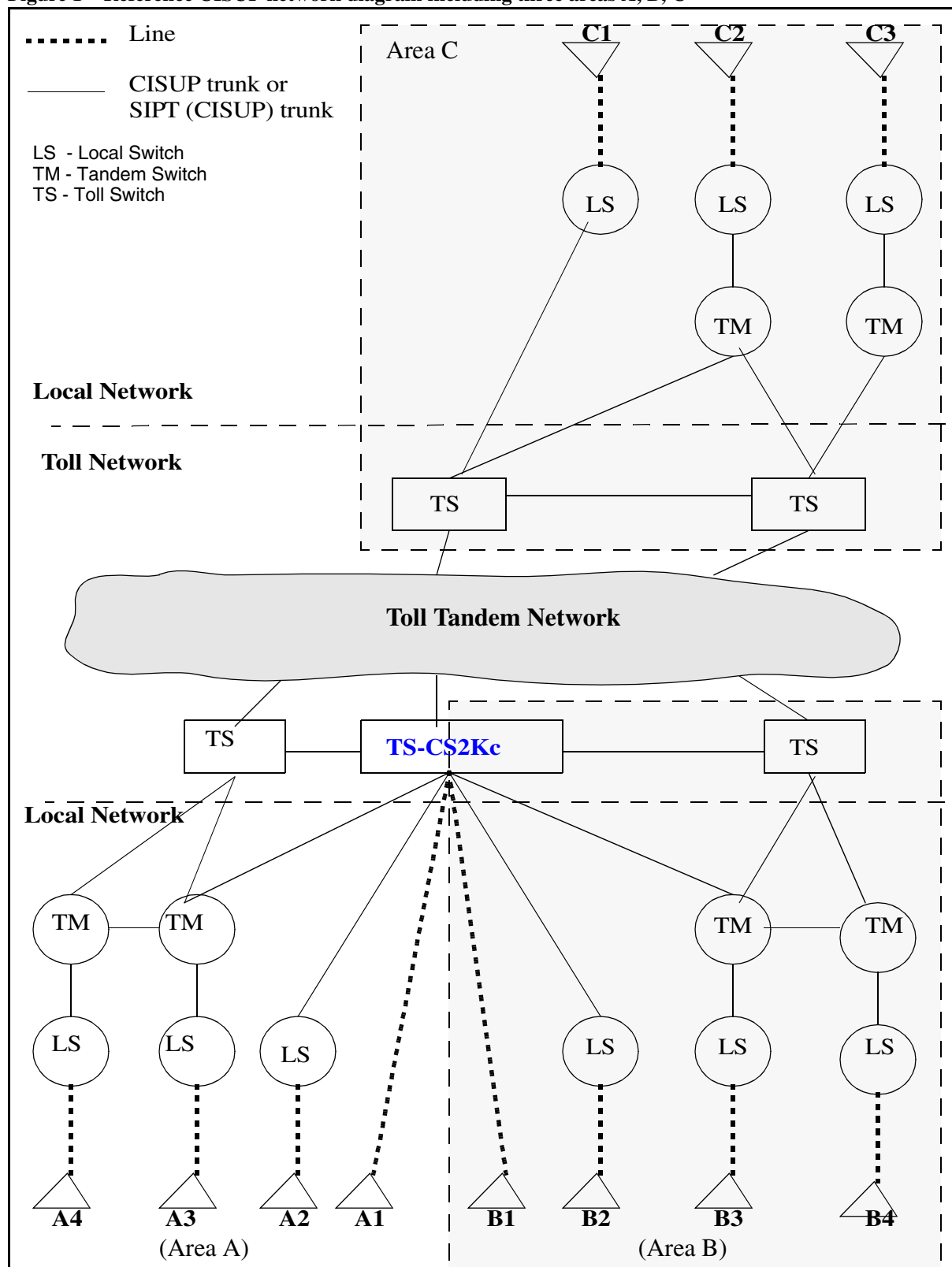
-
- For terminating switch, CGPN and OCN should be tandemed unchanged.
 - 7. YD/T 1157 8.1.3 If called party in a toll call registered call forward to local number (A->B->C), i.e. A and B have different area code while C has the same area code as B, CGPN and OCN should be as below:
 - For terminating tandem or local switch, CGPN should be tandemed unchanged. OCN should be a local number.

Moreover, the CISUP implementation on CS2Kc is required to have the capability to serve as local switch, local tandem switch and toll switch at the same time, and have the capability to serve multiple local networks.

Please refer to figure 1 for a reference CISUP network diagram.

Besides the general requirement above, there are still many specific deploy requirements from different customers. Please refer to SFR [reference 5] for a detail description.

Figure 1 Reference CISUP network diagram including three areas A, B, C



To meet the above requirements, a call control based CISUP parameter manipulation solution is provided by this activity. Operators can manipulate the following CISUP parameters according to different requirements through call control framework.

- calling party number (CGPN) CLI and NOA
- original called party number (OCN) CLI and NOA
- redirecting number (RGN) CLI and NOA

11.2.2 Introduction to Call Control

Universal Screening and call control allows the operator to 'Control' call processing events via datafill. Such events include invocation of screening and setting of internal translation/routing parameters.

Please refer to activity A59028780, A59033687 and A00004743 [reference 2, 3, 4] for more details on call control framework.

This activity enhances the call control functionality by:

1. supporting pre-translation call control trigger in table CUSTSTN for line originating calls.
2. supporting two new SCRNL options: 'OCN' and 'RGN'
3. enhancing DIGMAN setting option to manipulate CLI in OCN and/or RGN.
4. supporting a new setting option: 'NOA'

11.2.3 Feature Description

11.2.3.1 New Call Control Trigger in Table CUSTSTN

A new option 'CCNTLIDX' is added in table CUSTSTN to trigger call control functionality before translation for line originating calls. This option consists of a string of up to 32 characters which is used to set the index into table CALLCNTL. Only values that already exist in CALLCNTL can be datafilled in table CUSTSTN. This option allows CALLCNTL index to be associated with an IBN line.

Figure 2 Sample Datafill - Table CUSTSTN

TABLE CUSTSTN			
CUSTNAME	OPTNAME	OPTION	

CSGRPMB	CCNTLIDX	CCNTLIDX	CDPNSCRN

11.2.3.2 Two New SCR N Options: 'OCN' and 'RGN'

Two new SCR N options are added by this activity.

Table 1 New SCR N options

Option	Range of values	Description	Note
SCR N	SCR N_OPTION_RANGE: {CDPN, VAR, UKKCDPN, KK, CUSTGRP, CPCNAME, CDNNAME, CSP_CIC, RDRINFO, CGPNNOA, BC, CIP, TNS_CIC, TNS_CKT, OLI, CGPN, IPI, NCOS, CDPNLEN, OCN , RGN }	Enter OCN to screen original called number. The screen table is CGPNSCR N. Enter RGN to screen redirecting number. The screen table is CGPNSCR N.	'OCN' and 'RGN' are added by this activity

Figure 3 Sample Datafill - Table CALLCNTL

```
TABLE CALLCNTL
CALCTL_KEY CALCTL_OPTIONS
-----
200CN SCR N (OCN) $) $
200CN SCR N (RGN) $) $
```

- OCN screening

For line originating calls, OCN is present when call forwards occur in this switch. If SCR N option OCN is datafilled, the redirecting number in first call forward is retrieved and screened with the rule datafilled in the table CGPNSCR N.

For ISUP trunk originating calls, OCN is present when call forwards occur in proceeding switch or in this switch. If call forward occurs in proceeding switch, the OCN parameter in incoming message (CISUP IAM, CPRI SETUP or SIP INVITE) is retrieved and screened with the rule that datafilled in the table CGPNSCR N. If call forward occurs in this switch, the redirecting number in the first call forward is retrieved and screened with the rule datafilled in the table CGPNSCR N.

- RGN screening

For line originating calls, RGN is present when call forwards occur in this switch. If SCR N option RGN is datafilled, the redirecting number in last call forward is retrieved and screened with the rule datafilled in the table CGPNSCR N.

For ISUP trunk originating calls, RGN is present when call forwards occur in proceeding switch or in this switch. If call forward occurs in proceeding switch, the RGN parameter in incoming message (CISUP IAM, CPRI SETUP or SIP INVITE) is retrieved and screened with the rule that datafilled in the table CGPNSCRN. If call forward occurs in this switch, the redirecting number in the last call forward is retrieved and screened with the rule datafilled in the table CGPNSCRN.

11.2.3.3 Call control setting enhancement

- New DIGMAN_PARM 'OCN' and 'RGN' are added

Besides the existing DIGMAN_PARM 'CGPN' and 'CDPN', new DIGMAN_PARM 'OCN' and 'RGN' are provided in this activity to support CISUP OCN and RGN digit manipulation. The parameters in the outgoing CISUP messages (IAM/INF) can be changed according to the manipulation rule in table DIGMAN that the DMI index points to.

The OCN or RGN can be captured as calling dn in first AMA block for toll calls in toll originating switch when it is present in the incoming message (CISUP IAM, CPRI SETUP or SIP INVITE), the format is 'area code + local number'.

For forwarded calls in this switch, the original redirecting number is captured in 'CALLING DN' field in AMA blocks for forwarded calls.

- A new setting option 'NOA' is added

The NOA of CGPN, OCN and RGN in the outgoing CISUP messages (IAM/INF) can be set according to the datafilled NOA_Value.

Table 2 Enhanced Call Control Setting Options

Option	Range of Values	Description	Notes
DIGMAN	DIGMAN_PARM: {CDPN, CGPN, OCN , RGN }	Indicates which parameter is to be manipulated.	DIGMAN_PARM OCN and RGN are provided by this activity
	DMI: {0-32767}	Index into table DIGMAN to perform digit manipulation of the CDPN/CGPN/OCN/RGN (0 indicates NIL index).	
NOA	NOA_PARM: CGPN, OCN, RGN	Indicates which parameter is to be manipulated.	This option is added by this activity
	NOA_Value: {LCL, NATL}	overrides the NOA associated with the parameter.	

Figure 4 Sample Datafill - Table CGPNSCRN

TABLE: CGPNSCRN 20CGPNSCRN: CGPNDATA
FROMDIGS TODIGS CGPNINDX CCOPTION CGPNOPT

20 20 20CGPNSCRN (DIGMAN CGPN 020) (NOA CGPN LCL)
TABLE: CGPNSCRN 20OCNSCRN: CGPNDATA
FROMDIGS TODIGS CGPNINDX CCOPTION CGPNOPT

8331 8331 20OCNSCRN (DIGMAN OCN 30) (NOA OCN NATL)
TABLE: CGPNSCRN 20RGNSCRN: CGPNDATA
FROMDIGS TODIGS CGPNINDX CCOPTION CGPNOPT

8331 8331 20RGNSCRN (DIGMAN RGN 30) (NOA RGN NATL) \$

11.2.3.4 Traver tool support

The enhanced call control functionality can be verified using either the TRAVER tools.

Please refer to figure6 for a example traver with SCRN OCN, RGN and DIGMAN OCN, RGN and NOA (triggered from TRKOPTS)

11.2.3.5 New option CISUPAMA in table ISERVOPT

For China market specific requirment, a new option CISUPAMA is provided to control the format in AMA record for CISUP calls. The new option is added into table ISERVOPT.

New subfield PREFIX_0_TO_NATL_NUM_IN_AMA is provided under CISUPAMA option to control calling DN format. It can be datafilled as ‘Y’ or ‘N’.

Figure 5 Sample Datafill - Table ISERVOPT

TABLE: ISERVOPT
SOPTSKEY SOPTSVAR

CISUPAMA CISUPAMA Y

For the interworking mentioned in section 2.2.3.6, if PREFIX_0_TO_NATL_NUM_IN_AMA is datafilled as Y and the NOA of corresponding calling party number, OCN or RGN in the outgoing CISUP IAM is 0000011-national, the format of the calling DN in AMA should be ‘0+areacode+local number’ to indicate it is a national number. For wireless number, it should be ‘0+Carrier ID (13xx) + Subscriber number’.

For the interworking mentioned in section 2.2.3.6, if PREFIX_0_TO_NATL_NUM_IN_AMA is datafilled as N and the NOA of corresponding calling party number, OCN or RGN in the outgoing CISUP IAM is 0000011-national, the format of the calling DN in AMA should be 'areacode+local number'. For wireless number, it should be 'Carrier ID (13xx) + Subscriber number'.

If the option is not datafilled, the numbers in AMA record are the same as implemented as currently.

11.2.3.6 Interworking supported

The enhanced call control functionality are supported for following interworkings:

- Interworking from IBN line to CISUP/SIPT(CISUP)
- Interworking from V5.2 line to CISUP/SIPT (CISUP)
- Interworking from CISUP/ SIPT (CISUP) to CISUP/ SIPT (CISUP)
- Interworking form SIP to CISUP/ SIPT (CISUP)
- Interworking from China PRI to CISUP/SIPT (CISUP)

11.2.4 Usecase 1: Comply YD/T 1157 using enhanced call control

By using the enhanced call control functionality introduced above, requirements in YD/T 1157 can be met in CS2Kc.

CS2Kc can play different roles in the CISUP network. Please refer to the figure1 for a reference network diagram.

Table 3 CS2Kc CISUP (including SIPT (CISUP) YD/T 1157 compliance)

IC China ISUP IAM/ INF (from CISUP trunk or SIPT (CISUP) trunk)	CS2Kc role	call control is involved?	OG China ISUP IAM/INF (to CISUP trunk or SIPT (CISUP) trunk)	calling dn in AMA

Table 3 CS2Kc CISUP (including SIPT (CISUP) YD/T 1157 compliance)

NA	LS - local switch (Subscriber in this switch originates a call)	NA	CGPN: CGPN is built from the originating line. - Address Signal: local number - NOA: 0000001 - local OCN: OCN is built from the first call forward if call forwards occur in this switch. - Address Signal: local number - NOA: 0000001 - local RGN: RGN is built from the last call forward if call forwards occur in this switch. - Address Signal: local number - NOA: 0000001 - local	leg1: The originating number is captured in calling dn field. format: Depend on CISUPAMA option Leg2-n are present if call forwards occur in this switch leg2-n: The redirecting number is captured in calling dn field. format: Depend on CISUPAMA option

Table 3 CS2Kc CISUP (including SIPT (CISUP) YD/T 1157 compliance)

CGPN: local national OCN: local national OCN is not present RGN: local national RGN is not present	TM - tandem switch	NA	CGPN: CGPN is tandemmed unchanged, regardless whether call forwards occur in this switch. - Address signal: tandem unchanged. - NOA: tandem unchanged OCN: OCN is tandemmed unchanged if it is present in IC IAM, regardless whether call forwards occur in this switch. - Address signal: tandem unchanged. - NOA: tandem unchanged OCN is built from the first call forward if it is not present in IC IAM and call forwards occur in this switch. - Address Signal: local number - NOA: 0000001 - local RGN: RGN is tandemmed unchanged if it is present in IC IAM and no call forwards occur in this switch. - Address signal: tandem unchanged. - NOA: tandem unchanged RGN is built from the last call forward if call forwards occur in this switch. - Address Signal: local number - NOA: 0000001 - local	AMA is not required in tandem switch.

Table 3 CS2Kc CISUP (including SIPT (CISUP) YD/T 1157 compliance)

NA	TS - Toll switch (Subscriber in this switch originates a call)	Call control is triggered from table CUSTSTN (Please refer to figure5 for datafill example)	CGPN: CGPN is built from the originating line. If it has the same area code as the last forwarded number: - Address Signal: local number - NOA: 0000001 - local If it has different area code to the last forwarded number, - Address Signal: 0+ area code + local number - NOA: 0000011 - national OCN: OCN is built from the first call forward if call forwards occur in this switch. If it has the same area code as the last forwarded number: - Address Signal: local number - NOA: 0000001 - local If it has different area code to the last forwarded number, - Address Signal: area code + local number - NOA: 0000011 - national RGN: RGN is built from the last call forward if call forwards occur in this switch. If it has the same area code as the last forwarded number: - Address Signal: local number - NOA: 0000001 - local If it has different area code to the last forwarded number, - Address Signal: area code + local number - NOA: 0000011 - national	leg1: The originating number is captured in calling dn field format: Depend on CISUPAMA option Leg2-n are present if call forwards occur in this switch leg2-n: The redirecting number is captured in calling dn field. format: Depend on CISUPAMA option

Table 3 CS2Kc CISUP (including SIPT (CISUP) YD/T 1157 compliance)

CGPN: local national	TS - toll switch	Call control is triggered from table TRKOPTS (Please refer to figure5 for datafill example)	CGPN: CGPN is tandemed if it is present in IC IAM/INF, regardless whether call forwards occur in this switch. If it has the same area code as CDPN, - Address Signal: local number - NOA: 0000001 - local If it has different area code to CDPN, - Address Signal: 0 + area code + local number - NOA: 0000011 - national	For local tandem calls, AMA is not required. The AMA for toll calls is as below: Leg1: If RGN is present in the incoming IAM message, the RGN is captured in calling dn field. If RGN is not but OCN is present in the incoming IAM message, the OCN is captured in calling dn field. If both RGN and OCN are not present in the incoming IAM message, the CGPN is captured in calling dn field.
OCN: local national			OCN: OCN is tandemed if it is present in IC IAM, regardless whether call forwards occur in this switch. If it has the same area code as CDPN, Address Signal: local number NOA: 0000001 - local If it has different area code to CDPN, Address Signal: area code + local number NOA: 0000011 - national OCN is built from the first call forward if it is not present in IC IAM and call forwards occur in this switch. Its format follows the same rule above.	format: Depend on CISUPAMA option
OCN is not present			RGN: RGN is tandemed if it is present in IC IAM and no call forward occurs in this switch. If it has the same area code as CDPN, Address Signal: local number NOA: 0000001 - local If it has different area code to CDPN, Address Signal: area code + local number NOA: 0000011 - national	Leg2-n are present if call forwards occur in this switch. Leg2-n: The redirecting number is captured in calling dn field. format: Depend on CISUPAMA option
RGN is not present			RGN is built from the last call forward if call forward occurs in this switch. Its format follows the same rule above	

Figure5 shows a example datafill for CS2Kc toll switch in reference CISUP network diagram (figure1) to comply YD/T 1157 requirements using call control. In this case, the CS2Kc is not only serving as toll switch for two local areas: 20 and 30, but also is serving as originating switch and tandem switch at the same time for the two local areas.

Figure6 shows traver example with SCRN OCN, RGN and DIGMAN OCN, RGN and NOA (triggered from TRKOPTS)

Figure 6 Call control datafill example for toll switch serving multiple local network

```

TABLE: CUSTSTN
CUSTNAME OPTNAME OPTION
-----
CSGRPMB CCNTLIDX CCNTLIDX CDPNSCRN

Table TRKOPTS
OPTKEY OPTINFO
-----
CISUPTB_MB CCNTLIDX CCNTLIDX CDPNSCRN

TABLE: CALLCNTL
CALCTL_KEY CALCTL_OPTIONS
-----
CDPNNSCRN (SCRN (CDPN)) $
20CGPNNSCRN (SCRN (CGPN))(goto callcntl 20OCNSCRN)$
20OCNSCRN (SCRN (OCN))(goto callcntl 20RGNSCRN)$
20RGNSCRN (SCRN (RGN))$
30CGPNNSCRN (SCRN (CGPN))(goto callcntl 30OCNSCRN)$
30OCNSCRN (SCRN (OCN))(goto callcntl 30RGNSCRN)$
30RGNSCRN (SCRN (RGN))$
40CGPNNSCRN (SCRN (CGPN))(goto callcntl 40OCNSCRN)$
40OCNSCRN (SCRN (OCN))(goto callcntl 40RGNSCRN)$
40RGNSCRN (SCRN (RGN))$

TABLE CDPNSCRN
CDPNNSCRN_KEY CDPNDATA
-----
CDPNNSCRN (1)

TABLE: CDPNSCRN CGPNNSCRN: CDPNDATA
FROMDIGS TODIGS CDPNINDEX CCOPTION CDPNOPT
-----
% screen the CDPN and route to correct index.
% following tuples screen the toll call
030 030 30CGPNNSCRN $
040 040 40CGPNNSCRN $
050 050 50CGPNNSCRN $
% following tuples screen the local call
020 020 20CGPNNSCRN $
8222 8222 20CGPNNSCRN $
8223 8223 20CGPNNSCRN $
030 030 30CGPNNSCRN $
8332 8332 30CGPNNSCRN $
8333 8333 30CGPNNSCRN $

TABLE CGPNNSCRN
CGPNKEY CDPNDATA
-----
20CGPNNSCRN (1)
20OCNSCRN (1)
20RGNSCRN (1)
30CGPNNSCRN (1)
30OCNSCRN (1)
30RGNSCRN (1)
40CGPNNSCRN (1)
40OCNSCRN (1)
40RGNSCRN (1)

```


TABLE: CGPNNSCRN 20CGPNNSCRN: CGPNNDATA
FROMDIGS TODIGS CGPNINDX CCOPTION CGPNOPT

% area code 20 is served by this switch
% 1. CGPN is in this serving area (20) and in local format - do nothing
% 2. CGPN is in this serving area (20) and in national format - remove SNPA
% 3. CGPN is in other serving areas (30) and in local format - add SNPA
% 4. CGPN is in other serving areas (30) and in national format - do nothing
% 5. CGPN is out of serving areas, this is a tandem toll call. - tandem it
020 020 20CGPNNSCRN (DIGMAN CGPN 020) (NOA CGPN LCL)
20 20 20CGPNNSCRN (DIGMAN CGPN 020) (NOA CGPN LCL) (BILLCLI ORIG)
8331 8331 20CGPNNSCRN (DIGMAN CGPN 20) (NOA CGPN NATL)
8332 8332 20CGPNNSCRN (DIGMAN CGPN 20) (NOA CGPN NATL)

TABLE: CGPNNSCRN 20OCNSCRN: CGPNNDATA
FROMDIGS TODIGS CGPNINDX CCOPTION CGPNOPT

% the same screen rules as 20CGPNNSCRN, but OCN is manipulated this time.
020 020 20OCNSCRN (DIGMAN OCN 020) (NOA OCN LCL)
20 20 20OCNSCRN (DIGMAN OCN 020) (NOA OCN LCL)
8331 8331 20OCNSCRN (DIGMAN OCN 20) (NOA OCN NATL)
8332 8332 20OCNSCRN (DIGMAN OCN 20) (NOA OCN NATL)

TABLE: CGPNNSCRN 20RGNSCRN: CGPNNDATA
FROMDIGS TODIGS CGPNINDX CCOPTION CGPNOPT

% the same screen rules as 20CGPNNSCRN, but OCN is manipulated this time.
020 020 20RGNSCRN (DIGMAN RGN 020) (NOA RGN LCL)
20 20 20RGNSCRN (DIGMAN RGN 020) (NOA RGN LCL)
8331 8331 20RGNSCRN (DIGMAN RGN 20) (NOA RGN NATL)
8332 8332 20RGNSCRN (DIGMAN RGN 20) (NOA RGN NATL)

TABLE: CGPNNSCRN 40CGPNNSCRN: CGPNNDATA
FROMDIGS TODIGS CGPNINDX CCOPTION CGPNOPT

% area code 40 is not served by this switch
% 1. CGPN is in serving areas (20, 30) and in local format - add SNPA
% 2. CGPN is in serving areas (20, 30) and in national format - do nothing
% 3. CGPN is out of serving areas, this is a tandem toll call. - tandem it
8221 8221 40CGPNNSCRN (DIGMAN CGPN 20) (NOA CGPN NATL)
8222 8222 40CGPNNSCRN (DIGMAN CGPN 20) (NOA CGPN NATL)
8331 8331 40CGPNNSCRN (DIGMAN CGPN 30) (NOA CGPN NATL)
8332 8332 40CGPNNSCRN (DIGMAN CGPN 30) (NOA CGPN NATL)

TABLE: CGPNNSCRN 40OCNSCRN: CGPNNDATA
FROMDIGS TODIGS CGPNINDX CCOPTION CGPNOPT

% the same screen rules as 40CGPNNSCRN, but OCN is manipulated this time.
8221 8221 40OCNSCRN (DIGMAN OCN 20) (NOA OCN NATL)
8222 8222 40OCNSCRN (DIGMAN OCN 20) (NOA OCN NATL)
8331 8331 40OCNSCRN (DIGMAN OCN 30) (NOA OCN NATL)
8332 8332 40OCNSCRN (DIGMAN OCN 30) (NOA OCN NATL)

```
TABLE: CGPNSCRN 40RGNSCRN: CGPNDATA
FROMDIGS TODIGS CGPNINDX CCOPTION CGPNOPT
```

```
-----
% the same screen rules as 40CGPNSCRN, but RGN is manipulated this time.
```

```
8221 8221 40RGNSCRN (DIGMAN RGN 20) (NOA RGN NATL)
8222 8222 40RGNSCRN (DIGMAN RGN 20) (NOA RGN NATL)
8331 8331 40RGNSCRN (DIGMAN RGN 30) (NOA RGN NATL)
8332 8332 40RGNSCRN (DIGMAN RGN 30) (NOA RGN NATL)
```

```
TABLE: DIGMAN
DMIKEY DMIDATA
```

```
-----
20 (INC 020) $
020 (REM 3) $
30 (INC 030) $
030 (REM 3) $
40 (INC 040) $
040 (REM 3) $
```

Figure 7 Example TRAVER showing SCR N OCN, RGN and DIGMAN OCN, RGN and NOA

```

traver tr cisuptb_mb 03083333200 b
TABLE TRKGRP
CISUPTB_MB IBNT2 0 NPDGP NCRT CSGRPTB 0 MIDL 2 N ANSDISC 0 N N N N N N N 0 0 N
0 0 0 N N N N N N N NATL (ANISEND ALWAYS) $
TABLE TRKOPTS
CISUPTB_MB CCNTLIDX CCNTLIDX CDPNSCRN
TABLE CALLCNTL
CDPNSCRN
    (SCRN ( CDPN ) $)$
    . . TABLE CDPNSCRN
    . . CDPNSCRN (1)
    . . SUBTABLE CDPNDATA
    . . 03083333200 03083333200 30CGPNSCRN $ $
    . TABLE CALLCNTL
    . 30CGPNSCRN
    . (SCRN ( CGPN ) $) (GOTO CALLCNTL 30OCNSCRN ) $
PLEASE ENTER CLI DIGITS:
>82223200
    . . TABLE CGPNSCRN
    . . 30CGPNSCRN (1)
    . . SUBTABLE CGPNDATA
    . . 82223200 82223200 30CGPNSCRN ( DIGMAN CGPN 20) (NOA CGPN NATL)$ $
The Original Calling Party Number is: 82223200
    . . . TABLE DIGMAN
    . . . 20 (INC 020)
    . . . EXIT TABLE DIGMAN
The Calling Party Number has been set to: 02082223200
    . TABLE CALLCNTL
    . 30OCNSCRN
    . (SCRN ( OCN ) $) (GOTO CALLCNTL 30RGNSCRN ) $
PLEASE ENTER DIGITS FOR ORIGINAL CALLED NUMBER:
>82223201
    . . TABLE CGPNSCRN
    . . 30OCNSCRN (1)
    . . SUBTABLE CGPNDATA
    . . 82223201 82223201 30OCNSCRN ( DIGMAN OCN 20) (NOA OCN NATL)$ $
The Pre-modified Original Called Number is: 82223201
    . . . TABLE DIGMAN
    . . . 20 (INC 020)
    . . . EXIT TABLE DIGMAN
The Original Called Number has been set to: 02082223201
    . TABLE CALLCNTL
    . 30RGNSCRN
    . (SCRN ( RGN ) $) $
PLEASE ENTER DIGITS FOR REDIRECTING NUMBER:
>82223202
    . . TABLE CGPNSCRN
    . . 30OCNSCRN (1)
    . . SUBTABLE CGPNDATA
    . . 82223202 82223202 30RGNSCRN ( DIGMAN RGN 20) (NOA RGN NATL)$ $
The Pre-modified Redirecting Number is: 82223202
    . . . TABLE DIGMAN
    . . . 20 (INC 020)
    . . . EXIT TABLE DIGMAN
The Redirecting Number has been set to: 02082223202

```

```

TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP: no subscribed trigger.
TABLE NCOS
CSGRPTB 2 0 0 NCOSTB ( XLAS CSXLTB FEATXLA CSDIG)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CSGRPTB NXLA CSXLTB NXLA 0 CSDIG
TABLE DIGCOL
CSDIG 0 COL L 7
INAP Info Collected TDP: no subscribed trigger.
TABLE IBNXLA: XLANAME CSXLTB
CSXLTB 0 NET N N 0 N CSDIG N Y DOD N CSXLTB CSXLTB CS_NIL NONE $
TABLE DIGCOL
CSDIG 0 COL L 7
TABLE LINEATTR
CSXLTB IBN NONE NT 2 0 NILSFC 0 PX CSXLTB NIL 00 CSXLTB CS_NIL $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
CSXLTB NSCR 20 NPRT NONE N $ $
TABLE RATEAREA
CS_NIL NLCA NIL NILLATA $
TABLE PXHEAD
CSXLTB SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 03083333200
TABLE PXCODE
CSXLTB 030 030 RTE ( MM 3 18) ( DEST 33) ( CLASS NATL)$
TABLE: PXRTE
KEY: CSXLTB 33
. S CISUPTB_TA
EXIT TABLE PXRTE
INAP Info Analyzed TDP: no subscribed trigger.
INAP Route Select Failure TDP: no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 CISUPTB_TA 03083333200 ST

TREATMENT ROUTES. TREATMENT IS: GNCT
1 BUSY

+++ TRAVER: SUCCESSFUL CALL TRACE +

```

11.2.5 Usecase2: CGPN, OCN and RGN manipulation for interworking from SIP (no payload) to CISUP

For SIP to CISUP interworkings, the CGPN, OCN and RGN in the outgoing CISUP messages (IAM/INF) can be manipulated using enhanced call control framework.

Table4 shows a general manipulation rule for SIP to CISUP interworkings.

Figure7 shows a sample datafill in TM-CS2Kc or LS-CS2Kc for SIP to CISUP interworking.

Table 4 CGPN, OCN and RGN manipulation for SIP to CISUP interworking

IC SIP INVITE	CS2Kc role	call control is involved?	OG CISUP IAM/INF (to CISUP or SIPT (CISUP) trunk)	calling dn format in AMA
From header username: national number First “Remote-Party-ID” header in which party=redirect username: national number First “Remote-Party-ID” header in which party=redirect username: national number	LS - local switch or TM - tandem switch	Call control is triggered from table TRKOPTS (Please refer to figure7 for datafill example)	CGPN: CGPN is built from the From header. - Address Signals: local number - NOA: 0000001 - local OCN: OCN is built from the first Remote-Party-ID header in which party = redirect. - Address Signals: local number - NOA: 0000001 - local RGN: RGN is built from the first Remote-Party-ID header in which party = redirect. - Address Signals: local number - NOA: 0000001 - local	Leg1: The RGN in incoming INVITE message is captured in calling dn field. format: Depend on CISUPAMA option If RGN is not present and CGPN is present in the incoming INVITE message, the CGPN is captured in calling dn field. format: Depend on CISUPAMA option

Table 4 CGPN, OCN and RGN manipulation for SIP to CISUP interworking

From header username: national number First Remote-Party-ID header in which party=redirect username: national number First Remote-Party-ID header in which party=redirect username: national number	TS - Toll switch	Call control is triggered from table TRKOPTS The example datafill in figure5 for general toll switch can also be used in this case.	CGPN: CGPN is built from the From header. If it has the same area code as CDPN, - Address Signals: local number - NOA: 0000001 - local If it has the different area code as CDPN, - Address Signals: 0 + area code + local number - NOA: 0000011 - national OCN: OCN is built from the Remote-Party-ID header in which party = redirect. If it has the same area code as CDPN, - Address Signals: local number - NOA: 0000001 - local If it has the different area code as CDPN, - Address Signals: area code + local number - NOA: 0000011 - national RGN: OCN is built from the Remote-Party-ID header in which party = redirect. If it has the same area code as CDPN, - Address Signals: local number - NOA: 0000001 - local If it has the different area code as CDPN, - Address Signals: area code + local number - NOA: 0000011 - national	Leg1: The RGN in incoming INVITE message is captured in calling dn field. format: Depend on CISUPAMA option If RGN is not present and CGPN is present in the incoming INVITE message, the CGPN is captured in calling dn field. format: Depend on CISUPAMA option

Figure 8 Sample datafill in TM-CS2Kc or LS-CS2Kc for SIP to CISUP interworking

```

TABLE: CUSTSTN
CUSTNAME OPTNAME OPTION
-----
CSGRPMB CCNTLIDX CCNTLIDX CDPNSCRN

Table TRKOPTS
OPTKEY OPTINFO
-----
SIP_MCS CCNTLIDX CCNTLIDX SIPCGPNSCRN

TABLE: CALLCNTL
CALCTL_KEY CALCTL_OPTIONS
-----
SIPCGPNSCRN (SCRN (CGPN))(goto callcntl SIPOCNSCRN)$
SIPOCNSCRN (SCRN (OCN))(goto callcntl SIPRGNSCRN)$
SIPRGNSCRN (SCRN (RGN))$

TABLE CGPNSCRN
CGPNKEY CDPNDATA
-----
SIPCGPNSCRN (1)
SIPOCNSCRN (1)
SIPRGNSCRN (1)

TABLE: CGPNSCRN SIPCGPNSCRN: CGPNDATA
FROMDIGS TODIGS CGPNINDEX CCOPTION CGPNOPT
-----
% 1. CGPN is in serving areas (20,30) and in local format - do nothing
% 2. CGPN is in serving areas (20,30) and in national format - remove SNPA
% 3. CGPN is out of serving areas (40), this must be a terminating toll call or
% tandem toll call. jsut tandem it.
020 020 SIPCGPNSCRN (DIGMAN CGPN 020)(NOA CGPN LCL)
030 030 SIPCGPNSCRN (DIGMAN CGPN 030)(NOA CGPN LCL)

TABLE: CGPNSCRN SIPOCNSCRN: CGPNDATA
FROMDIGS TODIGS CGPNINDEX CCOPTION CGPNOPT
-----
% the same screen rules as SIPCGPNSCRN, but OCN is manipulated this time.
020 020 SIPOCNSCRN (DIGMAN OCN 020)(NOA OCN LCL)
030 030 SIPOCNSCRN (DIGMAN OCN 030)(NOA OCN LCL)

TABLE: CGPNSCRN SIPRGNSCRN: CGPNDATA
FROMDIGS TODIGS CGPNINDEX CCOPTION CGPNOPT
-----
% the same screen rules as SIPCGPNSCRN, but OCN is manipulated this time.
020 020 SIPRGNSCRN (DIGMAN RGN 020)(NOA RGN LCL)
030 030 SIPRGNSCRN (DIGMAN RGN 030)(NOA RGN LCL)

```

11.2.6 Usecase3: CGPN, OCN and RGN manipulation for interworking from China PRI to CISUP/SIPT(CISUP)

For China PRI (CPRI) to CISUP/SIPT(CISUP) interworkings, the CGPN, OCN and RGN in the outgoing CISUP messages (IAM/INF) can be manipulated using enhanced call control framework.

Table4 shows a general manipulation rule for CPRI to CISUP/SIPT(CISUP) interworkings.

Table 5 CGPN, OCN and RGN manipulation for CPRI to CISUP/SIPT(CISUP) interworking

IC CPRI SETUP	CS2Kc role	call control is involved?	OG CISUP IAM/INF (to CISUP or SIPT (CISUP) trunk)	calling dn format in AMA
Calling Party Number IE Number digits: area code + local number TypeofNumber: 010 - National number DivertingLegInfo2 component of FACILITY IE diverting number: areacode + local number original called number: areacode + local number	LS - local switch	Call control is triggered from table TRKOPTS	CGPN: CGPN is built from the From header. - Address Signals: local number - NOA: 0000001 - local OCN: OCN is mapped from diverting number in DivertingLegInfo2 component of FACILITY IE. - Address Signals: local number - NOA: 0000001 - local RGN: OCN is mapped from original called number in DivertingLegInfo2 component of FACILITY IE. - Address Signals: local number - NOA: 0000001 - local	Leg1: The diverting number in incoming SETUP message is captured in calling dn field. format: Depend on CISUPAMA option If diverting number is not present and CGPN is present in the incoming SETUP message, the CGPN is captured in calling dn field. format: Depend on CISUPAMA option

Table 5 CGPN, OCN and RGN manipulation for CPRI to CISUP/SIPT(CISUP) interworking

Calling Party Number IE Number digits: area code + local number Type of Number: 010 - National number Diverting Leg Info 2 component of FACILITY IE diverting number: areacode + local number original called number: areacode + local number	TS - Toll switch	Call control is triggered from table TRKOPTS The example datafill in figure 5 for general toll switch can also be used in this case.	CGPN: CGPN is built from the From header. If it has the same area code as CDPN, - Address Signals: local number - NOA: 0000001 - local If it has the different area code as CDPN, - Address Signals: 0 + area code + local number - NOA: 0000011 - national OCN: OCN is built from the Remote-Party-ID header in which party = redirect. If it has the same area code as CDPN, - Address Signals: local number - NOA: 0000001 - local If it has the different area code as CDPN, - Address Signals: area code + local number - NOA: 0000011 - national RGN: OCN is built from the Remote-Party-ID header in which party = redirect. If it has the same area code as CDPN, - Address Signals: local number - NOA: 0000001 - local If it has the different area code as CDPN, - Address Signals: area code + local number - NOA: 0000011 - national	Leg1: The diverting number in incoming SETUP message is captured in calling dn field. format: Depend on CISUPAMA option If diverting number is not present and CGPN is present in the incoming SETUP message, the CGPN is captured in calling dn field. format: Depend on CISUPAMA option

11.2.7 Usecase4: Manipulate non-wireline number resource

In China, some operators are using wireless number resource for lines in CS2Kc. wireless number plan is Carrier ID (13xx) + Subscriber number, which is different from the wireline number plan. For calls originating from lines with wireless number, CGPN, OCN and RGN in the outgoing CISUP messages (IAM/INF) should be a national significant number as below:

- Address Signals: 13xx + subscriber number
- NOA: 0000011 - national

The enhanced call control functionality can meet this specific requirement. Please refer to figure8 for sample datafill in CS2Kc. In this case, subscriber with wireless number originates a call in this switch.

Figure 9 Manipulate non-wireline number resource in LS-CS2Kc, TM-CS2Kc and TS-CS2Kc

```
TABLE: CGPNSCRN 20CGPNSCRN: CGPNDATA
FROMDIGS TODIGS CGPNINDX CCOPTION CGPNOPT
-----
% 1. CGPN is of wireless number plan format - change it to national significant
%      number
1360 1360 CGPNSCRN (NOA CGPN NATL)
```

11.3 Hardware Requirements or Dependencies

N/A

11.4 Software Requirements or Dependencies

N/A

11.5 Limitations and restrictions

1. New DIGMAN_PARM 'OCN' and 'RGN' are for CISUP outgoing OCN and RGN manipulation only. Other protocols are not considered in this activity.
2. New setting option 'NOA' is for CISUP outgoing NOA manipulation only. Other protocols are not considered in this activity.
3. This activity supports following interworkings:
 - Interworking from IBN line to CISUP/SIPT(CISUP)
 - Interworking from V5.2 line to CISUP/SIPT (CISUP)
 - Interworking from CISUP/ SIPT (CISUP) to CISUP/ SIPT (CISUP)
 - Interworking form SIP to CISUP/ SIPT (CISUP)
 - Interworking from CPRI to CISUP/SIPT (CISUP)

4. Currently, AMA billing is required only in local originating switch and toll originating switch. AMA billing in other types of switch is not considered in this activity.
5. The second leg line originated call in complex call scenarios except CFW is not supported by CUSTSTN line trigger.
6. The cases that the office code of CGPN, OCN or RGN in the incoming trunk (CISUP/ SIPT (CISUP)/SIP/CPRI) is same as the line area code when CS2kc roles as originating toll switch are not considered in this activity.

11.6 Interactions

1. Interaction between Call Control and Call Forward is as below:
 - For line originating calls with call control triggered in table CUSTSTN, if call forward occurs in this switch, call control functionality is triggered for the redirecting call with the call control index datafilled in table CUSTSTN for the redirecting line.
 - For trunk originating calls with call control triggered in table TRKOPTS, if call forward occurs in this switch, call control functionality is triggered for the redirecting call with the call control index datafilled in table CUSTSTN for the redirecting line.
 - Call Forward feature supported by this activity is as below:
 - Call Forward Unconditional
 - Call Forward Busy
 - Call Forward Don't answer

11.7 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_

Performance (includes operational measurements)_N/A_

11.8 Glossary

Table 6

Term	Description
IAM	Initial Address Message
CISUP	China ISUP
CGPN	CallinG Party Number
CDPN	CalleD Party Number
MII	Ministry of Information Industry
OCN	Original Called Number
RGN	RedirectinG Number

11.9 Reference

1. YD/T 1157-2001 The Transfer of Calling Party Number between Operators
2. A59028780: Call Control and Universal Screening
3. A59033687: Call Control and Universal Screening - Phase 2
4. A00004743: Line originations CLI modification through CALLCNTL
5. SFR V4 for China ISUP Enhancement

12: A00006636 Functional description (FN)

12.1 Feature name

First ITX on Answer.

12.2 Description

This activity, A00006636 “First ITX on Answer” in ISN08, provides the generation of the first ITX 500 msec after an answer. This is a TDM activity implemented on DMS100 MMP. Prior to this activity, first ITX is generated when the first interval (which is determined by the SSUTR2_ITX_RATE parameter in the table OFCENG) expires.

This feature is optional with a new SOC option. When the state of SOC is ON, the feature becomes active, otherwise the system behaves as it was before this functionality.

12.2.1 Background information

Currently, first ITX is generated when the first interval, which is equal to the SSUTR2_ITX_RATE value, expires. In the case of the call termination prior to the first interval expiry, the originator will not be charged for that call since no ITX message is received until the end of the call. With this activity the first ITX message is generated 500 msec after the RIU/ANM message is sent and therefore short duration calls can be charged for both the SSUTR2 and SPIROU terminating calls.

12.2.2 Existing ITX generation functionality

Please refer to the section AU3283, FN, Section 1.4.4. Datafill to Control ITX Generation.

12.2.3 Activation of the feature

Activation of the functionality is controlled by the SOC option NETK0086-”First ITX on Answer”.

First ITX on Answer is a state SOC and it has two states, ON and IDLE. Default state of *First ITX on Answer* is IDLE. When its state is ON, this feature becomes functional.

Table 1 SOC for Activation of Feature

SOC group:	NETK
SOC option name:	First ITX on Answer
SOC option title:	First ITX on Answer
SOC option control type:	state

New SOC option?	Yes
SOC option order code	NETK0086
Option defined in DRU:	WT21
Affected products:	ISN08

12.3 Sending first ITX after answer

Using this activity, the aim is to send the first ITX 500 msec after the ANM/RIU message is sent. Currently, calling subscriber cannot be charged, if the call is terminated prior to first ITX being sent. By sending the first ITX message 500 msec after RIU/ANM, short duration calls can be charged.

The count, to be carried by the first ITX sent 500 msec after the answer, is calculated according to the existing tuple in the MTRTARIF table for the first SSUTR2_ITX_RATE timer duration. There may be a difference between the first ITX count and the calculated count at the first SSUTR2_ITX_RATE expiry. This can be observed:

- If tariff changeover occurs (because of Time of Day, Day of Week, Day of Year etc.) or the tariff changes because of DMS system time changes before the first expiry of the SSUTR2_ITX_RATE during an active call.

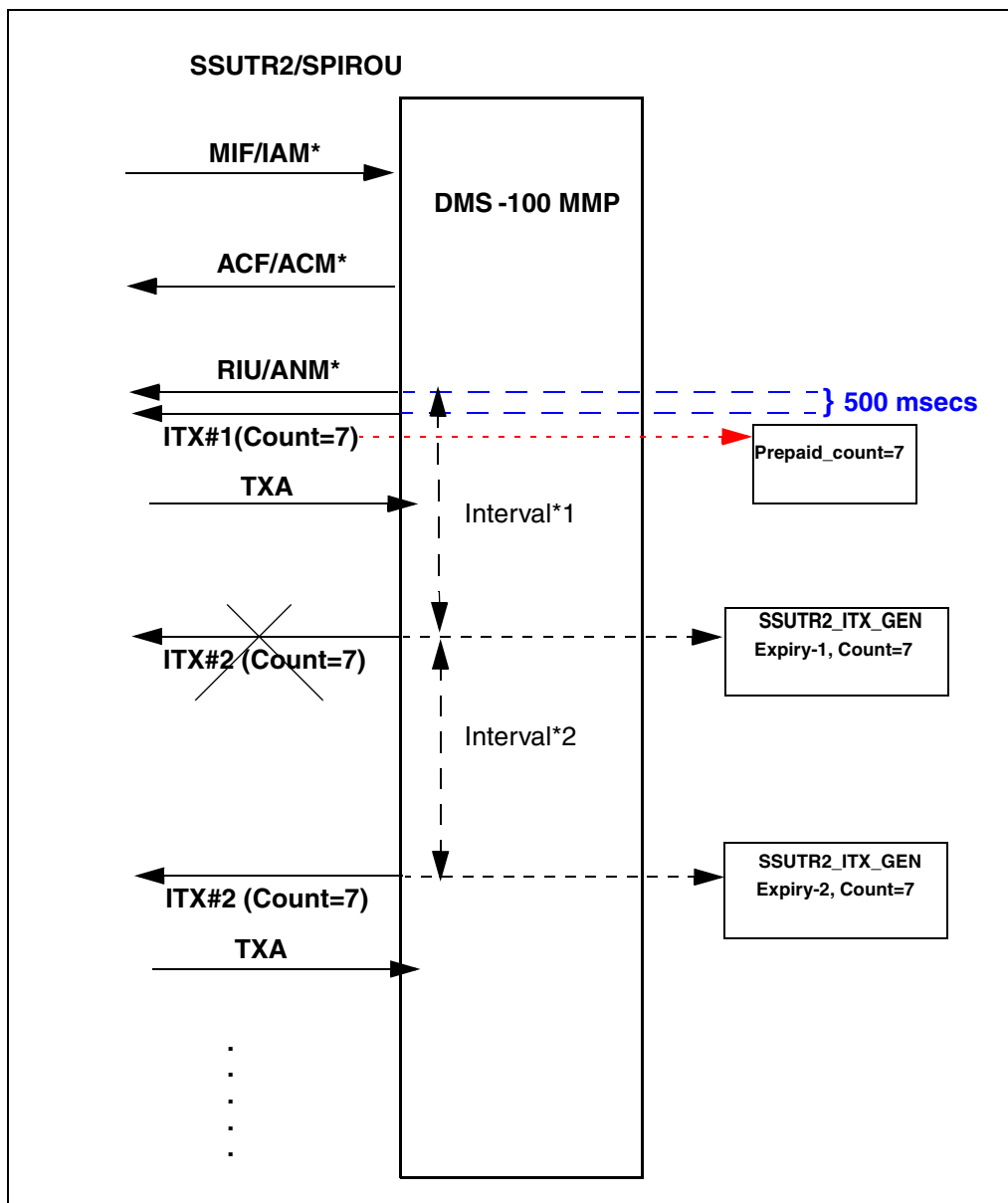
Please refer to the sections 1.4.1.1, 1.4.1.2, 1.4.1.3 to find how to handle this situation.

- If the phase starting times coincide with the times ITX messages are sent (determined by SSUTR2_ITX_RATE), please refer to 1.15 Appendix B to find examples for the following cases:
 - i. The case where SSUTR2_ITX_RATE coincides with datafilled burst duration.
 - ii. The case where SSUTR2_ITX_RATE does not coincide with datafilled burst duration.

12.3.1 ITX generation according to the tariff changes

12.3.1.1 No tariff change in active call:

If no tariff change occurs during an active call, no ITX is generated at the first SSUTR2_ITX_RATE expiry. At the second SSUTR2_ITX_RATE expiry, a second ITX is generated. Please refer to Figure 1 as an example.

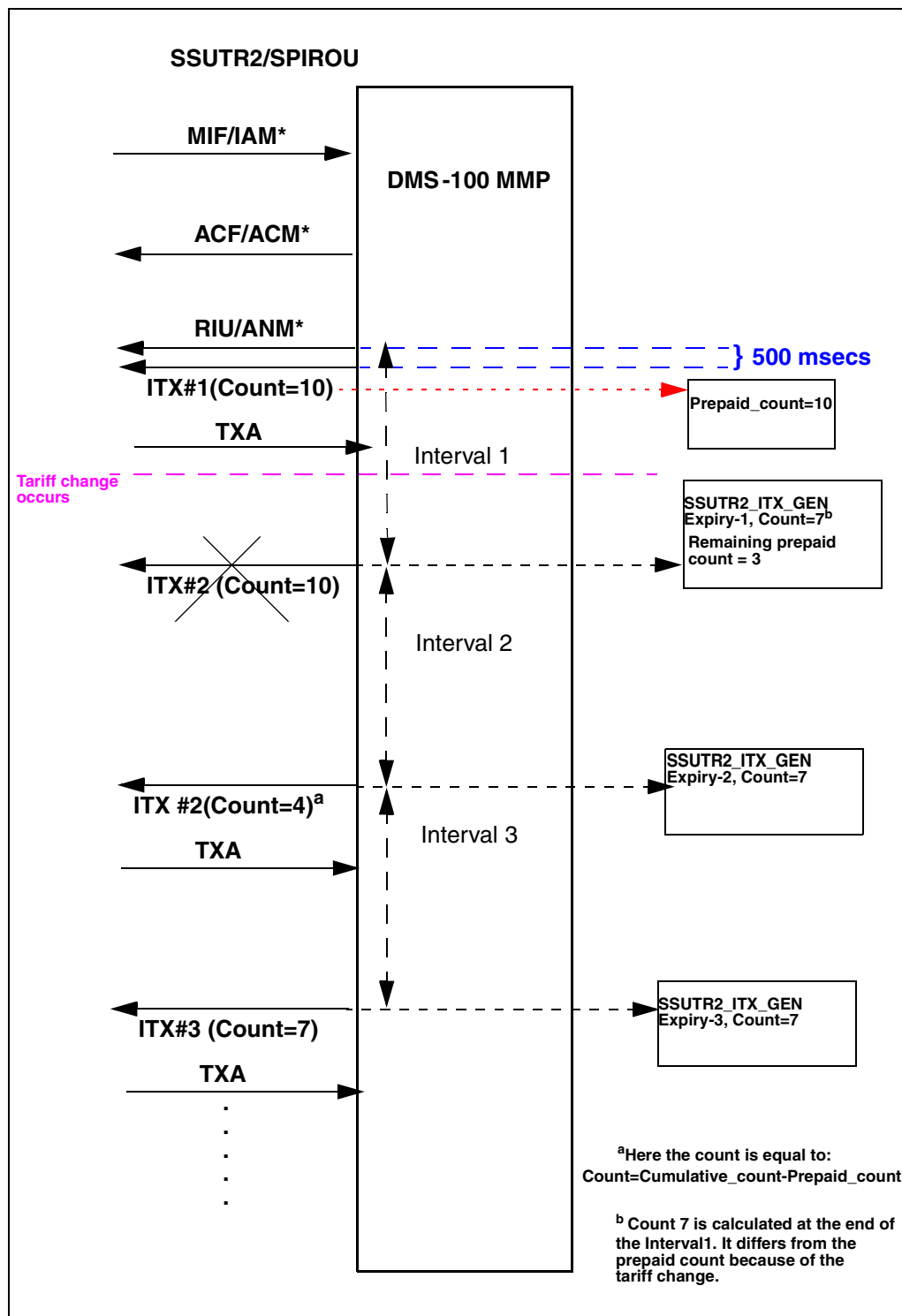
Figure 1 No Tariff Change During Active Call

*Interval value is determined by the SSUTR2_ITX_RATE parameter in the table OFCENG and is the same for all intervals.

12.3.1.2 Tariff Change to Lower Price in Active Call

Please refer to Figure 2 as an example.

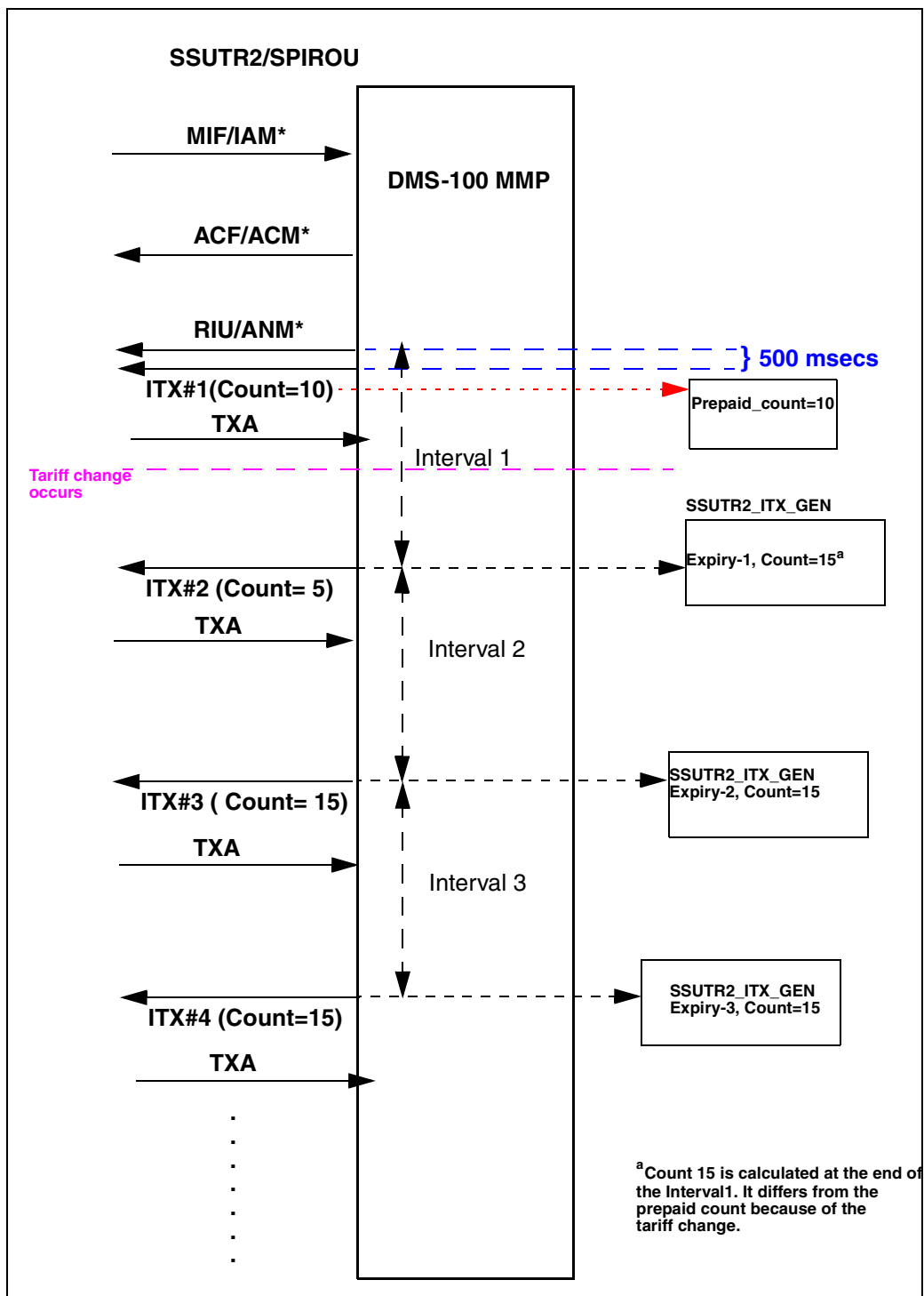
Figure 2 Tariff Change to Lower Price in Active Call



12.3.1.3 Tariff Change to Higher Price in Active Call

Please refer to Figure 3 as an example.

Figure 3 Tariff Change to Higher Price in Active Call



12.4 Interworkings

- SSUTR2 -> SPIROU
- SPIROU -> SSUTR2
- SSUTR2/SPIROU -> ETSI ISUP V1
- SSUTR2/SPIROU -> ETSI ISUP V2
- SSUTR2/SPIROU -> ETSI PRI
- SSUTR2/SPIROU -> QSIG
- SSUTR2/SPIROU -> Numeris VN4 PRI
- SSUTR2/SPIROU -> Numeris VN6 PRI

Note 1: If the required datafill exists for ITX generation, the first ITX is generated 500 msec after an answer at the SSUTR2/SPIROU side for interworkings listed above when the relevant SOC state is 'ON'.

Note 2: For non-SSUTR2/SPIROU to SSUTR2/SPIROU interworking, ITX which is sent by succeeding exchange is received. The mapping of this ITX message is not affected by this activity.

12.5 Datafill Requirements

There is no new datafill requirement for this feature. The existing datafill examples are provided in 1.14. Appendix A.

12.6 Hardware Requirements or Dependencies

This feature is supported only on the SX05 DTCO/DTCO2 processor.

12.7 Software Requirements or Dependencies

To make this new feature functional, the new state SOC option, “*First ITX on Answer*” is used. Since the SOC state will be IDLE after ONP is completed, it must be changed to ON manually to make the feature functional.

12.8 Limitations and restrictions

- All restrictions and limitations in AU3283-SSUTR2 SUPPORT FOR BACKWARD CHARGING, PLS DOC will be valid for this activity as well.
- It is recommended to use a metering tariff which does not coincide with the SSUTR2_ITX_RATE period for ITX generation.

As seen in the existing behavior, under some circumstances, the SSUTR2_ITX_RATE timer might coincide with the relevant phase duration timer datafilled in the MTRTARIF table. SSUTR2_ITX_RATE might expire just before or after the update of the stored metering count. Therefore, no precise count can be determined for that ITX if datafilled

burst duration for the relevant phase coincides with ITX generation period. That is why such usage is not recommended. Please refer the 1.15. Appendix B.

- If a tariff changeover occurs (because of Time of Day, Day of Week, Day of Year etc.) before the first expiry of the SSUTR2_ITX_RATE timer during an active call, then this change over is not considered for the first ITX message 500 msec after an answer.

For this exceptional case, any difference between the pulse count sent in the first ITX message and the real value at the ITX rate timer expiry will be reflected to the following (2nd, 3rd) ITX messages and total of the transmitted pulses will have the correct value at the end of the call.

If the call is ended before the mentioned pulse difference is reflected through subsequent ITX messages, then, the tariff change may not be applied to the call.

12.9 Interactions

No changes due to this feature.

12.10 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

12.11 Glossary

Table 2

Term	Description
ACF	ISDN address complete message with user to user facilities
ACM	Address Complete Message
AMA	Automatic Message Accounting
ANM	Answer Message
CM	Computing Module
DMS	Digital Multiplex System
FN	Functional Description
IAM	Initial Address Message
ITX	Charge Unit message
MIF	ISDN initial address message with user to user facilities
MMP	Multi-Market Product
RIU	Answer message with user to user information
SOC	Software Optionality Control
SPIROU	Signalisation Pour l'Interconnexion des Réseaux Ouverts
SSUTR2	Sous Systeme Utilisateur
TUP	Telephony User Part
TXA	Charging Acknowledgement message

12.12 References

- a. V 11-T 1998 Recommendation, Specification of the SSUTR2 user subsystem on the interface between the France Telecom fixed network and the third party networks at the VN6 functional phase
- b. AU3283-SSUTR2 SUPPORT FOR BACKWARD CHARGING, PLS DOC - CM part
- c. AU3284-SSUTR2 SUPPORT FOR BACKWARD CHARGING, PLS DOC - XPM part
- d. NTP 297-9051-020 MMP Metering Guide
- e. A00002101-Allow ITX only SSUTR2
- f. CR.Q00749093 - Zero ITX Charge count

12.13 Appendix A - Example datafill and traver for SSUTR2/SPIROU

12.13.1 Table TRKSGRP Datafill

- SSUTR2 trunk datafill:

2WFTUPAB 0 DS1SIG C7UP 2W N N UNEQ NONE Q767 THRH 0
DMS_NODE N N **FRANCE 100_BLUE** \$ FTUP2W CIC

- SPIROU trunk datafill:

SPIROUAB 0 DS1SIG C7UP 2W N N UNEQ NONE Q767 THRH 0 DMS N
N **SPIROU 100_EIV3** \$ 2WN7 CIC

12.13.2 Metering datafill example

TABLE OFCENG

SSUTR2_ITX_RATE 20

TABLE AMAOPTS

BACK_CHARGE ON

TABLE LTCINV

PDTC 1 1 IDTE 1 18 1 C 8 6X02UI QDT21XX (ABTRK DTCEX) \$ (2 48)
(2 49) (2 50) (2 51) (2 52) (2 53) (2 54) (2 55) (2 56) (2 57) (2 58) (2 59) (2 60)
(2 61) (2 62) (2 63) \$ (UTR9) (RAM6X69) (NT6X28) \$ TURKR1R2
SX05AA SX05AA 0 UPFWQM01 (CCS7) (FSTR2) (**METER**) \$ 6X40AC N

TABLE MTRLNET

LOC

TABLE MTRTARIF

53 SEC Y 0 1 0 12 1 15 0 1 0 16 1 15

TABLE MTRTTTS

LOC 8 Y 53 \$ \$ \$ \$ \$ \$ \$ \$

TABLE MTRMOTS

MOTS_2 LOC 4 8

TABLE MTRMOG

MDI4 MOTS_2 \$

TABLE DAYTYPES

NORMAL

SATDAY

SUNDAY

HOLIDAY

TABLE TODHEAD

LOC MTR LOC 0 NORMAL SATDAY SUNDAY \$

TABLE DAYOWEEK

LOC WED NORMAL

TABLE AOCBASIC

LOC 4 0 30

TABLE ACOPT

LOC 30 4 0 \$

TABLE CLISERV

METERING 1 SERVSCRN \$

TABLE CLISRVPF

1 METERING \$ \$

TABLE DNSCRN

1027835479 NETAOCD 30 CLISERV 1 \$

12.13.3 Traver example for SSUTR2-SSUTR2 call when NETAOCD is datafilled:

>traver tr mftupba 3967835480 tariff b

TABLE TRKGRP

MFTUPBA IBNT2 0 NPDGP NCRT SERKAN 0 LIDL 0 N ANSDISC 0 Y N
N N N N N 0

0 N 0 1 0 1 N N N N N N N N N NATL \$

TABLE CUSTSTN

TUPLE NOT FOUND

TABLE OFCVAR

AIN_OFFICE_TRIGGRP NIL

INAP Origination Attempt TDP: no subscribed trigger.

TABLE NCOS

SERKAN 0 0 0 \$ (XLAS MEHTAP MEHTAP NDGT)\$

TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA,
VACTRMT,

AND DIGCOL

SERKAN NXLA NETXLA NXLA 0 NDGT

TABLE DIGCOL

NDGT specified: digits collected individually

INAP Info Collected TDP: no subscribed trigger.

TABLE IBNXLA: XLANAME MEHTAP

TUPLE NOT FOUND

Default from table XLANAME:

MEHTAP

(NET N Y 0 N NDGT N Y DOD N 2 102_NPRT_1 NLCA_NILLA_1
NONE \$) \$ 9

TABLE DIGCOL

NDGT specified: digits collected individually

TABLE LINEATTR

2 IBN NONE NT 0 0 NILSFC 4 PX MEHTAP NIL 00 102_NPRT_1
NLCA_NILLA_1 \$

LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE

TABLE XLAPLAN

102_NPRT_1 NSCR 102 NPRT NONE N \$ GG

TABLE RATEAREA

NLCA_NILLA_1 NLCA NIL NILLATA \$

TABLE PXHEAD

MEHTAP DFLT FEATINFO VALIDATE (SUBSCRN (GENERAL N N N
N)\$) (CLISERV

METERING)\$ 0 1 20 PX NETXLA NODFOP NOCON F

THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
3967835480

TABLE PXCODE

TUPLE NOT FOUND

DEFAULT FROM HEAD TABLE USED

PLEASE ENTER CLI DIGITS:

>1027835479

TABLE CLISERV

. METERING 1 (SERVSCRN)\$

TABLE DNSCRN

. 1027835479 (NETAOCD 30) (CLISERV 1) \$

TABLE CLISRVPF

. 1 (METERING \$)\$

. Matched on METERING

. Service screening succeeded

TABLE PXHEAD

NETXLA SDFLT NODFOP NOCON F

THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
3967835480

TABLE PXCODE

NETXLA 396 396 RTE (PF 3) (MM 9 15) (DEST 394) (CLASS NATL) (LNET LOC)

(MZONE 4)\$

TABLE: PXRTE

KEY: NETXLA 394

. S MFTUPBC

EXIT TABLE PXRTE

INAP Info Analyzed TDP: no subscribed trigger.

INAP Route Select Failure TDP: no subscribed trigger.

TABLE MTRMOG

MDI4 MOTS_2 \$

TABLE MTRLNET

LOC

TABLE MTRMOTS

MOTS_2 LOC 4 8

TABLE MTRNETIF

TUPLE NOT FOUND

TABLE MTRMOTS

MOTS_2 LOC 4 8

TABLE MTRNAMES

TUPLE NOT FOUND

TABLE TODHEAD

LOC MTR LOC 0 (NORMAL) (SATDAY) (SUNDAY) \$

TABLE DAYOYEAR

TUPLE NOT FOUND

TABLE DAYOWEEK

LOC WED NORMAL

TABLE TIMEODAY

TUPLE NOT FOUND

WARNING: TIMEODAY datafill missing

The default TNT in table TODHEAD will be used

TABLE MTRTTS

LOC 8 Y 53 \$ \$ \$ \$ \$ \$ \$ \$

TABLE MTRTARIF

53 SEC Y 0 1 0 12 1 15 0 1 0 16 1 15

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 MFTUPBC 7835480 ST

TREATMENT ROUTES. TREATMENT IS: GNCT

1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>traver tr mftupcb 7835480 tariff b

TABLE TRKGRP

MFTUPCB IBNT2 0 NPDGP NCRT SERKAN 0 LIDL 0 N ANSDISC 0 Y N
N N N N N 0

0 N 0 1 0

1 N N N N N N N N NATL \$

TABLE CUSTSTN

TUPLE NOT FOUND

TABLE OFCVAR

AIN_OFFICE_TRIGGRP NIL

INAP Origination Attempt TDP: no subscribed trigger.

TABLE NCOS

SERKAN 0 0 0 \$ (XLAS MEHTAP MEHTAP NDGT)\$

TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA,
VACTRMT,

AND DIGCOL

SERKAN NXLA NETXLA NXLA 0 NDGT

TABLE DIGCOL

NDGT specified: digits collected individually

INAP Info Collected TDP: no subscribed trigger.

TABLE IBNXLA: XLANAME MEHTAP

TUPLE NOT FOUND

Default from table XLANAME:

MEHTAP

(NET N Y 0 N NDGT N Y DOD N 2 102_NPRT_1 NLCA_NILLA_1
NONE \$) \$ 9

TABLE DIGCOL

NDGT specified: digits collected individually

TABLE LINEATTR

2 IBN NONE NT 0 0 NILSFC 4 PX MEHTAP NIL 00 102_NPRT_1
NLCA_NILLA_1 \$

LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE

TABLE XLAPLAN

102_NPRT_1 NSCR 102 NPRT NONE N \$ GG

TABLE RATEAREA

NLCA_NILLA_1 NLCA NIL NILLATA \$

TABLE PXHEAD

MEHTAP DFLT FEATINFO VALIDATE (SUBSCRN (GENERAL N N N
N)\$) (CLISERV

METERING)\$ 0 1 20 PX NETXLA NODFOP NOCON F

THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
7835480

TABLE PXCODE

TUPLE NOT FOUND

DEFAULT FROM HEAD TABLE USED

PLEASE ENTER CLI DIGITS:

>1027835479

TABLE CLISERV

. METERING 1 (SERVSCRN)\$

TABLE DNSCRN

. 1027835479 (NETAOCD 30) (CLISERV 1) \$

TABLE CLISRVPF

. 1 (METERING \$)\$

. Matched on METERING

. Service screening succeeded

TABLE PXHEAD

NETXLA SDFLT NODFOP NOCON F

THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
7835480

TABLE PXCODE

NETXLA 783 783 CONT (PF 3) (MM 7 7) (CLASS NATL) (XLT OFC
OFC783) (LNET

LOC) (MZONE 4)\$

TABLE OFCHEAD

OFC783 DFLT TRMT (OFC VACT)\$ NODFOP NOCON STD

THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 5480

TABLE OFCCODE

OFC783 5 5 RTE (DEST 1)\$

TABLE: OFCRTE

KEY: OFC783 1

. T OFRT 783

. . TABLE OFRT

. . 783 DN 102 783 4

. . . TABLE TOFCNAME

. . . 102 783 \$

. . . TABLE DNINV

. . . 102 783 5480 L HOST 03 0 00 10

TABLE DNFEAT

TUPLE NOT FOUND

. . . TABLE DNATTRS

. . . TUPLE NOT FOUND

. . . TABLE DNGRPS

. . . TUPLE NOT FOUND

. . EXIT TABLE OFRT

EXIT TABLE OFCRTE

INAP Info Analyzed TDP: no subscribed trigger.

INAP Route Select Failure TDP: no subscribed trigger.

INAP Termination Attempt TDP: no subscribed trigger.

TABLE MTRMOG

MDI4 MOTS_2 \$

TABLE MTRLNET

LOC

TABLE MTRMOTS

MOTS_2 LOC 4 8

TABLE MTRNETIF

TUPLE NOT FOUND

TABLE MTRMOTS

MOTS_2 LOC 4 8

TABLE MTRNAMES

TUPLE NOT FOUND

TABLE TODHEAD

LOC MTR LOC 0 (NORMAL) (SATDAY) (SUNDAY) \$

TABLE DAYOYEAR

TUPLE NOT FOUND

TABLE DAYOWEEK

LOC WED NORMAL

TABLE TIMEODAY

TUPLE NOT FOUND

WARNING: TIMEODAY datafill missing

The default TNT in table TODHEAD will be used

TABLE MTRTTS

LOC 8 Y 53 \$ \$ \$ \$ \$ \$ \$ \$

TABLE MTRTARIF

53 SEC Y 0 1 0 12 1 15 0 1 0 16 1 15

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 LINE

1027835480

ST

TREATMENT ROUTES. TREATMENT IS: GNCT

1 OFL

+++ TRAVER: SUCCESSFUL CALL TRACE +++

12.14 Appendix B - Example datafills for the case where metering tariff coincides/not coincides with the SSUTR2_ITX_RATE

It is recommended to use a metering tariff which does not coincide with the SSUTR2_ITX_RATE period for ITX generation.

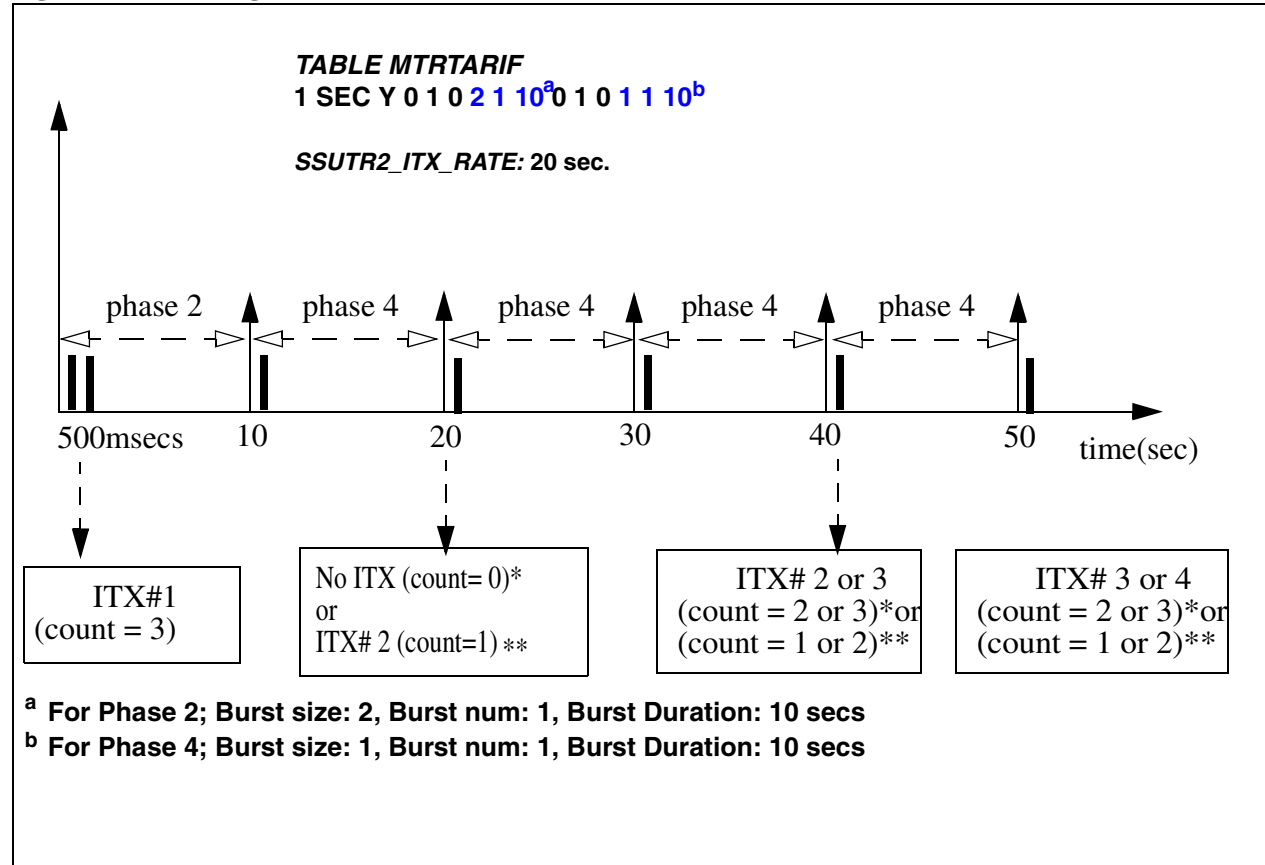
12.14.1 If metering tariff coincides with the SSUTR2_ITX_RATE

As an existing behavior, if the phase starting times of the tariff coincides with the ITX generation time (whose period is determined by the SSUTR2_ITX_RATE value), then it is not possible to determine the exact pulse count value to be sent within the ITX message. This is because metering is increased at the beginning of the phase and an ITX message which is generated at the phase starting time may include the pulses for the new phase and these pulses are sent with the next ITX message.

Therefore, the count in the ITX message (e.g. as seen in Figure 4) is not precise since the metering tariff coincides with the SSUTR2_ITX_RATE, that is why such usage is not recommended.

Below you can find an example MTRTARIF datafill and the relevant ITX generation diagram in Figure 4.

Figure 4 If metering tariff coincides with the SSUTR2_ITX_RATE

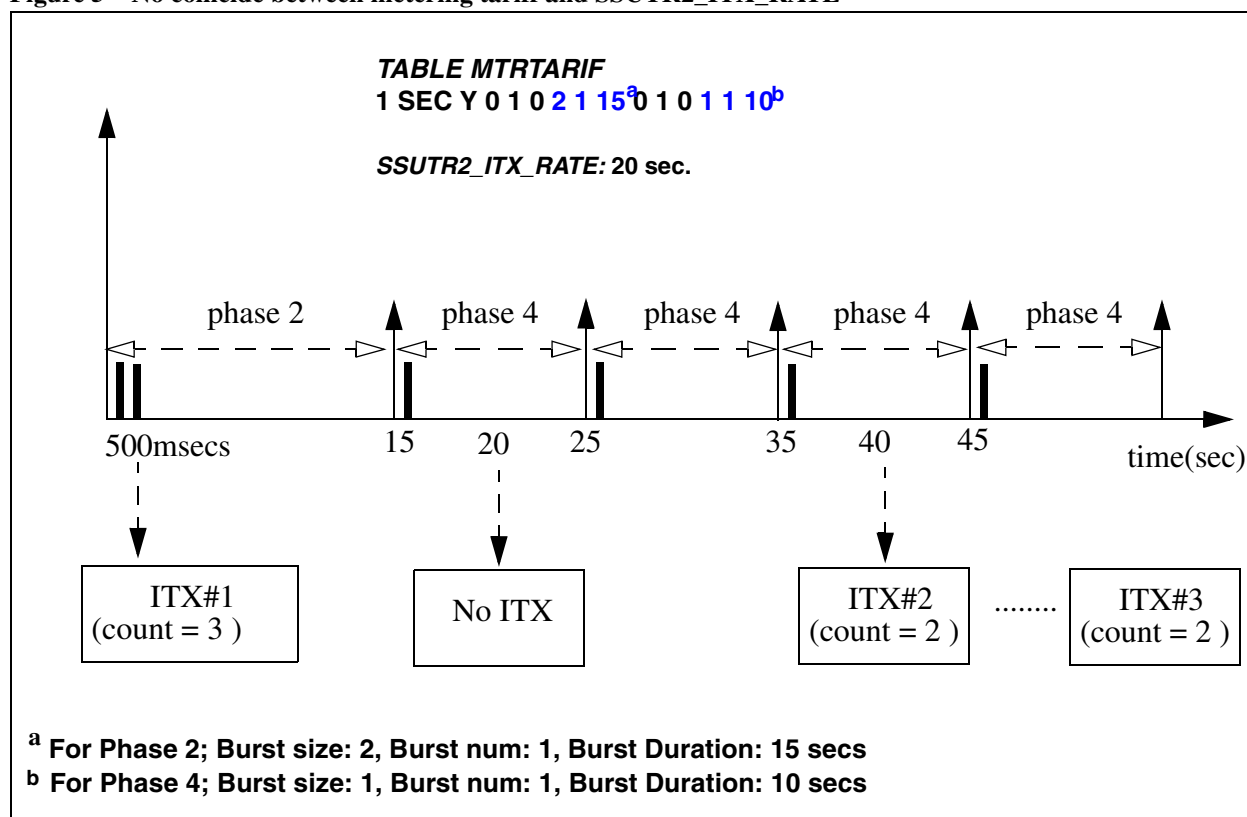


* If no ITX is generated at 20 sec, next ITX generated at 40 sec has the count 2 or 3.

**If ITX is generated with count 1 at 20 sec, next ITX generated at 40 sec has the count 1 or 2.

12.14.2 If metering tariff does not coincide with the SSUTR2_ITX_RATE

Figure 5 No coincide between metering tariff and SSUTR2_ITX_RATE



13: A00006660 Functional description (FN)

13.1 Feature name

DDRM Node Definition and Provisioning.

13.2 Description

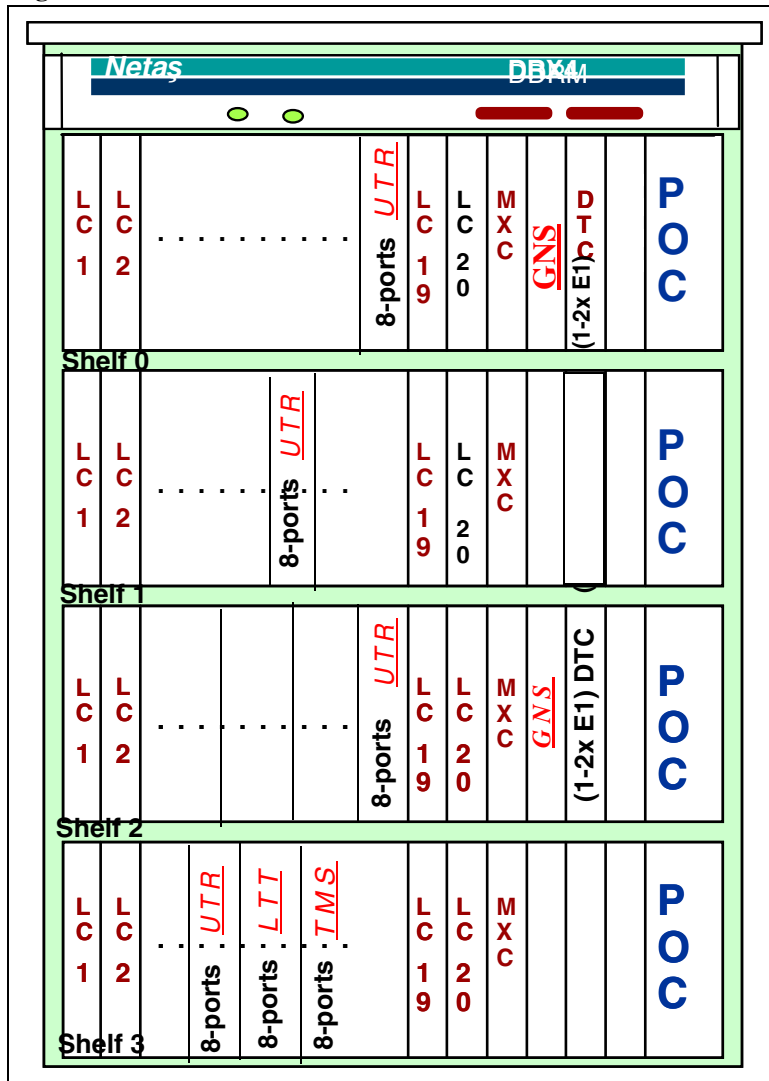
13.2.1 Introduction

DDRM (DMS Dicle Remote Module) project as a whole provides a platform which supports DDRM node as a remote line module of DMS. DDRM is connected to PLGC(SX05) via E1 links and upon successful deployment of this project it will be possible to maintain and administer DDRM related operations from DMS switches.

DDRM node is defined and provisioned in table LCMINV and this part of DDRM project implements the necessary changes for DDRM in table LCMINV.

13.2.2 DDRM Hardware Properties

Figure 1 DDRM hardware



DTC cards are E1 interface cards and support the C-side PCM30 links. DTC cards have 2 types; one can have 1 E1 link and the other can have 2 E1 links. There are 2 DTC cards per DDRM and hence the number of E1 links supported is between 2 and 4 and their locations are dedicated (cannot be placed in the line card slots).

MXC is capable of detecting on/off hooks and has call processing capabilities. There is 1 MXC per shelf and hence the number of MXCs implies the number of shelves and their locations are dedicated.

GNS provides the communication between the MXCs. There may be 1-2 GNSs per DDRM and are called single plane and double plane respectively. Double plane implies at least 2 shelves. Locations are again dedicated.

MTA is optional and consists of a pair of test cards - LTT (Line and Trunk Test Simulator) for loop terminations and TMS (Test Measurement and Signalling) for test. These cards are plugged into 2 line card slots (their locations are not dedicated but both must be on the same shelf) and occupy 16 ports (each line card slot provides 8 ports) per node.

UTR generates tones and receives tones. 1 UTR is enough for the whole DDRM but there may be more than 1 up to 4 each being plugged into line card slots and hence each occupying 8 ports.

POC is the power converter card and there is 1 POC card per shelf and their locations are dedicated.

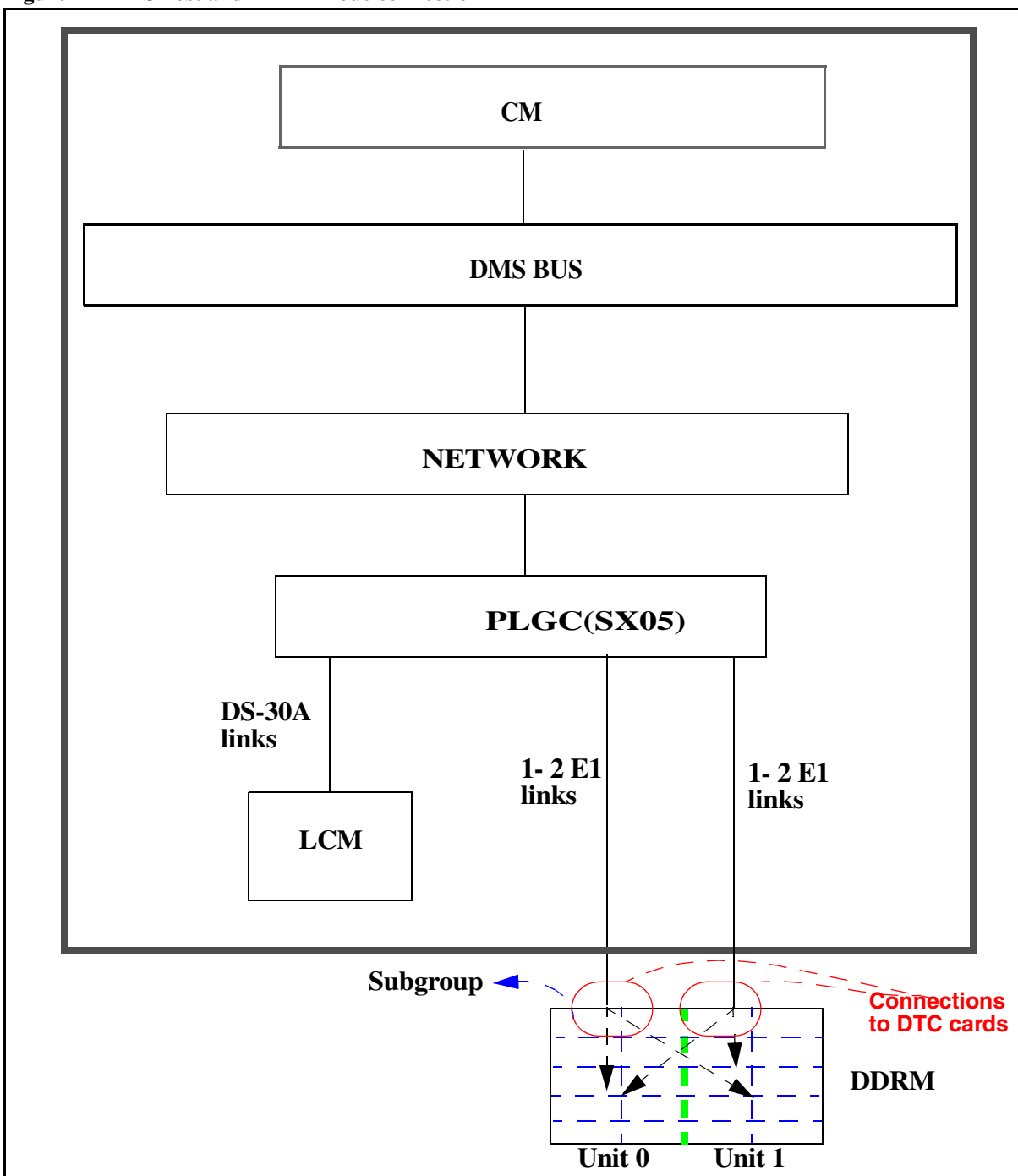
LC is the line card which provides 8 ports (lines). For more information on this please refer to A00006662 DDRM LINES INVENTORY FN.

MTA (consists of LTT and TMS) card set can be optional but UTR must be equipped for the ESA mode (A DDRM configuration without at least a UTR cannot be ESA enabled). If ESA will not be used, UTR is also optional. Also the shelf configuration is flexible, that is, between 1 and 4 shelves may be configured.

There are 20 line card slots per shelf and there are up to 4 shelves per cabinet. Each line card provides 8 ports (lines) and hence the maximum number of lines supported by DDRM is: 4 shelves x 20 line card slots x 8 ports = 640. If there are MTA card set and 4 UTRs then this number decreases to: 4 shelves x 16 (6 allocated for MTA card set and 4 UTRs) x 8 ports = 592. For more information on this please refer to A00006662 DDRM LINES INVENTORY FN.

13.2.3 DMS-DDRM Connection

Figure 2 DMS host and DDRM node connection



13.2.4 LCMINV Datafill for DDRM

In order to define DDRM, the steps explained in Table 1, “Steps For Defining DDRM,” on page 195 have to be performed.

Table 1 Steps For Defining DDRM

Table	Explanation
LTCINV	Existing logic is used. PLGC-host to which DDRM is connected is defined.
CARRMTC	Existing carrier logic for host PLGC is used.
LTCPSINV	Existing definitions and logic for host PLGC are used.
SITE	Existing logic is used. Site which the DDRM is situated is defined.
LCMINV	Existing logic is used with modifications and additions for DDRM. Current configuration of DDRM is defined.

No changes exist and existing datafill logic is used in tables LTCINV, CARRMTC, LTCPSINV and SITE.

A sample datafill for table CARRMTC is shown in Please refer to “Figure 3 Sample datafill for table CARRMTC” on page 195..

Figure 3 Sample datafill for table CARRMTC

PLGC DEFAULT 255 255 D30 NT6X27BB A_LAW NATL 30 30 4 20 30 30 4 20 30 30 4 20 30 30 4 20 30 30 4 20 4 20 4 20 Y 4 4 17 255 N N 5 5 205 914 G714 CASX

The changes in table LCMINV are shown in Please refer to “Figure 4 Changes in Table LCMINV Range for DDRM” on page 196.

Figure 4 Changes in Table LCMINV Range for DDRM

TABLE: LCMINV	
>ran	
1 LCMNM	LINE_MODULE_KEY
2 <i>FRTYPE</i>	FRAME_NAME
3 SHPOS	SHELF_POS
4 FLOOR	FLOOR_POS
5 ROW	ROW_POS
6 FRPOS	FRAME_POS
7 <i>EQPEC</i>	LCM_PEC
8 <i>LOAD</i>	NPMLOAD_INFO
9 <i>CSPMNO</i>	TPM_NAME
10 <i>BICTST</i>	BOOL
11 ADNUM	ADMIN_NUMBER
12 <i>MEMSIZE</i>	MEMSIZETAB
13 <i>LCMTYPE</i>	LCMTYPE_INFO
LOGICAL TUPLE TYPE: LCM_LOGTUPLE	
>	

The datafill guide for DDRM is shown in Table 2, “Datafill Guide for DDRM in Table LCMINV,” on page 196.

Table 2 Datafill Guide for DDRM in Table LCMINV

Field	Explanation
LCMNM	No change. Existing logic is used.
FRTYPE	FRAME_NAME range now includes “DDRM”. “DDRM” should be datafilled.
SHPOS	No change. Existing logic is used.
FLOOR	No change. Existing logic is used.
ROW	No change. Existing logic is used.
FRPOS	No change. Existing logic is used.
EQPEC	LCM_PEC range now includes “DDRMPC”. “DDRMPC” should be datafilled.
LOAD	No change. It will not be verified whether the load file exists in table PMLOADS or not. DRM21AA should be datafilled.
CSPMNO	No change. PLGC should be datafilled.

Table 2 Datafill Guide for DDRM in Table LCMINV

Field	Explanation
BICTST	No change. N needs to be datafilled as DDRM does not support BICTST otherwise an existing error message for LCMINV is generated which indicates that 'BIC Relay test only valid for XLCM and STAR HUB, LCMTYPE must be LCM or UREM'.
ADNUM	No change. Existing logic is used.
MEMSIZE	No change. 256K 256K should be datafilled for both units like RLCM.
LCMTYPE	• LCMTYPESEL This range now includes "DDRM". "DDRM" should be datafilled. • RGEQUIP Datafilled similar to RLCM. • LINKMAP Between 2-4 links is datafilled. • ESA Indicates whether ESA is allowed or not. Possible values: N, Y

Table 2 Datafill Guide for DDRM in Table LCMINV

Field	Explanation
	• GNS Indicates whether the DDRM is single plane or double plane. Possible values: SINGLE, DOUBLE • MXC_CONFIG Indicates which shelves have MXC cards in the format of SHELF0 SHELF1 SHELF2 SHELF3. Possible values: N,Y Example: Y Y N N means Shelves 0 and 1 have MXC cards. • UTR_CONFIG Indicates which shelves and which slots have UTR cards in the format of SHELF0 SHELF1 SHELF2 SHELF3. Possible values: UTRD0, UTRD1,...,UTRD18, UTRD19, N Example: UTRD3 UTRD5 N N means SHELF0 has UTR on 3rd slot and SHELF1 has UTR on 5th slot. Note that it is called UTRD in order to distinguish it from the DMS UTR. • MTA_AVAILABLE Indicates whether LTT-TMS cards are configured. Possible values: N, Y • If MTA_AVAILABLE is datafilled as Y • LTT-TMS Indicates which shelf and which slots have LTT-TMS cards in the format of SHELF_NUMBER LTT_SLOT TMS_SLOT. Possible values: SHELF0, SHELF1, SHELF2, SHELF3 Possible values: LTT0,..., LTT19 Possible values: TMS0, ..., TMS19

Verification messages which prevent datafill are shown in Table 3, “Verification Messages(errors) for DDRM Datafill in Table LCMINV,” on page 199.

Table 3 Verification Messages(errors) for DDRM Datafill in Table LCMINV

Field	Explanation
FRTYPE	If another value other than “DDRM” is datafilled: “Invalid FRTYPE...DDRM only.”
EQPEC	If another value other than “DDRMPC” is datafilled: “Invalid PEC...DDRMPC only.”
LOAD	No check is applied for this field but it must reflect the DDRM load.
CSPMNO	If another value other than PLGC is datafilled: “DDRM allowed off PLGC only.”

Table 3 Verification Messages(errors) for DDRM Datafill in Table LCMINV

Field	Explanation
LCMTYPE	• LINKMAP If the number of links datafilled is not between 2 and 4: “Number of links must be between 2 and 4.” • GNS, MXC_CONFIG, UTR_CONFIG, LTT_TMS, ESA If GNS is double plane and only 1 shelf is datafilled: “There must be at least 2 shelves.” If ESA is enabled and no UTR is datafilled: “To activate ESA there must be at least 1 UTR.” If UTR is datafilled on a non-datafilled shelf: “UTR cannot be datafilled on a nonexistent shelf.” If UTR is datafilled on a non-empty slot: “UTR should be datafilled on an empty slot.”

Table 3 Verification Messages(errors) for DDRM Datafill in Table LCMINV

Field	Explanation
	If LTT-TMS is datafilled on a non-datafilled shelf: “LTT-TMS cannot be datafilled on a nonexistent shelf.” If LTT-TMS is datafilled on a non-empty slot: “LTT-TMS should be datafilled on an empty slot.” If LTT and TMS is datafilled on the same slot: “LTT and TMS cannot be on the same slot.” If MXC_CONFIG is datafilled as N N N N: “There must be at least one MXC.” If a MXC is set to N while there are lines datafilled on the corresponding shelf: “There are lines datafilled on the shelf.”

Verification messages which does not prevent datafill are shown in Table 4, “Verification Messages (warnings) for DDRM Datafill in Table LCMINV,” on page 201.

Table 4 Verification Messages (warnings) for DDRM Datafill in Table LCMINV

Field	Explanation
MEMSIZE	If another value other than 256K 256K is datafilled: “Warning: Memory size for both units are 256K by default.”
LCMTYPE	If GNS, MXC, UTR, ESA or MTA configuration is changed: “Warning: Static data should be sent to DDRM. Please BUSY and RTS the node.”

Existing dynamic update process is also valid for DDRM. This does not however include card configuration and ESA field change. Card configuration and ESA field change is allowed but related information is not sent to DDRM via dynamic update process and it requires a manual action.

A sample datafill in action is shown in Table 5, “Adding DDRM in Table LCMINV,” on page 203.

The final look for a sample datafill is shown in Table 5, “LCMINV Sample Datafill for DDRM,” on page 205.

Table 5 Adding DDRM in Table LCMINV

```
>TABLE LCMINV
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LCMINV
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
LCMNM:
>REMO 00 0
FRTYPE:
>DDRM
SHPOS:
>0
FLOOR:
>0
ROW:
>A
FRPOS:
>0
EQPEC:
>DDRMPC
LOAD:
>DRM21AA
CSPMNO:
>PLGC 0
BICTST:
>N
ADNUM:
>55
MEMSIZE:
>256K 256K
```


Table 5 Adding DDRM in Table LCMINV

```

LCMYPESEL:
>DDRM
RGEQUIP:
>Y
RNGTYPE:
>C
LINKMAP:
>0
LINKMAP:
>2
LINKMAP:
>$
ESA:
>Y
GNS:
>DOUBLE
MXC_CONFIG:
>Y Y N N
UTR_CONFIG:
>UTRD1 UTRD2 N N
MTA_AVAILABLE:
>Y
LTT_TMS:
>SHELF0 LTT3 TMS4
TUPLE TO BE ADDED:
REMO 00 0 DDRM 0 0 A 0 DDRMPC DDRMLD PLGC 0 N 55 256K 256K DDRM
Y C (0) (2)
$Y DOUBLE Y Y N N UTRD1 UTRD2 N N Y SHELF0 LTT3 TMS4

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y

```

Figure 5 LCMINV Sample Datafill for DDRM

TABLE LCMINV									
LCMNM	FRTYPE	SHPOS	FLOOR	ROW	FRPOS	EQPEC	LOAD		
CSPMNO									
BICTST	ADNUM	MEMSIZE							
LCMTYPE									

REMO 00 0	DDRM 0	0	A	2	DDRMPC	DDRMLD	PLGC	0	
N	7	256K	256K						

13.3 Hardware Requirements or Dependencies

N/A.

13.4 Software Requirements or Dependencies

N/A.

13.5 Limitations and restrictions

N/A.

13.6 Interactions

N/A.

13.7 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)_____

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.

13.8 Glossary

Table 6

Term	Description
DDRM	DMS Dicle Remote Module
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
UTR	Universal Tone Receiver

13.9 References

- a. A00006638 DMS - DDRM HLD
- b. DMS_DDRM Spec.

14: A00006661 Functional description (FN)

14.1 Feature name

DDRM Node Maintenance

14.2 Description

DRX-4 (Dicle Rural Exchange-4) is a rural area exchange developed for the Turkey Market. The DDRM (DMS Dicle Remote Module) project, as a whole, provides a platform which supports the DDRM as a remote module of DMS. DDRM is deployment to maintain and administer DDRM related operations over DMS switches via E1 links over SX05 PLGC. In this way, the benefits of the DDRM in the Turkey market will be enhanced and the demands from the customer to reuse these switches as remote modules will be satisfied.

This activity provides DDRM **static data downloading, maintenance, and Human Machine Interface supports**. This activity also eliminates the unnecessary maintenance requests for DDRM.

- **STATIC DATA DOWNLOADING**

The main aim of a Static data system is to publish the configuration information and other related data from CM to XPM. Static Data declares the functionality of XPM hardware and software, such as node type and number, P-side nodes, terminals, option cards, application options etc.

But there are differences compared to the LCM. The DDRM needs card configuration, Line card codes, some of the office parameters (flash, ringing cadence) and ESA SD, translation tables, line Inventory information and System Time &Date. All of these are delivered by messages destined for DDRM through the host PLGC.

- **MAINTENANCE**

The execution of maintenance commands that are seen in user interface. For instance, BSY, RTS, and TST, commands are implemented in this area. The commands are generally unseen by the customer.

- **HUMAN MACHINE INTERFACE**

HMI provides a user interface platform for the craft person. The DDRM can be maintained from this level. The following figure gives a HMI view of the DDRM:

14.3.2 Human Machine Interface

Because of DDRM's capability, some commands are not available to it. In the example, DDRM cannot be remotely loaded with a new load. This is because DDRM can only be loaded by EPROM chips. Hence, the **Loadpm** command cannot be processed by DDRM. Similarly, DDRM architecture is not suitable for the **SwRg**, **SwLd**, and **RgStbit** commands.

Commands are also separated into two parts as DMS-X requires or not. The following table shows the commands for the standard LCM. Bold entries do not require any DMS-X messages; plain entries send the necessary DMS-X messages to DDRM and wait for a response; strikethroughs are out of the scope of DDRM; and italics are non-menu commands.

Table 1 Command classification for DDRM¹

No	LCM
0	Quit
2	Post_
3	ListSet
4	~~SwRg_~~
5	Trnsl_
6	Tst_
7	Bsy_
8	RTS_
9	OffL_
10	~~LoadPM_~~
11	Disp_
12	Next
13	~~SwLd_~~
14	QueryPM
15	~~RgStbit~~
16	<i>ABTK</i>

14.3.3 Validated PM states for DMS

Following PM states in "Table 2: PM maintenance states" will be valid for DDRM PM type as well.

During unexpected cases (card failures, alarms) the DDRM state can be set to ISTB or SYSB by the DDRM maintenance structure. "Table3: DDRM pm state regarding the card alarms" shows the Card alarm related actions on the DDRM state.

¹For detailed information about commands, please refer to CN section of this document.

Table 2 PM maintenance states

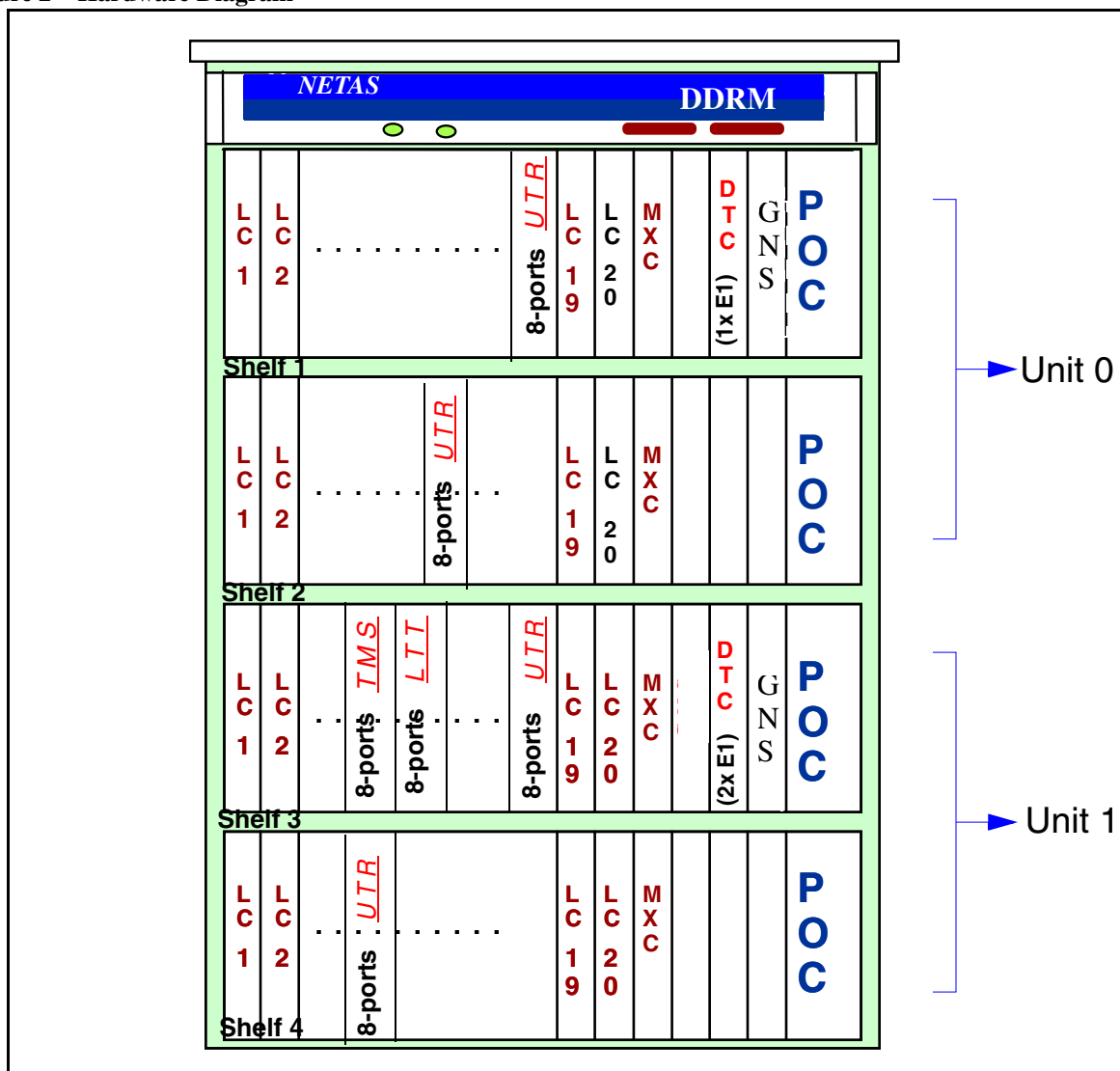
Code	Line state	Description
CBsy	Central side busy	The PM cannot communicate with the CM. The E1 links used to carry messages between PM and the DMS-100 switch are not available.
InSv	In service	The PM is free of service-affecting faults and can support any intended process, such as call processing.
ISTB	In-service trouble	The PM is in service (Insv).The PM has a minor fault.
ManB	Manual busy	The PM is busy. The switch operator issued Busy/BSY command from the MAP position.
Offl	Offline	The switch operator removed the PM from service to allow commissioning testing.The switch operator performed this procedure to hold the PM out of service (OOS) temporarily.
SysB	System busy	The system maintenance removed the PM from service as a result of faults.

Table 3 DDRM pm state regarding the card alarms

Card problems causing alarm message on DDRM	Alarm severity	DDRM State
Last GNS Card (single and double plane)	Critical	SYSB
One GNS Card (double plane)	Major	ISTB
MXC card (except the last MXC)	Major	ISTB
Last MXC card	Critical	SYSB
UTR card (except the last UTR)	Minor	ISTB
Last UTR card	Critical	ISTB
LTT - TMS card	Major	ISTB
POC card (except the standby)	Major	ISTB
Standby POC card	Major	ISTB
	Critical	SYSB
Ring generator on one POC card	Major	ISTB
Ring generator on one POC card	Major	ISTB
Ring generator on standby POC card	Major	ISTB
	Critical	SYSB

14.4 Hardware Requirements or Dependencies

Figure 2 Hardware Diagram



DTC cards are E1 interface cards and support the C-side PCM30 links. DTC cards can be of 2 types: one can have 1 E1 link and the other can have 2 E1 links. There are 2 DTC cards per DDRM and hence the number of E1 links supported is between 2 and 4 and their locations are dedicated (they cannot be placed in the line card slots).

MXC is capable of detecting on/off hooks and it transmits to the GNS in the same shelf. There is 1 MXC per shelf and hence the number of Midsts denotes the number of shelves and their locations are dedicated.

GNS provides the communication between the shelves. There may be 1 or 2 GNSs per DDRM. They are called single plane and double plane respectively. Double plane implies at least 2 shelves. Locations are again dedicated.

MTA (not shown above) is optional and consists of a pair of test cards (LTT for loop terminations and TMS for test). These cards are plugged into 2 line card slots (their locations are not dedicated) and occupy 16 ports (each line card slot provides 8 ports) per node.

UTR (not shown above) generates tones and receives tones in ESA mode. 1 UTR is enough for the whole DDRM but there may be more than 1. Up to 4 can be used, each being plugged into line card slots and each occupying 8 ports.

LTT - TMS LTT (Line and Trunk Test Simulator) and TMS (Test Measurement and Signalling) cards are used to ensure MTA test facilities for DDRM subscribers. LTT and TMS cards use 16 ports on any LC slot and the slots are not dedicated for them. These cards can be positioned in any shelf and in any LC slot. There is no obligation to replace these cards adjacent to each other. But both of them should be replaced in the same shelf.

POC is the power converter card and there is 1 POC card per shelf, their locations are dedicated. It also works as a Ring Generator.

LC is the line card which provides 8 ports (lines) and supports different LC card types (5 new line cards are defined with A00006662).

MTA (consists of LTT and TMS) card set can be optional but UTR must be equipped for the ESA mode.

For supported lines, please refer to FN document A00006662 “DDRM LINES INVENTORY”.

14.5 Software Requirements or Dependencies

This Feature depends on another activity which is implemented for DDRM: ACT.A00006660 “DDRM NODE DEFINITION AND PROVISIONING”.

14.6 Limitations and restrictions

DDRM is not a standard LCM. It is a new, remote peripheral and no limitations/ restriction are being introduced on the existing RLCM variant in the LCM family by this feature. However, DDRM cannot accommodate all of the specification of the existing RLCMs.

14.7 Interactions

Some interactions be possible for providing infrastructure for following two projects

- DDRM ALARMS AND AUDITS fmdoc.A00006663
- DDRM ESA SUPPORT fmdoc.A00006665

14.8 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)_____

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.

14.9 Glossary

Table 4

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

Table 4

Term	Description
MXC	Module Switching Controller
POC	Power Converter Card
RLCM	Remote Line Concentrating Module
TMS	Test Measurement and Signalling
HMI	Human Machine Interface
UTR	Universal Tone Receiver Cards

14.10 Recommended Reading/References

- a. A00006638 DMS - DDRM HLD
- b. DMS_DDRM
- c. A00006660 DDRM NODE DEFINITION AND PROVISIONING
- d. A00006662 DDRM LINES INVENTORY
- e. A00006663 DDRM ALARMS AND AUDITS
- f. A00006664 DDRM LINE TESTING
- g. A00006665 DDRM ESA SUPPORT
- h. A00006666 DDRM XPM SUPPORT AND MONITORING

15: A00006662 Functional description (FN)

15.1 Feature name

DDRM Line Definition and Line Maintenance

The DDRM (DMS Dicle Remote Module) project, as a whole, provides a platform which supports the DDRM node as a remote line module of DMS like a Remote Line Concentrating Module (RLCM).

A00006662 is responsible for handling the line provisioning and maintenance actions of the DDRM Remote Module on a regular MMP switch for ISN08 stream.

***Note:** As the whole DDRM project has been divided into two phases, some of the activities have been churned out from ISN08 and they will be implemented in ISN09, including A00006664, DDRM Line Tests.*

Some parts of this activity, A00006662, have interactions with activity A00006664. Affected parts are highlighted and detailed in red fonts throughout this document.

15.2 Description

15.2.1 Background Information

15.2.1.1 DDRM Node Configuration

DDRM is a new, remote peripheral connected to a MMP Switch via a host XPM peripheral (PLGC) through a maximum of 4 E1(PCM30) links.

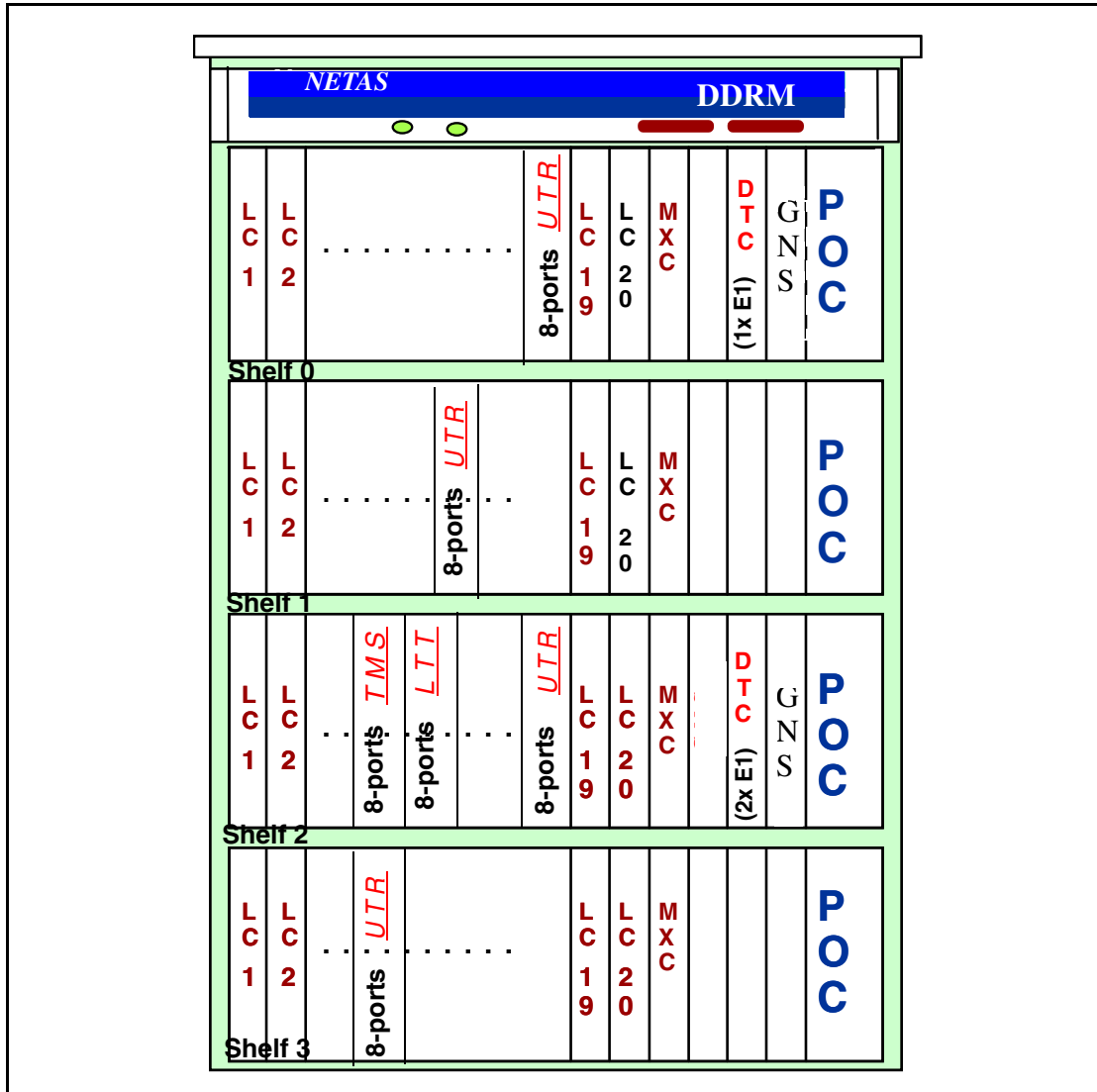
DDRM is based on a MMP RLCM which is developed for the Turkey Market. The purpose of the whole project is to enhance the benefits of the DDRM Rural Switches and to provide RLCM Node facility to the DDRM Rural exchanges in the Turkey Market. Thus maintenance and administration related operations are processed on DMS exchanges.

The DDRM module is configured as a one cabinet DDRM Local Switch, each of which consists of 4 shelves.*

***Note:** * The configuration with 4 shelves is not fixed and DDRM nodes with less than 4 shelves are available in the Turkey Market.*

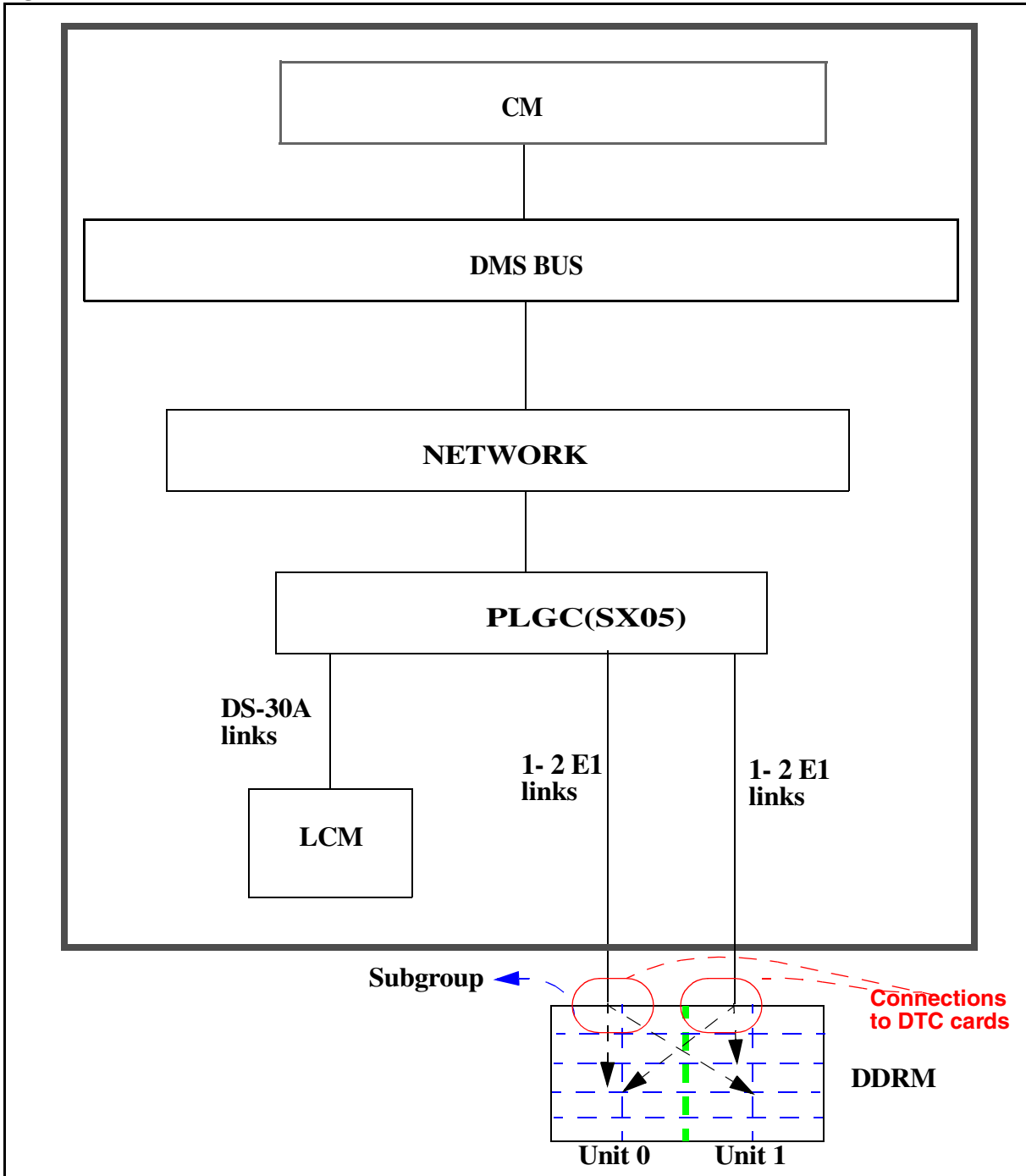
A DDRM node with a 4-shelf card configuration is as follows:

Figure 1 DDRM Hardware



The DDRM is connected to the PLGC with E1 links (between 2 and 4) and communicates via the DMS-X protocol. E1 link connections are provided by the DTC cards of DDRM. The connection is shown below:

Figure 2 DMS host and DDRM node connection



15.2.1.2 DDRM Line Configuration

Figure 3 RLCM configuration on DMS

Drwr 5	Drwr 6	Drwr 7	Drwr 8	Drwr 9	Unit 1
Subgrp11	Subgrp13	Subgrp15	Subgrp17	Subgrp19	
Subgrp10	Subgrp12	Subgrp14	Subgrp16	Subgrp18	
Drwr 0	Drwr 1	Drwr 2	Drwr 3	Drwr 4	Unit 0
Subgrp01	Subgrp03	Subgrp05	Subgrp07	Subgrp09	
Subgrp00	Subgrp02	Subgrp04	Subgrp06	Subgrp08	

According to the DDRM Configuration given in section 1.3.1.1, DDRM shelves must be mapped to a logical view of the RLCM Drawer configuration regarding 64 lines per drawer. This is because of the mismatch between the Shelf-based DDRM architecture and the Drawer-based RLCM architecture.

The architecture of the RLCM (shown above in Figure 3) is valid for the DDRM as well. The view of DMS line drawers are seen in order on the DDRM node starting from shelf 0 and ending with shelf 3.

Figure 4 DDRM Shelf -> RLCM Drawer Mapping:

	1. LC Slot	20.LC Slot		Drwr subgrp
Unit 0		Shelf 1	←	00,01,02,03,04
		Shelf 2	←	05,06,07,08,09
Unit 1		Shelf 3	←	10,11,12,13,14
		Shelf 4	←	15,16,17,18,19

The drawers 0, 1, 2, 3 and 4 are presented by shelf 1 and shelf 2 of the DDRM node. This means that:

-
- i. the lines on subgroups 00, 01, 02, 03 and 04 correspond to the lines on shelf 1 of the DDRM.
 - ii. the lines on subgroups 05, 06, 07, 08 and 09 correspond to the lines on shelf 2 of the DDRM.

The drawers 5, 6, 7, 8 and 9 are represented by shelf 3 and shelf 4 of the DDRM. This means that:

- iii. the lines on subgroups 10, 11, 12, 13 and 14 correspond to the lines on shelf 3 of the DDRM.
- iv. the lines on subgroups 15, 16, 17, 18 and 19 correspond to the lines on shelf 4 of the DDRM.

Note: Logical mapping of the shelf-based DDRM architecture to the drawer-based DMS architecture will be done on the DDRM side internally. The DMS recognizes the DDRM as it has really a drawer-based architecture. All of the DMS-X messages will be sent and got in this form. (Please refer to the DMS_DDRM architecture or the DDRM HLD.)

The supported number of subscribers is based on the DDRM Configuration.

The supported number of subscribers on the DDRM node are differentiated based on the shelf number, and the existence of UTR and/or LTT-TMS cards in the TT network.

The maximum shelf number on a DDRM cabinet is 4 and each shelf has 20 LC slots.

Thus the supported subscriber numbers of a DDRM node is 640 $((20 \times 8) \times 4)$.

UTR configuration - one LC slot on each shelf is generally used for a UTR card and each shelf supports 152 subscribers. So 608 subscribers are supported for 4 shelves. But it is possible that one UTR card can serve all subscribers of a DDRM node. In that case 8 more subscribers can be defined for a shelf.

UTR & LTT-TMS configuration - besides UTR cards on each shelf, if a pair of LTT-TMS cards is placed into 2 LC slots for the MTA facility the supported number of subscribers is decreased with 16 subscribers less. In the configuration with 4 shelves, the maximum number of supported subscribers is 592.

For one shelf:

- no UTR and no LTT-TMS: 160 subscribers
- no UTR only LTT-TMS: 144 subscribers
- UTR and no LTT-TMS: 152 subscribers

- UTR and LTT-TMS: 136 subscribers

For 4 shelves (one cabinet):

- no UTR and no LTT-TMS: 640 subscribers
- 4 UTR and no LTT-TMS: 608 subscribers
- 4 UTR and LTT-TMS: 592 subscribers
- no UTR only LTT-TMS: 624 subscribers
- 1 UTR and no LTT - TMS: 632 subscribers
- 1 UTR and LTT - TMS: 616 subscribers

There are frames with 2 and 3 shelves in the Turkey Market and supported number of subscribers are calculated based on the above formula.

15.2.2 Feature Synopsis

With the A00006662 activity, DDRM line provisioning and line maintenance actions on DMS site are provided. The feature includes:

- Support for new DDRM line cards
- Line provisioning
 - Line Provisioning in Table LNINV
 - Coin Line Provisioning
 - CI Tool for DDRM LEN mapping
- Table controls specific to the DDRM node
- Line maintenance actions and Line diagnostics:
 - Only the maintenance commands POST, BSY, RTS, FRLS and DIAG are in the scope of this activity whereas line tests will be handled by the activity “A00006664 - DDRM Line Testing”.
- Line Audits
- Static data handling of line cards needed by the DDRM node

15.2.3 Feature Description

The DDRM node only uses Standard IBN and Coin lines. Thus support is needed for these cards which can be grouped with the facilities below:

- Basic LCs
- Basic LCs with the Over-voltage Option
- Basic Testable LCs with the Over-voltage Option
- Basic Metering LCs
- Basic Metering Testable LCs with the Over-voltage Option

Table 1 DDRM Line Card Properties

	Testable	Metering	Over voltage
Basic LC			
Basic LC with Over-voltage			+
Basic Testable LCs with Over-voltage	+		+
Basic Metering LC		+	
Basic Metering Testable LCs with Over-voltage	+	+	+

According to this information and the background information about the DDRM node and the DDRM line configurations in section 1.3.1, expected behaviors for DDRM lines are detailed in the sections below.

15.2.4 Behavior Scenarios described

15.2.4.1 Line Provisioning Scenarios

Line provisioning is done in table LNINV for the DDRM lines by using node number, unit number, drawer number and circuit number, as it is done for RLCM.

The Table LNINV format is given below:

Figure 5 Table LNINV

```

TABLE: LNINV
>ran
1 LEN LNINV_KEY
2 CARDCODE AVAILABLE_LINE_CARDS_INDEX
3 PADGRP PAD_GROUP
4 STATUS CARD_STATE
5 GND BOOL
6 BNV BALANCED_NETWORK_VALUE
7 MNO BOOL
8 CARDINFO CARDINFO_TYPE
LOGICAL TUPLE TYPE:LNINV_LOG_TUPLE
>

```

The bold fields are the data that specifies the DDRM lines. Here is a brief explanation about these fields:

LEN: defines the physical location of the equipment that is connected to a specific telephone line.

Subfields of field LEN are: SITE, FRAME, LCM NUMBER, DRAWER, CIRCUIT.

Note: SITE information is taken according to the node definition made on table LCMINV. Please refer to software dependencies in section 1.5.

CARDCODE: Cardcodes will be one of the defined line card codes of a DDRM node. The following card codes will be used for DDRM line cards:

- DRBLCN---> Basic LC
- DRBLCP ---> Basic LC with Over-voltage Option
- DRDLCP ---> Basic Testable LC with Over-voltage Option
- DRMLCN ---> Basic Metering LC
- DRMLCP ---> Basic Metering Testable with Over-voltage Option

All fields of table LNINV, their explanation and valid entries for DDRM lines are shown in the table below:

Table 2 Field Descriptions of Table LNINV

Field	Entry	Explanation and Action
LEN	SITE, FRAME and LCM NUMBER information will be taken according to the node definition made on table LCMINV. For example if DDRM 01 0 is used in table LCMINV then DDRM 01 0 must be used in table LNINV. EX: DDRM 01 0 0 1	Line equipment number This field defines the physical location of the equipment that is connected to a specific telephone line. Field LEN consists of subfields SITE, FRAME, LCM NUMBER, LSG and CIRCUIT. (No change from existing RLCM logic)

Table 2 Field Descriptions of Table LNINV

Field	Entry	Explanation and Action
CARDCODE	One of the line cards of the DDRM can be used. DRBLCN DRBLCP DRDLCP DRMLCN DRMLCP	Card code Enter the product engineering code (PEC) of the line card. (No change from existing logic).
PADGRP	No change. One of the pre-defined values from table PADDATA can be used.	Pad group Enter the name of the pad group that is assigned to the line circuit in table PADDATA. Field PADGRP contains the name of the pad group in table PADDATA that lists the value of the pad circuits that can be switched into the line when the line is involved in a call. Different values for the pad circuits can be specified when the circuit connects to an agent with a different pad group.
STATUS	No change. One of the below values can be used: CUTOFF, HASU (hardware assigned/ software unassigned), RESERVED, UNEQUIP (unequipped), or WORKING	Line inventory availability status. Enter the line inventory availability status.
GND	DDRM lines do not support ground start mode. N	Ground If the line is ground start, enter Y (yes). If the line is loop start, enter N (no).
BNV	DDRM lines do not support Balance Network tests. NL	Balanced network value Enter L if the line circuit is configured for a loaded network. Enter NL for a non-loaded network.

Table 2 Field Descriptions of Table LNINV

Field	Entry	Explanation and Action
MNO	Manual Override is not allowed for DDRM lines as Balance Network Test is not supported. N	Manual override Enter Y if the on-hook balance network test is to be prevented from updating field BNV in table LNINV. Enter N to allow the off-hook balance network test to update field BNV.
CARDINFO	Default value will be used for DDRM lines. NIL	Card information

According to this explanation, the DDRM LEN definition in table LNINV will be as follows:

LEN CARDCODE PADGRP STATUS GND BNV MNO CARDINFO

DDRM 01 0 06 17 DRBLCN STDLN WORKING N NL N NIL

As usage of some values for some fields in table LNINV is restricted, verification messages about LNINV datafill will be used. They can be seen in the table below:

Table 3 Verification Messages for DDRM Line Datafill in table LNINV.

Field	Explanation
CARDCODE	Only DDRM line cards: DRBLCN, DRMLCN, DRBLCP, DRDLCP, DRMLCP can be assigned to a DDRM line
GND	Ground Start is not allowed for a DDRM line
BNV	Balance Network Value is not allowed for a DDRM line
MNO	Manual Override is not allowed for a DDRM line
CARDINFO	No card info is allowed for a DDRM line

Note: As it is the existing behavior for RLCM, a hardware configuration check will not be done in the datafill step to LNINV. Datafill can be done regardless of the hardware check. A hardware mismatch can only be understood when the LC config alarm is sent to DMS during RTS(RTS Drwr) and Test step (Tst Drwr). (Please refer to A00006663: “DDRM Alarms and Audits activity for LC config alarm”. And refer to A00006660:

“DDRM node maintenance activity for handling LC mismatch message in RTS step”.)

15.2.4.1.1 Coin Line Provisioning

There is a hardware restriction about coin lines of a DDRM node which is:

Total COIN Line number per shelf cannot exceed the 10% of total line number in shelf. (10% x 160 lines = 16 MAX coin per shelf)

This restriction will be provided by counting the coin card codes used in table LNINV. After a maximum count is reached for one shelf (2 coin cards per shelf), no more usage of the coin LC will be allowed in this shelf. A warning will be prompted then.

“No more coin card codes can be used for this shelf”

15.2.4.1.2 Command Interface (CI) Tool for DDRM Lines

A CI tool (named DDRMLLEN) is provided for DDRM lines that map the Shelf information of a line to Drawer information. This is needed because calculating the drawer information of a shelf is already difficult for a craft person.

Mapping will be done in both directions: shelf,lc,slot <-> LSG(logical drawer),circuit. To map shelf,lc,slot -> LSG, circuit SL option will be used and to map LSG, circuit -> shelf,lc,slot LS option will be used.

Here below the CI tool's format is given mainly:

```
>help ddrmlen
DDRM line SHELF <-> DRAWER Mapping Tool.
Parms: <Option> {SL [<Shelf> {0 TO 3}]
                 [<LC> {0 TO 19}]
                 [<Slot> {0 TO 7}],
                 LS [<LSG> {0 TO 19}]
                 [<Circuit> {0 TO 31}]}
```

```
> ddrmlen sl 0 1 7
> DMS: Line Subgroup = 0, Circuit = 15

>ddrmlen ls 0 15
>DDRM: Shelf= 0, LC=1, Slot=7
```

Details of the CI tool can be seen in the Configuration Section of this document.

15.2.4.2 Table Control Scenarios

Changes are needed in the table control procedures of LNINV in order to support DDRM.

New controls are stated below:

- One of the card codes of the DDRM must be used for the DDRM node.
(CardCode <-> DDRM PM Type)
- If there is an attempt to define a line into a LC slot of the DDRM that does not have a line card but UTR and/or LTT-TMS, a failure prompt on the DMS MAP is given:
“UTR/LTT/TMS has already defined for this slot in table LCMINV”
- For all of the table control operations (add, change and delete), line card code information (card index) will be sent to the DDRM node via a DMS-X message.

Table Control operations will be as follows:

- Write

Same card code must be used for the 8 slots in the same LCC.

LEN	CARDCODE	PADGRP	STATUS	GND	BNV	MNO	CARDINFO
DDRM 09 0 01	00 DRBLCN	STD LN	WORKING	N	NL	N	NIL
DDRM 09 0 01	01 DRBLCN						
DDRM 09 0 01	02 DRBLCN						
DDRM 09 0 01	03 DRBLCN						
DDRM 09 0 01	04 DRBLCN						
DDRM 09 0 01	05 DRBLCN						
DDRM 09 0 01	06 DRBLCN						
DDRM 09 0 01	07 DRBLCN						
DDRM 09 0 01	08 DRBLCP						
...							
...							
...							
DDRM 09 0 01	15 DRBLCP						

After the first entry has been added for one of the 8 slots, the others will be verified against this entry. This means the LCC with 8 slots will be identified by the first entry. When another card code needs to be used, the user will be prompted:

“All lines in this LC must use same card code, <>.”

“(On LSG: <drawer number>,”

“ between circuit <no>,”

“ and circuit <no>“

Line card code information will be sent to the DDRM when the first entry of the 8 slot has been added.

- Delete

Existing DMS behavior will be kept. LENS can be deleted one by one if they are not in use. Deleting the 8 lines together in the same LCC is not provided.

When the last entry of the 8 slots has been deleted, card code information for the empty LC will be sent to DDRM.

- Change

Changing the cardcode of 8 lines together will be provided and users will be informed via a message:

“All lines on this LC will be updated with card code <>.”

“(On LSG: <drawer number>,”

“ between circuit <no>,”

“ and circuit <no>“

As the DMS does for World Line Cards, line states, before changing operation, must in the MB/INB for the DDRM lines to prevent possible problems as a line can be using in CallP in that phase. If one of the 8 lines is not in the MB/INB then the prompt below will be printed:

“Cannot change the CARDCODE when the line is in service“

“Line states of each line on this LC must be MB/ INB“

Also, when the change operation succeeds, new card code information will be sent to the DDRM for that LC.

15.2.4.3 Line Maintenance and Line Diagnostic Scenarios

Line maintenance is responsible for the proper function of line cards, loop transmission facilities, subscribers terminating equipment and transitions of line states. It is handled in the same way as the RLCM, and so the same behaviors are kept for the DDRM.

Valid line maintenance commands (in LTP map level and its sub-levels) for DDRM Lines will be:

Table 4

Command	Function
Post	Posts a line or set of lines to the LTP.

Table 4

Command	Function
Bsy	Changes the state of the line in the control position, or optionally the complete set of posted lines, from IDL to MB.
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	Diagnose the posted line.
FRLS	This command is not visible at the LTP level. The FRLS command forcibly disconnects a line circuit from the test equipment or any other circuit and changes its state to MB.

DIAG (Diagnostic) will be provided for DDRM lines which has one of the testable line card codes.

Whereas SDIAG (Short Diagnostic in ALT level) will not be supported as the line diagnostic set is already very restricted for the DDRM. It consists of Battery Feed Resistor, Current Limit Test and Metering Test (for only testable Coin lines).

Table 5 Line Maintenance and Diagnostic Sets

	DRBLCN	DRBLCP	DRDLCP	DRMLCN	DRMLCP
Card Property	Basic IBN	Basic IBN with Over-voltage	Basic Testable IBN with Over-voltage	Basic Metering	Basic Metering Testable with Over-voltage
Maintenance	POST	POST	POST	POST	POST
Commands	BSY RTS	BSY RTS	BSY RTS	BSY RTS	BSY RTS
Diagnostics	<u>Not Allowed</u>	<u>Not Allowed:</u>	<u>Allowed:</u> Battery Feed Current Limit	<u>Not Allowed</u>	<u>Allowed:</u> Battery Feed Current Limit Metering Test

Existing line states and line state transitions for DMS lines will also be valid for DDRM lines. They can be seen in the tables below:.

Table 6 Valid Line States

Line State	Interpretation
IDL	Line is in service and on-hook.
CPB	Line is involved in a call.
MB	Line has been removed from service by the BSY command.
CPD	In CPB state, MB pending.
LMB	DDRM is either out of service, or both its C-side links are out-of-service.
LO	The switch has put the line in temporary out-of-service state.
PLO	Line is in off-hook state for an excessive time.
DEL	Temporary state between CPD and MB.
NEQ	Line is not data filled in LNINV table.
INB	Line is not datafilled in LENLINES table or the BSY INB command was performed.
CUT (For only over-voltage cards)	The cutoff relay in the line circuit is operated, disconnecting the subscriber loop from the line circuit.
HAZ (For only over-voltage cards)	A line hazard condition (foreign line voltage, leakage resistance) has been detected; the line's cutoff relay is operated.
SB	The line has been removed from service by the DMS switch because of an incoming message overload.

Table 7 Line State Transitions on DMS

From	To CPD	CUT	DEL	IDL	INB	MB
CPB	+			+		+
CPD			+			
CUT				+	+	+
DEL				+	+	+
IDL		+				+
INB		+				+
LMB				+	+	+

Table 7 Line State Transitions on DMS

From	To CPD	CUT	DEL	IDL	INB	MB
LO		+		+	+	+
MB		+		+	+	
PLO		+		+	+	

Line states can be changed according to some manual actions or can be done automatically by system maintenance. Maintenance actions performed on drawers such as RTS DRWR, TST DRWR will effect line status. Also, when LC Config mismatch is sent from the DDRM, line states will be updated if needed.

Note: Line diagnostics will be implemented with the activity A00006664 in the ISN09 stream.

15.2.4.4 Line Audits

DDRM is added to the list of peripherals on which line sync audit and babbler audits run. Thus they will be supported for the DDRM lines too.

The purpose of the babbler audit is to revisit babbling lines and return them to service instead of just denying them service because they once failed a diagnostic.

For all of the other scenarios for line audits, existing RLCM behavior will be kept for the DDRM lines.

Note: Line audit related DMS implementations are completed in ISN08. But as line audits execute line diagnostics, and as they will be available in ISN09, line audits will be available with the activity A00006664 in the ISN09 stream.

Line audits can be tested fully in ISN09.

15.2.4.5 Static Data Handling

The DDRM needs line card codes as static data. The codes will be sent to DDRM via DMS-X messages through the host PLGC. As DDRM supports 5 different type card codes, DMS will send an index to DDRM to indicate the card code.

LNINV static data is downloaded under the following conditions

- LCM RTS

Table LNINV card codes will be the part of the LCM RTS static data.

- LNINV table control operations: write, delete, change

While adding, deleting or changing a cardcode of a LEN, dynamic update of this data is needed.

15.3 Hardware Requirements or Dependencies

Not Applicable

15.4 Software Requirements or Dependencies

For successful deployment of this activity, the following two activities are required as DDRM lines can not be defined or maintained unless the DDRM node itself is defined and maintained:

- A00006660 - DDRM Node Definition and Provisioning
Line provisioning is dependent on a node definition made on table LCMINV by means of SITE information in table LNINV.
- A00006661 - DDRM Node Maintenance
Line maintenance is dependent on node maintenance.
- A00006666 - DDRM XPM Support and Monitoring
The DDRM emulator is needed for UT tests.

15.5 Limitations and restrictions

- Only DDRM Basic and COIN lines are supported for DDRM. All of the other types such as ISDN, PPHONE, V5.2 etc. will not be supported.
- The DDRM node has a restriction about Coin lines:
“Total COIN Line number per shelf cannot exceed the 10% of total line number in the shelf. (10% x 160 lines = 16 MAX coin per shelf).
- Maintenance: Non-menu command “FRLS” is supported for all DDRM lines. There are some actions which will not be supported: SDIAG (in ALT level.)

15.6 Interactions

Other line related activities may have some interactions with this activity:

- A00006664 - DDRM Line Testing
- A00006663 - DDRM Alarms and Audits

15.7 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)_____

15.8 References

- DDRM Spec. - module DMS_DDRM in fmdoc
- A00006638 DMS- DDRM HLD

15.9 Glossary

Table 8

Term	Description
DDRM	DMS Dicle Remote Module
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
UTR	Universal Tone Receiver

16: A00006666 Functional description (FN)

16.1 Feature name

DDRM XPM Support and Monitoring

The DDRM (DMS Dicle Remote Module) project as a whole provides a platform that supports the DDRM node as a remote line module of DMS like a Remote Line Concentrating Module (RLCM).

A00006666 is a sub-feature of the DDRM project and it is aimed to support the XPM part of this project on Host PLGC(XPM).

16.2 Description

16.2.1 Background Information

16.2.1.1 DDRM Node Configuration

The DDRM is a new, remote peripheral connected to a MMP Switch via a host XPM peripheral (PLGC) through a maximum of 4 E1(PCM30) links.

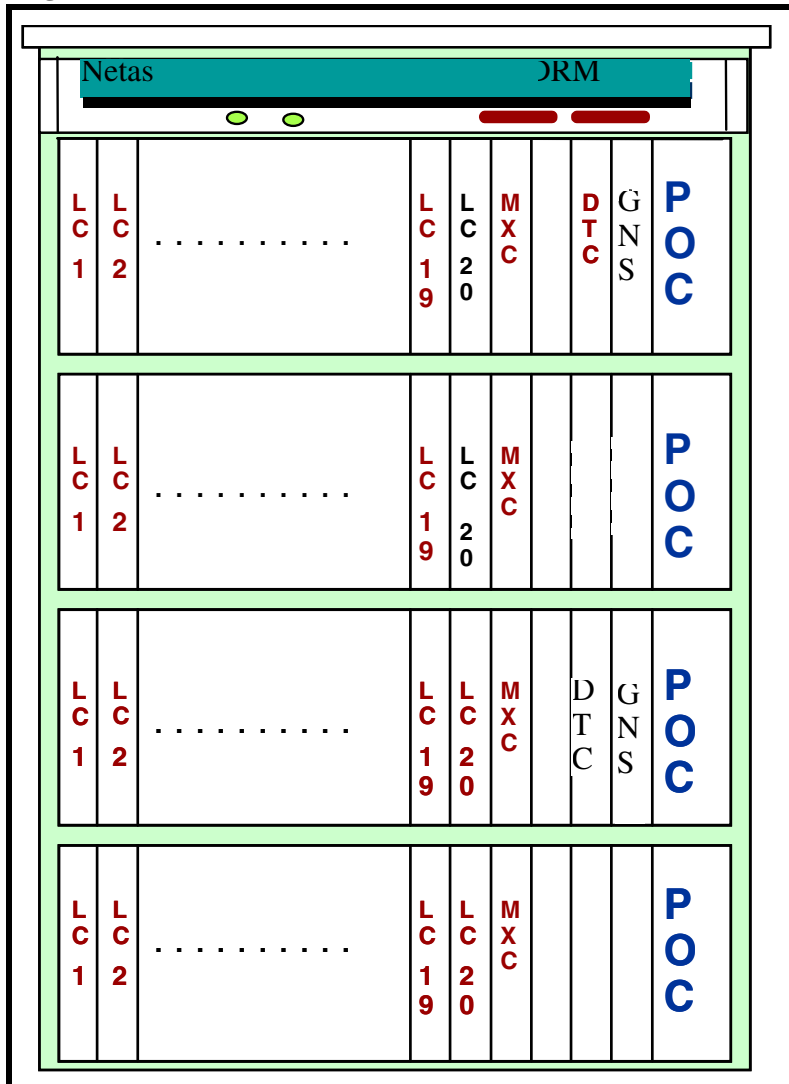
The DDRM is based on an MMP RLCM which is developed for the Turkey Market. The purpose of the whole project is to enhance the benefits of the DDRM Rural Switches and to provide the RLCM Node facility for the DDRM Rural exchanges in the Turkey market network. Thus maintenance and administration related operations are processed on DMS exchanges.

The DDRM module is configured as one cabinet DDRM Local Switch, each of which consists of 4 shelves.*

Note: * The configuration with 4 shelves is not fixed and the DDRM node with less than 4 shelves is available in the Turkey market network.

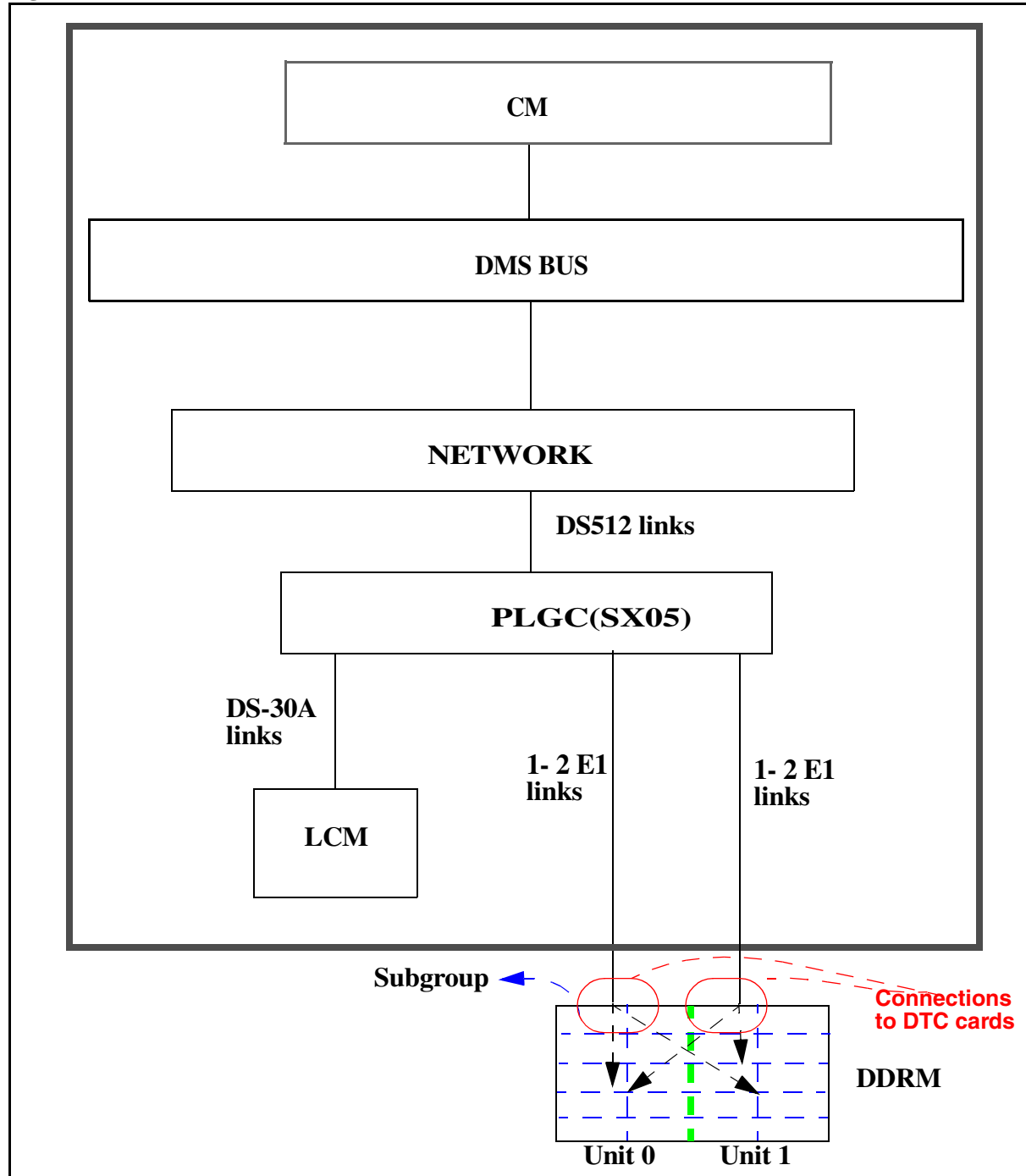
The DDRM node with 4-shelves card configuration is as follows:

Figure 1 DDRM Hardware



The DDRM is connected to the PLGC with E1 links (between 2 and 4) and communicates via the DMS-X protocol. E1 link connections are provided by DTC cards of the DDRM. Connection is shown below:

Figure 2 DMS host and DDRM node connection



16.2.2 Feature Synopsis

With the A00006666 activity, it is required to provide the DDRM XPM support and monitoring on a DMS site. The feature includes:

- New XPM DDRM PM Type and all relevant definitions on the Host PLGC.

Besides the above feature items, call process issues will be investigated under this feature. None of the related CM DDRM activities are aimed to change CALLP behavior. Therefore it is expected that the DDRM has similar CALLP behavior as the existing RLCM has.

16.2.3 Feature Description

16.2.3.1 Node Definition - XPM Part

According to selective design in related DDRM CM activities, the DDRM PM type needs to be defined as downloaded PM type information during PLGC RTS time as static data field.

Behind a new PM type there is usually specific hardware. The DDRM is also new hardware which has its own characteristics, the number of line drawers are the same but the number of lines may not be the same, since line card slots can also be used for other cards like UTRD and MTA cards. Likewise, the DDRM can be defined in a different configuration (single plane, double plane) while LCM cannot.

Despite the similarities existing between the RLCM peripherals, the DDRM differs from existing RLCM peripherals. In order to differentiate peripherals on the basis of their functional characteristics, definition of a new PM_TYPE is required.

16.3 Hardware Requirements or Dependencies

In order to test CALLP a INSV DDRM node is required.

16.4 Software Requirements or Dependencies

For successful deployment of this activity the following two activities are required as the DDRM lines cannot be defined or maintained unless the DDRM node itself is defined and maintained:

- A00006660 - DDRM Node Definition and Provisioning
DMS CM part of the DDRM provisioning has been implemented by this activity.
- A00006661 - DDRM Node Maintenance
The DDRM Node maintenance is implemented by this activity. And it is required to have a INSV DDRM node.
- A00006662 - DDRM Lines Inventory
The DDRM lines are provisioned by this activity. In order to test supplementary services on the DDRM this feature is required.

Also:

- The DDRM node, internal software

Mapping will be done internally in the DDRM node. DMS recognizes the DDRM as it has really Drawer-based architecture. All of the DMS-X messages will be sent and got in this form.

16.5 Limitations and restrictions

Because there are no enhancements targeted for the DDRM it is necessary to verify whether the existing RLCM call process has similar problems during CALLP related tests.

16.6 Interactions

None.

16.7 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)_____

16.8 Glossary

Table 1

Term	Description
DDRM	DMS Dicle Remote Module
DRX-4	Dicle Rural Exchange-4
DTC	Digital Trunk Card

Table 1

Term	Description
ESA	Emergency Stand Alone
LC	Line Card
LCM	Line Concentrating Module
RMM	Remote Maintenance Module
MCT	Malicious Call Trace
RLCM	Remote Line Concentrating Module

16.9 Recommended Reading/References

- a. DMS_DDRM at FMDOC
- b. A00006638 DDRM New Remote LCM High Level Design at PLS FMDO

17: A00006708 Functional description (FN)

17.1 Feature name

Metering on Israeli ISUP for IDDD calls

17.2 Description

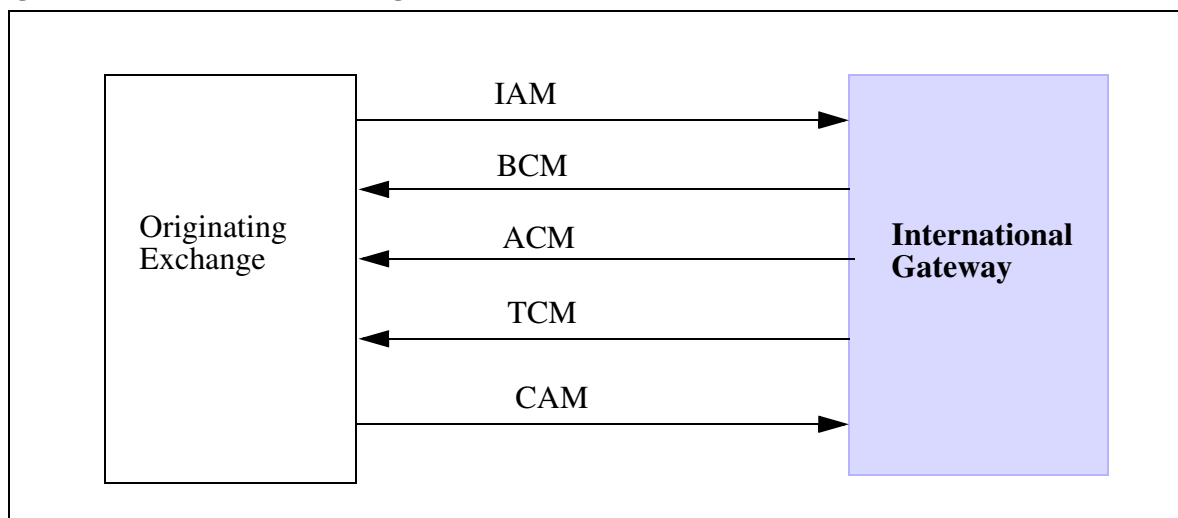
The Purpose of this activity is to populate Backward Charging Message (BCM) and Tariff Change Message (TCM) with Tariff data from NAOC tables for Israeli ISUP. The activity is applicable for both TDM and Succession CS2K solutions.

This feature supports the following issues:

1. Generation of BCM message based on datafills in NAOC specific tables.
2. Support to send TCM message in backward direction when Tariff change Over (TCO) happens.
3. Generation of AMA record for BCM/TCM based metering information.

17.3 Background information

Figure 1 BCM/TCM/CAM message flow



A call arrived on International Gateway is defined as outbound (International) in the following cases:

1. When a call comes from **TMX100** with Nature of Address indicator (NOA) received in IAM is **International**
2. If the Nature of Address Indicator (NOA) is **not International** & FCI (Forward Call Indicator) received in IAM is **International**.

The above conditions are needed for sending BCM and TCM messages.

For each call, after IAM is received, and prior to ACM, the International Gateway sends the BCM message. As the tariff may change during the call, the International gateway informs the Originating exchange using a TCM message. This TCM is acknowledged by the Originating exchange by sending Charging Acknowledgement Message (CAM). A basic framework for BCM message triggering was implemented with the activity A59034453 (International ISUP in SN04). The implementation for triggering the TCM message is being provided with the current activity.

17.4 Messaging.

17.4.1 BCM and TCM messages.

For charging purposes, the Israel Network requests metering messages for outbound calls.

The SN04 TDM activity (A59034453) provided a basic framework for the following message types :

- Backward Charging Message (BCM)
- Tariff Change Message (TCM)
- Charge Acknowledgement Message (CAM)

The purpose of this feature is to calculate actual charging information for BCM/TCM messages.

17.4.1.1 Calculation of actual metering charges for BCM message

17.4.1.1.1 BCM Message body

Table 1 BCM message fields

Message fields	Length (byte)
Message type	1
Charge Indicator	1
Current Charge Rate	2
Time Indicator	1
Next Charge Rate	2

17.4.1.1.2 BCM Metering calculation

Calculation of actual metering charges for BCM message will be done by reading data from the following metering tables by using NAO framework. The main NAO table used to retrieve the BCM metering information is :

- TARFDATA
- INTLZONE
- **TIMEODAY.**
- CURRCONV

BCM metering information that needs to be transported contains Charging Unit Repetition rate i.e. Pulse Rate. This means the charging unit has to be generated in every x seconds. This Charging Unit Repetition Rate is determined by dividing the currency value of a pulse from table CURRCONV by communication price in table TARFDATA.

A national indicator called Charging Message Indicator is used to differentiate between the BCM message and the TCM message. The format of this indicator is shown in Table 2, where only the bits A-D are used.

Table 2 Charging message indicator parameters field

8	7	6	5	4	3	2	1
H	G	F	E	D	C	B	A

Figure 2 on page 32 shows the Codes that are used in the charging message indicator field

Figure 2 Codes that are used in the Charging msg indicator parameter field

bit	BA:	Tariff indicator current tariff
00:		Current rate not present
01:		Current rate present - Rate expressed in deciseconds.
10:		Current rate present - Rate expressed in centiseconds
11:		Current rate present - Rate expressed in milliseconds
bits	DC:	Tariff indicator next tariff
00:		Time indicator not present
01:		Time indicator present - Rate expressed in deciseconds.
10:		Time indicator present - Rate expressed in centiseconds
11:		Time indicator present - Rate expressed in milliseconds
Bits E to H : spare		

The Current Charge Rate is coded in a national parameter (2 bytes, least significant byte first, most significant byte afterward). Tariff rates are expressed according to charging message indicators(2 bytes). Please refer to Table 4 for further details

Table 3 Current rate parameter

	8	7	6	5	4	3	2	1
LSB	H	G	F	E	D	C	B	A
MSB	P	O	N	M	L	K	J	I

17.4.1.1.3 Example for BCM coding

We assume that we use a charging unit value of 20 currency unit / charging unit. We also assume that a datafilled tariff of 0.4 currency units per second (see figures below)

Figure 3 Table CURRCONV

```
add DEFAULT 2 1
add EURO    2 1
```

Figure 4 Table TARFDATA

add CARRIER1 73 4 -1 0 N \$ 1 0 0 N

The resulting Charging Repetition Rate would be :

- Charging unit value / communication charge i.e. $20 / 0.4 = 50$ seconds or 500 deciseconds.
- Charging Message Indicator : 0000 0001
- Current Rate Parameter : 1111 0100 0000 0001 (#1F4)

The Current Rate Parameter (50 seconds) would be determined in the following way :

- The CHARGING unit value is retrieved from table CURRCONV as the EURO field i.e. 2 1 which means $2 * 10^1$ i.e. 20
- The numeric value of TARIFF is retrieved from table TARFDATA i.e. 4 -1 which means $4 * 10^{-1}$ i.e. 0.4
- Calculate the Current Rate Parameter by dividing CHARGING by TARFDATA value i.e. $20 / 0.4$ which is 50.

17.4.1.2 Building the TCM supervision

17.4.1.2.1 TCM message body

Table 4 TCM message fields

Message fields	Length (byte)
Message type	1
Charge Indicator	1
Time Indicator	1
Next Charge Rate	2

17.4.1.2.2 TCM Metering calculation

Calculation of actual metering charges for TCM supervision is similar to that of BCM. In addition to the BCM metering calculation, the TIME information and Charge Message Indicator would be calculated for TCM as well.

Please refer to Chapter 2.4.1.1.2 for the calculation of the current rate parameter and the charging message indicator

The TIME information would be obtained from table TIMEODAY. It would be multiplied by 2 to transport the time information in the requested format. For the format of Time Indicator please refer to Table 5 and Figure 3

Table 5 Time indicator parameter field

8	7	6	5	4	3	2	1
H	G	F	E	D	C	B	A

Figure 5 Codes that are used for time indicator parameter field

bits	HGFE DCBA		
	0 0 0 0 0 0 0 0	spare	
	0 0 0 0 0 0 0 1	00.30 hs	1 hex
	0 0 0 0 0 0 1 0	01.00 hs	2 hex
	.		
	.		
	0 0 1 1 0 0 0 0	24.00 hs	30 hex
	.	spare	
	.		

The following items have to be also considered for the generation of the TCM messages on the international gateway:

- **Max No** of TCMs that can be sent incase of non-receipt of CAM is **#5**
- **Timer** for Charging Acknowledgement (CAM) is **#36**

17.4.1.2.3 Example for TCM coding

We assume that that the same numerical values used for the BCM example are used in this case.. We assume here that tariff changeover would occur at 18:00 which would correspond to a value to be transported is 36 (#24).

- Charging Message Indicator : 0000 0100
- Current Rate Parameter : 1111 0100 0000 0001 (#1F4)

The TIME value would be determined in the following way :-

- TIME value would be retrieved from table TIMEODAY. It is 18:00 here.
- Multiply this value by 2. If the value is 0 then we write 48. For 18:00, the TIME value would be 0010 0100 (#24)

17.4.1.3 Triggering of TCM message

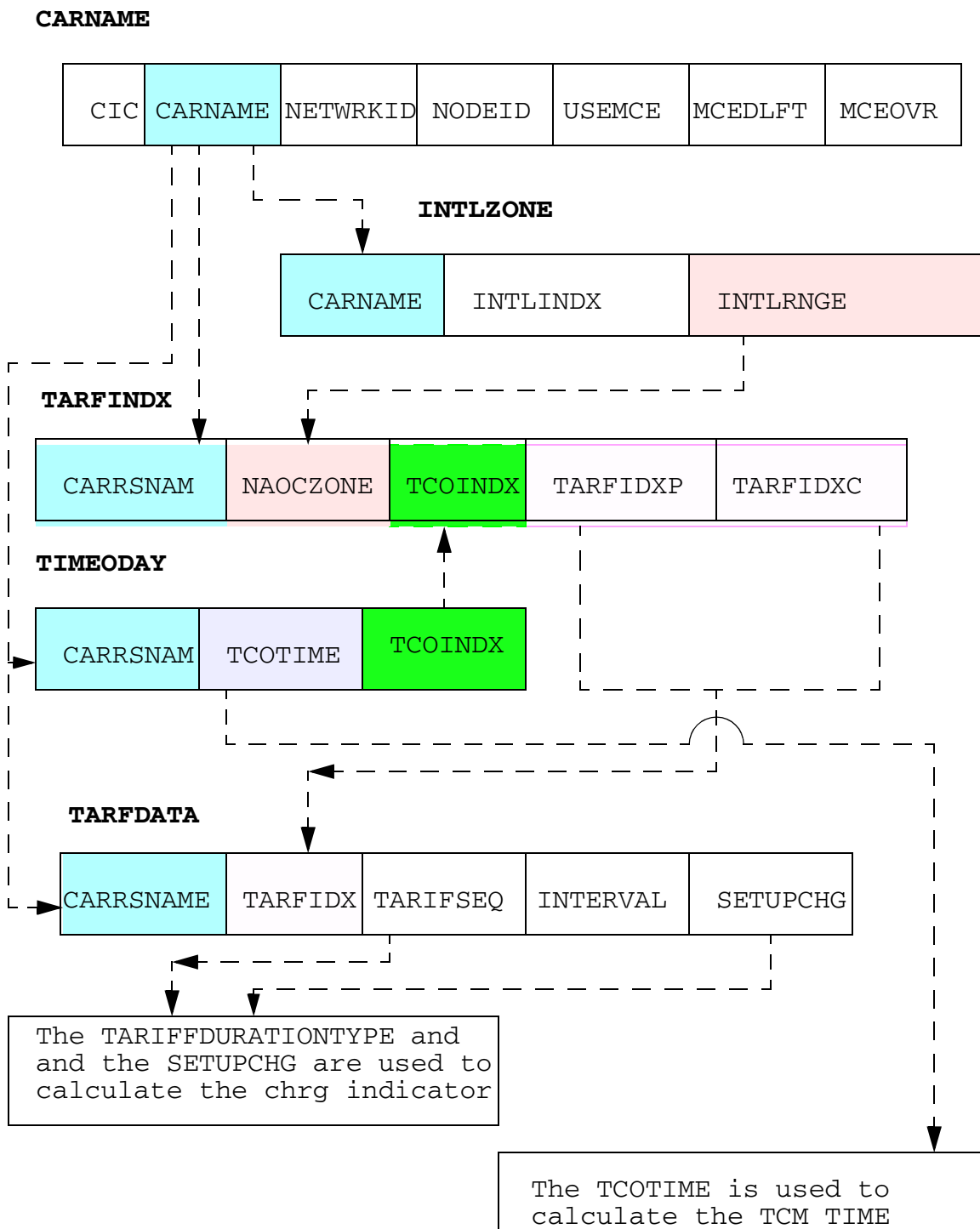
The TCM message will be triggered if there is a change in tariff when the call is in progress and only if BCM message for this call is already triggered. The TCM message will be sent in outbound (International) calls when

- a tariff update for this call is scheduled in table TIMEODAY
- **COFFTYPE** field is set in table TRKGRP
- the type of the terminator trunk is **International**.

The TCM message producing will be controlled by **INTMTR** option in table **TRKOPTS**. If the INTMTR option is defined for an incoming ISUP trunk and if the BCM message is already triggered, a TCM message will then be triggered.

17.5 Data Requirements or Dependencies

Figure 6 :Table which derives the Tariff Data



17.5.1 Table PXHEAD:

Figure 7 Table PXHEAD

```
add K5PSTN DFLT CONT (MM 7 24) (XLT OFC K5OFC) $ DFOP (NAOC INTL)
(CLASS INTL) (AMAXLAID PSTN) (CDNRTE ) $ NOCON
```

17.5.2 Table PXCDE

Figure 8 Table PXCDE

```
add K5PSTN 590 590 RTE (PF 3) (MM 4 18) (DEST 590) (NAOC INTL) (CLASS INTL)
$
```

17.5.3 Table OFCENG

Figure 9 Table OFCENG

```
add PRESELECTED_DEFAULT_CARRIER 1041
add ENABLE_METERING Y
```

17.5.4 Table TRKOPTS

Figure 10 Table TRKOPTS

```
add IP590EICHA INTMTR INTMTR
add IP590EICHB INTMTR INTMTR
```

17.5.5 Table TRKSGRP :

Figure 11 Table TRKGRPS

```
add IP590EICHA 0 DS1SIG C7UP 2W N N EXTERNAL NONE Q767 THRH      0
DMSNODE N Y ISRAEL100_WHITE $ ETSI2W CIC

add IP590EICHB 0 DS1SIG C7UP 2W N N EXTERNAL NONE Q767 THRH 0
DMSNODE N Y ISRAEL100_WHITE $ ETSI2W CIC
```

17.5.6 Table CURRCONV

```
add DEFAULT 2 1
add EURO    2 1
```

17.5.7 Table CARNAME

Figure 12 Table CARNAME

```
add 1041 CARRIER1 0 0 N CALL_BY_CALL USE_CALL_BY_CALL
```

17.5.8 Table TODHEAD

Figure 13 Table TODHEAD

```
add      CARRIER1 NAOC  WEEKDAY  WEEKEND  $
```

17.5.9 Table DAYOWEEK

Figure 14 Table DAYOWEEK

add	CARRIER1	MON	WEEKDAY
add	CARRIER1	TUE	WEEKDAY
add	CARRIER1	WED	WEEKDAY
add	CARRIER1	THU	WEEKDAY
add	CARRIER1	FRI	WEEKDAY
add	CARRIER1	SAT	WEEKEND
add	CARRIER1	SUN	WEEKEND

17.5.10 Table TIMEODAY

Figure 15 Table TIMEODAY

add	CARRIER1	WEEKDAY	0	0	NAOC	1
add	CARRIER1	WEEKDAY	2	0	NAOC	6
add	CARRIER1	WEEKDAY	3	0	NAOC	7
add	CARRIER1	WEEKDAY	8	0	NAOC	2
add	CARRIER1	WEEKDAY	12	0	NAOC	3
add	CARRIER1	WEEKDAY	18	0	NAOC	4
add	CARRIER1	WEEKDAY	0	0	NAOC	5

17.5.11 Table INTLZONE

add	CARRIER1	1	1	100	\$

17.5.12 Table TARFINDX

Figure 16 Table TARFINDX

add CARRIER1	1	1	73	73
add CARRIER1	1	2	73	73
add CARRIER1	1	3	73	73
add CARRIER1	1	4	73	73
add CARRIER1	1	5	73	73

17.5.13 Table TARFDATA

Figure 17 Table TARFDATA

add CARRIER1	73	4	-1	0	N	\$	1	0	0	N

Note: For more details on the inter dependencies of the above tables, refer to DS of the activity **naoc_etsi_isup_tariff_db_tco** in fmdoc.

17.6 Hardware Requirements or Dependencies

This activity does not add any additional hardware requirements and dependencies on top of those used for NAOC or for the features NAOC do interact with.

17.7 Software Requirements or Dependencies

This activity requires the following feature to be activated by SOC

- **NETK0024** : Network AOC Tariff
- **NSUP0020** : NAOC / PCA Supplementary Services
- **NSUP0023** : PCA SW Mtr Bill Supplementary Services

NAOC tariff information is required since this activity reuses the NAOC functionality. NAOC datafill including the NAOC tables and translation options have to be set up in an appropriate way.

17.8 Restrictions/Limitations

Only some few new limitations or restrictions are introduced by the current activity:

1. AOC calculation based on the charging interval introduced with A00002625 is not supported
2. Only the first subtariff of the NAOC tariff vector will be supported for BCM and TCM messages

17.8.1 Interactions

A brief overview of the supported agent interworkings is given below. The combinations of supported interworkings are listed in Figure 2 “Agent interworking for the current feature”. Only the agents marked green and with “X” are being supported. Other agents supported by NAOC which are not being covered by this activity are marked yellow and “N/A”.

Figure 18 Agent interworking for the current feature

Platform	Originator					
		IBN lines	ETSI PRI	Israeli ETSI ISUP	Other ISUP variants	SIP-T
TDM & CS2K	Israeli ETSI ISUP V2	N/A	X	X	N/A	N/A

17.9 References

REF #	Description of Reference
[1]	A59034453:International ISUP in MMP17.
[2]	A00004933:Indian Isup Charge support in CS2K
[3]	A00002637:Network AOC support for to Spanish Trunk Metering
[4]	A00002638:Software Metering Support for Billing
[5]	A59039734:eurotrunks enhancements III

Figure 19 Overview of the NAOC and PCA development

Type	Stream	ACTID	Description of Reference
N A O C	MMP12	59007987	<i>ETSI ISUP - Network AOC (CDP+CGP)</i> , Issue AA25, PLS FMDOC module: <i>network_aoc_etsi_isup</i> .
		59008229	<i>ETSI ISUP - Network AOC Tariff And Time Of Day Switchover (CDP)</i> , Issue AA67, PLS FMDOC module: <i>naoc_etsi_isup_tariff_db_tco</i> .
		59007780	<i>Network AOC CGP Function</i> , Issue AA18, PLS FMDOC module: <i>A59007780</i> .
	MMP13	59012308	<i>ETSI ISUP Network AOC - analog enhancement</i> , Issue AA15, PLS FMDOC module <i>A59012308 (TDM onlly)</i>
		59012315	<i>ETSI ISUP Network AOC - V5.2 enhancement</i> , Issue AA02, PLS FMDOC module <i>A59012315</i>
		59013775	<i>Network AOC: Integrated CGP and CDP</i> , Issue AA27, PLS FMDOC module: <i>A59013775</i> .
	ISNH03	59032878	<i>NAOC on PRI</i> , Issue AA05, PLS FMDOC module: <i>A59032878</i> .
P C A	SN04	59034497	<i>Payment ceiling for Succession Intl. Cable IP</i> , Issue AA32, PLS FMDOC module: <i>A59034497</i> .
	SN05	59039121	<i>NAOC and PCA Feature Interworkings with 3WC, CFx, CXR and HOLD</i> , Issue AA30, PLS FMDOC module: <i>A59039121</i> .
NAOC	SN06	89007454	<i>NAOC German Regulatory Enhancements</i> , Issue AA17, PLS FMDOC module: <i>A89007454</i> .
PCA		89007461	<i>Payment Ceiling Regulatory Enhancements</i> , Issue AA40, PLS FMDOC module: <i>A89007461</i> .
NAOC	SN06.2	A00001927	<i>Line Hardware Metering</i> , Issue AA03, PLS FMDOC module: <i>A00001927</i> .
		A00002938	<i>Full Line HW Metering / Billing Compliance</i> , Issue AA12, PLS FMDOC, module: <i>A00002625</i> .
	SN07	A00002625	<i>Full Line HW Metering / Billing Compliance</i> , Issue AA12, PLS FMDOC, module: <i>A00002625</i> .
		A00002637	<i>NAOC Trunk Metering Enhancements</i> , Issue AA02, PLS FMDOC module: <i>A00002637</i> .
		A00002909	<i>Telekom ISUP (T-ISUP)</i> , Issue AA24, PLS FMDOC module <i>A00002909</i>
		A00004933	<i>Indian ISUP Charging</i> , Issue AA02, PLS FMDOC module <i>A00004933</i>
		A00002638	<i>PCA SW Metering Billing Compliance</i> , Issue AA14, PLS FMDOC module <i>A00002638</i>
		S00002638	<i>Software Metering support for Billing</i> , Issue AA02, PLS FMDOC module <i>S00002638</i>
NAOC & PCA			

17.10 Applicable customer facing sections

Fault Management

Logs	N/A
Alarms	N/A
Configuration	
Data Schema	
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

17.11 Annex A: Used AMA Record Extension

The calculation of call charges is triggered by the NAOC framework and uses PCA utilities. In addition to sending the call charges as BCM/TCM messages, the calculated overall charges for a specific call are added to an AMA record as a module 612 extension.

The 30 BCD characters contained in this module 612 extension would be distributed as follows:

Figure 20 New module 612 extension used for NAOC/PCA billing

BCD Char	Length	Meaning
1 - 3	3	Rating Class at the beginning of the Call If the billing record is generated by basic call this field will contain the tariff index used for this call from Table TARFDATA, bound by an upper limit of 511 for the Spanish market. If the billing record is generated by a feature action this field will always be set to the value of "511".
4 - 11	8	Used Meter The total number of meter pulses used for this call or feature action.
12 - 15	4	Initial meter value MS The 4 most significant digits of the initial meter pulse value.

BCD Char	Length	Meaning
16 - 19	4	Initial meter value LS The 4 least significant digits of the initial meter pulse value.
20 - 27	8	Final Meter value The final meter pulse value, i.e., initial value + used value.
28 - 29	2	Call Type This field describes if this is a basic call or a feature action . If the billing record is generated by basic call this field will be equal to "00". If the billing record is generated by a feature action this field will be equal to a value based on the particular feature as it is provisioned in table NAOCFEAT (per the carrier/reseller).
30	1	Feature Action^a This field describes the type of feature action If the billing record is generated by basic call this field will be equal to "2". If the billing record is generated by a feature action this field will be equal to one of 10 values based on the type of action: (0) assign (1) deassign (2) administrative activation (3) administrative deactivation (4) administrative programming (5) subscriber activation (6) subscriber deactivation (7) subscriber programming (8) usage (9) interrogation

a. Feature billing is described in PLS FMDOC, Module a00002654.

Figure 21, "Sample AMA Record With Module 612 Extension" contains an example of an AMA record with the 612 extension.

Figure 21 Sample AMA Record With Module 612 Extension

HEX ID:	AA	
STRUCTURE CODE:	40510C	
CALL CODE:	006C	STATION PAID
SENSOR TYPE:	036C	DMS 100F
SENSOR ID:	0250250C	
REC OFFICE TYPE:	036C	DMS 100F
REC OFFICE ID:	0250250C	
DATE:	30903C	SEPTEMBER 03, 2003
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:	01418420317C	
ORIG OPEN DIGITS 2:	FFFFFFFF	
ORIGINATING CHARGE INFO:	FFFF	
DOMESTIC/INTL INDICATOR:	1C	DOMESTIC
SIG DIGITS NEXT FIELD:	007C	
TERM OPEN DIGITS 1:	00008406301C	
TERM OPEN DIGITS 2:	FFFFFFFF	
CONNECT TIME:	000000000C	000000:00.0
ELAPSED TIME:	000011204C	000011:20.4
MODULE CODE:	612C	GENERIC MOD: TWO DGT STR FMT
GENERIC CONTEXT ID:		
PARSE RULES	80070	NAOC PCA CHARGING INFO
SIGNIFICANT DIGITS	00C	NIL
GENERIC DIGIT STRING ONE:		
RATING CLASS	010	

18: A00006728 Functional description (FN)

18.1 Feature name

USPc Japan NTT Protocol Support

18.2 Description

Before this feature, there are two ISUP protocols for Japan market supported on CS2K with LPP signalling :

1. JPN ISUP (datafilled as external protocol JPNISUP), which is only supported on NTT MTP (datafilled as JPN7).
2. JI-ISUP (datafilled as variant JPN_INTERCONN under external protocol Q767), which is only supported on the TTC MTP (datafilled as TTC7).

There is another feature on USPL7.0.3 to support NTT MTP network, but there are some CRs left. This feature solves these problems.

This feature makes CS2Kc support NTT MTP(sometimes named JPN MTP in the Nortel product) on USPc, and also support JI-ISUP running over NTT MTP network.

Only JI-ISUP basic call is considered in this feature, it doesn't verify the supplementary services supported by JI-ISUP over NTT MTP.

18.2.1 Make CS2Kc support NTT MTP

Prior to this feature, NTT MTP is already supported in CORE on TDM side. This feature makes it also supported on IP side .

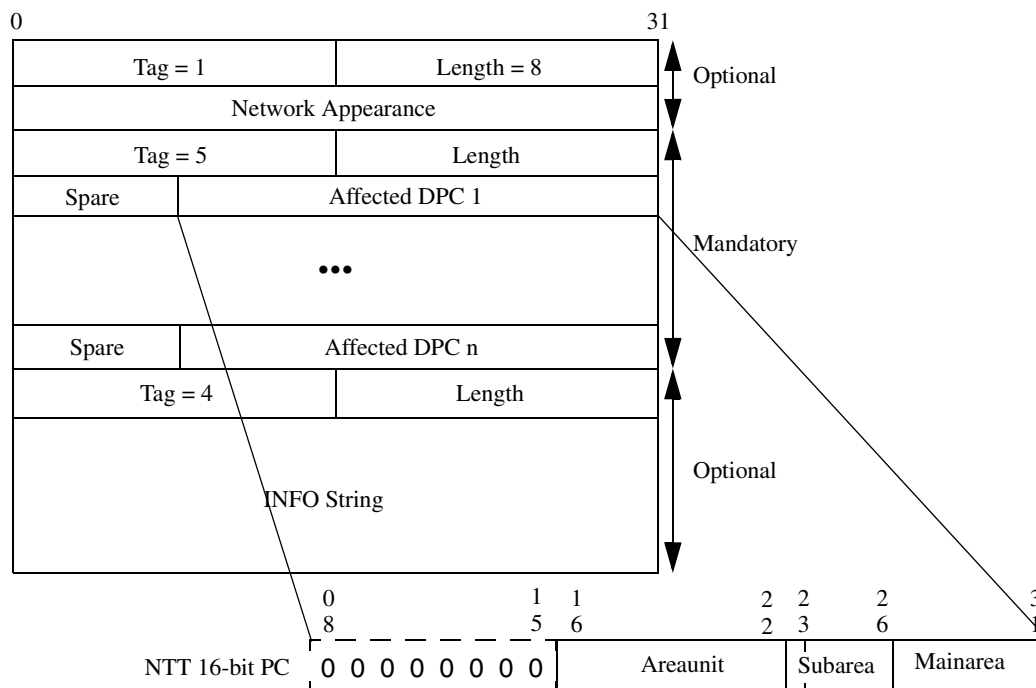
18.2.1.1 Encoding & Decoding NTT MTP PC of M3UA SSNM messages

The M3UA SSNM messages are management messages used to monitor the reachability state of the endpoints. Example messages are DAVA, DUNA, DAUD, SCON, etc.

DAUD is sent from Core to USPc to audit the availability/congestion state of SS7 routes from the USPc to one or more affected destinations.

DAVA / DUNA / SCON are sent from USPc to Core, indicating that the USPc has determined that one or more SS7 destinations are now reachable or unreachable or there is congestion in the SS7 network to one or more destinations.

The SSNM message format is illustrated in Figure 1, "M3UA (Ver 2) SSNM DUNA/DAVA/DAUD message format (NTT 16-bit)" on page 257. SCON message format differs a little in that the spare fields seen in above figure will contain congestion level information.

Figure 1 M3UA (Ver 2) SSNM DUNA/DAVA/DAUD message format (NTT 16-bit)

Note: The type of message is determined by the Msg Class and Msg Type fields in the M3UA header

18.2.1.2 C7NETWRK & C7RTESET Table Provisioning

On the CS2Kc platform the C7NETWRK and C7RTESET tables can not be modified by the craftsperson using the DMS table editor. The data of these two tables is provisioned and uploaded from the USPc.

Since C7RTESET data uploaded by the USPc contains no linkset, the dependency of C7RTESET table on the C7LKSET table is removed. The C7LKSET and C7LINK tables are always empty in the Core.

This work item is to make NTT network type can be provisioned to C7NETWRK and C7RTESET tables by the data uploaded from USPc.

Please refer to Figure 2, "C7NETWRK and C7RTESET Examples" on page 258 for provisioned examples of C7NETWRK and C7RTESET according to data from USPc.

Figure 2 C7NETWRK and C7RTESET Examples

```

TABLE: C7NETWRK
>lis
NETNAME NODETYPE PTCODE NI SLSROT TFR MCS CLUSTERS RCTEST MTPRES CNGCONT
SLSENH
-----
JPNNET1 SSP JPN7 5 7 126 NATL N N 3 N N N N N

TABLE: C7RTESET
>lis
ROUTESET NETNAME TFPBCAST DPC ROUTES
-----
RS_JPN1 JPNNET1 N JPN7 (5) (7) (105) $ $$

```

18.2.2 Support JI-ISUP over NTT MTP network

This feature does not change the behavior of the current JI-ISUP implemented on TTC MTP network on TDM side, but propagates it to NTT MTP network on CS2Kc .

Below is the comparison of ISUP header of TTC MTP network and NTT MTP network, we can see there is only one minor difference between these two headers.

Figure 3 Comparison of ISUP headers on two MTP networks.

TTC ISUP header	DPC 16bits		
	OPC 16bits		
	CIC(H) 8bits	Spare 4bits	SLS 4bits
	Message type 8bits	Spare 4 bits	CIC (L) 4bits
	Message body		

NTT ISUP header	DPC 16bits		
	OPC 16bits		
	CIC(H) 8bits	Spare3bits	SLS 5bits
	Message type 8bits	Spare 4 bits	CIC (L) 4bits
	Message body		

18.2.2.1 Call processing in JI-ISUP over NTT MTP network

JI-ISUP supports the call processing messages as below: IAM, ACM, CPG, CHG, ANM, REL, RLC, SUS, RES.

This feature makes these messages be sent and handled according to NTT MTP network specification and current implementation of JI-ISUP over TTC MTP on MMP.

According to the current implementation of JI-ISUP over TTC MTP, IAM, ACM, CPG, ANM, REL, RLC can be originated, tandemed and accepted by core. And CHG, SUS, RES can be tandem and accepted by core, but can not be originated. This feature propagates these behaviors to JI-ISUP over NTT MTP. But as this feature doesn't support the supplementary services over JI-ISUP, CPG origination is not considered so far.

18.2.2.2 Maintenance messages for JI-ISUP over NTT MTP network

JI-ISUP supports the maintenance messages as below: BLO, BLA, UBL, UBA, RSC, GRS, GRA, CQM, CQR. Besides, the maintenance system will send out REL message when needed.

This feature makes these messages be sent and handled according to the NTT MTP network specification and current implementation of JI-ISUP over TTC MTP.

According to the specification, there is a parameter 'pointer to optional' in JI-ISUP group messages(GRS/GRA/CQM/CQR). But currently, some switches may send out JI-ISUP group messages without this parameter. This feature supports these two types of group messages.

18.2.2.2.1 CQM/CQR/GRS/GRA messages sending and handling

This feature makes these messages be built in JI-ISUP format, and makes these messages be sent and handled according to JI-ISUP requirement.

18.2.2.2.2 Clear up the circuit state mismatch

CCS7 TTP sublevel command (TRKQRY) or ISUP remote audit process which runs in the early hours of each day checks the current CCS7 states of the

local and remote ends to determine if they are compatible. If different, the suggested actions can be taken to fix the problem. One action is “release” and a REL message is sent out.

This feature makes the REL message be sent out with JI-ISUP format.

18.2.2.2.3 Release of the test call

In a call made by OP command, a REL message will be sent out when RLS R command is used at C7TTP level. On the NTT MTP network, a REL message of JI-ISUP messages is built with relative cause location set according to the office parameter TEST_CALL_SPILL in table OFCVAR.

The logic is: if the office parameter TEST_CALL_SPILL contains more than 9 digits or nothing, then the cause location is set to 0111 (international network), otherwise the cause location is set to 0100 (public network serving remote user)

18.3 Hardware Requirements or Dependencies

N/A

18.4 Software Requirements or Dependencies

The feature on USPC that supports NTT MTP network.

18.5 Limitations and restrictions

N/A

18.6 Interactions

N/A

18.7 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___

18.8 Glossary

Table 1

Term	Description
CQM	Circuit Query Message
CQR	Circuit Query Response
CS2K	Communication Server 2000
CS2Kc	CS2K compact
DAUD	Destination State Audit
DAVA	Destination Available
DMS	Digital Multiplex System
DUNA	Destination Unavailable
GRA	Group Circuit Reset Acknowledgement
GRS	Group Circuit Reset
JI-ISUP	Japan Interconnect ISUP
LPP	Link Peripheral Processor
M3UA	SS7 MTP3 User Adaptation Layer
MTP	Message Transfer Part
NCCI	New Common Carrier Interface
NTT	Nippon Telegraph and Telephone
PC	Point Code
SCON	Signaling Congestion
SLS	Signalling Link Selection
SS7	Signaling System No. 7
SSNM	SS7 Signaling Network Management Messages
TPS	Transactor Processing System
TTC	Telecommunication Technology Committee
USP	Universal Signaling Point

Table 1

USPc	USP-Compact

19: A00006730 Functional description (FN)

19.1 Feature name

French NAOC on Succession CS2K

19.2 Description

19.2.1 Summary

This activity extends the existing implementation of the "SPIROU" French ISUP interconnect protocol to

- support generation of Advice of Charge (AOC) messaging to ETSI PRI & H.323 originating agents from Backwards charges received in SPIROU ITX messages (French NAOC) .

By using the NAOC framework on the originating side, interworking with the SN08 activity A00005822 can be guaranteed so that the French NAOC messages can also be applied to H.323 originating agents.

- support optional ITX charge recording to AMA at a SPIROU-SPIROU transit exchange.

Note: Some other French NAOC capabilities were already verified and supported on the CS2K for the SPIROU transit and ETSI PRI interworking scenarios under A59013177 and 59034482 and have not been changed by this feature.

- the ability to tandem ITX and TXA messages at the transit exchange,
- TXA message response & AMA generation for ITX messages received at the originating exchange

H323 to SPIROU interworking, including the TXA message response & AMA generation for ITX messages has already been verified in SN06.2 under the CSA process.

The ITX message generation (CDP functionality) is not officially supported on CS2000. However a preparatory implementation has been introduced by this feature for lab use only, to facilitate black box testing of the transit and originating node aspects. The CDP functionality introduced by this activity is based on the World Metering approach implemented on TDM by AU3283-AU3286, A59013177 and A00006306.

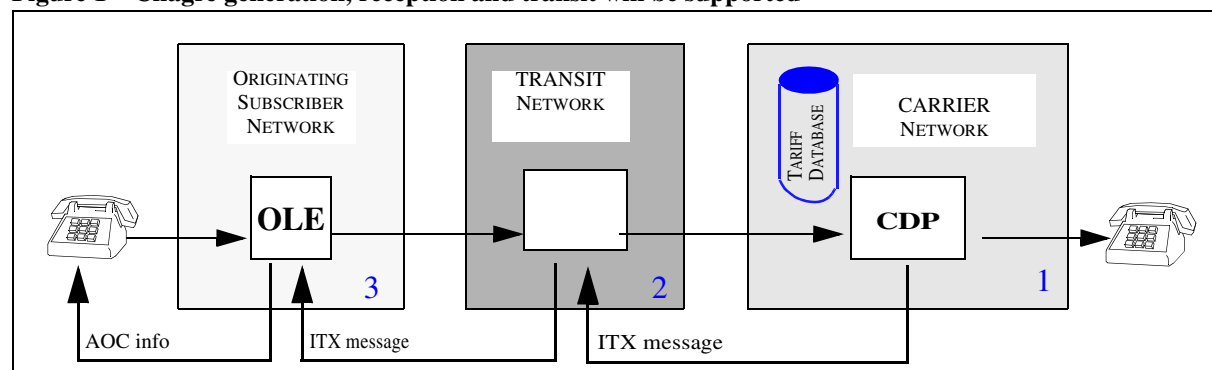
19.2.2 Background information

Network Advice Of Charge (NAOC) implements the tariffing of calls in a deregulated telecom market. It can provide tariff interchange between different operators within different networks.

Operators can be classified in 3 categories from an NAOC point of view (please refer to Figure 1, "Chagre generation, reception and transit will be supported" for further details)

1. **indirect access operators** responsible to generate charge messages and to feed them in backward direction into another operator's network. This functionality is currently not being supported on CS2K.
2. **transit operators** responsible for receiving the charging messages and tandeming them in backward direction
3. **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

Figure 1 Chagre generation, reception and transit will be supported



19.2.3 Feature description

‘**SPIROU Taxation**’ or ‘**French NAOC**’ allows operators and service providers to generate or receive charging information over the signalling system during the call and hence to control the billing for the call. This service is supposed to be used for

- indirect access calls (call by call or preselection calls) served and charged by another operator's network
- service calls served and charged by another operator's network

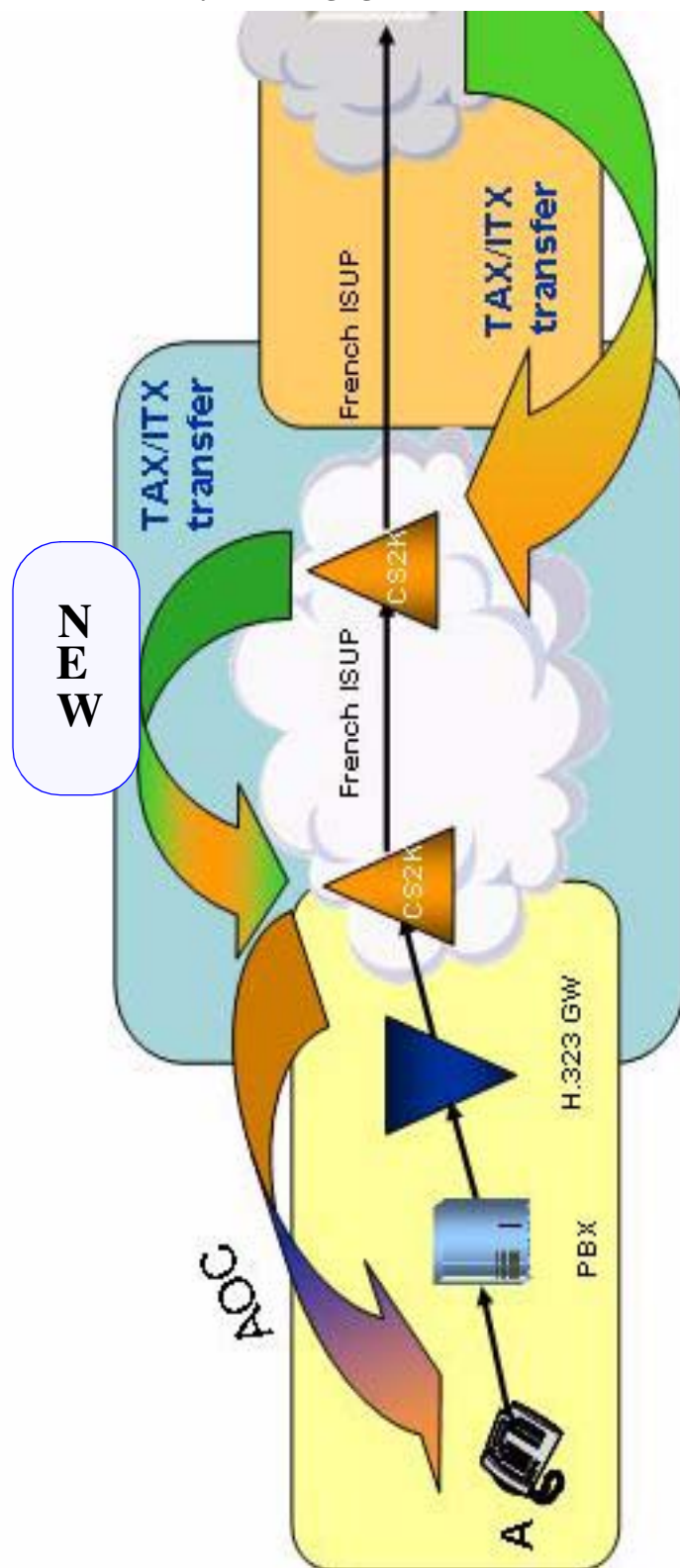
SPIROU supports the capabilities in the charging service, using nationally defined messages ITX (Charge Unit) and TXA (Charging Acknowledgement). The following applications are supported on the CS2K for SPIROU agents:

- **Charge message billing**: Allows an alternate operator to receive ITX messages and use them to bill the calls.
- **Charge message interworking to ISDN originators** on the originating exchange
- **Charge message tandeming** between SPIROU trunks on the transit exchange

- ***Charge message generation*** on the indirect access exchange (not covered by the actual activity)

A short overview of the newly introduced functionality is given in the figure below (For more information see “AOC over H.323 & QSIG” on page 45.)

Figure 2 New functionality does bridging between AOC and ISUP/NAOC



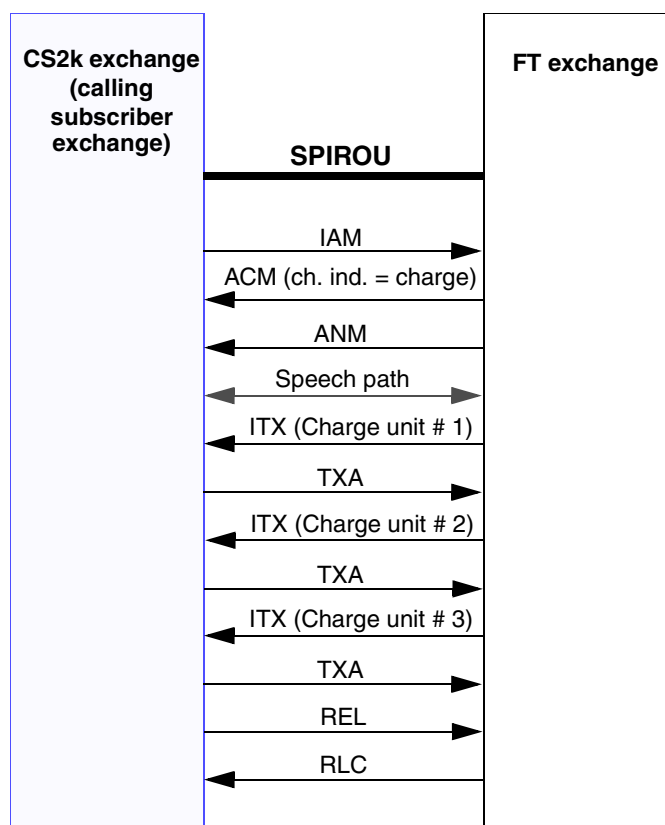
19.2.3.1 Charge message billing

The functionalities provided by this capability includes:

- reception and validation of ITX messages.
- acknowledgement of ITX via TXA messages.
- error scenarios and their responses.
- transit of ITX messages (SPIROU to SPIROU).
- presentation of the charging information in AMA billing record if the outgoing SPIROU trunk is datafilled as supporting the French NAOC Service (Option TELETAXE in table TRKOPTS).

19.2.3.2 CS2K as an originating exchange

Figure 3 CS2K as originating exchange



- Charge message interworking to ISDN originators: Allows an alternate operator to present charge information from ITX messages to ISDN users using the Advice of Charge (AoC) service. The provided functionality will be similar to the existing AOC functionality for ETSI PRI trunks on CS2K. The supported agents are

- **ISDN agents connected over H.323 GW** (see A00005822) marked as supporting the AoC-D service (AOCD or AOCE set Y option in table TRKOPTS). The H.323 interface pass this messages to an appropriate gateway, which then can support the following agents:
 - ETSI BRI
 - Euronumeris¹ / Euronumeris+² BRI
 - ETSI PRI,
 - Euronumeris / Euronumeris+ PRI
- on **ETSI PRI CS2K** trunks controlled over PVG. To provide this capability, the charge information in the ITX messages, is mapped to FACILITY (for ETSI PRI) messages if the PRI trunk is marked as supporting the AoC service (AOCD or AOCE set Y option in table TRKOPTS). The received ITX message is mapped to a NAOC based Facility message similar to the message used for the H.323 functionality.

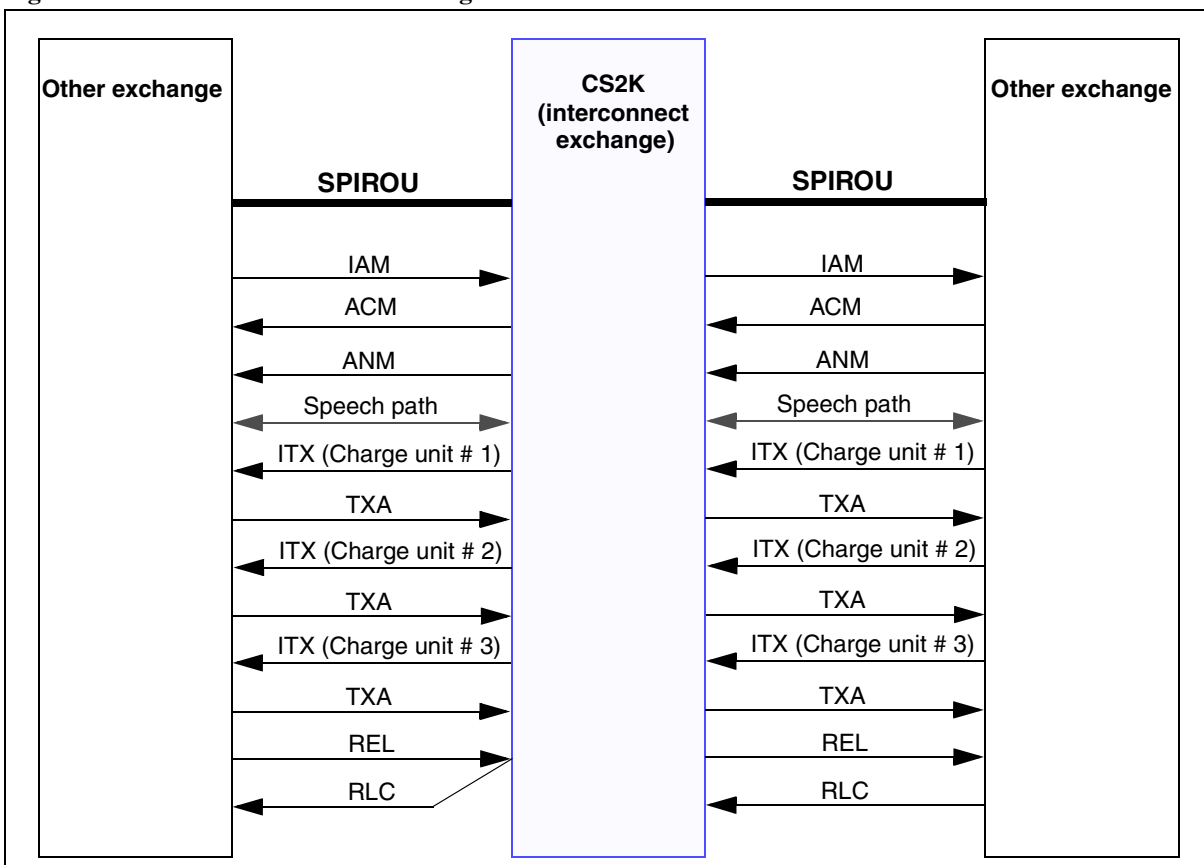
19.2.3.3 CS2K as an interconnect exchange

The interconnect exchange in an alternate operator's network normally performs billing of Indirect Access calls to the operator's network. The CS2K optionally captures, in the billing record, backward charging from ITX messaging received at a CS2K acting as the alternate operator's interconnect exchange.

In addition, the CS2K provides flexibility either to pass them on unchanged across the incoming SPIROU interconnect trunks as shown in Figure 4.

¹Euronumeris was formerly named VN4

²Euronumeris was formerly named VN6

Figure 4 CS2K as interconnect exchange

19.2.3.4 SPIROU backward charging messages and parameters

19.2.3.4.1 ITX message format

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

19.2.3.4.2 TXA message format

Table 2 TXA message format

Parameter	Type	Value	Length (octets)
Message type	F	#E2	1
End of optional parameters	O	All zeros	1

19.2.3.5 Handling receipt of ITX messages

19.2.3.5.1 CS2K as an originating exchange

This section summarises 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.

19.2.3.5.2 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 3.

See also the restrictions relating to handling of ITX and TXA messages in the case of an extended peripheral module (GWC) swact (switch activity) in section 19.5.3 on page 275.

Table 3 Error handling (CS2K as originating exchange)

Error	Action
An ITX is received before both the ACM and the ANM.	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 but before the ANM.	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	
An ITX has the same message number as the immediately preceding ITX but it contains different information.	

19.2.3.5.3 SPIROU transit calls

For transit calls (SPIROU to SPIROU potentially also for SPIROU to SSUTR2 and SSUTR2 to SPIROU 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 is performed. But if the ITX messages are received from the originating exchange or the TXA messages from the terminating exchange, then the transit CS2K exchange will ignore these messages if the call is in the answered state.

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, as for a subscriber exchange. This is controlled by the same datafill as for the subscriber exchange.

19.3 Hardware Requirements or Dependencies

N/A

19.4 Software Requirements or Dependencies

This feature requires the following features to be activated by SOC for the originating exchange:

- *NETK0024* Network AOC Tariff
- *NSUP0020* NAOC/PCA Supp Svcs
- *PBXT0011* ETSI PRI Info
- *PBXT0018* QSIG AOC

The following feature is optional:

- NSUP0023 PCA SW Metering Support for Billing

NAOC tariff information is required, since this feature reuses the NAOC framework. If the SW Metering Support for Billing feature (NSUP0023) is chosen and no NAOC information is provided, the metering counter withing the AMA 612 extension 88070 cannot be updated for that call. Therefore NAOC datafill including the NAOC tables and translation options have to be set up in a appropriate way. Please refer to [38], [41] for additional information.

19.5 Limitations and restrictions

19.5.1 Generic Restrictions/Limitations

The current activity does not introduce any new limitations or restrictions.

The enumeration below lists all known restrictions, which have been introduced by the previous activities AF7344 [35], A59024423 [36], A590038835 [37], A59020791 [33], A00005822 [25]:

1. Sending of AOC charge information as **currency** units is not supported for H.323 trunks yet.
2. AOC calculation based on the **charging interval** introduced with A00002625 [39] is not supported
3. A delta may exist between the number of charge units saved in the AMA record by the CM feature A00002638 [38] controlled by SOC NSUP0023 and the number of charge units provided by the AOC metering counter in the GWC. This is due to charge interval based calculation done in the CM.
4. The GWC calculation of the AOC does not influence or change AMA records extension introduced with A00002638 [38]. There are no direct interactions between the AMA billing system and the AOC functionality in the GWC.

5. 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 CS2000.
6. **AOC-S** (AOC at call setup) is not supported.
7. Provisioning of AOC can only be per trunk group and per GWC. AOC request is always on a per call basis.
8. Out of the supported AOC modes, only those will be delivered which are requested and provisioned at the same time.
9. Only connection-oriented charging information is transmitted to the user (charges for supplementary services are not included).
10. 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. If the AOCREL boolean is set in table **TRKOPTS**, the call is released, otherwise it is not released.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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
16. The SESM interface for table **SERVRINV** does not support the AOC option. This option has to be manually added to the table SERVRINV.
17. 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).
18. Interactions with supplementary services other than those specified in the AOC standards will not be handled.

- a. any '*aocComplete*' request at Call Transfer will be rejected with a ReturnError APDU with error code '*supplementaryServiceInteractionNotAllowed*';
 - b. any '*aocDivChargeReq*' will be ignored but not passed along towards the terminator.
19. A conversion factor change does not affect calls in progress; it only affects calls established after the change.
20. A dummy sourceEntityAddress = 0 will be coded in the NFE of outpulsed Facility IEs, because PINX are not supported by QSIG GF.
21. 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.
22. 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.
23. 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.
24. 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 $\geq$ 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.
25. Table *TRKOPTS*, AOC option, AOCREL = Yes datafill does not have an effect in the following situations (calls are not released):
 - a. 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.
 - b. 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.

-
26. 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.

19.5.2 CM switch activity restrictions

The stable teletax 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.

19.5.3 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.

19.5.3.1 Incoming trunk

The call remains in an answered state provided no Charging Acknowledgement (TXA) is received. No ITX messages will be generated after the swact.

If an ITX has been transmitted and an GWC swact occurs before receiving the acknowledgement TXA, the call is released when the TXA is received from the originating exchange.

19.5.3.2 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.

19.5.3.3 Transit exchange

Transiting of ITX and TXA messages is unaffected by an GWC swact.

19.6 Interactions

The actual functionality will allow feature interworking with ITX messages received over SPIROU trunks. The supported originating agents are either H.323 based or ETSI PRI. The combinations of supported interworkings are listed in “ ” on page 43 and “ ” on page 276. Only the agents marked green and with “X” are being supported. Other agents supported by the initial French NAOC features which are not being covered by this activity are marked yellow and “N/A”

Feature interactions are supported with the activity A00005822 AOC over H.323

Figure 5 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	SSURN2 (FTUP)	SPIROU
CS2K	H323	N/A								X
	ETSI PRI over PVG	N/A								X
CS2K	Euroneris over PVG	N/A								
	Euroneris+ over PVG	N/A								

Figure 6 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	SSURN2 (FTUP)	SPIROU
CS2K	SPIROU	N/A								X
CS2K	SSURN2 (FTUP)	N/A								

Figure 7 French NAOC Support on the indirect access exchange

Platform	Originator	Terminating agents								
		H323 agents	IBN lines	ETSI PRI	QSIG (95)	ETSI ISUP V1	ETSI ISUP V2/N2+	SIP-T	SSURN2 (FTUP)	SPIROU
CS2K	SPIROU	don't care about the terminator								
CS2K	SSURN2 (FTUP)	N/A								

19.7 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)_____

19.8 Glossary

Term	Description
AOC	Advice of Charge
BRI	Basic Rate interface
CDN	Called Party Directory Number
CDP	Charge Determination Point
CGN	Calling Party Directory Number
CGP	Charge Generation Point
CS	Carrier Selection
CS2000	Communication Server 2000
CS2K	Communication Server 2000
ELN	Essential Line
ETSI	European Telecommunication Standard Institute
IAM	Initial Address Message
IBN	Integrated Business Network
IP	Internet Protocol
ISUP	Integrated Services Digital Network User Part
LNP	Local Number Portability
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
UXLA	Universal Translations
XLA	Translations

19.9 References

REF #	Description of Reference
[1]	<i>ETS 300 178 - ISDN; Advice of Charge: charging information at call set-up time supplementary service, Service description, October 1992</i>
[2]	<i>ETS 300 179 - ISDN; Advice of Charge: charging information during the call supplementary service, Service description, October 1992</i>
[3]	<i>ETS 300 180 - ISDN; Advice of Charge: charging information at the end of the call supplementary service, Service description, October 1992</i>
[4]	<i>ETS 300 182 - ISDN; Advice of Charge supplementary service, DSS-1 protocol, April 1993</i>
[5]	<i>ITU-T H.225.0 - Call signalling protocols and media stream packetization for packet-based multimedia communication systems (2000)</i>
[6]	<i>ITU-T Q.931 - ISDN user-network interface layer 3 specification for basic call control</i>
[7]	<i>ITU-T Q.932 - Generic procedures for the control of ISDN supplementary services</i>
[8]	<i>ISO/IEC 11572 / ECMA-142 and ISO/IEC 11574 / ECMA-143 - QSIG Basic Call</i>
[9]	<i>ISO/IEC 11582 / ECMA-165 - QSIG Generic functional protocol</i>
[10]	<i>ISO/IEC 15049 / ECMA-211 - QSIG Advice of Charge - Specification, Functional Model and Information Flows</i>
[11]	<i>ISO/IEC 15050 / ECMA-212 - QSIG Advice of Charge - Interexchange Signalling</i>
[12]	<i>ITU-T X.680 Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation (1997)</i>
[13]	<i>ITU-T X.681 Information technology - Abstract Syntax Notation One (ASN.1): Information object specification (1997)</i>
[14]	<i>ITU-T X.682 Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification (1997)</i>
[15]	<i>ITU-T X.683 Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications (1997)</i>
[16]	<i>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)</i>

-
- [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 - NAOX 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 - NAOX Metering Framework description; PLS FMDOC*

Figure 8 Overview of the NAOC and PCA development

Type	Stream	ACTID	Description of Reference
N A O C	MMP12	59007987	<i>ETSI ISUP - Network AOC (CDP+CGP)</i> , Issue AA25, PLS FMDOC module: <i>network_aoc_etsi_isup</i> .
		59008229	<i>ETSI ISUP - Network AOC Tariff And Time Of Day Switchover (CDP)</i> , Issue AA67, PLS FMDOC module: <i>naoc_etsi_isup_tariff_db_tco</i> .
		59007780	<i>Network AOC CGP Function</i> , Issue AA18, PLS FMDOC module: <i>A59007780</i> .
	MMP13	59012308	<i>ETSI ISUP Network AOC - analog enhancement</i> , Issue AA15, PLS FMDOC module <i>A59012308 (TDM onlly)</i>
		59012315	<i>ETSI ISUP Network AOC - V5.2 enhancement</i> , Issue AA02, PLS FMDOC module <i>A59012315</i>
		59013775	<i>Network AOC: Integrated CGP and CDP</i> , Issue AA27, PLS FMDOC module: <i>A59013775</i> .
	ISNH03	59032878	<i>NAOC on PRI</i> , Issue AA05, PLS FMDOC module: <i>A59032878</i> .
P C A	SN04	59034497	<i>Payment ceiling for Succession Intl. Cable IP</i> , Issue AA32, PLS FMDOC module: <i>A59034497</i> .
	SN05	59039121	<i>NAOC and PCA Feature Interworkings with 3WC, CFx, CXR and HOLD</i> , Issue AA30, PLS FMDOC module: <i>A59039121</i> .
NAOC	SN06	89007454	<i>NAOC German Regulatory Enhancements</i> , Issue AA17, PLS FMDOC module: <i>A89007454</i> .
PCA		89007461	<i>Payment Ceiling Regulatory Enhancements</i> , Issue AA40, PLS FMDOC module: <i>A89007461</i> .
NAOC	SN06.2	A00001927	<i>Line Hardware Metering</i> , Issue AA03, PLS FMDOC module: <i>A00001927</i> .
		A00002938	<i>Full Line HW Metering / Billing Compliance</i> , Issue AA12, PLS FMDOC, module: <i>A00002625</i> .
	SN07	A00002625	<i>Full Line HW Metering / Billing Compliance</i> , Issue AA12, PLS FMDOC, module: <i>A00002625</i> .
		A00002637	<i>NAOC Trunk Metering Enhancements</i> , Issue AA02, PLS FMDOC module: <i>A00002637</i> .
		A00002909	<i>Telekom ISUP (T-ISUP)</i> , Issue AA24, PLS FMDOC module <i>A00002909</i>
		A00004933	<i>Indian ISUP Charging</i> , Issue AA02, PLS FMDOC module <i>A00004933</i>
		A00002638	<i>PCA SW Metering Billing Compliance</i> , Issue AA14, PLS FMDOC module <i>A00002638</i>
		S00002638	<i>Software Metering support for Billing</i> , Issue AA02, PLS FMDOC module <i>S00002638</i>
PCA			
NAOC & PCA			

NAOC	SN08	A00005822	AOC over H.323, <i>Issue AA08, PLS FMDOC module A00005822</i>
		A00006708	Metering on Israeli ISUP for IDDD calls, <i>Issue AA10, PLS FMDOC module A00006708</i>

19.10 Annex A: French NAOc impact

Activating French NAOc service has **1% to possibly more than 100% real-time impact** on GWCs having SPIROU trunks with NAOc metering turned on. There is a negligible real-time impact (<0.01%) on GWCs loads and no impact on GWC which doesn't have SPIROU trunks.

An initial degradation of approximately 1% will be experienced by activating metering for the GWC. The additional degradation then depends on:

- the total number of SPIROU trunks handled by the GWC.
- the percentage of calls on SPIROU trunks generating ITX messages.
- the percentage of calls on SPIROU trunks receiving ITX/TXA messages.
- the amount of traffic running on the various trunks (number of call originations per minute and average call duration).
- the rate at which ITX messages are generated. If the rate of generation is set to a lower value, then more number of ITX will be generated for each calls and the impact on real-time is high.

Assuming an average call holding time of 5 minutes and ITX rate of 1 per minute, the real-time increase for SPIROU calls is roughly estimated at 30%.

Backwards Charging will impact CC real-time performance of a Billing switch (Calling Subscriber or Indirect Access nodes) by a similar factor since the charge information in each received ITX message will be reported to the CM.

GWC static data download time is also increased slightly by the extra tariff downloading.

Therefore, the switch may require re-configuration to ensure that CM and peripherals are not overloaded.

19.11 Annex B: Backward metering generation

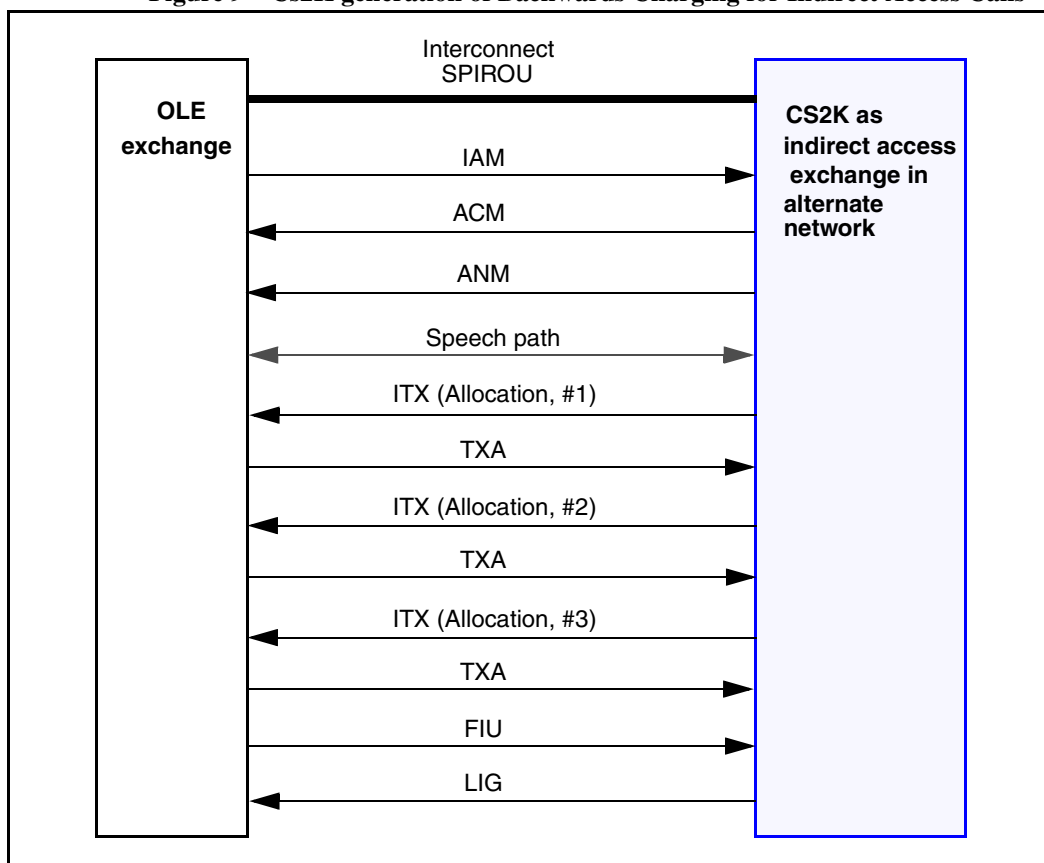
19.11.1 Backward charging on the indirect access (not supported)

The backward charging mechanism should provide the ability to originate ITX messages with charge units determined by on-switch World Metering or NAOC tables and send them backwards on incoming calls over SPIROU trunks to the CS2K.

This functionality would allow an alternate operator to send charge information using ITX messages in order to provide Advice of Charge to a subscriber for Indirect Access calls to the alternate operator.

Figure shows the message flow for the generation of ITX messages CS2K.

Figure 9 Cs2K generation of Backwards Charging for Indirect Access Calls



19.11.1.1 Datafill to control ITX generation

The mechanism used to determine whether to send ITX messages backwards on a SPIROU trunk is similar to that used for the French PRI AOC service, as described in the feature PRI AOC Variants (see document reference [7]). The mechanism uses the World Metering framework to calculate the charge units.

Backwards Charging signalling has a high network impact. Its use to provide a “networked” AOC service for Indirect Access calls where the call charges are determined by the Indirect Access switch, rather than the originating switch, is subject to bilateral agreements between network operators. Its use must be highly configurable.

The ability to generate ITX messages is controlled based on:

- The caller
- The incoming trunk group
- The destination number
- Metering datafill being provisioned for the call

Only if all these checks are passed will Backwards Charging be generated on the call. Otherwise, the call proceeds without Backwards Charging signalling.

19.11.1.2 Originating subscriber based control

The intention of this control is to limit the service to only registered network AOC customers.

The originator of the call is screened and recognized as a valid subscriber to the Backwards Charging (networked AOC) service. The screening uses the existing NETAOCD option in table DNSCRN. For details of the NETAOCD option, see document reference [8].

The DSCNT subfield is used to specify the discount class number to which the customer belongs.

19.11.1.3 Incoming trunk group control

The service must be blocked if the originating network does not wish to support the use of Backwards Charging signalling to provide “networked” AOC.

This may be done on a trunk group basis by datafilling the TELETAXE_NOSIG option in table TRKOPTS against the CLLI of the incoming SPIROU interconnect trunk(s); see section 19.11.1.

19.11.1.3.1 Destination number based control

True “Teletaxe” type calls will receive Backwards Charge messaging from the (terminating) service provider’s switch. This “Advice of Charge” Backwards Charging service from the Indirect Access switch should be blocked for such calls.

The REMOTEAOCD translations option (see section 19.11.1) is used to identify a true Teletaxe call from the destination address.

ITX backwards charging messages are only generated by the CS2K if the translations option REMOTEAO is not encountered in table xxHEAD/xxCODE for the route.

19.11.1.3.2 Metering datafill

The existing DMS metering system which is used to drive ISDN Advice of Charge is used to determine the number of charge units accrued for ITX generation on SPIROU. This system must be activated per GWC by the existing AOC option in table SRVRINV.

The rate at which charge units are accumulated during a call is known as a **tariff**. Different calls require different tariffs. For this reason, the DMS allows the telco to define tariffs which can depend on the following factors:

- The type of originator. This means that a call originated by user A may not have the same tariff as the same call originated by user B.
- The destination number. This means that the tariff incurred by user A may be different, depending on whether A calls user C or user D.
- The network used. This means that the tariff incurred by user A depends on the route taken to reach the called party.
- The time of day and day of the week. This means that when user A calls user B, the call tariff may change with the time of day and the day of the week.
- The **discount**. It is possible to have a per-call discount, depending on the type of originator, the destination number of the call, and the network or route used.

Please refer to the World Metering Rebase (document reference [9]) for full details of the metering system's capabilities.

19.11.1.3.3 ITX frequency control

Similarly to the ISDN Advice of Charge service, the CS2K sends ITX messages periodically, if the Call Charge has increased since the last ITX message, rather than sending a message exactly when a charge period expires.

The existing office parameter SSUTR2_ITX_RATE is used to define the frequency of ITX message generation. SSUTR2_ITX_RATE has a range of 5 to 255 seconds. The default is 20 seconds. For details of SSUTR2_ITX_RATE, see the Office Parameters Reference Manual (document reference [10]).

If the previous ITX has not yet been acknowledged when the CS2K wants to send a new ITX, the CS2K waits and tries again at the end of the next inter-ITX period.

The selected rate is a tradeoff between the network impact of very high messaging rates and the accuracy of the Advice of Charge. SPIROU cannot send charge information at the end of call, so if the ITX rate is lower than the charge rate then some call charges will not be transmitted, resulting in the Advice of Charge being lower than the real call cost.

19.12 Annex C: Background information

19.12.1 Charging Information at Call Set-up time (AOC-S)

When the *AOC-S* supplementary service is activated, the network shall provide the user with call charging information at call establishment. In addition, the network shall inform the served user if a change in charging rates takes place during the call.

The network shall provide the charging information during call establishment or at the latest at call connection. When there is a change in charging rate during the call, the network shall send information about the new charging rate to the served user.

19.12.2 Charging Information During the Call (AOC-D)

When the *AOC-D* supplementary service is activated, the network shall provide the user with call charging information during the active phase of a call. The network shall provide the charging information and transfer it to the user in an appropriate message. The supplied charging information shall be provided as a cumulative charge incurred so far for the call.

If the network has determined that the call is free of charge, the network shall send the user a free-of-charge indication. The network shall not send any further charging information during the call. When the call is released, the network shall send the free-of-charge indication in a call control message clearing the call.

19.12.3 Charging Information at the End of the Call (AOC-E)

When the *AOC-E* supplementary service is activated, the network shall provide the user with call charging information indicating the recorded charges when the call is released. The network shall send the user the charging information in one of the call control messages clearing the call.

19.12.4 Indication of Charge [télétaxe]

This term is used in France in order to describe the supplementary service which informs the user of the charges which have been attributed during the active phase of a call. With other words, it is another term for *AOC-D*. Please refer to chapter “2.3.2 Charging Information During the Call (AOC-D)” on page 39.

19.12.4.1 Total Cost

This term is used in France in order to describe the supplementary service which informs the user of the call charges when the call is released. It is another term for *AOC-E*. Please refer to chapter “2.3.3 Charging Information at the End of the Call (AOC-E)” on page 39.

19.12.4.2 Charging Units

In this variant of AOC, the AOC charging information is presented to the terminal in form of a pulse count. The subscriber or terminal has to know the amount and currency equivalent to one pulse in order to calculate the cost of a call.

19.12.4.3 Currency Units

In this variant of AOC, the AOC charging information is presented to the terminal in form of amount and currency.

19.12.4.4 Functional Protocol

The functional protocol is based on the use of the Facility information element and the FACILITY message, as well as of other specific functional messages specified in clause 7 of Recommendation Q.932.

This protocol is functional in the sense that it requires the knowledge of the related supplementary service by the user equipment supporting it. This facilitates user equipment operation without human intervention by defining semantics for the protocol elements which user equipment can process on its own.

The protocol is symmetrical and is applicable to both basic and primary rate interfaces.

The key characteristic of the functional protocol is that it may operate end-to-end as contrasted with the Keypad Protocol that is local in nature.

19.12.4.5 Keypad Stimulus Protocol

The Keypad protocol is a stimulus protocol providing a means of transferring a sequence of IA5-characters from the user to the network to control supplementary services and indicating network responses to the user. The Keypad protocol is based on the use of the Keypad facility and Display information elements. The Keypad facility information element may be included in the SETUP and INFORMATION messages. The Display information element may be included in any message sent by the network to the user according to Recommendation Q.931.

The Keypad protocol is a stimulus protocol in the sense that it does not require any knowledge about the invoked supplementary service by the user equipment. It may be used in any state of a call and in association with a call for supplementary service invocation. Whatever digits dialled by the user are sent, as such, in a Keypad IE to the network. The keypad facility codes used for the invocation of individual supplementary services are network dependent.

The protocol is applicable to both basic and primary rate interfaces.

In general, the keypad protocol has only a local significance.

19.12.4.6 AOC on request

In this variant of AOC, charging information is not sent for every call that the user originates but only for calls where the subscriber explicitly requests AOC information by adding a respective Facility Information Element (FAC IE) into the Q.931 SETUP message.

19.12.5 NAOC

Network **Advice Of Charge** (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 a charge message over the network (**CDP** and **CGP** on different exchanges¹) or passed internally to the CGP interface (**CGP** and **CDP** on the same exchange²).

¹This is the case where the originating network does not keep any tariff information for the selected carrier

²This is the case where the originating network has included the tariff information for the selected carrier in its local database

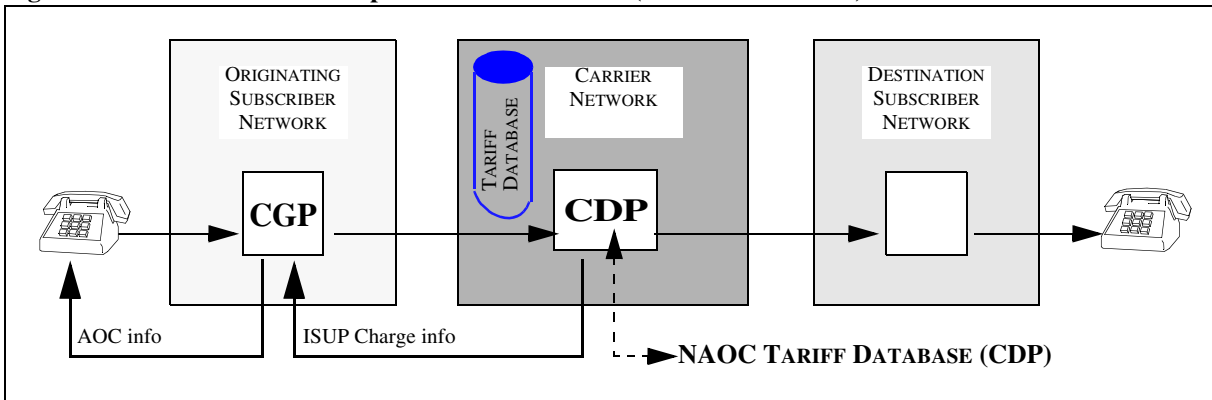
2. **CGP** - The **Charge Generation Point** is an exchange where the received charging information is converted into a format that is delivered to the subscriber.

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.

Based on these types of network nodes, there are two scenarios which have been considered for **NAOC**:

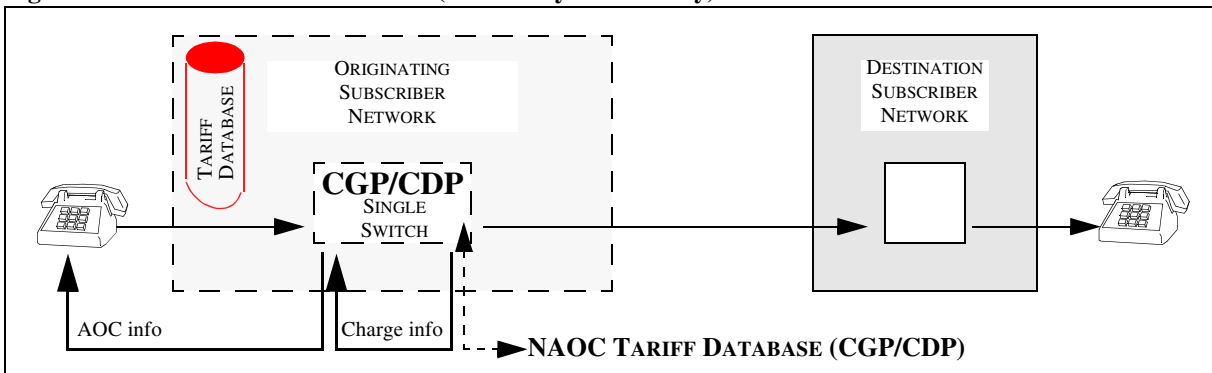
- **CDP** and **CGP** are located in different networks, so that the **CDP** has to send the tariff information over the network boundaries to the **CGP**. Please refer to Figure 2. This scenario will not be addressed by the current activity

Figure 10 CGP and CDP as Separate Network Nodes (not addressed here)



- **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 3. This is the valid scenario which will be addressed by the current activity.

Figure 11 Combined CGP and CDP (covered by this activity)



The decision whether a call has to be tariffed by the originating exchange (combined CGP/CDP functionality) or by another exchange located in an intermediate network (CDP tariffing) is made on a **per call basis**, based on the translations information datafilled at the originating exchange. This ensures that the network structure is dynamic.

19.12.5.1 Interactions with the existing (pre-SN08) metering framework

19.12.5.1.1 Generic

The existing NAOC metering provides the ability to determine the tariff and charge a call in real time. This functionality is available in a single carrier environment (single telco serving the market) and a multiple carrier environment (deregulated telecom market).

After call charges got successfully determined, they can be written into an AMA MC 612 extension based on the state of the SOC NSUP0023.

From an end user point of view, three types of metering features can be supported:

- Line HW Metering for IBN subscribers (CS2K¹ and TDM)
- AOC SW Metering for ETSI PRI (CS2K and TDM), H323(CS2K)
- PCA SW Metering for IBN and V5.2 IBN (both CS2K and TDM)

Call charges can be either determined on the originating local exchange (OLE) or received from another exchange using

- national standards (France)
- ETSI standards (Germany)

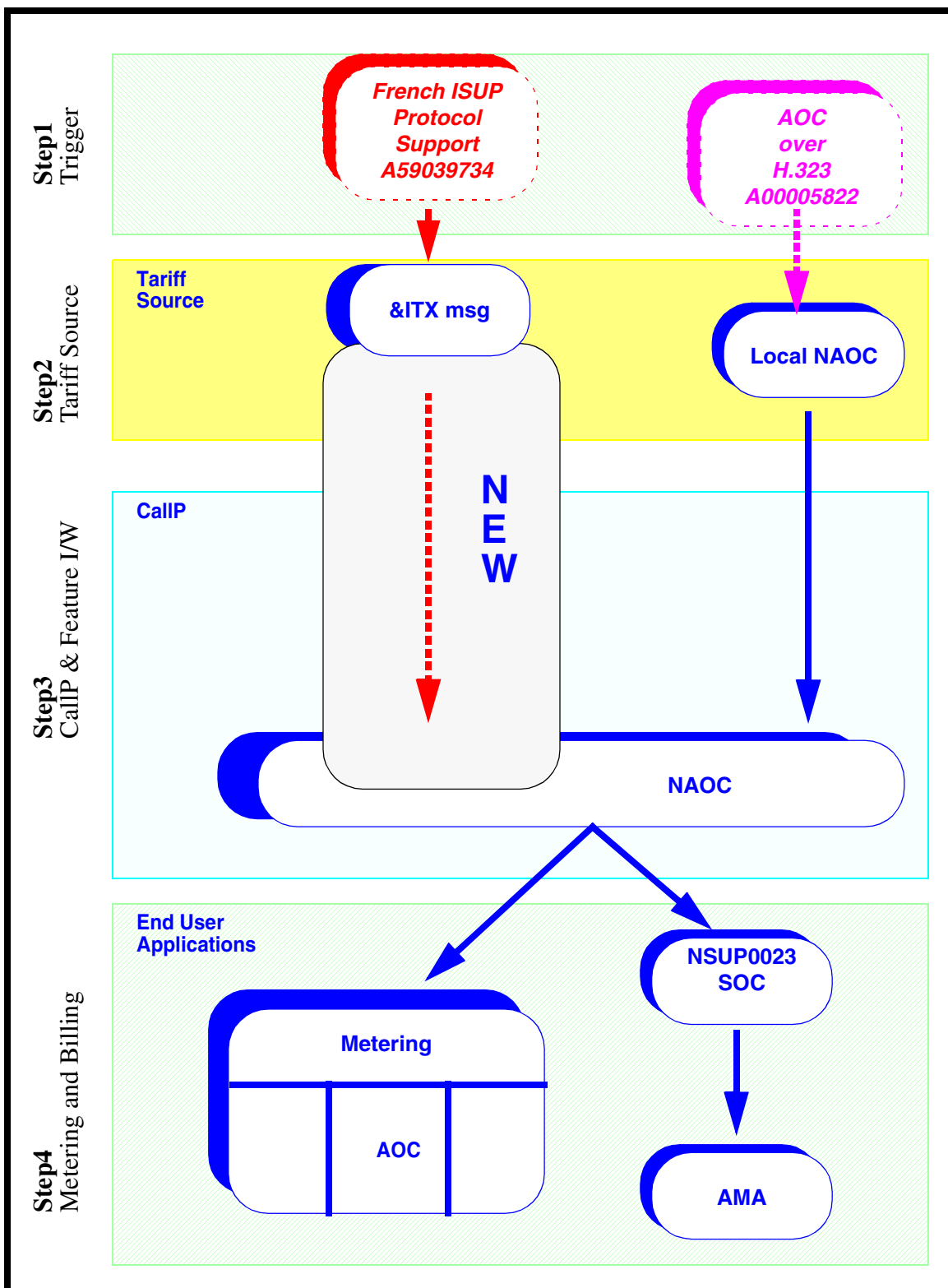
19.12.5.1.2 Current content

The current functionality bridges between the existing features

- French ISUP support provided on the CS2K by a CSA activity on top of A59013177 and 59034482
- AOC over H.323 (A00005822)
- NAOC metering framework on CS2K (A89007454, 59032878)

¹only for MGOK subscribers

Figure 12 How the new content interacts with existing features



20: A00006731 Functional description (FN)

20.1 Feature name

Handle Flash on Exit

20.2 Description

On TMX100 switches, hook flash is only enabled on those RES lines that have flash features assigned. Most customers do not use flash features. RES customers without hook flash features who flash are treated as exiting the current call and receive standard dial tone allowing them to initiate a new call.

When TMX100 sites migrate to ISN04 or later, customers are converted from RES to IBN line functionality and by default have hook flash enabled and will get second dial tone if they Flash (go on/off hook) instead of Exit. This difference in behavior is causing confusion and customer complaints at the Coteor site in Bolivia, the first local exchange migrating from TMX100 to ISN04. Similar complaints are expected when other sites convert (100-150 sites).

The purpose of the Exit on Flash (EOF) option is to resolve these customer complaints and to provide for a more seamless migration from TMX100 to ISN04.

Customer requirement of this activity is to develop a new line option that treats Flash as EXIT for IBN lines.

Without EOF:

- A Calls B
- B Answers
- A Flashes
- A gets Special Dial Tone
- A Calls C
- A Receives Feature Not Allowed (FNAL) treatment

With EOF:

- A has EOF option
- A Calls B
- B Answers
- A Flashes
- A and B Disconnect

A gets Dial Tone
 A calls C
 A to C call is established

This feature uses line option datafill. The advantages of offering this as a line option are:

- consistency with the current FIG (Flash Ignore) option
- ability to define option compatibilities using the OPTOPT table

20.3 Hardware Requirements or Dependencies

There is no hardware dependency. The option can be added to any line with an LCC of IBN.

20.4 Software Requirements or Dependencies

None.

20.5 Limitations and restrictions

EOF feature is only applicable to IBN lines in NA and WT.

EOF feature is not compatible with the following options:

CHD, CNF, CWI, CWX, CWT, CXR, FXR, DCBX, HLD, LDSA, LDSO, LDSR, LDST, LNPTST, MPB, PCWT, PRK, 3WC, 3WCPUB, VOWDN.

20.6 Interactions

Call Waiting Originate (CWO) and Dial Call Waiting (CWD) are both features compatible with the EOF feature. If another agent imposes CWT on an agent with EOF, this agent still has the ability to flash to the waiting call and maintain the original call instead of exiting.

A has EOF option
 A Calls B
 B Answers
 C with CWO/CWD calls A and imposes CWT on A
 A Flashes
 A to C call established while B is on hold
 A flashes again and A to B call established while C is on hold

Timed-release disconnect (TRD) timing is supported by EOF. If a call is setup for TRD timing with EOF and the terminating agent flashes, the terminating agent is reconnected to the originating agent instead of exiting.

A has EOF option

B calls A over IT trunk (see NTP 297-1001-190 for other TRD call scenarios)

A flashes

A to B call maintains connection

20.7 Applicable customer facing sections

Fault Management

Logs

Alarms

Configuration

Data Schema

___X__

User Interface

Element Management

Security

Service Order

___X__

Office Parameters

Accounting (includes AMA billing)_____

Performance (includes operational measurements)_____

21: A00006980 Functional description (FN)

21.1 Feature name

AMA Module Code 130 Flexibility

21.2 Description

This activity in ISN08 release is targeted to provide an optionality by datafill which allows the customer to append the Module Code 130 on tandem or terminating DMS-100 offices when a call is normally clear forwarded before the terminator goes off hook.

In fact, the AMA Module Code 130 is known as Termination Attributes Module and is appended to the AMA record when a treatment is applied to rejected or failed calls. A rejected call is a call that has not been answered and has been routed to a treatment or an announcement. There was an update in WT14 to conform the MC130 generation to this definition (that is also NTP 297-9051-800 definition). By this update, generation of MC130 was prevented for the calls that are clear forwarded before answer (not rejected and treated).

But, on this update, the Case 030316-85514 "Abort Swact due to Changes in AMA Module Code 130" was raised by a customer with the requirement to append MC130 again for the calls clear forwarded before the terminator goes off hook as well as the rejected calls. To meet this requirement, the patch FBB45 (for WT15 and WT17) was provided to remove the WT14 update and to append MC130 as requested by the customer.

The main purpose of this activity is to remove the need for patch FBB45 and implement the same functionality under optionality control by datafill.

This optionality is provided by a new AMA option in Table AMAOPTS. The name of the new option is MC130_FOR_CLF and it is set to ON to activate this feature. If it is set to OFF, the MC130 is appended for only rejected calls as before.

21.3 Background Information

The following information is provided by the NTP 297-9051-800 "DMS-100 MMP AMA Reference Guide".

AMA behavior for rejected calls:

For rejected calls, the record generation depends on whether the DMS is acting as:

- an originating node
- a terminating node

– a tandem node

- **Originating node:**

Interworkings from a line origination to the following agents are supported by the SOC option BILL0003: Lines, Trunks, Attendant Consoles, and digital recorded announcement machines (DRAM).

The call must route to treatment at this node so that the reject information is available. For such calls, the following information is captured:

- Representation of the Treatment Code as applied to the originator.
- Treatment origin and application. That is, where the call was rejected and where the treatment was applied.

- **Terminating node:**

Interworkings from a trunk termination to the following agents are supported: Lines, Attendant Console and DRAM.

This is supported if a treatment is set at the terminating node. This can result in a backwards release being sent from the terminator to the originator. For such calls the following information is provided:

- Representation of the Release Cause indication as given in the backwards release message.
- Treatment origin and application. That is, where the call was rejected and where the treatment was applied.

A terminating node can apply the treatment locally if required by datafill within table TMTMAP. In such a situation, the provision of the release cause is replaced by a numerical representation of the applied treatment.

Note: In a situation where a backwards release has been sent and it is unable to determine the true release cause, a release cause of 16 (Normal Call Clearing) is used.

- **Tandem node:**

Support is only provided for calls where either treatment is applied at this node or the release message is received by the CM (for example, interworking trunk types: BTUP-ETSI). No support is provided for calls where the release message is bounced by the XPMs (for example, same trunk types: BTUP-BTUP). The provided information is the same as when the DMS-100E switch acts as a Terminating Node.

The information for rejected call recording is contained in the Module Code 130 appended to Structure Code in the main AMA record.

Existing behavior for Module Code 130:

The Module Code 130 contains the treatment applied to the call or the CCITT release reason (as appropriate) for rejected or failed calls.

Module code 130 is only produced with Module 025 (unanswered call), since a treated call has to be an unanswered call.

Table 1 Module Code 130 Format

Information	Table Number	Number Of BCD Characters
Identification for Termination Attributes Module Code 130	88	4
Facility Release Cause	338	6
Call Characteristic	339	4

Module Size: 7 Bytes.

Field 88 ‘Module code’ identifies a module of data fields that can be appended to the record.

Field 338 ‘Facility Release Cause’ contains the definition of reject reason or treatment.

The range 500-995, is a specific numerical representation of a treatment or release reason, depending on the value of the Call Characteristic Field (339). If the Call Characteristic = 004, then the termination cause value represents the DMS treatment applied to the call. If the Call Characteristic = 005, then the termination cause value represents the CCITT release reason given in a backwards release message. For the mapping between the numerical values and treatment names, please refer to the NC0507FN document for the activity “Bellcore AMA (EBAF) Reject Call Recording”.

Table 2 Field 338-Facility Release Cause

BCD Character	Meaning
1	Source Of Termination Signal 0 = Character Not Used (used) 1 = Calling Party 2 = Called Party 3 = Originating Party 9 = Unknown
2	Context Of Termination Cause 0 = Character Not Used 1 = Completed 2 = Not Completed (used) 9 = Unknown

Table 2 Field 338-Facility Release Cause

BCD Character	Meaning
3-5	Termination Cause 000 = Character Not Used 001 = Busy 002 = No Circuits 003 = Ringing 500-995 = Mapped Termination Reason 999 = Unknown
6	Sign (hex C)

Field 339 ‘Call Characteristic’ is used to record whether treatment has been applied locally (004) or externally (005) in Module 130. These values are used to interpret the numerical values defined in the termination cause field (338).

Table 3 Field 339-Call Characteristic

BCD Character	Meaning
1-3	001 = Intra-site 002 = Intra-citywide 003 = Least Cost Routing 004 = Treated Locally 005 = Treated Externally 006 = IN standard announcement 007 = Special announcement 008 = IN return error 009 = IN reject 999 = Unknown
4	Sign (hex C)

Necessary provision for MC130:

The capture of billing information from rejected calls is triggered by the option FLEXRJCT in table AMAXLAID and/or FLEXAMA. This option is referenced from the related translation tables. The FLEXRJCT option has the sub-field REJECTMOD. If this is set to Y, it appends the module 130 to the triggered AMA record. However only FLEXRJCT does not trigger an AMA record by itself. Also, the related SOC option must be active. The Order Code of this SOC option is BILL00003 and the name is “AMA Reject Call”.

A SOC (Software Optionality Control) option is a grouping of one or more functionalities to form a customer controllable unit. The state of an option (IDLE or ON) may be changed directly by the customer, on site, causing the option’s component functionality to change state.

If the FLEXRJCT option is encountered in translations, an AMA record will be produced for rejected calls. If the SOC option BILL0003 is ON and the boolean datafilled with FLEXRJCT is set to Y, Module Code 130 will be appended to the record.

21.4 Desired Behavior in this activity

In addition to the existing conditions given above to generate the MC130, it is requested to append this module on the transit and terminating DMS-100 nodes for the calls clear forwarded before the terminator goes off hook (i.e. no treatment is applied and a normal clearing cause produced). This requirement has already been provided by the patch FBB45 for a customer (for Case 030316-85514). The aim of this activity is to remove the need for the patch FBB45 by providing the same functionality under optionality control by datafill.

For this purpose, a new AMA option is created in the Table AMAOPTS. The name of the new option is MC130_FOR_CLF and it is set to ON to activate this feature. The default value is OFF for this option.

Figure 1 New AMA option MC130_FOR_CLF in Table AMAOPTS

TABLE: AMAOPTS OPTION SCHEDULE ----- ... MC130_FOR_CLF ON

While activating and deactivating this option, a caution is printed as given below to indicate the change in the functionality:

For activation (ON state):

“This change results MC130 generation for unanswered calls clear forwarded normally”

For deactivation (OFF state):

“This change prevents MC130 generation for unanswered calls clear forwarded normally”

(For detailed information, please refer to the CN section of this activity.)

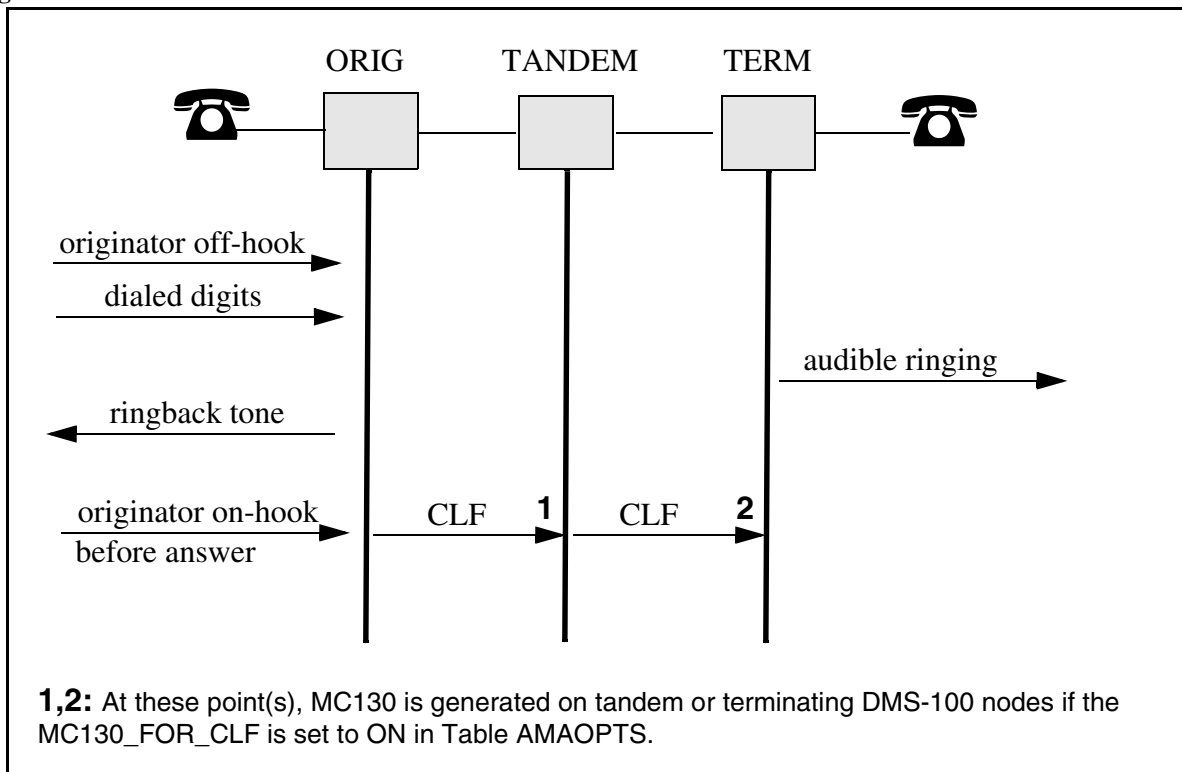
When the necessary provision (given in the “Section. 1.4 -Background Information” under the title “Necessary provision for MC130”) is done to generate the MC130 and the new option MC130_FOR_CLF is activated, then the MC130 is appended to the generated AMA record for the clear forward messages (CLF) before answer as well as the rejected calls. If the MC130_FOR_CLF is set to OFF, the MC130 is appended for only rejected calls as before.

Also, the option MC130_FOR_CLF is automatically set to ON over ONP if the patch FBB45 is active in the old side. This provides the continuity of the feature in the new side after transition. But this auto-activation facility is only for three releases from ISN08 (i.e. until ISN11).

Clear Forward Message (CLF) is the message indicating that the calling party (originator) goes on-hook in a call. When a PDTC receives a Release message, it sends a CLF message to CM to inform it for calling (originating) party release.

The following figure shows the case of the activated MC130_FOR_CLF option:

Figure 2 Functional Behavior



In this case: when the call is clear forwarded before the terminating agent goes off hook, the Module Code 130 is appended to the AMA records generated on the tandem or terminating DMS-100 offices.

The patch FBB45 was requested and tested with the following interworkings:

- IBN-ISUP(V2)-ISUP(V2)-IBN
- IBN-BTUP-BTUP-IBN
- IBN-DPNSS-DPNSS-IBN
- IBN-PRI-ISUP(V2)-IBN
- IBN-RBTUP-ISUP(V2)-IBN
- IBN-DPNSS-ISUP(V2) -IBN
- IBN-ISUP(V1)-PRI-IBN
- BRI-ISUP(V1)-PRI-IBN
- BRI-BTUP-BTUP-EBS
- EBS-DPNSS-ISUP(V2)-BRI

21.5 Hardware Requirements or Dependencies

No new customer hardware requirements or dependencies are introduced in this feature.

21.6 Software Requirements or Dependencies

No new customer software requirements or dependencies are introduced in this feature.

21.7 Limitations and restrictions

None.

21.8 Interactions

This feature uses the existing AMA/Billing framework and the existing components of this framework (MC130) with no change in their existing structures to realize customer's requirements.

21.9 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)_____

21.10 Glossary

Table 4

Term	Description
AMA	Automatic Message Accounting
CCITT	International Telegraph and Telephone Consultative Committee
CLF	Clear Forward Message
DMS	Digital Multiplex System
DRAM	Digital Recorded Announcement Machines
MC130	Module Code 130
MMP	Multi Market Product
SOC	Software Optionality Control
WT	World Trade (Non- North America contacts responsible for introducing products or solutions into new markets. Here it is used to identify a layer of the DMS software intended for the World Trade market. WT14, WT15 and WT17 are the particular releases of the WT software layer.

21.11 Recommended Reading/References

- Request For Feature (RFF) 292 ‘Module 130 Optionality’ that is accessible from the link <http://plm-pnd.europe.nortel.com/PLM/>.
- Design Document NC0507FN for the activity “Bellcore AMA (EBAF) Reject Call Recording”.
- Design Document AG5040FN for the activity “AMA Billing Enhancements for Indirect Access, CLI Capture and Rejected”.
- NTP 297-9051-800 “DMS-100 MMP AMA Reference Guide”

22: A0007038 Functional description (FN)

22.1 Feature name

Intl R2 CAS Framework - Flexible Digit Map support

22.2 Description

In the existing CS2K International FDCP CAS signaling system, when there is an incoming call, the digits are requested individually and the Media Gateway reports every digit as an event to the Media Gateway Controller. There is no support for Digit Collection using Digit Map mechanism. Systems that do not use Digit Map mechanism are very inefficient and create a lot of unnecessary traffic between Media Gateway Controller and Media Gateway. In order to improve digit collection efficiency, Digit Map mechanism should be implemented.

This activity provides:

- Digit Map mechanism for reporting digits from Media Gateway to Media Gateway Controller maintaining the end user Digit Collection control through CM tables DGHEAD and DGCODE.
- Framework for Digit Map mechanism so that other applications can reuse this component to implement Digit Map mechanism in the future.
- Digit Map mechanism for Overlap and End to End signaling modes.

Figure 1 Existing Digit reporting Mechanism

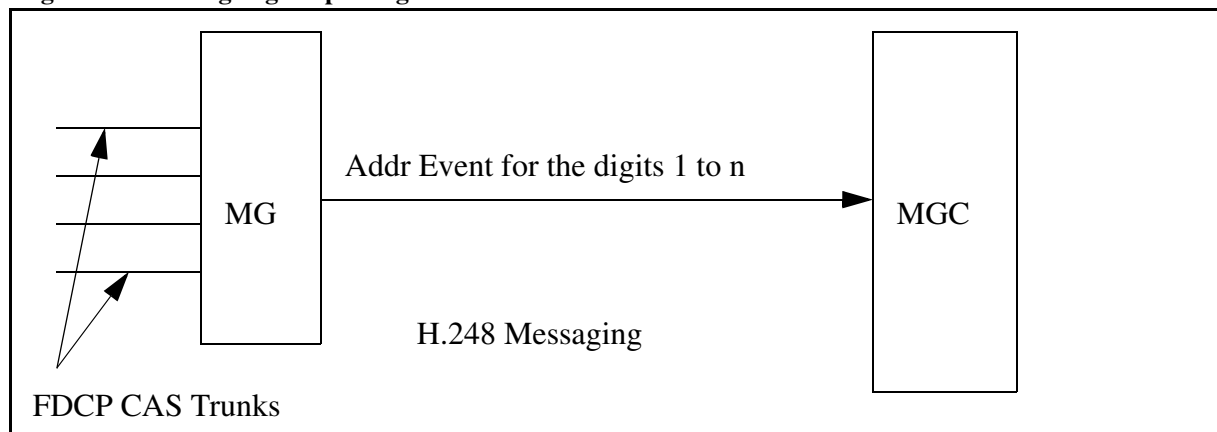
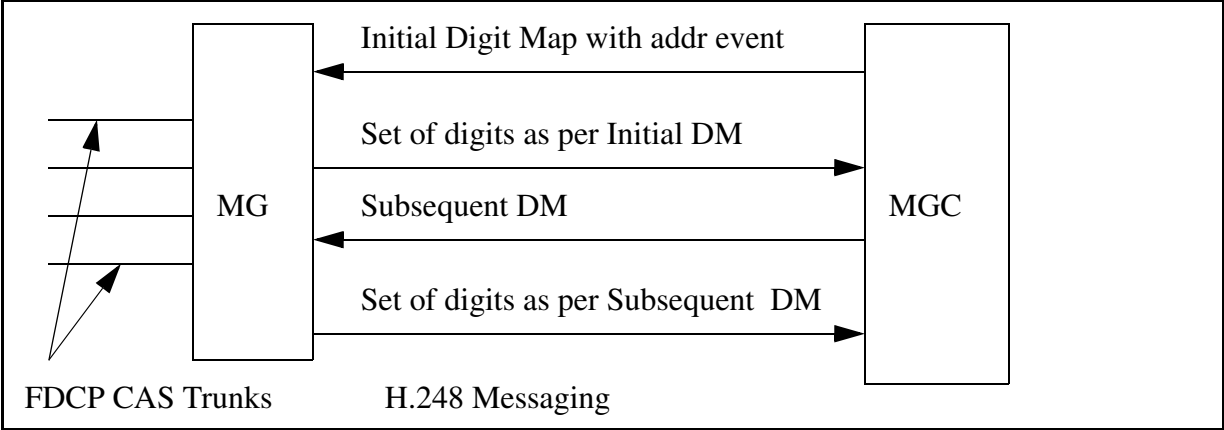


Figure 2 Digit Reporting after DM mechanism implementation



For a given trunk group, the DM behavior can be controlled via the CM tables DGHEAD and DGCODE. Option DIGCOL points to a DGHEAD instance which determines the DM behavior. Note that if the DM functionality for a particular trunk group is not required, the DIGCOL option should not be data filled in table TRKSGRP. The following example shows how it could be achieved.

The DGHEAD instance which defines the DM rules should be defined in table DGHEAD (as shown in Figure 3)

Figure 3 Definition of DGHEAD instance

TABLE DGHEAD
LCLCOLL 10 10 19 N NONE BOTH

Following changes should be done in TRKSGRP to enforce the DM behavior for FDCP CAS trunk with a CLI CASIC. DIGCOL option should point to a DGHEAD instance defined (LCLCOLL in figure 4)

Figure 4 Example showing the datafill for TRKSGRP

TABLE TRKSGRP
CASIC 0 P30CAS FST N NILTYPE Y 2W N NIL ITALY_RS
FDCP ITALCAS1
ITAL_TRT ITALY_VR ITALY_TM DTMF LNK NOVERLAP STAND
DEFAULT (DIGCOL LCLCOLL) \$

In table DGCODE, the intended DM behavior for different combinations of incoming digits are defined for a given DGHEAD instance. Field DGCLSEL in DGCODE determines the MGs behavior on receiving the specified digits. The possible selectors are

22.2.1 COLL - Collect a fixed number of digits

For a datafill shown in figure 5, if the digits received on CASIC are between 10 and 20, it instructs the MG to collect 6 digits and then report it to the MGC.

Figure 5 DGCODE datafill for COLLECT selector

TABLE DGCODE LCLCOLL 10 20 COLL 6 N

22.2.2 RAN - Collect a Range of digits

For datafill shown in figure 6, if the digits are between 40 and 50, the MG reports the digits to MGC if the number of digits received are in the range 3 to 8.

Figure 6 DGCODE datafill for RANGE selector

TABLE DGCODE LCLCOLL 30 40 RAN 3 8 5 N

22.2.3 CONT - Continue with a DGHEAD instance

For datafill shown in figure 7, if the digits received are between 40 to 75, the analysis would be continued as per another DGHEAD instance NATCOLL. Also REPORT field filled as N indicates that, the received digits need not be reported to CM before analyzing NATCOLL. Y in REPORT field indicates that, the received digits should be reported to the CM and then the analysis is continued.

When the REPORT field is datafilled as Y, the digits will be reported and the subsequent DM will be sent to the MG. This subsequent DM will be formed based on the DGHEAD instance with which it continues (i.e., NATCOLL in figure 7)

Figure 7 DGCODE datafill for CONTINUE selector

TABLE DGCODE LCLCOLL 40 75 CONT NATCOLL N NONE

22.2.4 REP selector - Report

For datafill shown in figure 8, if the digits are between 80 and 90, the MG reports the collected digits to MGC.

Figure 8 DGCODE datafill for REP selector

TABLE DGCODE LCLCOLL 80 90 REP

22.3 Hardware Requirements or Dependencies

Not Applicable.

22.4 Software Requirements or Dependencies

Not Applicable.

22.5 Limitations and restrictions

- Even though option COL2STEP could be datafilled in DGCODE table, for FDCP CAS platform, the Digit Map element won't be built for this tuple.
- For FDCP CAS platform, only 19 DGCODE tuples per DGHEAD tuple is supported.
- The maximum length of a Digit Map element supported is 31.
- DGTABLES SEND command is not supported to download the DGHEAD/DGCODE data to the GWC.

22.6 Interactions

Not Applicable.

22.7 Glossary

Table 1

Term	Description
CAS	Channel Associated Signaling
CLLI	Common Language Location Identifier
CM	Computing Module
CS2K	Call Server 2000
DC	Digit Collection
DGCODE	Digit Analysis Control Definition

Table 1

Term	Description
DGHEAD	Digit Analysis Head
DM	Digit Map
FDCP	Flexible Digit Collection Platform
GWC	Gateway Controller
MG	Media Gateway
MGC	Media Gateway Controller

22.8 References

- a. BC2256FN : International Digit Analysis Tables
- b. BF0974FN : International Digit Analysis

23: A00007040 Functional description (FN)

23.1 Feature name

Intl R2 CAS Framework - Error handling support

23.2 Description

This SN08 activity provides error handling support for FDCP CAS in CS2K. This feature handles errors encountered and reported by the Media Gateway (MG) to the Media Gateway Controller (MGC) during CAS call processing.

The various error scenarios generated by the CAS components in the MG has been classified into the following three categories.

1. **NACK** : NACK errors occur when the H.248 message fails a parsing or validation check. When MG is the receiver of the H.248 message and while processing the message it realizes that
 - the request is syntactically invalid or
 - the signals or events cannot be supported or
 - the signals cannot be applied,

the H.248 message is rejected and the MG reports the error to the MGC. It does so by sending a reply to the MGC including an ErrorDescriptor in the reply message. These reply messages with the error descriptor in them are referred to as NACK.

In the present implementation, for FDCP CAS, any NACK reported causes the call to be released irrespective of the state of the trunk.

This feature provides handling of NACKs for FDCP CAS based on the state of the trunk and the exception reason received. The action can be either to re-attempt or take down the call and generate logs. The following tables show the action taken for the various MGC exceptions in different states.

2. **CAS failure event in the observed events descriptor** : A CAS failure event is defined in every CAS package to enable the MG to report failures to the MGC, encountered while performing actions requested by MGC. This feature provides the functionality for the MGC to request a casf event of the package being used while sending the H.248 message.

If an error is detected by the MG a casf observed event will be built in the Observed Event Descriptor and sent to the MGC via a Notify message. These casf observed events contain an error code parameter based on which the respective error handling is done.

3. **NotifyCompletion parameter in Signal Complete event(g/sc) with an indication of signal not completed** : Since CAS Register Signalling duration is not instantaneous, the MGC can request the MG to be informed when a signal has successfully completed or has not completed due to a failure.

The optional parameter NotifyCompletion allows the MGC to indicate that it wishes to be informed of normal completion, being interrupted by an event, being interrupted by a new signals descriptor and not completed for other reasons.

If an error is detected during outpulsing and the g/sc had been previously requested for the Register signal, the MG will send a Notify message to the MGC to inform that signal playout has not finished (or was never started) due to a failure.

In the current implementation this event g/sc has been used only for bcasaddr package.

This feature will implement g/sc for the icasc. There are only two events implemented here. TO is timeout implying that the signal was completed successfully and nothing further is done on receiving this parameter in the notify message. NC implies that the signal could not be completed whereby it is sent for further treatment and the call is released by sending an SMP release message to the core.

23.3 Logs generated

The logs generated on encountering these errors are basically trunk logs. The log generated for bcas/SME is as follows :

CKT CAS3 1,

REASON: PTS ERROR CODE

DATA = 3902 0004 2C00 0006 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000

The above log indicates an FDCP protocol error for line signalling for the event bcas/SME in SZA_SENT state.

23.4 Hardware Requirements or Dependencies

N/A

23.5 Software Requirements or Dependencies

N/A

23.6 Glossary

Term	Description
CAS	Channel Associated Signalling.
CS2K	Call Server 2000
FDCP	Flexible Digital CAS Platform
MG	Media gateway
MGC	Media Gateway Controller
NACK	Negative Acknowledgement
NAPTS	North American Per Trunk Signalling
PVG	Passport Voice Gateway
LSF	Line Signalling Function

23.7 References

1. World CAS homepage

<http://pndinfo.europe.nortel.com/worldcas/>

Courses ->

1. CallMach Interface (GLUE)
2. CAS Domain Course
3. FDCP Architecture Course

2. CAS Livelink

<http://eur-livelink.europe.nortel.com/livelink/>

3. NAPTS error handling feature A00003506

24: A00007146 Functional description (FN)

24.1 Feature name

CM Audits and Carrier grade for Intl. FDCP CAS on CS2K

24.2 Description

This activity provides Core audits and Carrier Grade functionality for FDCP CAS on CS2K. The following items are covered in this activity.

- Core Audits
- CM maintenance actions
- GWC maintenance actions
- PVG maintenance actions

This activity applies generically to H.248 trunk Gateways although it is validated with only the PVG.

24.2.1 Core Audits

24.2.1.1 Background

The activity '59015654 -Disabling trunk audit functionalities for Call Server trunk maintenance' disabled audits for all the trunks that reside on the gateway. Currently, the trunk audit functionality is not enabled for FDCP CAS trunks on the GWC.

This activity enables core trunk member audit for FDCP CAS trunks on the GWC.

This causes the audit system to recover trunk members that have state mismatches. As a result, the following audit logs are generated for FDCP CAS trunks.

- AUDT108 - this is generated when a trunk audit discovers that a trunk without data is other than TK_UNEQUIPPED or when the trunk state does not match the condition bits.
- AUDT109 - this is generated when the trunk audit corrects trouble conditions.
- AUDT110 - this is generated when a trunk audit detects a terminal trunk state that is invalid.

These are the same set of logs that are generated for legacy FDCP CAS trunks.

24.2.2 CM Warm restart and GWC Warm Swact

Currently, FDCP trunks on the GWC involved in unstable calls are in CPB (Call Processing Busy) state after a core Warm restart and also on GWC warm swact.

During CM warm restart or GWC warm swact, the CM stops call processing, informs the GWC that a maintenance event has occurred and clears unstable calls and retains stable calls.

This activity recovers the FDCP CAS trunks that are involved in unstable calls after CM Warm restart or GWC swact. In the current implementation, the audit that runs to clear unstable calls recovers ISUP, PRI and PTS trunks only. This implementation is extended to include FDCP CAS trunks.

24.2.3 Other Maintenance activities

The following table gives the maintenance activities that are tested and verified.

Table 1 Expected behaviour of the maintenance activities

Type of Maintenance	Activity	Expected behaviour
CM Maintenance	Cold Restart	Stable and unstable calls are brought down. Trunks become IDL.
	Reload restart	Stable and unstable calls are brought down. GWC restarts and Trunks become IDL.
	Norestartswact and mteswact	Similar to Warm restart. Unstable calls are brought down. Trunks become IDL.
	BuSY	Trunk goes to BSY state.
	Return To Service	Trunk becomes IDL and available for Service.
	Force ReLeaSe	Trunk goes to BSY state and is NOT available to make calls.
	Installation BSY	Trunk goes to INB state and is NOT available to make calls.
GWC Maintenance	Warm Swact	Unstable calls are brought down. Trunks involved in unstable calls become IDL. Stable calls stay up. Active unit of GWC becomes Inactive and Inactive unit becomes active.
	Cold Swact	Both Stable and unstable calls are brought down. Trunks become IDL. GWC restarts. Active unit of GWC becomes Inactive and Inactive unit becomes active.
	Restart	Similar to Cold Swact
	Node bsy/rts	Similar to Cold Swact

Type of Maintenance	Activity	Expected behaviour
	Loss of Communication between GWC and CM	Stable calls stay up and Unstable calls are brought down.
PVG Maintenance	Loss of Communication between PVG and GWC	All calls are brought down. GWC recovers using SSC Hearbeat recovery.
	Carrier Reset	All calls are taken down. All trunks go to Carrier FailLure (CFL) state.

24.2.3.1 PVG testing

- Simultaneous swacts - Core + GWC
- PVG Swact
- PVG - Robustness, Congestion/Overload, VSP reset,TDM and IP reset.
- Support of a maximum of 1024 endpoints by the GWC & PVG.

24.3 Hardware Requirements or Dependencies

PVG 15K with VSP3o Card

24.4 Software Requirements or Dependencies

None.

24.5 Limitations and restrictions

- As PVG load was not available, PVG testcases are moved to ICAF. No PVG testcases are executed in IT.

24.6 Interactions

Not Applicable

24.7 Glossary

Table 2 Glossary

Term	Description
CAS	Channel Associated Signaling
CS2K	Call Server 2000
FDCP	Flexible Digital CAS Platform
GWC	GateWay Controller
ISUP	ISDN User Part

Table 2 Glossary

Term	Description
PRI	Primary Rate Interface
PTS	Per-Trunk Signaling
PVG	Passport Voice Gateway
SSC	Service State Controller
TDM	Time Division Multiplexing
VSP	Voice Signaling Processor

24.8 Reference

1. DMS-100 MMP Log Report Reference Manual Volume 2 of 7

25: A00007242 Functional description (FN)

25.1 Feature name

Dial Plan Enhancement for ETSI MWI TCAP

25.2 Description

In SN08, a new succession component, the SPC (Session Policy Controller) is being introduced. Its purpose is to provide the capability to apply policies during call-processing, e.g. policy-based codec selection, connection admission control etc. In general the policy may be implemented on the SPC itself, or (in the future) the SPC may communicate with other devices, such as intelligent middleboxes, in order to apply the policy.

In SN08, the SPC will support exactly one policy, that of Network Resource Reservation, using Virtual Connection Admission Control (VCAC) as the enforcement mechanism. Hence counting of available resource across Limited Bandwidth Links (LBLs) and connection admission decisions will be carried out on the SPC, instead of being done on the GWCs as in SN07 (SN07 feature A00002512). The SN08 GWCs communicate with the SPC to determine whether a call can be set-up. This will allow LBLs to be shared across different GWCs.

The SPC will reside on the NGSS platform. In SN08, the SPC encompasses a Topology Server application. In order to carry out VCAC, middlebox/zone topology information must be provisioned both into the SESM and into the SPC's Topology Server. The network configuration is shown in figure 1.

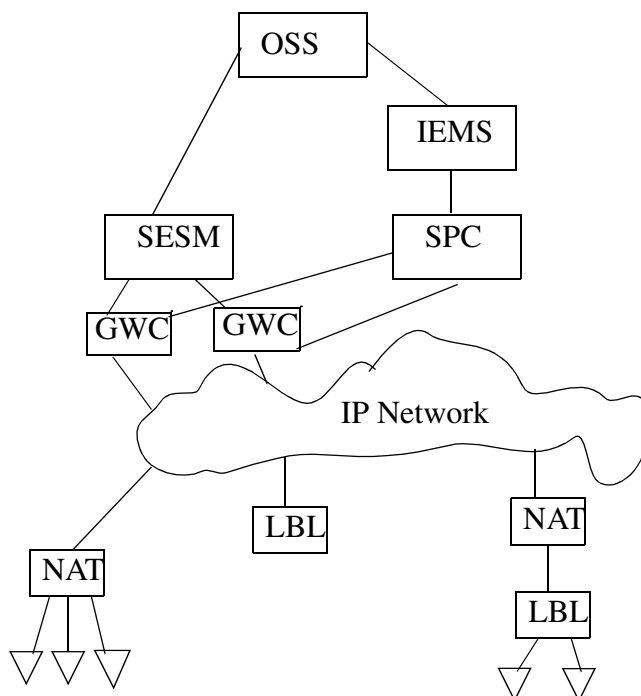
The SPC (Topology Server) will not communicate directly with the SESM. In addition there is no Succession flow-through provisioning interface to both systems. Hence the user (ie OSS/GUI user) is responsible for provisioning identical NAT and LBL topology information into both the SESM and the SPC. If identical information is not input into the two systems, VCAC may not work correctly.

For the GUI interface, the user should provision the information first into SESM and then into the SPC. It is important that the information is provisioned in the same order into each system. In particular, adding/deleting NATs & LBLs should be carried out identically in both systems. For example this could be achieved by adding an LBL to SESM and then to SPC, followed by adding the next LBL to SESM and then the SPC etc.

Hence in SN08, feature ACTID A00007242 covers the modifications required in SESM to integrate with the SPC and to provide provisioning for GWCs which support external counting. The resulting functional changes/additions are described in this document.

- Related activities are:
- ACTID A00007398_SPC_Topology_Manager
- GWC modifications for provisioning for external counting

Figure 1 SN08 Network Configuration with SPC



The user operations provided by this feature which affect the GUI client are:

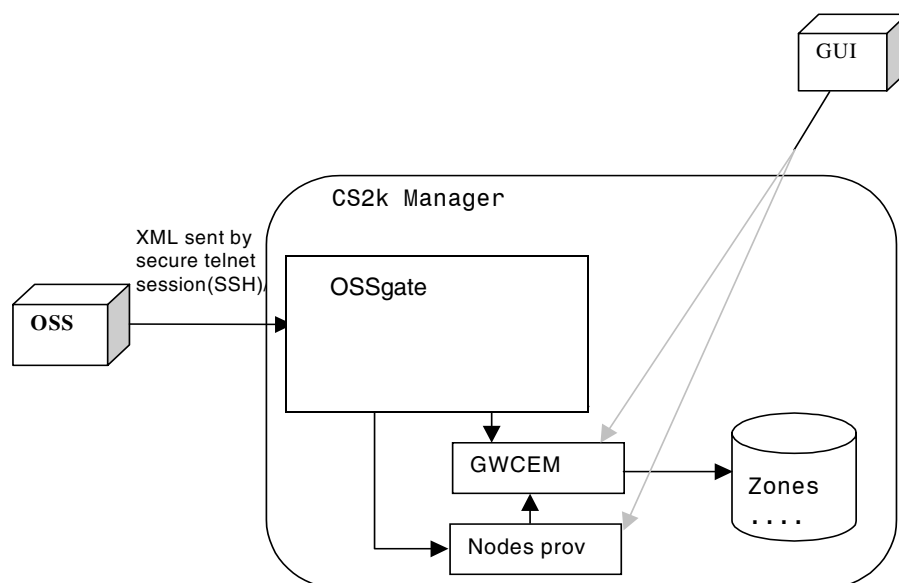
- Provide new GUI to set/change SPC parameters:
 - SPC name
 - SPC IP address

If there is only one supported protocol type and version in SN08 then these will be selected by default and the selections disabled.

- Provide new GUI to set Network VCAC on/off. If Network VCAC is set to 'on' (this requires an SPC to be provisioned), a warning message is provided indicating that:
 - VCAC counting will now be done on the SPC
 - all GWCs and XA-core should be at version SN08 (or above)
 - Reversion to internal counting ('Basic VCAC') is provided on a best effort basis

- Modifications to the existing GWCEM GUI as follows:
 - NAT and LBL panels will be situated on a new ‘Network Zones’ tab
 - It will be possible to provision (add/change/delete) a Network Zone which contains a NAT and an LBL. These Zones will be displayed on a new composite ‘NAT & LBL’ panel on the new ‘Network Zones’ tab
 - VCAC counting will now be done on the SPC
 - all GWCs and XA-core should be at version SN08 (or above)
 - Reversion to internal counting (‘Basic VCAC’) is provided on a best effort basis

Figure 2 GUI Client and OSSGate interfaces



25.3 Hardware Requirements or Dependencies

No new hardware is required or introduced by this feature. The application components provided by this feature execute as part of the SESM.

25.4 Software Requirements or Dependencies

Dependencies:

- CR.xxx: Extend Gateway Controller to support SPC provisioning and Network VCAC

25.5 Limitations and restrictions

- No MCS in SN08, but will be required in future releases

-
- Only one SPC per CS2k in SN08, but may be more in future releases
 - VCAC will be supported with SPC and without SPC.
 - There will be no provisioning connection between SPC and SESM in SN08. All topology information must be provisioned first into SESM and then into the SPC.
 - Topology data transfer from SESM to SPC when SPC is commissioned will be done manually using existing SESM GUI/OSS interfaces and minor interface enhancements to support bulk query of topology data. Automatic bulk data transfer from SESM to SPC will NOT be provided.
 - SESM will not provide an 'undo' capability to the GUI/OSS user.
 - In order to facilitate the flow-through provisioning function carried out by the OSS, each SPC command must map to the same SESM command.
 - Centralized authentication of passwords is not provided by base platform.
 - SPC will not co-reside with any other NGSS based application.
 - Bandwidth on-demand requests are incompatible with VCAC solution.
 - Upgrade to SN08 should be carried out as described in and limitations on operation of VCAC during upgrade as described there will apply.
 - Once Network VCAC is switched on, the SESM will remove any topology provisioning constraint checks which apply to Basic VCAC (internal counting). If Network VCAC is subsequently switched off, the internal counting checks will NOT be restored. It is not recommended to switch Network VCAC off once it has been switched on. Also, if it is switched off, Basic VCAC will only work correctly if the topology still meets the Basic VCAC/'internal counting' topology constraints. In normal use it is expected that Network VCAC will be switched on as soon as the upgrade and soak process is complete and SPC commissioned and will not be switched off.

25.6 Interactions

The following existing GUIs have been modified:

- Network Devices Panel
- Network Devices Panel, NATs tab.
- Network Devices Panel, LBLs tab.
- Add/change/delete NAT Dialogs
- Add/change/delete LBL dialogs
- change adjacent MB dialogs
- change root mb dialogs

The following GUIs have been added:

- SPC provisioning network panel.
- Add/change/delete SPC dialogs
- Network Zone tabbed Panel
- Composite NAT/LBL zone tabbed Panel
- Add/change/delete composite NAT/LBL zone dialogs

The following XML commands have been added:

- Add/change/delete/query Network Zone

The on-line help facility will be updated with information on the use, syntax and valid values for all the above modifications/additions.

25.7 Applicable customer facing sections

Fault Management

Logs _N/A_

Alarms _N/A_

Configuration

Data Schema _X_

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_

25.8 SPC Provisioning (including Network VCAC)

The General Network Settings display and change dialog will be modified to include a new panel which will allow setting/change of the SPC provisioning information and Network VCAC flag. Note that for SN08, at most one SPC can be provisioned.

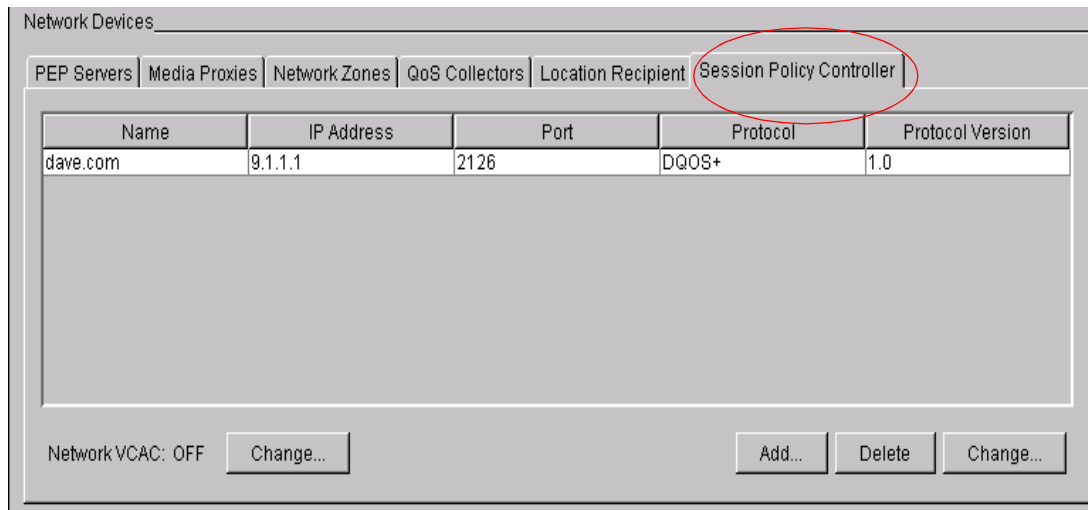
Provisioning constraints will be applied as per the GWCEM GUI guidelines, ie with disallowed input data resulting in a red outline to the input field and disabling of appropriate 'ok' buttons etc.

Note that in order to ensure optimum system operation is maintained during an upgrade, the upgrade of GWCs to SN08 should follow details specified in section xxxx.

25.8.1 Provision SPC information

The SPC information is displayed in the Gateway Controller Main Panel, as a tab in the 'Network Devices' area. This is shown in Figure 3

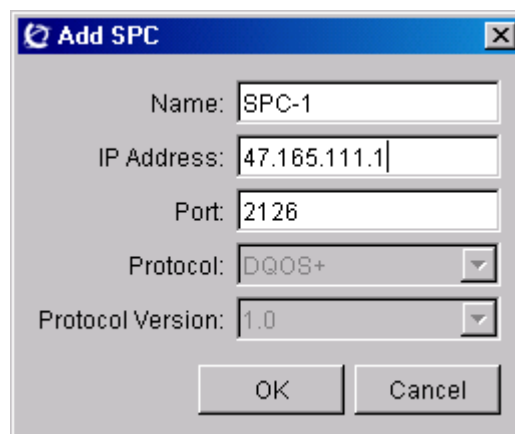
Figure 3 SPC Tab



Add SPC

An SPC can be added via the 'Add' button and Add SPC dialog, Figure 4

Figure 4 Add SPC Dialog

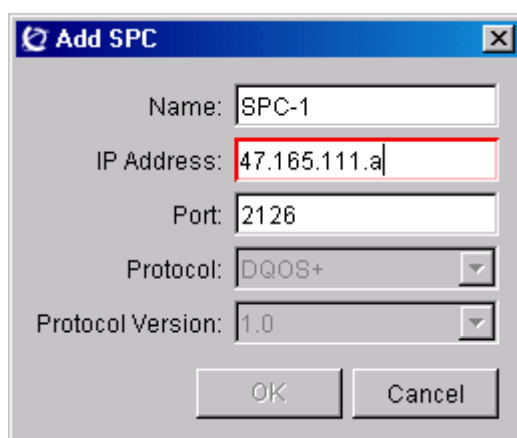


Following information must be added:

- Name (FQDN characters only)
- IP address (a.b.c.d) where a, b, c, d are integers between 0 and 255.
- Port (1 to 65535), defaults to DQOS port 2126.
- Protocol version (selected from list, or fixed at value if only one available)
- Protocol type (selected from list, or fixed at value if only one available)

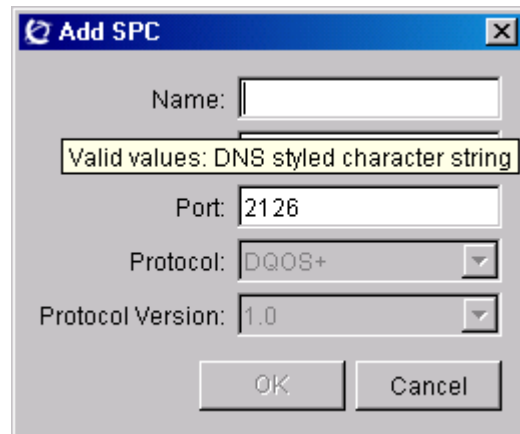
If invalid data is entered, the corresponding input field is outlined in red and the ok button is disabled, Figure 5

Figure 5 Add SPC Dialog - invalid data



The screenshot shows a Windows-style dialog box titled "Add SPC". It contains five input fields: "Name" with the value "SPC-1", "IP Address" with the value "47.165.111.a", "Port" with the value "2126", "Protocol" with a dropdown menu showing "DQOS+", and "Protocol Version" with a dropdown menu showing "1.0". The "IP Address" field is outlined in red, indicating invalid data. At the bottom of the dialog are "OK" and "Cancel" buttons. The "OK" button is disabled (grayed out), while the "Cancel" button is active.

Tool tips describe the valid input data for each text field, e.g. as shown in Figure 6

Figure 6 Add SPC dialog - example tool tip

The image shows a Windows-style dialog box titled "Add SPC". It contains four input fields: "Name:" (empty), "Port:" (2126), "Protocol:" (DQOS+), and "Protocol Version:" (1.0). A tooltip is displayed over the "Name:" field, showing the text "Valid values: DNS styled character string". At the bottom of the dialog are "OK" and "Cancel" buttons.

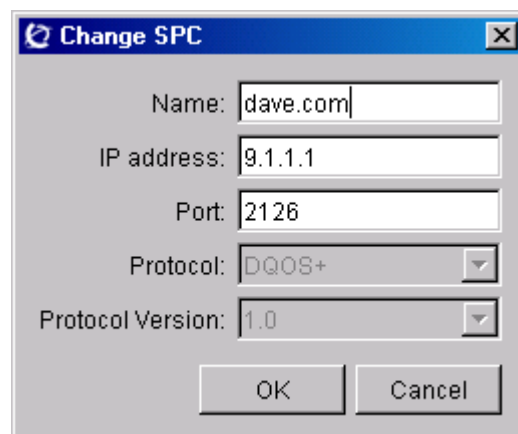
Delete SPC

If an SPC is selected in the table then the 'delete' button is enabled. If delete is clicked then a confirmation message is displayed and if the user confirms the action, the SPC is deleted.

An error dialog is displayed and the delete is not performed if a policy is enabled for the SPC.

Change SPC

If an SPC is selected in the table then the 'change' button is enabled. If change is clicked then a change dialog is displayed, Figure 7

Figure 7 Change SPC Dialog

The image shows a Windows-style dialog box titled "Change SPC". It contains five input fields: "Name:" (dave.com), "IP address:" (9.1.1.1), "Port:" (2126), "Protocol:" (DQOS+), and "Protocol Version:" (1.0). At the bottom of the dialog are "OK" and "Cancel" buttons.

The following fields can be changed:

- Name
- IP address
- Port
- Protocol type (only one protocol in SN08)
- Protocol version (only one protocol version in SN08)

If invalid data is entered, the corresponding input field is outlined in red and the ok button is disabled. Tool tips describe the valid input data

Set Network VCAC on/off

The SN08 Gateway Controllers can operate in two VCAC modes: they can either attempt to count resource usage on the GWC itself (internal counting, Network VCAC 'off') or they can rely on the SPC to count resource usage and signal to the SPC for admission control during call set-up (Network VCAC 'on').

The current state of Network VCAC is shown on the SPC Panel. The user can set the Network VCAC on/off by using the Network VCAC change button on the SPC panel, see Figure 8, "Network VCAC field". A confirmation message is displayed stating

- VCAC counting will now be done on the SPC
- all GWCs and XA-core should be at version SN08
- If this is the first time Nw VCAC is set on, warning indicating that internal counting provisioning checks will no longer be supported.

Figure 8 Network VCAC field

The screenshot shows a software interface titled "Network Devices". It has several tabs: "PEP Servers", "Media Proxies", "Network Zones", "QoS Collectors", "Location Recipient", and "Session Policy Controller". The "Session Policy Controller" tab is active. Below the tabs is a table with the following data:

Name	IP Address	Port	Protocol	Protocol Version
dave.com	9.1.1.1	2126	DQOS+	1.0

Below the table, there is a section labeled "Network VCAC: OFF". To its right is a button labeled "Change..." which is circled in red. Further to the right are three buttons: "Add...", "Delete", and "Change...".

Note that after Network VCAC is set on for the first time, SESM will no longer carry out 'internal counting' related provisioning checks, regardless of whether Network VCAC is later switched off or not.

25.9 Network Zone provisioning

25.9.1 XML Interface

New XML interfaces are added are implemented by this feature for use in network installations where the SESM platform is required to operate in conjunction with an SPC. These interfaces align with the provisioning model used by the SPC for NAT and VCAC functionality and is described in terms of Network Zones and Zone characteristics.

The XML interfaces are identical to those supported by the SPC. In order to provision any entity, the information must first be provisioned into SESM and then, if successful, the same information must be provisioned into the SPC. The provisioning should be done first on SESM because SESM has more constraints to check (e.g. whether the Zone is currently associated with a Gateway) and hence is more likely to fail the provisioning request. The XML and XSD for these interfaces are specified in the SPC FN [Ref: <http://livelink-asiapac.us.nortel.com/asiapac/livelink.exe?func=ll&objId=1534787&objAction=browse&sort=name>] and will not be repeated here.

The SESM model only supports a subset of the information used by the SPC. The following general rules will be used:

- Add/change/delete commands: where a parameter is specific to the SPC and of no meaning to SESM, it will be ignored. Where a parameter is interpretable by SESM, its value will be validated
- queries: all relevant parameters for the specific query that are supported by SESM will be returned with valid data. No other parameters will be returned

The SN07 ITRANS VCAC interfaces for NAT and LBL provisioning are still available. However, when a SPC is deployed in the network configuration, the SPC consistent provisioning model is provided via use of the Zone provisioning interfaces and the SN07 ITRANS VCAC interfaces for NAT and LBL provisioning are not required. A mapping is available in table 3.

Note that, when adding a Network Zone, Resource Usage Factor and Max Count values are not required as long as Network VCAC is on (Details of Logical Network Link sent in XML messages 'addNetworkZone' and 'changeNetworkZone' are ignored by SESM. However if Network VCAC is 'off', resource usage factor and max count details ARE required and hence the XML command 'addLBL' should be used to add LBL Network Zones. However it is not recommended to switch Network VCAC off once it has been switched on. Also, if it is switched off, Basic VCAC will only work correctly if the topology still meets the Basic VCAC/'internal counting' topology constraints.

25.9.1.1 Supported Interfaces For SPC Interworking

Add, Change and Delete Network Zone interfaces are implemented by SESM. In general, the Zone and the Zone parent can be referenced by either name or Zone ID, but not by both. For 'Add Network Zone', the Zone ID is optional and will be generated by SESM if not specified.

Table 1 XML Interfaces Specific To SPC Topology Server Interworking For ITRANS

Interface	SN07 VCAC ITRANS Equivalent	Description
addNetworkZone	addNAT or addLBL	Add either a NAT, LBL or Composite type network zone
changeNetworkZone	changeNAT or changeLBL	change either a NAT, LBL or Composite type network zone
deleteNetworkZone	deleteNAT or deleteLBL	delete either a NAT, LBL or Composite type network zone
queryNetworkZone	queryNAT plus queryLBL	query on NAT, LBL and Composite data fill

25.9.1.1.1 addNetworkZone Interface

This interface will add a new NAT, LBL or Composite type Network Zone. A composite Network Zone is one comprising the attributes of both a NAT and LBL type Network Zone.

The following parameters will be interpreted when adding a new Network Zone, with all other SPC specific parameters being ignored:

- <Name>NZ-Name</Name> - Unique name for the new Network Zone (NAT, LBL or Composite Name).
- <ID>1234</ID> - Unique ID for the Network Zone (NAT, LBL or Composite) to be created. If this is not specified, it is generated by SESM.
- <Parent> - Optional tag. Specified if Network Zone has a parent and contains tags ParentID or ParentName.
 - <ParentID>5678</ParentID> - ID of parent Network zone. Mutually exclusive with ParentName.

-
- <ParentName>Parent-Name</ParentName> - Name of parent Network zone. Mutually exclusive with ParentID.
 - </Parent>
 - <Service>NAT</Service> - Optional. Identifies Network Zone as being a NAT or Composite type Network Zone. For a Composite Network Zone the LogicalNetworkLink tag should also be present.
 - <LogicalNetworkLink> - Optional. Identifies the Network Zone as being an LBL or Composite Network zone. For a Composite Network Zone the Service tag should also be present.
 - ... Contents of LogicalNetworkLink are ignored but should be correctly populated.
 - </LogicalNetworkLink>

At least one of the tags Service and LogicalNetworkLink must be present.

If both Service and LogicalNetworkLink tags are present, the Zone is a composite NAT & LBL zone.

All other input data is ignored by SESM.

25.9.1.1.2 changeNetworkZone Interface

This interface will modify either a NAT, LBL or Composite type Network Zone.

For the change command, the user will specify tags for the parameters that are to be changed. Unchanged parameters do not have to be specified. The Network Zone name and ID cannot be changed. All other parameters can be changed. SESM will ignore changes to parameters that it does not hold (e.g. bandwidth, link types etc.).

Interpreted parameter tags are as follows:

- <Name>NZ-Name</Name> - Network Zone Name
- ** or **
- <ID>1234</ID> - Network Zone ID
- <Parent> - Optional tag identifying a new Parent Network Zone. Contains either ParentName or ParentID tags but not both.
 - <ParentID>5678</ParentID> - new parent ID. Set to 0 if no parent required. Mutually exclusive with ParentName.
 - <ParentName>New-Parent-Name</ParentName> - new parent Network Zone name. Mutually exclusive with ParentID.
- </Parent>

- <LogicalNetworkLink> - optional. If present the Network Zone type is checked to ensure it is not a NAT as the presence of this tag implies a change of Network Zone type which is not supported.
 - ... contents of LogicalNetworkLink are ignored
- </LogicalNetworkLink>

25.9.1.1.3 deleteNetworkZone Interface

This interface will delete either a NAT, LBL or Composite type Network Zone.

Interpreted parameter tags are as follows:

- <Name>NZ-Name</Name> - Name of Network Zone to be deleted.

**** OR ****

- <ID>1234</ID> - ID of the Network Zone to be deleted.

25.9.1.1.4 queryNetworkZone Interface

This interface will perform a selective query on the provisioned NAT, LBL and Composite type network zones. Based on the population of the request it is possible to retrieve a single network zone name or all network zones names. The network zone IDs may also be optionally retrieved. This command differs from the SN07 queryNAT and queryLBL interfaces in that the returned data is a combination of the provisioned NATs and LBLs. It is not possible to selectively retrieve those network zones of a particular service type.

In general, since SESM holds a subset of the topology information held by SPC (ie it has no link information), the user should carry out queries on SPC. SESM will support both individual and bulk queries, however it is expected that only the bulk queries will be used. Bulk queries will be needed e.g. to audit the SESM-SPC data consistency. The result of the bulk query will be sorted by ID.

Interpreted input parameter tags are as follows:

Name or ID - Optional parameter indicating we wish to query a specific Network Zone. If not specified it is assumed that all Network Zones should be queried.

- <Name>Bob</Name> - requests retrieval of “Bob” Network Zone OR
- <ID>1234</ID> - requests retrieval of Network Zone with ID 1234.

Filtering parameters to limit the number of zones returned. These are optionally present but only for bulk zone queries (ie when no name or id is specified)

- <IDMax>12000</IDMax> - maximum Network Zone ID
- <IDMin>11001</IDMin> - minimum Network Zone ID

- `<MaxZones>1234</MaxZones>` - maximum number of Zones to be returned. If more Zones exist than the maximum specified, this will be indicated via an error code.

Returned parameter tags are as follows:

- `<ID>1234</ID>` - Unique ID for a Network Zone.
- `<Name>NZ-Name</Name>` - Unique Network Zone name.
- `<ParentID>5678</ParentID>` - ID of parent Network Zone. Where there is no parent this will be set to 0.

Additionally for query of individual Network Zone, the following information is also returned:

- `<Service>NAT</Service>` - Service type indicating if this Network Zone is a NAT. If the zone is has no services, no service tag is returned.
- `<LogicalNetworkLink>` - returned only if the Network Zone type is LBL or Composite. This will contain LayerInfo, Layer and LinkLayerInfo tags, with the LinkLayerInfo tag assigned a dummy value of “UNKNOWN” as SESM has no knowledge of Network Zone parameter values.

25.9.1.2 Unsupported Interfaces

The SESM platform only supports a subset of the SPC Topology server VCAC ITRANS interfaces. In SN08, add/change/delete/query LinkLayer type are not supported by SESM. However, to aid simple XML command replication by the OSS, these will be a dummy commands in SESM & will always return an error code 306 and text 'SPC Interface Unsupported By Platform' . (The alternative is for SESM not to support this, however this means a single XSD cannot be published and requires OSS to understand which commands go only to the SPC.)

Unsupported interfaces are described in the following table:

Table 2 SPC Topology Server ITRANS Interfaces Unsupported By SESM

Interface	Description
addLinkLayerType	add a new link layer
changeLinkLayerType	change an existing link layer
deleteLinkLayerType	delete a link layer
queryLinkLayerType	query provisioned link layers

25.9.1.3 NAT/LBL provisioning interfaces

The SN07 ITRANS VCAC interfaces for NAT and LBL provisioning are still available. When a SPC is deployed in the network configuration, a consistent provisioning model is provided via use of the Zone provisioning interfaces.

However the SN07 interfaces remain valid ITRANS VCAC interfaces for NAT and LBL provisioning (table 3) and should be used when the SPC is not present in the network configuration.

Table 3 SN07 SESM ITRANS VCAC Interfaces.

Interface	Description
addNAT	Add NAT - use addNetworkZone.
changeNAT	Change NAT - use changeNetworkZone
deleteNAT	Delete NAT - use deleteNetworkZone
queryNAT	Query NAT - use queryNetworkZone. See Note following table.
addLBL	Add LBL - replaced by addNetworkZone. Resource usage and counter functionality is set to default values.
changeLBL	Change LBL - replaced by changeNetworkZone. Resource usage and counter functionality is set to default values.
deleteLBL	Delete LBL - replaced by queryNetworkZone.
queryLBL	Query LBL - use QueryNetworkZone Interface (safe but deprecated)
changeRootMiddleBoxes	Change Root Middle Boxes - use changeNetworkZone interface
changeAssocMB	Change associated middlebox - use changeNetworkZone interface
addRU	Add Resource Usage. SESM has no concept of resource usage where SPC Topology server is present. Internally default settings will be used for modelling purposes, and attempting manipulation would make no sense.
changeRU	Change Resource Usage.
deleteRU	Delete Resource Usage
queryRU	Query Resource Usage

Note: Interface remains used by CICM Element Manager.

25.9.2 Error codes

Each error code will have a descriptive text string associated with it. It is not possible to guarantee that the same error will result in the same error code being returned by SPC and SESM. However the sequential provisioning required (first into SESM and then into SPC) means that typically the OSS will get an error code back from one machine only - since if the SESM command fails, it will not continue to do the provisioning into SPC.

25.9.2.1 Examples Of XML Interface Usage

25.9.2.1.1 Add NAT using addNetworkZone (Request)

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <addNetworkZone usn="1" version="1.0"/>
        <Parameters>
          <ID>1001</ID>
          <Name>My_NAT</Name>
          <Service>NAT</Service>
          <Parent>
            <ParentID>1000</ParentID>
          </Parent>
          ...
        </Parameters>
      </addNetworkZone>
    </Methods>
  </Command>

```

Parent if we have a parent
 Named parent by ID

SPC Parameters, not shown, no logical network link is present

25.9.2.1.2 Add LBL using addNetworkZone (Request)

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <addNetworkZone usn="1" version="1.0">
        </Parameters>
        <Name>My_LBL</Name>
        <Parent>
          <ParentName>MyParent</Parent>
        </Parent>
        <LogicalNetworkLink>
          <BandwidthInfo>
            <Symmetry>true</Symmetry>
            <UpBWInfo>
              <BWCIR>1000</BWCIR>
              ... SPC specific parameters
            </UpBWInfo>
            <DownBWInfo>
              <BWCIR>1000</BWCIR>
              ... SPC specific parameters
            </DownBWInfo>
          </BandwidthInfo>
          ...SPC specific parameters
        </LogicalNetworkLink>
        ... SPC specific parameters
      </Parameters>
    </addNetworkZone>
  </Methods>
</Command>
</CommandList>

```

Parent if we have a parent
 Named using NZ Name
 Contents of BandwidthInfo
 loosely interpreted.
 Contents are ignored.

25.9.2.1.3 Add Composite NAT/LBL using addNetworkZone (Request)

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <addNetworkZone usn="1" version="1.0">
        </Parameters>
        <Name>My_LBL</Name>
        <Service>NAT</Service>
        <Parent>
          <ParentID>1010</ParentID>
        </Parent>
        <LogicalNetworkLink>
          <BandwidthInfo>
            <Symmetry>>false</Symmetry>
            <UpBWInfo>
              <BWCIR>1000</BWCIR>
              ... SPC specific parameters
            </UpBWInfo>
          </BandwidthInfo>
          ...SPC specific parameters
        </LogicalNetworkLink>
      </Parameters>
    </addNetworkZone>
  </Methods>
</Command>
</CommandList>

```

Optional ID not specified

Name parent using ID

Contents of BandwidthInfo loosely interpreted. Contents are ignored.

... SPC specific parameters

...SPC specific parameters

25.9.2.1.4 Change Network Zone (LBL or NAT) (Request)

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>ITranslf</Interface>
    <Methods>
      <changeNetworkZone usn="1" version="1.0">
        <Parameters>
          <Name>My_Zone</Name>
          <Parent>
            <ParentName>New-Parent</ParentName>
          </Parent>
          ...
        </Parameters>
      </changeNetworkZone>
    </Methods>
  </Command>
</CommandList>

```

Change parent using name

SPC specific parameters not shown

25.9.2.1.5 Delete Network Zone (LBL or NAT) (Request)

```

<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>ITranslf</Interface>
    <Methods>
      <deleteNetworkZone usn="1" version="1.0">
        <Parameters>
          <Name>My_Zone</Name>
        </Parameters>
      </deleteNetworkZone>
    </Methods>
  </Command>
</CommandList>

```

Target Network Zone using Name

25.9.2.1.6 Query Network Zone (All) (Request)

```
<?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>
```

25.9.2.1.7 Query Network Zone (Range Min ID Max ID) (Request)

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <queryNetworkZone usn="1" version="1.0">
        <Parameters>
          <IDMin>500</IDMin>
          <IDMax>900</IDMax>
        </Parameters>
      </queryNetworkZone>
    </Methods>
  </Command>
</CommandList>
```

25.9.2.1.8 Query Network Zone (Range Min ID MaxZones) (Request)

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <queryNetworkZone usn="1" version="1.0">
        <Parameters>
          <IDMin>500</IDMin>
          <MaxZones>200</MaxZones>
        </Parameters>
      </queryNetworkZone>
    </Methods>
  </Command>
</CommandList>
```

25.9.2.1.9 Query Network Zone (Individual ID Based) (Request)

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <queryNetworkZone usn="1" version="1.0">
        <Parameters>
          <ID>101</ID>
        </Parameters>
      </queryNetworkZone>
    </Methods>
  </Command>
</CommandList>
```

25.9.2.1.10 Query Network Zone (Individual Name Based) (Request)

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <queryNetworkZone usn="1" version="1.0">
        <Parameters>
          <Name>Peter67</Name>
        </Parameters>
      </queryNetworkZone>
    </Methods>
  </Command>
</CommandList>
```

25.9.2.1.11 Query Network Zone (All / Range) (Response)

```

<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
      <queryNetworkZone usn="1" version="1.0">
        <ReturnData>
          <NetworkZone>
            <ID>235</ID>
            <Name>NZ1</Name>
            <ParentID>0</ParentID>
          </NetworkZone>
          <NetworkZone>
            <ID>891</ID>
            <Name>NZ2</Name>
            <ParentID>235</ParentID>
          </NetworkZone>
          <NetworkZone>
            <ID>65539</ID>
            <Name>Nat.1</Name>
            <ParentID>0</ParentID>
          </NetworkZone>
          <NetworkZone>
            <ID>65540</ID>
            <Name>lbl1</Name>
            <ParentID>0</ParentID>
          </NetworkZone>
          <NetworkZone>
            <ID>65541</ID>
            <Name>comp1</Name>
            <ParentID>0</ParentID>
          </NetworkZone>
          <ReturnCode value="0" text="Successful result" />
        </ReturnData>
      </queryNetworkZone>
    </Methods>
  </Response>
</CommandList>

```

25.9.2.1.12 Query Network Zone (Individual) (Response)

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
      <queryNetworkZone usn="1" version="1.0">
        <ReturnData>
          <ID>65541</ID>
          <Name>comp1</Name>
          <Service>NAT</Service>
          <Parent>
            <ParentID>0</ParentID>
          </Parent>
          <LogicalNetworkLink>
            <LayerInfo>
              <Layer>
                <LinkLayerType>UNKNOWN</LinkLayerType>
              </Layer>
            </LayerInfo>
          </LogicalNetworkLink>
          <ReturnCode value="0" text="Successful result" />
        </ReturnData>
      </queryNetworkZone>
    </Methods>
  </Response>
</CommandList>
```

25.9.3 GUI Client

The GUI client for internet transparency NAT and VCAC entity provisioning will be available for network deployments where the SPC is present and for deployments where the SPC is not present. Hence the GUI must effectively support both the SN07 and SN08 models. Hence the GUI will not be changed significantly from the SN08. The changes are as follows:

25.9.3.1 Network Zone Display

There will be a new panel on the Network Devices tabbed panel, this will be a tabbed panel with tab 'Network Zones'.

The NAT and LBL provisioning panels will be moved from the Network devices tabbed panel to the Network Zones tabbed panel. In addition, there will be a new provisioning panel for provisioning composite NAT/LBL Network Zones (this functionality to be confirmed), see Figure 9

Figure 9 Network Zones tabbed panel

Network Devices _____

PEP Servers | Media Proxies | **Network Zones** | QoS Collectors | Location Recipient | Session Policy

NAT Zone | LBL Zone | NAT&LBL Zone

Name	NAT Type	
Fred.1	Non-Controlled	<none> (To
MFNAT.1	Non-Controlled	<none> (To
MFNAT.2	Non-Controlled	<none> (To
MFNAT.3	Non-Controlled	<none> (To
MFNAT.4	Non-Controlled	<none> (To
MFNAT.5	Non-Controlled	<none> (To
MFNAT.6	Non-Controlled	MFLBL.4

Add... Delete

25.9.3.2 Add/Change/Delete Zone

In the add/change/delete NAT & LBL dialogs and for add/change NAT/LBL associated to gateway, the word 'Middlebox' will generally be replaced with either 'Zone' or 'Network Zone', for example as in Figure 10.

Figure 10 Add NAT Zone

Add IP-VPN (NAT Zone)

Name: _____

☐ Shared Zone

NAT Type: Non-Controlled

Parent Zone Selection (create hierarchy)

☒ ALL ☐ IP-VPNs ☐ LBLs

Parent Zone: <none>

OK Cancel

25.9.3.3 LBL provisioning

When the SPC is present, the user does not need to provision the RU Profile Name and Max Count Value when provisioning an LBL. Hence, when the Network VCAC flag is switched 'on', fields to provision and change RU

Profile and Max count information will be hidden. Internally, the RU Profile will be set to a system provisioned RU Profile created on system initialisation, SPC_DEFAULT and the Max count set to 0 (tbc). Fields which display this information in the LBL zone table will also be hidden. If the Network VCAC flag is switched off, the RU Profile and max count information is displayed again.

Similarly, the RU provisioning panel will be hidden/displayed when the Network VCAC flag is switched on/off.

25.9.3.4 Composite NAT & LBL provisioning (this work item tbc)

Similar dialogs will be supported for add/change/delete composite NAT/LBL zone as for NAT zones. This option is only available when the SPC is used and RU Profile and max count information is not required. Hence similar dialogs/display will be supported for add/change/delete/display composite NAT/LBL zone as for NAT zones. Note that in this case, NO profile or max count information is sent to the GWC and, for internal counting, the zone is treated as a NAT zone.

25.10 XML Interfaces Supported By SPC

The SPC platform only supports a subset of the ITRANS XML interfaces. No attempt should be made to direct unsupported XML interface operations against the SPC.

The set of supported XML interfaces at the SPC are as follows. All other interfaces should be considered as supported only by SESM.

Table 4 ITRANS XML Interfaces Supported By The SPC Platform

Interface Name
addNetworkZone
changeNetworkZone
deleteNetworkZone
queryNetworkZone
addLinkLayerType
changeLinkLayerType
deleteLinkLayerType
queryLinkLayerType

25.11 Authorization for Commands

The security for the GUI Client and OSSgate interface includes support for permission or 'Authorization' levels for commands. Each command is associated with one or more user groups. In order to execute a command, a user must belong to at least one of the associated user groups. The user groups associated with the new /modified commands associated with this feature are specified in the table below.

Table 1 Internet Transparency Commands Authorization

Command	User Group				
	mgcadm	mgcrw	mgcmic	mgcsprov	mgcro
add SPC	X				
delete SPC	X				
change SPC	X				
display SPCs	X	X	X	X	X
set Network VCAC	X				
add Network Zone	X	X			
delete Network Zone	X	X			
change Network Zone	X	X			
query Network Zone	X	X	X	X	X
query all Network Zones	X	X	X	X	X

25.12 Upgrade

In order to ensure optimum system operation is maintained during an upgrade, the upgrade of GWCs to SN08 should follow details specified in the FN for feature A00007394

25.13 Glossary

Term	Description
CS2K	Communication Server 2000
GUI	Graphical User Interface
GWC	Gateway Controller
GWCEM	Gateway Controller Element Manager

Term	Description
ID	Identifier
IEMS	Integrated Element Manager System
LBL	Limited Bandwidth Link
ME	Media Endpoint
NAT	Network Address Translation
NGSS	Next Generation Sessions Server
OSS	Operations Support System
SESM	Succession Element and Sub-element Manager
SPC	Session Policy Controller
VCAC	Virtual Connection Admission Control
VPN	Virtual Private Network
XML	Extensible Markup Language

25.14 Appendix A: Error codes and messages

Table 2 Return codes when command is unsuccessful

Error meaning	Return code	Example return messages
Platform applications internal error: OSS Interface applications cannot connect to required server application	302	Interfacing error
Unable to provision requested data because a database error occurred	303	Database error occurred during setting of Network Zone
Unable to provision requested data because of problem with the GWCEM component of the CS2k Mgr.	304	Element Manager Initialisation in progress
No data for this query meets selection criteria or the filtering criteria specified do not exist	305	No Network Zones found

Error meaning	Return code	Example return messages
Interface is valid based on ITrans XSD schema but is unsupported by SESM (SPC specific)	306	SPC Interface Unsupported By Platform
User is not a member of any of the user groups allowed to perform this action	501	Insufficient permissions to perform this operation

25.14.1 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>

```

25.15 Appendix B: XML Commands: description of method parameters

25.15.1 Parameter definitions

Only those parameters that are read / returned by the VCAC ITrans interface are described.

- **encoding** - UTF-8.
- **version** - The version refers to the version of the method or operation - e.g., the addNAT operation may have version 1.0 and 2.0, where version 1.0 takes parameters X and Y and version 2.0 takes parms X, Y, and Z. TYPE *decimal*.
- **usn** - Unique Sequence Number. This parameter is introduced to facilitate sending multiple XML commands in one file. This parameter value will be used to match the responses with the requests. TYPE *integer*.

- **Name** - Unique Network Zone name.
- **ID** - Unique Network Zone ID.
- **ParentName** - Name of parent Network Zone.
- **ParentID** - ID of parent Network Zone.
- **Service** - Network Zone service type. Only supported value is “NAT”.
- **Symmetry** - LogicalNetworkLink - BandwidthInfo symmetry field. Boolean value but setting ignored by SESM but has meaning to SPC.
- **BWCIR** - LogicalNetworkLink - BandwidthInfo - UpBWInfo / DownBWInfo BWCIR setting. Value is ignored by SESM but has meaning to SPC.
- **LinkLayerInfo** - LogicalNetworkLink - LayerInfo - Layer - LinkLayerType field. Value is ignored by SESM being SPC specific.
- **IDMin** - Minimum Network Zone ID for a query.
- **IDMax** - Maximum Network Zone ID for a query.
- **MaxZones** - Maximum number of Network Zones for a query.
- **ReturnCode value**- A numeric value indicating the result of the attempted operation (see Table 3, for range and definitions of each possible value). TYPE *string*.
- **Return code text**- Appropriate text that describes the result of the operation. TYPE *string*.

25.15.2 Method Parameters

Method parameters are defined below. Input data is mandatory except where indicated otherwise.

1. **addNetworkZone** - Method that adds a new Network Zone. This method has the following parameters:
 - Input data:
 - usn
 - version
 - Name
 - ID (optional internally generated if not specified)
 - ParentName (optional and mutually exclusive with ParentID)
 - ParentID (optional and mutually exclusive with ParentName)
 - Service (optional only if NAT / Composite Network Zone required)
 - Symmetry (optional only if LBL / Composite Network Zone required)
 - BWCIR (optional only if LBL / Composite Network Zone required).

-
- 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. **changeNetworkZone** - Method that modifies a parent Network Zone. This method has the following parameters:
 - Input data:
 - usn
 - version
 - Name (Mutually exclusive with ID parameter)
 - ID (Mutually exclusive with Name parameter)
 - ParentName (optional and mutually exclusive with ParentID)
 - ParentID (optional and mutually exclusive with ParentName)
 - 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.
 - 3. **deleteNetworkZone** - Method that deletes a Network Zone. This method has the following parameters:
 - Input data:
 - usn
 - version
 - Name (Mutually exclusive with ID parameter)
 - ID (Mutually exclusive with Name parameter)
 - 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.
-

4. **queryNetworkZone** - Method that queries the Network Zones provisioned on the SESM platform. This method has the following parameters:

- Input data:

- usn
- version
- Name (optional and mutually exclusive with ID. Presence restricts query to a single Network Zone)
- ID (optional and mutually exclusive with Name. Presence restricts query to a single Network Zone)
- IDMin (Optional. Not valid if query targets a specific Network Zone).
- IDMax (Optional. Not valid if query targets a specific Network Zone).
- MaxZones (Optional. Not valid if query targets a specific Network Zone).

- Output data:

- usn (value should be the same as the input)
- version (value should be the same as the input)
- ID
- Name
- ParentID
- Service - where individual Network Zone is targeted and type is NAT or Composite. Value is set to “NAT”
- LinkLayerType - where individual Network Zone is targeted and type is LBL or Composite. Value is set to “UNKNOWN”
- 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.

26: A00007255 Functional description (FN)

26.1 Feature name

Dial Plan Enhancement for ETSI MWI TCAP

26.2 Description

26.2.1 Introduction

As a brief explanation, MWI enables the DMS-100MMP product to communicate with Voice Mail Centers (CU, Controlling User) and to inform the MWI subscriber (RU, Receiving User) of pending voice mails. MWI SCCP/TCAP provides network wide transmission of MWI supplementary service messages using CCS7 SCCP/TCAP signalling.

This feature provides flexibility in setting the DN of MWI subscriber in ETSI SS7 TCAP message for MWI (Message Waiting Indication). This activity covers:

- stripping the NAC (National Access Code) from the MWI agent's DN in the outgoing TCAP.
- delivering the MWI request, even the called DN parameter of the incoming ETSI MWI TCAP is different from the DN of the actual MWI agent.

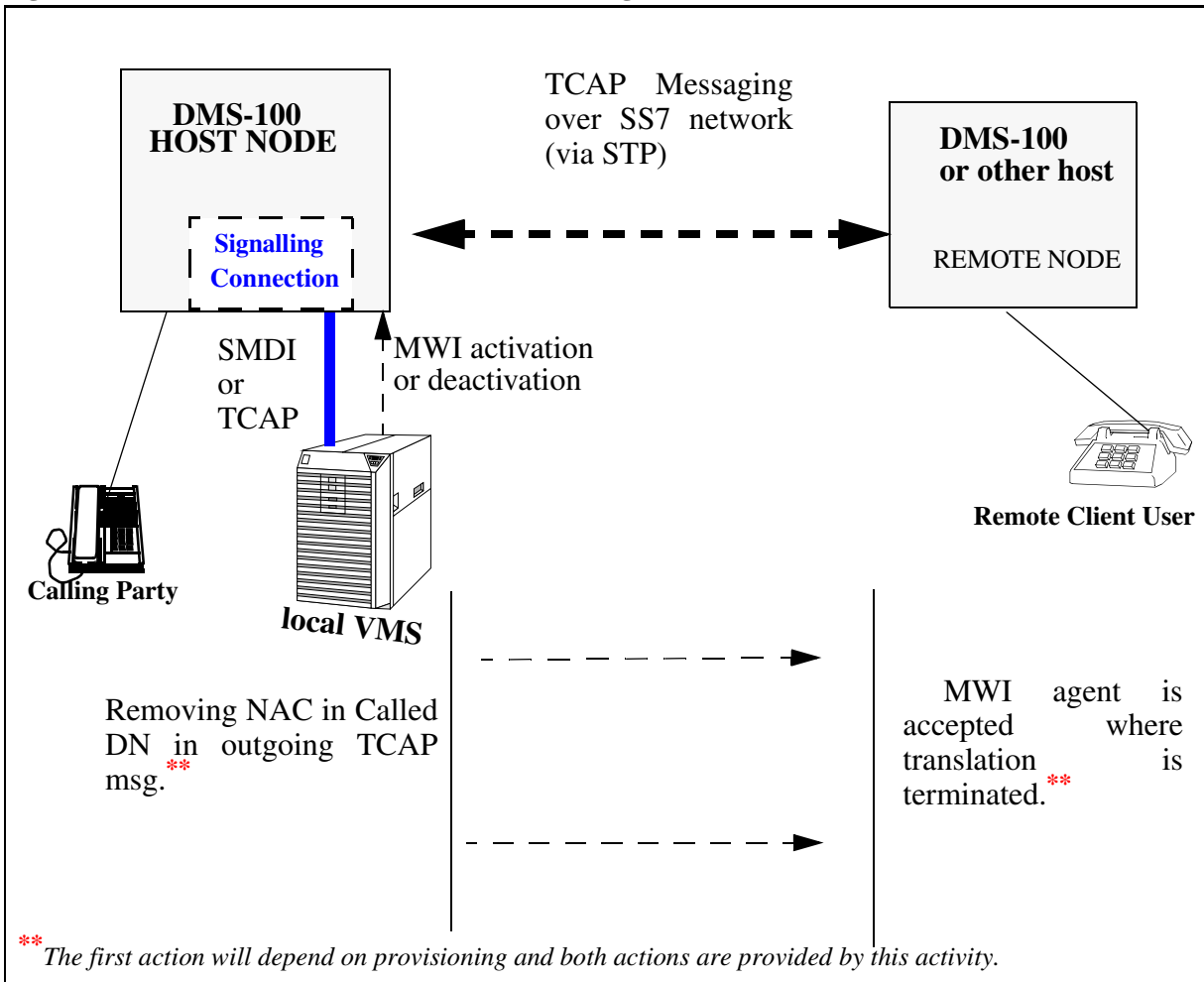
In existing functionality, while preparing the MWI TCAP message, if the called DN (MWI agent) starts with NAC, NAC is removed from the called DN by default. However, this issue causes translation problems in some markets which have some SNPA codes started with NAC.

Additionally, in the existing functionality, the MWI agent DN should be the same as the called DN in the TCAP message in order to deliver the MWI request even if the translation goes to the correct agent. This activity changes this process, and the agent where translation is terminated is accepted as the MWI agent even if the DN of this agent is different from the called DN in the incoming TCAP msg.

26.2.2 General Considerations

This feature only affects the called DN parameter of the EMWI TCAP message, the handling and sending of the EMWI TCAP message is not changed/affected by this feature. The related scenario of the EMWI is as shown in Figure 1.

Figure 1 Scenario of MWI act/deact via TCAP message



The first action mentioned above is provided as optional via provisioning of the newly defined tuple ETSI_MWI in the ISERVOPT table.

26.2.3 Provisioning parameters in the ISERVOPT table

There is a new tuple defined for this feature in the ISERVOPT table, and this tuple should be provisioned appropriately in order to make this feature work. This new tuple (EMWI) includes the following parameters:

- **DEFAULT_MWI_XLA_ENTRY:** indicates that the incoming TCAP message for the ETSI MWI request is translated according to the entered line attribute. This functionality is already provided via the office parameter DEFAULT_MWI_XLA_ENTRY by activity A59017265. This office parameter is moved to this ETSI MWI tuple in the ISERVOPT table to present the whole ETSI MWI provisioning in one place.

- **ALLOW_NAC_IN_TCAP**: indicates that the NAC is allowed or not in the called DN field of the TCAP message sent for MWI activation/deactivation

The ISERVOPT table can be datafilled as follows:

Figure 2 Example of datafilling EMWI tuple

```
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:
>EMWI
OPTION:
>EMWI
DEFAULT_XLA_ENTRY:
>100
ALLOW_NAC_IN_TCAP:
>n
TUPLE TO BE ADDED:
EMWI EMWI 100 N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

The tuple can be seen from the listing of the ISERVOPT table as follows:

Figure 3 The View of EMWI Tuple in ISERVOPT Table

```
>table iservopt

SOPTSKEY SOPTSVAR
-----
EMWI EMWI 100 N
```

While the EMWI TCAP message is received, the remote switch tries to find that MWI agent is residing within the switch or not by translating the called DN according to the entered line attribute in DEFAULT_MWI_XLA_ENTRY.

Please refer to APPENDIX A for EMWI translation/datafill examples.

26.3 Hardware Requirements or Dependencies

N/A

26.4 Software Requirements or Dependencies

N/A

26.5 Limitations and restrictions

- This feature is applicable for only ETSI MWI TCAP messages.
- The MWI request may be delivered to the MWI agent, translation is then terminated without comparing the called DN in the EMWI TCAP msg and the DN of the MWI agent.

26.6 Interactions

N/A

26.7 Glossary

Table 1

Term	Description
CCS7	Common Channel Signalling number 7
EMWI	ETSI Message Waiting Indication
MWT	Message Waiting (Line option for analogue lines)
SCCP	Signaling Connection Control Part
TCAP	Transaction Capabilities Application Part
VMS	Voice Mail Service

26.8 Appendix A: Datafill / Translation examples for EMWI

26.8.1 EXAMPLE 1: the MWI agent resides within the local switch where the VM is connected directly

TABLE TERMDEV

TCO4S0_3 0 23 SMDI B2400 EIA 1X67BC NONE N NONE ALL N

TABLE SLLNKDEV

TCO4S0_3 1X67 NONE NONE INOUTLK
(SMDIDATA (NUMOFDIGS 10) (XLA_ENTRY 1) (CGNADDRDN) \$)\$

VM DN: (Hunt Group)

>qdn 1027835466

```

-----
DN: 7835466
TYPE: PILOT OF DNH HUNT GROUP
SNPA: 102 SIG: DP LNATTIDX: N/A
HUNT GROUP: 1000 HUNT MEMBER: 0
LINE EQUIPMENT NUMBER: HOST 02 0 00 10
LINE CLASS CODE: IBN
IBN TYPE: STATION
CUSTGRP: CUST783 SUBGRP: 0 NCOS: 0
CARDCODE: 6X93AA GND: N PADGRP: STDLN BNV: NL MNO: N
PM NODE NUMBER : 44
PM TERMINAL NUMBER : 11
OPTIONS:
DP
GROUP OPTIONS:
RCVD SMDI 63 TCO4S0_3
MEMBER INFO:
-----

```

The translation should be like:

Assume that the VMS sends the MWI request for DN '1027835304'. Please note that the TRAVER is performed from the VM DN for only simulating. The important points here are:

- The line attribute index should be equal to the XLA_ENTRY field of the related SMDI link datafilled in the SLLNKDEV table.
- There should be an MWI agent associated with this DN sent by VMS in the local switch.

```

>traver l 1027835466 1027835304 b
TABLE IBNLINES
HOST 02 0 00 10 0 DP STN IBN 7835466 CUST783 0 0 102 $
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

```

CUST783 0 0 0 \$ (XLAS NETXLA STARCEPT NDGT) (OCTXLA OCTCEPT)\$
 TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
 CUST783 NXLA NETXLA NXLA 0 NDGT
 TABLE DIGCOL
 NDGT specified: digits collected individually
 TABLE IBNXLA: XLANAME NETXLA
 TUPLE NOT FOUND
 Default from table XLANAME:
 NETXLA
 (NET N Y 0 N NDGT N Y GEN (LATR 1 102_NPRT_1 NLCA_NILLA_1) \$)\$ 9
 TABLE DIGCOL
 NDGT specified: digits collected individually
 TABLE LINEATTR
1 IBN NONE NT 0 0 NILSFC 0 PX NETXLA NIL 00 102_NPRT_1 NLCA_NILLA_1 \$
 LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
 TABLE XLAPLAN
 102_NPRT_1 NSCR 102 NPRT NONE N \$ GG
 TABLE RATEAREA
 NLCA_NILLA_1 NLCA NIL NILLATA \$
 TABLE PXHEAD
 NETXLA SDFLT NODFOP NOCON F
 THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 1027835304
 TABLE PXCOD
NETXLA 102783 102783 DNRTE (DN 102 783)\$
 TABLE TOFCNAME
 102 783 \$
 TABLE DNINV
 102 783 5304 L HOST 02 0 00 18
 TABLE DNFEAT
 TUPLE NOT FOUND
 TABLE DNATTRS
 TUPLE NOT FOUND
 TABLE DNGRPS
 TUPLE NOT FOUND
 INAP Info Analyzed TDP: no subscribed trigger.
 INAP Route Select Failure TDP: no subscribed trigger.
 INAP Termination Attempt TDP: no subscribed trigger.

 +++ TRAVER: SUCCESSFUL CALL TRACE +++

 DIGIT TRANSLATION ROUTES

 1 LINE 1027835304 ST

 TREATMENT ROUTES. TREATMENT IS: GNCT
 1 MESAJ4
 2 2WIBN7AB

 +++ TRAVER: SUCCESSFUL CALL TRACE +++

The QDN output of MWI agent :

>qdn 1027835304

 DN: 7835304
 TYPE: SINGLE PARTY LINE
 SNPA: 102 SIG: DT LNATTIDX: N/A
 LINE EQUIPMENT NUMBER: HOST 02 0 00 18
 LINE CLASS CODE: IBN

IBN TYPE: STATION
 CUSTGRP: CUST783 SUBGRP: 0 NCOS: 0
 CARD CODE: 6X93AA GND: N PADGRP: STD LN BNV: NL MNO: N
 PM NODE NUMBER : 44
 PM TERMINAL NUMBER : 19
 OPTIONS:
 DGT MWT STD N N N

26.8.2 EXAMPLE 2: the MWI agent resides within the REMOTE switch

In this case, there are two possibilities:

- ALLOW_NAC is Y, which corresponds to the Called DN in the outgoing TCAP msg., could be started with NAC (National Access Code).
- ALLOW_NAC is N, which corresponds to the Called DN in the outgoing TCAP msg., could not be started with NAC, and NAC is stripped.

TABLE: OFCENG

NATIONAL_ACCESS_CODE	0

26.8.2.1 The example for ALLOW_NAC is Y.

TABLE: ISERVOPT

EMWI EMWI 100 Y

The VM sends the MWI request for the DN '0297835304', the local DMS decides to send the EMWI TCAP message (which means the MWI agent is in the remote office) if the following conditions are met:

- There should be no agent associated with this DN in the originating (local) office
- The translation should be terminated to the EISUP trunk

The translation example in the local office would be like:

```
>traver l 1027835466 0297835304 b
TABLE IBNLINES
HOST 02 0 00 10 0 DP STN IBN 7835466 CUST783 0 0 102 $
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
CUST783 0 0 0 $ ( XLAS NETXLA STARCEPT NDGT) ( OCTXLA OCTCEPT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783 NXLA NETXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE IBNXLA: XLANAME NETXLA
TUPLE NOT FOUND
Default from table XLANAME:
NETXLA
  (NET N Y 0 N NDGT N Y GEN (LATTR 1 102_NPRT_1 NLCA_NILLA_1) $ $) $ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
1 IBN NONE NT 0 0 NILSFC 0 PX NETXLA NIL 00 102_NPRT_1 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
NETXLA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:          0297835304
TABLE PXCORE
NETXLA 029783 029783 RTE ( DEST 151) ( CLASS NATL)$
TABLE: PXRTE
KEY: NETXLA 151
.S OGISP2AB
EXIT TABLE PXRTE
INAP Info Analyzed TDP: no subscribed trigger.
INAP Route Select Failure TDP: no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 OGISP2AB          0297835304          ST

TREATMENT ROUTES. TREATMENT IS: GNCT
1 MESAJ4
2 2WIBN7AB

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>clliref search OGISP2AB (verifying that it's the EISUP trunk)
CLLI "OGISP2AB" occurs in the following tuples:
Table  Key: Sub Tuple
----->-----
CLLI      OGISP2AB 215 200 OG_CCITT_Q767_ISUP_TRK
TRKGRP    OGISP2AB IBNTO 0 NPDGP NCRT CUST783 0 MIDL ANSDISC 0 N 0 0 0 Y N N N N NATL $
PXRTE     NETXLA 151 (S OGISP2AB) $
ISUPDEST  OGISP2AB 0 AB_ROUTES
PSTNTRK   OGISP2AB N
N7TRKMEM  OGISP2AB 0 3 10
CLLIMTCE  OGISP2AB OGISP2 5 10 15 NSS 0 0 N N (1)
TRKSGRP    OGISP2AB 0 DS1SIG C7UP OG N N UNEQ NONE Q767 THRH 0 DMS N N BASE 100_WHITE $ OGN7
TRKMEM    OGISP2AB 0 0 PDTC 12 2 7
TRKNAME    215 OGISP2AB
C7TRKMEM   OGISP2AB 0 106
=====
Total of      11 occurrences of OGISP2AB
```

And, when the incoming TCAP message is received in the remote switch, it is translated according to the line attribute datafilled in the DEFAULT_MWI_XLA_ENTRY (datafilled as ‘100’ in the example) as follows:

```
>traver tr icisp2ba 0297835304 b
TABLE TRKGRP
```

ICISP2BA IBNTI 0 NPDGP NCRT CUST783 0 2 7675451 ANSDISC 0 Y N N N N Y 0 0 N N
 N N N \$ NATL \$
 TABLE CUSTSTN
 TUPLE NOT FOUND
 TABLE OFCVAR
 AIN_OFFICE_TRIGGRP NIL
 INAP Origination Attempt TDP: no subscribed trigger.
 TABLE NCOS
 TUPLE NOT FOUND
 TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
 CUST783 NXLA NETXLA NXLA 0 NDGT
 TABLE DIGCOL
 NDGT specified: digits collected individually
 INAP Info Collected TDP: no subscribed trigger.
 TABLE IBNXLA: XLANAME NETXLA
 TUPLE NOT FOUND
 Default from table XLANAME:
 NETXLA
 (NET N Y 0 N NDGT N Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) \$ \$)\$ 9
 TABLE DIGCOL
 NDGT specified: digits collected individually
 TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 0 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1 \$
 LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
 TABLE XLAPLAN
 102_NPRT_1 NSCR 102 NPRT NONE N \$ GG
 TABLE RATEAREA
 NLCA_NILLA_1 NLCA NIL NILLATA \$
 TABLE PXHEAD
 PTTXLA DFLT TRMT (OFC VACT)\$ NODFOP NOCON F
 THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 0297835304
 TABLE PXCORE
PTTXLA 029783 029783 DNRTE (DN 029 783)\$
 TABLE TOFCNAME
 029 783 \$
 TABLE DNINV
 029 783 5304 L HOST 02 0 00 18
 TABLE DNFEAT
 TUPLE NOT FOUND
 TABLE DNATTRS
 TUPLE NOT FOUND
 TABLE DNGRPS
 TUPLE NOT FOUND
 INAP Info Analyzed TDP: no subscribed trigger.
 INAP Route Select Failure TDP: no subscribed trigger.
 INAP Termination Attempt TDP: no subscribed trigger.

 +++ TRAVER: SUCCESSFUL CALL TRACE +++

 DIGIT TRANSLATION ROUTES

 1 LINE 0297835304 ST

 TREATMENT ROUTES. TREATMENT IS: GNCT
 1 MESAJ4

 +++ TRAVER: SUCCESSFUL CALL TRACE +++

26.8.2.2 The example for ALLOW_NAC is N.

TABLE: ISERVOPT

EMWI EMWI 100 N

The translation in the local switch is the same as in the previous case where ALLOW_NAC is Y. The difference here is the EMWI TCAP msg. sent to the local office includes the called DN as '297835403' because NAC is stripped from the called DN.

So that, in this case translation in the terminating office should be like:

```
>traver tr icisp2ba 297835304 b
TABLE TRKGRP
ICISP2BA IBNTI 0 NPDGP NCRT CUST783 0 2 7675451 ANSDISC 0 Y N N N N Y 0 0 N N
  N N N $ NATL $
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP: no subscribed trigger.
TABLE NCOS
TUPLE NOT FOUND
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CUST783 NXLA NETXLA NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
INAP Info Collected TDP: no subscribed trigger.
TABLE IBNXLA: XLANAME NETXLA
TUPLE NOT FOUND
Default from table XLANAME:
NETXLA
  (NET N Y 0 N NDGT N Y GEN (LATTR 100 102_NPRT_1 NLCA_NILLA_1) $ $) $ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
100 NLCC NONE NT 0 0 NILSFC 0 PX PTTXLA NIL 00 102_NPRT_1 NLCA_NILLA_1 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
102_NPRT_1 NSCR 102 NPRT NONE N $ GG
TABLE RATEAREA
NLCA_NILLA_1 NLCA NIL NILLATA $
TABLE PXHEAD
PTTXLA DFLT TRMT ( OFC VACT)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:          297835304
TABLE PXCODE
PTTXLA 29783 29783 DNRTE ( DN 029 783)$
TABLE TOFCNAME
029 783 $
TABLE DNINV
029 783 5304 L HOST 02 0 00 18
TABLE DNFEAT
TUPLE NOT FOUND
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
INAP Info Analyzed TDP: no subscribed trigger.
INAP Route Select Failure TDP: no subscribed trigger.
INAP Termination Attempt TDP: no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 LINE          0297835304          ST

TREATMENT ROUTES. TREATMENT IS: GNCT
1 MESAJ4

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

27: A00007329 Functional description (FN)

27.1 Feature name

International H.323 2CLI (Calling Line Identity) Support

27.2 Description

The activity provides support for 2 CLI delivery to an International H.323 terminator and provides support to the following originating/terminating agent combinations:

- International H.323 -> ETSI ISUP v2 Base Variant
- ETSI ISUP v2 Base Variant -> International H.323
- International H.323 -> ETSI PRI
- ETSI PRI -> International H.323
- International H.323 -> International H.323
- SPIROU -> International H.323
- International H.323 -> SPIROU

The 2CLI functionality is associated with ISDN supplementary service provisioning option Calling Line Identification Presentation (CLIP) and Calling Line Identification Restriction (CLIR). With 2CLI the calling line has two identities, namely the Network Number (NN) and Presentation Number (PN).

A Network Number is a CLI which identifies the actual network termination point from which a call originates. The Presentation Number (PN) is a dialable number that the calling user wishes to display to the called user. The PN can be used to return a call to the originator. The NN and PN may or may not be the same. 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 2CLIs are delivered in the SETUP message by sending one CLI in the CGN IE (Calling Party Number Information Element) field and the other in the UUIE sourceAddress field.

This feature extends the existing functionality implemented by MMP14 feature A59016672 that developed 2CLI delivery for an ETSI PRI terminator to enable 2CLI support for an International H.323 terminator. Feature A59016672 works only in conjunction with feature “Presentation CLI Support” which is enhanced to support Special Arrangement on selected agents. The “Special Arrangement” feature, that was introduced by AJ5284, was developed to give selected customers the possibility to deliver Calling Party Numbers to the terminator that are not screened. So the number shown to the called user is not the real access number.

If Special Arrangement applies to a customer, the CGN digits delivered by him are not screened, but the NPI (Number Plan Indicator) and TON (Type of Number) information elements are screened.

This feature A00007329 will require that several datafill conditions be met by the call environment, similar to those required for A59016672, as A00007329 extends existing functionality implemented by A59016672. Details are included in the following section Figure 27.2.1, “2CLI Delivery Control for International H.323 Terminator”.

The mapping of 2 CLIs between H.323 and ISUP provided by this activity is in accordance with H.246 Annex C, building on the activity 59027509 that implemented 2CLI delivery between ETSI PRI and ETSI ISUP v2/SPIROU based on Q.699 and French specific requirement.

27.2.1 2CLI Delivery Control for International H.323 Terminator

The 2CLI functionality for a International H.323 terminator can be enabled on a trunk group basis by data filling the 2CLI option on the H.323 QSIG trunk. A sample datafill in table LTDATA is as follows:

Table 1 Table LTDATA - Datafill 2CLI Option (New Datafill)

LTDKEY	LTDRSLT	LTCLI_OPTION	LTCLI_OPTION
QSIG 2 CLI	CLI	2CLI	\$

The 2CLI is an existing option in table LTDATA. When the “2CLI” option is not data filled the QSIG interface will not generate 2CLI’s in the outgoing SETUP message. The delivery of the 2CLIs to a International H.323 terminator is dependent on several factors in addition to this option:

- CLIR option provisioned for the originator
- CLIP option provisioned for the terminator
- Screening for originator (Table LTDATA)
- CUSTGROUP public call (relation between originator and terminator)
- Presentation Number and Special Arrangement Applies to the originator

- PN_SUPPORTED = Y

27.2.1.1 CLIR option Table LTDATA (Existing Datafill)

The CLIR option is applicable for ETSI PRI and International H.323 originators. Sample datafill for the International H.323 originator is illustrated in the following table.

Table 2 Table LTDATA CLIR option

LTDKEY	LTDRLT	LTCLI_OPTION	PI	MODE
QSIG 1 CLI	CLI	DFLTPI	ALLOW	TEMP

27.2.1.2 CLIP option Table LTDATA (Existing Datafill)

The CLIP option is applicable to ETSI PRI and the International H.323 terminator. Sample datafill for the International H.323 terminator is as follows:

Table 3 Table LTDATA CLIP option

LTDKEY	LTDRLT	CGNDELV	CDNDELV
QSIG 1 CLI	SERV	SCREENED	ALWAYS

27.2.1.3 Screening in Table LTDATA (Existing Datafill)

This SCRNLTIID and SCRNDFLT option is applicable to ETSI PRI and the International H.323 as originator.

For the International H.323 the customer group will be datafilled in table LTCALLS or table LDATA. First of all the datafill in table LTCALLS is looked up. If there is no entry for the customer group, then the entry from table LTDATA is taken to determine the customer group. The concatenation of the NDC and DFLTSN entries gives the “Network provided number” which is provided to the terminator when Special arrangement applies or 2CLI applies to the terminating agent.

Table 4 Table LTDATA

LTDKEY	DATATYPE	OPTION	NDC	DN	DNBLKS	OPTION	DFLTSN	DFLTCGRP
QSIG 1 CLI	CLI	SCRNLTIID	131	8304	\$	SCRNDFLT	83040	CSLINES

27.2.1.4 CUSTGROUP Table CUSTNTWK (Existing Datafill)

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.

27.2.1.5 Presentation Number and Special Arrangement Applies (Existing Datafill)

This option is applicable for ETSI PRI and International H.323 originator. Sample datafill for the Presentation number and Special Arrangement for an International H.323 originator is as follows:

Table 5 Table LTDATA

LTDKEY	DATATYPE	OPTION	OPTION
QSIG 1 CLI	CLI	NOSCRN	SCRNPN

27.2.1.6 PN_SUPPORTED Table OFCENG (Existing Datafill)

This option is applicable for ETSI ISUP V2, SPIROU, ETSI PRI and International H.323. Datafill for the PN_SUPPORTED option is illustrated below:

Table 6 Table OFCENG

PARMNAME	PARMVAL
PN_SUPPORTED	Y N

27.2.2 2CLI Mapping for Interworking Scenarios Supported:

27.2.2.1 International H.323 to ETSI ISUP V2

The Calling Party Number parameter and the Generic Number parameter in the IAM shall be set as per the French National requirement document “CLI Handling between ISUP V2, SPIROU and Access Protocols NC/France/22 V1.0”.

27.2.2.1.1 Calling Party Number (CGPN) in the IAM

The CGPN in the IAM contains the line installation number and is set to the default number DFLTCGN stored in table LTDATA (for the International H.323 originator). Sample datafill for the default number datafilled for the International H.323 originator is as follows:

Table 7 Datafill for DFLTCGN option for International H.323

LTDKEY	LTDRSLT
QSIG 1 DN	DN 141 822 6035 \$

The CGPN values with the default number datafilled are as per the following table, the screening indicator is set to “Network Provided”.

Table 8 Coding of the Calling Party Number Parameter with DFLTCGN

Field	Value
"Odd/ even indicator"	- 0: even number of address signals - 1: odd number of address signals
"Nature of address indicator":	based on EDITCLI TON INTL - 00000011: national significant number - 00000100: international number
"Number complete indicator"	- 0: complete
"Numbering plan indicator"	- 001: ISDN numbering plan (E.164)
"Address presentation restricted indicator"	"Address presentation restricted indicator" is set according to the CLIR Supplementary Service: - 01: presentation restricted: a) if the subscriber has the restrict perm option, b) if the subscriber has the restrict temp option and no presentation indicator is received in the SETUP. c) if the presentation indicator received in the SETUP message is set to presentation restricted. - 00: presentation allowed in any other case. Note: DEFLTPI is assumed to be datafilled.
"Screening indicator"	- 11: network provided
Address signals	Address signals is set with the default number in table LTDATA.

Datafill in table LTDATA for DEFLTPI for option Restrict Temp, Restrict Perm and Allow Temp are as follows:

Table 9 Datafill for DFLTCGN option for International H.323

LTKEY	LTDRSLT
QSIG 1 CLI	CLI (DFLTPI RESTRICT TEMP)\$
QSIG 1 CLI	CLI (DFLTPI RESTRICT PERM)\$

Table 9 Datafill for DFLTCGN option for International H.323

LTDKEY	LTDRSLT
QSIG 1 CLI	CLI (DFLTPI ALLOW TEMP)\$

If the default number is not available, the Calling Party Number contains no address signal and is coded as follows, the Screening Indicator is set to Network Provided:

Table 10 Coding of the Calling Party Number Parameter with DFLTCGN

Field	Value
"Odd/ even indicator"	- 0: even number of address signals
"Nature of address indicator":	- 00000011: national significant number
"Number complete indicator"	- 0: complete
"Numbering plan indicator"	- 001: ISDN numbering plan (E.164)
"Address presentation restricted indicator"	- 10: address not available
"Screening indicator"	- 11: network provided
Address signals	None

27.2.2.1.2 Generic Number Parameter in the IAM

The Generic Number parameter is derived from the CGPN IE of the SETUP message. The address signals of the Generic Number is set with the address of the CGPN IE received in the SETUP message.

If no CGPN IE is received in an incoming SETUP message, then no Generic number parameter will be generated in the outgoing IAM. If two calling party numbers are received in the H.323 SETUP¹ message, they shall be mapped to the outgoing IAM as follows:

H.225 UUIE srcAddress <-> QSIG 1. CGN <-> ISUP Generic number

H.225 CGN <-> QSIG 2. CGN <-> ISUP Calling party number

¹The mapping of 2CLIs from ETSI PRI to ETSI ISUP v2 Base Variant as per Requirement Document NC/France/22 v1.0 states that - If two calling party number IE are received in the SETUP message, the first IE shall be taken into account for this section. The second IE is ignored. However, the 2CLI mapping being implemented by this feature is as per the FT requirement.

The above mapping shall apply only for a H.323 transit scenario i.e. ETSI ISUP v2--> International H.323 --> ETSI ISUP v2. In order to obtain the mapping of parameters as indicated above, it is imperative that the DFLTCGN for the International H.323 trunks not be datafilled in table LTDATA.

For H.323 access trunks, if 2CLIs are to be generated to an ETSI ISUP v2 Base Variant terminator then the DFLTCGN for the International H.323 access trunk must be datafilled in table LTDATA.

The coding of the Generic Number parameter if Special Arrangement applies to the International H.323 originator with the NOSCRN option datafilled in table LTDATA is as per Table 12, "Coding of the Generic Number with Special Arrangement," on page 363, the Screening Indicator is set to "User Provided Not Verified".

Sample datafill for the NOSCRN option in table LTDATA for the International H.323 terminator is as follows:

Table 11 Datafill for NOSCRN option for International H.323

LTDKEY	LTDRSLT
QSIG 1 CLI	CLI (NOSCRN)\$

Table 12 Coding of the Generic Number with Special Arrangement

Field	Value
"Number qualifier indicator":	- 00000110: additional calling party number
"Odd/ even indicator"	- 0: even number of address signals - 1: odd number of address signals
"Nature of address indicator"	"Nature of address indicator": See Table 5
"Number complete indicator"	See Table 5

Table 12 Coding of the Generic Number with Special Arrangement

Field	Value
"Address presentation restricted indicator"	"Address presentation restricted indicator" is set according to the CLIR Supplementary Service: - 01: presentation restricted: a) if the subscriber has the restrict perm option, b) if the subscriber has the restrict temp option and no presentation indicator is received in the SETUP. c) if the presentation indicator received in the SETUP message is set to presentation restricted. - 00: presentation allowed in any other case. Note: this parameter shall never be used for the CLIP service.
"Screening indicator"	- 00: all the values of the screening indicator received in the "calling party number" shall be mapped to user provided, not verified
Address signals	The "address signal" field is set with address signals received in the "calling party number".

The values of NOA and NPI in the Generic Number parameter are as per the following table.

Table 13 NPI and NOA mappings

NPI of SETUP message in incoming CgPN	TON of SETUP message in incoming CgPN	NPI of GNP in the outgoing IAM	NOA of GNP in the outgoing IAM
Unknown (0000)	Unknown (000)	E.164	National
Unknown (0000)	National (010)	E.164	National
Unknown (0000)	International (001)	E.164	International
Unknown (0000)	Subscriber	No GNP	No GNP
E.164 (0001)	Unknown (000)	E.164	National
E.164 (0001)	National (010)	E.164	National
E.164 (0001)	International (001)	E.164	International
E.164 (0001)	Subscriber	No GNP	No GNP
Private (1001)	Unknown (000)	Private	National
Private (1001)	National (010)	Private	National
Private (1001)	International (001)	Private	International
Private(1001)	subscriber number(100)	Private	Subscriber number

27.2.2.2 ETSI ISUP v2 Base Variant to International H.323

There are three possible cases:

27.2.2.2.1 “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 CLIP¹ supplementary service, then:

¹Data filled in table LTCDATA for the International H.323 terminator

Sample Datafill:

LTDKEY LTDRSTL CGNDELV CDNDELV

QSIG 1 CLI SERV SCREENED ALWAYS

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 14 Generic Number mapped to CGPN 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.
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 “calling party number” IE containing the “calling party number” shall be created. This IE is inserted after an eventual “calling party number” corresponding to the “generic number”. This IE contains the address signal received in the IAM and is coded as follows:

Table 15 Calling Party Number in SETUP Message (International H.323)

Bits	Value	
Octet 3 bits 765	Type of number is coded according to bits BA of identity of calling line	
	Received in IAM	Coding
	-10 -11	-National number - International number
Octet 3 bits 4321	Numbering Plan Identification -0001 E.164 ISDN	
Octet 3a bits 76	Presentation indicator is mapped transparently	
Octet 3a bits 21	Screening Indicator is mapped transparently	
Octet 4 and above	Address signals	

Note: The Presentation indicator of the GNP is not taken into account for the CLIP service.

27.2.2.2.2 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 16 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)

27.2.2.2.3 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 17 "Calling Party Number" in SETUP

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 restricted (01).
Octet 3a bits 21	"Screening indicator" is set to network provided (11)

27.2.2.3 SPIROU to International H.323

The CLI handling is the same as Figure 27.2.2.2, "ETSI ISUP v2 Base Variant to International H.323".

27.2.2.4 International H.323 to SPIROU

The mapping of Calling Party Number and Generic Number Parameter in the IAM from the SETUP message are as described in Figure 27.2.2.1, "International H.323 to ETSI ISUP V2" except that the “Nature of Address

Indicator” in the “Calling Party Number” parameter shall be set to “National Significant Number”.

27.2.2.5 Other supported interworking scenarios

Transparent parameter mapping shall be done for each of the following interworking scenarios:

- International H.323 -> ETSI PRI
- ETSI PRI -> International H.323
- International H.323 -> International H.323

27.3 Hardware Requirements or Dependencies

The H.323 Gateways must have the capability to transmit and receive 2CLIs.

27.4 Software Requirements or Dependencies

None

27.5 Limitations and restrictions

- 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.
- No CLI screening and editing is performed for the 2nd CLI which is started to be reported by this activity.
- For H.323 transit trunks the SCRNP and default PN option must not be assigned in table LTDATA.
- The NOSCRN option in table LTDATA is mandatory for the 2CLI mapping in the transit International H.323 to ETSI ISUP v2 Base Variant / SPIROU interworking scenario.
- The DFLTCGN option in table LTDATA must not be datafilled for transit International H.323 trunks.
- If only a CGN2 is received in the incoming SETUP message for the International H.323 originator, it shall be mapped to the CGPN in the outgoing IAM.

27.6 Interactions

None

27.7 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 following table 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 CGPN IE present, that have been verified by this feature.

AMACLID_IC_PRI_CGN is a option present in table AMAOPTS.

Table 18 Digits captured in Module 046 and the OOD of the AMA record

BILLDN	AMAC LID	Deflecting table LTDATA	AMACLID_IC_PRI_CGN	OOD (AMA Base Record)*	Screening/Editing of Incoming CLI provisioned?	OOD MODULE 46
-	TRUE	Datafilled	-	DFLCGN from table LTDATA.	-	-
-	TRUE	No		CLI from the SETUP message.	-	-
Datafilled	TRUE	No	ON	BILLDN	CLI Screening Passes	Unscreened/Unedited CLI (CLI from the SETUP message).

Table 18 Digits captured in Module 046 and the OOD of the AMA record

BILLDN	AMAC LID	Deflecting table LTDATA	AMACLI D_IC_PRI _CGN	OOD (AMA Base Record)*	Screening/ Editing of Incoming CLI provisioned?	OOD MODULE 46
Datafilled	TRUE	Datafilled	OFF	BILLDN	CLI Screening Passes	Screened/Edited CLI (DFLT CGN from table LTDATA)
Datafilled	TRUE	No	ON	BILLDN	N	CLI from the SETUP message. If AMACLI D_IC _PRI _CGN is OFF then 0's only are appended to the module 046.
-	-	No	-	CLI from the CGPN IE in the SETUP message	Screening passes or screening fails.	-
Datafilled	-	No	-	BILLDN	Screening passes or screening fails	-

The incoming 2nd CGN IE in the SETUP message that is starting to get reported by this feature is not captured in the AMA record.

The incoming 2nd CGN IE reported by this feature is not captured in the AMA record.

Performance (includes operational measurements) __N/A__

27.8 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

27.9 References

Table 19 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	Interworking between ISDN Access and Non-ISDN Access over ISDN User Part of Signalling System No. 7
H.246.0 Annex C	ISDN User Part Function - H.255.0 Interworking

28: A00007349 Functional description (FN)

28.1 Feature name

CPC Screening support for FDCP Trunks

28.2 Description

This feature implements Calling Party Category (CPC) routing on the MMP-100 for MFC trunks using the FDCP platform. The global CPC routing functionality was implemented on the DMS-MMP by feature AJ5343 “*Calling Party Category Routing*” and by feature A59028780 “*Call Control and Universal Screening*”. Our feature does not attempt to change the existing CPC routing functionality, but rather to allow FDCP trunks to support CPC routing. All the FDCP variants will be supported.

There is the feature A59014287 in MMP-100 that provides CPC routing for Brazilian R2/MFC trunks. However, the use of this feature was limited due to MFC signalling limitations allowing requests to CPC only after all the called digits were already collected. It really restricts use of CPC routing for such call scenarios as overlap or end-to-end, which are routed to the terminator in the early stages of digit collection before CPC is received.

The FDCP platform allows “quick” request of CPC in the earliest stages of digit collection, after the 1st called digit or after the 1st digit report. It is very important that early CPC request does not include the request of the calling number that “eats” a lot of real time.

This feature adds CPC routing support for FDCP incoming trunks based on the quick CPC request. This feature is based on the possibility of the FDCP platform getting CPC not only as a result of the CPC / CLI request (in the SMP_EVENT_INFO message) but also after the first called digit (in the SMP_SETUP_REQUEST message). It is handled by the option QUICK_REQ in the R2PROT table.

The detailed description of ‘**CPC Screening support for FDCP Trunks**’ requirements may be found in the Product Spec “New flow of signals and restriction of incoming call in according calling party category (CPC)”, (see **CPC_TRANSLATION.AA01** in the TLDOC library).

28.2.1 CPC screening - General

This feature should provide CPC screening for FDCP incoming calls. This category may be received, CPC is received either in SMP_EVENT_INFO message or in SMP_SETUP_REQUEST message. For more details see section 28.2.1.3.

The general view of the feature functionality is shown below. In Figure 1 the CPC is received in the SMP_EVENT_INFO message as result of CPC/CLI request. In Figure 2 the CPC is received in the SMP_SETUP_REQUEST message.

The CPC screening process is not described here, for more information please refer to the documents AJ5343, A59028780 or A59014287. The brief description of the tables used by the CPC screening is found below in 28.2.1.1 “CPC screening using CPCRTE option.” on page 375 and in 28.2.1.2 “CPC screening using CALLCNTL table.” on page 376

Figure 1 CPC as result of CPC/CLI request (in SMP_EVENT_INFO).

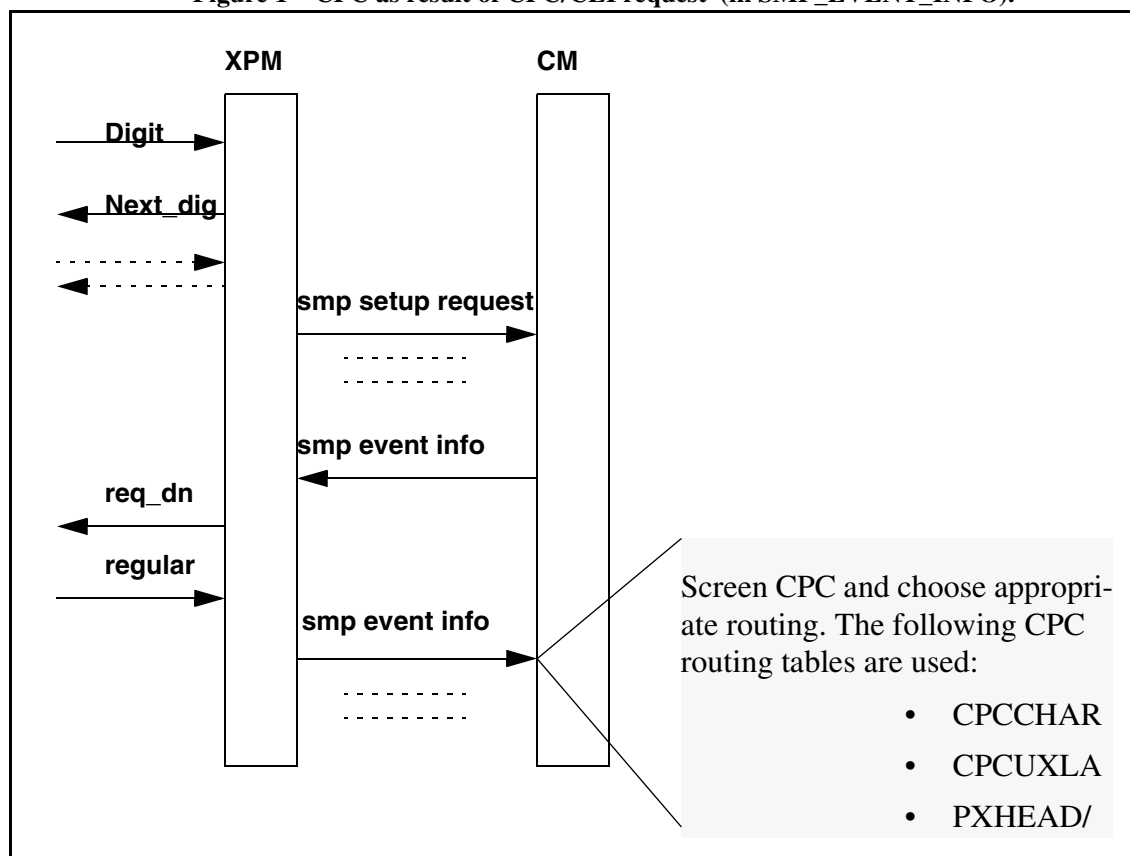
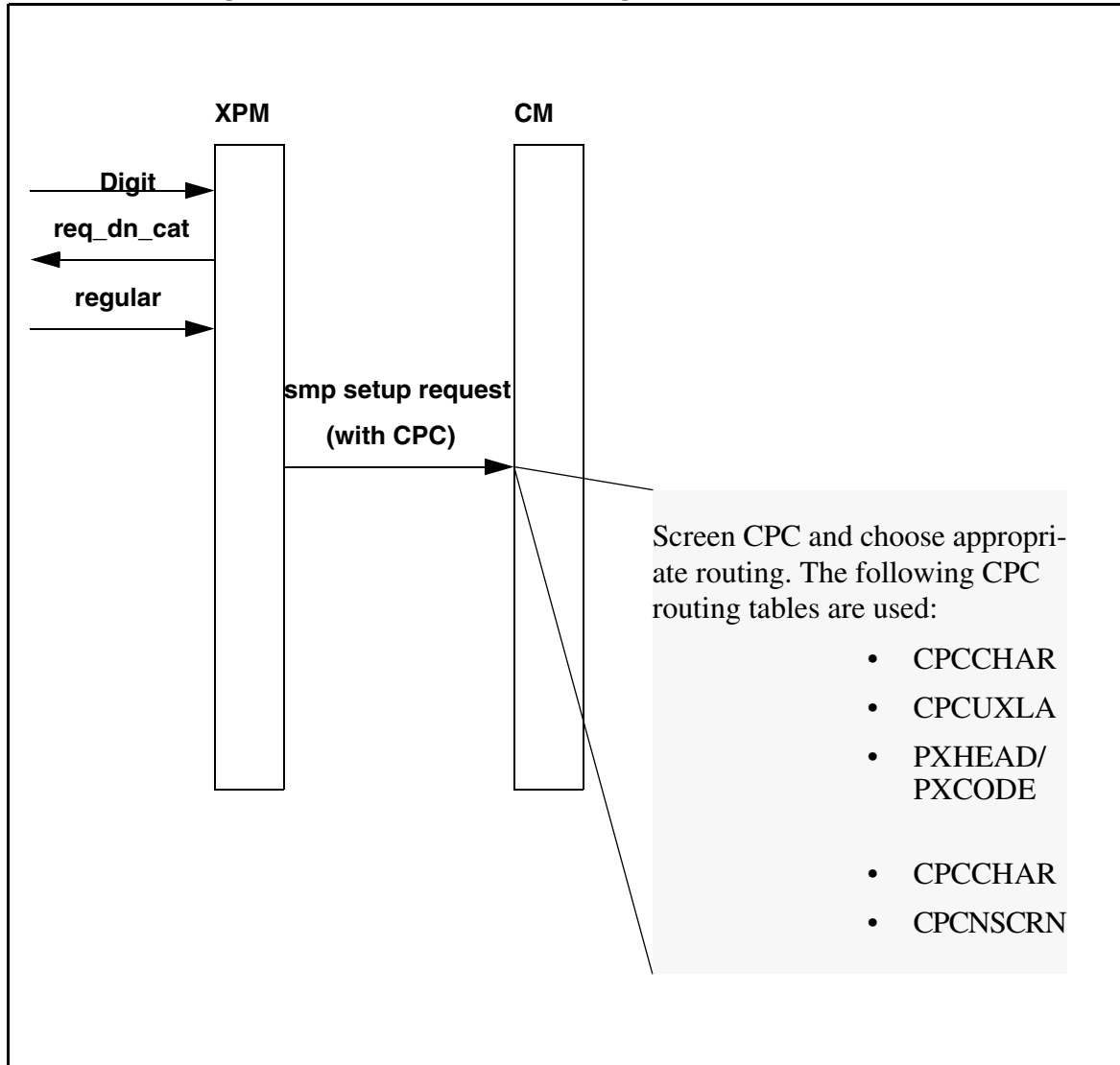


Figure 2 CPC after the first called digit (in SMP_SETUP_REQUEST).



28.2.1.1 CPC screening using CPCRTE option.

For CPC screening, for FDCP incoming calls, the QUICK_REQ option in table **R2PROT** should be defined with the value CAT_AFTER_1_DIG or ANI_AFTER_1_DIG. For more details see 28.2.1.3 “Quick Category Request in FDCP platform - background.” on page 376

This is the usual method of CPC screening, which is described in detail in the documents AJ5343 and A59014287. We illustrate here a brief description of CPC routing for this case.

The CPC screening is based on use of the **CPCRTE** option in the **xxHEAD/xxCODE** tables. The following tables are used to control CPC screening.

- Table **CPCCHAR** - assigns a unique name to a set of one or more protocol specific CPC values. This name is the **CPCNAME** key, it is then used to route the call. The detailed description of changes in this table is found in section 28.2.2.
- Table **CPCUXLA** - performs routing based on **CPCNAME** for the Universal translation system. This table matches a **CPCNAME** and a current Universal translation name datafilled in **xxHEAD/xxCODE** tables. If a match is found, the alternative route is chosen.
- Option **CPCRTE** - triggers entry into the **CPCUXLA** table. This option is assigned in the **xxHEAD/xxCODE** translation tables. If the **CPCRTE** option is encountered, the table **CPCUXLA** is used to route the call based on **CPCNAME**.

28.2.1.2 CPC screening using **CALLCNTL** table.

For CPC screening, for FDCP incoming calls, the **QUICK_REQ** option in table **R2PROT** should be defined with the value **CAT_AFTER_1_DIG** or **ANI_AFTER_1_DIG**. For more details see 28.2.1.3 “Quick Category Request in FDCP platform - background.” on page 376

The method is controlled by the **TRKOPTS** and **CALLCNTL** tables (See feature A59028780). The following tables are used here:

- Table **TRKOPTS** - defines the **CCNTLIDX** option for the incoming trunk, which triggers entry into **CALLCNTL** table.
- Table **CALLCNTL** - refers to the appropriate index in table **CPCNSCRN** according to the **SCRN_OPTION**.
- Table **CPCNSCRN** - performs alternative route based on **CPCNAME** from the **CPCCHAR** table.
- Table **CPCCHAR** - assigns a unique name to a set of one or more protocol specific CPC values. This name is the **CPCNAME** key, it is then used to route the call. The detailed description of changes in this table is found in section 28.2.2.

28.2.1.3 Quick Category Request in FDCP platform - background.

In order to implement CPC screening for the FDCP protocol, category should be delivered early enough, before the translation process is completed. In MFC, calls CPC (and CLI) are usually requested after all the called digits are already collected in the switch. At this stage translation is already completed.

In order to provide category in the proper time, we use the **QUICK_REQ** option in the **R2PROT** table for FDCP incoming trunks with one of the following values: **ANI_AFTER_1_DIG** or **CAT_AFTER_1_DIG**. See the datafill examples below.

Figure 3 Datafill of R2PROT table**TABLE R2PROT**

GEOPROT (40 41 40 41) (42 43 42 43) (40 44 44 41) (42 44 44 43)
 (42 43 42 46) \$ GEORGOG GEORGIC FDCP GEORGCAT
(QUICK_REQ ANI_AFTER_1_DIG)\$
 GEOPROT1 (40 41 40 41) (42 43 42 43) (40 44 44 41) (42 44

The option **QUICK_REQ** in the R2PROT table, introduced by the feature A59011824, allows request of CPC / CLI at the earliest stages of the call. The possible values of **QUICK_REQ** are:

- **CAT_AFTER_1_DIG** - CPC without CLI is requested after the 1st called digit
- **CAT_AFTER_LAST_DIG** - CPC without CLI is requested after all the called digits are collected
- **ANI_AFTER_1_DIG** - CPC and CLI are requested after the 1st called digit
- **ANI_AFTER_1ST_REP** - CPC and CLI are requested after the 1st report, **SMP_SETUP_REQUEST** message was received in CM.

As mentioned above, the values **CAT_AFTER_1_DIG** and **ANI_AFTER_1_DIG** should be used.

If the option **QUICK_REQ ANI_AFTER_1_DIG** is defined in the R2PROT table, the CPC that was received after the first called digit as a result of the CPC / CLI request is provided, as usual, in the **SMP_EVENT_INFO** message.

For option **QUICK_REQ CAT_AFTER_1_DIG** in the R2PROT table, the CPC, that was received after the first called digit as a result of the CPC request, is included in the **SMP_SETUP_REQUEST** message in field “Calling Party Category”.

In Figure 4 below, the **MP_SETUP_REQUEST** is received with 3 called digits and with the **MTC_EQ** category (decimal value 18).

Figure 4 After the first called digit (SMP_SETUP_REQUEST message) with CPC.

```

INCOMING 12:20:15.877 NODE TYPE= LTC_NODE SMP_SETUP_REQUEST_MSG
NN= 0064 TN= 0142 MSGTAG= 00 ROUTE= 4000 ERROR= 00
LENGTH= 21
AGENT= CKT      ORIRM2  1
09 03 14 00 00 B8 00 01 12 81 1F 00 F0 DF FF FF 02 00 03 8F 00 3F A5
0A 00

```

Message Type: SMP_SETUP_REQUEST_MESSAGE
Fixed Part:

Message Length: 20
Format Discriminator: 00
Map to SMP Bool: N
Protocol Variant: FDCP_BASIC
Protocol Class: CLASS_PTS

Progress Indicator Location: NIL PI LOCATION
Progress Indicator Description: NIL PI DESCRIPTION
Bearer Capability Name: SPEECH
Emergency Setup Message: N
Calling Party Category: 18
Calling Party Category Class: UNKNOWN
Local Setup Ack bool: N
Set Data : NOT REQUIRED
User Rate: NIL
ITC name: SPEECH
Teleservice: TELEPHONY
Transaction Id Value: 0
Transaction Id Flag: THIS SIDE ORIG
Setup Request Status Fields:

Satellite: NONE
Continuity: NIL
Echo Suppressor: NIL
National: NIL
End to End Method: NIL
Routing control indicator: RCI NOT ALLOWED
Interworking: NIL
End to End Information: NIL
C7 Indication: NIL
C7 Preferred: NIL
ISDN Originator Access: NIL
Verify Answer Time: NIL
Cross Border: NIL
Calling Number Incomplete: NIL

28.2.2 Routing for Matched CPC using CPCRTE option.

Table CPCCHAR is used to convert the protocol's CPC value into a generic protocol independent CPCNAME. This CPCNAME is then used for routing the call.

Each tuple in CPCCHAR comprises of a CPCNAME followed by a list of protocols. Currently valid protocols are: BTUP, BZR2, ETSIISUP, FTUP, BZISUP, REDBKTUP and BZTUP.

This feature adds to this set the **FDCP** protocol for MFC trunks using the FDCP platform. The fields in the CPCCHAR table for the FDCP protocol are shown in the table below.

Table 1 Field entries to CPCCHAR table for FDCP protocol

Field	Entry	Range
CPCNAME (key)	Unique CPCNAME	Alphanumeric
PROTOCOL	Protocol selector	FDCP
FDCP refinement	List of 1 to 16 CPC values	CP_ACTIVITY type

Example of CPCCHAR datafill for the FDCP protocol can be seen below.

Figure 5 Example of CPCCHAR datafill for FDCP protocol

TABLE: CPCCHAR	
CPCKEY	PROTLIST

BLOCKCPC (FDCP (MTC_EQ) (LOCAL_COIN) \$) \$	

When an incoming FDCP call CPC is received, the procedure CPCCHAR_PARAMETER_LOOKUP is used to pass a cpcchar protocol ID (in our case - FDCP) and the received CPC. It then searches table CPCCHAR for a match. If a match is found, it stores the CPCINDEX for the matching tuple in the extension block.

If one of the categories mentioned in the list above (see Figure 5) is received, the call is sent to the alternative route according to the table CPCUXLA.

Example of TRAVER for the CPC is found below, (see Figure 6). The table CPCCHAR is filled as shown above in Figure 5. The category received is LOCAL_COIN.

Figure 6 Traver for CPC as result of CPC / CLI request (in SMP_EVENT_INFO).

```

>traver tr orirm2 500002 b
TABLE TRKGRP
ORIRM2 IBNTI 0 LCO NCRT TRKPSTN 0 0 N ANSDISC 0 N N N N
N N N 0 0 N N N N N $
    NATL (ANIREC ALWAYS) (ANIFAIL CONT ) $
Originator is not an EIN agent, therefore EIN info is not processed.
TABLE NCOS
TRKPSTN 0 0 0 TRK ( XLAS PRTRK0 NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA,
FEATXLA, VACTRMT, AND DIGCOL
TRKPSTN NXLA CXTRK NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
Originator is not an EIN agent, therefore EIN info is not processed.
TABLE IBNXLA: XLANAME PRTRK0
TUPLE NOT FOUND
Default from table XLANAME:
PRTRK0
    (NET N N 0 N NDGT N Y GEN (LATTR 1000 TRKPLAN
NLCA_NILLA_0) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
1000 NLCC NONE NT 0 0 NILSFC 7 PX TAND NIL 00 TRKPLAN
NLCA_NILLA_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
TRKPLAN NSCR 250 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_0 NLCA NIL NILLATA $
TABLE PXHEAD
TAND DFLT CONT ( XLT PX TANDPXLA)$ NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
500002
TABLE PXCODE
TUPLE NOT FOUND
DEFAULT FROM HEAD TABLE USED
TABLE PXHEAD
TANDPXLA SDFLT NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:
500002
TABLE PXCODE
TANDPXLA 5 5 RTE ( MM 6 6) ( DEST 5) ( CLASS NATL) (
CPCRTE)$

```

28.2.3 Routing for Matched CPC using CALLCNTL table.

In the same way as described in section “28.2.2 Routing for Matched CPC using CPCRTE option” on page 362, here we pass also the category using the procedure CPCCHAR_PARAMETER_LOOKUP.

An example of TRAVER for CPC screening, using CALLCNTL, is found below in Figure 7. The table CPCCHAR is filled as shown in Figure 5. The category received is MTC_EQ.

Figure 7 Traver for CPC after the first called digit (in SMP_SETUP_REQUEST message).

```
>traver tr orirm2 500002 b
TABLE TRKGRP
ORIRM2 IBNTI 0 LCO NCRT TRKPSTN 0 0 N ANSDISC 0 N N N N
N N N 0 0 N N N N N $
  NATL (ANIREC ALWAYS) (ANIFAIL CONT ) $
TABLE TRKOPTS
ORIRM2 CCNTLIDX CCNTLIDX TEST_CPC
. TABLE CCNTLGRP
. TUPLE NOT FOUND
. TABLE CALLCNTL
. TEST_CPC (SCRN (CPCNAME ) )$
PLEASE ENTER VALUE FOR CPCCHAR PROTOCOL:
>FDCP
PLEASE ENTER VALUE FOR CALLING PARTY CATEGORY:
>MTC_EQ
. . Matched in table CPCCHAR on BLOCKCPC
. . TABLE CPCNSCRN
. . TEST_CPC BLOCKCPC TEST_CPC (NCOS 1) $
TABLE NCOS
TRKPSTN 1 0 0 TRK ( XLAS PRTRK1 NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA,
FEATXLA, VACTRMT, AND DIGCOL
TRKPSTN NXLA CXTRK NXLA 0 NDGT
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE IBNXLA: XLANAME PRTRK1
TUPLE NOT FOUND
Default from table XLANAME:
PRTRK1
  (NET N N 0 N NDGT N Y GEN (LATTR 1100 TRKPLAN
NLCA_NILLA_0) $ )$ 9
TABLE DIGCOL
TABLE LINEATTR
```

28.3 Hardware Requirements or Dependencies

N / A.

28.4 Software Requirements or Dependencies

N / A.

28.5 Limitations and restrictions

For both CPC screening methods, using the CPC RTE option and using the CALLCNTL table, the option QUICK_REQ in the R2PROT table (for incoming trunks) should be defined with one of the following values: ANI_AFTER_1_DIG or CAT_AFTER_1_DIG. For example, see Figure 3.

28.6 Interactions

N / A.

28.7 Glossary

Table 2

Term	Description
CPC	Calling Party Category
CLI	Calling Line Identification
FDCP	Flexible Digital CAS Platform
NCOS	Network Class Of Service
MFC	Multi Frequency Compelled

29: A00007380 Functional description (FN)

29.1 Feature name

INTL H.323 GW interworking to IWSPM for DTMF Relay and T.38

29.2 Description

The primary goal of this activity is to verify media interoperability between H.323 GWs and IWSPM. This includes DTMF relay (out of band to in band, in band to in band with RFC 2833) and T.38 fax. This is verified while H.323 endpoints are located behind NATs, therefore requiring insertion of the RTP media portal.

This activity is for H.323 in the International SN08 CS2K load.

The speech compression in codecs such as G.729 can greatly impair the ability of downstream systems to recognize in-band DTMF tones. Packet loss can also impair DTMF tone recognition. There are several solutions to this problem:

- Always use a high-bit rate codec such as G.711 combined with a low packet loss network to minimize packet loss and audible distortion.
- Instead of generating the tones at the ingress gateway, transmit special RTP data packets that instruct the downstream gateway to generate the appropriate tone (RFC 2833).
- Instead of generating the tones at the ingress gateway, signalling protocols (H.245) pass DTMF information to the downstream gateway, which generates the tones.

RFC 2833 is used for all tone transmissions in all codec types when provisioned as ON.

For IWSPM, the RFC 2833 and T.38 is enabled in table MNIPPARM by setting the values of RFC2833 and T38 fields to “ENABLE”.

Fax interworking is provided over Session Initiation Protocol (SIP-T).

This feature supports T.38 interworking with IWSPM depending on T.38 network option:

- If **Netopt is set to “T.38”** and both GW support T.38, then upon fax detection, switchover is done from G.729 (or G.711) to T.38 codec.
- If **Netopt is not set to “T.38”**, or a GW does not support T.38, then switchover to T.38 does not apply. If the call was set up with G.729 codec, switching is done from G.729 to G.711 codec. If the call was set up with G.711, no switchover occurs.

29.6 Interactions

This activity requires the following activities:

- A00006120, Mg4k IP H323 OOB DTMF
- A00005841, MG4K-IP H.323 Interworking For T.38 Fax
- A00007331, H.323 RFC 2833 DTMF Interop support S1KM/BCM

29.7 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

29.8 Glossary

Table 1

Term	Definition
DTMF	Dual-Tone Multi frequency
CM	Computing Module
GW	Gateway
GWC	Gateway Controller
IP	Internet Protocol
IWSPM	Interworking Spectrum Peripheral Module
MG	Media Gateway
MGC	Media Gateway Controller
NAT	Network Address Translator

Table 1

Term	Definition
RFC	Request For Communication
RTP	Realtime Transfer Protocol
SPM	Spectrum Peripheral Module

30: A00007383 Functional description (FN)

30.1 Feature name

DNH (Directory Number Hunting) enhancements: pilot DN charge and display

30.2 Description

30.2.1 General

This feature provides two new facilities for DNH groups. For any call originated from any DNH group member DN (MDN) or pilot DN (PDN), the group's **pilot DN** will be:

- Charged for the call,
- Presented as the Calling Line Number nodally or to the network to be displayed at the far end, if the call provides Calling Line Identification (CLI) by default or upon Automatic Number Identification (ANI) request.

These facilities are provided for all members of all the DNH groups on an office basis. It is possible to turn on or off each functionality separately. Thus, each functionality can be either applied or not applied officewide at once, i.e. all DNH groups follow the same behavior. These facilities are enabled by defining a new tuple in table **ISERVOPT**. Operating company personnel use table ISERVOPT to configure switch information for service-related features. Figure 1 shows a sample datafill for table ISERVOPT.

Figure 1 New ISERVOPT Tuple

SOPTSKEY	SOPTSVAR

DNH_OPTS	DNH_OPTS Y Y

The tuple introduces: a new entry *DNH_OPTS* in the field SOPTSKEY; a new entry *DNH_OPTS* in the field SOPTSVAR/subfield OPTI; and two new boolean subfields *PILOT_CHARGE*, *PILOT_DISPLAY*. The subfields' values 'Y/N' serve to turn functionalities on/off in the office.

30.2.2 Pilot DN Charge

30.2.2.1 Overview

The DNH group PDN can be charged for all calls originated by its members including calls originated by the PDN itself.

This functionality is achieved when the subfield *PILOT_CHARGE* value is set to 'Y' in the new ISERVOPT tuple.

The pilot DN charge functionality uses the existing line option **SPB** (Special Billing). The SPB option allows a number other than the subscriber's DN to be used for billing.

Thus, to supply the desired functionality, every single member DN of a DNH group must have the SPB option assigned on it, with the field SPBDN (Special Billing Directory Number) filled with the pilot DN of that group. As the PDN is also charged for its own calls, it is not allowed to have the SPB option.

30.2.2.2 Service Order

Therefore, after the functionality is activated, a number of restrictions to SO commands take place:

The field SPBDN of the SPB line option being assigned or changed on any DNH group member, accepts only the value of the PDN of that group.

The supported SO commands are: ADO 'SPB', CHF 'SPB', ADD a new DNH member with the SPB option, and EST a new DNH group with the SPB option on a member.

- Addition of the SPB option to a pilot DN with the ADO and EST commands, is forbidden.
- Deletion of the SPB option from a DNH member with the command DEO, is forbidden.
- Definition of a new DNH member without the SPB option, is forbidden. It concerns commands ADO 'DNH', ADD, and EST.

Every restriction is accompanied by displaying an appropriate message.

Deletion of the DNH option from a member DN is allowed. A user gets a reminder message that the SPB option remains on this DN.

30.2.3 Pilot DN Display

For any call providing CLI, originated from a DNH group MDN, only the group's PDN is presented as the Calling Line Number nodally or to the network to be displayed at far end, by default or upon ANI request. The functionality must be set in the new tuple of table ISERVOPT as described above.

The **IBN** and **ISDNKSET** originators and local terminators are supported.

The PDN sending as a calling number is supported for calls outgoing via **ISUP** and **MFC** trunks as described below.

ISUP:

When a call initiated by a DNH group member, goes out through an ISUP trunk, the Calling Party Number parameter in the ISUP Initial Address Message (**IAM**) contains the pilot DN of that group instead of the MDN.

As well, the PDN is also provided instead of the MDN in the INformation message (**INF**) that is sent in response to the received INformation Request message (INR).

MFC:

MFC (FDCP R2, Type-A) support: Similarly, instead of the DNH group MDN call originator, its PDN is presented as the DN of the calling party in the **setup** message and also in the **information** message sent in response to the information request message.

30.3 Hardware Requirements or Dependencies

Not applicable.

30.4 Software Requirements or Dependencies

Not applicable.

30.5 Limitations and restrictions

For both Pilot Charge and Pilot Display only homogeneous IBN/ISDN DNH groups are supported, i.e. those consisting from only IBN or only ISDN lines.

30.5.1 Pilot DN Charge.

All limitations and restrictions of the SPB feature take place.

After the functionality is activated in table ISERVOPT, this feature controls only **further** actions performed with **SO** commands. It is the responsibility of TELCO personnel to handle all SPB definitions on all DNH groups defined before the activation of the functionality. Any changes carried out by any other means, e.g. Table Control, are beyond the scope of the feature.

SO support performs **no automatic** actions (such as addition of the SPB option to a newly added MDN). An appropriate **message** is displayed each time any restriction to SO commands set by this feature is violated (see above), and the SO checking **rejects** the command. A user can then decide which further actions may be taken to achieve the goal, or may not take action at all.

30.5.2 Pilot DN Display.

For network calls, only **ISUP** and **MFC** trunk types are supported to send PDN as a calling number:

- **ISUP:** ETSI ISUP V2 Ethiopia (ETC) variant only;
To support other ISUP variants, additional development is required.

- **MFC:** FDCP R2 and Type A protocols.

Only **IBN** and **BRI** subscribers are supported as call originators, local terminators, and pilots.

30.6 Interactions

The key requirement of the Pilot Display is that the pilot DN must be seen on the terminator's telephone display as a calling number in every call originated by its member - if presentation of the CGN of the originator is not suppressed.

Therefore this feature, being in effect, takes precedence over all other features that modify the display of the CGN:

For local calls:

- All these features are ignored when the Pilot Display is active, and the pilot DN is displayed as it is datafilled in table DNINV etc without any modification;
- All the features that use CGN but that do not change its display for a terminator, are not affected.

For line-to-trunk calls:

As an originating switch always sends a PDN instead of its MDN as a CGN, all the features that manipulate with the CGN in their way, are suppressed by the Pilot Display.

Definite interest may be presented in analysis of the interaction with the **Call Forward** feature:

Pilot Charge.

When a call forward subscriber forwards a call, it pays for the second call leg, i.e. that between him and the terminator. The SPB feature covers this interaction, therefore no additional development is required to charge a pilot when its member forwards a call.

Pilot Display.

In a call forward scenario, the real originator, and not the call forwarder, is displayed at the terminator's display. Hence, if a member forwards a call, its DN does not appear as the calling party DN and therefore must not be replaced by the PDN in this interaction, which means that no development is required.

In **Malicious Call Trace** (MCT) feature, when MDN originated a call:

- For a **nodal** terminator, an MCT153 / MCT154 log is generated without any changes, i.e. the real originator (MDN, not PDN) appears at the field CALLING_PARTY;

-
- For a **remote** terminator accessed via trunks, the PDN appears at the field CALLING_PARTY.

30.7 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 __X__

Office Parameters _N/A_

Accounting (includes AMA billing) _N/A_

Performance (includes operational measurements) _N/A_

Note: * Preliminary estimates for system recovery and real time are entered in the real time (RT) template.

30.8 Glossary

Table 1

Term	Description
CLI	Calling Line Identification
CGN	CallinG Number
DN	Directory Number
DNH	Directory Number Hunting
PDN	Pilot DN
MDN	Member DN
ANI	Automatic Number Identification
SPB	SPecial Billing
SO	Service Order
TC	Table Control
ETSI	European Telecommunication Standards Institute
ISUP	ISDN User Part
ISDN	Integrated Services Digital Network
MFC	Multi Frequency Compelled
FDCP	Flexible Digital CAS Platform
CAS	Common Channel Signalling
IBN	Integrated Business Network

31: A00007405 Functional description (FN)

31.1 Feature name

Intl CAS - Korean R2 support

31.2 Feature Synopsis

This feature implements Korea R2 on the CS2K. It also provides the interworkings mentioned in Table 1, “Interworking Matrix for Korea R2,” on page 394.

Korea R2 provides connections from the CS2K to Private Branch eXchanges (PBX) and PSTN. Korea R2 is implemented over the E1 carrier and is deployed as an access as well as a Network protocol.

Korea R2 signaling systems are Multiple Frequency Compelled (MFC) systems where tones are sent in one direction and acknowledgment tones are returned.

31.3 Functional Overview

Implementation of Korea R2 on the CS2K is achieved by providing the customer with:

- The ability to define the CAS protocol via datafill
- Interworking with IBN (Cable MTA), V5.2, IBN, ETSI ISUP V2, SIP-T (MCS-5200), SIP-T (ETSI ISUP V2), H.323 (QSIG base), IN and ETSI PRI trunks.

This feature covers the following areas:

- Line Signalling
- MFC Register Signalling
- Protocol Timers
- Interworkings: For the list of interworkings supported, please refer to Table 1, “Interworking Matrix for Korea R2,” on page 394.

31.3.1 Interactions

31.3.1.1 Agency Interactions

Table 1, “Interworking Matrix for Korea R2,” on page 394 shows the agency interactions for Korea R2. The Interworking matrix denotes the agency interactions done in this feature.

Table 1 Interworking Matrix for Korea R2

	Korea R2	V5.2	IBN Lines	SIP-T (MCS-5200)	SIP-T (ETSI ISUP V2)	H.323 (QSIG base)	IN	ETSI ISUP V2	ETSI PRI
Korea R2	X	X	X	X	X	X	X	X	X
V5.2	X	*	*	*	*	*	*	*	*
IBN Lines	X	*	*	*	*	*	*	*	*
SIP-T (MCS-5200)	X	*	*	*	*	*	*	*	*
SIP-T(ETSI ISUP V2)	X	*	*	*	*	*	*	*	*
H323(QSIG)	X	*	*	*	*	*	*	*	*
ETSI ISUP V2	X	*	*	*	*	*	*	*	*
ETSI PRI	X	*	*	*	*	*	*	*	*

Notes: X - Interworking supported

Notes: * - Interworking out of scope of this feature

31.3.1.2 Service interactions

31.3.1.2.1 Inswitch Services

Table 2 Inswitch Services for Korea R2

Inswitch Services	Compliance
DDD/IDDD	Supported
Freephone	Translations based
CLI Screening	Not Supported for Korea R2.
Call Control/Universal Screening	Supported

31.3.1.2.2 IN Services

IN feature functionality is supported by Korean R2.

The following test items are covered in this activity

- TDP-2,3,4 and EDP-2,4,5,6,7,8,9,10

Different Tones and Treatments, Establish Temporary connection.

1. Korean R2 - QSIG interworking support for IN calls.

- QSIG to Korean R2
- Korean R2 -QSIG

The following Dacom INAP services are tested.

- Calling Card
- Universal Access Number
- Prepaid Card
- Personal Number
- Free Phone
- Number Portability
- Collect Call
- Color-ring (Korean R2 - Line interworking only)

2. Call Party Handling functionality for all Korean R2 interworkings required for Dacom:

- Korean R2 - ISUP V2
- Korean R2 - PRI
- Korean R2 - QSIG
- Korean R2 - Line
- Line - Korean R2
- QSIG - Korean R2
- PRI - Korean R2
- ISUP V2 - Korean R2

31.3.1.3 Call Processing / Translations Interactions

Existing call processing and translations are supported.

31.3.1.4 OA&M interactions

OA&M Functions	Impacted?	If impacted, explain how
HMI	N	
OM	N	
Logs	N	
Billing transfer (AFT, XFER, etc.)	N	
CDRSEARCH	N	
TRAVER	N	

31.3.1.5 Billing Interactions

The current AMA billing format on the CS2K is used for Korea R2.

31.4 Description

Subscriber access between Korea R2 and PBX/PSTN is via two-way trunks.

31.4.1 Line Signalling

31.4.1.1 Digital Line Signalling

The 2048 kbits/sec. PCM interface employs time slot 16 channel associated signalling in accordance with CCITT Recommendation G.704. 2E/M digital line signalling with R2 register signalling is intended for use in digital exchanges.

For the line signals used on Korea R2, please refer to Table 3, "Line Signals," on page 396.

Encoding for the line signals is done on the 'A' and 'B' bits. The 'C' and 'D' forward and backward line signalling bits take on the following default values as per CCITT recommendations:

— C = 0

— D = 1

Table 3 Line Signals

State	Transmit Direction	Forward Signal		Backward Signal	
		a _f	b _f	a _b	b _b

Table 3 Line Signals

Idle	B to A	1	0	1	0
(Release Guard)	A to B				
Seizure	A to B	0	0	1	0
Seizure Acknowledge	B to A	0	0	1	1
Answer	B to A	0	0	0	1
Clear forward	A to B	1	0	1 or 0	1
Clear Back	B to A	0	0	1	1
Re - Answer	B to A	0	0	0	1
Blocking	B to A	1 or 0	0	1	1

Notes: Idle is the same as Release Guard

31.4.1.2 Line Signalling Restrictions

No Type III operator line signals for TBI (Toll Break-In) are supported in the SN08 release.

31.4.2 Register Signalling

R2 Register Signalling must be in accordance with ITU Q.400, Q.440 to Q.480 and Q.490. Each in-band signal consists of the simultaneous presence of two out of six frequencies. The frequencies consists of two segregated groups, each using six frequencies. The two groups represent the forward and backward signals.

The forward signals utilize combinations of the following frequencies:

1380, 1500, 1620, 1740, 1860, and 1980 Hz

The backward signals utilize combinations of the following frequencies:

1140, 1020, 900, 780, 660, and 540 Hz.

For the frequency combinations for all fifteen forward and all fifteen backward signal codes, refer to the following table.

Table 4 Mapping of Register Signalling Code to Frequencies

Combinations		Frequencies (Hz)					
		f0	f1	f2	f3	f4	f5
Digit	Forward	1380	1500	1620	1740	1860	1980
	Backward	1140	1020	900	780	660	540
1	f0 + f1	X	X				
2	f0 + f2	X		X			
3	f1 + f2		X	X			
4	f0 + f3	X			X		
5	f1 + f3		X		X		
6	f2 + f3			X	X		
7	f0 + f4	X				X	
8	f1 + f4		X			X	
9	f2 + f4			X		X	
10	f4 + f4				X	X	
11	f0 + f5	X					X
12	f1 + f5		X				X
13	f2 + f5			X			X
14	f4 + f5				X		X
15	f4 + f5					X	X

31.4.2.1 Korea R2 Forward Signalling Register Groups

The Korea R2 forward multifrequency combinations are allocated in two groups Group I and Group II.

- Group I forward signals transmit information about both the called party address and calling party address.
- Group II forward signals transmit information about the calling party and billing categories.

The change from Group I to Group II takes place when requested by specific backward signals. The specific backward signals include A-3 and A-5 signals.

31.4.2.1.1 Forward Group I Functionality

Please refer to Table 5, “Group I Forward Signals,” on page 399.

This section outlines the forward signals in the Group I category for Korea R2 in CS2K. The CS2K datafill representation of the activity is also mentioned in bold.

- Signal I-1, I-2, ..., I-9, I-10: **DIGIT_1...DIGIT_0**

These activities correspond to digits 1 through 9 and digits 0. They are used to indicate the called party address digits. They are also used to indicate the calling party identity in response to a request from other system.

- Signal I-12: **REQ_NOT_ACC**

Refused request

This signal designates a request refused for calling number only.

- Signal I-13: **ACC_TEST_EQ**

Access To Test Equipment.

This activity indicates to access automatic test equipment.

This is not supported in SN08 release.

- Signal I-15: **END_OF_DIGS**

End of calling number, End of called digits.

This signal designates the end of the calling party's number. It should be sent in response to an A-5 signal to indicate the end of information if necessary.

This signal also designates the end of the called party digits

Table 5 Group I Forward Signals

Code combination	Signal code	Meaning of the signal
1	I - 1	Digit 1
2	I - 2	Digit 2
3	I - 3	Digit 3
4	I - 4	Digit 4
5	I - 5	Digit 5
6	I - 6	Digit 6
7	I - 7	Digit 7
8	I - 8	Digit 8
9	I - 9	Digit 9

Table 5 Group I Forward Signals

Code combination	Signal code	Meaning of the signal
10	I - 10	Digit 0
12	I -12	Request not Accepted
13	I -13	Access to Test Equipment (<i><u>not supported in SN08</u></i>)
15	I -15	End Of Digits

31.4.2.1.2 Forward Group II Functionality

For the Group II signals used in Korea R2, refer to “Group II Forward Signals” on page 401.

This section outlines the forward signals in the Group II category for Korea R2 for CS2K. The CS2K datafill representation of the activity is also mentioned in bold.

- **SIGNAL II-1 : REGULAR**

Regular subscriber

This signal indicates that the calling party terminal is not equipped with special features.

- **SIGNAL II-2 : PRIORITY**

Subscriber with Priority

This signal indicates that the calling party’s terminal has some special priority.

- **SIGNAL II-3 : MTC_EQ**

Maintenance equipment

This signal indicates that the call has been originated in maintenance equipment.

- **SIGNAL II-4: COIN**

Public Telephone

This signal indicates that the call has been originated on a payphone.

- **SIGNAL II-5: OPER**

Operator

This signal indicates that the call is set up by an operator.

- **SIGNAL II-6 : DATA**

Data communication equipment

This signal indicates that the call origination point is connected to data communication equipment.

Table 6 Group II Forward Signals

Code combination	Signal code	Meaning of the signal
1	II -1	Subscriber without priority
2	II -2	Subscriber with priority
3	II -3	Maintenance Equipment
4	II -4	Public Telephone
5	II -5	Operator
6	II -6	Data Transmission

31.4.2.1.3 Korea R2 Backward Signalling Register Groups

The backward multi frequency combinations are allocated in two groups Group A and Group B.

- Group A signals acknowledge the forward signals and instruct the preceding exchange what type of information to send next.
- Group B signals indicate the status of the called party and indicate whether charging is applicable for the call.

The change from Group A to Group B takes place on the reception of certain backward signals.

31.4.2.1.4 Backward Group A Functionality

This section outlines the backward signals in the Group A category for the Korean R2 application of CS2K. The CS2K datafill representation of the activity is also mentioned.

- **SIGNAL A-1: NEXT_DIGIT**

Send next digit

This signal is used to request the sending of the next digit (N+1), after reception of digit N.

- **SIGNAL A-2: LAST_BUT_1**

Re-send last but one digit (n - 1) - Send the digit previously sent before the latest digit (n) received. This activity is used when setting up an end-to-end R2 trunk to trunk call.

This is not supported in SN08 release.

- **SIGNAL A-3: REQ_CAT**

Prepare the reception of signals from Group B

This is the signal used to inform the originating exchange that the next signal to be sent in the backward direction is a Group B signal. It is also used to request for the calling party category.

- **SIGNAL A-4: CONGESTION**

Congestion

This signal is sent by the destination to indicate one of the following conditions:

- a. Congestion in the outgoing circuits bundle
- b. Congestion in the selection stages
- c. Time-out in the common control equipment or functions

- **SIGNAL A-5: REQ_DN_CAT**

Send calling party's category

This signal, when not preceded by the same signal, is used to request the calling party's category. On reception of more than one A-5, the calling party digits are sent.

- **SIGNAL A-6: CONNECT_CALL_CHG**

The called party is available, charge on answer.

- **SIGNAL A-7: LAST_BUT_2**

Re-send last but two digit (n - 2) - Send the digit that is two before the last digit (n) received. This activity is used when setting up an end-to-end R2 trunk to trunk call.

This is not supported in SN08 release.

- **SIGNAL A-8: LAST_BUT_3**

Re-send last but three digit (n - 3) - Send the digit that is three before the latest digit (n). This activity is used when setting up an end-to-end R2 trunk to trunk call.

This is not supported in SN08 release.

- **SIGNAL A-9: FIRST_DIGIT**

Re-send the first digit of the called DN. This activity is used when setting up an end-to-end R2 trunk to trunk call.

This is not supported in SN08 release.

Table 7 Group A Backward Signals

Code combination	Signal code	Meaning of the signal
1	A - 1	Send next digit (N+1)
2	A - 2	Send last but one digit (N-1) (<i>Not supported in SN08 release</i>)
3	A - 3	Address complete change-over to reception of Bn signals
4	A - 4	Congestion in the National Network
5	A - 5	Send calling party category
6	A - 6	Address complete, charge, set-up speech condition
7	A - 7	Send last but two Digits (N-2) (<i>Not supported in SN08 release</i>)
8	A - 8	Send last but three Digits (N-3) (<i>Not supported in SN08 release</i>)
9	A - 9	Send from first digit again (<i>Not supported in SN08 release</i>)

31.4.2.1.5 Backward Group B Functionality

This section outlines the backward signals in the Group B category on the CS2K. The CS2K datafill representation of the activity is mentioned in bold.

- SIGNAL B-2: **SUB_XFRD**

Subscriber transferred

This activity provides the called party status. It is used to indicate that the subscriber has been transferred and can no longer be reached at this called number.

- SIGNAL B-3: **SUB_BUSY**

Subscriber line busy

This activity provides the called party status. It is used to indicate that the subscriber is busy and cannot be currently reached.

- SIGNAL B-4: **CONGESTION**

Congestion

After changing to transmission of Group B signals, in case the call cannot be completed, signal B-4 is sent.

- SIGNAL B-5: **UNASSIGN_NUM**

Idle number or idle level

After reception of this signal, the call is routed to an announcement, or the unreachable number tone is played to the calling party.

- SIGNAL B-6: **CONNECT_CALL_CHG**

Subscriber's line free, charge

Upon receipt of this signal, the origination register commands the passing of circuits to the speech condition. In this case, the call is charged.

- SIGNAL B-7: **CONNECT_CALL_NOCHG**

Subscriber's line free, no charge

Upon receipt of this signal, the origination register commands the passing of circuits to the speech condition. In this case, the call is not charged.

- SIGNAL B-8: **TEMP_OUT_ORD**

Subscriber line out-of-service for incoming traffic

After reception of this signal, the call is routed to an announcement machine or to an operator, or the unreachable tone to be played to the calling party.

Table 8 Group B Backward Signals

Code combination	Signal code	Meaning of the signal
2	B - 2	Subscriber under changed
3	B - 3	Subscriber line busy
4	B - 4	Congestion
5	B - 5	Unallocated number
6	B - 6	Subscriber's line free,charge
7	B - 7	Subscriber's line free,no charge
8	B - 8	Subscriber's line out of order

31.4.3 CLI Collection Methods

Two methods of collecting the Calling Party Address (calling DN) or Calling Line Identification (CLI) are used by the CS2K. The different collection methods simply deal with the location of the Calling Party Address digits within the outpulsed digit stream. The two methods are known as:

- B-A Signalling
- B-A-B Signalling

where 'B' represents the Called Party Address and the 'A' represents the Calling Party Address.

Between GWC and GW, overlap is not supported in this feature. However the behaviour of the M2K GW is as per B-A-B signalling, after receiving the first called party digit, M2K requests for the calling party category and then calling party digits via A-5 signals and then called party digits via A-1 signals.

31.4.3.1 B-A Signalling

The B-A Signalling method involves the outpulsing of the Called DN ('B' party) by the preceding office, sending of the Calling party category, and finally the outpulsing of the Calling DN ('A' party) by the preceding office.

The signalling sequence would be as follows:

B-A Signalling	'B' Party (Called)			'A' Party (Calling)		
Forward Signals	5561025002	F	1	036320630	F	1
Backward Signals	1111111111	5	5	555555555	3	6
<i>Time -----></i>	<i>Outpulse B Digits</i>	<i>ANI Phase Begins</i>				

No Digit analysis is required to perform this form of ANI. Also note that outpulsing of the Calling digits must ALWAYS be followed by the sending of the END_OF_DIGS activity, but that this restriction does not apply when sending the Called party digits.

31.4.4 Timers

In WT16, the reanswer and preanswer timer values are picked from the table CTRLTMRS for FDCP as the terminating agent. These values are dependant on the type of translations used. If UNIVERSAL TRANSLATIONS are in use, the 'CLASS' option datafilled in table PXCODE determines the values. The values are picked from table CTRLTMRS corresponding to the 'CLASS' datafilled in table PXCODE. If no 'CLASS' option is datafilled in table PXCODE, the values are picked from 'IAGRP_CLASS' which is the default class set. If IBN TRANSLATIONS are in use, the values are picked from 'IAGRP_CLASS' of table CTRLTMRS since there is no class option in this type of translations. The values of reanswer and preanswer timers are datafillable and implemented for all the interworkings like ETSI ISUP, PRI, IBN/V5.2 LINES with FDCP (Korea R2) as the terminating agent. If the preanswer value is set to 255 sec which is the max. value, there will be no supervision sent to the GWC and hence GWC will start its timer of value 120 sec. Except for this value, all the values are executed as datafilled in table CTRLTMRS.

Table 9 Korea R2 Timers

Timer	Value
No SZA Timer	2s
Incomplete Address	20s
No Answer Timer	60s (Local) 90s (Toll) 120s (Intl.)
Re-answer Timer	60s (Local) 90s (Toll) 120s (Intl)
Busy tone supervision	40s
Clear forward Timer	20s
Release Guard Timer	5s
Time-out supervision	15s

31.4.5 Interworkings

31.4.5.1 Interworking with Lines (IBN)

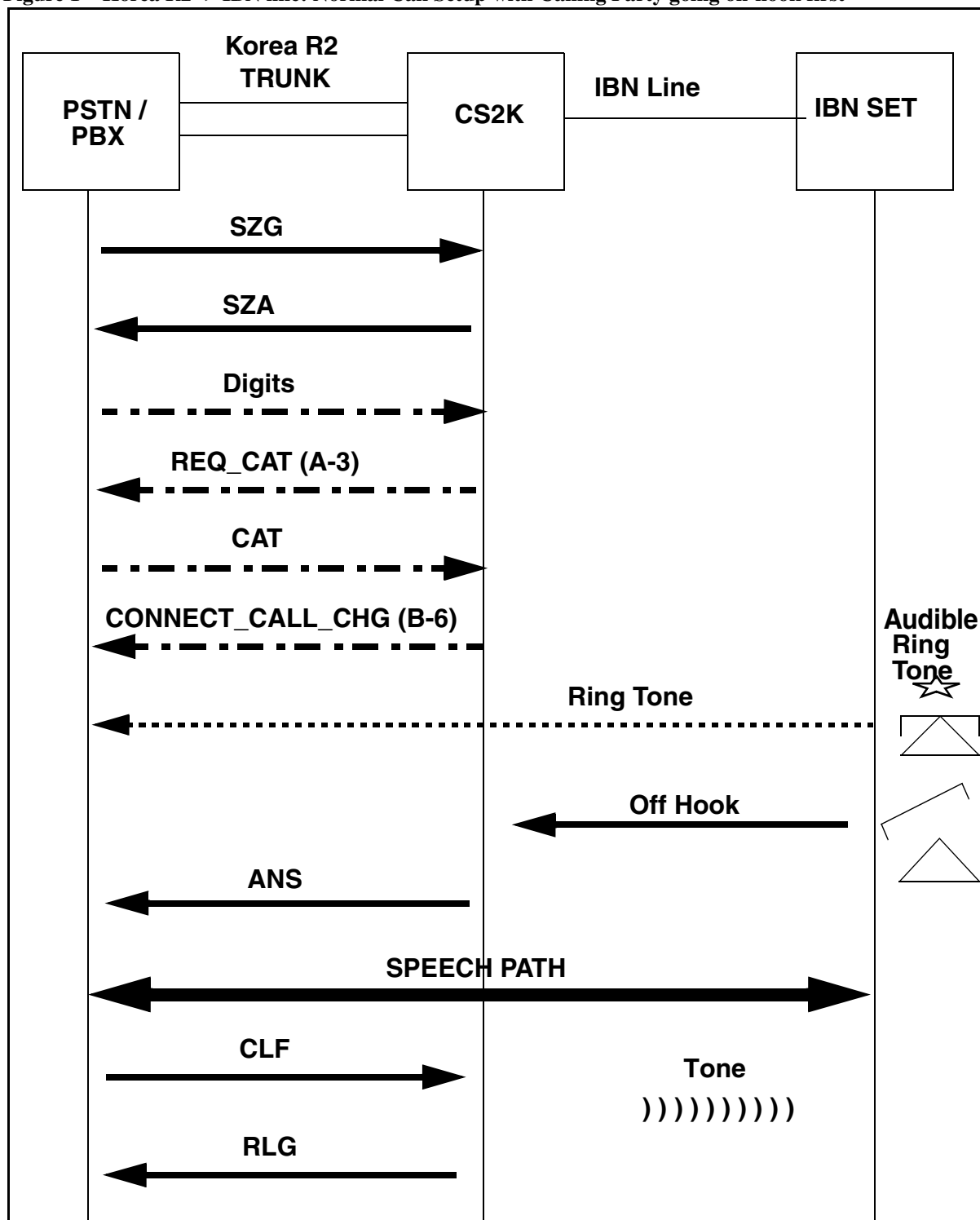
Note: Here, IBN lines indicate IBN, IBN (Cable MTA) and V5.2 lines.

31.4.5.1.1 Korea R2 to IBN Interworking

Normal Call Setup With Calling Party Going On-hook First

For an overview of the scenario, please refer to Please refer to “Figure 1 Korea R2 -> IBN line: Normal Call Setup with Calling Party going on-hook first” on page 407.. When the originator goes on-hook, a CLF signal is sent on the R2 trunk which triggers a RLG line signal from the succeeding exchange.

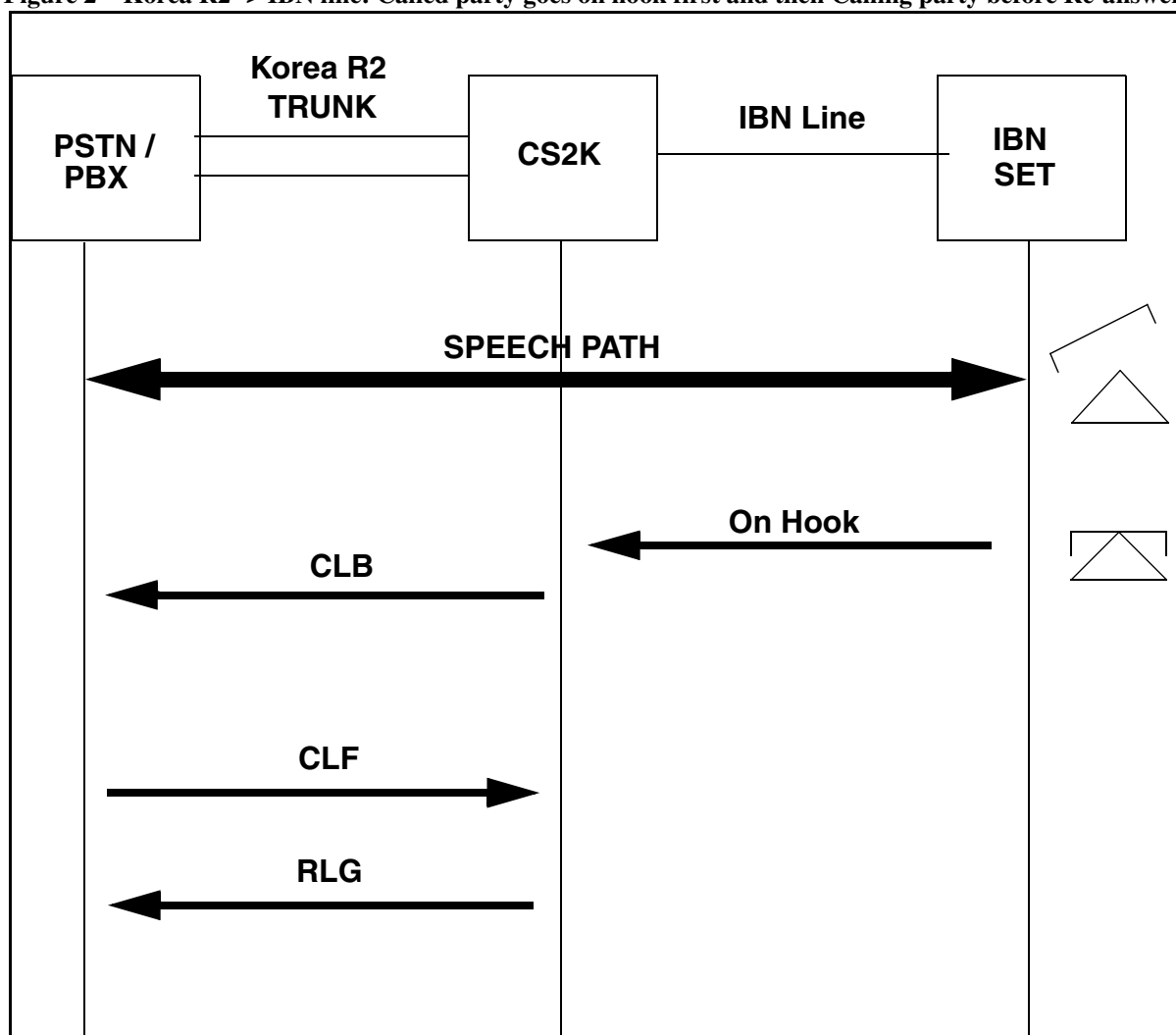
Figure 1 Korea R2 -> IBN line: Normal Call Setup with Calling Party going on-hook first



Normal Call Clearing with Backward Release

When the terminator goes on-hook, a CLB signal is sent on the Korea R2 trunk by CS2K and wait for the CLF signal from the originating exchange. For the overview of the scenario, please refer to "Figure 2 Korea R2 -> IBN line: Called party goes on hook first and then Calling party before Re-answer" on page 408..

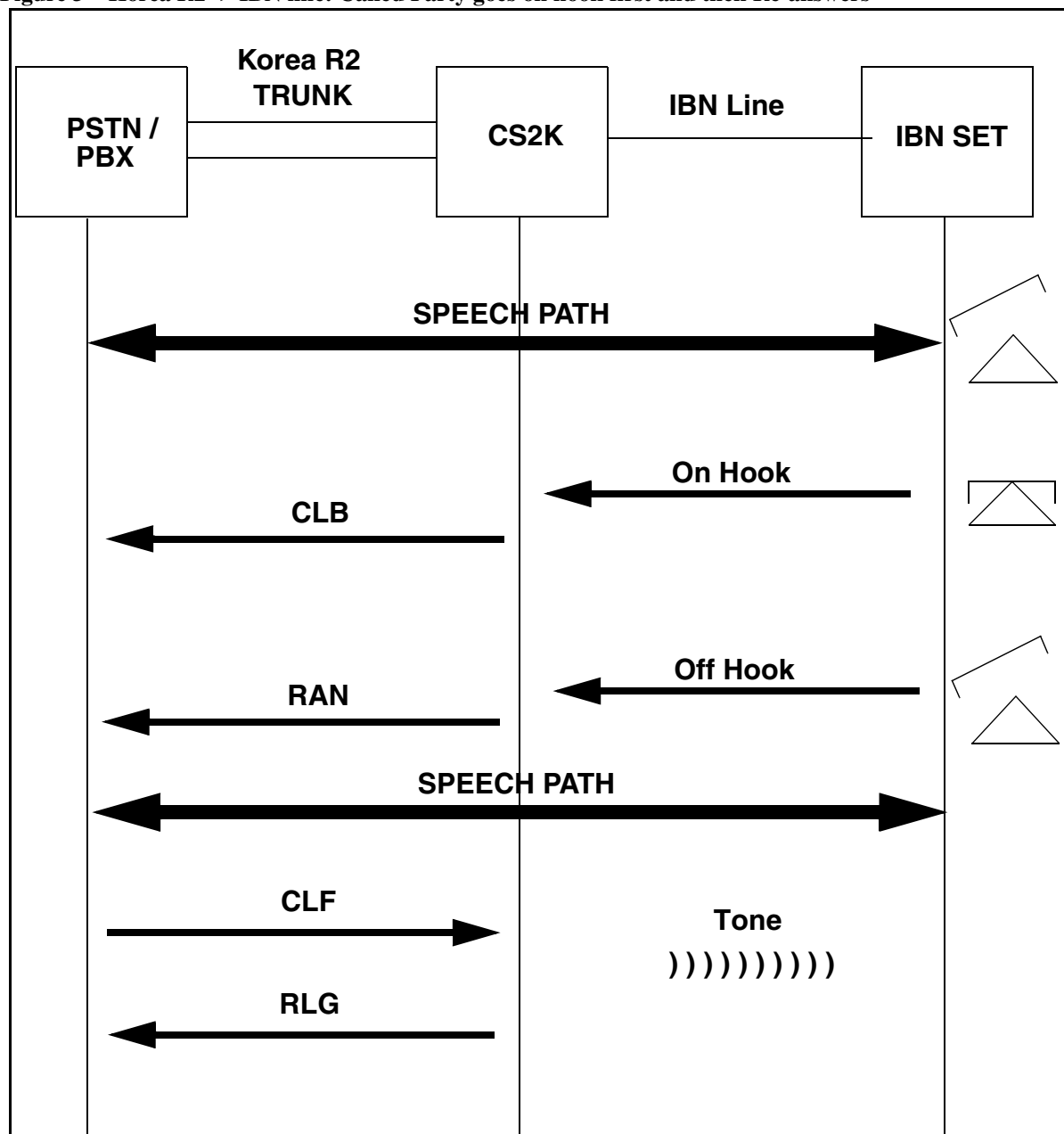
Figure 2 Korea R2 -> IBN line: Called party goes on hook first and then Calling party before Re-answer



Successful Reanswer

When the terminator goes on-hook, a CLB signal is sent on the Korea R2 trunk. Within the expiry of the timer, if the terminator goes off hook, a RAN signal is sent by the CS2K to the Korea R2 trunk and the speech path is re-established.

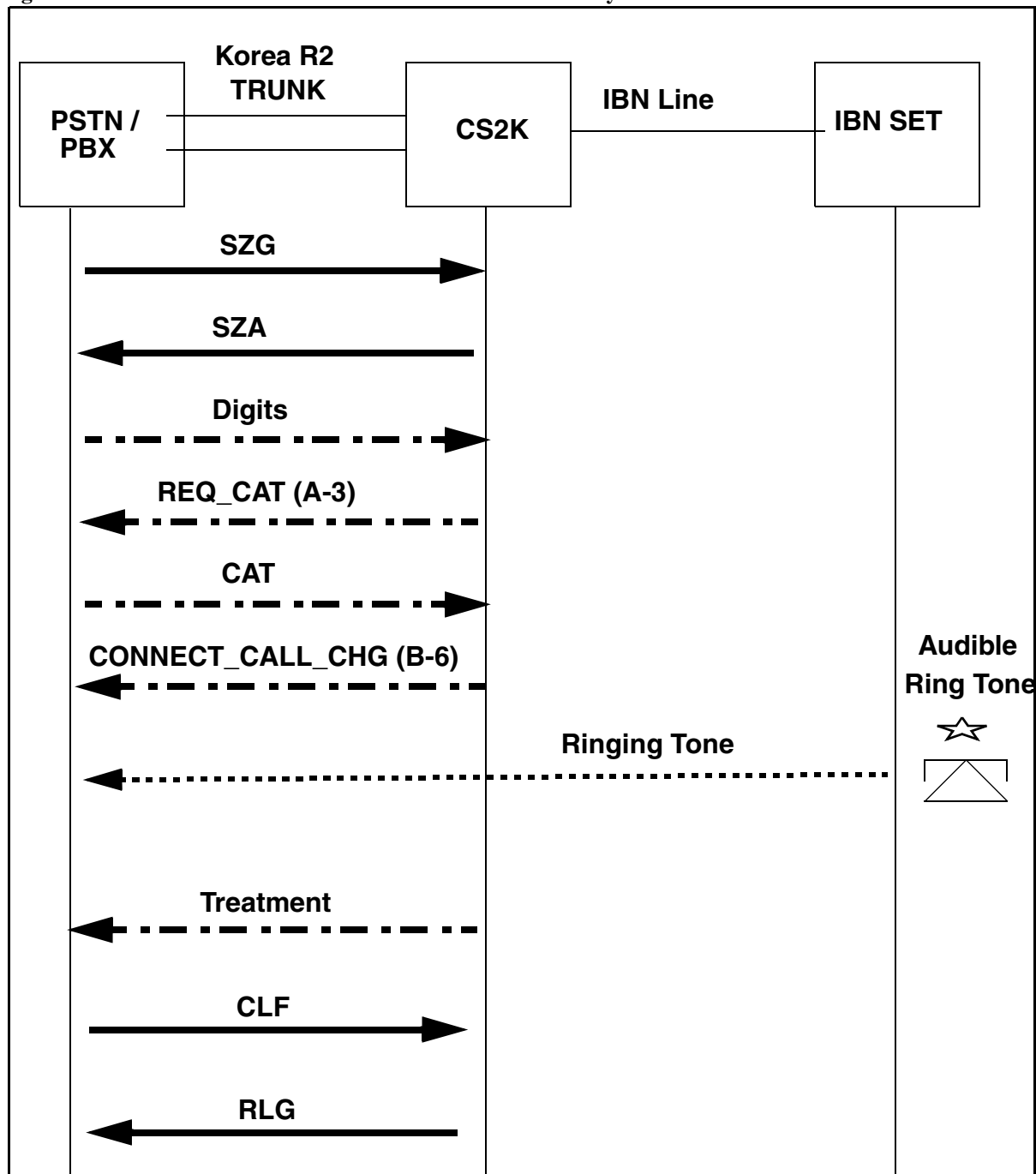
Figure 3 Korea R2 -> IBN line: Called Party goes on hook first and then Re-answers



Unsuccessful Call

Answer timer starts as soon as the B-6 signal is received on the originating exchange. If the Answer signal is not received within the expiry of that timer, then a treatment is applied.

Figure 4 Korea R2 -> IBN line: No Answer from Called Party



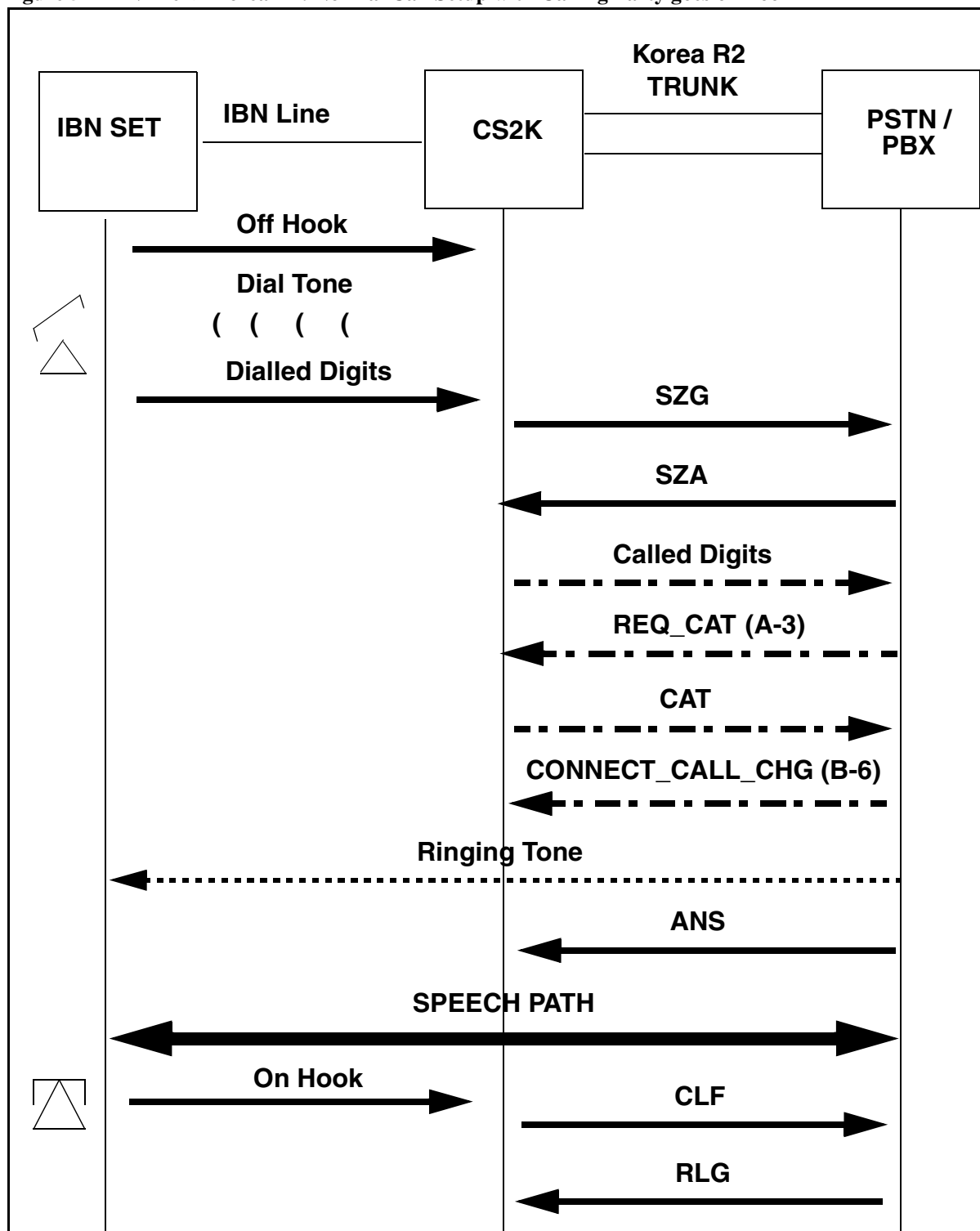
31.4.5.1.2 IBN Interworking to Korea R2

Normal Call Setup With Calling Party Goes On-hook First

For an overview of the scenario, refer to “IBN line -> Korea R2: Normal Call Setup with Calling Party goes on-hook” on page 411. When the originator

goes on hook, a CLF signal is sent on the R2 trunk which triggers a RLG line signal from the terminating exchange.

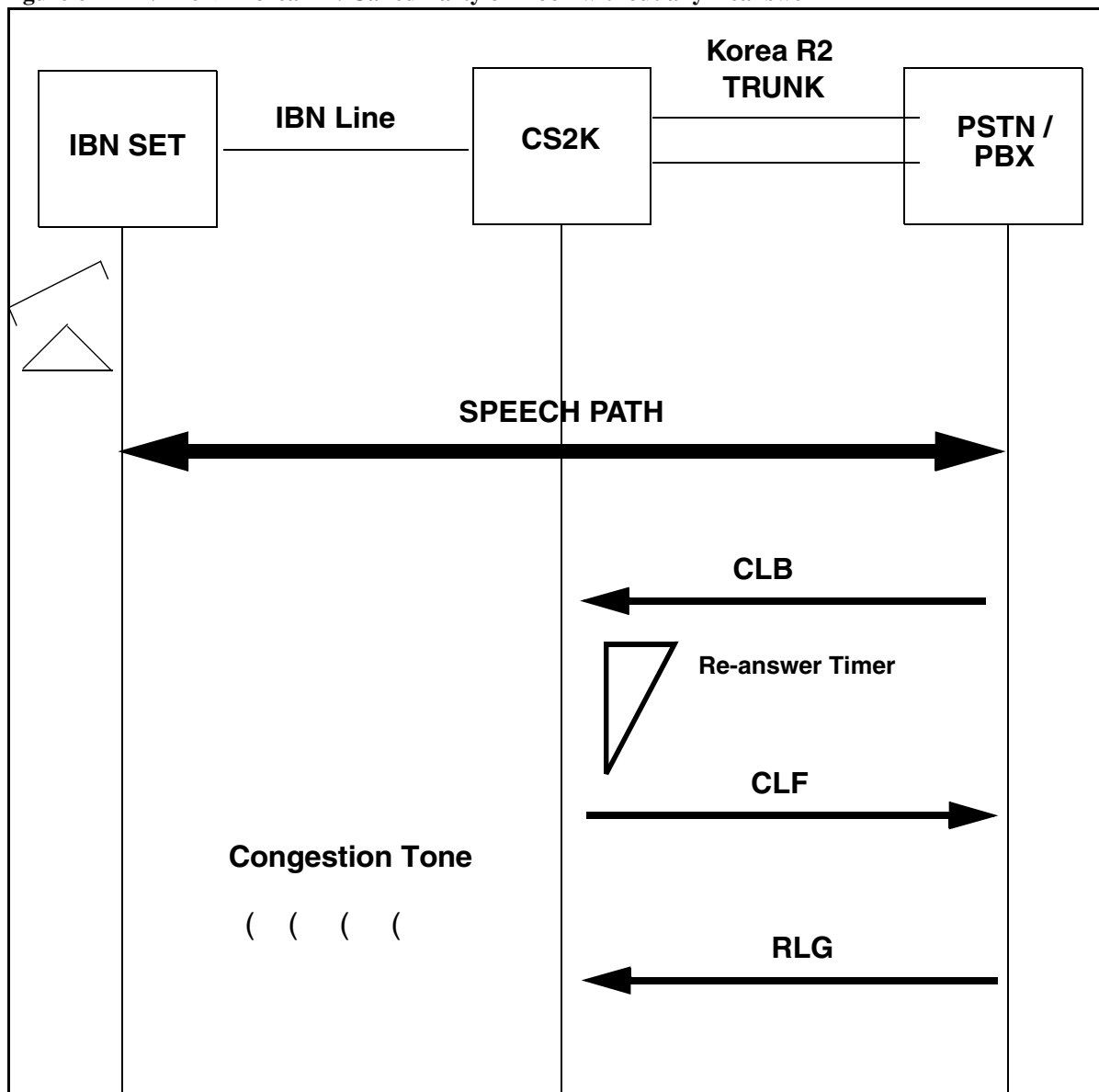
Figure 5 IBN line -> Korea R2: Normal Call Setup with Calling Party goes on-hook



Normal Call Clearing with Backward Release

When the terminator goes on-hook, a CLB signal is sent on the Korea R2 trunk and a re-answer timer is started on CS2K. On expiry of the re-answer timer a CLF is sent on the Korea R2 trunk. Upon the reception of the RLG line signal, trunk lockout timing is stopped. The re-answer timer is datafilled in table CTRLTMRS. For the overview of the scenario, please refer to “Figure 6 IBN line -> Korea R2: Called Party on-hook without any Reanswer” on page 412.

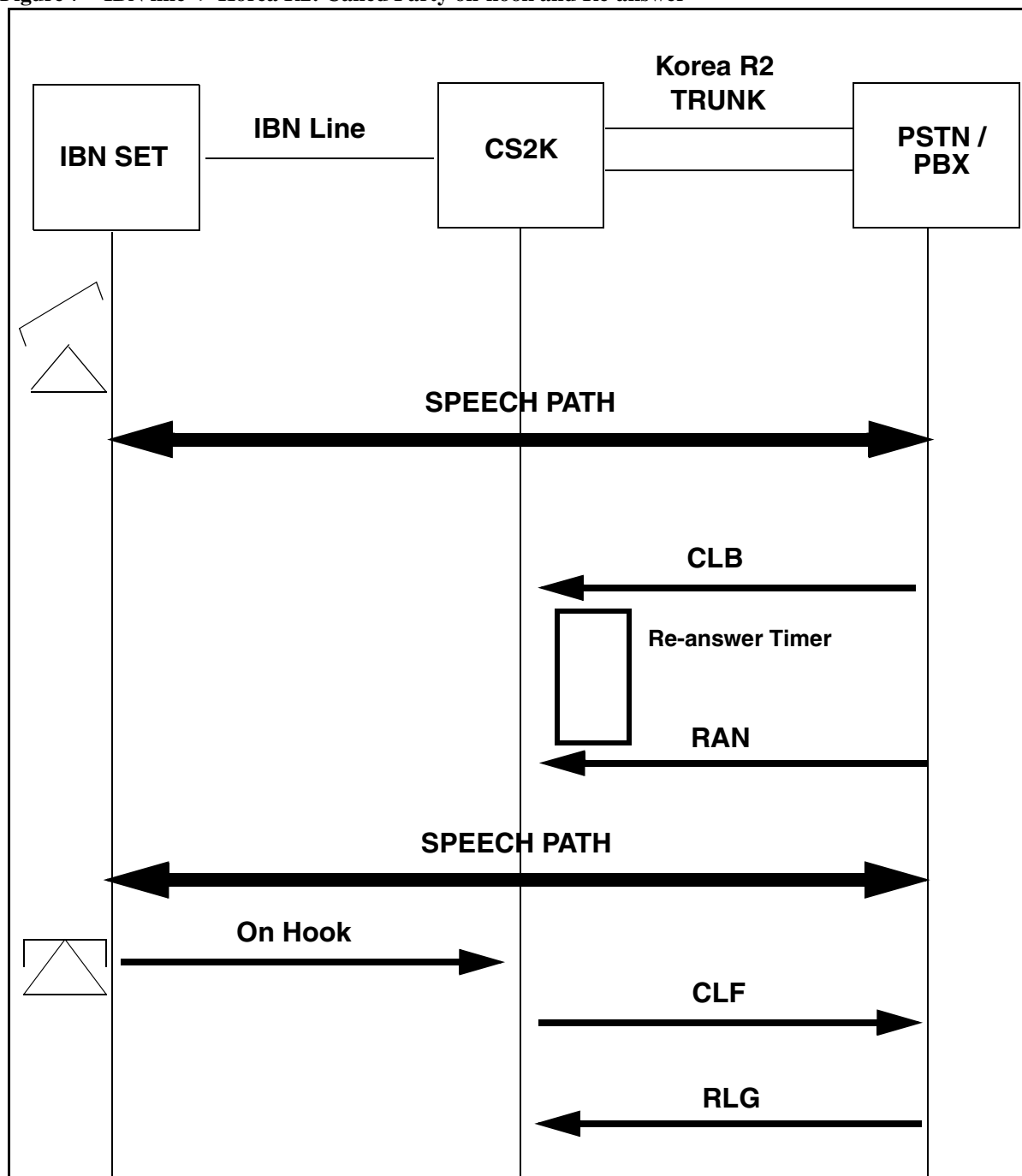
Figure 6 IBN line -> Korea R2: Called Party on-hook without any Reanswer



Successful Reanswer

When the terminator goes on-hook, a reanswer timer is started by the CS2K. If the called party goes off-hook before the expiry of the timer, then the speech path is re-established.

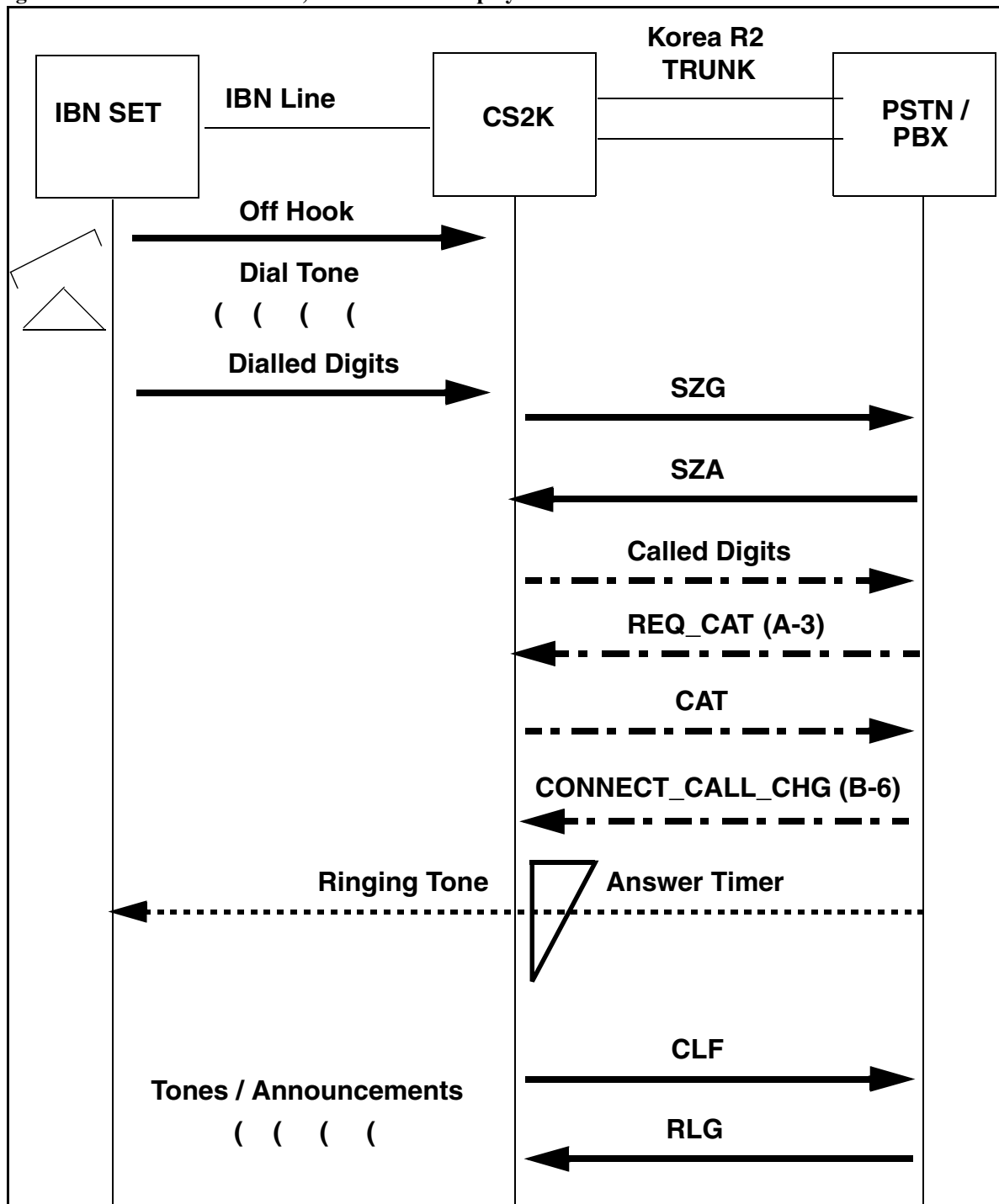
Figure 7 IBN line -> Korea R2: Called Party on-hook and Re-answer



Unsuccessful Call

Answer timer starts as soon as the B-6 signal is received. If the Answer signal is not received within the expiry of the timer, then a treatment is applied.

Figure 8 IBN line -> Korea R2, Answer timer Expiry



31.4.5.2 Interworking with Korea R2

The following MSCs cover the interworkings:

Korea R2 to Korea R2

Normal Call Setup with Forward Release

For an overview of the scenario, please refer to Please refer to “Figure 9 Korea R2 -->Korea R2, Successful Call” on page 417. and Please refer to “Figure 10 Korea R2 ->Korea R2 Call, Disconnection from Calling party” on page 418.. CS2K sends the SZA signal on the reception of the SZG signal from the originating side. After receiving the called party digits, CS2K outpulses the called party number to the outgoing trunk. After receiving the calling party category the terminating exchange sends B-6 signal and establishes the speech path.

When the originator goes on hook, a CLF signal is sent on the R2 trunk which triggers a RLG line signal from the succeeding exchange.

Figure 9 Korea R2 --> Korea R2, Successful Call

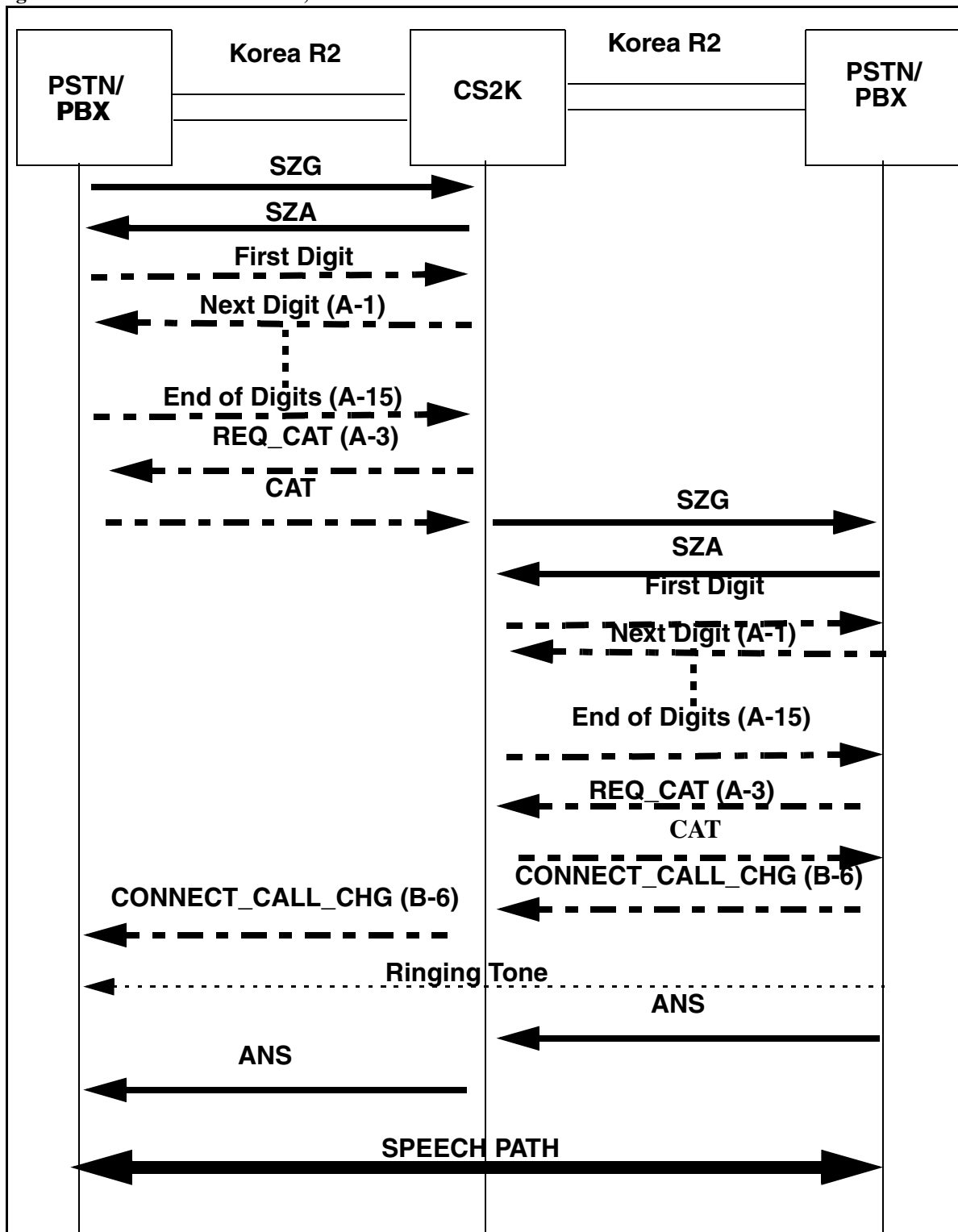
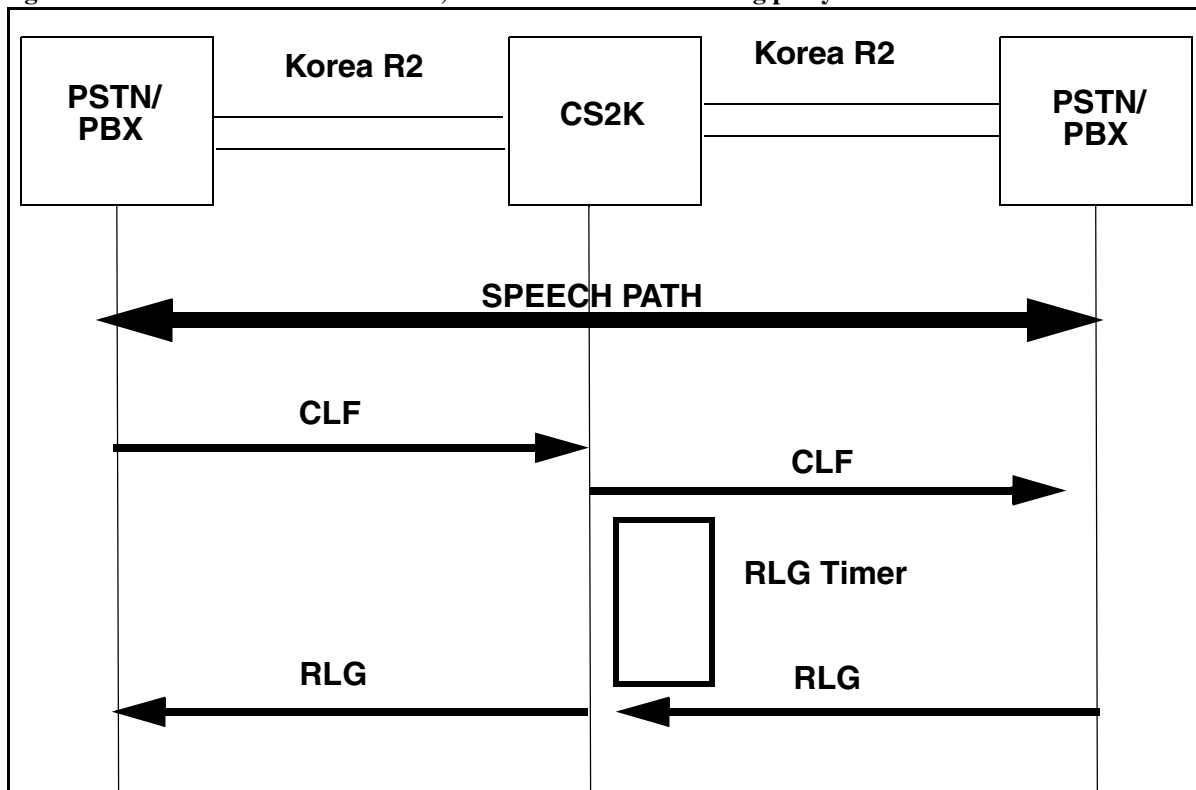


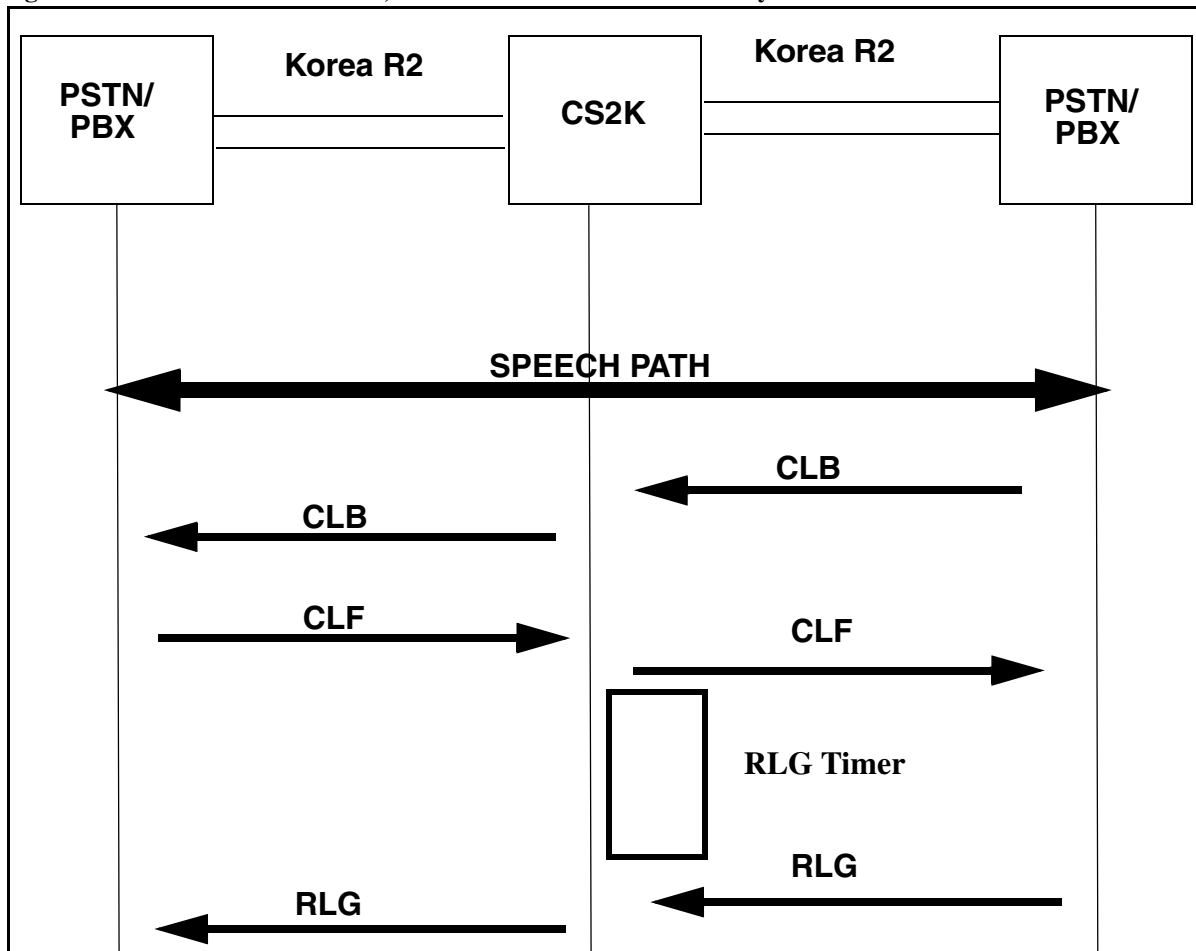
Figure 10 Korea R2 ->Korea R2 Call, Disconnection from Calling party



Called Party Disconnect

In this call scenario, the release of the connection is done by terminating the exchange by sending CLB. In response to this a CLF is sent by the originating exchange. For an overview of the scenario, please refer to “Figure 11 Korea R2 ->Korea R2, Disconnection from Called Party” on page 419..

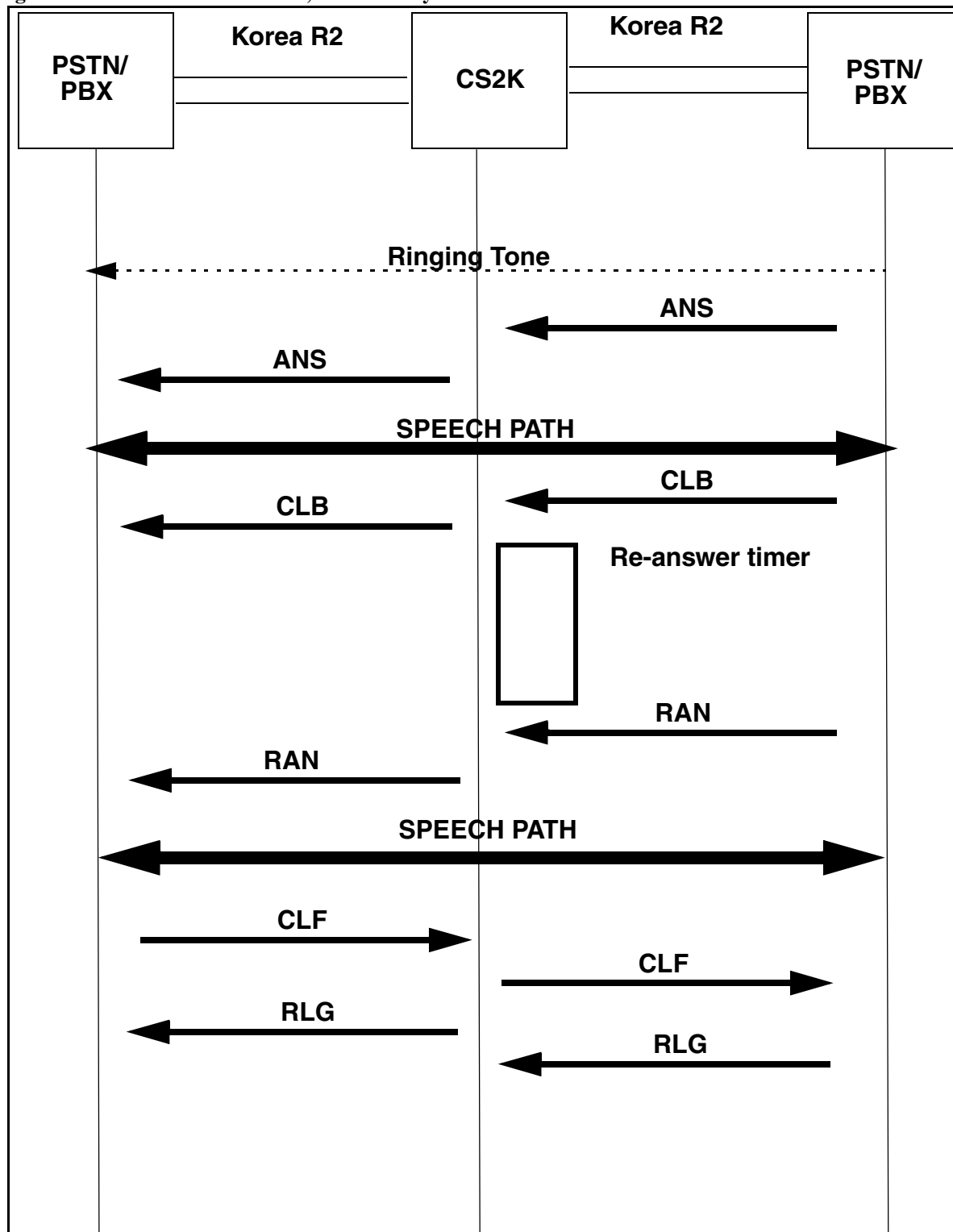
Figure 11 Korea R2 ->Korea R2, Disconnection from Called Party



Successful Reanswer

When the terminator goes on-hook, a reanswer timer is started by the CS2K. If the called party goes off-hook before the expiry of the timer, then the speech path is re-established by sending the signal RAN. For an overview of the scenario, please refer to “Figure 12 Korea R2 ->Korea R2, Called Party Disconnect and Re-answer” on page 420..

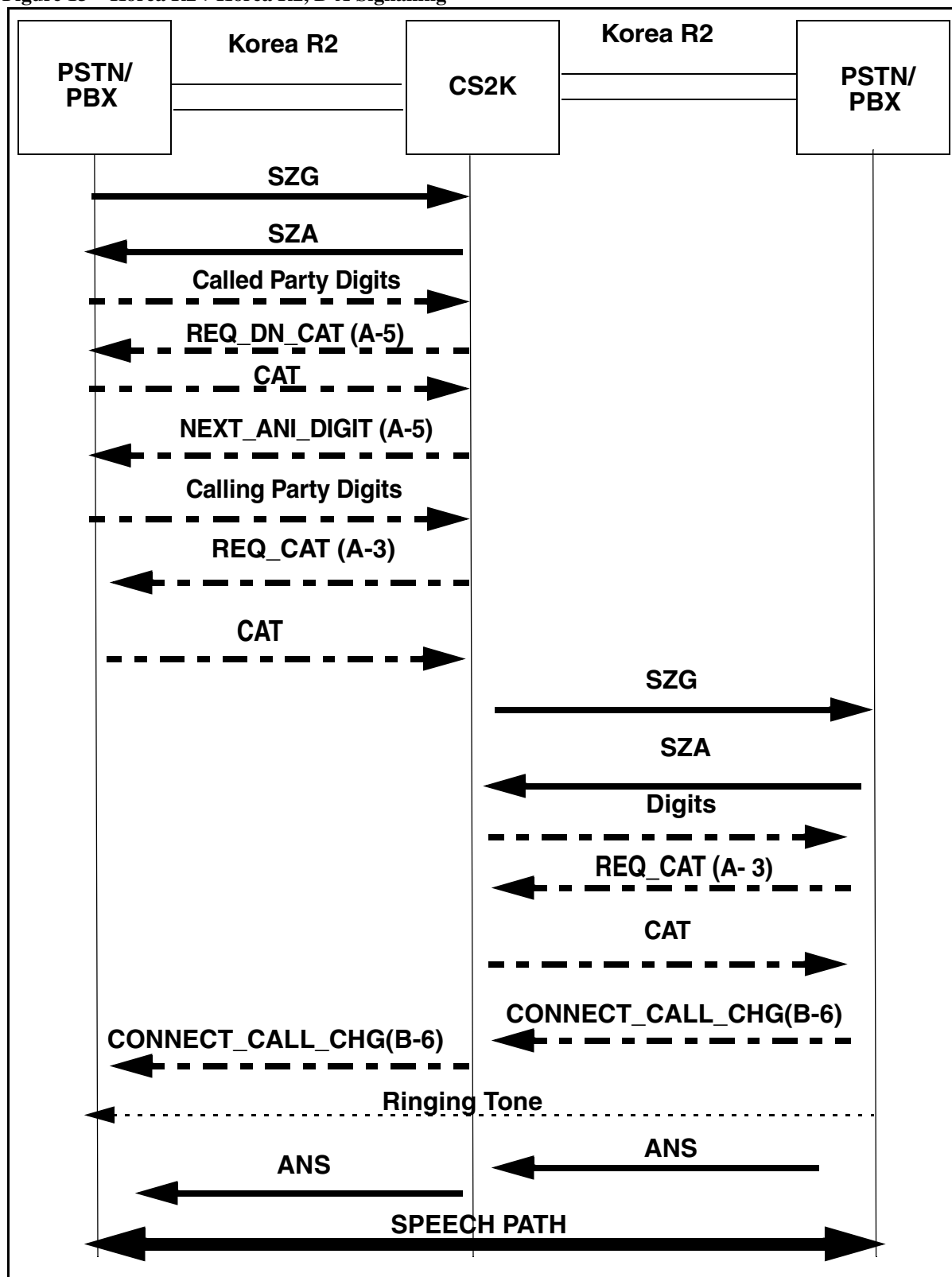
Figure 12 Korea R2 ->Korea R2, Called Party Disconnect and Re-answer



CLI Request

For an overview of the scenario, please refer to Please refer to “Figure 13 Korea R2->Korea R2, B-A Signalling” on page 422. In this scenario, after collecting the called party digits, CS2K requests for the calling party category and calling party digits by sending the signal A5 subsequently.

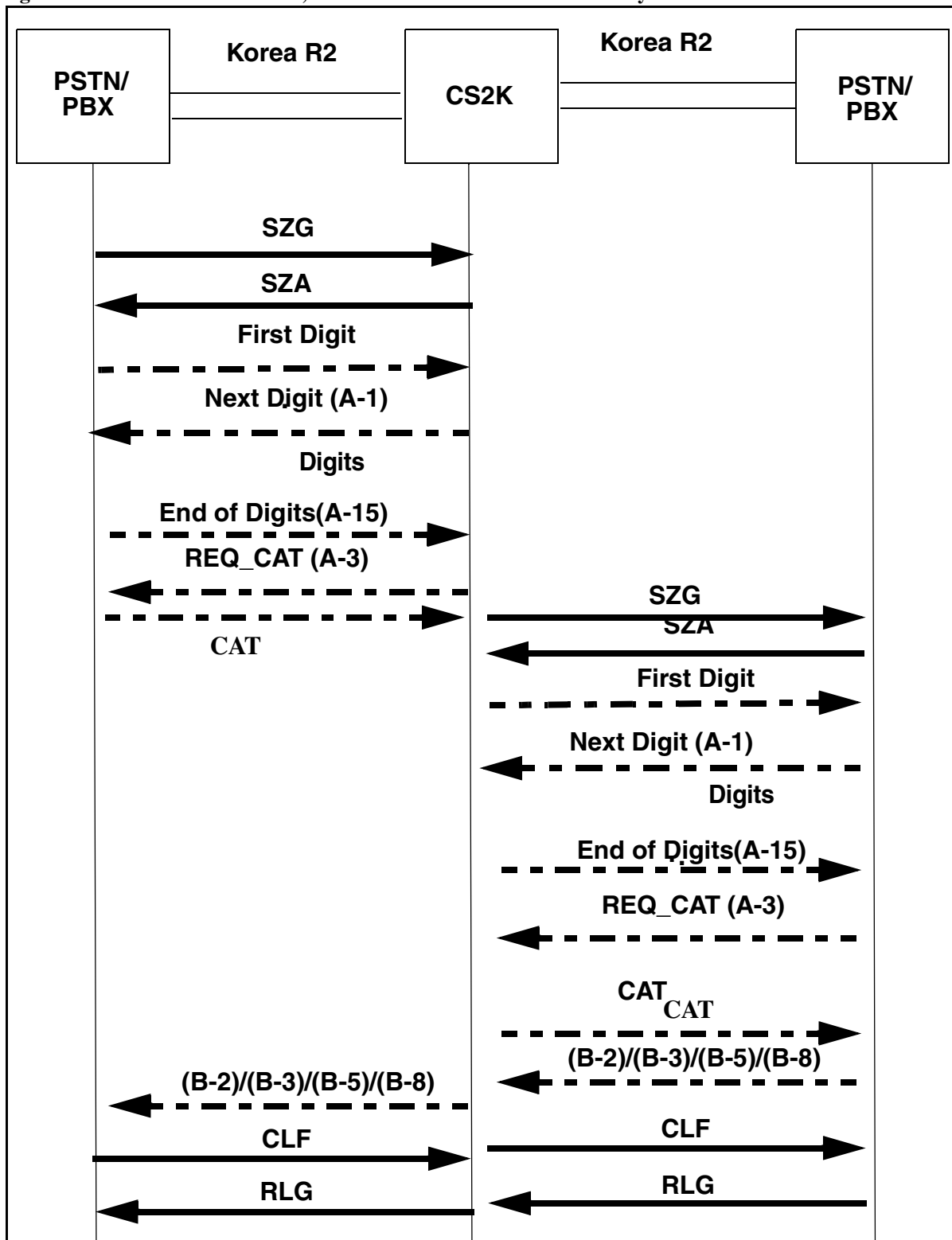
Figure 13 Korea R2->Korea R2, B-A Signalling



Unsuccessful Call

For an overview of the scenario, please refer to Please refer to “Figure 14 Korea R2->Korea R2, Unsuccessful call due to Called Party Status” on page 424.. In this scenario, the speech path is not established due to the called party’s status, which can be either subscriber busy, unassigned number, out of order or subscriber under change.

Figure 14 Korea R2->Korea R2, Unsuccessful call due to Called Party Status



31.4.5.3 Interworking with ETSI ISUP V2

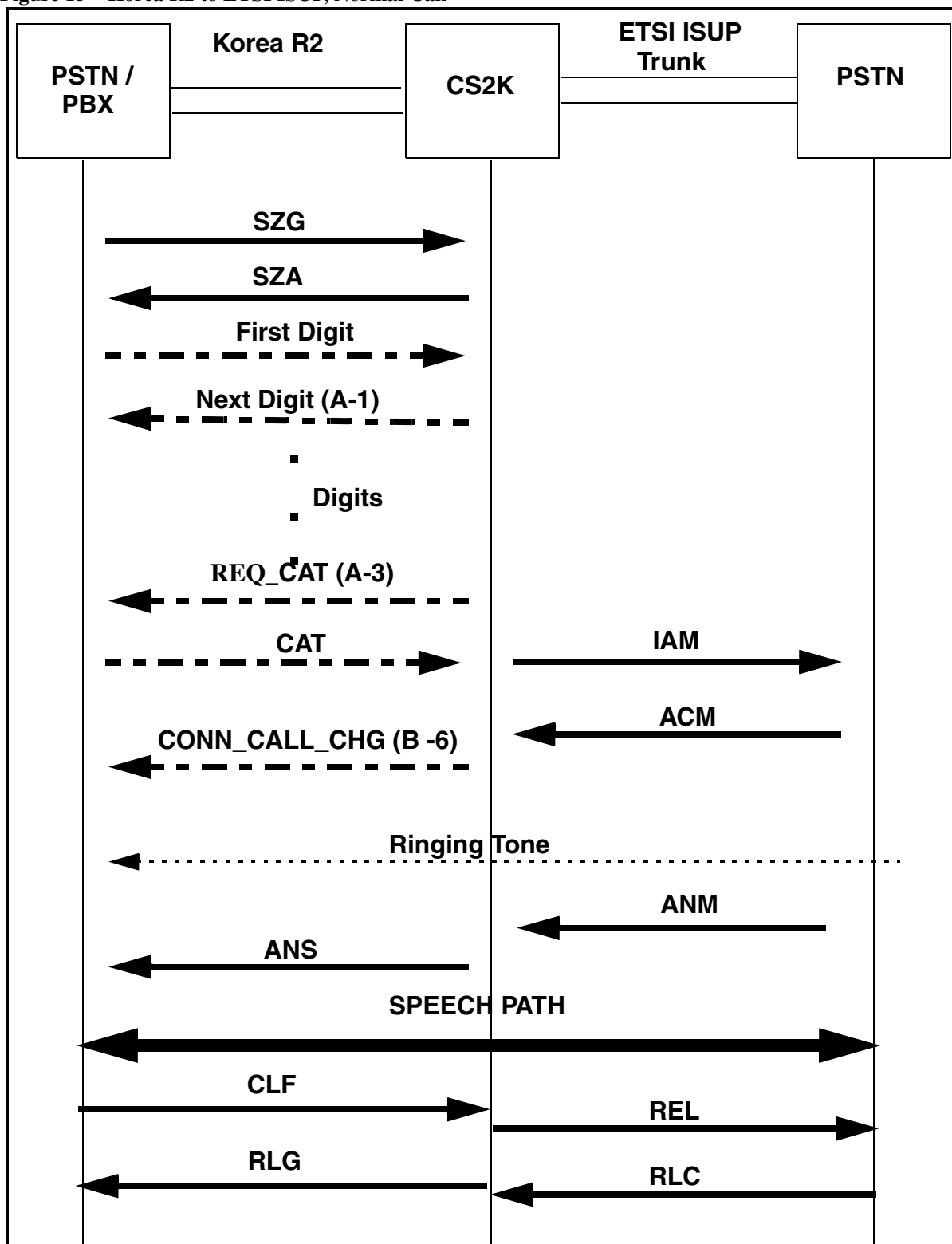
31.4.5.3.1 Korea R2 to ETSI ISUP Interworking

Normal Call Setup with Forward Release

For an overview of the scenario, please refer to Please refer to “Figure 15 Korea R2 to ETSI ISUP, Normal Call” on page 426.. At the interworking exchange, after the called digits and the category are obtained from the R2 side, the IAM is sent on the ETSI ISUP trunk.

On the called party being found, the ACM on ETSI ISUP is mapped to the corresponding R2 signal. This mapping is shown in “Mapping of Backward ISUP Messages to Korea R2 signals” on page 430.

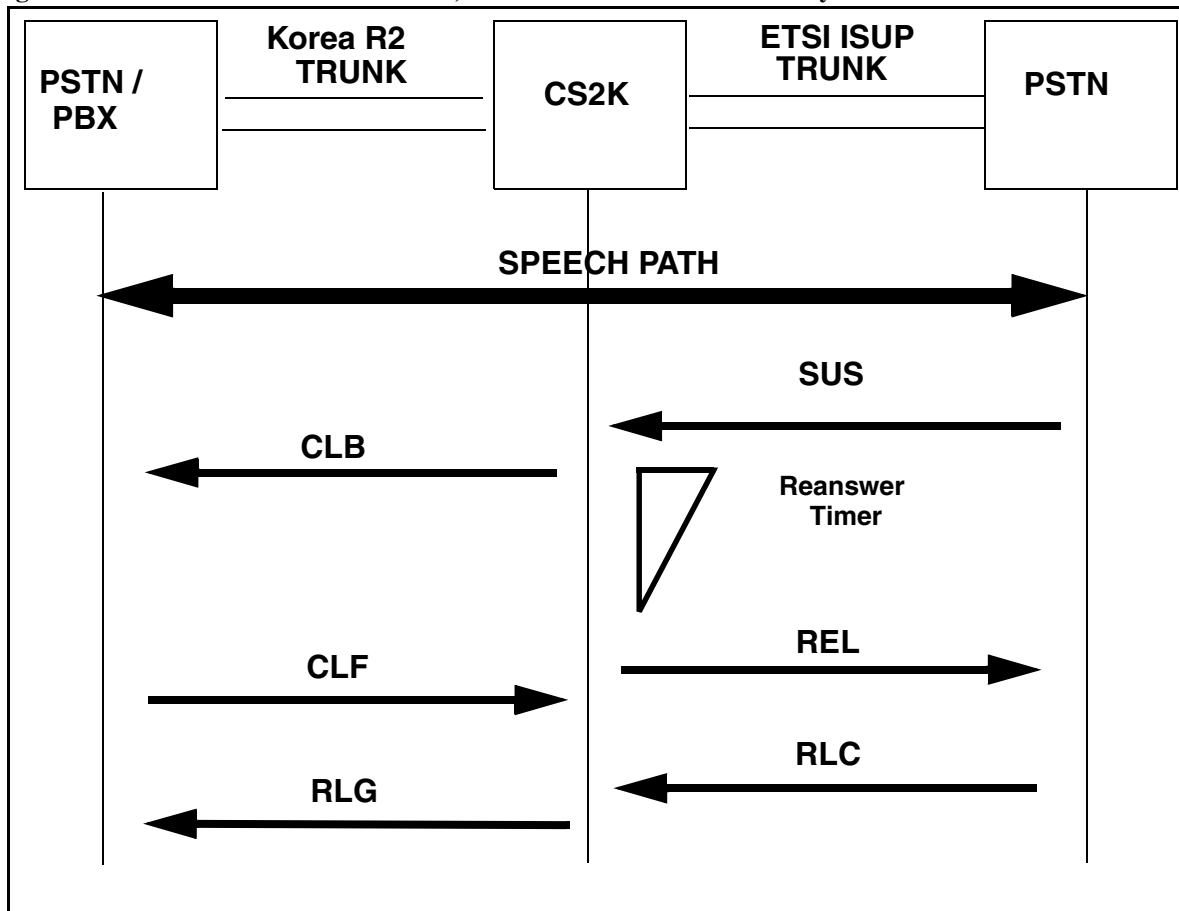
Figure 15 Korea R2 to ETSI ISUP, Normal Call



Normal Call Clearing with Backward Release

On receipt of a Suspend message with SUS / RES indicators “Network Initiated” on the ISUP trunk, a CLB signal is sent on the R2 side, and a reanswer timer is started. If the called party does not reanswer and the reanswer timer expires, a REL message is sent on the ISUP trunk. The R2 trunk is released when the calling party disconnects. This is shown in Please refer to “Figure 16 Korea R2 to ETSI ISUP Call, No Reanswer from Called Party” on page 427..

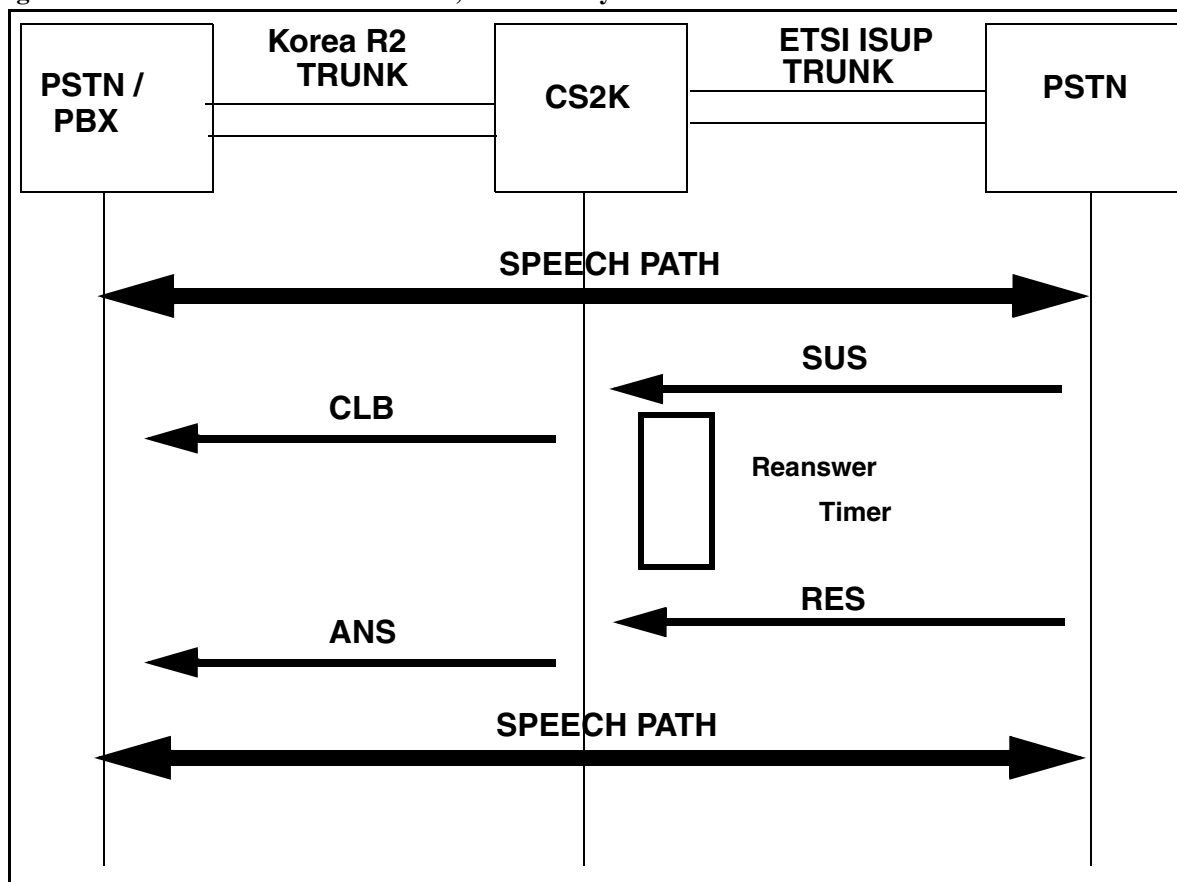
Figure 16 Korea R2 to ETSI ISUP Call, No Reanswer from Called Party



Called Party Reanswer

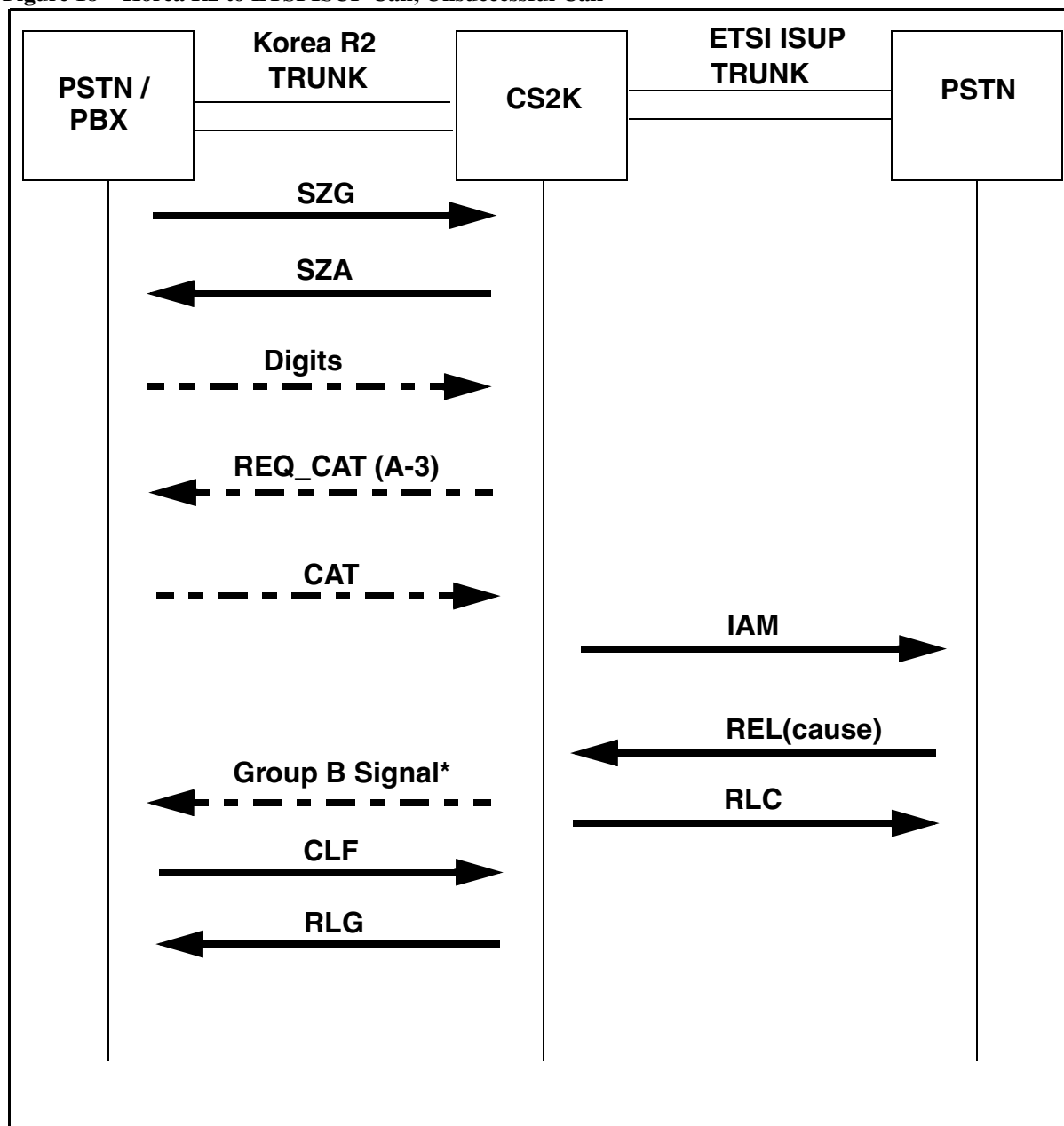
If the called party reanswers, a Reanswer message is sent on the ETSI ISUP trunk. This is then propagated back on the R2 trunk as shown in Please refer to “Figure 17 Korea R2 to ETSI ISUP Call, Called Party Reanswer” on page 428..

Figure 17 Korea R2 to ETSI ISUP Call, Called Party Reanswer

**Unsuccessful Attempt**

When an Release Message (REL) is received on the ISUP trunk, it is mapped to an appropriate Group B R2 signal as shown in Table , “,” on page 431.

Figure 18 Korea R2 to ETSI ISUP Call, Unsuccessful Call



*please refer to , “” on page 431.

Table 10 Mapping of Calling Party Category from Korea R2 to ETSI ISUP

R2 CPC Activity	ETSI ISUP CPC
Regular	Ordinary Calling Subscriber

Table 10 Mapping of Calling Party Category from Korea R2 to ETSI ISUP

Priority	Calling Subscriber with Priority
Mtc_eq	Test Call
Oper	Operator, English
Data	Data Call

Table 11 Mapping of forward Korea R2 signals to ISUP messages

Korea R2 Signal	ISUP Message	Comments
Seize + Seize acknowledgement + Called Digits + Calling Party Category	Initial Address Message (IAM)	Effectively mapped to IAM after digits received.
Clear forward	Release Message (REL)	Cause Value: Normal Clearing (16)
Calling Party Digits	Information message (INF)	If INR has been requested for and ANISEND is ALLOWED or ALWAYS.

Table 12 Mapping of Backward ISUP Messages to Korea R2 signals

ISUP Message	Korea R2 Signal	Comments
Address Complete (ACM)	connect_call_charge/ connect_call_nocharge.	If ACM comes with charge indicator 'charge' or 'no_indication' then connect_call_charge is sent on the R2 side If ACM comes with charge indicator 'no charge' then connect_call_nocharge is sent on the R2 side and answer signal is not sent.
Answer (ANM)	Answer	If connect_call_nocharge is sent then answer line signal is not sent after receiving the ANM.
Suspend (SUS)	Clear Back Signal	
Resume (RES)	answer maintained	
Release (REL)	Clear Back Signal	
Release Complete (RLC)	Not interworked	

ISUP Message	Korea R2 Signal	Comments
Confusion (CFN)	Not interworked	
Connect (CON)	connect_call_chg / connect_call_nochg +Answer	If CON comes with charge indicator 'charge' or 'no_indication' then connect_call_charge is sent on the R2 side If CON comes with charge indicator 'no charge' then connect_call_nocharge is sent on the R2 side and answer signal is not sent.
Information Request (INR) interworked only if it comes before ACM.	req_dn_cat + next_ani	
Reset Circuit Message (RSC)	Clear Back Signal / Congestion tone	If RSC is received before ANM after ACM then a congestion tone is fed to the originator. If RSC is received after ANM clear back signal is sent on the R2 trunk.
Group Reset Circuit (GRS)	Clear Back Signal	
Group Reset Circuit Acknowledge (GRA)	Not Interworked	
Blocking (BLO)	Clear Back Signal	
Blocking Acknowledge (BLA)	Not Interworked	
Hardware Circuit Group Blocking (CGB)	Clear Back Signal	
Maintenance Circuit Group Blocking (CGB)	Not Interworked	
Circuit Group Blocking Acknowledge (CGBA)	Not Interworked	

Table 13 ETSI ISUP REL cause value to Korea R2 Group B Signal mappings

ISUP REL Cause value	R2 Group B Signal
Unallocated Number (1)	B - 5
No Route to destination (3)	B - 5

Send Special Information Tone (4)	B - 2
Normal Call Clearing (16)	A- 4 / B- 4
User Busy (17)	B - 3
No User Responding (18)	A- 4 / B- 4
No User Responding (User Alerted) (19)	A- 4 / B- 4
Subscriber Absent (20)	A- 4 / B- 4
Call Rejected (21)	A- 4 / B- 4
Number Changed (22)	A- 4 / B- 4
Destination Out of Order (27)	B - 8
Invalid Number Format (28)	B - 5
Normal, Unspecified (31)	A- 4 / B- 4
No Circuit / Channel Available	A- 4 / B- 4

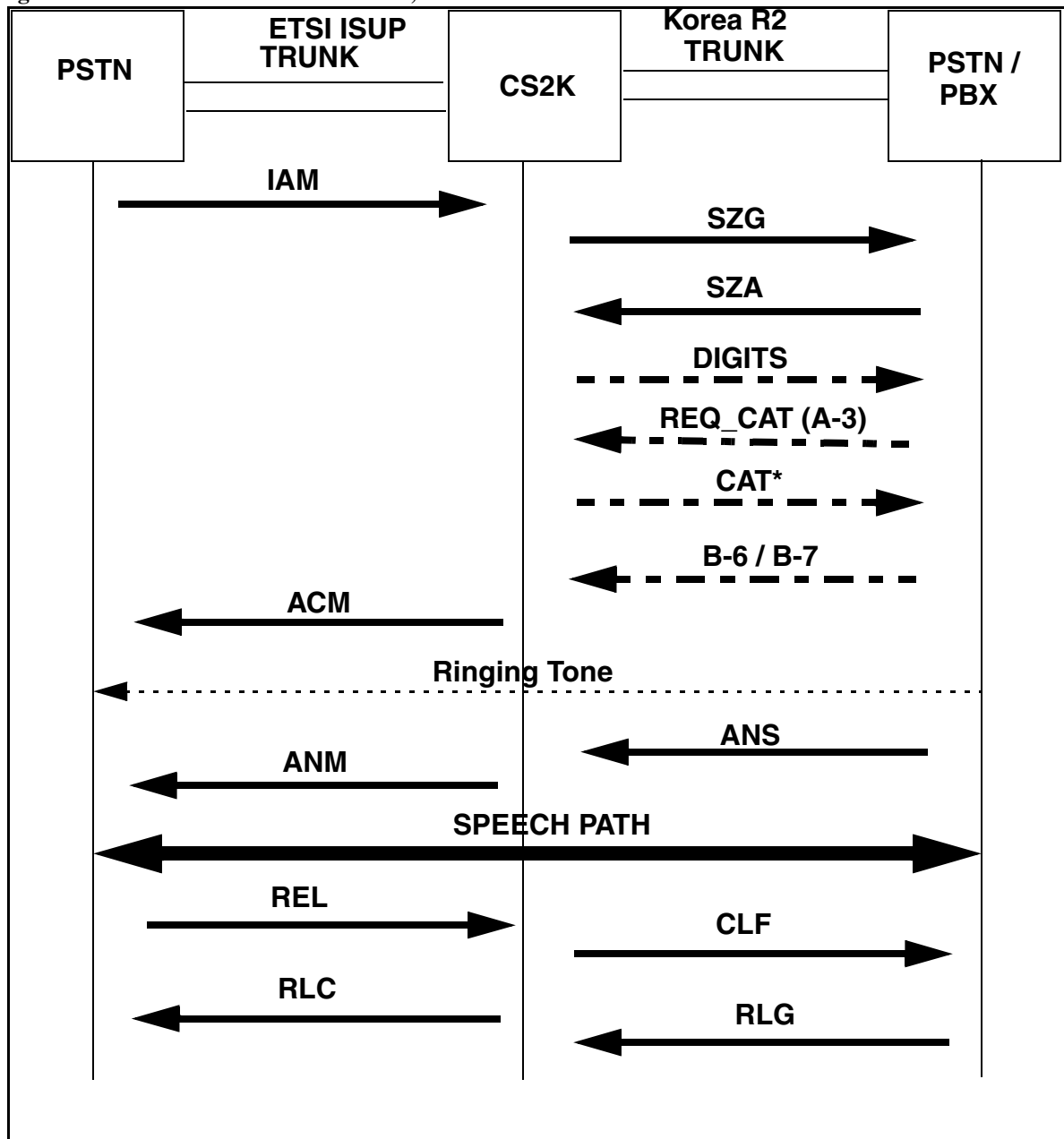
31.4.5.3.2 ETSI ISUP to Korea R2 Interworking

Normal Call Setup with Forward Release

On receipt of a Connect_call_chg (B-6)/Connect_call_no_chg (B-7), an ACM with the charge indication as shown in Table 15, “Mapping of R2 Backward Signals to ETSI ISUP Backward Messages,” on page 437, is sent on the ETSI ISUP trunk. On receipt of ANS from R2, the appropriate ANM message is sent on the ISUP trunk.

The calling party category is mapped as shown in Table 17, “Mapping of Calling Party Category from ETSI ISUP to R2,” on page 438.

Figure 19 ETSI ISUP to Korea R2 Call, Normal Call with Forward Release

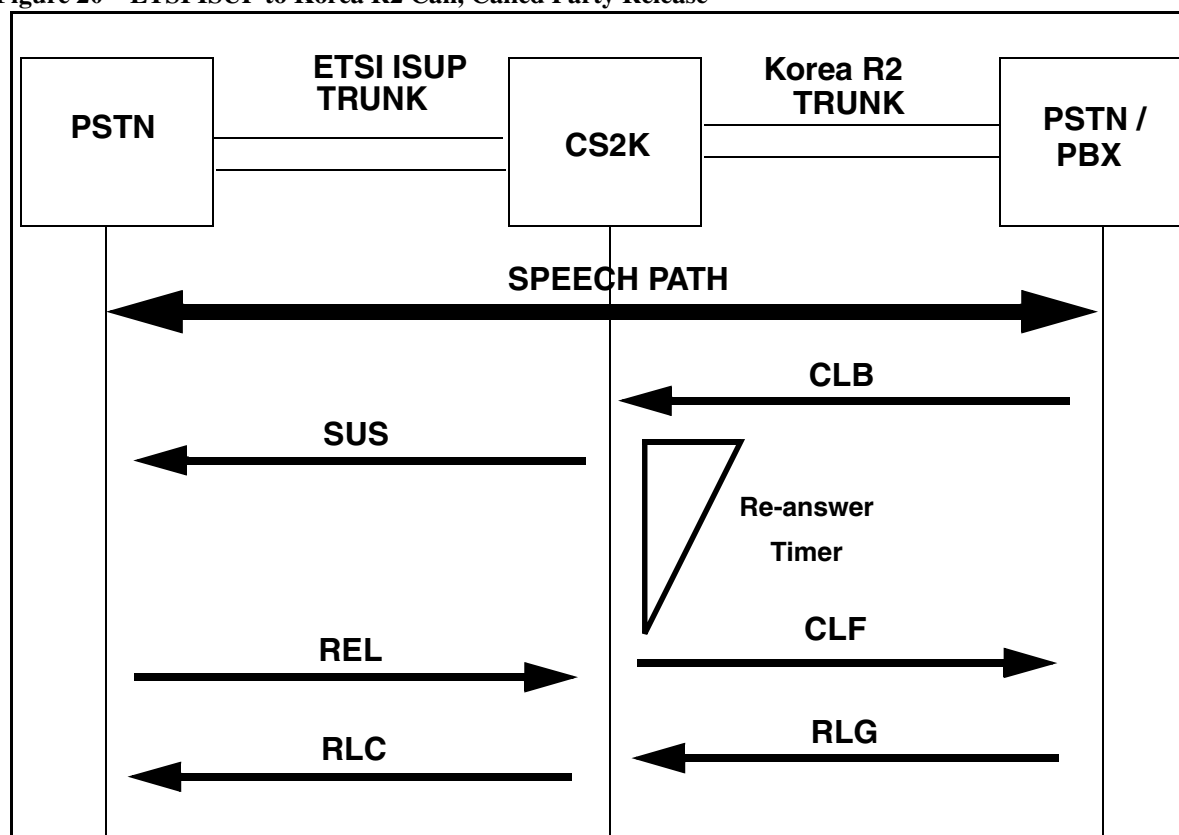


*please refer to Table 17 , “Mapping of Calling Party Category from ETSI ISUP to R2” on page 438.

Normal Call Clearing with Backward Release

The Clear Back signal received on the R2 trunk is propagated back as a SUS message on ETSI ISUP. The Sus / Res indicators of the message would be set to “Network Initiated”. On expiry of the Reanswer timer, the R2 trunk is released. When the calling party clears, then the ETSI ISUP trunk is released.

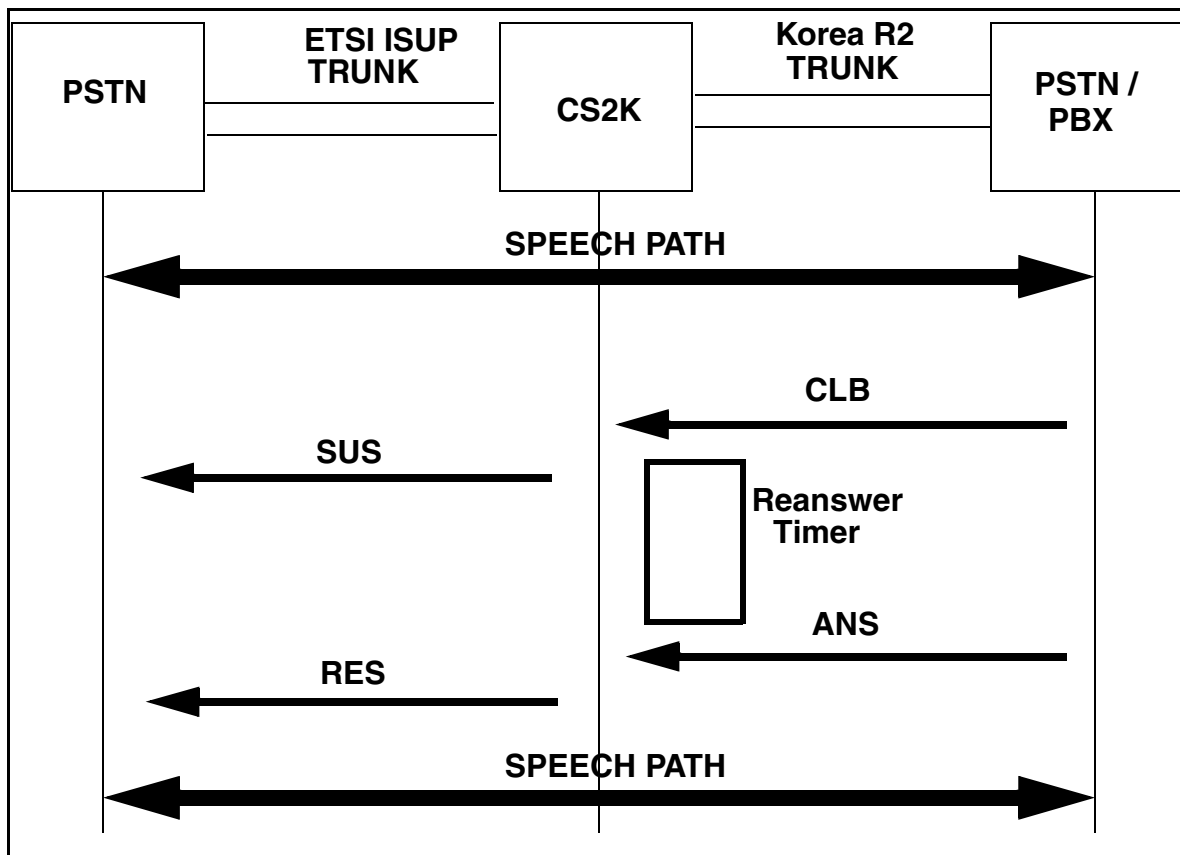
Figure 20 ETSI ISUP to Korea R2 Call, Called Party Release



Called Party Reanswer

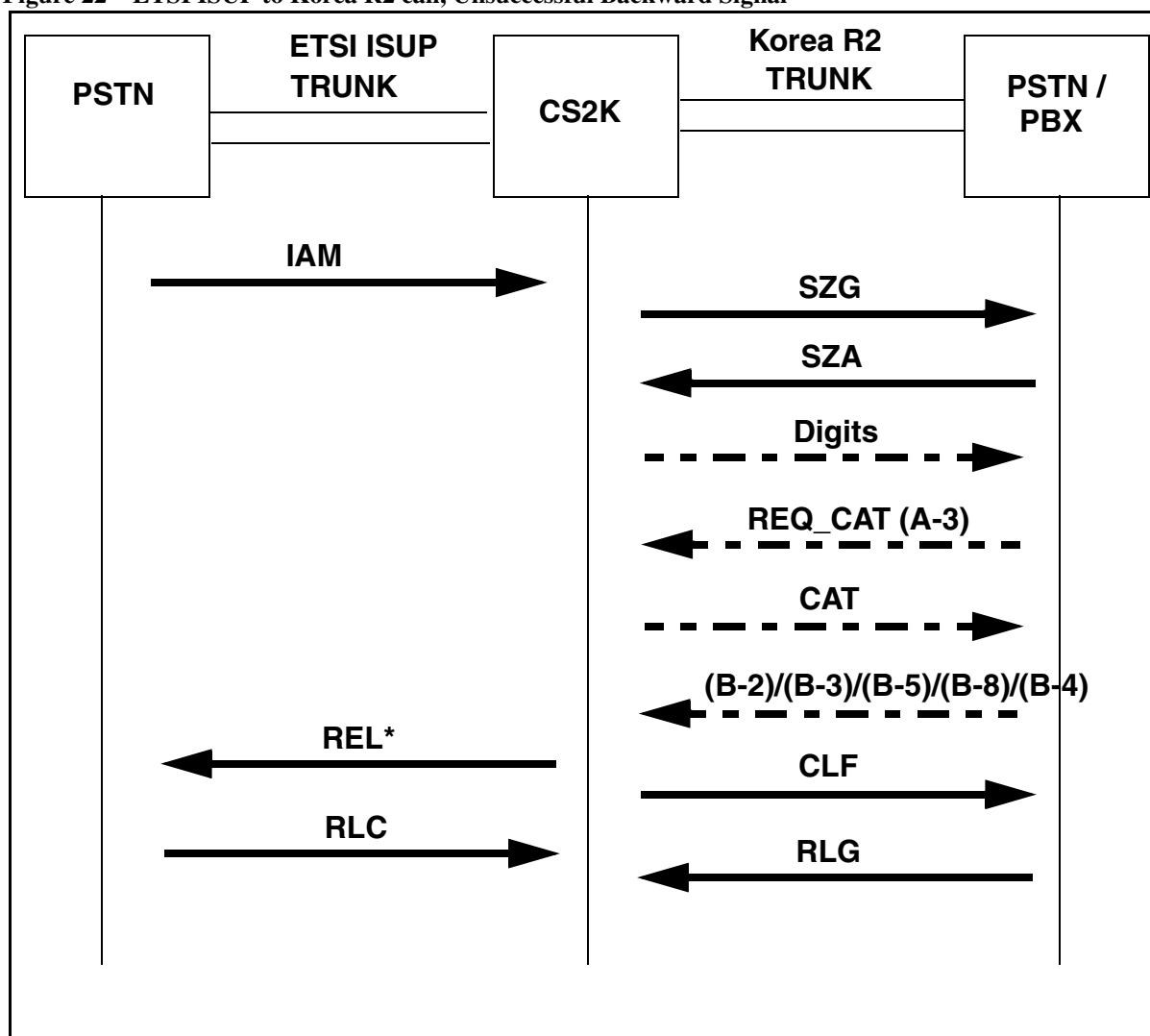
If the called party reanswers before the expiry of the reanswer timer, a RES message is sent on the ETSI ISUP trunk, and speech path is re-established.

Figure 21 ETSI ISUP to Korea R2 Call, Called Party Reanswer

**Unsuccessful Attempt**

On receipt of an unsuccessful backward signal as shown in “ETSI ISUP to Korea R2 call, Unsuccessful Backward Signal” on page 436, the mapping takes place as shown in Table 16, “Korea R2 Group B Signals to ISUP REL Cause Value Mappings,” on page 438.

Figure 22 ETSI ISUP to Korea R2 call, Unsuccessful Backward Signal



*Refer to “Korea R2 Group B Signals to ISUP REL Cause Value Mappings” on page 438.

Table 14 Mapping of ETSI ISUP Forward Messages to Forward Korea R2 Signals

ETSI ISUP Message	ETSI ISUP Parameters	Korea R2 Signals	Comments
IAM	Calling Party Category	Group II Forward Register Signals (Calling Party Category Activities)	Please refer to “Table 17 Mapping of Calling Party Category from ETSI ISUP to R2” on page 438.
	Address Signals (called party and calling party)	Group I Forward Register Signals	
	0000	0	
	0001	1	
	----	-	
	----	-	
	1001	9	
REL	Cause value	Clear Forward Signal	Clear Forward Signal is sent on the R2 trunk regardless of the cause value of the REL message.

Table 15 Mapping of R2 Backward Signals to ETSI ISUP Backward Messages

R2 Signal	ETSI ISUP Message	ETSI ISUP Parameter	Comments
B-6	ACM	Backward Call Indicators Charge Indicator = “Charge”	
B-7	ACM	Backward Call Indicators Charge Indicator = “No Charge”	
ANS	ANM	Backward Call Indicators	The Backward Call Indicators parameter will be the same as that sent in the ACM
CLB	SUS	Suspend Resume Indicators = “Network Initiated”	
ANS	RES	Suspend Resume Indicators = “Network Initiated”	

Table 16 Korea R2 Group B Signals to ISUP REL Cause Value Mappings

R2 Group B Signal	ISUP REL Cause value
B - 2	No.4 Send Special Information Tone
B - 3	No. 17 User Busy
B - 4	No. 31 Normal, Unspecified
B - 5	No. 1 Unallocated Number
B - 8	No. 27 Destination Out of Order

Table 17 Mapping of Calling Party Category from ETSI ISUP to R2

ETSI ISUP CPC	R2 CPC
Unknown Source	REGULAR
Operator, French	OPER
Operator, English	OPER
Operator, German	OPER
Operator, Russian	OPER
Operator, Spanish	OPER
Ordinary Calling Subscriber	REGULAR
Calling Subscriber with Priority	PRIORITY
Data Call	DATA
Test Call	MTC_EQ
All Other Calling Party Activities	REGULAR

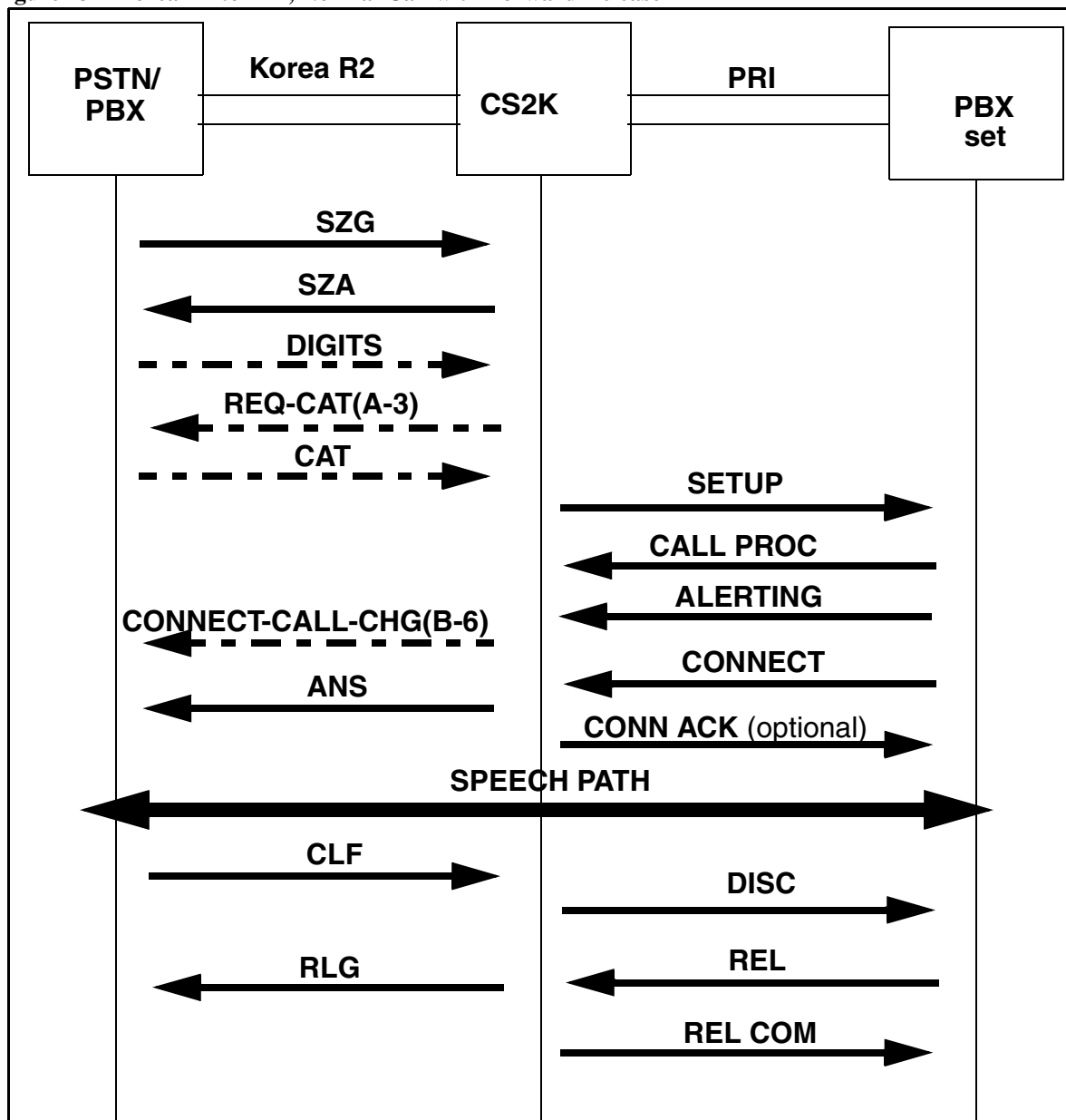
31.4.5.4 Interworking with ETSI PRI

31.4.5.4.1 Korea R2 interworking with PRI

Normal Call Setup with Forward Release

The scenario for normal call setup from Korea R2 to PRI with forward call release as shown in Please refer to “Figure 23 Korea R2 to PRI, Normal Call with Forward Release” on page 439..

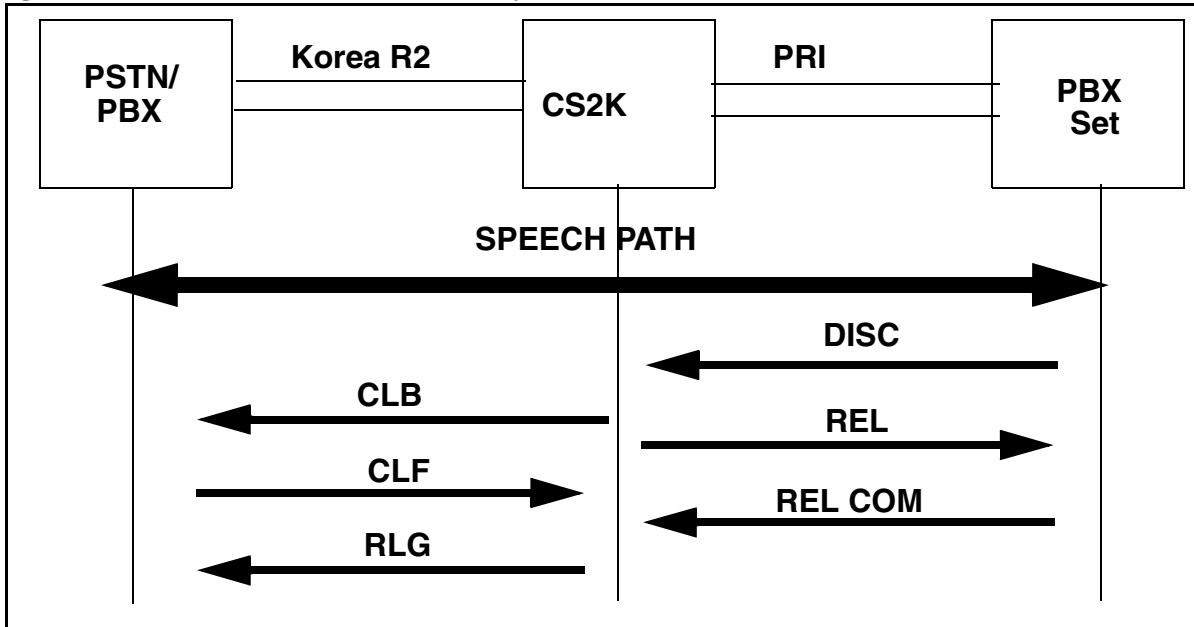
Figure 23 Korea R2 to PRI, Normal Call with Forward Release



Normal Call Clearing with Backward Release

A Korea R2 to PRI call with release from the called party is shown in Please refer to “Figure 24 Korea R2 to PRI call, Called Party Release” on page 440. A DISCONNECT from PRI is mapped to CLB on the Korea R2 trunk.

Figure 24 Korea R2 to PRI call, Called Party Release



Called Party Reanswer

Since ETSI PRI do not support reanswer, reanswer is not supported for Korea R2 to PRI calls.

Unsuccessful Attempt

On receipt of a REL COM plete from PRI, it is mapped as shown in Please refer to “Figure 25 Korea R2 to PRI Unsuccessful Call” on page 441. The mapping from PRI cause values to Korea R2 signals is as shown in Table 20, “Mapping of Release Cause values from PRI to Korea R2,” on page 442.

Figure 25 Korea R2 to PRI Unsuccessful Call

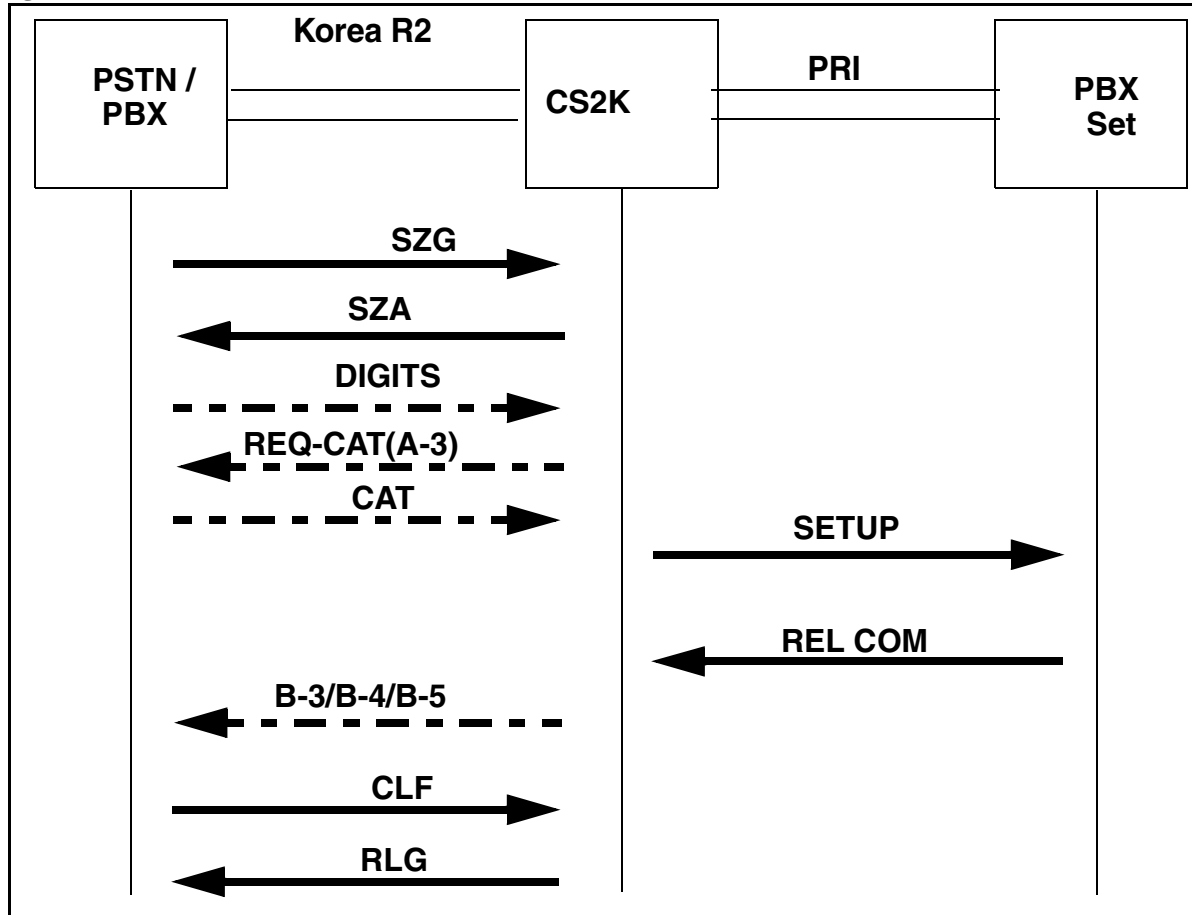


Table 18 Korea R2 Signals to ETSI PRI SETUP Message Mapping

Korea R2 signals	Setup message parameters	Comments
	Called Party Number	
Group-1 forward register signals (digit signals)	-- Address Digits -- Type of Number 000 = unknown -- Numbering Plan 0000 = unknown	The Type of number and Numbering Plan will be determined by translations.
	Calling Party Number	

Korea R2 signals	Setup message parameters	Comments
Group-1 forward register signals (digit signals)	-- Address Digits -- Type of Number 000 = unknown -- Numbering Plan 0001 = ISDN/Telephony -- Screening Indicator 00 = user provided, not screened -- Presentation Indicator 00 = presentation allowed	Only if ANI is provisioned on the R2 trunk. The Type of number and Numbering plan will be determined by translations.
	Bearer Capability	This indicates the type of call and the transmission rate requested.
Group-2 Calling Party Category activities	-- Transfer Capability 00000 = speech	R2 CPC value of data will be mapped to BC transfer capability unrestricted digital information. All other R2 CPC values will be mapped to speech.

Table 19 Mapping of PRI Messages to Korea R2 Signals

PRI Message	Korea R2 Signal	Comments
CALL PROCEEDING	Not inteworked	
ALERTING	connect_call_chg	
CONNECT	Answer signal (ANS)	

Table 20 Mapping of Release Cause values from PRI to Korea R2

Release Cause Value	R2 Signal
No. 21 Cause Rejected	B - 4
No. 34 Channel Unavailable	B - 4

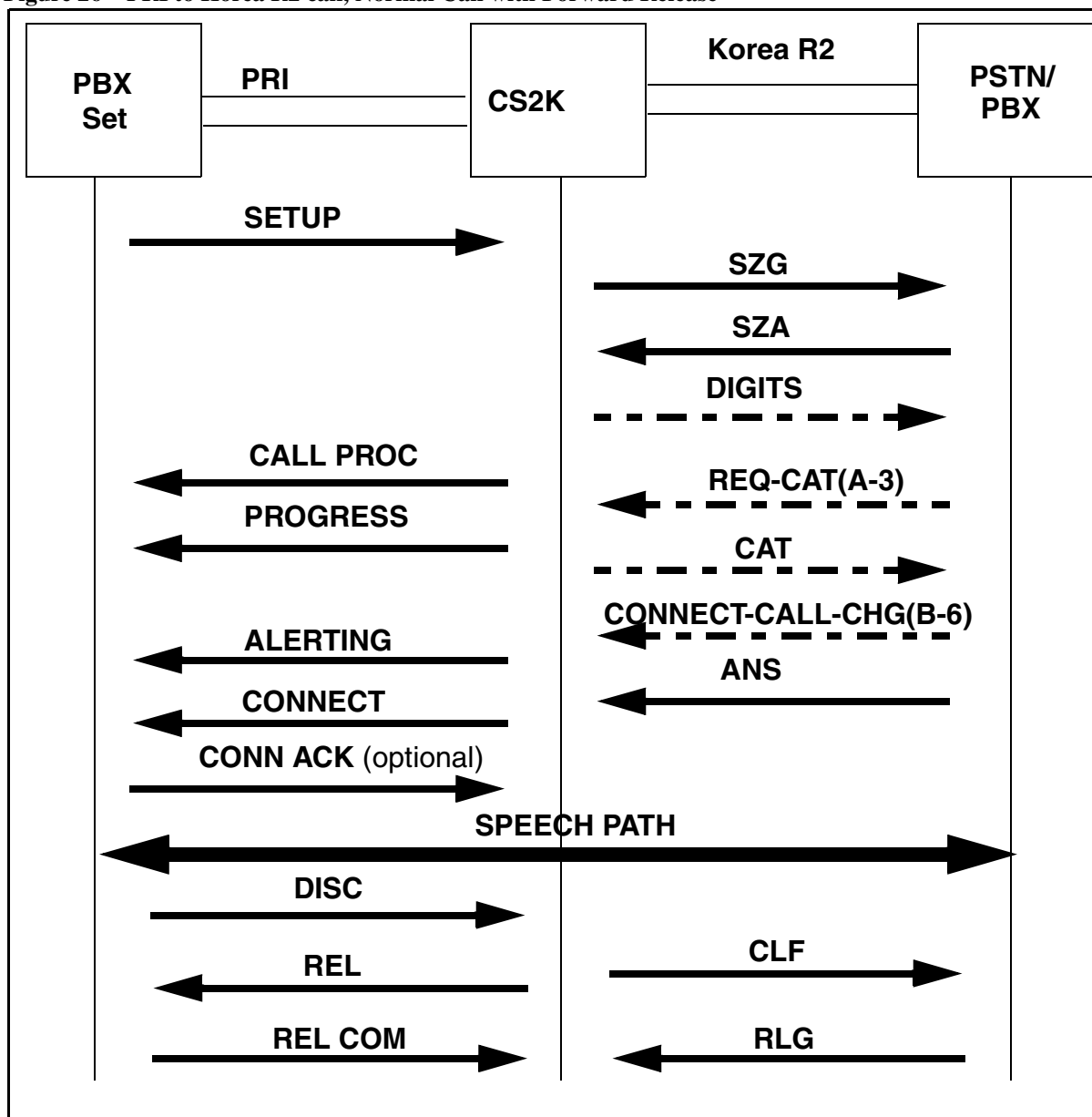
Table 20 Mapping of Release Cause values from PRI to Korea R2

No.17 User Busy	B - 3
No.1 Unallocated Number	B - 5
No. 102 Recovery on Timer Expiry	B - 4

31.4.5.4.2 PRI Interworking with Korea R2**Normal Call Setup with Forward Release**

The overview for a normal call from PRI to Korea R2 is shown in Please refer to “Figure 26 PRI to Korea R2 call, Normal Call with Forward Release” on page 444.

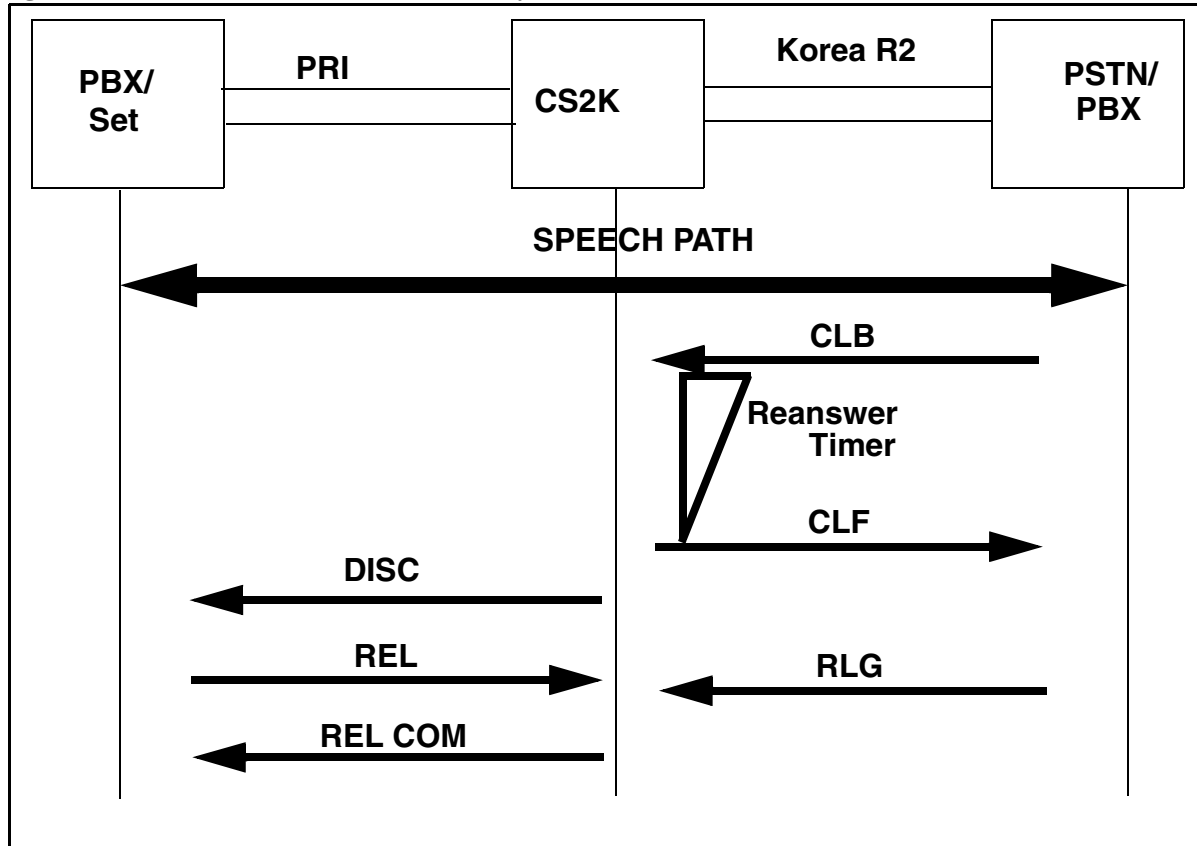
Figure 26 PRI to Korea R2 call, Normal Call with Forward Release



Normal Call Clearing with Backward Release

On release by the called party, a reanswer timer is started at the CS2K. On expiry of the reanswer timer, a CLF signal is sent on the R2 trunk and a DISConnect message is sent in the backward direction.

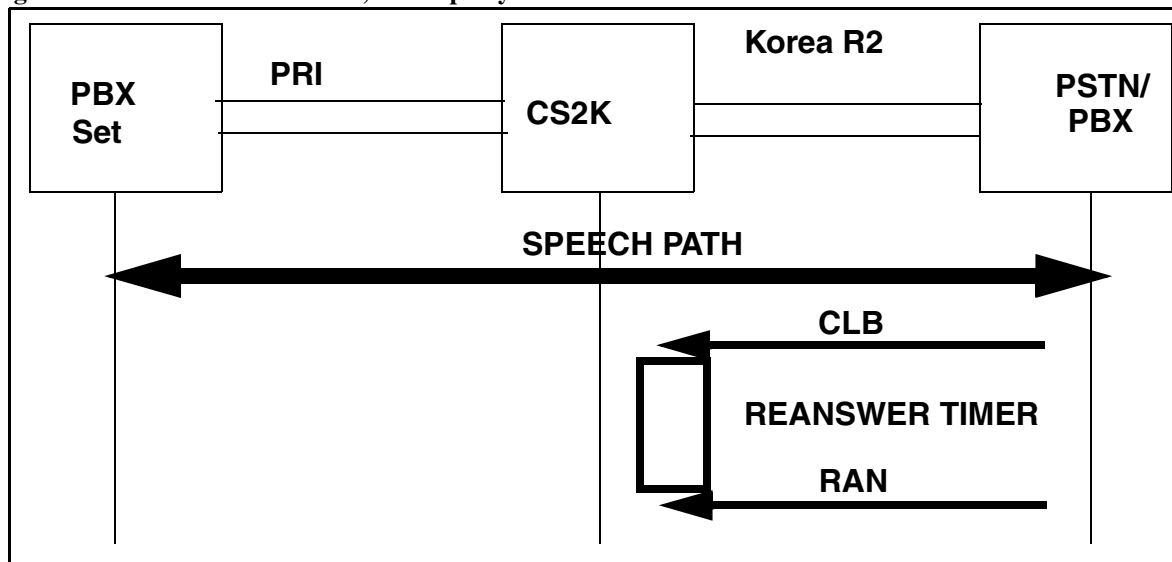
Figure 27 PRI to Korea R2 call, Called Party Release



Called Party Reanswer

If the called party goes off-hook before the expiry of the reanswer timer, then a RAN signal is received by the CS2K, as shown in the following figure as shown in Please refer to “Figure 28 PRI to Korea R2 call, called party reanswer” on page 446.

Figure 28 PRI to Korea R2 call, called party reanswer

**Unsuccessful Attempt**

The mapping from Unsuccessful Group-B signals to PRI Disconnect cause values is shown in Table 22, "Mapping of Korea R2 Signals to PRI Disconnect Cause Values," on page 449.

Figure 29 PRI to Korea R2 unsuccessful call

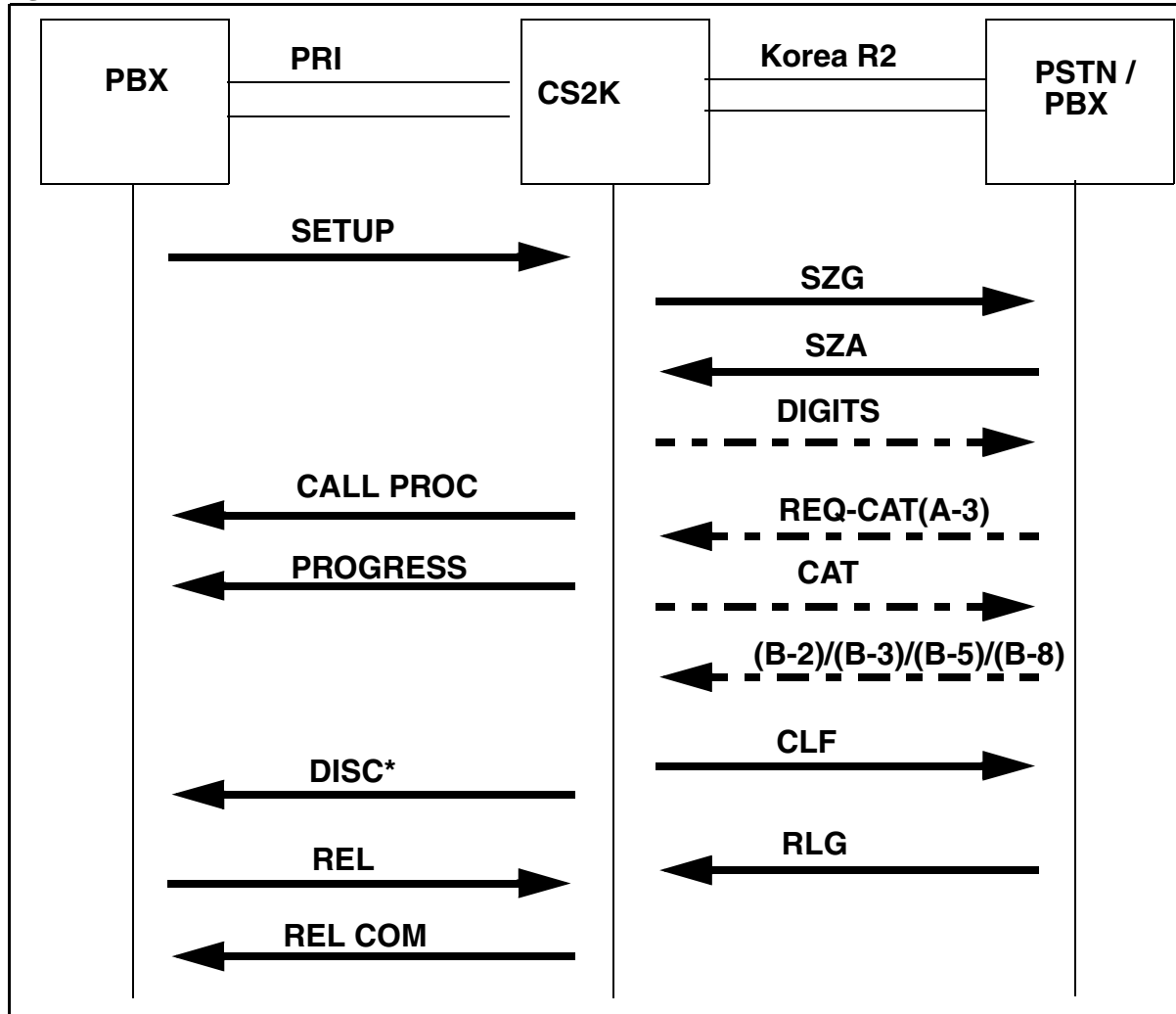


Figure 30 Mapping of PRI SETUP Message to Korea R2

PRI setup Information Element	Korea R2 Signals	Comments
Called Party Number		
-- Address Digits	Group-1 digit signals	Type of Number and Numbering Plan: All valid Q.931 values will be accepted and treated as "unknown",
-- Type of number		
000 = unknown		
-- Numbering Plan		
0000 = unknown		

PRI setup Information Element	Korea R2 Signals	Comments
Calling Party Number		
-- Address Digits -- Type of Number 000 = unknown -- Numbering Plan 0001 = ISDN/Telephony 1001 = private -- Screening Indicator 00 = user provided, not screened -- Presentation Indicator 00 = presentation allowed	Group-1 digit signals	Only if ANI is allowed on the outgoing R2 trunk. Type of Number and Numbering plan: All valid Q.931 values will be accepted and treated as "unknown".
Bearer Capability		This indicates the type of call and the transmission rate requested.
-- Transfer Capability Speech 3.1 kHz audio Unrestricted digital information		The other BC information such as '7 kHz audio' and video are not supported in the context of R2 interworking and the call is taken down in these cases.

Table 21 Mapping of Korea R2 Signals to PRI Messages

Korea R2 Signal	PRI Message	Comments
connect_call_chg / connect_call_nochg	ALERTING	
Answer signal (ANS)	CONNECT	

Table 22 Mapping of Korea R2 Signals to PRI Disconnect Cause Values

Group B Signal	Disconnect Cause Value
B-2	No.22 Number Changed
B-3	No.17 User Busy
B-5	No.1 Unallocated Number
B-8	No.27 Destination Out Of Order

Table 23 Normal Call Setup Message Mapping

Korea R2 Signal	Trigger Direction	ETSI PRI Message
SZG	=>	Setup
SZA		
GRP 1, A		
NEXT_DIGIT ^a		
Called Party Digit ^b		
GRP A-3 REQ_CAT		
GRP II Category		
No Mapping	<=	Call Proceeding
GRP B-6	<=	Alerting / Progress
CONNECT_CALL_CHARGE		
Answer	<=	Connect

a. Multiple NEXT_DIGIT signals will be sent until all Called Party Digits have been collected.

b. One Called Party Digit will be sent in response to each NEXT_DIGIT signal received

31.5 Provisioning

31.5.1 Datafill for a Korea R2 call

Table ACTSIG

% KOREA Outgoing Phase 0 or 3
100 DIGIT_1 1
100 DIGIT_2 2
100 DIGIT_3 3
100 DIGIT_4 4
100 DIGIT_5 5
100 DIGIT_6 6
100 DIGIT_7 7
100 REQ_NOT_ACC 12
100 DIGIT_8 8
100 DIGIT_9 9
100 DIGIT_0 10
100 END_OF_DIGS 15

% KOREA Incoming Phase 0
101 NEXT_DIGIT 1
101 REQ_CAT 3
101 CONGESTION 4
101 RCV_TMO_ACT 4
101 REQ_DN_CAT 5
101 CHANGE_TO_B 3

% KOREA Outgoing Phase 1 or 2 or 3
102 REGULAR 1
102 PRIORITY 2
102 MTC_EQ 3
102 COIN 4
102 OPER 5
102 DATA 6
102 REQ_NOT_ACC 12

% KOREA Incoming Phase 1 or 4
103 SUB_XFRD 2
103 SUB_BUSY 3
103 RCV_TMO_ACT 4
103 CONGESTION 4
103 UNASSIGN_NUM 5
103 CONNECT_CALL_CHG 6
103 CONNECT_CALL_NOCHG 7
103 SUB_OUT_ORD 8
103 CONNECT_CALL_CHG 1

% KOREA Incoming Phase 2
104 CONGESTION 4
104 NEXT_ANI_DIGIT 5
104 NEXT_DIGIT 1
104 CHANGE_TO_B 3

% KOREA Incoming Phase 3
105 NEXT_DIGIT 1
105 REQ_CAT 3
105 CONGESTION 4
105 NEXT_ANI_DIGIT 5

105 CHANGE_TO_B 3

Table SIGACT

% Incoming PHASE 0 or 3

100 1 DIGIT_1
 100 2 DIGIT_2
 100 3 DIGIT_3
 100 4 DIGIT_4
 100 5 DIGIT_5
 100 6 DIGIT_6
 100 7 DIGIT_7
 100 8 DIGIT_8
 100 9 DIGIT_9
 100 10 DIGIT_0
 100 12 REQ_NOT_ACC
 100 15 END_OF_DIGS

% KOREA Outgoing Phase 0

101 1 NEXT_DIGIT
 101 3 REQ_CAT
 101 4 CONGESTION
 101 5 REQ_DN_CAT

% Incoming PHASE 1 or 2

102 1 REGULAR
 102 2 PRIORITY
 102 3 MTC_EQ
 102 4 COIN
 102 5 OPER
 102 6 DATA
 102 12 REQ_NOT_ACC

% KOREA Outgoing Phase 1 or 4

103 2 SUB_XFRD
 103 3 SUB_BUSY
 103 5 UNASSIGN_NUM
 103 6 CONNECT_CALL_CHG
 103 7 CONNECT_CALL_NOCHG
 103 8 SUB_OUT_ORD
 103 1 CONNECT_CALL_CHG

% KOREA Incoming Phase 2

104 4 CONGESTION
 104 5 NEXT_ANI_DIGIT
 104 1 NEXT_DIGIT
 104 3 REQ_CAT

% KOREA Incoming Phase 3

105 1 NEXT_DIGIT
 105 3 REQ_CAT
 105 4 CONGESTION
 105 5 NEXT_ANI_DIGIT

% KOREA Incoming Phase 4

106 1 SPARE_CAT1
 106 2 SPARE_CAT1
 106 3 SPARE_CAT1
 106 4 SPARE_CAT1

106 5 SPARE_CAT1
106 6 SPARE_CAT1

Table ACTCTL

KORTLI DIGIT_1 NO_CHANGE NO_CHANGE
KORTLI DIGIT_2 NO_CHANGE NO_CHANGE
KORTLI DIGIT_3 NO_CHANGE NO_CHANGE
KORTLI DIGIT_4 NO_CHANGE NO_CHANGE
KORTLI DIGIT_5 NO_CHANGE NO_CHANGE
KORTLI DIGIT_6 NO_CHANGE NO_CHANGE
KORTLI DIGIT_7 NO_CHANGE NO_CHANGE
KORTLI DIGIT_8 NO_CHANGE NO_CHANGE
KORTLI DIGIT_9 NO_CHANGE NO_CHANGE
KORTLI DIGIT_0 NO_CHANGE NO_CHANGE
KORTLI REGULAR NO_CHANGE NO_CHANGE
KORTLI END_OF_DIGS NO_CHANGE NO_CHANGE
KORTLI OPER NO_CHANGE NO_CHANGE
KORTLI DATA NO_CHANGE NO_CHANGE
KORTLI COIN NO_CHANGE NO_CHANGE
KORTLI PRIORITY NO_CHANGE NO_CHANGE
KORTLI MTC_EQ NO_CHANGE NO_CHANGE
KORTLI INIT_IC_ACT GENERAL PHASE_0
KORTLI REQ_NOT_ACC NO_CHANGE NO_CHANGE
KORTLI REQ_CAT NO_CHANGE PHASE_1
KORTLI REQ_DN_CAT NO_CHANGE PHASE_2
KORTLI NEXT_ANI_DIGIT NO_CHANGE PHASE_3
KORTLI NEXT_DIGIT NO_CHANGE PHASE_0
KORTLI SUB_BUSY NO_CHANGE NO_CHANGE
KORTLI SUB_XFRD NO_CHANGE NO_CHANGE
KORTLI CONNECT_CALL_CHG NO_CHANGE NO_CHANGE
KORTLI CONNECT_CALL_NOCHG NO_CHANGE NO_CHANGE
KORTLI UNASSIGN_NUM NO_CHANGE NO_CHANGE
KORTLI SUB_OUT_ORD NO_CHANGE NO_CHANGE
KORTLI CONGESTION NO_CHANGE NO_CHANGE
KORTLI CONNECT_CALL_CHG NO_CHANGE NO_CHANGE
KORTLI RCV_TMO_ACT NO_CHANGE NO_CHANGE
KORTLI CHANGE_TO_B NO_CHANGE PHASE_4
KORTLI SPARE_CAT1 NO_CHANGE NO_CHANGE
KORTLI CONNECT_CALL_CHG NO_CHANGE NO_CHANGE
KORTLO INIT_OG_ACT GENERAL PHASE_0
KORTLO CONNECT_CALL_CHG NO_CHANGE NO_CHANGE
KORTLO SUB_XFRD NO_CHANGE NO_CHANGE
KORTLO DIGIT_1 NO_CHANGE NO_CHANGE
KORTLO DIGIT_2 NO_CHANGE NO_CHANGE
KORTLO DIGIT_3 NO_CHANGE NO_CHANGE
KORTLO DIGIT_4 NO_CHANGE NO_CHANGE
KORTLO DIGIT_5 NO_CHANGE NO_CHANGE
KORTLO DIGIT_6 NO_CHANGE NO_CHANGE
KORTLO DIGIT_7 NO_CHANGE NO_CHANGE
KORTLO DIGIT_8 NO_CHANGE NO_CHANGE
KORTLO DIGIT_9 NO_CHANGE NO_CHANGE
KORTLO DIGIT_0 NO_CHANGE NO_CHANGE
KORTLO REGULAR NO_CHANGE NO_CHANGE
KORTLO END_OF_DIGS NO_CHANGE NO_CHANGE
KORTLO REQ_NOT_ACC NO_CHANGE NO_CHANGE
KORTLO OPER NO_CHANGE NO_CHANGE
KORTLO DATA NO_CHANGE NO_CHANGE
KORTLO PRIORITY NO_CHANGE NO_CHANGE
KORTLO MTC_EQ NO_CHANGE NO_CHANGE
KORTLO COIN NO_CHANGE NO_CHANGE

Table CATCLASS

Table R2PROT

Table FDCPLSWF**Table FDCPLSTM**

Table CLLI

Table TRKGRP

Table RGSIGSYS

KOREA FDCPSPS 1500 2400 30 30 1500 500 10 15 20 6000 80 6000 0 0 0

Table ACTTRTMT

KORTRMT SUB_BUSY BUSY
 KORTRMT SUB_XFRD NINT
 KORTRMT CONGESTION GNCT
 KORTRMT UNASSIGN_NUM BLDN
 KORTRMT SUB_OUT_ORD TESS

Table TRTMTACT

KORTRMT BUSY SUB_BUSY
 KORTRMT GNCT CONGESTION
 KORTRMT NINT SUB_XFRD
 KORTRMT BLDN UNASSIGN_NUM
 KORTRMT TESS SUB_OUT_ORD
 KORTRMT RODR CONGESTION

Table FDCPLSVR

KOR_VR KOREACAS \$

Table TRKSGRP

KOREAR2LPA 0 P30CAS FST N NILTYPE Y 2W N NIL KOREA FDCP KORPROT KORTRMT +
 KOR_VR KOR_TM MFC LNK NOVERLAP STAND \$
 KOREAR2LPB 0 P30CAS FST N NILTYPE Y 2W N NIL KOREA FDCP KORPROT KORTRMT +
 KOR_VR KOR_TM MFC LNK NOVERLAP STAND \$

Table TRKMEM

KOREAR2LPA 10 0 GWC 100 27 10
 KOREAR2LPA 11 0 GWC 100 27 11
 KOREAR2LPA 12 0 GWC 100 27 12
 KOREAR2LPA 13 0 GWC 100 27 13
 KOREAR2LPB 1 0 GWC 100 27 1009
 KOREAR2LPB 2 0 GWC 100 27 1010
 KOREAR2LPB 3 0 GWC 100 27 1011
 KOREAR2LPB 4 0 GWC 100 27 1012

Table PXHEAD

IDCXLA SDFLT NODFOP NOCON STD
 IDCISD SDFLT NODFOP NOCON STD

Table PXCDE

IDCXLA 136 136 RTE PF 3 MM 5 18 DEST 136 CLASS NATL LNET LOCAL MZONE 0 \$

Table PXRTE

IDCXLA 136 S KOREAR2LPA \$

Table FAILMSG

Q767 USERBUSY FDCP N TREAT BUSY
 Q767 NUMCHANG FDCP N TREAT NINT
 Q767 UNALLOC FDCP N TREAT BLDN
 Q767 DOOSRVC FDCP N TREAT TESS
 Q764 USERBUSY FDCP N TREAT BUSY
 Q764 NUMCHANG FDCP N TREAT NINT
 Q764 UNALLOC FDCP N TREAT BLDN
 Q764 DOOSRVC FDCP N TREAT TESS

Table TMTMAP

PRI BUSY ALLBC PRI NOLOCAL USERBUSY Y
 PRI NINT ALLBC PRI NOLOCAL NUMCHANG Y
 PRI BLDN ALLBC PRI NOLOCAL UNALLOC Y
 PRI TESS ALLBC PRI NOLOCAL DOOSRVC Y

Table TRKOPTS

KNGA210ISBWE REANSTMR REANSTMR 30 This is datafilled against the interworking ANSI ISUP Trunk.

Table CTRLTMRS

LCL 60 60 0
 NATL 90 90 0
 INTL 120 120 0

31.5.2 Example of a traver for a Korea R2 to PRI Data call

```
>traver 1 7700073 136837700053 bc 64kdata b
Warning: Routing characteristics are present.
        Originator must be able to send in
        characteristics specified.
TABLE RTECHAR
. 64KDATA ( BC 64KDATA $)$
TABLE KSETLINE
HOST 04 1 02 03 1 DN Y 7700053 IDCGRP 0 1 905 (CFX) (LNRA) $ MBS
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
Originator is not an EIN agent, therefore EIN info is not processed.
Originator is not an EIN agent, therefore EIN info is not processed.
TABLE NCOS
IDCGRP 1 0 0 $ ( XLAS INLOOP IDCFEAT NDGT) ( ACR N)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
IDCGRP NXLA IDCXLA IDCFEAT 0 IDC
TABLE DIGCOL
IDC 1 RPT
TABLE XLAMAP
. 64KDATA INLOOP ( XLA 64KXLA)$
TABLE IBNXLA: XLANAME 64KXLA
TUPLE NOT FOUND
DEFAULT FROM TABLE XLANAME:
64KXLA
(NET N Y 0 N NDGT N Y GEN (LATTR 5 905_NPRT_0 NLCA_NILLA_0) $ $)$ 9
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
5 IBN NONE NT 0 0 NILSFC 0 PX IDCXLA NIL 00 905_NPRT_0 NLCA_NILLA_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
905_NPRT_0 NSCR 905 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_0 NLCA NIL NILLATA $
TABLE UNIRCXLA
. 64KDATA IDCXLA PX 64KXLA
. Attention: XLASYS or XLANAME or both changed.
. -----
.
TABLE PXHEAD
```

64KXLA DFLT TRMT (OFC VACT)\$ NODFOP NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 136837700053
TABLE PXCODE
64KXLA 136 136 RTE (PF 3) (MM 5 18) (DEST 136) (CLASS NATL) (LNET LOCAL) (MZONE 0)\$
Tuple not found
TABLE: PXRTE
KEY: 64KXLA 136
. S KOREAR2LPA
EXIT TABLE PXRTE
Originator is not an EIN agent, therefore EIN info is not processed.
Originator is not an EIN agent, therefore EIN info is not processed.

+++ TRAVER: SUCCESSFUL CALL TRACE +++
DIGIT TRANSLATION ROUTES

1 KOREAR2LPA 837700053 ST

TREATMENT ROUTES. TREATMENT IS: GNCT
1 GNCTANN
2 T60
3 LKOUT

+++ TRAVER: SUCCESSFUL CALL TRACE +++

31.6 Hardware requirements

--

31.7 Limitations and restrictions

31.7.1 Malicious Calls

There is no support for either Malicious Call Trace or Malicious Call Hold.

31.8 Interactions

None.

31.9 Logs (LG)

No logs added/modified. Existing logs are used.

31.10 Data Schema (DS)

31.10.1 New/Modified Tables

New tables are not added. Existing ones are not modified.

31.11 Office Parameters (OP)

No new parameters added.

31.12 Service Orders (SO)

No new parameters added.

31.13 Alarms (AL)

No new parameters added.

31.14 Command Interface (CI)

No new parameters added.

31.15 Operational Measurements (OM)

No new parameters added.

31.16 AMA/Billing Information (AM)

The AMA billing format that is currently supported on the CS2K is being used.

31.17 Software Optionality Control (SOC)

This section does not apply for this feature.

31.18 Glossary

Term	Description
AMA	Automatic Message Accounting
ACM	Address Complete Message
ANC	ANswer Charge
ANM	ANswer Message
ANN	ANswer No Charge
ANS	ANswer message
ANS	ANswer signal
ANU	ANswer Unqualified
BLO	BLOcking signal
BRI	Basic Rate Interface
CALL PROC	CALL PROCeeding message
CAS	Channel Associated Signalling
CCITT	Consultative Committee in International Telephone and Telegraph
CLB	Clear Backward signal
CLF	Calling Line identification with Flash
CLF	CLear Forward signal
CLI	Calling Line Identification
CONN ACK	CONNect ACKnowledge message

CPC	Calling Party Category
DISC	DISConnect message
ETSI	European Telecommunications Standards Institute
FDCP	Flexible Digital CAS Platform
FN	Functional description
GRQ	General Request Message
GSM	General Setup information Message
IAI	Initial Address message with additional Information
IAM	Initial Address Message
IBN	Integrated Business Network
IDL	IDLe message
ISUP	ISDN User Part
MFC	Multi Frequency Compelled
PBX	Private Branch Exchange
R2	Register Signalling Number 2
REL	RELease message
REL COM	RELease COMplete message
RLC	Release Complete message
SAM	Subsequent Address Message
SAO	Subsequent Address message with One digit
SZG	Seize signal

31.19 References

- [1] Flexible Channel Associated Signal Base
- [2] DMS100 Global R2 System Description
- [3] South Korea R2 Signalling Specification (TRS-96-238)
- [4] CCITT Red Book TUP Specifications (Q.721 - Q.724 1984)
- [5] ITU-T ISUP Specifications (Q.763, Q.764, Q.767)
- [6] CCITT R2 Specifications (Q.400 to Q.490)
- [7] ITU-T Recommendation Q.93

32: A00007440 Functional description (FN)

32.1 Feature name

ConnectToResource and PlayAnnouncement during Alert

32.2 Description

This design will extend functionality implemented on the DMS100 MMP SSP platform to accept ConnectToResource (CTR) and PlayAnnouncement (PA) operations from the SCP whilst the SSF FSM is in the Monitoring state and before the call has been answered.

In the current implementation the CTR and PA operations are accepted while the SSF FSM is in the Monitoring state but only after the call has been answered and is in talking state. This feature allow IN controlled announcements to be played to the calling party during alerting phase of a call instead of audible ringing tone. The required functionality will be developed in the ISN08 release.

32.2.1 Message flow examples

Figure 1 CTR, PA during Alerting - Success Path

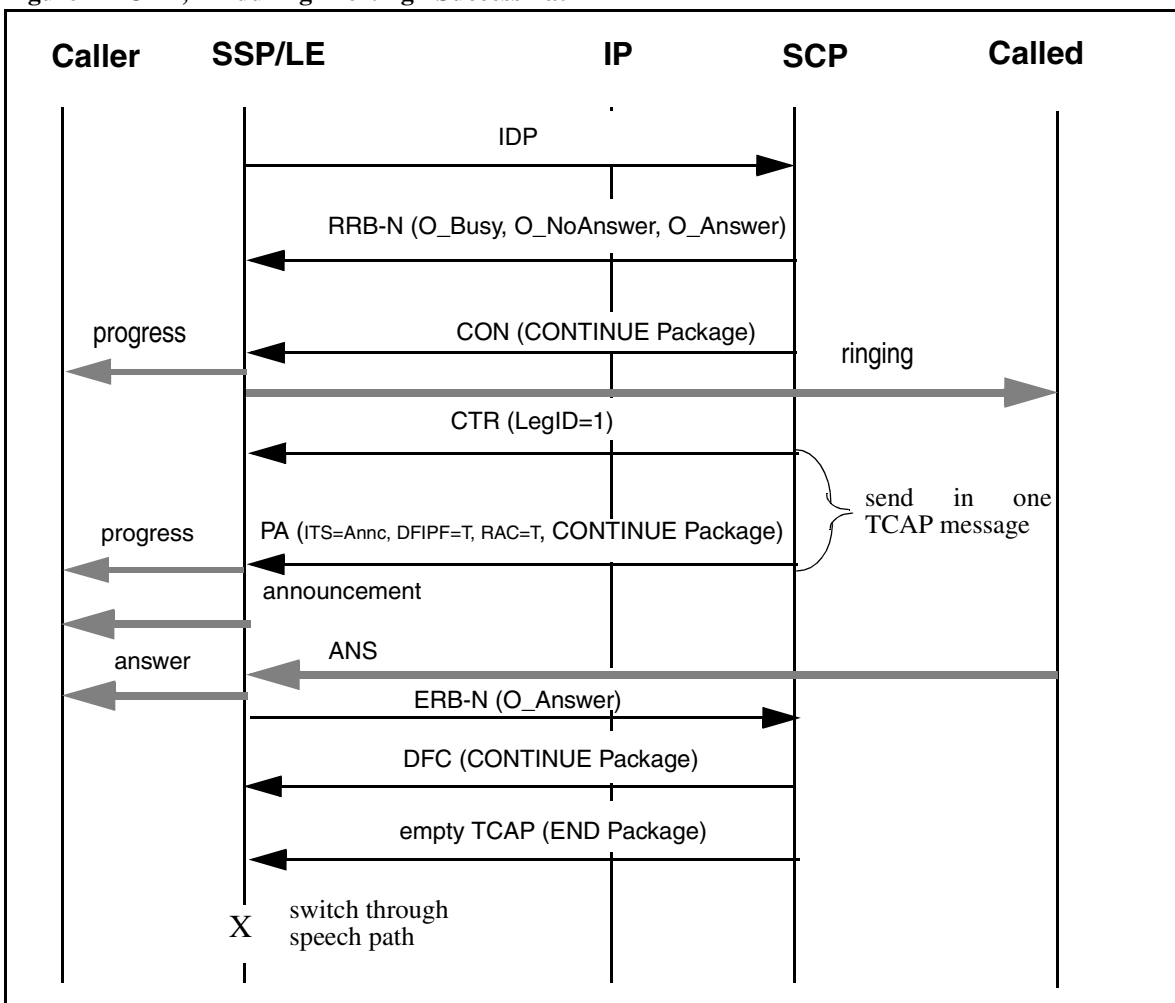


Figure 2 CTR, PA during Alerting - NoAnswer Path

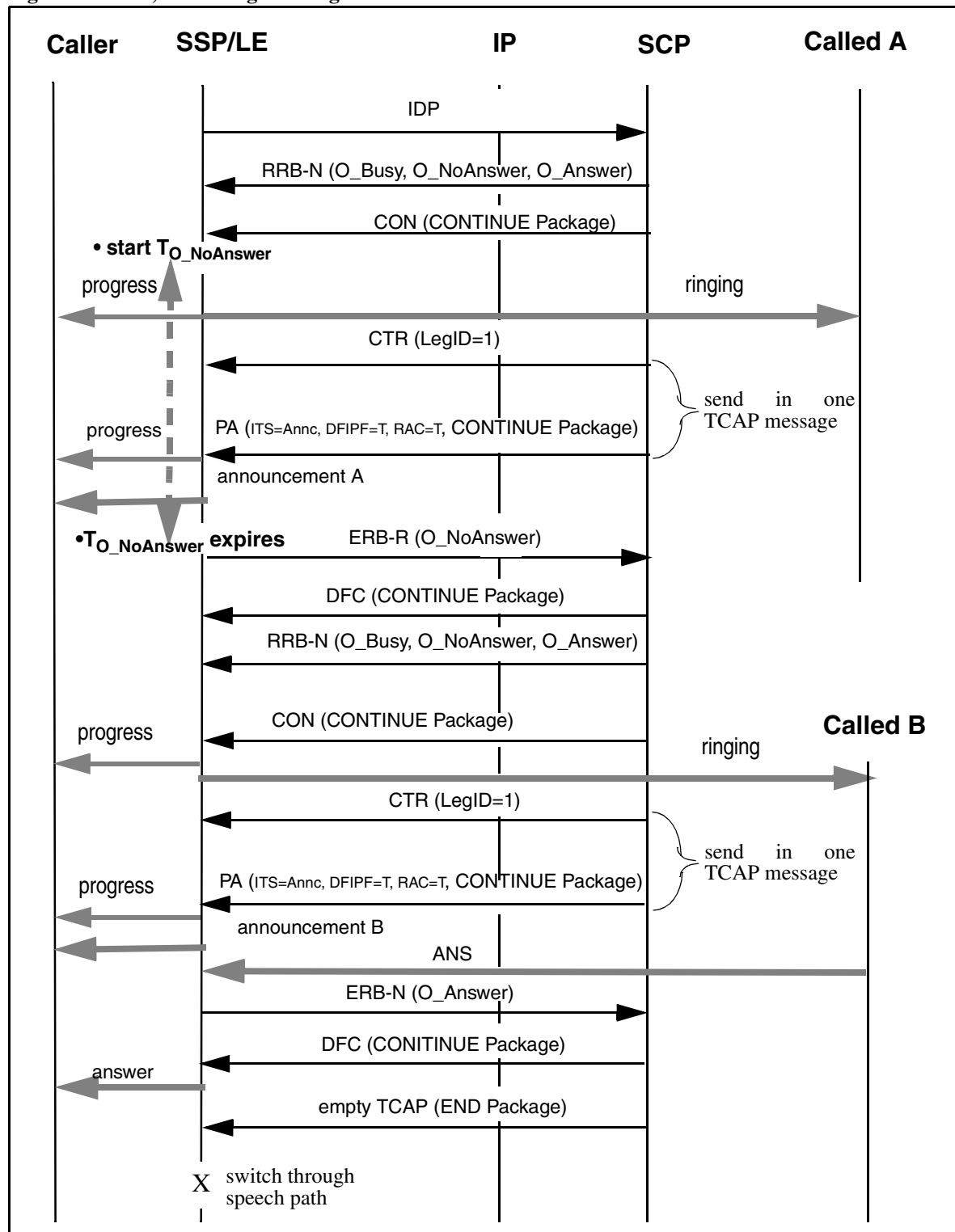
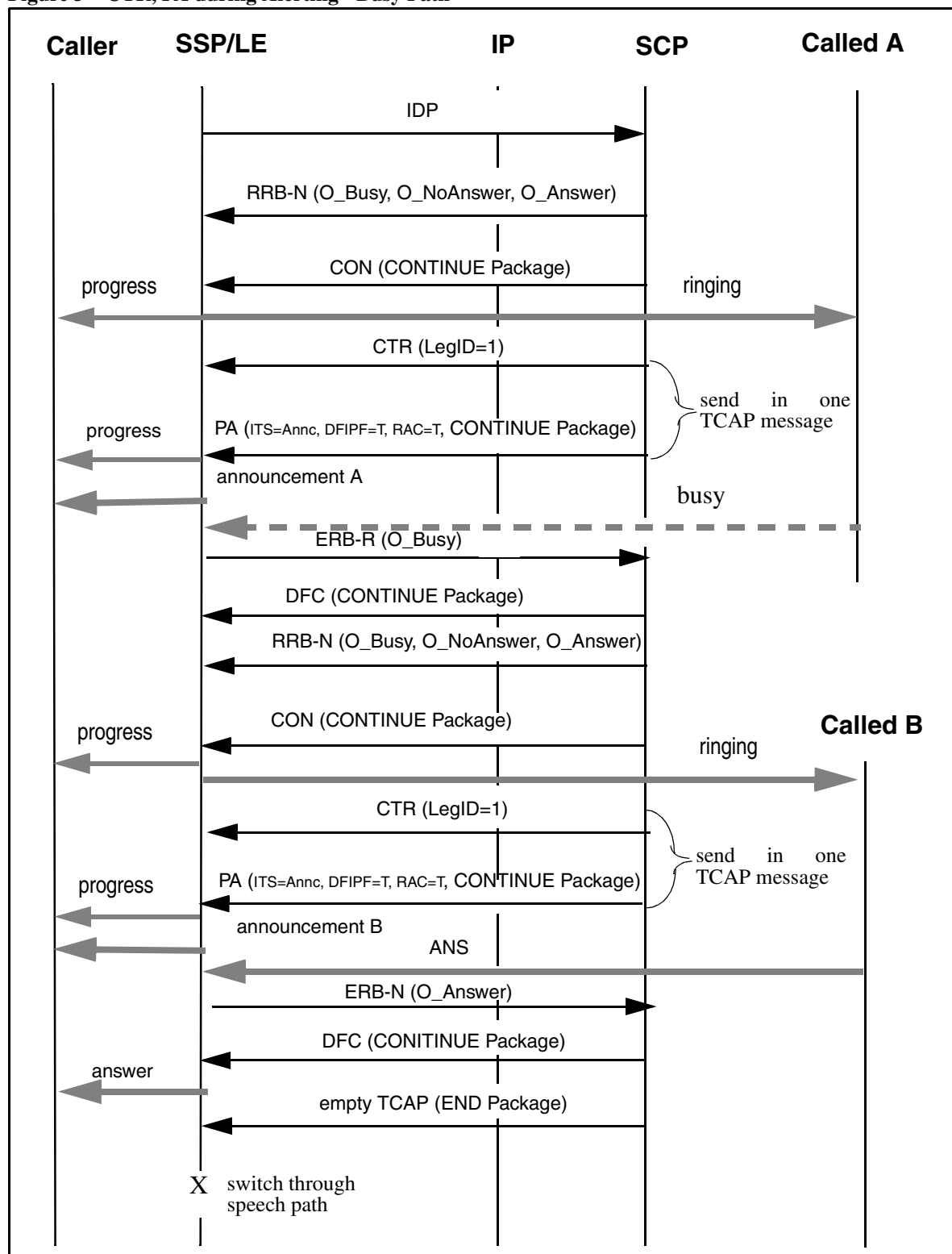
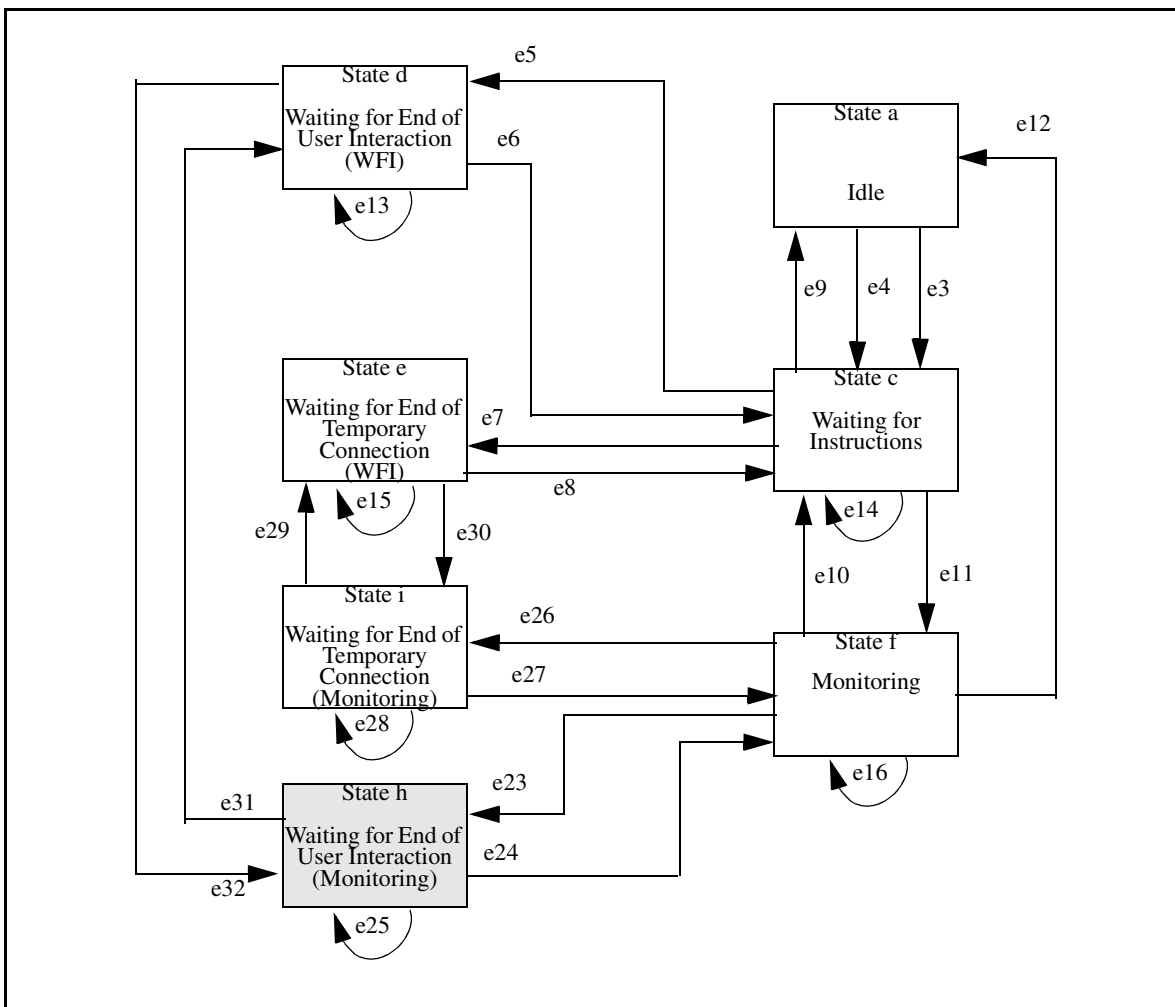


Figure 3 CTR, PA during Alerting - Busy Path



32.2.2 SSF FSM

acc. to ITU Q.1218



32.3 Hardware Requirements or Dependencies

None.

32.4 Software Requirements or Dependencies

This feature is an extension to the following feature: A59009460 - CTR in Monitoring

The code will be sourced in ISN08 (WT21).

Activation with SOC:
Order Code and Name: DSSP0029 - CTR Mon Mode pre Ans
needs DSSP0023 - CTR in Monitor Mode

32.5 Limitations and restrictions

Supported agents:

- Austrian ETSI ISUP V2
- PRI

Only for internal IPs (CTR / PA).

Announcement should be played continuously.

32.6 Interactions

None

32.7 Applicable customer facing sections

None

32.8 Glossary

Table 1

Term	Description
CTR	Connect To Resource
PA	Play Announcement

33: A00007749 Functional description (FN)

33.1 Feature name

MG9000 ABI Support for LGCO, LGCOi

33.2 Description

This feature provides the customer with the ability to host LGCO and LGCOi peripherals (datafilled as PLGCs in table LTCINV) off the ABI DS-512 interface on the MG9000 Gateway. Hosting this type of peripheral is required in the International market for Telstra to allow them to deploy Call Servers within their network.

Note: Only MX77 processor versions of the PLGC are supported in the patched back version of this activity into ISN07. This corresponds to the OGI and OLG PLGC loads which run on the MX77 processor based PLGCs. SX05 based PLGCs (QGI load) are only supported in ISN08 and beyond.

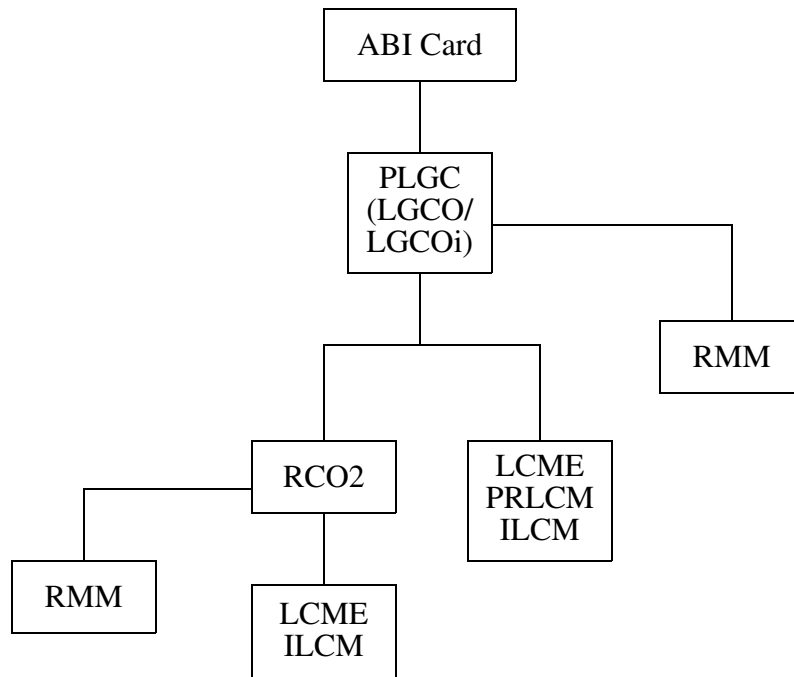
In ISN08 the customer will be able to datafill the EXTDS512 option on in a PLGC tuple in table LTCINV, which is required to support PLGCs on the ABI interface of the MG9000. In this release we will support only a limited set of interworkings in the international market for ABI lines. For example, interworking with native MG9000 lines will not be supported from ABI lines, nor will interworking to GWC hosted CICM lines (although interworking to XPM hosted CICM lines will be allowed as these lines appear as P-phone lines). ISDN BRI is also supported on the LGCOi (and RCO2), but only the TS13 version of BRI, and only a limited service set is allowed (specifically only BRI Data Services are supported for Telstra).

The feature also adds support for hosting of an Remote Maintenance Module (RMM) directly on a PLGC host peripheral. In the past RMMs were only supported on remote type peripherals (ie: RCO2s in the international market), but with this feature support has been added to allow a PLGC (LGCO/LGCOi) to have an RMM directly connected to it via a DS30A interface. This is needed, again for Telstra, to allow for Metallic Line Test access at collapsed office sites where previously there was a DMS-100 and an ENET with an MTM available. With the DMS and ENET/MTM no longer available at the site where the PLGC exists, the RMM serves as the interface for line test functions. Without the RMM it would not be possible to access line test functionality at the, now remote, site.

An issue with the RMM involves the hardware configuration. Specifically, the RMM has in the past always been sold by Nortel as a component of the RSC/RSCS, not as a stand-alone piece of hardware. For connection to a HOST type peripheral the RMM needs to be supported in a separate frame, and new cabling needs to be installed to allow it to be connected to the new host peripheral. This new hardware setup was implemented and documented as part of activity A00001898 - ABI RMM Support in SN07 for the North American market. The same hardware will be used for the international market as well for RMM support on PLGCs.

The following diagram (figure 1) shows the ISN08 configurations supported for Telstra. Note that this is a logical not physical diagram as a PLGC may support more than one of each type of subtending device.

Figure 1 Supported ISN08 ABI Configurations for the International Market



Note: Only single RCO2 configurations are supported in ISN08, not dual RCO2 setups.

33.2.1 Supported Line Class Codes and Features

The following tables lay out the Line Class Codes (LCCs) and features that are supported on the ABI PLGC.

Note: Although the subtending devices are not shown in the following list, they will support all the LCCs applicable for their host peripheral. For

example, an RCO2 subtending an ABI based PLGC will be able to support all the LCCs listed for the PLGC in the table below, assuming that the RCO2 supports that LCC in a legacy environment.

Table 1: ISN08 Supported LCCs for the PLGC

LCC	PLGC Support
1FR	-
1MR	-
2WW	-
CDF	-
CFD	-
EOW	-
ETW	-
IBN	ISN08
ISDNKSET	ISN08
INW	-
M5008	-
M5009	-
M5112	-
M5208	-
M5209	-
M5212	ISN08
M5216	ISN08
M5312	ISN08
M5316	ISN08
OWT	-
PBM	-
PBX	-
PSET	-
RES	-
TWX	-
ZMD	-

LCC	PLGC Support
ZMZPA	-

Note: A “-” in any cell of the above table means that the LCC is not supported for that XPM type. For example, RES is not supported on PLGC.

The following services are supported for the PLGC in SN08:

Table 2: ISN08 Supported Line Services

Service	Analog LCCs (IBN)	P-Phone LCCs (M5212/M5216/M5312/M5316)
Account Codes	Yes	Yes
Authentication Codes	Yes	Yes
Call Waiting	Yes	Yes
Directory Number	Yes	Yes
Call Barring (Network Class of Service)	Yes	Yes
Automatic Call Back (RAG)	Yes	Yes
Call Forward All Calls (CFI)	Yes	Yes
Call Forward Busy (CFB)	Yes	Yes
Call Forward Busy - Block Internal (CBI)	Yes	Yes
Call Forward No Answer (CFD)	Yes	Yes
Permanent Hold (HLD) including Music on Hold	Yes	N/A
Call Park (PRK)	Yes	Yes
Call Pickup Group (CPU)	Yes	Yes
Directed Call Pickup (DCPU)	Yes	Yes
Malicious Call Hold	Yes	Yes
Last Number Redial	Yes	N/A
Speed Call Short (SCS)	Yes	Yes
Tone Dialing (DGT)	Yes	N/A

Table 2: ISN08 Supported Line Services

Service	Analog LCCs (IBN)	P-Phone LCCs (M5212/M5216/ M5312/M5316)
Executive Busy Override	Yes	Yes
Executive Busy Override Exempt	Yes	Yes
Transfer, Hold & 3 Way Conference (CXR)	Yes	Yes
Terminating Line Select	Yes	Yes
Originating Line Select	Yes	Yes
Calling Number Delivery	Yes	Yes
Calling Name Delivery	Yes	Yes
Message Waiting	Yes	Yes
Music On Hold (fixed recording in UAS)	Yes	N/A
Last Number Redial from Set (LNRA)	N/A	Yes
Music on Hold (KSMOH)	N/A	Yes
Automatic Dial	N/A	Yes
Additional Directory Number	N/A	Yes
Multiple Appearance Directory Number (MDN)	N/A	Yes
Intercom Group (GIC)	N/A	Yes
Direct Intercom (ICM)	N/A	Yes
Speed Call Long (SCL)	Yes	Yes
Conference 6 (CNF CO6)	Yes	Yes
Conference - Executive	Yes	Yes
Conference - Preset	Yes	Yes
Key Short Hunt (KSH)	N/A	Yes
Call Forward Universal per Key	N/A	Yes
Camp-On (MBSCAMP)	Yes	Yes

Table 2: ISN08 Supported Line Services

Service	Analog LCCs (IBN)	P-Phone LCCs (M5212/M5216/ M5312/M5316)
Directed Call Park (DCPK)	Yes	Yes
Direct Station Select/Busy Lamp Field (BLF)	N/A	Yes
No Double Connect (NDC)	Yes	N/A
Line Hunt (DLH or MLH) (Circular or Sequential)	Yes	Yes
Privacy Release	Yes	Yes
Suppress	Yes	Yes
Line Overflow to DN (LOD & LOR)	Yes	Yes
Call Forward No Answer from Hunt Group	Yes	Yes
Directory Number Hunt (DNH)	Yes	Yes

Table 3: ISN08 Supported ACD Services

Service	System	Analog LCCs (IBN)	P-Phone LCCs (M5212/ M5216/ M5312/ M5316)
Abandoned Call Clearing	Yes	N/A	N/A
Additional/Second Directory Numbers	N/A	Yes	Yes
Agent Queue	N/A	Yes	Yes
Automatic ACD Not Ready	Yes	N/A	N/A
Automatic Overflow	Yes	N/A	N/A
Call Delay Announcements	Yes	N/A	N/A
Call Queue Slots	Yes	N/A	N/A
Call Processing Control	Yes	N/A	N/A

Table 3: ISN08 Supported ACD Services

Service	System	Analog LCCs (IBN)	P-Phone LCCs (M5212/M5216/M5312/M5316)
Called Name/Number Display (for ACD Directory Numbers)	N/A	Yes	Yes
Distinctive RInging	N/A	Yes	Yes
Overflow of Enqueued Calls to a DN	Yes	N/A	N/A
Priority Promotion	Yes	N/A	N/A
Ring Threshold	Yes	N/A	N/A
Second and Third Delay Announcements	Yes	N/A	N/A
Time Delay Overflow	Yes	N/A	N/A
Night Treatment	Yes	N/A	N/A
Night Recorded Announcement and Forward	Yes	N/A	N/A
Forced Announcement for New and Overflowed Calls	Yes	N/A	N/A
Music on Delay	Yes	N/A	N/A
Emergency Key Backup	N/A	N/A	Yes
Multi-Stage Queue Status	N/A	N/A	Yes
Optional Not Ready Key	N/A	N/A	Yes
Queue to Make Set Busy	Yes	N/A	N/A
Variable Wrap-up	Yes	N/A	N/A
ACD In Calls Key (DN on Key 1)	N/A	N/A	Yes
Make Set Busy/Login (MSB)	N/A	Yes	Yes
ACD Not Ready (ACDNR)	N/A	Yes	Yes
Call/Answer Supervisor (CLSUP)	N/A	N/A	Yes
Call Forcing	Yes	N/A	Yes

Table 3: ISN08 Supported ACD Services

Service	System	Analog LCCs (IBN)	P-Phone LCCs (M5212/ M5216/ M5312/ M5316)
Secondary Directory Number	N/A	Yes	Yes
Answer Agent Key (AAK)	N/A	N/A	Yes
Call Agent Key (CAG)	N/A	N/A	Yes
Control of Night Service Key (NGTSRVCE)	N/A	N/A	Yes
Controlled Interflow Key (CIF)	N/A	N/A	Yes
Forced Agent Availability Key (FAA)	N/A	N/A	Yes
Observe Agent Key (OBS)	N/A	Yes	Yes
Display Queue Status (DQS)	N/A	N/A	Yes
Display Agent Summary (DASK)	N/A	N/A	Yes
Agent Status Lamp (ASL)	N/A	N/A	Yes
Line of Business (LOB)	N/A	N/A	Yes
Display Queue Threshold (DQT)	N/A	N/A	Yes
Uniform Call Distribution	Yes	N/A	N/A
UCD Login Keys	N/A	N/A	Yes

Table 4: ISDN BRI Services Supported in ISN08

Service
3KHz Audio Call
64 Kb/s Unrestricted Data Call
CLI Presentation and Restriction

33.3 Hardware Requirements or Dependencies

33.3.1 RMM Hardware Frame

The RMM will be housed in a MIS frame. This is an existing frametype, but prior to the SN07 activity A00001898 (mentioned above), was not used to house RMM shelves.

33.3.2 RMM Circuit Packs

The following circuits packs will be supported in an RMM in the ABI configuration. The packs are:

- 0X10: Scan Detector
- 2X11: MTU (Mult-Line Test Unit)
- 2X57: Signal Distribution Card
- 2X90: Datafilled as a Montalk or NTT (No Test Trunk)
- 3Z09: MTA (Metallic Test Access)

33.3.3 DS30A Cards and Cables

See the Engineering Information section of this feature for more details than the summary below.

An RMM requires a DS30A interface to its host XPM. If a HOST PLGC does not already contain a DS30A card (6X48 card) it will need to be added before an RMM can be hosted off the PLGC.

33.4 Software Requirements or Dependencies

This activity will be implemented in the ISN08 release, but due to customer requirements will be patched back into the ISN07 release via a feature patch for Telstra.

33.5 Limitations and restrictions

The following restrictions exist on the PLGC External XPM added by this activity:

- PLGC ABI XPMs are only supported for IP Network configurations. Use of PLGCs in ATM AAL1 network configurations are not supported. ATM AAL5 (IP over ATM) networks are supported.
- Special Connections are not supported on any External XPM.
- External XPMs do not support broadcast loading or patching, although they do support parallel loading. Broadcast loading and patching are not supported due to the lack of support for IPMLs between the External XPMs.

- Only the circuits listed in “33.3 Hardware Requirements or Dependencies” on page 473 are supported on an ABI RMM. No effort has been made to prevent the datafill of other circuits packs, but they will not be supported.
- The RMM Selector field in table RMMINV will be set to RMMLTC for PLGCs. This is done because a PLGC is treated exactly the same as LTCs (and are essentially alike from a hardware perspective) in their handling.
- The severing of a connection between the MG9000 and the Call Server, between the ABI XPM (PLGC) and the MG9000, or between the RCO2 and the PLGC will cause the RCO2 to enter into ESA mode. When the connection is restored and the C-side links come back into service, the RCO2 will exit ESA. The RCO2 will perform a warm exit from ESA. ESA is not supported on the ABI PLGCs. Any lines directly on the HOST PLGC will lose service for the duration of the cut, no ESA will be available to those lines. If an RLCM is hosted on the PLGC then the RLCM will drop into ESA (if it is configured to support ESA).
- In ISN08, only offices with office parameter “TYPE_OF_NETWORK” (in table OFCENG) set to “INTERNATNL” are supported for ABI PLGCs. Offices with this office parameter set to “ALAW” are not supported as the version of A-Law speech encoding set by this parameter (All Bit Inversion in the case of ALAW) is not supported on the MG9000 in ISN08.

33.6 Interactions

- The severing of a connection between the MG9000 and the Call Server, between the ABI XPM and the MG9000, or between the RCO2 and the PLGC will cause the RCO2 to enter into ESA mode. When the connection is restored and the C-side links come back into service, the RCO2 will exit ESA. The RCO2 will perform a warm exit from ESA.

33.7 Glossary

Term	Description
New term	Definition

34: A00007793 Functional description (FN)

34.1 Feature name

IN: SCF Id, Correlation Id and QoR Base LNP Support (DACOM)

34.2 Description

The purpose of this activity is to meet the Dacom's requirements with the enhancement in the IN based Number Portability (NP) by the Query on Release (QoR) method, and with the ScfID & CorrelationID parameters handling in the ETC (Establish Temporary Connection) operation.

Also, Dacom specific extension is appended to the operations of InitialDP, CIRP (Call Information Report) and ERBCSM (Event Report BCSM).

The content of the activity are explained in seven parts in this document, as below:

- TDP4 QoR triggering for Dacom. Then extracting requested Extensions parameters (CDN, NPFI) from the INAP Connect Operation and storing them for the outgoing ETSI ISUP V2 IAM message.
- Handling the ScfID & CorrelationID Parameters in the INAP ETC (Establish Temporary Connection) Operation and storing them for the outgoing ETSI ISUP V2 IAM message.
- Datafilling the dacom_ext to the INITDP_EXTENSIONS in the table SERVINFO.
- Changing in the format of miscCallInfo field in the InitDP operation for Dacom.
- Appending the dacom specific extension to the operation of InitialDP.
- Appending the dacom specific extension to the operation of CIRP (Call Information Report).
- Appending the dacom specific extension to the operation of ERBCSM (Event Report BCSM)

Also, the EINTRACE tool is enhanced to capture the new Dacom extension parameters defined for Connect (CDN, NPFI), InitDP, ERBCSM and CIRP operations.

34.2.1 Dacom TDP4 QoR triggering and handling the requested Extensions parameters in Connect for outgoing IAM:

The TDP4 allows IN to be trigger on receipt of an ISUP REL message externally from the network. TDP4 QoR functionality is used in the IN based Number Portability service. QoR allows a call to be routed over ETSI ISUP trunks to the donor exchange. If the called directory number is ported, the donor exchange will release the call by sending ISUP REL cause 14 (QoR: PORTED NUMBER) to the QoR serving exchange. The QoR serving exchange (the originating, or in some case an intermediate exchange) upon receiving that REL 14 will trigger the IN service and a query will be sent to the SCP. The SCP will reply with the new routing number and the QoR serving exchange will route the call to the recipient exchange based on the new routing number provided by the SCP. These are the existing functionalities that this feature is based on.

In this feature, in a call over ETSI ISUP V2 trunk, if the outgoing trunk is datafilled in table ISUP SVC as MARKET KOREA, then the DMS SSP triggers IN (TDP4) according to the following Dacom criteria:

First of all the cause value of the received ETSI ISUP V2 REL message has to be equal to the cause value datafilled in table TRIGGRP.

Then if this cause value is 0x0E (14), diagnostic field is checked. If there is 1 byte diagnostic with value less than 0x10 (16) or there is no diagnostic, TDP4 is triggered. If the received cause value is different from 0x0E (14), TDP4 is triggered regardless of the diagnostic field.

If the outgoing trunk is not datafilled as MARKET KOREA in table ISUP SVC, TDP4 is triggered when the received cause value is the same as the datafilled cause value in table TRIGGRP (default criteria).

Table 1: Criteria required to trigger TDP4

ISUP SVC datafill for OG trunk	TRIGGRP datafill for REL cause	Received ISUP REL cause	Diagnostic field	TDP4 triggering (according to criteria)
MARKET KOREA	14	14	length: 1 byte, value: < 16	Yes (Dacom criteria)
MARKET KOREA	14	14	length: 1 byte, value: >= 16	No (Dacom criteria)
MARKET KOREA	14	14	length > 1 byte	No (Dacom criteria)

Table 1: Criteria required to trigger TDP4

ISUP SVC datafill for OG trunk	TRIGGRP datafill for REL cause	Received ISUP REL cause	Diagnostic field	TDP4 triggering (according to criteria)
MARKET KOREA	14	14	no diagnostic field	Yes (Dacom criteria)
MARKET KOREA	X	X	regardless of diagnostic	Yes (default criteria)
MARKET KOREA	Y	Z	regardless of diagnostic	No (default criteria)
not datafilled	Y	Y	regardless of diagnostic	Yes (default criteria)
not datafilled	Y	Z	regardless of diagnostic	No (default criteria)

X: any valid cause value for TDP4, different from 14.

Y: any valid cause value for TDP4.

Z: any valid cause value for TDP4, different from Y.

Then, the SCP returns the Routing Number (RN) in Destination Routing Address (DRA) parameter. The Called Directory Number (CDN) and Number Portability Forward Information (NPFI) are extracted from the Connect operation as the Dacom Extension parameters. They are stored in the HDB so that they can be put into outgoing ETSI ISUP IAM message by the other activity A00007807 “Base ETSI ISUP V2 support for Dacom IN”.

After TDP4 triggering, the following requirements are ensured for the outgoing Dacom ETSI ISUP V2 IAM message:

- For CDN parameter of outgoing ETSI ISUP V2 IAM:
 - The Directory Number (DN) is extracted from the CDN Extension parameter of INAP Connect and stored in the HDB created by the activity A00007807 “Base ETSI ISUP V2 support for Dacom IN”. While storing this parameter as CDN parameter of IAM, the Nature of Address Indicator (NOA) field is always set to “0000011” (Domestic Number) and Internal Network Number (INN) field is always set to “0”.
- For NPFI parameter of outgoing ETSI ISUP V2 IAM:
 - The NPFI value is extracted from the NPFI extension parameter of INAP Connect operation and stored in the HDB created by the activity

A00007807 “Base ETSI ISUP V2 support for Dacom IN”. NP Status Indicator (NPSI) field of NPFI is expected to be “0011” (NP query has been made, and the called subscriber has been ported) from SCP. However, the value received from SCP is stored as it is.

- For CdPN parameter of outgoing ETSI ISUP V2 IAM:

Receiving of both CDN and NPFI Extension parameters in the Connect operation from SCP means that the SCP returns Routing Number (RN) in the Destination Routing Address (DRA) parameter of Connect operation. In this case, Called Party Number (CdPN) parameter of outgoing ETSI ISUP V2 IAM message functions as RN (Routing Number) received from the SCP.

— In this activity, if both CDN and NPFI extensions are received from connect and put in the outgoing ETSI ISUP V2 IAM successfully, and also this outgoing trunk has been datafilled as MARKET KOREA in table ISUP SVC then the following settings are done in the CdPN parameter of this OG IAM message:

- Nature of Address Indicator (NOA) field is set to “0000110” (RN of the domestic number format),
- Internal Network Number (INN) field is set to “0”.

Otherwise, the NOA and INN values are not modified by this activity*.

Please refer to Table 2 for the CdPN parameter fields NOA and INN in the outgoing ETSI ISUP V2 IAM.

Table 2: NOA and INN settings of CdPN in the outgoing ISUP IAM message

ISUP SVC datafill for Dacom ETSI ISUP V2 trunks	CDN received from SCP and put in the OG IAM	NPFI received from SCP and put in the OG IAM	SSP settings in NOA and INN fields of CdPN of OG IAM.
MARKET KOREA	Yes	Yes	NOA = 6, INN = 0
MARKET KOREA	Yes	No	no setting
MARKET KOREA	No	Yes	no setting
MARKET KOREA	No	No	no setting
not datafilled	regardless of CDN&NPFI	regardless of CDN&NPFI	no setting

* But, CS2K may set the NOA of CdPN according to call class. Please note that this is the already existing and normal behaviour. In other words, this activity is not responsible for this change.

An additional information: The NOA value 01 for CdPN is not supported for ETSI ISUP V2 BASE Variant on CS2K. According to this existing behavior (not related with this activity), CS2K will take down an incoming call with CdPN NOA=01 if there is no ALL_NOA option in Table TRKSGRP.

Datafill requirement:

- To trigger TDP4 for Dacom criteria (please refer to Table 1), the ISUPSVC table is datafilled as MARKET KOREA for Outgoing ETSI ISUP V2 trunk in that call (as example in the first tuples of Figures 1 and 2). Otherwise, TDP4 is triggered when the received cause value is the same as the datafilled cause value in table TRIGGRP.
- When both CDN and NPFI extension parameters are received from SCP and put in the HDB for outgoing ETSI ISUP V2 IAM message, the NOA field is set to “0000110” (RN of the domestic number format) and INN field is set to “0” in the CdPN parameter of that IAM. These settings are done only if the MARKET KOREA is datafilled for Outgoing and Incoming sides of that trunk. However, it is necessary to datafill the ADDRESSING_METHOD SEPERATE_DIRECTORY_NUMBER in table ISUPSVC (as example in the second and third tuples of Figures 1 and 2) to support the NOA value #06 in the IAM message by the activity A00007807 “Base ETSI ISUP V2 support for Dacom IN”.

These ISUPSVC options have been created by the activity A00007807 “Base ETSI ISUP V2 support for Dacom IN” for KOREA market. For detailed information, please refer to the FN and CN sections of that activity.

Figure 1 Example datafill in Table ISUPSVC for DACOM

TABLE: ISUPSVC
KEY SERVICE

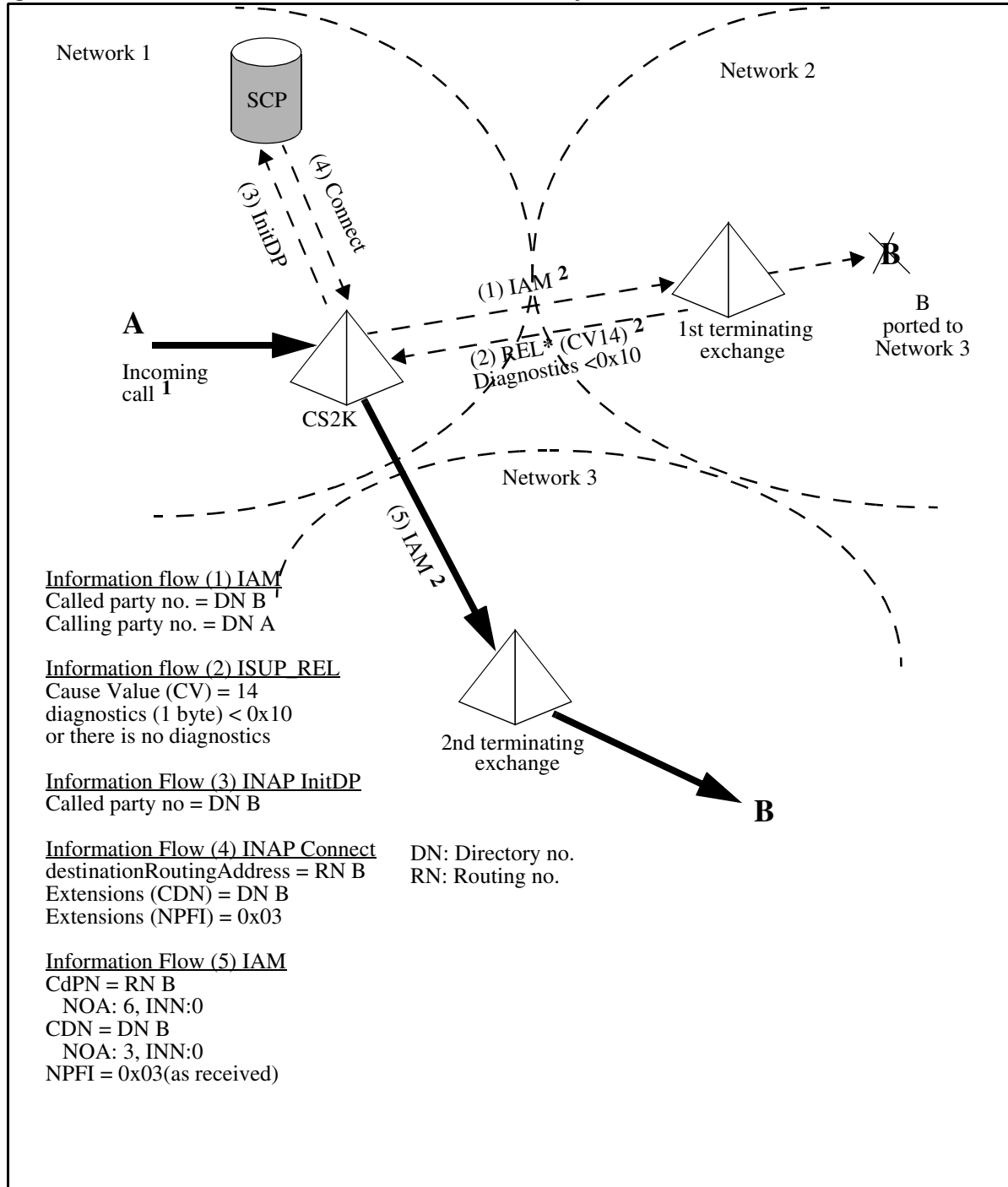
REL14_RCV (MARKET KOREA) \$
FOR_IAM (ADDRESSING_METHOD SEPERATE_DIRECTORY_NUMBER) (MARKET KOREA) \$

Figure 2 Example datafill in Table TRKOPTS for DACOM

TABLE TRKOPTS
OPTKEY OPTINFO

OGISUPV2AB ISUPSVCS ISUPSVCS REL14_RCV
OGISP2AB ISUPSVCS ISUPSVCS FOR_IAM
ICISP2BA ISUPSVCS ISUPSVCS FOR_IAM

- Also the datafills for TDP4 triggering and IN based QoR Number Portability are necessary to work this feature. Those datafills have already been present. Please refer to the Section 2.3. “Background Information”.

Figure 3 Functional behavior of IN Number Portability QoR Method

1 For the incoming call, supported interworkings are Line (V5.2, Cable MTA, IAD IBN line types), Base ETSI ISUP V2, ETSI PRI, Korea R2, H.323 “trunks” (defined as QSIG trunks in CS2000 table data-fill), SIP trunk connections to MCS5200 endpoints.

2 The all trunks on which REL 14 received and OG IAM is send after routing with the CDN and NPFI are Dacom BASE ETSI ISUP Version2 trunks.

* REL message with CauseValue=14 and diagnostic<16 can never be received after answer in Dacom.

The ASN.1 encoding for Dacom Extensions in Connect for Number Portability can be seen in the Figure 4.

Figure 4 ASN.1 encoding for Dacom Extensions in Connect for NP (Number Portability)

```

ExtensionField ::= SEQUENCE {
    type          INTEGER, -- shall identify the value of an EXTENSION type
    criticality    ENUMERATED {
        ignore (0),
        abort (1)
    } DEFAULT ignore,
    value          [1] ANY DEFINED BY type
}

CalledDirectoryNumber ::= OCTET STRING (SIZE (minCalledDirectoryNumberLength..
                                         maxCalledDirectoryNumberLength))

    ,where minCalledDirectoryNumberLength is 2 and maxCalledDirectoryNumberLength is 17.

NumberPortabilityForwardIndicator ::= OCTET STRING (SIZE(1))
    
```

Figure 5 Definition of the Connect Extensions (CDN)

field name	field value	Description
type	202	Integer
criticality	ignore(0)	In case of an extension field type that has not defined in the SSP coming, ignore it.
value	CDN Value	Called Directory Number

Figure 6 Definition of the Connect Extensions (NPFI)

field name	field value	Description
type	201	Integer
criticality	ignore(0)	In case of an extension field type that has not defined in the SSP coming, ignore it.
value	NPFI Value	Number Portability Forward Indicator

According to the Dacom requirement, the length of the CDN and NPFI parameters are given in the following table:

The length of the new additional optional parameters for Dacom

Parameter	length (octets)
Called Directory Number (CDN)	2-17
Number Portability Forward Information (NPFI)	1-1

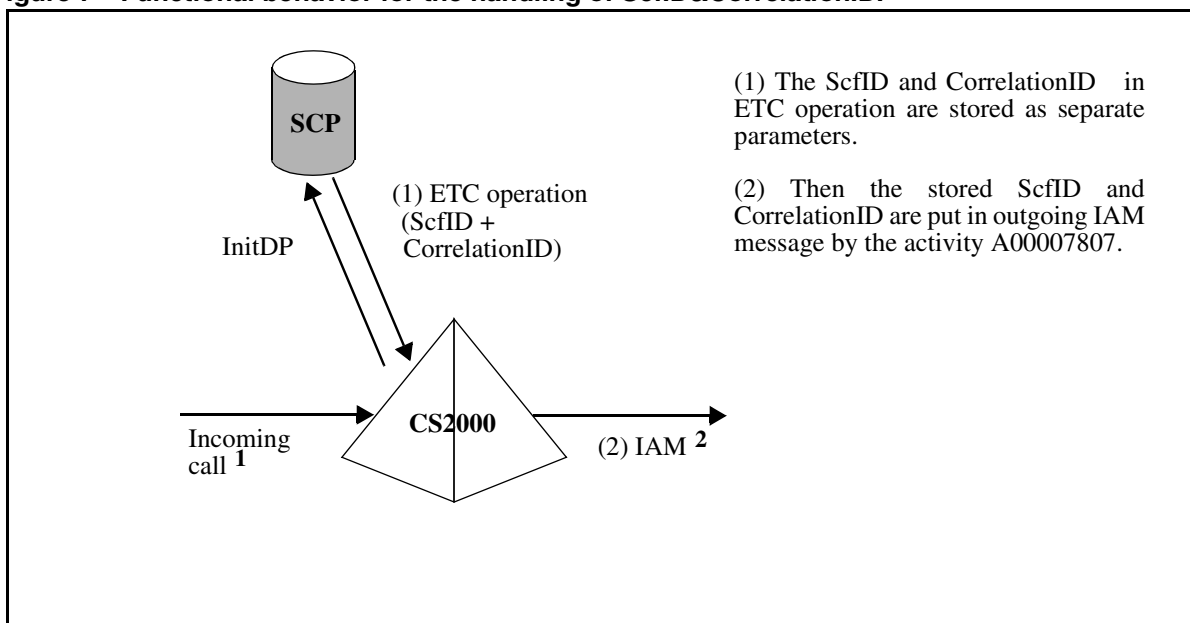
35.2.2 ScfID & CorrelationID Parameters handling in INAP ETC (Establish Temporary Connection) Operation:

This feature also handles the ScfID and CorrelationID parameters sent from SCP to CS2000 in the Establish Temporary Connection (ETC) operation to store them for using in the outgoing Dacom ETSI ISUP V2 IAM message.

The ETC operation is sent by the SCP to the SSP to set up a connection between an external IP and the SSP for the purposes of user interaction. It contains information which is used to correlate the SCP's request to the SSP for connection to an external IP with the responses received by the SCP from the external IP. This information is called the correlationID. ETC operation also contains the ScfID parameter that indicates the SCP to which service assisting procedure is delivered during this connection.

In this activity, the ScfID and CorrelationID are handled as the optional and separate parameters (i.e, not embedded in any other parameter) in the ETC operation and stored so that they can be used in the outgoing ETSI ISUP V2 IAM message by the other activity A00007807 "Base ETSI ISUP V2 support for Dacom IN". Please refer to the functional behavior diagram given in the Figure 7.

Figure 7 Functional behavior for the handling of ScfID&CorrelationID.



- 1 For the incoming call, supported interworkings are Line (V5.2, Cable MTA, IAD IBN line types), Base ETSI ISUP V2, ETSI PRI, Korea R2, H.323 “trunks” (defined as QSIG trunks in CS2000 table data-fill), SIP trunk connections to MCS5200 endpoints.
- 2 The trunk on which OG IAM is send with the ScfID and CorrelationID are BASE ETSI ISUP Version2 trunk.

According to Dacom requirement, CorrelationID should be a separate parameter. This is provided in this feature with a new datafill in the table SERVINFO.

So, a new suboption CORRELATIONID_TRANSPORT is added to the existing SRF_INFO option of table SERVINFO. This suboption is set to the IN_CRID value to handle the CorrelationID as a separate parameter for Dacom, as shown in Figure 8.

This datafill provides the Correlation_ID transport as a separate parameter only for outgoing ETSI ISUP V2 IAM message. Please refer to the CN section of this activity.

Figure 8 Example datafill for the new DACOM CorrelationID option in table SERVINFO

```
TABLE: SERVINFO
SERVIDX OPTION
-----
99
(SRF_INFO $ (CORRELATIONID_TRANSPORT IN_CRID) $) $
```

The new SERVINFO optionality is required for only CorrelationID not for ScfID. Because for the ScfID from ETC, there is no an existing default mapping such as the CorrelationID. So, it can be mapped to the separate ETSI ScfID parameter without needing any table control for Dacom.

The ASN.1 encoding for Dacom ETC operation can be seen in the Figure 9:

Figure 9 ASN.1 encoding for Dacom ETC operation

```

A.1. Operation
EstablishTemporaryConnection ::= OPERATION {
  ARGUMENT  EstablishTemporaryConnectionArg
  ERRORS    { ETCFailed,
              MissingParameter,
              SystemFailure,
              TaskRefused,
              UnexpectedComponentSequence,
              UnexpectedDataValue,
              UnexpectedParameter }
}

A.2. Argument data type
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,
  carrier [5]                      Carrier OPTIONAL,
  serviceInteractionIndicators[30] ServiceInteractionIndicators OPTIONAL
-- ...
}

ScfID:= OCTET STRING (SIZE (minScfIDLength.. maxScfIDLength))
CorrelationID:= OCTET STRING (SIZE (minDigitsLength.. maxDigitsLength))

where the minScfIDLength is 1 byte,
      maxScfIDLength is 4 byte,
      minDigitsLength is 2 byte
      maxDigitsLength is 13 byte

```

According to the Dacom spec, the required length of the ScfID and CorrelationID optional parameters are given in the following tables respectively.

SCF ID parameter length required for Dacom

Minimum length	Maximum length
1 byte	4 bytes

Correlation ID parameter length required for Dacom

Minimum length	Maximum length
2 bytes	13 bytes

In the SSP, according to the existing functionality, the acceptable limits of the both ScfID and CorrelationID lengths have already been defined as 1 to 16 bytes. So, the parameters received from SCP with the lengths greater than 16 bytes can not be accepted by SSP. Also, for CorrelationID parameter, only BCD defined values are supported.

However, in the activity A00007807 “Base ETSI ISUP V2 support for Dacom IN”, the lengths of the HDB that is created to store these parameters for outgoing IAM, are given in the following tables.

HDB length for ScfID in the feature A00007807

Minimum length	Maximum length
1 byte	20 bytes

HDB length for Correlation ID in the feature A00007807

Minimum length	Maximum length
2 bytes	13 bytes

Note: According to these definitions in the A00007807, the ScfID can be tandemed successfully with length of 1 to 20 bytes. But it will not be greater than 16 bytes because the max acceptable length of the received ScfID has already been restricted with 16 bytes in the SSP.

As a result, the real supported ScfID and CorrelationID lengths in this activity can be given as below:

SCF ID parameter length supported in this feature

Minimum length	Maximum length
1 byte	16 bytes

Correlation ID parameter length supported in this feature

Minimum length	Maximum length
2 bytes	13 bytes

Note: CorrelationID parameter value can not include non-BCD characters.

35.2.3 Datafilling the dacom_ext to the INITDP_EXTENSIONS in the table SERVINFO

To append the dacom specific extension to the operations of InitialDP, CIRP (Call Information Report) and ERBCSM (Event Report BCSM), the new sub option called DACOM_EXT is defined under the option of INITDP_EXTENSIONS in table SERVINFO. This sub-option must be datafilled for DACOM (Korea market). This option is used to understand whether the market is Korea or not.

Figure 10 Example datafill for the new DACOM_EXT sub-option in table SERVINFO

```
TABLE: SERVINFO
SERVIDX OPTION
-----
99
( INITDP_EXTENSIONS (DACOM_EXT) $) $
```

35.2.4 Changing in the format of miscCallInfo field in the InitDP operation for Dacom

When sending InitDP operation, if the dacom_ext was datafilled in the service key in the table SERVINFO which this call use, the format of the field of miscCallInfo in InitDP operation is changed. The information of SEQUENCE in miscCallInfo type is removed. Please look at Figure 11 on page 488 for detail information.

Note: MISC_CALL_INFO information is attached to the InitDP when MCI option is datafilled under the sub-option INIT_PARMS in table SERVINFO.

Figure 11 ASN.1 encoding for MiscCallInfo in InitDP operation

```
InitDPArg ::= SEQUENCE {
```

```
    .....
    misCallInfo    [11] MiscCallInfo OPTIONAL,
    .....
```

```
}
```

When the dacom_ext was not datafilled in table SERVINFO, MiscCallInfo is shown as follow

Symbolic:

```
-----
MiscCallInfo ::= SEQUENCE {
    MessageType [0] ENUMERATED {
        request(0),
        notification(1)
    },
}
```

Hex:

```
-----
#AB
#05
    #30
    #03
    #80 #01 The value of Message Type
```

If the dacom_ext was datafilled in table SERVINFO, MiscCallInfo is changed as follow

Symbolic:

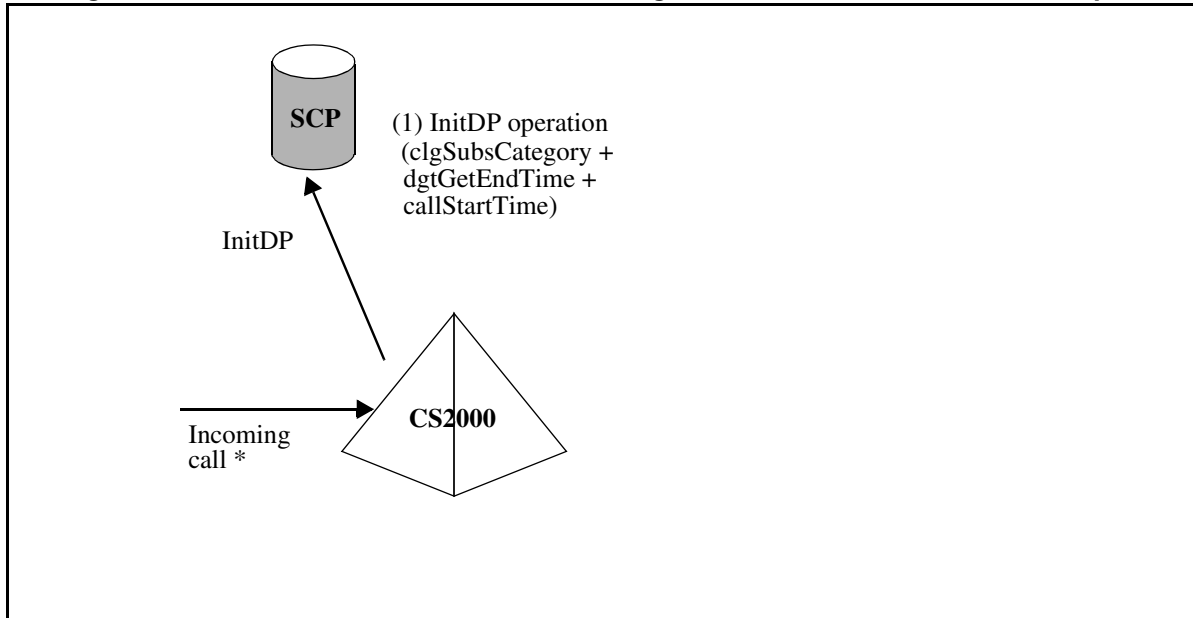
```
-----
MiscCallInfo ::= {
    MessageType [0] ENUMERATED {
        request(0),
        notification(1)
    },
}
```

Hex:

```
-----
#AB
#03
    #80 #01 The value of Message Type
```

35.2.5 Appending the dacom specific extension to the operation of InitialDP

When IN triggers in the call, it is checked that dacom_ext was datafilled in the service key in the table SERVINFO which this call use. If so, dacom specific extension is appended to the operation of InitialDP. Please look at the Figure 12 on page 489, Table 3 on page 489, Table 4 on page 489, Figure 13 on page 490 for detail information about the fields under the dacom extension of InitDP operation.

Figure 12 Functional behavior for the handling of dacom extension in InitialDP operation.**Table 3: Definition of the Dacom Extension in InitialDP operation (ExtIDPCdrType)**

field name	field value	Description
type	61	Integer
criticality	ignore(0)	In case of an extension field type that has not defined in the SSP coming, ignore it.
value	clgSubsCategory	calling subscriber category value: 1 - payphone, 0 - others
	dgtGetEndTime	digit get end time YYMMDD hh:mm:ss.msc
	callStartTime	SSP trigger time YYMMDD hh:mm:ss.msc

Table 4: The length of the new additional optional parameters for Dacom

Parameter	length (octets)
Calling Subscriber Category (clgSubsCategory)	1
Digit Get End Time (dgtGetEndTime)	7
SSP trigger time (callStartTime)	7

Note:

- clgSubsCategory is set to 0, everytime.

- DigitGetEndTime and CallStartTime is set to the same value (IN triggering time).

Figure 13 ASN.1 encoding for Dacom Extensions in InitDP

```

ExtensionField ::= SEQUENCE {
    type          INTEGER, -- shall identify the value of an EXTENSION type
    criticality    ENUMERATED {
        ignore (0),
        abort (1)
    } DEFAULT ignore,
    value         [1] ANY DEFINED BY type
}

ExtIDPCdrType ::= SEQUENCE {

    clgSubsCategory    [1] CallingSubsCategory
    dgGetEndTime       [8] DateandTimewithMs
    callStartTime      [9] DateandTimewithMs

}

CallingSubsCategory ::= OCTET STRING ( SIZE (1))
DateandTimewithMs   ::= OCTET STRING ( SIZE (7))

DateandTimewithMs is coded as YYMMDDHHMMSS.MSS with each digit coded BCD. The first octet contains YY and the remaining items are sequenced following.

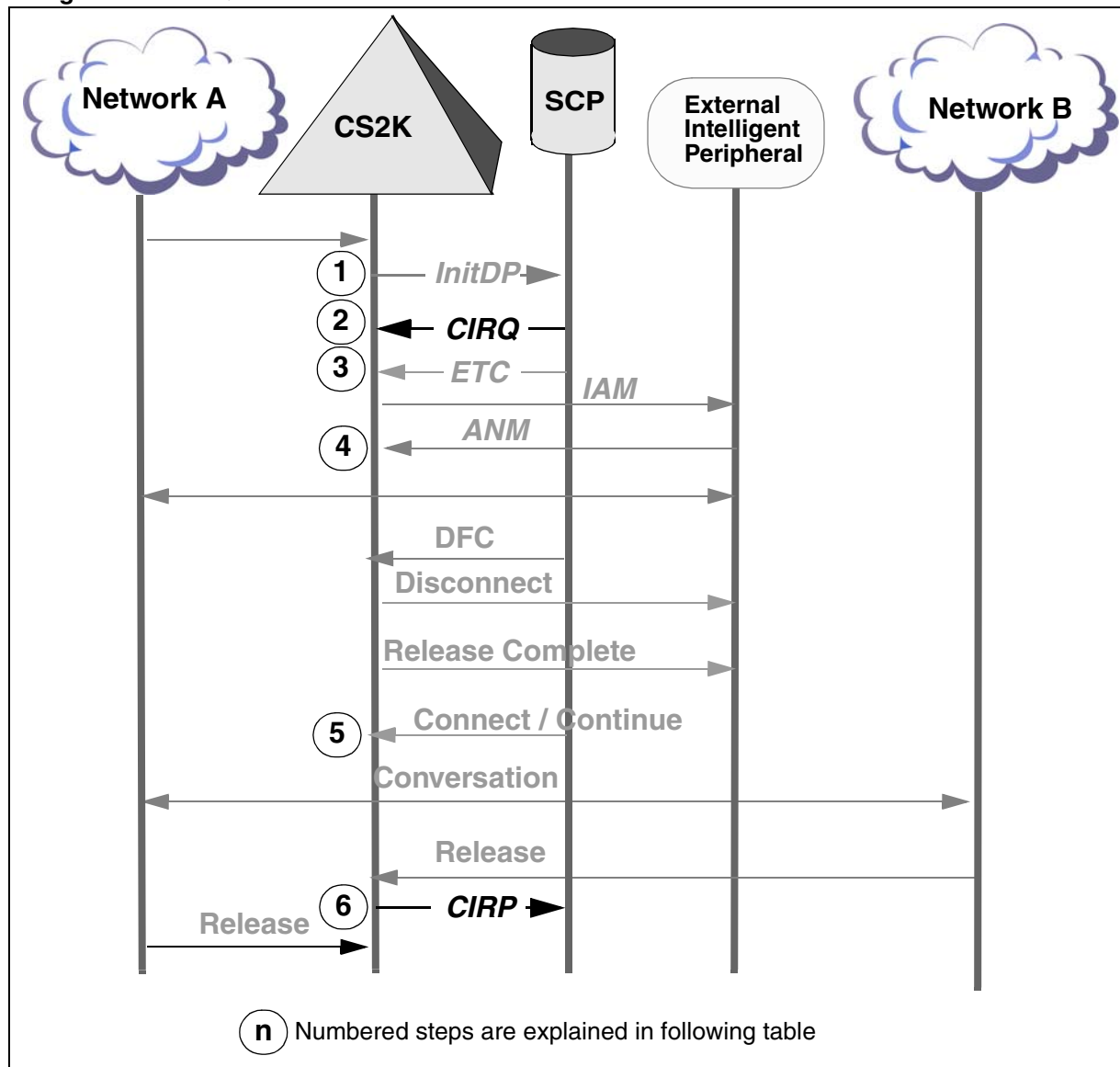
For Example, 2004 September 27th, 13:12:48.30 would be encoded as
#40 #90 #72 #31 #21 #84 #03

```

35.2.6 Appending the dacom specific extension to the operation of CIRP (Call Information Report)

When IN triggers in the call, if CIRQ (Call Information Request) operation is received from SCP, CIRP operation is sent to SCP when the call is released. If the dacom_ext was datafilled in the service key in this table SERVINFO which this call use, the dacom specific extension is appended to the operation of CIRP (Call Information Report). Please look at Figure 14 on page 491, Table 5 on page 492, Table 6 on page 492 and Figure 15 on page 493 for detail information.

Figure 14 CIRQ & CIRP Scenario



Step	Explanation
1	Incoming call triggers as an IN call. InitDP is sent to SCF.
2	The SCF sends a CIRQ operation to the SSF to request the some informations about the call.
3	The SCF sends a ETC operation to the SSF to connect to an external IP. After this operation, SSF and external IP talks to together.

Step	Explanation
4	external IP sends ANM to SSF and the originator of call is connected to the external IP. Then, SCF sends DFC(Disconnect Forward Connection) to SSF and the connection between SSF and external IP is disconnected. The time which ANM is received from external IP is used as rscConnectTime in the dacom extension of CIRP operation.
5	SCF sends a Connect or Continue operation to SSF to connect the terminating agent to the call. The time which the operation of Connect/Continue is received is used as outgoing trunk seizure time in the dacom extension of CIRP operation.
6	Once the call is released, the SSF sends a CIRP operation which contains the dacom specific informations to the SCF.

Table 5: Definition of the Dacom Extension in CIRP operation (ExtCIRpCdrType)

field name	field value	Description
type	62	Integer
criticality	ignore(0)	In case of an extension field type that has not defined in the SSP coming, ignore it.
value	outTrunkSeizureTime	Out-going trunk seizure time YYMMDD hh:mm:ss.msc
	rscConnectTime	resource connect time YYMMDD hh:mm:ss.msc This parameter defines the IP -Connection Time

Table 6: The length of the new additional optional parameters for Dacom

Parameter	length (octets)
outgoing Trunk Seizure Time (outTrunkSeizureTime)	7
Resource Connect Time (rscConnectTime)	7

Note:

The outTrunkSeizureTime and rscConnectTime are optional fields in the dacom extension. These fields are not put into the dacom extension in the following scenarios.

- If ETC operation is not received, the field of rscConnectTime is not put into the dacom extension in CIRP operation.
- ETC operation is received but If the connection is not established with external IP, the field of rscConnectTime is not put into the dacom extension in CIRP operation.

- If the terminator is a line subscriber in the same exchange, outTrunkSeizureTime field is not put into the dacom extension in the CIRP.

If Outgoing trunk seizure time and resource connect time is not available in the call, the dacom extension is not appended to the CIRP operation.

Figure 15 ASN.1 encoding for Dacom Extensions in CIRP (Call Information Report)

```

ExtensionField ::= SEQUENCE {
    type          INTEGER, -- shall identify the value of an EXTENSION type
    criticality    ENUMERATED {
        ignore (0),
        abort (1)
    } DEFAULT ignore,
    value         [1] ANY DEFINED BY type
}

ExtCIRpCdrType ::= SEQUENCE {
    outTrunkSeizureTime [1] DateandTimewithMs OPTIONAL,
    rscConnectTime      [2] DateandTimewithMs OPTIONAL
}

DateandTimewithMs ::= OCTET STRING ( SIZE (7))

DateandTimewithMs is coded as YYMMDDHHMMSS.MSS with each digit coded BCD. The first octet contains YY and the remaining items are sequenced following.

For Example, 2004 September 27th, 13:12:48.30 would be encoded as
    #40 #90 #72 #31 #21 #84 #03

```

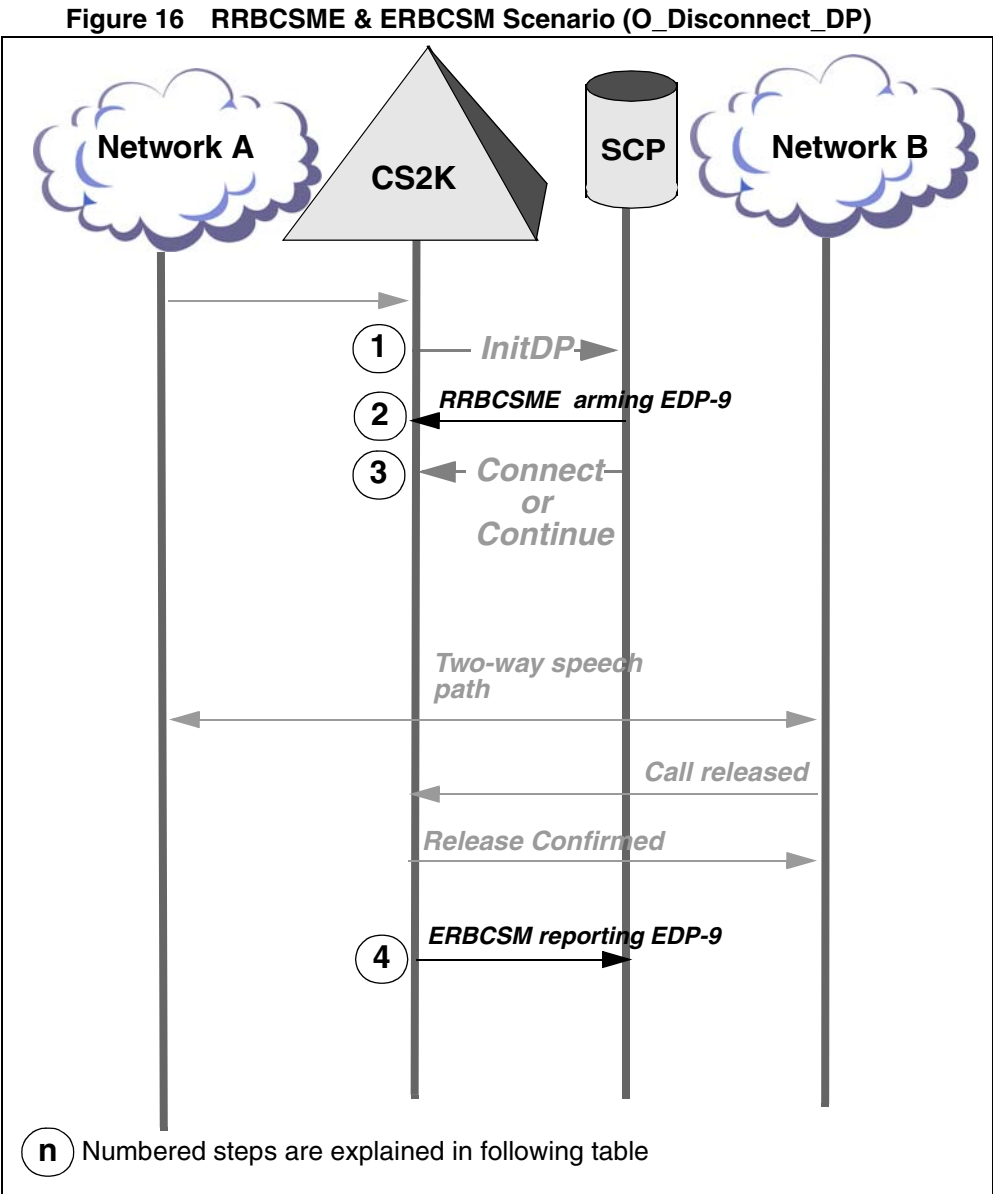
35.2.7 Appending the dacom specific extension to the operation of ERBCSM (Event Report BCSM).

When IN triggers in the call, if RRBCSME arming EDP-9 is received from SCP, ERBCSM is sent to SCP to report that the call is released during the call disconnection. If the dacom_ext was datafilled in the service key in this table SERVINFO which this call use, the dacom specific extension is appended to the operation of ERBCSM (Event Report BCSM).

EDP-9 can be armed to detect when either the originating or terminating leg of a call is released. The default is to arm on the passive leg (leg 2). To arm the call on the controlling (leg 1), a leg id parameter of 1 must be provided in the RRBCSME operation.

If no leg id parameter is included, the option EDP9_OPT in table SERVINFO specifies which leg is armed. If the option specifies leg 1, leg 1 is armed; if the option is not specified, the lowest passive leg is armed.

The dacom specific extension is only appended when SSP send ERBCSM operation for O_Disconnect_DP (eventTypeBCSM 9). Please look at Figure 16 on page 494, Table 7 on page 495, Table 8 on page 495 and Figure on page 496 for detail information about the fields under the dacom extension of ERBCSM operation.



Step	Explanation
1	Incoming call triggers as an IN call. InitDP is sent to SCF.

Step	Explanation
2	The SCF sends a RRBCSME operation to the SSF to arm EDP-9 as an EDP-R on the passive call leg (to report the call disconnection with ERBCSM operation to SCF) and then another messages are done between SSF and Network B and the call is established between Network A and Network B.
3	The SCF sends Connect or Continue operation to SSF and then call setup continues.
4	Once the call is released, the SSF sends an ERBCSM operation. If the dacom_ext is datafilled for this call in the table SERVINFO, the dacom extension is appended to the operation of ERBCSM. This dacom extension holds the two informations (the IN trigger time (time to send InitDP operation) as callStartTime and EDP-9 trigger time (time to send ERBCSM) as clgRecoveryTime).

Table 7: Definition of the Dacom Extension in ERBCSM operation (ExtEvtCdrType)

field name	field value	Description
type	63	Integer
criticality	ignore(0)	In case of an extension field type that has not defined in the SSP coming, ignore it.
value	callStartTime	IN trigger time YYMMDD hh:mm:ss.msc
	clgRecoveryTime	The time of O_Disconnect_DP YYMMDD hh:mm:ss.msc

Table 8: The length of the new additional optional parameters for Dacom

Parameter	length (octets)
IN Trigger Time (callStartTime)	7
The time of O_Disconnect_DP	7

Note:

Also, the dacom extension is appended to the ERBCSM operation for O_Disconnect generated because originator releases the call.

ASN.1 encoding for Dacom E

ExtensionField ::= SEQUENCE {
 type INTEGER, -- shall identify the value of an EXTENSION type
 criticality ENUMERATED {
 ignore (0),
 abort (1)
 } DEFAULT ignore,
 value [1] ANY DEFINED BY type
}

ExtEvtCdrType ::= SEQUENCE {

 callStartTime [0] DateandTimewithMs
 clgRecoveryTime [1] DateandTimewithMs

}

CallingSubsCategory ::= OCTET STRING (SIZE (1))
DateandTimewithMs ::= OCTET STRING (SIZE (7))

DateandTimewithMs is coded as YYMMDDHHMMSS.MSS with each digit coded BCD. The first octet contains YY and the remaining items are sequenced following.

*For Example, 2004 September 27th, 13:12:48.30 would be encoded as
#40 #90 #72 #31 #21 #84 #03*

35.3 Background Information

35.3.1 Configuration for TDP4

The criteria for triggering TDP-4 is based on the cause value received in the ISUP message. The release cause value required to trigger TDP-4 is specified in the criteria type CAUSE in table TRIGGRP. The CAUSE criteria can only be datafilled against NETBUSY triggers. Criteria matching will not be performed on digits at TDP-4, therefore an INFONAME is datafilled in table TRIGINFO before using the CAUSE criteria.

Figure 17 Example datafill SERVINFO

SERVIDX OPTION

1111
(INITDP_PARMS (SERVKEY) (CDPA) (CPC) (EVENT_TYPE) (CAUSE) \$)
(DIGIT_COLLECTION_INFO (FULL_CDPA) \$)
(EDPS_INFO (EXPLICIT) \$) (CS1R (CONTINUE) (CWA) \$) \$

Figure 18 Example datafill TRIGINFO

KEY ACTION OPTIONS

MDCKEY1 EVENT TCAP INAPV8 TCPIP 1 (SERVKEY 1111) (SERVINFO_INDEX 1111) \$

Figure 19 Example datafill TRIGGRP

```

KEY TRIGDATA
-----
          ETSIGRP NETBUSY
(GENTRIG ( CAUSE CSE_14) $ MDCKEY1)$

```

The following CAUSE values are supported (Note that unsupported values may still be datafilled however they may not trigger):

1-5, 8, 9, 14, 17-22, 27-29, 34, 38, 41-44, 46, 47, 50, 53, 55, 57, 58, 62, 63, 65, 69, 70, 79, 87, 88, 90, 91, 95, 97, 99, 102, 103, 110, 111, 126.

The criteria ASSIGNED is also valid at TDP4. In this case, all calls in which the originating trunk/line is subscribed to the TDP4 group will trigger at TDP4 when released.

If the CAUSE option is present within the INITDP_PARMS option in table SERVINFORM, the cause value used to trigger at TDP-4 is sent to the SCP in the InitDP.

Figure 20 Example datafill SERVINFORM

```

SERVIDX                                     OPTION
-----
4441      (INITDP_PARMS ( SERVKEY) (CDPA) (CPC) (EVENT_TYPE) (CAUSE) $)
          (DIGIT_COLLECTION_INFO ( FULL_CDPA ) $)
          (EDPS_INFO ( EXPLICIT ) $) (CS1R (CONTINUE) (CWA) $)$

```

In addition to the criteria matching, TDP-4 triggering is controlled on a per switch basis via the office parm WTIN_TDP4_ACTIVE in table OFCENG. The default value for this parm is FALSE, but it must be set to TRUE for triggering.

Figure 21 Example datafill OFCENG

```

PARMNAME          PARMVAL
-----
WTIN_TDP4_ACTIVE  Y

```

For trunk originations the TDP-4 trigger criteria needs to be specified in table TRIGGRP and the incoming trunk(s) subscribed to the trigger group, either on a per trunk basis in table TRKAIN or on an office wide basis with the AIN_OFFICE_TRIGGRP office parameter in table OFCVAR.

Figure 22 Example datafill TRIGGRP

KEY	TRIGDATA
TDP4GRP NETBUSY	(GENTRIG (CAUSE CSE_14) \$ MDCKEY1)\$

Figure 23 Example datafill TRKAIN

GRPKEY	AINGRP	AININFO
K1S5020EI2B	TDP4GRP	

Figure 24 Example datafill OFCVAR

PARMNAME	PARMVAL
AIN_OFFICE_TRIGGRP	ETSIGRP

For line originations the AIN line option needs to be added via SERVORD and WTIN_LINE_TRIGGERING_ACTIVE office parameter in table OFCENG should be set to Y.

Figure 25 Example Line datafill

>qdn 8226035	

DN:	8226035
TYPE:	SINGLE PARTY LINE
SNPA:	141 SIG: DT LNATTIDX: N/A
LINE EQUIPMENT NUMBER:	LG 01 2 00 35
LINE CLASS CODE:	IBN
IBN TYPE:	STATION
CUSTGRP:	CSLINES SUBGRP: 0 NCOS: 0
CARDCODE:	GWLPOT GND: N PADGRP: PKNIL BNV: NL MNO: N
PM NODE NUMBER :	72
PM TERMINAL NUMBER :	36
OPTIONS:	
LNR DGT	AIN TDP4GRP

Figure 26 Example datafill OFCENG

PARMNAME	PARMVAL
WTIN_LINE_TRIGGERING_ACTIVE	Y

35.3.2 TRAVER support for TDP4

The TRAVER tool can be used to verify TDP-4 functionality. If a TDP4 trigger is detected the user is prompted to input a cause value, this is then checked against the datafilled criteria.

Figure 27 Example TRAVER using CAUSE triggering at TDP-4

```

>traver 1 8226034 743012345 b
TABLE IBNLINES
LG 01 2 00 34 0 DT STN IBN 8226034 CSLINES 0 0 141 (LNR) $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
LG 01 2 00 34 0 AIN AIN TDP4GRP
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP ETSIGRP
INAP Origination Attempt TDP: no subscribed trigger.
INAP Info Collected TDP: no subscribed trigger.
TABLE NCOS
CSLINES 0 0 0 DFLT ( XLAS K1TYPE NXLA NDGT)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CSLINES NXLA K1PSTN CSFETXLA 0 CSACCDIG
TABLE DIGCOL
TUPLE NOT FOUND
Default is RPT
TABLE IBNXLA: XLANAME K1TYPE
K1TYPE 7 NET N N 0 N CSDIG N Y DOD N K1TYPE CS_NPRT CS_NIL NONE $
TABLE DIGCOL
CSDIG 7 COL L 7
TABLE LINEATTR
K1TYPE IBN NONE NT 0 0 NILSFC 0 PX TYPEPX NIL 00 CS_NPRT CS_NIL $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
CS_NPRT NSCR 141 NPRT NONE N $ $
TABLE RATEAREA
CS_NIL NLCA NIL NILLATA $
TABLE PXHEAD
TYPEPX DFLT CONT(XLT PX PUBAPSTN)$ DFOP(CLASS NATL)$NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 743012345
TABLE PXCODE
TYPEPX 7 7 CONT ( PF 1) ( MM 6 18) ( XLT PX ATMEPX)$
TABLE PXHEAD
ATMEPX SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 43012345
TABLE PXCODE
ATMEPX 430 430 RTE ( PF 3) ( DEST 430)$
TABLE: PXRTE
KEY: ATMEPX 430
. S K1197EISWBE
EXIT TABLE PXRTE
TABLE AMAXLAID
MANTEST DFLT (FLEXCTYP GENERIC 910 OVRDALL )$
TABLE TRIGGRP
ETSIGRP INFOANAL
. GENTRIG ( CDPN K1197)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
. GENTRIG ( CDPN SIMTOOL)$ NIL
Trigger INAPV8 GENTRIG is applicable to office.
INAP Info Analyzed TDP: trigger criteria not met.

```



```

TABLE TRIGGRP
TDP4GRP NETBUSY
. GENTRIG ( CAUSE CSE_14)$ MDCKEY1
Trigger INAPV8 GENTRIG is applicable to individual line.
PLEASE ENTER VALUE FOR RELEASE CAUSE (0..127)
>14
. . TABLE TRIGINFO
. . MDCKEY1 EVENT TCAP INAPV8 SS7 EIN_NATL_GTT DFLT (SERVKEY 1111)
. . (SERVINFORM_INDEX 1111) $
. . . TABLE SERVINFORM
. . . 1111
. . . (INITDP_PARM ( SERVKEY) (CDPA) (CLI) (CPC) (EVENT_TYPE) $)
. . . (BILL_INFORM (FCI_OPT FREEFORM ) $)
. . . (EDPS_INFORM ( EXPLICIT ) $) (CS1R (CONTINUE) (CWA) $)$
. . . TABLE C7GTTTYPE
. . . EIN_NATL_GTT CCITT7 0 NATL E164 $
. . . TABLE C7GTT
. . . EIN_NATL_GTT 1111 1111 PCSSN (K1197RS1 EIN 50) $ SSN
INAP Route Select Failure TDP: trigger criteria met, querying the database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++

INAP Route Select Failure TDP: trigger criteria met, querying the database.

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++

```

35.4 Hardware Requirements or Dependencies

None.

35.5 Software Requirements or Dependencies

Feature A00007807 “Base ETSI ISUP V2 support for Dacom IN”.

35.6 Limitations and restrictions

For the existing general limitations in the CS2K IN platform, please refer to the FN of the activity A00002678 ‘Telefonica IN Enhancements’

35.7 Interactions

None.

35.8 Glossary

Term	Description
ASN.1	Abstract Syntax Notation One
CDN	Called Directory Number
CIRQ	Call Information Request
CIRP	Call Information Report
CS2000	CallServer 2000
CS2K	CallServer 2000
DN	Directory Number
ERBCSM	Event Report BCSM
ETC	Establish Temporary Connection
ETSI	European Telecommunications Standards Institute
IAM	Initial Address Message
IN	Intelligent Network
INN	Internal Network Number
INAP	Intelligent Network Application Protocol
InitDP	InitialDP
IP	Intelligent Peripheral
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
LNP	Local Number Portability
NOA	Nature of Address
NP	Number Portability
NPFI	Number Portability Forward Information
NPI	Numbering Plan Indicator
NPSI	NP Status Indicator
PRI	Primary Rate Access
QoR	Query on Release
REL	RELease
RN	Routing Number

Term	Description
RRBCSME	Request Report BCSME
SCF	Service Control Function
SCFId	Service Control Function Id
SCP	Service Control Point
SSP	Service Switching Point
TDP	Trigger Detection Point
TRAVER	TRAnslations VERification

35.9 References

- [1] ITU Intelligent Networks Systems Guide (INSYSGDE in PLS FMDOC)
- [1] Specifications for Interface on Dacom Intelligent Network
- [2] A59027497 LNP Query on Release - Non IN
- [3] A00002678 Telefonica IN Enhancements
- [4] ACT.A00002713 Spanish ISUP Enhancements for Telefonica
- [5] Feature A00002900 “China INAP Compliance Enhancement part 2”.
- [6] A00007807 “Base ETSI ISUP V2 support for Dacom IN”.

36: A00007794 Functional description (FN)

36.1 Feature name

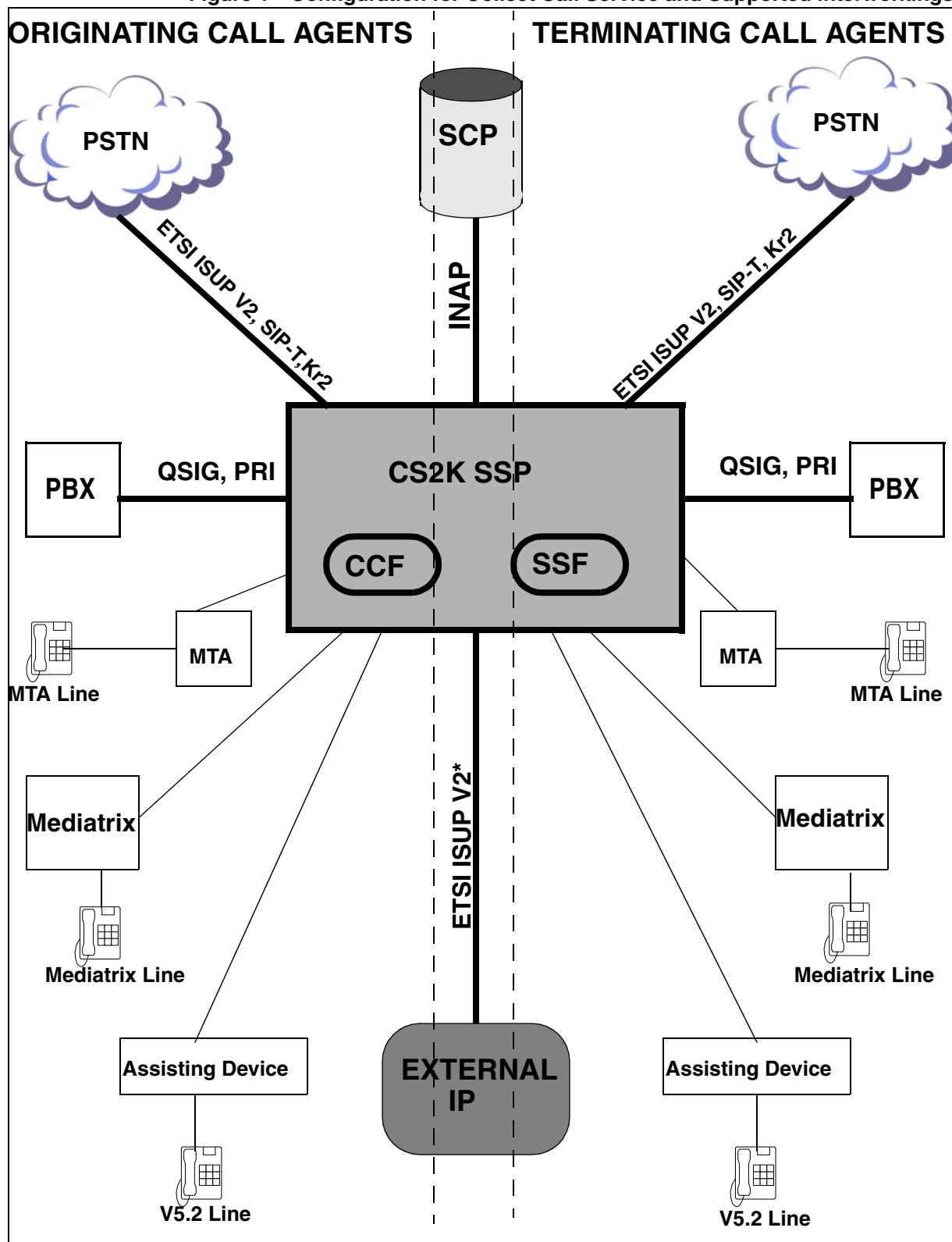
IN Collect Call Support (DACOM)

36.2 Description

Collect call is the service of charging the called party through announcement and called party identification which works as follows:

- When a call with collect call prefix digits is received by the SSP, the Intelligent Network service is triggered and an InitDP message is sent to the SCP
- The SCP instructs the SSP to monitor for the called party answer event, by arming the Answer EDP.
- Once the call is answered, ERBCSM(oAnswer) is sent to the SCP and SCP instructs SSP to connect both ends to the External IP device (through ETSI ISUP V2) to provide collect call announcements.
- Calling party will hear an announcement like “Please say your name after the signal” and the called party will hear an announcement like “<Name Surname> is calling, If you accept the charges for this call, please stay on line”
- If the called party accepts the call, SCP instructs SSP again to connect two parties after the announcement.

Figure 1 Configuration for Collect Call Service and Supported interworkings



*Please note that the parameters SCFid and CorrelationId required to connect to Assisting SSF, are supported by the activity A00007793.

This activity supports:

- CallSegmentID parameter in ETC operation,
- ETC (Leg2) and ETC (CallSegId 2) for connection to an external IP,
- DFCWA (leg2) and DFCWA (CallSegId 2) for disconnection from the external IP.

The supported originating and terminating agents for the IN Collect Call are shown in Figure: “Configuration for Collect Call Service and Supported interworkings” on page 504 and are listed in below table:

Table 1: Supported interworkings

Originating agents -> Terminating agents	lines	ETSI ISUP V2	ETSI PRI	QSIG (H.323)	SIP-T	Korean R2
lines ^a	*	*	*	*	*	*
ETSI ISUP V2	*	*	*	*	*	*
ETSI PRI	*	*	*	*	*	*
QSIG (H.323)	*	*	*	*	*	*
SIP-T	*	*	*	*	*	*
Korean R2	*	*	*	*	*	*

a. Supported line agents are Cable lines via MTA, IBN lines via Mediatrix and V5.2 (V5.2 BRI lines are not covered by this activity.)

Call Party Handling is supported for IN calls and is developed by activity A00007797: “Line Interworking Support For CPH (DACOM)”.

Also note that billing of collect calls are performed on the SCP so billing of DMS is not affected.

36.2.1 Functional Overview

36.2.1.1 Establish Temporary Connection Enhancement to support CallSegmentID Parameter

The ETC operation is enhanced to support CallSegmentID parameter. The LegID parameter and CallSegmentID parameters are defined as follows in the ETC operation in Q.1228 (INAP CS2) Specification:

```
EstablishTemporaryConnectionArg {PARAMETERS-BOUND : bound} ::=
SEQUENCE {
  assistingSSPIPRoutingAddress [0] AssistingSSPIPRoutingAddress { bound},
  correlationID [1] CorrelationID { bound} OPTIONAL,
  partyToConnect CHOICE {
    legID [2] LegID,
    callSegmentID [7] CallSegmentID { bound}
  } OPTIONAL,
  scfID [3] ScfID { bound} OPTIONAL,
  extensions [4] SEQUENCE SIZE(1..bound.&numOfExtensions)
    OF ExtensionField {bound} OPTIONAL,
  carrier [5] Carrier OPTIONAL,
  serviceInteractionIndicators [30] ServiceInteractionIndicators { bound}
    OPTIONAL,
  serviceInteractionIndicatorsTwo [6] ServiceInteractionIndicatorsTwo
    OPTIONAL,
  ...
}
```

With this enhancement it will be possible to connect the Called Party to the external IP using CallSegmentID parameter as well as the LegID parameter in the ETC operation.

Only one of these two parameters can be used in the ETC operation. If both of them are present in a received ETC, the operation will be rejected.

36.2.1.2 IN Collect Call Support

“Collect Call Flow Diagram” on page 507 illustrates the collect call flow.

Please note that IP to SCP operations which are independent of the SSP are not displayed in the message sequence and the incoming call and the connection to the external IP are assumed to be over ETSI ISUP V2 trunks.

Figure 2 Collect Call Flow Diagram

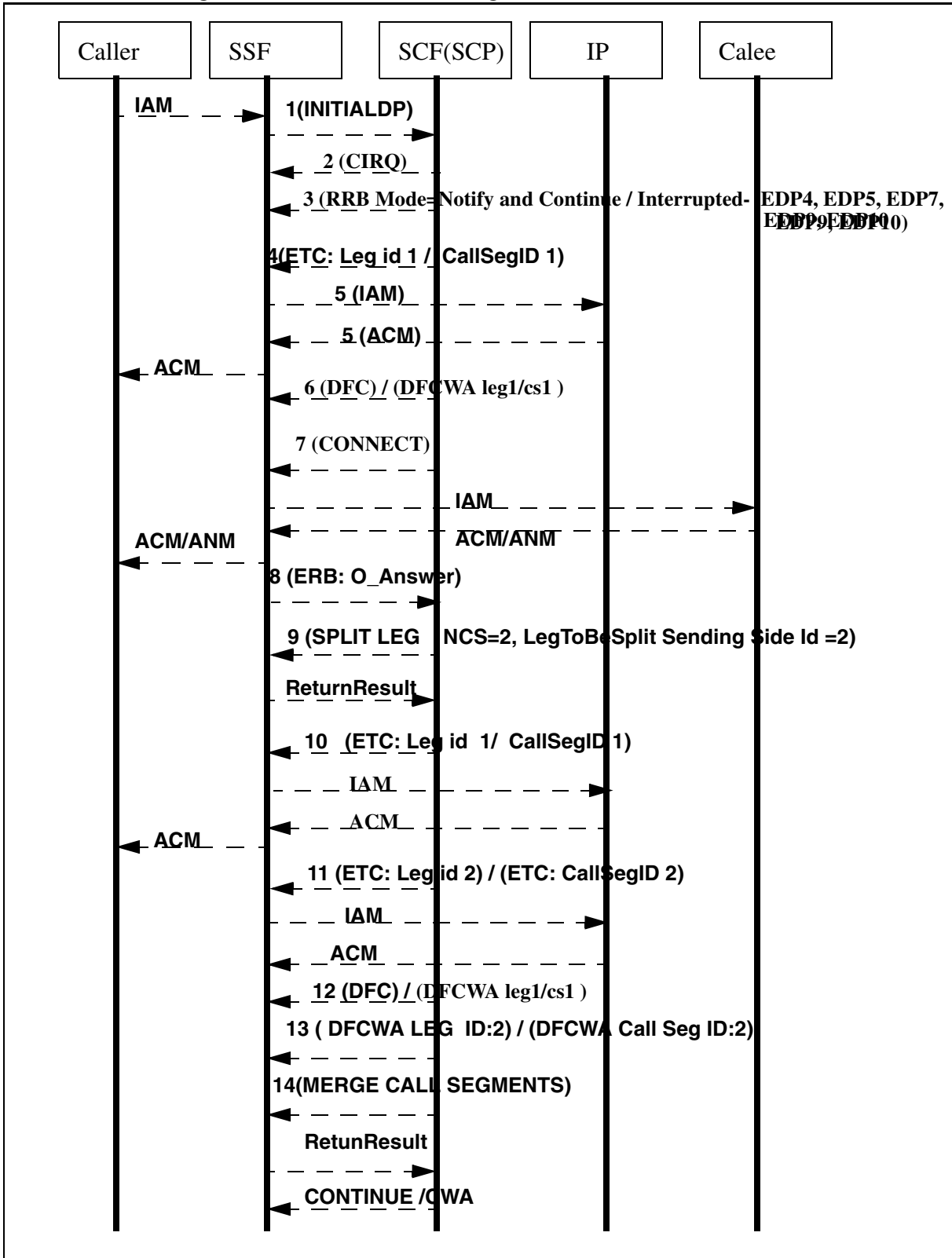
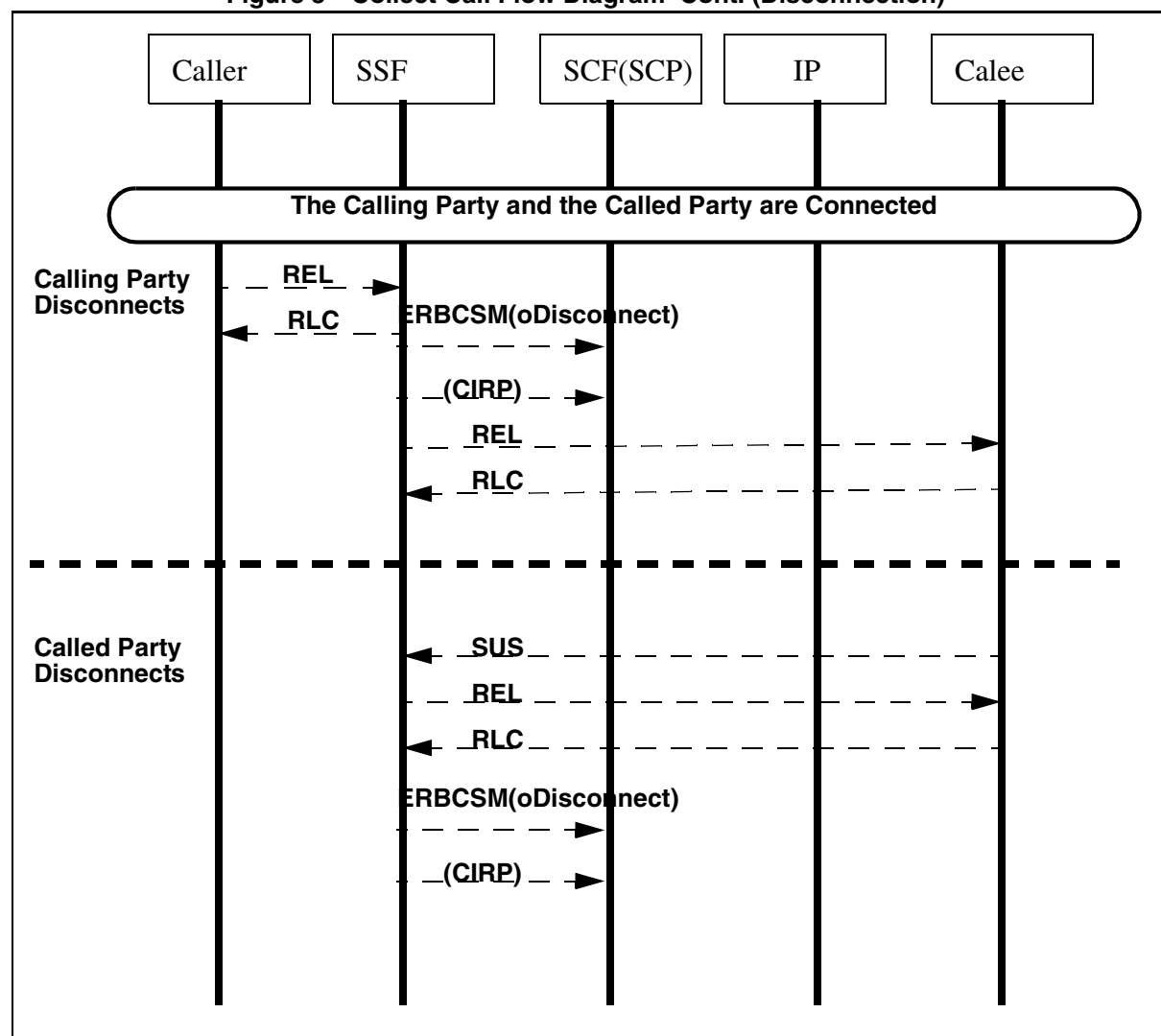


Figure 3 Collect Call Flow Diagram Cont. (Disconnection)

Please note that after the called party disconnects, the SCP may either disconnect the controlling (Leg 1) call or connect it to another announcement.

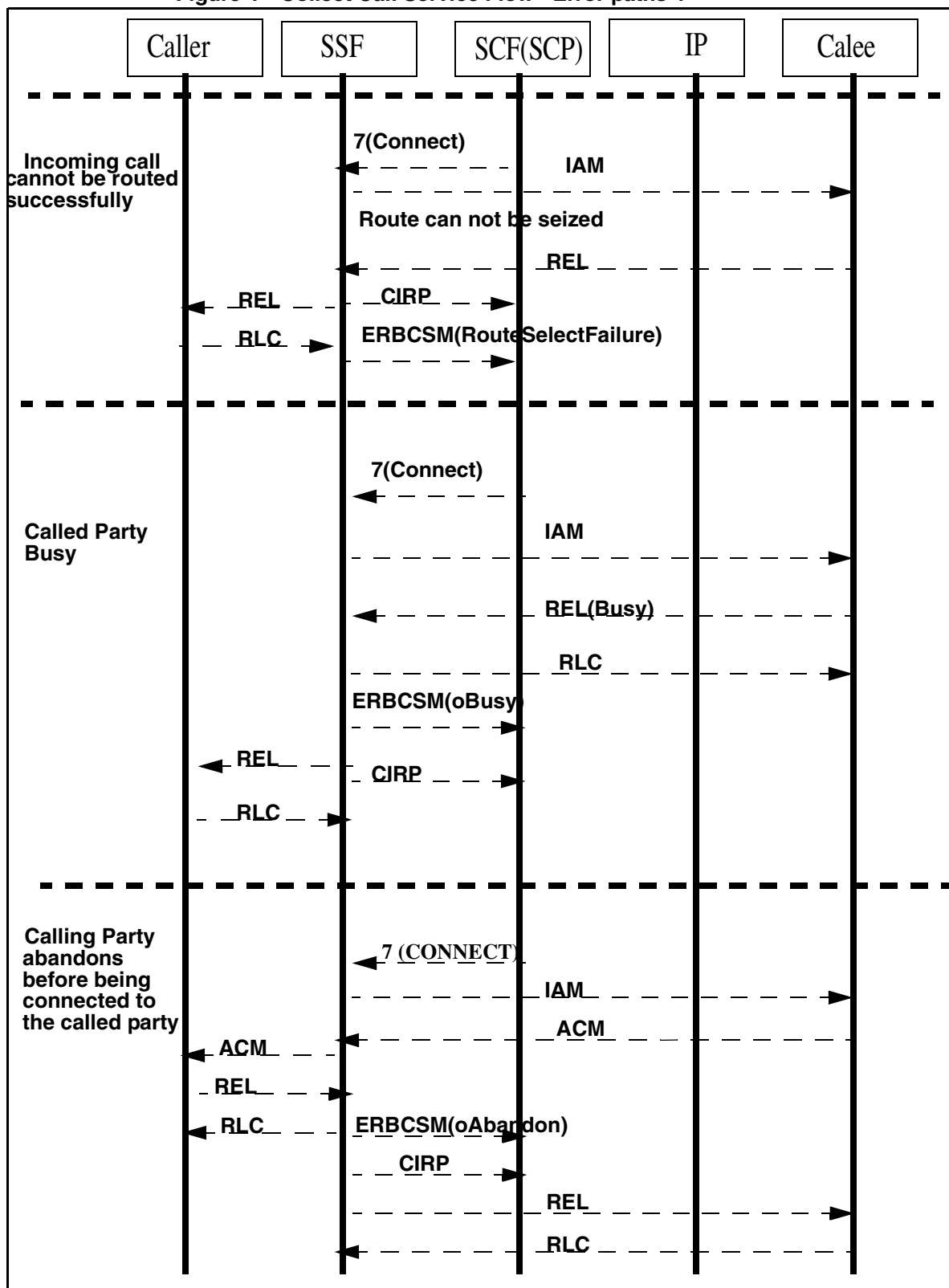
1. The switching system (SSP) recognizes Collect Call Prefix, and triggers intelligent call to SCP. The SCP is informed via InitialDP message.(Will be detected and triggered at TDP3)
2. The SCP sends CIRQ to SSP.
3. SCP arms EDP-7 (O_Answer Mode: N&C or Interrupted) so that when the terminating switch answers, the system will report the event to SCP. SCP also arms EDP4 (Route_Select_Failure), EDP5 (O_Called_Party_Busy), EDP9 (O_Disconnect), EDP10(O_Abandon)
4. SCP requests the switching system (SSP) to set up a call to IP. (DMS/SSP is expecting ETC message from SCP)

5. SSP requests external IP to set up call, and external IP sends ACK to SSP.
6. SCP commands SSP to disconnect external IP connection. (DFC)
7. SCP commands the switching system to connect calls to the reported called party number. (CONNECT)
8. If there is an answer from terminating switch, the system reports the event to SCP. (ERB: O_Answer)
9. SCP commands Split Leg operation to be able to connect both the caller and the called party to the external IP. **The Split Leg operation has the parameters New Call Segment = 02 and LegTo BeSplit (Sending Side Id = 02).**
10. SCP commands SSP to make connection to the ext.IP to provide announcement for the calling party (ETC: Leg ID = 1).
11. SCP commands SSP to make connection to the ext. IP to provide announcement for the called party. **(ETC: Leg ID = 2 or ETC:CallSegmentID=2)**
12. SCP commands SSP to release ext.IP connections for Leg 1(DFC).
13. SCP commands SSP to release ext.IP connections for Leg 2 **(DFCWA Leg 2 or DFCWA CallSegmentID 2)**
14. SCP commands SSP to Merge Call Segments.After the MergeCallSegments operation a Continue or CWA operation is needed to change the state from WFI to MON.
15. After the calling or the called party goes on-hook the call is released between the caller and the callee, SSP sends a Call Information Report (CIRP) to the SCP since it is requested from the SCP via CIRQ message.

36.2.1.3 Collect Call Service Error Paths

Figures 4 to 9 show error paths that may occur during Collect Call Service Flow. “Collect Call Flow Diagram” on page 507 is taken as the reference successful call path for all figures.

Figure 4 Collect Call Service Flow - Error paths-1



In the first two scenarios of “Collect Call Service Flow - Error paths-1” on page 510 the SCP may connect the caller to an announcement to indicate the unsuccessful status of the call.

Figure 5 Collect Call Service- Error Paths-2

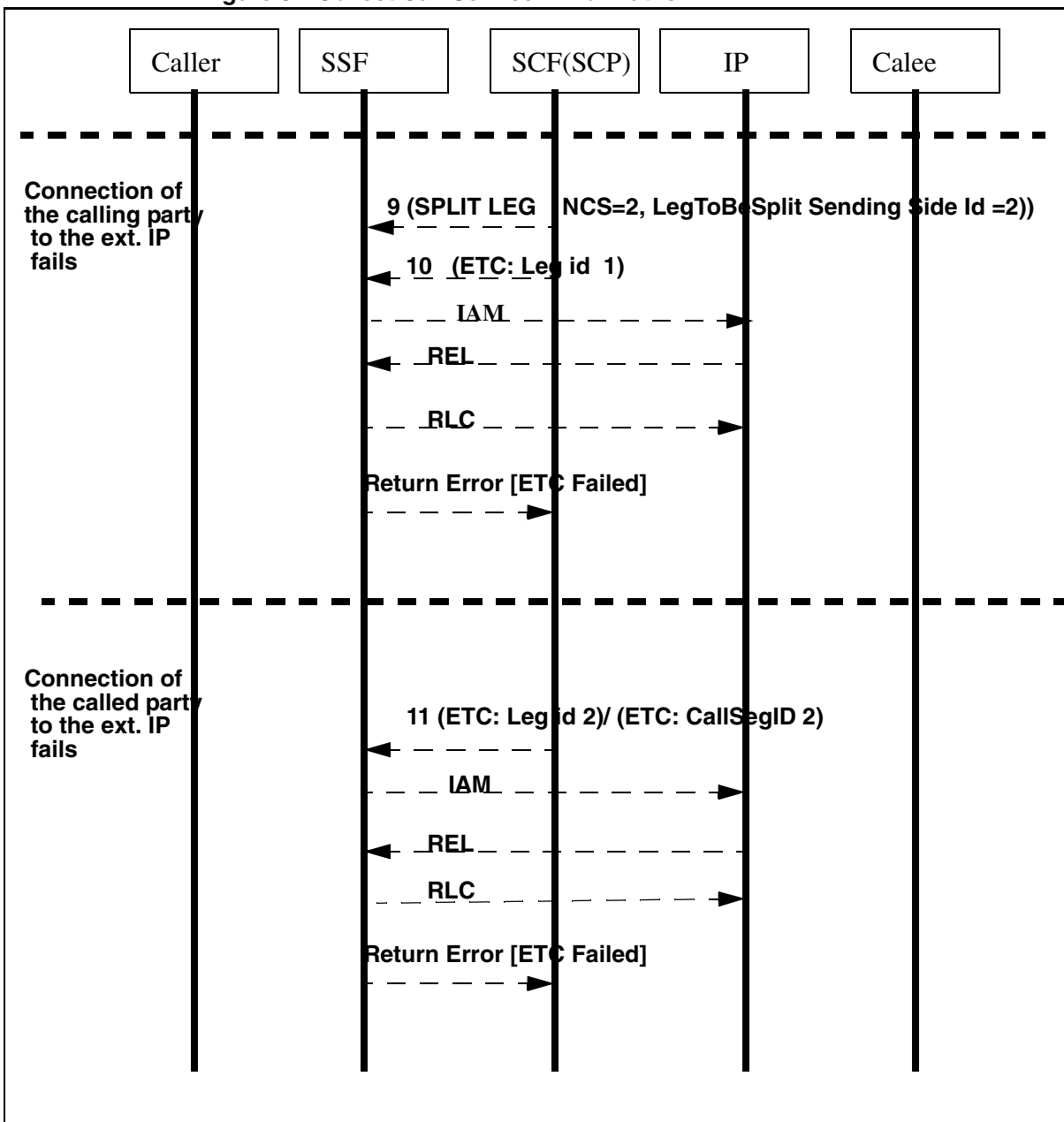


Figure 6 Collect Call Service- Error Paths- 3

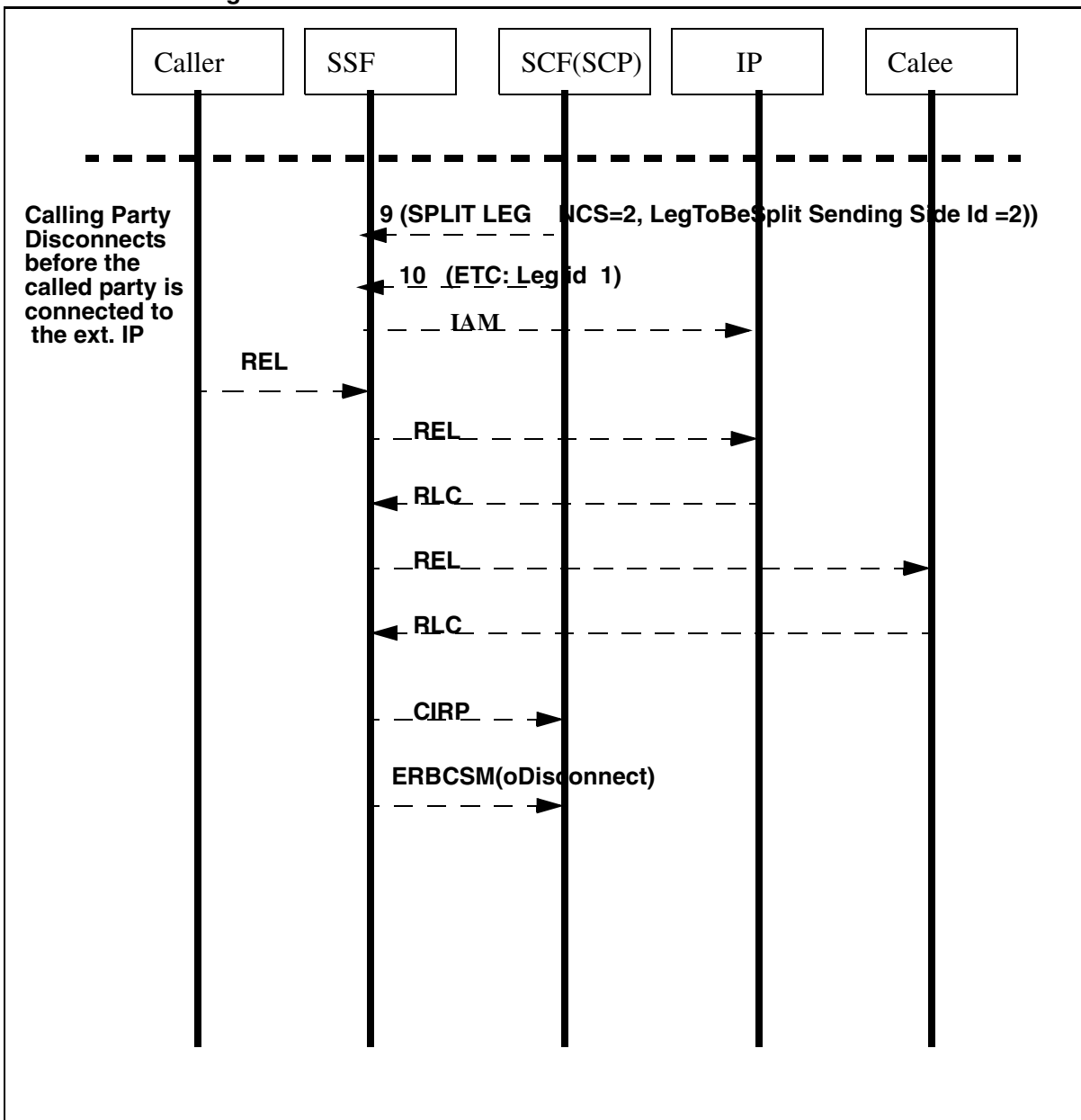


Figure 7 Collect Call Service- Error Paths -4

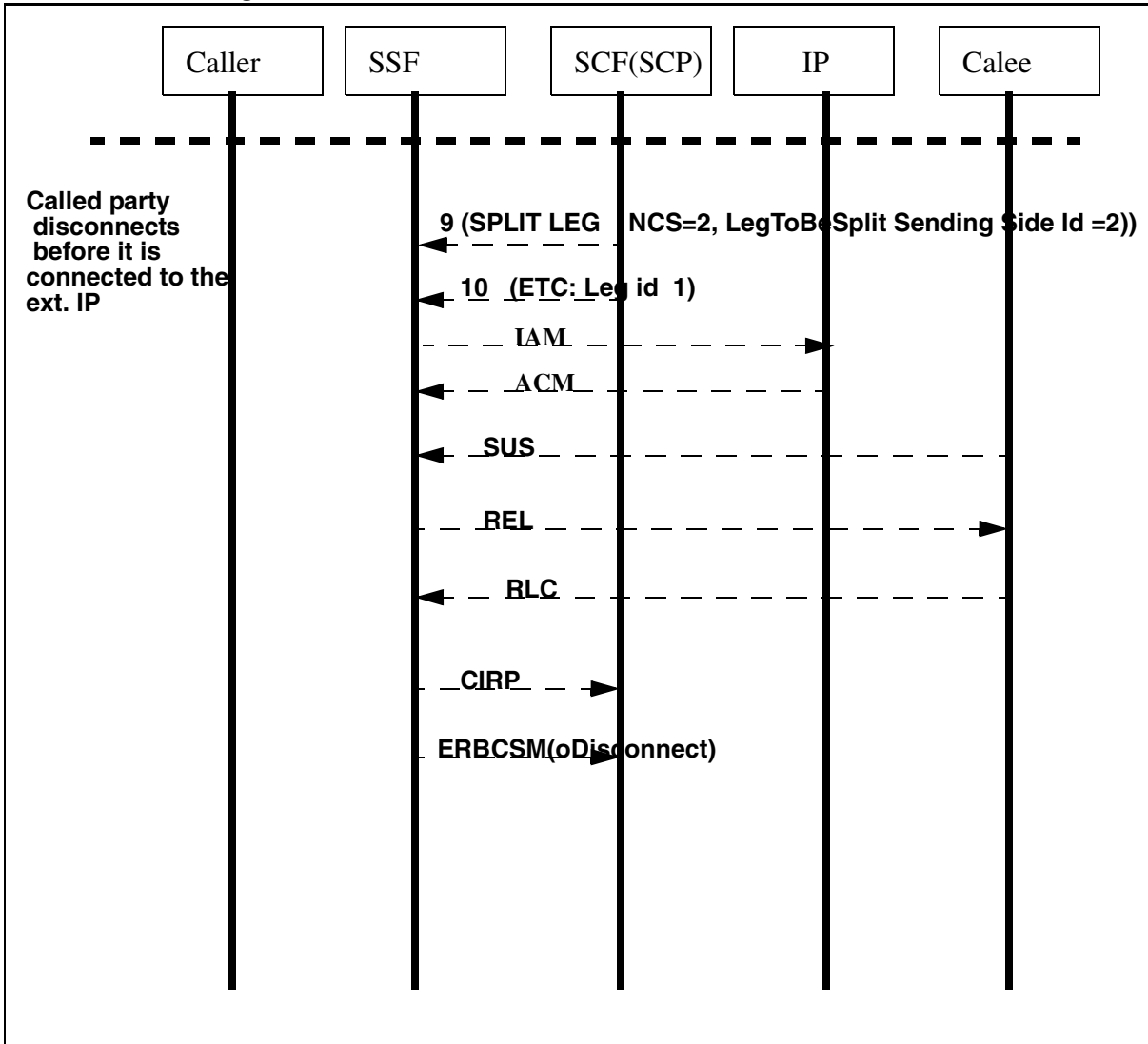


Figure 8 Collect Call Service- Error Paths -5

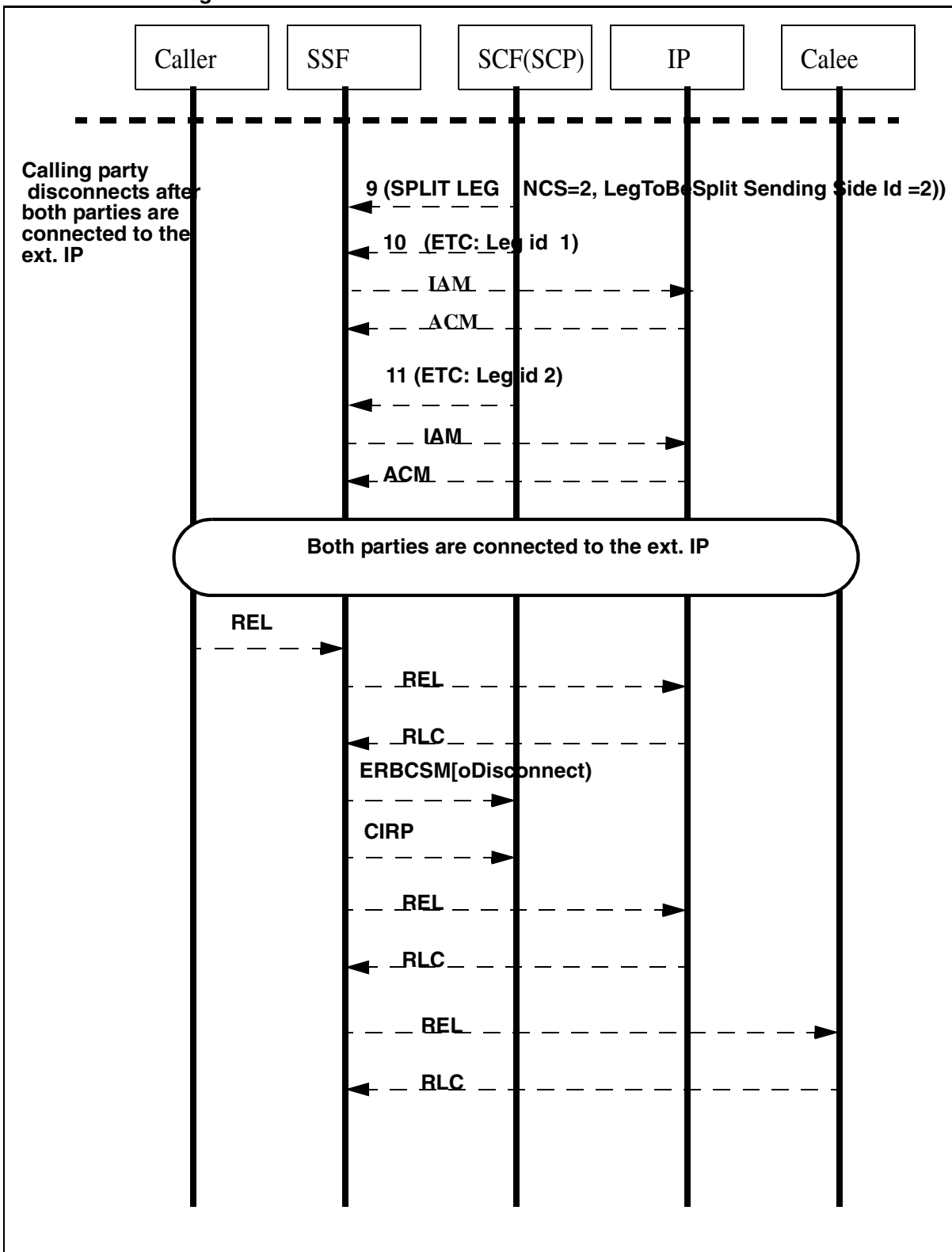
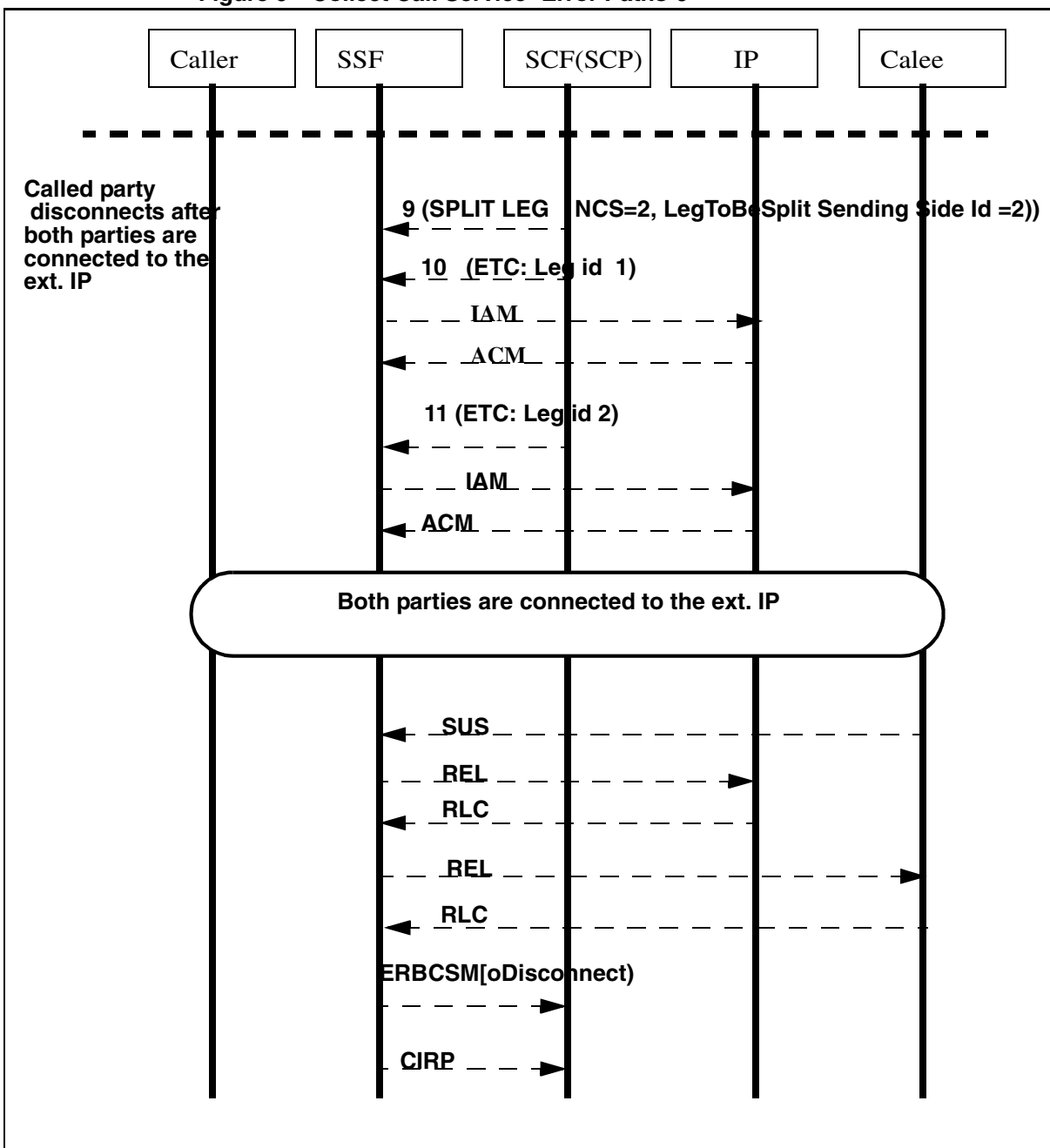


Figure 9 Collect Call Service- Error Paths-6

In the above figure; after the called party disconnects, SCP may either disconnect the controlling (Leg 1) call or connect this call to another announcement.

36.3 Hardware Requirements or Dependencies

IN Call Collect service is supported on Succession Offices.

36.4 Software Requirements or Dependencies

None.

36.5 Limitations and restrictions

- Call Party Handling is supported for IN calls and is developed by activity A00007797: “Line Interworking Support For CPH (DACOM)”.
- V5.2 BRI lines are not covered by this activity.
- **Line Feature Interactions:**
 1. The CPH functionality cannot co-exist with line features which involve multi-party call setup
 2. The DMS SSP can keep only one INAP dialogue open per call.

Therefore the following line features will be disabled while Collect Call Service is active on the call:

Three way calling, Conference Call, Call waiting, Call Transfer, Call Hold.

Note: In a Collect Call Scenario, Malicious Call Trace Feature can only work before the Split Leg operation or after the called party accepts the charges and the call is merged.

Note: The Call forwarding features can only work at the start of the Collect call before the called party answers.

36.6 Interactions

None

36.7 Glossary

Term	Description
BCSM	Basic Call State Machine
CIRP	Call Information Report
CIRQ	Call Information Request
CPH	Call Party Handling
DFC	Disconnect Forward Connection
DFCWA	Disconnect Forward Connection With Argument
ERBCSM	Event Report BCSM
ETC	Establish Temporary Connection

IP	Intelligent Peripheral
RRBCSM	Request Report BCSM
SCF	Service Control Function
SCP	Service Control Point
SSF	Service Switching Function
SUS	Suspend

37: A00007796 Functional description (FN)

37.1 Feature name

Color-ring Feature (DACOM)

37.2 Description

37.2.1 Functional Overview

Color-ring¹ is a IN service provided to the called subscriber through which the caller can hear specific sounds (hot music, sound effects, voice, etc.) that are pre-assigned by the service subscriber instead of the existing monotonous ring-back tone until the phone is answered. To enable the color-ring service on the DMS SSP, a new Event Detection Point (EDP) needs to be created on the DMS SSP to inform SCP of the ring signal (alerting message) received from the terminating party.

This feature introduces the CallAccepted Event Detection Point (EDP27) on the Terminating BCSM. The CallAccepted event is hit when an alerting type of message is received from the terminating agent, for certain protocols this message may be an 'address complete message' (ACM), but can be a different message for other protocols.

This feature enables the DMS SSP to :

- successfully decode a RequestReportBCSMEvent operation including the arming of CallAccepted event in request mode,
- to report the CallAccepted event to SCP with EventReportBCSMEvent operation when alerting type of message is received from the terminating agent.
- to be able to accept SplitLeg and MergeCallSegment operations when CallAccepted event is hit and convert to multy-party processing (Call Party Handling).

The supported originating agents are:

- lines (Cable lines via MTA, IBN lines via Mediatrix and V5.2²)
- ETSI ISUP V2
- ETSI PRI
- QSIG

¹Also known as Dacom Ring Back Tone service.

²Note that V5.2 BRI lines are not covered by this activity.

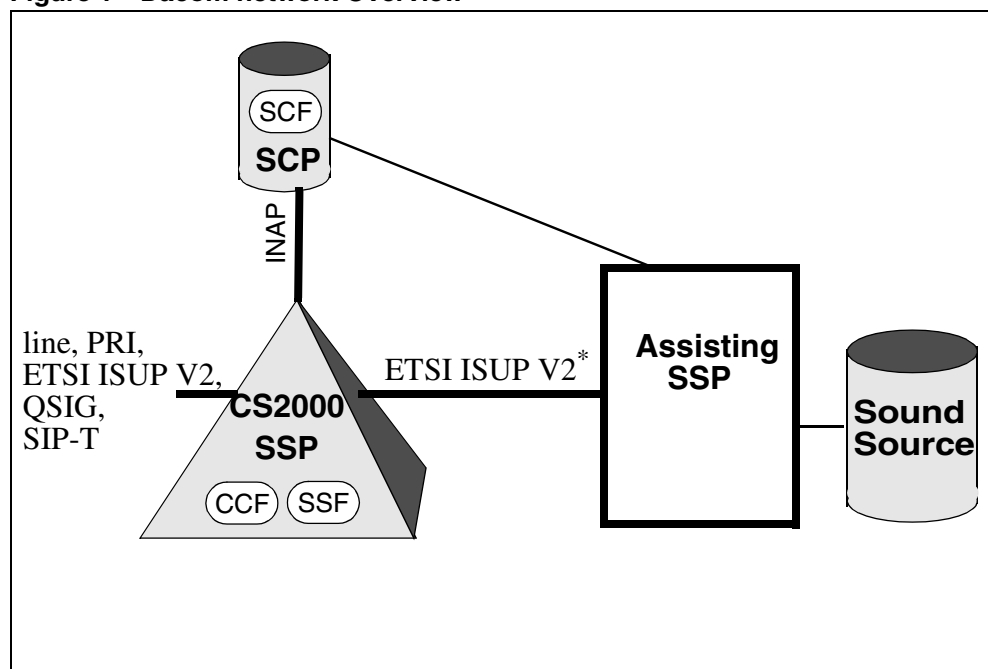
- SIP-T

The TDP12 triggering is supported on terminating lines. The following line agents are supported:

- Cable lines via MTA
- IBN lines via Mediatrix
- V5.2¹

Note that line interworking support for Call Party Handling operations such as SplitLeg and MergeCallSegments will be implemented by the activity A00007797 Line interworking support for CPH.

Figure 1 Dacom network Overview



*Please note that the parameters SCFid and CorrelationId required to connect to Assisting SSF, are supported by the activity A00007793.

37.2.1.1 Functional Requirements

The color-ring service implementation is as follows, please refer to Figure 2² for the service flow:

¹Note that V5.2 BRI lines are not covered by this activity.

²Note that the ISUP signaling messages are used on the message flow for consistency, however the calling party and called party on the DMS SSP can be any of the supported agents (line, ETSI PRI, ETSI ISUP, QSIG or SIP-T)

- The incoming call triggers IN if the terminating party is subscribed to TDP12 trigger. The SCP is informed via InitialDp message.
- SCP recognizes that the corresponding intelligent network number is registered for the color-ring service and requests the exchange to connect to real destination number at first. (SCP sends RRBCSM message to arm CallAccepted, tAnswer, tDisconnect(leg1, leg2) and tAbandon events then sends Continue message to the DMS SSP)
- The DMS SSP routes the call to the terminating party, in accordance with the instruction from the SCP. The terminating agent sends alerting message (ring signal) notifying the subscriber B of the arrival of call and delivers ring-back tone to the called party. The ring-back tone sent from the terminating party is not forwarded to the calling subscriber A.
- The DMS SSP detects CallAccepted event when ringing tone is applied to the terminating line and reports the CallAccepted event to the SCP via RRB message. The SCP instructs connection to the sound source delivery server for ring-back tone delivery. (SCP sends SplitLeg and ETC messages to connect A party to sound source)
- The DMS SSP connects the calling party to the sound source delivery server¹ the server responds to it. The DMS SSP receiving the response from the sound source delivery server connects a speech path between the incoming subscriber and the sound source delivery server.
- The sound source delivery server, which is requested to assign a call by the exchange, requests SCP to provide supplementary order, and the SCP instructs the sound source delivery server to connect to the resource. (The functionality between sound source delivery server and SCP are outside the scope of DMS functionality, they are included here to understand the complete scenario of the service)
- The sound source delivery server provides corresponding sound source (pre-assigned sound source by intelligent network service subscriber) instead of the ring-back tone to the calling subscriber.
- In case the called subscriber B answers, tAnswer EDP is detected by the DMS SSP.
- The DMS SSP reports answer event to the SCP. (DMS sends ERBCSM(tAnswer) to SCP.
- The SCP instructs the exchange to disconnect with the sound source delivery server via DFC message. The DMS SSP disconnects the calling party from the sound source server.

¹The DMS SSP supports connection to sound source delivery server via ETSI ISUP V2.

-
- The requested sound source delivery server for disconnection stops delivering sound source and releases the connection.
 - SCP instructs the release of connection with the sound source delivery server, and at the same time instructs call connection between the calling subscriber (A) and the called subscriber (B). (SCP sends MergeCallSegments message to DMS)
 - The DMS SSP, which is requested to connect the call, makes call between the caller A and the called party B. For ETSI ISUP originated calls, Nortel SSP propagates ISUP_ANM towards the originating exchange if not already sent during External IP connection.
 - When the A party or B party releases the connection, the DMS SSP reports tDisconnect event to SCP via ERBCSM message and sends the call information report (via CIRP message) which is requested from SCP in the beginning of the call via CIRQ message.

Figure 4 Color ring Service flow - success path

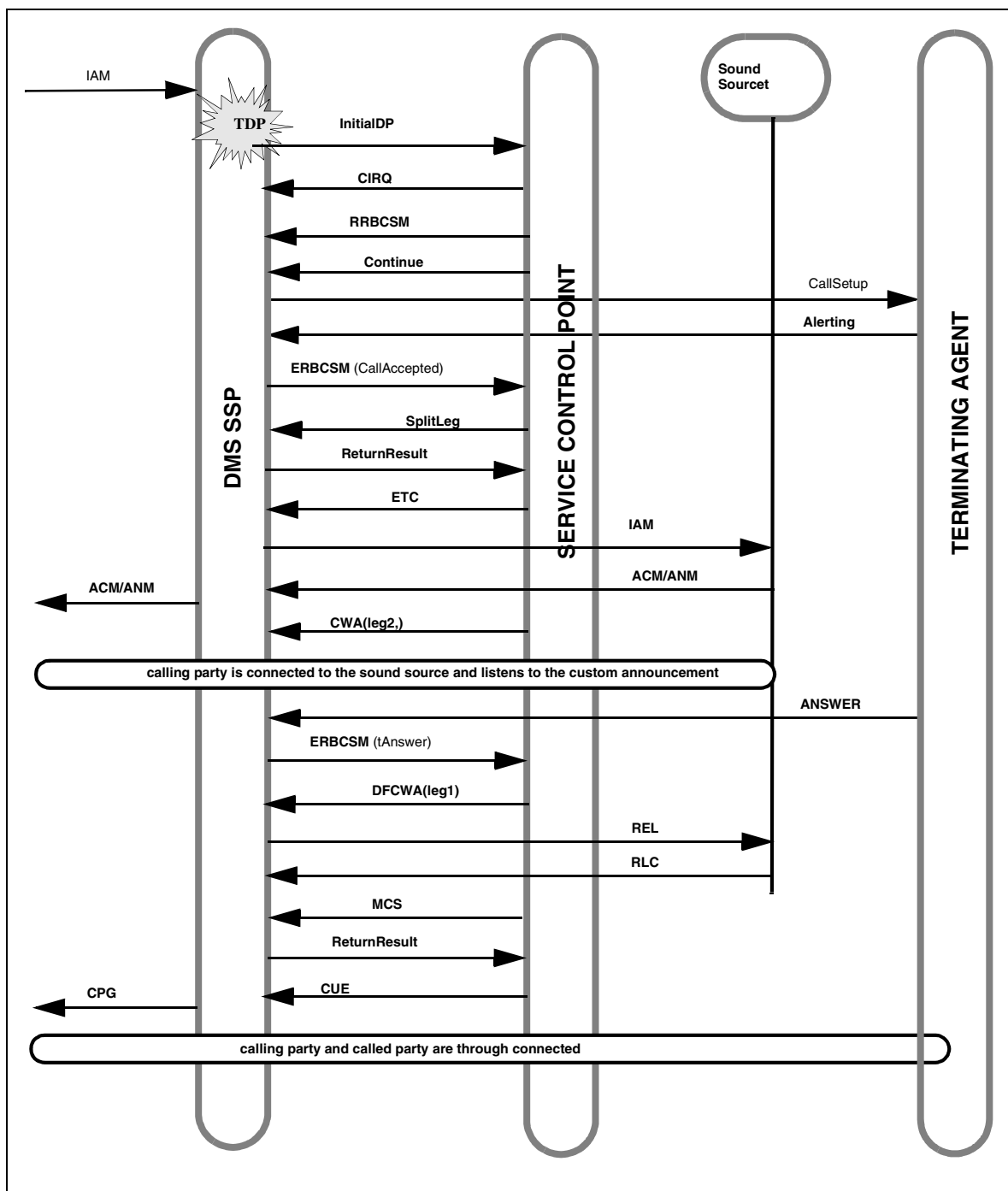
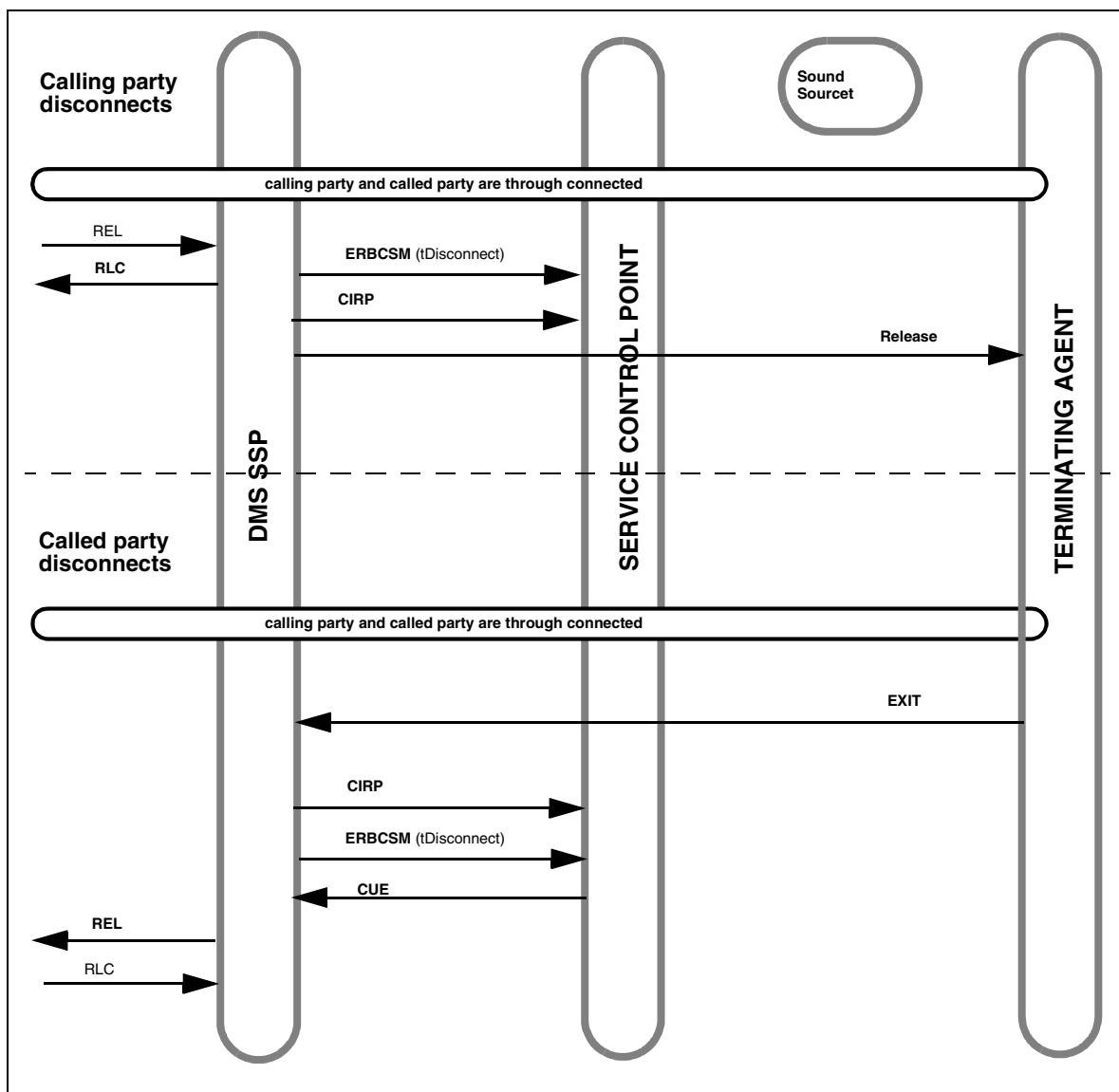


Figure 5 Color ring Service flow - success path cont. (disconnection)

**Error paths:**

The following event may occur before CallAccepted EDP event occurs:

- tAbandon :

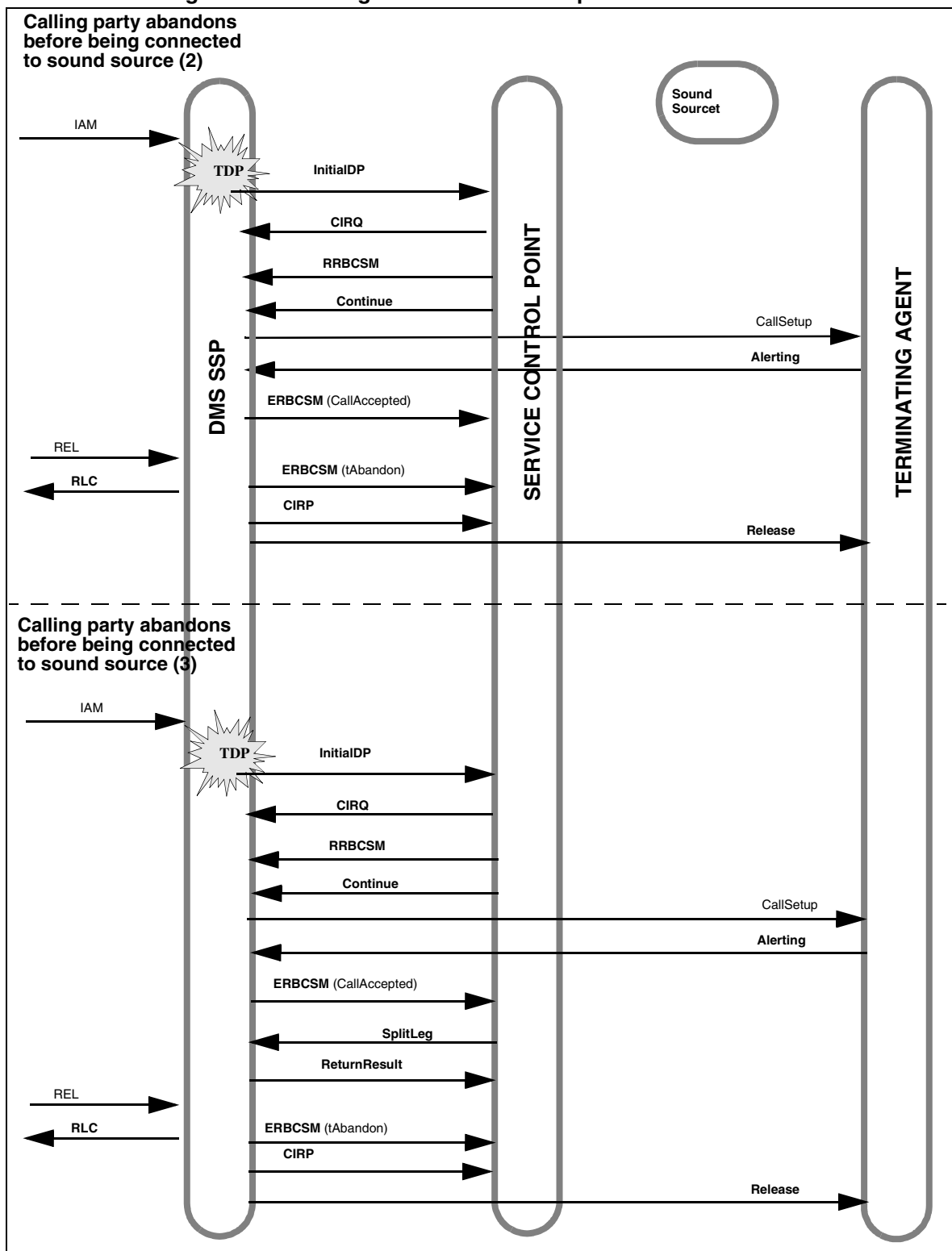
calling party abandons the call before being connected to sound source
or

calling party abandons before answer

The SCP may arm these EDPs and take appropriate actions when these events occur.

Please refer to Figure 4, 5 and 6 for the error paths that may occur during the color-ring service execution.

Figure 6 Color ring Service flow - error path



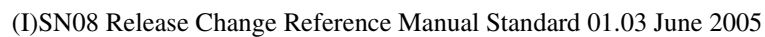
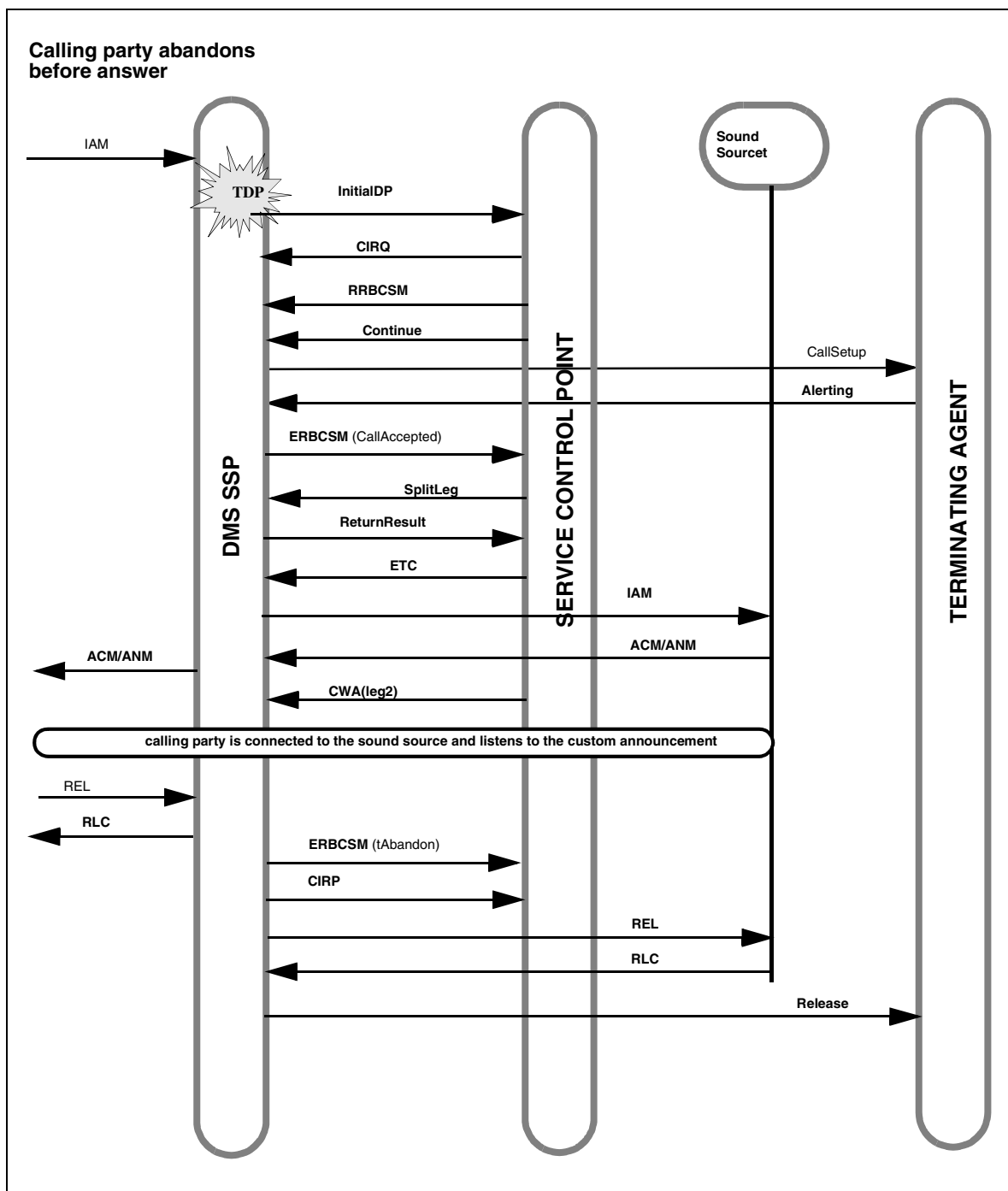


Figure 8 Color ring Service flow - error path cont.



37.2.1.2 Decoding & Encoding of CallAccepted in RRBCSM operation

The SCP sends the RRBCSM operation to arm CallAccepted EDP in request mode. The DMS SSP sends ERBCSM operation to notify SCP of the CallAccepted event. CallAccepted EDP will be represented by the value of decimal 27 in both operations.

CallAccepted event, like tAnswer can be armed for leg2 only.

EINTRACE tool is enhanced to display CallAccepted EDP in RRBCSM and ERBCSM operations.

Figure 2 RRBCSM & ERBCSM ASN.1 Encoding

```

RequestReportBCSMEventArg ::= SEQUENCE
{
  bcsmEvents [0] SEQUENCE SIZE(1..numOfBCSMEvents) OF BCSMEvent,
  extensions [2] SEQUENCE SIZE(1..numOfExtensions) OF ExtensionField OPTIONAL
  --
  ... }
  -- Indicates the BCSM related events for notification.

EventReportBCSMArg ::= SEQUENCE
{
  eventTypeBCSM [0] EventTypeBCSM,
  eventSpecificInformationBCSM [2] EventSpecificInformationBCSM OPTIONAL,
  legID [3] LegID OPTIONAL,
  miscCallInfo [4] MiscCallInfo DEFAULT {request},
  --
  ...
}

BCSMEvent ::= SEQUENCE
{
  eventTypeBCSM [0] EventTypeBCSM,
  monitorMode [1] MonitorMode,
  legID [2] LegID OPTIONAL,
  dpsSpecificCriteria [30] DPSpecificCriteria OPTIONAL
}

EventTypeBCSM ::= ENUMERATED
{
  origAttemptAuthorized(1),
  collectInfo(2),
  analyzedInformation(3),
  routeSelectFailure(4),
  oCalledPartyBusy(5),
  oNoAnswer(6),
  oAnswer(7),
  oMidCall(8),
  oDisconnect(9),
  oAbandon(10),
  termAttemptAuthorized(12),
  tAnswer(15),
  tDisconnect(17),
  tAbandon(18),
  CallAccepted(27)
}

MonitorMode ::= ENUMERATED
{
  interrupted(0),
  notifyAndContinue(1),
  transparent(2)
}

LegID ::= CHOICE
  sendingSideID [0] LegType
    -- used in operations sent from SCF to SSF
  receivingSideID [1] LegType
    -- used in operations sent from SSF to SCF
}

```

37.2.2 Arming and Detecting CallAccepted EDP

When CallAccepted event is detected by an EDP-R, the following events occur:

- 1) An ERBCSM operation is sent to the SCP reporting the EDP that was encountered.
- 2) The CallAccepted EDP is disarmed.
- 3) CSCV state performing Call Party Handling is updated. This item is explained in detail in the next section.
- 4) The SSF state machine changes to the Waiting for Instructions state.
- 5) T_{SSF} timer is started.

The SCP has been queried for further instructions on how to complete the call, and depending on how the SCP has been set up for the service, may send the following:

- SplitLeg operation to create multiple call segments.
- Continue to instruct SSF to continue with the call processing.

37.2.3 Effect of CallAccepted event on CPH

The Orig Setup CSCV represents a two-party call in the setup phase. There is a joined controlling leg and a pending passive leg attached to the connection point. The passive leg has an O-BCSM instance attached.

The CSCV state transits to Stable 2-party on detection of the CallAccepted DP for the passive leg.

The stable 2-party CSCV represents a stable or clearing 2-party call. There is a joined controlling leg and a joined passive leg attached to the connection point. The passive leg has an O-BCSM instance attached.

The SplitLeg INAP operation instructs the SSF to separate one party from its call segment and place it in a new associated call segment with a call segment ID specified in the operation's newCallSegment parameter.

The DMS SSP can accept SplitLeg operation during stable-2 party phase of the call. It is used by the ITU IN SSP for services to play announcements to the parties in the call or to collect digits from the parties of the call. Upon processing the SplitLeg operation, DMS SSP transits to multi-segment CSA.

The MergeCallSegments INAP operation is the inverse of SplitLeg, it instructs the SSF to merge two existing associated call segments into a single call segment and establish or re-establish a through speech connection among all the call legs.

For the color-ring service, the SCP sends MergeCallSegments upon detecting tAnswer event. The DMS SSP will convert the call from multi-party to stable 2-party call upon receiving MergeCallSegments. A through speech connection will be established between all call legs.

37.3 Hardware Requirements or Dependencies

Not applicable.

37.4 Software Requirements or Dependencies

This Functionality is implemented in ISN08.

37.5 Limitations and restrictions

Handling of tNoAnswer EDP-R in multi-segment CSA is not supported, if tNoAnswer EDP-R is detected while the DMS SSP is in multi-segment CSA, an EIN301 log is generated and the tNoAnswer EDP-R is ignored. If tNoAnswer EDP-N is detected in multi-segment CSA, call is released as in single-segment CSA.

CallAccepted EDP is not supported on ACD/UCD calls.

Line feature interactions: There are 2 main limitations on the line feature interactions:

1. The CPH functionality cannot co-exist with the line features which involve multi-party call setup.
2. The DMS SSP can keep only one INAP dialogue open per call.

Therefore the following line features will be disabled while color-ring service is active on the call:

Call Waiting, Three Way Call, Conference Call, Call Transfer, Call Hold, Call Forward No Answer.

37.6 Interactions

A00007796 Line interworking support for CPH: CPH operations SplitLeg and MergeCallSegments will be supported on line agents by this activity.

Connection to sound source server requires that the SCFid and CorrelationId parameters received in ETC message are mapped to the outgoing IAM SCFid and CorrelationId parameters. The following activities will implement the SCFid and CorrelationId support of DMS SSP:

A00007807 - Base ETSI ISUP V2 support for Dacom

A00007793 - SCFid, CorrelationId and QoR Based LNP

A00008464 - Terminating EDPs support

37.7 Operational Measurements (OM)

37.7.1 New/modified OM groups

EINEDP27H is added to OM group EIN2 and it is incremented when CallAccepted EDP is encountered.

37.8 AMA/Billing information (AM)

37.8.1 New/changed AMA/billing information

AMA record generated for the connection to external IP (sound source) contains Calling Party Number for originating digits.

37.9 Glossary

Term	Description
ACM	Alerting Message
ANM	Answer Message
BCSM	Basic Call State Model
CIRP	Call Information Report
CIRQ	Call Information Request
CPH	Call Party Handling
CIRQ	Call Information Request
CUE	Continue
CSA	Call Segment Association
CSCV	Call Segment Connection View
CWA	Continue With Argument
DFC	Disconnect Forward Connection

Term	Description
DMS	Digital Multiplexing System
ERBCSM	Event Report BCSM
ETC	Establish Temporary Connection
IAM	Initial Attempt Message
IN	Intelligent Networks
InitDP	Initial Detection Point
OBCSM	Originating BCSM
REL	Release Message
RLC	Release Complete Message
RRBCSM	Request Report BCSM
SCP	Service Control Point
SSP	Service Switching Point
TDP	Trigger Detection Point

38: A00007807 Functional description (FN)

38.1 Feature name

Base ETSI ISUP V2 support for Dacom IN

38.2 Description

The activity A00007807 handles adding of the new additional optional parameters

- SCF ID
- Correlation ID

to the outgoing IAM message if these parameters are sent by the SCP in the office where the IN interaction exists.

This activity also tandem the incoming REL message with cause value 14 (ported number) and diagnostics in intermediate exchange for Base ETSI ISUP V2 to Base ETSI ISUP V2 interworking.

If the IN is triggered by the incoming REL message with cause value 14 and diagnostics field and, if SCP sends CDN and NPFI extensions in the connect operation to the CS2000 SSP, these parameters are mapped to the outgoing IAM message as additional optional parameters:

- Called Directory Number
- Number Portability Forward Information

Triggering IN is out of scope of this activity. It is handled in the activity A00007793.

If the REL message with cause value 14 and diagnostics field is received in the originating office and there is no IN interaction the in this office, then the call is terminated according to the diagnostics field on REL message with cause value 14.

The lengths of the new optional parameters which are used by Dacom are given in Table 1, "The lengths of the new optional parameters used by Dacom". The lengths of the new optional parameters which are defined in the ISUP signalling is also given in Table 2,. These lengths do not include tag and length bytes of the parameters.

Table 1 The lengths of the new optional parameters used by Dacom

Parameter	Min Length	Max Length
SCF ID	1 byte	4 bytes
Correlation ID	2 bytes	13 bytes
Called Directory Number	2 bytes	17 bytes
Number portability forward information	1 byte	1 byte

Table 2 The lengths of the new optional parameters defined in ISUP

Parameter	Min Length	Max Length
SCF ID	1 byte	20 bytes
Correlation ID	2 bytes	13 bytes
Called Directory Number	2 bytes	17 bytes
Number portability forward information	1 byte	16 bytes

When these parameters are received from the SCP, SSP is going to receive and store these parameters (please refer to FN section of the activity A00007793). The outgoing IAM is built by using these stored parameters. During the adding of these parameters to the IAM message, the parameters that are stored by the SSP are used without doing any modification on the parameters. So the lengths of these parameters will be defined by the CS2000 SSP. It is SSP's responsibility to send the parameters in the correct length.

Mapping of the new additional optional parameters is supported only for the switch where IN triggering is done. Supported incoming agents for the IN triggering are:

- Line (V5.2, Cable MTA, IAD IBN line types)
- Base ETSI ISUP V2
- ETSI PRI
- H.323 trunks (defined as QSIG trunks in CS2000 table datafill)
- SIP-T trunk connections to MCS5200 endpoints
- Korean R2 trunks once developed in ISN08 (The Korean R2 and IN triggering from the Korean R2 are implemented with the activity A00007405 in ISN08)

Base ETSI ISUP V2 is going to be used for implementing the desired behavior. Tandeming of these additional optional parameters is supported only for Base ETSI ISUP V2 to Base ETSI ISUP V2 interworking.

When these additional optional parameters are added and sent in the outgoing IAM message, only all the way ISUP routing is supported.

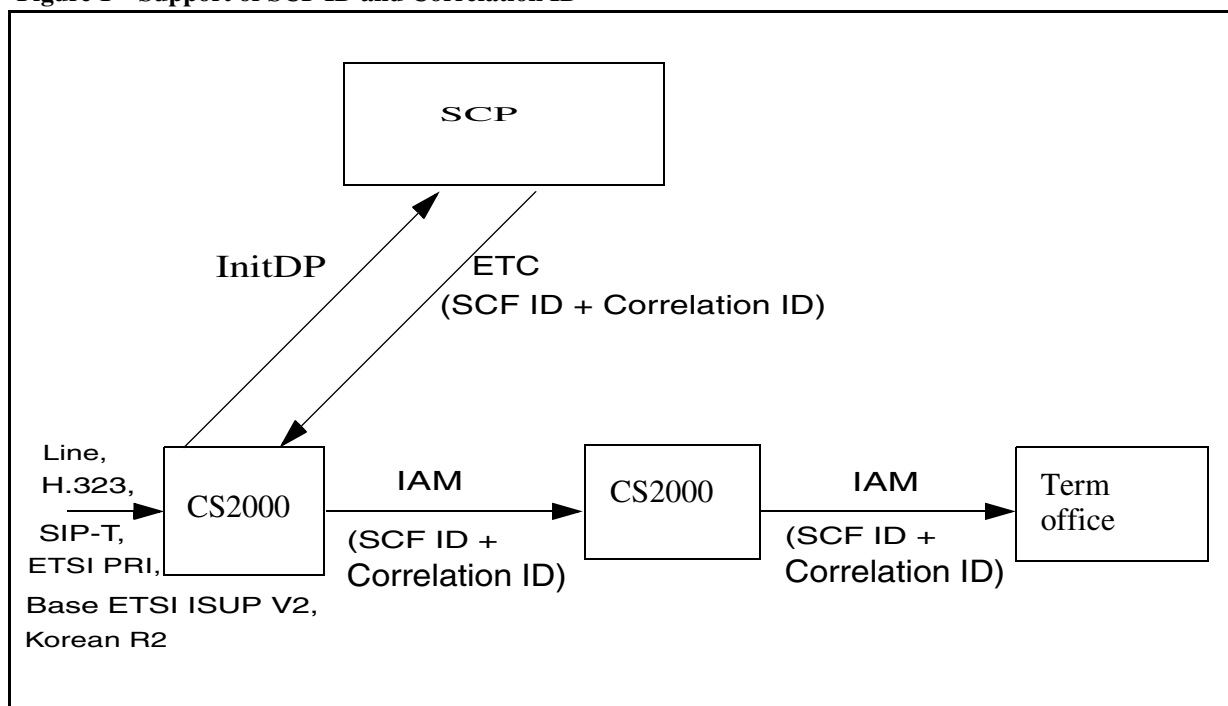
38.2.1 Support of SCF ID and Correlation ID parameters

SCF ID and Correlation ID parameters are sent from SCP to CS2000 in the ETC operation. These parameters are mapped to the SCF ID (#66) and Correlation ID (#65) parameters in the outgoing IAM message as an additional optional parameter (Please refer to Figure 1, "Support of SCF ID and Correlation ID").

Mapping of the SCF ID and Correlation ID is supported only for the switch where IN triggering is done.

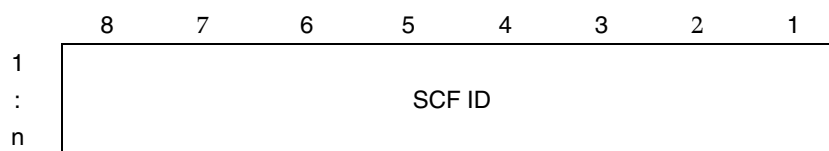
SCF ID and Correlation ID parameters in the IAM message are tandemed only for Base ETSI ISUP V2 to Base ETSI ISUP V2 interworking.

Figure 1 Support of SCF ID and Correlation ID



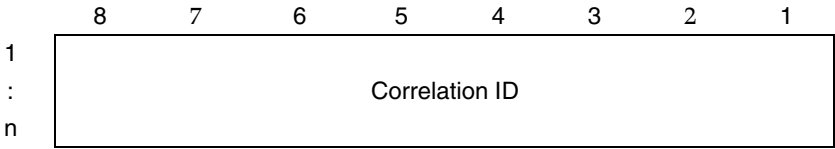
The format of the SCF ID parameter field is shown in Figure 2, "SCF ID parameter field".

Figure 2 SCF ID parameter field



The format of the Correlation ID parameter field is shown in Figure 3, "Correlation ID parameter field".

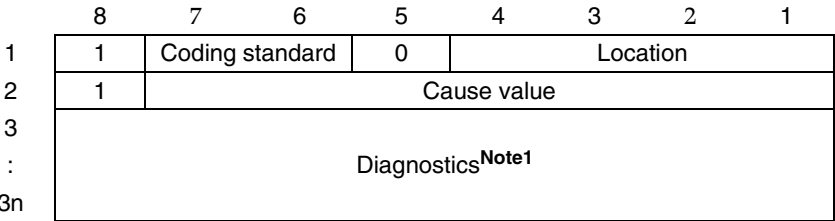
Figure 3 Correlation ID parameter field



38.2.2 Number Portability by QoR

In the number portability by QoR, if the called number is ported out, then a REL message with a specific cause value 14 (Ported Number) is received. The format of the cause indicator parameter field is shown in Figure 4, "Cause indicator parameter field".

Figure 4 Cause indicator parameter field



Note1 Diagnostics field may be omitted depending on the cause value. If the cause value is “ported number”, 1-octet diagnostics field is included.

The following codes are used in the cause indicators parameter field:

- Cause Value:

Following cause value is added to the codes defined in ITU-T Recommendation Q.850.

Description	7 6 5 4 3 2 1
Ported Number	0 0 0 1 1 1 0

- Diagnostics:

Description	8 7 6 5	4 3 2 1
No indication	0000	0000
Ported within the network (Location portability)	0000	0001
Ported between networks (Service provider portability)	0000	0010
Ported between networks (in the intelligent network)	0000	0011
Spare: by portability type	~~~~	~~~~
Unsubscribed after being ported	0001	0001

Ported number that has been routed in a wrong way ^{Note1}	0 0 0 1	0 0 1 0
Spare : Abnormal portability	~~~~	~~~~

Note1 This is when the called party is found not to subscribe the service in the destination network after number portability query is made. This is because number portability database of the originating network and the data of the destination network provider are not matching each other; therefore the data needs to be corrected to solve this cause.

If the cause value is “ported number”, 1-octet diagnostics field can be included. However, if this diagnostics field is not included, the field is considered as “no indication”.

If the REL message with cause value 14 has more than 1 octet diagnostics fields, this REL message is handled as if diagnostics is >#10.

Processing of received REL message with cause value 14 is different in the originating exchange and intermediate exchange.

Processing of REL message in the intermediate exchange is given in Figure 5, "Processing of REL message in the intermediate exchange" and Table 3, “Operation in intermediate exchange,” on page 539.

Figure 5 Processing of REL message in the intermediate exchange

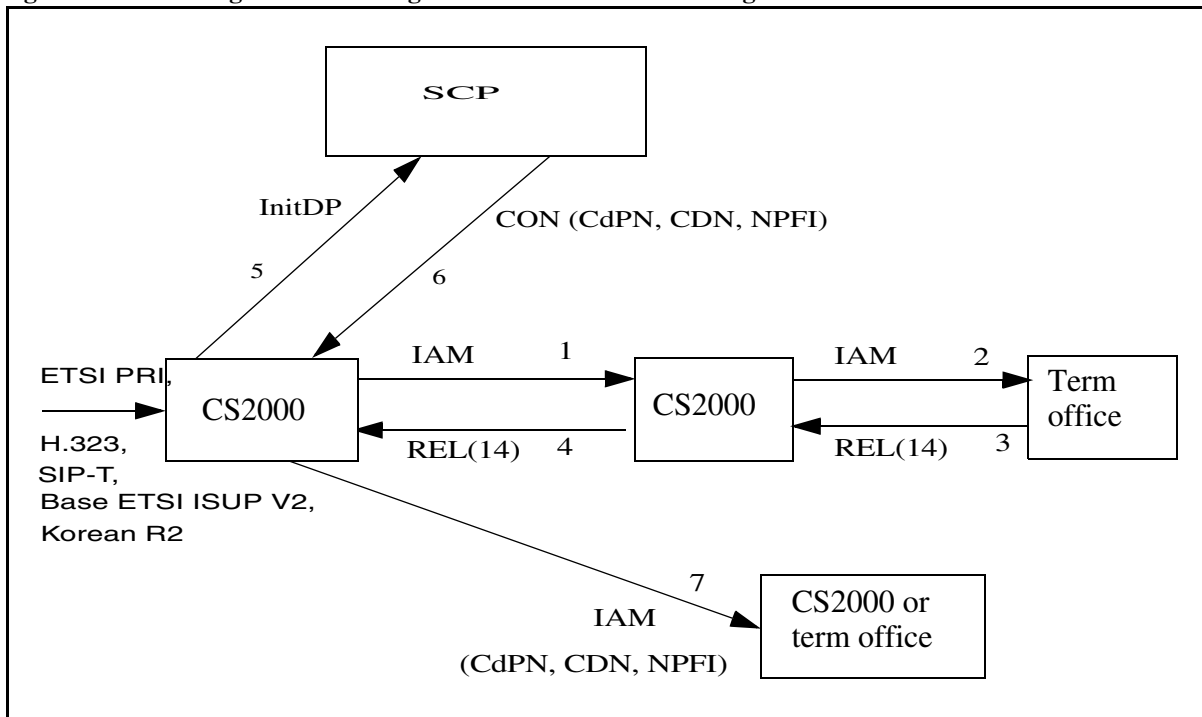


Table 3 Operation in intermediate exchange

Inputted REL		Functions of intermediate exchange	Outputted REL message		Outputted IAM message		
Cause value	Diagnostics	QoR	Cause value	Diagnostics	CdPN	CDN	NPFI
14	>= #10	*	(=)	(=)	n.a.	n.a.	n.a.
14	<#10	Not perform	(=)	(=)	n.a.	n.a.	n.a.
14	<#10	Perform/Succeeded	n.a.	n.a.	RN	DN	0x03

* : Any value. Or, don't care

(=) : Parameter pass

n.a. : Not applied

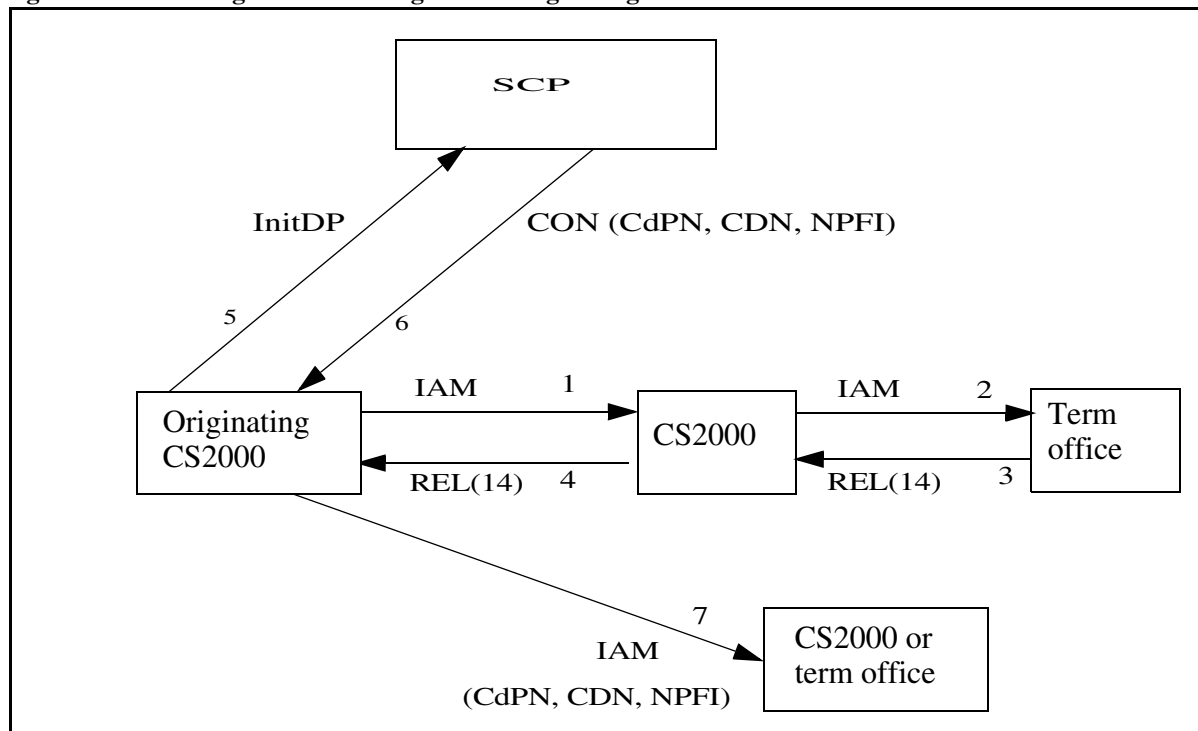
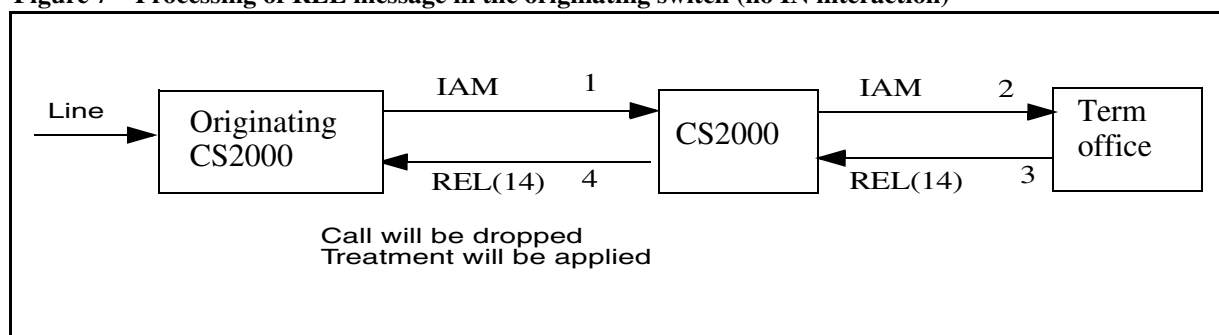
If the cause value of incoming REL message is ported number (14) and diagnostics is #10 or higher (abnormal number portability), REL message is directly passed to the preceding switching system.

If the cause value of inputted REL message is ported number (14) and diagnostics is lower than #10 (normal number portability):

- If the transit switch has not performed number portability query (i.e. transit switch has no IN interaction), REL message is directly passed to the preceding switching system.
- If the transit switch successfully sends the number portability query (i.e. transit switch has IN interaction), SCP returns the Called Party Number, CDN and NPFI in Connect operation. According to that received connect operation, IAM message is created and sent to the destination switch. CdPN, CDN and NPFI which are received from SCP are mapped to the Called Party Number (CdPN), Called Directory Number (CDN) and Number Portability Forward Information (NPFI) parameters respectively in outgoing IAM message.

Sending of number portability query to SCP by triggering IN, and receiving and storing the CdPN, CDN and NPFI parameters are handled by activity A00007793.

Processing of REL message in the originating switch is given in Figure 6, "Processing of REL message in the originating switch", Figure 7, "Processing of REL message in the originating switch (no IN interaction)" and Table 4, "Operation in the originating switch," on page 540.

Figure 6 Processing of REL message in the originating switch**Figure 7 Processing of REL message in the originating switch (no IN interaction)****Table 4 Operation in the originating switch**

Inputted REL		Functions of originating exchange	Call termination	IAM message output		
Cause value	Diagnostics	QoR		CdPN	CDN	NPFI
14	>= #10	*	Process based on the inputted cause value	n.a.	n.a.	n.a.

Table 4 Operation in the originating switch

14	<#10	Not perform	Process based on the cause value #1F	n.a.	n.a.	n.a.
14	<#10	Perform/Succeeded	n.a.	RN	DN	0x03

* : Any value. Or, don't care

n.a. : Not applied

If the cause value of inputted REL message is ported number (14) and diagnostics is #10 or higher (abnormal number portability), the existing call termination procedure is performed.

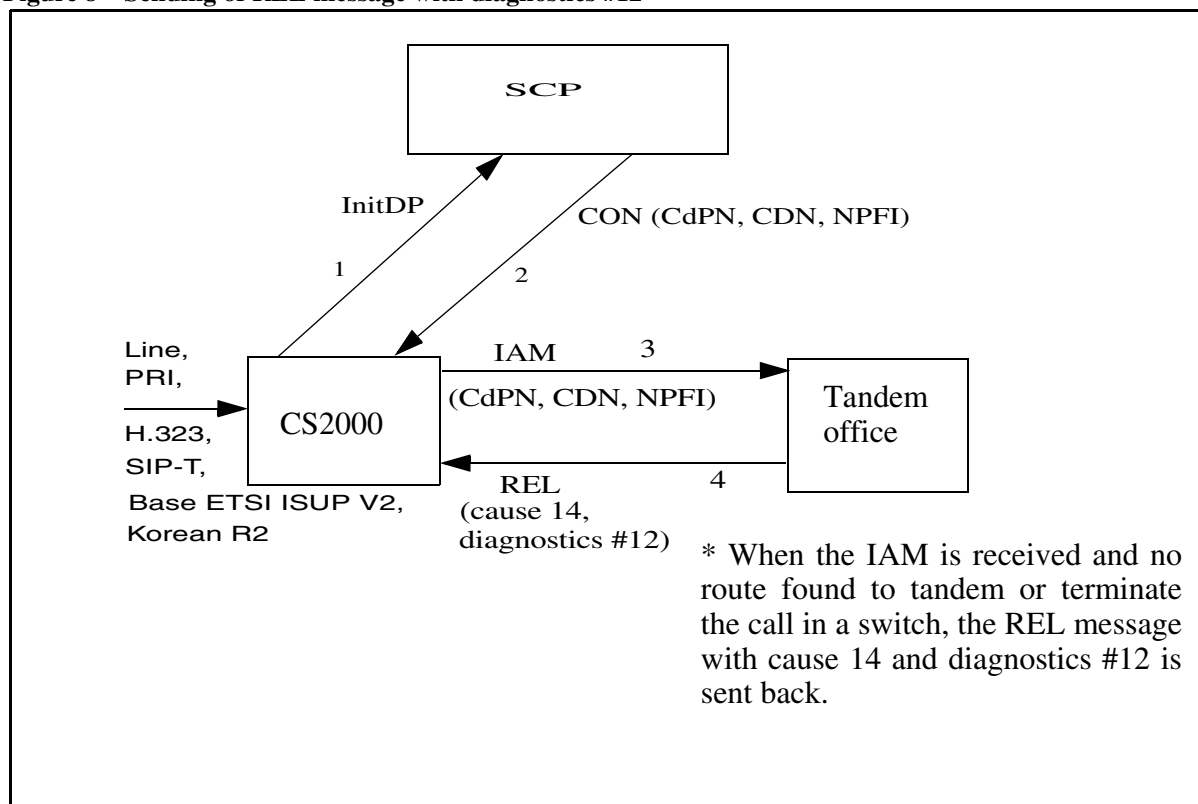
If the cause value of inputted REL message is ported number (14) and diagnostics is lower than #10 (normal number portability):

- If the originating switch does not include QoR capability (i.e. originating switch has no IN interaction), it terminates the call based on the cause value "normal - not defined (#1F)" (Please refer to Figure 7, "Processing of REL message in the originating switch (no IN interaction)").
- If the originating switch successfully sends the number portability query (i.e. originating switch has IN interaction), SCP returns the Called Party Number, Called Directory Number and Number Portability Forward Information in Connect operation. IAM message is created and then sent to the destination switch. CdPN, CDN and NPFI which are received from SCP are mapped to the Called Party Number (CdPN), Called Directory Number (CDN) and Number Portability Forward Information (NPFI) parameters respectively in outgoing IAM message.

Sending of number portability query to SCP by triggering IN, and receiving and storing the CdPN, CDN and NPFI parameters are handled by activity A00007793.

Tandeming of CDN and NPFI parameters: The new IAM message with the additional optional parameters CDN and NPFI is tandemed only for Base ETSI ISUP V2 to Base ETSI ISUP V2 interworking.

When this new IAM with CDN and NPFI parameters is received by a switch and the call cannot be routed in a tandem or terminating office (i.e. CdPN is a vacant code), the REL message with cause value 14 (ported number) and diagnostics #12 (ported number that has been routed in a wrong way) is sent to the preceding office. This behavior is specific only for Korean network. So, this is enabled by datafilling the new service 'MARKET' as 'KOREA' in table ISUP SVC. Please refer to Section 38.2.3 on page 545

Figure 8 Sending of REL message with diagnostics #12

Parameter format and codes of the Called party number, Called directory number and Number portability forward information are given in the sections below.

38.2.2.1 Called Party Number (CdPN)

Called Party Number (#04) is information to identify the called party to route the call to the terminating switch. In an environment where number portability is supported, the CdPN can function as the RN (routing number).

The format of the called party number parameter field is shown in Figure 9, "Called party number parameter field".

Figure 9 Called party number parameter field

	8	7	6	5	4	3	2	1
1	Odd/ even	Nature of address indicator						
2	INN	Numbering plan Ind.			Spare			
3	2nd address signal				1st address signal			
:	...							
n	Filler (if necessary)				nth address signal			

The following codes are used in the subfields of the called party number parameter field:

- *Nature of address indicator:*

Description	7 6 5 4 3 2 1
Spare	0 0 0 0 0 0 0
Subscriber number (for national use)	0 0 0 0 0 0 1
Not confirmed (for national use)	0 0 0 0 0 1 0
Domestic (Particular) number	0 0 0 0 0 1 1
International number	0 0 0 0 1 0 0
Particular network number (for national use)	0 0 0 0 1 0 1
RN of the domestic (particular) number format (for national use)	0 0 0 0 1 1 0
Spare	0 0 0 0 1 1 1 to 1 1 0 1 1 1 1
Reserved for national use	1 1 1 0 0 0 0 to 1 1 1 1 1 1 0
Spare	1 1 1 1 1 1 1

If CdPN functions as RN, “0000110” is used for the NOA. This NOA value is not supported in the existing behavior of the Base ETSI ISUP V2. With this activity, this value is going to be supported in the Base ETSI ISUP V2, if the new service ‘ADDRESSING_METHOD’ in table ISUPSVC is datafilled as ‘SEPERATE_DIRECTORY_NUMBER’. Please refer to Section 38.2.4 on page 546. Please note that, when the routing number is received from the SCP, the SSP will change the NOA value of the called party number as #06 in activity A00007793.

- Internal network number indicator (INN):

Not used. Coded into “0” (This value is also set by the activity A00007793).

38.2.2.2 Called Directory Number (CDN)

Called Directory Number (#7D) is information to identify the ported phone number. In other words, CDN sends the Directory Number (DN). The DN is allocated to the subscriber for the call service within the national telephone number system, and generally includes the area code.

The format of the called directory number parameter field is shown in Figure 10, "Called directory number parameter field".

Figure 10 Called directory number parameter field

8	7	6	5	4	3	2	1

1	Odd/ even	Nature of address indicator	
2	INN	Numbering plan Ind.	Spare
3	2nd address signal		1st address signal
:	...		
n	Filler (if necessary)		nth address signal

The following codes are used in the subfields of the called directory number parameter field:

- *Nature of address indicator:*

Description	7 6 5 4 3 2 1
Spare	0 0 0 0 0 0 0
Subscriber number (for national use)	0 0 0 0 0 0 1
Not confirmed (for national use)	0 0 0 0 0 1 0
Domestic (Particular) number	0 0 0 0 0 1 1
Reserved	0 0 0 0 1 0 0
RN of the domestic (particular) number format (for national use)	0 0 0 0 1 1 0
Spare	0 0 0 0 1 1 1 to 1 1 0 1 1 1 1
Reserved for national use	1 1 1 0 0 0 0 to 1 1 1 1 1 1 0
Spare	1 1 1 1 1 1 1

“0000011” is used for NOA of the CDN. This value is also set by activity A00007793.

- Internal network number indicator (INN):

Not used. Coded into “0” (This value is also set by the activity A00007793).

38.2.2.3 Number Portability Forward Information (NPFI)

Number Portability Forward Information (#8D) is information sent forward for number portability processing.

The format of the number portability forward information parameter field is shown in Figure 11, "Number Portability Forward Information parameter field".

Figure 11 Number Portability Forward Information parameter field

8	7	6	5	4	3	2	1
Ext.	Spare			NP status indicator			

The following codes are used in the subfields of the number portability forward information parameter field:

- *Extension indicator:*
 - 0 information continues in the next octet
 - 1 last octet
- *NP Status Indicator (NPSI):*

Description	4 3 2 1
No indication	0 0 0 0
NP query has not been made for the called number	0 0 0 1
NP query has been made, and the called subscriber has not been ported	0 0 1 0
NP query has been made, and the called subscriber has been ported	0 0 1 1
Spare	~

In QoR of this standard, only “0011” is actually (normally) used while other codes are not used.

The NPFI parameter is added to the outgoing IAM message by using the stored NPFI octet by CS2000 SSP. It is SSPs responsibility to send the parameter in the correct length.

38.2.3 Controlling of the Korean specific message handlings

If the incoming IAM message contains CdPN, CDN and NPFI parameters and the call cannot be routed to a tandem or terminating office (i.e. the called number is a vacant code), the REL message with cause value 14 and diagnostics #12 is sent to the preceding office. This behavior is specific to the Korean network. Not to break the existing behavior of the Base ETSI ISUP V2, this functionality is handled only for the Korean network specifically by datafilling the new service ‘MARKET’ as ‘KOREA’ in table ISUPSVC. This new service controls what behavior will be in effect for the call.

The new service ‘MARKET’ in table ISUPSVC must be datafilled with the new option KOREA for all Base ETSI ISUP V2 trunks that support the number portability in the Korean network. The datafilled option specifies what market behavior is supported on that trunk.

- KOREA - Handling of the incoming messages is done according to Korean specification.

Lack of the MARKET service or another option than KOREA indicates the existing handling of the incoming messages is in effect.

ISUPSVC options can be assigned to ISUP trunk groups in 2 ways:

- In the “default” tuple for all trunks of a particular ISUP protocol variant type by entering the option in the default ISUP SVC tuple keyed by the protocol variant.
- On a per trunk group basis.

This is done by adding an option ISUP SVC containing the key field of an ISUP SVC tuple to be used by that trunk group in table TRKOPTS. The MARKET service is then added to the specified tuple in ISUP SVC. A TRKOPTS specified tuple overrides the “default” tuple keyed by the protocol variant of the trunk.

Please find the datafill of the new service to enable the incoming message handling according to the Korean specification in Figure 12, "Example 'MARKET' service datafill in Table ISUP SVC". Also, Figure 8, "Example datafill for the new DACOM CorrelationID option in table SERVINFO" shows assigning ISUP SVC to the trunk.

Figure 12 Example 'MARKET' service datafill in Table ISUP SVC

TABLE: ISUP SVC	
KEY	SERVICE

TEST1 (MARKET	(KOREA)\$)\$
BASE_EIV2 (MARKET	(KOREA)\$)\$

Figure 13 Example datafill in Table TRKOPTS

TABLE: TRKOPTS			
>LIS			
	OPTKEY	OPTINFO	

OGISUPAB	ISUP SVC	ISUP SVC	TEST1
OGISUPBC	ISUP SVC	ISUP SVC	BASE_EIV2

38.2.4 Supporting of the NOA value #06

If SCP sends the routing number in CdPN, the NOA value of the called party number is set as #06 by the CS2000 SSP in activity A00007793. During building of the outgoing IAM message, this NOA value is used. Also the called party number which includes the NOA value #06 is tandemed for Base ETSI ISUP V2 to Base ETSI ISUP V2 interworking.

In the existing behavior of Base ETSI ISUP V2, the NOA value #06 is not supported and the call is dropped when this value is received in the incoming IAM message. To support the NOA value #06, the new service ADDRESSING_METHOD must be datafilled in table ISUPSVC. This new service enables/disables the supporting of the NOA value #06.

The new service 'ADDRESSING_METHOD' must be datafilled with the option SEPERATE_DIRECTORY_NUMBER for all Base ETSI ISUP V2 trunks that support the number portability in the Korean network. The datafilled option specifies what level of ADDRESSING_METHOD is supported on that trunk.

- SEPERATE_DIRECTORY_NUMBER - the Separate Directory Number Addressing method is used. In this method, the routing number is transferred in the Called Party Number parameter and directory number is transferred in the Called Directory Number parameter. The CdPN is coded with NOA value 0000110 (#06).

Lack of the ADDRESSING_METHOD service or another option than SEPERATE_DIRECTORY_NUMBER indicates that NOA value #06 is not supported.

ISUPSVC options can be assigned to ISUP trunk groups in 2 ways:

- In the "default" tuple for all trunks of a particular ISUP protocol variant type by entering the option in the default ISUPSVC tuple keyed by the protocol variant.
- On a per trunk group basis.

This is done by adding an option ISUPSVC containing the key field to an ISUPSVC tuple to be used by that trunk group in table TRKOPTS. The ADDRESSING_METHOD service is then added to the specified tuple in ISUPSVC. A TRKOPTS specified tuple overrides the "default" tuple keyed by the protocol variant of the trunk.

Please find the datafill of the new service to support NOA value #06 in Figure 14, "Example 'ADDRESSING_METHOD' service datafill in Table ISUPSVC". Also, Figure 15, "Example datafill in Table TRKOPTS" shows assigning ISUPSVC to the trunk.

Figure 14 Example 'ADDRESSING_METHOD' service datafill in Table ISUP SVC

TABLE: ISUP SVC	
KEY	SERVICE

TEST2	(ADDRESSING_METHOD (SEPERATE_DIRECTORY_NUMBER)\$)\$
BASE_EIV2	(ADDRESSING_METHOD (SEPERATE_DIRECTORY_NUMBER)\$)\$

Figure 15 Example datafill in Table TRKOPTS

TABLE: TRKOPTS			
>LIS			
	OPTKEY	OPTINFO	

OGISUPAB	ISUP SVC	ISUP SVC	TEST2
OGISUPBC	ISUP SVC	ISUP SVC	BASE_EIV2

38.3 Hardware Requirements or Dependencies

This activity is supported only on the Gateway Controller (GWC) in International trunks load (GI).

38.4 Software Requirements or Dependencies

None

38.5 Limitations and restrictions

None

38.6 Interactions

None

38.7 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

Performance (includes operational measurements)N/A

38.8 Glossary

Table 5

Term	Description
CS2000	Call Server 2000
CdPN	Called Party Number
CDN	Called Directory Number
ETC	Establish Temporary Connection
ETSI	European Telecommunications Standards Institute
GWC	Gateway Controller
IAM	Initial Address Message
IN	Intelligent Network
ISUP	ISDN User Part
NOA	Nature of Address
NPFI	Number Portability Forward Information
QoR	Query on Release
REL	RELease message
SCP	Service Control Point
SSP	Service Switching Point

38.9 Recommended Reading/References

- a. ISUP Protocol Standard for 2G Mobile Number Portability by QoR
- b. Dacom RFP Feature Support Analysis

- c. Dacom INAP 350632-1204
- d. A00007793: SCF ID, correlation ID and QoR Base LNP Support for Dacom IN
- e. ITU-T Recommendation Q763: Signalling System No.7 - ISDN User Part Formats and Codes
- f. ITU-T Recommendation Q769.1: Signalling System No.7 - ISDN User Part enhancements for the support of number portability
- g. A59027497: LNP Query on Release - Non IN
- h. A00007405: Korean R2 on the GWC

39: A00007864 Functional description (FN)

39.1 Feature name

Pakistan ISUP tandeming on CS2Kc

39.2 Description

This activity introduces Pakistan ISUP and provides Pakistan ISUP to Pakistan ISUP interworking on CS2Kc as part of ISN08 IP side functionality.

Pakistan ISUP is implemented as a national ISUP variant of ETSI ISUP V2 conforming to the Pakistan ISUP specification (CCS0101/0103/0104/0105¹).

This activity also provides the functionalities of Charge Determination Point for Pakistan ISUP.

39.2.1 Functional Overview

This activity introduces Pakistan ISUP on ISN08, provides handling of messages, parameters and supports Pakistan ISUP to Pakistan ISUP interworking as well as NAOC CDP charge function.

39.2.1.1 Functional Requirements

Functional requirements for this activity are described by the following documents:

1. CCS0101, General Aspects of CCS NO.7 Signalling for the National Network of Pakistan, issue1.0, Date 22.01.1996
2. CCS0103, ISUP Specification for National and International Interconnections, issue1.0, Date 22.01.1996
3. CCS0104, National ISUP Messages and Parameters for Specific Functions of the National Network of Pakistan, issue1.1, Date 22.01.1996
4. CCS0105, ISUP Specification for the National Network of Pakistan Special Procedures and Representative Message Flow Diagrams, issue 1.1, Date 22.01.1996

39.2.1.2 Pakistan ISUP Datafill

To provide Pakistan ISUP, the datafill in table TRKSGRP shown in the example below is necessary:

‘100_WHITE’ indicates that the ISUP variant is based on ITU white book (ETSI ISUP V2) or later version specifications and ‘PAKISTAN’ marks the country specific variant based on 100_WHITE.

¹CCS0101/0103/0104/0105 are Pakistan ISUP specifications.

39.2.1.3 Protocol Messages and Parameters

Table 1, “Supported Pakistan ISUP Messages”, on page 552 represents the set of messages that are required by Pakistan ISUP variant.

Table 2, “Supported Pakistan ISUP parameters”, on page 553 represents the set of parameters that are required by Pakistan ISUP variant.

The highlighted messages and parameters are Pakistan national messages and parameters.

Table 1 Supported Pakistan ISUP Messages

Message Type	Bin Code	Hex Code
Address complete	00000110	06
Answer	00001001	09
Blocking	00010011	13
Blocking acknowledgement	00010101	15
Call progress	00101100	2C
Circuit group blocking	00011000	18
Circuit group blocking acknowledgement	00011010	1A
Circuit group reset	00010111	17
Circuit group reset acknowledgement	00101001	29
Circuit group unblocking	00011001	19
Circuit group unblocking acknowledgement	00011011	1B
Charge information	00110001	31
Connect	00000111	07
Continuity	00000101	05
Continuity check request	00010001	11
Forward transfer	00001000	08
Information	00000100	04
Information request	00000011	03
Initial address	00000001	01
Release	00001100	0C
Release complete	00010000	10
Reset circuit	00010010	12
Resume	00001110	0E
Subsequent address	00000010	02
Suspend	00001101	0D
Unblocking	00010100	14
Unblocking acknowledgement	00010110	16
Identification	11111110	FE
On Hook	11111100	FC
End of Hold	11111101	FD

Table 1 Supported Pakistan ISUP Messages

Trunk Offer	11111111	FF

Table 2 Supported Pakistan ISUP parameters

Parameter Name	Code	Hex Code
Access transport	00000011	03
Automatic congestion level	00100111	27
Backward call indicators	00010001	11
Call Diversion Information	00110110	36
Called party number	00000100	04
Calling party number	00001010	0A
Calling party's category	00001001	09
Cause indicators	00010010	12
Circuit group supervision message type indicator	00010101	15
Closed user group interlock code	00011010	1A
Connected number	00100001	21
Continuity indicators	00010000	10
End of optional parameters	00000000	00
Event information	00100100	24
Forward call indicators	00000111	07
Generic Digits	11000001	C1
Generic Notification Indicator	00101100	2C
Generic Number	11000000	C0
Information indicators	00001111	0F
Information request indicators	00001110	0E
Nature of connection indicators	00000110	06
National forward call indicators	11111101	FD
Optional backward call indicators	00101001	29
Optional forward call indicators	00001000	08
Original called number	00101000	28
Range and status	00010110	16
Redirecting number	00001011	0B
Redirection information	00010011	13
Subsequent number	00000101	05
Suspend/Resume indicators	00100010	22
Transmission medium requirement	00000010	02
User service information	00011101	1D
User-to-user indicators	00101010	2A
User-to-user information	00100000	20

Table 2 Supported Pakistan ISUP parameters

Charge Band Number	11111111	FF
Number of Charging Units	11111110	FE

39.2.2 ISUP Messages and Parameters Supported for Pakistan ISUP

39.2.2.1 Address Complete (ACM)

The format of ACM message in Pakistan network is indicated in Table 3, “Supported Parameters (Message type: Address complete)”, on page 554. The parameters changed by this activity are highlighted.

Table 3 Supported Parameters (Message type: Address complete)

Parameter Name	Type	Length (Octet)
Message type	F	1
Backward call indicators	F	1
Optional backward call indicators	O	3
Cause indicators	O	4
User-to-user indicators	O	3
User-to-user information	O	3-131
Access transport	O	3-?
Generic Notification Indicator	O	3
End of optional parameters	O	1

The functionality of ACM message is defined in Pakistan specifications, with the following implementation:

- Call Diversion Indicator field in Optional Backward Call Indicator parameter of ACM and CPG. And only value 1 (Call Diversion Forwarding May Occur) is used. If the value is 0, it is changed to 1 in the outgoing message. Please refer to Table 4, “Optional Backward Call Indicator”, on page 554.

Table 4 Optional Backward Call Indicator

OBCI	H G F E D C B A
Call Diversion Indicator	1

- The supported values of Generic Notification Indicator are defined in Table 5, “Supported Values of Notification Indicator field”, on page 555. If a value not listed below is received in this field, the parameter is

discarded.

Table 5 Supported Values of Notification Indicator field

Notification indicator	H G F E D C B A
Call is Waiting Call	1 1 0 0 0 0 0
Remote Hold	1 1 1 1 0 0 1
Call is diverting	1 1 1 1 0 1 1

39.2.2.2 Answer (ANM)

The format of ANM message in Pakistan network is indicated as Table 6, “Supported Parameters (Message type: Answer)”, on page 555. The parameters changed by this activity are highlighted.

Table 6 Supported Parameters (Message type: Answer)

Parameter Name	Type	Length (Octet)
Message type	F	1
Backward call indicators	O	4
User-to-user information	O	3-131
Connected number	O	4-12
Access transport	O	3-?
Generic Number	O	4-12
Generic Notification Indicator	O	3
End of optional parameters	O	1

The functionality of ANM message is defined in Pakistan specifications, with the following implementation:

- In Generic Number Parameter, the supported values of Number Qualifier Indicator field are defined in Table 7, “Supported Values of Number Qualifier Indicator field”, on page 555. If a value not listed below is received in this field, the parameter is discarded.

Table 7 Supported Values of Number Qualifier Indicator field

Number Qualifier Indicator	H G F E D C B A
Additional Connected Number	0 0 0 0 0 1 0 1
Additional Calling Party Number	0 0 0 0 0 1 1 0

- In Connected Number parameter, the supported values of Nature of Address field are defined in Table 8, “Supported Values of Nature of Address Field”, on page 556. If a value not listed below is received in this field, the parameter is discarded.

Table 8 Supported Values of Nature of Address Field

Nature of Address	H G F E D C B A
Subscriber Number	0 0 0 0 0 0 1
National Significant Number	0 0 0 0 0 1 1

- The supported value of Generic Notification Indicator are defined in Table 5, “Supported Values of Notification Indicator field”, on page 555. Please refer to “39.2.2.1 Address Complete (ACM)” on page 554.

39.2.2.3 Call Progress (CPG)

The format of CPG message in Pakistan network is indicated in Table 9, “Supported Parameters (Message type: Call progress)”, on page 556. The parameters changed by this activity are highlighted.

Table 9 Supported Parameters (Message type: Call progress)

Parameter Name	Type	Length (Octet)
Message type	F	1
Event information	F	1
Cause indicators	O	4
Backward call indicators	O	4
Optional backward call indicators	O	3
User-to-user information	O	3-131
Access transport	O	3-?
Generic Notification Indicator	O	3
Call Diversion Information	O	3
End of optional parameters	O	1

The functionality of CPG message is defined in Pakistan specifications, with the following implementation:

- Call Diversion Indicator field in Optional Backward Call Indicator parameter of ACM and CPG. And only value 1 (Call Diversion Forwarding May Occur) is used. If the value is 0, it is changed to 1 in the outgoing message. Please refer to Table 4, “Optional Backward Call Indicator”, on page 554. Please refer to “39.2.2.1 Address Complete (ACM)” on page 554.

- The supported values of Generic Notification Indicator are defined in Table 5, “Supported Values of Notification Indicator field”, on page 555. If a value not listed below is received in this field, the parameter is discarded. Please refer to “39.2.2.1 Address Complete (ACM)” on page 554.

39.2.2.4 Connect (CON)

The format of CON message in Pakistan network is indicated in Table 10, “Supported Parameters (Message type: Connect)”, on page 557. The parameters changed by this activity are highlighted.

Table 10 Supported Parameters (Message type: Connect)

Parameter Name	Type	Length (Octet)
Message type	F	1
Backward call indicators	F	2
Connected number	O	4-12
User-to-user indicators	O	3
User-to-user information	O	3-131
Access transport	O	3-?
Generic number	O	4-12
Generic Notification Indicator	O	3
End of optional parameters	O	1

The functionality of CON message is defined in Pakistan specifications, with the following implementation:

- In Generic Number Parameter, the supported values of Number Qualifier Indicator field are defined in Table 7, “Supported Values of Number Qualifier Indicator field”, on page 555. If a value not listed below is received in this field, the parameter is discarded. Please refer to “39.2.2.2 Answer (ANM)” on page 555.
- In Connected Number parameter, the supported values of Nature of Address field are defined in Table 8, “Supported Values of Nature of Address Field”, on page 556. If a value not listed below is received in this field, the parameter is discarded. Please refer to “39.2.2.2 Answer (ANM)” on page 555.
- The supported values of Generic Notification Indicator are defined in Table 5, “Supported Values of Notification Indicator field”, on page 555. If a value not listed below is received in this field, the parameter is discarded. Please refer to “39.2.2.1 Address Complete (ACM)” on page 554.

39.2.2.5 Initial Address (IAM)

The format of IAM message in Pakistan network is indicated in Table 11, “Supported Parameters (Message type: Initial address)”, on page 558. The parameters changed by this activity are highlighted.

Table 11 Supported Parameters (Message type: Initial address)

Parameter Name	Type	Length (Octet)
Message type	F	1
Nature of connection indicators	F	1
Forward call indicators	F	2
Calling party's category	F	1
Transmission medium requirement	F	1
Called party number	V	4-11
Calling party number	O	4-12
Optional forward call indicators	O	3
Redirecting number	O	4-12
Redirection information	O	3-4
Closed user group interlock code	O	6
Original called number	O	4-12
User-to-user information	O	3-131
Access transport	O	3-?
User service information	O	4-13
National forward call indication	O	3
End of optional parameters	O	1

The functionality of IAM message is defined in Pakistan specifications, with the following implementation:

- The Supported Calling Party Category in Pakistan ISUP are defined in Table 12, “Supported Calling Party Categories in Pakistan ISUP”, on page 558. The national defined CPC are highlighted. The supported CPC is tandemed without change.

Table 12 Supported Calling Party Categories in Pakistan ISUP

Calling Party Categories	HGFEDCBA	Hex	Notes
Operator, language French	0 0 0 0 0 0 0 1	01	
Operator, language English	0 0 0 0 0 0 1 0	02	
Operator, language German	0 0 0 0 0 0 1 1	03	
Operator, language Russian	0 0 0 0 0 1 0 0	04	
Operator, language Spanish	0 0 0 0 0 1 0 1	05	

Table 12 Supported Calling Party Categories in Pakistan ISUP

National operator	0 0 0 0 1 0 0 1	09	National
Ordinary calling subscriber	0 0 0 0 1 0 1 0	0A	
Calling subscriber with priority	0 0 0 0 1 0 1 1	0B	
Data call	0 0 0 0 1 1 0 0	0C	
Test call	0 0 0 0 1 1 0 1	0D	
Payphone	0 0 0 0 1 1 1 1	0F	
Maintenance line	1 1 1 0 0 0 0 0	E0	National
Multi party line	1 1 1 0 0 0 0 1	E1	National
VIP subscriber	1 1 1 0 0 0 1 0	E2	National
Charge information request	1 1 1 0 0 0 1 1	E3	National
IDS barred subscriber	1 1 1 0 0 1 0 0	E4	National
ANI- equipment trouble	1 1 1 0 0 1 0 1	E5	National

Any other values not listed above are regarded as unrecognized CPC values.

On receipt of unrecognized CPC value at tandem office over Pakistan ISUP, the CPC is mapped to a default value “ordinary subscriber” #0A.

- The Supported Nature of Address in Pakistan ISUP are defined as Table 13, “Supported Nature of Address in Pakistan ISUP”, on page 559. The supported NOA is tandemed without change.

Table 13 Supported Nature of Address in Pakistan ISUP

Nature of Address	H G F E D C B A	Supported in parameter
Subscriber Number	0 0 0 0 0 0 1	CGPN, CDPN , OCN, RGN
National Significant Number	0 0 0 0 0 1 1	CGPN, OCN, RGN

Any other values not listed above are regarded as invalid NOA value.

For CDPN, if the incoming NOA value is invalid, the ALL_NOA option in table TRKSGRP is checked. If ALL_NOA is present, the parameter is tandemed according to datafill of XXCODE tables. Otherwise, call will be released with cause value 28 (#1C).

For CGPN, OCN, RGN, if the incoming NOA value is invalid, this parameter is discarded.

- The call diversion parameters in IAM includes Original Called Number, Redirecting Number and Redirection Information. The supported values are defined in Table 14, “Supported Values of Call Diversion Parameters in IAM”, on page 559.

Table 14 Supported Values of Call Diversion Parameters in IAM

Parameter	Indicator	H G F E D C B A

Table 14 Supported Values of Call Diversion Parameters in IAM

Original called number	Numbering plan indicator	0 0 1
	Address presentation restricted	0 0
		0 1
		1 1
Redirecting number	Numbering plan indicator	0 0 1
	Address presentation restricted	0 0
		0 1
		1 1
Redirection information	Redirecting indicator	0 1 1
		1 0 0
	Original redirection reason	0 0 0 0
	Redirecting reason	0 0 0 0

Any other values not listed above are regarded as invalid value.

If the values are invalid, they are built as the value above.

- The National Forward Call Indicator in Pakistan ISUP is newly defined parameter. Please refer to “Table 15 Supported National Forward Call Indicator Field” on page 560.

Table 15 Supported National Forward Call Indicator Field

8	7	6	5	4	3	2	1
H	G	F	E	D	C	B	A

- Bit A Zoning Indicator
 - 1 Zoning Done
 - 0 Zoning Not Done
- Bit H-B Not Used, Set to “0”

Bit A should be passed unchanged. Bit H to B should be set to “0”.

39.2.2.6 Information Request and Information (INR / INF)

The format of INR / INF message in Pakistan network is indicated in Table 16, “Supported Parameters (Message type: Information request)”, on page 561

and Table 17, “Supported Parameters (Message type: Information)”, on page 561.

Table 16 Supported Parameters (Message type: Information request)

Parameter Name	Type	Length (Octet)
Message type	F	1
Information request indicators	F	2
End of optional parameters	O	1

Table 17 Supported Parameters (Message type: Information)

Parameter Name	Type	Length (Octet)
Message type	F	1
Information indicators	F	2
Calling party number	O	5-12
Calling party category	O	1
End of optional parameters	O	1

INR / INF messages are tandemed without change.

39.2.2.7 Charge (CRG)

The format of CRG message in Pakistan network is indicated in Table 18, “Supported Parameters (Message type: Charge)”, on page 561. The parameters created by this activity are highlighted.

Table 18 Supported Parameters (Message type: Charge)

Parameter Name	Type	Length (Octet)
Message type	F	1
Charge Band Number	O	3
Number of Charging Units	O	3
End of optional parameters	O	1

CRG message is sent in backward direction of accounting and call charging purposes. Please refer to “39.2.3 Charging for Pakistan ISUP” on page 564.

Charge Band Number and Number of Charge Unit parameters can be included in CRG message. They are defined in Table 19, “Supported Charge Band Number Parameter”, on page 562 and Table 20, “Supported Number of Charge Unit Parameter”, on page 562.

Table 19 Supported Charge Band Number Parameter

8	7	6	5	4	3	2	1
Charge Band Number							

The following codes shall be used in the charge band number parameter field:

000 No charge
 001-255 Charge Band Number

Table 20 Supported Number of Charge Unit Parameter

8	7	6	5	4	3	2	1
Number of charging units							

The following codes shall be used in the Number of charging units parameter field:

0 Spare
 1 Number of charging units

39.2.2.8 National Messages for Pakistan ISUP

This activity provides tandeming of 4 national messages (HOLD / ONHOOK / IDENT / TOF). These messages are used in malicious call holding and trunk offering features.

In the tandem office, only tandeming function is done in appropriate states of a call. Gateway or end office will provide the handling of these messages.

HOLD / ONHOOK / IDENT Messages for Malicious Call Holding Feature

Hold message is sent in backward direction in order to release the holding of the connection.

Table 21 Supported HOLD Message

Parameter	Code	Type	Length (Octet)
Message Type: End of Hold	11111101	F	1
End of optional parameter	00000000	O	1

ONHOOK message is sent in forward direction to inform that the call has been released by the calling party.

Table 22 Supported ONHOOK Message

Parameter	Code	Type	Length (Octet)
Message Type: On hook	11111100	F	1
End of optional parameter	00000000	O	1

IDENT message is sent in the backward direction, indicating that the malicious call data should be print out or be stored in a file.

Please refer to “39.2.4.4 HOLD / ONHOOK / IDENT Messages for Malicious Call Holding Feature” on page 569.

Table 23 Supported IDENT Message

Parameter	Code	Type	Length (Octet)
Message Type: Identification	11111110	F	1
End of optional parameter	00000000	O	1

39.2.2.8.1 TOF Message for Trunk Offering Feature

TOF is sent in forward direction indicating an operator’s request for trunk offering. This activity only provides tandem function for this message.

Table 24 Supported TOF Message

Parameter	Code	Type	Length (Octet)
Message Type: Trunk Offer Message	11111111	F	1
End of optional parameter	00000000	O	1

Please refer to “39.2.4.5 TOF Message for Trunk Offering Feature” on page 570.

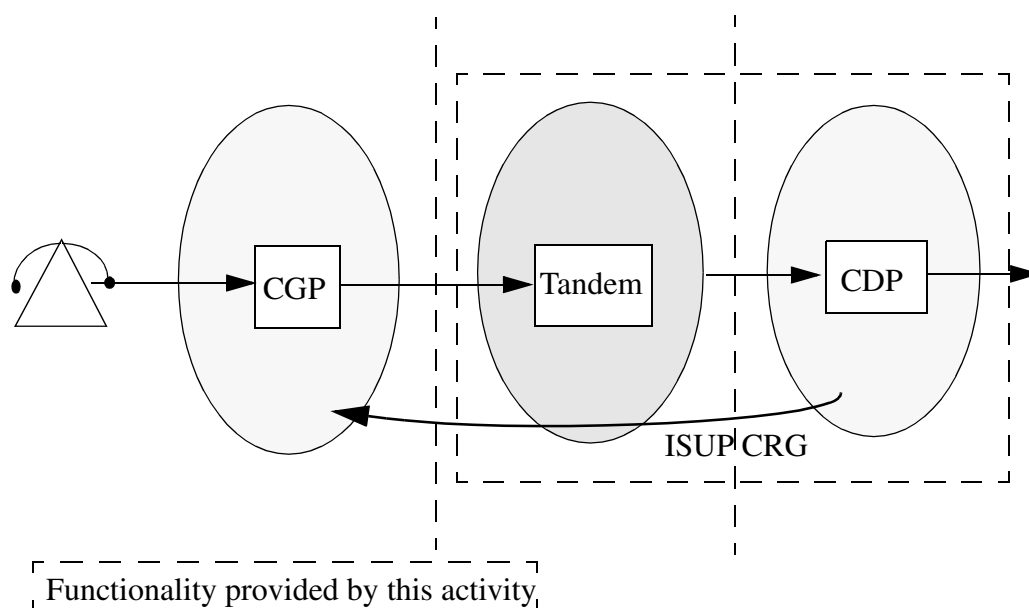
39.2.2.9 Other Messages

Other messages which are not mentioned here, please refer to Annex C of Q.767.

39.2.3 Charging for Pakistan ISUP

This activity deals with the following functionalities using NAOC framework based on the Pakistan ISUP charge requirement.

- Charge Determination Point functionality
- Charge functionality in tandem exchange

Figure 5 NAOC support for Pakistan ISUP Charging

39.2.3.1 Charge Determination Point functionality

Main function of CDP is to determine charge Band number and generation of CRG message.

If the NAOC translation is used at CDP node, the charge band number (CBN) is calculated and send in ISUP CRG message to CGP which uses this information to get the tariff information with the existing charge band table. ISUP charge message with CBN parameter is generated for all calls before ACM at the CDP node. Pakistan CRG message contains the national specific Charge Band Number Parameter. Charge Band Number Parameter contains CBN.

The calculation of CBN is done at CDP using NAOC framework. At the outgoing trunk, if NAOC datafill is found after successful translation, the TARFINDXP indices in the table TARFINDX is taken and treated as CBN. This CBN is put in the CRG message and sent to the preceding node.

The generation of the other parameter, Number of Charge Units, is not included in CDP functionality of this feature.

39.2.3.2 Charge functionality in tandem exchange

In Pakistan ISUP to Pakistan ISUP interworking, if the backward CRG message is received, the CRG is tandemed transparently in GWC with valid parameters in all stages of the call. The CRG message is not reported to CORE to do metering.

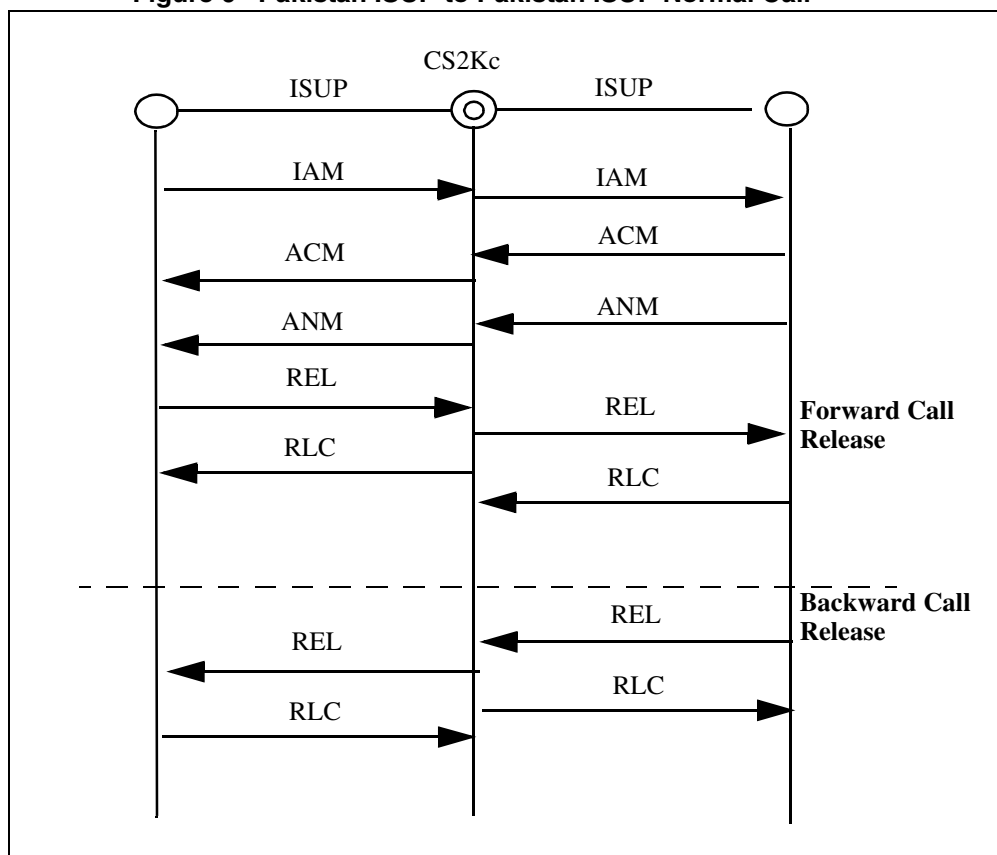
39.2.3.3 NAOC datafill

CDP datafill is done by entering the keyword NAOC in the translation. For the datafill details, please refer to NAOC or Indian ISUP document. This activity uses the existing NAOC datafill structure.

39.2.4 Call Scenarios

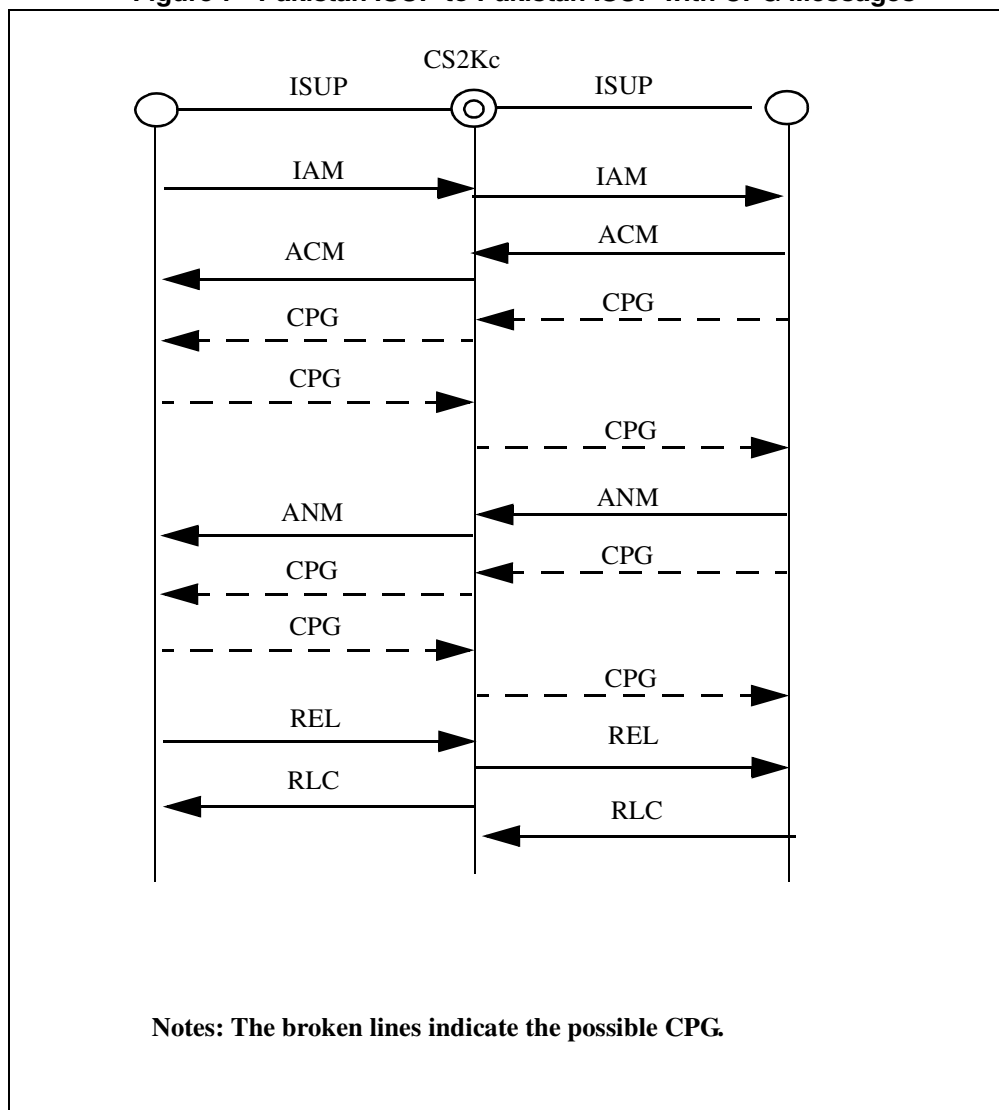
39.2.4.1 Normal Call Scenario

Figure 6 Pakistan ISUP to Pakistan ISUP Normal Call



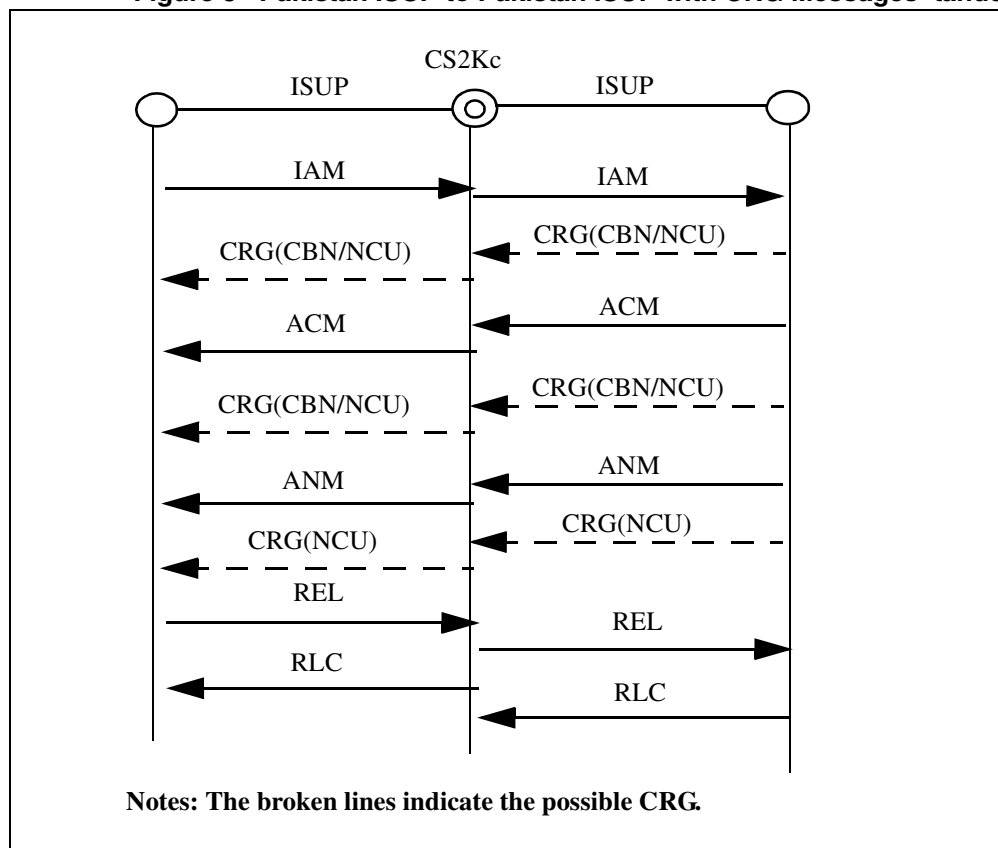
39.2.4.2 Call Scenario with CPG message

Figure 7 Pakistan ISUP to Pakistan ISUP with CPG Messages



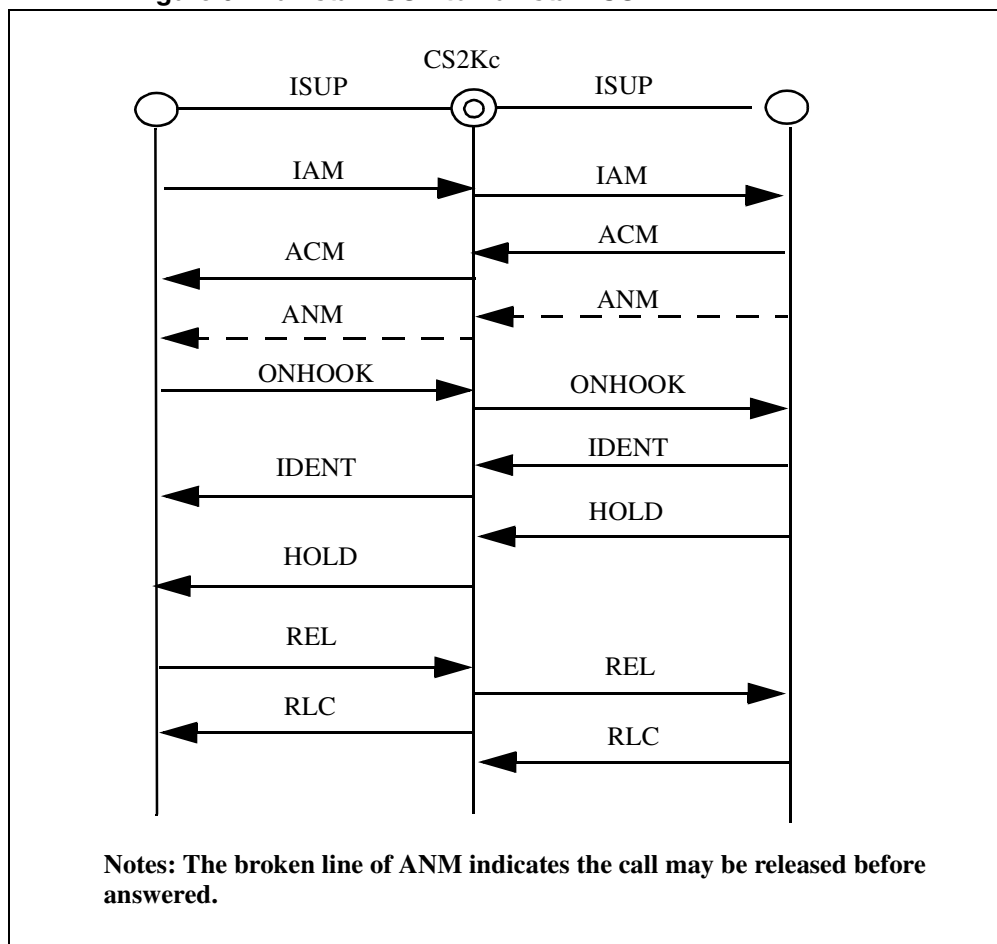
39.2.4.3 Call Scenario with CRG messages

Figure 8 Pakistan ISUP to Pakistan ISUP with CRG Messages' tandem



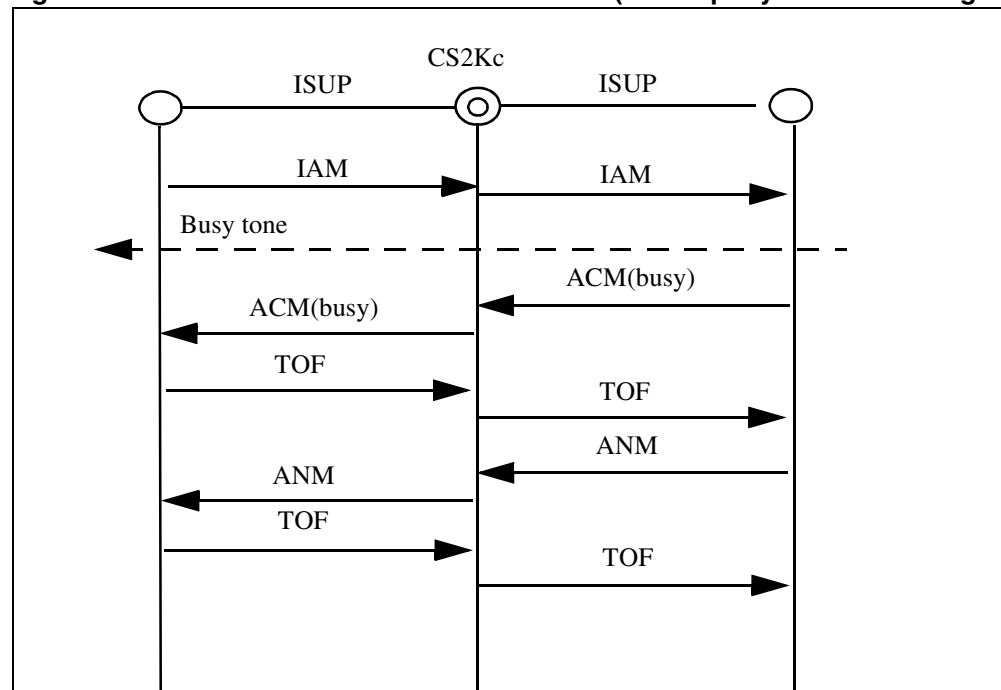
39.2.4.4 HOLD / ONHOOK / IDENT Messages for Malicious Call Holding Feature

Figure 9 Pakistan ISUP to Pakistan ISUP

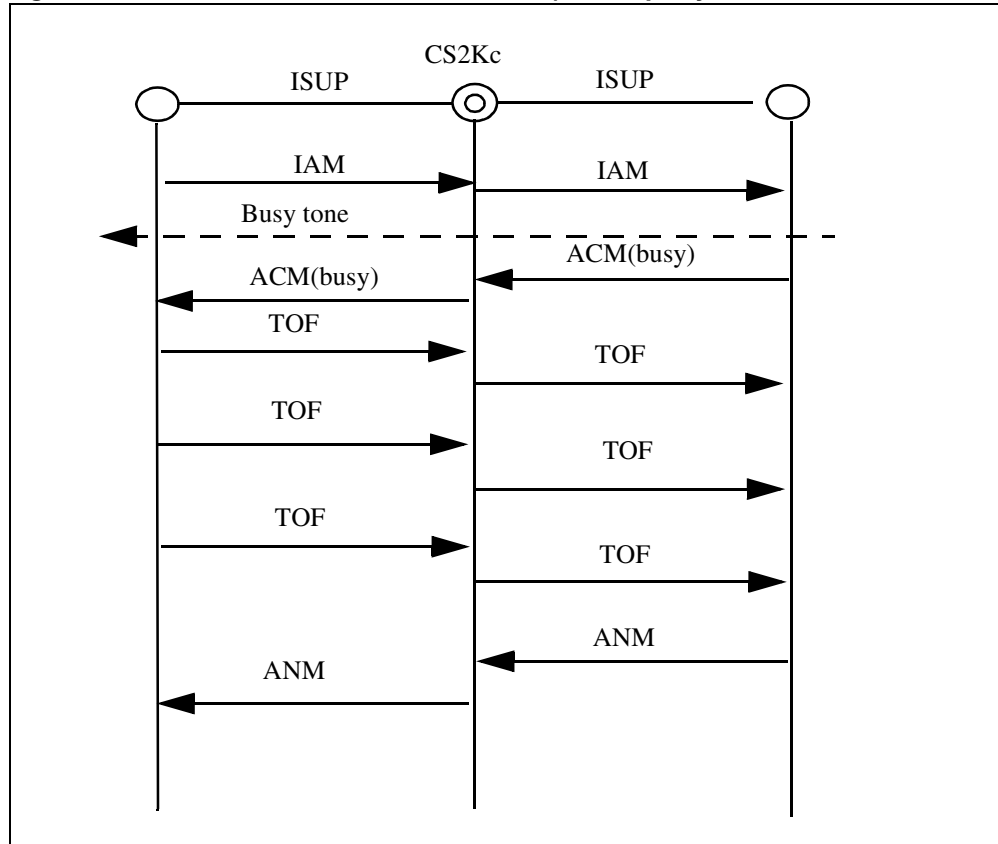


39.2.4.5 TOF Message for Trunk Offering Feature

Figure 10 Pakistan ISUP to Pakistan ISUP with (Called party on hook during trunk



offering)

Figure 11 Pakistan ISUP to Pakistan ISUP (Called party answer after trunk offering)

39.3 Hardware Requirements or Dependencies

Not applicable.

39.4 Software Requirements or Dependencies

This activity requires the following features to be activated by SOC:

- **NETK0019** Network AOC
- **NETK0024** Network AOC Tariff

NAOC tariff information is required, since this activity reuses the **NAOC** functionality. NAOC datafill including the NAOC tables and translation options have to be set up in a appropriate way.

39.5 Limitations and restrictions

- CRG message with NCU parameter can only be tandemed from Pakistan ISUP trunk to Pakistan ISUP trunk in this feature and no special handling is provided.

- National messages can only be tandemed from Pakistan ISUP trunk to Pakistan ISUP trunk. The generation and handling of these messages are not supported by this activity.
- INR / INF are tandemed unchanged.
- Handling not described in FN is conformed to that of ETSI ISUP V2.
- The same limitation as ETSI ISUP V2.

39.6 Interactions

Not applicable.

39.7 Glossary

Term	Description
CBN	Charge Band Number
CCITT	International Telegraph and Telephone Consultative Committee
CDP	Charge Determination Point
CDPN	Called Party Number
CGP	Charge Generation Point
CGPN	Calling Party Number
CM	Computing Module
CPC	Calling Party Category
DRU	Delivery Release Unit
ISUP	ISDN User Part
MCI	Message Compatibility Information
NAOC	Network Advice Of Charge
NCU	Number of Charge Unit
NOA	Nature of Address
OCN	Origin Called Number
PCI	Parameter Compatibility Information
RGN	Redirecting Number

Configuration Management (CN) List

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
A00005315	Calling Number Delivery for PRI, ISUP & CS-1
A00005962	CLIR Removal For Centrex Intragroup Calls
A00005980	GSP IN CONNECT Operation Enhancement to support RouteList Parameter
A00005981	GSP IN InitDP Operation Enhancement to support POE (Path Of Entry) Parameter
A00006064	DNSCRN Disable CCR Screening
A00006387	Support of SUSpend/RESume over ETSI ISUP QFT (QSIG Feature Transparency)
A00006407	China ISUP Enhancement
A00006636	First ITX on Answer
A00006660	DDRM Node Definition and Provisioning
A00006661	DDRM Node Maintenance
A00006662	DDRM Line Definition and Line Maintenance
A00006731	Handle Flash on Exit
A00006980	AMA Module Code 130 Flexibility

A00007255	Dial Plan Enhancement for ETSI MWI TCAP
A00007349	CPC Screening support for FDCP Trunks
A00007383	DNH (Directory Number Hunting) enhancements: pilot DN charge and display
A00007749.AA06	MG9000 ABI Support for LGCO, LGCOi
A00007793	IN: SCF Id, Correlation Id and QoR Base LNP Support (DACOM)
A00007807	Base ETSI ISUP V2 support for Dacom IN

1: A00005315 Configuration (CN)

1.1 Feature name

Calling Number Delivery for PRI, ISUP & CS-1

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)

1.6.1 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)
CGPNBLDR	Changed	Unchanged
CGBLDADD	Changed	Unchanged
CGBLDDGL	Changed	Unchanged
CGBLDDIG	Changed	Unchanged
CGBLDNI	Changed	Unchanged
CGBLDPI	Changed	Unchanged
CGBLDSIN	New	New

1.6.2 Table/MIB/Remote Database Schema information

1.6.2.1 Name: CGPNBLDR

Calling Party Number Builder

1.6.2.1.1 Functional description

N/A.

1.6.2.1.2 Usage sequence and implications (CM Only)

N/A.

1.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CGPNBLDR	Unchanged	Unchanged	

1.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for CGPNBLDR.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Range of Values	Description
CGNBDKEY			String of up to 20 characters	alphanumeric (1 to 20 characters)

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Range of Values	Description
CBOPTION	New	IC_VAR_SCRN: Variable Type Variable Name NEWBDKEY CONTINUE	{SMALLINT} String of up to 8 characters String of up to 20 characters(a new CGPNBLDR index) Y or N	Allows the operator to screen the variables that are datafilled in table VARDEF. This option currently only supports to screen the small integer (0-255) type variables. The value of the variable can be set for the incoming trunk using the SETVAR SMALLINT option in table CALLCNTL or one of its screening tables. The table CGBLDSIN is accessed to find if the match can be found for a given CGPNBLDR Index, variable and its value. If screening fails, the CGPNBLDR process can be terminated or continued based on the datafill of field CONTINUE. <i>Please note that if a variable is not assigned to the incoming trunk, the screening returns failed result by default.</i>

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Range of Values	Description
	New	CND_GOTO: CONDITION NEWBDKEY	{IC_INAP} String of up to 20 characters(a new CGPNBLDR index)	Allows the operator to change the CGPNBLDR index when the incoming call accords with the condition. Currently, only incoming IN call will be checked
	New	DIGMAN: DMI	0 to 32767	Allows the operator to change the CLI. And the field DMI is indexed to the table DIGMAN which is used to manipulate the CLI digits.
	New	ENHANCED_DI GSCRN: DMI	0 to 32767	Indicates the digits of the address to be screen, this option is associated with table CGBLDDIG. And the field DMI is indexed to the table DIGMAN which is used to manipulate the CLI digits temporarily before entering the table CGBLDDIG. The manipulation can only be seen when processing in CGBLDDIG, it can not take effect to the real CLI after returning from CGBLDDIG.

1.6.2.1.5 Datafill example

The following shows datafill example for table CGPNBLDR.

TABLE: CGPNBLDR

SCRN_CHOSEN_IC_ADDR

(IC_ADDR_SCRN (ADDRTYPE) (DIGLEN) \$) (SETPI ALLOWED) (SETNI COMLETED) \$

SCRN_IC_VAR (IC_VAR_SCRN (SMALLINT IC_VAR) \$ Y) \$

1.6.2.1.6 Table release history update

New CGPNBLDR options IC_VAR_SCRN, CND_GOTO, DIGMAN, ENHANCED_DIGSCRN are added to table CGPNBLDR.

1.6.2.1.7 Supplementary information

N/A.

1.6.2.1.8 Translation verification other tools

N/A.

1.6.2.2 Name: CGBLDADD

Address-Type Screening

1.6.2.2.1 Functional description

N/A.

1.6.2.2.2 Usage sequence and implications (CM Only)

N/A.

1.6.2.2.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CGBLDADD	Unchanged	Unchanged	

1.6.2.2.4 Fields/OIDs

The following table lists fields/OIDs for CGBLDADD.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Range of Values	Explanation and action
CGNADDRK	N/A	CGNBDKEY ADDRTYPE	String of up to 20 characters One of {CLI, RDN, CHARGE, PN, CONTRACTOR, GENERIC_NO}	The key is composed of two subfields.
NEWBDKEY	N/A	N/A	String of up to 20 characters	A new CGPNBLDR Index.
CBOPTION	Changed	N/A	CGPNBLDR Options: SETPI, SETNI, DIGMAN	Allows setting of the PI, NI and CLI value of the outgoing CGPN as performed in table CGPNBLDR.

1.6.2.2.5 Datafill example

The following shows datafill example for table CGBLDADD.

TABLE: CGBLDADD

SCRN_IC_ADDR CLI SCRN_IC_CGPN (**DIGMAN 10**)\$

1.6.2.2.6 Table release history update

New CGPNBLDR option DIGMAN is added.

1.6.2.2.7 Supplementary information

N/A.

1.6.2.2.8 Translation verification other tools

N/A.

1.6.2.3 Name: CGBLDDGL

Digit-Length Screening

1.6.2.3.1 Functional description

N/A.

1.6.2.3.2 Usage sequence and implications (CM Only)

N/A.

1.6.2.3.3 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CGBLDDGL	Unchanged	Unchanged	

1.6.2.3.4 Fields/OIDs

The following table lists fields/OIDs for CGBLDDGL.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Range of Values	Explanation and action
CGNDGLK	N/A	CGNBDKEY DIGLEN	String of up to 20 characters {0 TO 30}	The key is composed of two subfields.
NEWBDKEY	N/A	N/A	String of up to 20 characters	A new CGPNBLDR Index.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Range of Values	Explanation and action
CBOPTION	Changed	N/A	CGPNBLDR Options: SETPI, SETNI, DIGMAN	Allows setting of the PI, NI and CLI value of the outgoing CGPN as performed in table CGPNBLDR.

1.6.2.3.5 Datafill example

The following example shows datafill example for table CGBLDDGL.

TABLE: CGBLDDGL

 SCRN_IC_CGPN 10 IC_CGPN_LENGTH_10 (**DIGMAN 10**) \$

1.6.2.3.6 Table release history update

New CGPNBLDR option DIGMAN is added.

1.6.2.3.7 Supplementary information

N/A.

1.6.2.3.8 Translation verification other tools

N/A.

1.6.2.4 Name: CGBLDDIG

Digit Screening

1.6.2.4.1 Functional description

N/A.

1.6.2.4.2 Usage sequence and implications (CM Only) N/A.**1.6.2.4.3 Size****Table 8 Table size**

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CGBLDDIG	Unchanged	Unchanged	

1.6.2.4.4 Fields/OIDs

The following table lists fields/OIDs for CGBLDDIG.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Range of Values	Explanation and action
CGNDGKEY	N/A	CGNBDKEY	String of up to 20 characters	The key is composed of three subfields.
		FROMDIGS	1-15 digits	
		TODIGS	1-15 digits	
NEWBDKEY	N/A	N/A	String of up to 20 characters	A new CGPNBLDR Index.
CBOPTION	Changed	N/A	CGPNBLDR Options: SETPI, SETNI, DIGMAN	Allows setting of the PI, NI and CLI value of the outgoing CGPN as performed in table CGPNBLDR.

1.6.2.4.5 Datafill example

The following shows datafill example for table CGBLDDIG.

TABLE: CGBLDDIG

CGNDGKEY NEWBDKEY CBOPTION

BASE 77 77 SCR_N_RETURN (SETPI NOT_AVAIL)\$

BASE 88 88 PREFIX_88 (**DIGMAN 10**) \$

1.6.2.4.6 Table release history update

New CGPNBLDR option DIGMAN is added.

1.6.2.4.7 Supplementary information

N/A.

1.6.2.4.8 Translation verification other tools

N/A.

1.6.2.5 Name: CGBLDNI

NI Screening

1.6.2.5.1 Functional description

N/A.

1.6.2.5.2 Usage sequence and implications (CM Only)

N/A.

1.6.2.5.3 Size

Table 10 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CGBLDNI	Unchanged	Unchanged	

1.6.2.5.4 Fields/OIDs

The following table lists fields/OIDs for CGBLDNI.

Table 11 Table field descriptions

Field	New or Changed	Subfield or refinement	Range of Values	Explanation and action
CGNNIKEY	N/A	CGNBDKEY NI	String of up to 20 characters One of {COMPLETE, INCOMPLETE}	The key is composed of two subfields.
NEWBDKEY	N/A	N/A	String of up to 20 characters	A new CGPNBLDR Index.
CBOPTION	Changed	N/A	CGPNBLDR Options: SETPI, SETNI, DIGMAN	Allows setting of the PI, NI and CLI value of the outgoing CGPN as performed in table CGPNBLDR.

1.6.2.5.5 Datafill example

The following shows datafill example for table CGBLDNI

TABLE: CGBLDNI

SCRN_IC_CGPN COMPLETE NI_0 (**DIGMAN 10**)\$

1.6.2.5.6 Table release history update

New CGPNBLDR option DIGMAN is added.

1.6.2.5.7 Supplementary information

N/A.

1.6.2.5.8 Translation verification other tools

N/A.

1.6.2.6 Name: CGBLDPI

PI Screening

1.6.2.6.1 Functional description

N/A.

1.6.2.6.2 Usage sequence and implications (CM Only)

N/A.

1.6.2.6.3 Size

Table 12 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CGBLDPI	Unchanged	Unchanged	

1.6.2.6.4 Fields/OIDs

The following table lists fields/OIDs for CGBLDPI.

Table 13 Table field descriptions

Field	New or Changed	Subfield or refinement	Range of Values	Explanation and action
CGNPIKEY	N/A	CGNBDKEY PI	String of up to 20 characters One of { ALLOWED, RESTRICTED, NOT_AVAIL, SPARE }	The key is composed of two subfields.
NEWBDKEY	N/A	N/A	String of up to 20 characters	A new CGPNBLDR Index.
CBOPTION	Changed	N/A	CGPNBLDR Options: SETPI, SETNI, DIGMAN	Allows setting of the PI, NI and CLI value of the outgoing CGPN as performed in table CGPNBLDR.

1.6.2.6.5 Datafill example

The following shows datafill example for table CGBLDPI.

TABLE: CGBLDPI

SCRN_IC_CGPN ALLOWED PI_00 (SETPI ALLOWED) (**DIGMAN 10**) \$

1.6.2.6.6 Table release history update

New CGPNBLDR option DIGMAN is added.

1.6.2.6.7 Supplementary information

N/A.

1.6.2.6.8 Translation verification other tools

N/A.

1.6.2.7 Name: CGBLDSIN

SMALLINT Screening

1.6.2.7.1 Functional description

Table CGBLDSIN allows the operator to screen the variable and its value assigned to the incoming trunk.

1.6.2.7.2 Usage sequence and implications (CM Only)

Enter the datafill into table VARDEF before this table.

1.6.2.7.3 Size

Table 14 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CGBLDSIN	0	4096*1023 ^a *256	

a. There is a limit of 1023 values for the number of CGPNBLDR indices. These indices are used for all of the screening tables so the maximum number of tuples in any table created by this feature is dependent on the overlap of CGPNBLDR keys used between all the tables.

1.6.2.7.4 Fields/OIDs

The following table lists fields/OIDs for CGBLDSIN.

Table 15 Table field descriptions

Field	New or Changed	Subfield or refinement	Range of Values	Explanation and action
SINTVAR	New	SINTVAR	Variable name (1-8 characters) from table VARDEF	The key is composed of three subfields.
		CGNBDK	String of up to 20 characters	
		VALUE	{0 TO 255}	
NEWBDKEY	New	N/A	String of up to 20 characters	A new CGPNBLDR Index.

Field	New or Changed	Subfield or refinement	Range of Values	Explanation and action
CBOPTION	New	N/A	CGPNBLDR Options: SETPI, SETNI, DIGMAN	Allows setting of the PI, NI and CLI value of the outgoing CGPN as performed in table CGPNBLDR.

1.6.2.7.5 Datafill example

The following shows datafill example for table CGBLDSIN.

TABLE: CGBLDSIN

IC_PROT SCRN_IC_PROT 1 IC_AGENT_IS_ISUP (SETPI SPARE) (SETNI INCOMPLETE) \$

IC_PROT SCRN_IC_PROT 2 IC_AGENT_IS_PRI (SETPI NOT_AVAIL) \$

1.6.2.7.6 Table release history update

New table CGBLDSIN is added.

1.6.2.7.7 Supplementary information

N/A.

1.6.2.7.8 Translation verification other tools

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 User interface changes

N/A.

1.11 OSSGate Interface Changes

N/A.

1.12 Security

N/A.

1.13 Configuration Walkthrough

N/A.

2: A00005962 Configuration (CN)

2.1 Feature Name

CLIR Removal For Centrex Intragroup Calls

2.2 Hardware and Software Requirements

2.3 Initial Configuration

2.4 Office/Subnet parameters (OP/SP) (CM & SESM)

2.5 Upgrade Impact

2.6 Data schema (DS) (CM, MIBS, RDB)

2.6.1 New/modified tables, MIBs, or Database Schema

CUSTSTN

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/ UNCHANGED)
CUSTSTN	CHANGED	UNCHANGED

2.6.2 Table/MIB/Remote Database Schema information

2.6.2.1 Name: CUSTSTN

This table is used for customer group basis option provisioning.

2.6.2.1.1 Functional description

This activity enhances one of the CUSTSTN options named CNDBO by adding a subfield named CNDBOTYPE.

CNDBOTYPE: { ALL, INTRAONLY }

This subfield determines whether CNDBO option will be valid for all calls terminating to subscribers at this customer group in existing way by being datafilled as ALL, or the option will be valid only on calls which both

originating and terminating subscribers are in that customer group by being datafilled as INTRAONLY.

Figure 1 Example CUSTSTN datafill for customer group CNDBO

TABLE: CUSTSTN			
CUSTNAME	OPTNAME	OPTION	
CUSTYAS	CNDBO	CNDBO	<u>INTRAONLY</u>

2.6.2.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

2.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CUSTSTN	0	1	

2.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for CUSTSTN.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CNDBOTYPE	NEW	subfield	ALL, INTRAONLY	Determines whether the CNDBO option will be

2.6.2.1.5 Datafill example

The following example shows sample datafill for table CUSTSTN.

Figure 2 Example of table CUSTSTN datafill

```

CI:
>table custstn
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: CUSTSTN
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
CUSTNAME:
>custyas
OPTNAME:
>cndbo
OPTION:
>cndbo
CNDBOTYPE:
>intraonly
TUPLE TO BE ADDED:
      CUSTYAS      CNDBO      CNDBO INTRAONLY
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE

```

2.6.2.1.6 Table release history update

None.

2.6.2.1.7 Supplementary information

None.

2.6.2.1.8 Translation verification other tools

None.

2.7 Service Orders (SO) (CM & SESM)**2.8 Software optionality control (SOC)**

2.9 Element Management

2.10 Command interface changes

2.11 Security

2.12 Configuration Walkthrough

3: A00005980 Configuration (CN)

3.1 Feature Name

GSP IN CONNECT Operation Enhancement to support RouteList Parameter

3.2 Hardware and Software Requirements

None.

3.3 Upgrade Considerations

None.

3.4 Data schema (DS) (CM, MIBS, RDB)

3.4.1 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)
RTELMAP	New	New

3.4.2 Table/MIB/Remote Database Schema information

3.4.2.1 Name: RTELMAP

Route List Mapping Table

3.4.2.1.1 Functional description

New Table RTELMAP has been created/developed to provide a datafillable mapping from a BusinessLineID (an index in the range {0 to 65535}) to an OVR Table ID and Key. This mapping will be used to define the physical route(s) to associate with a BusinessLineID received in the INAP CONNECT RouteList parameter.

3.4.2.1.2 Usage sequence and implications (CM Only)

For an OVR Table ID and Key to be datafilled in Table RTELMAP, that OVR Table ID (Tables OVR0 - OVR89) must first be datafilled in that OVR Table Key position ({0 to 1023}).

When the datafill of a Key in an OVR Table is attempted to be changed or deleted, if this OVR Table ID and Key is already datafilled in Table RTELMAP, a delete will not be allowed, and a change will be allowed but a Warning message will be printed to notify the operator that this OVR tuple is datafilled in Table RTELMAP. In order to delete an OVR Key from the

associated OVR Table, all datafills of this OVR Table ID & Key in Table RTELMAP must be deleted.

3.4.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
RTELMAP	0	65535	Memory for the whole table (potential 65536 tuples) is automatically allocated during the initialization of Table RTELMAP.

3.4.2.1.4 Fields/OIDs

The following table lists fields for Table RTELMAP.

Table 3 Table RTELMAP field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BLINEID	New	N/A	{0..65535}	Business Line ID
OVRTABID	New	TABID	OVR0 - OVR89	OVR Table ID
		KEY	{0..1023}	OVR Table Key

3.4.2.1.5 Datafill example

The following example shows sample datafill for Table RTELMAP.

```
TABLE: RTELMAP
>
>lis all
TOP
BUSINESSLINEID
-----
0 OVR74 44
16 OVR6 7
315 OVR4 371
4426 OVR4 6
37354 OVR74 24
65535 OVR6 373
BOTTOM
>
```

3.4.2.1.6 Table release history update

Table is newly created.

3.4.2.1.7 Supplementary information

None.

3.4.2.1.8 Translation verification and other tools

The following examples show the output from GTRAVR when it is used to trace the outgoing route(s) for a received BusinessLineID in an INAP CONNECT RouteList parameter.

```
>GTRAVR TR GM2WEISV2BA 0500 T
TABLE TRKGRP
GM2WEISV2BA AXXESS 0 NPDGP NCIT 2W NPRT MIDL 16 7 16 16 4 5
  4 ALERTING NIL_COSGRP 0 103 NONE 0 0 NIL_CUST 1 Y Y NODEF
  NO_OVERRIDE VOICE_DATA Y Q764 N 1 0 0 0 N N NIL NIL ISUP $ 45
  STD N Y NIL 0 N
TABLE ISUPATTR
45 EISUPV2 NIL THRH 0 Y NATL N 0 N N UNEQ 2WN7 NONE CIC N
  NOVERI N N NIL FILTER 0
TABLE INTRK
GM2WEISV2BA PINAR
TABLE OFCVAR
IN_OFFICE_TRIGGRP NIL
INAP TDP-2 (Info Collected): no subscribed trigger.
TABLE INTRK
GM2WEISV2BA PINAR
TABLE GTRIGGRP
PINAR INFOANAL
. GENTRIG (CDPN PINAR)$ NIL
Trigger INAP GENTRIG is applicable to individual trunk.
. . TABLE GTRIGDIG
. . PINAR 0500 GINDCT CALLED (SERVKEY 4) (SERVINFO_INDEX 4)
$
. . . TABLE GSERVINF
. . . 4 (INITDP_INFO Y N N N N N N) $
. . . TABLE C7GTTTYPE
. . . GINDCT CCITT7 3 NATL E164 $
. . . TABLE C7GTT
```

```

. . . GINDCT 0500 0500 PCSSN (DCT2KRTESET GIN 0) $ SSN
INAP TDP-3 (Info Analyzed): trigger criteria met.
Select the INAP Operation expected from the SCP:
1- Connect
2- Continue
>1
Enter NOA and Destination Number expected in Connect operation:
>3
Next par is: <DEST DIGITS> STRING
Enter: <DEST DIGITS>
>7835453
Enter a BusinessLineID {0-65535} if expected from SCP in RouteList,
else press Return:
>416
Translating with BusinessLineID: 416
Pretranslating with Pretranslator: NPRT
Translating with STS 103 and CUSTNAME NIL_CUST
TABLE RTELMAP
416 OVR4 16
TABLE OVR4
. 16 S A GM2WEISV2BA
The Outpulsed Number is : 6067835452
.GBL GRX PINARX N N N 416
TABLE DIGEDIT
416 (CL BEG) (REM 3)
EXIT TABLE DIGEDIT
. . TABLE CALLCNTL
. . PINARX (PRTNM PINAR) (STS 103) (CUSTNAME NIL_CUST) $
.CND NRR SK 0
.S A GM2WFTUPBA
The Outpulsed Number is : 7835452
.GBL GRX CLICNTL_NOSCRN_BL_CLI N N N 8965
TABLE DIGEDIT
8965 (CL BEG) (INC 600)
EXIT TABLE DIGEDIT
. . TABLE CALLCNTL
. . CLICNTL_NOSCRN_BL_CLI (CLICNTL NOSCRN_BL_CLI) $
.T OVR89 65

```

TABLE POECRTE
 TUPLE NOT FOUND
 . . TABLE OVR89
 . .65 S A GM2WFTUPBA
 The Outpulsed Number is : 6007835452
 . . EXIT TABLE OVR89
 TABLE STDPRTCT
 PINAR (1) (0) 3
 . SUBTABLE STDPRT
 . 6 9 CT OFFNET PX 1 24 0 416 NAT
 Translating with STS 103 and CUSTNAME NIL_CUST
 TABLE PXTRAN
 103 NIL_CUST PXOFF PXON PXOFF PXIP
 TABLE PXHEAD
 PXOFF DFLT CONT (XLT FA FAOFF) \$ DFOP \$ NOCON STD
 THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 6007835452
 TABLE PXCORE
 PXOFF 600 600 RTE (PF 3) (DEST 606) (CLASS NATL) (LNET NAT)
 (MZONE 1) \$
 TABLE: PXRTE
 KEY:PXOFF 606
 . S GM2WEISV2BA
 The Outpulsed Number is : 7835452
 EXIT TABLE PXRTE

 +++ TRAVER: SUCCESSFUL CALL TRACE +++

>GTRAVER TR GM2WEISV2BA 0800 T
 TABLE TRKGRP
 GM2WEISV2BA AXCESS 0 NPDGP NCIT 2W NPRT MIDL 16 7 16 16 4
 5 4 ALERTING
 NIL_COSGRP 0 103 NONE 0 0 NIL_CUST 1 Y Y NODEF
 NO_OVERRIDE VOICE_DATA Y Q764
 N 1 0 0 0 N N NIL NIL ISUP \$ 45 STD N Y NIL 0 N

TABLE ISUPATTR

45 EISUPV2 NIL THRH 0 Y NATL N 0 N N UNEQ 2WN7 NONE CIC N
NOVERI N N NIL FILTER

0

TABLE INTRK

GM2WEISV2BA PINAR

TABLE OFCVAR

IN_OFFICE_TRIGGRP NIL

INAP TDP-2 (Info Collected): no subscribed trigger.

TABLE INTRK

GM2WEISV2BA PINAR

TABLE GTRIGGRP

PINAR **INFOANAL**

. GENTRIG (CDPN PINAR)\$ NIL

Trigger INAP GENTRIG is applicable to individual trunk.

. . TABLE GTRIGDIG

. . PINAR 0800 GINDCT CALLED (SERVKEY 2209) (SERVINFO_INDEX
2209) \$

. . . TABLE GSERVINF

. . . 2209 (INITDP_INFO Y N N N N N N Y) \$

. . . TABLE C7GTTTYPE

. . . GINDCT CCITT7 3 NATL E164 \$

. . . TABLE C7GTT

. . . GINDCT 0800 0800 PCSSN (ISTEPRSET2 SS108 2) \$ SSN

INAP TDP-3 (Info Analyzed): trigger criteria met.

The Called Party NOA sent to the SCP is: 2 (Unknown)

The Called Party Number sent to the SCP is: 0800

Select the INAP Operation expected from the SCP:

1- Connect

2- Continue

>1

Enter NOA and Destination Number expected in Connect operation:

>4

Next par is: <DEST DIGITS> STRING

Enter: <DEST DIGITS>

>6067835452

**Enter a BusinessLineID {0-65535} if expected from SCP in RouteList,
else press Return:**

>

No RouteList-BusinessLineID expected from SCP.
 Translating only with DRA.
 TABLE OFCVAR
 IN_PRTNM NPRT
 Pretranslating with Original Pretranslator: NPRT
 Translating with STS 103 and CUSTNAME NIL_CUST
 TABLE PXTRAN
 103 NIL_CUST PXOFF PXON PXOFF PXIP
 TABLE PXHEAD
 PXOFF DFLT CONT (XLT FA FAOFF)\$ DFOP \$ NOCON STD
 THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 6067835452
 TABLE PXCODE
 PXOFF 606 606 RTE (PF 3) (DEST 606) (CLASS NATL) (LNET NAT)
 (MZONE 1)\$
 TABLE POECRTE
 TUPLE NOT FOUND
 TABLE: PXRTE
 KEY:PXOFF 606
 . S GM2WEISV2BA
 The Outpulsed Number is : 7835452
 EXIT TABLE PXRTE

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>GTRAVER TR GM2WEISV2BA 0800 T
 TABLE TRKGRP
 GM2WEISV2BA AXXESS 0 NPDGP NCIT 2W NPRT MIDL 16 7 16 16 4
 5 4 ALERTING
 NIL_COSGRP 0 103 NONE 0 0 NIL_CUST 1 Y Y NODEF
 NO_OVERRIDE VOICE_DATA Y Q764
 N 1 0 0 0 N N NIL NIL ISUP \$ 45 STD N Y NIL 0 N
 TABLE ISUPATTR
 45 EISUPV2 NIL THRH 0 Y NATL N 0 N N UNEQ 2WN7 NONE CIC N
 NOVERI N N NIL FILTER

```

0
TABLE INTRK
GM2WEISV2BA PINAR
TABLE OFCVAR
IN_OFFICE_TRIGGRP NIL
INAP TDP-2 (Info Collected): no subscribed trigger.
TABLE INTRK
GM2WEISV2BA PINAR
TABLE GTRIGGRP
PINAR INFOANAL
. GENTRIG (CDPN PINAR)$ NIL
Trigger INAP GENTRIG is applicable to individual trunk.
. . TABLE GTRIGDIG
. . PINAR 0800 GINDCT CALLED (SERVKEY 2209) (SERVINFO_INDEX
2209) $
. . . TABLE GSERVINF
. . . 2209 (INITDP_INFO Y N N N N N N Y) $
. . . TABLE C7GTTYPE
. . . GINDCT CCITT7 3 NATL E164 $
. . . TABLE C7GTT
. . . GINDCT 0800 0800 PCSSN (ISTEPRSET2 SS108 2) $ SSN
INAP TDP-3 (Info Analyzed): trigger criteria met.
The Called Party NOA sent to the SCP is: 2 (Unknown)
The Called Party Number sent to the SCP is: 0800
Select the INAP Operation expected from the SCP:
1- Connect
2- Continue
>1
Enter NOA and Destination Number expected in Connect operation:
>3
Next par is: <DEST DIGITS> STRING
Enter: <DEST DIGITS>
>6067835452
Enter a BusinessLineID {0-65535} if expected from SCP in RouteList,
else press Return:
>2474
Translating with BusinessLineID: 2474
Pretranslating with Pretranslator: NPRT

```

Translating with STS 103 and CUSTNAME NIL_CUST

TABLE RTELMAP

TUPLE NOT FOUND

TABLE TMTCNTL

AXXESS (0)

. SUBTABLE TREAT

KEY NOT FOUND

DEFAULT OFFTREAT IS USED

TABLE TMTCNTL

OFFTREAT (223)

. SUBTABLE TREAT

. AINF Y S 120T0

+++ TRAVER: SUCCESSFUL CALL TRACE +++

>GTRAVER TR GM2WEISV1BA 0800 T

TABLE TRKGRP

GM2WEISV1BA AXXESS 0 NPDGP NCIT 2W NPRT MIDL 16 7 16 16 4
5 4 ALERTING

NIL_COSGRP 0 103 NONE 0 0 NIL_CUST 1 Y Y NODEF
NO_OVERRIDE VOICE_DATA Y Q764

N 1 0 0 0 N N NIL NIL ISUP \$ 44 STD N Y NIL 0 N

TABLE ISUPATTR

44 EISUPV1 NATIONAL NOVERI NIL THRH 0 Y Y N 0 N N UNEQ 2WN7
NONE CIC N NOVERI N

N NIL FILTER 0

TABLE INTRK

GM2WEISV1BA PINAR1

TABLE GTRIGGRP

PINAR1 **INFOCOL**

. GENTRIG (SPC PINAR)\$ NIL

Trigger INAP GENTRIG is applicable to individual trunk.

. . TABLE GTRIGDIG

```

. . PINAR 0800 GINDCT CALLED (SERVKEY 2209) (SERVINFO_INDEX
2209) $
. . . TABLE GSERVIN
. . . 2209 (INITDP_INFO Y N N N N N N Y) $
. . . TABLE C7GTTTYPE
. . . GINDCT CCITT7 3 NATL E164 $
. . . TABLE C7GTT
. . . GINDCT 0800 0800 PCSSN (ISTEPRSET2 SS108 2) $ SSN
INAP TDP-2 (Info Collected): trigger criteria met.
The Called Party NOA sent to the SCP is: 2 (Unknown)
The Called Party Number sent to the SCP is: 0800
Select the INAP Operation expected from the SCP:
1- Connect
2- Continue
>1
Enter NOA and Destination Number expected in Connect operation:
>10
Next par is: <DEST DIGITS> STRING
Enter: <DEST DIGITS>
>6017835452
Enter a BusinessLineID {0-65535} if expected from SCP in RouteList,
else press Return:
>345
Translating with BusinessLineID: 345
Pretranslating with Pretranslator: NPRT
Translating with STS 103 and CUSTNAME NIL_CUST
Routing with a BusinessLineID is not allowed for TDP-2 triggered
calls.
TABLE TMTCNTL
AXCESS ( 0)
. SUBTABLE TREAT
KEY NOT FOUND
DEFAULT OFFTREAT IS USED
TABLE TMTCNTL
OFFTREAT ( 223)
. SUBTABLE TREAT
. FNAL Y S 120T0

+++ TRAVER: SUCCESSFUL CALL TRACE +++

```

>GTRAVR TR GM2WEISV1BA 0800 T
TABLE TRKGRP
GM2WEISV1BA AXXESS 0 NPDGP NCIT 2W NPRT MIDL 16 7 16 16 4
5 4 ALERTING
 NIL_COSGRP 0 103 NONE 0 0 NIL_CUST 1 Y Y NODEF
NO_OVERRIDE VOICE_DATA Y Q764
 N 1 0 0 0 N N NIL ISUP \$ 44 STD N Y NIL 0 N
TABLE ISUPATTR
44 EISUPV1 NATIONAL NOVERI NIL THRH 0 Y Y N 0 N N UNEQ 2WN7
NONE CIC N NOVERI N
 N NIL FILTER 0
TABLE INTRK
GM2WEISV1BA PINAR1
TABLE GTRIGGRP
PINAR1 INFOCOL
 . GENTRIG (SPC PINAR)\$ NIL
Trigger INAP GENTRIG is applicable to individual trunk.
 . . TABLE GTRIGDIG
 . . PINAR 0800 GINDCT CALLED (SERVKEY 2209) (SERVINFO_INDEX
2209) \$
 . . . TABLE GSERVINF
 . . . 2209 (INITDP_INFO Y N N N N N N Y) \$
 . . . TABLE C7GTTYPE
 . . . GINDCT CCITT7 3 NATL E164 \$
 . . . TABLE C7GTT
 . . . GINDCT 0800 0800 PCSSN (ISTEPRSET2 SS108 2) \$ SSN
INAP TDP-2 (Info Collected): trigger criteria met.
The Called Party NOA sent to the SCP is: 2 (Unknown)
The Called Party Number sent to the SCP is: 0800
Select the INAP Operation expected from the SCP:

```

1- Connect
2- Continue
>1
Enter NOA and Destination Number expected in Connect operation:
>3
Next par is: <DEST DIGITS> STRING
Enter: <DEST DIGITS>
>6017835452
Enter a BusinessLineID {0-65535} if expected from SCP in RouteList,
else press Return:
>
No RouteList-BusinessLineID expected from SCP.
Translating only with DRA.
TABLE OFCVAR
IN_PRTNM NPRT
Pretranslating with Original Pretranslator: NPRT
Translating with STS 103 and CUSTNAME NIL_CUST
TABLE PXTRAN
103 NIL_CUST PXOFF PXON PXOFF PXIP
TABLE PXHEAD
PXOFF DFLT CONT ( XLT FA FAOFF)$ DFOP $ NOCON STD
THE DIGITS USED TO INDEX THE NEXT TABLE ARE: 6017835452
TABLE PXCODE
PXOFF 601 601 RTE ( PF 3) ( DEST 601) ( CLASS NATL) ( LNET NAT)
( MZONE 1)$
TABLE POECRTE
TUPLE NOT FOUND
TABLE: PX RTE
KEY:PXOFF 601
. S GM2WEISV1BA
The Outpulsed Number is : 7835452
EXIT TABLE PX RTE

+++ TRAVER: SUCCESSFUL CALL TRACE +++

```

3.5 Service Orders (SO) (CM & SESM)

N/A

3.6 User interface changes

3.6.1 Command: EINTRACE

3.6.1.1 Command description

EINTRACE is a tracing tool of the INAP dialogue between the DMS-SSP and the SCP. The OPEN;BACK ALL command prints the INAP operations in the TCAP packages for the INAP dialogue that took place between a START and a STOP command.

3.6.1.2 Responses

The EINTRACE tool has been enhanced to decode and print the contents of the RouteList parameter if received in an INAP CONNECT operation in a TCAP package.

3.6.1.3 Example

Table 4 Usage example for EINTRACE OPEN or BACK command

Description of task:	OPEN / BACK (to display a TCAP package containing an INAP CONNECT operation)

Table 4 Usage example for EINTRACE OPEN or BACK command

Command: OPEN / BACK	
MAP response:	<pre> 21:07:54 TCAP MESSAGE Tid : 2 ===== 65 73 48 04 00 00 00 03 49 04 00 00 01 00 6C 65 A1 63 02 01 03 02 01 14 30 5B A0 06 04 04 83 13 87 03 83 01 04 A7 4E 24 40 04 02 34 75 04 02 78 90 04 02 24 53 04 02 12 34 04 02 00 00 04 02 04 44 04 02 FF FF 04 02 01 11 04 02 D6 C7 04 02 00 03 04 02 00 01 04 02 00 0D 04 02 00 16 04 02 00 1E 04 02 01 01 04 02 56 78 24 04 04 02 06 13 24 04 04 02 F4 01 ===== Type of Package : 65 = CONTINUE Originating TRID : 00 00 00 03 Destination TRID : 00 00 01 00 Component Type : A1 = INVOKE Invoke ID : 03 Operation : 14 = CONNECT Destination Routing Address Called Party Number Odd/Even Indicator : 1 = ODD Nature Of Address : 03 = NATIONAL (SIGNIFICANT) NUMBER INN Indicator : 0 = ROUTING TO INTERNAL NETWORK NUMBER ALLOWED Numbering Plan Indicator : 01 = ISDN (TELEPHONY) NUMBERING PLAN (E164) Digits : 87 03 = 783 Cut And Paste : 04 = 4 Route List Route List Octet String 1 BusinessLineID 1 : 13429 BusinessLineID 2 : 30864 BusinessLineID 3 : 9299 BusinessLineID 4 : 4660 BusinessLineID 5 : 0 BusinessLineID 6 : 1092 BusinessLineID 7 : 65535 BusinessLineID 8 : 273 BusinessLineID 9 : 54983 BusinessLineID 10 : 3 BusinessLineID 11 : 1 BusinessLineID 12 : 13 BusinessLineID 13 : 22 BusinessLineID 14 : 30 BusinessLineID 15 : 257 BusinessLineID 16 : 22136 Route List Octet String 2 *** RouteList Octet String 2 NOT DECODED *** Route List Octet String 3 *** RouteList Octet String 3 NOT DECODED *** </pre>

4: A00005981 Configuration (CN)

4.1 Feature name

GSP IN InitDP Operation Enhancement to support POE (Path Of Entry)
Parameter

4.2 Data schema (DS) (CM, MIBS, RDB)

4.2.1 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)
GSERVINF	CHANGED	UNCHANGED

4.2.2 Table/MIB/Remote Database Schema information

4.2.2.1 Name: GSERVINF

GSP SERVICE INFORMATION

4.2.2.1.1 Functional description

A new field named PATH_OF_ENTRY is added under INITDP_OPTION.

4.2.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

4.2.2.1.3 Datafill example

The following example shows sample datafill for table GSERVINF with the newly defined PATH_OF_ENTRY field which is in bold face.

Figure 1 Example GSERVINF tuple with Path_Of_Entry Datafill

TABLE: GSERVINF

```

>pos 2209
2209 (INITDP_INFO N N N N N N N N) $
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
OPTION: INITDP_INFO
>
CALLING_PN: N
>
BEARER_CAPABILITY: N
>
FORWARD_CALL_INDICATOR: N
>
ORIG_CALLED_NUMBER: N
>
REDIRECTING_NUMBER: N
>
IN_BUSINESS_GROUP: N
>
REDIRECTION_INFORMATION: N
>
PATH_OF_ENTRY: N
>
OPTION:
>

```

4.2.2.1.4 Table release history update

PATH_OF_ENTRY field added under INITDP_INFO option.

4.3 User interface changes**4.3.1 Command: EINTRACE:OPEN**

The output range of the EINTRACE Open command is enhanced for an INITDP Message with Path Of Entry parameter.

4.3.1.1 Command description

EINTRACE tracks IN messages based on the originating trunk involved in the IN call. The EINTRACE buffer is displayed with the OPEN command.

4.3.1.2 Responses

“Usage example for EINTRACE Open command” on page 608 shows an example of a response to the EINTRACE Open command.

4.3.1.2.1 Example

Table 2 Usage example for EINTRACE Open command

Command:	11:55:31 TCAP MESSAGE	Tid : 26 514
MAP response: (Changed for INITDP)	Agent : CKT GANSIAT1N01A 1601	
=====		
62 33 48 04 00 00 19 00 6C 2B A1 29 02 01 00 02		
01 00 30 21 80 02 08 A1 82 06 81 10 80 00 11 01		
83 06 80 10 87 53 54 06 85 01 00 9C 01 03 9F 1F		
04 02 00 0C 00		
=====		
Type of Package : 62 = BEGIN		
Originating TRID : 00 00 19 00		
Component Type : A1 = INVOKE		
Invoke ID : 00		
Operation : 00 = INITIAL DP		
Service Key : 08 A1 = 2209		
Called Party Number		
Odd/Even Indicator : 1 = ODD		
Nature Of Address : 01 = SUBSCRIBER NUMBER		
INN Indicator : 0 = ROUTING TO INTERNAL NETWORK		
NUMBER ALLOWED		
Numbering Plan Indicator : 01 = ISDN (TELEPHONY)		
NUMBERING PLAN (E164)		
Digits : 80 00 11 01 = 0800111		
Calling Party Number		
Odd/Even Indicator : 1 = ODD		
Nature Of Address : 00 = *** UNSUPPORTED VALUE ***		
NI Indicator : 0 = COMPLETE		
Numbering Plan Indicator : 01 = ISDN (TELEPHONY)		
NUMBERING PLAN (E164)		
Presentation Restriction : 00 = PRESENTATION ALLOWED		
Screening Indicator : 00 = USER PROVIDED, NOT VERIFIED		
Digits : 87 53 54 06 = 7835456		
Calling Partys Category : 00 = UNKNOWN AT THIS TIME		
Event Type BCSM : 03 = ANALYZED INFORMATION		
Path Of Entry:		
Poe Group : POECGRP_T		
Poe Index : 000C = 12		

5: A00006064 Configuration (CN)

5.1 Feature name

DNSCRN Disable CCR Screening

5.2 Hardware and Software Requirements

NA

5.3 Initial Configuration

NA

5.4 Office/Subnet parameters (OP/SP) (CM & SESM)

NA

5.5 Upgrade Impact

None

5.6 Data schema (DS) (CM, MIBS, RDB)

None

5.7 Service Orders (SO) (CM & SESM)

NA

5.8 Software optionality control (SOC)

There is one new SOC option that is introduced with this feature.

Table 1 SOC

SOC option name:	XLAS
SOC option title:	CCR Screen Enh
SOC option control type:	<state
New SOC option?	Yes
SOC option order code	XLAS0056
Option defined in DRU:	WT
Affected products:	ISN)*

5.9 Element Management

NA

5.10 Command interface changes

NA

5.11 Security

NA

5.12 Configuration Walkthrough

NA

6: A00006387 Configuration (CN)

6.1 Feature name

Support of SUSpend/RESume over ETSI ISUP QFT (QSIG Feature Transparency)

6.2 Hardware and Software Requirements

N/A.

6.3 Initial Configuration

N/A.

6.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A.

6.5 Upgrade Impact

N/A.

6.6 Data schema (DS) (CM, MIBS, RDB)

6.6.1 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)
ISERVOPT	CHANGED	UNCHANGED

6.6.2 Table/MIB/Remote Database Schema information

6.6.2.1 Name: ISERVOPT

This table is used to configure switch wide information for service related feature.

6.6.2.1.1 Functional description

This activity introduces a new tuple named **QFT_SUS_RES_SUPPORT** of type Y or N in table ISERVOPT.

6.6.2.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

6.6.2.1.3 .Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	0	1	

6.6.2.1.4 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
SOPTSKEY	NEW		QFT_SUS_RES_SUPPORT	This is the key in ISERVOPT
OPTION	NEW		QFT_SUS_RES_SUPPORT	This is the option name
QFT_SUS_RES_SUPPORT	NEW		Y, N	control the enablement/disablement of SUS/RES generation over ETSI ISUP QFT.

6.6.2.1.5 Datafill example

The following example shows sample datafill for table ISERVOPT.

Figure 1 Example of ISERVOPT table datafill (QFT_SUS_RES_SUPPORT is Y)

```
>table iservopt
>add
SOPTSKEY:
>qft_sus_res_support
OPTION:
>qft_sus_res_support
QFT_SUS_RES_SUPPORT:
>y
TUPLE TO BE ADDED:
QFT_SUS_RES_SUPPORT QFT_SUS_RES_SUPPORT Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

**Figure 2 The View of QFT_SUS_RES_SUPPORT Tuple in ISERVOPT Table
(QFT_SUS_RES_SUPPORT is Y)**

```
>table iservopt

SOPTSKEY          SOPTSVAR
-----
QFT_SUS_RES_SUPPORT QFT_SUS_RES_SUPPORT Y$
```

Figure 3 Example of ISERVOPT table datafill (QFT_SUS_RES_SUPPORT is N)

```
>table iservopt
>add
SOPTSKEY:
>qft_sus_res_support
OPTION:
>qft_sus_res_support
QFT_SUS_RES_SUPPORT:
>n
TUPLE TO BE ADDED:
QFT_SUS_RES_SUPPORT QFT_SUS_RES_SUPPORT Y

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
```

**Figure 4 The View of QFT_SUS_RES_SUPPORT Tuple in ISERVOPT Table
(QFT_SUS_RES_SUPPORT is N)**

```
>table iservopt

SOPTSKEY          SOPTSVAR
-----
QFT_SUS_RES_SUPPORT QFT_SUS_RES_SUPPORT N$
```

6.6.2.1.6 Supplementary information

N/A.

6.6.2.1.7 Translation verification other tools

N/A.

6.7 Service Orders (SO) (CM & SESM)

N/A.

6.8 Software optionality control (SOC)

N/A.

6.9 Element Management

N/A.

6.10 Command interface changes

N/A.

6.11 Security

N/A.

6.12 Configuration Walkthrough

N/A.

7: A00006407 Configuration (CN)

7.1 Feature name

China ISUP Enhancement

7.2 Hardware and Software Requirements

N/A

7.3 Initial Configuration

N/A

7.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

7.5 Upgrade Impact

N/A

7.6 Data schema (DS) (CM, MIBS, RDB)

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
CUSTSTN	CHANGED	UNCHANGED
CALLCNTL	CHANGED	UNCHANGED
CGPNSCRN	CHANGED	UNCHANGED
CDPNSCRN	CHANGED	UNCHANGED
BCSCRN	CHANGED	UNCHANGED
CDPNLSCR	CHANGED	UNCHANGED
CGRPSCRN	CHANGED	UNCHANGED
CKTSCRN	CHANGED	UNCHANGED
CPCNSCRN	CHANGED	UNCHANGED
CPNNSCRN	CHANGED	UNCHANGED
IPISCRN	CHANGED	UNCHANGED
NCOSSCRN	CHANGED	UNCHANGED
NOASCRN	CHANGED	UNCHANGED
OLISCRN	CHANGED	UNCHANGED

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
RDRISCRN	CHANGED	UNCHANGED

7.6.1 Table/MIB/Remote Database Schema information**7.6.1.1 Name: CUSTSTN**

Customer Group Station Option

7.6.1.1.1 Functional description

Unchanged

7.6.1.1.2 Usage sequence and implications (CM Only)

Unchanged.

7.6.1.1.3 Size

Unchanged.

7.6.1.1.4 Fields/OIDs

The following table lists fields/OIDs for CUSTSTN.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTNAME	Changed		One of {CPC, CNDDTMF, CMI, SPL, CEPT, PCI, ACB, AIN, AINLATA, AINPRECE, AMBISC, AMBZERO, AR, ASP, AUTODISP, CBQ, CFCW, CFDATIM, CFDCET, CFIND, CFRA, CFWVAL, CFXFEAT, CFXOL, CFXOPT, CHD, CMCF, CNAB, CNDB, CNDBO, CNDBRI, COT, CPARK, CRINTER, CRRNOKSH, CTFP, CTW, CWD, CWO, CWTC, CXFER, CXFE RSUP, DCBITONE, DE NYCWTC, DINALT, DISPDIGS, DISTCWTN, DMCT, DND, DRING, E BOM, GICNOCFW, GICPAGE, INSPACT, INSPDISP, JCNDFORM, KSMOH, MBSCAMPO, MCGROUP, MSB, NAME DISP, NUMDGCMP, N3WCRRNG, PCACIDS, PCSOPT, PCWTTO, PHOLD, RAGRCOPT, RAGTIM, REASDISP, RE DIRECT, RND, SCPAUSE , SCUTDNO, SCVAL, SE RVCTL, SLE, SOR, SPP, 3WCSFLSH, TAFAS, UAWUCR, BRITONUN, MOT, VOWDN, CCNTLIDX }	Option nameEnter the name of the option,
OPTION	Changed			OptionThis field consists of subfield OPTION.
	New	OPTION	CCNTLIDX	Enter the name of option, and datafill refinement CCNTLIDX.
	New	CCNTLIDX	SCRN_INDXX	Call Control Index enter the index into table CALLCNTL.

7.6.1.1.5 Datafill example

The following example shows sample datafill for table CUSTSTN

Figure 1 Sample Datafill - Table CGPNSCRN

```
TABLE CUSTSTN
CUSTNAME OPTNAME OPTION
-----
CSGRPMB CCNTLIDX CCNTLIDX CDPNSCRN
```

7.6.1.1.6 Table release history update

The following information is added:

New option 'CCNTLIDX'

7.6.1.1.7 Supplementary information

None

7.6.1.1.8 Translation verification other tools

The following example shows the output from TRAVER when it is used to verify CUSTSTN.

Figure 2

```
traver 1 82223202 03083333200 b
TABLE IBNLINES
LG 00 2 01 82 0 DT STN IBN 82223202 CSGRPMB 0 2 20 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE CUSTSTN
CSGRPMB CCNTLIDX CCNTLIDX CDPNSCRN
TABLE CALLCNTL
CGPNSCRN
  (SCRN ( CGPN) $)$
PLEASE ENTER CLI DIGITS:
>82223202
TABLE CGPNSCRN
. CGPNSCRN
. SUBTABLE CGPNDATA
. . 82223202 82223202 CGPNMAN $
TABLE CALLCNTL
CGPNMAN (DIGMAN CGPN 20) (NOA CGPN NATL)$
The Original Calling Party Number is: 82223202
. . . TABLE DIGMAN
. . . 20 (INC 020)
. . . EXIT TABLE DIGMAN
The Calling Party Number has been set to: 02082223202
```

7.6.1.2 Name: CALLCNTL

CALL CONTROL

7.6.1.2.1 Functional description

Unchanged

7.6.1.2.2 Usage sequence and implications (CM Only)

Unchanged.

7.6.1.2.3 Size

Unchanged.

7.6.1.2.4 Fields/OIDs

The following table lists fields/OIDs for CALLCNTL.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CALCTL_OPTIONS	Changed		Vector of up to 8 of {SCRN, SETCODEC, DIGCOLL, DEFNUM, TNS_OVERI, CNDGOTO, SAT, SE TVAR, BC, POECNAME, CLICNTL, DIGMAN, CHE CKRETRY, COLLE CTCALL, INCRRETRY, MCTLOG, LNP, TREAT, CLIXLA, ACCTVIDX, CUSTGRP, GOTO, SRVCODE, NCOS, SE TCDN, COS, NOA }	List of up to 8 CALLCNTL options
	Changed	SCRN	Vector of up to 8 of {CDPN, VAR, UKKCDPN, KK, CUSTGRP, CPCNAME, CDNNAME, CSP_CIC, RDRINFO, CGPNNOA, BC, CIP, TNS_CIC, TNS_CKT, OLI, CGPN, IPI, NCOS, CDPNLEN, OCN, RGN }	List of 1 to 8 parameters to screen. Datafill the subfield SCRN. OCN - Original Called Number RGN - Redirecting Number

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
	Changed	DIGMAN	One of {CDPN, CGPN, OCN, RGN }	Enter the parameter to manipulate. OCN - Original Called Number RGN - Redirecting Number.
			DMI	Enter the index into table DIGMAN.
	New	NOA	NOA_PARM NOA_VALUE	Override the NOA of CGPN, OCN or RGN, datafill subfield NOA_PARM and NOA_VALUE.
	New	NOA_PARM	One of {CGPN, OCN, RGN}	Enter the parameter to override. CGPN - Calling Party Number OCN - Original Called Number RGN - Redirecting Number
	New	NOA_VALUE	One of {LCL, NATL}	Enter the new NOA value. LCL - NOA is local NATL - NOA is national

7.6.1.2.5 Datafill example

The following example shows sample datafill for table CALLCNTL.

Figure 3 Sample Datafill - Table CALLCNTL

```
TABLE CALLCNTL
CALCTL_KEY CALCTL_OPTIONS
-----
OCNSCRN (SCRN (OCN) $)$
RGNSCRN (SCRN (RGN) $)$
CGPNMAN (DIGMAN CGPN 30) (NOA CGPN LCL)
OCNMAN (DIGMAN OCN 30) (NOA OCN LCL)
RGNMAN (DIGMAN RGN 30) (NOA RGN NATL)
```

7.6.1.2.6 Table release history update

The following information is added:

New SCRN option 'OCN' and 'RGN'

New DIGMAN_PARM 'OCN' and 'RGN'

New CALLCNTL_OPTIONS 'NOA'

7.6.1.2.7 Supplementary information

None

7.6.1.2.8 Translation verification other tools

The following example shows the output from TRAVER when it is used to verify CALLCNTL.

```
traver tr cisuptb_mb 03083333200 b
TABLE TRKGRP
CISUPTB_MB IBNT2 0 NPDGP NCRT CSGRPTB 0 MIDL 2 N ANSDISC 0 N N N N N N N 0 0 N
0 0 0 N N N N N N N N NATL (ANISEND ALWAYS) $
TABLE TRKOPTS
CISUPTB_MB CCNTLIDX CCNTLIDX OCNSCRN
TABLE CALLCNTL
OCNSCRN
  (SCRN ( OCN) $)$
PLEASE ENTER DIGITS FOR ORIGINAL CALLED NUMBER:
>82223200
TABLE CGPNSCRN
. OCNSCRN
. SUBTABLE CDPNDATA
. . 82223200 82223200 OCNMAN $
TABLE CALLCNTL
OCNMAN (DIGMAN OCN 20) (NOA OCN NATL)$
The Pre-modified Original Called Number is: 82223200
. . . TABLE DIGMAN
. . . 20 (INC 020)
. . . EXIT TABLE DIGMAN
The Original Called Number has been set to: 02082223200
```

7.6.1.3 Name: List as below

The following screening tables are changed since the field CCOPTION is of TYPE CALLCNTL_OPTION_RANGE which is changed in table CALLCNTL.

BCSCRN Bearer Capability Screen

CDPNLSCR Called Party Number Length Screen

CDPNSCRN Called Party Number Digits Screen

CGPNSCRN Calling Party Number Screen

CGRPSCRN Customer Group Screen

CKTSCRN Transit Network Selector Circuit Screen

CPCNSCRN Called Number NOA & NPI Screen

CPNNSCRN Calling Number NOA Screen

IPISCRN Carrier Identification Code Screen

NCOSSCRN Network Class of Service Screen

NOASCRN ISDN Preference Indicator Screen

OLISCRN Originating Line Identity Screen

RDRISCRN Redirection Information Indicator Screen

7.6.1.3.1 Functional description

Unchanged

7.6.1.3.2 Usage sequence and implications (CM Only)

Unchanged

7.6.1.3.3 Size

Unchanged.

7.6.1.3.4 Fields/OIDs

The following table lists fields/OIDs for screening tables.

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CCOPTION	Changed		Vector of up to 8 of {SCRN, SETCODEC, DIGCOLL, DEFNUM, TNS_OVERI, CNDGOTO, SAT, SE TVAR, BC, POECNAME, CLICNTL, DIGMAN, CHE CKRETRY, COLLE CTCALL, INCRRETRY, MCTLOG, LNP, TREAT, CLIXLA, ACCTVIDX, CUSTGRP, GOTO, SRVCODE, NCOS, SE TCDN, COS, NOA }	List of up to 8 CALLCNTL options
	Changed	DIGMAN	One of {CDPN, CGPN, OCN , RGN } DMI	Enter the parameter to manipulate. OCN - Original Called Number RGN - Reidrecting Number. Enter the index into table DIGMAN.
	New	NOA	NOA_PARM NOA_VALUE	Override the NOA of CGPN, OCN or RGN, datafill subfield NOA_PARM and NOA_VALUE.
	New	NOA_PARM	One of {CGPN, OCN, RGN}	Enter the parameter to override. CGPN - Calling Party Number OCN - Original Called Number RGN - Redirecting Number

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
	New	NOA_VALU E	One of {LCL, NATL}	Enter the new NOA value. LCL - NOA is local NATL - NOA is national

7.6.1.3.5 Datafill example

The following example shows sample datafill for table CGPNNSCRN.

Figure 4 Sample Datafill - Table CGPNNSCRN

```
TABLE: CGPNNSCRN OCNSCRN: CGPNNDATA
FROMDIGS TODIGS CGPNINDEX CCOPTION CGPNOPT
-----
020 020 20OCNSCRN (DIGMAN OCN 020) (DIGMAN RGN 020) (NOA OCN LCL) (NOA RGN NATL)
```

The following example shows sample datafill for table CDPNSCRN.

Figure 5 Sample Datafill - Table CDPNSCRN

```
TABLE: CDPNSCRN OCNSCRN: CDPNDATA
FROMDIGS TODIGS CDPNINDEX CCOPTION CDPNOPT
-----
020 020 20CDNSCRN (DIGMAN OCN 020) (DIGMAN RGN 020) (NOA OCN LCL) (NOA RGN 020) $$
```

7.6.1.3.6 Table release history update

The following information is added:

New DIGMAN_PARM 'OCN' and 'RGN'

New CALLCNTL_OPTIONS 'NOA'

7.6.1.3.7 Supplementary information

None

7.6.1.3.8 Translation verification other tools

The following example shows the output from TRAVER when it is used to verify CGPNSCRN.

The following example shows the output from TRAVER when it is used to

```
traver tr cisuptb_mb 03083333201 b
TABLE TRKGRP
CISUPTB_MB IBNT2 0 NPDGP NCRT CSGRPTB 0 MIDL 2 N ANSDISC 0 N N N N N N N 0 0 N
0 0 0 N N N N N N N N NATL (ANISEND ALWAYS) $
TABLE TRKOPTS
CISUPTB_MB CCNTLIDX CCNTLIDX OCNSCRN
TABLE CALLCNTL
OCNSCRN
(SCRN ( OCN) $)$
PLEASE ENTER DIGITS FOR ORIGINAL CALLED NUMBER:
>82223200
TABLE CGPNSCRN
. OCNSCRN
. SUBTABLE CGPNDATA
. . 82223200 82223200 OCNSCRN (DIGMAN OCN 20)(NOA OCN NATL)$
The Pre-modified Original Called Number is: 82223200
. . . TABLE DIGMAN
. . . 20 (INC 020)
. . . EXIT TABLE DIGMAN
The Original Called Number has been set to: 02082223200
```

verify CDPNSCRN.

Figure 6

```
>traver tr cisuptb_mb 03083333200 b
TABLE TRKGRP
CISUPTB_MB IBNT2 0 NPDGP NCRT CSGRPTB 0 MIDL 2 N ANSDISC 0 N N N N N N N 0 0 N
0 0 0 N N N N N N N N NATL (ANISEND ALWAYS) $
TABLE TRKOPTS
CISUPTB_MB CCNTLIDX CCNTLIDX CDPNSCRN
TABLE CALLCNTL
CDPNSCRN
(SCRN ( CDPN ) $)$
. . TABLE CDPNSCRN
. . CDPNSCRN (1)
. . SUBTABLE CDPNDATA
. . 03083333200 03083333200 CDPNSCRN ( DIGMAN OCN 20) (NOA OCN NATL)$ $
PLEASE ENTER DIGITS FOR ORIGINAL CALLED NUMBER:
>82223201
The Pre-modified Original Called Number is: 82223201
. . . TABLE DIGMAN
. . . 20 (INC 020)
. . . EXIT TABLE DIGMAN
The Original Called Number has been set to: 02082223201
```

7.6.1.4 Name: ISERVOPT

International Service Option

7.6.1.4.1 Functional description

Unchanged

7.6.1.4.2 Usage sequence and implications (CM Only)

Unchanged.

7.6.1.4.3 Size

Unchanged.

7.6.1.4.4 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
SOPTSKEY	Changed			Service Options Key. This field contains the option name.
	New	SOPTSKEY	CISUPAMA	CISUPAMA - China ISUP AMA option
SOPTSVAR	Changed			
	New	OPTION	CISUPAMA	CISUPAMA - China ISUP AMA option
	New	PRE FIX_0_TO_N ATL_NUM_IN _AMA	Y,N	Y - The format of calling DN in AMA for CISUP outgoing calls is '0+areacode+local number' N - The format of calling DN in AMA for CISUP outgoing calls is 'areacode+local number'

7.6.1.4.5 Datafill example

The following example shows sample datafill for table ISERVOPT

Figure 7 Sample Datafill - Table ISERVOPT

TABLE: ISERVOPT SOPTSKEY SOPTSVAR ----- CISUPAMA CISUPAMA Y

7.6.1.4.6 Table release history update

The following information is added:

New option 'CISUPAMA'

7.6.1.4.7 Supplementary information

This option is supported for following interworkings:

- Interworking from IBN line to CISUP/SIPT(CISUP)
- Interworking from V5.2 line to CISUP/SIPT (CISUP)
- Interworking from CISUP/ SIPT (CISUP) to CISUP/ SIPT (CISUP)
- Interworking form SIP to CISUP/ SIPT (CISUP)
- Interworking from China PRI to CISUP/SIPT (CISUP)

Please refer to A00006407 FN for more detail.

7.6.1.4.8 Translation verification other tools

None

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 Command interface changes

N/A

7.11 Security

N/A

7.12 Configuration Walkthrough

N/A

8: A00006636 Configuration (CN)

8.1 Feature name

First ITX on Answer

8.2 Hardware and Software Requirements

This feature is supported only on the SX05 DTCO/DTCO2 processor.

8.3 Initial Configuration

N/A.

8.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A.

8.5 Upgrade Impact

8.5.1 Dump and Restore

None.

8.5.2 Element Management Upgrade

N/A.

8.6 Data schema (DS) (CM, MIBS, RDB)

N/A.

8.7 Service Orders (SO) (CM & SESM)

N/A.

8.8 Software optionality control (SOC)

There is a new SOC option that is introduced with this feature: ***First ITX on Answer***.

First ITX on Answer is defined under NETK SOC group. Functionality of the feature is controlled with this SOC option. It is a state SOC, whose states can be ON or IDLE. When state of *First ITX on Answer* is ON, the feature becomes functional and the first ITX is sent 500 msec after an answer for SSUTR2/SPIROU ITX generating calls.

Table 1 SOC for Activation of Feature

SOC group:	NETK
SOC option name:	First ITX on Answer

SOC option title:	First ITX on Answer
SOC option control type:	state
New SOC option?	Yes
SOC option order code	NETKXXXX
Option defined in DRU:	WT21
Affected products:	ISN08

8.9 Element Management

N/A.

8.10 Command interface changes

N/A.

8.11 Configuration Walkthrough

N/A.

9: A00006660 Configuration (CN)

9.1 Feature name

DDRM Node Definition and Provisioning

9.2 Hardware and Software Requirements

9.3 Initial Configuration

9.4 Office/Subnet parameters (OP/SP) (CM & SESM)

9.5 Upgrade Impact

9.6 Data schema (DS) (CM, MIBS, RDB)

9.6.1 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)
LCMINV	CHANGED	UNCHANGED

9.6.2 Table/MIB/Remote Database Schema information

9.6.2.1 Name: LCMINV

LCM Inventory Table

9.6.2.1.1 Functional description

It is not a new table.

9.6.2.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Current datafill order unchanged.

9.6.2.1.3 Size

It is not a new table.

9.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for LCMINV.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FRTYPE	Changed		DDRM is added to the range.	DDRM is the frame name for DDRM node.
EQPEC	Changed		DDRMPC is added to the range.	DDRMPC is the equipment pec for DDRM node.
LCMTYPE	Changed	DDRM refinement is added.	DDRM is added to the range of LCMTYPE SEL.	RGEQUIP is the ringing data for DDRM.
			RGEQUIP	LINKMAP indicates the C-side links to the host PLGC.
			LINKMAP	ESA shows whether ESA mode is enabled or not.
			ESA	
			GNS	GNS indicates whether the DDRM node is single plane or double plane.
			MXC_CONFIG	
			UTR_CONFIG	MXC_CONFIG shows which shelves have MXC.
			MTA_AVAILABLE	UTR_CONFIG shows which shelves have UTR.
			LTT-TMS	MTA_AVAILABLE shows whether the DDRM has the MTA card set or not.
				LTT_TMS shows the MTA card set configuration.

9.6.2.1.5 Datafill example

The following example shows sample datafill for table LCMINV.

Figure 1 LCMINV Sample Dataflow for DDRM

TABLE LCMINV

LCMNM **FRTYPE** SHPOS FLOOR ROW FRPOS **EQPEC** LOAD CPMNO

BICST ADNUM MEMSIZE

LCMTYPE-----
REMO 00 0 **DDRM** 0 0 A 2 **DDRMPC DDRMLD** PLGC 0

N 7 256K 256K

DDRM Y C (0) (2) (1) (3)\$Y DOUBLE Y Y Y Y UTR10 UTR10 UTR10 UTR10 Y**SHELF0 LTT17 TMS10****9.6.2.1.6 Table release history update**

DDRM node can now be datafilled in table LCMINV.

9.6.2.1.7 Supplementary information

None.

9.6.2.1.8 Translation verification other tools

LCMINV does not use translation verification tools.

9.7 Service Orders (SO) (CM & SESM)**9.8 Software optionality control (SOC)****9.9 Element Management****9.10 Command interface changes****9.11 Security****9.12 Configuration Walkthrough**

10: A00006661 Configuration (CN)

10.1 Feature name

DDRM Node Maintenance

10.2 Hardware and Software Requirements

DDRM should be connected to DDRM properly, and DDRM should be defined on the DMS switch. This is implemented by another Activity A00006660 “DDRM Node definition and Provisioning”.

10.3 Initial Configuration

Not Applicable.

10.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

10.5 Upgrade Impact

Not Applicable.

10.6 Data schema (DS) (CM, MIBS, RDB)

Not Applicable.

10.7 Service Orders (SO) (CM & SESM)

Not Applicable.

10.8 Software optionality control (SOC)

Not Applicable.

10.9 Element Management

Not Applicable.

10.10 Command interface changes

10.10.1 Directory: DDRMDIR

This feature implements commands in the DDRMDIR directory.

10.10.1.1 Directory description

The commands in this directory help the craft person to operate and maintain the DMS DICLE Remote Module (DDRM) at the node level.

The following figure shows the MAP view when DDRM is posted.

Figure 1 Functional Diagram

```

CM  MS  IOD  Net  PM  CCS  Lns  Trks  Ext  APPL
CM Flt SysB NOSMDR . 1SysB 1 PSET PS DF 37CC. . .
M  M  *C*      M  *C*  *C*  *C*
DDRM
0 Quit      PM      SysB  ManB  OffL  CBsy  ISTb  InSv
2 Post_     DDRM      0  0  0  0  0  0
3 ListSet
4      DDRM      Links OOS: Cside  Pside
5 Trnsl_   Unit0:
6 Tst_     Unit1:
7 Bsy_           11 11 11 11 11 RG:
8 RTS_     Drwr: 01 23 45 67 89 01 23 45 67 89
9 OffL_     .. -- -- -- -- -- -- -- --
10
11 Disp_
12 Next
13
14 QueryPM
15
16
17

```

10.10.1.2 Accessing directory: DDRMDIR

10.10.1.2.1 Access to directory or MAP level and return to CI

To access the DDRMMDIR level from the CI environment, type:

```
>MAPCI;MTC;PM;POST DDRM <node_no>
```

or

```
>MAPCI;MTC;PM;POST DDRM all
```

This is an example of entering the command:

```
>MAPCI;MTC;PM;POST DDRM 0
```

To return to the CI environment, type:

```
>QUIT ALL
```

10.10.2 Command: QUIT

10.10.2.1 Command type: MENU

10.10.2.2 Command target: All

10.10.2.3 Command availability: RES

10.10.2.4 Command description.

This command enables going to upper level.

10.10.2.5 Command syntax

Figure 2 DDRM QUIT command syntax

<pre>QUIT Parms: < nlevels incrname ALL ></pre>

10.10.2.6 Qualifications and warnings

No warnings are displayed.

10.10.2.7 Responses.

N/A.

10.10.3 Command: POST

10.10.3.1 Command type: MENU

10.10.3.2 Command target: All

10.10.3.3 Command availability: RES

10.10.3.4 Command description.

This command provide post specified PMs for maintenance.

10.10.3.5 Command syntax

Figure 3 DDRM POST command syntax

```

POST
Parms: [<All PMs> {AllPMs}]
  [<All> {All}]
  [<Site> STRING]
  [<Frame> {0 TO 511}]
  [<Unit> {0 TO 9}]
  [<PMType>... {TM2 [<All> {All}]}
    [<PMNo>... {0 TO 2047}],
    RMM [<All> {All}]
    [<PMNo>... {0 TO 254}],
    IDTC [<All> {All}]
    [<PMNo>... {0 TO 255}],
    ILCM [<All> {All}]
    [<Site> STRING]
    [<Frame> {0 TO 511}]
    [<Unit> {0 TO 9}]
    [<...> {0 TO 0}],
    ...
    DDRM [<All> {All}]
    [<Site> STRING]
    [<Frame> {0 TO 511}]
    [<Unit> {0 TO 9}]
    [<...> {0 TO 0}]]]
  [<State>... {SysB,
    ManB,
    OffL,
    CBSy,
    ISTb,
    InSv}]
  [<Alarm>... {Minor,
    Major,
    Crit}]

```

10.10.3.6 Qualifications and warnings

No warnings are displayed.

10.10.3.7 Responses.

N/A.

10.10.4 Command: LISTSET

10.10.4.1 Command type: MENU

10.10.4.2 Command target: All

10.10.4.3 Command availability: RES

10.10.4.4 Command description.

This Command lists the contents of the post set.

10.10.4.5 Command syntax

Figure 4 DDRM LISTSET command syntax

```
LISTSET

no parm - the current pm type on the screen
ALL      - The entire post set
Parms: [<PARMS> {TM2,
                  TM4,
                  ATM,
                  ILCM,
                  VLCM
                  DDRM}
```

10.10.4.6 Qualifications and warnings

No warnings are displayed.

10.10.4.7 Responses.

DDRM will be listed as below (example is given for 4 DDRM)

>post DDRM all >Listset	>post DDRM 1 >Listset
"DDRM 1,2,3,4."	"DDRM 1."

10.10.5 Command: TRNSL

10.10.5.1 Command type: MENU

10.10.5.2 Command target: All

10.10.5.3 Command availability: RES

10.10.5.4 Command description.

The Translate command identifies the C-side and P-side speech links of a posted DDRM. It also displays the status and type of the links, But for DDRM there is no P-Side link.

10.10.5.5 Command syntax

Figure 5 DDRM TRNSL command syntax

```
TRNSL: DISPLAY C SIDE LINK INFORMATION
Parms: <FUNCTION> {C}
```

10.10.5.6 Qualifications and warnings

The "TRNSL P" command is removed from the MAP screen as DDRM has no P-side links.

10.10.5.7 Responses.

For C-side, the TRNSL command gives the following responses. As for RLCM:

Link 1: PLGC 1 2;Cap MS;Status:OK ,P;MsgCond:CLS

Link 0: PLGC 1 0;Cap MS;Status:OK ,P;MsgCond:CLS

10.10.6 Command: TST**10.10.6.1 Command type: MENU****10.10.6.2 Command target: All****10.10.6.3 Command availability: RES****10.10.6.4 Command description.**

Tests the whole PM, a UNIT, or a LC. The ALL parameter will execute TST on all PMs in the post set of the same PM type as that displayed on the MAP.

The card configuration test will also be processed during this period. The test compares the card configuration on DDRM with the Static Data configuration.

BICRELAY (Bus Interface Card Relay) and Covrex¹ are not applicable to DDRM. But REX (Routine exercise) tests are applicable.

10.10.6.5 Command syntax

Figure 6 DDRM TST command syntax

```
TST
Parms: <DEVICE> {UNIT <UNIT_NO> {0 TO 1}
               [<ALL> {ALL}]},
               PM [<ALL> {ALL}],
               LC  <DRAWER_NO> {0 TO 19}
               REX <REX_ACTION> {ON,
                                OFF,
                                QUERY,
                                NOW [<NOWAIT> {NOWAIT}]}},
```

10.10.6.6 Qualifications and warnings

The “TST LINK” command is removed from the MAP screen as DDRM has no P side links.

The “TST DRWR2 command is replaced by the “TST LC” command. TST LC command has drawer numbers 0 to 19. It checks the Line Card Configuration on the DDRM side.

¹The voltage test and continuity test are not applicable for the POC card.

The “TST COVREX” command is removed from MAP screen too. Because COVREX test is not supported for DDRM.

10.10.6.7 Responses.

For the MANB unit OOS the test will be processed and the following results will be able to shown. (We suppose that unit 0 is MANB).

“Unit 0 OSvce Tests Initiated”

“Unit 0 Tst Passed” /Failed (if “Failed”, the reason will be shown)

For the InSv unit, the InSvce test will be processed and following results will be shown. (We suppose that unit 1 is InSv).

“Unit 1 InSvce Tests Initiated”

“Unit 1 Tst Passed” /Failed (if “Failed”, the reason will be shown)

For DRWR 0 the InSv test will be processed and the following results will be shown.

“InSvce Tests Initiated”

“Drwr 0 Tst Passed”

10.10.7 Command: BSY

10.10.7.1 Command type: MENU

10.10.7.2 Command target: All

10.10.7.3 Command availability: RES

10.10.7.4 Command description.

DDRM is posted to the ManB state via this command. The command is applicable for one or both units of the posted DDRM or to a specified P-side link.

10.10.7.5 Command syntax

Figure 7 DDRM BSY command syntax

```
BSY
Parms: <DEVICE> {UNIT <UNIT_NO> {0 TO 1},
      PM,
      DRWR <DRWR_NO> {0 TO 19}}
      [<FORCE> {FORCE}]
      [<NOWAIT> {NOWAIT}]
      [<ALL> {ALL}]
```

10.10.7.6 Qualifications and warnings

The “BSY LINK” command is removed from the MAP screen as DDRM has no P-side links.

For “BSY DRWR” command, DRAWER number is in the range 0 to 19.

“BSY SMEM” is removed as it is not supported for DDRM.

If DDRM is InSv following warning message will be shown

DDRM will be taken out of service

Please confirm ("YES", "Y", "NO", or "N"):

10.10.7.7 Responses.

After DDRM status changes to MANB, the following response will be shown:

“Bsy Passed”

10.10.8 Command: RTS

10.10.8.1 Command type: MENU

10.10.8.2 Command target: All

10.10.8.3 Command availability: RES

10.10.8.4 Command description.

Returns to service one or both units of a specified P-side link in a posted DDRM. Test routines are performed and RTS is executed if tests succeed. Each unit must be in the ManB or SysB state.

In the same way, inservice (InSv) and out of service comments will be processed for RTS as in the TST command. But with an exception, PM status can be set to InSv, ISTb or SysB as the result of these tests.

10.10.8.5 Command syntax

Figure 8 DDRM RTS command syntax

```
RTS
Parms: <DEVICE> {UNIT <UNIT_NO> {0 TO 1},
      PM,
      DRWR <DRWR_NO> {0 TO 19}}
      [<NOWAIT> {NOWAIT}]
      [<ALL> {ALL}]
```

10.10.8.6 Qualifications and warnings

The “RTS LINK” command is removed from the MAP screen as DDRM has no P-side links.

For the “RTS DRWR” command, the DRAWER number is in the range 0 to 19.

“RTS SMEM”, “RTS SWLD”, and “RTS FORCE” are removed as they are not supported for DDRM.

No warnings are displayed.

10.10.8.7 Responses.

After DDRM status changes to InSv, the following response will be shown for both units (X is unit #):

“Unit X OSvce Tests Initiated”

“Unit X Tst Passed”

“Unit X Rts Passed”

“Unit X InSvce Tests Initiated”

“Unit X Tst Passed”

10.10.9 Command: OFFL

10.10.9.1 Command type: MENU

10.10.9.2 Command target: All

10.10.9.3 Command availability: RES

10.10.9.4 Command description.

Simultaneously makes offline all the specified DDRM unit(s), the whole DDRM, or the posted set

10.10.9.5 Command syntax

Figure 9 DDRM OFFL command syntax

```
OFFL
Parms: <DEVICE> {PM [<ALL> {ALL}]},
          DRWR <DRWR_NO> {0 TO 19}}
```

10.10.9.6 Qualifications and warnings

For the “Offl DRWR” command, the DRAWER number is in the range 0 to 19.

DDRM should be MANB in order to set OFFLINE. If it is INSERVICE, the following message will be shown:

“Request Invalid: PM is InSv”

10.10.9.7 Responses.

After DDRM status changes to OFFL, the following response will be shown:

“Offl Passed”

10.10.10 Command: DISP

10.10.10.1 Command type: MENU

10.10.10.2 Command target: All

10.10.10.3 Command availability: RES

10.10.10.4 Command description.

Display all the PMs in the specified PM state. The DiagHist option displays a summary of the diagnostic failures.

10.10.10.5 Command syntax

Figure 10 DDRM DISP command syntax

```
DISP
Parms: <Option> {STATE <state> {SysB,
                                ManB,
                                OffL,
                                CBsy,
                                ISTb,
                                InSv},
                                DIAGHIST}
    [<PM Type> {TM2,
               TM4,
               ATM,
               TM8,
               MTM,
               ...
               DDRM} ]
```

10.10.10.6 Qualifications and warnings

No warnings are displayed.

10.10.10.7 Responses.

In the example, if we want to list offline PMs, the following response can be shown for offline PMs.

>Disp state offl

OffL DDRM : 0

10.10.11 Command: NEXT

10.10.11.1 Command type: MENU

10.10.11.2 Command target: All

10.10.11.3 Command availability: RES

10.10.11.4 Command description.

Step to the next PM in the post set or to the first PM of the next pm_type in the post set.

10.10.11.5 Command syntax

Figure 11 DDRM NEXT command syntax

```
Next
Parms: [<PM TYPE> {PMTYPE}]
```


10.10.11.6 Qualifications and warnings

No warnings are displayed.

10.10.11.7 Responses.

N/A.

10.10.12 Command: QueryPM**10.10.12.1 Command type: MENU****10.10.12.2 Command target: All****10.10.12.3 Command availability: RES****10.10.12.4 Command description.**

Query miscellaneous information about the DDRM. The information includes fault conditions on the posted DDRM units, the DDRM link and unit maintenance counters, and resetting the link and unit maintenance counters.

10.10.12.5 Command syntax

Figure 12 DDRM QueryPM command syntax

```
QueryPM
Parms: [<OPTION> {FLT,
          CNTRS [<CLEAR CNTRS> {CLEAR}],
          DRWR,
          LC}]
```

10.10.12.6 Qualifications and warnings

The “QUERYPM OOS” command is removed from the MAP screen as it is not supported for DDRM.

The “QUERYPM LC” command is added to the MAP screen to enable display of the Line Card status of DDRM.

No warnings are displayed.

10.10.12.7 Responses.

For the “FLT” option, suspected Cards will be listed with this command.

Suspected cards and their related alarms will be kept in a table which is implemented in Feature “DDRM ALARMS AND AUDITS” (fmdoc A00006665)

For the “QUERYPM LC” command LC status will be shown as for DRWRs.
Below is an example::

```
QueryPM LC

LC          11 1111 1111 2222 2222 2233 3333 3333
Number: 0123 4567 8901 2345 6789 0123 4567 8901 2345 6789
State :  .- - - - - - - - - - - - - - - - - - - - - - - - - - - -

LC          4444 4444 4455 5555 5555 6666 6666 6677 7777 7777
Number: 0123 4567 8901 2345 6789 0123 4567 8901 2345 6789
State :  - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

For the “CNTRS” option, the maintenance counters in “Table 4: OM fields for QueryPM CNTRS command” are shown

Table 1 OM fields for QueryPM CNTRS command

OM Fields	Explanation
WFSND	Wait for send timeout on message to LTC
WFNX	Wait for link idle after NACK
DNACK	(Double) negative acknowledgement
WFNR	Wait for link idle after positive acknowledgement
OVFL	Message has more than permitted number of bytes
IDL_STATE	Spurious frame output
RCVD_SUCC	Successfully received message count
IUC_NACK	IUC (Inter Unit Communication link) NACK received
IUC_INV_BYTE	IUC received an invalid byte
IUC_INV_MSG	IUC received invalid message
WFAK	Wait for acknowledgement timeout on the message to LTC
NACK	(Single) negative acknowledgement
WFMSG	Wait for start-of-message timeout on the message from LTC
CRC	Incorrect CRC on the received message
NULL_MSG	NULL message received that was not a reset message
INV_NODE	Message received had an invalid node number

OM Fields	Explanation
XMIT_SUCC	Successfully transmitted messages
IUC_INV_CHAR	IUC received an invalid character
IUC_INV_CKSM	IUC received an invalid checksum

10.10.13 Command: ABTK

10.10.13.1 Command type: NON-MENU

10.10.13.2 Command target: All

10.10.13.3 Command availability: RES

10.10.13.4 Command description.

This Command aborts all active maintenance tasks on the peripheral

10.10.13.5 Command syntax

There is no additional parameter, so directly run the “ABTK” command from the PM level while DDRM is posted.

10.10.13.6 Qualifications and warnings

No warnings are displayed.

10.10.13.7 Responses.

N/A.

10.10.14 Unsupported Non-Menu Commands

The following LCM commands in Table 5 are not supported by DDRM.

Table 2 Unsupported Non-Menu Commands for DDRM

Level and command	Explanation
ILD Remark: Not supported in CO	Used to access the ILD level.
ZLCM Remark: Does not exist in NTP	This sets the OFFICE_CAN_DATAFILL_ZLCM Parameter to ‘true’ or ‘false’.
OPM256	Can only be performed on an OPM (Outside Plant Module)
pretrip	AVAILABLE RINGING PRETRIP OPTIONS

10.11 Security

Not Applicable.

10.12 Configuration Walkthrough

Not Applicable.

11: A00006662 Configuration (CN)

11.1 Feature name

DDRM Line Definition and Line Maintenance

11.2 Hardware and Software Requirements

The DDRM should be connected to the DMS switch and the DDRM node should be maintained properly. These items are in the scope of the following two activities:

A00006660 - DDRM Node Definition

A00006661 - DDRM Node Maintenance

11.3 Initial Configuration

N/A

11.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

11.5 Upgrade Impact

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 Command interface changes

This feature adds a new CI command (DDRMLLEN), whose function is to transform the Physical View of a DDRM line's location (shelf, LC, slot) into the Logical View (line subgroup, circuit).

Table 1 DDRMLen CI command

Command Name	Abbreviation	Option	Parameters	Range
Transform DDRM shelf, LC, slot into LEN line subgroup, circuit	DDRMLen	SL (Shelf to LEN Mapping) or LS (LEN to Shelf Mapping)	shelf, LC, slot (for SL option) or line subgroup, circuit (for LS option)	shelf --> 0 to 3 LC --> 0 to 19 slot --> 0 to 7 LSG --> 0 to 19 circuit --> 0 to 31

Table 2 Examples

Some examples of legal commands
DDRMLen 0 1 6 % shelf 0, LC 1, slot 6
DDRMLen 1 19 3 % shelf 1, LC 19, slot 3
DDRMLen 2 4 0 % shelf 2, LC 4, slot 0
DDRMLen 3 10 7 % shelf 3, LC 10, slot 7
Some examples of illegal commands
DDRMLen 1 20 6 % DDRM shelves has only 20 LCs, ranging from 0 to 19.
DDRMLen 2 19 9 % slot must be in range 0 to 7
DDRMLen 5 1 3 % DDRM has only 4 shelves, ranging from 0 to 3

Table 3 System Responses

input	output
HELP DDRMLEN	DDRM line SHELF <-> DRAWER Mapping Tool. Parms: <Option> {SL [<Shelf> {0 TO 3}] [<LC> {0 TO 19}] [<Slot> {0 TO 7}], LS [<LSG> {0 TO 19}] [<Circuit> {0 TO 31}]}
DDRMLEN SL 0 2 7	Line Subgroup = 0, Circuit = 23
DDRMLEN SL 2 8 4	Line Subgroup = 12, Circuit = 3
DDRMLEN SL 2 19 9	Invalid Slot: Shelves have a maximum 7 slots available.
DDRMLEN LS 0 31	Shelf= 0, LC=3, Slot= 7

Note: The DDRMLEN command makes no assumptions about the actual system configuration. It simply reports what the line subgroup and circuit would be for a specified shelf, LC and slot, or vice versa.

11.11 Security

N/A

11.12 Configuration Walkthrough

N/A

12: A00006731 Configuration (CN)

12.1 Feature name

Handle Flash on Exit

12.2 Hardware and Software Requirements

There is no hardware or software dependencies.

12.3 Upgrade Impact

No impact on upgrades.

12.4 Data schema (DS) (CM, MIBS, RDB)

12.4.1 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)
IBNLINES	changed	unchanged

12.4.2 Table/MIB/Remote Database Schema information

12.4.2.1 Name: IBNLINES

IBN Line Assignment Table

12.4.2.1.1 Functional description

Table IBNLINES contains the line assignments for each 500/2500 set assigned to an Integrated Business Network (IBN), Residential Enhanced Services (RES), and Multiple Appearance Directory Number (MADN) station number. This table also contains the line assignments for the IBN attendant consoles (AC).

12.4.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

12.4.2.1.3 Size

Unchanged.

12.4.2.1.4 Fields/OIDs

The following table lists fields/OIDs for IBNLINES.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RESULT	Changed	OPTLIST	EOF	Option List. Added EOF to OPTLIST as another line option. Enter EOF for Exit On Flash option.

12.4.2.1.5 Datafill example

The following example shows sample datafill for table IBNLINES.

```
>table ibnlines
>list
LEN DNNO RESULT
-----
HOST 00 0 00 01 0 DT STN IBN 6210201 350 819_P621_2 L819_NILLA_2 819 (EOF) $
```

12.4.2.1.6 Table release history update

ISN08 - Feature (A00006731) Handle Flash on Exit adds new OPTLIST option EOF.

12.5 Service Orders (SO) (CM & SESM)**12.5.1 Service order change details****12.5.1.1 LCC and options**

New line option, EOF, can only be assigned to LCC of IBN.

Option EOF is not compatible with the following options and features:

CHD, CNF, CWI, CWX, CWT, CXR, FXR, DCBX, HLD, LDSA, LDSO, LDSR, LDST, LNPTST, MPB, PCWT, PRK, 3WC, 3WCPUB, VOWDN.

12.5.2 New commands**12.5.2.1 How service order options are presented****12.5.2.1.1 Description**

The EOF option enables the subscriber on the assigned line to exit on flash.

12.5.2.1.2 Example

Figure 1 Example of the EOF option in prompt mode

```
SERVORD
SO:
>ado
SONUMBER:      NOW    4    1 14 PM
>
DN_OR_LEN:
>6137220110
OPTION:
>eof
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 4 1 14 PM 6137220110 ( EOF ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>Y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>Y
```

Figure 2 Example of the EOF option in no-prompt mode

```
SERVORD
SO:
>ado $ 6137220110 eof $ Y Y
```

12.5.2.1.3 Option prompts

Table 3 System prompts for EOF option

Prompt	Valid input	Description	Areas affected by prompt
OPTION	EOF	Assigns Exit On Flash feature to line	None

12.5.2.1.4 Line class code compatibility

Table 4 EOF compatibility to LCC

Line class code	Compatible?
IBN	Yes

12.5.2.1.5 Option prerequisites

EOF has no prerequisites

12.5.2.1.6 Notes

None.

12.5.2.1.7 Feature identification

Feature number: A00006731

13: A00006980 Configuration (CN)

13.1 Feature name

AMA Module Code 130 Flexibility

13.2 Hardware and Software Requirements

No new software and hardware requirements.

13.3 Initial Configuration

The following provisioning is already present and initially required to append Module Code 130 to the AMA record. For more details, please refer to the NTP 297-9051-800 “DMS-100 MMP AMA Reference Guide”.

The capture of billing information from rejected calls is triggered by the option FLEXRJCT in table AMAXLAID and/or FLEXAMA. This option is referenced from the related translation tables. The FLEXRJCT option has the sub-field REJECTMOD. If this is set to Y, it appends the module 130 to the triggered AMA record.

However only FLEXRJCT does not trigger an AMA record by itself. Also, the SOC option BILL0003 “AMA Reject Call” must be active.

13.4 Upgrade Impact

None.

13.5 Data schema (DS)

13.5.1 New/modified tables

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

13.5.2 Table modification information

A new option is created in Table AMAOPTS. The name of the option is MC130_FOR_CLF and it is set to ON to activate this feature. The default value is OFF for this option.

While activating and deactivating this option, a caution is printed as given below to indicate the change in the functionality:

For activation (ON state):

“This change results MC130 generation for unanswered calls clear forwarded normally”

For deactivation (OFF state):

“This change prevents MC130 generation for unanswered calls clear forwarded normally”

13.5.2.1 Datafill example

Figure 1 Activating the new option MC130_FOR_CLF.

```
>table AMAOPTS
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: AMAOPTS
>pos MC130_FOR_CLF
MC130_FOR_CLF 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:
MC130_FOR_CLF ON
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
This change results MC130 generation for unanswered
calls clear forwarded normally.
TUPLE CHANGED
JOURNAL FILE INACTIVE
>
>pos MC130_FOR_CLF
MC130_FOR_CLF 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:
MC130_FOR_CLF OFF
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
This change prevents MC130 generation for unanswered
calls clear forwarded normally.
TUPLE CHANGED
JOURNAL FILE INACTIVE
>
>pos MC130_FOR_CLF
MC130_FOR_CLF OFF
>
```

Figure 2 The view of the option MC130_FOR_CLF in Table AMAOPTS

TABLE: AMAOPTS OPTION SCHEDULE ----- ... MC130_FOR_CLF ON

13.5.2.2 Functional description

This ISN08 activity is targeted to provide an optionality by datafill which allows the customer to append the Module Code 130 on tandem or terminating DMS-100 offices when a call is normally clear forwarded before the terminator goes off hook.

This optionality is provided by a new AMA option MC130_FOR_CLF in Table AMAOPTS.

If the MC130_FOR_CLF option is set to ON, MC130 is appended to the AMA records generated on the tandem or terminating DMS-100 offices for the clear forward messages (CLF) before terminator goes off hook, as well as the rejected calls.

If the MC130_FOR_CLF option is set to OFF, the MC130 is appended for only rejected calls as before.

13.6 Service Orders (SO) (CM & SESM)

Not applicable.

13.7 Software optionality control (SOC)

Not applicable.

13.8 Element Management

Not applicable.

13.9 Command interface changes

Not applicable.

13.10 Security

Not applicable.

13.11 Configuration Walkthrough

Not applicable.

14: A00007255 Configuration (CN)

14.1 Feature name

Dial Plan Enhancement for ETSI MWI TCAP

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)
OFCENG	default_mwi_xla_entry	DELETED	

14.4.2 Parameter information

14.4.2.1 DEFAULT_MWI_XLA_ENTRY

<DEFAULT_MWI_TRANSLATION_ENTRY>

14.4.2.1.1 Functional description

This parameter is already provided by the activity A59017265, please refer to the OP section of this activity for more details.

As a brief explanation, this office parameter provides a default entry point to translations for ETSI MWI requests. For the ETSI MWI implementation, message waiting indication requests are run through universal translations to determine the receiving user of the request.

14.4.2.1.2 Provisioning rules

This office parameter is removed by this activity. It is moved to a newly defined EMWI tuple in the ISERVOPT tuple as a parameter with same name. This is so that all the provisioning of the ETSI MWI can be performed in the same place.

14.4.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
0 alphanumeric characters	16 alphanumeric characters	NIL string

There is no change in the range of this office parameter.

14.4.2.1.4 Activation

Immediate

14.4.2.1.5 Dependencies

The string must exist as a tuple key in the table LINEATTR.

14.4.2.1.6 Consequences

If not present, MWI requests incoming on TCAP cannot be processed. A default value is not available for SMDI interfaces.

14.4.2.1.7 Verification

Perform traver for the incoming ISUP V2 and check the line attributes index being used.

14.4.2.1.8 Memory requirements

No memory impact.

14.4.2.1.9 Parameter release history update

The parameter is deleted. (It is moved into the EMWI tuple in the ISERVOPT table, additionally this parameter will be automatically transferred during ONP).

14.5 Upgrade Considerations

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)
ISERVOPT	Changed	Unchanged

14.6.2 Table/MIB/Remote Database Schema information

14.6.2.1 Name: ISERVOPT

This table is used to configure switch wide information for the service related feature.

14.6.2.1.1 Functional description

This activity introduces a new tuple named as EMWI in the ISERVOPT table.

Fields of the EMWI tuple:

- **DEFAULT_MWI_XLA_ENTRY:** indicates that the incoming TCAP message for the ETSI MWI request is translated according to the entered line attribute. This functionality is already provided, via the office parameter DEFAULT_MWI_XLA_ENTRY, by activity A59017265. This office parameter is moved to this ETSI MWI tuple in the ISERVOPT table to present whole ETSI MWI provisioning in one place. The functionalities of this field are same as the old office parameter as indicated below.

In case the controlling user, sending the request, is ETSI TCAP this field is always used to get the line attributes index to be used to access the translation system and the name of the index in the table LINEATTR.

In case the controlling user is SMDI, this field is used to enter universal translation, as stated above, if the line attributes index is not datafilled for the SMDI link in table SLLNKDEV.

If this field is left empty (NIL), which is the default datafill, ETSI MWI functionality is deactivated for TCAP controlling users.

If this field is left empty and no XLA_ENTRY option is datafilled in the table SLLNKDEV, ETSI MWI functionality is deactivated for SMDI controlling users.

- **ALLOW_NAC_IN_TCAP:** indicates that NAC is allowed or not in the called DN field of the TCAP message sent for MWI activation/deactivation

14.6.2.1.2 Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

14.6.2.1.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	0	1	

14.6.2.1.4 Fields/OIDs

The following table lists the fields/OIDs for the EMWI tuple of table ISERVOPT.

Table 5 Field descriptions for the EMWI tuple in the ISERVOPT table

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSKEY	NEW		EMWI	This is the key in ISERVOPT
OPTION	NEW		EMWI	This is the option name
DEFAULT_MWI_X LA_ENTRY	NEW		LINEATTR_ KEY	Translation of the incoming ETSI MWI message is done according to this LATTR index.
ALLOW_NAC_IN_ TCAP	NEW		Y, N	indicates NAC is allowed or not in the outgoing ETSI MWI TCAP message.

14.6.2.1.5 Datafill example

The following example shows sample datafill for table ISERVOPT.

```
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:
>EMWI
OPTION:
>EMWI
DEFAULT_XLA_ENTRY:
>100
ALLOW_NAC_IN_TCAP:
>n
TUPLE TO BE ADDED:
EMWI EMWI 100 N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
```

The tuple can be seen from the listing of the ISERVOPT table as follows:

Figure 1 The View of EMWI Tuple in ISERVOPT Table

```
>table iservopt
SOPTSKEY SOPTSVAR
-----
EMWI EMWI 100 N
```

14.6.2.1.6 Table release history update 14.6.2.1.7 Supplementary information

If MARKET_OF_OFFICE is AUSTRALIA, ALLOW_NAC field is set as ‘Y’ by default, in order not to affect existing behavior since this functionality is already provided for this market before.

This EMWI tuple is automatically added/updated during the ONP.

14.6.2.1.8 Translation verification and other tools I

SERVOPT table does not use translation verification tools.

15: A00007349 Configuration (CN)

15.1 Feature name

CPC Screening support for FDCP Trunks

15.2 Hardware and Software Requirements

There is no special Hardware / Software Requirements.

15.3 Initial Configuration

N / A.

15.4 Office/Subnet parameters (OP/SP) (CM & SESM)

N / A.

15.5 Upgrade Considerations

N / A.

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)
CPCCHAR	CHANGED	UNCHANGED

15.6.2 Table/MIB/Remote Database Schema information

15.6.2.1 Table Name: CPCCHAR.

15.6.2.1.1 Functional description

Table CPCCHAR is used to convert the protocol's CPC value into a generic protocol independent CPCNAME. This CPCNAME is then used for routing the call.

Each tuple in table CPCCHAR comprises of a CPCNAME, followed by between one and eight protocols, of which seven protocols are currently valid. Four of these protocols were introduced by feature AJ5343: BTUP, ETSIISUP, FTUP, and REDBKTUP. Three of these protocols, BZISUP, BZTUP and BZR2, are introduced by feature A59014287. Each protocol has a list of between one and sixteen CPC values to match. The CPC value is specified in decimal.

This feature adds to this set the **FDCP** protocol for MFC trunks using the FDCP platform. The fields in the CPCCHAR table for the FDCP protocol are shown in the table below.

Table 2 Field entries to CPCCHAR table for FDCP protocol

Field	Entry	Range
CPCNAME (key)	Unique CPCNAME	Alphanumeric
PROTOCOL	Protocol selector	FDCP
FDCP refinement	List of 1 to 16 CPC values	CP_ACTIVITY type

15.6.2.1.2 Usage sequence and implications (CM Only)

The current datafill order is unchanged.

15.6.2.1.3 Size

Table 3 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CPCCHAR	0	1024	

15.6.2.1.4 Fields/OIDs

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PROTOCOL	Changed	refinement	FDCP	See 12.5.2.1.1

15.6.2.1.5 Datafill example

The following examples shows datafill for the FDCP protocol in table **CPCCHAR**.

```

TABLE: CPCCHAR
>ran 2
  2 PROTLIST          CPCPROT_LIST
TYPE IS CPCPROT_LIST VECTOR OF UP TO 8 MULTIPLES WITH
  PROTOCOL
{BTUP,BZR2,ETSIISUP,FTUP,BZISUP,REDBKTUP,BZTUP,FDCP} RE
  FINEMENTS:
    {BTUP}          MULTIPLE WITH
      CPC          VECTOR OF UP TO 16 MULTIPLES WITH
        CPCVALUE BTUP_CPC_RANGE
    {FDCP}          MULTIPLE WITH
      CPC          VECTOR OF UP TO 16 MULTIPLES WITH
        CPCVALUE CP_ACTIVITY
    {BZTUP}          MULTIPLE WITH
      CPC          VECTOR OF UP TO 16 MULTIPLES WITH
        CPCVALUE BZTUP_CPC_RANGE
    {REDBKTUP}       MULTIPLE WITH
      CPC          VECTOR OF UP TO 16 MULTIPLES WITH
        CPCVALUE RED_BOOK_TUP_CPC_RANGE
    {BZISUP}          MULTIPLE WITH
      CPC          VECTOR OF UP TO 16 MULTIPLES WITH
        CPCVALUE BZISUP_CPC_RANGE
    {FTUP}           MULTIPLE WITH
      CPC          VECTOR OF UP TO 16 MULTIPLES WITH
        CPCVALUE FTUP_CPC_RANGE
    {ETSIISUP}       MULTIPLE WITH
      CPC          VECTOR OF UP TO 16 MULTIPLES WITH
        CPCVALUE ETSI_ISUP_CPC_RANGE
    {BZR2}           MULTIPLE WITH
      CPC          VECTOR OF UP TO 16 MULTIPLES WITH
        CPCVALUE {0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15}

```

```

TABLE: CPCCHAR
CPCKEY          PROTLIST
-----
BLOCKCPC (FDCP (MTC_EQ) (LOCAL_COIN) $) $

```

15.6.2.1.6 Datafill example

The following examples shows datafill for the FDCP protocol in table **R2PROT**.

TABLE R2PROT IDX	PHASES
OGACTCTL ICACTCTL	BASEDATA

GEOPROT1	
(162 163 162 163) (160 164 164 161) (162 164 164 163) (162 163 162 166)\$	
GEORGOG GEORGIC	
FDCP GEORGCAT (QUICK_REQ CAT_AFTER_1_DIG) \$	

In MFC calls, CPC and CLI are usually requested after all the called digits are already collected in the switch, and the CPC is received as a result of the CPC / CLI request (in *SMP_EVENT_INFO* message).

The option **QUICK_REQ** in the R2PROT table, allows requesting of CPC / CLI on the earliest stages of the call. If the value is: **CAT_AFTER_1_DIG**, the CPC without CLI will be included in the SMP_SETUP_REQUEST message in the field “Calling Party Category” after the 1st called digit.

15.6.2.1.7 Table release history update

15.6.2.1.8 Supplementary information

None.

15.6.2.1.9 Translation verification and other tools

- An example of TRAVER for CPC after the first called digit (in the SMP_SETUP_REQUEST message) may be found in the FN section.
- An example of TRAVER for CPC as a result of a CPC / CLI request (in the SMP_EVENT_INFO message) may be found in Figure 6.

15.7 Service Orders (SO) (CM & SESM)

N / A.

15.8 Software optionality control (SOC)

N / A.

15.9 Element Management

N / A.

15.10 User interface changes

N / A.

15.11 OSSGate Interface Changes

N / A.

15.12 Security

N / A.

15.13 Configuration Walkthrough

N / A.

16: A00007383 Configuration (CN)

16.1 Feature name

DNH (Directory Number Hunting) enhancements: pilot DN charge and display

16.2 Hardware and Software Requirements

The feature is developed in ISN08 (MMP21) s/w release and patched back to ISN04 (MMP17).

16.3 Initial Configuration

In loads older than ISN08 (MMP21), the patches containing the development code, are to be applied using the Post Release Software Manager (PRSM).

16.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

16.5 Upgrade Impact

16.5.1 Dump and Restore

Data of the only modified table ISERVOPT are transferred from the old s/w release to the new s/w release as usual within the data transfer process during ONP. Table changes do not require a reformat, since area refinement is added only.

It is obvious that if the table ISERVOPT being transferred, has the new tuple in the old release side, the patches must be applied in the new release side (unless the new release is ISN08 or higher).

16.5.2 Element Management Upgrade

Not applicable.

16.6 Data schema (DS) (CM, MIBS, RDB)

16.6.1 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)
ISERVOPT	changed	unchanged

16.6.2 Table/MIB/Remote Database Schema information

16.6.2.1 Name: ISERVOPT

International SERVice OPTion

16.6.2.1.1 Functional description

Operating company personnel use table ISERVOPT to configure switch information for service-related features. This table groups multiple related pieces of data in a single entry.

Each service that uses this table provides a subfield related to that service. Each subfield asks for information in a format relevant to the service. This table accepts an entry if operating company personnel enter a service that is in the load.

16.6.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

16.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISERVOPT	Unchanged	Current maximum tuples + 1	Memory is automatically allocated for additional tuple.

16.6.2.1.4 Fields/OIDs

The following table lists fields for ISERVOPT.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSKEY	Changed		DNH_OPTS	Directory Number Hunting Options. New entry DNH_OPTS in field SOPTSKEY is the key in ISERVOPT.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SOPTSVAR	Changed	OPTION	DNH_OPTS	Directory Number Hunting Options. New entry DNH_OPTS in field OPTION is the option name.
		PILOT_CHARGE	Y or N	PILOT_CHARGE controls activation of the Pilot Charge functionality. When PILOT_CHARGE is set to N, the Pilot Charge functionality has no impact. When PILOT_CHARGE is set to Y, the Pilot Charge functionality is activated. The default value is N.
		PILOT_DISPLAY	Y or N	PILOT_DISPLAY controls activation of the Pilot Display functionality. When PILOT_DISPLAY is set to N, the Pilot Display functionality has no impact. When PILOT_DISPLAY is set to Y, the Pilot Display functionality is activated. The default value is N.

16.6.2.1.5 Datafill example

The following example shows sample datafill for table ISERVOPT.

Figure 1 Map display example for DNH_OPTS option in table ISERVOPT

```

SOPTSKEY SOPTSVAR
-----
DNH_OPTS DNH_OPTS Y Y

```

Note: The following list gives datafill examples for the DNH_OPTS service. They are based on the four possible values for the DNH_OPTS tuple, namely: KEY (SOPTSKEY), OPTION (SOPTSVAR), PILOT_CHARGE, and PILOT_DISPLAY.

No enhancements are turned on:
DNH_OPTS DNH_OPTS N N

With this datafill neither functionality has impact. The tuple can be absent.

- Only the pilot charge enhancement is operational:
DNH_OPTS DNH_OPTS Y N
- Only the pilot display enhancement is operational:
DNH_OPTS DNH_OPTS N Y

- Both pilot charge and pilot display enhancements are operational;
DNH_OPTS DNH_OPTS Y Y

16.6.2.1.6 Table release history update

The following information was added:

- Entry DNH_OPTS added to field SOPTSKEY
- Entry DNH_OPTS added to field SOPTSVAR/OPTION
- New subfields PILOT_CHARGE and PILOT_DISPLAY added to entry DNH_OPTS in field SOPTSVAR/OPTION.

Maximum table size increased in number of one tuple.

16.6.2.1.7 Supplementary information

This table does not contain initial datafill. The operating company using this table provides datafill that refers to indicated services.

The default values of parameters PILOT_CHARGE and PILOT_DISPLAY are N. Even if tuple does not exist in ISERVOPT, the state is considered to be N for both functionalities. If the state of either parameter is Y, the respective functionality of the feature is available officewide. If the state is N, the respective functionality is suppressed.

PILOT_CHARGE and PILOT_DISPLAY require no restarts.

Every change of PILOT_CHARGE and PILOT_DISPLAY values including tuple addition/deletion is accompanied by displaying an appropriate message. This message informs a user about which functionality is activated/deactivated (one or both), briefly describes it, and informs a user about what actions are required from his side, if any. For more information please refer to section “Pilot DN Charge” in the FN portion of this feature.

16.6.2.1.8 Translation verification other tools I

SERVOPT does not use translation verification tools.

16.7 Service Orders (SO) (CM & SESM)

16.7.1 Service order change details

Only **pilot charge** functionality has impacts on Service Order.

The overall impact consists in **additional** servord **checking** carried out when the pilot charge functionality is in active state (subfield *PILOT_CHARGE* value is set ‘Y’ in the *DNH_OPTS* ISERVOPT tuple).

The brief background of this functionality explaining **why** additional SO checking is needed, is as follows.

The pilot DN charge functionality uses the existing line option **SPB** (SPeial Billing). The SPB option allows a number other than the subscriber's DN to be used for billing. To charge a pilot DN (PDN) for all the calls originated by its members DN (MDN), **every** single **MDN** of a DNH group **must have** the SPB option assigned on it, with the field **SPBDN** filled with the PDN of that group. The **PDN** is also charged for its own calls therefore it is **not allowed** to have the SPB option. Therefore any SO command that may **violate** this state, passes through additional checking to avoid this. Besides, in one special case the additional SO checking is done in order to only attract a user's **attention** to possible need of further actions. SO support performs **no automatic** actions. That means:

- All the DNH groups that exist **at the moment** of activation of the pilot charge functionality, must be checked by the TELCO personnel for the correspondence with the state described above, and appropriate actions should be taken to bring them into this state. When setting this functionality 'Y', a user gets a message - see "16.6.2.1.7 Supplementary information" on page 670, and also "Pilot DN Charge" in the FN portion of this feature.
- If a performed SO command did not pass additional checking, only an appropriate **message** is displayed, and the command is **rejected** (except for the one special case mentioned above when the additional checking **allows** the command). A user can then decide which further actions may be taken to archive the goal, or may not take action at all.

This feature does not introduce any new LCC.

This feature does not introduce any new option.

16.7.1.1 LCC and options

Neither a new LCC nor option is introduced by this feature.

All the limiting conditions of the SPB option remain valid.

This feature supports only **IBN** and **ISDNKSET** LCC.

16.7.2 New commands

This feature does not provide any new commands.

16.8 Software optionality control (SOC)

Table 4 SOC

SOC option name:	DNH Pilot Enh
SOC option title:	DNH Pilot Num for CLI and Billing
SOC option control type:	Tracked
New SOC option?	Yes
SOC option order code	SVBI0035
Option defined in DRU:	WT
Affected products:	DMS100

All tracked SOC are automatically created via PCA enforcement and no longer require design implementation.

16.9 Element Management

Not applicable.

16.10 Command interface changes

Not applicable.

16.11 Security

Not applicable.

16.12 Configuration Walkthrough

Not applicable.

17: A00007749 Configuration (CN)

17.1 Feature name

MG9000 ABI Support for LGCO, LGCOi

17.2 Hardware and Software Requirements

- The RMM has been installed in a MIS frame within 50 feet of the host peripheral
- A DS30A card has been installed in the host peripheral 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 PLGC load has been installed in the XPM

17.3 Initial Configuration

Not Applicable.

17.4 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable

17.5 Upgrade Considerations

The RMM load is unchanged by this activity and therefore is not required to be upgraded from the currently available load. All other loads are upgraded in the standard fashion and the upgrade procedure is not impacted by this activity.

The standard DMS processes for upgrade order applies to ABI XPMs. With regard to GWCs and XPMs, the XPMs are upgraded first, followed by the GWCs.

17.6 Data schema (DS) (CM, MIBS, RDB)

17.6.1 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)
Table LTCINV	Changed	Unchanged
Table RMMINV	Changed	Unchanged

17.6.2 Table/MIB/Remote Database Schema information

17.6.2.1 Name: TABLE RMMINV

Long Table Name: Remote Maintenance Module Inventory

17.6.2.1.1 Functional description

Table RMMINV contains the inventory list for all the RMMs provisioned in the office. Each tuple contains the RMM's site, the PEC code for the hardware, information about the RMM load, the EXEC lineup for the RMM, and finally, a pointer to the C-side peripheral upon which the RMM is hosted.

This activity has altered this table to allow the C-side PM to include a new allowable XPM type, PLGC.

17.6.2.1.2 Usage sequence and implications (CM Only)

Current datafill order is unchanged.

17.6.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
RMMINV	unchanged by this activity	unchanged by this activity	unchanged by this activity

17.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for RMMINV.

CSPMINFO = "<RMMLTC> <XPM Key from LTCINV> <Port Number of DS30A Link from LTCPSINV>"

For Example:

CSPMINFO = "RMMLTC PLGC 0 18"

where "PLGC 0" is the XPM key from LTCINV and "18" is the port number in LTCPSINV of a DS30A link on PLGC 0.

Note: It should be noted that the RMM Selector for the North American LTC and LGC peripherals is the same (RMMLTC). This is due to the fact that these peripherals are simply variations of the same hardware, and are also treated identically in the software.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CSPMINFO	Changed	The handling of the CSIDEPM has been modified such that when an RMM Selector of RMMLTC is entered the allowed C-side PM types now includes PLGC.	CSIDEPM	When RMMLTC is entered as the RMM Selector for the CSPMINFO field the user is then prompted for the name/number of the PLGC/LTC/LGC and the DS30A port to use (fields CSIDEPM and CSIDPORT). The DS30A port number must match that provisioned in table LTCPSINV for the XPM.

17.6.2.1.5 Datafill example

The following 3 examples show sample datafill for table RMMINV. The first example shows the provisioning of an RMM hosted on an SMA2, the second shows the provisioning of an RMM on an LTC, and the third shows the provisioning of an RMM on an LGC. The changes from the prior allowed datafill is highlighted with **bold** characters.

Example - RMM hosted on PLGC:

```

CI:
>table rmminv
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: RMMINV
>add
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
RMMNAME:
>rmmms rmm 5
FRTYPE:
>mis
FRNO:
>4
SHPOS:
>20
FLOOR:
>2
ROW:
>m
FRPOS:
>1
EQPEC:

```



```

>6x13aa
LOAD:
>rmm10a
EXECS:
>rsMex
RMMSELECTOR:
>rmm1tc
CSIDEPM:
>plgc 0
CSIDPORT:
>18
TUPLE TO BE ADDED:
RMMS      RMM  5      MIS   4      20      2      M      1 6X13AA      RMM10A
      RSMEX  RMMLTC      PLGC   0 18
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
Static data update for PLGC  0 UNIT 0 submitted.
Static data update for PLGC  0 UNIT 1 submitted.
Static data updates completed.
TUPLE ADDED
JOURNAL FILE INACTIVE
>

```

17.6.2.1.6 Table release history update

The following changes have been made to table RMMINV in this release:

1. For RMMSELECTOR of RMMLTC the following peripheral types are now supported for the CSIDEPM field:
— PLGC
2. The CSIDPORT for peripherals with a RMMSELECTOR of RMMLTC must be between 0 and 19. This is unchanged from previous releases and is simply shown for informational purposes.

17.6.2.1.7 Supplementary information

Limitations:

- The RMM is only supported on the PLGC ABI XPM. It should also be noted that the RMM is not supported on the legacy (ENET-based) version of this peripheral type.
- The CHANGE operation cannot alter the content of the C-side Port portion of the tuple. Any attempt to alter this value will result in an error and the tuple will be rejected by table control. If the C-side port information needs to be altered then the RMM must be deleted and re-added to the table. Note that this is not new behavior, it simply reflects the existing restriction for RMMs.

17.6.2.1.8 Translation verification and other tools

Output from the check all table control command and tabaudit will be included at a later date, but no issues are expected with these commands as the changes to RMMINV are minor.

17.6.2.2 Name: LTCINV

Full Table Name: Line/Trunk Controller Inventory Table

17.6.2.2.1 Functional description

Table LTCINV lists all the line and trunk controlling peripherals that were historically directly connected to the ENET (although this is no longer the case as of SN05 with the additional of the EXTDS512 optional field). Tuples are added to this table for PLGCs.

Prior to this activity the EXTDS512 optional attribute was only allowed to be provisioned on North American versions of host peripherals (LGC/LTC/SMA2/SMS). After this activity PLGC (the international variant of LGC) will be allowed to have the EXTDS512 optional attribute assigned to it as well.

There is no change in the format of the table or in the format of the optional field, all that has been changed is the types of peripherals that are allowed to have the field provisioned. All other types of peripherals that can be added in table LTCINV will continue to receive an error message if the EXTDS512 field is provisioned.

Note: Please refer to the documentation for SN05 activity A59038361 for more detailed information of the initial EXTDS512 design, and activity A00001847 documentation for details about the ABI expansion to include additional peripheral types in SN06.2/SN07.

17.6.2.2.2 Usage sequence and implications (CM Only)

Current datafill order unchanged (Table GATWYINV must be datafilled prior to adding EXTDS512 ABI peripherals in LTCINV).

17.6.2.2.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LTCINV	Unchanged by this activity.	Unchanged by this activity.	All existing tuples, regardless of whether the EXTDS512 attribute is provisioned or not, have the physical space allocated for the information contained in this field; therefore, there is no memory impact from this activity as the memory is already allocated for all tuples in this table.

17.6.2.2.4 Fields/OIDs

The following table lists fields for LTCINV.

CSLNKTAB = "\$"

OPT_ATTR = EXTDS512

When provisioning an external (non-ENET hosted) peripheral in LTCINV the EXTDS512 OPT_ATTR must be added. This optional attribute includes the SITE of the external XPM (must align with datafill in table SITE) and the Gateway Host information (Gateway Type and Gateway Number) as provisioned in table GATWYINV. Note that for ABI XPMs the Gateway Type must be ABI.

It should be noted that the CSLNKTAB portion of the tuple is not datafilled when adding external XPMs. The content of the CSLNKTAB field is automatically generated by the LTCINV code and no longer refers to real C-side links to the ENET. A "\$" should be entered when prompted for the CSLNKTAB entry (this is unchanged from SN05 behavior).

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CSLNKTAB	Changed	Unchanged from SN05	None	For External XPMs this field no longer contains real C-side ENET links. Instead, "\$" should be entered when prompted for this field. With this activity you should now enter "\$" when provisioning External PLGC tuples in LTCINV.
OPT_ATTR (EXTDS512)	Changed	Unchanged from SN05	Unchanged from SN05	When datafilling external PLGC peripherals you should add this field and enter the SITE of the ABI XPM and the Gateway information for the DS512 card (from table GATWYINV) in the MG9000.

17.6.2.2.5 Datafill example

The following example shows sample datafill for table LTCINV. The changes from standard ENET-based peripheral datafill is highlighted with **bold** characters.

```
TABLE: LTCINV
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
LTCNAME:
>plgc 5
ADNUM:
>1001
FRTYPE:
>ltei
FRNO:
>0
SHPOS:
>32
FLOOR:
>1
ROW:
>d
FRPOS:
>32
EQPEC:
>6X02NA
LOAD:
>OGI20AH
EXECTAB:
>KEYSET      KSETEX
EXECTAB:
>$
CSLNKTAB:
>$
OPTCARD:
>UTR15
OPTCARD:
>MSG6X69
OPTCARD:
>CMR13
CMRLOAD:
>CMR10A
OPTCARD:
>ISP
SLOT_NUMBER:
>16
OPTCARD:
>$
TONESET:
>CHINA100
PROCPEC:
>MX77AA MX77AA
EXTLINKS:
>0
E2LOAD:
>UPFWQM01
OPT_ATTR:
>EXTDS512
```

```

SITE:
>REM1
GTWY_HOST:
>ABI 3
OPT_ATTR:
>$
PEC6X40:
>6X40FC
EXTSHELF: N
>

```

The following shows the range values for the OPTATTR field of table LTCINV. Note that this has not changed from the SN05 version.

```

TABLE: LTCINV
>ran
 1 LTCNAME          XPM_KEY
 2 ADNUM            ADMIN_NUMBER
 3 FRTYPE           FRAME_NAME
 4 FRNO             FRAME_NO
 5 SHPOS            SHELF_POS
 6 FLOOR            FLOOR_POS
 7 ROW              ROW_POS
 8 FRPOS            FRAME_POS
 9 EQPEC            PEC
10 LOAD             NPMLOAD_INFO
11 EXECTAB          TERM_EXEC_TC_TAB
12 CSLNKTAB         XPM_NET_CSLINK_TC_TAB
13 OPTCARD          EXT_OPT_CARD_TC_TAB
14 TONESET          TONE_SET_TYPE
15 PROCPEC          XPM_PEC_AREA_TAB
16 EXTLINKS         NUM_EXT_LNKS_RANGE
17 E2LOAD           NPMLOAD_INFO
18 OPTATTR          LTCINV_OPT_ATTR_VECTOR
19 PEC6X40          NT_6X40_PEC
20 EXTINFO          EXTENSION_INFO
LOGICAL TUPLE TYPE: LTC_LOGTUPLE
>ran 18
18 OPTATTR          LTCINV_OPT_ATTR_VECTOR
TYPE IS LTCINV_OPT_ATTR_VECTOR VECTOR OF UP TO 13 MULTIPLES WITH
      OPT_ATTR      LTCINV_OPT_ATTR REFINEMENTS:
      {EXTDS512}    MULTIPLE WITH
          SITE      VECTOR OF UP TO 16 CHAR'S
          GTWY_HOST MULTIPLE WITH
              GTWY_TYPE {NLGW, ABI, CICM, GW, ITP, PVG, UAS}
              GTWY_NO  {0 TO 1023}
      OTHERWISE     LTCINV_OPT_ATTR_NIL_DATA

```

17.6.2.2.6 Table release history update

The following changes were made:

1. EXTDS512 OPT_ATTR is now allowed for PLGC peripheral type.
2. "\$" should be entered in the CSLNKTAB field for external XPMs (the C-side link information will be generated automatically).

17.6.2.2.7 Supplementary information

Limitations:

- The CSLNKTAB and EXTDS512 optional attribute must align in each tuple in LTCINV. This means that if EXTDS512 exists then a “\$” must have been entered in the CSLNKTAB field. A tuple must be either ENET based on External but not a combination of both.
- Multiple tuples of each type (ENET and External) can exist in the table at the same time.
- The EXTDS512 optional attribute can be provisioned only against LTC, LGC, SMA2, SMS, and PLGC peripheral types. Attempting to add the optional attribute to other peripheral types will result in the tuple failing verification and an error will be displayed. Note that this list includes both North American as well as International peripheral types.
- The derived CSLNKTAB entries for External XPMs cannot be changed by the user.
- The EXTDS512 optional attribute cannot be added to an existing tuple using the change command in table control, nor can it be removed using change.

17.6.2.2.8 Translation verification other tools

Output from the check all table control command and tabaudit will be included at a later date, but no issues are expected with these commands as the changes to LTCINV are minor.

17.7 Service Orders (SO) (CM & SESM)

Not Applicable.

17.8 Software optionality control (SOC)

Not Applicable.

17.9 Element Management

Not Applicable

17.10 User interface changes

MAP screen changes will occur for the PLGC exactly in the same way as was done for activity A00001847 - ABI Expansion. Please refer to the User Interface section of the CN Chapter of the documentation for activity A00001847 for more information.

The MAP displays will also be updated for the PLGC with the hosting of the RMM in the same way as was done with activity A00001898 - ABI RMM Support. Please refer to the User Interface section of the CN Chapter of the documentation for activity A00001898 for more information.

17.11 OSSGate Interface Changes

Not Applicable.

17.12 Security

Not Applicable.

17.13 Configuration Walkthrough

Not Applicable.

18: A00007793 Configuration (CN)

18.1 Feature name

IN: SCF Id, Correlation Id and QoR Base LNP Support (DACOM)

18.2 Hardware and Software Requirements

This activity is implemented in the ISN08 release.

18.3 Initial Configuration

None.

18.4 Office/Subnet parameters (OP/SP) (CM & SESM)

None.

18.5 Upgrade Considerations

None

18.6 Data schema (DS)

18.6.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SERVINFO	CHANGED	UNCHANGED

SERVINFO: Intelligent Network Service Information Table

Table SERVINFO contains information related to an international intelligent network (IN) service. Services are identified by the service index, which is the key to table SERVINFO. This gives the customer the ability to tailor and adapt IN services on a per-customer, per-service basis (Service Profiling).

18.6.1.1 New CORRELATIONID_TRANSPORT in the SRF_INFO option

18.6.1.1.1 Functional description

This activity introduces a new sub-option CORRELATIONID_TRANSPORT for the existing SRF_INFO option of the table SERVINFO. This is needed to meet the Dacom's requirement that the CorrelationID parameter from ETC operation should be handled as a separate parameter. For detailed information, please refer to the FN section of this activity.

The CORRELATIONID_TRANSPORT is set to the IN_CRID value to handle the CorrelationID as a separate parameter for Dacom, as shown in Figure 1 and 2.

18.6.1.1.2 Usage sequence and implications (CM Only)

None.

18.6.1.1.3 Size

The minimum and maximum number of tuples allowed in the table ISUPSVC is not changed by this activity.

18.6.1.1.4 Fields/OIDs

The following table lists fields/OIDs for the table SERVINFO:

Field	Subfield	New/ Change d/ Not changed	Required Entry for this feature	Explanation and action
SERVIDX	-	Not changed	0 to 9999	SERVINFO index. This field indicates an IN service on the DMS SSP switch. This field is the key from tables TRIGINFO and TRIGDIG. Enter a key number to uniquely identify the IN service.
OPTION	INITDP_PARMS, BILL_INFO, DIGIT_COLLECTI ON_INFO, SRF_INFO, RESPONSE_INFO , EDPS_INFO, MSG_INFO, TCAP_INFO, FI, CS1R, INITDP_EXTENSI ONS	Not changed	SRF_INFO	These are the main categories from which various per-service options and controls reside. For this feature SRF_INFO is datafilled in the OPTION field.
	SRF_INFO	Changed	(See subfields INTERNAL_SRF_INFO_ OPTION and EXTERNAL_SRF_INFO_ _OPTION)	INTERNAL_SRF_INFO is the existing suboption of the SRF_INFO. There is no change. EXTERNAL_SRF_INFO is newly added in this activity.

Field	Subfield	New/ Change d/ Not changed	Required Entry for this feature	Explanation and action
	INTERNAL_SRF_I NFO_OPTION	Not changed	\$	The existing subfield INTERNAL_SRF_INFO datafill is not needed in this feature.
	EXTERNAL_SRF_ INFO_OPTION	New	CORRELATIONID_TRA NSPORT (See subfield CORRELATIONID_TRA NSPORT_DATA)	This is the newly created option for CorrelationID in this feature. It can take the value: IN_CRID
	CORRELATIONID _TRANSPORT_D ATA	New	IN_CRID	In this feature, for Dacom, the CORRELATIONID_TRA NSPORT should be set to IN_CRID to handle the Correlation ID as a separate parameter.

18.6.1.1.5 Datafill example

The following figures show sample SERVINFO datafills for this feature:

Figure 1 Example datafill for the new DACOM CorrelationID option in table SERVINFO

```

CI:
>table servinfo
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: SERVINFO
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>Y
SERVIDX:
>99
OPTION:
>SRF_INFO
INTERNAL_SRF_INFO_OPTION:
>$
EXTERNAL_SRF_INFO_OPTION:
>CORRELATIONID_TRANSPORT
CORRELATIONID_TRANSPORT_DATA
>IN_CRID
EXTERNAL_SRF_INFO_OPTION:
>$
OPTION:
>$
TUPLE TO BE ADDED:
      99      (SRF_INFO $ (CORRELATIONID_TRANSPORT IN_CRID) $) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE

```

Figure 2 Example view of the new DACOM CorrelationID option in table SERVINFO

```

TABLE: SERVINFO

SERVIDX  OPTION
-----
99
(SRF_INFO $ (CORRELATIONID_TRANSPORT IN_CRID) $) $

```

18.6.1.1.6 Table release history update

None.

18.6.1.1.7 Supplementary information

None.

18.6.1.1.8 Translation verification and other tools

None.

18.6.1.2 New DACOM_EXT in the INITDP_EXTENSIONS option

18.6.1.2.1 Functional description

The other sub-option introduced in this activity is DACOM_EXT for the existing INITDP_EXTENSIONS option of the table SERVINFO.

The INITDP_EXTENSIONS is set to the DACOM_EXT, as shown in Figures 3 and 4, to append the Dacom specific extension to the operations InitialDP, CIRP (Call Information Report) and ERBCSM (Event Report BCSM). For detailed information, please refer to the FN section of this activity.

18.6.1.2.2 Usage sequence and implications (CM Only)

None.

18.6.1.2.3 Size

The minimum and maximum number of tuples allowed in the table ISUPSVCS is not changed by this activity.

18.6.1.2.4 Fields/OIDs

The following table lists fields/OIDs for the table SERVINFO:

Field	Subfield	New/ Changed/ Not changed	Required Entry for this feature	Explanation and action
SERVIDX	-	Not changed	0 to 9999	SERVINFO index. This field indicates an IN service on the DMS SSP switch. This field is the key from tables TRIGINFO and TRIGDIG. Enter a key number to uniquely identify the IN service.
OPTION	INITDP_PARMs, BILL_INFO, DIGIT_COLLECTIO N_INFO, SRF_INFO, RESPONSE_INFO, EDPS_INFO, MSG_INFO, TCAP_INFO, FI, CS1R, INITDP_EXTENSIO NS	Not changed	(See subfield INITDP_EXTEN SIONS)	These are the main categories from which various per-service options and controls reside. For this feature INITDP_EXTENSIONS is datafilled as option.
	INITDP_EXTENSIO NS	Changed	(See subfield INITDP_EXT_IN FO)	DACOM_EXT is newly added to the existing INITDP_PARM_EXT_TYPE.

Field	Subfield	New/ Changed/ Not changed	Required Entry for this feature	Explanation and action
	INITDP_EXT_INFO	New	DACOM_EXT	INITDP_PARM_EXT_TYPE {NATIONAL_FWD_CALL_IND, PRESENTATION_NO, LAST_DIV_LINE_ID,PARTIAL_CLI, CALLED_SUBS_BSM, CALLING_SUBS_BSM,CALLING_S UBS_OFM, CALLED_SUBS_TFM,CLI_NAME,SF _ENC,GAP_INT,NCPC, IN_CONT, DACOM_EXT }

18.6.1.2.5 Datafill example

The following figures show sample SERVINFO datafills for this feature:

Figure 3 Example datafill for the new DACOM_EXT option in table SERVINFO

```

CI:
>table servinfo
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: SERVINFO
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SERVIDX:
>9
OPTION:
>INITDP_EXTENSIONS
INITDP_EXT_INFO:
>DACOM_EXT
INITDP_EXT_INFO:
>$
OPTION:
>$
TUPLE TO BE ADDED:
      9      (INITDP_EXTENSIONS ( DACOM_EXT) $)$
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y
TUPLE ADDED
JOURNAL FILE INACTIVE

```

Figure 4 Example view of the new DACOM_EXT option in table SERVINFO

```

TABLE: SERVINFO
SERVIDX OPTION
-----
9
( INITDP_EXTENSIONS (DACOM_EXT) $) $

```

18.6.1.2.6 Table release history update

None.

18.6.1.2.7 Supplementary information

None.

18.6.1.2.8 Translation verification and other tools

None.

18.7 Service Orders (SO) (CM & SESM)

N/A.

18.8 Software optionality control (SOC)

N/A.

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: A00007807 Configuration (CN)

19.1 Feature name

Base ETSI ISUP V2 support for Dacom IN

19.2 Hardware and Software Requirements

This activity is supported only on the Gateway Controller (GWC) in International trunks load (GI).

19.3 Initial Configuration

None

19.4 Office/Subnet parameters (OP/SP) (CM & SESM)

None

19.5 Upgrade Considerations

None

19.6 Data schema (DS) (CM, MIBS, RDB)

19.6.1 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)
ISUPSVC	CHANGED	UNCHANGED

19.6.2 Table/MIB/Remote Database Schema information

19.6.2.1 Name: ISUPSVC

ISUP SerViceS

Table ISUPSVC holds entries for specific ISUP service behaviors. The presence of a service in a tuple means that the service is supported by trunks using that tuple. The datafilled option and suboption(s) specify the behavior of that service.

19.6.2.1.1 Functional description

This activity introduces the new services named ADDRESSING_METHOD and MARKET in table ISUPSVC.

19.6.2.1.2 Usage sequence and implications (CM Only)

It is necessary first of all to enter one or more tuples in table ISUPSVC. Afterwards, it is possible to add ISUPSVC options in table TRKOPTS. This allows the character string defined in table ISUPSVC to be seen by TRKOPTS.

19.6.2.1.3 Size

The minimum and maximum number of tuples allowed in the table ISUPSVC is not changed by this activity.

19.6.2.1.4 Fields/OIDs

The following table lists fields/OIDs for ISUPSVC.

Table 2 Table field descriptions

Field	Service	New or changed	Option	New or changed	Explanation and action
KEY					
SERVICE	MARKET ^{Note1}	NEW	KOREA	NEW	This is the market name
			SPARE1	NEW	For future use
			SPARE2	NEW	For future use
	ADDRESSING_METHOD ^{Note2}	NEW	SEPERATE_DIRECTORY_NUMBER	NEW	This is the addressing method
			SPARE1	NEW	For future use
			SPARE2	NEW	For future use

Note1 - Market option controls the handling of the behavior according to the market

Note2 - Addressing_method option controls the supporting of the NOA value #06

19.6.2.1.5 Datafill example

The following example shows sample datafill for table ISERVOPT.

Figure 1 Example of ISUPSVC datafill for MARKET and ADDRESSING_METHOD

>table isupsvc					
KEY	SERVIOCE				

TEST1	(	MARKET		(KOREA)\$)\$	
TEST2	(		ADDRESSING_METHOD		(
SEPERATE_DIRECTORY_NUMBER)\$)\$					

TDM/Carrier VoIP
Double click to update ProductName

Copyright © 2005 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-SN08-004
Product release: (I)SN08
Document release: Standard 01.03
Date: March 2005
Printed in the United States of America.