



ATM/IP Fault management

What's new in this release

The following table highlights the features introduced in this release. Refer to the OSS Advanced Feature Guide for more information about new features in this release.

Note: The terms Succession, Preside MDM and Passport 8600 have been re-branded in conjunction with the new Nortel Networks' brand simplified naming format. Succession is now Carrier Voice over IP (CVoIP), Preside MDM is now referred to as MDM, and Passport 8600 is now Ethernet Routing Switch 8600.

Table 1
(I)SN08 ATM/IP features (Sheet 1 of 9)

Feature descriptions
CS 2000 features A00006979 -- Synchronized Backup and Restore Manager (Intl IAW, NA PT-IP, NA UA-AAL1, NA UA-IP)

Table 1
(I)SN08 ATM/IP features (Sheet 2 of 9)

Feature descriptions
This feature implements a centralized mechanism for a synchronized backup of the following components • Integrated Element Management System (EMS) • CS 2000 Management Tools • MG 9000 Manager • CS 2000 Core Manager or Core and Billing Manager Note: The Integrated EMS may reside with the CS 2000 Management Tools applications on the CS 2000 Management Tools server. The Synchronized Backup Manager generates the following logs: • BKM600 for a successful backup • BKM601 for an unsuccessful backup • a security log when the Backup Manager is invoked by a user without the correct permissions A00007040 -- Intl R2 CAS framework - error handling support (Intl PT-IP) This SN08 activity provides error handling support for FDCP CAS in CS 2000. This feature handles errors encountered and reported by the Media Gateway (MG) to the Media Gateway Controller (MGC) during CAS call processing. CS 2000-Compact features A00008431 -- System Mastership for CS 2000-Compact Geographic Redundant configuration (NA IAC, NA PT-IP, NA UA-IP, Intl IAC, Intl IAW, Intl PT-IP, Intl UA-IP) This activity supports the Geographic Redundant (GR) configuration of the CS 2000-Compact by modifying the mastership selection algorithm to obtain better performance during normal and disaster scenarios. This feature creates the following logs and alarms: • CCA685 log • CCA 686 log • extended mate connection alarm GWC features A00007071 -- 3rd party Interopt profiles (Intl IAW)

Table 1
(I)SN08 ATM/IP features (Sheet 3 of 9)

Feature descriptions
This activity provides a flexible system for defining gateway profiles without making excessive, time-consuming software updates. This activity amends the alarm system to include new alarms related to the importation and removal of certificates. The alarms are triggered from the CS 2000 GWC Manager. The following conditions will generate alarms: • 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 existing gateways are still using the profile A00007102 -- GWC Telnet authentication (NA PT-IP, NA UA-IP, Intl IAW, Intl PT-IP, Intl UA-IP) In SN07, a GWC allowed serial port access with no login, telnet access from the SESM with no login, and telnet access protected by (a single hard-coded) password from any device. There is no idle timeout and no logging of access or commands used. Any user who learns to access PMDebug has full access to tools which range from viewing provisioning data to altering of memory contents on the device, and this can represent a security vulnerability. This activity adds to the secure-ability of the solution by providing a standardized user-id/password based login for the GWC devices. Central account management via the Integrated EMS allows existing defined accounts to be used, as authorized, instead of a separate password management strategy. Additional standard services like idle timeout and security logging are also provided. A00007102 -- Dual C-side IP for GWC (Intl IAW) This feature eliminates the requirement to provision a default gateway IP address when provisioning a GWC. The gateway IP are automatically provisioned for all GWCs. This eliminates provisioning errors. When the call server is an XA-Core, the two available core IP addresses are automatically distributed across the GWCs. A00007113 -- GWC External interface robustness (NA PT-IP)

Table 1
(I)SN08 ATM/IP features (Sheet 4 of 9)

Feature descriptions

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 the USP. New alarms are added to report communication path lost and new Operational Measurements (OMs) are collected by Integrated EMS every 5 minutes.

The customer will use the existing CS 2000 GWC Manager to view the new alarms. Integrated EMS 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 the table.

Session Server features

A00006893 -- TLS support for Session Server (NA UA-IP)

This feature allows the Session Server to establish Transport Level Security (TLS) sessions with a remote Call Server that is both SIP and TLS aware. TLS protocol sessions provide secure communications over non-secured networks. This protocol allows client/server applications to communicate with privacy, integrity, and communication.

This feature creates the following logs and alarms to support TLS:

- Logs
 - CRTM100
 - CRTM200
 - SIPS200
 - SIPS300
 - SIPS400
 - SIPS500
 - SIPS600
 - SIPS700
- Alarms
 - connection requests dropped
 - connection authentication failures
 - local certificate expiry

USP features

A00007576 -- Message Trace (NA PT-AAL1, NA PT-IP, NA UA-AAL1, NA UA-IP, Intl PT-AAL2, NA PT-IP, NA UA-IP)

Table 1
(I)SN08 ATM/IP features (Sheet 5 of 9)

Feature descriptions
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. Media Gateway 15000/Multiservice Switch 15000 features MG 9000 features A00006894 -- Internodal Emergency Stand Alone for MG 9000 InterNodal Emergency Stand Alone (ESA) provides the ability to make calls while in ESA between MG 9000 nodes. In doing so, the Telco's will also be provided the ability to provision a "Community of Interest" (COI) which defines which MG 9000 nodes can make ESA calls between one another. Calls can not be made between the two communities, only within a given community. If an MG 9000 does not have access to a LAN Switch, it will operate in the pre-SN08 manner of routing calls between VMGs within a single MG 9000 node. Also, although a COI is defined, each node must be in ESA for it to participate in the community. Nodes are not forced to enter ESA. This feature creates a new alarms that is generated whenever any node of the COI loses connectivity. A00007115 -- MG 9000 In-service fault isolation (NA UA-AAL1, NA UA-IP) This feature improves fault detection and recovery of MG 9000 ITP Digital Signal Processors (DSPs). This feature creates two new alarms. DPT Media Anchor features A00007120 -- DPT Media Anchor Introduction (NA IAC, NA PT-IP, NA UA-IP, Intl IAC, Intl IAW, Intl PT-AAL2, Intl PT-IP, Intl UA-IP)

Table 1
(I)SN08 ATM/IP features (Sheet 6 of 9)

Feature descriptions
This feature 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. The Audiocodes 2010/2020 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 CS 2000, 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. To better enable troubleshooting of 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 potential announcement, conference or BCT resource set up issues that require addressing. IW-SPM features A00007121 -- IW-SPM 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. This feature also creates the following new logs: • IWBM502 • IWBM503 • IWBM504 • IWBM505 Integrated EMS features A00007302 -- Integrated EMS-Core Element Manager integration (NA UA-AAL1, NA UA-IP)

Table 1
(I)SN08 ATM/IP features (Sheet 7 of 9)

Feature descriptions
This feature integrates the functionality of CEM (Core Element Manager) to the Integrated EMS. The CEM includes the Resource Discovery (RD), Fault Management (FM) and Performance Management (PM) support for the CS 2000. Adding, deleting and managing CEM will be possible from Integrated EMS. The CEM system is the Nortel implementation of a Element Management System. It provides the following features: • 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 CEM, installed on a PC or Sun platform. • Mediation functionality (data accumulation, filtering, manipulation, and transfer) between the network elements and the CEM workstation. CS 2000 Core Manager/CBM features A00007602 -- SDM software authenticity (NA PT-IP) This feature adds additional security to the SDM software delivery and provides a guarantee that the SDM deliverable sent to the field is authenticated by Nortel. New alarms and security logs are created by this feature to reflect patch signature check failures. CS 2000 Management Tools features A00008338 - QCA Log/Alarm Consolidation (NA IAC) It is the purpose of this activity is to design a method for reporting Quality of Service (QoS) parameters on a per call basis for the purposes of • Network engineering • Trend analysis • Trouble-shooting network problems • SLA validation This feature generates several logs and alarms.

Table 1
(I)SN08 ATM/IP features (Sheet 8 of 9)

Feature descriptions
A00008902 -- Adding category and cause values to CS 2000 SAM21 Manager alarms (NA UA-AAL1) In the pre-SN08 CS 2000 SAM21 Manager implementation, the Manager generated syslogs for alarms do not contain values for category or probable cause. Also, the Manager used a field name 'Reason:' instead of 'Description:' to provide details about the alarm. Therefore, CS 2000 SAM21 Manager alarms were not correctly categorized by Integrated EMS, nor was the Reason information displayed in the Integrated EMS message field. This feature adds the category and probable cause to the body of the CS 2000 SAM21 Manager alarm logs. In addition, Integrated EMS will put the contents of the Reason information from the log into its message field. These changes make the CS 2000 SAM21 Manager alarm logs consistent with other application fault logs when they are displayed by Integrated EMS or sent northbound.
MG 9000 Manager features A00007213 -- MG 9000 5 and 30 minute OM's (NA UA-AAL1, NA UA-IP) This feature allows the user to configure sample and summary intervals on the MG 9000 using the MG 9000 Manager. This feature generates a log when OM Data Collection fails or the failure condition is cleared. A00007415 -- Internodal ESA for the MG 9000 Manager (NA UA-AAL1, NA UA-IP) Internodal ESA provides the ability to make calls while in ESA between MG 9000 nodes. In doing so, the Telco's will also be provided the ability to provision a "Community of Interest" (COI) which defines which MG 9000 nodes can make ESA calls between one another. A community must have access to a LAN Switch (i.e. Media Gateway 15000 or equivalent) in order for Inter Nodal ESA calls to complete. This feature will cause an alarm to be generated by a node when it cannot communicate with a peer node in the community.
TOPS features A00007271 - TOPS EOL for SN08 (NA PT-AAL1, NA PT-IP, Intl PT-IP)

Table 1
(I)SN08 ATM/IP features (Sheet 9 of 9)

Feature descriptions
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 Enhanced TOPS Message Switch (ETMS) functionality. • Disables the TOPS Operator Centralization (OC) via ETMS functionality. • Identifies usage of OSSAIN Management Information System (MIS) in TOPS EOL logs. • Removes tables, parms, and OM groups which are obsolete.
A00007713 - TOPS-IP Robustness (NA PT-AAL1, NA PT-IP, Intl PT-AAL2, Intl PT-IP) This 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;topspol 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;topspol level is enhanced to display the auto-compression status for the posted position.

Fault management strategy

In all CVoIP solutions, fault management capabilities provide three main functions:

- Fault delivery
- Testing and diagnostic capabilities
- OSS interface

Fault Delivery

Log reports

A log report is a record of a message that the system generates when a significant event occurs in a network element. Log reports include status and activity reports, as well as reports on hardware or software faults, test results, changes in state, and other events or conditions likely to affect the performance of the switch. Either a system or a manual action can generate a log report.

Log adapter The SCC2/STD log adapter receives CS 2000, MG 4000, IW SPM, DPT SPM, MDM, and Multiservice Switch/Media Gateway logs. The adapter is a one-way translator that translates events received from network managers and network elements into the format required by the customer log system. The interface between the Log Adapter and CS 2000 Core Manager applications is the CORBA interface. When the system starts up, the Log Adapter application registers with the CS 2000 Core Manager applications for events that the Log Adapter will report to the fault OSS.

The primary events are

- alarm-raised
- alarm-cleared
- service state change

When the Log Adapter receives an event, it converts the event into an SCC2 or DMS STD format and sends the log to the Log Delivery application.

For more information on the CVoIP Log Delivery application, refer to *Core and Billing Manager 850 Fault Management*, NN10351-911.

Log Delivery application The Log Delivery application provides log reports in Switching Control Center 2 (SCC2) format. Log reports in SCC2 format do not specify the switch or network element name. The Log Delivery application transfers log reports in normal ASCII text across a TCP/IP connection to the fault OSS.

The log categories are fault and status changes. The network elements detect, timestamp, and log the event on a log report.

For more information on the CVoIP Log Delivery application, refer to *Core and Billing Manager 850 Fault Management*, NN10351-911.

Alarms

Alarms provides notice of problems or conditions that can change the performance or working state of a network or network element. Daily operation of the network requires monitoring for alarms and checking that functions continue without interruption. Alarms provide notification that a system hardware or software-related event has occurred.

The following list shows the fault delivery features available:

- Fault collecting and reporting
- Fault isolation and identification
- Storage, delivery, and formatting (Operational Support Systems [OSS] interfaces)

Testing and Diagnostics

The following list shows the testing and diagnostic capabilities available:

- Line and loop testing
- Trunk and carrier testing
- ATM loopback testing
- Routine exercise testing
- Misconnected link diagnostics
- USP message tracing tool

Line and loop testing

For additional information on line or loop test, refer to the following component documentation:

- Access Care product documentation
- *MG 9000 Fault Management module*, NN10074-911
- DMS legacy documentation

Trunk and carrier testing

PT-AAL1 trunk testing capabilities Developed for the AAL1 hybrid switch configuration contains an ENET and an Integrated Service Module. The ISM is specifically designed to accommodate a variety of test hardware which can perform maintenance testing on TDM trunks. This solution takes advantage of the TDM to IP bridge capabilities of the IW-SPM, to provide connectivity between the Gateway TDM trunk under test and the test hardware located in the ISM.

Both solutions are fully integrated with the XA-Core. This means that test execution, results and logs are equivalent to the Legacy TDM environment.

The Hybrid Switch Solution supports the following trunk test functionality. Customers can test TDM trunks via the MAPCI TTP level

and ATT level interfaces. The applicable Nortel documentation reference is provided for each MAPCI level.

Table 2 TTP level commands (297-8001-821, Volume 10)

Command	Description
CktInfo	Displays the name and state of the PM and the state of the circuit of a trunk
Ckt	Connects a specified circuit to a trunk
StkSdr	Allows access to the Stuck Sender feature, which identifies trunks with outpulsing problems.

Table 3 Manual level commands (297-1001-821, Volume 7)

Command	Description
LOSS	Manually measures transmission loss
TGEN	Manually generates a tone of desired frequency and level
Noise	Manually measures transmission noise
OP	Permits the ability to seize and outpulse a set of desired digits over a trunk
TDet	Manually measures the presence of an incoming tone
HSet	Connects an available headset to a trunk
SGNL	Executes a bit signaling test on a trunk
TST	Permits the user to run a number of supported tests, including the following: • ISUP continuity test (ICOT) • T100 (originating and terminating) • T102 (originating and terminating) • T104 (originating and terminating) • T105 (originating and terminating)

Table 4 Monitor level commands (297-8001-821, Volume 7)

Command	Description
MonPost	Provides the user the ability to monitor a trunk circuit in posted position
MonLink	Provides the user the ability to monitor a trunk circuit in the linked position
Montalk (L)	Listen provides the user the ability to monitor a trunk circuit in both directions in a listen only mode.
Montalk (T)	Talk provides the user the ability to monitor a trunk circuit in both directions while participating in the call (listen and talk mode).
CktMon	Displays messages on the MAP from the digital PM of the circuit without interrupting normal call processing.
CPos	Executes a test to a Centralized Automatic Message Accounting (CAMA) or Remote Operator Number Identification (RONI) trunk.

Table 5 C7TTP level commands (297-1001-821, Volume 2)

Command	Description
CVTest	Performs a Circuit Validation Test on a trunk
TrkQry	Displays the local or remote state of a trunk
QrySig	Queries the signaling availability and the state of a trunk
RouteSet	Displays the route set CLLI of a CCS7 trunk
CIC	Displays the circuit identification code of a trunk

Note: All commands at the Automatic Test Trunk (ATT) level are supported.

The following tests are supported but are not supported by the MAPCI. Refer to the *DMS-100 Family Maintenance and Operations Manual*,

297-8991-500, or the *DMS-100 Family Trunks Maintenance Guide*, 297-1001-595 for more information.

- T108 Terminating Test Line - a non-inverting digital loopback connection
- T101/C101 trunk call
- Digital Remote Office Test Line (ROTL) - 100/200 trunk types only

Note: Additional equipment is required.

- Automatic Trunk Routing (ATR) - 250 trunk types only

Note: Additional equipment is required.

PT-IP trunk testing capabilities There are currently two solutions for trunk troubleshooting in the PT-IP solution:

- Hybrid switch solution (AAL5 IP only)
- Non-hybrid/CS 2000-Compact solution (AAL2 and AAL5)

Developed for the AAL5 hybrid switch configuration, the Hybrid switch solution contains an ENET and an Integrated Service Module (ISM). The ISM is specifically designed to accommodate a variety of test hardware which can perform maintenance testing on TDM trunks. This solution takes advantage of the TDM to IP bridge capabilities of the IW-SPM, to provide connectivity between the Gateway TDM trunk under test and the test hardware located in the ISM.

Developed for the AAL2 and AAL5 switch configurations that do not contain an ENET or ISM, the solution utilizes the 3rd party Media Server 2000 Series as a limited replacement for the ISM. The MS 2000 Series provides the trunk test functionality to the Gateway TDM trunk under test.

Both solutions are fully integrated with the XA-Core. This means that test execution, results and logs are equivalent to the Legacy TDM environment. However, since the Hybrid solution utilizes the ISM, there are more trunk testing options available to the customer than the initial Non-hybrid/CS 2000-Compact solution.

The Hybrid Switch Solution supports the following trunk test functionality. Customers can test TDM trunks via the MAPCI TTP level

and ATT level interfaces. The applicable Nortel documentation reference is provided for each MAPCI level.

Table 6 TTP level commands (297-8001-821, Volume 10)

Command	Description
CktInfo	Displays the name and state of the PM and the state of the circuit of a trunk
Ckt	Connects a specified circuit to a trunk
StkSdr	Allows access to the Stuck Sender feature, which identifies trunks with outpulsing problems.

Table 7 Manual level commands (297-1001-821, Volume 7)

Command	Description
LOSS	Manually measures transmission loss
TGEN	Manually generates a tone of desired frequency and level
Noise	Manually measures transmission noise
OP	Permits the ability to seize and outpulse a set of desired digits over a trunk
TDet	Manually measures the presence of an incoming tone
HSet	Connects an available headset to a trunk
SGNL	Executes a bit signaling test on a trunk
TST	Permits the user to run a number of supported tests, including the following: • ISUP continuity test (ICOT) • T100 (originating and terminating) • T102 (originating and terminating) • T104 (originating and terminating) • T105 (originating and terminating)

Table 8 Monitor level commands (297-8001-821, Volume 7)

Command	Description
Montalk (L)	Listen provides the user the ability to monitor a trunk circuit in both directions in a listen only mode.
Montalk (T)	Talk provides the user the ability to monitor a trunk circuit in both directions while participating in the call (listen and talk mode).
CktMon	Displays messages on the MAP from the digital PM of the circuit without interrupting normal call processing.
CPos	Executes a test to a Centralized Automatic Message Accounting (CAMA) or Remote Operator Number Identification (RONI) trunk.

Table 9 DATATTP level commands (297-1001-821, Volume 3)

Command	Description
Bertime	Sets the length of time a BERT will run
BTerm	Sets the type of outpulse or digits for a BERT
BERT	Executes a Bit Error Rate Test on a trunk

Table 10 C7TTP level commands (297-1001-821, Volume 2)

Command	Description
CVTest	Performs a Circuit Validation Test on a trunk
TrkQry	Displays the local or remote state of a trunk
QrySig	Queries the signaling availability and the state of a trunk
RouteSet	Displays the route set CLLI of a CCS7 trunk
CIC	Displays the circuit identification code of a trunk

Note: All commands at the Automatic Test Trunk (ATT) level are supported.

The following tests are supported but are not supported by the MAPCI. Refer to the *DMS-100 Family Maintenance and Operations Manual*, 297-8991-500, or the *DMS-100 Family Trunks Maintenance Guide*, 297-1001-595 for more information.

- T108 Terminating Test Line - a non-inverting digital loopback connection
- T101/C101 trunk call
- Digital Remote Office Test Line (ROTL) - 100/200 trunk types only

Note: Additional equipment is required.

- Automatic Trunk Routing (ATR) - 250 trunk types only

Note: Additional equipment is required.

The Non-Hybrid/CS 2000-Compact Switch Solution supports the following trunk test functionality. Customers can test TDM trunks via the MAPCI TTP level and ATT level interfaces. Trunk test functionality is provided by the Media Server 2000 series products, MS 2010 (AAL5) and MS 2020 (AAL2). The applicable Nortel documentation reference is provided for each MAPCI level.

Table 11 TTP level commands (297-1001-821, Volume 10)

Command	Description
CktInfo	Displays the name and state of the PM and the state of the circuit of a trunk
StkSdr	Allows access to the Stuck Sender feature, which identifies trunks with outpulsing problems

Table 12 Manual level commands (297-1001-821, Volume 7)

Command	Description
OP	Permits the ability to seize and outpulse a set of desired digits over a trunk

Table 12 Manual level commands (297-1001-821, Volume 7)

Command	Description
SGNL	Executes a bit signaling test on a trunk
TST	Permits the user to run a number of supported tests, including the following: • ISUP continuity test (ICOT) • T100 (originating and terminating) • T102 (originating and terminating) • T105 (originating and terminating) Note: T105 termination on the MS 2000 series supports only the LSC, L, NSC, RN, N, and NT subtests.

Table 13 Monitor level commands (297-8001-821, Volume 7)

Command	Description
CktMon	Displays messages on the MAP from the digital PM of the circuit without interrupting normal call processing.

Table 14 C7TTP level commands (297-1001-821, Volume 2)

Command	Description
CVTest	Performs a Circuit Validation Test on a trunk
TrkQry	Displays the local or remote state of a trunk
QrySig	Queries the signaling availability and the state of a trunk
RouteSet	Displays the route set CLLI of a CCS7 trunk
CIC	Displays the circuit identification code of a trunk

Note: All commands at the Automatic Test Trunk (ATT) level are supported.

The T108 Terminating Test Line test is supported but is not associated with the MAPCI. Refer to the *DMS-100 Family Maintenance and Operations Manual*, 297-8991-500 for more information.

Testing for DMS and SPM-based equipment For DMS and SPM-based equipment, the customer can test equipment and the ATM layer using the test command that is supported on the CS 2000 Core Manager CLUIs. The equipment consists of hardware including the CEM and RMs. All other diagnostics, including testing of trunks and carriers, are tested at the carrier and trunk test position (TTP) levels of the MAP interface.

Note: For additional information on trunk testing, see [Fault management trunk testing](#) in this Fault Information module.

The customer cannot set parameters for testing. There are only two types of service diagnostics:

- in-service (InSv) test that runs while the system is InSv
- out-of-service (OOS) test that runs while the system is OOS

The InSv test can change states, but the OOS test cannot. If the InSv test fails, noncritical test failure causes the unit to become in-service trouble (ISTb). However, the system continues to generate the noncritical fault log. Critical test failure results in trigger recovery and causes the unit to become system busy (SysB). The system discontinues fault reporting during critical test failure.

Trunk testing using the ISM/MTM with an IW-SPM This was developed for the IP Hybrid (AAL5) switch configuration, which contains an ENET and Integrated Service Module (ISM) or Maintenance Trunk Module (MTM). The ISM or MTM is specifically designed to accommodate a variety of test hardware which can perform testing on TDM trunks. This solution takes advantage of the TDM to IP bridge capabilities of the IW-SPM to provide connectivity between the Gateway TDM trunk under test and the test hardware located in the ISM or MTM.

The following trunk testing commands are available.

Command
MAPCI TTP level commands CktInfo, Ckt, StkSdr
MAPCI Manual level commands Loss, TGen, Noise, OP, TDet, HSet, SGNL
TST command options ICOT, T100, T102, T103, T104, T105
MAPCI Monitor level commands Montalk L & T, CktMon, Cpos
MAPCI DATATTP level commands Bertime, BTerm, BERT
MAPCI ATT level commands TestReq, LstStop, LstWait, LstCLLI, DelMan, Stop, Start, HaltATT, RunATT, SetSTst
MAPCI C7TTP level commands CVTest, TrkQry, QrtSig, RouteSet, CIC
Additional tests supported but not associated with the MAPCI T108 Terminating Loopback Test Line T101/C101 Trunk Call

Trunk testing on the Call Agent This solution was developed for the ATM (AAL2) and IP (AAL5) Compact switch configurations that do not contain an ENET or ISM/MTM. The solution utilizes a combination of 3rd party test equipment as well as non-hardware related MAPCI trunk test commands. Either the UAS with Sage 945RTS test unit or the MS 2000 Series can be used in this solution as a limited replacement for the ISM/MTM.

The following trunk testing commands are available on the Call Agent.

Command
MAPCI TTP level commands CktInfo, StkSdr
MAPCI Manual level commands OP, SGNL

Command**TST command options**

ICOT, T100, T102, T105

Note: T100, T102, and T105 support is available through the UAS/Sage or MS 2000 Series

MAPCI Monitor level commands

CktMon

MAPCI ATT level commands

TestReq, LstStop, LstWait, LstCLLI, DelMan, Stop, Start, HaltATT, RunATT, SetSTst

MAPCI C7TTP level commands

CVTest, TrkQry, QrtSig, RouteSet, CIC

Additional tests supported but not associated with the MAPCI

T108 Terminating Loopback Test Line

Trunk testing with the UAS An H.248 configured UAS supports testing trunks on TDM trunk gateways in CVoIP networks deployed in North America. Trunk testing with the UAS is provided in combination with a Sage 945RTS test unit, which has T1 interfaces directly connected to the UAS (to the AG4000 card in an ATM configuration or CG6000 card in an IP configuration).

The Sage test unit will be configured to support a combination of types of tests based on the engineering of the customer's network. Each DS0 circuit to the Sage is dedicated to one type of trunk test. Parallel provisioning will exist on the UAS node to group circuits supporting the same test type into trunk groups. Each test type will have its own trunk group. The provisioning and data representation for these resources are provided by separate features with the UAS.

The Test Line trunk tests currently supported by the UAS with Sage:

- TL100, which provides far-to-near end signal loss and noise measurements.

Note: The Sage 945RTS does not provide a TL100 trunk test as defined by GR-822 (Issue 1, December 1995). It provides instead a silent termination TL100 trunk terminator.

- TL102, which provides far-to-near end signal loss measurement.
- TL105, which provides two-way signal loss and noise measurements along with noise and loss self check (if available).

The above tests are available for both origination and termination and are fully integrated with the XA-Core. This means that test execution, results and logs are equivalent to the traditional TDM environment. Available for IP (AAL5) in SN06 and for ATM (AAL2) in SN06.2.

Trunk testing using the MS 2000 Series An H.248 configured MS 2010 or MS 2020 supports testing trunks on TDM trunk gateways in CVoIP networks deployed in North America. Trunk testing is provided directly from the MS 2000 Series and requires no additional hardware unlike the UAS.

The Test Line trunk tests currently supported by the MS 2000 Series include the following tests:

- TL100, which provides far-to-near end signal loss and noise measurements.
- TL102, which provides far-to-near end signal loss measurement.
- TL105, which provides two-way signal loss and noise measurements along with noise and loss self check (if available).

The above tests are available for both origination and termination and are fully integrated with the XA-Core. This means that test execution, results and logs are equivalent to the traditional TDM environment. Available for IP (AAL5) is the MS2010 in SN06.2 and for ATM (AAL2) is the MS 2020 in SN07.

ATM loopback testing

ATM Loopback testing is used for on-demand connectivity monitoring and fault localization on AAL1 bearer connections, as well as AAL5 PVCs and SVCs, and pre-service connectivity verification on AAL5 PVCs. A loopback test or trace through I.610 or Multiservice Switch proprietary OAM cells on ATM connections can be performed on any ATM-equipped CVoIP Spectrum peripheral (MG 4000, IW -SPM (ATM),

DPT-SPM, MG 9000). This functionality is available through three different MAP levels:

- CoreConn level
- PeerConn level
- BearConn level

In addition, the *AtmLb* command is available for use at any MAP level for loopback requests.

CoreConn level The CoreConn level gives access to the AAL5 PVC Messaging connections between the core and an MG 4000. Two commands are available: Tst and Trace.

The Tst command performs an I.610 loopback test on the specified core connection for the posted MG 4000. The user specifies the connection to test (0 or 1), and whether to perform a segment test or an end-to-end test. The test is always originated on the posted MG 4000. A segment test is terminated at the first defined segment endpoint along the connection (may be an ATM switch or the XA-Core). An end-to-end test is terminated at the connection endpoint (XA-Core).

The Trace command performs an I.610 or Multiservice Switch loopback trace on the specified core connection for the posted MG 4000. The user specifies the connection to test (0 or 1), and whether to perform an I.610 type trace or a Multiservice Switch proprietary trace. The trace is originated on the posted MG 4000 and terminated at the far end of the connection (the XA-Core). The loopback trace sends a result back from every port between the originating and terminating nodes. Each Multiservice Switch node returns two results - one for the 'ingress' port (where the segment enters the Multiservice Switch node) and one for the 'egress' port (where it exits the node).

PeerConn level The PeerConn level gives access to the AAL5 SVC messaging connections between an MG 4000 and its MG 4000s. PeerConn only supports the MG 4000. As with the CoreConn level, a Tst and Trace command are offered.

The Tst command performs an I.610 loopback test on the specified peer connection for the posted MG 4000. The user specifies the peer MG 4000 connection to test, and whether to perform a segment test or an end-to-end test. The test is always originated on the posted MG 4000. A segment test is terminated at the first defined segment endpoint along the connection (may be an ATM switch or the peer MG 4000). An end-to-end test is terminated at the peer MG 4000 (connection) endpoint.

The Trace command performs an I.610 or Multiservice Switch loopback trace on the specified peer connection for the posted MG 4000. The user specifies the peer MG 4000 connection to test, and whether to perform an I.610 type trace or a Multiservice Switch proprietary trace. The trace is originated on the posted MG 4000 and terminated at the far end of the connection (the peer MG). The loopback trace sends a result back from every port between the originating and terminating nodes. Each Multiservice Switch node returns two results - one for the 'ingress' port (where the segment enters the Multiservice Switch node) and one for the 'egress' port (where it exits the node).

BearConn level The BearConn level gives access to the AAL1 SVC Bearer connections on the ATM Framework of a given SPM. At this time, BearConn supports the MG 4000, IW-SPM, DPT-SPM, and MG 9000. The Tst and Trace commands are available.

Note: DPT connections are not supported by the Tst and Trace commands.

The Tst command performs an I.610 loopback test on the specified bearer connection from the posted SPM. The user can specify the connection to test by supplying either a TID or a trunk name. The user also indicates whether to perform a segment test or an end-to-end test. The test is always originated on the posted SPM. A segment test is terminated at the first defined segment endpoint along the connection (may be an ATM switch or an end node). An end-to-end test is terminated at the end node of the connection.

The Trace command performs an I.610 or Multiservice Switch loopback trace on the specified bearer connection for the posted SPM. The user can specify the connection on which to perform a trace by supplying either a TID or a trunk name. The user also specifies whether to perform an I.610 type trace or a Multiservice Switch proprietary trace. The trace is originated on the posted SPM and terminated at the far end of the connection. The loopback trace sends a result back from every node and port between the originating and terminating nodes. Each Multiservice Switch node returns two results - one for the 'ingress' port (where the segment enters the Multiservice Switch node) and one for the 'egress' port (where it exits the node).

AtmLb command The AtmLb command performs an ATM LoopBack request on the ATM connection identified by the command parameters. The connection can be identified by a TID (node number, terminal number) or TRK name (CLLI and member number). Options are also provided for Core and Peer connections. Parameters are provided to specify what type of loopback to perform (i.e. Test versus Trace).

The command will determine which SPM hosts the connection in question, and will send a request to that SPM to perform the loopback. The results are returned to the MAP and displayed.

Additional information For additional information on ATM loopback testing, refer to the following documents:

- *MG 4000 Fault Management module*, NN10076-911
- *IW-SPM (ATM) Fault Management module*, NN10077-911
- *DPT-SPM (ATM) Fault Management module*, NN10080-911

Routine Exercise (REX) testing

REX testing is used to improve fault coverage and system reliability on SPM nodes (including MG 4000, IW-SPM, and DPT-SPM). A REX test generally consists of a combination of out-of-service diagnostics, in-service diagnostics and activity switching for duplex nodes. Some examples of REX tests are:

- CM REX test
- MS REX test
- ENET REX test
- XPM REX test

REX test of CEMs includes the following steps:

- Reset on Inactive CEM
- OOS Test on Inactive CEM
- RTS on Inactive CEM
- SWACT to the Inactive CEM

The default scheduled frequency is currently once every 7 days during the REX maintenance window. This means that ideally, REX test on an SPM node is run once every week.

For additional information on REX testing, refer to the following documents:

- *MG 4000 Fault Management module*, NN10076-911
- *IW-SPM (ATM) Fault Management module*, NN10077-911
- *IW-SPM (IP) Fault Management module*, NN10078-911
- *DPT-SPM (ATM) Fault Management module*, NN10080-911

Misconnected DS512 link diagnostics

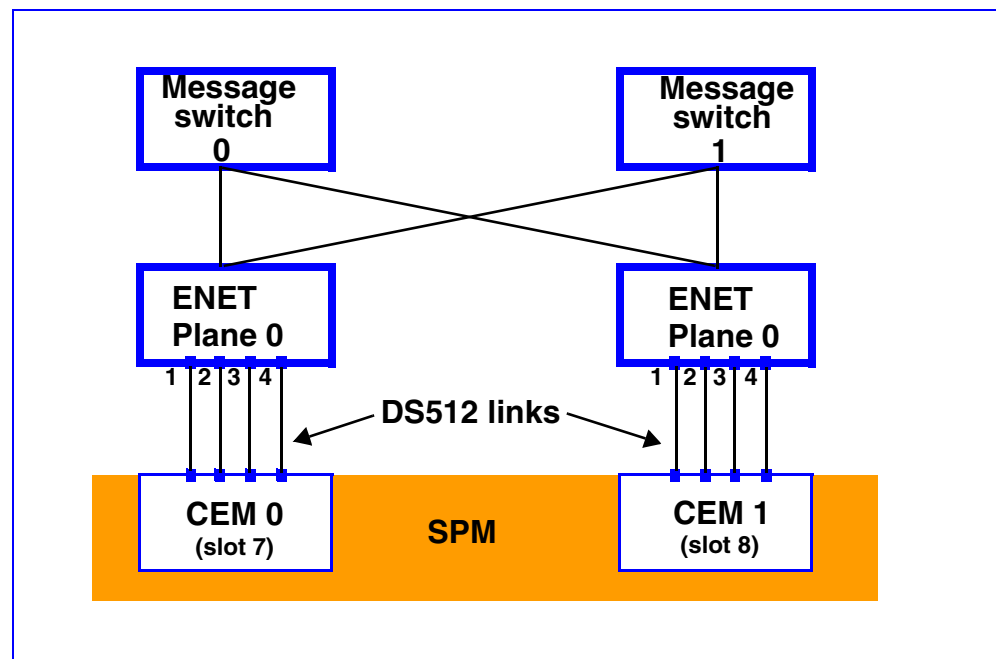
This PT-AAL1 feature detects DS512 host links that are misconnected between the ENET (enhanced network) and the CEMs (common equipment modules) of legacy SPMs (Spectrum peripheral modules), or DPT SPMs, or IW SPMs. You must connect DS512 host links between the ENET and the SPM according to the following rules:

- Links from ENET plane 0 must terminate on CEM 0 (of the SPM) and links from ENET plane 1 must terminate on CEM 1.
- You must ensure that the datafill in table MNLINK, that defines which ENET links connect to which CEM ports, exactly matches the physical connections.

The Misconnected Link Diagnostics feature only detects misconnected DS512 links that are connected to the wrong CEM, but that are connected to the right port (according to table MNLINK). The message switch (MS) port that is associated with the misconnected ENET link remains system busy until the link is properly connected. The detection of misconnected links is only possible if the CEM has software on it and the CEM is not isolated.

[Figure 1](#) shows the correct way to connect DS512 links from the ENET to the CEM ports of an SPM.

Figure 1
Correct method of connecting DS512 links

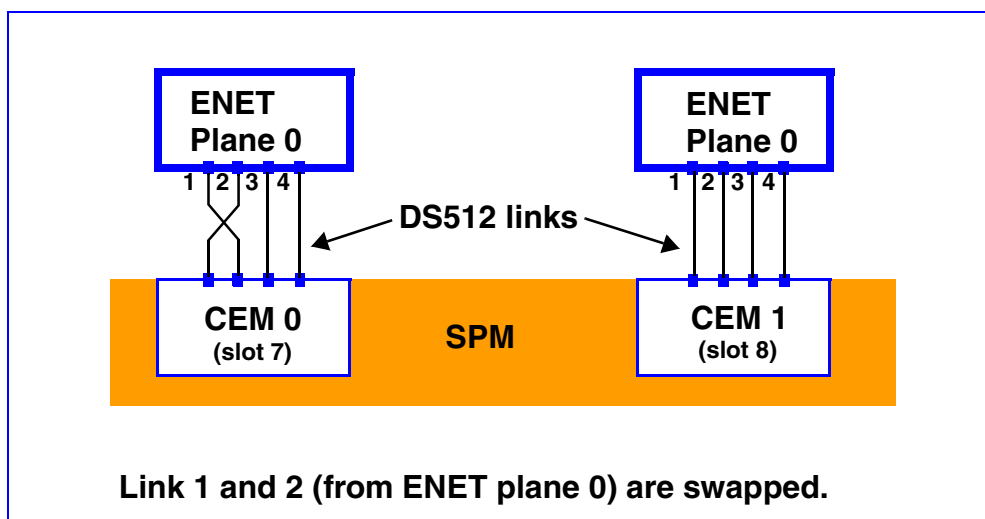


[Figure 2](#) shows an example of an improper method of connecting DS512 links from the ENET to the CEMs of an SPM. In this case, link 1 and 2, from ENET plane 0, to CEM 0 are swapped. Although this is an incorrect method of connecting DS512 links, in this example, the CEM software is not swapped across the CEMs.

Note: The Misconnected Link Diagnostics feature does not detect this type of incorrect connection.

In the example in [Figure 2](#), the misconnected links (1 and 2) between ENET plane 0 and CEM 0 remain in-service. The MS ports associated with the misconnected links are out-of-service. The system does not generate logs to indicate that there are misconnected links.

Figure 2
Misconnection of DS512 links within a CEM



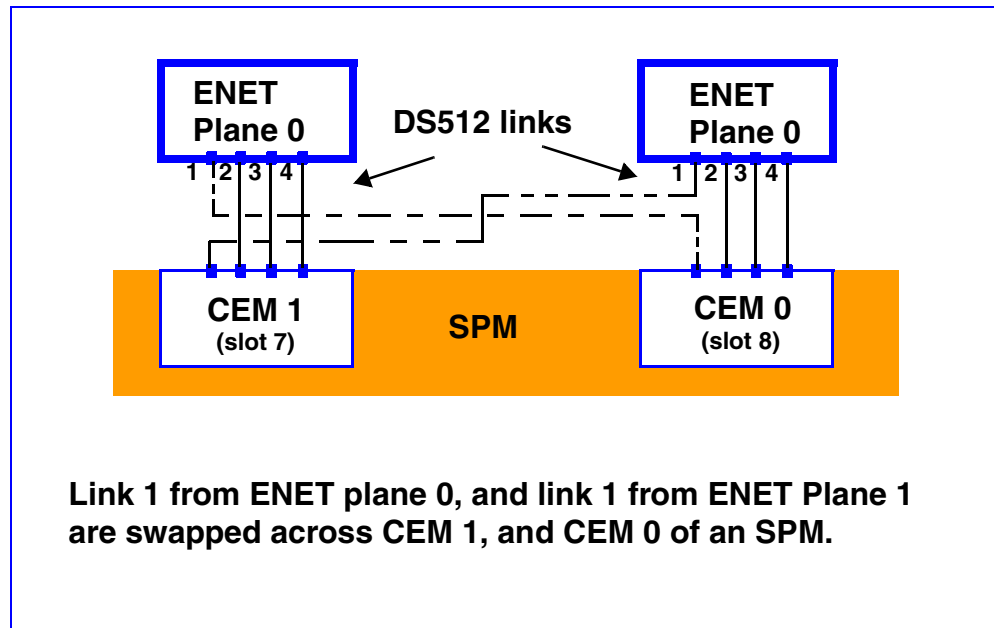
[Figure 3](#) shows an example of an improper method of connecting DS512 links from the ENET to the CEMs of an SPM. In this case, link 1 from ENET plane 0, and link 1 from ENET plane 1 are swapped. With this configuration, if a misconnected link is used to load the CEM, the CEM software is swapped.

Note: The Misconnected Link Diagnostics feature does detect this type of incorrect connection.

In the example in [Figure 3](#), the misconnected link 1 from ENET plane 0, and ENET plane 1 (to the CEMs) remains in service. Links 2, 3, and 4 to CEM 0 and CEM 1 remain in-service. The MS ports associated with links 2, 3, and 4 are out-of-service. The MS port associated with the misconnected links (link 1) remain in-service. The system generates Link 300 logs for the two link 1s that are swapped and misconnected

across the CEMs. The system does not generate a log when the fault clears.

Figure 3
Misconnection of DS512 links across CEMs (software is swapped)

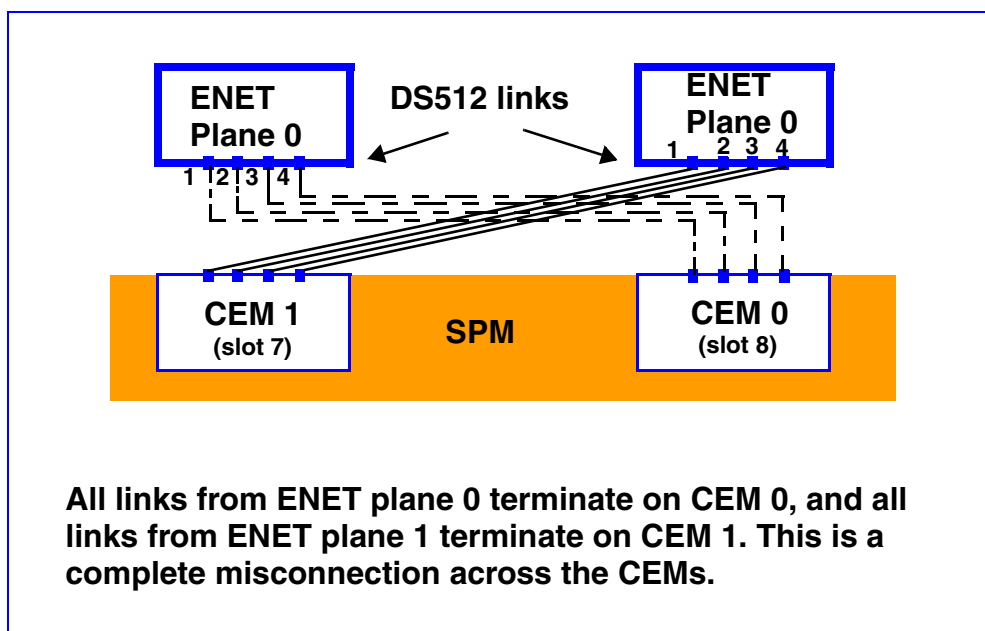


[Figure 4](#) shows an example of an improper method of connecting DS512 links from the ENET to the CEMs of an SPM. In this case, all the links between the ENET and CEM are swapped exactly across CEM 1 and 0 of an SPM. This configuration causes the software load to be swapped between the two CEMs.

Note: The Misconnected Link Diagnostics feature does detect this type of incorrect connection.

In this example in [Figure 4](#), all four misconnected links from ENET plane 0 to CEM 1, and all four links from ENET plane 1 to CEM 0 remain in service. The MS port associated with each of the misconnected links remains in service. The system generates Link 300 logs for each link that is swapped and misconnected across the CEMs. The system does not generate a log when the fault clears.

Figure 4
Complete misconnection of DS512 links

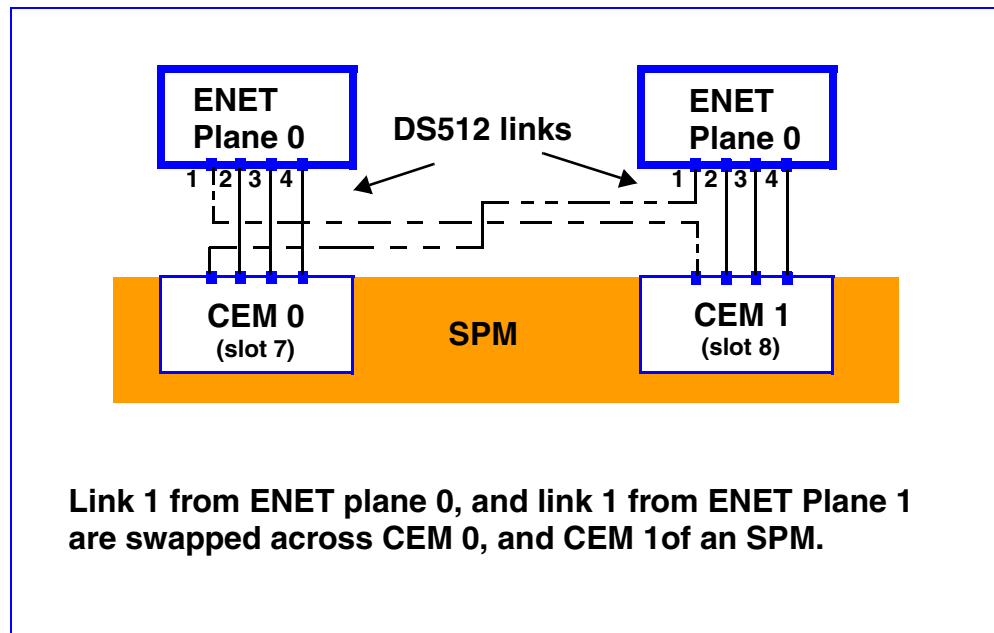


[Figure 5](#) shows an example of an improper method of connecting DS512 links from the ENET to the CEMs of an SPM. In this case, link 1 from ENET plane 0, and link 1 from ENET plane 1 are swapped. With this configuration, if a misconnected link is used to load the CEM, the CEM software is swapped.

Note: The Misconnected Link Diagnostics feature does detect this type of incorrect connection.

In the example in [Figure 5](#), the misconnected link 1 from ENET plane 0, and ENET plane 1 (to the CEMs) remains in service. The MS port associated with the misconnected links (link 1) is taken out-of-service. The system generates Link 300 logs for the two link 1s that are swapped and misconnected across the CEMs. The system does not generate a log when the fault clears.

Figure 5
Misconnection of DS512 links across CEMs (software is not swapped)



The Wrong Application Data Detection feature provides detection and diagnostic support for situations where an SPM with DS512 misconnections to the ENET are mistakenly loaded with the wrong application data. If one or more of the DS512 links between the ENET and the SPM are misconnected, then there is a possibility of the CEM (common equipment module) receiving the wrong application data during a reload restart. The phrase “wrong application data” means that the CEM in slot 7, of the SPM, receives application data for CEM 1, and the CEM, in slot 8, receives application data for CEM 0. The NODE 303 log indicates that a CEM contains wrong application data. In addition, MAPCI responses at the SPM common equipment level (SPMCEDIR) and the SPM upgrade level (SPMUPGDIR) notify the user when a CEM has been loaded with the wrong application data.

Note: A CEM that is loaded with the wrong application data cannot return to service.

Multiservice Switch/I.610 Loopback feature

The Multiservice Switch/I.610 Loopback feature allows you to isolate faults on connections across an ATM (asynchronous transfer mode) network. [Table 15](#) lists the connection paths that you can troubleshoot using the Multiservice Switch/I.610 Loopback feature.

Table 15
Connection paths

MAP level	Source of trace	Destination of trace	Signal Type	Circuit Type
ATMconn/CoreConn	MG 4000	XA-Core	AAL5	PVC
ATMconn/PeerConn	MG 4000	MG 4000	AAL5	SVC
ATMconn/BearConn	MG 4000	MG 4000	AAL1	SVC
ATMconn/BearConn	MG 4000	IW SPM	AAL1	SVC
ATMconn/BearConn	IW SPM	MG 4000	AAL1	SVC

Figure 6 shows an MG 4000 to XA-Core AAL5 PVC (permanent virtual circuit) messaging connection.

Figure 6
MG 4000 to XA-Core connection

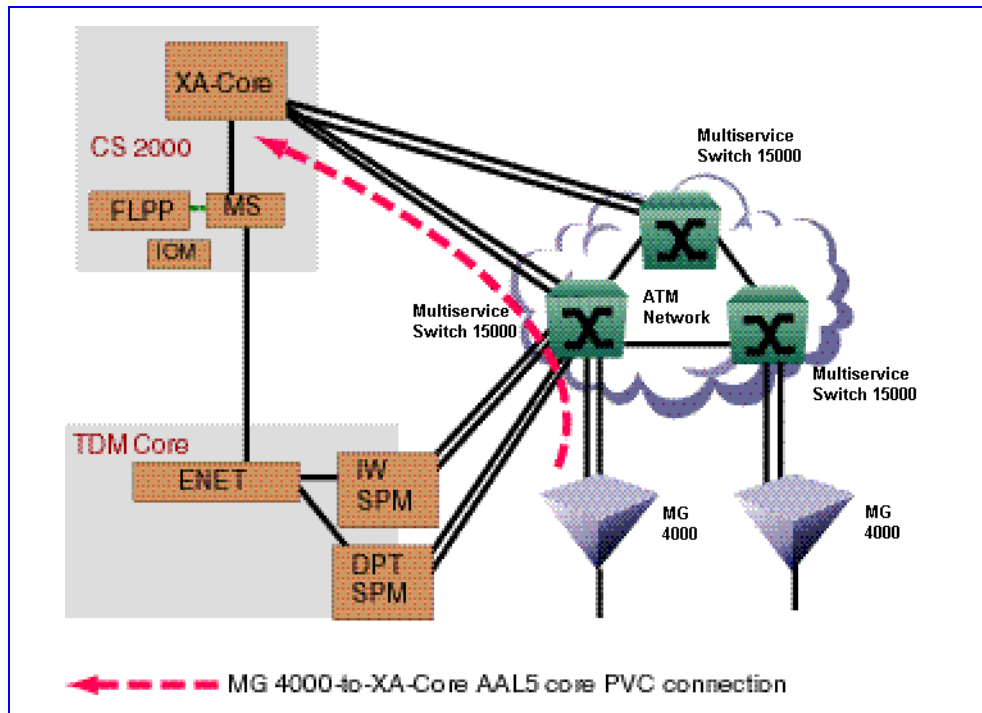


Figure 7 shows a peer SVC AAL5 messaging connection between two MG 4000s.

Figure 7
MG 4000-to-MG 4000 peer AAL5 messaging connection

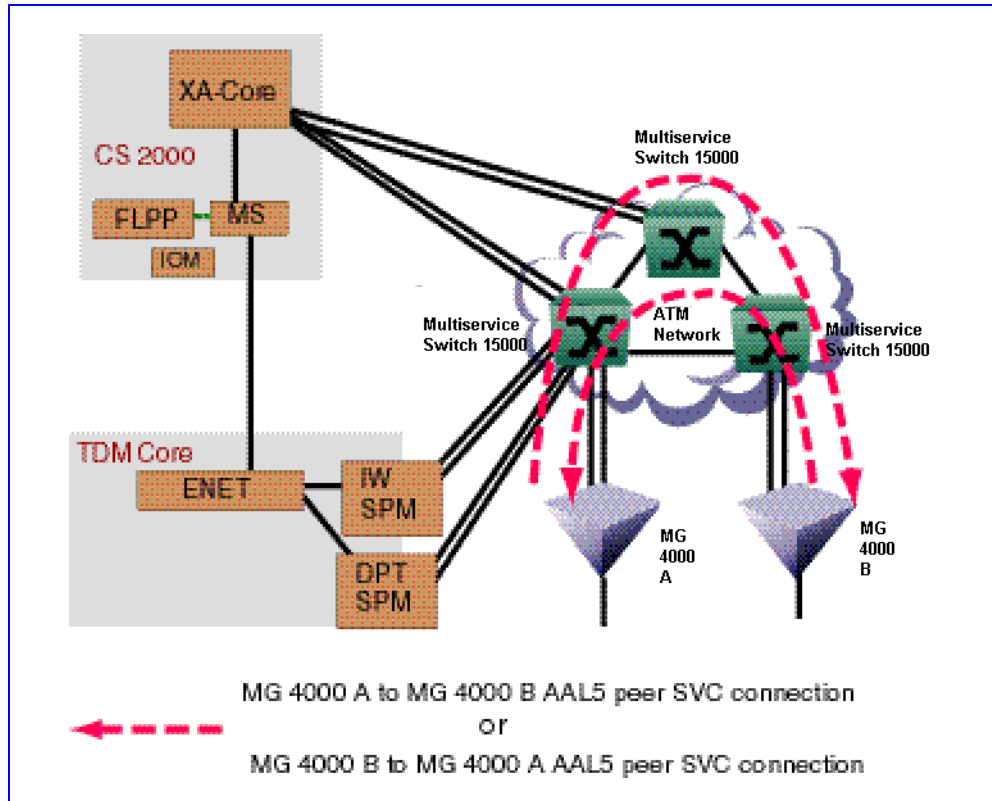


Figure 8 shows an SVC AAL1 bearer connection between two MG 4000s.

Figure 8
MG 4000-to-MG 4000 AAL1 bearer connection

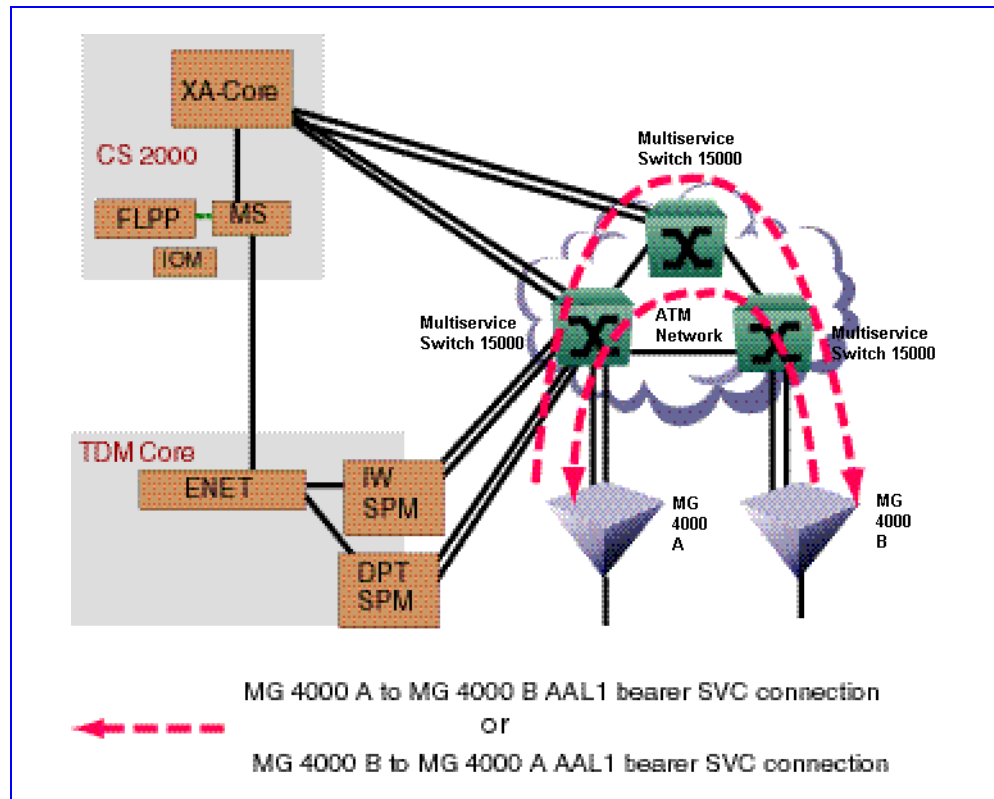
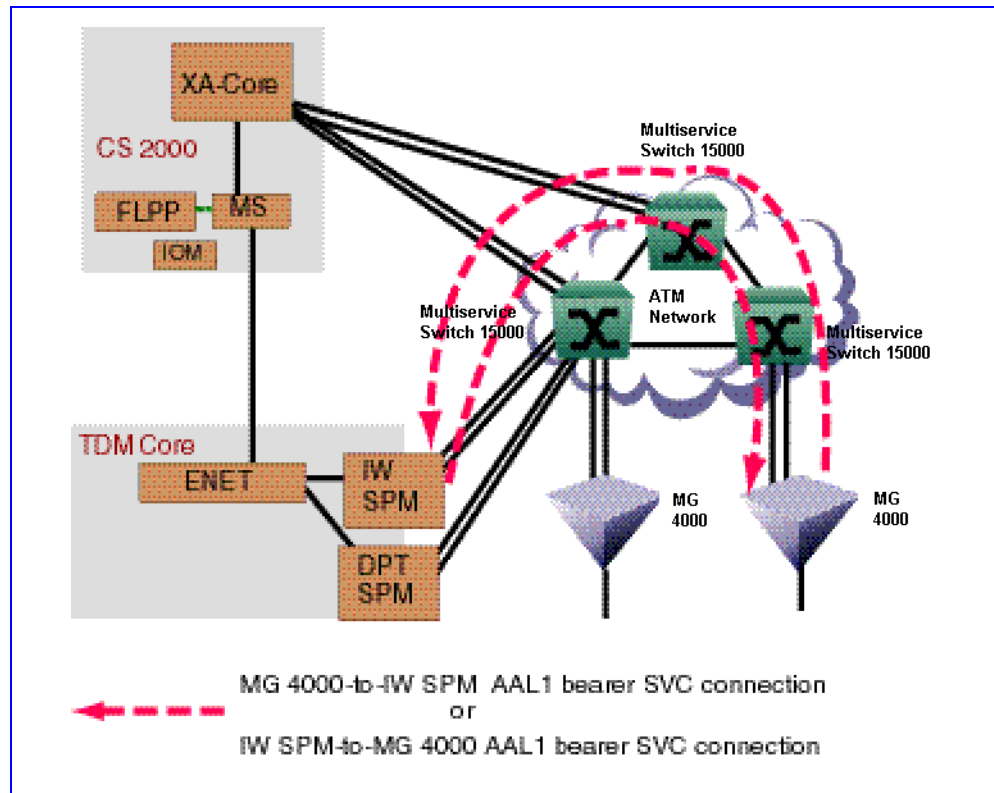


Figure 9 shows an SVC AAL1 bearer connection between an MG 4000 and an IW SPM.

Figure 9
MG 4000-to-IW SPM AAL1 bearer connection



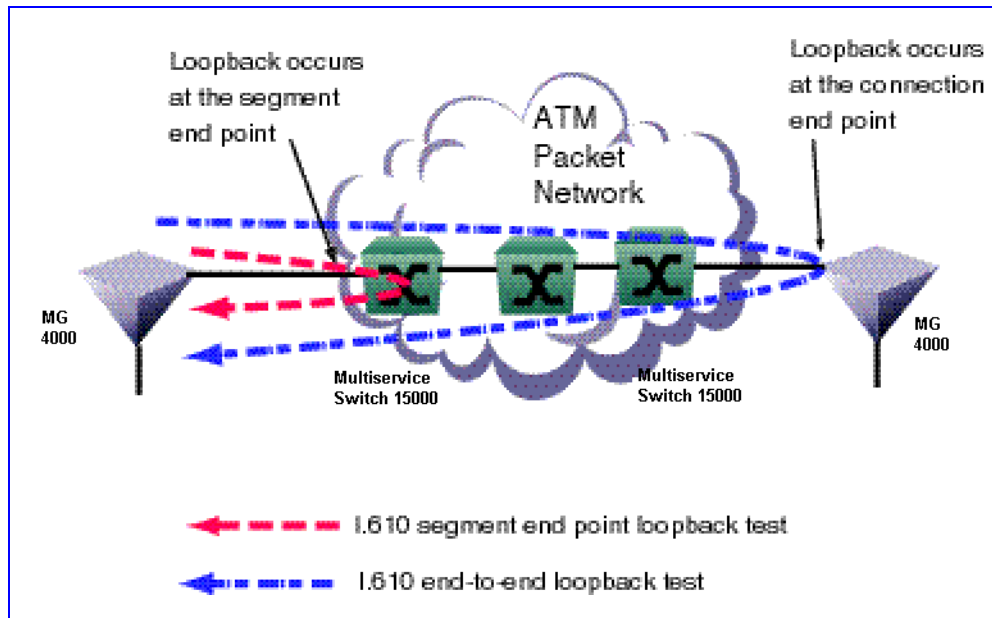
The Multiservice Switch/I.610 Loopback feature displays the results of both proprietary and standards-based ATM loopback queries. The four types of queries are as follows:

- I.610 trace
- Multiservice Switch trace (provides proprietary information for Multiservice Switch 15000 switches)
- I.610 segment end point loopback test (provides information on the segment end-node)
- I.610 end-to-end endpoint loopback test (provides information on the connection end-node)

Figure 10 shows an I.610 end-to-end loopback test, and an I.610 segment-end-point loopback test. These two types of I.610 loopback tests, test the connectivity between two points. The I.610 end-to-end test, tests from the beginning end point to the connection end point. The I.610 segment-end-point loopback test, tests from the beginning end

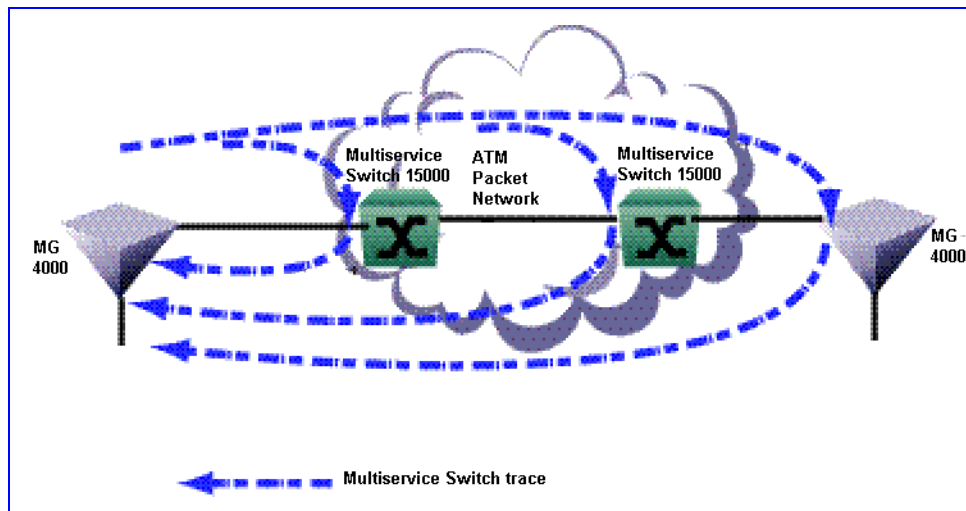
point to the segment-end-point. In [Figure 10](#), the end points are shown as MG 4000s and the ATM switches as Multiservice Switch 15000s.

Figure 10
i.610 end-to-end loopback test and, I.610 segment end point loopback test



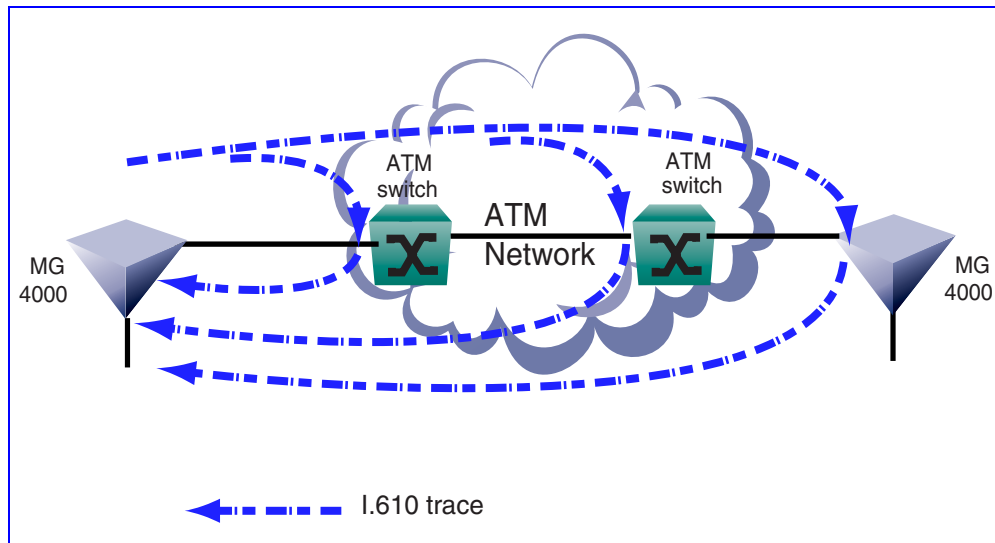
[Figure 11](#) shows an example of the Multiservice Switch trace. You would only use the Multiservice Switch trace on Multiservice Switch 15000 ATM switches. During the trace, the system software forwards a loopback cell from one Multiservice Switch 15000 to the next. Each Multiservice Switch 15000 returns two loopback responses, one for the ingress and, and another for the egress port. In other words, each ATM node along the connection path, returns information.

Figure 11
Multiservice Switch trace



[Figure 12](#) shows an example of the I.610 trace. The I.610 trace is similar to the Multiservice Switch trace, except that you use the I.610 trace on ATM switches that are supplied by vendors other than Nortel Networks (in other words, ATM switches that are not Multiservice Switch 15000s).

Figure 12
I.610 trace

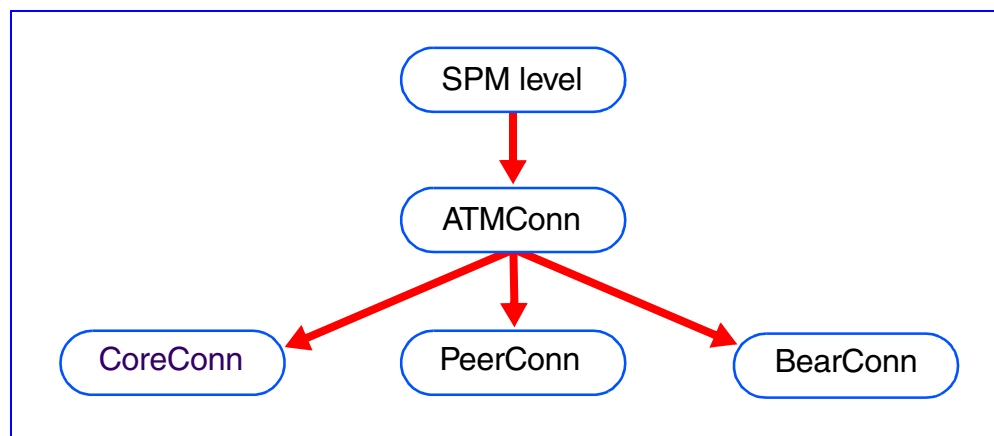


Typically, to troubleshoot an ATM connection where the ATM network consists of Multiservice Switch 15000s, you first run an I.610 end-to-end test to check for continuity. If that test fails, you then, run a Multiservice Switch trace.

The MAPCI (maintenance and administration position command interpreter) is the tool you use to perform Multiservice Switch/I.610 Loopback tests or traces. The Multiservice Switch/I.610 Loopback feature uses the ATMConn directory, as well as three sublevel directories below ATMConn. You perform a Multiservice Switch/I.610 Loopback test or trace by running the test command at the appropriate sublevel of the ATMConn directory.

[Figure 13](#) shows the MAPCI hierarchy for the ATMConn directory.

Figure 13
MAPCI levels used for Multiservice Switch/I.610 Loopback feature



ATMConn is the ATM (asynchronous transfer mode) connectivity MAPCI level. This MAPCI directory deals with the SPM (Spectrum peripheral module) interfaces to the ATM network. These interfaces are also known as the ATM framework. The commands available at ATMConn sublevels are valid for MG 4000s, and IW SPMs. CoreConn, PeerConn, and BearConn are the three MAPCI sublevels below the ATMConn directory.

The CoreConn directory provides maintenance, testing, and performance monitoring commands for AAL5 PVC (permanent virtual circuit) connections from an MG 4000 to the CS 2000. The PeerConn directory provides maintenance, testing, and performance monitoring commands for the SVC (switched virtual circuit) AAL5 peer messaging connections between two MG 4000s. The BearConn directory provides maintenance, testing, and performance monitoring commands for the AAL1 SVC bearer connections.

For detailed procedures on how to perform a Multiservice Switch/I.610 Loopback trace or test that originates from an MG 4000, see *MG 4000 Fault Management*, NN10076911 on this disk. To perform a

Multiservice Switch/I.610 Loopback test or trace that originates from a IW SPM, see *IW SPM Fault Management*, NN1007791.

USP message tracing tool

Before (I)SN08, 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.

(I)SN08 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.

OSS interface

Fault aggregation can be performed by the Integrated EMS. Among the features offered are a consolidated fault feed (ntstd, scc2, snmp or custolog) for a CVoIP network to the OSS.

North-bound fault interfaces are available for CS2000, SAM21, Universal Audio Server (UAS), Gateway Controller (GWC), Multiservice Switch 15000/Media Gateway 15000 and Multiservice Switch 7400/Media Gateway 7400, Ethernet Routing Switch 8600, and Universal Signaling Point (USP). The OSS interfaces include the following interfaces:

- A single SCC2/NT Standard fault interface is provided for faults coming from the CS2000 Core, SAM21, Call Agent, STORM, SDM

platform, Media Gateway 9000 (MG 9000), APS, SSPFS platform, UAS, and GWC.

- The Simple Network Management Protocol (SNMP) interface is available for Ethernet Routing Switch 8600, MCS, and USP.
- A single CORBA fault interface is provided for faults generated by the UAS, Audio Provisioning Server (APS), MG 9000, and GWC.
- An API is available on Multiservice Data Manager (MDM) for faults for the Multiservice Switch 15000/Media Gateway 15000 or Multiservice Switch 7400/Media Gateway 7400. The GW service fault alarms are raised by GWCs for Multiservice Switch 15000/Media Gateway 15000.
- A SYSLOG is available for GWC, SAM21, SSPFS Platform, UAS, APS, and MG 9000.

Note: The CS 2000 Core Manager also supports alarm reporting. See [Alarm Reporting on page 52](#)

The user can view the hardware status information through each component's element manager graphical user interface (GUI). This includes alarms related to the TDM core, UAS, APS, GWC, Multiservice Switch 15000/Media Gateway 15000, Multiservice Switch 7400/Media Gateway 7400, and Ethernet Routing Switch 8600.

The SNMP/Corba interfaces described above do not report faults from line gateways. Line gateways must have a compatible third-party element manager. Typically, a line gateway communicates with its element manager using SNMP. The methods used for communication between the element manager and the network management layer are vendor-specific; for details, refer to the vendor's documentation. It is the gateway supplier's responsibility to ensure that line gateway faults can be obtained from the gateway when required.

In (I)SN06.2, an alternative was introduced to log/fault delivery from each separate element management system. Syslog can be used to aggregate some of the individual fault/log streams into the SCC2/NT STD stream on the CS 2000 Core Manager/SDM. The fault stream from MDM can be passed to the SDM and converted to SCC2/NT STD. Also, the fault streams from the Gateway Controller (GWC) and Universal Audio Server (UAS) can be passed to the SDM using syslog, and converted to SCC2/NT STD.

Tools and utilities

IAC Tools and Utilities

Fault management for the IAC solution is performed at the element management layer (EML) using the following managers:

- Integrated Element Management System (EMS)
- SDM/Communication Server 2000 (CS 2000) Core Manager
- Core and Billing Manager
- CS 2000 Service Application Module 21 (SAM21) Manager
- CS 2000 Gateway Controller (GWC) Manager
- Session Server Manager
- Universal Audio Server (UAS) Manager
- Media Server 2000 (MS 2000) Series
- Audio Provisioning Server (APS)
- Universal Signalling Point (USP) Manager
- Multiservice Data Manager (MDM)
- Device Manager for Ethernet Routing Switch 8600
- Call Agent Manager
- STORage Management Manager (STORM Manager)
- Nuera Configurator
- NueraView
- HP Openview

Intl IAC Tools and Utilities

Fault management for the Intl IAC solution is performed at the element management layer (EML) using the following managers:

- Integrated Element Management System (EMS)
- SDM/Communication Server 2000 (CS 2000) Core Manager
- Core and Billing Manager
- CS 2000 Service Application Module 21 (SAM21) Manager
- CS 2000 Gateway Controller (GWC) Manager
- Universal Audio Server (UAS) Manager
- Media Server 2000 (MS 2000) Series
- Audio Provisioning Server (APS)
- Universal Signalling Point (USP) Manager

- Multiservice Data Manager (MDM)
- Device Manager for Ethernet Routing Switch 8600
- Call Agent Manager
- STORage Management Manager (STORM Manager)

Intl IAW Tools and Utilities

Fault management for the Intl IAW solution is performed at the element management layer (EML) using the following managers:

- Integrated Element Management System (EMS)
- SDM/Communication Server 2000 (CS 2000) Core Manager
- Core and Billing Manager
- CS 2000 Service Application Module 21 (SAM21) Manager
- CS 2000 Gateway Controller (GWC) Manager
- Universal Audio Server (UAS) Manager
- Media Server 2000 (MS 2000) Series
- Audio Provisioning Server (APS)
- Universal Signalling Point (USP) Manager
- Multiservice Data Manager (MDM)
- Device Manager for Ethernet Routing Switch 8600
- Call Agent Manager
- STORage Management Manager (STORM Manager)

PT-AAL1 Tools and Utilities

Fault management for the PT-AAL1 solution is performed at the element management layer (EML) using the following managers:

- SDM/Communication Server 2000 (CS 2000) Core Manager
- Multiservice Data Manager (MDM)
- Device Manager for Ethernet Routing Switch 8600

PT-IP Tools and Utilities

Fault management for the PT-IP solution is performed at the element management layer (EML) using the following managers:

- Integrated Element Management System (EMS)
- SDM/Communication Server 2000 (CS 2000) Core Manager
- CS 2000 Service Application Module 21 (SAM21) Manager
- CS 2000 Gateway Controller (GWC) Manager

- Session Server Manager
- Universal Audio Server (UAS) Manager
- Media Server 2000 (MS 2000) Series
- Audio Provisioning Server (APS)
- Universal Signalling Point (USP) Manager
- Multiservice Data Manager (MDM)
- Device Manager for Ethernet Routing Switch 8600
- Call Agent Manager
- STORage Management Manager (STORM Manager)

Intl PT-IP Tools and Utilities

Fault management for the Intl PT-IP solution is performed at the element management layer (EML) using the following managers:

- SDM/Communication Server 2000 (CS 2000) Core Manager
- Core and Billing Manager
- CS 2000 Service Application Module 21 (SAM21) Manager
- CS 2000 Gateway Controller (GWC) Manager
- Session Server Manager
- Universal Audio Server (UAS) Manager
- Media Server 2000 (MS 2000) Series
- Audio Provisioning Server (APS)
- Universal Signalling Point (USP) Manager
- Multiservice Data Manager (MDM)
- Device Manager for Ethernet Routing Switch 8600
- Call Agent Manager
- STORage Management Manager (STORM Manager)

PT-XA-Core and PT-SN70EM Tools and Utilities

Fault management for the PT-XA-Core and PT-SN70EM solutions is performed at the element management layer (EML) using the following managers:

- SDM/Communication Server 2000 (CS 2000) Core Manager

UA-AAL1 Tools and Utilities

Fault management for the UA-AAL1 solution is performed at the element management layer (EML) using the following managers:

- Integrated Element Management System (EMS)
- SDM/Communication Server 2000 (CS 2000) Core Manager
- Core and Billing Manager
- Media Gateway 9000 (MG 9000) Manager
- CS 2000 Service Application Module 21 (SAM21) Manager
- CS 2000 Gateway Controller (GWC) Manager
- Universal Audio Server (UAS) Manager
- Media Server 2000 (MS 2000) Series
- Universal Signalling Point (USP) Manager
- Multiservice Data Manager (MDM)
- Device Manager for Ethernet Routing Switch 8600

UA-IP Tools and Utilities

Fault management for the UA-IP solution is performed at the element management layer (EML) using the following managers:

- Integrated Element Management System (EMS)
- SDM/Communication Server 2000 (CS 2000) Core Manager
- Core and Billing Manager
- Media Gateway 9000 (MG 9000) Manager
- CS 2000 Service Application Module 21 (SAM21) Manager
- CS 2000 Gateway Controller (GWC) Manager
- Universal Audio Server (UAS) Manager
- Media Server 2000 (MS 2000) Series
- Audio Provisioning Server (APS)
- Universal Signalling Point (USP) Manager

- Multiservice Data Manager (MDM)
- Device Manager for Ethernet Routing Switch 8600
- Call Agent Manager
- STORage Management Manager (STORM Manager)

Intl UA-IP Tools and Utilities

Fault management for the Intl UA-IP solution is performed at the element management layer (EML) using the following managers:

- Integrated Element Management System (EMS)
- SDM/Communication Server 2000 (CS 2000) Core Manager
- Core and Billing Manager
- CS 2000 Service Application Module 21 (SAM21) Manager
- CS 2000 Gateway Controller (GWC) Manager
- Universal Audio Server (UAS) Manager
- Media Server 2000 (MS 2000) Series
- Audio Provisioning Server (APS)
- Universal Signalling Point (USP) Manager
- Multiservice Data Manager (MDM)
- Device Manager for Ethernet Routing Switch 8600
- Call Agent Manager
- STORage Management Manager (STORM Manager)

Integrated Element Management System (EMS)

Fault management for Integrated EMS consists of working with alarms and events, as well as configuring Northbound fault feeds. Integrated EMS supports both a Java Web Start and HTML client.

Working with Alarms in the Java Web Start Client and HTML Client

The Integrated EMS Alarm browser provides a consolidated real-time view of the events that have occurred in a CS 2000 central office. It provides a tool to view and page through the alarms from the Nortel Networks EMs, NEs, platforms, and applications in a common graphical interface. The Alarms browser provides a wide range of features to manage and view alarms in a centralized location. Alarms are generated when a fault is detected in a network device. The devices

forward these alarms to the Integrated EMS. The alarms have one of the following severities:

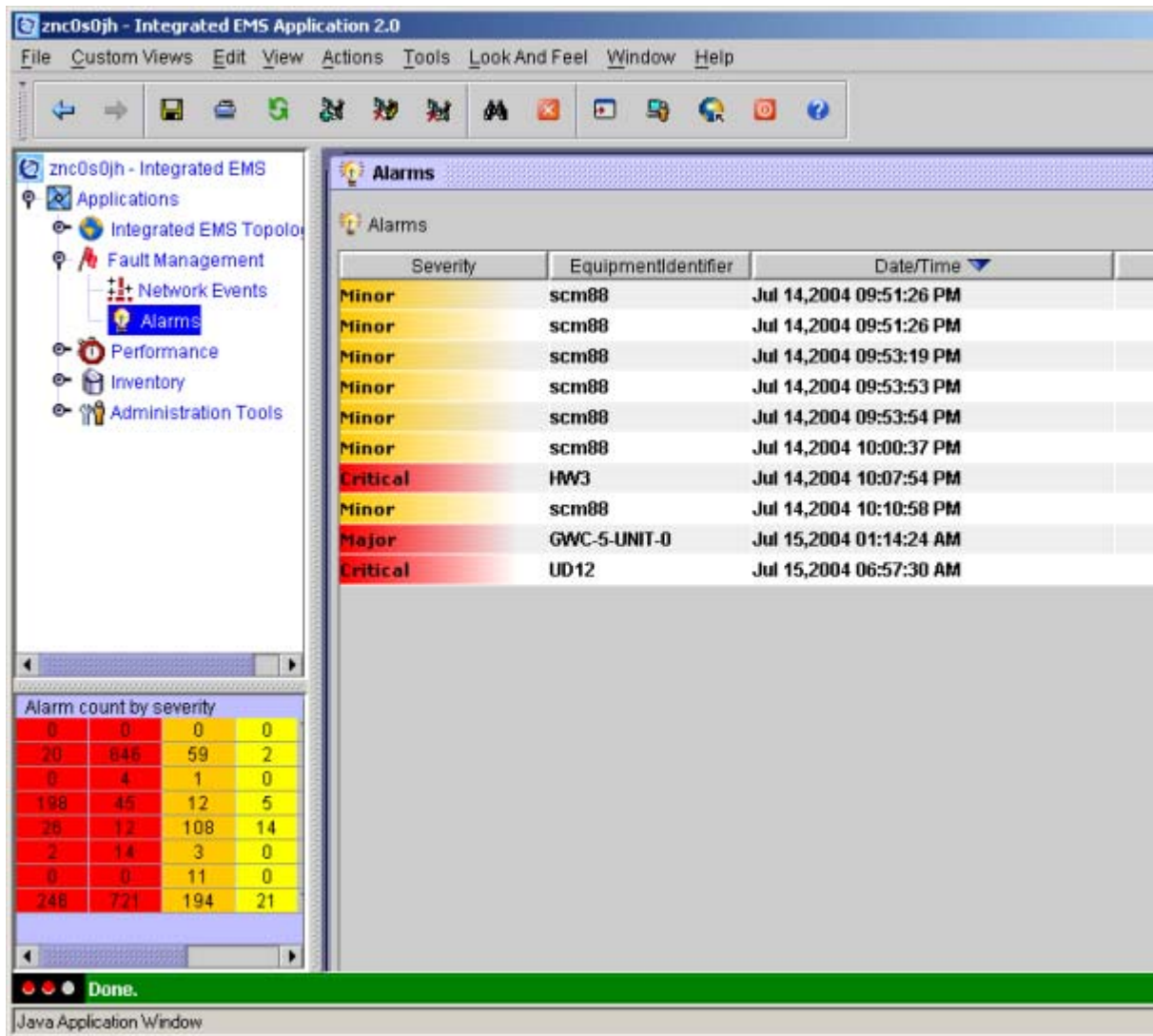
- Critical
- Major
- Minor
- Warning

The significance of the color (background color of rows in Alarms panel) for each severity levels is listed in the following table.

Color	Severity Level
Red	Critical
	Major
Orange	Minor
Yellow	Warning

To access the Java Web Start Client Alarms browser, select the Alarms node (sub-node of Fault Management) in the Integrated EMS tree. The following figure illustrates the Java Web Start Client Alarms browser.

Figure 14 Java Web Start Client Alarms browser



To access the HTML Client Alarms browser, select the Fault Management tab at the top of the page, and then select Alarms on the left side of the refreshed browser window. The following figure illustrates the HTML Client Alarms browser.

Figure 15 HTML Client Alarms browser

Showing 1158 to 1183 of 1183 | Page: 44 45 46 47 [48]

Status	EquipmentIdentifier	Date / Time	Owner	Log Name	Log Number
Critical	UD12	Jul 15, 2004 07:57:30 AM	MGEM		301
Major	GWC-5-UNIT-0	Jul 15, 2004 02:14:24 AM	GWC		304
Minor	scm88	Jul 14, 2004 11:10:58 PM	NE		301
Critical	HW3	Jul 14, 2004 11:07:54 PM	MGEM		301
Minor	scm88	Jul 14, 2004 11:00:37 PM	SHLF		393
Minor	scm88	Jul 14, 2004 10:53:54 PM	NE		305
Minor	scm88	Jul 14, 2004 10:53:53 PM	NE		305
Minor	scm88	Jul 14, 2004 10:53:19 PM	NE		305
Minor	scm88	Jul 14, 2004 10:51:26 PM	SHLF		335
Minor	scm88	Jul 14, 2004 10:51:26 PM	SHLF		334
Minor	47.131.125.6	Jul 14, 2004 06:11:55 PM	STM		801
Major	GWC-5-UNIT-0	Jul 14, 2004 05:02:14 PM	GWC		304
Major	Ud8	Jul 14, 2004 01:02:44 PM	MGEM		302

Alarm Count	Category
20	other
1	qualityOfService
190	communications
26	equipment
1	processingError
1	environmental
246	Total

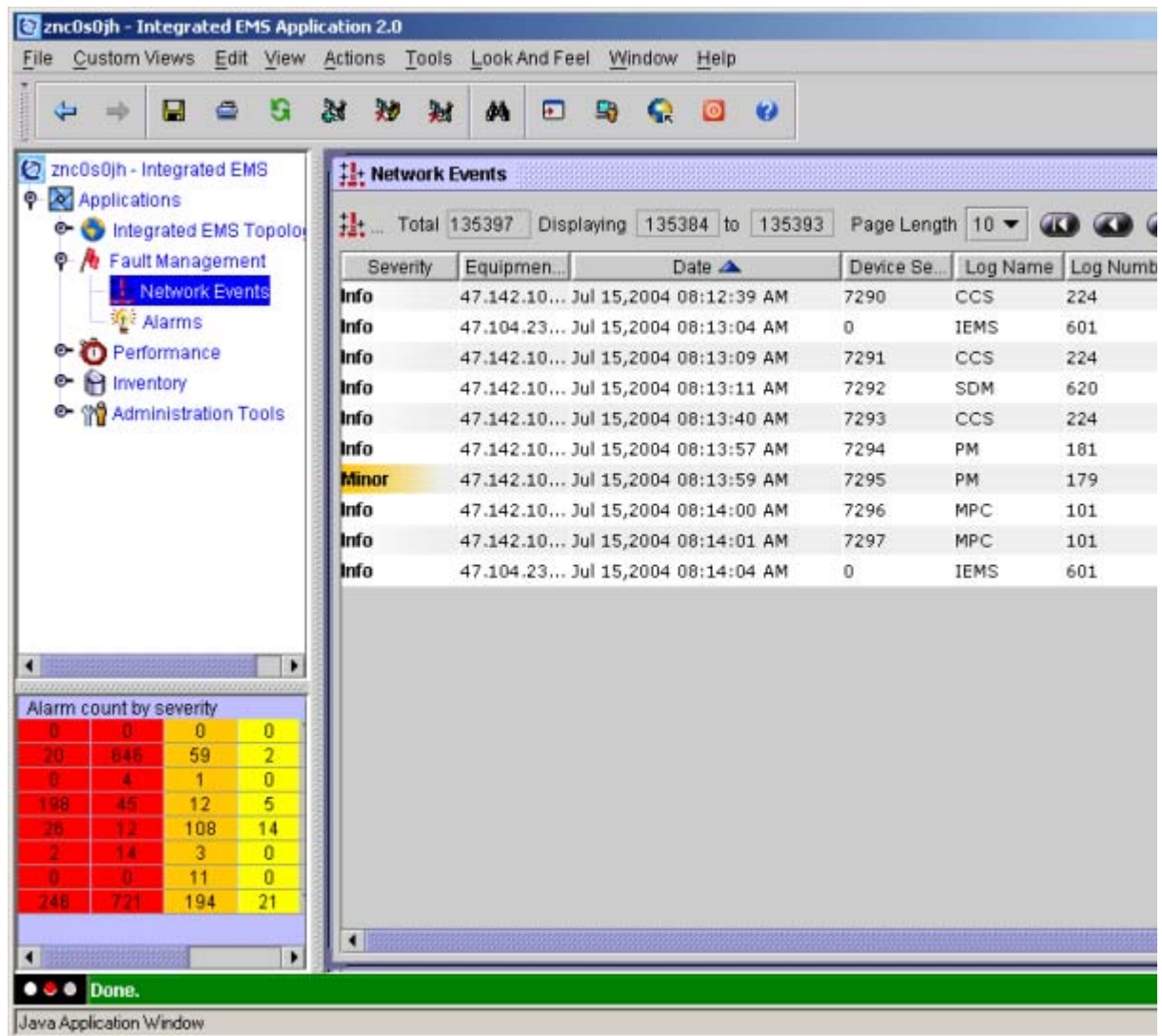
For additional information, refer to *Integrated EMS Fault Management*, NN10334-911.

Working with Events in the Java Web Start Client and HTML Client

The Integrated EMS event browser provides a consolidated historical and real-time view of the events that have occurred in a CS 2000 central office. Event browser is a tool to view the events from the Nortel Networks EMSs, NEs, platforms, and applications in a common GUI. The event browser serves as a key tool that enables the monitoring and debugging of network activities and issues.

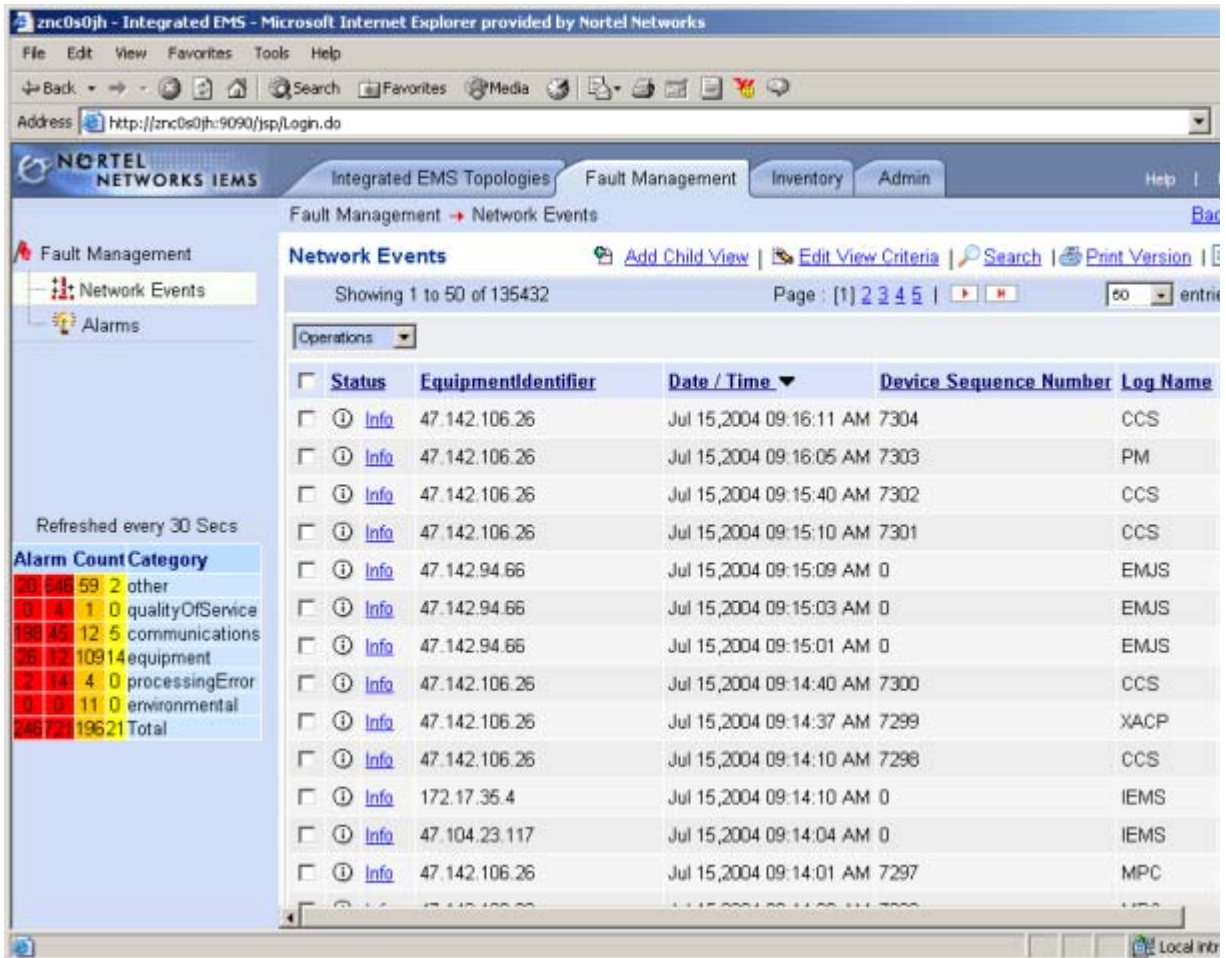
To access the Java Web Start Client Events browser, select the Network Events node (sub-node of Fault Management) in the Integrated EMS tree. The following figure illustrates the Java Web Start Client Event browser.

Figure 16 Java Web Start Client Events browser



To access the HTML Client Events browser, select the Fault Management tab at the top of the page, and then select Network Events on the left side of the refreshed browser window. The following figure illustrates the HTML Client Events browser.

Figure 17 HTML Client Events browser



For additional information, refer to *Integrated EMS Fault Management*, NN10334-911.

Configuring Northbound fault feeds

The Integrated EMS standardizes the fault interfaces from the various EMSs, NEs, applications, and platforms that it manages. It normalizes the events received from these interfaces and converts them into a

common format. The Integrated EMS supports the following northbound event interfaces.

- SCC2
- SNMP
- Customerlog SYSLOG
- NTSTD

Providing a common set of northbound OSS interfaces that are based on common standards simplifies the effort for third party vendors to integrate and monitor the event stream from a Nortel Networks office.

For additional information, refer to *Integrated EMS Fault Management*, NN10334-911.

SDM/CS 2000 Core Manager

The SDM/CS 2000 Core Manager performs the following fault management functions:

- alarm surveillance
- alarm history retrieval and browsing
- test invocation (access only)
- fault correction (access only)
- fault verification (access only)
- maintenance
- alarm configuration per device
- log collection configuration

The user can view the alarms and the status of hardware components through the SDM/CS 2000 Core Manager which also supports the following tasks:

- Alarm Reporting
 - MAP Alarm banner
 - MAP subsystem and status summary field
- Troubleshooting tools and utilities

Alarm Reporting

In addition to the fault management functions listed above, SDM/CS 2000 Core Manager also supports alarms reporting. The tasks that allow generation of reports about alarms or inhibit the generating of reports are all performed on the SDM/CS 2000 Core Manager. The

tasks that allow generation of and viewing of information about logs are all performed on the SDM/CS 2000 Core Manager. For information on how to configure reporting of alarms and view information about logs, refer to the following component documentation:

- *CS 2000 Fault Management module*, NN10083-911
- *CS 2000 Core Manager Fault Management module*, NN10082-911

SDM/CS 2000 Core Manager events are recorded internally to the SDM/CS 2000 Core Manager in a series of log reports. SDM/CS 2000 Core Manager log reports are local and do not appear in the generic DMS log utility stream except log reports SDM550 and SDM650.

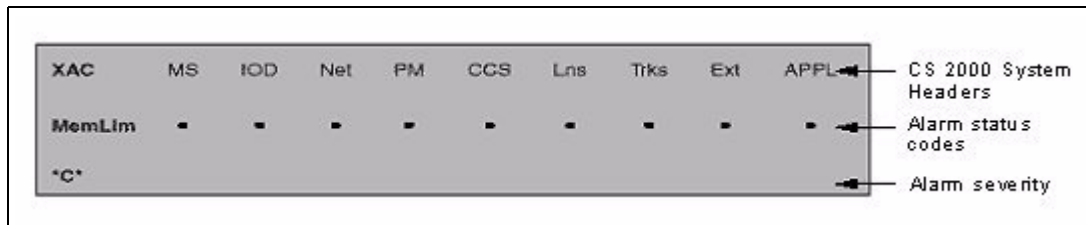
The SDM/CS 2000 Core Manager provides a network-level view of SDM/CS 2000 Core Manager, XA-Core or SN70EM, CS 2000, IW SPM, and MG 4000 fault data through the MAP interface.

For Multi-Service Gateway 4000 (MG 4000) and Interworking SPM (IW SPM), the alarm reporting system integrates event detection and alarm notification functions. An alarm becomes active when a reduced service, reliability, or test condition occurs in the network or network element. The alarm remains active until a system event or activity performed by operating company personnel clears the alarm condition. The alarm system includes audible notification and visual display through warning lights and the MAP terminal.

The MAP terminal displays alarm codes in the banner and the subsystem status summary field (SSSF). The alarm banner displays alarm codes that indicate the effect of the alarm event on the network or network element. The SSSF displays alarm codes that indicate equipment faults of system states.

MAP Alarm banner

MAP alarm banner software monitors for equipment or software events or faults. For events that affect performance or redundancy, the system raises and displays an appropriate system alarm in the MAP alarm banner. The MAP alarm banner displays alarm codes that indicate the effect of the alarm event on the system. To see an example of a memory limit (MemLim) alarm with a critical severity level, refer to [Figure 18](#).

Figure 18 MAP alarm banner

For information on the alarm banner, refer to [Table 16](#).

Table 16 MAP alarm banner summary field

Alarm banner	Description
CS 2000 system headers	The CS 2000 headers permanently display a set of titles indicating the different switch CS 2000 nodes. The XA-Core MAP system displays the CS 2000 headers on all XA-Core MAP levels.
Alarm status codes	The alarm status codes indicate the system alarm status. The alarm status fields display the alarm status code under each of the CS 2000 headers. If there are multiple faults in a single switch system, the alarm status field displays the most important fault.
Alarm severity	The alarm severity field displays the severity of the alarm condition. Each CS 2000 subsystem reports on critical, major and minor alarm conditions. If there are multiple faults in a single switch system, the alarm severity field displays the most important fault. The alarm banner displays the alarm severity under the alarm indicator in XAC header.

For information on possible alarm severity conditions, their status and description, refer to [Table 17](#).

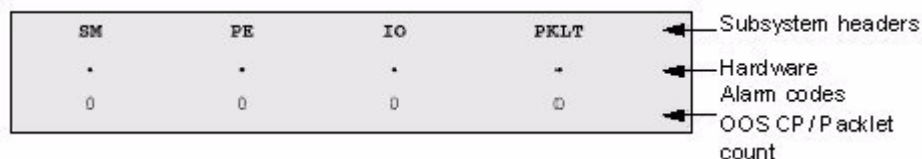
Table 17 Alarm severity conditions

Alarm	Status	Description
“.”	No alarm	A no alarm indicates that there are no problems in the network.
“m”	minor alarm	A minor alarm indicates a small loss of redundancy. The next fault of the same type does not cause degradation of service.

Table 17 Alarm severity conditions

Alarm	Status	Description
“M”	Major alarm	A major alarm indicates lost redundancy. The next fault of the same type can cause a reduction or complete loss of service. There is no backup if another fault occurs on the active system. This alarm level can be generated when service decreases below an operating company defined threshold.
“C”	Critical alarm	A critical alarm indicates a reduced service condition or complete loss of service. A critical alarm indicates that the system can no longer perform its design function. The alarm condition requires immediate correcting action so that the performance of the system can return to its design function.

MAP subsystem and status summary field The subsystem status summary field (SSSF) displays the working status of the equipment subsystems. The SSSF has three rows and four columns of fields that are shown in [Figure 19](#).

Figure 19 XA-Core MAP subsystem and status summary field

[Table 18](#) shows the MAP subsystem and status summary field. The alarm banner shows one active alarm at a time in the alarm status code field. The alarm banner displays the most important alarm.

Table 18 MAP subsystem and status summary field

MAP subsystem	Description
Subsystem headers	The subsystem headers permanently display a set of titles that describe the equipment subsystems.

Table 18 MAP subsystem and status summary field

MAP subsystem	Description
Hardware alarm codes	The hardware alarm code fields display hardware alarms for each subsystem type. If there are multiple faults in a single CP/packet type, the hardware alarm field displays the most important.
Out-of-service (OOS) circuit pack/packet count	The OOS CP/packet count fields display the total number of out-of-service CPs or packets in each of the subsystems. The count can increase for each alarm condition. The count does not increase for noncritical device faults and trouble conditions.

Analyzing fault data from DMS and SPM-based equipment DMS and SPM-based equipment uses the DMS proprietary states to report the status of network devices. The following list identifies the DMS proprietary states:

- Offline (Offl)
- Manual Busy (ManB)
- In Service (InSv)
- In-service Trouble (ISTb)
- C-side Busy (CBsy)
- System Busy (SysB)

Troubleshooting tools and utilities

The CS 2000 Core Manager uses tools that are within the software to gather information for troubleshooting. These tools apply to the different elements of CVoIP Solutions:

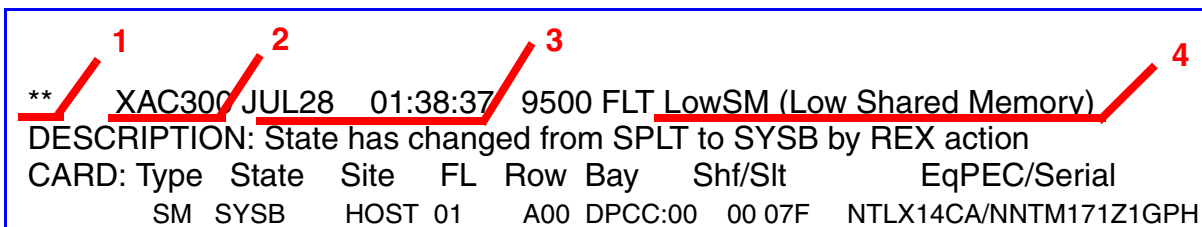
- Traver - used to show the path a call takes from the switch perspective
- logutil - used to view logs that have been recently generated
- Dlog - disk volume stores logutil messages
- OMSHOW - displays performance metrics collected by CS 2000 equipment as well gateway equipment.

Recording information from the CS 2000 Core Manager, XA-Core, SN70EM, or SPM based log

[Figure 20](#) shows an example of an XAC 300 log with SCC2 header. The major alarm priority (**) is shown (see arrow 1). The log name and number (XAC300) is shown (see arrow 2). The date and time

(JUL 28 01:38:37) is shown (see arrow 3). The alarm name (LowSM (Low Shared Memory)) is shown (see arrow 4).

Figure 20
Log with SCC2 header format



```

** XAC300 JUL28 01:38:37 9500 FLT LowSM (Low Shared Memory)
DESCRIPTION: State has changed from SPLT to SYSB by REX action
CARD: Type State Site FL Row Bay Shf/Slt EqPEC/Serial
      SM SYSB HOST 01 A00 DPCC:00 00 07F NTLX14CA/NNTM171Z1GPH
  
```

Enhanced log information for SPM logs

The Enhanced Logs feature provides additional text for the following classes of log reports:

- ATM
- CARR
- CCMT
- DPTM
- IWBM
- SPM

Two enhancements are made:

- identifying the SPM node type for ATM and CARR logs
- identifying the fabric for all SPM-related logs

The ATM and CARR logs provide information on the four SPM (Spectrum peripheral module) network elements: IW SPM, DPT SPM, MG 4000 and legacy SPMs. The additional text, in the ATM, and CARR logs, consists of the SPM location (SPM number) and SPM type (DMSCP, IW, SMG4, DPT). [Table 19](#) maps the four SPM network elements to the values in the SPM type field.

Table 19
Mapping type value to SPM node

Value in the type field of the ATM log	Corresponding SPM network element
DMSCP	Legacy SPM
SMG4	MG 4000

Table 19
Mapping type value to SPM node

Value in the type field of the ATM log	Corresponding SPM network element
IW	IW SPM
DPT	DPT SPM

The value for Fabric comes from table MNCKTPAK and the Fabric values will be assigned according to the following table.

Table 20 Fabric values from table MNCKTPAK

Datafilled CPKTYPE	Fabric
GEM	IP
ATM	ATM
anything other value	UNK
not datafilled	UNK

Note: If the Type in table MNODE is DMSCP, then the fabric portion of the line will not be used.

[Figure 21](#) shows an example of an SCC2 header format for an ATM300 log. The log name and number (ATM300) is shown (see arrow 1). The alarm name (ATM LCD Alarm) is shown (see arrow 2). The location of the network element and the network element type (in this case a DPT SPM) is shown (see arrow 3). Additionally, the fabric (in this case ATM) is shown (see arrow 4).

For the ATM and CARR logs, the location and type field (see arrow 3) only appears in the SN05 and following software release and only if the office parameter SPM_ENHANCED_OUTPUT in table OFCVAR is set to ON. The fabric field (see arrow 4) only appears in SN06 and following software releases if the office parameter SPM_ENHANCED_OUTPUT is set to ON. If the office parameter SPM_ENHANCED_OUTPUT is set to OFF, the location and type fields do not appear on the ATM and CARR logs. New ATM and CARR logs created in SN05 or later display the location and type fields by default, regardless of the value of SPM_ENHANCED_OUTPUT.

Figure 21
ATM300 log with SCC2 header format

```

00  ATM  300  6217  INFO  ATM  LCD  Alarm  Raised
      Location: SPM 0 ATM RM in SLOT: 10  (InAct )
      Description: ATM LCD alarm raised.
      Location: SPM 0 Type: DPT Fabric: ATM
  
```

[Table 21](#) shows the ATM300 log in both NT Standard and SCC2 log formats. In addition [Table 21](#) shows the ATM300 log with and without the enhanced text that gives the location and type of SPM (see bold text in row two and four of [Table 21](#)). The enhanced text is only visible when office parameter SPM_ENHANCED_OUTPUT is set to ON in table OFCVAR. You can turn the office parameter OFF and ON as frequently as you wish without causing negative effects. Changing this office parameter does not require a restart or any other switch action. The settings of the SPM_ENHANCED_OUTPUT parameter are able to survive all restarts.

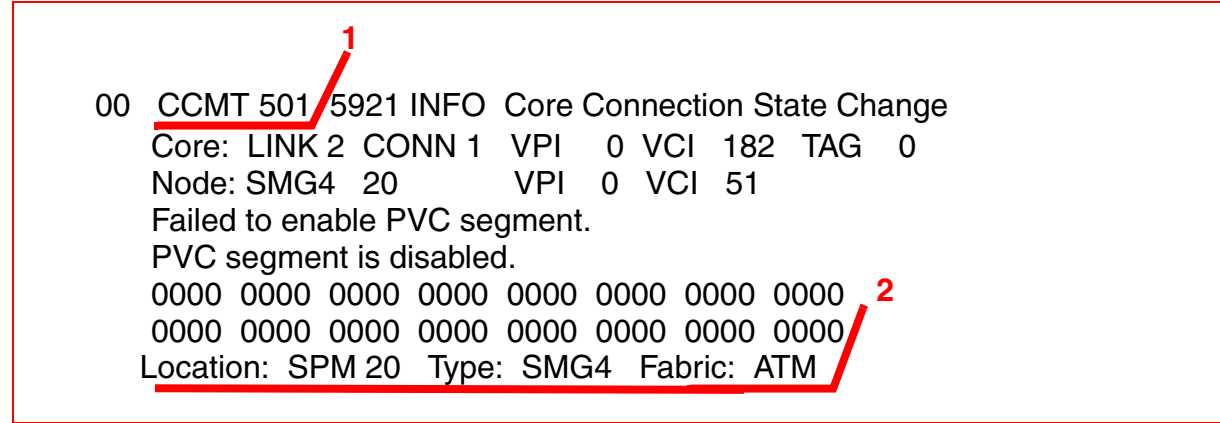
Table 21
Comparison of an ATM log with and without enhanced text

Log Format		Four variations of the ATM300 log	
NT Standard (no enhanced text)	RPTN04BF **	ATM300 FEB16 09:22:24 3496 FLT ATM LCD Alarm Raised Location: SPM 0 ATM RM in Slot: 10 (InAct) Description: ATM LCD alarm raised.	
NT Standard (with enhanced text)	RPTN04BF **	ATM300 FEB16 09:22:24 3496 FLT ATM LCD Alarm Raised Location: SPM 0 ATM RM in Slot: 10 (InAct) Description: ATM LCD alarm raised. Location: SPM 0 Type: DPT Fabric: ATM	
SCC2 (no enhanced text)	ATM 00	300 6217 INFO ATM LCD Alarm Raised Location: SPM 0 ATM RM in Slot: 10 (InAct) Description: ATM LCD alarm raised.	
SCC2 (with enhanced text)	ATM 00	300 6217 INFO ATM LCD Alarm Raised Location: SPM 0 ATM RM in Slot: 10 (InAct) Description: ATM LCD alarm raised. Location: SPM 0 Type: DPT Fabric: ATM	

[Figure 22](#) shows an example of an SCC2 header format for a CCMT501 log. The log name and number (CCMT501) is shown (see arrow 1). The location of the network element, the network element type (in this case an MG 4000), and the fabric (in this case ATM) is shown (see arrow 2).

For the CCMT, DPTM, IWB, and SPM logs, the location and type field and the fabric field (see arrow 2) only appears in the SN06 and following software release and only if the office parameter SPM_ENHANCED_OUTPUT in table OFCVAR is set to ON. If the office parameter SPM_ENHANCED_OUTPUT is set to OFF, the location and type fields do not appear on the logs. New logs created in SN06 or later display the location and type fields by default, regardless of the value of SPM_ENHANCED_OUTPUT.

Figure 22
CCMT501 log with SCC2 header format



```

00 CCMT 501 5921 INFO Core Connection State Change
Core: LINK 2 CONN 1 VPI 0 VCI 182 TAG 0
Node: SMG4 20 VPI 0 VCI 51
Failed to enable PVC segment.
PVC segment is disabled.
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
Location: SPM 20 Type: SMG4 Fabric: ATM

```

[Table 21](#) shows the CCMT501 log in both NT Standard and SCC2 log formats. In addition [Table 21](#) shows the CCMT501 log with and without the enhanced text that gives the location and type of SPM (see bold text in row two and four of [Table 21](#)). The enhanced text is only visible when office parameter SPM_ENHANCED_OUTPUT is set to ON in table OFCVAR. You can turn the office parameter OFF and ON as frequently as you wish without causing negative effects. Changing this office parameter does not require a restart or any other switch action. The

settings of the SPM_ENHANCED_OUTPUT parameter are able to survive all restarts.

Table 22
Comparison of a CCMT log with and without enhanced text

Log Format		Two variations of the CCMT501 log
NT Standard (no enhanced text)	RTPN05AV **	CCMT501 JUN12 02:15:09 9700 INFO Core Connection State Change Core: LINK 2 CONN 1 VPI 0 VCI 182 TAG 0 Node: SMG4 20 VPI 0 VCI 51 Failed to enable PVC segment. PVC segment is disabled. 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
NT Standard (with enhanced text)	RTPN05AV **	CCMT501 JUN12 02:15:09 9700 INFO Core Connection State Change Core: LINK 2 CONN 1 VPI 0 VCI 182 TAG 0 Node: SMG4 20 VPI 0 VCI 51 Failed to enable PVC segment. PVC segment is disabled. 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 Location: SPM 20 Type: SMG4 Fabric: ATM
SCC2 (no enhanced text)	00 CCMT	501 5921 INFO Core Connection State Changed Core: LINK 2 CONN 1 VPI 0 VCI 182 TAG 0 Node: SMG4 20 VPI 0 VCI 51 Failed to enable PVC segment. PVC segment is disabled. 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
SCC2 (with enhanced text)	00 CCMT	501 5921 INFO Core Connection State Changed Core: LINK 2 CONN 1 VPI 0 VCI 182 TAG 0 Node: SMG4 20 VPI 0 VCI 51 Failed to enable PVC segment. PVC segment is disabled. 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 Location: SPM 0 Type: SMG4 Fabric: ATM

[Table 23](#) lists the SPM-related logs that display the optional SPM location and type field when office parameter SPM_ENHANCED_OUTPUT is set to ON (in table OFCVAR).

Table 23
SPM-related logs that have the optional location and type fields

Log number	Description
ATM300	ATM LCD Alarm raised
ATM301	ATM LCD alarm cleared
ATM500	ATM ILMI status
ATM501	ATM Signaling status
ATM600	ATM Address registration
ATM601	ATM Address de-registration
ATM604	ATM Recovery audit
ATM605	ATM Overload event
CARR300	Carrier failure event set
CARR310	Carrier failure event cleared
CARR330	Facility protection switch
CARR331	Failed facility protection switch
CARR340	Simplex set
CARR341	Simplex clear
CARR500	Carrier state change to InSv from ManB or SysB
CARR501	Carrier state change to CBsy from SysB or ManB
CARR510	Carrier state change to ManB from InSv, SysB, or C-side CBsy
CARR511	Carrier state change to SysB from InSv or CBsy

Table 23
SPM-related logs that have the optional location and type fields

Log number	Description
CARR512	OC3 carrier state changes to CBsy from InSv, ManB, or SysB
CARR800	Threshold crossing alert (TCA)
CARR801	Maintenance limits reset
CARR810	Threshold crossing alert (TCA) set (LBC, OPT,OPR)
CARR811	Threshold crossing alert (TCA)
CCMT301	Core PVC Segment Fault
CCMT501	Core Connection State Change
CCMT502	Peer Connection State Change
CCMT601	Core PVC Segment Fault Cleared
DPTM500	INSV State change
DPTM501	SYSB State change
DPTM502	MANB State change log
DPTM503	PMB State change log
DPTM504	INB State change
DPTM 700	DPT DDM Data Mismatch
DPTM701	DPT Data Mismatch Clear
IWBM500	IW_Bridges OOS
IWBM501	IW_Bridges INSV
IWBM600	Connectivity Mismatch
IWBM601	Audit Action
IWBM900	Bridge depleted
SPM300	Device fault

Table 23
SPM-related logs that have the optional location and type fields

Log number	Description
SPM301	Clock Range
SPM310	Suspend Echo Cancellor Report
SPM311	SW Exception Report
SPM312	TBL Trap
SPM313	MIM Fault
SPM314	TBL IMC
SPM330	SPM Datasync Report
SPM331	Failed Protection Switch
SPM332	Sync Reference Switched
SPM333	SPM REX Failed
SPM340	FAIL CM WarmSwact
SPM350	Free Resources Low
SPM500	Device State Change
SPM502	ATM Connection State Change
SPM503	ATM Carrier State Change
SPM504	ATM Device State Change
SPM600	MS Mode Change
SPM630	Successful Sparing Event
SPM632	SPM REX start time
SPM633	SPM REX Success
SPM650	SPM Device Loader Success
SPM651	SPM Device Loader Failure

Table 23
SPM-related logs that have the optional location and type fields

Log number	Description
SPM660	Continuous Echo Canceller Performance
SPM661	Continuous Echo Canceller Performance Change
SPM680	MBM log message
SPM681	MBM Pool Low
SPM700	DDM Audit Fail
SPM701	DDM Audit Succeeded
SPM702	DDM Dynamic Update Failed
SPM703	DDM Audit Updated Trunk
SPM704	DDM Dynamic Update failed for trunk
SPM705	Trunk State Change
SPM706	Trunk Automatic RTS
SPM707	ISDNPARAMETER DDM Dynamic Update
SPM708	ISDNPARAMETER DDM Audit
SPM709	ISDNPROT DDM Dynamic Update
SPM710	ISDNPROT DDM Audit

For detailed information on setting office parameter SPM_ENHANCED_OUTPUT in table OFCVAR see, *MG 4000 Operational Configuration*, NN10098-511, *IW SPM (ATM) Operational Configuration*, NN10099-511, *IW SPM (IP) Operational Configuration*, NN10100-511, or *DPT SPM (ATM) Operational Configuration*, NN10102-511. For additional information on the Enhanced Logs feature, see *MG 4000 Fault Management*, NN10076-911, *IW SPM (ATM) Fault Management*, NN10077-911, *IW SPM (IP) Fault Management*, NN10078-911, or *DPT SPM (ATM) Fault Management*, NN10080-911.

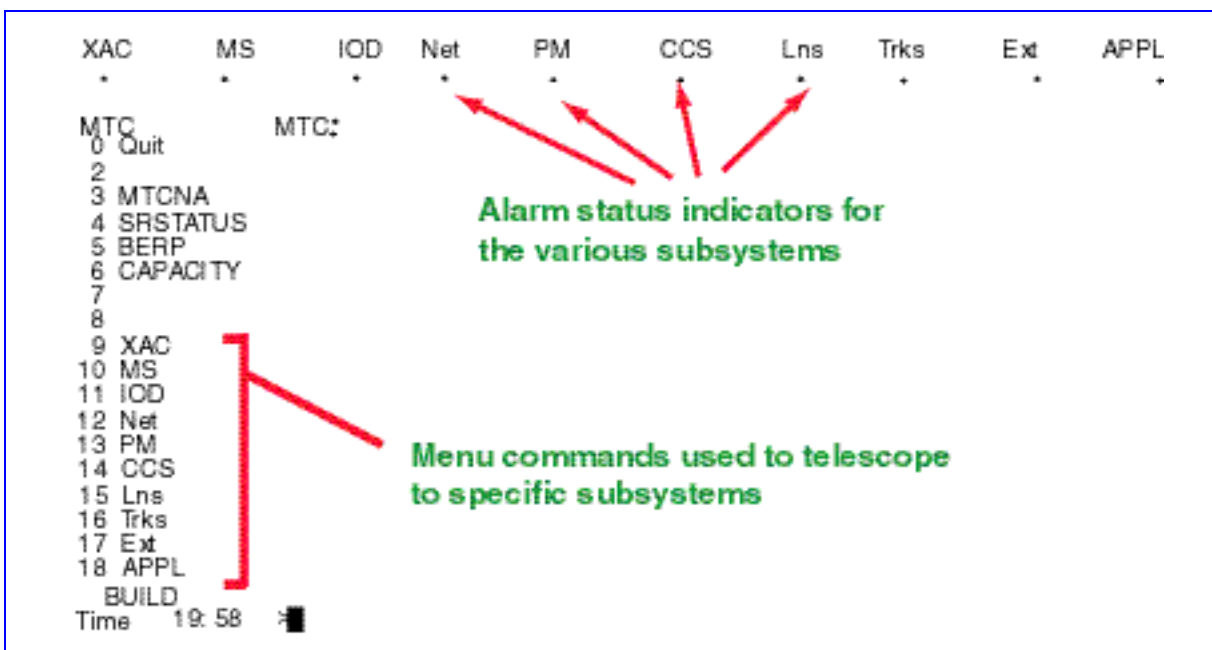
Logging in to the Map and accessing the maintenance level

For detailed information on logging in to the MAP and understanding the general display, see the DMS-100 Family Maintenance System Man-Machine Interface Description, 297-1001-520 on Helmsman.

Once you log in to the maintenance level of the MAP, you can see alarm status indicators along the top status area (see [Figure 23](#)). The alarm status indicators appear under the subsystem codes (for example, XAC, MS, and IOD are subsystem). The dot (*) under a subsystem indicates there is no alarm. When an alarm is present, the priority is shown (*C* is critical, M is major, and blank is minor) with a numerical value to indicate the number of alarms of a given priority.

The log information recorded earlier will assist you in finding the alarm indicator in the status banner, under the appropriate subsystem. If there is more than one alarm, troubleshoot the highest priority (most critical) alarm first.

Figure 23
Example screen showing the maintenance level of the MAP



Navigating to the appropriate subsystem of the MAP

[Figure 24](#) shows an example of the MAP maintenance level for the XAC subsystem and [Figure 25](#) shows an example of the MAP maintenance level for the PM (peripheral module) subsystem.

Note 1: Although DPT (dynamic packet trunk) alarms appear under the PM subsystem on the alarm banner, you obtain additional

information about DPT alarms by accessing the DPTTRM (DPT Terminal Resource Manager) level of MAP. The DPTTRM level is found under the TRKS (trunks) subsystem. To view the DPTTRM level of MAP, use the following path: MAPCI;MTC;TRKS;DPTTRM. For information on clearing DPT alarms appearing under the PM banner, refer to *MG 4000 Fault Management*, NN10076-911, and *DPT SPM Fault Management*, NN10080-911.

Note 2: The DPTRKS level of the MAP is the subsystem where you can view the status of the CICs (circuit identification codes) that are datafilled against each DPT. For an example of the DPTRKS level of MAPCI, see [Figure 26](#). The DPTRKS level is found under the TRKS (trunks) subsystem. To view the DPTRKS level of MAP, use the following path: MAPCI;MTC;TRKS;DPTRKS. The DPTRKS level also allows you to reset single CICs or ranges of CICs, and to busy and return to service CICs.

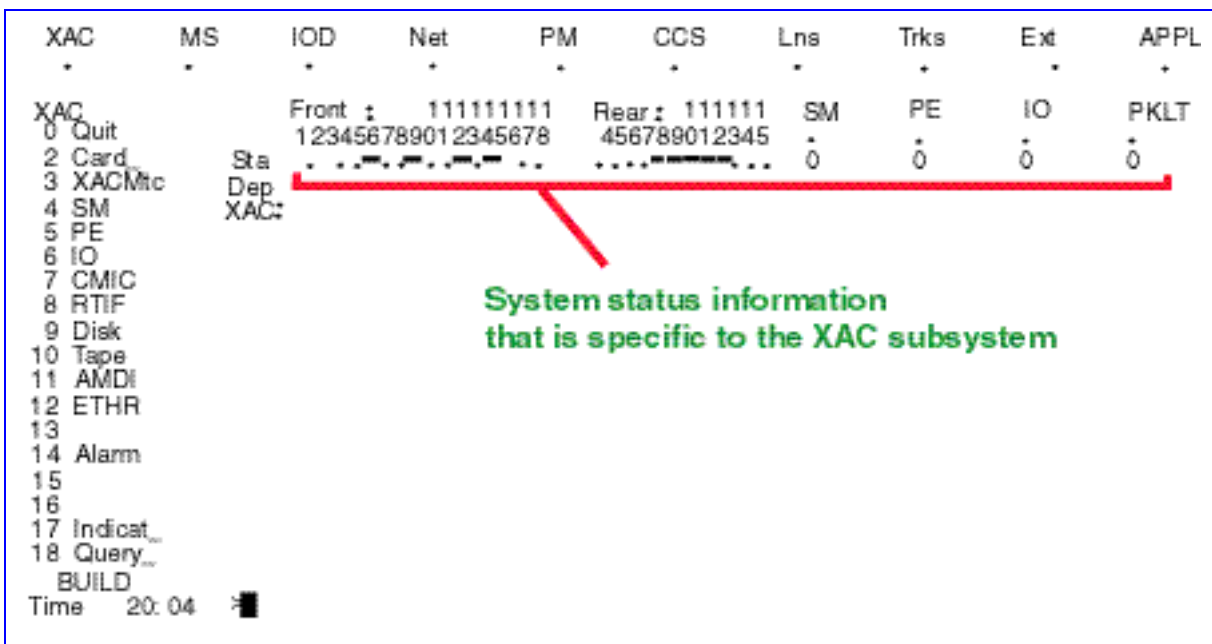
Note 3: There are three ways you can detect STS-1 carrier faults on the MG 4000. The first way is by means of the DMS LOGUTIL system (logs 300 and 310). Secondly, STS-1 carrier faults appear as SYSB at the carrier MAP level. Lastly, you can use the Listlalarm command at the carrier MAP level, to display any faults for a posted carrier.

Note 4: You can use the QueryPM command with the Reason option (for example, QueryPM Flt Reason), for posted SPMs (Spectrum peripheral modules) to find out the reason why the RM (resource module), or CEM (common equipment module) is in an in-service trouble or system busy state. You can use this command on SPMs such as the IW SPM, MG 4000, DPT SPM, as well as legacy SPMs connected to the ENET. The QueryPM command with the Reason option is available at the PM level of the MAP once you've posted one or more SPMs.

You can display a list of alarms at the PM level of the MAP by using the ListAlm (list alarms) and Disp_ (display alarms) commands. You can view current logs at any time on the MAP by using the LOGUTIL tool. For detailed information on the log system see the North American Log Report Reference Manual, 297-8021-814 on Helmsman.

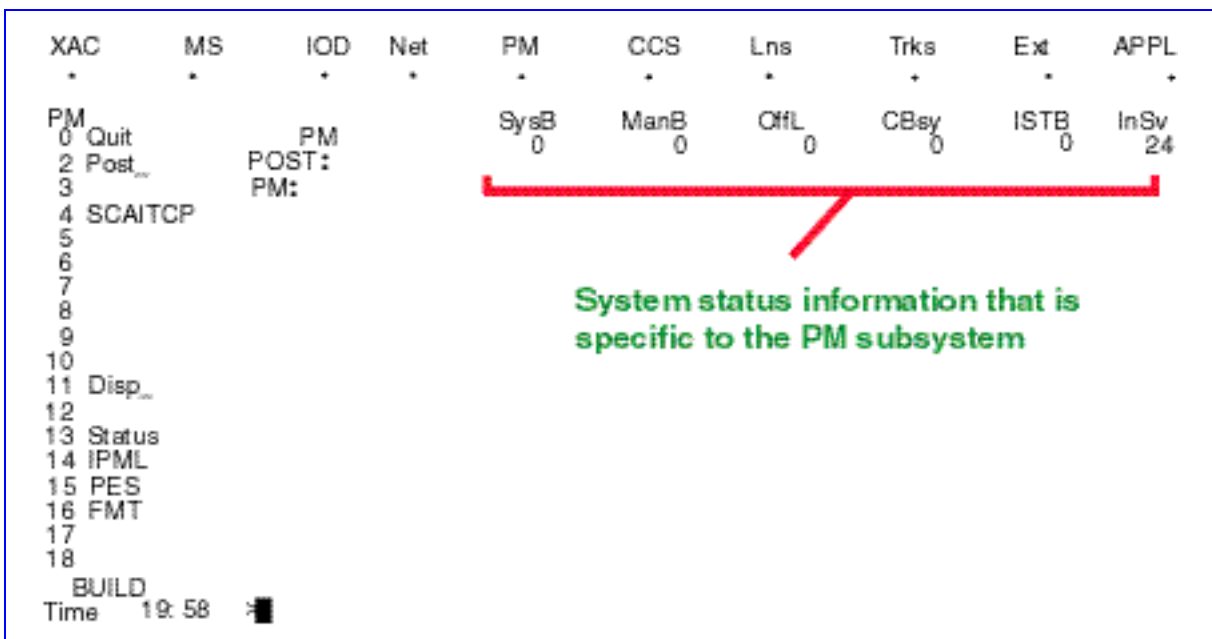
For detailed information on telescoping between subsystems of the MAP, see the DMS-100 Family Maintenance System Man-Machine Interface Description, 297-1001-520 on Helmsman.

Figure 24
Example MAP display of the XAC subsystem



[Figure 25](#) shows an example of the MAP maintenance level for the PM (peripheral module) subsystem.

Figure 25
Example MAP display of the PM subsystem



DPT and DPT trunk maintenance MAPCI level enhancements

The DPT trunks (DPTRKS) MAPCI level includes a display of the number of call identifier codes (CICs) that are in the maintenance (MTC) state. There are three sub-statuses of this maintenance state: PV (protocol violation), FE_BLK (far_end blocked), and FE_UnEQ (far_end unequipped). (See [Figure 26](#).) In [Figure 26](#), the three sub-statuses are shown in bold type with red underline. Beside each sub-status name is the number of CICs currently in that maintenance state. In addition, the busy (BSY_) command (without any arguments) and return to service (RTS_) command (without any arguments) are available at the DPTRKS level.

For procedures on how to use the commands at the DPTRKS level of MAPCI, see *MG 4000 Operational Configuration*, NN10098-511, or *DPT-SPM (ATM) Operational Configuration*, NN10102-511.

When BICC DPT trunk groups go out of service, the local switch automatically sends group blocking messages to the far-end switch. Reacting to the group blocking messages, the far end switch sets the associated CICs to a state of FE BLK (far_end blocked) so that no traffic is directed from the far end switch to the local switch. When BICC DPT trunk groups return to service, group unblocking messages are automatically sent from the local switch to the far-end switch. Once the group unblocking messages are received, the far-end switch sets the associated CICs to a state of FE IDL (far_end idle) to allow them to handle traffic again.

Figure 26
DPTRKS level of MAPCI

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
ETHR	.	POOL05	.	1 SPM	.	.	C	1 Min	.
M				*C*					
DPTRKS									
0 Quit									
2 Post_		CKT	TYPE	COM	LANG		STATE	RANGE	
3		2W	ISP	DPTEANLOOP			INSV 30000	32046	
4									
5 BSY		IDL:	0						
6 RTS		CPB:	0						
7 OP		MTC:	2046						
8 FRLS		PV: 0		FE BLK: 2046		FE UnEQ: 0			
9 Reset		PENDING:	0						
10									
11 PREV									
12 NEXT									
13									
14									
15 TrkQry									
16 QrySig									
17 RouteSet									
18 QryMtc									

The local switch does not send out a group blocking message to a far-end switch if the affected CICs (either the starting CICs or the entire range of CICs) at the far-end switch are not provisioned. In other words the CICs are in a FE_UNEQ (far_end unequipped) state, the local switch does not send out a group blocking message.

If the far-end switch receives a group blocking message and the starting CIC in the range (or the entire range of CICs) are not provisioned, or the range state of the DPT trunk is in INB, then the far-end switch sends out one UCIC (unequipped circuit identification code) message to the local switch. Next, the far-end switch discards the group blocking message.

Fast routeset recovery after switch initialization

Nortel Networks has defined a proprietary group reset message that resets all of the CICs (circuit identification codes) in one routeset. This super group reset message reduces the time necessary for routeset recovery. In SN05 a switch can have up to 38 million CICs.

In order to use the super group routeset message, you must provision the SGRPRSC field in table ADJNODE (adjacent node). The super group routeset message only works in networks where the far end switch is a Nortel Networks DMS (digital multiplex system) switch running a CVoIP SN05 (or higher) software load. Any far-end switch that does not meet these requirements treats the group reset message as unrecognizable and discards the message. For information on provisioning the SGRPRSC field in table ADJNODE, see *CS 2000 Operational Configuration*, NN10201-511.

Assuming the far-end switch is a DMS running SN05 or higher, the local switch continues to send the group reset message in 60 second intervals until one of the following events occurs:

- the local switch receives the group reset acknowledgement from the far-end switch
- all of the ranges within the routeset are placed in an INB (installation busy) state through manual intervention at the MAPCI using the busy or installation busy commands
- the super group reset option (SGRPRSC) is deleted in table ADJNODE.

During a reload or a cold restart, the DPT range state is set to the RINI (range initialization) state if the SGRPRSC field is set in table ADJNODE. After the local switch receives an acknowledgement for the super group reset message, the local switch changes the RINI state to

the recovery state for the routeset to which the DPT trunk group belongs.

The RPV (range protocol violation state) for DPT trunks indicates that the far-end switch has not acknowledged a message from the local switch. The RPV state is replaced by the recovery state after the local switch receives the acknowledgement. When the RPV state is set on a range of CICs, the call processing software can not use any CICs within that range. You can use the manual MAPCI commands “bsy inb” to change the RINI or RPV state to INB (installation busy).

Clearing flash memory before a CEM is moved or de-commissioned

Flash memory in the common equipment module (CEM) of an SPM (Spectrum peripheral module) stores the IP (Internet Protocol) address, and the load of the CEM. If you move the CEM from the current SPM shelf to a different location or platform (or de-commission the CEM), you must clear the flash memory of the CEM. Otherwise, the information in the CEM may cause the following problems to occur:

- there are two CEMs trying to own the same IP address
- the CEM is not able to recover due to a mismatch in the IP address
- the CEM may auto-boot an incorrect software load

You can use the erase flash (ERASEFL) command at the MAPCI CEM level to erase the flash memory of CEMs. The erase flash command is supported for legacy SPMs, IW SPMs, MG 4000s, and DPT SPMs.

For detailed procedures telling you how to erase CEM flash memory, see *IW SPM (ATM) Fault Management*, NN10077-911, *MG 4000 Fault Management*, NN10076-911, or *DPT SPM Fault Management*, NN10080-911, or *SPM Fault Management*, NN10075-911.

Additional information

For additional details on fault management tools and utilities, refer to the following component documentation:

- *SPM Fault Management*, NN10075-911
- *MG 4000 Fault Management*, NN10076-911
- *IW-SPM (ATM) Fault Management*, NN10077-911
- *IW-SPM (IP) Fault Management*, NN10078-911
- *SDM Fault Management*, NN10081-911
- *CS 2000 Core Manager Fault Management*, NN10082-911

- *CS 2000 Fault Management, NN10083-911*

Core and Billing Manager

ATTENTION

The Core and Billing Manager (CBM) does not apply to the PT-AAL1 solution.

The CBM provides fault management functions for alarms and logs.

CBM alarms

The CBM provides the alarm status dynamically in the CBM maintenance interface (MI). The status of the CBM and its components are also available through command line query commands.

The CBM's aggregated product state will also be reflected in the server LEDs for critical, major and minor alarms as well as through the office alarm unit (OAU) in the breaker interface panel of the PTE2000, MIS or CMIS frame. The CBM800 link alarms are reported on the Core. The CBM800 aggregated node state will be aggregated with the link states and alarmed on the Core.

CBM logs

CBM applications and services generate customer logs. These customer logs are written to persistent storage in a simple text file. These files are rotated daily or when disk space is limited. The CBM base will generate an aggregated system log describing the overall system state.

These CBM logs as well as the managed Core logs are provided to the customer in SCC2 or Nortel Standard format through the Log Delivery Service ([linke here?](#)). The Log Delivery Service provides the ability to configure multiple log streams (or devices) which can be files or incoming or outgoing TCP-IP connections. In addition the customer logs are stored local on the CBM, for a configure-able number of days, available for review through the LOGQUERY interface which operates similarly the DMS CI; LOGUTIL interface.

Media Gateway 9000 Manager

ATTENTION

The MG 9000 Manager only applies to the UA-AAL1, UA-IP, and Intl UA-IP solutions.

The Media Gateway 9000 (MG 9000) Manager is a server/client application that runs on a Sun Solaris workstation. A graphical user interface (GUI) allows fault handling and reporting.

The MG 9000 Manager allows the following fault management functions:

- retrieve, view, acknowledge/unacknowledge, and report alarms
- retrieve and view logs
- test lines
- perform line circuit diagnostics

Alarms

Alarm surveillance, correlation, and reporting is performed at the Alarm Browser screen. The Alarm Browser screen is accessed from the Alarm menu option, which appears at the top of all screens. The Alarm Browser screen consists of multiple sections used to view and retrieve and view frame and shelf level MG 9000 alarms. The alarms are displayed as table list in the Alarm Browser. To maximize the performance of the Alarm Browser, alarms are displayed one page at a time. By selecting one of the alarms, the alarm related information can be seen at the alarm text panel at the lower portion of the Alarm Browser. The alarm counts can be viewed from each Subnet Icon, Frame, Shelf, Card, Port, and Circuit Listing GUIs. The generated alarm events are reported to NML's OSS client through a dedicated OSS Corba Event Channel.

Logs

When MG 9000 logs are generated, they are written to the MG 9000 Manager screen and are then directed to log files. The logs are written into the following two files:

- /data/mg9kem/logs/mg9kem.custlog (customer log file)
- /data/mg9kem/logs/mg9kem.deslog (designer log file)

The log files are named according to the type of log. The customer logs are directed to the custlog file using Syslog. The design logs from all the processes are directed to the deslog file using the Unix Syslog daemon.

The custlog seen at the MG9000 Manager correlates to alarms seen at the Alarm Browser screen and the traps generated from Gateway when the status changes. The designer logs seen at the MG 9000 Manager records tracing and debugging history of the manager execution. The designer can use it to correct the bug when the MG 9000 Manager is in an unstable state. In addition to the alarms being viewed at the MG 9000 Manager, alarms are also forwarded to the Operator Services System (OSS) for network level alarm monitoring.

Line test and diagnostics

The following functions are available for line test:

- **MAPCI user interface**

Testing and troubleshooting of lines faults is available using a Maintenance and Administration Position (MAP) user interface at the levels below the LNS MAP level. The LNS MAP level contains the lines test position (LTP) menu commands, the automatic line testing (ALT) menu commands and the lines service trouble (LNSTRBL) commands.

- **MTAP test manager**

The metallic test access point (MTAP) line test screen provides an interface to pass line test commands from the manager to external test equipment.

The Nortel Networks Access Care external test system has direct access to test heads collocated with the MG 9000 for line testing and communicates with the manager line test manager through an ethernet port. The manager software provides the line test management application to convert the Access Care parameters into commands that can be forwarded and processed in the MG 9000. The GUI specifies the test heads for Access Care use when testing a specified line circuit.

- **DTA test manager**

DTA (Digital Test Access) is the functionality used to test private lines circuits by setting up test access connections with external test equipment. Compatible external test systems pass TL1 (Transaction Language 1) requests through an ethernet port to the MG 9000 Manager to set up appropriate MG 9000 connections to collocated testheads or remote test units.

Line circuit diagnostics

The Line Circuit Diagnostic subsystem provides utilities that perform diagnostics on line circuits on the following cards:

- POTS multi-circuit line card (POTS-32)
- Service Adaptive Access circuits (SAA-12 card)
- ADSL DMT Combo 8x8 card (8x8 ADSL)

For more information on Media Gateway 9000 Manager fault management, refer to the following documents:

- *MG 9000 Fault Management module*, NN10074-911
- Access Care documentation

CS 2000 SAM21 Manager**ATTENTION**

The CS 2000 SAM21 Manager does not apply to the PT-AAL1 solution.

The CS 2000 SAM21 Manager performs the following fault management functions:

- Manages faults in the individual shelf slots and the hardware configured and installed in the application slots
- Manages Maintenance functions associated with the individual shelf slots and the hardware configured and installed in the application slots
- Uses the provisioning information to deliver a graphical representation of each SAM21 shelf within the call server
- Uses the graphical representation of each SAM21 shelf to identify, acknowledge, study, resolve and clear alarms
- Generates SAM21 log reports to indicate
 - raising and clearing of alarms for all cards in the shelf
 - state transition for all card types in the shelf
 - card insertion and removal for all card types
 - ATM faults if the Shelf Controller uses the ATM interface and is deployed in an ATM network

Log reporting for CS 2000 Management Tools applications

All applications and devices under the CS 2000 Management Tools use the SSPFS Logging API to record their logs. This API doubles as the custlog feed to the OSS Fault Collector. It supports five levels of logs:

- critical
- major
- minor
- warning
- none

The API also provides four types of logs

- customer logs - alarms and other customer visible events
- audit logs - user actions taken
- authentication logs -security events
- debug logs - software or hardware errors

Controlling the forwarding of logs is done through use of the *syslog.conf* file on the SSPFS machine. This file (a standard syslog file) is used by syslog to dictate its behavior. This file is a simple text file that can be edited to define whether to record the logs on the local machine and/or whether to send them to another machine (i.e. the OSS Fault Collector). The level of control is on a log level basis, so critical logs can be handled one way and warning logs another. By default, the only logs that are forwarded are the customer logs (alarms), although, as noted above, this is customizable.

Note: Currently, the CS 2000 GWC Mgr and CS 2000 UAS Mgr send logs northbound though other 3rd party interfaces as well.

CS 2000 Gateway Controller Manager**ATTENTION**

The CS 2000 GWC Manager does not apply to the PT-AAL1 solution.

The CS 2000 Gateway Controller Manager GUI/CLUI performs the following fault management functions:

- Service data required for call processing
- Interfaces required to collect and distribute the data
- Provisioning data rules

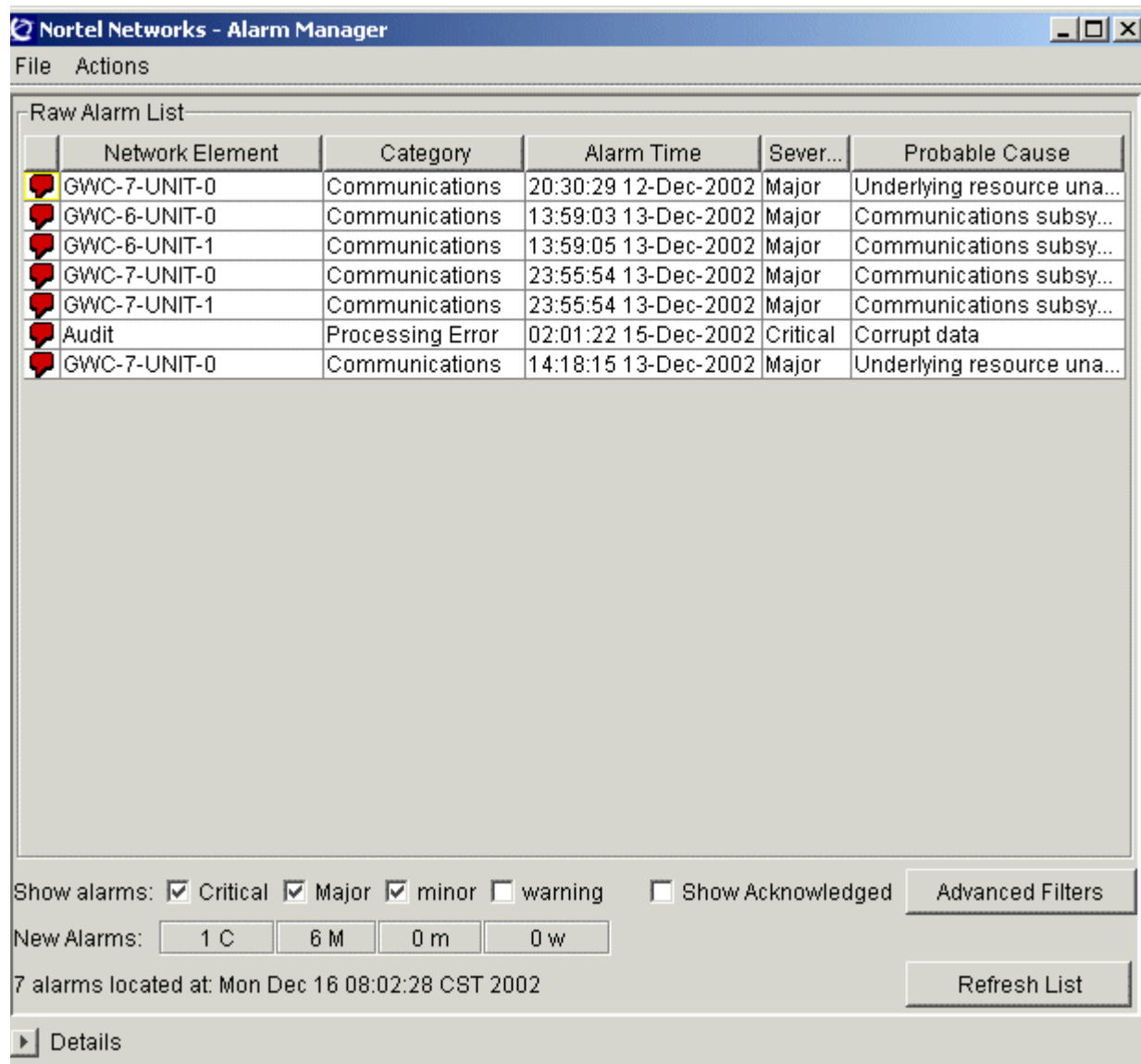
- Manages Maintenance state
- Manages alarm collection and reporting
- fault verification
- maintenance

The user can view the alarms and the status of hardware components through the CS 2000 Gateway Controller Manager which also supports the following activities:

- Alarm Reporting
- Alarm History retrieval and browsing

Alarm Reporting

The CS 2000 Gateway Controller Manager Alarm Manager is launched from the 'Fault' pull-down menu on the Call Server Management Tools GUI. The Alarm Manager pops up to the foreground. [Figure 27](#) shows the Alarm Manager without details.

Figure 27 Alarm Manager without details

After the browser pops up, the user has the ability to filter for severity and acknowledgement state. Alarms are displayed in the center alarm table panel. The headers for the center alarm table panel are Network Element Name, Alarm Level, Category, Alarm Time, Probable Cause, Acknowledge Time, System Uptime, Component ID, Alarm Description, and Specific Problem. Category and Network Element Name can be filtered by selecting the Advanced Filters button. Below the filters are the alarm counters. From here the user can see the total number of alarms present in the system, broken down by severity. Also, the display

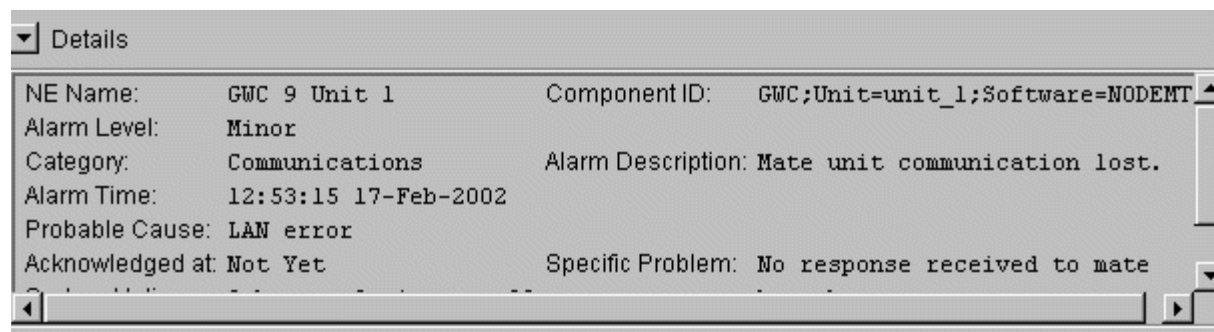
contains a total count and the time in which the last alarm was received or the last time the GUI was refreshed.

The retrieve button activates the search for the desired alarms as per the customer settings. The Alarm Manager components display an active list of the most current alarms on the system. It is updated automatically when an alarm occurs on a managed device. When an alarm is cleared, it disappears from the display. The new Alarm Manager also gives the user the ability to acknowledge an alarm. This acknowledgment state is applied to all active Alarm Managers, and is persisted with the alarm in the database.

At the bottom of the display is the details panel. The details of an alarm can be displayed by ensuring the details panel is showing (select the arrow button to point down), and then selecting the alarm from the Alarm Table. The user can show and hide this panel by selecting the arrow button beside the Details label. This panel shows all information in the alarm. In order to display the information for the current alarm in the details panel, the user can select the row of interest. This processes a request to the database to gather this information.

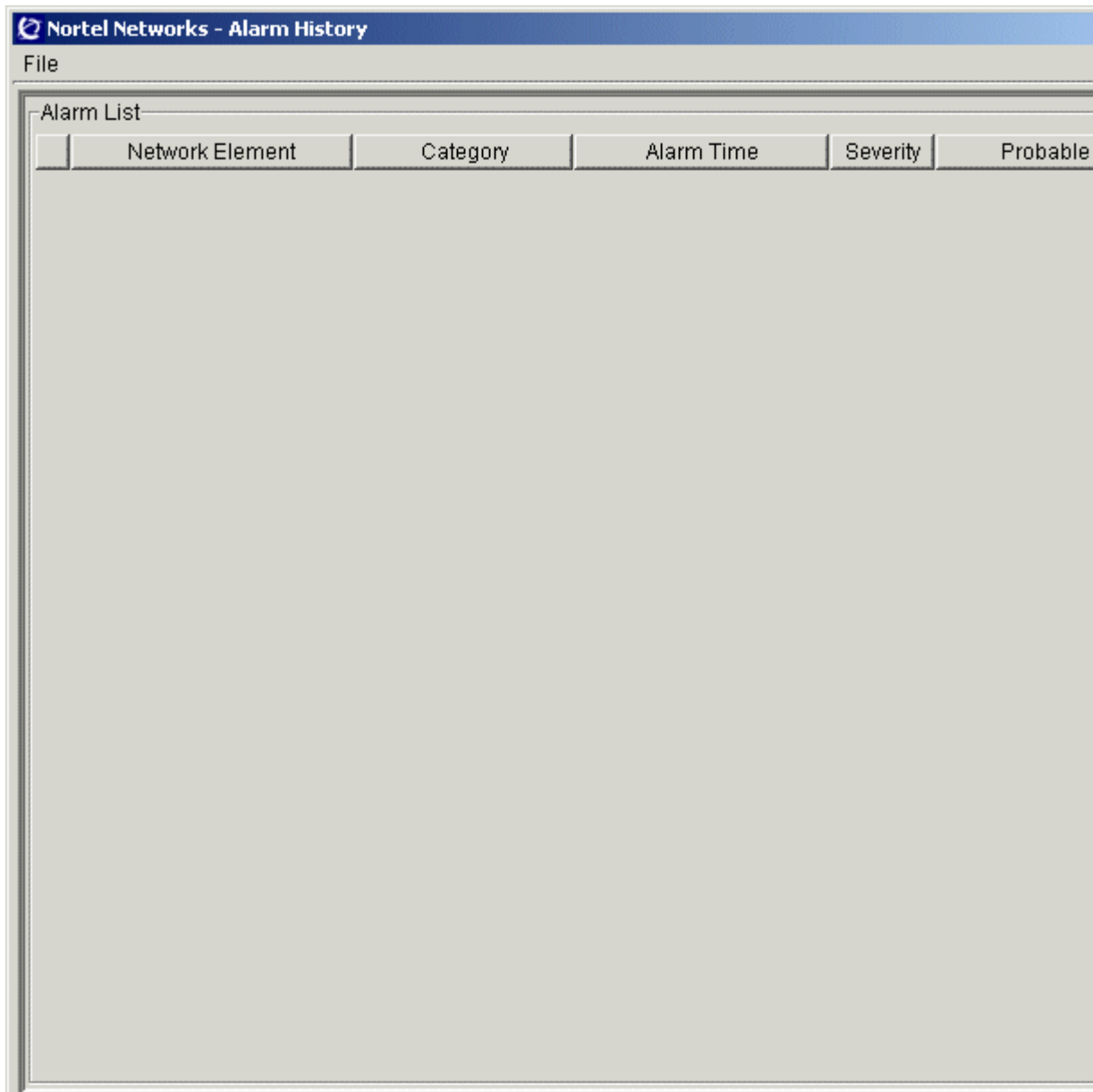
Alarm Totals can be viewed at the bottom left just above the details panel. Alarm totals are for critical, major, minor, and warning alarms. Once an alarm has been cleared, its corresponding field is decremented. There is also a total alarm count which includes the time of the last update to the display. [Figure 28](#) shows the Details panel of the Alarm Manager window.

Figure 28 Alarm Manager details



Alarm History retrieval and browsing

Unlike the Alarm Manager, the Alarm History is a static view of the system. The Alarm History window is launched from the 'Fault' pull-down menu on the Call Server GUI. The Alarm History pops up to the foreground. [Figure 29](#) shows the alarm history without details.

Figure 29 Alarm History without details

The Alarm History gives the ability to search based on Network Element Name, Alarm Level, Category, Alarm Time, Probable Cause, Acknowledge Time, System Uptime, Component ID, Alarm Description, and Specific Problem. To update the list of network elements currently displayed, the user can refresh the list by the Action pull-down menu, and Refresh Network Element List. All alarms are stored in the Alarm History table and in the event history syslog. The event history syslog resides in the CS 2000 Gateway Controller Manager or the Universal

Audio Server Manager server under “ptmlog” file name. Location of the file is /var/log.

The Alarm History gives the user the ability to view both active and inactive alarms that have existed on the system for some time. It uses the concept of paging to avoid keeping many alarms in memory at a given time. It displays the same information that the Alarm Manager does, as well as the time in which the alarm was cleared, if it was. The Alarm History is a frame and as such is independent from the main CS 2000 Gateway Controller Manager or the Universal Audio Server Manager GUI.

Once the user selects Search, one page of a fixed size displays on the screen. To advance the display, the user can select Next Page, and can go back to the beginning by selecting First Page. The Alarm History display has a details panel that is almost identical to the Alarm Manager. In addition, it also has the Clear Time. This can be accessed by the arrow button, just as the details panel in the Alarm Manager.

If the number of alarms from the current search is greater than 25, the user can select the Next Page button to see the next batch of alarms. There is a First page button which resets the search to the beginning. The details panel works exactly as it does in the Alarm Manager. First the user must ensure it is displayed using the arrow button in the lower left of the display. Then select an alarm from the Alarm Table, and the details display similar to how they are displayed in the Alarm Manager.

CS 2000 GWC Manager logs

For information on CS 2000 GWC Manager logs, refer to [Log reporting for CS 2000 Management Tools applications on page 76](#).

Session Server Manager

ATTENTION

The Session Server Manager only applies to the IAC, PT-IP, and Intl PT-IP solutions.

Alarms and logs for the Session Server are viewed through the Session Server Manager.

Alarms

The Session Server Manager has the capability for applications or the system itself to generate alarms. These alarms can be viewed on the Session Server Manager's Alarm web page. Information shown about

particular alarms include the type, identifier, time-stamp, host (unit from which the alarm was raised), severity, and a description of the alarm.

The user may view alarms by going to the alarms web page. The alarm web page is located in the Monitoring menu folder.

Once the craftsperson clicks on Alarms, the alarm web page is presented in the right frame with the current alarm list. The alarm web page updates every 30 seconds and the user also has the option of invoking a re-query of alarms. This is similar to the Alarm implementation for the Storm system.

The following figure shows a sample alarms web page for the Session Server Manager.

Figure 30 Session Server alarms web page

Unit	Activity	Jam	State	Connectivity	Host Name	Last Update Time
1	Active	no	1C+	.	sp2k-2	01:41:40

The Alarms panel updates every 45 seconds Datestamp of last update: Friday April 30th 2004 01:41:23 PM EST					
Type	ID	Timestamp	Host	Severity	Description
Communications	Out of Service	Friday April 30th 2004 01:36:25 PM	sp2k-1	Critical	SIP Gateway Application System Busy
Communications	Application Subsystem Failure	Friday April 30th 2004 01:36:31 PM	sp2k-2	Major	SIP Gateway Application Mtc Out Of Sync
Communications	Application Subsystem Failure	Friday April 30th 2004 01:36:24 PM	sp2k-1	Major	SIP Gateway Application Mtc Out Of Sync

Additional information is available in *Session Server Fault Management*, NN10332-911.

Logs

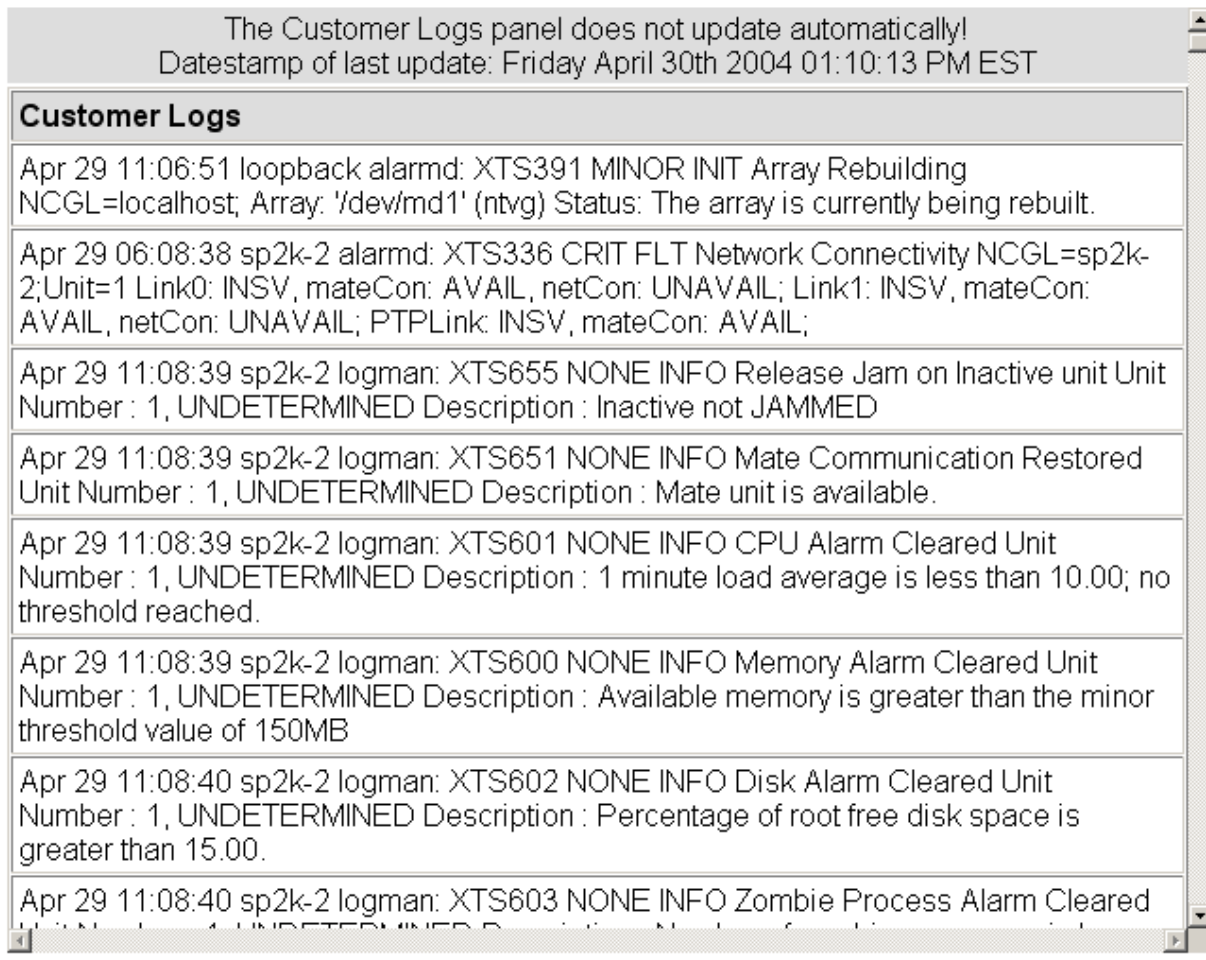
The Session Server Manager has the capability for applications or the system itself to generate logs. These logs can be viewed on the

Session Server Manager's log web page. Information shown about a particular log includes the following data:

- Timestamp
- Session Server device name
- Process that generated the log
- Log ID and number
- Alarm severity
- Log type
- Log label
- Additional information

The user may view logs by going to the logs web page located in the Monitoring menu folder.

Once the craftsperson click on Logs, the log web page is presented in the right frame with the current log list. Unlike the alarms page, the logs page does not update automatically. A sample log web page is shown below.

Figure 31 Session Server logs web page

Note: The body of log formats shown in this document are the formats for Session Server logs if viewed from the Integrated EMS. Log formats may differ if logs are viewed from the Session Server Web Interface. The content of the logs will not differ, only the formatting.

Additional information is available in *Session Server Fault Management*, NN10332-911.

Universal Audio Server Manager

ATTENTION

The UAS Manager does not apply to the PT-AAL1 solution.

The Universal Audio Server (UAS) Manager performs the following fault management functions:

- allows for retrieval of logs and responses to clear system faults that generated the logs
- allows for retrieval of alarms and responses to clear the faults that generated the alarms

UAS fault reporting is based on Simple Network Management Protocol (SNMP). Both alarm and log retrieval, and system correction tasks are performed either through the Universal Audio Server Manager GUI or through commands entered at a command line or Windows interface. The Universal Audio Server Manager also supports the following functions:

- Alarm Reporting
- Alarm History retrieval and browsing

Alarm Reporting

The alarm reporting for the Universal Audio Server Manager is the same as the alarm reporting for CS 2000 Gateway Controller Manager. For details, refer to the Alarm Reporting information under CS 2000 Gateway Controller Manager of this section.

Alarm History retrieval and browsing

The alarm history retrieval and browsing for the Universal Audio Server Manager is the same as the alarm history retrieval and browsing for the CS 2000 Gateway Controller Manager. For details, refer to the Alarm History retrieval and browsing information under CS 2000 Gateway Controller Manager in this section.

UAS Manager logs

For information on UAS Manager logs, refer to [Log reporting for CS 2000 Management Tools applications on page 76](#).

Media Server 2000 (MS 2000) Series

ATTENTION

The MS 2000 Series does not apply to the PT-AAL1 solution.

MS 2000 Series fault reporting is based on Simple Network Management Protocol (SNMP). The MS 2000 Series carrier-grade alarm system provides a reliable alarm reporting mechanism that takes into account element manager outages, network outages, and an unreliable transport mechanism (SNMP over UDP). A carrier-grade alarm system is characterized by the following capabilities:

- a mechanism to allow an EM to determine which alarms are currently active in the NE. (The NE maintains an active alarm table.)
- a mechanism to allow an EM to detect lost alarm raise and clear notifications. [seq no in trap, current seq no mib object]
- a mechanism to allow an EM to recover lost alarm raise and clear notifications [keep a log history]
- the ability to send a cold start trap to indicate that it is starting. This allows the EM to synchronize its view of the NE's active alarms.
- clear alarms before shutting down if possible.

Both a listing of active alarms and a history of alarm are maintained on the MS 2000 Series servers using the standard NOTIFICATION-LOG-MIB and draft of the ALARM-MIB for the alarm history and active alarms.

The source for these traps is a proprietary enterprise SNMP MIB for the 2000 Series, called "AcBoard". Traps are generated off the Trunk Pack Modules (TPMs). Either TPM for the MS 2010 can generate traps. In the case of the MS 2020, there is only one TPM.

Customer logs

The traps mentioned above are sent from the MS 2000 series. These traps are received and processed by the Integrated EMS system in the network. The MS 2000 server must be added to Integrated EMS for monitoring and management. AMS numbers are added to the MS 2000 SNMP traps as they are processed by the management server and are visible in the Integrated EMS user interface.

BootP operation

A BootP server is configured on the SDM or CBM for the MS 2000 Series. The BootP server is needed, initially, for assigning an IP address for a MS 2000 Series node when it is installed. After installation

is complete, the BootP server is used as a backup configuration repository for MS 2000 Series software loads (CMP file) and the basic configuration file (INI file).

A request to reload the CMP and INI files to a MS 2000 Series node from the BootP server is generated in response to the following events:

- the MS 2000 Series node is power-cycled
- the MS 2000 series is reset
- a watchdog process running on the MS 2000 Series node determines that a fatal error has occurred in the IPM-1610 board

Audio Provisioning Server (APS)

ATTENTION

APS does not apply to the PT-AAL1 and UA-AAL1 solutions.

APS Fault Management consists of handling logs and alarms. Both logs and alarms for the APS utilize a management station. A management station can be one of the following platforms:

- a desktop PC running Windows NT 4.0 with Service Pack 4 or higher and all PTM daemons
- a Solaris workstation running the PTM software and an Oracle database
- a desktop PC running an MIB browser

APS logs

APS logs are collected from various sources in the APS and are optionally sent to a management station through SNMP traps. Sources of APS logs include the following locations:

- APS administration
- APS Audio Management
- APS File Upload
- APS Servlet Requests
- IPS software

Logs from each of the above sources can be of type information, warning, or error.

APS alarms

Alarms are sent from the various APS software components to the management station. The following table lists the fields that are associated with APS alarms.

Table 24 APS alarm fields

Field	Description
severity	warning, minor, major, or critical
probable cause	Qualifies the cause of the alarm condition. Takes the form of an integer from a range of standardized values from the NORTEL-NMI-TC-MIB . Possible values includes the following causes: • 1-adapter error • 7-configuration or customization error • 8-congestion • 17-file error • 46-software error
problem type	This type categorizes the alarm. Possible values include the following types: • communication • environmental • equipment • quality of service • processing error
specific problem	A number that uniquely identifies the alarm.
component name	Name of the software or hardware component for which this alarm is associated.
additional text	Text description of the alarm.

Network Patch Manager (NPM)

ATTENTION

The NPM application does not apply to the PT-AAL1 solution.

The NPM application utilizes an SSPFS-based API interface to capture logs and alarms and send them northbound to the CS 2000 Core Manager or any type of OSS Fault Collector.

Universal Signalling Point Manager

ATTENTION

The USP Manager does not apply to the PT-AAL1 solution.

USP Manager performs the following fault management functions:

- viewing alarms
- selecting alarms
- printing alarms
- clearing alarms
- viewing logs
- retrieving logs
- printing logs
- testing links
- maintenance

For additional details on the fault management aspects of the USP Manager, refer to the *USP Fault Management* module, NN10071-911.

Multiservice Data Manager

MDM performs the following fault management functions:

- supports maintenance
- supports configuration
- supports reporting of faults for the Multiservice Switch 15000/Media Gateway 15000 or Multiservice Switch 7400/Media Gateway component faults

- supports the API to deliver log and alarm data to an OSS
- supports carrier maintenance activity for Multiservice Switch 15000/Media Gateway 15000 and Multiservice Switch 7400/Media Gateway 7400

The user can view the status of hardware components through the MDM which also supports the following tasks:

- Alarm Surveillance
- Alarm Reporting
 - Network status bar
 - Network viewer
 - Component information viewer
- Alarm History retrieval and browsing
- Alarm Display
- Alarm Help

Alarm Surveillance

MDM Advisor toolset provides alarm surveillance to the Multiservice Switch 15000/Media Gateway 15000 and Multiservice Switch 7400/Media Gateway 7400. The MDM tools are launched from a launch pad called the MDM toolset. This set of tools provides a common view of network surveillance data across all supported devices. The Advisor toolset provides both alarm and state based surveillance. For detailed information, see the MDM User Guide, 241-6001-011.

Alarm Reporting

The MDM collects Multiservice Switch 15000/Media Gateway 15000, Multiservice Switch 7400/Media Gateway 7400, and MDM alarm and log data, through Ethernet connections to each. The MDM includes both graphical and command-line user interfaces to perform the various network management activities. Within the MDM, device states, device subcomponents, and links are represented by a specific color. The mapping from state to color is user configurable. Alarms are presented on the MDM with a color to distinguish the alarm severity. The color to alarm severity mappings are configurable.

[Table 25](#) shows default state to color mapping.

Table 25 Default state to color mapping

State	Color	Explanation
Unknown (UNKN)	Grey	The component is unreachable
Out-of-Service (OOS)	Red	The component is no longer operational
In Service Trouble (ISTB)	Orange	At least one important sub-component is out-of-service
In Service Trouble	Yellow	Secondary sub-components are out-of-service
In Service (INSV)	Green	The component is operational

[Table 26](#) shows default alarm severity to color mapping.

Table 26 Default alarm severity to color mapping

Alarm Severity	State
Unknown	Light blue
Warning	Dark blue
Minor	Yellow
Major	Orange
Critical	Reg

Network status bar This MDM tool provides a high-level view of all network element alarms in the network ([Figure 32](#)). The Network Status bar gives the total and the severity of the alarms. In addition, the Network Status bar performs the following functions:

- Provides a high-level view of component states
- Displays only the troubled components (if requested)
- Allows users to acknowledge the current state of the network
- Allows users to drag and drop troubled components on to the Component Information Viewer and the Command Console GUIs

Figure 32 MDM Network Status bar

Component States	Totals	OOS	ISTB	INSV	UNKN
Modules/Subcomponents	16/3375	548	18	1592	1233
Links/DBNLs	44/0				

Active Alarms Total/Rate	Critical	Major	Minor	Warning	Unknown
610/11	135	439	32	4	0

Buttons: Refresh, Troubled Components..., Acknowledge

Network viewer This MDM tool presents a real-time graphical network map of all Multiservice Switch 15000/Media Gateway 15000 and Multiservice Switch 7400/Media Gateway 7400 configuration elements, including components, trunks, and links. The Network Viewer of the MDM provides the following functionality:

- Represents different device types by the shape of the icon and represents the states of components by the color of the icon.
- Monitors and displays component states for first-alert surveillance.
- Provides flexibility to display an organization view of Multiservice Switch 15000/Media Gateway 15000 and Multiservice Switch 7400/Media Gateway 7400 configuration elements by grouping the objects in a way that reflects the required view by function.
- Displays a high-level view of each Multiservice Switch 15000/Media Gateway 15000 and Multiservice Switch 7400/Media Gateway 7400 shelf for quick identification of areas that require action.
- Provides access to other Advisor tools through main menus and pop-up menus displayed after selecting a network element in the map.

Component information viewer The MDM tool provides diagnostic analysis of a component in relation to an event identified by the other surveillance tools such as Network Viewer and Alarm Display. The Component Information Viewer displays an active or recent alarm list as well as component status records, and correlates fault impacts and causes. This tool also has filtering options that allow viewing of impact on related components.

Alarm history retrieval and browsing

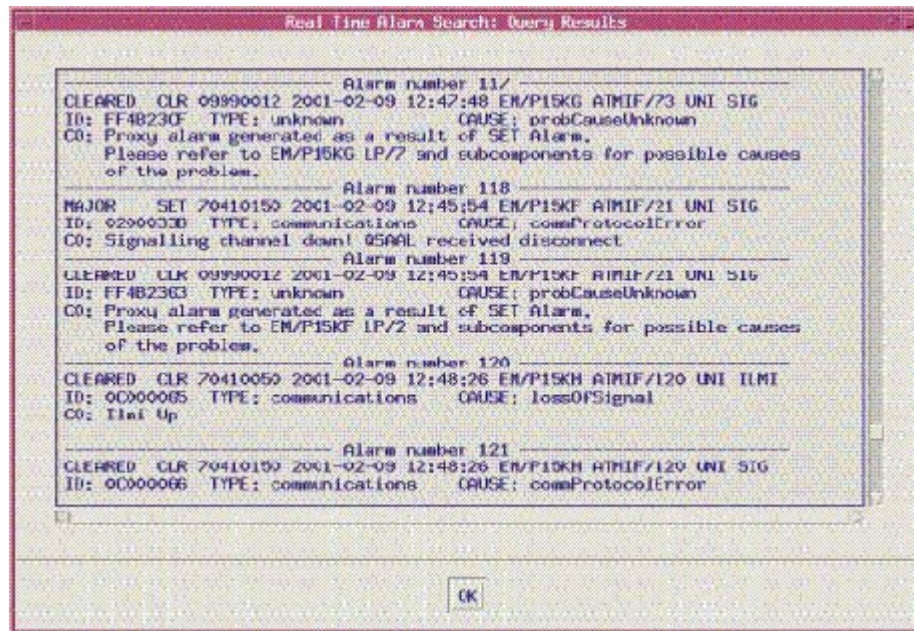
The MDM command-line tool allows a query of old alarms, and supports various search criteria including start and end time, fault code, component name and criticality.

Short-term Historical Alarm Reporting provides the ability to query old alarms and supports the following various search criteria:

- start time
- end time
- fault code
- component name
- criticality

Short-term Historical Alarm Reporting is a command-line tool. Search results are viewed from a window or saved to a file. [Figure 33](#) shows the Historical Alarm reporting tool.

Figure 33
Query results from Short-term Historical Alarm Reporting

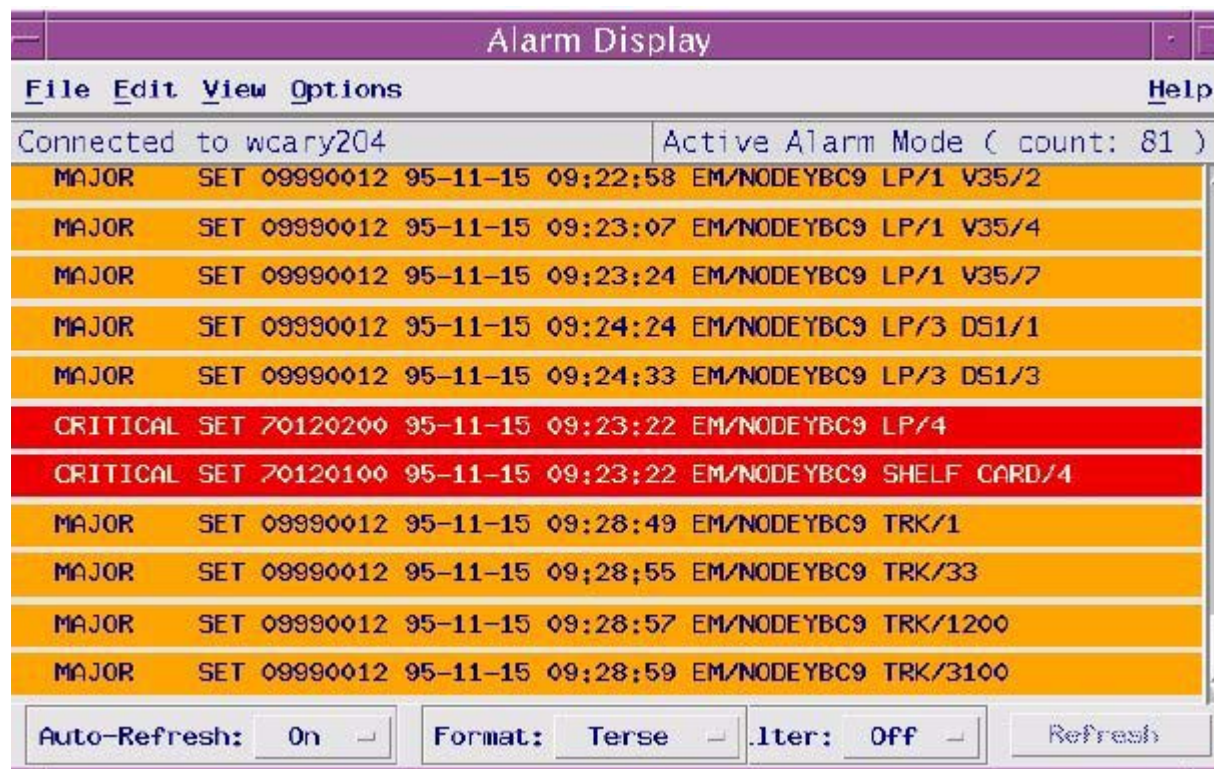


Alarm Display

The MDM tool, Alarm Display, provides a common format for viewing logs for Multiservice Switch 15000/Media Gateway 15000 and Multiservice Switch 7400/Media Gateway 7400 ([Figure 34](#)). Alarm Display supports both Alarm Log and Active Alarm display modes, and provides both accept and reject filters to allow viewing of a specific subset of alarms. This tool also provides access to diagnostic information for a selected alarm by using Alarm Help. In addition, Alarm Display has an Alarm Acknowledgment utility that allows the user to indicate that an alarm is being investigated. The indication shows the user who is responsible for the acknowledgement (or

non-acknowledgement) and the reason for the acknowledgement (or non-acknowledgement).

Figure 34
MDM Alarm Display



Alarm Help

This MDM tool provides a view of diagnostic information for a selected alarm. The description provides details on what the alarm means and also the action that is necessary to fix the problem. This tool can be started by selecting an alarm from the Alarm Display and choosing the Alarm Help submenu item. Alarm Help uses the Netscape Web browser to display the requested alarm text.

Recording alarm information from a Multiservice Switch/Media Gateway SCC2 log

[Figure 35](#) shows an example of an SCC2 log. Field 1 in the header, identifies the log name and number (P15K025). In the example, the log name P15K corresponds to a Multiservice Switch 15000/Media Gateway 15000 network element.

The Multiservice Switch 15000/Media Gateway 15000 is identified in field 2 as EM/P15E LP/5 Sonet/2. The NETTypeID (network type ID) is

identified as 138 in field 3. The specificProblems (specific problems) eight-digit code is identified in field 4 as 70115202.

Figure 35
Example of a Multiservice Switch/Media Gateway SCC2 alarm log

```
*C35 P15K025 4790 TBL arfProbableCause.42 Lp/5 Sonet/2
1 managedObjectInstance: 1030:MDMFmRmMoa, 1028:EM/P15KE, 11004:Lp/5 Sonet/2
notificationID: 67109941
2 perceivedSeverity: Critical
logRecordID:
CLFI:
eventTime:20010306153519Z
eventType: 5002
equipmentType:
managedObjectClass: 11004
NE TypeID: 138
3 specificProblems: 70115202
4 probableCause: arfProbableCause.42
correlatedNotifications:
trendIndication:
thresholdInfo:
activeStatus: TRUE
unknownStatus: FALSE
alarmDisplayInfo: SubcomponentID=lp/5 SONET/2,NEUserLabel=EM/P15KE,NENum
ber=138
vendorSpecificInfo: alarmSupportManualClear=TRUE
technologySpecificInfo:
additionalText: Probable Cause: remoteNodeTransmissionError - A Line Ala
rm Indication Signal has been received (rxAisAlarm).
```

Determining a Multiservice Switch/Media Gateway log

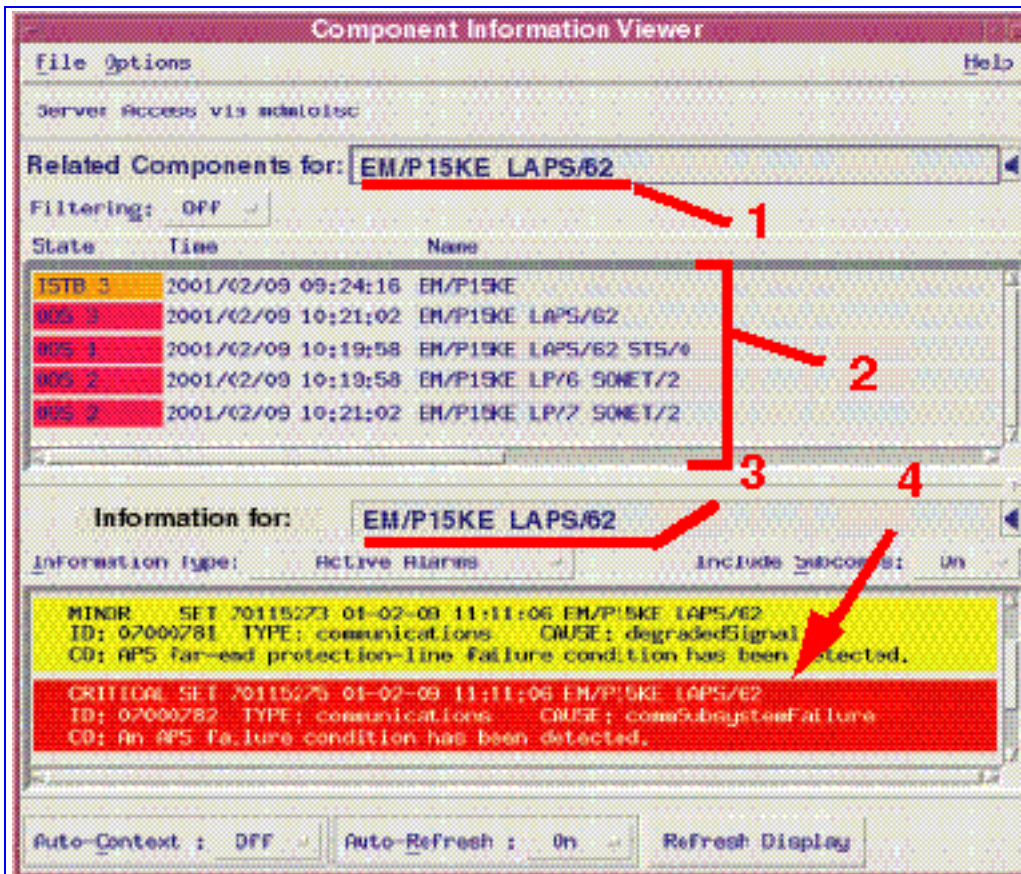
[Figure 36](#) shows an example of an SCC2 log. In [Figure 36](#), the log name and number appears as P15K162 (see field 1). The log name P15K corresponds to a Multiservice Switch/Media Gateway network element. There are two possible Multiservice Switch/Media Gateway network element types shown in the following table.

Multiservice Switch log name	Type of Multiservice Switch/Media Gateway network element	Network element Type ID
P15K	Multiservice Switch 15000 or Media Gateway 15000	138
MDM	MDM	86

Alarm Help displays detailed information on specific alarms and also provides suggestions for remedial action.

For detailed information on logging into the MDM and launching the Component Information Viewer, and acknowledging, clearing and displaying Multiservice Switch alarms, see *Multiservice Data Manager Advisor User Guide*, 241-6001-011.

Figure 37
Example view of the Component Information Viewer

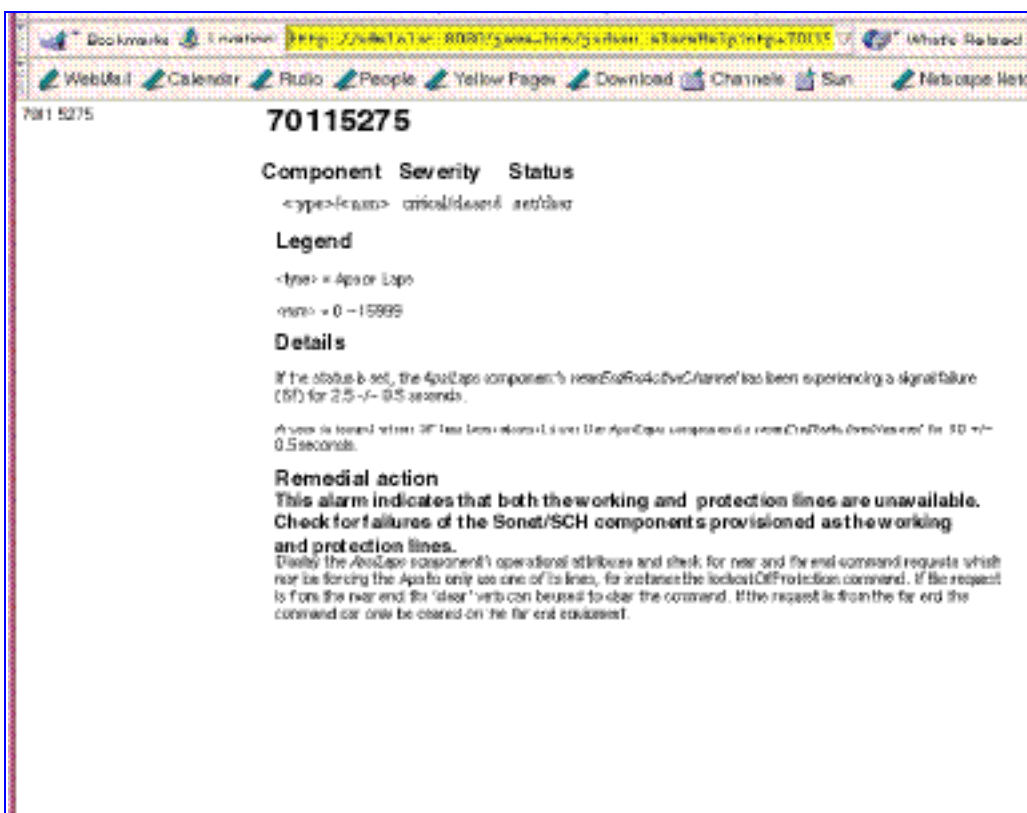


Obtaining remedial action for a Multiservice Switch alarm

Use the Alarm Help utility to obtain specific information for Multiservice Switch alarms (see [Figure 38](#)). The Alarm Help utility uses the eight-digit alarm code that appears on the SCC2 alarm log in the specificProblems field.

Note: The alarm described in the example Alarm Help screen in [Figure 38](#) does not relate to the SCC2 alarm log shown earlier.

Figure 38
Example alarm information from the Alarm Help utility



Fault management suggestions for the Multiservice Switch 15000

The Multiservice Switch 15000 switch is routinely monitored to determine if problems exist and if traffic is properly handled. Regularly monitoring the system helps identify and prevent potential problems. You use the MDM Advisor Performance Viewer tool to generate statistics for ATM services on the following ATM equipment: ATM function processors, ATM interfaces, ATM connections. For more information on these Multiservice Switch 15000 tests, see Multiservice Switch Fault Information, and MDM fault Information.

Monitoring ATM function processors on the Multiservice Switch 15000

Begin monitoring your Multiservice Switch ATM system by examining the ATM function processors. If the function processors are not operating properly, none of the other elements of the system can effectively process ATM traffic.

Monitoring ATM interfaces on the Multiservice Switch 15000

After the function processors have been examined, the ATM interfaces on each function processor are the next system component that you

need to examine. Each interface supports a variety of traffic types and connections, and provides a summary of all connections on that link.

Monitoring ATM connections on the Multiservice Switch 15000

Once you have determined how the function processors and ATM interfaces are operating, start examining the individual connections that are supported on each ATM interface. When monitoring each connection, review how the configured routing and signaling are operating.

Hardware LED status indicators on Multiservice Switch 15000

The status of hardware equipment on Multiservice Switch 15000 is indicated by a system of colored and shaped LEDs. A lit LED indicates one status in one color. On the same type of component or assembly, the LED is always in the same position relative to its mates. While the equipment is powered, there is always one LED that is lit.

Isolating faults on the Multiservice Switch 15000

Fault management for Multiservice Switch 15000 involves the following tasks:

- Control processor test
- Control processor disk diagnostics
- Function processor test
- Function processor lock and unlock
- Port lock and unlock
- Function processor loopback port test
- Remote loopback port test
- Manual loopback port test

Note 1: You must perform Multiservice Switch 15000 fault management tasks using MDM tools. You cannot perform Multiservice Switch 15000 fault management tasks through the OSS interface.

Note 2: For more information on these Multiservice Switch 15000 tests, see *Multiservice Switch 15000 and MDM in CVoIP Networks Product and Technology Fundamentals PT-AAL1*, NN10028-111.

Multiservice Switch 15000 Control processor test You perform this test following a control processor fault or failure. You use the MDM Advisor Command Console to perform the test. The most common problems with a control processor are software load failures and

crashes. These problems can affect both the active and the standby control processor. Problems include the following errors:

- the control processor does not load
- the control processor crashes
- the control processor switchover
- standby control processor does not load

Multiservice Switch 15000 Control processor disk diagnostics

You perform these diagnostics following control processor disk fault or failure, and you use the MDM Advisor Command Console. Disk tests verify the integrity of the disk. Test a disk only when you suspect a fault in the disk hardware. You cannot test the disk on the active control processor. If the disk you want to test is currently active, switch control between the active and the standby control processors.

Multiservice Switch 15000 function processor test You perform this test following a function processor fault or failure, using the MDM Advisor Command Console. You must test the 16-port OC-3 ATM IP function processor.

Multiservice Switch 15000 function processor lock and unlock

You perform this test prior to replacing a function processor, and you use the MDM Advisor Command Console to perform the test.

Multiservice Switch 15000 loopback port lock unlock You perform port lock prior to running diagnostics or deleting a port, and you perform port unlock after completing diagnostics. Use the MDM Advisor Command Console to perform these operations. You can lock and unlock the following ports: SONET, Ethernet, Ethernet OAM&P, BITS timing.

Multiservice Switch 15000 function processor loopback port test You perform this test following a port fault or failure using the MDM Advisor Command Console. The function processor loopback test verifies the internal working of the function processor and the line interface. This test transmits a test pattern through the internal circuits and processors. Data is transmitted back from the link interface of the port.

Multiservice Switch 15000 remote loopback port test You perform this test following a port fault or failure using the MDM Advisor Command Console. Ports that can be tested are OAM&P Ethernet and SONET ports. You can use remote tests to verify the full length of the transmission facility.

Manual loopback port test You perform this test following a port fault or failure using the MDM Advisor Command Console. Most port tests set up their own loopbacks. The manual test requires you to arrange for a loopback to be inserted at some point along the connection. A loopback loops the received data back to the function processor under test. Loopbacks do not produce test results for the local node because they loop received information back to the switch under test.

Additional information

For additional details on fault management tools and utilities for MDM, refer to the following component documentation:

- *MDM Fault Management User Guide*, 241-6001-011
- *MDM Fault Management Summary Card*, 241-6001-909

Device Manager for Ethernet Routing Switch 8600

The Device Manager uses Simple Network Management Protocol (SNMP) to provide alarm monitoring for the Ethernet Routing Switch 8600 through a Graphical User Interface (GUI). Configurations on the Ethernet Routing Switch 8600 can also be viewed through a Web interface.

Remote monitoring is available through Device Manager and provides four main functions to monitor devices on a port by port basis:

- setting alarms for user-defined events
- gathering real-time and historical Ethernet statistics
- logging events
- sending traps for events

The user can configure switching or routing configurations and enable other features such as RMON alarms and port mirroring to analyze traffic on a per-port basis. The RMON MIB is an interface between the RMON agent on the Ethernet Routing Switch 8600 Series switch and the Device Manager. It defines objects that are suitable for the management of any type of network, but some groups are targeted for Ethernet networks in particular. Remote monitoring (RMON) is a management information base (MIB) or a group of "management objects" that you use to "get" or "set" values. Using Device Manager, you enable RMON globally for devices on the switch. When RMON is enabled globally, you then enable monitoring for individual devices on a port-by-port basis.

Within Device Manager, you can set RMON alarms that relate to specific events or variables simply by selecting these variables from a

drop-down menu. You specify events associated with alarms to be set to either trap or log-and-trap. In turn, these alarms, when tripped, are trapped or logged.

The user can view the alarms and the status of hardware components through the Network Patch Manager which also supports the following Troubleshooting tools and utilities:

- Testing the switch fabric and address resolution table
 - You can test the switch fabric and check the address resolution (AR) table for consistency. The Fabric test causes the CPU to generate traffic and send it through the switch fabric. Given the forwarding rate of Passport 8000 Series switches, the CPU does not generate much traffic, but it performs a simple test of the switch fabric memory. The AR table test performs a consistency check on address resolution table entries.
- Monitoring how often a port goes down
 - You can monitor the number of times a link is going up or down rapidly (that is, flapping) on a port. This action can be detrimental to network stability because it could trigger spanning tree and routing table recalculation. If the number exceeds a given boundary during a specified interval, the port is forced out of service.
- Configuring and monitoring port mirroring
 - You can use port mirroring to specify a destination port on which you want to see mirrored traffic and specify the source ports from which traffic is mirrored. Any packets entering or leaving the specified ports are forwarded normally and a copy of the packets is sent out the mirror port. You can also use the port mirroring feature to monitor traffic from MAC addresses where traffic with a given MAC source address (SA) or MAC destination address (DA) is copied to the mirror port. This feature is enabled by setting the Monitor field to true for a MAC address in the Forwarding dialog box.
- Trapping errors
 - All errors detected are then sent to a log that you can view in Device Manager.
- Viewing address resolution statistics
 - The AR Stats tab shows statistics for the internal state of the address translation table. These statistics are debugging aids;

use them only when consulting with Nortel Networks support personnel.

- Enabling the system log
 - You can enable the system log feature globally to send messages to up to 10 syslog hosts. By default, five hosts are supported.
- Receiving system log messages
 - You can use the system log-messaging feature of the Passport to manage switch event messages on any UNIX-based management platform. The Passport syslog software supports this functionality by communicating with a counterpart software component named syslog on your management workstation. The UNIX daemon syslog is a software component that receives and locally logs, displays, prints, and/or forwards messages that originate from sources internal and external to the workstation.
- Changing the severity level mapping
- Checking the MIB status
- Checking the details of the MIB status

For more information on Device Manager fault reporting, refer to the Ethernet Routing Switch 8600 component documentation.

Call Agent Manager

ATTENTION

The Call Agent Manager does not apply to the PT-AAL1 and UA-AAL1 solutions.

Call Agent alarms

Platform faults such as simplex operation, Central Processing Unit (CPU) and memory threshold crossing, connectivity, and call processing application synchronization are reported to the Call Agent Manager.

For information on Call Agent Manager MAPCI, refer to Figure [39](#).

Figure 39 Call Agent Manager MAPCI

	IOD	CCS	Lms	Trks	APPL
CAPACITY	.	.	.	.	.
0 Quit	CATMP/HR	CCOVRD	IDLE		
2 Parns	103320	OFF	YES		
3 SchedMap					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
USERNAME					
Time 10:29	>				

Call Agent logs

Call Agent logs are available from the platform, the call processing application, and the Operations Support System (OSS) network.

STORage Management Manager (STORM Manager)**ATTENTION**

The STORM Manager does not apply to the PT-AAL1 and UA-AAL1 solutions.

STORM Manager performs the following fault management functions:

- views current alarms
- sorts current alarms
- filters current alarms
- displays current log reports

For information on STORM Manager Alarm Screen, refer to the Communication Server 2000 Storage Manager GUI in Figure [40](#).

Figure 40 STORM Manager Alarm Screen

Type	ID	Timestamp	Severity	Description
Quality of service	Threshold Crossed	Monday April 14th 2003 01:01:24 PM	Major	Status: Alarm raised. Five minute load average is 14.00. Five minute load threshold value is 14.00.

For information on STORM Manager Log Screen, refer to the STORM Manager GUI in Figure 41.

Figure 41 STORM Manager Log Screen

Mar 17 10:28:00 beta alarmd: STM301 MINOR INIT Array: '/dev/md1' (stormvg) Status: The array is currently being rebuilt.

Mar 17 10:38:56 beta alarmd: STM301 NONE INIT Array: '/dev/md1' (stormvg) The array has been rebuilt.

Nuera Configurator

For information on Nuera Configurator, refer to the ORCA BTX-Series Software Manual or the BTX System Overview.

NueraView

For information on NueraView, refer to the ORCA BTX-Series Software Manual or the BTX System Overview.

HP OpenView

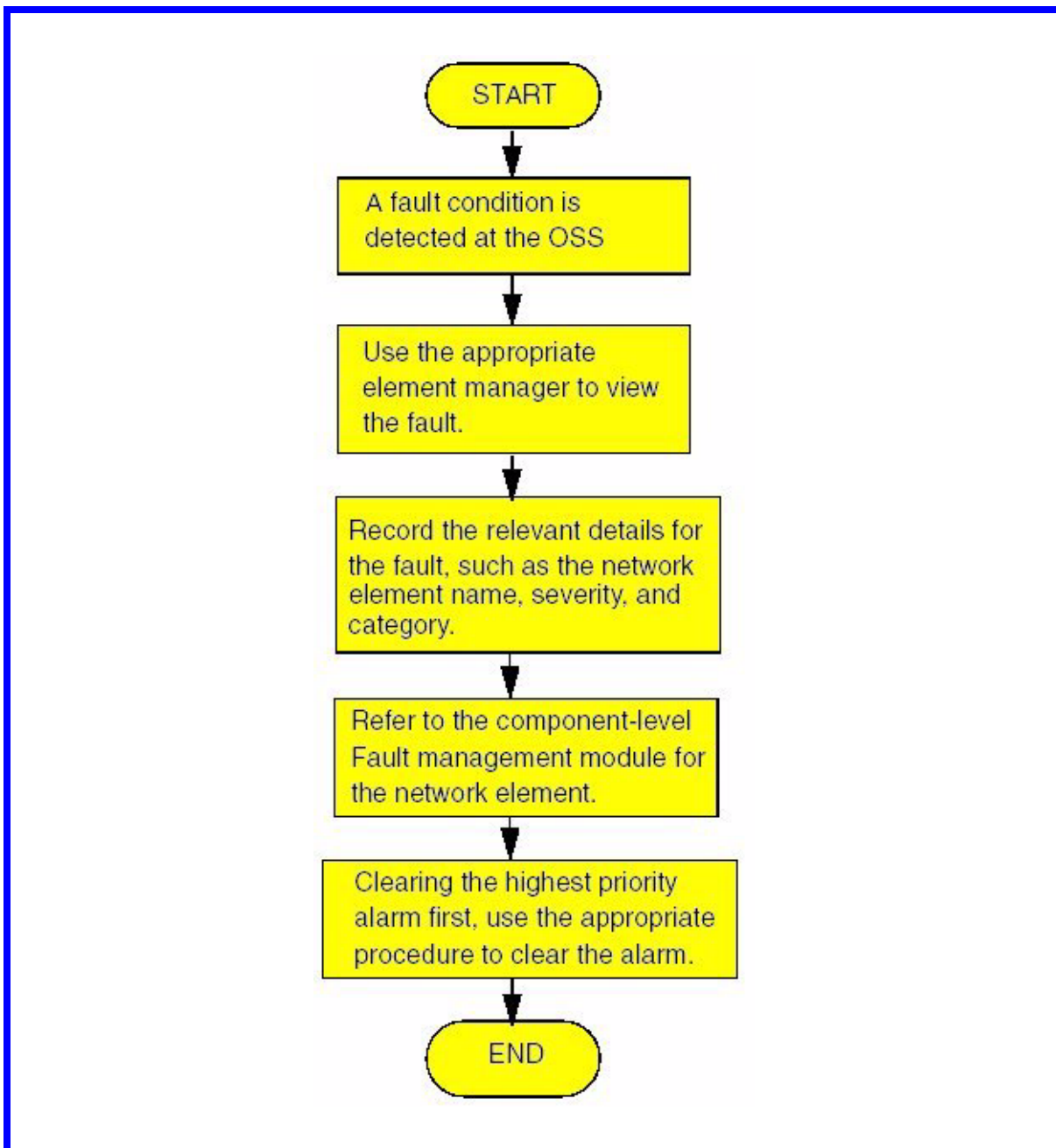
For information on HP OpenView, refer to the ORCA BTX-Series Software Manual or the BTX System Overview.

Fault management task flow

This section outlines the sequence of steps to follow in order to clear an alarm detected at the OSS (operations support system). [Figure 42](#) displays this sequence of actions in the form of a flow chart.

For detailed information on task flows, refer to the component documentation.

Figure 42
Fault Management task flow





Carrier VoIP lines testing

Introduction

This document describes the Carrier VoIP lines testing solution. This information applies to the Carrier VoIP UA-AAL1 and UA-IP MG 9000 for North America.

Overview of line testing

This document is divided into the following sections that describe the two methods of supporting Carrier VoIP lines testing applications:

- MG 9000 lines testing - This section describes the MG 9000 line test subsystem.
- CS 2000-based lines testing - This section describes CS 2000-based tests that use the Maintenance and Administration Position (MAP) commands.

Both sections show capabilities, provisioning rules, and user information.

MG 9000 lines testing

MG 9000 lines testing tests lines that connect to line cards in the MG 9000 and require the following:

- metallic access for loop and line test
- line circuit diagnostics

Line test systems generally use metallic access to test and troubleshoot problems with the twisted pair loop from the MG 9000 line card to the customer premise.

The MG 9000 provides metallic access for external or adjunct loop and line test systems, and for available cutover service (automatic board to board testing [ABBT]). These can be connected to MG 9000s by either direct network interface or no-test trunk (NTT).

CS 2000-based lines testing

CS 2000 MAP-based lines testing tests lines using traditional MAP terminal commands available from the LNS MAP level. This configuration requires a maintenance trunk module (MTM) or remote maintenance module (RMM) be available.



MG 9000 lines testing

Types of testing supported

This section describes the supported means of MG 9000 lines testing which include

- metallic access
- circuit diagnostics

Metallic access

There are two metallic access configurations of line and loop test systems for MG 9000 lines:

- metallic access through a network interface
- metallic access through NTT

Metallic access through a network interface

Carrier VoIP provides an IP interface for requesting metallic access, and metallic test access pair terminations (MTAPT) for test head connections.

This interface allows call center operators to use the operating company's line test operations support system (OSS) to perform metallic tests on the loop in real time. This interface also allows basic line equipment tests and other features as driven by the operating company's line test OSS. The metallic access features include

- loop tests (split-out connections)
- monitor and talk functions (bridged connections)
- line tests (split-in connections)
- wide band test access for loop prequalification (a temporary restriction does not permit wide band access to ADSL cards)
- forced connections (override to allow connections to lines that appear to be call-processing busy [CPB]).

Note: For MTAPT provisioning information, refer to *MG 9000 Fault Management*, NN10074-911.

Metallic access through NTT

No Test Trunk (NTT) support is provided for test systems that do not currently use Nortel's MG 9000 MTA network interface for loop testing.

NTT is an analog test trunk used to interface test measurement units with telephony switches. This interface is typically used for signaling and for the metallic tip/ring path back to the measurement unit. Analog test trunks are supported at remote sites through remote maintenance modules (RMM).

Features supported by NTT depend on the test vendor.

Note: Wide band test is not supported through NTT.

Line circuit diagnostics

Line circuit diagnostics, also known as service verification tests, ensure the MG 9000 and its line circuits can provide service. The MG 9000 supports two types of line circuit diagnostics, self-diagnostics and service verification. This document addresses service verification. Line circuit diagnostics are addressed in *MG 9000 Fault Management*, NN10074-911

Service verification is an in-system test. It uses a test response circuit in the MTA-TRC card to simulate a telephone set. The tests that are run on POTS and Coin circuits are off-hook and on-hook signaling, ringing, and ring trip. For Coin lines, it also tests the circuit's ability to affect coin return, coin collect, and reverse battery voltages. Service verification also provides off-hook tests for ground start lines.

The user interface for service verification is at the MG 9000 Manager. The MG 9000 Manager can also be configured to run bulk line circuit self-diagnostics and service verification tests.

TL1 line test interface for MG 9000 lines

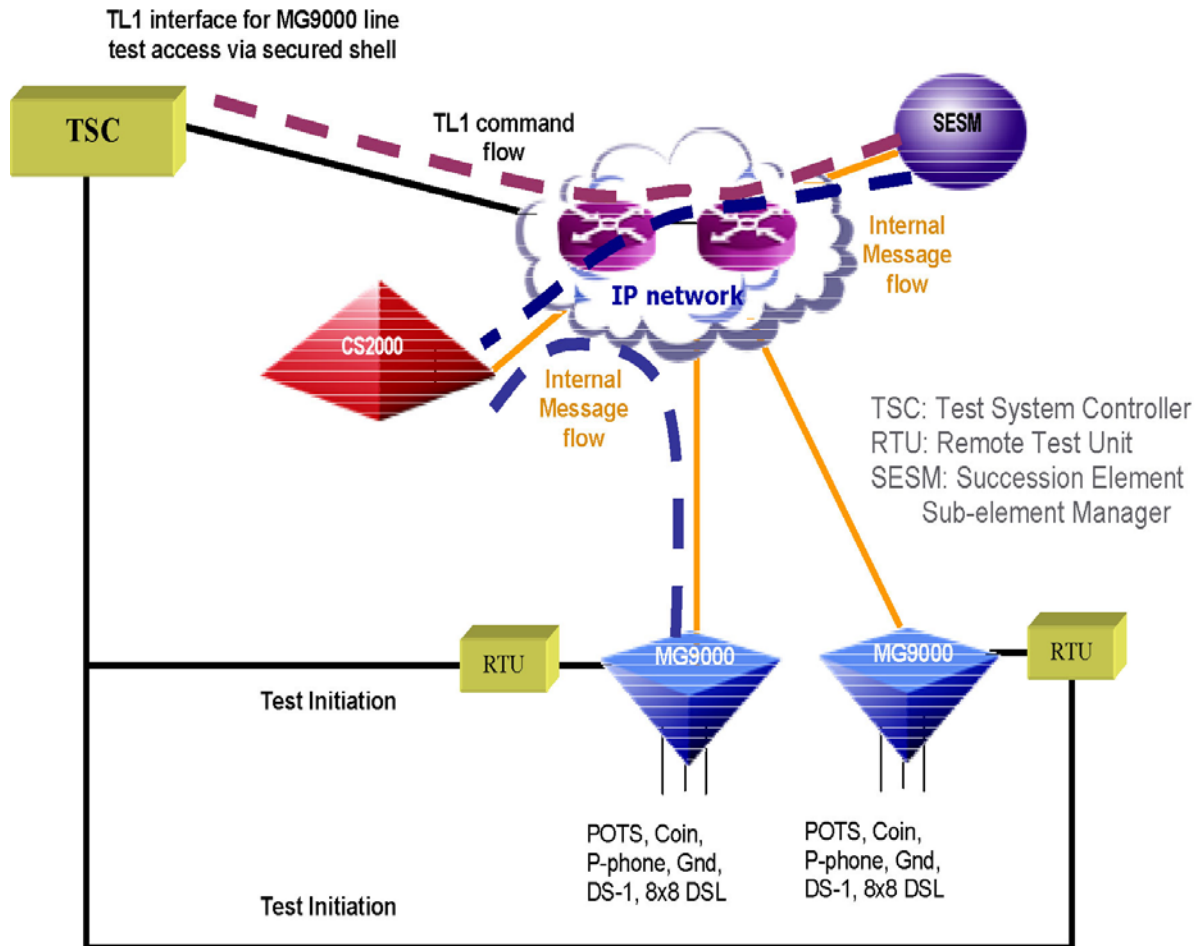
The TL1 line test interface allows for subscriber line test access of MG 9000 lines. This interface is an alternative to the no-test trunk interface.

The traditional no-test trunk interface supports the narrowband line test requirement. As access network technology evolves from POTS services to POTS and xDSL services, wide band test and internet service diagnostics capabilities are available in external line test equipment. Carrier VoIP network customers can take advantage of new

test functionalities without purchasing new hardware, by using the TL1 interface.

The following figure shows the architecture of the TL1 interface.

TL1 line test interface



The following describe the information in the previous figure:

The communication link between the third party test controller and SESM (Succession Element Sub-element Manager) is over secured shell (SSH). The subscriber line test access control uses the TL1 interface language. A test head tip-ring pair must be wired to one of the eight test access ports on a MG 9000. The test controller is required to communicate with the test head for test measurement independently from its TL1 interface.

A typical test sequence is described next. The test controller communicates with

- the SESM to request for the access of a subscriber line for testing
- the test head to perform measurements
- the SESM to request for tearing down the test access

The TL1 line test interface supports the following functions:

- line test access setup with voice busy detection
- line test access tear down
- set test direction to OUT (towards the facility with line circuit being cutoff)
- set test direction to IN (towards the equipment with loop to the customer premises being cut off)
- set test direction to BRIDGED (monitoring mode)

To facilitate the test controller's need for customer line information, an additional query of line circuit information is available. The query outputs the following information:

- MG 9000 node number (0 through 999, unique per call server)
- gateway name
- line status (for example, IDL, CPB etc.)
- line equipment number (for example, CARY 000 1 01 09)
- line type (for example, POTS, ISDN, P-phone)
- line frame type (for MG9000 return UE9000MG)
- line class code
- card code (for example, GWLPOT, RDTLSG, 6X21AC)
- end point name on the gateway
- options (line options on Call Server)

To use the TL1 Interface, the following limitations apply:

- A third party line test controller vendor must provide the transparent line test of MG 9000 lines for its customers. It is not intended for manual test access.
- A license from Nortel Networks must be obtained by the third party line test controller vendor to implement the TL1 interface. Contact your Nortel Networks sales representative regarding a TL1 interface license.

System description

This sections provides system descriptions for:

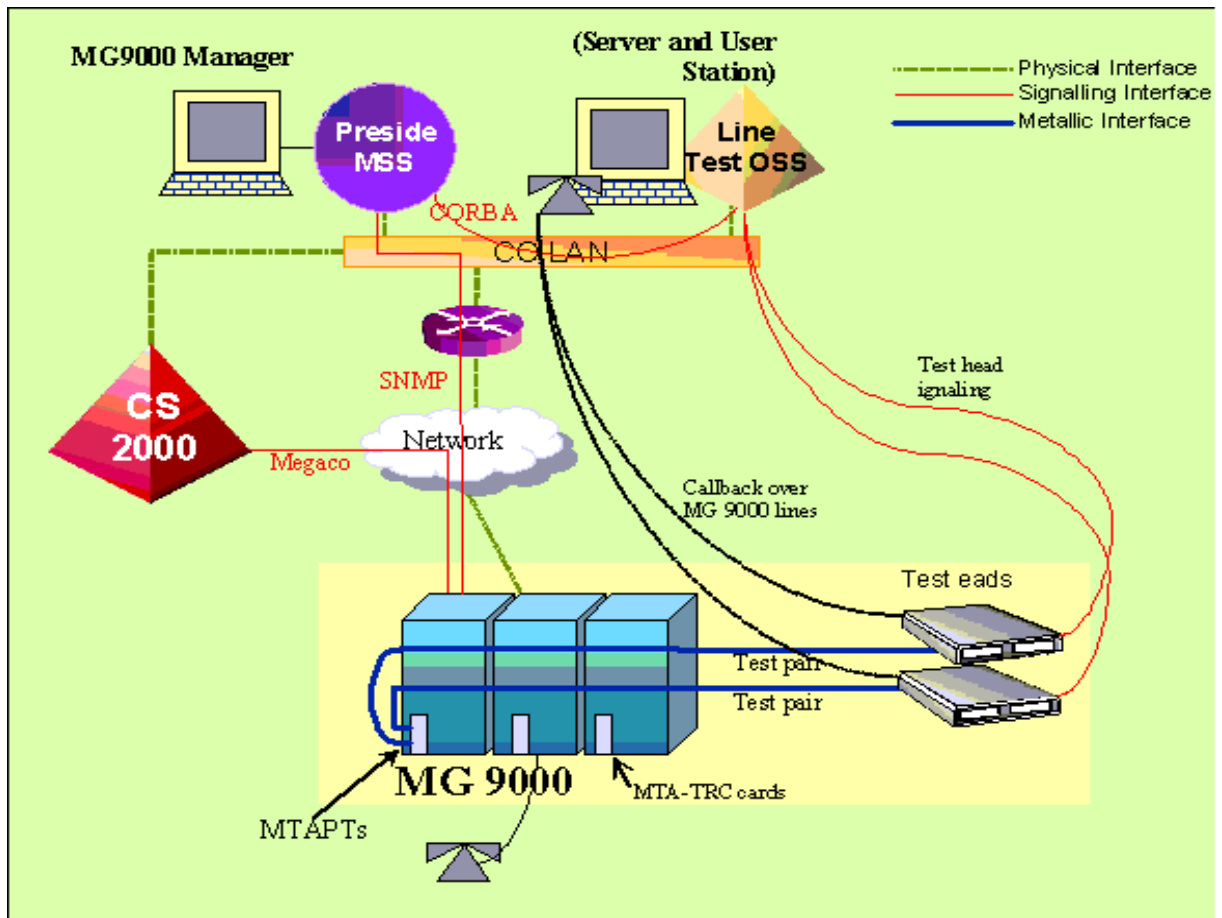
- Metallic access through a network interface
- Metallic access through NTT

Metallic access through a network interface

A line test OSS is typically comprised of servers and test heads. For metallic access through a network interface, the OSS server has IP access to the CS 2000 Management Tools, which it uses to request metallic connections. It typically uses IP, serial, or dialup access to its test heads to drive loop test functions. The test heads are connected via metallic test pair to MG 9000 MTAPTs. Wide band metallic access is supported.

To perform a loop test, the OSS requests the Line Test Manager on CS 2000 Management Tools for a metallic connection between a loop and a test head, then uses the test head to take measurements. This is explained in detail in the following sections.

System view, MG 9000 MTA through a network interface



Interfaces for metallic access through a network interface

This section describes the interfaces for metallic access through a network interface.

Line test OSS and CS 2000 Management Tools This is a proprietary CORBA interface with the Line Test Manager in CS 2000 Management Tools. This interface supports signal requests for metallic connections. The OSS passes the Line Test Manager, a directory number and MTAPT number, and other physical and administrative parameters. The OSS can poll to see when the request has been completed, and the Line Test Manager can send unsolicited connection status messages.

MG 9000 Manager and MG 9000 The MG 9000 Manager converts all supported CORBA transactions into SNMP transactions with the MG 9000. In addition, it generates its own SNMP transactions for MTAPT provisioning driven by the MTAPT provisioning screen, and for

service verification as driven by the Line Circuit Diagnostic window and Bulk Line Test.

- MTAPT provisioning - MTAPT provisioning data is written to the MG 9000 on startup if needed, and when there are modifications to the line test configuration.
- Metallic connection requests - The MIB entry for this request contains the desired and actual direction (such as, test in, test out, and monitor), desired and actual bandwidth (voice band or wide band), and how the request will be treated when the line is busy. Then the MG 9000 sets up the corresponding metallic test path. The Call Server is notified through Megaco and the GWC that the line is busy for test.

The MG 9000 issues an SNMP trap when it has completed processing metallic connection requests. The trap and MIB entry provide the request's result and connection status information.

- Service verification testing - The MG 9000 Manager is used to request service verification (circuit diagnostic) tests on individual analog line circuits. The MG 9000 uses the industry standard test MIB for service verification testing. The user can specify the test type (test all, off hook, on hook, ring, coin collect, coin return, and reverse battery). The MG 9000 saves the results in the test MIB when it has completed the diagnostic.

Metallic: MG 9000 and test head Test heads are connected through tip/ring pairs to MG 9000 MTAPTs. Each of the eight MTAPTs is the left side of an MTA-TRC card horizontal, which is part of an inter-frame test bus in multi-frame MG 9000's

Line test OSS to test head The OSS must interface with its test heads out-of-band. It can use a CO LAN to a terminal server collocated with the test head, or it can use the test head's internal dialup modem through a dedicated MG 9000 POTS line.

Line test OSS test position to test head This is a voice interface for Monitor and Talk functions. The test head can use a dedicated line on the MG 9000 for call back. After the OSS signals the MG 9000 to set up a metallic path to the line, the OSS instructs the test head to monitor that line. The test head calls back, that is, it uses the dedicated call back line to dial the directory number of the phone at the operator test position, and patches the target line to the dedicated line. From here, the operator can talk or listen as required. Therefore, Mon/Talk functions can be supported without an Analog Trunk interface such as NTT.

How metallic access through a network interface test works

The line test operator posts a line and requests a test. The line test OSS determines which test head to use, and sends a request for a metallic connection over CORBA to the Line Test Manager process in CS 2000 Management Tools. The line may be specified by a 10-digit directory number, or the full MG 9000 termination name.

If the directory number is passed, the Line Test Manager uses the Line Maintenance Manager to look up the physical location of the circuit serving the line under test. The LMM issues a Call Server query and local queries to return the MG 9000 network element number, frame, shelf, slot, and circuit. The Line Test Manager forwards the request with this identifier to the MG 9000 Manager process identified by the network element number.

The MG 9000 Manager reformats the CORBA request to issue an SNMP set request to the MG 9000's MTA enterprise MIB.

The MG 9000 busies the line if there is no call on it. This is reflected via Megaco back to the Call Server. Then the MG 9000 sets up the desired metallic connection. Usually the request is for a split-out connection. If there is a call on the line, the MG 9000 sets up a "bridged" connection to prevent call trampling. The MG 9000 updates the connection status, and indicates that the metallic connection has been made.

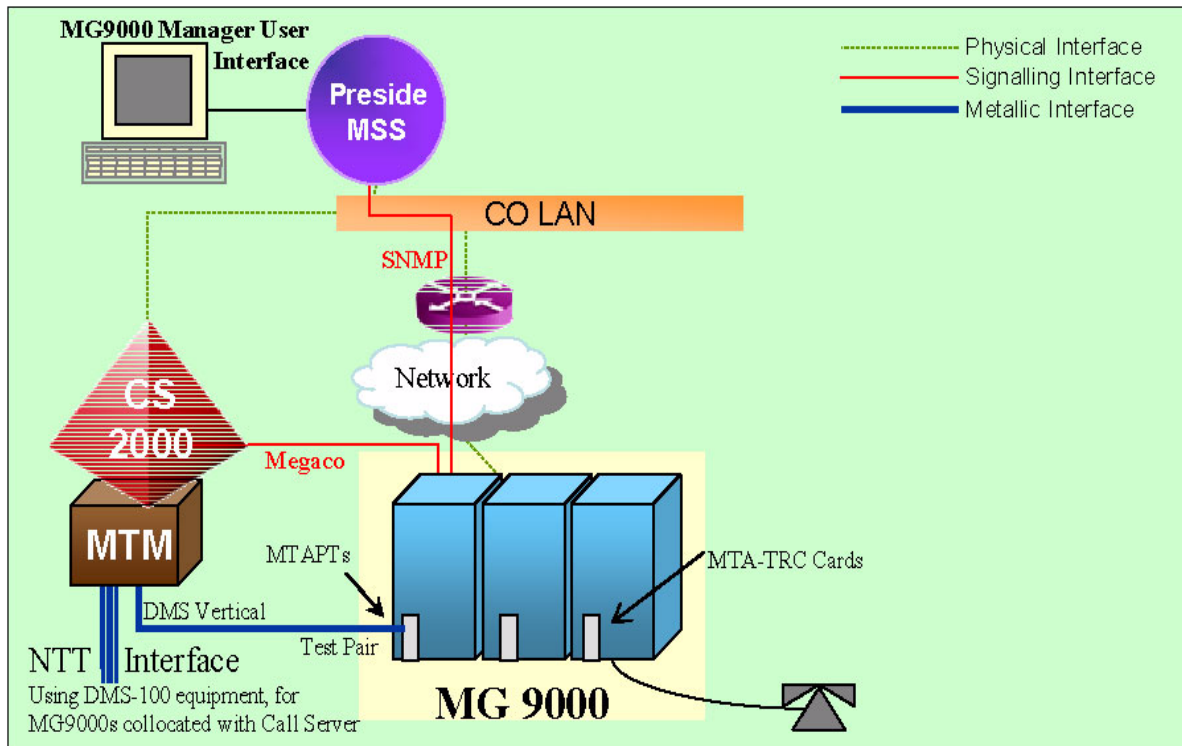
When the OSS determines that the connection has been made, it instructs the test head to make the required measurements.

When the line test operator is done with the test session, the line test OSS instructs the MG 9000, by way of CS 2000 Management Tools and the MG 9000 Manager, to take the metallic connection down.

Metallic access through NTT

Line test systems that do not currently use the MG 9000 network interface for line testing, such as Tollgrade's Loop Care (formerly Lucent's LMOS/MLT) and Teradyne's 4TEL can be supported using this interface. This is diagrammed in the [System view, NTT support, MG 9000 collocated with CS 2000](#) figure. The line and loop test features provided by this configuration are dependent on the vendor.

System view, NTT support, MG 9000 collocated with CS 2000



Interfaces for NTT support

The following are supported NTT interfaces in Carrier VoIP:

- **Metallic—NTT Interface** - This is the analog interface between a third party test head and DMS-100 test equipment. It consists of ring, tip, sleeve, and ground connections to a DMS-100 NT2X90 test trunk card. Once a test session is set up, Tip and ring are connected through to a DMS-100 horizontal on an NT3X09 MTA card, which can be connected to a vertical which goes to an MG 9000.
- **Metallic—DMS-100 test equipment and MG 9000** - This is a ring/tip pair between a vertical on an NT3X09 MTA card and an MG 9000 MTAPT. This connection must be provisioned in tables LGRPINV and MTAVERT, and in the MG 9000 Manager's MTAPT provisioning screen.
- **Megaco—Call Server to MG 9000** - This is a signaling interface which uses the proprietary MTA Megaco package. It specifies the target line and MTAPT, and the desired direction (such as, test in, test out, and monitor). In this case, the MG 9000 does not request the line to be busied by the Call Server. It is assumed that since the request came from the Call Server, it has already placed the line in

MTAPT to tell the MG 9000 to use. The setup dialogue requires two messages, which are described as follows:

- The first message from XA Core is intended to reserve MTA resources in the MG 9000. The message includes the line to be tested, the MTAPT number, and requests a “loop around” configuration. Although the MG 9000 does not physically provide a metallic tip/ring loop around, if resources are available it sets up a metallic connection from the MTAPT to the shelf the circuit resides on, and acknowledges that the connection has been made.
- The second message from XA Core requests the desired MTA configuration (usually Split Out). The MG 9000 then isolates the loop from the line circuit, and connects the loop to the MTAPT for test. When this is complete, the MG 9000 signals the XA Core, which in turn signals the test system that the connection is ready.

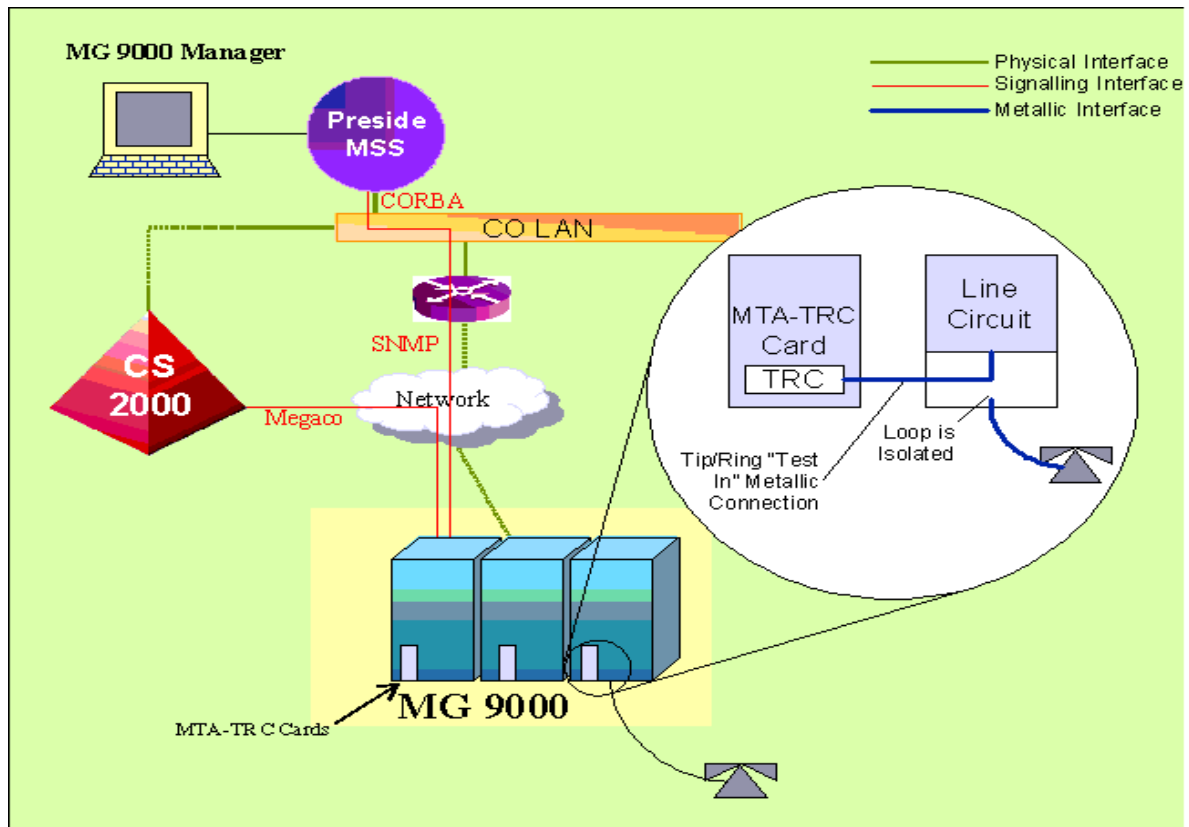
The end result is a tip/ring metallic connection from the test head's NTT trunk to the loop. The connection traverses NTT, through the NT2X90 card to a DMS-100 horizontal, which is connected through an NT3X09 card to a vertical which corresponds to an MG 9000 MTAPT. From here, it is routed through the MG 9000 MTA system to the loop under test.

Service verification test

Service verification tests use test response circuits on the MTA-TRC card to verify that POTS, Coin, and Ground Start line circuits can process calls. The tests are driven from the MG 9000 Manager. The MG 9000 Manager is used to initiate line circuit diagnostics, and to collect the results.

The Test All diagnostic on POTS, Coin and Ground Start circuits tests the circuit's ability to detect and report off-hook, on-hook, and ring trips. It also tests the circuit's ability to ring the line. For Coin lines, the circuit's ability to provide dc phone control is also tested (Coin Collect, Coin Return, and Reverse Battery).

Service verification tests, system view



Each line circuit in the MG 9000 has access to an MTA-TRC card in the same frame. Each MTA-TRC card has two TRCs. When a line circuit diagnostic is requested, the line is busied at the Call Server, the subscriber's loop is isolated, and the line is metallically connected to one of the TRCs. Supervision (on-hook and off-hook) messages are routed to the test software. Each of the basic tests are described next.

- off-hook - The TRC is told to apply an off-hook termination to the line. The TRC checks for normal voltage at the loop, and applies a 900 ohm tip/ring termination. When the circuit diagnostic software sees the off-hook report from the line circuit, the test has passed.
- on-hook - Assumes an off-hook termination is applied, and the line card is scanning for on-hook. The TRC is told to remove the off-hook termination, which opens the tip/ring connection. When the circuit diagnostic software sees the on-hook report from the line circuit, the test has passed.
- ringing and ring trip - The line circuit is told to apply ringing. The TRC looks for ringing. When the TRC sees ringing voltages (20Hz, 86v or 100v RMS), it applies an off-hook (900 ohm tip/ring termination).

The line card ring trips and sends the off-hook message. When the circuit diagnostic software sees the off-hook report (ring trip), the test has passed.

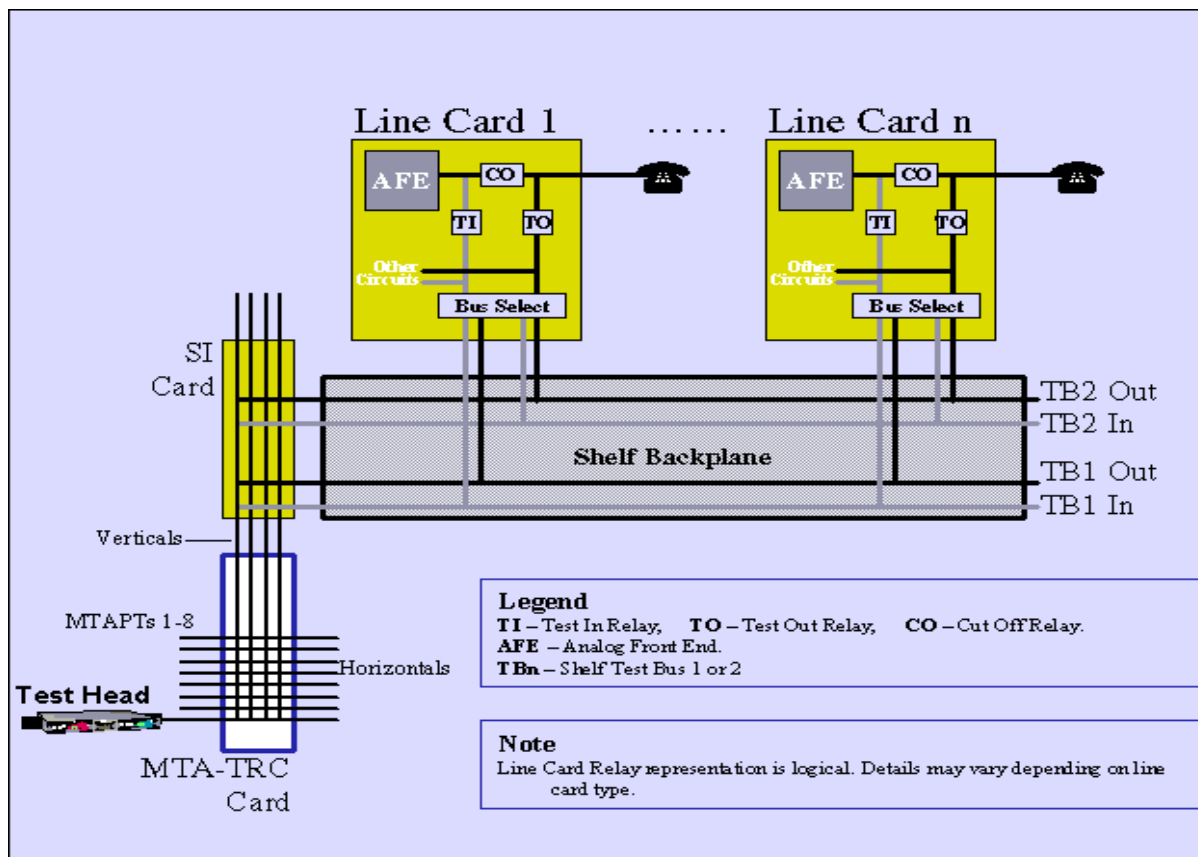
MG 9000 hardware components and configurations

This section refers to MG 9000 hardware which supports line and loop test. It provides an overview of what is involved in providing metallic connections between an MG 9000 line and an MTAPT, and in performing line circuit diagnostics.

Components

The MG 9000 components providing metallic connections are described in this section. Refer to the following figure.

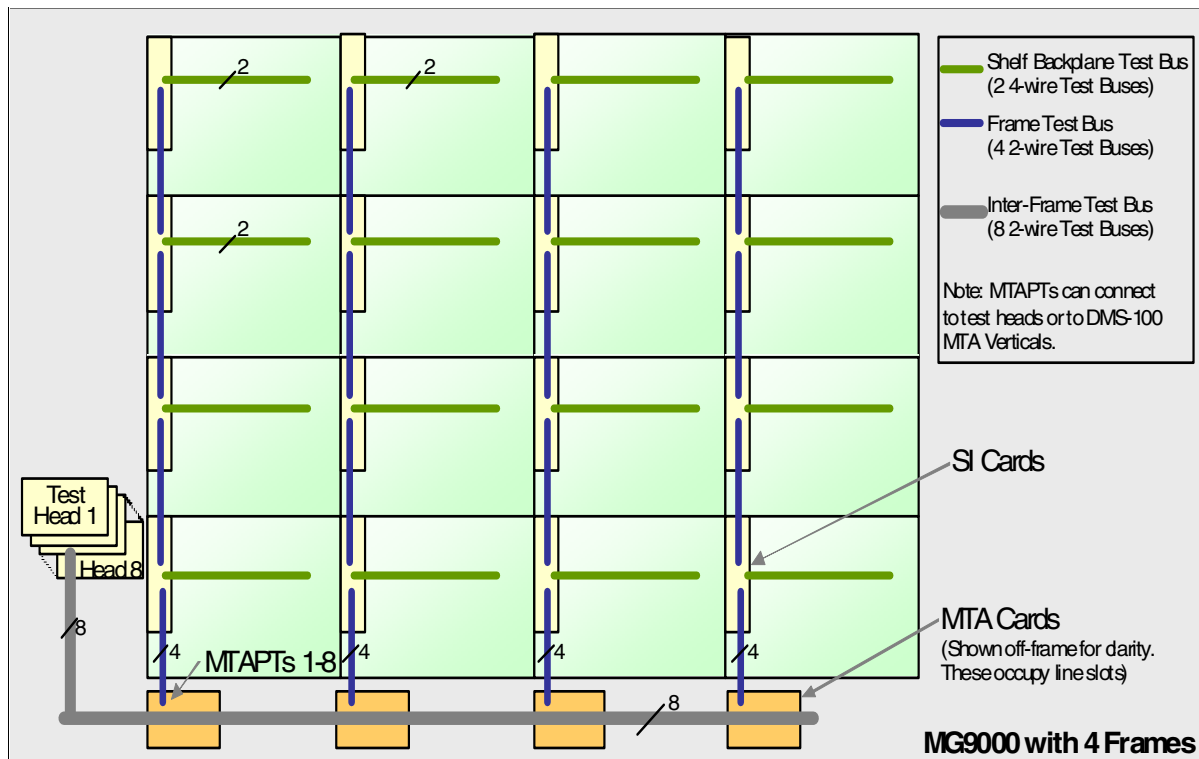
MG 9000 metallic test access components



- MG 9000 nodes with MTA-TRC cards (typical) - Each MTA-TRC card has a metallic relay matrix that can connect eight tip/ring horizontals to four tip/ring verticals. Verticals are connected to the SIC card for shelf access. The eight possible MTAPTs (metallic test access points) for test head connections physically are the left end of each horizontal. For multi-frame MG 9000s, the right side of each

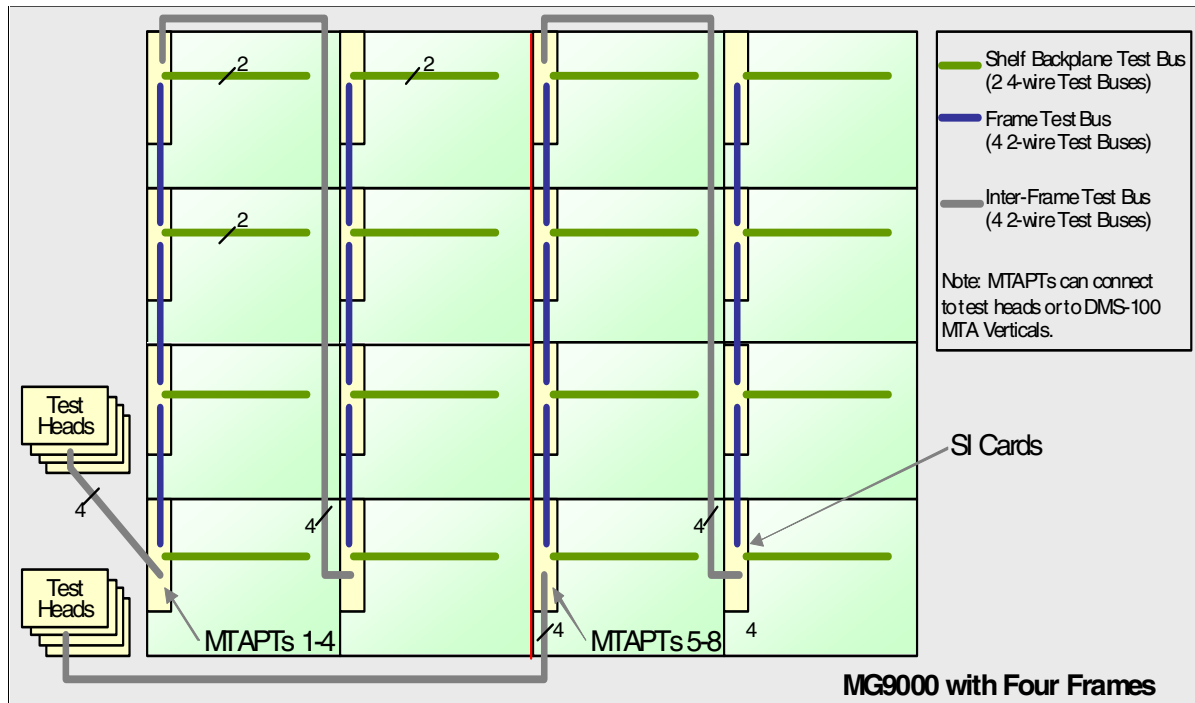
horizontal is extended to the MTA-TRC card on the right-adjacent frame, so any line in the MG 9000 can be accessed from any MTAPT. The MTAPTs are always on the left-most frame. From the SIC card, the four verticals are daisy chained to all of the MG 9000's shelves in that frame. For wide band test signal integrity, the relay matrix on the MTA-TRC card eliminates bridge taps by cutting off the horizontal downstream of active vertical connections. This is illustrated in the following figure.

Metallic access configuration, MTA-TRC cards



- MG 9000 nodes without MTA-TRC cards: Although supported, this configuration is not typical. Four two-wire MTAPTs (tip/ring) are provided for each two frames, on the bottom shelf of the left frame of each pair. The MTAPTs are physically the bottom edges of the four frame verticals. These are daisy-chained from shelf to shelf for each frame pair in the MG 9000. Refer to the following figure.

Metallic access configuration, MTAPTS on SI cards



- On each shelf, the SI Card provides shelf access to the four tip/ring verticals. A 4x4 metallic relay matrix allows any vertical to be connected to the shelf. Each shelf has two 4-wire test buses on the backplane which provide access to any line card in the shelf. Each bus provides separate 2-wire (tip/ring) paths for test-in and test-out. Any of these tip/ring paths can be connected to any frame-level vertical in the SI Card. For wide band test signal integrity, the relay matrix on the SI card eliminates bridge taps by cutting off the vertical past active connections to shelves.
- Each line card has a 4-wire metallic test bus, to provide separate paths for test-in and test-out. The card's bus can be isolated from or connected to either of the backplane's metallic test buses using the backplane test bus select relays. Each line card can support one test at a time. Each subscriber circuit on the line card can connect to the card's bus, and has a relay set that allows metallic test-in (with the loop isolated), test-out (with the line circuit isolated), bridged (line and loop are connected intact via the test-out bus), cut-off (protection) and simultaneous full split (test-in and test-out at the same time).

Configurations

The two supported configurations are discussed next.

MG 9000 with MTA card: With this configuration, there are 8 MTAPTs on the MTA-TRC card in the left-most frame. Each test head is connected directly to a “horizontal” inter-frame test bus. Metallic connectivity is daisy-chained to each frame via its MTA-TRC card, and to each shelf via its SI Card. The test connection is always to the left of the MTA-TRC card, and always down from the SI Card. Refer to the figure [Metallic access configuration, MTA-TRC cards](#). All lines in an 8-frame node can be tested every week in a 5 to 6 hour maintenance window every night with a test head on each of the eight MTAPTS.

MG 9000 with no MTA card This is not a typical configuration and does not support line diagnostics (service verification). This configuration requires frames to be wired together in pairs. Refer to Metallic Access Configuration, MTAPTS on SI cards. Each pair of frames has four MTAPTs, so up to four test heads can be connected. If there are an odd number of frames in the lineup, the last frame gets its own set of four MTAPTs.

Line test setup and configuration

This section is a guide for setting up line test configurations.

Connecting the MG 9000 MTA system

Configurations with MTA cards

The MG 9000 MTA system uses the MTA-TRC card. The MTA card is deployed using the following rules.

- Each MG 9000 will have one MTA-TRC card for every frame it occupies. For example:
 - Each single-shelf MG 9000 has its own MTA-TRC card, so it is possible to install up to 4 MTA-TRC cards in one frame.
 - If there are two MG 9000s in one frame, there will be two MTA-TRC cards in that frame. For example, with two 2-shelf MG 9000s in a frame, each subtended shelf will have one MTA-TRC card.
 - A 5 to 8-shelf MG 9000 in two frames will have two MTA-TRC cards.
 - A 9 to 12 shelf MG 9000 in three frames will have three MTA-TRC cards.
- MTA-TRC Card Location: In single shelf MG 9000s, the MTA-TRC card goes in slot 9. For multi-shelf and multi-frame MG 9000s, the MTA-TRC card goes in subtended shelves. In frame 0 (the frame with the master shelf), it goes in slot 2 of the first subtended shelf (for example, if the master shelf is 0, the MTA-TRC card goes in

shelf 1). In subtended frames, MTA-TRC card is installed in slot 2 of shelf 0.

Configurations with no MTA cards The MG 9000 can have metallic test access to subscriber loops without MTA-TRC cards, but this is not recommended.

Provisioning MTAPTs

MTAPT provisioning is performed at the MG 9000 Manager, using the Services->MTAP Test Manager available from the menu bard at either the Frame View or the Shelf View.

Three questions need to be answered when determining how to provision MTAPTs:

- Are the MTAPTs on MTA-TRC cards or SI cards? Typical installations use MTA-TRC cards.
- Which MTAPTs are going to be connected to test heads?
- How many frames are in the MG 9000?

MTAPTs on MTA-TRC Cards When the MTAPT provisioning window is opened, the status will indicate that the system is MTA Card Ready. If not, verify that the rules in [Connecting the MG 9000 MTA system](#) have been followed, and that all MTA-TRC cards are on line and unlocked.

With the answers to the questions in [Provisioning MTAPTs](#) above, perform the “Setting up the MTAP Test Manager” procedure on MTA cards in *MG 9000 Fault Management*, NN10074-911.

MTAPTs on SI Cards When the MTAPT provisioning window is opened, the status will indicate that the system is SI Card Ready. If not, delete all MTAPTs. Then, lock, offline, and de-provision all MTA-TRC cards in the MG 9000, and pull the MTA-TRC cards out.

With the answers to the questions in [Provisioning MTAPTs](#) above, perform the “Setting up the MTAP Test Manager” procedure on SIC cards in *MG 9000 Fault Management*, NN10074-911.

CS 2000 Management Tools and MG 9000 Manager

This section applies to MTA access through a network interface. When the Line Test Manager on the CS 2000 Management Tools server initializes, it automatically sets up a signaling connection with the MG 9000 Manager for MTA transactions. In addition, the Line Test Manager requires a Line Maintenance Manager process. This also is started automatically as required.

SDM applications

This section applies to an MTA access through a network interface. The Line Test Manager (and Line Maintenance Manager) in the CS 2000 Management Tools, rely on the SDM for interpreting the directory number passed by the line test OSS through the network interface. One of the required SDM applications is the “DMS Maintenance Application”. The earliest acceptable version is 2.0.99.0. If an MG 9000 line test has never been run on the CS 2000, verify that “DMS Maintenance Application” exists, is InSv, and at the correct version. Use the following procedure to determine the DMA version.

Determining the DMS Maintenance Application (DMA) version***At the CS 2000 Management Tools Manager***

- 1 Log into SDM
- 2 Enter “sdmmtc” to go into maintenance application.
- 3 Enter “appl” to see running applications
- 4 Scroll up/down to verify that “DMS Maintenance Application” is present and running.
- 5 Use the “swim” command to verify that the DMA version is at least 2.0.99.0.

Note: If the DMA is System Busy, it needs to be busied and returned to service. If there are other problems, contact SDM support for assistance.

- 6 This procedure is complete.

MG 9000 lines provisioning

Lines have defined permanent terminations for MTA access and line circuit testing. Line testing does not run on lines that have not been provisioned in the MG 9000. Permanent terminations can be defined automatically when a line card is inserted in the shelf.

Troubleshooting subscriber lines

This section is a guide to provide an example of how the MG 9000 line test system can be used to troubleshoot subscriber problems.

To use this section, find the symptom in the following table that most closely matches the subscriber complaint, and follow directions for that symptom. The symptom table references testing procedures that follow this table.

Line circuit troubleshooting guide

Symptom	Action	Result	Corrective Action
No Dial Tone No Ringing	Post line at CS 2000 MAP terminal. Refer to "Posting line" in <i>DMS-100 Family Lines Maintenance Manual</i> , 297-1001-594	Line is INB or MB	RTS the line.
		Line is PLO or IDL	Perform the General line testing - loop test
		Line is out of service (such as SB, LMB).	Perform the General line testing - loop test
Phone rings, but can't receive calls	Perform the Loop Test in General line testing - loop test		
One-Way Speech (either way)		Problem Solved	No Further Action
Noise on Line		Problem Not Solved	Perform the "Speech Test Procedure".

General line testing - loop test***At the MG 9000 Manager***

- 1 Perform a loop test from the loop test system.
- 2 The next step is determined based on the information in the following table.

If	Do
the loop test passes	Perform the line circuit test
the loop test fails	Perform the General line testing - customer premise equipment test

- 3 This procedure is complete.

General line testing - customer premise equipment test***At the MG 9000 Manager***

- 1 Have the customer disconnect phones and modems. Run a loop test with the loop test system.
- 2 The next step is determined based on the information in the following table.

If	Do
the loop test passes	Equipment on customer premise is faulty.
the loop test fails	Dispatch loop repair.

- 3 This procedure is complete.

General line testing - line equipment test***At the MG 9000 Manager***

- 1 Post the MG 9000 at the MG 9000 Manager. Check for alarms or faulty equipment at the Alarm Browser that may affect the line.
- 2 The next step is determined based on the information in the following table.

If	Do
line equipment faults or alarms	Dispatch equipment repair.
no equipment faults exist	Perform the General line testing - line circuit test

- 3 This procedure is complete.

General line testing - line circuit test***At the MG 9000 Manager***

- 1 Post the line circuit at the MG 9000 Manager. Refer to *MG 9000 Fault Management*, NN10074-911.
- 2 The next step is determined based on the information in the following table.

If	Do
the circuit is locked	Unlock the circuit
the circuit is unlocked but in alarm	Clear the alarm. Refer to <i>MG 9000 Fault Management</i> , NN10074-911
the circuit is unlocked but appears to be operational	Perform the General line testing - line card default diagnostic

- 3 This procedure is complete.

General line testing - line card default diagnostic

At the MG 9000 Manager

- 1 From the line circuit's diagnostic window, run the default diagnostic.
- 2 The next step is determined based on the information in the following table.

If	Do
the circuit fails	Move the subscriber or replace the line card
the circuit passes (POTS and Coin)	Perform the General line testing - service verification test
the circuit passes (EBS)	Perform the Next level debugging, generic - perform a continuous loop test

- 3 This procedure is complete.

General line testing - service verification test

At the MG 9000 Manager

- 1 From the line circuit's diagnostic window, perform a "Test All."
- 2 The next step is determined based on the information in the following table.

If	Do
the circuit fails	Move the subscriber or replace the line card
the circuit passes but a ringing problem is revealed	Perform the Next level debugging, ringing problem on POTS and Coin lines - check subscriber phone
the circuit passes but a dial tone problem is revealed	Perform the Next level debugging, generic - perform a continuous loop test
the circuit passes but another problem is revealed	Return to symptom "Problem not solved" line in Line circuit troubleshooting guide

- 3 This procedure is complete.

Speech test - speech test***At the MAP terminal***

- 1 Use the loop test system to monitor the line to verify problem.
- 2 If a problem exists, use the loop test system to ring the subscriber. Listen for defects in voice transmission over loop.
- 3 The next step is determined based on the information in the following table.

If	Do
no problem observed	Perform the Check transmission equipment procedure.
an audible problem (not CO noise through the headset) is detected	Perform the Speech test - subscriber premise equipment test

- 4 This procedure is complete.

Speech test - subscriber premise equipment test***At the MAP terminal***

- 1 With loop test system connection from ABOVE still up, have subscriber connect a different phone, remove the last phone used. Listen for defects in voice transmission over loop with new phone.
- 2 The next step is determined based on the information in the following table.

If	Do
no problem observed	Inform the customer of defective equipment.
an audible problem is detected	Perform the Speech test - check the last phone

- 3 This procedure is complete.

Speech test - check the last phone***At the MAP terminal***

- 1 With loop test system connection from ABOVE still up, have subscriber connect a different phone, remove the last phone used. Listen for defects in voice transmission over loop with new phone.
- 2 The next step is determined based on the information in the following table.

If	Do
no problem observed	Inform the customer of defective equipment.
an audible problem is detected	Perform the Speech test - check the transmission equipment

- 3 This procedure is complete.

Speech test - check the transmission equipment***At the MG 9000 Manager***

- 1 From the Alarm Browser, check ITP, ITX, and DCC cards for alarms.
- 2 Perform relevant self-diagnostics as described in *MG 9000 Fault Management*, NN10074-911.
- 3 The next step is determined based on the information in the following table.

If	Do
no alarms or failures are observed	Perform the Speech test - check the network
PCM or Packet Component Alarms or failures are present	Dispatch MG 9000 repair and retest.

- 4 This procedure is complete.

Speech test - check the network***At the MAP terminal***

- 1 Check Network for alarms or faults. Run appropriate network diagnostics.
- 2 The next step is determined based on the information in the following table.

If	Do
no alarms exist	Go to Next level debugging. generic - perform a continuous loop test
transmission alarms or failures are observed	Dispatch network repair and retest.

- 3 This procedure is complete.

Next level debugging, ringing problem on POTS and Coin lines - check subscriber phone***At the MAP terminal***

- 1 Subscriber plugs in phones and modems. Use the loop test system to ring the subscriber phone.
- 2 The next step is determined based on the information in the following table.

If	Do
no ring or no ring trip is present	Customer equipment problem. Dispatch loop repair to site based on local procedures.
no problem is observed	Go to Next level debugging. generic - perform a continuous loop test

- 3 This procedure is complete.

Next level debugging, generic - perform a continuous loop test***At the MAP terminal***

- 1** Use the loop test system to run continuous loop measurements on the loop.
- 2** The next step is determined based on the information in the following table.

If	Do
a fault is discovered	Dispatch loop repair to site based on local procedures.
no problem is observed	Dispatch to move subscriber or replace line card and retest.

- 3** This procedure is complete.



CS 2000-based lines testing

Introduction

Testing and troubleshooting of line faults are done using the Maintenance and Administration Position (MAP) user interface at the levels below the LNS MAP level. The LNS MAP level contains the following commands:

- lines test position (LTP)
- automatic line testing (ALT)
- lines service trouble (LNSTRBL)

This section identifies the supported MAP commands in the LTP, ALT, and LNSTRBL levels available for testing Carrier VoIP MG 9000 POTS, Ground Start, Coin, and Electronic Business Set (EBS) lines connected to MG 9000 line cards and to XPMs subtended from MG 9000 using DS512 access bridging interface (ABI) cards and remote digital terminal (RDT) lines. These commands are provided for the UA-AAL1 solution. Some commands rely on an MTM in the host office to conduct the tests. However, in the UA-IP solution, many commands are not supported.

Line maintenance commands

Line maintenance commands for lines that terminate on an MG 9000 line are the same as DMS-100 line maintenance commands with most commands being supported. However, some commands are not supported because they do not support DMS-100 RDT types of lines or POTS, Ground Start, Coin, or EBS.

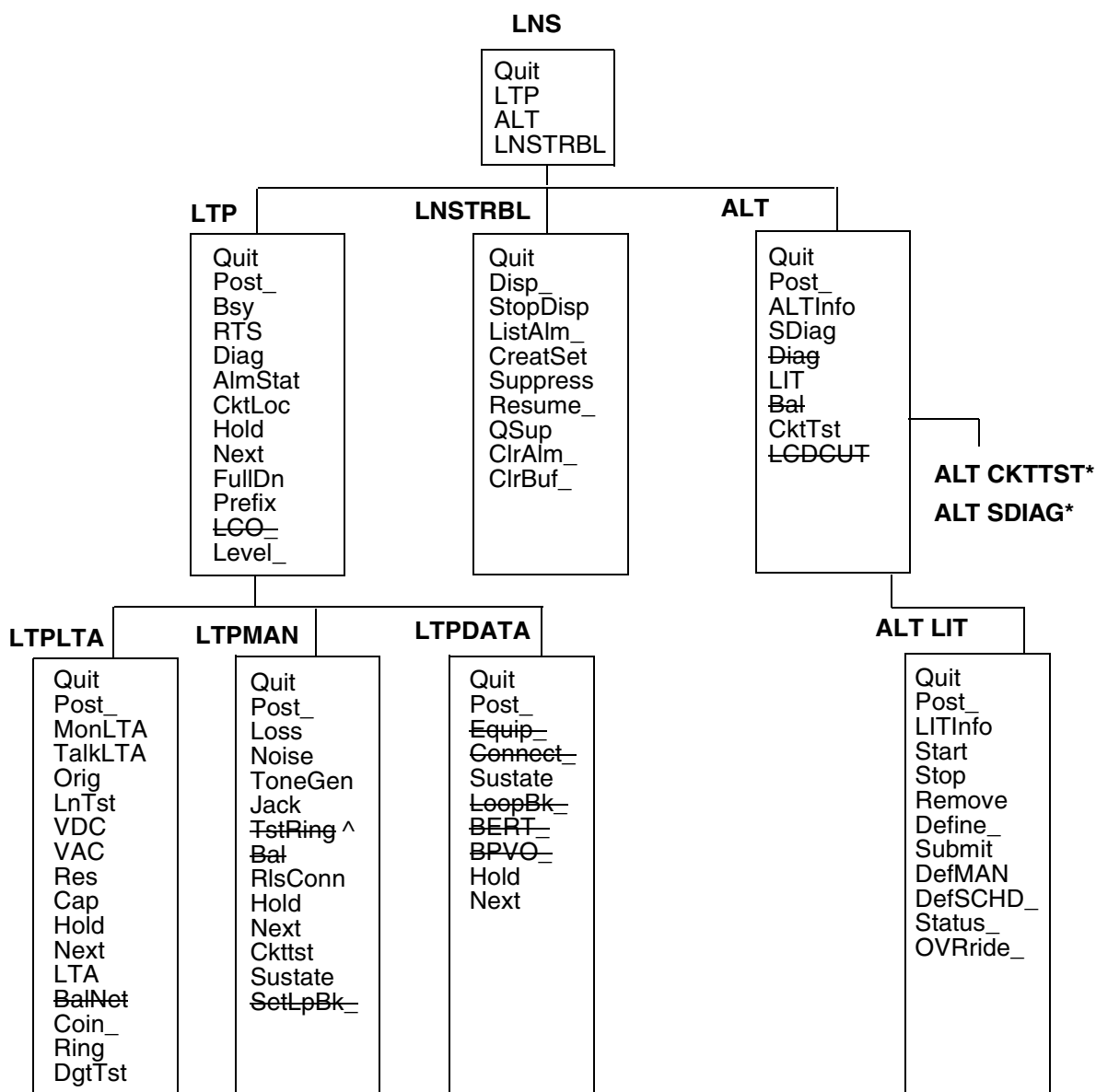
The following figure lists the line maintenance commands and their respective levels that support native MG 9000 lines. The unsupported

commands are indicated by a strikethrough. The legend in the figure provides additional clarification.

Note: Some command levels or sublevels are not shown in the figure for the following reasons:

- LTP IBNCON - This level is used for testing attendant console lines. The commands at this level are not applicable to Carrier VoIP MG 9000 lines.
- LTP DCTLTP - This level is the data call tester line (DCT) test position. The commands at this level are not applicable to Carrier VoIP MG 9000 lines.
- LTP LTPISDN - This level applies to ISDN lines. The commands at this level are not supported for lines that terminate on the MG 9000, because ISDN is not supported on the MG 9000.
- ALT LCDCUT - The commands at this level are not applicable to Carrier VoIP MG 9000.
- ALT DIAG - The commands at this level are not supported for MG 9000.
- ALT BAL - The commands at this level are not valid for RDTLSG, RDTCN, or RDTEBS lines.

Line maintenance commands



Legend:

* :The menu of commands for the other ALT levels are the same as the commands for the ALT LIT level.

^ : Indicates that a message is displayed referring the user to use the DIAG command.

A strike through indicates that the command is not supported.

Menu commands

The following sections describe the supported menu commands for lines that terminate on an MG 9000.

LTP menu commands

The following table describes supported LTP commands.

LTP commands

Command	Description
Quit	leaves the current level and returns to a higher level
Post_	posts a line or set of lines to the LTP
Bsy	changes the state of the line in the control position, or optionally all lines posted to a specific state
RTS	changes the state of the line in the control position, or optionally the complete set of posted lines, from MB to IDL
Diag	performs an extended diagnostic on a line in the control position that is in the MB or IDL state, and displays the results on the LTP screen
AlmStat	triggers the alarm system of the LNS subsystem and displays the status of alarms in the full switch by type or alarm, when used without parameters. The command is used with parameters to display all or selected alarms at specified units in the host or remote sites, or to change the thresholds of the alarm classes in the full switch.
CktLoc	locates and identifies the circuit card used for the line circuit in the control position, and displays circuit characteristics. Note: Some of the displayed information for the Floor and Row position, which consists of both the row and frame position, is dependent on the datafill of the LGRPLOC option in table LGRPINV. If this option is not provided, this information is displayed with default values of "00" for the Floor and "A00" for the Row position. The Bay ID consists of frame type, which is displayed as "MG9F," and the frame number. LEN information stored in table LNINV is also displayed.

LTP commands

Command	Description
Hold	moves the line in the control position to a spare hold position, and the next line from the posted set, if any, to the control position
Next	moves the line in a specified HOLD position to the control position, or replaces the line in the control position with the line in the specified hold position; and exchanges, saves, or drops the replaced line from LTP control
FullDn	displays the full national number
Prefix	clears the LTP of prefix digits. Optionally, it sets or changes prefix digits.
Level_	gives the user access to the sublevels LTPLTA, LTPMAN, LTPDATA, IBNCON, and DCTLTP at the MAP

LTPLTA menu commands

The following table describes supported LTPLTA commands.

LTPLTA commands

Command	Description	Metallic and non-metallic information
Quit	leaves the current level and returns to a higher level	
Post_	posts a line or set of lines to the LTP	
MonLTA	connects a headset circuit to the MG 9000 line in the control position for listening purposes	Metallic and non-metallic versions available
TalkLTA	connects a talk circuit to a subscriber on an MG 9000 line, and optionally connects a talk battery so the tester can converse with the subscriber when the cutoff (CO) relay is operated	Metallic and non-metallic versions available

LTPLTA commands

Command	Description	Metallic and non-metallic information
Orig	configures the loop side of a line circuit in either the off-hook mode or the on-hook mode, or alternates between modes	Metallic version supported
LnTst	performs resistance, capacitance, and voltage tests on an MG 9000 line Note: When using the LnTst command on lines connected to an MG 9000 GLC 32 line card, incorrect readings may be given for tip and ring voltage. Measure the ac-dc tip and ac-dc ring voltages using the LTPLTA VDC command.	Uses a metallic loop
VDC	performs a dc voltage measurement on a subscriber loop	Uses a metallic loop
Res	performs resistance measurements on an subscriber loop	Uses a metallic loop
VAC	performs an ac voltage measurement on a subscriber loop	Uses a metallic loop
CAP	performs a capacitance measurement on a subscriber loop	Uses a metallic loop
Hold	moves the line in the control position to a spare hold position, and the next line from the posted set, if any, to the control position	
Next	moves the line in a specified HOLD position to the control position, or replaces the line in the control position with the line in the specified hold position; and exchanges, saves, or drops the replaced line from LTP control	
LTA	connects the LTA to a line card, or releases the LTA from a line card Note: The LTA command is not valid for LNTST, RES, and CAP. If LTA is IN and LNTST, RES, or CAP is invoked, LTA is switched to OUT and the command is run.	Uses a metallic loop

LTPLTA commands

Command	Description	Metallic and non-metallic information
Coin_	sends a +130 V pulse on the subscriber loop to operate the coin collect mechanism in the coin station, or a -130 V pulse to operate the coin return mechanism	Metallic and non-metallic versions available
Ring	places ringing voltage on the loop of an MG 9000 line	Metallic and non-metallic versions available
DgtTst	tests the DIGITONE pad or dial on the subscriber station	Metallic and non-metallic versions available

LTPMAN menu commands

The following table describes supported LTPMAN commands.

LTPMAN commands

Command	Description	Metallic and non-metallic information
Quit	leaves the current level and returns to a higher level	
Post_	posts a line or set of lines to the LTP	
Loss	measures the insertion loss of a test tone sent from the subscriber end of a loop to its line circuit	Uses a metallic loop
Noise	measures the C-message weighted circuit noise on a subscriber loop	Uses a metallic loop
ToneGen	transmits a tone on a subscriber loop	Metallic and non-metallic versions available
Jack	connects a jack-ended trunk to a subscriber line, or a jack to a subscriber loop while bypassing the line card	Metallic and non-metallic versions available

LTPMAN commands

Command	Description	Metallic and non-metallic information
TstRing	tests the ringing relay in the line card for proper functioning. Since this functionality is performed during the Diag command, a message referring the user to run the Diag command is displayed.	
RlsConn	releases test equipment connected to a line	
Hold	moves the line in the control position to a spare hold position, and the next line from the posted set, if any, to the control position	
Next	moves the line in a specified HOLD position to the control position, or replaces the line in the control position with the line in the specified hold position; and exchanges, saves, or drops the replaced line from LTP control	
Ckttst	sends test messages to test the posted line. No external test equipment is required.	
Sustate	determines the status of the MBS connected to the Business Set line in the control position. No external test equipment is required.	
Note: The Ckttst and Sustate commands use the EBS run integrity test (RIT) command to verify messaging to specific P-phone components.		

LTPDATA menu commands

The following table describes supported LTPDATA commands.

LTPDATA commands

Command	Description
Quit	leaves the current level and returns to a higher level
Post_	posts a line or set of lines to the LTP
Sustate	determines the status of the MBS connected to the Business Set line in the control position

LTPDATA commands

Command	Description
Hold	moves the line in the control position to a spare hold position, and the next line from the posted set, if any, to the control position
Next	moves the line in a specified HOLD position to the control position, or replaces the line in the control position with the line in the specified hold position; and exchanges, saves, or drops the replaced line from LTP control

LNSTRBL menu commands

The following table describes supported LNSTRBL commands.

LNSTRBL commands

Command	Description
Quit	leaves the current level and returns to a higher level
Disp_	displays call processing trouble entries in the upper buffer that is allocated to an LCD
StopDisp	discontinues the periodic updating of the call processing trouble displays that were initiated by the command DISP
ListAlm_	displays a list of LCDs that have call processing fault alarms, and the class of alarm that exists in each LCD
CreatSet	posts a set of call processing trouble upper buffer entries
Suppress	causes specified trouble types to be ignored by the buffering process and by alarm generation
Resume_	discontinues the suppression of specified types of call processing troubles
QSup	lists the code number and description of the types of troubles that are currently suppressed

LNSTRBL commands

Command	Description
ClrAlm_	clears the call processing alarms in a specified LCD and resets attempt and failure counters to zero
ClrBuf_	deletes part or all of the contents of the upper buffer that is allocated to a specified LCD

ALT menu commands

The following table describes supported ALT commands.

ALT commands

Command	Description
Quit	leaves the current level and returns to a higher level
Post_	posts the scheduled ALT TESTID stored in memory (table ALTSCHED)
ALTInfo	checks test data stored in memory (table ALTSCHED)
SDiag	performs routine diagnostics for MG 9000 lines. If a TESTID is not entered as a parameter, a new TESTID must be defined with the DEFSCHD or DEFMAN command. Note: ALT SDiag supports all the MG 9000 line card types (POTS-32, SAA-12, and 8x8 DSL).
LIT	checks the electrical characteristics of the MG 9000 loops to ensure they are within the expected ranges of electrical characteristics. If a TESTID is not entered as a parameter, a new TESTID must be defined with the DEFSCHD or DEFMAN command.
CktTst	checks P-phone lines to ensure messaging to the line cards and phone sets. If a TESTID is not entered as a parameter, a new TESTID must be defined with the DEFSCHD or DEFMAN command.

ALT sublevel commands

The following table describes supported ALT sublevel commands.

ALT sublevel commands

Command	Description
Quit	leaves the current level and returns to a higher level
Post_	posts the scheduled ALT TESTID stored in memory (table ALTSCHED) and corresponds to the current sublevel
LITInfo	displays the system default values for the LIT parameters. Note: This command applies only to the ALTLIT menu level.
Start	sets the posted scheduled ALT test to run at the next scheduled time
Stop	stops a test and changes the status of the TESTID
Remove	removes the data associated with the posted TESTID from memory (table ALTSCHED). If the TESTID is for a scheduled test, the system prompts for a YES or NO confirmation.
Define_	defines test data for the specified TESTID
Submit	submits the defined test data for the posted TESTID into memory (table ALTSCHED)
DefMAN	assigns a TESTID to the test that corresponds to the current ALT sublevel. For example, the DEFMAN command entered at the LIT level of MAP device number 7 will be assigned a TESTID of MANUAL07.
DefSCHED_	assigns a TESTID to the scheduled test that corresponds to the current ALT sublevel
Status_	checks the status of the posted TESTID
OVRride_	overrides a scheduled test so testing will not start until a specified day and time has passed

Configurations

The following sections describe hardware and software requirements for CS 2000 line test support.

CS 2000 hardware

The following hardware is required.

Trunk modules

The CS 2000 supports an array of test heads and supporting hardware. The circuit packs are contained in trunk modules. Supported trunk modules include ISM, MTM, and RMM.

Test circuits

The following CS 2000 test heads and supporting hardware are required to support MG 9000 line testing:

- NT4X45AA EDTU (or NT1X90/NT2X96 TTT, NT2X47/NT2X56 TTU, NT4X23 DTU)
- NT2X10/NT2X11 MTU
- NT2X90AD MONTALK Circuit
- NT5X30AA 101 Communication Test Line (HSET)
- NT1X54AA Jack-ended trunk (JACK)
- NT2X90AD INC/OC Test Trunk (analog test trunk interface)

The CS 2000 also requires the NT2X57 SD card for MTL test trunks.

Note: For additional information about the circuit packs listed, refer to *DMS-100 Family Quick Reference Guide*, TAM-1001-018, available through Helmsman in the DMS-100 Carrier Solutions collection.

MTA matrix

The CS 2000 supports two types of test heads:

- transmission test heads - connect to the line under test through the bearer network
- metallic test heads - connect to the line under test through a metallic test access matrix

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

The CS 2000 supports the NT3X09BA 8x8 Matrix Card for implementing the MTA matrix.

The trunk modules also contain the MTA matrix cards.

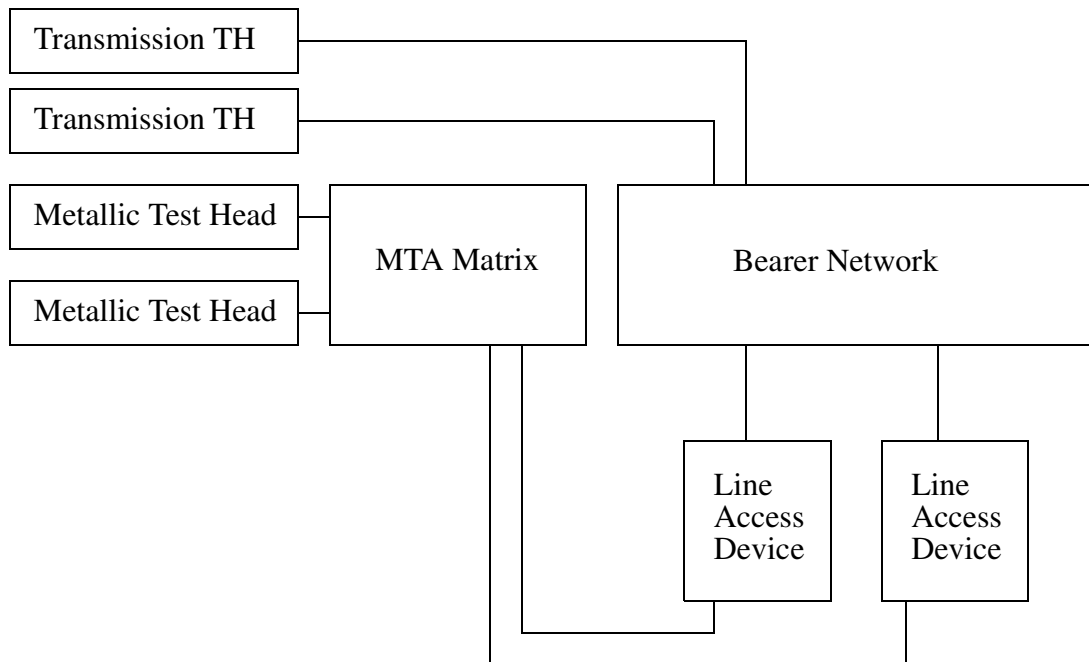
Test configurations

The following figures illustrate the hardware configuration required to support CS 2000-based line testing for MG 9000 lines.

In figure [Logical view of test equipment](#), the transmission test heads have access to the bearer network. The test heads are connected to the line access devices through the bearer network.

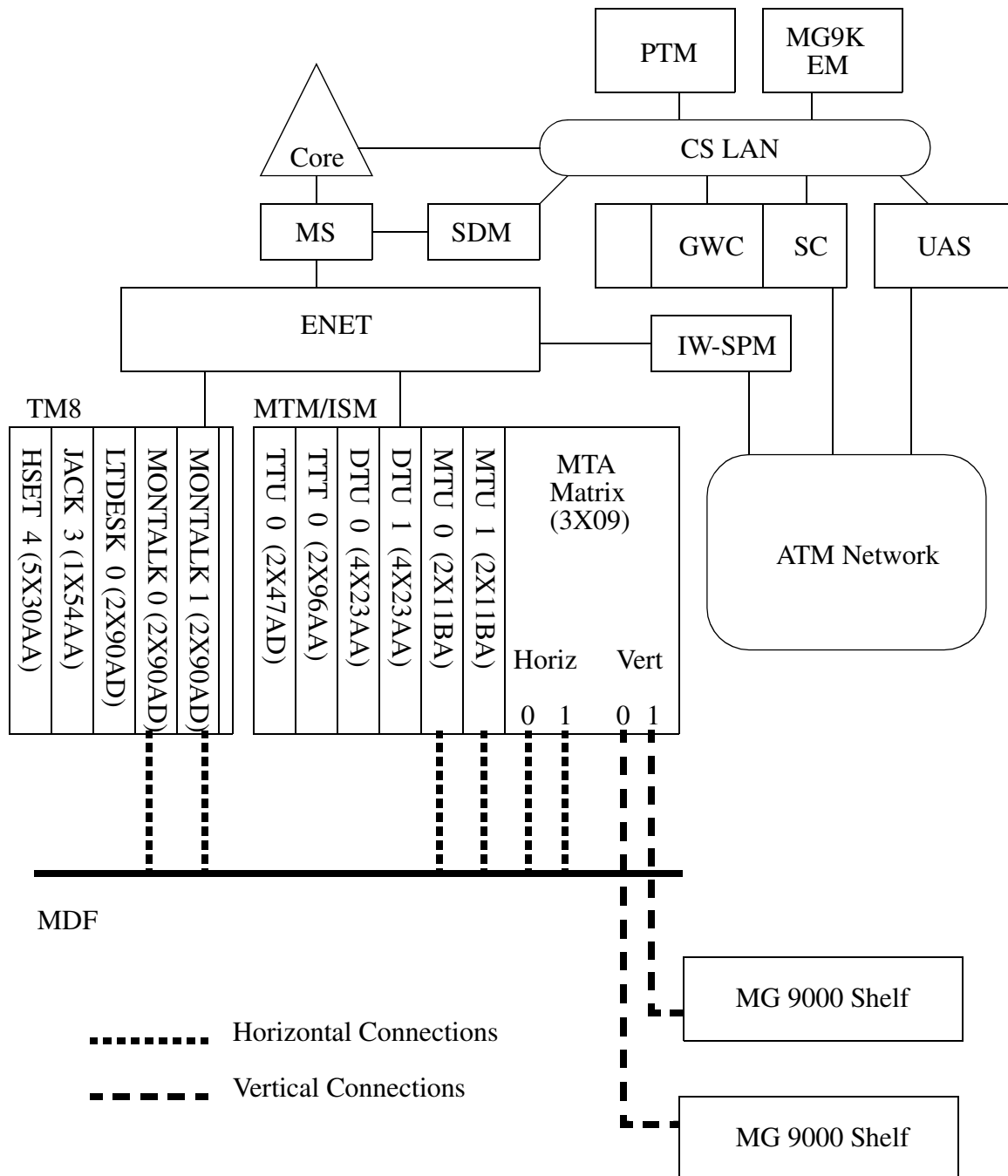
The metallic test heads are connected to horizontal leads on the MTA matrix. The line access devices are connected to the vertical leads on the MTA matrix. In this configuration, any metallic test head can be cross-connected to any line on any line access device.

Logical view of test equipment



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

Physical implementation



References

Refer to the following NTPs, available from the DMS-100 Carrier Solution collection in Helmsman, for additional information:

- *DMS-100 Family Lines Maintenance Guide*, 297-1001-594, provides a more complete description of the test equipment and the provisioning of the test equipment.
- *DMS-100 Family Hardware Description Manual*, 297-8991-805, provides additional details on the hardware described.
- *DMS-100/200 Hardware Planning Guide*, 50041.08

MG 9000 hardware

The MG 9000 requires the following hardware to support line testing:

- one metallic access test response circuit (MTA-TRC) card per node per frame
- one shelf interface card (SIC) per shelf

Third-party gateways

The CS 2000 line test functionality supports any third-party gateway that supports the H.248 extension. Specific information on the hardware requirements for third-party gateways is not provided.

Software requirements

The following types of equipment or connectivity datafill are required to support the CS 2000 line test functionality.

- First, provision the trunk modules that contain the CS 2000 test equipment.
- Second, provision the CS 2000 test heads and supporting hardware.
- Third, provision the MTA matrix for the CS 2000.
- Fourth, provision the metallic test head connectivity to the horizontals on the MTA matrix.
- Fifth, provision the line concentrating device connectivity to the verticals on the MTA matrix.

Note 1: Additional datafill is required for individual line test applications. For example, the subscriber premise tests are supported for MG 9000 lines; however, the subscriber premise tests require translations in the CS 2000 to function correctly. For information about provisioning and translations for individual line test applications, refer to *DMS-100 Family Lines Maintenance Guide*, 297-1001-594, where the existing provisioning and translations methods apply to LGRP lines on the CS 2000.

Note 2: The tables in the following examples are shown in packed format.

Trunk module provisioning

The trunk modules are provisioned in tables TMINV and RMMINV. Provisioning includes shelves such as TM8, MTM, and RMM. In the following example, RMMs are not shown. However, RMMs can be used in remote sites for MG 9000 line testing. The sample datafill shows a single MTM and TM8 shelf for this CS 2000.

Example

```
TMNM FRTYPE FRNO SHPOS FLOOR ROW FRPOS LKDATA
EQPEC LOAD EXEC S CTMLOC
```

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

The CS2000 uses the same trunk module provisioning as the DMS-100. Refer to *DMS-100 Family Lines Maintenance Guide*, 297-1001-594, for details on trunk module provisioning for the CS 2000.

Test head and supporting hardware provisioning

The test heads and supporting hardware are provisioned in tables TRKGRP and TRKMEM.

Example

```
TABLE: TRKGRP
```

```
GRPKEY GRPTYP TRAFSNO PADGRP NCCLS GRPINFO
```

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

```
TABLE: TRKMEM
```

```
CLLI EXTRKNM SGRP MEMVAR
```

```
-----
TTU 0 0 MTM 0 21
TTT 0 0 MTM 0 16
DTU 0 0 MTM 0 18
DTU 1 0 MTM 0 19
```

```

MTU 0 0 MTM 0 10
MTU 1 0 MTM 0 11
MONTALK 0 0 TM8 0 8
MONTALK 1 0 TM8 0 10
HSET 4 0 TM8 0 2
JACK 3 0 TM8 0 18
LTDESK 0 0 TM8 0 6

```

The CS2000 uses the same test head provisioning as the DMS-100. Refer to *DMS-100 Family Lines Maintenance Guide*, 297-1001-594, for details on test head provisioning for the CS 2000.

MTA matrix provisioning

The MTA matrix is provisioned in table MTADRV. The following example shows an MTA matrix with a single MTA matrix card. The CS 2000 supports a significantly larger MTA matrix. The MTA matrix for a CS 2000 is created by linking together multiple MTA cards in both vertical and horizontal directions.

Example

TABLE: MTAMDRV

```

MTAMEM VERT HORIZ TMTYPE TMNO TMCKTNO MTACARD
-----

```

```

0 0 0 MTM 0 6 3X09BA

```

The CS2000 uses the same MTA matrix provisioning as the DMS-100. Refer to *DMS-100 Family Lines Maintenance Guide*, 297-1001-594, for details on MTA matrix provisioning for the CS 2000.

Horizontal connectivity provisioning

Horizontal connectivity is provisioned in table MTAHORIZ. The following example shows a pair of MTUs connected to the first two horizontals on the MTA matrix, along with a single analog test trunk for supporting external test systems such as Access Care, 4TEL, and Loop Care.

Example

TABLE: MTAHORIZ

```

HORIZ HORIZGRP HORIZAGT MTAGRP
-----

```

```

0 0 L MTU 0 Y (0 0) $
1 0 L MTU 1 N (0 1) $
3 0 T LTDESK 0 (0 3) $

```

The CS2000 uses the same horizontal connectivity provisioning as the DMS-100. Refer to *DMS-100 Family Lines Maintenance Guide*, 297-1001-594, for details on horizontal connectivity provisioning for the CS 2000.

Vertical connectivity provisioning

Vertical connectivity provisioning for LGRPs differs from vertical connectivity provisioning for existing DMS-100 peripherals.

The line concentrating devices are assigned to verticals on the MTA matrix. For LGRPs, verticals are assigned to specific MG 9000 metallic test access points and shelves through tables LGRPINV and MTAVERT.

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

Example

TABLE: LGRPINV

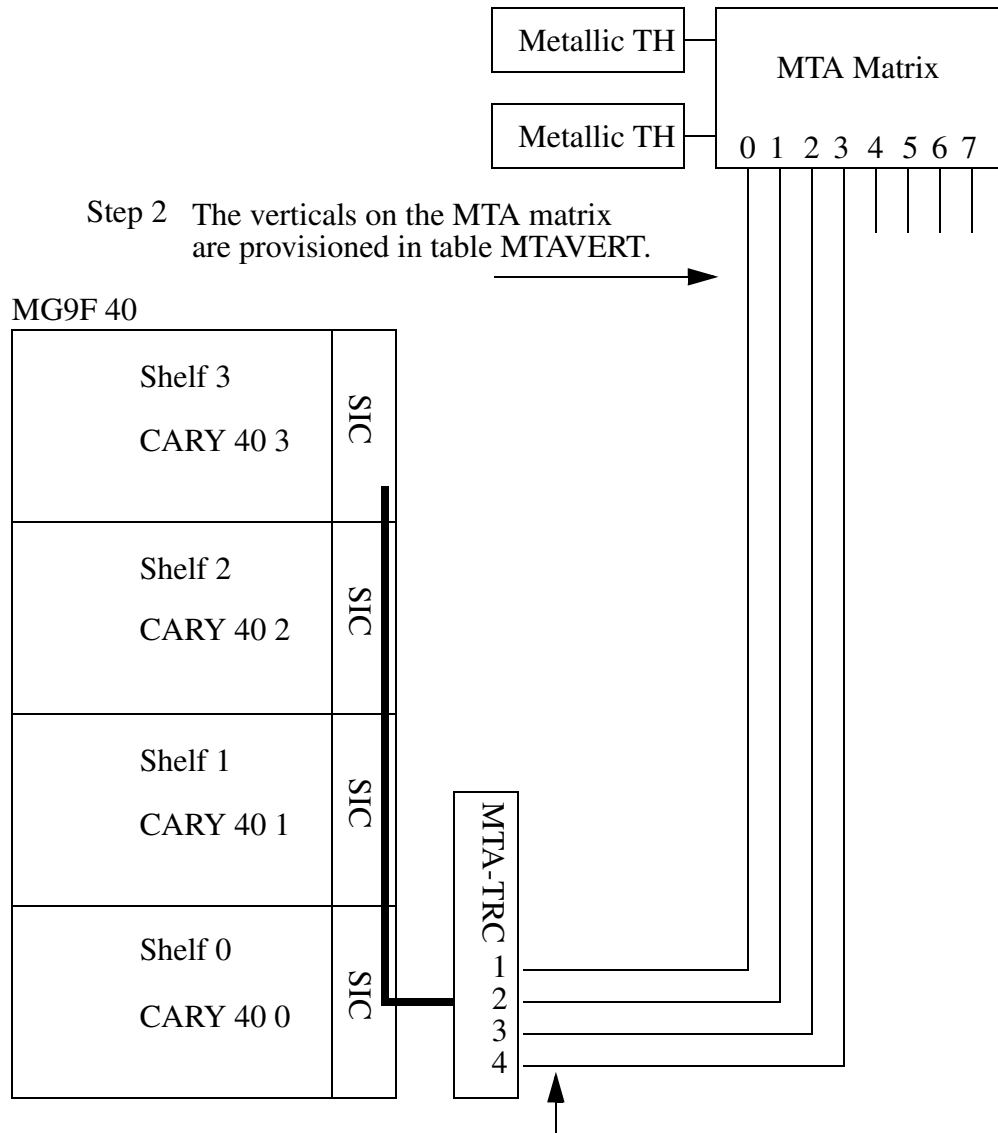
GRPNO	SRVRNAME	GRPTYPE	LGRPPTS
CARY 77 1	GWC	5	S (MTSTAPT CARY (0 1))\$
CARY 40 2	GWC	5	S (MTSTAPT CARY (1 1))\$

TABLE: MTAVERT

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

The following figure shows examples of provisioning tables LGRPINV and MTAVERT for MG 9000 to MTA matrix connectivity.

Provisioning tables LGRPINV and MTAVERT



Step1 The metallic test access points on the MG 9000 are provisioned in table LGRPINV with a designation of the attached vertical on the MTA matrix.

Table LGRPINV

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

Table MTAVERT

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

Vertical
Metallic Test Access Point

Provisioning rules for MG 9000 verticals are as follows:

- The metallic test access connections for the MG 9000s are provisioned in table LGRPINV first and then in table MTAVERT.
- Table LGRPINV allows up to eight metallic test access points (with verticals) to be provisioned for each LGRP. (The eight metallic test access points are for future flexibility to increase the number of simultaneous tests for each MG 9000.)

Note: Currently, only one metallic test access point for each LGRP in table LGRPINV (each LGRP being a single MG 9000 shelf) can be provisioned.

- LGRPs are assigned to verticals in table MTAVERT. The tuple for the LGRP in table LGRPINV must have a metallic test access point associated to the vertical before an LGRP is assigned to a vertical in table MTAVERT.

A single physical MG 9000 can support up to 16 shelves. However, a single physical MG 9000 can support only eight metallic test access points. When an MG 9000 grows beyond eight shelves, verticals must be shared across multiple shelves. The provisioning recommendations are as follows:

- For MG 9000 nodes with eight or fewer shelves, each shelf on the MG 9000 needs to be assigned to a unique metallic test access point and vertical.
- As an MG 9000 grows beyond eight shelves, the metallic test access points and verticals used on shelves 0 through 7 need to be reused on shelves 8 through 15 sequentially.
- If wide band testing is required on the MG 9000 to support DSL lines, one or more of the metallic test access points needs to be reserved for the wide band test head.

The following two examples show provisioning for tables LGRPINV and MTAVERT for a 16-shelf MG 9000. In the examples, the MG 9000 node is in the Cary site and occupies frames 40, 41, 42, and 43.

The first example shows all eight metallic test access points wired to verticals on the MTA matrix.

Example

TABLE: LGRPINV

GRPNO SRVRNAME GRPTYPE LGRPOPTS

```
-----
CARY 40 0 GWC 0 S (MTSTAPT CARY (0 1) $ ) $
CARY 40 1 GWC 0 S (MTSTAPT CARY (1 2) $ ) $
CARY 40 2 GWC 0 S (MTSTAPT CARY (2 3) $ ) $
CARY 40 3 GWC 0 S (MTSTAPT CARY (3 4) $ ) $
CARY 41 0 GWC 0 S (MTSTAPT CARY (4 5) $ ) $
CARY 41 1 GWC 0 S (MTSTAPT CARY (5 6) $ ) $
CARY 41 2 GWC 0 S (MTSTAPT CARY (6 7) $ ) $
CARY 41 3 GWC 0 S (MTSTAPT CARY (7 8) $ ) $
CARY 42 0 GWC 1 S (MTSTAPT CARY (0 1) $ ) $
CARY 42 1 GWC 1 S (MTSTAPT CARY (1 2) $ ) $
CARY 42 2 GWC 1 S (MTSTAPT CARY (2 3) $ ) $
CARY 42 3 GWC 1 S (MTSTAPT CARY (3 4) $ ) $
CARY 43 0 GWC 1 S (MTSTAPT CARY (4 5) $ ) $
CARY 43 1 GWC 1 S (MTSTAPT CARY (5 6) $ ) $
CARY 43 2 GWC 1 S (MTSTAPT CARY (6 7) $ ) $
CARY 43 3 GWC 1 S (MTSTAPT CARY (7 8) $ ) $
```

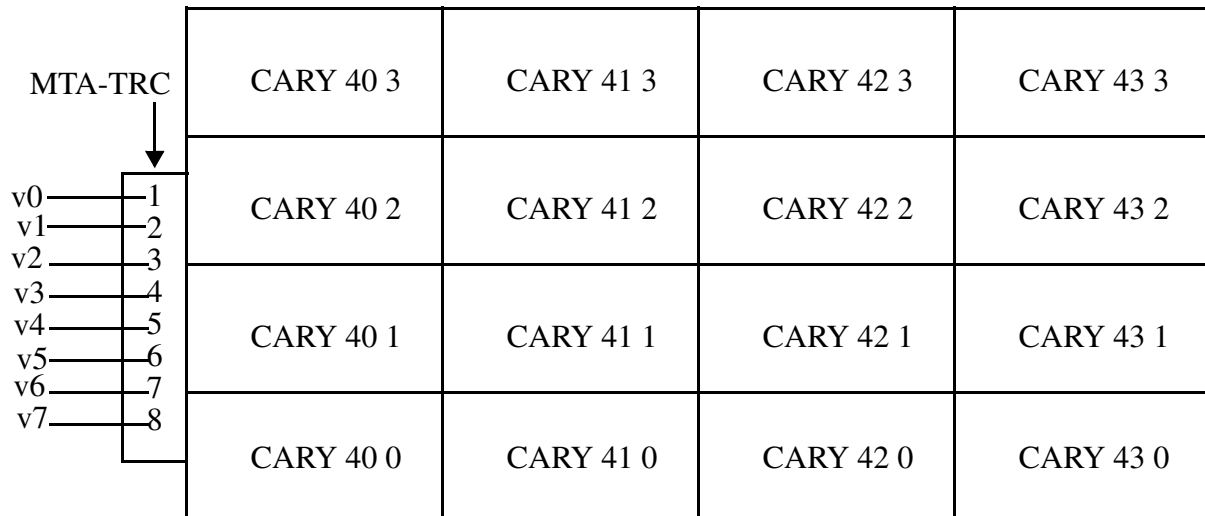
TABLE: MTAVERT

VERT VERTCONN

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

The following figure shows all eight metallic test access points assigned to verticals. In this configuration, a single vertical can be shared by up to 1024 lines.

All eight metallic test access points assigned to verticals



The second example shows only six metallic test access points wired to verticals on the MTA matrix. Two metallic test access points are reserved for wide band testing.

Example

TABLE: LGRPINV

GRPNO SRVRNAME GRPTYPE LGRPPTS

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

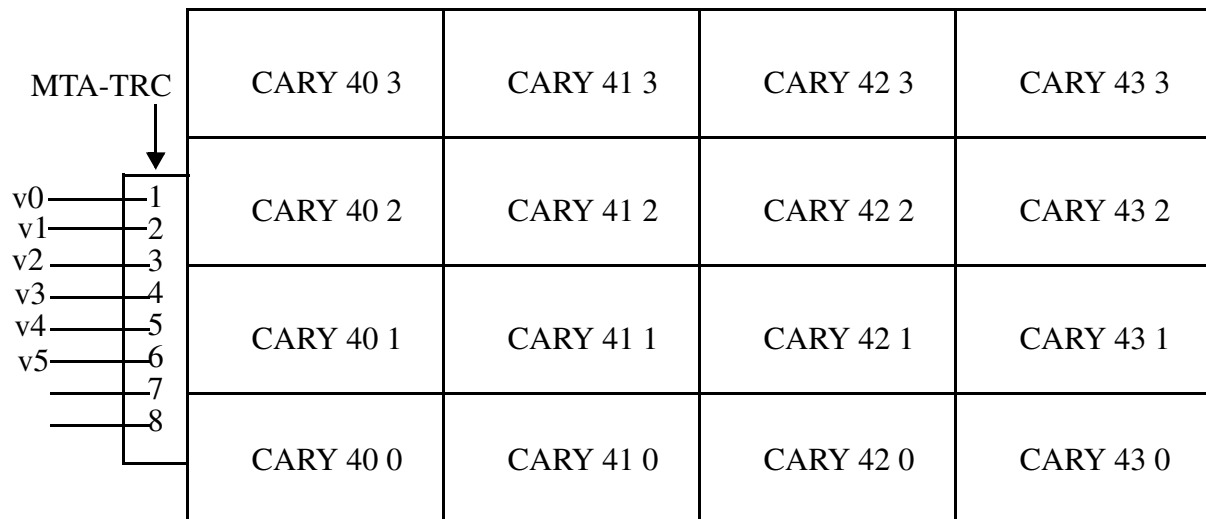
TABLE: MTAVERT

VERT VERTCONN

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

The following figure shows six metallic test access points wired to verticals on the MTA matrix, with two metallic test access points reserved for wide band testing. In this configuration, a single vertical can be shared by up to 1536 lines.

Two metallic access points reserved



Line states

This section provides information on MG 9000 line states, including the interfaces for checking the line states and what the line states mean.

CS 2000 line states

The following table shows a complete list of CS 2000 line states and their meanings. The table indicates whether the line states apply to MG 9000 lines.

CS 2000 line states

Line state	Meaning	Applicable to MG 9000 lines?
CPB (Call processing busy)	The line is in use by a subscriber. (Call processing is taking place.)	Yes
CPD (Call processing deload)	The line is in use by a subscriber, and a maintenance request to place the line in the deloaded (DEL) state is pending. The state changes momentarily to DEL when call processing ends, and then to state MB.	Yes
CUT (Cutoff)	The cutoff relay in the line circuit is operated, disconnecting the subscriber loop from the line circuit.	No
DEL (Deloaded)	The line is removed from availability for call processing by a maintenance order, in preparation for testing activity. (DEL is a temporary state after the CPD state and before the MB state.)	Yes
DMB	Applies to ISDN lines. See <i>Basic Rate Interface Maintenance Guide</i> , 297-2401-501.	No

CS 2000 line states

Line state	Meaning	Applicable to MG 9000 lines?
HAZ (Hazard)	A line hazard condition (foreign line voltage, leakage resistance) has been detected. The line's cutoff relay is operated.	No
IDL (Idle)	The line is in service and available to process calls.	Yes
INB (Installation busy)	The line is not available for call processing for one or more of the following reasons: • some required data has not been assigned • a data change has been made • an LTP operator has entered an instruction	Yes
LMB (Line module busy)	Call processing cannot take place because the LM or LCM is out of service.	Yes
LO (Lock-out)	The line has been removed from service by the CS 2000, preventing call processing. Manual action is required to change the state.	Yes
MB (Maintenance busy)	The line has been removed from service by maintenance personnel or by the CS 2000. Call processing cannot take place.	Yes
NEQ (not equipped)	The LEN has not been datafilled. Call processing cannot take place.	Yes

CS 2000 line states

Line state	Meaning	Applicable to MG 9000 lines?
PLO (PSPD lock-out)	This state is a variety of the state LO. The line has been removed from service by the CS 2000 because of a PSPD condition. Call processing cannot take place until the condition no longer exists and the CS 2000 restores the line state to IDL.	Yes
SB	The line has been removed from service by the CS 2000. A range of error conditions can cause an MG 9000 line to be set to the SB state in the CS 2000. The CS 2000 can set the line to the SB state if it detects an error condition for the line. The CS 2000 can also set the line to the SB state if it receives an indication from the GWC that the line is not capable of providing service, which could represent a data error in the GWC or MG 9000, or it could represent a fault condition for the line at the MG 9000 such as an overcurrent protection condition.	Yes
SZ	This is a future line state.	No

MG 9000 line states

The state of the MG 9000 circuits is checked at the MG 9000 Manager. The MG 9000 Manager shows the status of the physical line circuit and the status of the H.248 line termination.

Line circuit

The state of the physical line circuit is checked by opening the line card at the MG 9000 Manager and opening the port on the line card. The following table shows state information for the MG 9000 physical line circuit.

State information for the MG 9000 physical line circuit

State	Information
Administrative	Shows the requested user state. The values can be locked and unlocked. • Locked indicates the circuit has been manually taken out of service. • Unlocked indicates the circuit has <i>not</i> been manually taken out of service.
Operational	Shows the current service state. The values can be enabled or disabled. • Enabled indicates the circuit is in the working state. • Disabled indicates the circuit is <i>not</i> in the working state.
Fault	Indicates the line maintenance subsystem on the MG 9000 determined the selected circuit is in a fault condition and is not providing service. The CS 2000 state will be set to SB.

State information for the MG 9000 physical line circuit

State	Information
Protection	Indicates the excess voltage/current was detected for the selected circuit. MG 9000 line maintenance placed the circuit in the protection state. Lines in this state cannot provide subscriber service. When MG 9000 lines are in the protection state, the CS 2000 line state is set to SB.
Babble	Indicates the selected circuit is a babbler, meaning the circuit is generating excessive circuit state indications. Line maintenance disables babbling circuits to protect the MG 9000. Lines in this state cannot provide subscriber service. When line maintenance takes the circuit to the disabled state, the CS 2000 line state is set to SB.

H.248 line termination

The state of the H.248 line termination is shown at the Switched Lines Services Manager on the MG 9000 Manager. The H.248 line termination represents the logical call processing service for the subscriber circuit. The state of the H.248 line termination is tied to the CS 2000 line state.

If the service is turned down on the CS 2000, the CS 2000 will set the H.248 line to the disabled state. When service is restored for a line at the CS 2000, the CS 2000 will set the H.248 termination to the enable state.

The H.248 line termination state is also dependent on the physical line circuit. If the physical line circuit is in the disabled state, the gateway moves the H.248 line termination to the disabled state. The CS 2000 line state is then set to the SB state.

The following table shows the state information from the switched lines services manager for the H.248 line terminations.

State information for H.248 line terminations

State	Information
Operational	Shows the current service state of the H.248 line termination. The values are enabled, disabled, and test. • Enabled indicates the H.248 line termination is in the working state and providing service. • Disabled indicates the H.248 line termination is not in the working state and not providing service. • Indicates the line is currently under test.
Termination Test	Provides additional information for terminations under test. The values are Not Testing, Testing via Call Service, and Testing via EM. • Not Testing indicates the line is not currently under test. • Testing via Call Server indicates the line is currently under test from the Call Server. • Testing via EM indicates the line is currently under test from the MG 9000 Manager.

Line options

The following line options affect the CS 2000 line test subsystem and are supported for MG 9000 lines:

- No Double Connect (NDC) - prevents a line from being connected to a verification or test circuit when the line is off-hook.
- No Hazard Test (NHT) - prevents a line from being tested for a hazard condition. Line hazard conditions are low resistance or high voltage on the subscriber loop.
- No Line Insulation Test (NLT) - allows the automatic line insulation test to skip a line.

Line diagnostics

The CS 2000 line diagnostics verify a line is capable of providing service. The CS 2000 line diagnostics are integrated with the embedded MG 9000 circuit diagnostics. When an MG 9000 circuit is diagnosed from the CS 2000, the embedded MG 9000 line diagnostics are executed and additional network tests are performed to ensure the circuit is providing service.

The following table shows the tests the CS 2000 line diagnostics perform for MG 9000 lines and compares the MG 9000 line diagnostics to the diagnostics supported for host lines and GR-303 lines.

CS 2000 line diagnostics

Test	Host	TR-303	LGRP
Provisioning data	See note 1	x	x
Missing card test	x	x	See note 2
Transhybrid loss	x	x	x
Pads	x	See note 3	x
Weighted or notched noise	x	x	x
Flux cancellation/echo return	x	x	See note 4
Off-hook detection	x	x	x
On-hook detection	x	x	x
Ringling	x	x	x
Ground start	x	x	x
T/R reversal	x	x	x
Coin collect	x	x	x
Coin return	x	x	x
P-phone OPCODE signaling	x	x	x
P-phone provisioning audit	x	x	x
Battery feed	x	See note 5	See note 5

CS 2000 line diagnostics

Test	Host	TR-303	LGRP
Cutoff relay	x	See note 5	See note 5
Test access relay	x	See note 5	See note 5
Facility check	x	See note 5	See note 5

x - denotes supported tests

Note 1: The provisioning in GR-303 digital loop carriers and H.248 gateways must match provisioning in the CS 2000 to provide service. Host lines do not have remote provisioning data and the provisioning data test is not required.

Note 2: The MG 9000 does not support a missing card test. MG 9000 lines affect the CS 2000 line state. If the line card is missing or disabled, the CS 2000 line state is set to SB to indicate the line is in a trouble condition.

Note 3: The CS 2000 does not support analog pad control for GR-303 lines. Therefore, the analog padding test is not supported for GR-303 lines.

Note 4: The MG 9000 has echo cancellers for all line types. Therefore, an echo return test is not performed.

Note 5: GR-303 and MG 9000 line diagnostics do not include facility and line card relay tests.

The line diagnostics check the line card hardware and the integrity of the network solution. The following sections provide details about the MG 9000 line diagnostics.

Line diagnostic results are delivered through a combination of the following:

- printing results at the MAP
- generating appropriate logs
- setting or clearing alarm flags for the line

Line logs

The MG 9000 line diagnostic reports results to logs LINE100 and LINE 101.

Log LINE100 indicates a line diagnostic has passed.

Example

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

Log LINE 101 indicates a line diagnostic has failed.

Example

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

Alarm flags

Various errors and actions in the CS 2000 can mark failure flags against a line. The failure flags provide information about lines in trouble that need corrective action.

The alarm flags supported for MG 9000 lines are shown in the following table.

CS 2000 MAP-level alarm flags supported for MG 9000 lines

Alarm flag	Problem
D	long diagnostic has failed
S	short diagnostic has failed
N	needs long diagnostic
Q	line is in ShowerQ
L	line has failed loop signaling at the line card
I	line has failed loop signaling at the terminal

Line states supported for line diagnostics

The following diagnostics are supported for MG 9000 lines:

- LTP DIAG
- ALT SDIAG
- ShowerQ

Note: MLT trunks do not execute a line card diagnostic for MG 9000 lines. Therefore, MLT trunk diagnostics are not covered here.

The LTP process must process the diagnostic message. Based on the data in the line card diagnostic message, the LTP process generates the line log, updates the line alarms, and prints the test results at the LTP position.

LTP DIAG

The LTP DIAG is supported on MG 9000 lines in the following state:

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

ALT DIAG

The ALT DIAG tests lines in the following states:

- INB
- MB
- IDL

ShowerQ

Failure conditions cause the MG 9000 line to be registered in a shower queue (a system-originated diagnostic schedule) and released for a second call attempt.

Failure conditions include the following:

- line card not in place
- test register not functioning
- message signaling is not successful

If any of the tests fail a second time, the MG 9000 line is subjected to diagnostic tests for fault identification. Shower queue results are reported to the log system.

The ShowerQ tests lines in the following states:

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

For more information on the command line states, refer to *DMS-100 Family Lines Maintenance Guide*, NTP 297-1001-594.

Diagnostic results

This section shows the diagnostic results and indicates the actions the user needs to take for each result.

Diagnostic passed

Log example

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

Description

The line tested is functioning correctly.

Alarm

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

User action

No user action is required.

CS 2000 software error**Log example**

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

Description

A CS 2000 software error has occurred.

Alarm

The line failure flag is not affected.

User action

Capture the CS 2000 SWERR log and try the test again.

GWC processing error**Log example**

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

Description

A GWC software error has occurred.

Alarm

The line failure flag is not affected.

User action

Capture the GWC logs and try the test again.

GWC provisioning faults detected

The GWC provisioning faults detected include the following:

- missing node data
- missing line data

These faults are described in the following sections.

Missing node data**Log example**

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

Description

A GWC provisioning problem has occurred. The GWC is missing the node provisioning data for the MG 9000 shelf. This problem prevents the entire MG 9000 shelf from providing service.

Alarm

The failure flag for the line under test is not affected.

User action

Check the node provisioning data for the GWC.

Missing line data

This sections provides information about missing line data in the GWC.

Log example

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

Description

The provisioning data for the line under test is missing in the GWC. The line cannot provide service with this error condition.

Alarm

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

User action

Check the line provisioning data in the GWC.

Node state faults detected in the GWC**Log example**

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

Description

Gateway is out of service in GWC.

Alarm

The node that represents the MG 9000 shelf state is out of service in the GWC. The lines will be transitioned to the LMB state in the CS 2000. If the line is not in the LMB state, a node mismatch exists between the CS 2000 and the GWC.

User action

Check the line state in the CS 2000. If the line state is not LMB and this diagnostic error persists, attempt to correct the MG 9000 shelf state mismatch between the CS 2000 and the GWC.

Line termination out of service in GWC**Log example**

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

Description

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

Alarm

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

User action

Check the state of the line circuit at the MG 9000 Manager to ensure the line circuit is in the enabled state.

If the line circuit is in the enabled state at the MG 9000 Manager, BSY and RTS the line to attempt to bring the line termination back to a working state. After doing the BSY and RTS, repeat the diagnostic. If the problem persists, contact the next level of support.

GWC to MG 9000 messaging error**Log example**

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

Description

The GWC timed out waiting for a response from a test request sent to the MG 9000.

Alarm

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

User action

Try the diagnostic again. If the problem persists, a messaging problem exists between the GWC and the MG 9000 that can affect call processing.

MG 9000 processing error**Log example**

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

Description

The MG 9000 failed to process a line test request.

Alarm

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

User action

Check the MG 9000 logs for SWERRs and try the test again. If the problem persists, contact the next level of support.

MG 9000 test resources unavailable**Log example**

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

Description

The MG 9000 line test resources are out of service.

Alarm

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

User action

Check the state of the line test hardware at the MG 9000. Check the state of the MTA-TRC pack and the SIC cards, which provide the line test functions in the MG 9000.

MG 9000 test resource busy**Log example**

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

Description

The MG 9000 line test resources are currently in use.

Alarm

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

User action

All the line test resources in the MG 9000 are currently in use, and no type of equipment fault is indicated. Attempt the test again.

Line provisioning mismatch in the MG 9000**Log example**

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

Description

The diagnostic detected a mismatch between the line termination provisioning date in the MG 9000 and provisioning date in table LNINV.

Alarm

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

User action

Correct the line data mismatch at the MG 9000.

Line card diagnostic failures

Line card diagnostic failures include the following:

- off-hook detection failure
- on-hook detection failure
- single-party ringing failure
- tip ring reversal failure
- coin collect or coin return failure
- transhybrid loss failure
- weighted or notched noise failure
- line card pads failure
- line card messaging failure
- mainset messaging failure
- add-on/extension provisioning mismatch
- no free vertical available

These failures are described in the following sections.

Off-hook detection failure

Log example

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

Description

The line card does not detect and report the subscriber off-hook condition correctly.

Alarm

The line failure flag for the line is set to **D** to indicate the line card diagnostic has failed. The CS 2000 identifies lines marked with the **D** failure flag as incapable of providing service and require user maintenance.

The following command line prints a report containing all the lines served by the CS 2000 with a **D** failure flag:

```
>mapci nodisp;mtc;lms;ltp;post df d print
```

The following command line prints a report containing all the lines served by the CS 2000 with any flag failure set:

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

User action

Replace the line circuit or move the subscriber to another circuit.

On-hook detection failure**Log example**

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

Description

The line card does not detect and report the subscriber on-hook condition correctly.

Alarm

The line failure flag for the line is set to **D** to indicate the line card diagnostic has failed. The CS 2000 identifies lines marked with the **D** failure flag as incapable of providing service and require user maintenance.

The following command line prints a report containing all the lines served by the CS 2000 with a **D** failure flag:

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

The following command line prints a report containing all the lines served by the CS 2000 with any flag failure set:

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

User action

Replace the line circuit or move the subscriber to another circuit.

Single-party ringing failure**Log example**

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

Description

The line card does not generate the correct ringing voltage and frequency.

Alarm

The line failure flag for the line is set to **D** to indicate the line card diagnostic has failed. The CS 2000 identifies lines marked with the **D** failure flag as incapable of providing service and require user maintenance.

The following command line prints a report containing all the lines served by the CS 2000 with a **D** failure flag:

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

The following command line prints a report containing all the lines served by the CS 2000 with any flag failure set:

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

User action

Replace the line circuit or move the subscriber to another circuit.

Tip ring reversal failure**Example log**

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

Description

Indicates the line card does not provide tip ring reversal correctly.

Note: Tip/ring reversal signaling is used only by coin lines.

Alarm

The line failure flag for the line is set to **D** to indicate the line card diagnostic has failed. The CS 2000 identifies lines marked with the **D** failure flag as incapable of providing service and require user maintenance.

The following command line prints a report containing all the lines served by the CS 2000 with a **D** failure flag:

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

The following command line prints a report containing all the lines served by the CS 2000 with any flag failure set:

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

User action

Replace the line circuit or move the subscriber to another circuit.

Coin collect or coin return failure**Log example**

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

Description

The line card does not generate coin collect or coin return voltages correctly.

Note: If a coin return failure occurs, the diagnostic result displays, "Test failed: Coin return."

Alarm

The line failure flag for the line is set to **D** to indicate the line card diagnostic has failed. The CS 2000 identifies lines marked with the **D** failure flag as incapable of providing service and require user maintenance.

The following command line prints a report containing all the lines served by the CS 2000 with a **D** failure flag:

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

The following command line prints a report containing all the lines served by the CS 2000 with any flag failure set:

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

User action

Replace the line circuit or move the subscriber to another circuit.

Transhybrid loss failure**Log example**

The example shows a line card that does not pass low frequency tones correctly. The transhybrid loss test has failed.

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

Description

The transhybrid loss test passes a series on tones through a line card in both directions to verify the line card will encode and decode speech correctly for voice frequencies. This test also verifies the hybrid circuit in the line card is not defective. The transhybrid loss test uses the following frequencies: 304, 704, 1504, and 4305 Hz. The measured transhybrid loss at each test frequency is displayed in the diagnostic failure log.

The transhybrid loss test will fail if too much loss or gain is detected when the tones pass through the line under test. Different line cards have different transmission characteristics. The following tables show the test ranges considered passing for the MG 9000 line cards.

POTS-32 and 8x8 ADSL

	304 Hz	704 Hz	1504 Hz	3204 Hz
Minimum (loaded)	Not supported	Not supported	Not supported	Not supported
Maximum (loaded)	Not supported	Not supported	Not supported	Not supported
Minimum (non-loaded)	-5.0 dB	-4.5 dB	-4.5 dB	-5.0 dB
Maximum (non-loaded)	1.0 dB	1.5 dB	1.5 dB	1.0 dB

SAA-12

	304 Hz	704 Hz	1504 Hz	3204 Hz
Minimum (loaded)	Not supported	Not supported	Not supported	Not supported
Maximum (loaded)	Not supported	Not supported	Not supported	Not supported
Minimum (non-loaded)	-8.0 dB	-7.5 dB	-7.0 dB	-7.5 dB
Maximum (non-loaded)	-2.0 dB	-1.5 dB	-1.0 dB	-1.5 dB

Alarm

The line failure flag for the line is set to **D** to indicate the line card diagnostic has failed. The CS 2000 identifies lines marked with the **D** failure flag as incapable of providing service and require user maintenance.

The following command line prints a report containing all the lines served by the CS 2000 with a **D** failure flag:

```
>mapci nodisp;mtc;lms;ltp;post df d print
```

The following command line prints a report containing all the lines served by the CS 2000 with any flag failure set:

```
>mapci nodisp;mtc;lms;ltp;post df print
```

User action

If the diagnostic failure shows excess loss or gain in the line card, replace the line card or move the subscriber to another circuit.

Note: The MG 9000 does not support loaded lines. If an MG 9000 line is provisioned as a loaded line in table LNINV, the transhybrid loss test will fail. In this event, correct the provisioning error in table LNINV.

Continuity failure

Log example

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

Description

When the transhybrid loss test indicates -88.8 for all frequencies, the problem is most likely a bear path problem, rather than a line card problem.

Alarm

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

User action

Attempt the test again. If multiple lines show the same behavior, troubleshoot the bearer network connection faults.

Weighted or notched noise failure

Log examples

```
RTPU07BC ***+LINE101 OCT26 09:50:13 6200 FAIL LN_DIAG
CARY 00 0 00 14      DN 2145201001
DIAGNOSTIC RESULT Noise Level 44.1DB Notch Noise
ACTION REQUIRED Replace Card
CARD TYPE RDTLSG
```

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

Description

The weighted or notched noise tests have failed for the line card. The noise limits for the MG 9000 line cards are as follows:

- notched noise must be less than 42.0 dB
- weighted noise must be less than 30.0 dB

Alarm

The line failure flag for the line is set to **D** to indicate the line card diagnostic has failed. The CS 2000 identifies lines marked with the **D** failure flag as incapable of providing service and require user maintenance.

The following command line prints a report containing all the lines served by the CS 2000 with a **D** failure flag:

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

The following command line prints a report containing all the lines served by the CS 2000 with any flag failure set:

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

User action

Replace the line circuit or move the subscriber to another circuit.

Line card pads failure

Log example

```
RTPU07BC ***+LINE101 OCT26 09:44:19 2700 FAIL LN_DIAG  
CARY 00 0 00 14 DN 2145201001  
DIAGNOSTIC RESULT -1.7 -2.2 -.4 -.4 Pad 1DB Test  
ACTION REQUIRED Replace Card  
CARD TYPE RDTLSG
```

Description

The line card pad test failed. The CS 2000 supports per call gain control, referred to as padding. The line card pad test verifies the CS 2000 can adjust pads in an MG 9000 line card. The line card pad test measures the gain applied by a line card when a 1, 3, 5, and 7 dB pad are applied to the line under test. The line card pad test verifies the correct gain applied at 304, 704, 1504, and 4305 Hz.

Note: The example log shows a diagnostic that failed the 1dB pad test. The diagnostic allows a 1 dB variance from the requested gain. In the example, the 704 Hz frequency had a loss of -2.2 dB when a -1.0 dB pad was requested.

Alarm

The line failure flag for the line is set to **D** to indicate the line card diagnostic has failed. The CS 2000 identifies lines marked with the **D** failure flag as incapable of providing service and require user maintenance.

The following command line prints a report containing all the lines served by the CS 2000 with a **D** failure flag:

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

The following command line prints a report containing all the lines served by the CS 2000 with any flag failure set:

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

User action

Replace the line circuit or move the subscriber to another circuit.

Line card messaging failure**Log example**

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

Description

P-phones or Electronic Business Set (EBS) lines use out-of-band signaling, which is OPCODE signaling. The line card diagnostic for an MG 9000 P-phone line verifies the OPCODE signaling to the line card and to the P-phone set. The diagnostic error log indicates the OPCODE signaling test to the line card has failed. The diagnostic failure log also contains the number of OPCODE messages sent to and received back from the line card.

Alarm

The line failure flag for the line is set to **L** to indicate the line card diagnostic has failed the OPCODE signaling test to the line card itself. The CS 2000 identifies lines marked with the **L** failure flag as incapable of providing service and require user maintenance.

The following command line prints a report containing all the lines served by the CS 2000 with an **L** failure flag:

```
>mapci nodisp;mtc;lns;ltp;post df lcard print
```

The following command line prints a report containing all the lines served by the CS 2000 with any flag failure set:

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

User action

Use the CKTTST command to perform additional manual OPCODE signaling tests on the suspected line.

Replace the line circuit or move the subscriber to another circuit.

Main set messaging failure

Log example

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

Description

The line card diagnostics for an MG 9000 P-phone line verify the OPCODE signaling to the line card and P-phone set. The diagnostic error log indicates the OPCODE signaling test to the P-phone set has failed. The diagnostic failure log also contains the number of OPCODE messages sent to and received back from the P-phone set.

Alarm

The line failure flag for the line is set to **I** to indicate the line card diagnostic has failed the OPCODE signaling test to the phone set. The CS 2000 identifies lines marked with the **I** failure flag as incapable of providing service. For this failure flag, a working P-phone is assigned to the line under test, and the CS 2000 cannot successfully exchange OPCODE messages with a set on the loop.

The following command line prints a report containing all the lines served by the CS 2000 with an **I** failure flag:

```
>mapci nodisp;mtc;lns;ltp;post df lset print
```

The following command line prints a report containing all the lines served by the CS 2000 with any flag failure set:

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

User action

Verify the set is connected to the loop.

Use the CKTTST command to perform additional manual OPCODE signaling tests.

If the CKTTST command verifies the signaling to the mainset is not working and the set is connected to the loop, replace the line card. If the problem persists, replace the set.

Use the Station Ringer test to verify the new set is fully functional from the subscriber premise.

Add-on/extension provisioning mismatch**Log example 1**

Example 1 shows a line with an extension provisioned in the CS 2000 that cannot be detected on the loop.

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

Log example 2

Example 2 shows a line with an add-on provisioned in the CS 2000 that cannot be detected on the loop.

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

Log example 3

Example 3 shows a line where the diagnostic has detected an extension, which is not provisioned in the CS 2000, on the loop being tested.

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

Log example 4

Example 4 shows a line where the diagnostic has detected an add-on, which is not provisioned in the CS 2000, on the loop being tested.

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

Description

The line card diagnostic on an MG 9000 P-phone line audits the hardware on the loop and compares the hardware to the provisioning in the CS 2000. The CS 2000 can support up to three add-ons and three extensions for each P-phone line. If the line diagnostic finds a mismatch

between the hardware and the provisioning in the CS 2000, the diagnostic will fail.

Alarm

The line failure flag for the line is set to **D** to indicate the line card diagnostic has failed. The CS 2000 identifies lines marked with the **D** failure flag as incapable of providing service and require user maintenance.

The following command line prints a report containing all the lines served by the CS 2000 with a **D** failure flag:

```
mapci nodisp;mtc;lms;ltp;post df d print
```

The following command line prints a report containing all the lines served by the CS 2000 with any flag failure set:

```
mapci nodisp;mtc;lms;ltp;post df print
```

User action

Use the SUSTATE command to evaluate the CS 2000 provisioning compared to the hardware connected to the line. When the mismatch is identified, the provisioning or hardware error needs to be corrected.

No free vertical available

Log example 1

Example 1 shows a Silent Switchman subscriber premise test which failed because no free vertical was available to conduct the test.

```
RTPS      LINE210 JUL29 14:37:50 0300 INFO No Free  
          Vertical Available  
          UAIP 01 0 02 01 DN 6105205533  
          Reason :Silent Switchman - No Free Vert
```

Log example 2

Example 2 shows a dialable short circuit subscriber premise test that failed because no free vertical was available to conduct the test.

```
RTPS      LINE210 JUL29 14:22:23 4100 INFO No Free  
          Vertical Available  
          UAIP 01 0 02 00 DN 6105205532  
          Reason :Dialable ShortCkt - No Free Vert
```


Description

Single vertical connectivity for each MG 9000 shelf is supported for MAP-based line testing of MG 9000 lines. For all the tests listed below, the first vertical provisioned in table LGRPINV will be seized during the test and unavailability of that vertical.

The following tests are run from the LTPLTA level and require vertical connectivity:

- MonLTA
- TalkLTA
- LnTst
- VDC
- VAC
- RES
- CAP

The following tests are run from LTPMAN and only the metallic version of these tests require vertical connectivity:

- Tonegen (Metallic)
- Jack (Metallic)

If no vertical is available for the previous LTPLTA and LTPMAN level tests because the vertical is in use by some other line in the LGRP, the following message is output on the MAP terminal.

```
No Free Vertical Available
MTAPT is in use by another Line on Same LGRP
mtapt : 3
NN : 104
TN : 49
LEN : UAIP 01 0 02 00
```

If no vertical is available for the previous LTPLTA and LTPMAN level tests because the vertical is in use by some other line in a different LGRP, the following message is output on the MAP terminal.

```
No Free Vertical Available
```

The following subscriber run tests require vertical connectivity:

- SSMan
- DsCkt

If no free vertical is available for SSMan or DsCkt tests, a LINE210 log is output as presented in Log examples 1 and 2 of this section.

Alarm

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

User action

Attempt the test again.

Multicircuit line cards

When the diagnostics detect a fault that requires intervention by a user, the CS 2000 raises a failure flag against that line. See the list of supported diagnostic failure flags in table [CS 2000 MAP-level alarm flags supported for MG 9000 lines on page 169](#).

The diagnostic failure flag can be cleared by replacing the line card and reexecuting the diagnostic. When the diagnostic passes, the CS 2000 automatically clears the failure flag.

Note: For multicircuit line cards, the user cannot replace the entire pack if only a few circuits on the line card are defective. In this scenario, the user cannot clear the diagnostic failure flag by reexecuting the diagnostic.

Use the following procedure to manage *individual* defective circuits on a multicircuit line card.

- If a subscriber is assigned to the defective circuit, move the subscriber off the defective circuit to a working circuit.
- Select the circuit at the gateway manager.
- Lock the individual defective circuit. If a circuit is in the locked state, the CS 2000 will not attempt to test the line. The CS 2000 will also not be able to return the line to the IDL state if service is reassigned to the defective circuit by mistake.
- Enter the LGRP Line Test Tool (LGLTT). Type LGLTT at the CI prompt. Use the ClrFlag command to clear the failure flag against the line. See [LGLTT on page 217](#).
- Post the line at the LTP level of the MAP. Verify the failure flag has been cleared for the circuit. Verify the DIAG command is not allowed for the line.

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

Lines routine maintenance

The following NTPs, available from the DSM-100 Carrier Solutions collection from Helmsman, provide extensive information on the recommended routine maintenance procedures for CS 2000 lines.

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

The following sections describe lines routine maintenance for MG 9000 lines.

ALT support for lines that terminate on an MG 9000

ALT provides as much testing concurrency as possible. The user enters into ALT the range of LENSs to test, which can span multiple nodes. ALT runs through the range of LENSs to determine test tests for the range of LENSs.

ALT then creates a set of test streams, which represents the resources available to perform ALT tests. ALT attempts to create as many streams as possible and divides the test sets among the streams for maximum testing concurrency. The following figure shows a configuration where ALT calculates 10 possible test sets for a range of LENSs and divides the test set among four test streams.

10 possible test sets divided among four test streams

	Test Set 1	Test Set 2	Test Set 3
Stream 1			
	Test Set 4	Test Set 5	Test Set 6
Stream 2			
	Test Set 7	Test Set 8	Test Set 9
Stream 3			
	Test Set 10		
Stream 4			

ALT tests subscriber lines without manual intervention by maintenance personnel. Line maintenance personnel define the test parameters at the ALT menu levels. The system starts the defined tests at the scheduled times. Table ALTSCHEd is used to define the test parameters for ALT procedures.

Only the following ALT tests are enabled for MG 9000 lines:

- SDiag
- LIT
- CktTst

ALT SDiag

ALT SDiag will be scheduled and executed on MG 9000 lines. ALT SDiag routinely runs the line diagnostics to detect functional, state, or provisioning errors that prevent subscriber service.

Each MG 9000 shelf is represented as an LGRP in the Call Server. A single MG 9000 frame is represented in the CS 2000 as four distinct nodes. Therefore, a single MG 9000 frame will be divided into four separate ALT test sets (one set for each shelf).

ALT SDIAG is dependent on the TTU resources in the MTM and the MTA-TRC resources in the MG 9000.

- The TTU resources are required to perform transmission tests on the MG 9000 line cards.
- The MTA-TRC card provides the supervision and ringing test resources.

ALT SDIAG calculates the test streams for MG 9000 lines based on the available TTUs. ALT creates a single test stream for each TTU available for ALT SDIAG testing.

Note: An MG 9000 frame has a single MTA-TRC card. Each MTA-TRC card provides only two TRC circuits. Therefore, for a single MG 9000 frame, only two MG 9000 line card diagnostics can be executed simultaneously.

The following examples illustrate the previous note:

- A user requests ALT to perform diagnostics for all the MG 9000 lines in a single frame.
- Each MG 9000 shelf is represented in the Core as an LGRP. Each node in the CS 2000 is assigned to a unique test set. Therefore, each MG 9000 shelf will be assigned to a unique test set.

- Because the line card diagnostic requires only one TTU in the CS 2000, ALT attempts to create four test streams, one for each test set, and assigns a TTU to each stream.
- ALT then assigns each test set, one for each shelf, to the four test streams.
- When the test sets are assigned to test streams, ALT begins processing the ALT test streams in parallel. ALT attempts line card diagnostics on all four shelves in an MG 9000 frame concurrently. Because the MG 9000 can support only two simultaneous line card diagnostics, there will be resource contentions in the MG 9000. Two of the ALT test streams will execute correctly, and two of the ALT test streams will fail due to unavailable resources at the MG 9000.

Note: To avoid resource contention, the user needs to create tests on a per MG 9000 shelf basis and ensure ALT SDIAG is not scheduled on more than one shelf per frame concurrently.

ALT LIT

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

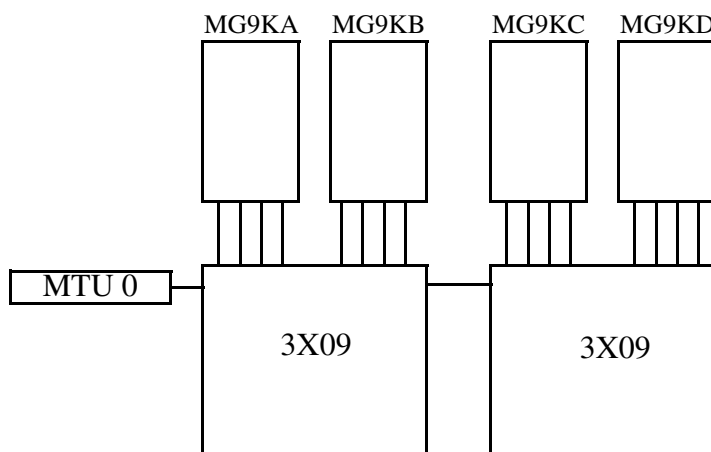
ALT LIT requires an MTU to test the subscriber loop. ALT uses the dedicated MTUs in the switch.

There are two test configuration options for MG 9000 lines:

- Single dedicated MTU for a pair of NT3X09s - If you use the Wide band Test Access (WTA) panel, there will be a single dedicated MTU for a pair of NT3X09s.
- Dedicated MTU for each NT3X09 - If you wire the test equipment together through the main distribution frame (MDF), a dedicated MTU can be assigned to each NT3X09.

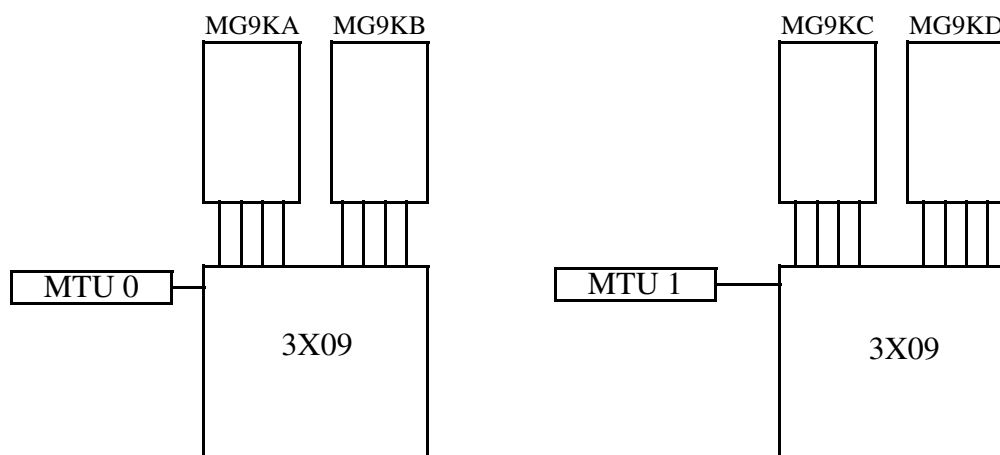
The single dedicated MTU configuration is shown in the following figure.

Single dedicated MTU for a pair of 3X09s



The dedicated MTU for each 3X09 is shown in the following figure.

Dedicated MTU for each 3X09



Note: An MG 9000 node cannot span across multiple 3X09 circuit packs. Therefore, in either configuration, a given MG 9000 can use only one possible dedicated MTU for performing ALT LIT tests.

When ALT LIT creates its test streams, it will create a test stream for each MTU in the switch that has the ALT option set to Y. As ALT LIT is

assigning MG 9000 test sets to the test streams, the MG 9000 test sets for a single MG 9000 (one for each shelf) will go into the test stream, because all the shelves for a given MG 9000 must use the same MTU. All the shelves in an MG 9000 physical node will be tested serially, ensuring there is no contention for MG 9000 resources while ALT LIT is testing MG 9000 lines.

Note: The option the user chooses to deploy for the 3X09 configurations depends on the maintenance window allowed for ALT LIT testing.

ALT CKTTST

ALT CKTTST performs messaging to the MG 9000 to check the ability to loopback P-phone messages at the line card or phone set. For the MG 9000, each shelf is represented as a node in the Core. Each MG 9000 LGRP is considered a single test set. No test equipment is required to perform a CKTTST; therefore, ALT can create a unique test stream for each test, up to the maximum number of ALT test streams allowed.

Note: ALT CKTTST can run concurrently across all MG 9000 shelves in the office.

Subscriber premises test support for lines that terminate on an MG 9000

The subscriber premises tests are a series of tests maintenance personnel can invoke from the subscriber premises.

The following subscriber premise tests are supported:

- Silent switchman test (SSMAN)
- Dialable short circuit test (DSCKT)
- Station ringer test (SRT)

Note: For a complete description of these tests, refer to *DMS-100 Family Lines Maintenance Guide*, 297-1001-594. This NTP contains additional information about subscriber premises tests and translations required to support these tests.

SSMAN

The SSMAN test checks the subscriber loop for facility faults. The test circuit is accessed by dialing a service code or a seven-digit number. After a confirmation tone is returned, the MG 9000 line is disconnected from the office battery and ground for a defined interval as datafilled in table OFCENG as SILENT_SWITCHMAN_TIMEOUT, allowing facility faults to be checked.

DCKT

The DCKT test involves placing a short circuit to loop of the MG 9000 line when a code is dialed to access the short circuit. The short circuit persists on the line under test for a period of time as established by the operating company in table OFCENG as CABLE_SHORT_TIMEOUT, or for the default period of three minutes. When the short circuit ends its established duration, the subscriber's line is returned to regular service.

SRT

The SRT verifies the functionality of the subscriber's set. The SRT is initiated by dialing a customer-defined access code. When the test is initiated, the user can verify the following set functions:

- POTS, Coin, or Groundstart
 - DP or DTMF digits
 - Flash key or flash hook
 - RLS key or on-hook
 - Talk key or off-hook
 - Set ringer
- P-phone
 - Meridian set function keys
 - Meridian set lamps
 - Meridian set display

Note: The circuit test part of the SRT for KSET lines is not supported. The results for circuit test are shown by LED displays 1, 2, and 8 turning on. The number of messages is not displayed. The test can be exited by pressing the Hold key.

Lines troubleshooting

CS2000 lines

The following NTPs provide extensive information on the recommended routine maintenance and troubleshooting procedures for CS 2000 lines:

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

MG 9000 lines

This section provides recommendations for faults on MG 9000 lines.

No dial tone**Procedure 1 Troubleshooting no dial tone*****At the customer loop testing OSS***

- 1 Perform a detailed loop test to determine if the problem is outside the plant.

If	Do
the fault is outside the plant	Dispatch outside plant personnel. Go to step 10 .
the fault is inside the plant	step 2

At the MAP

- 2 Post the line at the CS 2000 and check the CS 2000 line state.

If	Do
the line is in the manual busy state	Stop troubleshooting. Go to step 10 .
the line is in the SB state	step 3
the line is in the IDL state	step 8

- 3 Attempt to BSY and RTS the line.

If	Do
the line returns to the IDL state	Verify dial tone is restored. Go to step 10 .
the line remains SB	step 4

At the MG 9000 Manager

- 4 Check the line circuit for faults at the MG 9000 Manager.

Note: The line circuit must be in the enabled state before the CS 2000 line state will return to IDL.

If	Do
there is a circuit fault at the MG 9000	Resolve the MG 9000 circuit fault. Go to step 5 .
there is not a circuit fault at the MG 9000	step 8

- 5 Verify the line circuit fault is resolved and line circuit is restored to the enabled state.

At the MAP

- 6 Verify the line has returned to the IDL state in the CS 2000.

- 7 Verify dial tone is restored.

If	Do
dial tone is restored	step 10
the CS 2000 line is IDL and there is no dial tone	step 8

- 8 Execute the DIAG command on the line.

Note: The DIAG command verifies the line provisioning data in the CS 2000, GWC, and MG 9000. When the provisioning data is verified, the DIAG requests the MG 9000 to execute the embedded circuit diagnostics, which will execute the following tests:

- off-hook detection
- on-hook detection
- ringing
- for coin lines: coin collect, coin return, or reverse battery
- for P-phone lines, OPCODE signaling is verified instead of analog signaling

If	Do
the line diagnostic fails	Resolve the issue reported in the diagnostic. If there is still no dial tone, go to step 9 .
the line diagnostic passes	step 9

- 9 Check for dial tone at the tip and ring (T/R) pair attached to the face plate on the line card.

Note: The TALKTA and ORIG commands can be used remotely to pull dial tone from the T/R of the line card.

If	Do
there is no dial tone and the line diagnostic passed for the line	Escalate to the next level of support. Go to step 10 .
there is dial tone	step 10

- 10 You have completed this procedure.

Poor speech quality

Procedure 2 Troubleshooting poor speech quality

At the customer loop testing OSS

- 1 Perform a detailed loop test to determine if the problem is outside the plant.

If	Do
the problem is outside the plant	Dispatch outside plant personnel. Go to step 3 .
the problem is inside the plant	step 2

At the MAP

- 2 Post the line at the CS 2000 MAP position and execute the DIAG command.

Note: The DIAG command verifies the transmission characteristics of the line.

If	Do
the DIAG fails	Move the subscriber to a different circuit. Go to step 3 .
the DIAG passes	Use the TONEGEN, LOSS, and NOISE commands to perform manual transmission tests on the subscriber's line card and loop. Go to step 3 .
the problem cannot be isolated	Escalate to the next level of support. Go to step 3 .

- 3 You have completed this procedure.

Line does not ring**Procedure 3 Troubleshooting a line that does not ring*****At the customer loop testing OSS***

- 1 Perform a detailed loop test to determine if the problem is outside the plant.

If	Do
the fault is outside the plant	Dispatch outside plant personnel. Go to step 10 .
the fault is inside the plant	step 2

At the MAP

- 2 Post the line at the CS 2000 and check the CS 2000 line state.

If	Do
the line is in the manual busy state	Stop troubleshooting. Go to step 10 .
the line is in the SB state	step 3
the line is in the IDL state	step 8

- 3 Attempt to BSY and RTS the line.

If	Do
the line returns to the IDL state	Verify dial tone is restored. Go to step 10 .
the line remains SB	step 4

At the MG 9000 Manager

- 4 Check the line circuit for faults at the MG 9000 Manager.

Note: The line circuit must be in the enabled state before the CS 2000 line state will return to IDL.

If	Do
there is a circuit fault at the MG 9000	Resolve the MG 9000 circuit fault. Go to step 5 .
there is not a circuit fault at the MG 9000	step 8 .

- 5 Verify the line circuit fault is resolved and line circuit is restored to the enabled state.

At the MAP

6 Verify the line has returned to the IDL state in the CS 2000.

7 Verify dial tone is restored.

If	Do
dial tone is restored	step 10
the CS 2000 line is IDL and there is no dial tone	step 8

8 Execute the DIAG command on the line.

Note: The DIAG command verifies the line provisioning data in the CS 2000, GWC, and MG 9000. When the provisioning data is verified, the DIAG requests the MG 9000 to execute the embedded circuit diagnostics, which will execute the following tests:

- off-hook detection
- on-hook detection
- ringing
- for coin lines: coin collect, coin return, or reverse battery
- for P-phone lines, OPCODE signaling is verified instead of analog signaling

If	Do
the line diagnostic fails	Resolve the issue reported in the diagnostic. If there is still no ringing voltage, go to step 9 .
the line diagnostic passes	step 9

9 Check for ringing voltage at the T/R pair attached to the face plate on the line card.

If	Do
there is no ringing voltage and the line diagnostic passed for the line	Escalate to the next level of support. Go to step 10 .
there is ringing voltage	step 10

10 You have completed this procedure.

Call not completed correctly**Procedure 4 Troubleshooting a call not completed correctly*****At the MAP***

- 1 Use TRAVER to verify translations will correctly route the dialed digits for the line being tested.

If	Do
translations are verified to be correct	step 2
translations are not correct	Escalate to the next level of support. Go to step 6 .

At the customer loop testing OSS

- 2 Perform a detailed loop test to determine if the problem is outside the plant.

If	Do
the fault is outside the plant	Dispatch outside plant personnel. Go to step 6 .
the fault is inside the plant	step 3

At the MAP

- 3** Post the line at the CS 2000 MAP and execute the DIAG command on the line.

Note: The DIAG command verifies the transmission characteristics of the line card and executes the following tests:

- off-hook detection
- on-hook detection
- ringing
- for coin lines: coin collect, coin return, or reverse battery
- for P-phone lines, OPCODE signaling is verified instead of analog signaling
- transhybrid loss
- weighted and notched noise
- padding

If	Do
the diagnostic passes	step 4
the diagnostic fails	Resolve the issue reported in the diagnostic. If the problem is not resolved, go to step 4 .

- 4** Test the line's ability to collect and report digits to the CS 2000.

Note: Use the TALKTA and ORIG commands to simulate a test call. Use these commands to capture and observe any digits actually collected for the line under test.

If	Do
the test passes	step 6
the test fails	step 5

- 5** Manually troubleshoot the line to isolate the problem.

If	Do
manual troubleshooting cannot isolate the problem	Escalate to the next level of support. Go to step 6 .
manual troubleshooting isolates the problem	Resolve the problem. Go to step 6 .

- 6** You have completed this procedure.

P-phone lines not functioning correctly

Procedure 5 Troubleshooting P-phone lines

At the customer loop testing OSS

- 1 Perform a detailed loop test to determine if the problem is outside the plant.

If	Do
the fault is outside the plant	Dispatch outside plant personnel. Go to step 4 .
the fault is inside the plant	step 2

At the MAP

- 2 Post the line at the CS 2000 and execute the DIAG command on the line.

Note: The DIAG command on a P-phone line verifies the provisioning in the CS 2000 matches the set hardware, and it verifies the signaling between the CS 2000, the line card, and the P-phone set. The DIAG command executes the following tests:

- off-hook detection (analog lines)
- on-hook detection (analog lines)
- ringing (analog lines)
- coin collect, coin return, or reverse battery (coin lines)
- OPCODE signaling (P-phone lines)
- transhybrid loss (analog lines)
- weighted and notched noise (analog lines)
- padding (analog lines)

If	Do
the diagnostic passes	step 3
the diagnostic fails	Resolve the problem reported in the diagnostic. If the problem is not resolved, go to step 3 .

On-site

- 3 Execute the station ringer test on-site to verify the P-phone set.

If

the problem is resolved

the problem cannot be isolated

Do

step [4](#)

Escalate to the next level of support. Go to step [4](#).

- 4 You have completed this procedure.

Logs

The following NTPs, available on the Carrier VoIP Networks Solutions collection in Helmsman, provide maintenance-related log information for the CS 2000.

- *DMS-100 Family Lines Maintenance Guide*, 297-1001-594
- *Carrier VoIP Fault Management Log Reference*, NN10275-909

Note: The SN06.2 release introduced log LINE811. Refer to *Carrier VoIP Fault Management Log Reference*, NN10276-909, for information about log LINE811.

OMs

The following NTPs, available on the Carrier VoIP Networks Solutions collection in Helmsman, provide information about OMs:

- *DMS-100 Family Lines Maintenance Guide*, 297-1001-594, provides recommendations for monitoring lines troubles for CS 2000.
- *DMS-100 Family Trunks Maintenance Guide*, 297-1001-595, provides information about CS 2000 OMs for the CS 2000 test equipment.

Lines alarms

The following NTPs, available on the Carrier VoIP Networks Solutions collection in Helmsman, provide information about lines alarms:

- *DMS-100 Family Lines Maintenance Guide*, 297-1001-594, provides recommendations for monitoring lines troubles for CS 2000.
- *DMS-100 Family NA100 Alarm Clearing and Performance Monitoring Procedures*, 297-8001-543, volume 2, provides information about lines alarms clearing procedures.

The SN06.2 release introduced a new alarm for SYSB lines. The SYSB alarm is described in the following sections.

ALMSTAT command

MG 9000 lines support the CS 2000 line failure flags, enabling the ALMSTAT command for MG 9000 lines. The ALMSTAT command allows the user to:

- query the line alarms for an office
- set thresholds for updating office alarms for excessive line failures

ALMSTAT QUERY

AlmStat at the LTP level was changed in SN06.2 to display and modify the threshold of SYSBALARM. Sample output of the ALMSTAT QUERY follows.

OFFICE TOTALS

OFFICE LINE FAILURE TOTALS

	OFFICE CURRENT	OFFICE MINOR	OFFICE MAJOR	OFFICE CRITICAL
Ext Diag Fail (D)	1	10	20	30
Facility Fault (F)	0	10	20	30
Short Diag Fail (S)	0	10	20	30
Needs Ext Diag (N)	0	10	20	30
Set Missing (MSET)	0	10	20	30
Card Missing (MCARD)	7	100	150	200
Shower Queue (QUEUE)	0	100	150	200
Major ICMOLINE(IMAJ)	0	100	150	200
Minor ICMOLINE(IMIN)	0	100	150	200
Loop Sig Set (LSET)	0	100	150	200
Loop Sig Card(LCARD)	0	100	150	200
TCM sync loss (T)	0	100	150	200
Loop Performance (P)	0	100	150	200
Major CPERROR (CMAJ)	0	5	10	15
Minor CPERROR (CMIN)	0	5	10	15
Major RapidMSG(OMAJ)	0	10	20	30
Minor RapidMSG(OMIN)	0	10	20	30
Utility Card (U)	0	100	150	200
State = PLO (PSPD)	6	10	20	30
State = SYSB (SYSB)	6	10	20	30
State = HAZ (HAZARD)	0	0	1	10

ALMSTAT SET

The user can use the ALMSTAT command to set the thresholds for minor, major, and critical office alarms.

For example, in the previous sample output from the ALMSTAT QUERY, the total number of SysB lines in the office is “6.” Use the following command to change the SYSB threshold:

AlmStat SYSB minor_value major_value critical_value

Note 1: The input values must be in ascending order or the command will be rejected. If the user attempts to change the threshold through table OFCVAR, the following warning will be displayed on the MAP: “WARNING: This parameter should only be changed using the AMSTAT command at the LTP.”

Note 2: This alarm can be disabled by changing the threshold to (0 0) through table control on table OFCVAR; however, a warning message will be displayed for this action.

SYSB alarm

The SYSB alarm applies only to Carrier VoIP offices and applies only to Carrier VoIP lines (excluding ABI) in the entire office. The class of the alarm (MINOR, MAJOR, or CRITICAL) is displayed in the system status display area under the Lns header of the mapci;mtc display.

A sample MAP display follows:

```

XAC  MS      IOD  Net  PM   CCS  Lns Trks Ext APPL
.    .      .   .   .   .   LGRP .   .   .
                      *C*

MTC
0 Quit
2
3 MTCNA
4 SRSTATUS
5 BERP
6 CAPACITY
7
8
9 XAC
10 MS
11 IOD
12 Net
13 PM
14 CCS
15 Lns
16 Trks
17 Ext
18 APPL
YD
Time 10:56 >
```

The severity of the alarm is based on alarm thresholds, which are set independently. The new office parameter SYSBALARM will be created in table OFCVAR. The SYSBALARM parameter has a default value {10, 20, 30}, which will be set at IPL time and will survive all restarts.

The following table shows the character display of the multiple alarms that can occur at a given time. The “Multiple alarms” column shows the acronym for the combined alarms. The other five columns indicate with an “X” which components make up the multiple alarm. For example, in the first row, CT SB is a combination of the CUT and SYSB alarms. In the second row, DF SB is a combination of the DF and SYSB alarms, and so on.

Multiple alarms	Cutoff (CUT)	Diagnostic failure (DF)	Hazard (HAZ)	Permanent signal partial dial (PSPD)	System busy (SYSB)
CT SB	X				X
DF SB		X			X
CD SB	X	X			X
HZ SB			X		X
CH SB	X		X		X
DH SB		X	X		X
CDHSB	X	X	X		X
PS SB				X	X
CP SB	X			X	X
DP SB		X			X
CDPSB	X	X		X	X
HP SB			X	X	X
CSPSB	X		X	X	X
DHPSB		X	X	X	X
CDHPS	X	X	X	X	X

PM MAP level for LGRP

The PM subdirectory, LGRP, raises the PM alarm when the number of SysB LGRPs reaches a certain number.

The SYSB alarm is displayed under the PM banner and will be raised when lgrp nodes are in SysB. The state of the posted lgrp is displayed, along with the total number of LGRPs in each state. The following example shows lgrp posted at the PM maintenance level.

```

XAC MS   IOD   Net   PM   CCS   Lns   Trks   Ext   APPL
.   .   .       .   2lgrp .   .   .   .   .
          *C*
LGRP      SysB   ManB   OffL   CBsy   ISTb   InSv
0 Quit          PM      4       0       0       0       0
2 Post_        LGRP    2       0       0       0       0
3 Listset
4          LGRP: LG   00 0       SysB
5
6          POST:
7 Bsy
8 Rts
9 OffL
10
11 Disp_
12 Next
13
14 QueryPM
15
16
17
18
    YD
Time 09:05 Pref>

```

Note 1: The severity of the alarm follows the rules of existing PM alarms. If the number of SysB LGRPs exceeds 10 percent of the total PMs in the office of all types, set the alarm class to CRITICAL. Otherwise, if there is at least one SysB LGRP, set the alarm class to MAJOR. The alarm will be cleared only when the state of all LGRP nodes changes to another state through the Bsy or Offl commands.

Note 2: The commands Bsy, Rts, and Offl can be issued only for the large node lgrp (in other words, only for an S type lgrp).

LGRP commands

The following table describes supported LGRP commands.

Command	Description
Post_	posts the lgrp PM
Bsy	busies the posted lgrp PM Note: The Bsy nowait command is also supported. This command can be issued only in a node state of offline, system busy, or inservice.
Rts	returns the posted lgrp PM to service. This command can be issued only in the ManB state. Note: If a 90-second timeout occurs, a “TIMEOUT on WAIT FOR REPLY FROM GWC” message will be displayed on the MAP and no state change will occur. The following commands are also supported: • Rts force • Rts nowait • Rts force nowait
Offl	takes the posted lgrp to an unequipped state. This command can be issued only in the ManB state. Note: The lgrp node state will be set to OFFFL after node provisioning. The user must perform manual action to bring the node into service.
QueryPM	shows the posted lgrp node data information

The following example shows sample output from the QueryPM command.

```

XAC  MS  IOD  Net      PM      CCS      Lns      Trks      Ext      APPL
.    .    NODLOG .      .      .      .      .      .      .

LGRP
0 Quit  PM      0      0      43      0      1      30
2 Post_ LGRP    0      0      7      0      0      5
3 Listset
4      LGRP: HOST 01 3      OffL
5
6      QueryPM
7 Bsy    PM Type: LGRP  Node_No: 150 INT. No: 0 Office LM:18
Type: S
8 Rts    Cside Host: GWC 0  Node_No: 89      IP: 47.142.92.68
9 OffL   Node_Status      MTC_Node_Status      Callp_Node_Status
10      {OFFL FALSE}      {OFFL FALSE}      {OFFL FALSE}
11 Disp_ Site  Flr      RPos      Bay_id      Shf      Description
12 Next  HOST  1      A 1      MG9F  1      3      LGRP  1 3
13
14 QueryPM
15
16
17
18

YD

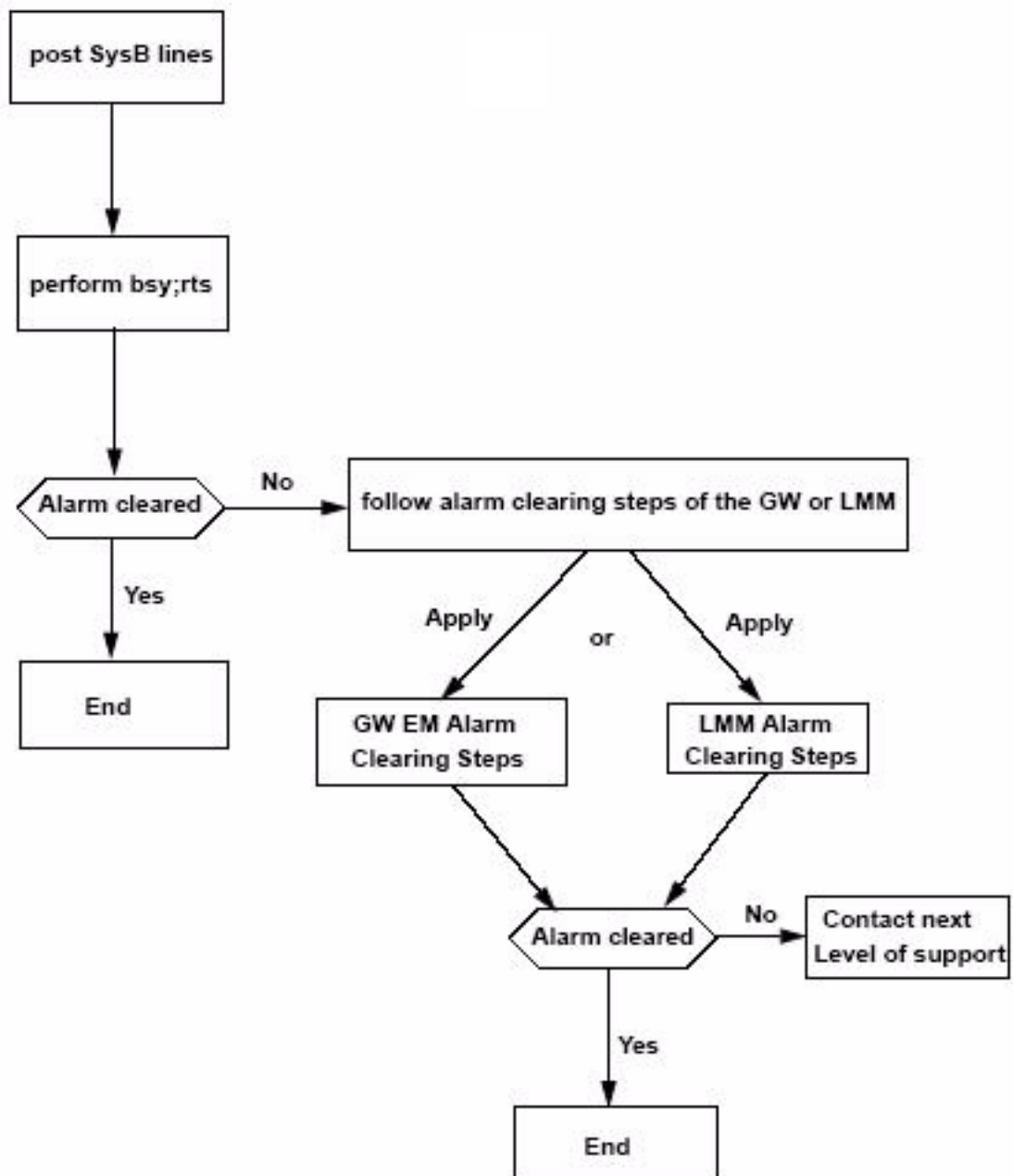
```

Time 14:50 >

Clearing a SysB Ins alarm

Refer to the summary flowchart to clear the SysB Lns alarm.

Summary of clearing a SysB line alarm



Software upgrades for LGRP

The initial LGRP node state will be set to OFFL upon provisioning. Therefore, SWACT applications need to be provided for the following Core upgrades:

- SN07 to SN07 - The InSv state will be transferred to the inactive side during the ONP. The following table shows the pre-SWACT node status check for LGRP.

Active side (state)	Inactive side (states)				
	OFFL	INSV	SYSB	MANB	CSBY
OFFL	match	---	---	---	---
INSV	match	match	---	---	match
other state	---	---	---	---	---
Note: Only entries marked as “match” will pass the pre-SWACT node status check.					

- SN06 to SN07 - In SN06, the initial LGRP node state is InSv or SysB. A patch will be required to bypass the node status check for LGRP so the pre-SWACT will always pass the LGRP node status check.

User error responses

This section describes some of the more common error responses.

Line state errors

When an MG 9000 line is being tested, the line termination is set to the TEST state. If the CS 2000 fails to set the termination to the TEST state, the user receives one of the following error responses described in this section.

Failed to determine the termination state

The CS 2000 failed to determine the current state of the line at the MG 9000. Attempt the test again. If the problem persists, contact the next level of support.

Failed to put the termination in the test state

The CS 2000 requested the MG 9000 to place the line in the TEST state and the request was unsuccessful. Check the state of the line termination in the MG 9000.

Line is an ESA call

The CS 2000 has determined the line is involved in an ESA call.

Line is out of service at the MG 9000

The CS 2000 has determined the line is out of service at the MG 9000. Check the state of the line at the MG 9000 Manager to isolate the fault.

Line test provisioning errors

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

When a line test was attempted on an MG 9000 line, the CS 2000 failed to access the metallic test point provisioning data for the MG 9000 in table LGRPINV. Check the provisioning in table LGRPINV.

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

When a line test was attempted on an MG 9000 line, the CS 2000 failed to access the metallic test point provisioning data for the MG 9000 in table LGRPINV. Check the provisioning in table LGRPINV.

Vertical is not datafilled in MTAVERT; Test cannot be performed

When a line test was attempted on an MG 9000 line, the CS 2000 failed to access the vertical provisioning data for the MG 9000 in table MTAVERT. Check the provisioning in table MTAVERT.

Tools

The No Fault Found (NFF) utility allows the user to capture and query results from individual tests performed during the line diagnostics.

NFF command help reference

The NFF utility is entered by typing NFF at the CS 2000 CI prompt. The following example shows the command help reference.

No Fault Diagnostic (NFF) utility.

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

Valid commands are:

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

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

NFF utility for an MG 9000 line

The following example shows the data provided by the NFF utility for an MG 9000 line.

```
>mapci nodisp;mtc;lms;ltp;post 1 ud17 5 3 2 0
MAPCI:
MTC:
LMS:
LTP:
>nff start sfdev diag1
>diag
RTD ***+LINE100 OCT30 08:52:43 1200 PASS LN_DIAG
      UD17 05 3 02 00      DN 6136211701
      DIAGNOSTIC RESULT Card Diagnostic OK
      ACTION REQUIRED None
      CARD TYPE RDTLSG
>nff stop
NFF stopped
>nff print
No fault found diagnostic result
-
```

Diagnostic intermediate result for LEN: UD17 05 3 02
00 on OCT-30 08:52:33

Transhybrid loss test result:

	304	704	1504	3204	Hz
Max	10	15	15	10	db*10
Actual	-22	-16	-15	-18	db*10
Min	-50	-45	-45	-50	db*10

-

Test pads in line card result:

	304	704	1504	3204	Hz
1 db pad:	-10	-10	-10	-10	db*10
3 db pad:	-30	-30	-30	-30	db*10
7 db pad:	-70	-70	-70	-70	db*10
0 db pad:	0	0	0	0	db*10

-

Noise test result: 56 db*10 noise level

-

Noise test result: 282 db*10 noise level

LGLTT

The LGLTT can be used to clear the failure flag against a defective MG 9000 circuit. To do so, enter the ClrFlag command at the CS 2000 CI prompt, followed by the DN or LEN of the defective circuit. The following example shows the use of this command.

```

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

>quit

```

MTA through NTT provisioning

This section applies to MTA access through NTT and for many MAP tests. Two tables need datafill for NTT and MAP test access to MG 9000. These are LGRPINV and MTAVERT. The data associates MG 9000s and their MTAPTs to MTA verticals. The verticals and MTAPTs must be added to table LGRPINV before the verticals can be provisioned in MTAVERT.

Table LGRPINV

MG 9000 line groups are datafilled in table LGRPINV. If XA-Core-driven MTA access is required for an MG 9000, an MTA option field (MTSTAPT) is added to the table entries for each of the MG 9000 shelves. This option relates 3x09 verticals to the MG 9000 MTAPTs.

TABLE: LGRPINV

GRPNO	SRVRNAME	GRPTYPE	LGRP_OPTS
CO10 07 0	GWC 1 S	(MTSTAPT AAAA (6 1) (7 2) \$) \$	
CO10 07 1	GWC 1 S	(MTSTAPT BBBB (6 1) (7 2) \$) \$	
CO10 07 2	GWC 1 S	(MTSTAPT CO10 (6 1) (7 2) \$) \$	
CO10 07 3	GWC 1 S	(MTSTAPT 07_0 (6 1) (7 2) \$) \$	

The MTSTAPT option format is

```
MTSTAPT <site name> (<MTA Vertical> <MTAPT>) ...
```

The site name is free format, and unused by the Core. Its original purpose was to annotate the entry to indicate which physical MG 9000 the vertical is connected to. All line groups have names that reflect the physical shelf (for example, line group “CO10 07 0” is physically MG 9000 CO10 frame 7 shelf 0), so this field is redundant or can be used for other purposes. One suggested use is to reflect the shelf number of the physical MTAPT, as shown in the fourth entry above.

Table MTAVERT

Table MTAVERT associates MTA verticals with MG 9000 shelves (line groups). In the following example, the new connection identifier G (Group) denotes a group connection which is different than “M” (Multiple) in that it can allow more than one vertical per LCD. Up to eight verticals are allowed per MG 9000. The “O” indicates that odd verticals can be used. Following is sample data-fill for a 4-shelf MG 9000 (CO10) with 2 verticals. This example finishes the datafill started in the example for table LGRPINV.

TABLE: MTAVERT

VERT VERTCONN

```
-----
 6    G (O CO10 07 0 ) (O CO10 07 1 ) (O CO10 07 2 )
(O CO10 07 3 ) $
 7    G (O CO10 07 0 ) (O CO10 07 1 ) (O CO10 07 2 )
(O CO10 07 3 ) $
```

Where G = Group, O = Odd, and “CO10 07 <shelf>” are the VMGs (shelves).

Fault management trunk testing

The following section of fault management deals with trunk testing.

Trunk testing

This section provides information on the trunk tests you can perform in an ATM solution for TDM (time division multiplex) trunks that terminate on the MG 4000. You must perform all the trunk tests described in this section from the trunk maintenance level of the MAP (which you access through the CS 2000 Core Manager).

For more detailed information on trunk testing, see DMS-100 Family Trunks Maintenance Guide, 297-1001-595, on Helmsman.

100 test line (TL100)

The 100 Test line trunk test, also known as a quiet or balanced termination, provides noise and loss measurements. Three versions of the TL100 are present: T100, S100, and N100. Use the T100 when the equipment at the terminating office is unknown. When the T100 test line test is complete, a two second time-out attempts to detect a milliwatt tone. If the time-out does not detect a tone, the S100 version of the test runs. The S100 version provides a quiet termination for noise measurements only. The N100 includes a milliwatt test. You can use the N100 for far-to-near loss measurements. If you know the version of the distant office test line, you can run that version of the test directly. A two second delay for each trunk is not required.

Performing a TL100 trunk test

The following procedure outlines the test sequence for the TL100 trunk test.

Initiating a TL100 trunk test at the originating office

At the system level

- 1 The originating office transmits the test code to the terminating office. The terminating office responds with an off-hook signal when the test code establishes a connection.
- 2 The originating office connects the Transmission Test Trunk (TTT) to the trunk under test.
- 3 The terminating office delays the off-hook signal and the start of the milliwatt test tone by 300 ms.
- 4 The originating office detects the milliwatt test tone and a level meter measures the far-to-near loss. The milliwatt tone is

- present for a maximum of six seconds. The terminating office provides a quiet termination.
- 5 The terminating office maintains the quiet termination for as long as the originating office holds the incoming trunk.
 - 6 The originating office measures noise on the trunk.
 - 7 The originating office sends an on-hook signal to the terminating office to indicate the end of the test, and releases the incoming trunk.

The following MAPCI output demonstrates the activation of the TL100 Trunk test.

```
>MTC;TRKS;TTP
MTC:
TRKS:
SHORT CLLI IS: ATM01S
POSITION RESTARTED
TTP:
>post g ATM01S7ITW2
LAST CKTN = 48
POSTED CKT IDLED
SHORT CLLI IS: ATM01S
OK, CKT POSTED
>tst t100
MSH3_TM03BM ***+ TRK127 NOV 13 13:53:29 8900 PASS
TL100 PASSED
CKT ATM01S7ITW2
TTT = TTT 1 EML = 0.0 DB
F_N DEV = 0.0 DB NOISE = 1.2 DBRN
NML = 50 DBRN NIAL = DBRN
```

101 Test line (TL101)

Use the 101 Test Line trunk test to establish two-way talk between a test position and a trunk (incoming or outgoing). The trunk must associate with the switch (DMS-200). The number of test lines depends on the office size. The operating company assigns the 101 Test Lines in data table TRKGRP.

Terminating a TL101 trunk test

The following procedure outlines the test sequence when the TL101 test call terminates on a switch.

Terminating a TL101 trunk test

At the system level

- 1 The XA-Core or SN70EM receives an incoming 101 test call from a distant office, and a TL101 test trunk.
- 2 The XA-Core or SN70EM applies ringing to all telephone sets connected to that test trunk and returns audible ringing tone to the calling far-end.
- 3 When any of the connected telephone sets go off-hook, the XA-Core or SN70EM removes ringing and audible ringing tone and enters the talking phase.
- 4 If the receiving telephone line is on hold, ring forward applies ringing until the telephone line answers. A flash-hook from the receiving telephone set sends ringing to the calling end.

102 test line (TL102)

The 102 Test line trunk test, also called a milliwatt test line, provides far-to-near transmission loss measurements. The far-end sends a nine second off-hook signal, and applies the milliwatt test tone. An on-hook signal and quiet termination follow the tone. If the far-end is a local office, the test tone repeats in ten second cycles: nine seconds on, and one second off. For a toll office, quiet termination continues until the near-end releases the connection or requests another test cycle. The toll office makes the test cycle request with a ring-forward signal. The milliwatt source levels in use depend on the office type and the trunk group.

Performing a TL102 trunk test

The following procedure outlines the test sequence for the TL102 trunk test.

Originating a TL102 trunk test

At the system level

- 1 The originating office transmits the test code to the terminating office.
- 2 When the test code establishes a connection, the terminating office returns an off-hook signal.
- 3 The originating office connects the DTU (digital test unit) to the trunk under test.
- 4 The terminating office introduces a 300 ms delay, followed by a 1004 Hz milliwatt tone.

- 5 The originating office detects the tone and a level meter measures far-to-near loss.
- 6 The terminating office maintains the tone for nine seconds. After nine seconds the terminating office sends an on-hook signal followed by quiet termination.
- 7 The originating office releases the connection or requests another test sequence through a ring forward signal.

The following MAPCI output demonstrates the activation of the TL102 Trunk test.

```
>MTC;TRKS;TTP
MTC:
TRKS:
SHORT CLLI IS: ATM01S
POSITION RESTARTED
TTP:
>post g ATM01S7ITW2
LAST CKTN = 48
POSTED CKT IDLED
SHORT CLLI IS: ATM01S
OK, CKT POSTED
>tst t102
TEST OK
MSH3_TM03BM ***+ TRK125 NOV13 13:55:43 0800 PASS
TL102 PASSED
CKT ATM01S7ITW2
EML = 0.0 DB F_N DEV = 0.0 DB
```

104 test line (TL104)

The 104 Test line provides:

- measurement of two-way transmission loss
- measurement of far-to-near noise
- a check of near-to-far noise

Performing a TL104 trunk test

The following procedure outlines the test sequence for the TL104 trunk test.

Originating a TL104 trunk test

At the system level

- 1 The originating office transmits the test code, and when the terminating circuit connects, the terminating office responds with an off-hook signal.
- 2 The originating office connects the DTU (digital test unit) to the trunk under test.
- 3 The originating office sends a milliwatt tone for three seconds. The terminating office measures the near-to-far loss.
- 4 The terminating office sends a milliwatt tone for three seconds. The originating office measures the far-to-near loss.
- 5 A delay occurs. The terminating office sends a milliwatt tone for three seconds attenuated by the near-to-far loss measures in [step 3](#). This tone enables the originating office to measure the near-to-far and far-to-near losses.
- 6 Immediately following the attenuated milliwatt tone, the originating office measures the far-to-near noise level. The terminating office measures the near-to-far noise level after two seconds.
- 7 If the near-to-far level exceeds 41 dBm, the terminating office sends a tone at 30 or 120 IPM (impulses per minute).
- 8 The originating office sends on-hook supervision to the terminating office to stop the test.

The following MAPCI output demonstrates the activation of the TL104 Trunk test.

```
>MTC;TRKS;TTP
MTC:
TRKS:
SHORT CLLI IS: ATM01S
POSITION RESTARTED
TTP:
>post g ATM01S7ITW2
LAST CKTN = 48
POSTED CKT IDLED
SHORT CLLI IS: ATM01S
OK, CKT POSTED
>tst t104
TEST OK
MSH3_TM03BM ***+ TRK134 NOV13 13:58:09 7300 PASS
TL104 PASSED
CKT ATM01S7ITW2 1
EML = 0.0 DB F_N DEV = 0.0 DB
N_F DEV = 0.0 DB F_N NOISE = 1 DBRN
NML = 50 DBRN NIAL 50 DBRN
```

105 test line (TL105)

The 105 Test line trunk test provides two-way testing from the originating office. The types of measurement include:

- loss
- noise
- echo return loss
- transmission loss
- singing point return
- high and low frequency measurements

The TL105 tests run automatically. Each designation code causes the system to run a different group of tests. [Table](#) lists the designation codes and associated tests.

TL105 Test combination description (Sheet 1 of 4)

Code	Tests	Description
T105	LSC, L, NSC, RN, N	Loss measurement with self-check at 0 dBm and 1004 Hz. Noise measurement with self-check (quiet termination; C-message filter).
T105	LSC, L, NSC, RN, N	Loss measurement with self-check at 0 dBm and 1004 Hz. Noise measurement with self-check (quiet termination; C-message filter).
TL0N	L, RN, N	Loss measurement at 0 dBm and 1004 Hz. Noise measurement (quiet termination; C-message filter).
TL0S	LSC, L	Loss measurement with self-check at 0dBm and 1004 Hz. Noise measurement (quiet termination, C-message filter).
TL05	L	Loss measurement at 0 dBm and 1004 Hz.
TL165	LSC4, LSC10, LSC28, L4, L10, L28, NTSC, NT	Loss measurement at -16 dBm and 404, 1004 2804 Hz. Noise measurement with self-check (tone at -16dB, 1004 Hz. C-notched filter).

TL105 Test combination description (Sheet 2 of 4)

Code	Tests	Description
TL6N	L4, L10, L28, NT	Loss measurement at –16 dBm and 404, 1004 2804 Hz. Noise measurement (tone, C-notched filter).
TL6S	LSC4, LSC10, LSC28, L4, L10, L28	Loss measurement with self-check –16 dBm and 404, 1004 2804 Hz.
TL65	L4, L10, L28	Loss measurement at –16 dBm and 404, 1004 2804 Hz.
TS05	LSC, NSC	Far-end loss self-check at 1004 Hz, and 0 dBm. Far-end noise self-check (quiet termination, C-message filter).
TS65	LSC4, LSC10, LSC28, NTSC	Far-end loss self-check at –16 dBm and 404, 1004, 2804 Hz.
T5SB	ERLSC, SRLSC, SHISC	Return loss measurement and self-check.
T5BS	ERL, ERLSC, SRLLO, SRLSC, SHI, SHISC	Return loss measurement and self-check.
TERL	ERL	Echo return loss measurement.
T5LH	SRL, SHI	Singing return loss (low and high) measurements.

TL105 Test combination description (Sheet 3 of 4)

Code	Tests	Description
T5AS	LSC, L, NSC, RN, N, ERL, ERLSC, SRLLO, SRLSC, SHI, SHISC	Loss measurement and self-check at 0 dB and 1004 Hz. Noise measurement and self-check (C-message filter). Return loss measurement and self-check.
T5AT	L, RN, N, ERL, SRLLO, SHI	Loss measurement at 0dB and 1004 Hz. Noise measurement (C-message filter). Return loss measurement.
T50L	L, ERL, SRLLO, SHI	Loss measurement at 0dB and 1004 Hz. Return loss measurement.
T56N	L4, L10, L28, NT, ERL, SRLLO, SHI	Loss measurement at -16 dB and 404, 1004 2804 Hz. Noise measurement (C-notched filter). Return loss measurement.
T5LB	L4,10, L28, ERL, SRLLO, SHI	Loss measurement at -16 dB and 404, 1004 2804 Hz. Return loss measurement.

TL105 Test combination description (Sheet 4 of 4)

Code	Tests	Description
TSBS	LSC, NTSC, SRLSC, SHISC	Loss self-check at –16 dB and 404, 1004 2804 Hz. Noise self-check (C-notched filter). Return loss self-check.
TSBT	ERL, SRLLO, SHI	Return loss measurement.

The system groups tests in layers, named layer 2 or layer 3. Each test has an associated Multi-Frequency (MF) digit, but two tests in different layers can share the same MF digit. The MF transmits with you request a test. Another MF digit, known as a “layer change request” digit (1100/1700 Hz) goes before a request for a test in layer 3. If this digit is not present, the system selects the associated test in layer 2 by default. [Table](#) lists the individual tests with their associated layers and MF digits.

A Noise Metering Set (NMS) reads noise levels. Noise passes through a C-message filter before measurement. The filter reads the noise as C-level noise. For trunks on a carrier that compresses and expands signals, a 1004 Hz tone is transmitted over the trunk with the NMS measurements. A C-notch filter filters out the tone, and reads the noise as C-notch noise. See [Table](#) and [Table](#) for tests that use these filters.

Test and layer format description (Sheet 1 of 3)

Test	Layer	MF digit	MF Frequency	Test description
ERL	2	C	700/1700	Echo return loss measurement with quiet termination
ERLSC	3	A, C	700/1700	Echo return loss self-check with quiet termination
L	2	2	700/1100	Two-way loss measurement at 0 dBm and 1004 Hz.

Test and layer format description (Sheet 2 of 3)

Test	Layer	MF digit	MF Frequency	Test description
LA	2	6	1100/1300	Two-way loss measurement at –16 dBm and 404 Hz.
L10	2	C	1500/1700	Two-way loss measurement at –16 dBm and 1004 Hz.
L28	2	E	1300/1700	Two-way loss measurement at –16 dBm and 2804 Hz.
LSC	2	1	700/900	Far-end loss self-check at 0 dBm and 1004 Hz.
LSC4	3	6	1100/1300	Far-end loss self-check at –16 dBm and 404 Hz.
LSC10	3	c	1500/1700	Far-end loss self-check at –16 dBm and 1004 Hz.
LSC28	3	E	1300/1700	Far-en loss self-check at --16 dBm and 2804 Hz.
N	2	3	900/1100	Far-end noise measurement with C-message filter.
NSC	2	4	700/1300	Far-end noise self-check with C-message filter.
NT	2	F	700/1700	Two-way noise tone measurement with C-notched filter.
NTSC	3	F	700/1700	Far-end noise/tone self check with C-notched filter at –16 dBm and 1004 Hz.
RN	2	A	1300/1500	Near-end noise measurement with C-message filter. Filter at –16 dBm and 1004 Hz tone.
SHI	3	2	700/1100	High frequency singing return loss measurement with quiet termination.
SHISC	3	A, 1	700/900	High frequency singing return loss self-check with quiet termination.

Test and layer format description (Sheet 3 of 3)

Test	Layer	MF digit	MF Frequency	Test description
SRLHI	3	A, 2	2200/3400	High frequency singing return loss with quiet termination.
SRLLO	2	8	900/1500	Low frequency singing return loss measurement with quiet termination.
SRLSC	3	A, 8	900/1500	Low frequency singing return loss self-check with quiet termination.

Performing a TL105 trunk test

The following procedure outlines the test sequence for the TL105 trunk test.

Originating a TL105 trunk test***At the system level***

- 1 The originating office transmits the number, that is assigned to the TL105 test line in the terminating office.
- 2 After the terminating office receives this assigned number, the terminating TL105 test line connects to the incoming trunk. The terminating TL105 test line sends a 2225 Hz Test Progress Tone (TPT) to the originating end.
- 3 The originating office connects the DTU (digital test unit) to the trunk under test.
- 4 When the terminating office is ready to start the test, the terminating office removes the Test Progress Tone (TPT).
- 5 The originating office detects the removal on the TPT and starts with the requested group of tests. The tests run in the following order.
 - loss self-checks
 - loss measurements
 - noise self-checks
 - noise measurements
 - Echo-return losses

Note: The specified group of tests does not affect this sequence. A request sent to the far end starts each test. The request is one or two MF digits.

The following MAPCI output demonstrates the activation of the TL105 Trunk test.

```
>MTC;TRKS;TTP
MTC:
TRKS:
SHORT CLLI IS: ATM01S
POSITION RESTARTED
TTP:
>post g ATM01S7ITW2
LAST CKTN = 48
POSTED CKT IDLED
SHORT CLLI IS: ATM01S
OK, CKT POSTED
>tst t105
TEST OK
MSH3_TM03BM ***+ TRK172 NOV13 13:59:29 7300 PASS
TL105 PASSED
CKT ATM01S7ITW2 1
LOSS MEAS AT 0 DB 1003 HZ EML = 0.0
FN_DEV = 0.0 NF_DEV = 0.-1 DB
NOISE MEAS C-MESSAGE. NML = 50 NIAL = 50 DBRN
FN_NSE = 1 NF_NSE = 16 DBRN
```

108 test line (TL108)

The 108 Test line is a disable method for accessing the dialed loopback on trunks feature known as TRKLBPBK. TL108 can be used to isolate trunk troubles and to measure net loss, noise and run BERT (bit error rate test) for trunks at the DS0 rate.

Performing a TL108 trunk test

The following procedure outlines the test sequence for the TL108 trunk test.

Originating a TL108 trunk test

At the system level

- 1 The originating toll office connects the ESMS (Echo Suppressor Measuring Set) and seizes an outgoing intertoll trunk.

- 2** After the originating office seizes the trunk, the originating office dials a T108 Test Line code. The seized trunk is the trunk under test.
- 3** The terminating office translates the T108 Test Line code and connects the incoming trunk to test Port-0 of the T108 Test Line. The terminating office uses a 1kHz tone to calibrate the ESMS. The terminating office sends the tone to the originating office.
- 4** The originating office seizes another outgoing trunk, called the auxiliary trunk and dials the T108 Test Line code again.
- 5** The terminating office translates the T108 code and connects the auxiliary trunk to test Port-1 of the T108 Test Line. The terminating office cuts off the 1 kHz tone and establishes a connection to Port-0.
- 6** When the terminating office establishes a connection, the originating office transmits a 1 kHz tone on the auxiliary trunk. This tone passes through the T108 Test Line, back over the trunk under test. The tone completes the calibration of the ESMS. The office uses the Auxiliary trunk as a reference trunk for later tests of echo suppressors.
- 7** When tests on the trunk under test complete, the originating office releases the trunk under test. The originating office seizes the next trunk for test, dials the T108 Test Line code over this trunk. When all tests are complete, the originating office goes on-hook on both the trunk under test, and the auxiliary trunk. The terminating office releases (idles) the T108 Test Line termination set.

The following MAPCI output demonstrates the activation of the TL108 Trunk test.

```
>MTC;TRKS;TTP
MTC:
TRKS:
SHORT CLLI IS: ATM57S
POSITION RESTARTED
TTP:
>datattp
DATATTP:
>bterm dig 2349002
Information registered
BERT termination : DIGITS : 2349002
It will be used on next BERT test request
>bert start 56 p511
BERT test time : No time specified - forever
BERT termination : DIGITS : 2349002
BERT test started
>bert stop
BERT test stopped
```

ISUP continuity test (ICOT)

The ISUP continuity test validates the datafill and speech path for trunks that use CCS7 signaling.

Performing an ISUP continuity test

The following procedure outlines the steps you must perform from the MAP (maintenance and administration position) to perform an ISUP continuity test on a trunk.

Running an ISUP continuity test

At the MAPCI;MTC;TRKS;TTP level of the MAP

- 1 Post the trunk you wish to test.

Example

```
post g ATM01S7ITW2
```

```
LAST CKTN = 48
POSTED CKT IDLED
SHORT CLLI IS: ATM01S
OK, CKT POSTED
```

- 2 Test the trunk for continuity.

Example

```
tst icot
```

```
TEST OK
```

CVTEST

The CVTest verifies trunk datafill parameters including glare. The CVTest command is found at the C7TTP MAP level. The CVTest performs a circuit validation test on the posted ISUP trunk. The test verifies that the circuit group characteristics pertaining to the trunk are datafilled consistently at the two connected offices. The CVTest checks the compatibility of the datafill for the glare resolution methods, found in the GLARETYP field of table TRKSGRP.

Performing a CVTest

The following procedure outlines the steps you must perform from the MAP (maintenance and administration position) to perform a CVTest on an ISUP trunk.

Running an CVTest

At the MAPCI;MTC;TRKS;TTP;C7TTP level of the MAP

- 1 Post the trunk you wish to test.

Example

```
post g ATM01S7ITW2
```

```
LAST CKTN = 48  
POSTED CKT IDLED  
SHORT CLLI IS: ATM01S  
OK, CKT POSTED
```

- 2 Run the CVTest.

Example

```
cvtest
```

```
SUCCEEDED, GLARE control data compatible with  
remote office.
```

QRYSIG

The QRYSIG test displays the signaling status of the posted CCS7 trunk.

Performing a QRYSIG test

The following procedure outlines the steps you must perform from the MAP to perform a QRYSIG test on an ISUP trunk.

Running an QRYSIG test***At the MAPCI;MTC;TRKS;TTP;C7TTP level of the MAP***

- 1 Post the trunk you wish to test.

Example

```
post g ATM01S7ITW2
```

```
LAST CKTN = 48  
POSTED CKT IDLED  
SHORT CLLI IS: ATM01S  
OK, CKT POSTED
```

- 2 Run the QRYSIG test.

Example

```
qrsig
```

```
Signaling Available
```

TRKQRY

The TRKQRY test displays the local or remote status of the posted trunk.

Performing a TRKQRY test

The following procedure outlines the steps you must perform from the MAP to perform a TRKQRY on an ISUP trunk.

Running an TRKQRY test***At the MAPCI;MTC;TRKS;TTP;C7TTP level of the MAP***

- 1 Post the trunk you wish to test.

Example

```
post g ATM01S7ITW2
```

```
LAST CKTN = 48  
POSTED CKT IDLED  
SHORT CLLI IS: ATM01S  
OK, CKT POSTED
```

- 2 Run the TRKQRY test.

Example

```
>trkqry
```

Local Trunk State: IDLE, LOCALLY AND REMOTELY
BLOCKED
Remote Trunk State: IDLE, LOCALLY AND REMOTELY
BLOCKED
States are compatible - No (protocol) action
required

Logs and operational measurements supported by CEM

Logs

For logs generated by the core and sent to the CEM and then to the Integrated EMS, see the following table.

Log numbers	Documentation reference
ESA120, ESA121	<i>North American DMS-100 Log Report Reference Manual, 297-8021-840</i>
ATM300, ATM301, ATM501, ATM600, ATM605	<i>North American DMS-100 Log Report Reference Manual, 297-8021-840</i>
XPKT806, XPKT807	<i>Carrier VoIP Fault Management Logs Reference, NN10275-909</i>
BITS300, BITS310, BITS500, BITS600, BITS601, BITS610	<i>Carrier VoIP Fault Management Logs Reference, NN10275-909</i>
BOOT101	<i>North American DMS-100 Log Report Reference Manual, 297-8021-840</i>
C7UP104, C7UP109, C7UP113, C7UP114, C7UP120, C7UP130, C7UP310	<i>CDMA/TDMA Logs Reference Manual, 411-2131-510</i>
CARR300, CARR310, CARR320, CARR330, CARR331, CARR340, CARR341, CARR500, CARR501, CARR510, CARR511, CARR512, CARR800, CARR801, CARR811	<i>CDMA/TDMA Logs Reference Manual, 411-2131-510</i>
CCMT301, CCMT501, CCMT502, CCMT601	<i>North American DMS-100 Log Report Reference Manual, 297-8021-840</i>

Log numbers	Documentation reference
DPTM500, DPTM501, DPTM502, DPTM503, DPTM504, DPTM550, DPTM560, DPTM700, DPTM701	<i>North American DMS-100 Log Report Reference Manual, 297-8021-840</i>
ENET308, ENET311	<i>North American DMS-100 Log Report Reference Manual, 297-8021-840</i>
EXT102, EXT108	<i>North American DMS-100 Log Report Reference Manual, 297-8021-840</i>
IWBm500, IWBm501, IWBm603, IWBm800, IWBm801, IWBm802, IWBm803	<i>Carrier VoIP Fault Management Logs Reference, NN10275-909</i>
LINK300	<i>Carrier VoIP Fault Management Logs Reference, NN10275-909</i>
NODE300, NODE303, NODE323, NODE326, NODE450, NODE500, NODE600	<i>GSM NSS/UMTS VCN OAM Reference Manual, 411-8111-511</i>
	<i>Carrier VoIP Fault Management Logs Reference, NN10275-909</i>
SDM300, SDM301, SDM302, SDM303, SDM306, SDM308, SDM309, SDM314, SDM315, SDM317, SDM321, SDM327, SDM500, SDM501, SDM502, SDM503, SDM504, SDM505, SDM550, SDM600, SDM601, SDM602, SDM603, SDM604, SDM608, SDM609, SDM617, SDM621, SDM627, SDM630, SDM650, SDM700	<i>Carrier VoIP Fault Management Logs Reference, NN10275-909</i>

Log numbers	Documentation reference
SDMB300, SDMB310, SDMB315, SDMB316, SDMB320, SDMB321, SDMB330, SDMB350, SDMB355, SDMB360, SDMB365, SDMB367, SDMB375, SDMB380, SDMB390, SDMB400, SDMB530, SDMB531, SDMB550, SDMB600, SDMB610, SDMB615, SDMB620, SDMB621, SDMB625, SDMB650, SDMB655, SDMB660, SDMB675, SDMB680, SDMB820	<i>Carrier VoIP Fault Management Logs Reference,</i> NN10275-909
SOS701, SOS702, SOS703	<i>XA-Core Reference Manual,</i> 297-8991-810
SPM301, SPM310, SPM311, SPM312, SPM313, SPM314, SPM330, SPM331, SPM332, SPM334, SPM335, SPM336, SPM337, SPM338, SPM339, SPM340, SPM341, SPM342, SPM344, SPM350, SPM352, SPM353, SPM352, SPM355, SPM356, SPM357, SPM370, SPM370, SPM399, SPM500, SPM501, SPM510, SPM600, SPM619, SPM630, SPM637, SPM638, SPM641, SPM642, SPM644, SPM650, SPM651, SPM652, SPM653, SPM654, SPM655, SPM656, SPM657, SPM658, SPM660, SPM661, SPM625, SPM670, SPM700, SPM701, SPM702, SPM703, SPM704, SPM705, SPM706, SPM707, SPM708, SPM709, SPM710	<i>Carrier VoIP Fault Management Logs Reference,</i> NN10275-909
TMN301, TMN302, TMN304, TMN303, TMN304, TMN309, TMN311, TMN600, TMN601, TMN604, TMN605	<i>Carrier VoIP Fault Management Logs Reference,</i> NN10275-909
TRK882	<i>North American DMS-100 Log Report Reference Manual,</i> 297-8021-840

Log numbers	Documentation reference
XAC300, XAC302, XAC303, XAC304, XAC305, XAC306, XAC307, XAC308, XAC309, XAC310, XAC312, XAC320, XAC321, XAC322, XAC323, XAC324, XAC325, XAC326, XAC327, XAC329, XAC330, XAC333, XAC400, XAC413, XAC415, XAC418, XAC420, XAC600, XAC601, XAC602, XAC603, XAC604, XAC605, XAC606, XAC607, XAC608, XAC609, XAC610, XAC612, XAC613, XAC614, XAC615, XAC618, XAC619, XAC620, XAC622, XAC623, XAC624, XAC625, XAC626, XAC627, XAC628, XAC629, XAC630, XAC631, XAC632, XAC633, XAC634, XAC635, XAC640, XAC641, XAC801, XAC814	<i>XA-Core Reference Manual</i> , 297-8991-810
XACP300, XACP500, XACP600	<i>XA-Core Reference Manual</i> , 297-8991-810

Log reports CSEM300 and CSEM600

Log reports CSEM300 and CSEM600 address a change of format for northbound events on the log feeds of Integrated EMS when used in conjunction with CEM. Log reports CSEM300 and CSEM600 act as an envelope to contain Communication Server 2000 (CS 2000) and SuperNode Data Manager (SDM) logs. The logs in Integrated EMS are encapsulated inside the log reports CSEM300 and CSEM600 in the northbound NT STD and SCC2 feeds. Log report CSEM300 indicates alarm sets and alarm clears for these logs. Log report CSEM600 indicates INFO and unmapped logs for these logs.

Log numbers	Documentation reference
CSEM300, CSEM600	<i>Carrier VoIP Fault Management Logs Reference</i> , NN10275-909

Suppressed logs

When the Store and Forward service is enabled, the logs in the following table are disabled at the Core for the SDM/CBM log stream. These logs are not available through the Log Delivery application. For the procedure to unsuppress these logs, refer to “Changing the set of

logs sent from the CM” in *CS 2000 Core Manager Fault Management*, NN10082-911.

Suppressed logs

Logs that are DELREPEd by the SAF service at the Core

AUTH, CAFT, CALM, CDPD, CHIP, CLFL, CPER, CPRT, CTID, DEPS, DFA, DIM, DROP, ERV, ESNF, FCEL, FRAU, FRS, GAME, 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, RSSI, SMO, SMS, SMT, SPRF, SSR, TIER, TUPL, X75

Operational Measurements

For performance management functionality, all of CS 2000 OMs are supported. OM groups can be selected and exported in tab delimited format or switch format.

For details of CS 2000 OMs that are available through the CEM interface, refer to the following documents:

- *XA-Core Reference Manual*, 297-8991-810
- *DMS-SPM Feature Description Reference Manual*, 297-1771-330
- *DMS-100 Family Extended Peripheral Module Operational Measurements Reference Manual*, 297-8321-814
- *DMS-GSP Operational Measurements Reference Manual*, 297-2651-814
- *DMS SuperNode Signaling Transfer Point Operational Measurements Reference Manual*, 297-8101-814
- *DMS SuperNode STP/SSP Integrated Node Operational Measurements Reference Manual*, 297-8083-814
- *Carrier VoIP Performance Management Operational Measurements Reference*, NN10264-709

Preventative maintenance for CVoIP components

This section provides a list of procedures used to perform preventative maintenance for CVoIP components. Preventative maintenance is required on components to prevent service-impacting fault conditions. The procedures are divided into the following categories:

- [Tasks to be performed daily](#)
- [Tasks to be performed weekly](#)
- [Tasks to be performed monthly](#)
- [Tasks to be performed per office schedule or as required](#)
- [Backup and restore](#)

Tasks to be performed daily

Component	Task	Document	Notes
GWC	Monitor for alarms and check that functions continue without interruptions	<i>GWC Fault Management, NN10090-911</i>	
Media Server 2000 series	Monitor alarms	<i>Media Server 2000 Series Fault Management, NN10328-911</i>	
Passport 8600	Monitor alarms and LEDs	<i>Passport 8010co Chassis hardware components, 312746-B</i>	
Multiservice Switch/Media Gateway 7400/15000	Monitor alarms	<i>Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting, NN10600-520</i>	
Multiservice Switch/Media Gateway 15000	Monitoring equipment status LEDs	<i>Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade, NN10600-130</i>	

Tasks to be performed daily

Component	Task	Document	Notes
Multiservice Switch 7400/15000	Monitoring ATM services	<i>Nortel Networks Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management,</i> NN10600-715	
Multiservice Switch/Media Gateway 15000 or 7400	Using status indicator LEDs and sounds	<i>Nortel Networks Multiservice Switch 15000/20000 Hardware Description,</i> NN10600-120	
SAM21 SC	Monitor alarms and check that functions continue without interruptions	<i>SAM21 Shelf Controller Fault Management,</i> NN10089-911	
Session Server	Monitor alarms and logs	<i>Session Server Fault Management,</i> NN10332-911	
UAS	Monitor alarms	<i>UAS Fault Management,</i> NN10073-911	
XA-Core	Monitor alarms	<i>CS 2000 Fault Management,</i> NN10083-911	

Tasks to be performed weekly

Component	Task	Document	Notes
GWC	Inspect the LEDs on all GWC cards in your system to ensure there are no faults and that all cards appear to be functioning properly.	<i>GWC Fault Management</i> , NN10090-911	
Session Server	Inspect the LEDs front panel of both units and ensure there are no faults indicated.	HP Carrier-Grade Server cc3310 Product Guide, HP part number: cc3310_Product	acquire HP guide from HP.com website
USP	Visually inspect the LEDs	<i>USP Security and Administration</i> , NN10159-611	

Tasks to be performed monthly

Component	Task	Document	Notes
XA-Core/Call Agent	Perform LED maintenance	<i>XA-Core Maintenance Manual</i> , 297-8991-510	

Tasks to be performed per office schedule or as required

Component	Task	Document	Notes
Contivity VPN Switch	Saving current system configuration	<i>Reference for the Contivity VPN Switch</i> , 311643-D	perform immediately upon completion of the configuration or when changes are made to the configuration/firmware

Tasks to be performed per office schedule or as required

Component	Task	Document	Notes
Contivity VPN Switch	Performing file maintenance	<i>Reference for the Contivity VPN Switch, 311643-D</i>	perform immediately upon completion of the configuration or when changes are made to the configuration/firmware
Contivity VPN Switch	Creating a recovery disk	<i>Reference for the Contivity VPN Switch, 311643-D</i>	perform immediately upon completion of the configuration or when changes are made to the configuration/firmware
Core Billing Manager	Monitor log files in the /var/adm directory for system or security abnormalities	no formal procedure required	as part of scheduled maintenance
CS 2000 Core Manager	Monitor log files in the /var/adm directory for system or security abnormalities	no formal procedure required	as part of scheduled maintenance
GWC	Configure a recurring data integrity audit	<i>GWC Configuration Management, NN10205-511</i>	includes Line, Trunk, V5.2, and CS 2000 data integrity audits
GWC	Take a manual software image	<i>GWC Upgrades, NN10068-461</i>	should be taken after patches have been applied

Tasks to be performed per office schedule or as required

Component	Task	Document	Notes
GWC	Retreive GWC services alarm history	<i>GWC Fault Management</i> , NN10090-911	
GWC	Retrieve and correlate GWC PM logs	<i>GWC Fault Management</i> , NN10090-911	
GWC	Retrieve and correlate Syslog logs	<i>GWC Fault Management</i> , NN10090-911	
Preside MDM	Clean up accumulated log files	<i>Preside MDM Administrator Guide</i> , 241-6001-303	This procedure is not normally necessary because there is one log file for each day of the week and information can only accumulate in a log file for a one week period, then the file is automatically overwritten. Should it become necessary, there are two ways to clean up current log files: manually by entering a command, or automatically by running the command as a cron job

Tasks to be performed per office schedule or as required

Component	Task	Document	Notes
Session Server	Monitor GWC logs to verify connectivity has not been lost with the Session Server and to identify any call processing problems.	<i>GWC Fault Management</i> , NN10090-911	Schedule can be adjusted to correspond with GWC log monitoring schedule.
Session Server	Monitor Core Logs to verify that DPT trunks do not unexpectedly go out of service. Each outage should have corresponding logs in the Session Server to explain why. The lack of corresponding Session Server logs indicates a problem.	<i>CS 2000 Fault Management</i> , NN10083-911	Schedule can be adjusted to correspond to XA-Core log monitoring schedule.
Session Server	Monitor alarms and logs	<i>Session Server Fault Management</i> , NN10332-911	
XA-Core/Call Agent	Create a test volume on disks	<i>XA-Core Maintenance Manual</i> , 297-8991-510	perform after installation of new disk in disk drive packlet in the IOP card
XA-Core/Call Agent	Create volumes on disks	<i>XA-Core Maintenance Manual</i> , 297-8991-510	perform on an unformatted or earlier formatted disk, or perform after installation of the disk in the disk drive packlet in the IOP card

Backup and restore

For component-level backup and restore procedures, refer *ATM/IP Administration and Security*, NN10402-600.

Upgrade rollbacks

This section contains software rollback procedures for the Ethernet Routing Switch 8600 and the CS 2000 Management Tools.

Rolling Back the Ethernet Routing Switch 8600 Software for CS-LAN

Introduction

This procedure rolls back software upgrades to Ethernet Routing Switch 8600 (formerly known as the “Passport 8600”) pairs that support the Carrier Voice over IP (VoIP) Communication Server LAN (CS-LAN). The rollback uses a phased approach to prevent service interruption.

Note: Refer to NTP “Upgrading a Carrier Voice over IP Network,” NN10440-450, for procedure “Upgrading the Ethernet Routing Switch 8600 Software for the CS-LAN.”

ATTENTION

Nortel urges users of this rollback procedure to read thoroughly this Introduction, especially [Important rollback considerations](#) before attempting procedure [Rolling Back Software Upgrades on Ethernet Routing Switch 8600s Supporting CS-LANs](#).

What’s new in this release

This section highlights the functionality introduced in this release.

- Beginning with release (I)SN08, the following branding conventions appear in this procedure:
 - “Ethernet Routing Switch 8600” replaces “Passport 8600.”
 - “Carrier VoIP” replaces “Succession.”
- Added Trimodal support options.
- Added new USPc GUI information.
- Added Geographic Survivability impacts involving MS 2000 Series node, Call Agent, and STORM servers.
- Added steps addressing the RTP Media Portal, whereby the portal must be shut down gracefully to prevent it from accepting service requests during an Ethernet Routing Switch 8600 upgrade.

Important rollback considerations



CAUTION

Manually entered configuration changes executed since the completion of an Ethernet Routing Switch 8600 upgrade are lost when rolling back to version 3.7.0.0.

Nortel strongly recommends re-entering configuration changes after the completion of the rollback procedure.

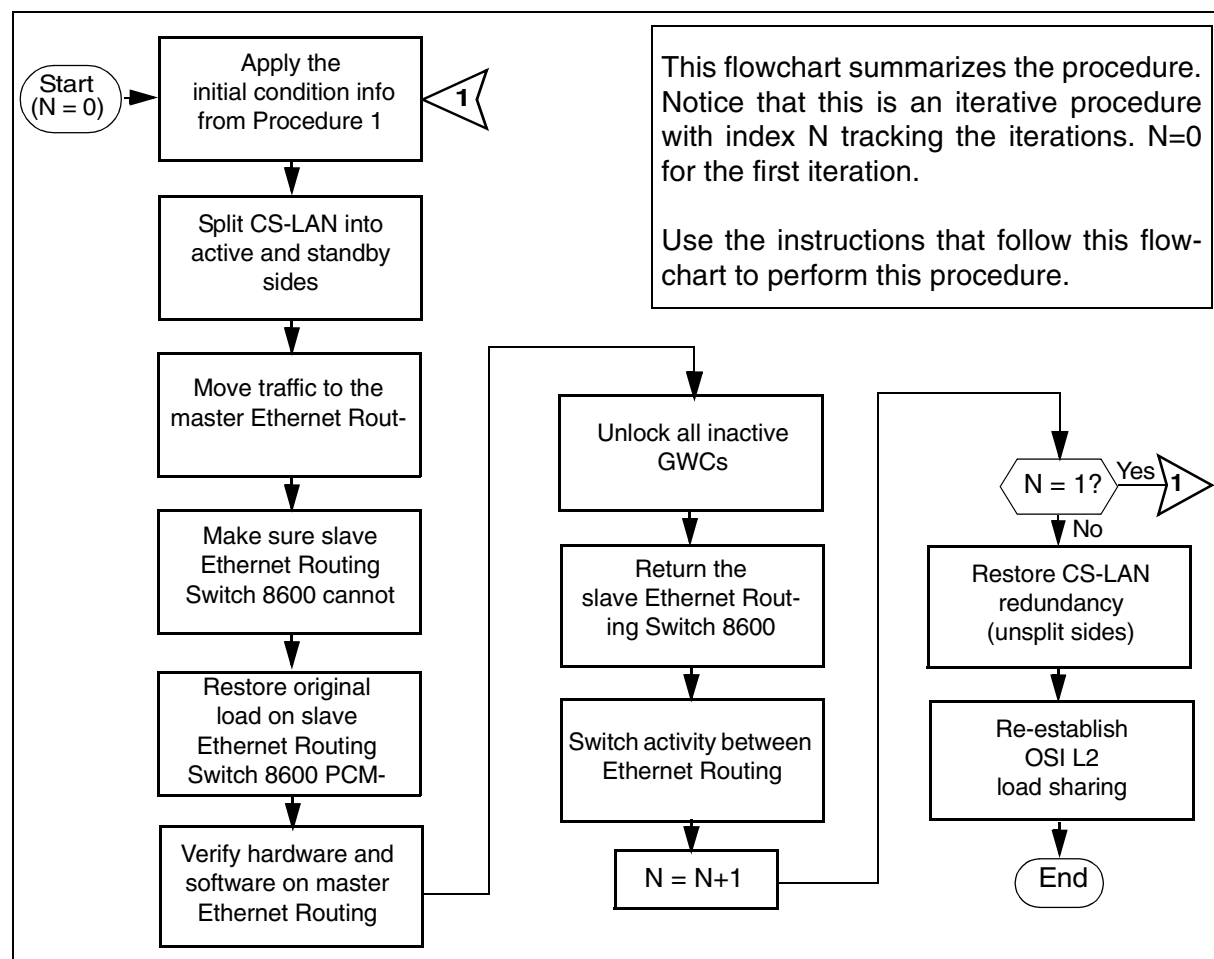
This rollback procedure addresses Ethernet Routing Switch 8600 configurations with dual call processing units (CPU). Therefore, execute all CPU-related commands on the master CPU, except where otherwise noted. Also an Ethernet Routing Switch 8600 must be running with a v3.7.0.0 software load *before* a dual CPU with a high-availability (HA) mode is configured for it.

Note: Also, if rolling back to pre-v3.7.0.0 software version after having attempted a v3.7.0.0 software upgrade for a dual CPU configuration, users must disable the dual CPU HA flag setting *before* the rollback begins.

Also refer to sub-section [Text conventions](#) for brief descriptions and examples of filenames that appear in commands throughout this procedure. This subsection also includes descriptions for distinguishing between the master and standby CPUs in the command line interface (CLI).

The following flowchart summarizes the Ethernet Routing Switch 8600 rollback procedure.

Rolling back a software upgrade on Ethernet Routing Switch 8600s for the CS-LAN



Text conventions

This procedure uses the following text conventions for displaying filenames that appear in commands.

Note: Refer to this section, as needed throughout the course of the upgrade and rollback procedures, for clarifications on the different software files.

<a.b.c.d>

is the IP address of the TFTP server

<bootbkup>

is the name of the backup copy of the boot configuration file on the PCMCIA card

<cfgbkup>

is the name of the backup copy of the software configuration file on the PCMCIA card

<new3DES>

is the name of the new Triple data encryption standard (3DES) file on the PCMCIA card

for example:

p80cXXX.img

where:

cXXX is the release number

<newATM>

is the name of the new ATM load file on the PCMCIA card

for example:

p80tXXXX.dld

where:

XXXX is the release number of the load

<newboot>

is the name of the new boot monitor image file on the PCMCIA card

for example:

p80bXXXX.img

where:

XXXX is the release number of the load (for example, p80b3320.img)

Note: Use the boot monitor image file when executing a boot command.

<newDES>

is the name of the new data encryption standard (DES) file on the PCMCIA card

for example:

p80cXXX.des

where:

cXXX is the release number

<newload>

is the name of the new software image file on the PCMCIA card

for example:

p80aXXXX.img

where:

XXXX is the version of the software (for example, p80a3320)

Note: Use the primary or secondary (or both) software image files when configuring a bootconfig command.

<old3DES>

is the name of the original DES file

for example:

p80cXXX.img

where:

cXXX is the release number

<oldATM>

is the name of the original ATM load file

for example:

p80tXXXX.dld

where:

XXXX is the release number of the load

<oldboot>

is the name of the original boot monitor image file

for example:

p80bXXXX.img

where:

XXXX is the release number of the load (for example, p80b3320.img)

<oldDES>

is the name of the original DES file

for example:

p80cXXX.des

where:

cXXX is the release number

<oldload>

is the name of the original software image file

for example:

p80aXXXX.img

where:

XXXX is the version of the software (for example, p80a3320)

<slot>

is the slot number for the Ethernet Routing Switch 8600

<sonetif >

is the Sonet interface on the ATM blade

<swloadbkup>

is the name of the backup version of the software image file

for example:

p80aXXXX.img

where:

XXXX is the version of the software (for example, p80a3320)

<vid>

is the identifier of each virtual local area network (VLAN)

<vrid>

is the VRRP identifier

CPU syntax

The CLI prompt syntax for the CPUs is as follows:

<Ethernet_Routing_Switch_8600_chassis_name>:CPU-slot#

where:

the absence or inclusion of the “@” symbol at the beginning of the command syntax identifies the master or standby CPU, respectively.

8600_04:5#

refers to the master CPU

@8600_04:6#

refers to the standby CPU

DNS entries

Due to the implementation of domain name service (DNS), the peer command option is not available unless you add the peer IP address in a new file called flash/etc/hosts.

You must create this file. No default file exists. Use a simple text editor to create it, similar to the text editor provided by the Ethernet Routing Switch 8600.

The following figure shows a sample of flash/etc/hosts file.

Sample flash/etc/hosts file of CPU in slot 5

```
198.202.188.44 inthp04.labpc.ernet.in labpc
206.236.134.194 inthp04.labpc1.ernet.in lacpc
198.202.188.174 ipksun05.accelar.wall.com ipksun05
198.202.188.34 dhcp.accelar.wall.com dhcpserver
127.0.0.6 peer cpuslot6
```

In the figure, the peer address corresponds to 127.0.0.6 for the CPU in slot 5. For the CPU in slot 6, the peer address would correspond to 127.0.0.5.

Note: To swap the CPU from slot 5 to slot 6, manually modify the address in the file.

Procedure

Use this procedure to roll back the software of an Ethernet Routing Switch 8600 to a previous release.

Rolling Back Software Upgrades on Ethernet Routing Switch 8600s Supporting CS-LANs

ATTENTION

This rollback procedure assumes that procedure [Upgrading Ethernet Routing Switch 8600 Software for the CS-LAN](#) was aborted after some stage of progress. This procedure further assumes that steps 1 through 9 of the Ethernet Routing Switch 8600 upgrade procedure were completed successfully.

Refer to NTP “Upgrading a Carrier Voice over IP Network,” NN10440-450, for procedure “Upgrading the Ethernet Routing Switch 8600 Software for the CS-LAN.”

Refer to [Procedure Upgrading Ethernet Routing Switch 8600 software for the CS-LAN](#).

- 1 This procedure is iterative (iteration index is N). Use the conventions defined in the following table to complete this procedure.

Iteration	Slave Ethernet Routing Switch 8600	Master Ethernet Routing Switch 8600
First Pass	Chassis N = 0	Chassis X = 1
Second Pass	Chassis N = 1	Chassis X = 0

- 2 Refer to [step 5](#) in [Upgrading Ethernet Routing Switch 8600 software for the CS-LAN](#) and reproduce the **VID (P/V)**, **VRID**,

OSPF, and **PRIO** information for Ethernet Routing Switch 8600 Chassis 0 and 1 in the following table.

Ethernet Routing Switch 8600 - Initial conditions

Status					
VID (P/V)	VRID	Chassis 0		Chassis 1	
		OSPF Metric	VRRP PRIO	OSPF Metric	VRRP PRIO
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Note: As Ethernet Routing Switch 8600 does not carry call processing traffic in the PT-AAL1 solution, not all the Carrier VoIP componentry in this rollback procedure applies to PT-AAL1. Therefore if rolling back the upgrade of the Ethernet Routing Switch 8600 software in a PT-AAL1 solution, skip to [step 99](#).

Use the Ethernet Routing Switch 8600 CLI to split the Ethernet Routing Switch 8600 into active and standby sides

- 3 Make sure Ethernet Routing Switch 8600 Chassis N is the slave as follows:
 - a set the VRRP priority to 1 by typing

config vlan <vid> ip vrrp <vrid> prio 1

Note: Setting Ethernet Routing Switch 8600 Chassis N <prio> to 1 makes it slave.
 - b set the OSPF priority to 1000 by typing

config vlan <vid> ip ospf metric 1000
 - c repeat sub-[step a](#) and sub-[step b](#) for each VLAN provisioned
- 4 Save the new Ethernet Routing Switch 8600 Chassis N configuration by typing:

sav config

This updates the new Ethernet Routing Switch 8600 configuration so that VRRP settings are maintained after any subsequent reboot.

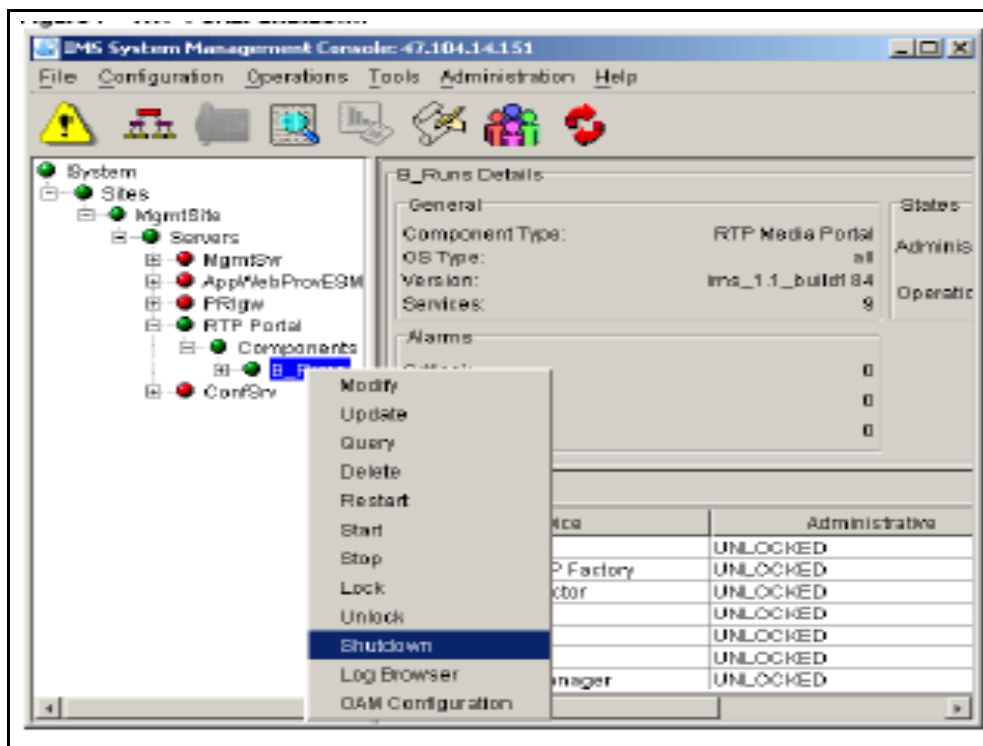
- 5 Select the next step as follows:

If your configuration includes:	Do
multiple RTP Media Portals directly connected to the Ethernet Routing Switch 8600	step 6
does not include an RTP Media Portal	step 9

Use the System Management Console to shut down the RTP Media Portal connected to Chassis N to prevent it from accepting new service requests

- 6 In the System tree, right click on the target RTP Media Portal component.

Note: Ensure you are addressing the port that is connected directly to the Ethernet Routing Switch 8600.
- 7 From the pop-up menu, select **Shutdown**.



Note: Alternately, the **Shutdown** command is available from the pull-down Operations menu.

A confirmation window appears.

Shutdown will affect the operations of this component.

Do you want to continue?

- 8 Click the Yes button.

The RTP Media Portal shuts down gracefully and transitions into a LOCKED state when the last active media session ends. (Refer to the General Information area of the System Management Console.)

- 9 Select the next step as follows:

If your CS-LAN:	Do
includes ATM PVGs directly connected to the Ethernet Routing Switch 8600 (i.e., a non-VR solution)	step 10
includes PVGs connected by Gig Ethernet (GigE)	step 25
does not include PVGs	step 25

If your CS-LAN:**Do**

includes ATM interfaces connected to a PVG
15000/7400 chassis running VR or VrAp

[step 25](#)

Note 1: The following steps ([step 10](#) to [step 24](#)) offload PVG traffic from the Ethernet Routing Switch 8600 chassis undergoing a software upgrade. Offloading PVG traffic using these steps minimizes the impact of the software upgrade process on call processing.

Note 2: These steps apply to full-featured Packet Trunking Transit solutions that use Passport Voice Gateways with the CS-LAN.

Use the PVG CLI to determine the PVG IP addresses

- 10** Check the provisioning information for the VSPs, NSTA, and VGS subcomponents as follows:
- a** display media and signaling gateway IP addresses by typing:

d -p nsta/* vgs ctrl/*

The following list provides sample MG and SG IP addresses for a single VSP card provisioned in slot 7.

Nsta	Ctrl	ipAddr	dnsList
7	mg	172.16.201.2	
7	sg	172.16.201.6	

Note: The... **nsta/* vgs ctrl/*** component of this command causes IP addresses for all provisioned VSP cards to be displayed. The example only shows MG and SG IP addresses for a single VSP card provisioned in slot 7.

- b** display the IPmcon IP address by typing:

d -p nsta/* vgs ipmcon

The following list provides a sample IPmcon IP address for a single VSP card provisioned in slot 7:

Nsta	ipAddr	udpBa	Response
		se	
7	172.16.201.10	49152	

Note: The ... *nsta/* vgs ipmcon* component of this command causes IP addresses for all provisioned VSP cards to be displayed. The example only shows IPmcon IP address for a single VSP card provisioned in slot 7.

Use each Ethernet Routing Switch 8600 CLI to verify that the PVGs are set up redundantly

- 11 Check the VLAN configuration file by typing the following command on each Ethernet Routing Switch 8600 chassis:

sho config module vlan

This command outputs all VLANs provisioned on the Ethernet Routing Switch 8600 Chassis. The example that follows shows the output of this command for only one VSP blade:

```
vlan 702 create byport 1 name "PVG40-vsp07-mg"
vlan 702 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8 member portmember
vlan 702 ports add 8/1 member portmember
vlan 702 ip create 172.16.201.1/255.255.255.252 mac_offset 5
vlan 706 create byport 1 name "PVG40-vsp07-sg"
vlan 706 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8 member portmember
vlan 706 ports add 8/1 member portmember
vlan 706 ip create 172.16.201.5/255.255.255.252 mac_offset 14
vlan 710 create byport 1 name "PVG40-vsp07-media"
vlan 710 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8 member portmember
vlan 710 ports add 8/1 member portmember
vlan 710 ip create 172.16.201.9/255.255.255.252 mac_offset 6
```

Note: Both Ethernet Routing Switch 8600s should display the identical PVG VLAN configuration. The **vlan ### ports add** entry identifies each VSP ATM Sonet connection. This information is required in [step 17](#).

- 12 Select an Ethernet Routing Switch 8600 chassis (Chassis N or Chassis X) and record the routing table information for all of its VSP VLANs as follows:

Note: Sub-step c repeats this step for the other chassis

a type:

sho ip route info ip x.y.z

where x.y.z specifies the IP Net address provided at [step 10](#).

Note: Specifying the x.y.z octets limits the command output to those nodes served by the specified IP Net.

Refer to the figure in [step 16](#) of [Upgrading Ethernet Routing Switch 8600 software for the CS-LAN](#) for more information about IP Net addressing.

The following list provides an example for the command output for one of the Ethernet Routing Switch 8600s:

```
=====
                        Ip Route
=====
```

DST	MASK	NEXT	COST	VLAN	PORT	PROT	AGE	TYPE	PRF
172.16.201.0	255.255.255.252	172.16.201.1	1	702	-/-	LOC	0 DB	0	
172.16.201.4	255.255.255.252	172.16.201.5	1	706	-/-	LOC	0 DB	0	
172.16.201.8	255.255.255.252	172.16.201.9	1	710	-/-	LOC	0 DB	0	

2 out of 360 Total Num of Dest Networks,360 Total Num of Route Entries displayed.

```
=====
```

TYPE Legend:
I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, E=Ecmp Route,
U=Unresolved Route, N=Not in HW

The following list provides an example for the command output for the other Ethernet Routing Switch 8600 Chassis:

```
=====
                        Ip Route
=====
```

DST	MASK	NEXT	COST	VLAN	PORT	PROT	AGE	TYPE	PRF
172.16.201.0	255.255.255.252	172.30.242.230	20	80	-/-	OSPF	0 IB	120	
172.16.201.4	255.255.255.252	172.30.242.230	20	80	-/-	OSPF	0 IB	120	
172.16.201.8	255.255.255.252	172.30.242.230	20	80	-/-	OSPF	0 IB	120	

2 out of 360 Total Num of Dest Networks,360 Total Num of Route Entries displayed.

```
=====
```

TYPE Legend:
I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, E=Ecmp Route,
U=Unresolved Route, N=Not in HW

ATTENTION

The routing information under the PROT column heading should indicate either VSP subnet LOC or OSPF.

If both Ethernet Routing Switch 8600s indicate the same status for the same VSP subnet, this is a non-standard condition. Contact your next level of support.

To prevent service interruption, VSP VLANs on Chassis N of the Ethernet Routing Switch 8600 must be OSPF (LOC for Chassis N). See [step 19](#) for detailed steps for forcing compliance to this requirement.

- b** repeat sub-[step a](#) for each VSP VLAN on the selected Ethernet Routing Switch 8600 chassis.
- c** select the other Ethernet Routing Switch 8600 chassis and repeat sub-[step a](#) and sub-[step b](#).

Use the PVG CLI to verify the correct provisioning of each VSP

- 13** Check the SPVCAP subcomponent of each VSP VGS Ctrl/<mg,sg> and IPmcon as follows:
- a** display the provisioning information for each VSP by typing:

d -p -no nsta/* vgs ctrl/* spvcap

The following list shows VSP provisioning information for slot 7. The actual command output lists all VSP information.

```
Nsta/ 7 VGS Ctrl/mediaGateway SpvcAp
  atmServiceCategory = nrtVariableBitRate
  peakCellRate      = 800 cells
  sustainedCellRate= 400 cells
  maximumBurstSize= 100 cells
  retryLimit        = 0
  localAddress      = 45613512123400002F000000010020480D527001
  remoteVpiVci      = 7.2
  addressToCall     = 45613512123400002F000000010020480D008D00
Nsta/ 7 VGS Ctrl/signalingGateway SpvcAp
  atmServiceCategory = nrtVariableBitRate
  peakCellRate      = 450 cells
  sustainedCellRate= 210 cells
  maximumBurstSize= 60 cells
  retryLimit        = 0
  localAddress      = 45613512123400002F000000010020480D527002
  remoteVpiVci      = 7.2
  addressToCall     = 45613512123400002F000000010020480D008D00
```

b type:

d -p -no nsta/* vgs ipmcon spvcap

*The following list shows information for the IPmcon in slot 7.
The actual command output lists information for all IPmcon
sub-components of the NSTA VGS.*

```
Nsta/ 7 VGS IpMcon SpvcAp
  atmServiceCategory = rtVariableBitRate
  peakCellRate       = 336000 cell/s
  sustainedCellRate  = 336000 cell/s
  maximumBurstSize   = 1 cells
  retryLimit         = 0
  localAddress       = 45613512123400002F000000010020480D517000
  remoteVpiVci       = 7.10
  addressToCall      = 45613512123400002F000000010020480D008D00
```


- 14 Confirm that the VSP VGS **addressToCall** (ATMIF UNI address) for **Ctrl/mediaGateway**, **Ctrl/signaling Gateway**, and **IpMcon** are identical.

Note: If they are not identical, contact your next level of support.

- 15 Check the ATMIF UNI addresses provisioned as primary and alternate by typing:

l atmif/* uni addr/*

A sample of the command output for the ATMIFs present on the PVG shelf follows:

```
Atmif/141 Uni Addr/45613512123400002F000000010020480D008D00, primary
Atmif/151 Uni Addr/45613512123400002F000000010020480D008D00, alternate
Atmif/151 Uni Addr/45613512123400002F000000010020480D009700, primary
```

Note: Make sure the ATMIF UNI provisioning reflects a Primary and Alternate configuration for the same address for each VSP (Refer to your engineering guidelines for more information). If they do not match, contact your next level of support.

Use the PVG CLI to verify the PVG ATM (software) connection to the Ethernet Routing Switch 8600s

- 16 Determine which ATMIF the VSP VGS Ctrl/<mg,sg> and IPmcon ATMCON subcomponents point to as follows:
- a display the VGS Ctrl/<mg,sg> ATMCON subcomponent for all VSPs by typing:

d nsta/* vgs ctrl/* atmconn

A sample of the command output for a VSP provisioned in slot 7 follows. The actual command output lists all connection states and the ATMIFs they use.

```

+=====+-----+-----+-----+-----+
|Nsta |Ctrl|           nextHop           |state
+=====+-----+-----+-----+-----+
|      7|mg  |AtmIf/141 Vcc/7.2 Ep|connec
|      7|sg  |AtmIf/141 Vcc/7.6 Ep|connec

```

Note: Make sure the *AtmIf* information for each VSP is identical to the primary interface information listed in [step 15](#). If it is not contact your next level of support.

- b** display the NSTA VGS IPmcon ATMCON subcomponent for the VSPs by typing:

d nsta/* vgs ipmcon atmcon

A sample of the command output for a VSP provisioned in slot 7 follows. The actual command output lists all connection states and the ATMIFs they use.

```

+=====+-----+-----+-----+-----+
| Nsta|           nextHop           |state |Response
+=====+-----+-----+-----+-----+
|      7|AtmIf/141 Vcc/7.10|connec |

```

Note: Make sure the *AtmIf* information for each VSP is identical to the primary interface information listed in [step 15](#). If is not contact your next level of support.

- 17** Check the physical connections between each PVG ATM interface and their related Ethernet Routing Switch 8600s.

Note: See [step 11](#) for the Ethernet Routing Switch 8600 local route tables for the VSPs to be offloaded and verify the fiber connectivity between the PVGs and Ethernet Routing Switch 8600s. Refer to your engineering guidelines for additional information.

Use the PVG CLI to disable the ATM interface to the Ethernet Routing Switch 8600 undergoing the software upgrade.

- 18** Select the next step as follows (refer to [step 12](#)):

If all VSP VLANs for Ethernet Routing Switch 8600 Chassis N are	Do
OSPF (see Note)	step 25
Anything except OSPF	step 19

Note: OSPF routing does not require manual maintenance to reduce the risk of call processing outages, as the link redundancy on PVGs fails over nearly immediately.

- 19** Disable the ATM interface for each VSP as follows:
- a** identify the ATM interfaces and Sonet layer by typing:

d -p -no lp/* sonet/* sts/0

A sample of the command output for the first Sonet interface on each card follows. The actual command output lists all Sonet interfaces on the PVG.

```
Lp/14 Sonet/1 Sts/0
  applicationFramername    = Atmif/141
  txPathTrace              = ""
  expectedReceivePathTrace = ""
  concatNumber             = 0
  customerIdentifier       = 0
  ifAdminStatus            = up
  ifIndex                  = 6

Lp/15 Sonet/1 Sts/0
  applicationFramername    = Atmif/151
  txPathTrace              = ""
  expectedReceivePathTrace = ""
  concatNumber             = 0
  customerIdentifier       = 0
  ifAdminStatus            = up
  ifIndex                  = 472
```

- b** LOCK all Sonet layer connections related to the ATM ports connected to Ethernet Routing Switch 8600 Chassis N by typing:

lock -force lp/<slot> sonet/<sonetif>

where <slot> is the slot number of the ATMIF blade

<sonetif> is the Sonet interface on the ATM blade

Note: This command results in Sonet layer ALARMS.

c record all locked Sonet interfaces

20 Confirm the ATM (software) connection switch over is successful as follows:

a display the VGS Ctrl/<mg,sg> ATMCON subcomponent for the VSPs by typing:

d nsta/* vgs ctrl/* atmconn

A sample of the command output for the switched ATMCON for the Ctrl/ to the ATMIF in slot 7 follows. This example shows a switchover from AtmIf/141 (see [step 16](#)) to AtmIf151.*

```

=====+-----+-----+-----+-----+
|Nsta |Ctrl|           nextHop           |state |
=====+-----+-----+-----+-----+
|      7|mg |AtmIf/151 Vcc/7.2 Ep|connec
|      7|sg |AtmIf/151 Vcc/7.6 Ep|connec

```

b display the VGS IPmcon ATMCON subcomponent for the VSPs by typing:

d nsta/* vgs ipmcon atmcon

A sample of the command output for the switched ATMCON for the IPmcon in slot 7 follows. This example shows a switchover from AtmIf/141 (see [step 16](#)) to AtmIf/151.

```

=====+-----+-----+-----+-----+
|Nsta |           nextHop           |state |Response|
=====+-----+-----+-----+-----+
|      7|AtmIf/151 Vcc/7.10 |connec|

```

Use the Ethernet Routing Switch 8600 CLI to verify the IP route table for the offloaded VSP VLANs

21 Display the routing table for both Ethernet Routing Switch 8600s by typing:

sho ip route info ip x.y.z

where x.y.z is the IP Net address (see [step 12](#))

Note: The routing information under the PROT column heading should indicate OSPF for all VSP VLANs on Ethernet Routing Switch 8600 Chassis N.

- 22** Select the next step as follows:

If all VSPs are:	Do
not switched over (incomplete)	step 19
switched over (complete)	step 23

Use the PVG CLI to re-enable all disabled ATM ports

- 23** Unlock all Sonet ports locked at [step 19](#) by typing:

unlock Ip/<slot> sonet/<sonetif>

where **<slot>** is the slot number of the ATMIF blade
<sonetif> is the Sonet interface on the ATM blade

Use the Ethernet Routing Switch 8600 CLIs to check the IP route tables

- 24** Make sure all VSP VLANs remain OSPF on Ethernet Routing Switch 8600 Chassis N and LOC on Ethernet Routing Switch 8600 Chassis X by typing:

sho ip route info ip 172.16.201

The routing information under the PROT column heading must indicate OSPF for all VSP VLANs on Ethernet Routing Switch 8600 Chassis N. If it does not, contact your next level of support.

Use CS 2000 Management Tools to make the devices that subtend Ethernet Routing Switch 8600 Chassis N inactive:

- 25** Launch CS 2000 Management Tools from your web browser.

Note: If Java Web Start is not installed on your workstation, you will be prompted to install Java Web Start.

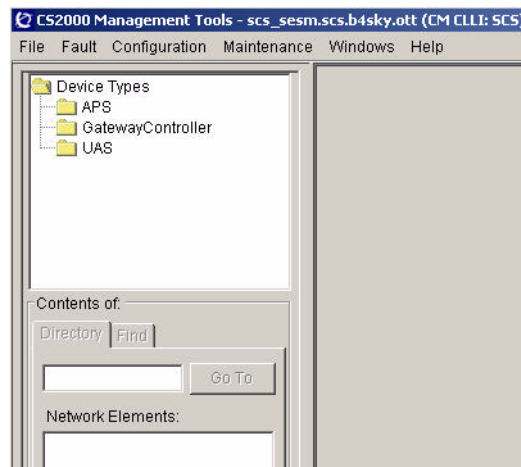
- 26** Click on the CS2000 Management Tools link.

The Login window appears.

- 27 Enter your Login Name. Press the tab key or click in the Password field and enter your Password, which is not echoed for security purposes. Click the Log In button.

Note: Make sure to login with RWA privileges. (See subsection [Instructions](#) in *Ethernet Routing Switch 8600 Software Upgrade for the CS-LAN* for details.)

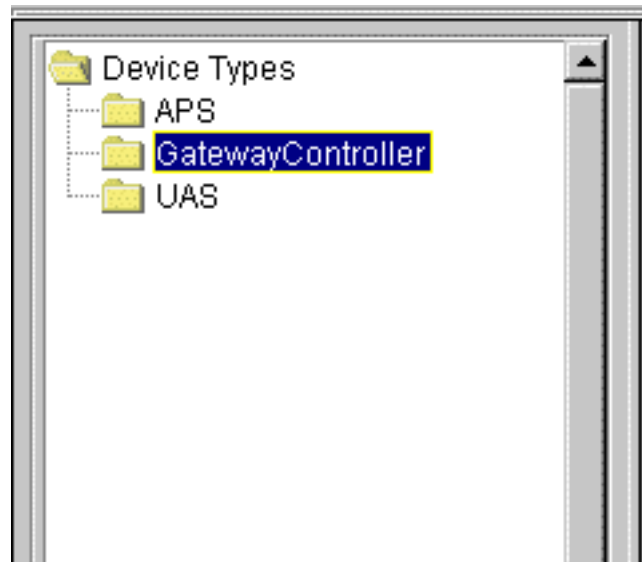
The CS 2000 Management Tools GUI opens in a new browser window.



- 28 Activate the Maintenance information window for the GWCs as follows:

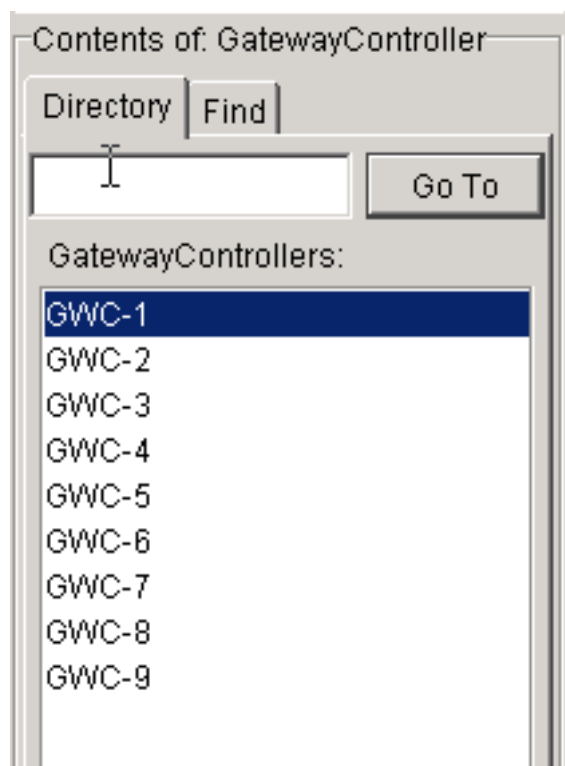
- a select **GatewayController** from the **Device Types** field of the CS2000 Management Tools GUI

*The **GatewayController** folder in the **Device Types** field is highlighted.*



- b select the **Directory** tab on the **Contents of: Gateway Controller** field

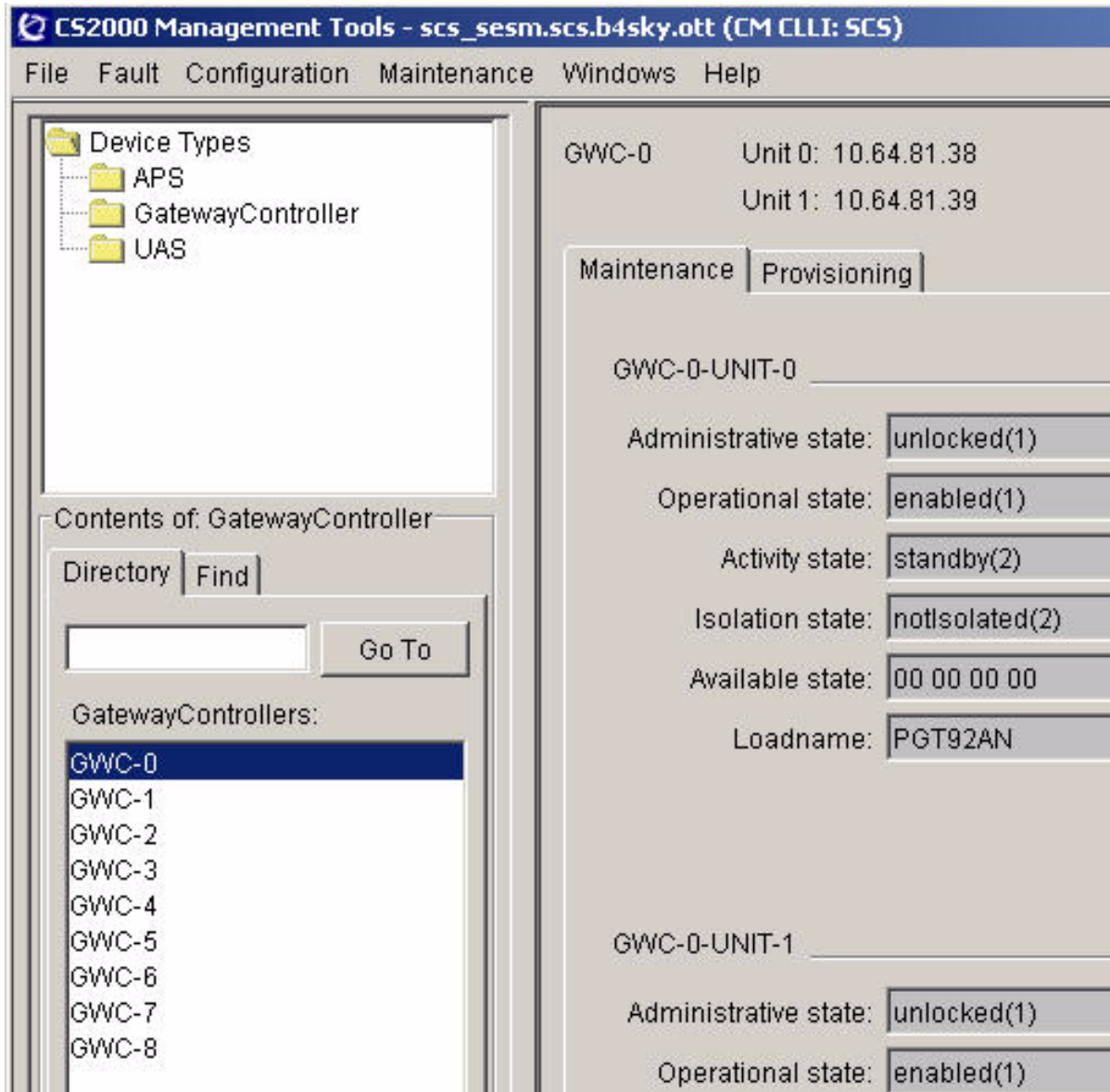
The list of Gateway Controllers appears.



- c select the first GWC in the list displayed in the **Contents of: Gateway Controller** field

The GWC is highlighted and the related Maintenance or Provisioning information, depending on the active tab, appears in the large right hand field.

- d select the **Maintenance** tab to make sure the Maintenance information is active.



- 29** Make all GWCs inactive on Ethernet Routing Switch 8600 Chassis N.

Note: Recall that the recommendation in [step 1](#) requires that GWC unit 0s subtend Ethernet Routing Switch 8600 Chassis 0. GWC unit 1s subtend Ethernet Routing Switch 8600 Chassis 1. The following table reiterates the Ethernet Routing Switch 8600 Chassis configurations.

Iteration	Slave Ethernet Routing Switch 8600	Master Ethernet Routing Switch 8600
First Pass	Chassis N = 0	Chassis X = 1
Second Pass	Chassis N = 1	Chassis X = 0

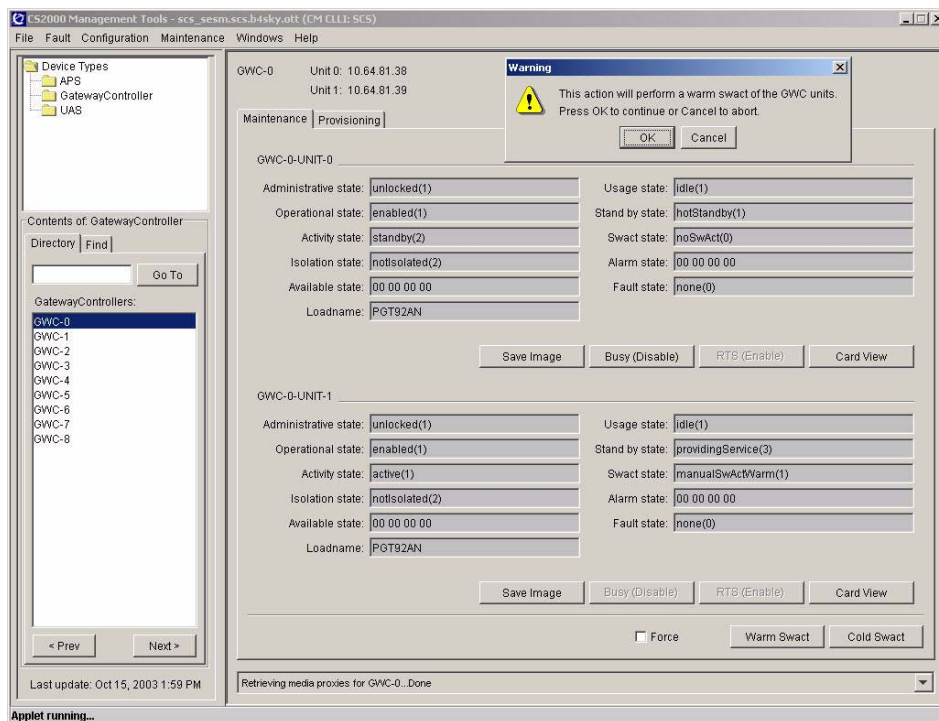
- a** check the **Activity State** field for GWC unit N to determine which unit is **active** and which is **standby**

If the Activity State field is	Do
active	sub- step b
standby, instead of inactive	sub- step f

Note: For the first iteration, all GWC unit 0s should be standby. For the second iteration, all GWC unit 1s are standby.

- b** press **WarmSwact**
A warning window appears.

Press OK to continue or Cancel to abort.



- c press OK and wait for the activity change to complete

The selected GWC undergoes a change of activity. The change of activity can take a minute or two.

- d Select the next step as follows.

If the GWC software release is	Do
from lower than SN06	step 29e
from SN06 or greater	step 29f

- e press **Busy (Disable)** button to manually busy the selected inactive GWC unit (the button is located at the bottom of the **Maintenance** information window).

Note: A warning message may appear for GWC Units provisioned with MG9Ks that are set up with the ABI option. Check the Force option and re-press the **Busy (Disable)** button to complete this sub-step.

The selected inactive unit of the GWC is set to the manually busy state.

- f select the next GWC in the **Contents of: Gateway Controller** list and repeat these substeps until the **Activity State** field for **Unit: N Status** is **inactive** for all GWCs in the list.

30 Select the next step as follows:

If the Communication Server uses:	Do
an XA-Core	step 31
a Compact chassis	step 33

Use the XA-Core MAP terminal to disable the Ethernet link with Ethernet Routing Switch 8600 Chassis N

31 Access the ETHR level of the MAP display by typing:

>MAPCI;MTC;XAC;ETHR

Note: Refer to the IP addresses in table CMIPADDR. Verify that HIOP links 5R and 14R map to the correct arp table on both Ethernet Routing Switches.

32 Refer to the following tables and disable the Ethernet link between the XA-Core and Ethernet Routing Switch 8600 Chassis N by doing either sub-step a or sub-step b as appropriate.

Note: Refer to the figures supporting [step 35](#) and [step 37](#) in [Upgrading Ethernet Routing Switch 8600 software for the CS-LAN](#) for more information.

- a if the XA-Core uses HIOPs or HCMICs, type (otherwise do sub-step b):

bsy <slot> r link force

HIOPs/HCMICs	N = 0	N = 1
<slot>	5	14

go to [step 33](#)

- b if the XA-Core uses IOPs with ETHR packets, type:

bsy <slot1> r l link force

wait for the command to complete then type:

bsy <slot2> r l link force





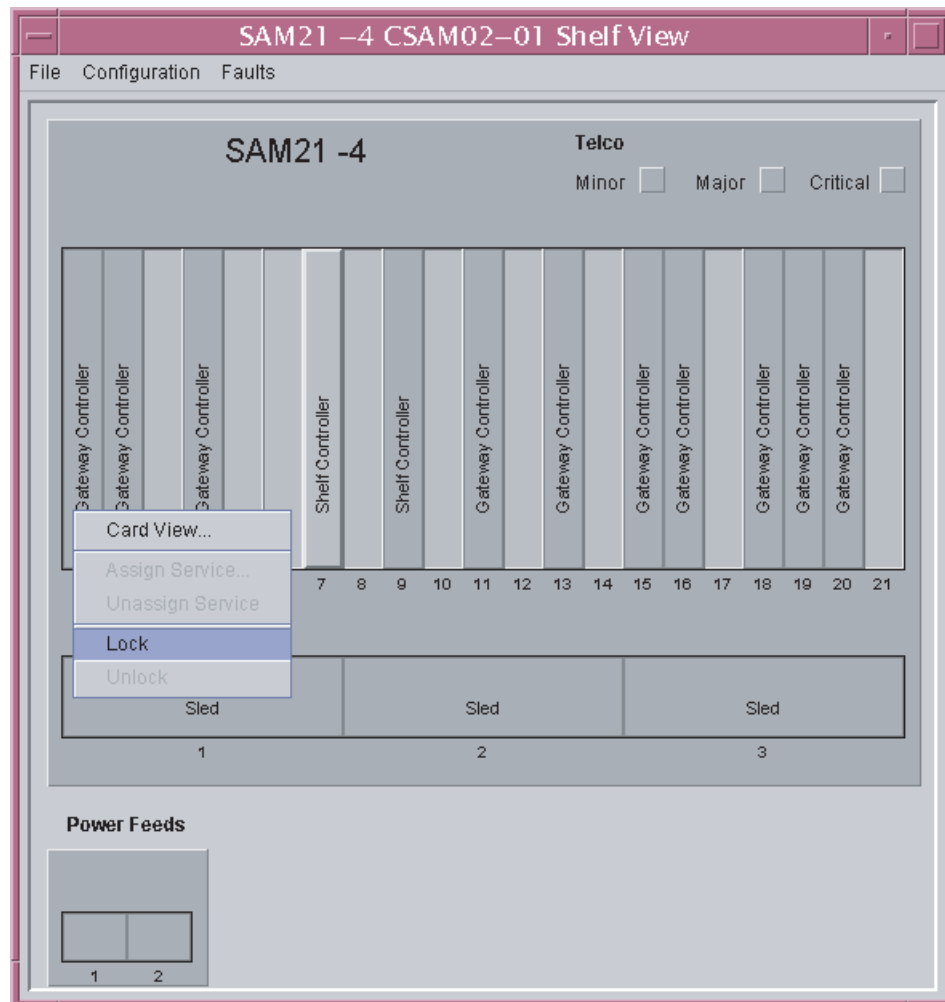
IOP with ETHRs	N = 0	N = 1
<slot1>	5	6
<slot2>	13	14

- 33** Select the next step as follows.

If the GWC software release is	Do
from lower than SN06	step 34
from SN06 or greater	step 35d

Use the SAM21 Element Manager to lock the inactive GWCs:

- 34** Launch the SAM21EM client.
The SAM21 EM GUI appears.
- 35** Lock the inactive GWCs as follows:
- from the SAM21 EM shelf view, right click on each **standby** Gateway Controller Unit (see [step 29a](#)) in turn



- b** select **Lock** from the drop-down menu that appears.

*This sets the **standby** GWC Units to Locked.*

Note: If the SAM21 EM displays a warning message stating the GWC Unit is in service, abort the lock, go to [step 29](#), and make sure the GWC Unit is inactive. If the warning persists contact your next level of support.

- c** repeat sub-[step a](#) and sub-[step b](#) until all **standby** Gateway Controller Units are locked.

d select the next step as follows:

If you have	Do
a 3PC with a USP Compact	step 36
a 3PC with a standard USP	step 59
an XA-Core	step 68

Use the USP Compact (USPc) GUI to prepare the slave USPc blade for locking:

36

ATTENTION

Prior to adhering to steps [37](#) to [52](#), ensure that the slave USPc blade is being addressed during the first iteration of the Ethernet Routing Switch 8600 software upgrade.

Refer to your network diagram and determine the USPc blade-to-Ethernet Routing Switch 8600 connectivity. The slave USPc blade must connect to Chassis N of the Ethernet Routing Switch 8600; master USPc blade to Chassis X. (This information coincides with the network element-to-Ethernet Routing Switch 8600 assumptions stated in [step 1](#) of this procedure.)

37 Launch the USPc GUI.

38 Select **Configuration --> platform --> Node**.

The Administration tab of the USPc GUI displays.

The screenshot shows the Administration tab of the USPc GUI. The interface includes a top toolbar with icons 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

slot-type	usp-compact
slot-name	USP1
slot-description	USP-Compact #1
shelf	0
slot	15
t1-e1-mode	t1
ext-ip-address	47 . 131 . 125 . 82
ext-subnet-mask	255 . 255 . 255 . 128
ext-gateway	47 . 131 . 125 . 126
front-pec	NTRX51FN

Operational Data

operational-state	enabled
administrative-state	unlocked
procedural-state	null
availability-state	null
activity-state	inactive
rex-status	

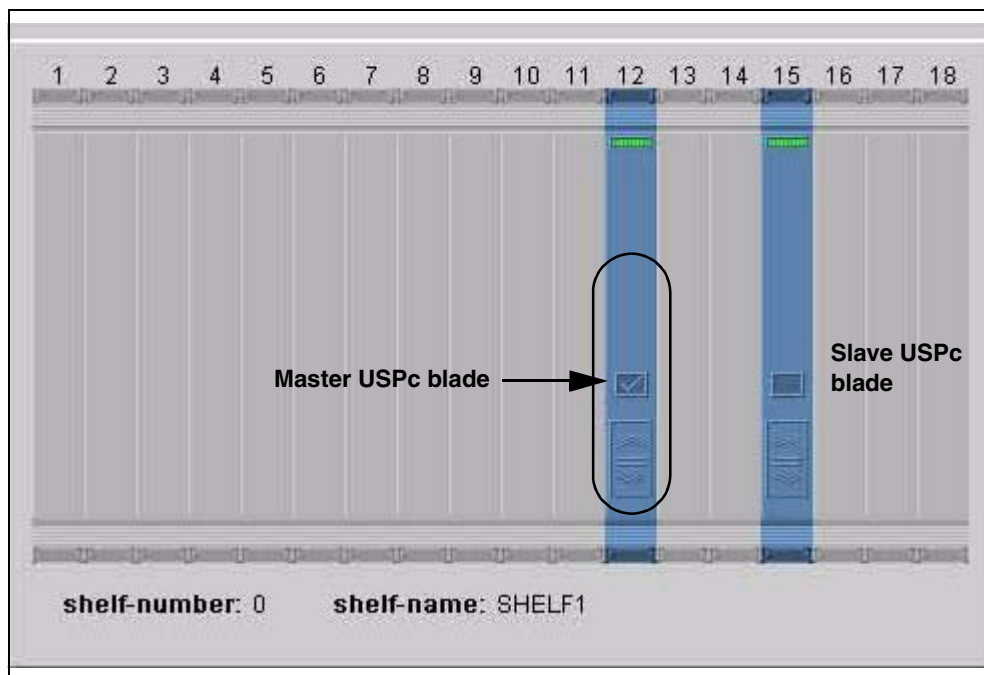
Boot Data

status-message	
running-image	samss7_ppc750_10_00_01_06g
ha-running-image	ss7t1e1ha_ppc8260_10_00_01_06g
running-snapshot	current active
boot image	uspc_10_00_01_06g_base
ha-boot-image	uspc_10_00_01_06g_t1e1ha
boot-snapshot	current active
snapshot-description	current active
snapshot-date	
snapshot-version	

At the bottom of the window, there is a status bar showing "loading complete" and a navigation bar with buttons for back, forward, and search.

- 39** Verify the master and slave USPc blade-to-Ethernet Routing Switch 8600 connectivity by selecting the Graphical View tab.

The following figure displays the Graphical View of the USPc blades.



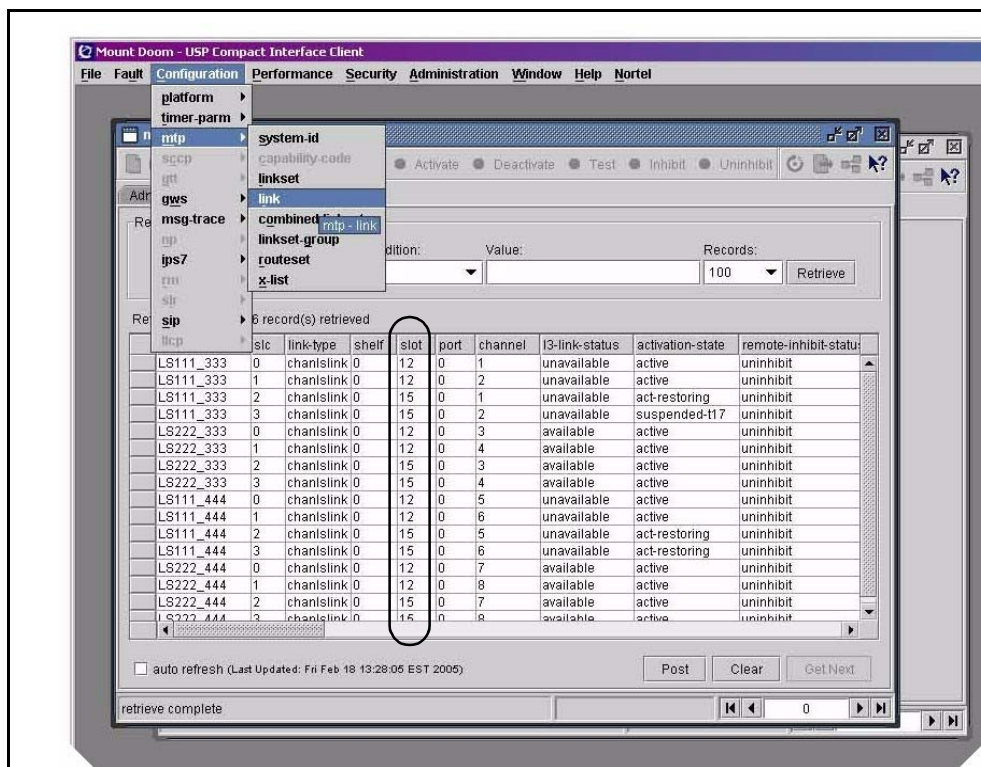
The blade icon with a checkmark identifies the master USPc. Slot 12 contains the master USPc blade. Slot 15 contains the slave USPc blade.

- 40** Select the next step as follows.

If the slave USPc blade is	Do
<i>not</i> connected to Chassis N of the ERS 8600	step 41
connected to Chassis N of the ERS 8600	step 42

- 41** Perform a SWACT on the two USPc blades.
- a** During display of the Administration tab, press the Swact button in the upper right-portion of the screen.
 - b** Continue to [step 42](#).
- 42** Turn down the paths and the links associated with the slave blade to be unlocked.
- Select **Configuration --> MTP --> Links** from the pull-down menu.

The following figure displays.



- 43** Refer to the Slot column to verify the SS7 links against the USPc blades. Select any SS7 links that are against the slave USPc blade.

Click the Inhibit button towards the upper-right portion of the screen.

The following prompt displays.

The inhibit command will be executed for all posted records.

Are you sure you want to continue?

- 44** Click Yes to execute the command on the selected links.
- 45** Using the same screen, reselect the links. Click the Deactivate button in the upper-middle portion of the screen.

The following prompt displays.

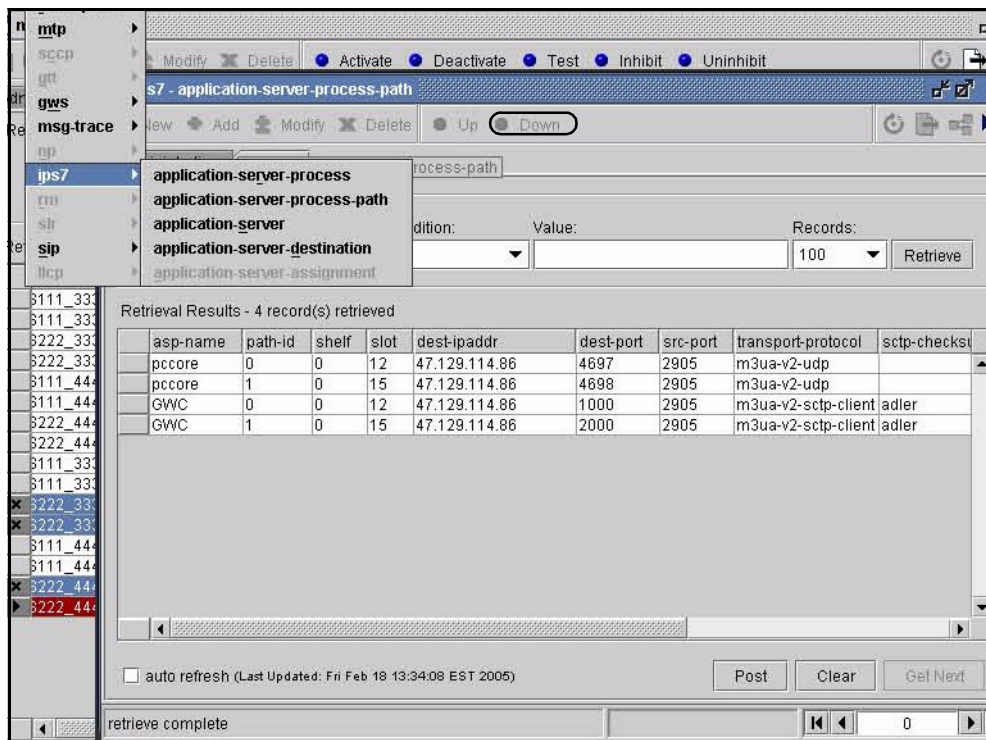
The deactivate command will be executed for all posted records.

Are you sure you want to continue?

- 46** Click Yes to execute the command on the selected links.
- 47** Post the IPS7 paths that use the slave USPc blade.

Select **Configuration --> ips7 --> application-server-process-path**.

The following figure displays.



- 48** Select all the IPS7 paths against the slave USPc blade. Click the Down button in the upper-right portion of the screen.

The following prompt displays:

The down command will be executed for all posted records. Are you sure you want to continue?

- 49** Click Yes to execute the command on the IPS7 paths on the slave USPc blade.

At this point, the IPS7 paths and SS7 links against the slave USPc blade have been deactivated.

- 50** Lock the slave USPc blade.

Select **Configuration --> platform --> Node**.

The Administration tab, as shown in [step 38](#), redisplays.

- 51** Click the Lock button at the upper-middle portion of the platform-nodes screen.

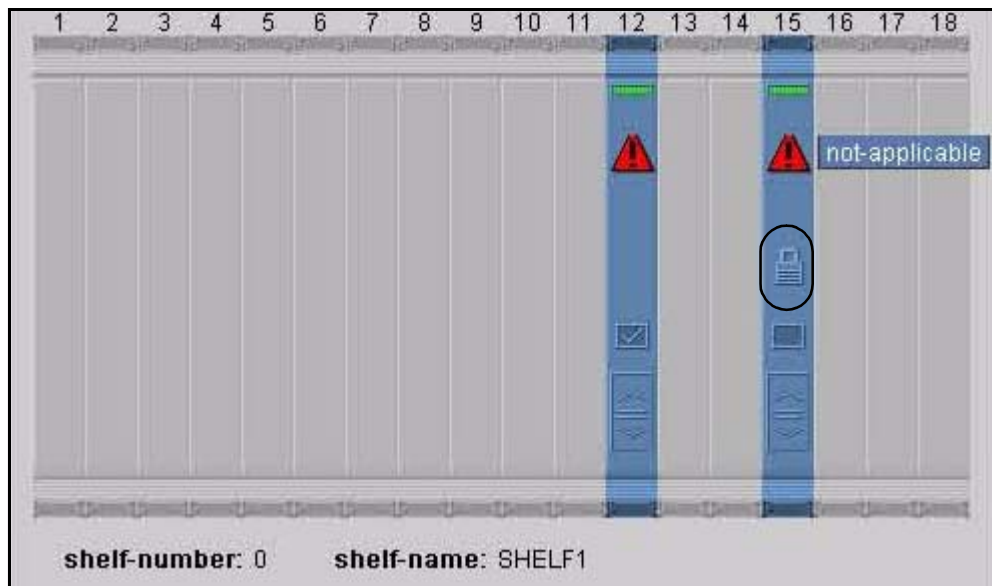
The following prompt displays:

The node lock command will impact the last in-service link from at least 1 linkset which may impact network traffic. Do you want to continue?

- 52** Click Yes to lock the USPc blade.

Click the Graphical View tab.

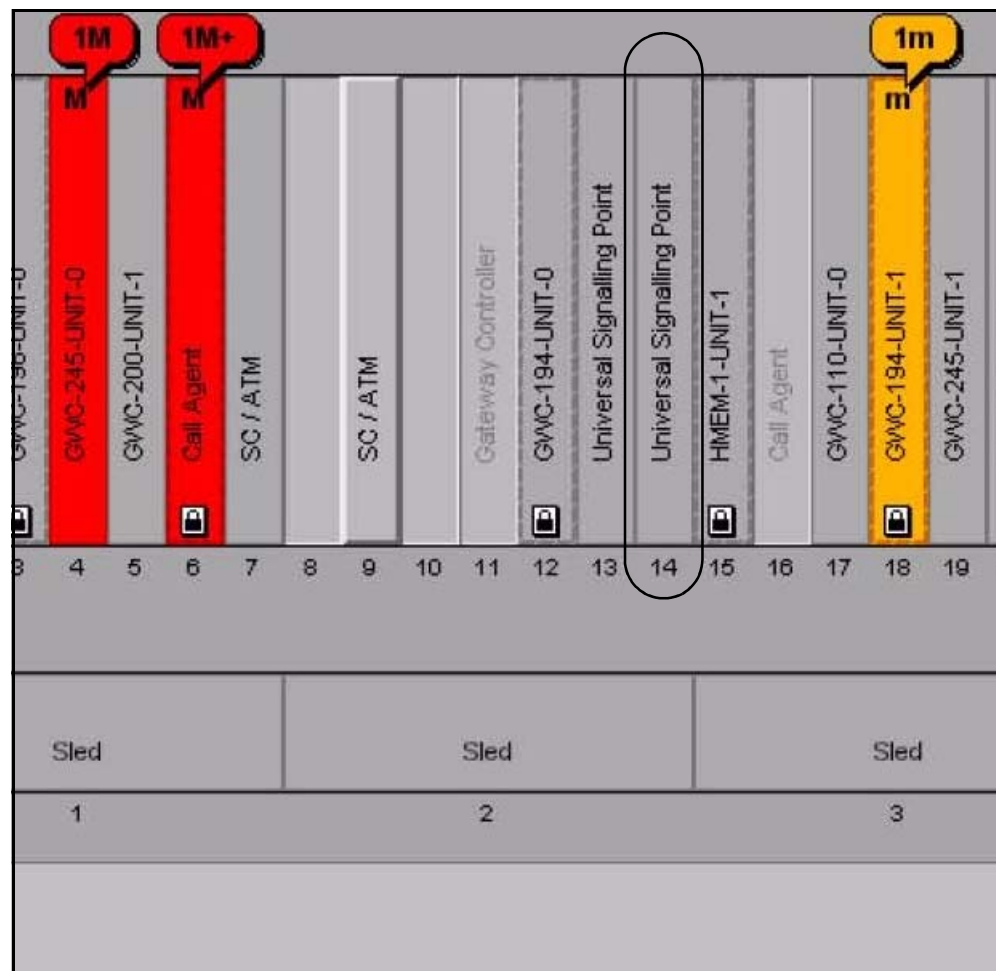
The Graphical View tab shows that the USPc blade has a lock icon next to it, indicating it has been locked.



Use the SAM21 Element Manager to lock the USPc blade:

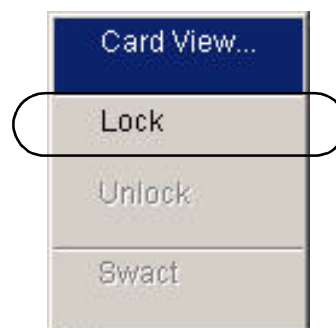
- 53** Access the SAM21 EM GUI.
- 54** Select the shelf by double clicking on its icon.

The following figure shows an example in which the slave USPc blade resides on slot 14.



- 55 Right click on the icon which corresponds to where the slave USPc blade resides.

*A sub-window appears with the **Card View** and **Lock** selections enabled.*



56 Click Lock.

The slave USPc blade is locked.

Note 1: This prevents an automatic change of activity from occurring. An automatic SWACT at this point could cause a system outage.

Note 2: An alternative method to Lock the blade from the SAM21 EM is to first open the card by double clicking on it. Then click the Lock button towards the upper-right portion from display of the States tab.

Decide if STORM devices require rotating, demounting and busying

57**ATTENTION**

Before proceeding with the following STORM-related steps, consider if other applications might be affected by the loss of STORM disk volumes.

58 Select the next step as follows

If	Do
STORM uses a Dothill device	step 59
STORM IA (SAM-XTS) device ¹	step 68

1. The SAM-XTS configuration uses dual-homed split multilink trunks (SMLT). Both STORM volumes are recognized by both Ethernet Routing Switch 8600 routers. Therefore, taking down one router in an SAM-XTS configuration does not affect the STORM volume being addressed.

59 Select the next step as follows

If	Do
the volumes on any STORM disk (for example, sd01) are actively mounted in DIRP ¹	step 60
the volumes on the STORM disk are not actively mounted in DIRP ²	step 68

1. Loss of network connectivity between SOS, the call processing application, and the active STORM disk can cause some or all DIRP volumes to be marked "INER-ROR," resulting in permanent loss of data.

2. Regardless of whether DIRP volumes are mounted, the procedure can result in an unavailable STORM disk and associated volumes.

- 60** Refer to your network diagram and verify that the STORM device-to-Ethernet Routing Switch 8600 connectivity in your configuration is set up as follows:
- STORM volumes prefixed with sd00 reside on STORM device 0, which *must* connect to Ethernet Routing Switch 8600 Chassis 0.
 - STORM volumes prefixed with sd01 reside on STORM device 1, which *must* connect to Ethernet Routing Switch 8600 Chassis 1.

Note: This information coincides with the network element-to-Ethernet Routing Switch 8600 assumptions stated in [step 1](#) of this procedure.

If the STORM-to-Ethernet Routing Switch 8600 connections in your configuration do not match these assumptions, adjust the commands in steps [61](#) to [67](#) to address the appropriate STORM device.

- 61** From the Core MAP command line, list all available DIRP subsystems (field SYSSNAME in table DIRPSSYS) for the Core.

>table dirpssys; lis all

- 62** Access the DIRP level in SOS by typing:

>mapci nodisp;mtc;iod;dirp

- 63** Query all volumes associated with the subsystem.

>query <subsystem> all

where:

<subsystem> is from the list of available subsystems executed in [step 61](#).

The following figure shows an example of this command for the dlog subsystem with an active file highlighted.

```

>query dlog all
SSNAME SSNO SEQNO ROTATES POOLNO PARLPOOL EMERGENCY
DLOG      1      1      3      7  NONE      ***YES***

REGULAR
FILE(S)   STATE VOLUME      RECCOUNT BLOCK E   V  V_B VLID FNUM FRN#
ACTIVE    AVAIL SD00DLG1      1      1 0 71 NO 8448 000D 1014
STANDBY1  AVAIL SD01DLG1      0      0 0 70 NO 8408 0015 3012

PARALLEL
FILE              STATE VOLUME      BLOCK E   V  V_B VLID FNUM FRN#
                NONE

REGULAR VOLUME(S)
VOL# VOLNAME  STATE      IOC CRD PORT VOL FSEG ROOM VLID FILES
  70 SD01DLG1 READY      N/A N/A N/A   8   10   11 8408 S1
  71 SD00DLG1 READY      N/A N/A N/A   8  112  116 8448 A

REGULAR SPACE
VOL# VOLNAME  STATE      SEGS   EXP UNEXP TOTAL
  70 SD01DLG1 READY      10     1    0    11
  71 SD00DLG1 READY     112     4    0   116

```

- 64** Rotate the active volume for each subsystem if it is located on a STORM blade connected to the router being upgraded for this iteration. Manually rotate all subsystems until the active files reside on STORM volumes connected to the Ethernet Routing Switch 8600 chassis that is not being upgraded for this iteration.

>rotate <subsystem> <variable>

where:

<variable> is *regular*, *paralel*, or *both* (Enter *regular* to rotate regular volumes. Enter *paralel* to rotate parallel volumes. Enter *both* to rotate both volumes.)

Note 1: Parallel is intentionally misspelled.

Note 2: Volumes associated with the slave Ethernet Routing Switch 8600 should *not* be active. Ensure that no volumes are active in each pass which are prefixed with:

sd0N

where N = 0 (first pass)

N = 1 (second pass)

For example, sd00 volumes should not be active during the first pass. Sd01 volumes should not be active during the second pass. (Rotate each subsystem with volumes prefixed with sd0N that are active.)

Note: To minimize risk, rotate and demount the AMA subsystem last. Then restore the AMA subsystem first.

The following figure shows example of input for variable regular.

```
>rotate dlog REGULAR
ACTIVE FILE WILL BE CLOSED IF POSSIBLE (ROTACLOS).
SENDING REQUEST TO SUBSYSTEM
Please confirm ("YES", "Y", "NO", or "N"):
>y
REQUEST SENT TO SUBSYSTEM, CHECK DIRP LOG FOR DETAILS
```

- 65 Repeat [step 64](#) to ensure that all volumes needing rotating have been rotated successfully.

- 66 Demount all DIRP volumes connected to the Ethernet Routing Switch 8600 chassis that is to be upgraded.

>dmnt <subsystem> <volume> <variable>

where:

<volume> is the volume on the STORM (prefixed with sd0N where N is defined in [Note 2](#) of [step 64](#))

<variable> is *regular* or *parallel*

Note 1: The **<variable>** parameter is not required when mounting and demounting regular DIRP volumes.

Note 2: Nortel recommends recording all subsystems, volume, and variable information for each volume being demounted in this step.

- 67 Busy all STORM volumes connected to the Ethernet Routing Switch 8600 chassis to be upgraded.

>diskadm sd0N; bsy all

where:

sd0N is the STORM volume defined in [Note 2](#) of [step 64](#)

Note 1: Nortel does not recommend using option *bsy all force*.

Note 2: Issuing a bsy all command affects all volumes serviced by that STORM blade, not just those used by DIRP.

68 Select the next step as follows:

If the CS-LAN is used with	Do
a Trimodal solution	step 69
an ATM-based solution	step 69
an IP-based solution	step 71

Use the SAM21 EM to lock the inactive Shelf Controller blade connected to Chassis N:

69

ATTENTION

During a SWACT on the Shelf Controllers (SC), flapping (that is, rapid enabling and disabling) of the router port connected to a SC can result in a temporary loss of Ethernet connectivity. This could cause ongoing failures on the newly active SC following the SWACT.

To prevent the possibility of an outage due to this condition, monitor ongoing or recent logs for Ethernet instability on the router ports that are associated with SCs.

Do **not** SWACT the SCs until all network problems involving flapping are addressed.

Confirm that Shelf Controller (SC) blade connectivity complies with all topology recommendations.

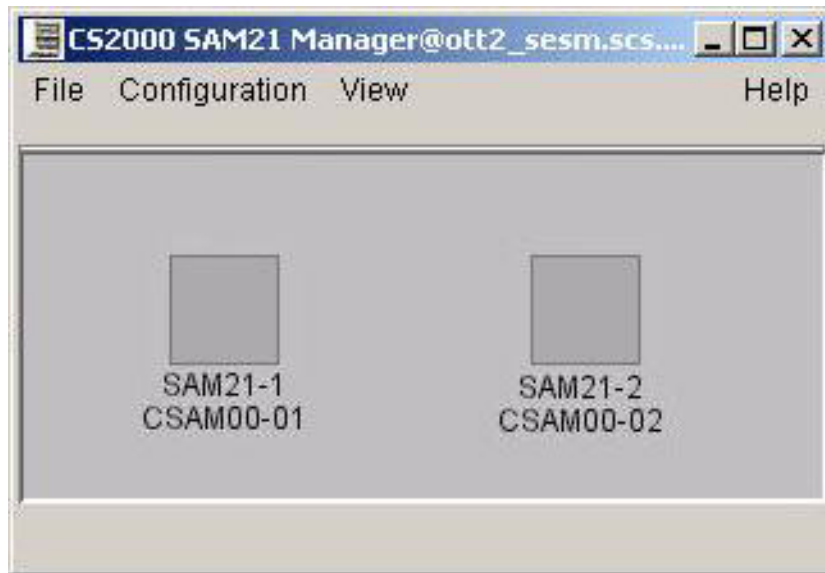
Note: The recommendation step 1 in procedure [Upgrading Ethernet Routing Switch 8600 software for the CS-LAN](#) requires SC unit 0s (in slot 7) subtend Ethernet Routing Switch 8600 Chassis 0, and SC unit 1s (in slot 9) subtend Ethernet Routing Switch 8600 Chassis 1. If the SAM21 shelf varies from this recommendation, adjust this procedure accordingly.

Refer to NTP “Upgrading a Carrier Voice Over IP Network,” NN10440-450.

70 Lock the inactive SAM21 SC blade for each SAM21 shelf in turn as follows:

a launch the SAM21 EM

The SAM21 EM GUI appears with the related shelf icons displayed.



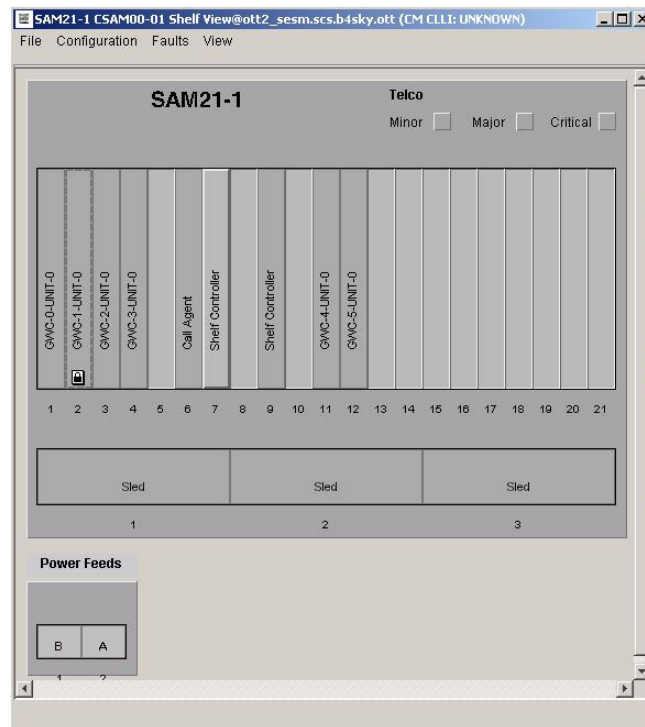
- b** use the cursor to select the shelf icon for the first SAM21 shelf displayed

Example

The first shelf in the figure above is SAM21-1
CSAM00-01

- c** double-click the selected shelf icon

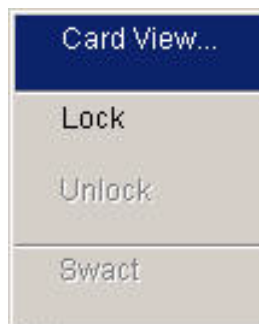
The SAM21 EM shelf view for the selected shelf appears.



- d right-click on the icon for the SC blade associated with the inactive Ethernet Routing Switch 8600 Chassis

Note: The SC blade in slot 7 subtends Ethernet Routing Switch 8600 Chassis 0, slot 9 subtends Chassis 1 (see note to [step 69](#))

*A sub-window appears with the **Card View** and **Lock** selections enabled.*



e click **Card View**

The SC Card View appears.

The screenshot shows a web-based interface for managing system components. The top navigation bar includes tabs for 'Alarms', 'Equip', 'States', 'Diags', and 'Provisioning'. The 'States' tab is currently active. The main content area is titled 'SC Card View' and contains three primary sections. The 'Activity' section at the top shows a 'Status' dropdown menu set to 'Active' and a 'Swact' button. The 'OSI' section in the middle contains three dropdown menus for 'Administrative' (set to 'Unlocked'), 'Operational' (set to 'Enabled'), and 'Availability' (set to 'None'), along with 'Lock' and 'Unlock' buttons. The 'History' section at the bottom is a large, empty text area. At the very bottom of the interface are 'Save' and 'Clear' buttons.

f select the **State** tab and make sure the SC is inactive

*If the SC state is **Active**, press the **SWACT** button to change the activity status to **Inactive**.*

g close the **Card View**

*The **Shelf View** reappears.*

h right-click on the icon for the inactive SC blade

*A sub-window appears with the **Card View** and **Lock** selections enabled.*

i click **Lock**

The inactive SC blade is locked.

Note: This prevents an automatic change of activity from occurring. An automatic SWACT at this point could cause a system outage.

j close the **Shelf View**

The SAM21 EM view reappears.

k select the next step as follows

If the (inactive) SC cards are	Do
locked on all SAM21 shelves	step 98
not all locked	select the next SAM21 Shelf and go to sub- step c

Note: Repeat sub-[step c](#) through sub-[step j](#) until the inactive SCs are all locked.

71 Select the next step as follows:

If your office is	Do
in a Geographic Survivability environment	step 72 through step 97
not in a Geographic Survivability environment	step 98

Use the Integrated Element Management System (IEMS) GUI to lock the Media Server 2000 (MS 2000) Series node connected to Chassis N

72 Launch the IEMS GUI.

Note: Refer to NTP *Integrated EMS Basics*, NN10329-111, for details on logging into the IEMS GUI.

73 Select **Applications ---> Integrated EMS --->Network Elements**.

74 Select the MS 2000 Series node to be locked and right click on its icon.

75 Select the Config and Maintenance Tool from the pop-up menu.

The Config and Maintenance Tool launches.

Note: For details, refer to procedure “Launching the Maintenance and Configuration tool” in section *Configuring and maintaining MS 2000 devices*, NTP *Integrated EMS Configuration Management*, NN10330-511.

76 From the left side of the Config and Maintenance Tool screen, click the **Graceful Lock** button under the Lock State options to lock the MS 2000 node.

Note: A graceful lock signals to the node that a lock has been requested. The node then stops allocating new audio resources and waits for the last resource to be freed before

locking the node. (A forced lock causes the node to immediately free up any resources in use and lock the node.)

- 77** Click the Lock button to gracefully lock short-duration calls from the MS 2000 node.

Note: Since a graceful lock prevents new calls from being originated on the node, existing calls will be taken down on their own. Therefore for calls still active after an extended period of time, *it is up to the discretion of the craftsperson to determine whether to issue a forced lock, or to proceed when the Ethernet Routing Switch 8600 is rebooted.*

Drop sync the inactive Call Agent

- 78** Before locking the inactive Call Agent card, perform a drop synchronization on the inactive Call Agent card from the active Call Agent Manager, enter the following commands.

```
> ccamtc
> coremtc
> appl
> dpsync
```

- 79** Select the next step as follows

If the (active) Call Agent card is	Do
connected to the ERS 8600 Chassis N	step 80
not connected to the ERS 8600 Chassis N	step 87

Use the MAP display to perform a LIMITED_PRESWACT

- 80** At the MAP display, enter the following command:

```
> BCSUPDATE; LIMITED_PRESWACT
```

Note 1: If a LIMITED_PRESWACT process fails to complete, LIMITED_PRESWACT stops and displays additional information. When this occurs, use the information to investigate and correct the problem.

Note 2: All LIMITED_PRESWACT steps must be completed prior to SWACTing.

The LIMITED_PRESWACT command displays a warning:

```
Limited_Preswact should not be used for
BCSUPGRADE SWACTs. Do you wish to continue?
Please confirm ("YES", "Y", "NO", "N"):
```

81 Enter Y.

> Y

A series of steps execute and complete. LIMITED_PRESWACT stops at MATE_RESTART_RELOAD.

```
MATE_RESTART_RELOAD           executing
There are users still logged on the Inactive.
Do you want to continue?
MATE_RESTART_RELOAD           not complete
ACT - Error: Restart aborted. Type
LIMITED_PRESWACT to continue
Investigate and correct if needed.
```

82 If the LIMITED_PRESWACT process halts, re-enter the following command to continue.

> LIMITED_PRESWACT

The following warning displays.

```
MATE_RESTART_RELOAD           executing
There are users still logged on the Inactive.
Do you want to continue?
Please confirm ("YES", "Y", "NO", "N"):
```

83 Enter Y.

> Y

The inactive unit indicates /restart at the Call Agent Manager. Several more steps execute and complete at the MAP. Successful completion is indicated by display of the following message:

```
Total execution time for all complete procedures
00:07:31.362
All LIMITED_PRESWACT steps completed
successfully.
```

Perform a NORESTARTSWACT

- 84** If the active Call Agent card is connected to the Ethernet Routing Switch 8600 to be upgraded, minimize the possibility of an outage by performing a NORESTARTSWACT.

- a** Check the status:

> BCSUPDATE;SWACTCI;STATUSCHECK

The following response displays:

```
SWACTCI:
Checking Nodes Status
STATUSCHECK successful
```

- b** Execute the NORESTARTSWACT.

> NORESTARTSWACT

Progress is printed and the process stops to verify that the inactive Call Agent is not jammed.

```
Beginning SWACT checks:
All the SWACT checks have finished
successfully.
The VR_PRESWACT_TRANSFER step completed
successfully.
All INSV and ISTB series 1 PMs will have execs
loaded after the SWACT.
Device Checking Status:
NOMATCH option is set to OFF <default
setting>.
Device matching during CC WARM SWACT Enabled.
Do you wish to continue?
Please confirm ("YES", "Y", "NO", or "N"):
>
```

- c** Enter a Y if the only alarm is an APPL simplex.

> Y

The final progress follows. Activity also switches at the Call Agent Manager.

```
All Pre_SWACT checks completed. Starting Warm
SWACT now.
**** The cursor will not be returned. ****
**** unless a critical failure occurs. ****
**** Now monitoring Warm SWACT messages. ****

Pre-initialization done
Communication established
```


Exchange of data with the mate done
Transfer of data done (FASPECT)
Data estimation done

- d** The telnet session to the active and inactive call processing applications are lost. Re-establish the connection. Refer to the Interface set in section Call Agent Upgrades for this procedure.

Perform a POSTSWACT

- 85** At the MAP display, enter the following command to run a Postswact through completion.
> BCSUPDATE;POSTSWACT
- 86** Enter N when prompted at the CA_SYNC step to leave the switch out of sync.
> N

Lock the inactive Call Agent card

87



CAUTION

Possible service interruption

DO NOT ATTEMPT TO LOCK THE ACTIVE CALL AGENT CARD.

Locking the active until causes a complete service outage.

To lock the inactive Call Agent, follow these steps:

- a** Access the SAM21 EM GUI.
- b** Select the SAM21 shelf by double clicking on its icon.
- c** From the Shelf View, right click on the card that corresponds to the inactive Call Agent card.
- d** Select the **Lock** option from the context menu.
Note: Lock is also available from the States tab of the Card View window.
- e** Wait for the Lock icon to appear on the selected card.

Demount active DIRP volumes off of SD01

- 88** At the MAP display, enter the DIRP level.
>MAPCI NODISP;MTC;IOD;DIRP
- 89** Query the subsystem to determine which files are active and which are standby.
>QUERY JF FILES
>QUERY DLOG FILES
- 90** Demount all volumes on SD01 for the subsystems that are not active.
>DMNT DLOG SD01DLG0
>DMNT DLOG SD01DLG1
>DMNT DLOG SD01DLOG2
- 91** Rotate the subsystems to a standby volume on SD00.
>ROTATE JF
>ROTATE DLOG
- 92** Query the subsystem again to verify that the active files are on SD00.
>QUERY JF FILES
>QUERY DLOG FILES
- 93** Demount any remaining volumes on SD01.
>DMNT JF SD01JF
>DMNT DLOG SD01DLG3
- 94** Query the subsystem again to verify that no volumes on SD01 are used.
>QUERY JF FILES
>QUERY DLOG FILES
The display should indicate that the JF and DLOG subsystems are not using any volumes on SD01.
- 95** Repeat [step 89](#) for any additional DIRP subsystems.
- 96** Quit the DIRP level.
>QUIT ALL

Busy all STORM disk volumes on SD01 to ensure that the call processing application does not attempt to access the STORM unit

- 97** At the MAP display, enter the following command to busy all disk volumes on device SD01.

>DISKADM SD01;BSY ALL

If the devices do not pass, determine which application has open files. Perform maintenance on those applications so that the application closes the files.

Note: Refer to the STORM upgrade documentation, *Upgrading the STORM*, in this document for details.

Use the Ethernet Routing Switch 8600 CLI to make devices subtending Chassis X of Ethernet Routing Switch 8600 active (Chassis N devices inactive):

- 98** Recheck the address resolution protocol information by typing:

sho ip arp info

The IP ARP file appears. Verify that active units subtend the Ethernet Routing Switch 8600 Chassis X (inactive units subtend Chassis N)

Note 1: For more information IR ARP information, select option Documentation under Ethernet Routing Switch 8600 Routing Switch on the Nortel website. Or contact your next level of support.

Note 2: If any units do not meet this requirement, repeat [step 29](#). If the problem persists, contact your next level of support.

Use the Ethernet Routing Switch 8600 CLI to restore the original software load on Ethernet Routing Switch 8600 Chassis N:

- 99** Select the next step as follows

If your CS-LAN:	Do
is a dual CPU configuration	step 100
is a single CPU configuration	step 105

100

ATTENTION

Refer to section [Text conventions](#) for brief definitions and examples of the software filenames used the following commands.

ATTENTION

Before addressing any commands with a peer option, ensure that the DNS entries were created previously for each CPU. For details on creating DNS entries, refer to the v3.7.X.X Release Notes.

Due to the implementation of DNS, the peer command option is not available unless you add the peer IP address in a new file called flash/etc/hosts.

You must create this file. No default file exists. Use a simple text editor to create it, similar to the text editor provided by the Ethernet Routing Switch 8600.

For an Ethernet Routing Switch 8600 with a dual-CPU configuration, TFTP the upgrade software to the flash on the master CPU. Then copy it to the standby CPU.

In the following sub-steps, both commands must be executed on the master CPU.

Note: The Ethernet Routing Switch 8600 automatically copies files to the flash card using the same name as the current file. When entering the copy command if a destination name is not specified, then the system uses the same name as the source filename. Therefore, it is not necessary to enter a new filename for the backup version of this file in [step 100a](#) through [step 100e](#).

- a** TFTP the new software image file.

Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	<pre>copy <a.b.c.d>:/swd/pp8600/XXX/<newload> /flash/</pre> <pre>copy /flash/<newload> peer:/flash/</pre>

If using a(n)	Type
CBM	<pre>copy <a.b.c.d>:/pp8600/XXX/<newload> /flash/</pre> <pre>copy /flash/<newload> peer:/flash/</pre>
where <a.b.c.d> is the IP address of the TFTP server, and <newload> is the name of the new software image file b TFTP the new boot monitor image file. Type the following commands depending on your core manager platform.	
If using a(n)	Type
SDM/CS 2000 Core Manager	<pre>copy <a.b.c.d>:/swd/pp8600/XXX/<newboot> /flash/</pre> <pre>copy /flash/<newboot> peer:/flash/</pre>
CBM	<pre>copy <a.b.c.d>:/pp8600/XXX/<newboot> /flash/</pre> <pre>copy /flash/<newboot> peer:/flash/</pre>
where <newboot> is the name of the new boot monitor image file <i>The boot flash image and software image is backed up to the PCMCIA card on the Ethernet Routing Switch 8600 Chassis N.</i> Note 1: If either file transfer fails, verify TFTP server IP address and connectivity with Ethernet Routing Switch 8600 Chassis N. Confirm Ethernet Routing Switch 8600 TFTP flag is set to true by typing: <pre>config bootconfig flags info</pre> If the tftpd flag is set to false, reset the flag to true by typing: <pre>config bootconfig flags tftpd true</pre> Confirm the flag is now set to true, then retry the transfer. If the problem persists, contact your next level of support. Note 2: If the transfer completes but the file is corrupted, verify original file and PCMCIA card and transfer the file again. If the problem persists, contact your next level of support.	

Note 3: Compare file parameters such as file size to check for possible corruption.

- c** **Only** if Chassis N of Ethernet Routing Switch 8600 uses an ATM blade, TFTP the ATM Flash image to the Flash card on the Ethernet Routing Switch 8600 Chassis N.

Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	copy <a.b.c.d>:/swd/pp8600/XXX/<newATM> /flash/
	copy /flash/<newATM> peer:/flash/
CBM	copy <a.b.c.d>:/pp8600/XXX/<newATM> /flash/
	copy /flash/<newATM> peer:/flash/

where **<newATM>** is the name of the new ATM file

Otherwise go to [step 101](#).

Note: Notes 1 and 2 from [step 100b](#) apply.

- d** If the Ethernet Routing Switch 8600 uses DES, TFTP the file.
Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	copy <a.b.c.d>:/swd/pp8600/XXX/<newDES> /flash/
	copy /flash/<newDES> peer:/flash/
CBM	copy <a.b.c.d>:/pp8600/XXX/<newDES> /flash/
	copy /flash/<newDES> peer:/flash/

where **<newDES>** is the name of the new DES file

- e** If the Ethernet Routing Switch 8600 uses 3DES, TFTP the file.

Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	copy <a.b.c.d>:/swd/pp8600/XXX/<new3DES> /flash/ copy /flash/<new3DES> peer:/flash/
CBM	copy <a.b.c.d>:/pp8600/XXX/<new3DES> /flash copy /flash/<new3DES> peer:/flash/

where **<new3DES>** is the name of the new 3DES file

- 101 Verify that the software has been copied to the master and standby CPUs.
 - a For the master CPU, type

dir
 - b For the standby CPU, at the prompt of the master CPU, type

peer telnet

dir
- 102 Exit the standby CPU.

exit
- 103 Prepare to boot both CPUs. Select the next sub-step as follows.

If	Do
rolling back to a pre-3.7.0.0 software load	step 103a
rolling back to a 3.7.0.0 (or greater) software load	step 103b

a

WARNING

Failure to observe this step can result in loss of configuration.

Disable the flag setting before saving the bootconfig file.

config bootconfig flags ha-cpu false

- b config bootconfig choice primary image-file /flash/<oldload>**

where **<oldload>** is the name of the current software image file

Note: There is a mandatory space between **image-file** and **/flash** in the syntax this sub-step.

- c** save the bootconfig file by typing:

sav bootconfig

Note: If the switch response does not show the file being saved to the standby CPU, copy the files to the standby CPU by typing:

copy /flash/boot.cfg peer:/flash/boot.cfg

This prepares Ethernet Routing Switch 8600 Chassis N to reboot.

104

WARNING

When booting the dual CPUs, do not wait for the standby CPU to complete the boot process before booting the master CPU. Waiting results in different images on each CPU. While in the high-availability (HA) mode, booting the master CPU and the standby CPU with different software images can crash the standby CPU.

Boot both CPUs in rapid sequential order, booting the standby CPU first and immediately booting the master CPU next.

- a** Boot the standby CPU. In the standby CPU session, type

peer telnet**boot /flash/<oldboot> [config /pcmcia/<cfgbkup>]**

where **<oldboot>** is the name of the current boot monitor image file

b**ATTENTION**

This command upgrades the primary-image file (including the ATM-image if present) and boot monitor at the same time.

ATTENTION

Do not interrupt the reboot process. The CPU card can be damaged if the reboot is interrupted incorrectly.

Immediately boot the master CPU. In the master CPU session, type

boot /flash/<oldboot> [config /pcmcia/<cfgbkup>]

Go to [step 109](#).

105 Prepare to reboot Ethernet Routing Switch 8600 Chassis N as follows:

- a** only if the original software has already been deleted from the Ethernet Routing Switch 8600, type:

copy /pcmcia/<oldload> /flash/

- b** only if the original boot monitor file has already been deleted from the Ethernet Routing Switch 8600, type:

copy /pcmcia/<oldboot> /flash/

- c** only if an ATM blade exists and the original ATM image file has already been deleted from the Ethernet Routing Switch 8600, type:

copy /pcmcia/<oldatm> /flash/

- d** If the Ethernet Routing Switch 8600 uses DES, TFTP the file. Type:

copy /pcmcia/<oldDES> /flash/

where **<oldDES>** is the name of the original DES file

- e** if the Ethernet Routing Switch 8600 uses 3DES, TFTP the file. Type:

copy /pcmcia/<old3DES> /flash

where **<old3DES>** is the name of the original 3DES file

- f** set the primary image file to the saved load by typing:

**config bootconfig choice primary image-file
/flash/<oldload>**

Note: There is a mandatory space between **image-file** and **/flash** in the syntax this sub-step.

- g** set the primary config file to the saved configuration by typing:

**config bootconfig choice primary config-file
/pcmcia/<cfgbkup>**

Note: Configure the primary config file to ensure that the original configuration was not changed during the upgrade process.

- h** save the bootconfig file by typing:

sav bootconfig

- 106** Roll back Ethernet Routing Switch 8600 Chassis N software upgrade by typing:



boot /flash/<oldboot>

ATTENTION

This command automatically upgrades the primary-image file (including the ATM-image if present) and boot monitor at the same time.

The Ethernet Routing Switch 8600 reboots loading the original software image. The reboot takes approximately 15 to 20 seconds. Serial connectivity is maintained during the reboot.

Note: If the reboot is unsuccessful make sure the path is correct and try again. If the problem persists contact your next level of support.

- 107** If using an XA-core, skip to [step 112](#).

- 108** Select the next step as follows

If the STORM disk is on	Do
a Dothill device	step 109
a STORM IA (SAM-XTS) device ¹	step 112

1. The SAM-XTS configuration uses dual-homed split multilink trunks (SMLT). Both STORM volumes are recognized by both Ethernet Routing Switch 8600 routers. Therefore, taking down one router in an SAM-XTS configuration does not affect the STORM volume being addressed.

109 Select the next step as follows.

If	Do
the volumes on any STORM disk (for example, sd01) are actively mounted in DIRP ¹	step 110
the volumes on the STORM disk are not actively mounted in DIRP ²	step 112

1. Loss of network connectivity between SOS, the call processing application, and the active STORM disk can cause some or all DIRP volumes to be marked “INER-ROR,” resulting in permanent loss of data.

2. Regardless of whether DIRP volumes are mounted, the procedure can result in an unavailable STORM disk and associated volumes.

110 Return to service all disk volumes connected to the Ethernet Routing Switch 8600 chassis that was upgraded.

>diskadm sd0N; rts all

where:

sd0N is the STORM volume defined in [Note 2](#) of [step 64](#)

111 Individually remount all volumes in DIRP. (Ensure you are at the nodisp;mtc;iod;dirp level of the MAPCI for this step.)

>mnt <subsystem> <volume> <variable>

Note 1: The <variable> parameter is not required when mounting and demounting regular DIRP volumes.

Note 2: Nortel recommends recording all subsystems, volume, and variable information for each volume remounted in this step.

Use the Ethernet Routing Switch 8600 CLI to verify all hardware and software on the master Ethernet Routing Switch 8600:

- 112** Confirm master Ethernet Routing Switch 8600 is operating correctly as follows:

Note: Refer to [step 3](#) of [Upgrading Ethernet Routing Switch 8600 software for the CS-LAN](#) for more information

- a** check the log file by typing:

sho log file

Review the info and correct any errors or problems reported.

- b** check the configuration by typing:

sho config

Output similar to the following appears.

```
#<output date and time info>
#boxtype : Passport-8010
#software version : W.X.Y.Z
#monitor version : W.X.Y.Z/NNN
#<output continues>
```

where W.X.Y.Z provides release information and the NNN can be ignored.

Review the configuration file (showing network topology and configuration) and correct any incorrect configurations.

Note: Software version is the load or image version.
Monitor version is the bootflash version.

- c** check the address resolution protocol information by typing:

sho ip arp info

Review the IP ARP file and correct any MAC address problems.

Use the SAM21 EM to unlock the inactive GWCs and SCs:

- 113** Launch the SAM21EM client.

The SAM21 EM GUI appears.

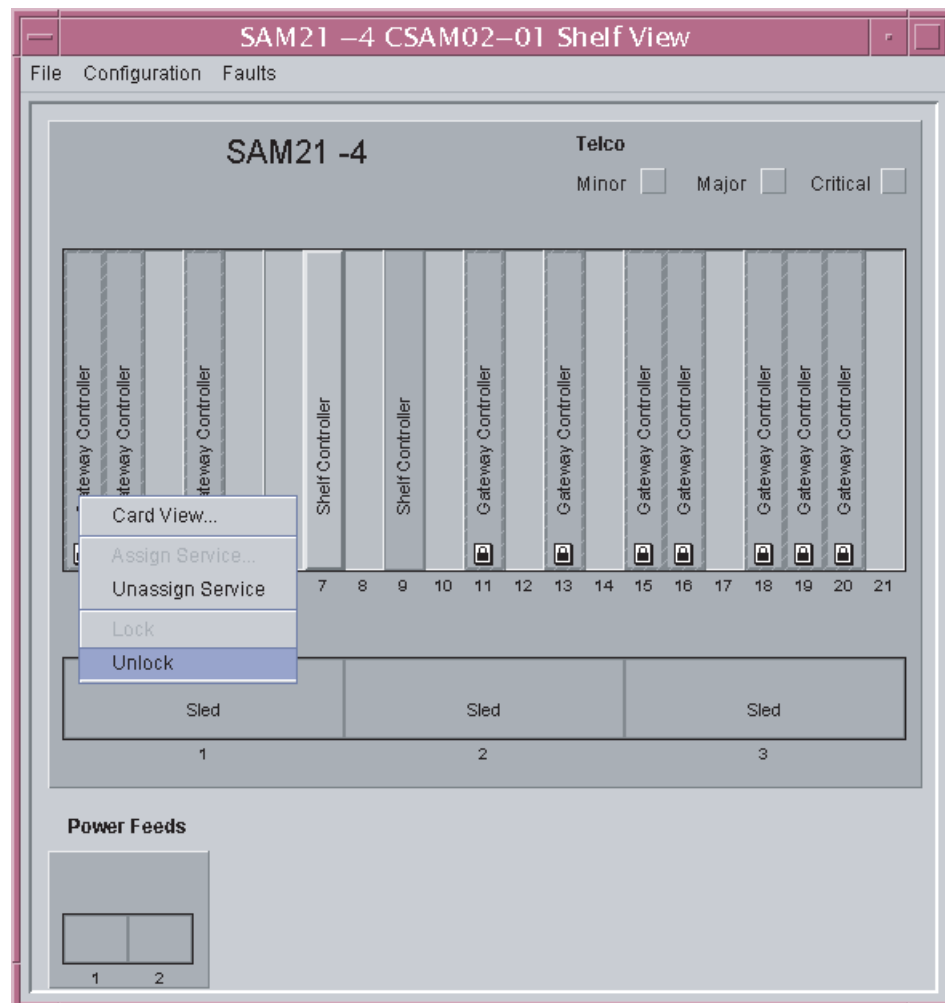
114 Select the next step as follows:

If the GWC software release is	Do
from lower than SN06	step 115
from SN06 or greater	step 116

115 Unlock each locked Gateway Controller unit as follows:

- right click on a locked Gateway Controller Unit
- select **Unlock** from the drop-down menu that appears
- repeat sub-[step a](#) and sub-[step b](#) until all units are unlocked.

Note: A padlock icon identifies locked GWC units.



- 116** Select the next step as follows:

If rolling back with an	Do
Trimodal solution	step 117
ATM solution	step 117
IP solution	step 119

Use the SAM21 Element Manager to unlock the inactive SCs:

- 117** Launch the SAM21 Element Manager.

The SAM21 EM GUI appears. Padlock icons identify locked SC blades.

- 118** From the SAM21 EM shelf view, right click on each of the locked SC blades in turn and do the following:

- a** Select **Unlock** from the drop-down menu that appears.
- b** Repeat sub-[step a](#) until all locked SC blades are unlocked.

- 119** Select the next step as follows:

If the USP Compact is:	Do
used	step 120
not used	step 156

Use the SAM21 EM to perform the following additional steps (for USP Compact only):

- 120** Re-access the SAM21 EM. Unlock the slave USPc.

Note 1: Unlocking the slave USPc from the SAM21 EM enables the USPc GUI.

Note 2: An alternative method to Unlock the blade from the SAM21 EM is to first open the card by double clicking on it. Then click the Unlock button towards the upper-right portion from display of the States tab.

Use the USPc GUI to perform the following additional steps:

- 121** Re-access the USPc GUI, waiting to ensure that the inactive blade is enabled and locked.

Note: Re-accessing the USPc GUI can take several minutes.

- 122** Select **Configuration --> platform --> Node**.

The Administration tab of the USPc GUI displays.

The screenshot shows the Administration tab of the USPc GUI. The interface includes a top toolbar with buttons for New, Add, Modify, Delete, Lock, Unlock (highlighted), 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:**
 - slot-type: usp-compact
 - slot-name: USP1
 - slot-description: USP-Compact #1
 - shelf: 0
 - slot: 15
 - t1-e1-mode: t1
 - ext-ip-address: 47.131.125.82
 - ext-subnet-mask: 255.255.255.128
 - ext-gateway: 47.131.125.126
 - front-pec: NTRX51FN
- Operational Data:**
 - operational-state: enabled
 - administrative-state: unlocked
 - procedural-state: null
 - availability-state: null
 - activity-state: inactive
 - rex-status:
- Boot Data:**
 - status-message:
 - running-image: samss7_ppc750_10_00_01_06g
 - ha-running-image: ss7t1e1ha_ppc8260_10_00_01_06g
 - running-snapshot: current active
 - boot image: uspc_10_00_01_06g_base
 - ha-boot-image: uspc_10_00_01_06g_t1e1ha
 - boot-snapshot: current active
 - snapshot-description: current active
 - snapshot-date:
 - snapshot-version:

At the bottom, there is a status bar showing "loading complete" and a navigation bar with buttons for back, forward, and search.

123 Unlock the slave USPc blade.

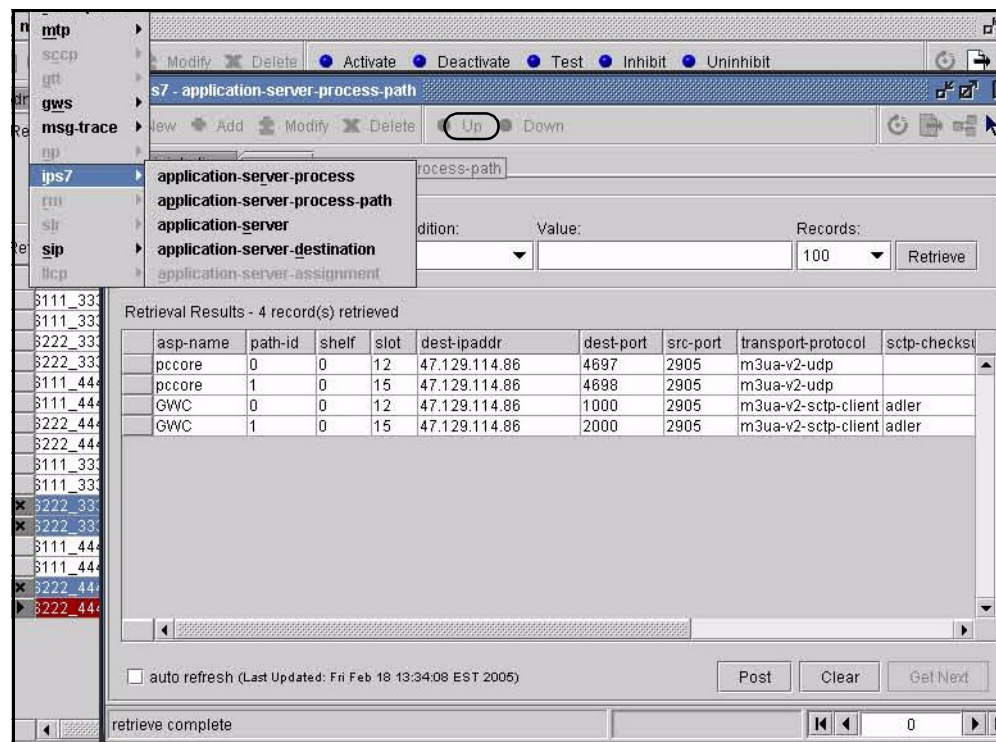
Click the Unlock button in the upper-middle portion of the screen.

124 Reactivate the IPS7 paths and the SS7 links associated with the slave USPc blade.

125 Post the IPS7 paths that use the slave USPc blade.

From the menu, select **Configuration --> ips7 --> application-server-process-path** from the pull-down menu.

The following figure displays.



- 126** Select all the IPS7 paths against the slave USPc blade. Click the Up button in the upper-right portion of the screen.

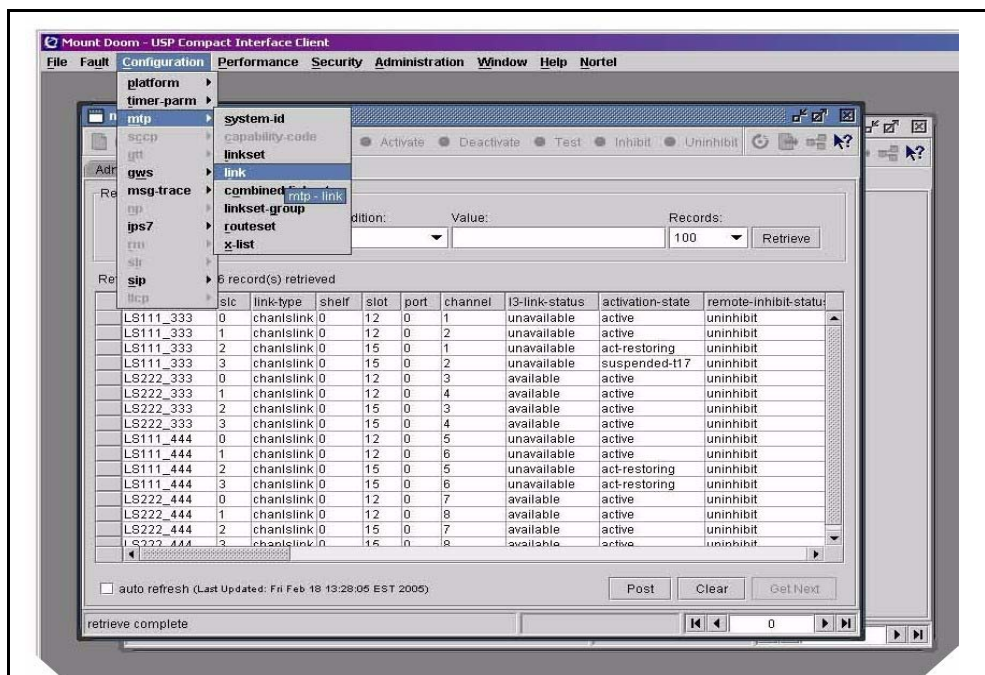
The following prompt displays:

The up command will be executed for all posted records. Are you sure you want to continue?

- 127** Select Yes to execute the command on the IPS7 paths on the slave USPc blade.
- 128** Reactivate the SS7 links and the paths associated with the slave USPc blade.

From the Administration tab, select **Configuration --> MTP --> Links** from the pull-down menu.

The following figure appears.



- 129 Select any SS7 links displayed in the form that are against the slave blade. Click the Activate button towards the upper-middle portion of the screen.
- 130 Select Yes to execute the command on the selected links.
- 131 Using the same screen, reselect the links. Click the Uninhibit button in the upper-right portion of the screen.
- 132 Select Yes to execute the command on the selected links.
- 133 If desired, perform an optional SWACT on the USPc blades to restore initial mastership states.

To perform a SWACT, redisplay the Administration tab, as shown in [step 122](#). Press the Swact button in the upper-right portion of the screen.

- 134 Select the next step as follows:

If your office is	Do
in a Geographic Survivability environment	step 135 through step 155
not in a Geographic Survivability environment	step 157

Use the SAM21 EM to unlock the inactive Call Agent card

- 135** Re-access the SAM21 EM. Unlock the locked inactive Call Agent card.

Note: An alternative method to Unlock the blade from the SAM21 EM is to first open the card by double clicking on it. Then click the Unlock button towards the upper-right portion from display of the States tab.

- 136** Wait for the lock icon to disappear.
- 137** At the Call Agent Manager, verify that the call processing application loads successfully and waits for synchronization.

Use the MAP display to perform a LIMITED_PRESWACT on the inactive Call Agent

- 138** If the switch is in sync, first perform a drop synchronization from the ccamtc apply level.

> **ccamtc**
> **coremtc**
> **appl**
> **dpsync**

- 139** At the MAP display, enter the following command:

> **BCSUPGRADE; LIMITED_PRESWACT**

Note 1: If a LIMITED_PRESWACT process fails to complete, LIMITED_PRESWACT stops and displays additional information. When this occurs, use the information to investigate and correct the problem.

Note 2: All LIMITED_PRESWACT steps must be completed prior to SWACTing.

The LIMITED_PRESWACT command displays a warning:

*Limited_Preswact should not be used for
BCSUPGRADE SWACTs. Do you wish to continue?
Please confirm ("YES", "Y", "NO", "N"):*

- 140** Enter Y.

> **Y**

- 141** If the LIMITED_PRESWACT process halts, re-enter the following command to continue.

> **LIMITED_PRESWACT**

The inactive unit indicates /restart at the Call Agent Manager. Several more steps execute and complete at the MAP. Successful completion is indicated by display of the following message:

*Total execution time for all complete procedures
00:07:31.362
All LIMITED_PRESWACT steps completed
successfully.*

142 Select the next step as follows

If the (inactive) Call Agent card is	Do
not connected to the ERS 8600 being upgraded	step 143
connected to the ERS 8600 being upgraded	step 157

Perform a NORESTARTSWACT

143 If the active Call Agent card is connected to the Ethernet Routing Switch 8600 to be upgraded, minimize the possibility of an outage by performing a NORESTARTSWACT.

a Check the status:

> BCSUPDATE:SWACTCI;STATUSCHECK

The following response displays:

*SWACTCI:
Checking Nodes Status
STATUSCHECK successful*

b Execute the NORESTARTSWACT.

> NORESTARTSWACT

Progress is printed and the process stops to verify that the inactive Call Agent is not jammed.

*Beginning SWACT checks:
All the SWACT checks have finished
successfully.
The VR_PRESWACT_TRANSFER step completed
successfully.
All INSV and ISTB series 1 PMs will have execs
loaded after the SWACT.
Device Checking Status:
NOMATCH option is set to OFF <default
setting>.
Device matching during CC WARM SWACT Enabled.
Do you wish to continue?*

Please confirm ("YES", "Y", "NO", or "N"):
>

- c** Enter a Y if the only alarm is an APPL simplex.

> Y

The final progress follows. Activity also switches at the Call Agent Manager.

All Pre_SWACT checks completed. Starting Warm SWACT now.

***** The cursor will not be returned. *****
***** unless a critical failure occurs. *****
***** Now monitoring Warm SWACT messages. *****

Pre-initialization done
Communication established
Exchange of data with the mate done
Transfer of data done (FASPECT)
Data estimation done

- d** The telnet session to the active and inactive call processing applications are lost. Re-establish the connection. Refer to the Interface set in section Call Agent Upgrades for this procedure.

Perform a POSTSWACT

- 144** At the MAP display, enter the following command to run a Postswact through completion.

> BCSUPDATE;POSTSWACT

- 145** Enter Y when prompted at the CA_SYNC step.

> Y

Verify availability of NFS mounts on STORM

- 146** At the Call Agent Manager, query the NFS mounts to ensure that they are accessible on STORM 1.

> ccamtc

> coremtc

> sys

> querynfs

- 147** From the resulting screen display, verify that all mounts are accessible.

- 148** Select the next step as follows.

If all mounts	Do
are accessible	step 149
are not accessible	Refer to procedure “Verify NFS Availability” in section <i>Upgrading the STORM</i> in this document for details.

Return to service disk volumes on SD0X

- 149** Return to service all disk volumes connected to the Ethernet Routing Switch 8600 chassis that were upgraded.

>diskadm sd0N; rts all

where:

sd0N is the STORM volume defined in [Note 2](#) of [step 64](#)

Mount DIRP volumes

- 150** Individually remount all volumes in DIRP. (Ensure you are at the nodisp;mtc;iod;dirp level of the MAPCI for this step.)

>mnt <subsystem> <volume> <variable>

Note 1: The <variable> parameter is not required when mounting and demounting regular DIRP volumes.

Note 2: Nortel recommends recording all subsystems, volume, and variable information for each volume remounted in this step.

Use the IEMS GUI to unlock the MS 2000 node

- 151** Launch the IEMS GUI.

Note: Refer to NTP *Integrated EMS Basics*, NN10329-111, for details on logging into the IEMS GUI.

- 152** Select **Applications ---> Integrated EMS --->Network Elements**.

- 153** Select the MS 2000 Series node to be unlocked and right click on its icon.

- 154** Select the Config and Maintenance Tool from the pop-up menu.
The Config and Maintenance Tool launches.

- 155** From the left side of the Config and Maintenance Tool screen, click the **Unlock** button under the Lock State options to unlock the MS 2000 node.

156 Select the next step as follows:

If the Communication Server uses:	Do
an XA-Core	step 157
a Compact chassis	step 159

Use the XA-Core MAP terminal to enable the Ethernet link with Ethernet Routing Switch 8600 Chassis N

157 Access the ETHR level of the MAP display by typing:

MAPCI;XAC;MTC;ETHR

158 Refer to the tables below and enable the Ethernet link between the XA-Core and Ethernet Routing Switch 8600 Chassis N by doing either sub-step a or sub-step b as appropriate.

- a** if the XA-Core uses HIOPs or HCMICs, type (otherwise do sub-step b):

rts <slot> r link

HIOPs/HCMICs	N = 0	N = 1
<slot>	5	14

go to [step 159](#)

- b** if the XA-Core uses IOPs with ETHR packlets, type:

rts <slot1> r l link

wait for the command to complete then type:

rts <slot2> r l link

IOP with ETHRs	N = 0	N = 1
<slot1>	5	6
<slot2>	13	14



Use the Ethernet Routing Switch 8600 CLI to reset the VRRP priority settings and OSPF cost metrics and swap the Ethernet Routing Switch 8600 master/slave status:

- 159** Make sure Ethernet Routing Switch 8600 Chassis N is in service as follows:

- a** check the IP route information by typing:

sho ip route info

The IP route information file appears. Review the file and verify that the route information is correct.

- b** check the IP VRRP information by typing:

sho ip vrrp info

The IP vrrp information file appears. Review the file and verify that the information is correct.

- 160** Reset the VRRP priority and OSPF metrics for Chassis N as follows:

- a** type:

config vlan <vid> ip vrrp <vrid> prio <setting>

Note: See [step 2](#) for <vid> and <vrid> values for Chassis N.

The VRRP priority metric is reset to its operational value.

- b** type:

config vlan <vid> ip ospf metric <value>

Note: See [step 2](#) for the OSPF metric for <value>.

The OSPF metrics reset to their original value.

- c** Save the new Ethernet Routing Switch 8600 configuration by typing:

sav config

This updates the new Ethernet Routing Switch 8600 configuration so that VRRP settings are maintained after any subsequent reboot.

- 161** Swap the Ethernet Routing Switch 8600 master/slave status on Chassis X by typing:

config vlan <vid> ip vrrp <vrid> priority <prio>

where <prio> is priority information that determines which Ethernet Routing Switch 8600 is master and which one is slave.

Note 1: Refer to [step 2](#) for the applicable <vid>, <vrid>, and <prio> values.

Note 2: The Ethernet Routing Switch 8600 <prio> is higher for the master Ethernet Routing Switch 8600 chassis than for slave.

The master Ethernet Routing Switch 8600 becomes the new slave Ethernet Routing Switch 8600 (the old slave Ethernet Routing Switch 8600 becomes the new master).

- 162** Increment the iteration index ($N = N+1$) and select the next step as follows:

If	Do
N = 1	step 3 (second pass)
N = 2	step 163

Note: In the second iteration (where $N = 1$), when repeating [step 3](#) through [step 162](#), use Chassis X in place of Chassis N. Ethernet Routing Switch 8600 Chassis 1 (identified as Chassis N) is the slave and Ethernet Routing Switch 8600 Chassis 0 (identified as Chassis X) is the master.

- 163** The procedure is complete.

Downgrading the CS 2000 Management Tools software

This section provides the information required to roll back a software upgrade and revert to the previous release of the software. Follow the link associated with the release you are downgrading to.

- [Downgrading to \(I\)SN06.2 on page 325](#)
- [Downgrading to \(I\)SN07 on page 328](#)

Note: It is highly recommended that all console and telnet sessions used during rollbacks, be logged to a file to assist in any necessary troubleshooting.

Downgrading to (I)SN06.2

Follow the link according to your office configuration.

- [Rollback on Sun Netra t1400 and Sun Netra 240 one-server configuration on page 325](#)
- [Rollback on Sun Netra 240 two-server configuration on page 326](#)

Rollback on Sun Netra t1400 and Sun Netra 240 one-server configuration

Use the table below as a checklist during the rollback of the SSPFS and CS 2000 Management Tools software to (I)SN06.2. Place a check (✓) in the ✓column as you complete each procedure.

Downgrading a Sun Netra t1400 or Sun Netra 240 (one-server configuration) to (I)SN06.2

Activities	✓	Procedures
1 Restore the file systems and Oracle data from backup media.		Refer to procedure Performing a full system restore on an SSPFS-based server on page 331 .
2 Restore the APS audio files from backup media. Note: Only perform this procedure if the APS is present on the server.		Refer to procedure Performing a restore of APS audio files from tape on page 343 or Performing a restore of APS audio files from CD on page 345 .
3 Clear the Java™ Web Start (JWS) cache on the client workstation.		Refer to procedure Clearing the JWS cache on a client workstation on page 347 .

Note: Restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN08.

Rollback on Sun Netra 240 two-server configuration

Follow the link according to whether only one server in the cluster was upgraded to (I)SN08, or both servers in the cluster were upgraded to (I)SN08.

- [Downgrading the only upgraded server in the cluster on page 326](#)
- [Downgrading both upgraded servers in the cluster on page 327](#)

Downgrading the only upgraded server in the cluster

Use the table below as a checklist during the rollback of the SSPFS and CS 2000 Management Tools software to (I)SN06.2 on the only upgraded server. Place a check (✓) in the ✓column as you complete each procedure.

Downgrading the only upgraded server to (I)SN06.2

Activities		✓	Procedures
1	Clone the image of the server with the (I)SN06.2 software onto the other (upgraded) server.		Refer to procedure Cloning the image of one node in a cluster to the other node on page 351 .

Note: Cloning the image of the (I)SN06.2 server onto the server that was upgraded, restores the server as it was before the upgrade to (I)SN08.

Downgrading both upgraded servers in the cluster

Use the table below as a checklist during the rollback of the SSPFS and CS 2000 Management Tools software to (I)SN06.2 on both upgraded servers. Place a check (✓) in the ✓column as you complete each procedure.

Downgrading both upgraded servers to (I)SN06.2

Activities	✓	Procedures
1 Restore the file systems and Oracle data from backup media.		Refer to procedure Performing a full system restore on an SSPFS-based server on page 331 .
2 Restore the APS audio files from backup media. Note: Only perform this procedure if the APS is present on the server.		Refer to procedure Performing a restore of APS audio files from tape on page 343 or Performing a restore of APS audio files from CD on page 345 .
3 Clone the image of the server you just downgraded to (I)SN06.2, onto the other server.		Refer to procedure Cloning the image of one node in a cluster to the other node on page 351 .
4 Clear the Java™ Web Start (JWS) cache on the client workstation.		Refer to procedure Clearing the JWS cache on a client workstation on page 347 .

Note: Restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN08.

Downgrading to (I)SN07

Follow the link according to your office configuration.

- [Rollback on Sun Netra t1400 and Sun Netra 240 one-server configuration on page 325](#)
- [Rollback on Sun Netra 240 two-server configuration on page 326](#)

Rollback on Sun Netra t1400 and Sun Netra 240 one-server configuration

Use the table below as a checklist during the rollback of the SSPFS and CS 2000 Management Tools software to (I)SN06.2. Place a check (✓) in the ✓column as you complete each procedure.

Downgrading a Sun Netra t1400 or Sun Netra 240 (one-server configuration) to (I)SN06.2

Activities		✓	Procedures
1	Restore the file systems and Oracle data from backup media.		Refer to procedure Performing a full system restore on an SSPFS-based server on page 331 .
2	Clear the Java™ Web Start (JWS) cache on the client workstation.		Refer to procedure Clearing the JWS cache on a client workstation on page 347 .

Note: Restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN08.

Rollback on Sun Netra 240 two-server configuration

Follow the link according to whether only one server in the cluster was upgraded to (I)SN08, or both servers in the cluster were upgraded to (I)SN08.

- [Downgrading the only upgraded server in the cluster on page 326](#)
- [Downgrading both upgraded servers in the cluster on page 327](#)

Downgrading the only upgraded server in the cluster

Use the table below as a checklist during the rollback of the SSPFS and CS 2000 Management Tools software to (I)SN06.2 on the only upgraded server. Place a check (✓) in the ✓column as you complete each procedure.

Downgrading the only upgraded server to (I)SN06.2

Activities	✓	Procedures
1 Clone the image of the server with the (I)SN07 software onto the other (upgraded) server.		Refer to procedure Cloning the image of one node in a cluster to the other node on page 351 .

Note: Cloning the image of the (I)SN07 server onto the server that was upgraded, restores the server as it was before the upgrade to (I)SN08.

Downgrading both upgraded servers in the cluster

Use the table below as a checklist during the rollback of the SSPFS and CS 2000 Management Tools software to (I)SN06.2 on both upgraded servers. Place a check (✓) in the ✓column as you complete each procedure.

Downgrading both upgraded servers to (I)SN06.2

Activities	✓	Procedures
1 Restore the file systems and Oracle data from backup media.		Refer to procedure Performing a full system restore on an SSPFS-based server on page 331 .
2 Clone the image of the server you just downgraded to (I)SN07, onto the other server.		Refer to procedure Cloning the image of one node in a cluster to the other node on page 351 .
3 Clear the Java™ Web Start (JWS) cache on the client workstation.		Refer to procedure Clearing the JWS cache on a client workstation on page 347 .

Note: Restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN08.

Performing a full system restore on an SSPFS-based server

Application

Use this procedure to perform a full system restore from backup media on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra t1400 or Sun Netra 240).

A full system restore consists of reverting to the previous release of SSPFS, restoring the file systems, and restoring the oracle data.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

Note: Restoring the oracle data does not apply to the CBM as it does not use an oracle database.

ATTENTION

System logs indicating application and database errors generate until the file systems and oracle data are restored on the system using this procedure and procedure [Restoring the oracle data on an SSPFS-based server on page 337](#). No database errors generate on the CBM as it does not use an oracle database.

Prerequisites

This procedure has the following prerequisites:

- SSPFS CD disk#1 for the release you are reverting to
- tape, CD or DVD on which you backed up the file systems
- tape, CD or DVD on which you backed up the oracle data

Action

Use one of the methods below according to your office configuration.

- [Simplex configuration \(one server\) on page 332](#)
- [High-availability configuration \(two servers\) on page 334](#)

Note: Only the [Simplex configuration \(one server\)](#) uses a full system restore from tape on a Sun Netra t1400 server.

Simplex configuration (one server)

At the server console

- 1 Log in to the server through the console (port A) using the root user ID and password.
- 2 Bring the system to the OK prompt by typing
`# init 0`
and pressing the Enter key.
- 3 Insert SSPFS CD disk#1 into the drive.
- 4 Use the following table to determine your next step.

If restoring from	Do
tape	step 5
CD or DVD	step 6

- 5 Insert the tape with the backed up file systems into the drive.
- 6 At the OK prompt, restore the system by typing
`OK boot cdrom - restore`
and pressing the Enter key.
- 7 When prompted, accept the software license restrictions by typing
`ok`
and pressing the Enter key.

The system reboots.

If restoring from CD or DVD, you will be prompted to insert Volume 1 of the backup CD or DVD into the drive. Insert the CD or DVD on which you backed up the file systems. During the restore process, the system will prompt you for additional Volumes if more than one CD or DVD was used during the backup of file systems.

The restore process can take several hours to complete depending on the number and size of the files that are being restored.

Note: Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.

8 Eject the backup CD or DVD from the drive as follows:

a Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

b Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

Note: If the DVD drive tray does not open (if not busy or being read from or written to), enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.

c Remove the backup CD or DVD from the drive.

9 Proceed as follows:.

If	Do
this SSPFS-based server is hosting the CBM	step 13
otherwise	step 10

10 List the oracle groups by typing

```
# groups oracle
```

and pressing the Enter key.

If the output is	Do
oinstall data dba or oinstall dba data	step 11
oinstall dba data	step 12

- 11 Correct the oracle groups by typing
`# usermod -g oinstall -G data,dba oracle`
and pressing the Enter key.
- 12 Restore the oracle data using procedure [Restoring the oracle data on an SSPFS-based server on page 337](#). Once the data restore is complete, continue to [step 13](#).
- 13 Reboot the server by typing
`# init 6`
and pressing the Enter key.
- 14 The procedure is complete.

High-availability configuration (two servers)

At the console connected to the inactive node

- 1 Log in to the inactive node through the console (port A) using the root user ID and password.
- 2 Bring the system to the OK prompt by typing
`# init 0`
and pressing the Enter key.

At the console connected to the active node

- 3 Log in to the active node through the console (port A) using the root user ID and password.
- 4 Access the OK prompt by typing
`# init 0`
and pressing the Enter key.
- 5 Insert SSPFS CD disk#1 into the drive.
- 6 At the OK prompt, restore the system by typing
`OK boot cdrom - restore`
and pressing the Enter key.
- 7 When prompted, accept the software license restrictions by typing
`ok`
and press the Enter key.
The system reboots.

- 8 When prompted, insert Volume 1 of the CD or DVD on which you backed up the file systems, into the drive.

Note: During the restore process, the system will prompt you for additional Volumes if more than one CD or DVD was used during the backup of file systems.

The restore process can take several hours to complete depending on the number and size of the files that are being restored.

Note: Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.

- 9 Eject the backup CD or DVD from the drive as follows:

- a Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

- b Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

Note: If the DVD drive tray does not open (if not busy or being read from or written to), enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.

- c Remove the backup CD or DVD from the drive.

- 10 Use the following table to determine your next step.

If	Do
this SSPFS-based server is hosting the CBM	step 14
otherwise	step 11

- 11 List the oracle groups by typing
groups oracle
and pressing the Enter key.

If the output is	Do
oinstall data dba or oinstall dbs data	step 12
oinstall dba data	step 13

- 12 Correct the oracle groups by typing
usermod -g oinstall -G data,dba oracle
and pressing the Enter key.
- 13 Restore the data using procedure [Restoring the oracle data on an SSPFS-based server on page 337](#). Once the data restore is complete, execute [step 14](#) and [step 15](#).
- 14 Reboot the server by typing
init 6
and pressing the Enter key.
- 15 Re-image the inactive node using the active node's image. If required, refer to procedure [Cloning the image of one node in a cluster to the other node](#).
You have completed this procedure.

Restoring the oracle data on an SSPFS-based server

Application

Use this procedure to restore the oracle data from a backup tape, CD or DVD on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra t1400 or Sun Netra 240). Also use this procedure to restore the data that was automatically backed up to a file on the server by the backup restore manager.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

Note: Restoring the oracle data is not applicable to the CBM as it does not use an oracle database.

Prerequisites

This procedure requires the oracle data backup tape, CD or DVD. If the data was saved through the backup restore manager, the name of the file located in directory “/data/bkresmgr/backup” is required.

Action

Perform the following steps to complete this procedure.

At the server

- 1 Insert the tape, CD or DVD containing the oracle data backup into the drive. If restoring the data from a file, start at [step 2](#).

At your workstation

- 2 Log in to the server by typing
`> telnet <server>`
 and pressing the Enter key.
 where
 server
 is the IP address or host name of the SSPFS-based server on which you are performing the data restore
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing
`$ su - root`
 and pressing the Enter key.
- 5 When prompted, enter the root password.
- 6 Verify the permissions on the restore log directory (bkslog) by typing
`# ls -alrt /var/opt/nortel`
 and pressing the Enter key.

Example response

```
total 22
lrwxrwxrwx  1 root    succssn      28 Dec 22  2003 gwc
-> /net/47.141.126.131//swd/gwc
drwxrwxr-x  4 root    other         512 Dec 22  2003 .
drwxr-xr-x  7 root    sys           512 Sep 10 12:41 ..
drwxr-xr-x  2 oracle  oinstall    512 Dec  8 15:58 db
drwxrwxrwt  2 root    other        6656 Dec 15 19:56 bkslog
```

**If the permissions of
bkslog**

Do

are drwxrwxrwt

[step 8](#)

are not drwxrwxrwt

[step 7](#)

- 7 Change the permissions of bkslog by typing
chmod 777 /var/opt/nortel/bkslog
- 8 If not already done, stop the server applications that run on the server.

For	Refer to
CS 2000 Management Tools server applications	Stopping the SESM server application Stopping the SAM21 Manager server application Stopping the NPM server application in <i>ATM/IP Security and Administration</i> , NN10402-600
MG 9000 Manager and mid-tier server applications	the <i>MG9000 Security and Administration</i> , NN10162-611
Integrated EMS server application	<i>IEMS Security and Administration</i> , NN10336-611

- 9 Use the following table to determine your next step.

If	Do
restoring from tape, CD or DVD	substep a
restoring from a file	substep b

- a Restore the database from backup tape, CD or DVD by typing
\$ **/opt/nortel/sspfs/bks/rsdata**
and pressing the Enter key.
Proceed to [step 10](#).

- b** Restore the database from the backup file by typing

```
$ /opt/nortel/sspfs/bks/rsdata -f  
/data/bkresmgr/backup/<filename>
```

and pressing the Enter key.

where

filename

is the name of the backup file created by the backup restore manager

Proceed to [step 11](#).

- 10** Remove the tape from the drive, or eject the CD or DVD from the drive as follows:

- a** Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

- b** Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

Note: If the DVD drive tray does not open (if not busy or being read from or written to), then enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Press the eject button located on the front of the DVD drive.

- c** Remove the CD or DVD from the drive.

- 11** Verify that the database restored properly.

12 Start the server applications that run on the server.

For	Refer to
CS 2000 Management Tools server applications	Starting the SESM server application Starting the SAM21 Manager server application Starting the NPM server application in <i>ATM/IP Security and Administration</i> , NN10402-600
MG 9000 Manager and mid-tier server applications	the <i>MG9000 Security and Administration</i> , NN10162-611
Integrated EMS server application	<i>IEMS Security and Administration</i> , NN10336-611

You have completed this procedure.

Performing a restore of APS audio files from tape

Application

Use this procedure to perform a restore of APS audio files from a backup tape on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun t1400) running the SN06.2 or greater release of the SSPFS.

ATTENTION

This procedure only applies to a Sun Netra t1400-type server with a DAT drive. If you have a Sun Netra 240-type server, use procedure [Performing a restore of APS audio files from CD on page 345](#).

Prerequisites

You need the tape on which you backed up the APS audio files.

At the server

- 1 Insert the tape on which you backed up the APS audio files into the DAT drive on the server where the APS resides.

At the server

- 2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server on which you are restoring the APS audio files
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 5 When prompted, enter the root password.

- 6 Change directory to the root file system by typing

```
# cd /
```

and pressing the Enter key.

- 7 Restore the audio files to the file system by typing

```
# tar xvf /dev/rmt/0
```

The files are read from tar and placed in the following file systems: /audio_files and /user_audio_files.

You have completed this procedure.

Performing a restore of APS audio files from CD

Application

Use this procedure to perform a restore of APS audio files from a backup CD or DVD on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra 240) running the SN06.2 or greater release of the SSPFS.

ATTENTION

This procedure only applies to a Sun Netra 240-type server with a CD/DVD drive. If you have a Sun Netra t1400-type server, use procedure [Performing a restore of APS audio files from tape on page 343](#).

Prerequisites

You need the CD or DVD on which you backed up the APS audio files.

At the server

- 1 Insert the CD or DVD on which you backed up the APS audio files into the drive on the server where the APS resides.

At the server

- 2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server on which you are restoring the APS audio files
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- 5 When prompted, enter the root password.

- 6 Change directory to the root file system by typing

```
# cd /
```

and pressing the Enter key.

- 7 Restore the audio files to the file system by typing

```
# cp /cdrom/cdrom0/* /
```

and pressing the Enter key.

The files are read from cd and placed in the following file systems: /audio_files and /user_audio_files.

You have completed this procedure.

Clearing the JWS cache on a client workstation

Application

Use this procedure to clear the Java™ Web Start (JWS) cache on a client workstation.

The JWS cache on a client workstation needs to be cleared after an HTTPS certificate is installed on an existing Sun server that was not previously using a certificate. Clearing the cache allows you to properly launch the CS 2000 Management Tools client applications from your workstation.

Prerequisites

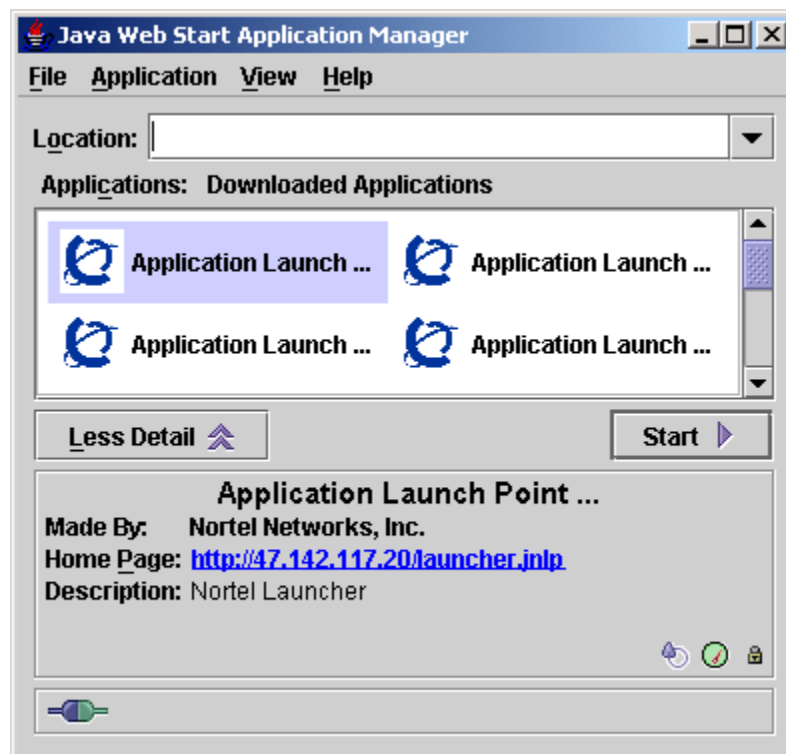
None

Action

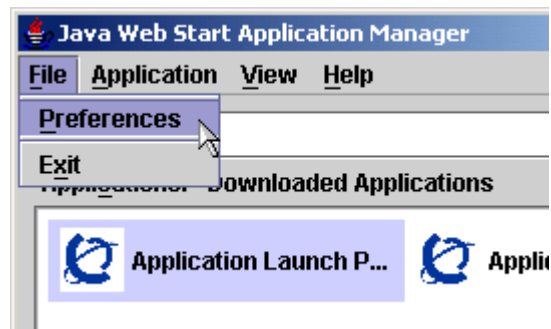
Perform the following steps to complete this procedure.

At your workstation

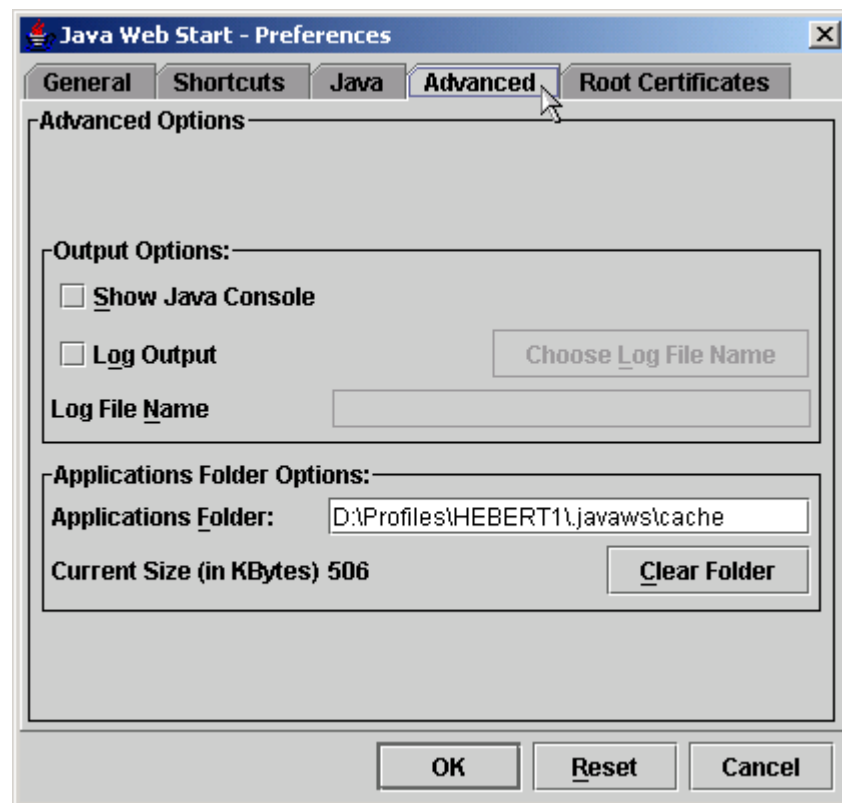
- 1 Access the Java Web Start Application Manager.



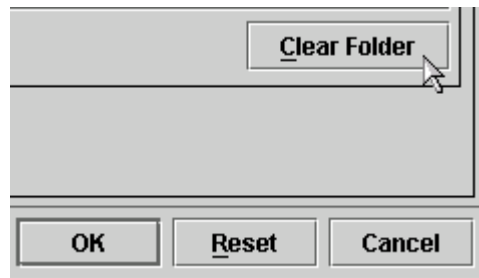
- 2 Click **File->Preferences** to access the Preferences window.



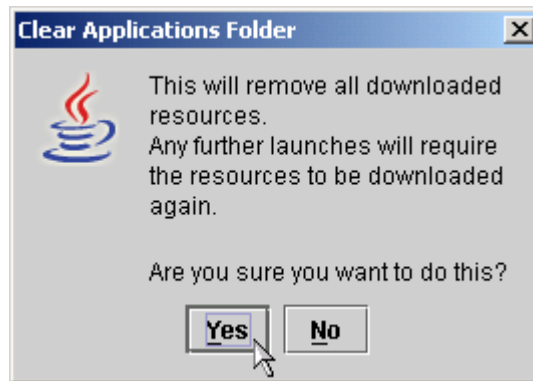
- 3 Click the **Advanced** tab to access the Advanced window.



- 4 Click **Clear Folder** to clear the cache.



- 5 Click **Yes** to confirm you want to clear the cache (remove all downloaded resources).



- 6 Click **OK** to close the Preferences window.
- 7 Exit the Java Web Start Application Manager.
- You have completed this procedure.

Cloning the image of one node in a cluster to the other node

Application

Use this procedure to clone the image of the active node in a cluster to the inactive node.

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password
- you need console access to the Inactive node if this is the first time you clone, or if you replaced the Inactive unit or executed a reverse restore (switched unit 0 and 1)

ATTENTION

Ensure no provisioning activities are in progress, or are scheduled to take place during this procedure.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Establish a login session to the Active node using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- 2 Log in to the Active node using telnet (unsecure) as follows:
 - a Log in to the Active node by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the cluster IP address, which automatically defaults to the Active node in the cluster
 - b When prompted, enter your user ID and password.

- c Change to the root user by typing
`$ su - root`
and pressing the Enter key.
 - d When prompted, enter the root password.
Proceed to step [4](#).
- 3 Log in using ssh (secure) as follows:
 - a Log in to the Active node by typing
`> ssh -l root <server>`
and pressing the Enter key.
where
server
is the cluster IP address, which automatically defaults to the Active node in the cluster
Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter *yes* at the prompt.
 - b When prompted, enter the root password.
- 4 Verify the status of replicated disk volumes by typing
`# udstat`
and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 5
not ACTIVE	contact your next level of support

5 Determine the server profile as follows:**a** 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 - exit
```

```
select -
```

b Enter the number next 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 wrtypyxp)
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 - exit
```

```
select -
```

c Enter the number next to the “sspfs_soft” option in the menu.

Example response

```
=== Executing "sspfs_soft"
```

```
SSPFS version: 08.0 Build: 200508421 Server
Profile: cbm850
```

```
=== "sspfs_soft" completed successfully
```

d Note the Server Profile.

If the Server Profile is	Do
cbm850	step 17
anything else	step 6

6 Verify that all applications on the server are running by typing

```
# servquery -status all
```

and pressing the Enter key.

Example response:

APP NAME	STATUS
=====	=====
SNMP_POLLER	RUNNING
DELEGATE	RUNNING
PROP_SRV	RUNNING
WEBSERVER	RUNNING
DATABASE	RUNNING
SAM21EM	RUNNING
SESMSERVICE	RUNNING
CORBA	RUNNING
ORA_ARCHIVE_ROTATOR	RUNNING
OMPUSH	RUNNING
BOOTP	RUNNING
WEBSERVICES	RUNNING
ORA_AUTO_BACKUP	RUNNING
APS	RUNNING
NPM	RUNNING

7 Use the following table to determine your next step.

If	Do
all applications are running	step 10
one or more applications are not running	step 8

8 Start each application that is not running by typing

```
# servstart <app_name>
```

and pressing the Enter key.

where

app_name

is the name of the application that is not in a “RUNNING” state, for example, SAM21EM

- 9 Use the following table to determine your next step.

If	Do
one or more applications do not start	contact your next level of support
all applications are running	step 10

- 10 Use the following table to determine your next step.

If this server is	Do
running the NPM software	step 11
not running the NPM software	step 13

Note: The Network Patch Manager (NPM) software is running on this server if NPM appeared in the response from step [6](#).

- 11 Verify the Patching Server Element (PSE) server application is running by typing

pse status

and pressing the Enter key.

If PSE is	Do
running	step 13
not running	step 12

- 12 Start the PSE server application by typing

pse start

and pressing the Enter key.

If PSE	Do
does not start	contact your next level of support
starts	step 13

- 13 Use the following table to determine your next step.

If this server is	Do
running the CS 2000 Management Tools software	step 14
not running the CS 2000 Management Tools software	step 17

- 14 Verify that the SESMservice application is fully functional by typing

```
# ptmctl status
```

and pressing the Enter key.

Example response:

```
SESM STATUS
```

```
-----
COMPONENT          STATUS
-----
Proxy Agent        RUNNING
RMI Registry        RUNNING
Snmpfactory         RUNNING
MI2 Server          RUNNING
```

```
Current number of SESM processes running: 4 (of 4)
```

```
SESM APPLICATION STATUS: All Applications ready
```

- 15 Use the following table to determine your next step.

If the SESMService is	Do
not fully functional	contact your next level of support
fully functional	step 16

- 16 Deconfigure NDS replication before cloning the node by typing

```
#cp /etc/nsswitch.files /etc/nsswitch.conf
#cp /etc/pam.conf.orig /etc/pam.conf
#cd
/opt/nortel/applications/security/current_slisext/swmgmt/bin
#./configure_slisext.sh -replica disable
and pressing the Enter key.
```


- 17 Use the following table to determine your next step.

If	Do
this is the first time you are cloning the unit, or you replaced the unit or executed a reverse restore (i.e. switched unit 0 and unit 1)	step 18
this is not the first time you are cloning the unit, and you did not replace the unit or execute a reverse restore (i.e. switched unit 0 and unit 1)	step 21

- 18 Use the following table to determine your next step.

If you	Do
know the Ethernet address of the Inactive unit	step 20
do not know the Ethernet address of the Inactive unit	step 19

At the console connected to the inactive node

- 19 Determine the Ethernet address of the Inactive node as follows:

- a Log in to the inactive node through the console (port A) using the root user ID and password.

Note: Ensure you are on the Inactive server by typing `ubmstat`. If `ClusterIndicatorACT` is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server. The response must display `ClusterIndicatorSTBY`, which indicates you are on the Inactive server.

- b Bring the system to the OK prompt by typing

`init 0`

and pressing the Enter key.

- c At the OK prompt, display the Ethernet address of the inactive node by typing

OK **banner**

and pressing the Enter key.

Example response:

```
Sun Fire V240, No keyboard
Copyright 1998-2002 Sun Microsystems, Inc.
All rights reserved. OpenBoot 4.8.0.build_04,
2048 MB memory installed, Serial #52964131.
Ethernet address 0:3:ba:28:2b:23, Host ID:
83282b23.
```

- d Take note of the Ethernet address that is displayed.

At your workstation (login session to the Active node)

- 20 Start the cloning process by typing

startb <Ethernet address>

and press the Enter key.

where

Ethernet address

is the Ethernet address of the Inactive unit

Proceed to step [22](#)

- 21 Start the cloning process by typing

startb

and press the Enter key.

- 22 Use the following table to determine your next step.

If the system	Do
prompts you to enter the command "boot net - image"	step 23
does not prompt you to enter the command "boot net - image"	step 27

- 23 Connect to the console port of the Inactive node.

If the console displays	Do
the OK prompt	step 26
the login prompt	step 24

At the console connected to the inactive node

- 24** Log in using the root user ID and password.
- 25** Bring the system to the OK prompt by typing
`# init 0`
and pressing the Enter key.
- 26** At the OK prompt, boot the inactive node from the image of the active node by typing
`OK boot net - image`
and press the Enter key.

Note: There must be a space between the “-” and “image”.

Example response:

SC Alert: Host System has Reset

Sun Fire V240, No Keyboard
Copyright 1998-2002 Sun Microsystems, Inc. All
rights reserved. OpenBoot 4.8.0.build_04, 2048
MB memory installed, Serial #52964131. Ethernet
address 0:3:ba:28:2b:23, Host ID: 83282b23.

Rebooting with command: boot net - image

.
.
.

SC Alert: Host System has Reset

At your workstation (login session to the Active node)

- 27** Monitor the progress of the cloning from the active node. Cloning the inactive node takes approximately one hour to complete.

Example response:

```
Waiting for network response from unit1-priv0...
received network response from unit1-priv0...
Waiting for unit1-priv0 to clone data...
waiting...1
waiting...2
waiting...3
unit1-priv0 is cloning: /export/d2
.
.
.
Verifying cluster status of unit1-priv0
waiting for cluster filesystem status to become
normal.
Deleted snapshot 0.
Deleted snapshot 1.
Deleted snapshot 2.
Deleted snapshot 3.
d99: Soft Partition is cleared
```

- 28** Once the cloning is complete, wait approximately 5 minutes before you proceed to the next step.

At your workstation (login session to the Active node)

- 29** Verify the status of replicated disk volumes by typing

udstat

and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 30
not ACTIVE	contact your next level of support

At your workstation

- 30** Establish a login session to the Inactive node using one of the following methods:

If using	Do
telnet (unsecure)	step 31
ssh (secure)	step 32

- 31** Log in to the Inactive node using telnet (unsecure) as follows:
- a** Log in to the Inactive node by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the physical IP address of the Inactive node in the cluster
 - b** When prompted, enter your user ID and password.
 - c** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
 - d** When prompted, enter the root password.
Proceed to step [33](#).
- 32** Log in using ssh (secure) as follows:
- a** Log in to the Inactive node by typing

```
> ssh -l root <server>
```

and pressing the Enter key.
where
server
is the physical IP address of the Inactive node in the cluster
Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter *yes* at the prompt.
 - b** When prompted, enter the root password.

- 33** Verify the status of replicated disk volumes by typing
`# udfstat`
and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 34
not ACTIVE	contact your next level of support

At your workstation (login session to the Active node)

- 34** Complete the cloning process by typing
`# finishb`
and pressing the Enter key.

Sessions on both the Active and Inactive nodes

- 35** Reconfigure NDS replication on both the active and inactive nodes after the cloning process is completed by typing
`#cp /etc/nsswitch.saml /etc/nsswitch.conf`
`#cp /etc/pam.conf.is /etc/pam.conf`
and pressing the Enter key.
You have completed this procedure.



ATM Solutions troubleshooting

Use this document to isolate and resolve network faults for the PT-AAL1 or UA-AAL1 solutions.

Troubleshooting workflow

This document contains troubleshooting tasks for the DMS and SPM (Spectrum peripheral module) based hardware and software used in the PT-AAL1 or UA-AAL1 solutions. The table [DMS and SPM-based troubleshooting tasks](#) lists these troubleshooting tasks and provides links to the tasks in this document.

The PT-AAL1 or UA-AAL1 troubleshooting tasks for the Multiservice Switch 15000 and Preside MDM are not contained in this document. Instead, these tasks are found in Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP), NN10198-912. The table [Multiservice Switch 15000 and Preside MDM troubleshooting tasks](#) lists the Multiservice Switch 15000 and Preside MDM troubleshooting tasks that are contained in NN10198-912.

Finding the troubleshooting tasks in this document

The table [DMS and SPM-based troubleshooting tasks](#) lists the DMS and SPM-based troubleshooting tasks that are found in this document.

The table [Multiservice Switch 15000 and Preside MDM troubleshooting tasks](#) lists the Multiservice Switch 15000 and Preside MDM tasks that are found in the document Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault

Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP),
NN10198-912.

DMS and SPM-based troubleshooting tasks

Troubleshooting task

ATM framework and call processing problems

[Troubleshooting general ATM networking problems](#)

[Troubleshooting ATM call processing problems](#)

MG 4000 CEM maintenance or recovery problems

[Troubleshooting XA-Core to MG 4000 connectivity problems](#)

[Troubleshooting MG 4000 CEM Loadmod failures](#)

[Troubleshooting MG 4000 CEM Resetmod failures](#)

[Troubleshooting a failure to RTS an MG 4000 CEM \(SysB\)](#)

[Troubleshooting a failure to RTS an MG 4000 CEM \(IsTb\)](#)

[Troubleshooting MG 4000 CEM protection switch failures](#)

Resource Module maintenance and recovery problems

[Troubleshooting a SysB or IsTb MG 4000 resource module \(RM\)](#)

[Troubleshooting Loadmod or Resetmod failures for an MG 4000 RM](#)

[Troubleshooting a failure to RTS an MG 4000 resource module \(RM\)](#)

[Troubleshooting MG 4000 RM protection switch failures](#)

Multiservice Switch 15000 and Preside MDM troubleshooting tasks (Sheet 1 of 6)

Troubleshooting Task	Document containing the task
Voice quality and call processing failures Troubleshooting call processing failures due to ATM framework problems	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting call quality problems due to ATM framework problems	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Problems updating time of day for seasonal time changes Troubleshooting problems when the seasonal time of day is not updating	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Multiservice Switch 15000 ATM backbone failures and service degradations Troubleshooting ATM backbone failures due to ATM routing problems Troubleshooting service degradation due to ATM routing problems	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP) NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Multiservice Switch 15000 base software problems	

Multiservice Switch 15000 and Preside MDM troubleshooting tasks (Sheet 2 of 6)

Troubleshooting Task	Document containing the task
Troubleshooting file system failures	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting data collection failures	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting FTP session failure	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting Userids and password failures	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting service degradation due to network synchronization problem	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting service degradation due to time server problems	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)

Multiservice Switch 15000 and Preside MDM troubleshooting tasks (Sheet 3 of 6)

Troubleshooting Task	Document containing the task
Troubleshooting service degradation due to ATM routing s problems	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Multiservice Switch 15000 hardware problems	
Troubleshooting shelf failures	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting control processor card failure	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting logical processor (LP) / function processor (FP) failures	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting LAPS failures	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting service degradation due to fabric card problems	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)

Multiservice Switch 15000 and Preside MDM troubleshooting tasks (Sheet 4 of 6)

Troubleshooting Task	Document containing the task
Troubleshooting service degradation due to SONET problems	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting service degradation due to LAPS problems	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting function processor, and sparing problems	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting control processor, and sparing problems	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Multiservice Switch 15000 recovery and upgrade problems	
Troubleshooting hitless software migration (HSM) problems	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting active equipment crashes during a migration	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)

Multiservice Switch 15000 and Preside MDM troubleshooting tasks (Sheet 5 of 6)

Troubleshooting Task	Document containing the task
Troubleshooting software and patch loading problems	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting fabric card version problems during a migration	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Preside MDM server problems	
Troubleshooting alarm display tool failures	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting PM collection failure	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting connection failures between the Multiservice Switch 15000 switch and the Preside MDM server	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)

Multiservice Switch 15000 and Preside MDM troubleshooting tasks (Sheet 6 of 6)

Troubleshooting Task	Document containing the task
Troubleshooting connection failures between the Preside MDM server and the CS 2000 Core Manager	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
Troubleshooting an IP broadcast storm	NN10198-912 Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)

Detailed troubleshooting procedures

The detailed troubleshooting procedures contained in this section are intended to be used in conjunction with the troubleshooting tasks. When you troubleshoot ATM network problems, you normally start by accessing the appropriate troubleshooting task. Within the troubleshooting tasks are references to the detailed troubleshooting procedures. If you feel that you need additional information, you simply go to the detailed procedure, then return to the troubleshooting task to continue the troubleshooting process.

The following table lists the detailed troubleshooting procedures for the ATM solutions that are included in this document.

Detailed procedure
<u>Determining the state of the ATM framework from the XA-Core</u>
<u>Determining the state of a resource module</u>
<u>Determining the state of the OC3S, STS3L, or STS3CP carriers</u>
<u>Determining the state of the PVC connections from the XA-Core to an MG 4000</u>
<u>Determining the state of the peer SVC connections for an MG 4000</u>
<u>Determining the state of the AMDI links</u>

Detailed procedure

[Correcting common problems relating to CEM configuration datafill](#)

[Determining the state of the ATMFW from the MG 4000, IW SPM, or DPT SPM](#)

[Checking the configuration of an ATM network](#)

[Resolving LAN problems](#)

[Pinging the MG 4000 CEM](#)

[Reseating a circuit pack on an MG 4000](#)

[Replacing a CEM circuit pack](#)

[Determining the state of Ethernet links](#)

[Checking the LAN configuration](#)

[Analyzing SPM 313 logs or QueryPM fault reason output for a CEM](#)

[Analyzing SPM 300 logs or QueryPM fault reason output for an RM](#)

[Replacing a resource module circuit pack](#)

[Checking the resource module configuration](#)

[Determining the state of a common equipment module](#)

Troubleshooting general ATM networking problems

Use this task to troubleshoot general ATM networking problems that occur in the ATM framework of the MG 4000, IW SPM, or DPT SPM. This task applies to situations where the ATM framework is in one of the following states:

- unequipped
- C-side busy
- system busy (not operational)
- PVC capable
- PVC-SVC capable

The following procedure describes the sequence of steps you must follow to troubleshoot general ATM networking problems.

- If the ATM framework is system busy (not operational) then jump to [step 4](#) of the procedure.
- If the ATM framework is PVC capable only, and the node is an MG 4000, then jump to [step 14](#) of the procedure.
- If the ATM framework is PVC capable only, and the node is an IW SPM or DPT SPM, then jump to [step 17](#) of the procedure.
- If the ATM framework is PVC-SVC capable, then jump to [step 21](#) of the procedure.

Note: Refer to the procedure [Determining the state of the ATM framework from the XA-Core](#) for information on how you can obtain the states above.

Procedure for troubleshooting general ATM networking problems

ATTENTION

If this is a live MG 4000, IW SPM, or DPT SPM, and the ATM framework is unequipped, then contact your next level of support.

- 1 Determine if the ATM RMs are in-service.
Refer to [Determining the state of a resource module](#).

If the ATM RMs are	Do
in-service	step 4

		If the ATM RMs are	Do
		not in-service	step 2
2	Return the ATM RMs to service.		
3	Determine if the problem still exists.		
		If the problem	Do
		has been solved	step 23
		has not been solved	step 4
4	Determine if the OC3S carriers are in-service. Refer to Determining the state of the OC3S, STS3L, or STS3CP carriers .		
		If the OC3S carriers are	Do
		in-service	step 7
		not in-service	step 5
5	Return the OC3S carriers to service.		
6	Determine if the problem still exists.		
		If the problem	Do
		has been solved	step 23
		has not been solved	step 7
7	Determine if the STS3L carriers are in-service. Refer to Determining the state of the OC3S, STS3L, or STS3CP carriers .		
		If the STS3L carriers are	Do
		in-service	step 10
		not in-service	step 8
8	Return the STS3L carriers to service.		
9	Determine if the problem still exists.		
		If the problem	Do
		has been solved	step 23
		has not been solved	step 10

- 10** Determine if the STS3CP carriers are in-service.
Refer to [Determining the state of the OC3S, STS3L, or STS3CP carriers](#).
- | If the STS3CP carriers are | Do |
|-----------------------------------|-------------------------|
| in-service | step 13 |
| not in-service | step 11 |
- 11** Return the STS3CP carriers to service.
- 12** Determine if the problem still exists.
- | If the problem | Do |
|-----------------------|-------------------------|
| has been solved | step 23 |
| has not been solved | step 13 |
- 13** Determine if the core PVC connections are in-service.
Refer to [Determining the state of the PVC connections from the XA-Core to an MG 4000](#).
- | If the core PVC connections are | Do |
|--|-------------------------|
| in-service | step 16 |
| not in-service | step 14 |
- 14** Determine if the AMDI links are in-service.
Refer to [Determining the state of the AMDI links](#).
- | If the AMDI links are | Do |
|------------------------------|-------------------------|
| in-service | step 17 |
| not in-service | step 15 |
- 15** Attempt to return the AMDI links to service.
- | If you are | Do |
|--|-------------------------|
| able to return the AMDI links to service | step 13 |
| unable to return the links to service | step 17 |
- 16** Determine if the peer SVC connections are in-service.

Refer to [Determining the state of the peer SVC connections for an MG 4000](#).

If the peer SVC connections are	Do

in-service	step 20

not in-service	step 17

17 Determine if there are problems with ATM or CEM datafill.

Refer to [Correcting common problems relating to CEM configuration datafill](#).

If there are	Do

problems with datafill	step 18

no problems with datafill	step 20

18 Correct the problems.

19 Determine if the problem still exists.

If the problem	Do

has been solved	step 23

has not been solved	step 20

20 Determine if the ATM framework on the DPT SPM, IW-SPM, or MG 4000 is operational and without problems.

Refer to [Determining the state of the ATMFW from the MG 4000, IW SPM, or DPT SPM](#).

If the ATM framework	Do

is operational	step 23

is not operational	step 21

21 Determine if there are configuration problems with the ATM network.

Refer to [Checking the configuration of an ATM network](#).

If there are	Do

configuration problems	step 22

no configuration problems	step 23

22 Contact your next level of support.

23 You have completed this procedure.

Troubleshooting ATM call processing problems

For information on ATM call processing problems, see the appropriate procedure in the document *Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)*, NN10198-912.

Troubleshooting XA-Core to MG 4000 connectivity problems

Use this task to troubleshoot general XA-Core to MG 4000 CEM connectivity problems when the MG 4000 CEM is in an isolated not available (NA) state. In other words, the state of the MG 4000 common equipment module (CEM) is either system busy not available (SysB NA) or manual busy not available (ManB NA).

Note: If the MG 4000 CEM is system busy not available, or manual busy not available, there may be no communication between the MG 4000 and the XA-Core.

The following procedure shows the sequence of steps you must follow to troubleshoot general XA-Core to MG 4000 CEM connectivity problems when the MG 4000 CEM is isolated.

Procedure for troubleshooting XA-Core to MG 4000 connectivity problems

- 1 Determine if there is a local area network (LAN) problem.
Refer to [Resolving LAN problems](#).

If there	Do
is a LAN problem	step 2
is not a LAN problem	step 4

- 2 Resolve the LAN problem.
- 3 Determine if the problem still exists.

If the problem	Do
still exists	step 4
has been fixed	step 16

- 4 Determine if the MG 4000 CEM is configured properly.
Refer to [Correcting common problems relating to CEM configuration datafill](#).

If the MG 4000 CEM	Do
is configured properly	step 7
is not configured properly	step 5

5 Correct the MG 4000 CEM configuration problem(s).

6 Determine if the problem still exists.

If the problem**Do**

still exists

[step 8](#)

has been fixed

[step 16](#)

7 Attempt to ping the CEM.

Refer to [Pinging the MG 4000 CEM](#).

If the CEM**Do**

responds to ping attempts

[step 10](#)

does not respond to ping attempts

[step 8](#)

8 Reseat the MG 4000 CEM circuit pack.

Refer to [Reseating a circuit pack on an MG 4000](#).

9 Determine if the problem still exists.

If the problem**Do**

still exists

[step 10](#)

has been fixed

[step 16](#)

10 Determine if the MG 4000 CEM Ethernet cable is properly connected.

If the cable**Do**

is properly connected

[step 13](#)

is not properly connected

[step 11](#)

11 Connect the cable properly

12 Determine if the problem still exists.

If the problem**Do**

still exists

[step 13](#)

has been fixed

[step 16](#)

13 Replace the affected MG 4000 CEM circuit pack.

Refer to [Replacing a CEM circuit pack](#).

- 14** Determine if the problem still exists.

If the problem

Do

still exists[step 15](#)

has been fixed

[step 16](#)

- 15** Contact your next level of support.

- 16** You have completed this procedure.

Troubleshooting MG 4000 CEM Loadmod failures

Use this task to troubleshoot loadmod failures that occur while trying to load an MG 4000 common equipment module (CEM).

Background information for loading software on the MG 4000 CEM

Once you issue the Loadmod command at the MAPCI, the MG 4000 CEM software performs several operations in order to obtain the MG 4000 CEM IP (Internet Protocol) addresses, and the new load. The following steps describe the sequence of events that occur from the time the Loadmod command is issued.

1. When you input the Loadmod command at the MAPCI, the system software sends a reset UDP (User Data Protocol) message to the MG 4000 CEM by means of Internet Protocol.
2. The MG 4000 CEM sends a BOOTP (Bootstrap Protocol) request to the BOOTP server on the XA-Core.
3. The BOOTP is constantly listening for incoming requests from the datafilled MG 4000 CEMs. Once the BOOTP server receives a request from an MG 4000 CEM, the BOOTP server sends the MG 4000 CEM BOOTP reply. Contained within the reply is the IP address of the CEM, the IP address of the TFTP (trivial file transfer protocol) server, the loadname of the MG 4000 CEM load that is stored on the XA-Core, and netmask information. In addition, for multi-subnet configurations, the BOOTP reply also contains the edge router information.
4. Once the MG 4000 CEM receives the response from the BOOTP server, the MG 4000 CEM sends a "read" request to the TFTP server to begin the transfer of the load. Contained in the request is the IP address of the MG 4000 CEM to which the load is to be transferred, and the name of the load.
5. Once the TFTP server receives a request, the server "looks" up the loadname, prepares the load for transfer, provisions the load, and then begins to transfer the load to the MG 4000 CEM.
6. At this point in time, the MG 4000 CEM is waiting for the data transfer from the TFTP server. The progress of the loading process is displayed on the MAPCI by a percentage value under each MG 4000 CEM that is receiving a new load.

Troubleshooting task for MG 4000 CEM loadmod failures

The following procedure describes the sequence of steps you must perform to troubleshoot MG 4000 CEM Loadmod failures.

Procedure for troubleshooting MG 4000 CEM Loadmod failures

- 1 Determine if the Ethernet links on the XA-Core are in-service.
Refer to [Determining the state of Ethernet links](#).

If the Ethernet links are	Do
in-service	step 4
not in-service	step 2

- 2 Return the Ethernet links to service.

- 3 Determine if you have eliminated the LoadMod failures.

If you have	Do
eliminated the LoadMod failures	step 17
not eliminated the LoadMod failures	step 4

- 4 Determine if the IP and MAC addresses are correct.

Refer to [Correcting common problems relating to CEM configuration datafill](#).

If the addresses	Do
are correct	step 7
are incorrect	step 5

- 5 Correct the datafill problem(s).

- 6 Determine if you have eliminated the LoadMod failures.

If you have	Do
eliminated the LoadMod failures	step 17
not eliminated the LoadMod failures	step 7

- 7 Determine if the MG 4000 CEM is isolated.

If the MG 4000 CEM	Do
is isolated	step 8
is not isolated	step 9

- 8 Perform the procedure [Troubleshooting XA-Core to MG 4000 connectivity problems](#).

- Go to [step 17](#).
- 9** Determine if the MG 4000 CEM loading progresses beyond 0%.
- | If the loading | Do |
|-----------------------------|-------------------------|
| progresses beyond 0% | step 12 |
| does not progress beyond 0% | step 10 |
- 10** There is a problem with the MG 4000 CEM IP address. Resolve this problem.
Refer to [Checking the LAN configuration](#).
- 11** Determine if you have eliminated the LoadMod failures.
- | If you have | Do |
|-------------------------------------|-------------------------|
| eliminated the LoadMod failures | step 17 |
| not eliminated the LoadMod failures | step 12 |
- 12** Determine if the loading progresses to the load initialization stage.
- | If the loading | Do |
|--|-------------------------|
| progresses to the load initialization stage | step 13 |
| does not progress to the load initialization stage | step 16 |
- 13** Determine if your site is a multi-subnet site.
- | If your site | Do |
|----------------------------|-------------------------|
| is a multi-subnet site | step 14 |
| is not a multi-subnet site | step 16 |
- 14** There is a problem with the Gateway Address. Correct the problem.
Refer to [Correcting common problems relating to CEM configuration datafill](#).
- 15** Determine if you have eliminated the LoadMod failures.
- | If you have | Do |
|---------------------------------|-------------------------|
| eliminated the LoadMod failures | step 17 |

	If you have	Do
	not eliminated the LoadMod failures	step 16
16	Contact your next level of support.	
17	You have completed this procedure.	

Troubleshooting MG 4000 CEM Resetmod failures

Use this task to troubleshoot a failure to reset an MG 4000 common equipment module (CEM) circuit pack.

The following procedure describes the sequence of steps you must follow to troubleshoot MG 4000 Resetmod failures.

Procedure for troubleshooting MG 4000 CEM Resetmod failures

- 1 Determine if the MG 4000 CEM is isolated.

If the MG 4000 CEM	Do
is isolated	step 2
is not isolated	step 3

- 2 Perform the procedure [Troubleshooting XA-Core to MG 4000 connectivity problems](#).

Go to [step 11](#).

- 3 Determine if the MG 4000 CEM is configured properly.
Refer to [Correcting common problems relating to CEM configuration datafill](#).

If the MG 4000 CEM	Do
is configured properly	step 6
is not configured properly	step 4

- 4 Correct the MG 4000 CEM configuration problem.

- 5 Determine if you have solved the problem.

If the problem	Do
has been fixed	step 11
has not been fixed	step 6

- 6 Reseat the MG 4000 CEM.

Refer to [Reseating a circuit pack on an MG 4000](#).

- 7** Allow recovery of the MG 4000 CEM. Then attempt another ResetMod.

If the ResetMod**Do**

succeeded

[step 11](#)

failed

[step 8](#)

-
- 8** Replace the affected MG 4000 CEM.
Refer to [Replacing a CEM circuit pack](#).

- 9** Determine if you have solved the problem.

If the problem**Do**

has been fixed

[step 11](#)

has not been fixed

[step 10](#)

-
- 10** Contact your next level of support.
- 11** You have completed this procedure.

Troubleshooting a failure to RTS an MG 4000 CEM (SysB)

Use this task to troubleshoot a failure to return to service (RTS) an MG 4000 common equipment module (CEM), if the MG 4000 CEM drops to a system busy (SysB) state.

The following procedure describes the sequence of steps you must follow to troubleshoot a failure to RTS an MG 4000 CEM if the MG 4000 CEM is SysB.

Procedure for troubleshooting RTS failures on an MG 4000 CEM (SysB)

- 1 Allow at least 4 minutes to pass for the MG 4000 CEM to go through Sysb recovery.

If, after 4 minutes, the MG 4000 CEM	Do
recovers	step 9
does not recover	step 2

- 2 Determine if the MG 4000 CEM is isolated and in the not available (NA) state.

If the MG 4000 CEM	Do
is isolated	step 3
is not isolated	step 4

- 3 Perform the procedure [Troubleshooting XA-Core to MG 4000 connectivity problems](#).

Go to [step 9](#).

- 4 Reseat the MG 4000 CEM.

Refer to [Reseating a circuit pack on an MG 4000](#).

- 5 Allow recovery of the MG 4000 CEM. Then attempt another return to service (RTS).

If the RTS command	Do
succeeded	step 9
failed	step 6

- 6 Replace the affected MG 4000 CEM.

Refer to [Replacing a CEM circuit pack](#).

- 7** Determine if you have solved the problem.

If the problem	Do
has been fixed	step 9
has not been fixed	step 8

- 8** Contact your next level of support.

- 9** You have completed this procedure.

Troubleshooting a failure to RTS an MG 4000 CEM (IsTb)

Use this task to troubleshoot a failure to return to service (RTS) an MG 4000 common equipment module (CEM) if the MG 4000 CEM drops to an in-service-trouble (IsTb) state.

The following procedure describes the sequence of steps you must follow to troubleshoot a failure to RTS an MG 4000 CEM if the MG 4000 CEM is IsTb.

Procedure for troubleshooting RTS failures on an MG 4000 CEM (IsTb)

- 1 Allow at least 4 minutes to pass for the MG 4000 CEM to go through IsTb recovery.

If, after 4 minutes, the MG 4000 CEM	Do
recovers	step 10
does not recover	step 2

- 2 Determine if you have checked SPM logs.

If	Do
you have checked SPM logs	step 5
you have not checked SPM logs	step 3

- 3 Check SPM logs and follow any actions associated with those logs.

Refer to [Analyzing SPM 313 logs or QueryPM fault reason output for a CEM](#).

- 4 Determine if you have solved the problem.

If the problem	Do
has been fixed	step 10
has not been fixed	step 5

- 5 Reseat the MG 4000 CEM.

Refer to [Reseating a circuit pack on an MG 4000](#).

- 6** Allow recovery of the MG 4000 CEM. Then attempt another return to service (RTS).

If the RTS command**Do**

succeeded

[step 10](#)

failed

[step 7](#)

-
- 7** Replace the affected MG 4000 CEM.
Refer to [Replacing a CEM circuit pack](#).

- 8** Determine if you have solved the problem.

If the problem**Do**

has been fixed

[step 10](#)

has not been fixed

[step 9](#)

-
- 9** Contact your next level of support.
- 10** You have completed this procedure.

Troubleshooting MG 4000 CEM protection switch failures

Use this task to troubleshoot MG 4000 common equipment module (CEM) protection switch failures.

The following procedure describes the sequence of steps you must follow to troubleshoot MG 4000 CEM protection switch failures.

Procedure for troubleshooting MG 4000 CEM protection switch failures

- 1 Determine if both MG 4000 CEMs are in-service.
Refer to [Determining the state of a common equipment module](#).

If	Do
both MG 4000 CEMs are in-service	step 9
only one or neither MG 4000 CEMs are in service	step 2

- 2 Determine if one or both of the MG 4000 CEMs are manual busy (ManB).

If	Do
one or both MG 4000 CEMs are ManB	step 4
neither MG 4000 CEM is ManB	step 3

- 3 Determine if you are able to RTS the ManB MG 4000 CEMs and eliminate the protection switch failures.

If you have	Do
eliminated the failures	step 10
not eliminated the failures	step 9

- 4 Determine if one or both of the MG 4000 CEMs are system busy not available (SysB NA).

If	Do
one or both MG 4000 CEMs are SysB NA	step 5
neither MG 4000 CEM is SysB NA	step 6

- 5 Perform the procedure [Troubleshooting XA-Core to MG 4000 connectivity problems](#).
Go to [step 10](#).
- 6 Determine if one or both MG 4000 CEMs are in-service trouble (IsTb).

If	Do
one or both MG 4000 CEMs are IsTb	step 7
neither MG 4000 CEMs are IsTb	step 9
- 7 Check the SPM logs and follow any actions specified in the logs.
Refer to [Analyzing SPM 313 logs or QueryPM fault reason output for a CEM](#).
- 8 Determine if you are able to RTS the ManB MG 4000 CEMs and eliminate the protection switch failures.

If you have	Do
eliminated the failures	step 10
not eliminated the failures	step 9
- 9 Contact your next level of support.
- 10 You have completed this procedure.

Troubleshooting a SysB or IsTb MG 4000 resource module (RM)

Use this task to troubleshoot an MG 4000 resource module (RM) that is in either a system busy (SysB) or in-service-trouble busy state.

The following procedure describes the sequence of steps you must follow to troubleshoot an MG 4000 RM in a SysB or IsTb state.

Procedure for troubleshooting an MG 4000 RM in a SysB or IsTb state

- 1 Allow at least 4 minutes to pass for the MG 4000 RM to go through SysB or IsTb recovery.

If, after 4 minutes, the MG 4000 RM	Do
recovers	step 10
does not recover	step 2

- 2 Determine if you have checked the fault indicators at the MAPCI to resolve the problem.

If	Do
you have checked the MAPCI	step 5
you have not checked the MAPCI	step 3

- 3 Use the QUERYPM FLT REASON command at the MAPCI and perform the recommended actions.

Refer to [Analyzing SPM 300 logs or QueryPM fault reason output for an RM](#).

- 4 Determine if you have solved the problem.

If the problem	Do
has been fixed	step 10
has not been fixed	step 5

- 5 Reseat the MG 4000 RM.

Refer to [Reseating a circuit pack on an MG 4000](#).

- 6** Allow recovery of the MG 4000 RM. Then attempt another return to service (RTS).
- | If the RTS command | Do |
|---------------------------|-------------------------|
| succeeded | step 10 |
| failed | step 7 |
- 7** Replace the affected MG 4000 RM.
Refer to [Replacing a resource module circuit pack](#).
- 8** Determine if you have solved the problem.
- | If the problem | Do |
|-----------------------|-------------------------|
| has been fixed | step 10 |
| has not been fixed | step 9 |
- 9** Contact your next level of support.
- 10** You have completed this procedure.

Troubleshooting Loadmod or Resetmod failures for an MG 4000 RM

Use this task to troubleshoot a failure to reset or load an MG 4000 resource module (RM) circuit pack.

The following procedure describes the sequence of steps you must follow to troubleshoot Loadmod or Resetmod failures for an MG 4000 RM.

Procedure for troubleshooting Loadmod or Resetmod failures on an MG 4000 RM

- 1 Determine if the MG 4000 RM is configured properly.
Refer to [Checking the resource module configuration](#).

If the MG 4000 RM	Do
is configured properly	step 4
is not configured properly	step 2

- 2 Correct the MG 4000 RM configuration problem.
- 3 Determine if the problem has been solved.

If the problem	Do
has been solved	step 17
has not been solved	step 4

- 4 Determine if one or both accessible MG 4000 CEMs are in-service (InSv) or in-service trouble (IsTb).
Refer to [Determining the state of a common equipment module](#).

If	Do
one or both accessible MG 4000 CEMs are InSv or IsTb	step 6
neither accessible MG 4000 CEMs are InSv or IsTb	step 5

- 5 Perform the procedure [Troubleshooting a failure to RTS an MG 4000 CEM \(SysB\)](#).
Go to [step 17](#)

- 6** Determine if there was a concurrent maintenance action being performed on the on the inactive MG 4000 CEM at the time of the RM loadmod or resetmod failures.

If	Do
there was a concurrent maintenance action performed	step 7
there was no concurrent maintenance action performed	step 9

- 7** A message should have been displayed on the MAPCI that reads:

Task aborted by higher priority maintenance task. Retry the loadmod or resetmod operation on the MG4000 RM.

- 8** Retry the loadmod or resetmod command.
Determine if the problem has been solved.

If the problem	Do
has been solved	step 17
has not been solved	step 9

- 9** Check the fault indicators at the MAPCI.

- 10** Use the QUERYPM FAULT REASON command at the MAPCI and perform the recommended actions.

Refer to [Analyzing SPM 300 logs or QueryPM fault reason output for an RM](#).

- 11** Retry the loadmod or resetmod command.
Determine if the problem has been solved.

If the problem	Do
has been solved	step 17
has not been solved	step 12

- 12** Reseat the MG 4000 RM.

Refer to [Reseating a circuit pack on an MG 4000](#).

- 13** Determine if you have solved the problem.

If the problem	Do
has been fixed	step 17

		If the problem	Do
		has not been fixed	step 14
14	Replace the affected MG 4000 RM. Refer to Replacing a resource module circuit pack .		
15	Determine if you have solved the problem.		
		If the problem	Do
		has been fixed	step 17
		has not been fixed	step 16
16	Contact your next level of support.		
17	You have completed this procedure.		

Troubleshooting a failure to RTS an MG 4000 resource module (RM)

Use this task to troubleshoot a failure to return to service (RTS) an MG 4000 resource module (RM).

The following procedure describes the sequence of steps you must follow to troubleshoot a failure to RTS and MG 4000 RM.

Procedure for troubleshooting RTS failures on an MG 4000 RM

- 1 Allow at least 4 minutes to pass for the MG 4000 RM to go through Sysb recovery.

If, after 4 minutes, the MG 4000 RM	Do
recovers	step 17
does not recover	step 2
- 2 Determine if there was a concurrent maintenance action being performed on the inactive MG 4000 CEM at the time of the RM RTS failures.

If	Do
there was a concurrent maintenance action performed	step 3
there was no concurrent maintenance action performed	step 5
- 3 A message should have been displayed on the MAPCI that reads:
 Task aborted by higher priority maintenance task. Retry the RTS operation on the MG4000 RM.
- 4 Retry the RTS command.
 Determine if the problem has been solved.

If the problem	Do
has been solved	step 17
has not been solved	step 5
- 5 Check the fault indicators at the MAPCI.

- 6 Use the QUERYPM FAULT REASON command at the MAPCI and perform the recommended actions.

Refer to [Analyzing SPM 300 logs or QueryPM fault reason output for an RM](#).

- 7 Retry the RTS command.

Determine if the problem has been solved.

If the problem	Do
has been solved	step 17
has not been solved	step 12

- 8 Determine if you have performed a resetmod on the MG 4000 RM yet.

If	Do
you have performed a resetmod	step 12
you have not performed a resetmod	step 9

- 9 Perform a resetmod operation on the MG 4000 RM.

If the resetmod operation	Do
succeeded	step 11
failed	step 10

- 10 Perform the procedure [Troubleshooting Loadmod or Resetmod failures for an MG 4000 RM](#).

Go to [step 17](#)

- 11 Determine if you have solved the problem.

If the problem	Do
has been fixed	step 17
has not been fixed	step 12

- 12 Reseat the MG 4000 RM.

Refer to [Reseating a circuit pack on an MG 4000](#).

- 13 Determine if you have solved the problem.

If the problem	Do
has been fixed	step 17

		If the problem	Do
		has not been fixed	step 14
14	Replace the affected MG 4000 RM. Refer to Replacing a resource module circuit pack .		
15	Determine if you have solved the problem.		
		If the problem	Do
		has been fixed	step 17
		has not been fixed	step 16
16	Contact your next level of support.		
17	You have completed this procedure.		

Troubleshooting MG 4000 RM protection switch failures

Use this task to troubleshoot MG 4000 resource module (RM) protection switch failures with “No spare available.”

The following flowchart describes the sequence of steps you must follow to troubleshoot MG 4000 RM protection switch failures with “No spare available.”

Procedure for troubleshooting MG 4000 RM protection switch failures with “No spare available”

- 1 Determine if both the active and inactive MG 4000 RMs are in-service (InSv).

If	Do
both the active and inactive MG 4000 RMs are InSv	step 6
one or neither MG 4000 RM is InSv	step 2
- 2 Determine if one or both of the MG 4000 RMs are manual busy (ManB).

If	Do
one or both MG 4000 RMs are ManB	step 3
neither MG 4000 RMs are ManB	step 4
- 3 Determine if you are able to return to service (RTS) the ManB MG 4000 RM(s) and eliminate the protection switch failures.

If the problem	Do
has been fixed	step 7
has not been fixed	step 6
- 4 Determine if one or both of the MG 4000 RMs are system busy (SysB) or in-service trouble (IsTb).

If	Do
one or both MG 4000 RMs are SysB or IsTb	step 5

	If	Do
	neither MG 4000 RM is SysB or IsTb	step 6
5	Perform the procedure Troubleshooting a SysB or IsTb MG 4000 resource module (RM) . Go to step 7 .	
6	Contact your next level of support.	
7	You have completed this procedure.	

Determining the state of the ATM framework from the XA-Core

Use the following procedure to determine the state of the asynchronous transfer mode framework (ATMFw) for a specific MG 4000, IW SPM, or DPT SPM. There are two MAPCI levels where you find information on the state of the ATMFw:

- ATMFw level
- ATMCONN level

At the ATMFw level, you determine the state of the ATMFw (UnEq, CBsy, SysB, ISTb, or Insv). At the ATMCONN level, you obtain additional information including the overall ATMFw status, and the configuration state.

Determine the state of the ATMFw

At the MAP terminal

- 1 Access the ATMFw level of MAPCI, by typing

>MAPCI;MTC;APPL;ATMFw

and pressing the Enter key.

Example of a MAP screen:

```

XAC      MS      IOD  Net      PM      CCS      Lns      Trks      Ext      APPL
.         .         .   .         .         .         .         .         .         .
ATM
0  Quit
2
3  QueryFl_      ATMFW  STATES
4
5                  111111111122222222223333333333444
6                  01234567890123456789012345678901234567890123456789012
7                  -----C-...
8
9                  444444445555555555666666666677777777778888888
10                 34567890123456789012345678901234567890123456789012345
11                 ---I-S-----
12
13 KEY:  '-' = UnEq, ATM RM is UnEquipped
14       'C' = CBsy, ATM RM is OSS
15       'S' = SysB, ATMFW is not providing any service
16       'I' = ISTB, ATMFW is providing partial service
17       '.' = InSv, ATMFW is providing full service
18
19 ATMFW:
20
21 ETAS
Time 11: 10 >■

```

- 2 Check the STATES field to determine the state (UnEq, CBsy, SysB, ISTb, or Insv) of the ATMFw which is of interest to you. The following table explains the state symbols used in the MAPCI level.

Note: On the ATMFw level there are 85 ATMFw STATES fields. The maximum number of network elements (MG 4000, IW SPM, and DPT SPM combined) is 85. Each ATMFw, on the screen, is associated with one of the 85 possible network elements. In the MAP screen example, the ATMFw state for ATMFw 40 is InSv (in-service). This means that the ATMFw for the network element (defined as spm_no = 40) is in-service.

Key for determining the state of the ATMFw

Symbol	Explanation
'_'	UnEq: The ATM RM is unequipped
'C'	CBsy: The ATM RM is out of service. To recover the ATMFw, you must recover the ATM RM.
'S'	SysB: The ATMFw is not providing any service. This means that the ATMFw is neither PVC Capable or PVC and SVC capable due to possible carrier problems.
'I'	ISTb: The ATMFw is providing partial service.
'.'	InSv: The ATMFw is providing full service.

- 3 If the ATMFw is unequipped, or CBsy (C-side busy), or SysB (system busy), return to the task [Troubleshooting general ATM networking problems](#), otherwise, proceed to the next step in this procedure.

Note: Cbusy or SysB means the ATMFw is not operational.

- 4 If the ATMFw is ISTb, then proceed to step [5](#), otherwise if the ATMFw is InSv proceed to step [7](#).
- 5 To determine the cause of the in-service trouble condition, query the ATMFw, by typing

>QUERYFL <spm_no>

and pressing the Enter key.

where

spm_no

is the number of the SPM (0 to 85)

- 6 Examine the MAP response to your query of the in-service trouble ATMFw, and check the following table for explanations and actions.

Responses to the queryfl command for an ISTb ATMFw

Response	Explanation and action
ATMFw not initialized	The ATMFw is not initialized. In other words, the system has not yet ensured that the ATM functionality has been activated. ATM service is not being provided. This is a temporary or transient state that would usually only be seen right after an ATM RM is brought into service. If the ATM RM is active, and in-service, and this response persists for more than 1 minute, then you should attempt manual action. Perform a protection switch, then manual busy, then return to service the (currently active) ATM RM. If the problem persists after taking manual action, contact your next level of support.
UNI Signalling suspended - new SVCs not allowed	The ATMFw is PVC (permanent virtual circuit) capable and SVCs (switched virtual circuits) that are up, will remain up and stable, but new SVCs cannot be established.
UNI Signalling down - no SVCs possible	The ATMFw is PVC (permanent virtual circuit) capable only.

- 7 An alternate method for determining the state of the ATMFw is as follows:

- a Access the MG 4000, or DPT SPM, or IW SPM level of MAPCI, by typing

```
>MAPCI;MTC;PM;POST spm_no
```

and pressing the Enter key.

where

spm_no

is the number of the network element (MG 4000, or IW SPM, or DPT SPM) and is a value from 0-85.

- b Query the ATM (asynchronous transfer mode) connection to see the overall ATMFw status, by typing

```
>ATMCONN;QUERY ATMFw
```

and pressing the Enter key.

Example of a MAP screen:

```
ATM Framework Configuration for SPM 40, ATM 0 (active)
-----
ATM Framework Configuration
  FrWk Status: PVC & SVC Capable
  Config State: Complete
  AESA       : 45 11 11 11 11 11 11 11 1f 4 f 0 0 0 0 0 0 0 0
  Format      : NSAP Format - {Static}
  Connections: 45 of 2300 Virtual Channels. 1 Of 1 Virtual Paths.
ILMI                               UNI/SAAL
  Configured : No                   Configured: Yes
  Version    :                     Version    : 4.0
  Link State :                     Saal State: Connected
  VPI/VCI    :                     VPI/VCI    : ( 0, 5)

  Address Reg:
Crossover/APS Layer
  Self: XoverMode TxAct OwnRxFiber
  Mate: XoverMode TxinAct MyOwnRxFiber
Carrier/Physical Layer
  Status: Up
>
```

- c** Ensure that there are no problems at the ATMCONN level.
- 8** You have completed this procedure. Return to the CI level of the MAP screen, by typing
>QUIT ALL
and pressing the Enter key.

Determining the state of a resource module

Use the following procedure to determine the state of the resource module (RM) for an SPM (Spectrum peripheral module) such as an MG 4000, IW SPM, or DPT SPM.

Determine the state of an RM

At the MAP terminal

- 1 Post the SPM, by typing
>MAPCI;MTC;PM;POST SPM spm_no
 and pressing the Enter key.
where
spm_no
 is the number of the SPM (0 to 85)

Example of a MAP screen:

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL												
.	.	.	.	.	.	.	.	.	.												
SPM				SysB	ManB	OffL	CBsy	ISTb	InSv												
0	Quit	PM		0	0	0	0	3	23												
2	Post_	SPM		0	0	0	0	2	2												
3	ListSet																				
4	ListRes	SPM	40	InSv	Class: SMG4																
5	Trnsl																				
6		Shlf0	SL	A	Stat	Shlf0	SL	A	Stat	Shlf1	SL	A	Stat								
7	ATMConn	ATM	0	1	A	InSv	CEM	1	8	I	InSv	DLC	0	1	I	InSv	-----	8	-	----	
8		ATM	1	2	I	InSv	OC3	0	9	I	InSv	-----	2	-	----	DSP	0	9	A	InSv	
9		-----	3	-	----	OC3	1	10	A	InSv	-----	3	-	----	DSP	1	10	A	InSv		
10		-----	4	-	----	-----	11	-	----	-----	4	-	----	DSP	2	11	I	InSv			
11	Disp_	-----	5	-	----	-----	12	-	----	-----	5	-	----	-----	12	-	----				
12	Next	-----	6	-	----	VSP	0	13	A	InSv	-----	6	-	----	-----	13	-	----			
13	Select_	CEM	0	7	A	InSv	VSP	1	14	I	InSv	DLC	1	7	A	InSv	ALM	0	14	A	OffL
14	QueryPM																				
15	ListAlm																				
16																					
17	SPERFORM																				
18	Upgrade_	SPM:																			
	USER																				
Time	15: 06	>																			

- 2 Determine the state of the RM, by typing
>SELECT pack_type unit_no
 and pressing the Enter key.
where

pack_type

is the type of circuit pack (CEM, ATM, OC3, DSP, VSP, or DLC)

unit_no

is the number of the RM. ALM, ATM and OC3 are (0 to 1), and VSP, TIM, IEM, DSP, and DLC are (0 to 27)

Example of a MAP screen:

```

XAC      MS      IOD  Net    PM    CCS    Lns    Trks    Ext    APPL
.        .        .    .      .      .      .      .      .      .
OC3
0  Quit          PM          0      0      0      0      3      23
2          SPM          0      0      0      0      2      2
3  ListSet      OC3          0      0      0      0      0      2
4
5          SPM  40  OC3  0  InAct  InSv
6  Tst
7  Bsy          Loc : Row A FrPos  7 ShPos  6 ShId 0 Slot  9  Prot Grp : 1
8  RTS          Default Load: OC418B0          Prot Role: Working
9  OffL
10 LoadMod      OC3:
11
12 Next
13 Select_
14 QueryMod
15 ListAlm
16 Prot
17 SPERFORM
18
      ETAS
Time  15: 14 >

```

- 3** You have completed this procedure. Return to the CI level of the MAP screen, by typing:

>QUIT ALL

and pressing the Enter key.

Determining the state of the OC3S, STS3L, or STS3CP carriers

Use the following procedure to determine the state of the OC3S, STS3L, and STS3CP high-speed carriers on an MG 4000, IW SPM, or DPT SPM.

Determine the state of OC3S, STS3L, or STS3CP carriers

At the MAP terminal

- 1 Access the carrier level of MAPCI, by typing
>MAPCI;MTC;TRKS;CARRIER
 and pressing the Enter key.
- 2 Post the MG 4000, IW SPM, or DPT-SPM, by typing
>POST SPM <spm_no> <carrier_type>
 and pressing the Enter key.

where

spm_no

is the number of the SPM (0 to 85)

carrier_type

is the type of carrier (OC3S, or STS3L, or STS3CP)

Example of a MAP screen when posting an OC3S carrier:

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
Post		CLASS	ML OS	ALRM	SYSB	MANB	UNEQ OFFL	CBSY PBSY	INSV
0 Quit		TRUNKS	3 0	0	0	0	0 0	0 0	228
2 Post_		HSCARR	4 0	1	0	0	0 0	2 0	200
3		OC3S							
4		N CLASS	SITE SPM RM	OCS3	CKT	STATE	TR MA		
5 Loop_		0 HSCARR	HOST 40 0	0	1	INSV			
6 Tst_		1 HSCARR	HOST 40 1	0	2	INSV			
7 Bsy_		2 HSCARR	HOST 40 0	0	176	CBSY	** ..		
8 RTS_		3 HSCARR	HOST 40 1	0	177	INSV			
9 OffL_		SIZE OF POSTED SET		: 4					
10									
11 Disp_		Post:							
12 Next									
13									
14 Detail_									
15 ListAlm_									
16									
17 Perfmon_									
18									
		USER1							
Time	11: 30	>							

This OC3S carrier
is C-side busy

- 3 Check the STATE field to determine the state (UnEq, CBsy, SysB, IStb, or Insv) of the carrier.
Note: If the carriers are not in-service (InSv), perform the appropriate alarm clearing procedure in *DMS-100 MMP Alarm Clearing and Performance Monitoring Procedures Vol 4* or 4, 297-9051-5432.
- 4 You have completed this procedure. Return to the CI level of the MAP screen, by typing
>QUIT ALL
and pressing the Enter key.

Determining the state of the PVC connections from the XA-Core to an MG 4000

Use the following procedure to determine the state of the permanent virtual circuit (PVC) connections from the XA-Core to an MG 4000.

Determine the state of the PVC connections from the XA-Core to MG 4000

At the MAP terminal

- 1 Access the PM level of MAPCI, by typing
>MAPCI;MTC;PM
and pressing the Enter key.
- 2 Post the MG 4000, by typing
>POST SPM <spm_no>
and pressing the Enter key.
where
spm_no
is the number of the SPM (0 to 85)
- 3 Access the CoreConn level, by typing
>ATMCONN;CORECONN
and pressing the Enter key.

Example of a MAP screen

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
CORECONN				SYSB	MANB	OffL	CBsy	ISTb	InSv
0 Quit	PM			0	0	0	0	0	24
2	SPM			0	0	0	0	0	2
3									
4	SPM 40			Class: SMG4					
5 Trnsl_									
6 Tst_			Core to ATM		PM to ATM				
7 Bsy_			Link VPI VCI	VPI VCI					
8 RTS_	Conn 0:		3	0	140	0	50	InSv	
9	Conn 1:		2	0	140	0	51	InSv	
10 PeerConn									
11									
12									
13									
14 Query_									
15									
16 PmStat_									
17									
18									
USER1									
Time 11: 30 >									

State of the PVC connections from the XA-Core to the MG 4000

- 4 Check the state of the PVC connections (see the MAP screen example in step 2).
- 5 You have completed this procedure. Return to the CI level of the MAP screen, by typing
>QUIT ALL
 and pressing the Enter key.

Determining the state of the AMDI links

Use the following procedure to determine the state of the asynchronous transfer mode Multi-node Data Interface (AMDI) links.

Determine the state of the AMDI links

At the MAP terminal

- 1 Access the AMDI level of MAPCI, by typing

>MAPCI;MTC;XAC;AMDI

and pressing the Enter key.

Example of a MAP screen

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
AMDI		Front:	111111111	Rear:	111111	SM	PE	IO	PKLT
0 Quit		123456789012345678	456789012345	.	.	.	.	.	.
2	Sta	.		.	...		0	0	0
3	Dep								
4	Typ:				**	**			
5	Slot:	Side:	Packlet:	Status:	Port0:	Port1:	Link0:	Link1:	
6 Tst_	5	Rear	Lower	.	.	.	.	.	
7 Bsy_	6	Rear	Lower	.	.	.	.	.	
8 RTS_	13	Rear	Lower	.	.	.	.	.	
9	14	Rear	Lower	.	.	.	.	.	
10 LoadFW_									
11									
12 Uneq_									
13									
14 Alarm_									
15 Cntrs_									
16									
17 Indicat_									
18 Query_									
USER1									
Time 11: 30 >									

State of the
AMDI links

- 2 Check the state of the AMDI links (see the MAP screen example in step 1).

Note: If there are problems with the AMDI links, see the alarm clearing procedures in the *XA-Core Maintenance Manual*, 297-8991-510.

- 3 You have completed this procedure. Return to the CI level of the MAP screen, by typing

>QUIT ALL

and pressing the Enter key.

Determining the state of the peer SVC connections for an MG 4000

Use the following procedure to determine the state of the peer switched virtual circuit (SVC) connections between MG 4000 nodes.

Determine the state of the SVC connections for an MG 4000

At the MAP terminal

- 1 Post the MG 4000, by typing
>MAPCI;MTC;PM;POST SPM <spm_no>
 and pressing the Enter key.
where
spm_no
 is the MG 4000 number (0 to 85)
- 2 Access the ATMCONN;PeerConn level, by typing
>ATMCONN;PeerConn
 and pressing the Enter key.

Example

MAPCI;MTC;PM;POST SPM 40;ATMCONN;PEERCONN

Example of a MAP screen for MG 4000 40

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	4 SPM	.	.	3C	.	.
				M					
PEERCONN				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		0	0	0	0	1	25
2		SPM		0	0	0	0	1	3
3									
4		SPM 40		Class: SMG4					
5									
6 Tst_				11111111112222222222333333333344444444445555555555					
7				012345678901234567890123456789012345678901234567890123456789					
8		0		-----					
9		60		-----					
10		120							
11		180							
12		240							
13									
14 Query_									
15									
16 PmStat_									
17									
18									
USER1									
Time 11: 30 >									

The peer SVC connection
from MG 4000 40 to MG 4000 41
is in-service

The peer SVC connection
from MG 4000 40 to
MG 4000 46 is also in-service

- 3 Obtain more information about a single peer SVC connection, by typing

>QUERY <peer_mg>

and pressing the Enter key.

where

peer_mg

is the number of the peer MG 4000 (0 to 85)

Note: This command displays information about the peer SVC connection between the posted MG 4000 (in the example, this is 40) and the peer MG 4000 (in the example, this is 41 or 46).

Example of a MAP screen

```
Peer connection to MG 41 is Insv.  
Last stored fault: 16 - No ATM service available in ATM RM
```

- 4 You have completed this procedure. Return to the CI level of the MAP screen, by typing

>QUIT ALL

and pressing the Enter key.

Correcting common problems relating to CEM configuration datafill

In certain circumstances, you may be able to trace a node maintenance problem to a specific MG 4000, IW SPM, or DPT SPM. An example of this type of node maintenance problem would be if you were unable to return a CEM to service. When attempting to solve these problems, you should always perform the basic datafill and configuration checks that are outlined in the following procedure.

Correcting CEM configuration datafill

At the MAP level

1 Check the datafill in table MNNODE as follows:

a Access table MNNODE, by typing

>TABLE MNNODE

and pressing the Enter key.

b Position on the appropriate tuple, by typing

>POS SPM spm_no

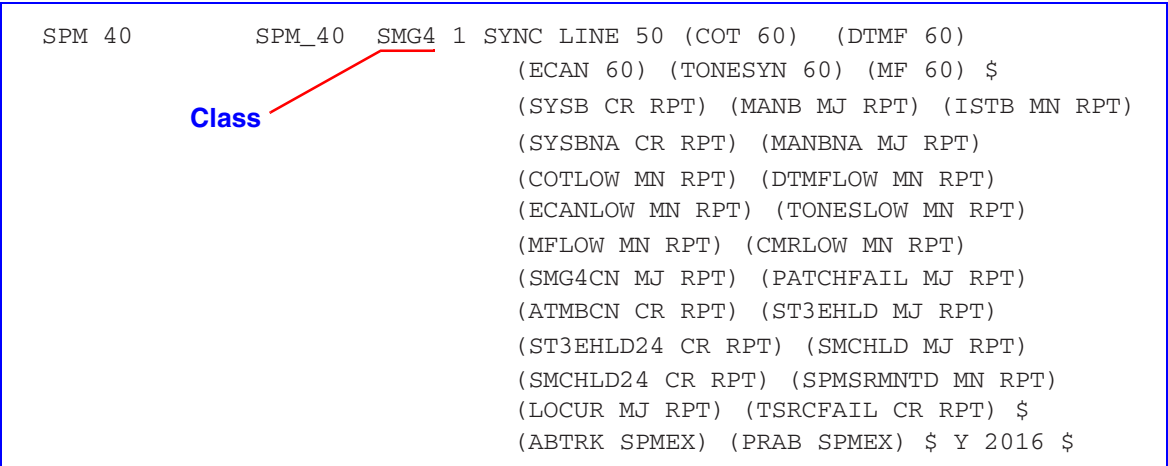
and pressing the Enter key.

where

spm_no

is the number of the SPM (0 to 85)

Example of a MAP screen:



```

SPM 40          SPM_40  SMG4 1 SYNC LINE 50 (COT 60) (DTMF 60)
                                     (ECAN 60) (TONESYN 60) (MF 60) $
Class          (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT)
               (SYSBNA CR RPT) (MANBNA MJ RPT)
               (COTLOW MN RPT) (DTMFLOW MN RPT)
               (ECANLOW MN RPT) (TONESLOW MN RPT)
               (MFLOW MN RPT) (CMRLOW MN RPT)
               (SMG4CN MJ RPT) (PATCHFAIL MJ RPT)
               (ATMBCN CR RPT) (ST3EHL2 MJ RPT)
               (ST3EHL24 CR RPT) (SMCHLD MJ RPT)
               (SMCHLD24 CR RPT) (SPMSRMNTD MN RPT)
               (LOCUR MJ RPT) (TSRCFAIL CR RPT) $
               (ABTRK SPME) (PRAB SPME) $ Y 2016 $

```

c Ensure that the class is datafilled with the value “SMG4” for an MG 4000, and “IW” for an IW SPM or DPT SPM. (If necessary, correct the value.)

d Exit table MNNODE, by typing

>QUIT

and pressing the Enter key.

2 Check the datafill in table MNCKTPAK as follows:

a Access table MNCKTPAK, by typing

>TABLE MNCKTPAK

and pressing the Enter key.

b Display heading information for the table by typing

>HEADING

and pressing the Enter key.

c Position on the tuples associated with the CEM cards for the SPM, by typing

Note: CEM 0 is always in shelf 0 slot 7, and CEM 1 is always in shelf 0 slot 8.

>POS SPM *spm_no* *shelf_no* *slot_no*

where

spm_no

is the number of the SPM (0 to 85)

shelf_no

is the shelf number of the SPM (0 or 1)

slot_no

is the slot number of the CEM (7 or 8)

Example of a MAP screen:

CPKKEY									
CPKINFO									
			PEC		RELEASE		LOAD		MAC address
SPM	40	0	7	CEM	0	(00603887758D0)	\$	(SYSB CR RPT)	(MANB MJ RPT)
						(ISTB MN RPT)		(SYSBNA CR RPT)	(MANBNA MJ RPT)
						(HLDVR MJ RPT)		(HLDVR24 MJ RPT)	(VCX070 MN RPT)
						(VCX090 MJ RPT)		(CLKOOS MJ RPT)	(PATCHFAIL MJ RPT)
									\$
						NTLX82BA	02	MG418BS	

the MG 4000 load is part of the SP18 load line-up (version 18)

- d** Ensure that the MAC address datafilled in table MNCKTPAK matches the MAC address on the faceplate of the CEM. (If necessary, correct the MAC address).

Note: A CEM will repeatedly fail to reset if the MAC address in table MNCKTPAK does not match the MAC address on the CEM faceplate.

- e** Ensure that the product engineering code (PEC) datafilled in table MNCKTPAK matches the PEC displayed on the CEM cards that are inserted in the SPM shelf. (If necessary, correct the PEC).
- f** Ensure that the CEM card is inserted in the correct slot.
- g** Ensure that CEM load, that is datafilled in table MNCKTPACK, is the correct load as follows.
- i** Use the most recent Release Notes document to check the proper CEM load.
- Note:** You receive the Release Notes with the SPM load tape.
- ii** At the MAPCI determine the version of the XA-Core load, by typing
- >IMAGENAME**
- and pressing the Enter key.

Note: The version of the CEM load (that you are using) must be equal to, or greater than the XA-Core load, but

no more than three releases greater than the XA-Core load. In the preceding MAP screen example, the load (MG418BS0 is an MG 4000 load that is part of the SP18 load line-up. In other words, the version is 18.

Example of a MAP screen

```

XANA1 BCS 53 BI built on 2002-SEP-09 at 17:06:00 using
psnn05bk
PRODUCT: SNNCS.005
LOAD: SN000.005
LAYER: BAS.19.0.BI
LAYER: TL.18.0.BI
LAYER: SHR.18.0.AA
LAYER: CCM.18.0.BK
LAYER: CNA.18.0.BK
LAYER: UCS.18.0.BK
LAYER: TOPSC.18.0.BK
LAYER: CNATOPS.18.0.BK
LAYER: BCTOPS.18.0.BK
LAYER: NCS.18.0.BK
LAYER: MSH.18.0.BK
LAYER: SNNCSH.05.0.BK

```

The software release is SN05

Base layer is 19
and is 1 release ahead

The XA-Core load is based on
CSP18 layers (version 18)

- iii Compare the version of the SPM load in table MNCKTPAK with the version of the XA-Core load (using the IMAGENAME CI tool). Ensure that the version of the CEM load is equal to, or greater than the XA-Core load, but no more than three releases greater than the XA-Core load.

- iv If you can successfully load the SPM, check the load names of the load files, by typing

```

>MAPCI NODISP;MTC;PM;POST SPM
<spm_no>;QUERYPM FILES

```

and pressing the Enter key.

where

spm_no

is the number of the SPM (0 to 85)

Note: The SPM load line-up should be equal to, or no more than three releases above the XA-Core load. If you can successfully load the MG 4000, IW SPM, or DPT SPM, then you can directly query the load files from the MAP.

Example

MAPCI;NODISP;MTC;PM;POST SPM 40;QUERYPM
FILES

Example of a MAP screen

SPM 40	Insv		
	.		
	.		
	.		
CEM 0	InSv Act	Default Loadname:	MG418BS
		Default Filename:	MG418BS_010044
		Running Load:	MG418BS_010044
		Load in Flash:	MG418BS_010044
CEM 1	InSv Act	Default Loadname:	MG418BS
		Default Filename:	MG418BS_010044
		Running Load:	MG418BS_010044
		Load in Flash:	MG418BS_010044

- v Ensure that both CEMs (0 and 1) have the same load, and that both the running load and the load in flash are the same in both CEMs.

3 Check the datafill in table PMLOADS as follows:

- a Access table PMLOADS, by typing

>TABLE PMLOADS

and pressing the Enter key.

- b Display heading information, by typing

>HEADING

and pressing the Enter key.

- c Position on the load name that matches the datafill in table MNCKTPAK (see step 2), by typing

>POS <load_name>

where

load_name

is the load name of the SPM (for example, MG418BS)

and pressing the Enter key.

Example

>POS MG418BS

Example of a MAP screen

LOADNAME		ACTVOL	UPDACT
ACTFILE	BKPFIL	BKPVOL	
MG418BS			
MG418BS_010044		F17LPML2	
MG418BS_010044		F17LPML2	N

- d Ensure that the load file names and volume names are correct by listing the files on the respective volumes.
- 4 You have completed this procedure. Return to the CI level of the MAP screen, by typing
- >QUIT ALL**
- and pressing the Enter key.

Determining the state of the ATMFW from the MG 4000, IW SPM, or DPT SPM

Use the following procedure to determine the state of the asynchronous transfer mode (ATM) framework (ATMFW) by remotely logging in to dShell (on the MG 4000, IW SPM, or DPT SPM), and then logging in to the respective ATM resource module (RM)

Determine the state of an ATMFW

At the MAP terminal

- 1 Access the dShell of the RM, by typing
>REMLOGIN SPM <spm_no> <unit_no>
and pressing the Enter key.

where

spm_no

is the number of the SPM (0 to 85)

unit_no

is the number of the CEM (0 or 1)

Example

>REMLOGIN SPM 40 0

- 2 Remotely log in to the ATM RM whose ATMFW you wish to analyze, by typing

dSH> remlogin -s<slot_no>

and pressing the Enter key.

where

slot_no

is the logical slot number of the ATM RM. The value is (1 or 2) for an MG 4000, or (9 or 10) for and IW SPM, or DPT SPM.

- 3 Display the ATMFW status associated with the ATM RM, by typing

>dSH> /ATMHL

Example of a MAP screen:

```

+== Atm Freamework Configuration  [...] =====+
|
| Framework      : PVC & SVC Capable / Configuration State : Complete
| AESA           : 45 11 11 11 11 11 11 11 1F 4 F 0 0 0 0 0 0 0 0
|                 NSAP Format - {Static}
|
| Connections    : 4 of 2300 Virtual Channels.  1 of 1 Virtual Paths.
|
+== ILMI  [...] =====+== UNI/SAAL [...] =====+
|
|                                     Version          : 4.0
|                                     SaalState         : Connected
|
| ILMI is disabled.                  VPI/VCI        : { 0,  5}
|                                     Signalling Configured : Yes
|
+== Carrier/Physical Layer [...] =====+
|
| Up
|
+== CrossOver/APS Layer  =====+
|
| Self:  XoverMode TxAct   OwnRxFiber
| Mate:  XoverMode TxInAct MyOwnRxFiber
|
+=====+

```

- 4 Return to the CEM dShell level, by typing
dSH> REMLOGOUT
 and pressing the Enter key.
- 5 You have completed this procedure. Retrurn to the CI level, by
 typing
dSH> EXIT
 and pressing the Enter key.

Checking the configuration of an ATM network

Use the following procedure to check the configuration of an asynchronous transfer mode (ATM) network. This procedure assumes that your ATM network uses the Multiservice Switch 15000. If your ATM network uses other ATM equipment, then do not use this procedure. Instead, refer to the applicable product documentation for your ATM network to perform the equivalent troubleshooting.

This procedure provides steps for checking the ATM network configuration for a four-link configuration consisting of the following elements:

- MG 4000 ATM interface
- IW SPM, or DPT SPM link interface
- CS 2000 link configuration
- PNNI ATM network links

You can find the correct values for the ATM network configuration in the *Nortel Networks Multiservice Switch 15000 and Media Gateway 15000 in Succession Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP*, NN10225-512.

The following procedure describes the commands you use to display all the attributes found in the document *Nortel Networks Multiservice Switch 15000 and Media Gateway 15000 in Succession Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP*, NN10225-512, relating to the four the four types of link configurations (see above). When you are using this procedure, you should focus on the interfaces that are associated with the problems that you are investigating.



CAUTION

Only qualified personnel who fully understand the impacts of configuration changes and who perform changes in accordance with all Nortel Networks procedures and specifications should make changes to the ATM network configuration.

For additional information on configuring Multiservice Switch 15000 and Preside MDM, see the following documents:

- *Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Configuration Overview* PT-AAL1/UA-AAL1/UA-IP, NN10114-511
- *Nortel Networks Multiservice Switch 15000 and Media Gateway 15000 in Succession Networks Configuration Attribute Summary* PT-AAL1/UA-AAL1/UA-IP, NN10225-512

Obtain an overview of the Multiservice Switch 15000 link configuration

In a log in session on the Multiservice Switch 15000

- 1 Obtain a quick ATM link configuration overview for the Multiservice Switch 15000, by typing

```
d -p atmif/* remote
```

and pressing the Enter key.

Note: The output resulting from this command allows you to determine the ATM interfaces that are configured.

- 2 Determine the UNI (User Network Interface) interface addresses that are configured, by typing

```
I atmif/* uni addr/*
```

and pressing the Enter key.

Note: You can compare the UNI addresses, that are output by this command, to the addresses that are datafilled for each SPM (MG 4000, IW SPM, or DPT SPM) in table MNATMIF on the XA-Core.

- 3 Use the commands shown in the following table to check the configuration attributes for each applicable MG 4000, IW SPM, DPT SPM, CS 2000, or PNNI interface.

Note: In the following table, an example command is shown for each of the components for which you can check configuration datafill. Compare the output values to those that are listed in the document *Nortel Networks Multiservice Switch 15000 and Media Gateway 15000 in Succession*

Networks Configuration Attribute Summary
PT-AAL1/UA-AAL1/UA-IP, NN10225-512.

Multiservice Switch 15000 command to display attribute (where X = logical slot number, and Z = port number)	
Attribute	
Logical processor	L : d -p lp/*
SONET	d -p lp/* sonet/*
Bridged SONET	display lp/* bso/*
Laps	d -p laps/XZ
Laps Sts	d -p laps/XZ sts/0 atmcell
AtmIf interfaceName	d -p atmif/XZ remoteAtmInterfaceLabel
AtmIf Connection Administrator (CA)	d -p atmif/XZ ca
AtmIf RealTimeVariableBitRate	d -p atmif/XZ ca rtvbr/0
AtmIf ConstantBitRate	d -p atmif/XZ ca cbr/0
AtmIf NonRealTimeVariableBitRate	d -p atmif/XZ ca nrtvbr/0
AtmIf UserNetworkInterface	d -p atmif/XZ uni
AtmIf Uni Ilmi	d -p atmif/XZ uni ilmi
AtmIf Uni Signaling	d -p atmif/XZ uni sig
AtmIf Uni Sig VirtualChannelDescriptor	d -p atmif/XZ vcc/0.50 vcd Note: For all MG 4000s and on the MG 4000 to Passport interfaces, Nortel Networks uses the (VPI,VCI) combination of (0,50) and (0,51) to define the VCC connections.
AtmIf Vcc Vcd TrafficManagement	d -p atmif/XZ vcc/0.50 vcd tm

Multiservice Switch 15000 command to display attribute (where X = logical slot number, and Z = port number)	
Attribute	
AtmIf VirtualChannelConnection (Vcc)	d -p atmif/XZ vcc/0.50 vcd
AtmIf Vcc NailedUpRelayPoint (Nrp)	d -p atmif/XZ vcc/0.50 nrp
AtmIf ConnectionMapping (ConnMap) Override (For 16pOC3 Multiservice Switch 15000 cards only)	d -p atmif/XZ ConnMap ov
AtmIf Private Network-Network Interface (PNNI)	d -p atmif/* pnni aco d -p atmif/* pnni act
PGB connection on all PBG protected links	1 > display pbg/* 1 > display pbg/* sts/0
To verify the UNI signaling channel traffic	d -p atmif/* uni sig vcd tdp

4 You have completed this procedure.

Checking the LAN configuration

Use the following procedure to verify that the MG 4000 CEM (common equipment module) IP (Internet Protocol) address is configured correctly. To perform this procedure, you will require the following information from your LAN (local area network) administrator:

- the MG 4000 CEM IP address
- the MG 4000 subnet mask
- the MG 4000 edge gateway IP address

If the above information is not available from your LAN administrator, and the CEM has previously been loaded, then you should consider the CEM IP address information in table MNIP to be correct until the LAN administrator determines the information is incorrect.

The following procedure requires that you verify certain configuration data on the edge router to which the MG 4000 CEM is connected.

Check the LAN configuration

At the MAP terminal

- 1 Obtain the MG 4000 CEM IP address, subnet mask and edge gateway IP address that were assigned by your LAN administrator. (If unavailable, skip steps 2, 4, 4, and 5 and go directly to step 6.)

Note: If this information is not available, then you should consider the IP address information in table MNIP to be correct until this data can be compared with the actual assigned values.

- 2 At the MAP terminal, access table MNIP and, by typing
>TABLE MNIP
and pressing the Enter key.
- 3 Display the heading information for table MNIP, by typing
>HEADING
and pressing the Enter key.
- 4 Position on the MG 4000 tuple that you are troubleshooting, by typing
>POS SPM <spm_no>
and pressing the Enter key.

where

spm_no

is the SPM number (0 to 85)

Example

>POS SPM 40

Example of a MAP screen using MG 4000 number 40

MNIPKEY	SUBNET0	CEM0IP	GATEWAY0	SUBNET1	CEM1IP	GATEWAY1
SPM 40	255 255 255	0 10 102	8 148 \$	255 255 255	0 10 102	8 149 \$

- 5 Verify that the IP address, subnet mask and edge gateway IP address information that is datafilled in table MNIP matches the values assigned by the LAN administrator.
- 6 If the MG 4000 CEM is located on a different subnet than the XA-Core Ethernet links, then you must verify that the edge router (to which the CEM is connected) is configured as follows:
 - has proxy-ARP enabled for the subnet on which the MG 4000 CEM is located.

Note: Proxy-ARP must be enabled because the firmware IP stack does not support a default gateway. Loading a CEM uses TFTP (a UDP protocol) while at firmware.
 - has been configured with the same subnetting information as the CEM (on the interface that connects to the CEM)
- 7 You have completed this procedure. Return to the CI level, by typing

>QUIT ALL

 and pressing the Enter key.

Resolving LAN problems

Use the following procedure when an the an MG 4000 CEM is isolated with a state of not available (NA). For the MG 4000 CEM, the not available state means that the BootP request from the CEM was not received after a reset request was initiated by the XA-Core software. A reset request may be sent by the XA-Core software during a system busy (SYSB) recovery or during the manual execution of the resetmod or loadmod commands.

Resolve the MG 4000 CEM LAN problem

At the MAP terminal

- 1 Verify that the Ethernet links are in-service by performing the procedure to [Determining the state of Ethernet links](#).
- 2 If the MG 4000 CEM is on the same subnet as the XA-Core Ethernet links, then the MG 4000 CEM is not isolated by LAN problems, and you have completed this procedure. If MG 4000 CEM is not on the same subnet as the XA-Core Ethernet links, proceed to step [3](#).
- 3 Use the DAMTSTCI tool to verify that the BootP request from the MG 4000 CEM is received, as follows:
 - a Post the SPM and select the CEM, by typing

```
>MAPCI;MTC;PM;POST SPM <spm_no>;SELECT CEM <cem_no>
```

and pressing the Enter key.

where

spm_no
is the number of the SPM (0 to 85)

cem_no
is the number of the MG 4000 CEM (0 or 1)
 - b If the MG 4000 CEM is SysB (system busy), then manually busy the CEM, by typing

```
>BSY
```

and pressing the Enter key.

Note: The MG 4000 CEM is now manually busy (ManB (NA).
 - c Reset the MG 4000 CEM, by typing

```
>RESETMOD
```

and pressing the Enter key.

- d** Quit the MAPCI, by typing

>QUIT ALL

and pressing the Enter key.

- e** Start the DAMTSTCI tool, by typing

>DAMTSTCI

and pressing the Enter key.

- f** Dump the trace buffer for the MG 4000 CEM and verify that a BootP request (whoami) has been captured, by typing

>TBDUMP SPM <spm_no> CEM <cem_no>

and pressing the Enter key.

where

spm_no

is the number of the SPM (0 to 85)

cem_no

is the number of the MG 4000 CEM (0 or 1)

Example of a MAPCI screen for SPM 4 CEM 0

```
0> NOV-01 13:14:50 MG 4 Unit 0 reset restart pushed
0> NOV-01 13:14:50 MG 4 Unit 0 set FTS state pushed
0> NOV-01 13:14:50 MG 4 Unit 0 set FTS state popped
0> NOV-01 13:14:50 MG 4 Unit 0 reset to firmwar pushed
0> NOV-01 13:15:10 MG 4 Unit 0 whoami received
0> NOV-01 13:15:10 MG 4 Unit 0 reset to firmwar popped
0> NOV-01 13:15:10 MG 4 Unit 0 changed

Node status:      ISTB      Trouble Active   NoMIP
Unit 0 status:    MANB Avail Trouble Inactive NoMIP
Unit 1 status:    ISTB      Trouble Active   NoMIP
0> NOV-01 13:15:59 MG 4 Unit 0 reset restart popped
```

- 4** If the “whoami received” message is displayed, then you have cleared the isolated not available (NA) state for the MG 4000 CEM. If the “whoami received” message is not displayed, then the resetmod command will fail and it is possible that either the reset message sent to the CEM IP address was not received (lost) or the BootP Request from the CEM was not forwarded properly to the XA-Core BootP server.
- 5** Verify that there is a route through the network to the MG 4000 CEM as follows:

- a Use the procedure [Pinging the MG 4000 CEM](#) to ping the CEM.
 - b If there is a response to the ping, then the problem is most likely with the configuration of the BootP agent (typically a software application configured on the edge IP router to which the CEM is connected).
 - c If there is no response to the ping, then use the procedure [Pinging the MG 4000 CEM](#) to ping the edge router address by substituting the GATEWAY <x> IP address from table MNIP for the CEM <x> address. This will confirm whether or not there is a path through the network to that subnet.
- 6 Verify the configuration of the BootP Relay agent for the subnet to which the CEM is connected. Verify with the LAN administrator that the configuration is correct and that the BootP requests from the CEM subnet are being forwarded to one of the XA-Core active IP addresses.
- 7 You have completed this procedure. Return to the CI level of the MAP screen, by typing:
>QUIT ALL
and pressing the Enter key.

Pinging the MG 4000 CEM

Use the following procedure when you are attempting to ping the CEM from the XA-Core Ethernet packet. A “ping” is an ICMP query packet sent to an IP address in order to determine whether it is reachable by means of the Ethernet network, and is able to respond with an ICMP reply. The command interface (CI) on the XA-Core that allows you to generate a ping request is called XAIPTOOL. This tool allows you to generate a ping request from the Ethernet links that are datafilled in table CMIPADDR. The IP addresses of the MG 4000 CEMs are datafilled in table MNIP.

Ping the MG 4000 CEM

At the MAP terminal

- 1 Access table CMIPADDR, and list all of the tuples, by typing
>TABLE CMIPADDR;LIST ALL
 and pressing the Enter key.

Note: In this example, you are pinging MG 4000 40 with CEM 0. Notice in the example MAP screen the CMHOST 0, CMHOST 1 entries. These entries are your active IP addresses that are assigned to the Ethernet links on the Ethernet packets of the XA-Core.

Example of a MAP screen using MG 4000 40, and CEM 0

KEY		DATA	
-----		-----	
GATEWAY 0	GW	(10 102 8 130) 0	CMHOST 0
CMHOST 0	HOST	(10 102 8 144) 22 0	CHHOST 1
CMHOST 1	HOST	(10 102 8 145) 22 0	
ETHRLNK 0	ETHR 5 REAR UPPER	(10 102 8 140) 22 (10 102 8 146) 22 (10 102 8 133) 0	
ETHRLNK 1	ETHR 14 REAR UPPER	(10 102 9 141) 22 (10 102 8 147) 22 (10 102 8 133) 0	
BOTTOM			

- 2 Access table MNIP, display the heading information for the table and position on the MG 4000 you are trying to ping, by typing
>TABLE MNIP;HEADING;POS SPM <spm_no>
 and pressing the Enter key.
where

spm_no

is the number of the SPM (0 to 85)

Note: In this example, the MG 4000 number is 40.

Example of a MAP screen for MG 4000 40

MNIPKEY	SUBNET0	CEM0IP	GATEWAY0	SUBNET1	CEM1IP	GATEWAY1
SPM 40	255 255 255	0 10 102 8 148	\$ 255 255 255	0 10 102	8 149	\$

CEM 0 IP address

3 Make note of the CEM IP (Internet Protocol) address.

4 Exit from the Table Editor, by typing

>QUIT ALL

and pressing the Enter key.

5 Access the XAIPTOOL CI level, by typing

>XAIPTOOL

and pressing the Enter key.

6 List the available host IP addresses, by typing

>HOSTS

and pressing the Enter key.

Example of a MAP screen

- Selected Host IP	: 0 0 0 0
- Active IP Address	: 10 102 8 144
- Mtce IP Address	: 10 102 8 147
- Active IP Address	: 10 102 8 145
- Mtce IP Address	: 10 102 8 146

Active IP address

7 Select an active IP address, by typing:

>SETHOST <active ip_address>

and pressing the Enter key.

where

active ip_address

is an active IP address from the list output by the HOSTS command of the XAIPTOOL.

Note: The active IP address defines the source IP address for the PING request, and is used by the MG 4000 CEM as the destination IP address for the response.

Example

SETHOST 10 102 8 144

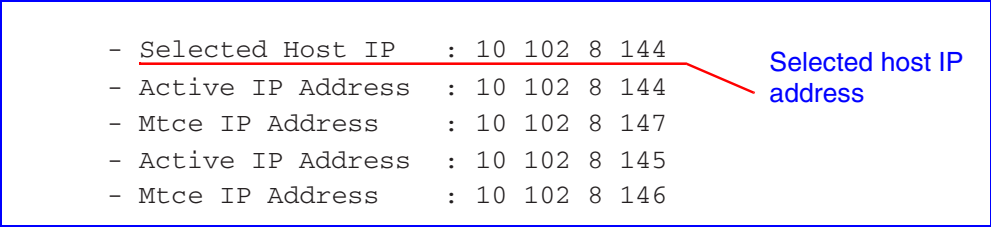
SUCCESS: Host IP has been Set

- 8** Again, list the available host IP addresses, by typing

>HOSTS

and pressing the Enter key.

Example of a MAP screen



```
- Selected Host IP      : 10 102 8 144
- Active IP Address    : 10 102 8 144
- Mtce IP Address      : 10 102 8 147
- Active IP Address    : 10 102 8 145
- Mtce IP Address      : 10 102 8 146
```

- 9** Generate the PING request to the MG 4000 CEM IP address, by typing

>PING <cem ip_address> <no_requests>

and pressing the Enter key.

where

cem ip_address

is the IP address of the CEM that you recorded from table MNIP in step [3](#)

no_requests

is the number of ICMP (Internet Control Message Protocol) query packets that you wish to send (typically you would send between 2 and 5 packets)

Example

PING 10 102 8 148 5

Example of a MAP screen

```
PING DEST: 10 102 8 148 FROM HOST: 10 102 8 144 SIZE: 64 bytes
64 Bytes from 10 102 8 148: icmp_seq=0 time=32 ms
64 Bytes from 10 102 8 148: icmp_seq=1 time=43 ms
64 Bytes from 10 102 8 148: icmp_seq=2 time=37 ms
64 Bytes from 10 102 8 148: icmp_seq=3 time=32 ms
64 Bytes from 10 102 8 148: icmp_seq=4 time=36 ms
---PING DEST: 10 102 8 148 FROM HOST: 10 102 8 144 Statistics ---
5 packets sent, 5 packets received, 0% packet loss
round-trip (ms) min/avg/max = 32/36/43
```

sequence number and time

line indicating the 3rd PING request was received

10 Interpret the results from the PING request.

Note: Each PING request generates a line in the screen output if a reply is successfully received. The line corresponding to each reply packet includes the sequence number of the packet for which there was a reply, and the time taken to receive the reply. The last two lines of the output provide a statistical summary. If no replies are received (100% packet loss) this implies that either there is no route through the network to the MG 4000 CEM Ethernet interface, or the CEM is not able to respond to the request. If all replies are received (0% packet loss) then the CEM is able to respond and there is a working route through the network to the CEM. If only some replies are received (packet loss between 0% and 100%) then the CEM is able to respond, but the integrity of the network path between the ETHRLINK and the CEM is suspect. Excessive delay in the time values may also indicate a network issue such as congestion.

11 You have completed this procedure. Return to the CI level of the MAP screen, by typing

>QUIT ALL

and pressing the Enter key.

Reseating a circuit pack on an MG 4000

Use the following procedure to reseat a circuit pack on an MG 4000.



CAUTION

Before reseating any circuit pack, Nortel Networks recommends that you dump the local logs, if possible. These logs are erased when the card is pulled, but may offer valuable data to Nortel Networks support personnel in the event that a follow-up investigation is required. Depending on the state of the hardware, it may not be possible to collect the local logs prior to reseating the circuit pack.

Reseat a circuit pack on an MG 4000

At the MAP terminal

- 1 Determine if it is possible to dump the local logs prior to reseating the circuit pack. If it is not possible, then proceed to step [7](#). If it is possible to dump the local logs, proceed to step [2](#).
- 2 If possible, remotely log in to the CEM circuit pack, by typing

```
>REMLOGIN SPM <spm_no> <unit_no>
```

and pressing the Enter key.
where
spm_no
is the SPM number (0 to 85)
unit_no
is the number of the CEM (0 or 1)
- 3 If you are not reseating a resource module (RM) circuit pack then proceed to step [6](#), otherwise, if you are reseating an RM, then proceed to step [4](#):
- 4 Determine the logical slot number of the RM to which you wish to log, as follows:

Note: The remote log in command in the dShell requires that you specify the RM based on a logical slot number that is derived from the following equation: slot number = ((14 X shelf number) + slot number).

- a** Post the MG 4000, by typing

```
>MAPCI;MTC;PM;POST SPM <spm_no>
```

and pressing the Enter key.

where

spm_no

is the number of the SPM (0 to 85)

Example of a MAP screen

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
SPM				SysB	ManB	OffL	CBsy	ISTb	InSv
0	Quit	PM		0	0	0	0	3	23
2	Post_	SPM		0	0	0	0	2	2
3	ListSet								
4	ListRes	SPM 40	InSv	Class: SMG4					
5	Trns1								
6		Shlf0	SL	A Stat	Shlf0	SL	A Stat	Shlf1	SL
7	ATMConn	ATM 0	1	A InSv	CEM 1	8	I InSv	DLC 0	1
8		ATM 1	2	I InSv	OC3 0	9	I InSv	-----	2
9		-----	3	-	-----	10	A InSv	-----	3
10		-----	4	-	-----	11	-	-----	4
11	Disp_	-----	5	-	-----	12	-	-----	5
12	Next	-----	6	-	-----	13	A InSv	-----	6
13	Select_	CEM 0	7	A InSv	VSP 1	14	I InSv	DLC 1	7
14	QueryPM								
15	ListAlm								
16									
17	SPERFORM								
18	Upgrade_	SPM:							
	USER								
	Time	15: 06	>						

For example, ATM 0 is in shelf 0, slot 1

- b** To calculate the logical slot number of the RM, to which you wish to log in, use the following equation:

$$\text{logical slot number} = ((14 \times \text{shelf number}) + \text{slot number})$$

Example

Using the example in the MAP screen in step [4a](#) (for MG 4000 number 40) the logical slot number for ATM RM 0 = ((14 x 0) + 1) = 1

- c** Calculate the value of the logical slot number for the RM to which you wish to log in to, and record the value for use in step [5](#).

- 5** Remotely log in to the RM circuit pack, by typing

```
>REMLOGIN -S<slot_number>
```

and pressing the Enter key.

where

slot_number

is the logical slot number of the RM that you calculated in step 4c of this procedure.

- 6 Dump the log buffers to file (and capture the data contained in the buffers) by typing

```
>AER/QUERYBUFFS <month> <day> <hour> <minute>
```

and pressing the Enter key.

where

month

is the month of the year from which to dump log buffers

day

is the day from which to dump log buffers

hour

is the hour from which to dump log buffers

minute

is the minute from which to dump log buffers. You should set this value to zero (0) in order to collect logs for the full hour.

Note: Nortel Networks recommends that you repeat this command for the previous two hours, as well as the hour when the failure condition was first noticed. This will ensure that all relevant log information is collected. The following example, shows the command to use to capture logs for the full hour starting at 2:00 P.M. on Nov 8.

Example

```
>AER/QUERYBUFFS NOV 8 14 0
```

- 7 Reseat the circuit pack on the MG 4000 by following the appropriate procedure in *DMS-100 MMP Card Replacement Procedures Vol 3 of 7*, 297-9051-5473.
- 8 If you have remotely logged in to an MG 4000 RM, return to the CEM dShell level, by typing

```
dSH> REMLOGOUT
```

and pressing the Enter key.

- 9 You have completed this procedure. Return to the CI level, by typing

```
dSH> EXIT
```

and pressing the Enter key.

Replacing a CEM circuit pack

To replace a CEM circuit pack in an MG 4000, see *MG 4000 Fault Management*, NN10076-911.

To replace a CEM circuit pack in an IW SPM, see *IW SPM (ATM) Fault Management*, NN10077-911.

To replace a CEM circuit pack in a DPT SPM, see *DPT SPM (ATM) Fault Management*, NN10080-911.

Determining the state of Ethernet links

Use the following procedure to determine the state of the Ethernet links terminating on the XA-Core.

Determine the state of XA-Core Ethernet links

At the MAP terminal

- 1 Access the Ethernet level of MAPCI, by typing

>MAPCI;MTC;XAC;ETHR

and pressing the Enter key.

where

Example of a MAP screen:

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
ETHR		Front:	111111111	Rear:	111111	SM	PE	IO	PKLT
0 Quit		123456789012345678	456789012345	.	.	.	.	.	.
2	Sta	.	-.-	..	...-.-.-...	0	0	0	0
3	Dep								
4	Typ:				*	*			
5	Slot:	Side:	Packlet:	Status:	Port:	Link:			
6 Tst_	5	Rear	Upper	.	.	.			
7 Bsy_	14	Rear	Upper	.	.	.			
8 RTS_									
9									
10 LoadFW_									
11									
12 Uneq_									
13									
14 Alarm_									
15 Cntrs_									
16									
17 Indicat_									
18 Query_									
USER1									
Time 11: 30 >									

Ethernet link state

- 2 For further information on alarm clearing procedures that relate to the *XA-Core Ethernet links*, see *XA-Core Maintenance Manual*, 297-8991-510.

- 3 You have completed this procedure. Return to the CI level of the MAP screen, by typing:

>QUIT ALL

and pressing the Enter key.

Determining the state of a common equipment module

Use the following procedure to determine the state of the common equipment module (CEM) for an SPM (Spectrum peripheral module) such as an MG 4000, IW SPM, or DPT SPM.

Determine the state of a CEM

At the MAP terminal

- 1 Post the SPM, by typing
>MAPCI;MTC;PM;POST SPM spm_no
 and pressing the Enter key.
where
spm_no
 is the number of the SPM (0 to 85)

Example of a MAP screen:

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
SPM				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		0	0	0	0	3	23
2 Post_		SPM		0	0	0	0	2	2
3 ListSet									
4 ListRes	SPM	40	InSv	Class:	SMG4				
5 Trnsl									
6	Shlf0	SL	A	Stat	Shlf0	SL	A	Stat	Shlf1
7 ATMConn	ATM	0	1	A	InSv	CEM	1	8	I
8	ATM	1	2	I	InSv	OC3	0	9	I
9	-----	3	-	-----	OC3	1	10	A	InSv
10	-----	4	-	-----	-----	11	-	-----	-----
11 Disp_	-----	5	-	-----	-----	12	-	-----	-----
12 Next	-----	6	-	-----	VSP	0	13	A	InSv
13 Select_	CEM	0	7	A	InSv	VSP	1	14	I
14 QueryPM						DLC	1	7	A
15 ListAlm								ALM	0
16									14
17 SPERFORM									A
18 Upgrade_	SPM:								OffL
USER									
Time 15: 06	>								

- 2 Select the CEM, by typing
>SELECT CEM unit_no
 and pressing the Enter key.
where

unit_no

is the number of the CEM (0 or 1)

Example of a MAP screen:

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
CEM				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		0	0	0	0	3	23
2		SPM		0	0	0	0	2	2
3 ListSet		CEM		0	0	0	0	1	1
4									
5 Trnsl		SPM	40	CEM 0	Act	InSv			
6 Tst									
7 Bsy		Loc : Row A	FrPos	7	ShPos	6	ShId	0	Slot 7 Class: SMG4
8 RTS		Default Load:	MG418BS						
9 OffL		Clock:							
10 LoadMod		Input	Ref: Line	Source: ATM	0				Current Mode: Sync
11									
12 Next									
13 Select_									
14 QueryMod									
15 ListAlm									
16 Prot									
17 EraseFl									
18									
		ETAS							
Time	15: 14	>							

state of CEM 0 for MG 4000 40

- 3** You have completed this procedure. Return to the CI level of the MAP screen, by typing:

>QUIT ALL

and pressing the Enter key.

Replacing a resource module circuit pack

To replace a resource module (RM) circuit pack in an MG 4000, see *MG 4000 Fault Management*, NN10076-911.

To replace a resource module (RM) circuit pack in an IW SPM, see *IW SPM (ATM) Fault Management*, NN10077-911.

To replace a resource module (RM) circuit pack in a DPT SPM, see *DPT SPM (ATM) Fault Management*, NN10080-911.

Checking the resource module configuration

Use the following procedure to check the configuration datafill of a resource module (RM) on an SPM of the type MG 4000, IW SPM, or DPT SPM.

Note: If you are able to isolate an RM maintenance problem to a specific RM, then you should perform datafill and configuration checks to identify possible errors.

Check the configuration of an RM

At the MAP terminal

- 1 Post the SPM, by typing
>MAPCI;MTC;PM;POST SPM spm_no
 and pressing the Enter key.
 where
spm_no
 is the number of the SPM (0 to 85)

Example of a MAP screen:

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL			
.	.	.	.	.	.	.	.	.	.			
SPM				SysB	ManB	OffL	CBsy	ISTb	InSv			
0 Quit		PM		0	0	0	0	3	23			
2 Post_		SPM		0	0	0	0	2	2			
3 ListSet												
4 ListRes	SPM	40	InSv	Class: SMG4								
5 Trns1												
6	Shlf0	SL	A	Stat	Shlf0	SL	A	Stat	Shlf1	SL	A	Stat
7 ATMConn	ATM 0	1	A	InSv	CEM 1	8	I	InSv	DLC 0	1	I	InSv
8	ATM 1	2	I	InSv	OC3 0	9	I	InSv	-----	2	-	-----
9	-----	3	-	-----	OC3 1	10	A	InSv	-----	3	-	-----
10	-----	4	-	-----	-----	11	-	-----	-----	4	-	-----
11 Disp_	-----	5	-	-----	-----	12	-	-----	-----	5	-	-----
12 Next	-----	6	-	-----	VSP 0	13	A	InSv	-----	6	-	-----
13 Select_	CEM 0	7	A	InSv	VSP 1	14	I	InSv	DLC 1	7	A	InSv
14 QueryPM									ALM 0	14	A	OffL
15 ListAlm												
16												
17 SPERFORM												
18 Upgrade_	SPM:											
USER												
Time	15: 06	>										

various resource modules (RMs)

- 2 Access table MNCKTPAK, by typing

>TABLE MNCKTPAK

and pressing the Enter key.

- 3 Display heading information for the table, by typing

>HEADING

- 4 Position on the tuple in table MNCKTPAK that is associated with the RM card (you are interested in) by typing

>POS SPM <spm_no> <shlf_no> <slot_no>

and pressing the Enter key.

where

spm_no

is the number of the SPM (0 to 85)

shlf_no

is the number of the SPM shelf (0 or 1)

slot_no

is the slot number (1 to 14)

Example of a MAP screen using VSP 0 in shelf 0 slot 13

CPKKEY									
CPKINFO									
			PEC	RELEASE			LOAD		

SPM 40 0			13	VSP 0 1 WORKING (ECAN 256) \$ (SYSB CR RPT)					
			(MANB MJ RPT) (ISTB MN RPT) (PROTFAIL CR RPT)						
			(PATCHFAIL MJ RPT) \$						
Slot			NTLX66BA	01		DSP18BR			
			PEC			The MG 4000 load is part of the SP18 load line-up (version 18)			

- 5 Ensure that the datafilled Product Engineering Code (PEC) matches the PEC of the RM card that is inserted into the SPM shelf.
- 6 Ensure that the RM card is inserted into the correct slot (and matches the datafilled slot number).
- 7 Ensure that the RM load, that is datafilled in table MNCKTPACK, is the correct load as follows:

- a Use the most recent Release Notes document to check the proper CEM load.

Note: You receive the Release Notes document with the SPM load tape.

- b At the MAPCI, determine the version of the XA-Core load, by typing

>IMAGENAME

and pressing the Enter key.

Note: The version of the RM load (that you are using) must be equal to, or greater than the XA-Core load, but no more than three releases greater than the XA-Core load. In the preceding MAP screen example, the load (DSP18BR is a VSP/DSP load that is part of the SP18 load line-up. In other words, the version is 18.

Example of a MAP screen

```
XANA1 BCS 53 BI built on 2002-SEP-09 at 17:06:00 using
psnn05bk
PRODUCT: SNNCS.005
LOAD: SN000.005
LAYER: BAS.19.0.BI
LAYER: TL.18.0.BI
LAYER: SHR.18.0.AA
LAYER: CCM.18.0.BK
LAYER: CNA.18.0.BK
LAYER: UCS.18.0.BK
LAYER: TOPSC.18.0.BK
LAYER: CNATOPS.18.0.BK
LAYER: BCTOPS.18.0.BK
LAYER: NCS.18.0.BK
LAYER: MSH.18.0.BK
LAYER: SNNCSH.05.0.BK
```

The software release is SN05

Base layer is 19
and is 1 release ahead

The XA-Core load is based on
CSP18 layers (version 18)

- c Compare the version of the RM load in table MNCKTPAK with the version of the XA-Core load (using the IMAGENAME CI tool). Ensure that the version of the RM load is equal to, or greater than the XA-Core load, but no more than three releases greater than the XA-Core load.
- d If the RM can be successfully loaded, check the load names of the load files, by typing

**>MAPCI NODISP;MTC;PM;POST SPM
<spm_no>;QUERYPM FILES**

and pressing the Enter key.

where

spm_no

is the number of the SPM (0 to 85)

Note: The SPM load line-up should be equal to, or no more than three releases above the XA-Core load. If you can successfully load the RM, then you can directly query the load files from the MAP.

Example

MAPCI;NODISP;MTC;PM;POST SPM 40;QUERYPM
FILES

Example of a MAP screen

```
SPM 40 Insv
      .
      .
      .
VSP  0 InSv Act   Default Loadname: DSP18BR
                  Default Filename: DSP18BR_010043
                  Running Load:    DSP18BR_010043
                  Load in Flash:   DSP18BR_010043
```

- e If the RM can be successfully loaded, ensure that the running load, and the load in flash are the same (see MAP screen output for step [7d](#)).
- 8** Check the datafill in table PMLOADS as follows:
- a Access table PMLOADS, by typing

>TABLE PMLOADS

and pressing the Enter key.
 - b Display heading information, by typing

>HEADING

and pressing the Enter key.
 - c Position on the RM load name that matches the datafill in table MNCKTPAK (see step [4](#)), by typing

>POS <load_name>

where

load_name

is the load name of the SPM (for example, MG418BS) and pressing the Enter key.

Example

>POS DSP18BR

Example of a MAP screen

LOADNAME			ACTVOL	UPDACT
ACTFILE			BKPVOL	
BKPFIL				
Active file name		DSP18BR		Active volume name
		DSP18BR_010043	F17LPML1	
		DSP18BR_010043	F17LPML1	
				N

d Ensure that the load file names and volume names are correct by listing the files on the respective volumes.

9 You have completed this procedure. Return to the CI level of the MAP screen, by typing:

>**QUIT ALL**

and pressing the Enter key.

Analyzing SPM 313 logs or QueryPM fault reason output for a CEM

Use the following procedure to troubleshoot system busy (SysB) or in-service trouble (ISTb) CEM conditions using SPM 313 logs and the QueryPM fault reason output. Using these approaches, you can query these CEM device faults and arrive at some recovery actions.

Troubleshoot a SysB or ISTb CEM

At the MAP terminal

- 1 Post the SPM with the CEM that is SysB or ISTb, by typing

```
>MAPCI;MTC;PM;POST SPM spm_no
```

and pressing the Enter key.

where

spm_no

is the number of the SPM (0 to 85)

Note: If you do not know the SPM number, you can post the SPM by specifying the state (for example, POST SPM SYSB).

- 2 Query the fault reasons for all circuit packs on the SPM, by typing

```
>QUERYPM FLT REASON
```

and pressing the Enter key.

- 3 Record the reason that is output by the QueryPM Fault Reason command (in step [2](#)).

- 4 Consult the following table and try and find the “reason” that you recorded (in step [2](#)) within a row in the first column (the “CEM QueryPM Flt Reason” column) of the table.

- 5 If you are able to find a match in the table, then perform the actions described in the second column (Required Action or Comments).

Note: You can also observe the fault reasons for CEM faults, by examining the SPM 313 log. You can view the log by typing:
>LOGUTIL;OPEN SPM 313;BACK ALL.

- 6 If you are unable to find the reason in the table (the table only contains a partial list of fault reasons) then return to procedure from which you came.

CEM Fault reasons that are output by the command QueryPM Flt Reason		Required actions or comments
Loadname mismatch		1. Verify that the loadname in table MNCKPAK is correct for the CEM. 2. If the loadname is not correct, change the datafill to the correct loadname. 3. If the loadname is correct, determine the running load on the CEM (POST the SPM at the MAP, and use the QUERYPM FILES command to list the loads associated with the CEM) and compare the datafilled loadname to the running load on the CEM. 4. If there is a mismatch, then perform a loadmod on the CEM to correct the mismatch.
Unit is in OVERLOAD		If the problem persists, take steps to partially off load traffic from the SPM. Contact your respective Network Engineering department.
Trap critical limit Trap noncritical limit 5 traps in 5 seconds Available sys heap < 1% Available sys heap < 5%		The Resource Monitor on the SPM has detected a problem. Likely, there is a software or hardware problem. Contact your next level of support to collect footprint and logs.

CEM Fault reasons that are output by the command QueryPM Fit Reason	Required actions or comments
Flash integrity error detected	1. Manually busy the CEM if it is not already manually busy. 2. Perform a LOADMOD on the CEM. 3. If the LOADMOD is successful, then return the CEM to service. 4. If the fault still exists after the load and return to service, then replace the CEM circuit pack and re-evaluate the problem. 5. If the LOADMOD operation fails, then replace the CEM circuit pack and re-attempt the LOADMOD command the return to service, then re-evaluate. 6. If the problem persists, contact your next level of support
Shelf PEC doesn't match prov. data	This is a datafill or provisioning problem. Verify and correct the datafill in table MNSHELF.
CPK PEC doesn't match prov. data	This is a datafill or provisioning problem. Verify and correct the datafill in table MNKTPAK, or if necessary, replace the CEM circuit pack with a CEM circuit pack that has the correct PEC.
Own Clock/Frame Error Mate Clock/Frame Error	Likely, there is either faulty hardware on the CEM (that is reporting the fault) or possibly there is faulty hardware on the mate CEM.
RMs are not all InSv or not all OffL Required RM not available	Go to the applicable task flowchart: Troubleshooting a SysB or IsTb MG 4000 resource module (RM) or Troubleshooting Loadmod or Resetmod failures for an MG 4000 RM or Troubleshooting a failure to RTS an MG 4000 resource module (RM) or Troubleshooting MG 4000 RM protection switch failures in this document, and recover the RMs that are not in-service.
MtcDB data not avail-SYNC fails	No provisioning information has been received by the ClkSync subsystem, thus preventing the CEM from returning to service. This should never happen once the CEM is in-service. Check the datafill integrity for the ILM links and Clock fields, then perform a RESETMOD command on the CEM.

CEM Fault reasons that are output by the command QueryPM Fit Reason	Required actions or comments
CARM data not avail-SYNC fails	No carrier information has been received from carrier maintenance. This should not block an CEM state transitions; however, it will prevent the CEM from entering loop-timed operation. 1. Check the state of the OC-3/STS-3 carriers and the OC-3 RMs. If these are all in-service, then validate carrier provisioning. 2. If there are no provisioning issues detected, then attempt a RESETMOD operation on the CEM.
MS Sync data unavailable	No information has been received from the message switch (MS) clocks to indicate what state they are in. This should not block any CEM state transitions; however, it will prevent the CEM from entering loop-timed operation. 1. Check the state of the message switch clocks at the MS Clock MAP level. 2. If everything there is normal and the MS is in sync, there has been data loss between the MS and the CEM. Perform a RESETMOD operation on the CEM.
ILM data unavailable	No information about the DS-512 link states has been received from ILM. This prevents the CEM from returning to service, since there are no C-side links available to start synchronization of the CEM. Check the ENET plane or link states and attempt a recovery of any problems you find. If you are unsuccessful, perform a RESETMOD operation on the CEM.
No clock signal to S-link ASICs	There is no S-Link clock being generated by the CEM oscillator. This is a hardware fault. Replace the CEM.

CEM Fault reasons that are output by the command QueryPM Fit Reason	
Reason	Required actions or comments
System Clk25 signal not present System Clk20 signal not present System Clk15 signal not present System Clk10 signal not present System Clk5 signal not present	There is no (25ns or 20ns or 15ns or 10ns or 5ns) delayed frame pulse being generated by the TIC (which refers to the CEMs clocking system ASIC). Likely, this is a hardware fault. Replace the CEM.
Mate system clock signal lost	This is an indication that the mate CEM cannot see the 32 Mhz system clock from the other CEM. This is not a fault on the CEM that is reporting it, but on the mate CEM. If this log gets generated, no action need be taken on the unit reporting it, but the mate CEM should be checked to determine if it is reporting any problems of its own, or is locked up. Check and possibly replace the mate CEM.

CEM Fault reasons that are output by the command QueryPM Fit Reason	Required actions or comments
No frame pulse from OC-3 RM 0 No frame pulse from OC-3 RM 1	This is an indication that the TIC (which refers to the CEMs clocking system ASIC) does not detect a frame pulse coming from the indicated OC-3 RM, even though carrier maintenance is reporting the RM and OC-3/STS-3 carriers are in-service. This could arise due to a true hardware fault on either the OC-3 RM, or the CEM. It could also arise due to a message loss problem between CarM and ClkSync. Attempt the following recovery steps: 1. Check the RM and OC-3/STS-3 carriers, and if they appear to be normal, then APS the OC-3 RM, then busy and return to service the RM. 2. If the previous step fails, attempt a RESETMOD of the CEM. 3. If both of the previous steps fail, likely, there is a hardware problem. Isolate the problem to either the RM or the CEM by performing card replacements.
No frame pulse from Sync RM 0 No frame pulse from Sync RM 1	This is an indication that the TIC (which refers to the CEMs clocking system ASIC) does not see a frame pulse coming from the indicated SyncRM, even though BITS maintenance is reporting the RM and BITS links are in-service. This may be caused by a hardware fault on either the SyncRM, or the CEM. It could also arise due to a message loss problem between BITS maintenance and ClkSync. Attempt the following recovery steps: 1. Check the RM and BITS links. If they show all is normal, then busy and return the RM to service. 2. If this fails, attempt a RESETMOD of the CEM. 3. If both the previous steps fail, likely there is a hardware problem, so isolate the problem to either the RM or the CEM by performing card replacements.

CEM Fault reasons that are output by the command QueryPM Fit Reason	Required actions or comments
No frame pulse from mate CEM	This is an indication that the TIC (which refers to the CEMs clocking system ASIC) that the mate CEM is not generating a frame pulse across the backplane. Likely, there is a hardware fault. If CEM 0 reports the fault, then CEM 1 has the fault, and vice versa. Note that this signal is used only by the inactive CEM where it constitutes a critical fault. On the active CEM, it's an info log indicating a problem with the inactive CEM. 1. Attempt a RESETMOD on the mate CEM to ensure that there is not a hardware lockup condition. If this fails to clear the problem, then replace the CEM circuit pack.
No frame pulse from DS-512 #0 No frame pulse from DS-512 #1 No frame pulse from DS-512 #2 No frame pulse from DS-512 #3	This is an indication that the TIC (which refers to the CEMs clocking system ASIC) does not see a frame pulse coming from the indicated DS-512 link, even though ILM is reporting the links are in-service. This may be due to a hardware fault on the CEM. It could also be due to a message loss problem between the ILM and ClkSync. 1. Check the ENET plane/link states and attempt recovery of any problems. Failing that, perform a RESETMOD on the CEM. If the problem persists, replace the CEM.
TIC loopback fault	There is a hardware fault being raised in the TIC (which refers to the CEMs clocking system ASIC) as a result of one or more of its pins being stuck at a high or low logic state. Replace the defective CEM.
MC68307 Bus Timed Out MC68307 Halted	The Sync Real-Time Processor (SyncP) code execution path resulted in either a bus timeout, or a halted processor. This is the result of a device on the processor bus not responding due to a hardware lockup or a hardware fault. Perform a RESETMOD on the CEM. If that does not resolve the problem, replace the CEM.

CEM Fault reasons that are output by the command QueryPM Fit	
Reason	Required actions or comments
MC68307 was RESET	The Sync Real-Time Processor (SyncP) has its reset line stuck. This is because a device on the processor bus is not responding, due to a hardware lockup or a hardware fault. Perform a RESETMOD on the CEM. If that does not resolve the problem, replace the CEM.

CEM Fault reasons that are output by the command QueryPM Fit Reason	Required actions or comments
MC68307 has a bus error MC68307 Addressing error MC68307 Illegal Instr. error MC68307 Divide by 0 error MC68307 Check Instr. Viol. err. MC68307 trapped on a TRAPV MC68307 Privilege Violation MC68307 TRACE Interrupt hit MC68307 1010EM Interrupt hit MC68307 1111EM Interrupt hit MC68307 Generic ISR hit MC68307 Uninit Interrupt Vector MC68307 trapped on a TRAPN MC68307 NMI hit MC68307 Interrupt hit MC68307 Invalid Checksum	The Sync Real-Time Processor (SyncP) has encountered an unexpected software problem. This may be because of a software defect, or a corrupted SyncP software load. Perform a RESETMOD operation on the affected CEM. If the problem persists, perform a LOADMOD operation on the affected CEM to force a RELOAD of the SyncP software.

CEM Fault reasons that are output by the command QueryPM Fit Reason	Required actions or comments
SYNC DAC Error	A SyncP data write to TIC hardware failed because of a hardware lockup or hardware fault. First attempt a RESETMOD on the affected CEM. If the RESETMOD is unsuccessful or fails to clear the fault condition, then replace the CEM.
MC68307 in RESET during CONFIG	The SyncP was found to be in the reset state when the Clock HAL attempted to configure it. This is because of a software defect, a corrupted SyncP software load, or a hardware fault. Perform a RESETMOD on the affected CEM. If the problem persists, perform a LOADMOD to force a reload of the SyncP software. If the fault persists, then replace the CEM.
MC68307 Lost Sync w/ Reference	The SyncP is unable to continue tracking a reference because of a software defect, a corrupted load, or a potentially bad signal. SWACT CEMs to see if SyncP recovers. Check the status of the reference signal. Then, perform a RESETMOD or LOADMOD as necessary to recover the CEM.
MC68307 Status Invalid	The SyncP is reporting that it is in a state that is not recognized by the ClkSync application layer. This is a result of a software defect or a corrupted load. Perform a RESETMOD on the affected CEM. If the problem persists, then perform a LOADMOD to force a reload of the SyncP software.
Failed to Acquire Stable SYNC MC68307 Lost All References	The SyncP is unable to achieve proper lock to any of the available clock signals because of a software defect, a corrupted load, or data, or because of a potentially bad signal.

CEM Fault reasons that are output by the command QueryPM Fit Reason	Required actions or comments
MC68307 Has No FW Load	The Sync Real-Time Processor (SyncP) software load initialization did not complete properly because of a software defect, or a corrupted SyncP software load. Perform a RESETMOD on the affected CEM. If the problem persists, do a LOADMOD to force a reload of the SyncP software.
TIC access protocol violation	TIC or PBAC hardware is locked up due to ASIC defects, and a software workaround failed to prevent lockup. Perform a RESETMOD on the affected CEM. If the problem persists, reseal the CEM to clear the hardware lockup. If this is not successful, replace the CEM circuit pack.
Pointer to MC68307 Load Bad MC68307 FW Load Info Bad	The Clock HAL loader for the SyncP software either does not have a pointer to valid load records, or has mismatched data about the software load. Perform a RESETMOD on the affected CEM. If the problem persists, perform a LOADMOD to force a reload of the SyncP software.
MC68307 Reset Op FAILED	A reset operation on the SyncP failed to properly reset the SyncP. This is due to a hardware lockup or a hardware fault. Perform a RESETMOD on the affected CEM. If the problem persists, reseal the CEM to clear the hardware lockup. If this is not successful, replace the CEM.
MC68307 TIMER Int (unused)	The SyncP detected the firing of an unused hardware timer. This could be due to a software defect, corrupted software or a hardware fault. Perform a RESETMOD on the affected CEM. If the problem persists, reseal the CEM to clear the hardware lockup. If this is not successful, replace the CEM.

CEM Fault reasons that are output by the command QueryPM Fit Reason	Required actions or comments
SHARED RAM Mem. Readback Fault	The Clock HAL was unable to read back data it wrote into the SyncP shared memory. This could be due to a software defect, corrupted software or a hardware fault. Perform a RESETMOD on the affected CEM. If the problem persists, reseal the CEM to clear the hardware lockups. If this is not successful, replace the CEM as there is a hardware fault.
SYNC Non-Recoverable Mem. Fit	The clock application software encountered a memory fault in the CEM memory space. This could be a software defect, but is more likely a CEM hardware fault. Perform a RESETMOD on the affected CEM. If the problem persists, reseal the CEM to clear the hardware lockups. If this is not successful, replace the CEM as there is a hardware fault.
Failed to Access TIC	The Clock HAL was unable to access a TIC (which refers to the CEMs Clocking System ASIC) register, or shared RAM which is controlled by the TIC. This could be due to a software defect, corrupted software, or a hardware fault. Perform a RESETMOD on the affected CEM. If the problem persists, reseal the CEM to clear the hardware lockups. If this is not successful, replace the CEM as there is a hardware fault.
VCXO Over 70% of Tuning Range	The CEM oscillator has been aging over time resulting in a 70% DAC offset from the nominal center value (0%) to maintain the nominal frequency. This is not a critical fault, but is an indication that the customer should be monitoring this circuit pack for further aging. This is a normal aging process for high-stability oscillators. No action is required other than to ensure there is a spare CEM circuit pack available, in the event that the oscillator performance degrades further.

CEM Fault reasons that are output by the command QueryPM Fit Reason	Required actions or comments
VCXO Over 90% of Tuning Range	The CEM oscillator has been aging over time resulting in a 90% DAC offset from the nominal center value (0%) to maintain the nominal frequency. This is not a critical fault, but is an indication that the customer should replace this circuit pack because the it will lose its ability to track a clock reference and could cause clocking problems in the office. This is a normal aging process for high-stability oscillators. Replace the CEM circuit pack.
CRC Mismatch on MC68307 PW	The SyncP software load is corrupt and its CRC is no longer consistent with the calculated CRC running in the background as a diagnostic. This is likely a software defect. Perform a LOADMOD on the affected CEM to force a reload of the SyncP software.
SYNC Critical Software Problem	This is an indication that a critical fault has been detected by the clock application. It occurs when non-specific faults are identified and do not specifically fall into one of the other fault categories. An instance of this would be loss of superframe sync on the inactive CEM. Perform a RESETMOD on the affected CEM. If the problem persists, reseal the CEM to clear the hardware lockups. If this is not successful, replace the CEM as there is a hardware fault.
Cannot Sync to Mate Unit	The inactive CEM is unable to achieve synchronization to the active CEM and is thus unable to achieve "mate-sync". This is a critical fault, but could be due to software or hardware. Perform a RESETMOD on the affected CEM. If the problem persists, reseal the CEM to clear the hardware lockups. If this is not successful, replace the CEM as there is a hardware fault.

CEM Fault reasons that are output by the command QueryPM Fit Reason	
Reason	Required actions or comments
Sync Not Responding After Diag	The Sync RMM either received a “failed” response to a diagnostic invocation, or failed to get any response at all. This could be due to clock software or hardware. Perform a RESETMOD on the affected CEM. If the problem persists, reseal the CEM to clear the hardware lockups. If this is not successful, replace the CEM as there is a hardware fault.
No SYNC RM Refs Available	This is an indication that the TIC (which refers to the CEM’s Clocking System ASIC) does not see a frame pulse coming from the SyncRM, even though BITS maintenance is reporting the BITS links are in-service. This is due to a true hardware fault on either the SyncRM or the CEM. It could also be due to a message loss problem between BITS maintenance and ClkSync. Attempt the following recovery steps: 1. Check RM and BITS links. If they show all is normal, busy and return to service the RM. 2. If this fails, attempt a RESETMOD on the CEM. 3. If both of these steps fail, it is a hardware problem, so you must isolate the problem to either the RM or the CEM by doing card swaps.
TIC Reported PCI Bus Fault	The PCI-8 bus used by the PowerPC to communicate with the TIC (which refers to the CEM’s Clocking System ASIC) is locked up and no further communication is possible. This could be due to a software defect or a hardware fault. Perform a RESETMOD on the affected CEM. If the problem persists, reseal the CEM to clear the hardware lockups. If this is not successful, replace the CEM as there is a hardware fault.

CEM Fault reasons that are output by the command QueryPM Fit Reason	Required actions or comments
SYNC OOSpec. prim. ref. NA	The CEM is provisioned for loop-timing, however, there are no OC-3 carriers available for it to use to synchronize to the network. Check that there is at least one OC-3 RM in-service, and that the OC-3 and STS-3 carriers on that RM are also in-service. If these conditions are met, then there is a frequency drift in the office between the MS Clocks and the downstream SONET element driving the OC-3 carriers into the SPM. This is an office clocking problem and must be resolved. Depending on the amount of frequency drift, the CEM could be raising or clearing this condition on a periodic basis. The greater the drift, the more frequently this switching will take place. If the difference is great enough, there will be no switching: the node will simply keep the fault raised.
SYNC using last avail. ref.	The active CEM is down to its last DS-512 link from the ENET as a sync source. If the situation with the C-side carriers is not promptly recovered, the active CEM could drop into a holdover state, triggering a SWACT. The cause of this problem is external to the CEM and likely originates with the state of the links at the ENET. Correct the problem that is causing the C-side links to be unable to provide a proper clocking signal for the active CEM.
SYNC hold/Acq mode unexp.	In normal operation, the CEM clock should always be in sync to the reference source. If those references become unstable, the CEM clock will drop into acquisition mode which is not a normal operating mode for a stable node. If the references fail altogether, then the CEM clock will drop into a holdover mode which will ultimately result in the node going system busy unless a SWACT takes place. This condition is engineered to raise degradations in order to trigger a SWACT. Correct the cause of the C-side link instability or loss of signal. Attempt a CEM SWACT to re-stabilize the node, then issue a RESETMOD on the CEM that was experiencing the problems.

CEM Fault reasons that are output by the command QueryPM Fit Reason	Required actions or comments
Minor freq shift detected (2000) Major freq shift detected (1500) Crtcl freq shift detected (1000)	This is related to the phase creep that ultimately leads to the QLC lockup problem. This is a warning that a threshold has been crossed and that the phase error accumulation is starting to creep towards the QLC problem range. This means there is an office sync problem such that sync frequency traceability between the MS Clocks and the OC-3 carriers has been lost. This condition should be addressed by the Auto-phase bleed functionality that was introduced in SPD17. Contact your next level of support for problem clearing and follow-up investigation.
UNUSED ID - CantGetSemaphore.	The TIC (which refers to the CEM's Clocking System ASIC) hardware handshaking mechanism is locked up and no communication between the PowerPC and SyncP is possible. This should be considered critical. This could be due to a software defect or a hardware fault. Perform a RESETMOD on the affected CEM. If the problem persists, reseal the CEM to clear the hardware lockups. If this is not successful, replace the CEM as there is a hardware fault.
MC68307 Load Length Invalid	The SyncP software load length indicator is corrupt rendering the load unusable by the SyncP. This is a critical problem. This is caused by a software defect or a corrupted CEM load. Perform a LOADMOD on the affected CEM to force a reload of the SyncP software.

- 7 You have completed this procedure. Return to the CI level of the MAP screen, by typing:

>QUIT ALL

and pressing the Enter key.

Analyzing SPM 300 logs or QueryPM fault reason output for an RM

Use the following procedure to troubleshoot system busy (SysB) or in-service trouble (ISTb) RM conditions using SPM 300 logs and the QueryPM fault reason output. Using these approaches, you can query these RM faults and arrive at some recovery actions.

Troubleshoot a SysB or ISTb CEM

At the MAP terminal

- 1 Post the SPM with the CEM that is SysB or ISTb, by typing

```
>MAPCI;MTC;PM;POST SPM spm_no
```

and pressing the Enter key.

where

spm_no

is the number of the SPM (0 to 85)

Note: If you do not know the SPM number, you can post the SPM by specifying the state (for example, POST SPM SYSB).

- 2 Query the fault reasons for all circuit packs on the SPM, by typing

```
>QUERYPM FLT REASON
```

and pressing the Enter key.

- 3 Record the reason that is output by the QueryPM Fault Reason command (in step [2](#)).

- 4 Consult the following table and try and find the “reason” that you recorded (in step [2](#)) within a row in the first column (the “CEM QueryPM Flt Reason” column) of the table.

- 5 If you are able to find a match in the table, then perform the actions described in the second column (Required Action or Comments).

Note: You can also observe the fault reasons for CEM faults, by examining the SPM 300 log. You can view the log by typing:
>LOGUTIL;OPEN SPM 300;BACK ALL.

- 6 If you are unable to find the reason in the table (the table only contains a partial list of fault reasons) then return to procedure from which you came.

RM Fault reasons that are output by the command QueryPM Fit Reason	Required actions or comments
Loadname mismatch	1. Verify that the loadname in table MNCKPAK is correct for the RM. 2. If the loadname is not correct, change the datafill to the correct loadname. 3. If the loadname is correct, determine the running load on the RM (POST the SPM at the MAP, and use the QUERYPM FILES command to list the loads associated with the RM) and compare the datafilled loadname to the running load on the RM. 4. If there is a mismatch, then perform a LOADMOD on the RM to correct the mismatch.
No card in slot: Insert or OFFL the RM card or No card in slot: Load preparation rejected	Reseat or insert the RM circuit pack into the RM slot.
RM reset/restart failed, received Unexpected WAI	Contact your next level of support to collect the footprint and trap information logs from the RM. The problem may be due to a trap or bad hardware. If the RM is Sysb, wait four minutes for the Sysb recovery before taking manual action to recover the RM.

RM Fault reasons that are output by the command QueryPM Fit Reason	Required actions or comments
Please delete all STA resources	This indicates that STA resources are configured on a DSP or VSP. These resources are no longer supported. Contact your next level of support to have these resources deleted.
Check messaging: Inactive CEM to RM loopback test time-out.	1. Remotely log in to the inactive CEM and record the output from the following commands: <pre>/footprint/display active /aer/display ERRORBUF /aer/display IDMBUF /aer/display SPMLM /aer/display HALBUF2</pre> 2. Remotely log in to the affected RM (this can be performed from the inactive CEM, but if this is unsuccessful, then attempt to remotely log in from the active CEM). 3. Record the output from the following command: <pre>/footprint/display active</pre> 4. Provide the information derived from the above commands to Nortel Networks in the event that the problem persists. 5. Perform a busy operation, followed by a RESETMOD, and then RTS on the affected RM. 6. Monitor the status and if the fault still occurs, perform a busy, then a RESETMOD, then an RTS on the inactive CEM. 7. If the problem persists, call your next level of support.

- 7** You have completed this procedure. Return to the CI level of the MAP screen, by typing:

>QUIT ALL

and pressing the Enter key.



IP Solutions troubleshooting

Use this document to isolate and resolve certain network faults for the Succession IP solutions: PT-IP, Intl PT-IP, PT-AAL2, Intl PT-AAL2, UA-IP, Intl UA-IP, IAC, Intl IAC, and Intl IAW.

Troubleshooting workflow

This document contains some troubleshooting tasks for the Succession IP solutions. The table [IP solutions troubleshooting tasks](#) lists these troubleshooting tasks and provides links to the actual tasks (found in this document).

Finding the troubleshooting tasks in this document

The following table lists the IP solutions troubleshooting tasks that are included in this document.

IP solutions troubleshooting tasks (Sheet 1 of 3)

Troubleshooting task
CS 2000 problems
Troubleshooting multiple DS1 carriers in a Carrier Fail Loss (CFL) state
Troubleshooting DS1 carriers in an intermittent Carrier Fail Loss (CFL) state
Troubleshooting DS0s trunks that are in a Carrier Fail Loss (CFL) state
Troubleshooting DS0s trunks that are in a permanent manual busy (PMB) state
Troubleshooting DS0s trunks that are in a System Busy (SB) state
Troubleshooting DS0 trunks that are in a lock out (LO) state
Troubleshooting DS0s trunks that are in a remote manual busy (RMB) state
Troubleshooting line(s) in a permanent lock out (PLO) state

IP solutions troubleshooting tasks (Sheet 2 of 3)

Troubleshooting task
<u>Troubleshooting line(s) in a manual busy (MB) state</u> <u>Troubleshooting line(s) in a system busy (SB) state</u>
GWC problems <u>Troubleshooting a GWC that continuously initializes and fails to return to service (RTS)</u> <u>Troubleshooting a GWC that fails to boot</u> <u>Troubleshooting a GWC that has a poor call completion rate</u> <u>Troubleshooting PRI trunks that remain in a lockout state</u> <u>Troubleshooting a failed attempt to create a GWC image</u> <u>Troubleshooting alarms generated on a GWC</u> <u>Troubleshooting GWC peripheral module log reports</u>

IP solutions troubleshooting tasks (Sheet 3 of 3)

Troubleshooting task

CS 2000 Management Tools problems

[Troubleshooting a failed attempt to add and provision a GWC or to associate a gateway with a GWC](#)

[Troubleshooting a failure to add or delete a GWC](#)

[Troubleshooting when an OSSGate session fails to launch from a PC](#)

[Troubleshooting a connection failure when adding a GWC node](#)

[Troubleshooting a failure to start the SESM server application](#)

[Troubleshooting a failure of the CS 2000 Management Tools alarm manager to properly set alarm date and time](#)

[Troubleshooting small gateway IP addresses that are reset to 0.0.0.0 in the CS 2000 Management Tools server](#)

[Troubleshooting a failure to RTS a DMS Maintenance Application that is IsTb](#)

[Troubleshooting a failure to add a fourth Media Gateway 15000 to a GWC](#)

[Troubleshooting a failure to perform maintenance actions while using the CS 2000 Management Tools](#)

[Troubleshooting a failure to launch CS 2000 SAM21 Manager, CS 2000 Management Tools GUI, or Network Patch Manager](#)

[Troubleshooting problems arising when an SSL certificate is changed and the CM hostname is new or changed](#)

[Troubleshooting combined CS 2000 Management Tools failures](#)

[Troubleshooting a failure to delete a line from a media gateway in the IAC or Intl IAC solution](#)

[Troubleshooting a failed attempt to input the SDNA command in OSSGate](#)

[Troubleshooting a failure to add an endpoint to a GWC during line provisioning of the IAC or Intl IAC solution](#)

Detailed troubleshooting procedures

The detailed troubleshooting procedures contained in this section are intended to be used in conjunction with the troubleshooting tasks.

When you troubleshoot IP network problems, you normally start by accessing the appropriate troubleshooting task. Within the troubleshooting tasks are references to the detailed troubleshooting procedures. If you feel that you need additional information, you simply go to the detailed procedure, then return to the troubleshooting task to continue the troubleshooting process.

The following table lists the detailed troubleshooting procedures for the IP solutions that are included in this document.

Detailed procedures (Sheet 1 of 2)

Detailed procedure
How to correlate carrier information from the MAPCI, to the GWC, and Media Gateway 15000/7400
View GWC PM logs
Checking for Media Gateway logs
Checking for CS 2000 or CS 2000-Compact logs
View and troubleshoot GWC service alarms
View GWC platform hardware alarms
Troubleshooting a provisioning error with a GWC card or node
Returning a trunk member to service
How to correlate line information from the MAPCI to the GWC and line gateway
Passport 8600 Ethernet port configuration, and 100Base-T cable replacement
Viewing SESM configuration settings
Diagnose problems with a GWC card that cannot be booted
Restart or reboot a GWC card
View media proxy configuration data for a GWC node
Setting the CS 2000 CLI on an SSPFS-based server

Detailed procedures (Sheet 2 of 2)**Detailed procedure**

[View and troubleshoot GWC service alarms](#)

[View GWC platform hardware alarms](#) [Retrieve and correlate GWC logs in customer log files](#)

[View GWC logs in syslog files](#) [View GWC PM logs](#)

[Perform a CS 2000 data integrity audit](#)

[Take a manual GWC software image](#) (the last page of the procedure)

[Increasing the size of a logical volume](#)

[Viewing a Media Gateway 15000/7400 endpoint and determining if the endpoint is correctly named](#)

[Pinging the CS 2000 Core Manager](#)

[Ensuring that the OSS Comms Svcs and OSS and Application Svcs are in service](#)

[Checking the status of the DDMS proxy](#)

[Stopping and starting the DDMS proxy](#)

[Starting the SESM server application](#)

[Troubleshooting APS login problems](#)

[Reconfigure NTP service](#)

[Adding the CS 2000 Management Tools Server as a DDMS client of the CS 2000 Core Manager](#)

[Restarting the Apache Web server](#)

[Configuring the SESM server application](#)

[Checking the occupancy of the /opt/ directory on the CS 2000 Management Tools server](#)

[Changing the Oracle user password on an SSPFS-based server](#)

[Adding LEN information back into the XA-Core](#)

[Deleting a line](#)

[Using the table editor to delete a tuple from a table](#)

Troubleshooting multiple DS1 carriers in a Carrier Fail Loss (CFL) state

Use this task to troubleshoot multiple DS1 carriers in a Carrier Fail Loss (CFL) state.

The following procedure describes the sequence of steps you must follow to troubleshoot multiple DS1 carriers in a CFL state.

Procedure for troubleshooting multiple DS1 carriers in a CFL state

- 1 Use the MAPCI and CS 2000 Management Tools applications to correlate the DS1 CFL alarms to the associated GWC and Media Gateway.

Refer to [How to correlate carrier information from the MAPCI, to the GWC, and Media Gateway 15000/7400](#).

- 2 Determine if the DS1 carriers (in the CFL state) span more than one GWC.

If the DS1 carriers	Do
span more than one GWC	step 3
do not span more than on GWC	step 4

- 3 There is a problem with the GWC. Use the appropriate alarm clearing procedure in *GWC Fault Management*, NN10202-911, to fix the problem. Go to [step 15](#).

- 4 Determine if all the DS1 carriers in the CFL state are on a single GWC.

If all the DS1 carriers in the CFL state are	Do
on a single GWC	step 5
not on a single GWC	step 7

- 5 Use the procedures in *GWC Fault Management*, NN10202-911, to ensure that the GWC is up and running. Check the status of the GWC and check for alarms. If there are alarms, use the appropriate alarm clearing procedure in *GWC Fault Management*, NN10202-911, to clear the alarms.

- 6** Determine if you have resolved the problem of DS1 carriers in the CFL state.
- | If the problem is | Do |
|--------------------------|-------------------------|
| fixed | step 15 |
| not fixed | step 7 |
- 7** Determine if the DS1 carriers in the CFL state span all VSP cards in a single Media Gateway.
- | If the DS1 carriers in the CFL state | Do |
|---|-------------------------|
| span all VSP cards | step 8 |
| do not span all VSP cards | step 14 |
- 8** From the GWC, ping the host name that is associated with each VSP card on the Media Gateway that terminates DS1 carriers that are CFL.
- 9** Determine if all the VSP cards respond to the ping attempts.
- | If | Do |
|-------------------------------------|-------------------------|
| all VSP cards respond | step 10 |
| some, but not all VSP cards respond | step 11 |
| none of the VSP cards respond | step 13 |
- 10** There is a physical problem between the public switched telephone network DS1 carriers and the time division multiplex function processor (FP) on the Media Gateway.
Take the necessary steps to isolate the problem. Go to [step 15](#).
- 11** Reset the VSP cards on the Media Gateway that did not respond to the ping attempts.
- 12** Determine if the problem has been resolved.
- | If the problem | Do |
|-----------------------|-------------------------|
| has been resolved | step 15 |
| has not been resolved | step 14 |
- 13** There is a problem with the Media Gateway. Refer to *Nortel Networks Media Gateway 7480/15000 Technology Fundamentals*, NN10600-780 to resolve the problems. Go to [step 15](#) once the problem is resolved.

- 14** Contact your next level of support.
- 15** You have completed this procedure.

Troubleshooting DS1 carriers in an intermittent Carrier Fail Loss (CFL) state

Use this task to troubleshoot DS1 carriers that are intermittently in a Carrier Fail Loss (CFL) state.

The following procedure describes the sequence of steps you must follow to troubleshoot DS1 carriers in an intermittent CFL state.

Procedure for troubleshooting DS1 carriers in an intermittent CFL state

- 1 Use the MAPCI and CS 2000 Management Tools applications to correlate the DS1 CFL intermittent alarms to the associated GWC and Media Gateway.

Refer to [How to correlate carrier information from the MAPCI, to the GWC, and Media Gateway 15000/7400](#).

- 2 Determine if there are any GWC PM logs being generated at the CS 2000 or CS 2000-Compact.

Refer to [View GWC PM logs](#).

If there are	Do

GWC PM logs being generated	step 3

no GWC PM logs being generated	step 5

- 3 There is a problem with the GWC. Use *GWC Fault Management*, NN10202-911, if necessary, to determine if there is any action necessary to fix the problem.

- 4 Determine if the original DS1 problem has been resolved.

If the problem	Do

has been resolved	step 18

has not been resolved	step 5

- 5 Determine if the Media Gateway that terminates the DS1 carrier with the CFL alarms is generating any logs.

If the Media Gateway	Do

is generating logs	step 6

is not generating logs	step 8

- 6 There is a problem with the Media Gateway. Refer to *Nortel Networks Media Gateway 7480/15000 Technology Fundamentals*, NN10600-780 to resolve the problems.
- 7 Determine if the original DS1 problem has been resolved.
- | If the problem | Do |
|-----------------------|-------------------------|
| has been resolved | step 18 |
| has not been resolved | step 8 |
- 8 Determine if there are logs being generated by the routing equipment in the IP packet network.
- | If | Do |
|-----------------------------------|-------------------------|
| there are logs being generated | step 9 |
| there are no logs being generated | step 11 |
- 9 There is a problem with the router equipment in the IP packet network. Use the documentation provided by your 3rd party vendor to fix the problem.
- 10 Determine if the original DS1 problem has been resolved.
- | If the problem | Do |
|-----------------------|-------------------------|
| has been resolved | step 18 |
| has not been resolved | step 11 |
- 11 Determine if there are any CS 2000 or CS 2000-Compact logs being generated.
- | If | Do |
|-----------------------------------|-------------------------|
| there are logs being generated | step 12 |
| there are no logs being generated | step 14 |
- 12 There is a problem with the CS 2000 or CS 2000-Compact. Use the log information to determine what action (if any) is necessary to fix the problem. For more information on CS 2000 or CS 2000-Compact logs, refer to the *XA-Core Reference Manual*, 297-8991-510.
- For information on Call Agent hardware and software logs, STORage Management (STORM) logs, and SAM21 logs, refer to *Succession Fault Management Logs Reference*, NN10275-909.

- 13** Determine if the original DS1 problem has been resolved.
- | If the problem | Do |
|-----------------------|-------------------------|
| has been resolved | step 18 |
| has not been resolved | step 14 |
- 14** Determine if there are any GWC service or hardware alarms.
- | If | Do |
|--|-------------------------|
| there are any GWC service or hardware alarms | step 15 |
| there are no GWC service or hardware alarms | step 17 |
- 15** Refer to *GWC Fault Management*, NN10202-911, to fix the problem.
For details on individual alarms related to NSS cards in the SAM21 shelf, refer to the appropriate information in this document.
- 16** Determine if the original DS1 problem has been resolved.
- | If the problem | Do |
|-----------------------|-------------------------|
| has been resolved | step 18 |
| has not been resolved | step 17 |
- 17** Contact your next level of support.
- 18** You have completed this procedure.

Troubleshooting DS0s trunks that are in a Carrier Fail Loss (CFL) state

Use this task to troubleshoot one or more DS0 trunks that are in a Carrier Fail Loss (CFL) state.

The following procedure describes the sequence of steps you must follow to troubleshoot DS0s in a CFL state.

Note: The CFL status may be the result of the Media Gateway sending Change Status Notification messages to the CS 2000 informing the system that the DS0 trunk is unequipped.

Procedure for troubleshooting DS0 trunks in a CFL state

- 1 Use the MAPCI and CS 2000 Management Tools applications to correlate the DS0 CFL alarms to the associated GWC and Media Gateway.

Refer to [How to correlate carrier information from the MAPCI, to the GWC, and Media Gateway 15000/7400](#).

- 2 Determine if there are any GWC PM logs being generated at the CS 2000 or CS 2000-Compact.

Refer to [View GWC PM logs](#).

If	Do
there are GWC PM logs being generated	step 2
there are no GWC PM logs being generated	step 5

- 3 Check to see if there is a GWC provisioning error.

Refer to [Troubleshooting a provisioning error with a GWC card or node](#).

- 4 Determine if the original DS0 problem has been resolved.

If the problem	Do
has been resolved	step 8
has not been resolved	step 5

- 5 Attempt to return the DS0 trunk to service.

Refer to [Returning a trunk member to service](#).

At the same time, use the Sniffer Network Analyzer to collect signalling information or perform a GWC trace.

If you were**Do**

able to return the DS0 trunk(s) to service

[step 6](#)

unable to return the DS0 trunk(s) to service

[step 7](#)

-
- 6** Check the CS 2000 and GWC history logs to determine the cause of the failure.
- Also check the results of the Sniffer Network Analyzer and the GWC trace to determine the cause of the problem with the Media Gateway equipment.
- Go to [step 8](#).
- 7** Contact your next level of support.
- 8** You have completed this procedure.

Troubleshooting DS0s trunks that are in a permanent manual busy (PMB) state

Use this task to troubleshoot one or more DS0 trunks that are in a permanent manual busy (PMB) state.

The following procedure describes the sequence of steps you must follow to troubleshoot DS0 trunks in a PMB state.

Procedure for troubleshooting DS0 trunks in a PMB state

- 1 A GWC is not accessible, with the result that one or more DS0s are in a PMB state. Refer to *GWC Fault Management*, NN10202-911, to fix the problem.

If the problem	Do
has been corrected	step 3
has not been corrected	step 2

- 2 Contact your next level of support.
- 3 You have completed this procedure.

Troubleshooting DS0s trunks that are in a System Busy (SB) state

Use this task to troubleshoot one or more DS0 trunks that are in a System Busy (SB) state.

The following procedure describes the sequence of steps you must follow to troubleshoot DS0 trunks in an SB state.

Procedure for troubleshooting DS0 trunks in an SB state

- 1 There is a status mismatch between the CS 2000 and the GWC. To fix the problem, check logs and alarms for the CS 2000 and GWC, and follow the appropriate procedures for clearing them. Refer to the following documents:

- *Communication Server 2000 Fault Mananagement*, NN10083-911
- *XA-Core Reference Manual*, 297-8991-810
- *Succession Fault Management Logs Reference*, NN10275-909
- *GWC Fault Management*, NN10202-911

- 2 Determine if you have fixed the problem and are able to return the DS0 links to service.

If the problem	Do
has been resolved	step 4
has not been resolved	step 3

- 3 Contact your next level of support.

- 4 You have completed this procedure.

Troubleshooting DS0 trunks that are in a lock out (LO) state

Use this task to troubleshoot one or more DS0 trunks that are in a lock out (LO) state.

The following procedure describes the sequence of steps you must follow to troubleshoot DS0 trunks in an LO state.

Procedure for troubleshooting DS0 trunks in an LO state

- 1 There is an SS7 problem. Check for logs and alarms to isolate the problem. Refer to the following documents for more information:

- *Communication Server 2000 Fault Management*, NN10083-911
- *XA-Core Reference Manual*, 297-8991-810
- *Succession Fault Management Logs Reference*, NN10275-909
- *USP Fault Management*, NN10071-911

- 2 Determine if you have fixed the SS7 problem and are able to return the DS0 trunks to service.

If the problem	Do
has been fixed	step 4
has not been fixed	step 3

- 3 Contact your next level of support.

- 4 You have completed this procedure.

Troubleshooting DS0s trunks that are in a remote manual busy (RMB) state

Use this task to troubleshoot one or more DS0 trunks that are in a remote manual busy (RMB) state.

The following procedure describes the sequence of steps you must follow to troubleshoot DS0 trunks in an RMB state.

Procedure for troubleshooting DS0 trunks in an RMB state

- 1** The far end public switched telephone network (PSTN) has placed one or more DS0 trunks in a manually busy state. These DS0 trunks must be returned to service at the PSTN site before the DS0 trunk(s) can resume carrying traffic.
- 2** Return the DS0 trunks to service using the appropriate procedure.
- 3** You have completed this procedure.

Troubleshooting line(s) in a permanent lock out (PLO) state

Use this task to troubleshoot one or more lines in a permanent lock out (PLO) state.

This task applies to the UA-IP and IAC solutions. In the UA-IP solution, the line-terminating gateway is the MG 9000. In the IAC solution the line-terminating gateway is the Media Terminal Adapter (MTA).

The following procedure describes the sequence of steps you must follow to troubleshoot lines in a PLO state.

Procedure for troubleshooting lines in a PLO state

- 1 Use the MAPCI and CS 2000 Management Tools applications to correlate the lines alarms to the associated GWC and gateway that terminates the line.

Refer to [How to correlate line information from the MAPCI to the GWC and line gateway](#).

- 2 From the GWC, ping the MG 9000 (for a UA-IP solution) or MTA (for an IAC solution) to determine if the device can be reached.

If the device	Do
can be reached	step 8
cannot be reached	step 3

- 3 From the GWC, perform an IP trace route (a ping with the IP trace route option) to the network element (the MG 9000 or MTA) to determine if the device can be reached.

If the device	Do
can be reached	step 8
cannot be reached	step 4

- 4 Use the IP trace route software to determine if you can reach the edge router that serves the MG 9000 or MTA.

If the edge router	Do
can be reached	step 8
cannot be reached	step 3

- 5 Use the IP trace route software to determine if you are able to reach the edge router that serves the CS 2000.
- | If the edge router | Do |
|--------------------|------------------------|
| can be reached | step 6 |
| cannot be reached | step 7 |
- 6 There is a problem with the IP core packet network. Use the appropriate third party management system and documentation to fix the problem.
Go to [step 9](#).
- 7 There is a problem with the Passport 8600. Use the Device Manager and the appropriate Passport 8600 documentation to fix the problem.
Go to [step 9](#).
- 8 If you are working in a UA-IP solution, then there is a problem with the MG 9000. Use the MG 9000 Manager and *MG 9000 Fault Management*, NN10074-911, to correct the problem.

If you are working with an IAC solution, then there is a problem with the third-party MTA equipment. Use the third-party MTA management system and the appropriate third-party documentation to correct the problem.
- 9 You have completed this procedure.

Troubleshooting line(s) in a manual busy (MB) state

Use this task to troubleshoot one or more lines in a manual busy (MB) state.

The following procedure describes the sequence of steps you must follow to troubleshoot lines in a MB state.

Procedure for troubleshooting lines in a MB state

- 1** The lines have been manually removed from service. To clear the alarm, manually return the line(s) to service. If the line(s) fail to return to service, use the appropriate maintenance procedure to correct the problem.
- 2** You have completed this procedure.

Troubleshooting line(s) in a system busy (SB) state

Use this task to troubleshoot one or more lines in a system busy (SB) state.

The following procedure describes the sequence of steps you must follow to troubleshoot lines in a SB state.

Procedure for troubleshooting lines in a SB state

- 1 If you are working in a UA-IP solution, then there is a problem with the MG 9000. Use the MG 9000 Manager and the appropriate procedures in *MG 9000 Fault Management*, NN10074-911, to correct the problem.

If you are working on an IAC solution, then there is a problem with the third-party MTA equipment. Use the third-party MTA management system and the appropriate third-party documentation to correct the problem.
- 2 You have completed this procedure.

Troubleshooting a GWC that continuously initializes and fails to return to service (RTS)

Use this task to troubleshoot a GWC that continuously initializes and fails to return to service (RTS).

The following procedure describes the sequence of steps you must follow to troubleshoot a GWC that continuously initializes and fails to RTS.

Procedure to troubleshoot a GWC that continuously initializes and fails to RTS

- 1 Determine the setting of the ethernet port on the Passport 8600. Refer to [Passport 8600 Ethernet port configuration, and 100Base-T cable replacement](#).

If the Passport 8600 is set to	Do
100Base-T Half Duplex Auto Negotiate = N	step 2
anything else	step 4

- 2 Change the Ethernet port settings on the Passport 8600 to **100Base-T Half Duplex Auto Negotiate = N**.

Refer to [Passport 8600 Ethernet port configuration, and 100Base-T cable replacement](#).

- 3 Determine if you are able to successfully return the GWC to service.

If you are	Do
able to RTS the GWC	step 11
unable to RTS the GWC	step 4

- 4 Determine if the IP addressing scheme for the GWC is correct. Refer to [View media proxy configuration data for a GWC node](#).

If the IP addressing scheme	Do
is correct	step 5

If the IP addressing scheme		Do
is incorrect		step 7
5	Assign four consecutive IP addresses to the GWC. The first IP address must be divisible by 4. For more information, refer to <i>GWC Configuration Management</i> , NN10205-511, in the introductory section. This contains information on how to modify the base configuration of a GWC.	
6	Determine if you are able to successfully return the GWC to service.	
If you are		Do
able to RTS the GWC		step 11
unable to RTS the GWC		step 7
7	Determine if the cabling between the GWC and the Passport 8600 router is correctly installed and fully functional. Refer to Passport 8600 Ethernet port configuration, and 100Base-T cable replacement .	
If the cabling		Do
is functional		step 10
not functional		step 8
8	Replace the cabling between the GWC and the Passport 8600 router with cabling that supports 100Mb/s bandwidth. Refer to Passport 8600 Ethernet port configuration, and 100Base-T cable replacement .	
9	Determine if you are able to successfully return the GWC to service.	
If you are		Do
able to RTS the GWC		step 11
unable to RTS the GWC		step 10
10	Contact your next level of support.	
11	You have completed this procedure.	

Troubleshooting a GWC that fails to boot

Use this task to troubleshoot a GWC that fails to boot.

The following procedure describes the sequence of steps you must follow to troubleshoot a GWC that fails to boot.

Procedure for troubleshooting a GWC that fails to Boot

- 1 There is a problem with the GWC. Diagnose the problems that prevent the GWC from booting.

Refer to [Diagnose problems with a GWC card that cannot be booted](#).

- 2 Determine if you can boot the GWC successfully.

Refer to [Restart or reboot a GWC card](#).

If you are	Do
able to boot the GWC successfully	step 4
unable to boot the GWC successfully	step 3

- 3 Contact your next level of support.
- 4 You have completed this procedure.

Troubleshooting a GWC that has a poor call completion rate

Use this task to troubleshoot a GWC that has a poor call-completion rate.

The following procedure describes the sequence of steps you must follow to troubleshoot a GWC that has a poor call-completion rate.

Procedure for troubleshooting a GWC that has a poor call completion rate

- 1 Determine the setting of the ethernet port on the Passport 8600. Refer to [Passport 8600 Ethernet port configuration, and 100Base-T cable replacement](#).

If the Passport 8600 is set to	Do

100Base-T Half Duplex Auto Negotiate = N	step 2

anything else	step 4

- 2 Change the Ethernet port settings on the Passport 8600 to **100Base-T Half Duplex Auto Negotiate = N**. Refer to [Passport 8600 Ethernet port configuration, and 100Base-T cable replacement](#).

- 3 Determine if the GWC call completion rate is acceptable.

If the GWC call completion rate is	Do

acceptable	step 5

unacceptable	step 4

- 4 Contact your next level of support.
- 5 You have completed this procedure.

Troubleshooting PRI trunks that remain in a lockout state

Use this task to troubleshoot primary rate interface (PRI) trunks that remain in a lockout state.

The following procedure describes the sequence of steps you must follow to troubleshoot PRI trunks that remain in a lockout state.

Procedure for troubleshooting PRI trunks that remain in a Lockout state

- 1 Determine if the Media Gateway hostname matches the gateway name that is datafilled in the CS 2000 Management Tools software.

If the Media Gateway host-name	Do

matches the gateway name	step 2

does not match the gateway name	step 5

- 2 Determine if the Media Gateway carrier endpoint name contains a leading 0 (zero), for example **DS1_02031.1**

Refer to [Viewing a Media Gateway 15000/7400 endpoint and determining if the endpoint is correctly named](#).

If the carrier endpoint name	Do

contains a leading zero	step 7

does not contain a leading zero	step 3

- 3 There is a problem with the Media Gateway. Refer to *Nortel Networks Media Gateway 7480/15000 Technology Fundamentals*, NN10600-780, to fix the problem.

- 4 Determine if you have eliminated the PRI trunk lockout state.

If the PRI trunk lockout state	Do

has been eliminated	step 8

has not been eliminated	step 7

- 5 Change the Media Gateway hostname to match the gateway name in the CS 2000 Management Tools datafill. For detailed

information, refer to *Nortel Networks Media Gateway 7480/15000 Switched Service Configuration Management*, NN10600-782.

- 6** Determine if you have eliminated the PRI trunk lockout state.

If the PRI trunk lockout state	Do

has been eliminated	step 8

has not been eliminated	step 7

- 7** Contact your next level of support.

- 8** You have completed this procedure.

Troubleshooting a failed attempt to create a GWC image

Use this task to troubleshoot a failed attempt to create a GWC image.

The following procedure describes the sequence of steps you must follow to troubleshoot a failed attempt to create a GWC image.

Procedure for troubleshooting a failed attempt to create a GWC image

- 1 In the response dialog at the GWC Manager client window, click the Show Details button after a failure to take the image.

- 2 Examine the Return Code (RC) value in the dialog box.

If the RC value equals	Do
-4	step 3
-9	step 5
any other value	step 7

- 3 The directory permissions for the directory /swd/gwc/ on the CS 2000 Core Manager are incorrect. Change the directory permissions to 777 using the chmod command.

Refer to [Take a manual GWC software image](#) (the last page of the procedure).

- 4 Determine if you are able to correct the problem and successfully create a GWC image.

If	Do
you are able to create a GWC image	step 10
you are unable to create a GWC image	step 9

- 5 There is not enough space allocated on the CS 2000 Core Manager for directory /swd/gwc/. Increase the disk space allocated on the CS 2000 Core Manager for the /swd/gwc/ directory using the SDM RMI sdmmtc->storage->change lv command.

- 6** Determine if you are able to correct the problem and successfully create a GWC image.

If	Do
you are able to create a GWC image	step 10
you are unable to create a GWC image	step 9

- 7** Use the following table to correct the FTP problem.

RC value	Reason for the FTP error	Explanation
-1	BAD_HOST_IP	incorrect Host IP
-2	BAD_USER	incorrect UserID
-3	BAD_DIR	incorrect directory
-5	ABORT_SERV	A service has aborted.
-6	ABORT_USER	A user has aborted.
-7	ERROR	error
-8	ERROR_DATA_CONN	data connection error
-10	ERROR_CMD	incorrect command
-11	FILE_NOTFOUND	The file was not found.
-12	BUFFER_TOO_SMALL	The buffer is too small.
-13	TRANSFER_INCOMPLETE	Transfer is incomplete
-14	RENAME_ERROR	An error in renaming
-15	IMAGE_FILE_FAIL	Failure to create an image file.

- 8** Determine if you are able to correct the problem and successfully create a GWC image.

If	Do
you are able to create a GWC image	step 10
you are unable to create a GWC image	step 9

- 9** Contact your next level of support.
- 10** You have completed this procedure.

Troubleshooting alarms generated on a GWC

For information on troubleshooting GWC alarms, see the document *GWC Fault Management*, NN10202-911.

Troubleshooting GWC peripheral module log reports

For information on troubleshooting GWC peripheral module (PM) log reports, see the document *GWC Fault Management*, NN10202-911.

Troubleshooting a provisioning error with a GWC card or node

Use this task to troubleshoot a provisioning error with a GWC card or node.

The following procedure describes the sequence of steps you must follow to troubleshoot a provisioning error with a GWC card or node.

Procedure for troubleshooting a provisioning error with a GWC card

- 1 Determine if there are logs or alarms generated indicating a possible GWC card or node provisioning problem.

If there are	Do

alarms or logs generated	step 2

no alarms or logs generated	step 4

- 2 Perform a data integrity audit using the procedure “Perform a GWC line data integrity audit” in *GWC Fault Management*, NN10202-911. Then perform the actions necessary to fix the problem.

- 3 Determine if you have corrected the provisioning error associated with the GWC card.

If the provisioning error is	Do

corrected	step 5

not corrected	step 4

- 4 Contact your next level of support.
- 5 You have completed this procedure.

Troubleshooting a failed attempt to create a GWC image from the CS 2000 Management Tools GUI

In order to troubleshoot a failed attempt to create a GWC image from the CS 2000 Management Tools GUI, use the procedure [Troubleshooting a failed attempt to create a GWC image](#) that is located in this document.

Troubleshooting a failed attempt to add and provision a GWC or to associate a gateway with a GWC

Use this task to troubleshoot a failed attempt to add and provision a GWC. In addition, use this task to troubleshoot a failed attempt to associate a gateway (such as line, or trunk media gateway) with a GWC.

The following procedure describes the sequence of steps you must follow to troubleshoot a failed attempt to add and provision a GWC or to associate a gateway with a GWC.

Procedure for troubleshooting a failed attempt to add or provision a GWC or to associate a gateway with the GWC

- 1 The computing module common language location identifier (CM CLLI) may be configured incorrectly on the CS 2000 Management Tools server. The CM CLLI is the name of the office and is case sensitive. However, there are many other reasons why this problem might occur.
- 2 Determine if the CM CLLI is correctly configured on the CS 2000 Management Tools server.

Refer to [Viewing SESM configuration settings](#).

If the CM CLLI is configured	Do

correctly	step 5
incorrectly	step 3

- 3 Correct the CM CLLI on the CS 2000 Management Tools server. Refer to [Setting the CS 2000 CLLI on an SSPFS-based server](#).
- 4 Determine if you were able to correct the problem and that you are now able to add and provision GWCs or associate gateways successfully.

If	Do

you have corrected the problem	step 6
you have not corrected the problem	step 5

- 5 Contact your next level of support.
- 6 You have completed this procedure.

Troubleshooting a failure to add or delete a GWC

Use this task to troubleshoot a failed attempt to add or delete a GWC.

Note: This problem only occurs during initial provisioning of the office.

The following procedure describes the sequence of steps you must follow to troubleshoot a failed attempt to add or delete a GWC.

Procedure for troubleshooting a failed attempt to add, or delete a GWC

- 1 There is a failed attempt to add or delete a GWC. The reason for this failure is that Table SITE does not have an entry with a key of "LG".
- 2 Using the appropriate procedure, add an entry to table SITE with a key of "LG" using the Table Editor. Then reattempt to add or delete a GWC.
- 3 Determine if you are now able to add or delete a GWC successfully.

If	Do
you are able to add or delete a GWC successfully	step 5
you are unable to add or delete a GWC successfully	step 4

- 4 Contact your next level of support
- 5 You have completed this procedure.

Troubleshooting when an OSSGate session fails to launch from a PC

Use this task to troubleshoot an OSSGate session that fails to launch from a an IBM type of personal computer (PC) .

The following procedure describes the sequence of steps you must follow to troubleshoot a failure to launch an OSSGate session from a PC.

Procedure for troubleshooting an OSSGate session that fails to launch from a PC

- 1 The Windows Telnet client sends the username and password character-by-character to the OSSGate application; however, the OSSGate application expects the username and password to be sent in an entire line. As a result, the OSSGate application displays the following error message.

`"Incomplete login information supplied"`

To fix this problem, launch the OSSGate session from a Unix Telnet client instead of from a PC Telnet client.

- 2 Determine if you were able to correctly launch OSSgate.

If	Do
you were able to launch OSSGate	step 4
you were unable to launch OSSGate	step 3

- 3 Contact your next level of support.
- 4 You have completed this procedure.

Troubleshooting a connection failure when adding a GWC node

Use this task to troubleshoot a connection failure when adding a GWC node.

Note: Use this procedure if there is connection failure when adding a GWC node, and you receive the following error message: *“An error has been detected while trying to communicate to the Server. Please close the current session and restart the client.”*

The following procedure describes the sequence of steps you must follow to troubleshoot a connection error when adding a GWC node.

Flowchart for troubleshooting a connection failure when adding a GWC node

- 1 Determine if you received the following message when attempting to add the GWC node:
“An error has been detected while trying to connect to the Server. Please close the current session and restart the client.”

If	Do
you received the message	step 2
you did not receive the message	step 12
- 2 There is a communication failure between the SESM server application and the OSSComms system on the CS 2000 Core Manager.
This may be a network-wide problem. Attempt to ping the CS 2000 Core Manager from the CS 2000 Management Tools Server. Refer to [Pinging the CS 2000 Core Manager](#).

If	Do
you were able to ping the CS 2000 Core Manager	step 4
you were unable to ping the CS 2000 Core Manager	step 3
- 3 There is a network wide problem. Check for alarms and logs using the appropriate procedures to fix the network problem.

Then attempt to add the GWC node.

		If	Do
		you were able to add the GWC node	step 13
		you were unable to add the GWC node	step 4
4	The OSSComms and the OSS and Applications services applications may be in a failed state on the CS 2000 Core Manager.		
5	Log in to the CS 2000 Core Manager console and check the state of the OSS Comms Svcs and OSS and Applications Svcs applications. Refer to Ensuring that the OSS Comms Svcs and OSS and Application Svcs are in service.		
6	Determine if the two applications are in-service.		
		If the two applications are	Do
		in-service	step 8
		not in-service	step 7
7	Manually busy, then return to service the OSS Comms Svcs application and the OSS and Application Svcs application. Then attempt to add the GWC node.		
		If	Do
		you were able to add the GWC node	step 13
		you were unable to add the GWC node	step 8
8	Check the status of the DDMS proxy utility that runs on the CS 2000 Management Tools server. Refer to Checking the status of the DDMS proxy.		
		If the DDMS proxy utility	Do
		is running	step 12
		is not running	step 9
9	Restart the DDMS proxy utility. Refer to Stopping and starting the DDMS proxy.		

- 10** Restart the SESM server application.
Refer to [Starting the SESM server application](#).
- 11** Determine if the communication problem is fixed and you are able to add a GWC.

If	Do
the problem is fixed	step 13
the problem is not fixed	step 12

- 12** Contact your next level of support.
- 13** You have completed this procedure.

Troubleshooting a failure to start the SESM server application

Use this task to troubleshoot the SESM server application when the application fails to start, and there is an mi2 log that states:
ORA-01034 ORACLE not available;
ORA-27101 shared memory realm does not exist,
SVRA Error No such file or directory.

The following procedure describes the sequence of steps you must follow to troubleshoot the SESM server application when the application fails to start.

Procedure for troubleshooting a failure to start the SESM server application

- 1 If the SESM server fails to start, determine if you have received the following CS 2000 Management Tools server database error message:

```
java.sql.SQLException:  
ORA-01034:ORACLE not available  
ORA-27101:shared memory realm does not exist  
SVR4 Error 2: No such file or directory
```

If	Do
you received the message	step 2
you did not receive the message	step 5

- 2 At the APS server, determine if the Oracle server is running.
Refer to [Troubleshooting APS login problems](#).

If the Oracle server	Do
is running	step 5
is not running	

- 3 Start the Oracle database.
Refer to [Troubleshooting APS login problems](#).

- 4** Determine if you are able to start the SESM server application.

If**Do**

you are able to start the SESM
server application

[step 6](#)

you are unable to start the SESM
server application

[step 5](#)

- 5** Contact your next level of support.

- 6** You have completed this procedure.

Troubleshooting a failure of the CS 2000 Management Tools alarm manager to properly set alarm date and time

Use this task to troubleshoot a failure of the CS 2000 Management Tools alarm manager to properly set alarm date and time.

Use this task when the alarms are being output with date or time such those shown in following example: 21:37:10 3-Mar-2036. While this problem is occurring, the date and time on the CS 2000 Core Manager, the CS 2000 Management Tools, and the CS 2000 are all set correctly. When this problem occurs, the inaccurate date is also shown in the details sub-window at the bottom of the main window.

The following procedure describes the sequence of steps you must follow to troubleshoot a failure of the CS 2000 Management Tools alarm manager to properly set alarm date and time.

Procedure for troubleshooting the CS 2000 Management Tools alarm manager

- 1 Determine if you received the following problem indicators for the CS 2000 Management Tools alarm manager.
 - The alarms are being output with a date and time such as **21:37:103-Mar-2036**
 - The inaccurate date is also shown in the details sub-window at the bottom of the main window.

If

Do

you received the problem indicators

[step 2](#)

did not receive the problem indicators

[step 5](#)

- 2 The source for the Network Time Protocol (NTP) server for the SAM21 shelf is incorrectly set to the CS 2000 Core Manager. This is an error because the CS 2000 Core Manager does not provide NTP.

- 3 Reconfigure the NTP service.

Refer to [Reconfigure NTP service](#).

When you come to the steps for changing the Primary and Secondary NTP server addresses, proceed as follows:

- a** Change the primary IP to the IP address of the master NTP server (master DCE server).
 - b** Change the secondary NTP to **0.0.0.0**.
 - 4** Determine if you are able to correct the original date and time problem.

If	Do
you are able to correct the problem	step 6
you are unable to correct the problem	step 5
- 5** Contact your next level of support.
- 6** You have completed this procedure.

Troubleshooting small gateway IP addresses that are reset to 0.0.0.0 in the CS 2000 Management Tools server

Use this task to troubleshoot the Internet Protocol (IP) addresses of small gateways that are reset to 0.0.0.0 in the CS 2000 Management Tools server.

The following procedure describes the sequence of steps you must follow to troubleshoot small gateway IP addresses that are reset to zero in the CS 2000 Management Tools server.

Procedure for troubleshooting small gateway IP addresses that are reset to zero

- 1 Determine if the IP addresses of all small gateways are reset to 0.0.0.0 in the CS 2000 Management Tools server and that there is no call processing on the associated GWCs after reloading.

If both cases	Do

are true	step 2

are not true	step 6

- 2 The Domain Name Server (DNS) capability is not set up for the IP addresses of the small gateways.

- 3 Determine if you have a backup of the file systems of the CS 2000 Management Tools server.

If	Do

you have a backup	step 4

you do not have a backup	step 6

- 4 Restore the latest CS 2000 Management Tools backup. Refer to the section on Backup and Restore in *Global Administration and Security*, NN10402-600.

- 5 Determine if you were able to correct the original problem.

If	Do

you were able to correct the problem	step 7

you were unable to correct the problem	step 6

- 6** Contact your next level of support.
- 7** You have completed this procedure.

Troubleshooting a failure to RTS a DMS Maintenance Application that is IsTb

Use this task to troubleshoot a failure to return to service (RTS) a digital multiplex system (DMS) Maintenance Application (DMA). After the return-to-service (RTS) fails, the DMA remains in an in-service-trouble (IsTb) state.

The following procedure describes the sequence of steps you must follow to troubleshoot a failure to RTS a DMA that is IsTb.

Procedure for troubleshooting a failure to RTS a DMA that is IsTb

- 1 If the DMS is IsTb and fails to RTS, ensure that the following DMA500 and SDM303 logs have been generated.

- DMA500 NONE TBL Process Status
In Service Trouble. DMA is unable to register with DMI.
- SDM303 MINOR TBL SDM Base Maintenance Package:
SDM_DMA.dma
Process: mtcapp
Trouble condition asserted
Reason: DMA is unable to register with BMI

Note 1: You access the DMA500 log in the directory **/var/adm/custlog** on the CS 2000 Core Manager console.

Note 2: You see the SDM303 log by logging in to the CS 2000 Core Manager as a maint or root user, accessing the **sdmmtc;mtc** level, and inputting the **querysdm flt** command.

- 2 Contact your next level of support.
- 3 You have completed this procedure.

Troubleshooting a failure to add a fourth Media Gateway 15000 to a GWC

Use this task to troubleshoot a failure to add a fourth Media Gateway 15000 to a GWC.

The following procedure describes the sequence of steps you must follow to troubleshoot a failure to add a fourth Media Gateway 15000 to a GWC.

Procedure for troubleshooting a failure to add a fourth Media Gateway 15000 to a GWC

- 1 The typical reason for a failure to add a fourth Media Gateway 15000 is that the first three Media Gateway 15000s were added as media gateways of type PVG15K. The PVG15K media gateway type reserves 1120 endpoints for each Media Gateway 15000. A GWC can only support a total of 4096 endpoints for all of the gateways with which the GWC is associated ($4096 - (3 \times 1120) = 736$). Since a PVG15K media gateway type requires 1120 endpoints, and only 736 are available, the fourth Media Gateway 15000 could not be added.

You have the option of choosing from three Media Gateway 15000 types:

- PVG15K
- PVG15K_1000
- PVG15K_PARTIAL

PVG15K requires 1120 available endpoints.

PVG15K_100 requires 1000 available endpoints.

PVG15K_PARTIAL requires 624 available endpoints.

- 2 To fix the problem, add the fourth Media Gateway 15000 as a PVG15K_PARTIAL since there are only 736 endpoints available.

If	Do
you are able to add the fourth Media Gateway 15000	step 4
you are unable to add the fourth Media Gateway 15000	step 3

- 3 Contact your next level of support.

4 You have completed this procedure.

Troubleshooting a failure to perform maintenance actions while using the CS 2000 Management Tools

Use this task to troubleshoot a failure to perform maintenance actions while using the CS 2000 Management Tools when the XA-Core does not respond.

The following procedure describes the sequence of steps you must follow to troubleshoot a failure to perform maintenance actions while using the CS 2000 Management Tools.

Procedure for troubleshooting a failure to perform maintenance actions while using the CS 2000 Management Tools

- 1 Determine if there is any response from the XA-Core.

If the XA-Core	Do

responds	step 5

does not respond	step 2

- 2 You are experiencing these problems because the common language identifier (CLLI) name of the CM (the host name of the CS 2000 Core Manager) is incorrect in the configuration data of the SESM server application.

Refer to [Setting the CS 2000 CLLI on an SSPFS-based server](#) to correct the CLLI name.

- 3 Additionally, you need to add the CS 2000 Management Tools server as a DDMS client of the CS 2000 Core Manager.

Refer to [Adding the CS 2000 Management Tools Server as a DDMS client of the CS 2000 Core Manager](#).

- 4 Determine if you are now able to perform maintenance activities using the CS 2000 Management Tools and that the XA-Core responds.

If	Do

you are able to perform maintenance activities and the XA-Core responds	step 6

you are unable to perform maintenance activities or the XA-Core does not respond	step 5

- 5** Contact your next level of support.
- 6** You have completed this procedure.

Troubleshooting a failure to launch CS 2000 SAM21 Manager, CS 2000 Management Tools GUI, or Network Patch Manager

Use this task to troubleshoot a failure to launch the CS 2000 SAM21 Manager, the CS 2000 Management Tools GUI, or the Network Patch Manager from the Application Launch Point applet screen.

After failing to launch one of these GUIs, you may receive one of the following error messages:

- SAM21 client must exit
- SESM is down, unreachable or incorrect version
- Check Apache server status (/etc/init.d/apache status). Please correct the problem before logging in through SESM

The following procedure describes the sequence of steps you must follow to troubleshoot a failure to launch CS 2000 SAM21 Manager, CS 2000 Management Tools GUI, or Network Patch Manager.

Procedure for troubleshooting a failure to launch CS 2000 SAM21 Manager, CS 2000 Management Tools GUI, or Network Patch Manager

- 1 Determine if you received one of the following error messages:
 - SAM21EM client must exit
 - SESM is down, unreachable or incorrect version
 - Check Apache server status (/etc/init.d/apache status). Please correct the problem before logging in through SESM

If	Do
you received one of the messages	step 2
you did not receive one of the messages	step 4

- 2 Restart the Apache Web Server.
Refer to [Restarting the Apache Web server](#).
- 3 Wait a minimum of 10 minutes, and then attempt to re-launch to GUIs.

If	Do
you are able to launch the GUIs	step 5

	If	Do
	you are unable to launch the GUIs	step 4
4	Contact your next level of support.	
5	You have completed this procedure.	

Troubleshooting problems arising when an SSL certificate is changed and the CM hostname is new or changed

Use this task to troubleshoot problems arising when a secure socket layer (SSL) certificate is changed and the computing module (CM) hostname (CM CLLI) is new or changed.

Use this troubleshooting procedure if

- A temporary SSL certificate is installed with an Internet Protocol (IP) address instead of a CM hostname (CLLI).
- An SSL certificate is installed using the CM hostname, but afterwards, the hostname is changed.

The following procedure describes the sequence of steps you must follow to troubleshoot problems arising when an SSL certificate is changed and the CM hostname (CM CLLI) is new or changed.

Procedure for troubleshooting problems arising when an SSL certificate is changed and the CM hostname is new or changed

- 1 This situation may arise when a temporary SSL certificate is installed with an IP address instead of a CM hostname, but the CM hostname is subsequently changed.
- 2 Configure the SESM server application with the correct CM hostname.
Refer to [Configuring the SESM server application](#).
- 3 Determine if the problem has been solved.

If the problem	Do
has been solved	step 5
has not been solved	step 4
- 4 Contact your next level of support.
- 5 You have completed this procedure.

Troubleshooting combined CS 2000 Management Tools failures

Use this task to troubleshoot combined failures

- to start the Succession Element and Sub-Network Manager (SESM) server application
- to apply a patch to SESM
- to associate gateways and add endpoints using CS 2000 Management Tools GUIs

The following procedure describes the sequence of steps you must follow to troubleshoot combined failures to start the SESM server application, to apply a patch to SESM, and to associate gateways and endpoints using CS 2000 Management Tools GUIs.

Procedure for troubleshooting combined failures to start SESM server application, to apply a patch to SESM, and to add gateways and endpoints

- 1 Determine if the **/opt/** directory on the CS 2000 Management Tools server is full.

Refer to [Checking the occupancy of the /opt/ directory on the CS 2000 Management Tools server](#).

If the /opt/ directory	Do
is full	step 2
is not full	step 4

- 2 The **/opt/** directory is full because the Oracle system password has expired. Correct the problem by setting a new Oracle system password.

Refer to [Changing the Oracle user password on an SSPFS-based server](#).

- 3 Determine if the original problem has been corrected.

If the problem	Do
has been corrected	step 5
has not been corrected	step 4

- 4 Contact your next level of support.
- 5 You have completed this procedure.

Troubleshooting a failure to delete a line from a media gateway in the IAC or Intl IAC solution

Use this task to troubleshoot a failure to delete a line from a Media Terminal Adapter (MTA) media gateway in the Integrated Access-Cable (IAC) or International (Intl) IAC solution.

This problem occurs when you attempt to delete a line from an IAC or Intl IAC MTA (with the OUT command) in OSSGate with enhanced SERVORD commands, using the line equipment number (LEN) instead of the endpoint information. In OSSGate, with enhanced SERVORD (also referred to as SERVORD+) commands the media gateway name and the termination point name, together define the endpoint. In OSSGate, the endpoint has replaced the LEN. Note, that the terminal point name alone may not be unique in the CS 2000, but the media gateway name and terminal point pair together uniquely describe a subscriber line. In OSSGate, when provisioning lines using SERVORD+ commands, you must always use the endpoint information (terminal point name, and media gateway name) rather than the LEN.

If you attempt to delete a line in OSSGate with SERVORD+ commands using a LEN instead of an endpoint, you create a data mismatch between the XA-Core and the CS 2000 Management Tools data. In the XA-Core, the system deletes the line from table LNINV and cancels service on the LEN. However, in the CS 2000 Management Tools, the endpoint data for the line will still exist.

Once this data mismatch occurs, you will receive an error message stating that the "MG has provisioned endpoints." In addition, using the Gateway Controller (GWC) Manager client graphical user interface (GUI) you will see that the deleted line is still associated with the media gateway.

The following procedure describes the sequence of steps you must follow to troubleshoot a failure to delete a line from an MTA in the IAC or Intl IAC solution.

Procedure for troubleshooting a failure to delete a line from an MTA in the IAC or Intl IAC solution

- 1 There is a data mismatch between the XA-Core and the CS 2000 Management Tools data. In the XA-Core, the line is elected, but in the CS 2000 Management Tools data, the endpoint data for the line still exists.

- 2** To correct the problem, first add the LEN information back into the XA-Core.

Refer to [Adding LEN information back into the XA-Core](#).

- 3** In OSSGate, delete the line using endpoint information.

Refer to [Deleting a line](#).

- 4** Determine if you have corrected the original problem.

If	Do
you have corrected the problem	step 6
you have not corrected the problem	step 5

- 5** Contact your next level of support.

- 6** You have completed this procedure.

Troubleshooting a failed attempt to input the SDNA command in OSSGate

Use this task to troubleshoot a failed attempt to input a SERVORD+ command to set up directory number (DN) attributes (SDNA).

Note: The term SERVORD+ means enhanced SERVORD. You input enhanced SERVORD commands in OSSGATE.

Use this task if you receive the following error messages after the SDNA command fails:

- Unable to allocate new store
- Update to table DNGRPS failed
- Journal File Record Not Created

The following procedure describes the sequence of steps you must follow to troubleshoot a failed attempt to input the SDNA command.

Procedure for troubleshooting a failed attempt to input the SDNA command

- 1 The reason the SDNA command failed is because table DNGRPS in the XA-Core is full.
Correct the problem by removed unused entries in table DNGRPS.
Refer to [Using the table editor to delete a tuple from a table](#).
- 2 Determine if you are now able to input the SDNA command.

If	Do
you are able to input the command	step 4
you are unable to input the command	step 3
- 3 Contact your next level of support.
- 4 You have completed this procedure.

Troubleshooting a failure to add an endpoint to a GWC during line provisioning of the IAC or Intl IAC solution

Use this task to troubleshoot a failure to add an endpoint to a Gateway Controller (GWC) during line provisioning of the IAC or Intl IAC solution.

This failure to add a line endpoint occurs when you attempt to input the New command in OSSGate. Use this task, if after your failed attempt, the system displays the error message: "System: LineProv: EndPoint can not be added to GWC."

In addition, log PM181 is generated with the information that "Static data update Failed—Reason: Failed to Send Static Data."

OSSGate provides the interface through which you input enhanced SERVORD commands. The term SERVORD+ means enhanced SERVORD. When you successfully provision a line in OSSGate using the New command, the system datafills a tuple in table LNINV for the logical group node (LGRP) line.

The following procedure describes the sequence of steps you must follow to troubleshoot a failure to add an endpoint to a GWC during line provisioning of the IAC or Intl IAC solution.

Procedure for troubleshooting a failure to add a line endpoint to a GWC during line provisioning of the IAC or Intl IAC solution

- 1 The boolean **xpm_supports_dynamic_sd** in the XA-Core is corrupted so that it now contains a value of **false**. This value causes the system to block downloads of static data.
- 2 Contact your next level of support.
- 3 You have completed this procedure.

Viewing CS 2000 GWC alarms and logs

This page provides you with the links to the necessary procedures for viewing CS 2000 Gateway Controller (GWC) alarms and logs.

For information on service-related alarms, see [View and troubleshoot GWC service alarms](#).

For information on platform-related alarms, see [View GWC platform hardware alarms](#).

For information on gaining access to customer log files, see [Retrieve and correlate GWC logs in customer log files](#).

For information on gaining access to system log files, see [View GWC logs in syslog files](#).

For information on gaining access to peripheral module (PM) log files, see [View GWC PM logs](#).

Changing the directory permissions on the directory containing the CS 2000 GWC image

To change the directory permissions on the directory containing the CS 2000 image file, use this [Troubleshooting](#) procedure.

Viewing a Media Gateway 15000/7400 endpoint and determining if the endpoint is correctly named

This page provides you with links to procedures for

- viewing a Media Gateway carrier endpoint
- determining if an existing Media Gateway carrier endpoint name violates the required naming conventions

Viewing Media Gateway carrier endpoints

For information on viewing Media Gateway carrier endpoints, see [View carrier provisioning data for a GWC node](#).

Naming conventions for Media Gateway carrier endpoint names

For information on the naming conventions for Media Gateway carrier endpoints, see the *OSSGate User's Guide*, NN10004-512, in the section on provisioning conventions for carrier endpoint names (at the end of the document).

Note: The first digit, in the carrier endpoint name, represents the logical processor (LP) number on the Media Gateway, and is a number from 1 to 15. If the carrier is associated with LP one, then you would use the digit 1, not 01 to indicate this LP. You are not permitted to use a leading zero. For example, DS1_101.1 is correct, but DS1_0101.1 is incorrect.

Pinging the CS 2000 Core Manager

Use this procedure to ping the CS 2000 Core Manager from the CS 2000 Management Tools server.

Pinging the CS 2000 Core Manager

At your workstation

- 1 Telnet to the CS 2000 Management Tools server, by typing
> telnet <server>
and pressing the Enter key.
where
<server>
is the Internet Protocol (IP) address, or host name of the CS 2000 Management Tools server
 - 2 When prompted, enter your user ID, and password.
 - 3 Determine the IP address of the CS 2000 Core Manager as follows:
 - a Change to the root user, by typing
\$ su - root
and pressing the Enter key.
 - b When prompted, enter the root password.
 - c Change directory, by typing
cd /bin
and pressing the Enter key.
 - d Execute the configuration script, by typing
./configure
and pressing the Enter key.
- System response*
- SESM configuration
- 1 - SESM common configuration (IP addresses, Market, CM CLLI)
 - 2 - SESM database tools
 - 3 - SESM related applications configuration (MG9K, LMM)
 - 4 - SESM provisioning configuration

5 - SESM logging configuration 9syslog, sesm debug log)

6 - view sesm configuration settings

x - exit

select -

- e Select option six (view sesm configuration settings), by typing

select - 6

and pressing the Enter key.

Example system response

```
NPM Server IP           : 127.0.0.1
Debuglog Filename       : "ptmdebuglog"
Syslog Backup Hour      : 3
PA Debuglog Level       : "CRT"
SESM Syslog Max File Size : 6144
TrunkProv Max Tuples    : 100
V5.2 Supported          : False
TrunkProv Default Tuples : 50
MI2 Debuglog Level      : "CRT"
CM CLLI                 : RTPS
Office Provisioning Type : line
UE Hostname             : 47.142.89.69
RTPS SDM IP             : 172.17.40.250
Debuglog Max File Size  : 20560
Market                  : NA
SESM Server IP          : 47.142.89.70
Alarm Syslog Enabled    : TRUE
SESM Syslog Backup Minute : 0
SESM Oracle Server IP   : 47.142.89.70
Debuglog File Rotation  : "-lrs"
Debuglog Max # Of Files : 7
Alarm GUI Use Server Timezone: FALSE
```

**CS 2000 Core
Manager IP
address**

- f Note the IP address of the CS 2000 Core Manager.

- g Exit from the SESM Server Application configuration utility, by typing

select - x

and press the Enter key.

- 4 Ping the CS 2000 Core Manager, by typing

ping <ip_address>

and press the Enter key.

where

<ip_address>

is the IP address of CS 2000 Core Manager that you obtained in [step 3](#) substep [f](#).

Example

```
# ping 172.17.40.250
```

Example system response

```
172.17.40.250 is alive
```

- 5** Note there is communication between the CS 2000 Management Tools server and the CS 2000 Core Manager (alive indicates there is communication, dead indicates that there is no communication).
- 6** You have completed this procedure.

Ensuring that the OSS Comms Svcs and OSS and Application Svcs are in service

Use this procedure to determine if the applications OSS Comms Svcs and the OSS Application Svcs are in-service on the CS 2000 Core Manager. If these applications are not in-service, this procedure provides the steps for returning the applications to service.

Ensuring that the applications OSS Comms Svcs and OSS and Application Svcs are in-service

At any workstation or console

- 1 Log in to the CS 2000 Core Manager.
- 2 Access the Application level by typing

sdmmtc appl

and press the Enter key.

Note: Use the up and down commands to scroll through the list of applications.

Example response:

Appl	SDM	CON	512	NET	APPL	SYS	HW	CLLI: SNM3
0 Q	■		■	■	■	■	■	Host: wcary2p3
2			■					Fault Tolerant
3								
4 Logs								
5								
6								
7 Bsy								
8 RTS								
9 OffL								
10								
11								
12 Up								
13 Down								
14 QuerySDM								
15 Locate								
16								
17 Help_								
18 Refresh								

#	Application	State
11	Generic Data Delivery	■
12	SDM_BASE.me4	■
13	SDM_BASE.m1	■
14	SDM_BASE.m8	■
15	SDM_BASE.me8	■
16	OSS Comms Svcs	■
17	Log Delivery Service	■
18	Basic Maintenance Interface	■
19	DNBD Call Data Delivery	■
20	OSS and Application Svcs	■

Applications showing: 11 to 20 of 20

In this example, both applications (16 and 20) are in service

Time 10:58 >■

- 3 Determine the state of the two applications: OSS Comms Svcs and OSS and Application Svcs.

If	Do
both applications are in-service	step 7 , you have completed this procedure
one or both applications are out-of-service	step 4

- 4 Busy the out-of-service application by typing

> **bsy** <application_number>

and press the Enter key.

where

<application_number>

is the number used to identify the application in the list (in the example system display in [step 2](#), the application OSS Comms Svcs is identified by the number 16)

If you	Do
successfully busied the application	step 5
did not successfully busy the application	contact your next level of support

- 5 Return to service the out-of-service application by typing

> **rts** <application_number>

and press the Enter key.

where

<application_number>

is the number used to identify the applications in the list (in the example screen in [step 2](#), the application OSS Comms Svcs is identified by the number 16)

If you	Do
successfully returned to service the application	step 6
did not successfully return the application to service	contact your next level of support

- 6 Repeat [step 4](#) and [step 5](#) for the second out-of-service application if necessary.

- 7 You have completed this procedure.

Checking the status of the DDMS proxy

Use this procedure to check the status of the DMS Data Management System (DDMS) proxy that runs on the CS 2000 Management Tools server.

Checking the status of the DDMS proxy

At your workstation

- 1 Telnet to the CS 2000 Management Tools server by typing
> telnet <ip_address>
and press the Enter key.
where
<ip_address>
is the Internet Protocol (IP) address of the CS 2000 Management Tools server
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing
\$ su - root
and press the Enter key.
- 4 When prompted, enter the root password.
- 5 Determine if the DDMS proxy is running, by typing
/etc/init.d/ddmsproxy status
- 6 Note whether the DDMS proxy is running or not running.
- 7 You have completed this procedure.

Adding the CS 2000 Management Tools Server as a DDMS client of the CS 2000 Core Manager

Use the following procedure to add the CS 2000 Management Tools Server as a DDMS client of the CS 2000 Core Manager.

Add the CS 2000 Management Tools Server as a DDMS client

At the local or remote VT100 console

- 1 Log into the CS 2000 Core Manager as a maint class user or root user and access the maintenance interface by typing

sdmmtc

and press the Enter key.

- 2 Access the Config level by typing

config

and press the Enter key.

Example of a screen showing the Config level on the CS 2000 Core Manager

```

SDM      CON      512      NET      APPL      CCS      SYS      HW      CLI:  SNM0
.         .         .         .         .         .         .         .      Host:  wcaru2p5
Config   Fault Tolerant
0 Quit
2
3
4
5
6
7 Select
8 Config
9
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
root
Time 10: 58 >■ Select 1

Filter: OFF
# Fileset Description Status
1 OSS Comms Svcs Configured
2 Enhanced Terminal Access Configured
3 Passport Log Steamer Configured
4 Remote Registration System Configured
5 Secure File Transfer Anon: Y;Normal: Y;Secured: N
Configuration programs: 1 to 5 of 5
  
```

Fileset numbers

Selecting the OSS Comms Svcs fileset

- 3 In the list of filesets, find OSS Comms Svcs and note the fileset number to the left of the Fileset Description.

- 4 Select OSS Comms Svcs by typing

select <fileset number>

and pressing the Enter key.

where

<fileset number>

is the number shown to the left of the Fileset Description.

Example

select 1

- 5 Start to configure the OSS Comms Svcs fileset by typing

config

and pressing the Enter key.

Example of a screen showing system output

```
#####
# Configuring 'SDM_DDMS.osscomms'.
#####
#####
# User Administration Disabled... #
#####
setting authentication_enabled=0 in uAdmin.cfg
User authentication is disabled.
#####
# Adding DDMS logroute configuration
#####
Please add DDMS log routing:
    Device Type = file
    File        = /data/logs/ossaps/ossapslog
    Routing     = addrep
    log_type    = DDMS
Press <RETURN> when ready
```

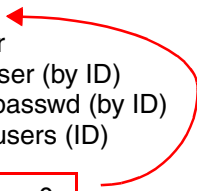
- 6 Advance to the CM User Setup screen by pressing the Enter key.

Example of the CM User Setup screen

CM User Setup

- 0. QUIT
- 1. Add user
- 2. Delete user (by ID)
- 3. Update passwd (by ID)
- 4. Display users (ID)

Enter choice: 0



7 Advance to the DDMS Clients Configuration screen by typing:

0

and pressing the Enter key.

Example of the DDMS Clients Configuration screen

DDMS Clients Configuration

- 0. QUIT
- 1. Add new clients
- 2. Remove existing client
- 3. List existing clients

Enter choice: 1



8 From the DDMS Clients Configuration list choose to add new clients, by typing

1

and pressing the Enter key.

9 Enter the Internet Protocol (IP) address of the CS 2000 Management Tools Server by typing

<CS2K_tool_server_ip_address>

and pressing the Enter key.

where

<CS2K_man_server_ip_address>

is the IP address of the CS 2000 Management Tools server

Example

47.142.89.70

- 10 Exit from the DDMS Clients Configuration screen by typing
done
and pressing the Enter key.
- 11 If the addition fails, contact your next level of support.
- 12 You have completed this procedure.

Restarting the Apache Web server

Use the following procedure to restart the Apache Web server if you are unable to launch CS 2000 SAM21 Manager, CS 2000 Management Tools GUI, or Network Patch Manager. The Apache Web server is one of the servers included in the Succession Server Platform Foundation Software (SSPFS) which in turn is a software package included in the CS 2000 Management Tools suite of software.

Restart the Apache Web server

At the local or remote VT100 console

- 1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.
where

```
<server>
```

is the Internet Protocol (IP) address, or host name of the CS 2000 Management Tools 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 your root password.
- 5 Restart the Apache Web server by typing

```
# /etc/init.d/apache restart
```

and pressing the Enter key.
- 6 If the restart fails, contact your next level of support.
- 7 You have completed this procedure.

Checking the occupancy of the /opt/ directory on the CS 2000 Management Tools server

Use the following procedure to check the occupancy of the /opt/ directory on the CS 2000 Management Tools server. Use this procedure to verify that the /opt/ directory is full.

Check the occupancy of the /opt/ directory

At your workstation

- 1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

<server>

is the Internet Protocol (IP) address or host name of the CS 2000 Management Tools server.

- 2 When prompted, enter your user ID and password.
- 3 Determine the occupancy of the /opt/ directory by typing

```
$ df -k
```

Example of a screen showing occupancy of the /opt/ directory at 98%

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/md/dsk/d2	4129290	917130	3170868	23%	/
/proc	0	0	0	0%	/proc
fd	0	0	0	0%	/dev/fd
mnttab	0	0	0	0%	/etc/mnttab
/dev/md/dsk/d8	2053605	61268	1930729	4%	/var
swap	3657696	40	3657656	1%	/var/run
/dev/md/dsk/d11	5161437	5161437	3717413	98%	/opt
/dev/md/dsk/d25	6192797	6168	6124720	1%	/user_audio_files
swap	524288	504	523784	1%	/tmp
/dev/md/dsk/d23	10322300	10259	10208818	1%	/audio_files
/dev/md/dsk/d24	10322300	10258	10208819	1%	/PROV_data
/dev/md/dsk/d20	3080022	248034	2770388	9%	/data
/dev/md/dsk/d21	3080022	134091	2884331	5%	/opt/nortel
/dev/md/dsk/d22	12386331	8771798	3490670	72%	/data/oradata

- 4 You have completed this procedure.

Adding LEN information back into the XA-Core

Use the following procedure to add line equipment number (LEN) information back into the XA-Core by using the NEW command in OSSGate. Only use this procedure if you have attempted to delete a line in OSSGate using the OUT command and you have incorrectly specified the LEN instead of the endpoint. As a result, there is now a data mismatch (relating to the deleted line) that exists between the XA-Core and the CS 2000 Management Tools data. In the XA-Core the line has been deleted, but in the GWC Manager client, the line endpoints still exist. Once you have added the LEN information back into the XA-Core (using this procedure), you can then correctly delete the line in OSSGate using the OUT command by specifying the endpoint information (termination point name, and media gateway name).

Note: This procedure requires that you Telnet to the OSSGate application that resides on the CS 2000 Management Tools server.

Add the LEN information back into the XA-Core

At the PC connected to the local area network (LAN)

- 1 Initiate a Telnet session to OSSGate by typing
telnet <ossgate_server_name> <port_number>
and pressing the Enter key.
where
<ossgate_server_name>
is the hostname or the IP address of the server on which
OSSGate is running
<port_number>
is the server port used by OSSGate (the default is 10023)

Example

telnet wcn0s5jk 10023

Example of system response:

Trying 47.142.94.80...

Connected to wcn0s5jk.

Escape character is '^['.

Enter username and password

2 Enter your user name and password by typing

<username> <password>

and pressing the Enter key.

Example

user1 passwd

Example of a system response

```
*****
**                                     **
**                                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.          **
**                                     **
*****
```

3 You have connected to OSSGate, and the system is displaying a prompt (the ">" character) in the telnet window on your screen. Now you must put the telnet session into CI mode. Proceed as follows.

a Hold down the control key and type B.

Example of system response:

?

- b** At the question-mark prompt enter the command interpreter mode by typing

mode ci

and press the Enter key.

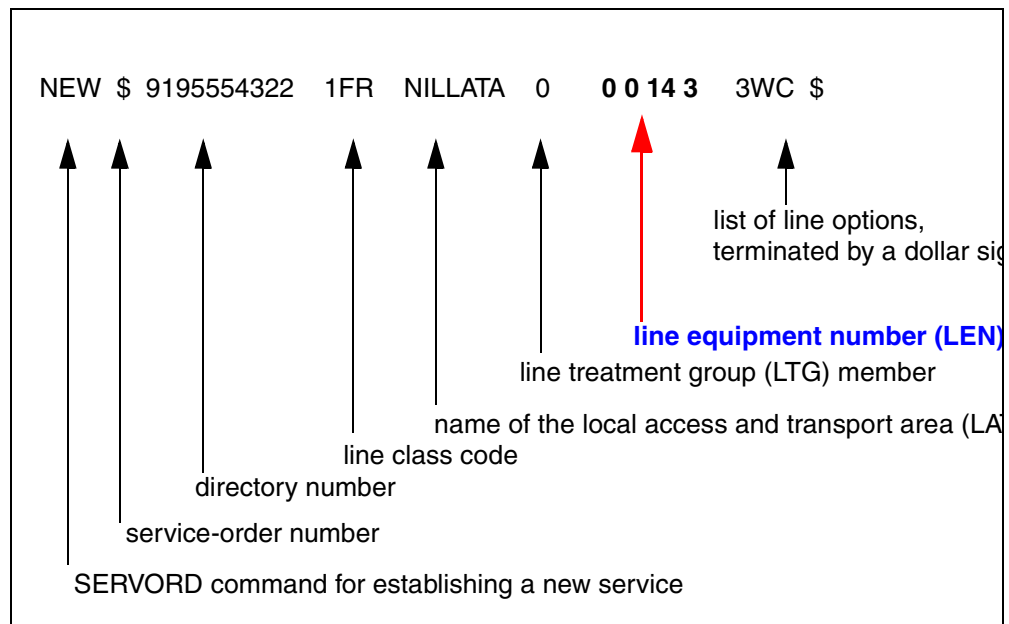
Example of system response:

Mode is CI.

>

- 4** Add the LEN information back into the XA-Core by entering the NEW command at the ">" prompt. NEW is the SERVORD command that you use to provision a line.

Example of the NEW command with the LEN instead of endpoint



- 5** You have completed this procedure, but you may wish to input other commands in OSSGate before disconnecting to OSSGate. If so, return to the procedure that directed you here originally. If you wish to disconnect from OSSGate now, follow the remaining steps in this procedure.

- 6 Disconnect from OSSGate. Proceed as follows.
 - a Hold down the control key and type B.
Example of system response:
?
 - b At the question-mark prompt, type **logout**
and press the Enter key.
Example of system response:
user1 logged out.

>
- 7 Terminate the telnet session. Proceed as follows.
 - a Hold down the control key and type B.
Example of system response:
?
 - b At the question-mark prompt, type **clearconv**
and press the Enter key.
Example of system response:
SESSION TERMINATED.

Connection closed by foreign host.
- 8 You have completed this procedure.

How to correlate line information from the MAPCI to the GWC and line gateway

Use this task to correlate line information from the maintenance and administration position command interpreter (MAPCI) to the Gateway Controller (GWC), and media gateway. This task shows how to correlate line information from the MAPCI, to GWC, and then to either the Succession Media Gateway 9000 (MG 9000), or Multimedia Terminal Adapter (MTA).

This task begins at the line test position (LTP) of the MAPCI where you post the line from which you want to derive endpoint information.

Correlating line information from MAPCI to GWC and MG 9000 or MTA

At the MAPCI

- 1 Use the following table to decide your next step:

If you want	Do
information on a line that terminates on an MTA	step 2
information on a line that terminates on an MG 9000	step 11

- 2 Access the line test position, by typing

```
> mapci;mtc;lms;ltp
```

and press the Enter key.
- 3 Post one, or more lines based on the line state. For example, post lines that are system busy (sb), by typing

```
> post s sb
```

and press the Enter key.

Example of a MAP screen

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
LTP									
0 Quit		POST	SB	DELQ		BUSYQ		PREFIX	
2		LEN	LG	00 0 00 44					
3 Post		LCC	PTY	RNG				STA F S LTA	TE RESULT
4		IBN				DN 613 621 6901	SB		
5 Bsy									
6 RTS									
7 Diag									
8									
9 AlmStat									
10 CktLoc		Post	s	sb					
11 Hold									
12 Next									
13									
14									
15 FullDn									
16 Prefix									
17 LCO									
18 Level									
Time	10: 58								

The LEN of a posted MTA line that is currently in a system busy state

- 4 If there is more than one line in the posted set, find the MTA line in the posted set, that is of interest to you. Record the LEN (see the previous figure).
- 5 At a PC connected to the local area network, initiate a Telnet session to OSSGate, by typing
telnet <ossgate_server_name> <port_number>
 and press the Enter key.

where

<ossgate_server_name>

is the hostname or the IP address of the server on which OSSGate is running

<port_number>

is the server port used by OSSGate (the default is 10023)

Example

telnet wcn0s5jk 10023

Example of a system response

Trying 47.142.94.80...

Connected to wcn0s5jk.

Escape character is '^]'.
 Enter username and password

- 6 Enter your user name and password, by typing
<username> <password>
and pressing the Enter key.

Example

user1 maint

Example of a system response

```
*****
**                                     **
**                                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.          **
**                                     **
*****
```

- 7 You have connected to OSSGate, and the system is displaying a prompt (the ">" character) in the Telnet window on your screen. Now you must put the telnet session into command interpreter (CI) mode. Proceed as follows:

- a** Hold down the control key and type B.

Example of a system response:

?

- b** At the question-mark prompt, enter the command interpreter mode, by typing

mode ci

and pressing the Enter key.

Example of a system response:

Mode is CI.

>

- 8 Perform a query of the LEN information that you recorded in [step 4](#), by typing

```
> qlen <len>
```

Where

<len>

is the line equipment number that you recorded from the LTP level of the MAP in [step 4](#).

Example

```
qlen LG 00 0 00 44
```

Example of a system response:

```
LEN:      LG      00 0 00 44
END POINT: CUST34671.rdu.attcable.net aaln/1
TYPE: SINGE PARTY LINE
SNPA: 613
DIRECTORY NUMBER:      6216901
LINE CLASS CODE:      IBN
IBN TGRP:      GNPS_IBN      SUBGRP: 0  NCOS: 0
CARDCODE: RDTLSG GND: N PADGRP: PKNIL BNV: NL MNO: N
PM NODE NUMBER      :      109
PMTERMINAL NUMBER   :      45
OPTIONS:
CWT 3WC DGT CND NOAMA CNAMD NOAMA
```

MTA port number

The domain name of the MTA including host name.

GWC node number and terminal number

- 9 From the system response to the query LEN command, you can obtain the MTA domain name (including host name), as well as the port number. In addition, the response to the command supplies the GWC node number (109 in the example), and the GWC terminal number (45 in the example).
- 10 Proceed to [step 19](#).
- 11 Access the line test position, by typing
- ```
> mapci;mtc;lns;ltp
```
- and press the Enter key.
- 12 Post one or more MG 9000 lines based on the line state. For example, post lines that are system busy (sb), by typing
- ```
> post s sb
```
- and press the Enter key.

Example of a MAP screen

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
LTP									
0 Quit		POST	SB	DELQ		BUSYQ		PREFIX	
2		LEN	MG9A	01 3 05 00					
3 Post		LCC	PTY	RNG				STA F S LTA	TE RESULT
4		IBN				DN 613 748 9898	SB		
5 Bsy									
6 RTS									
7 Diag									
8									
9 AlmStat									
10 CktLoc		Post s sb							
11 Hold									
12 Next									
13									
14									
15 FullDn									
16 Prefix									
17 LCO									
18 Level									
Time	10: 58								

The LEN of a posted MG 9000 line that is currently in a system busy state

- 13** If there is more than one line in the posted set, find the MG 9000 line in the posted set, that is of interest to you. Record the LEN (see the previous figure).

- 14** At a PC connected to the local area network, initiate a Telnet session to OSSGate, by typing

```
telnet <ossgate_server_name> <port_number>
```

and press the Enter key.

where

<ossgate_server_name>

is the hostname or the IP address of the server on which OSSGate is running

<port_number>

is the server port used by OSSGate (the default is 10023)

Example

```
telnet wcn0s5jk 10023
```

Example of a system response

Trying 47.142.94.80...

Connected to wcn0s5jk.

Escape character is '^['.

Enter username and password

- 15** Enter your user name and password, by typing

<username> <password>

and pressing the Enter key.

Example

user1 maint

Example of a system response

```
*****
**                                     **
**                                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.          **
**                                     **
*****
```

- 16** You have connected to OSSGate, and the system is displaying a prompt (the ">" character) in the Telnet window on your screen. Now you must put the telnet session into command interpreter (CI) mode. Proceed as follows:

- a** Hold down the control key and type B.

Example of a system response:

?

- b** At the question-mark prompt, enter the command interpreter mode, by typing

mode ci

and pressing the Enter key.

Example of a system response:

Mode is CI.

>

- 17** Perform a query of the LEN information that you recorded in [step 13](#), by typing

```
> qlen <len>
```

Where

<len>

is the MG 9000 line equipment number that you recorded from the LTP level of the MAPCI in [step 13](#).

Example

```
qlen LG 00 0 00 44
```

Example of a system response:

```
LEN:      LG      00 0 00 44
END POINT: CUST511-7-3  tp/21/31
TYPE: SINGE PARTY LINE
SNPA: 613
DIRECTORY NUMBER:      7489898
LINE CLASS CODE:      IBN
IBN TGRP:      GNPS_IBN      SUBGRP: 0  NCOS: 0
CARDCODE?: RDTLSG GND: N PADGRP: PKNIL BNV: NL MNO: N
PM NODE NUMBER      :      101
PMTERMINAL NUMBER   :      14
OPTIONS:
CWT 3WC DGT CND NOAMA CNAMD NOAMA
```

Card, and circuit number on the MG 9000

The site, frame, logical frame, and shelf of the MG 9000.

GWC node number and terminal number

- 18** From the system response of the query LEN command, you can obtain site, frame, logical frame, and shelf data for the MG 9000 that terminates the line (see the end point information in the previous figure). The end point field also contains the number of the card and the circuit. In addition, the PM Node Number, and PM terminal number fields in the system output, provide you with the GWC node number and terminal number.

- 19** Disconnect from OSSGate as follows:

- a** Hold down the control key and type B.

Example of a system response:

```
?
```

- b** Logout, by typing

```
logout
```

and press the Enter key.

Example of a system response:

```
user1 logged out.
```

```
>
```

- 20 Terminate the Telnet session as follows:
 - a Hold down the control key and type B.
Example of a system response:
?
 - b Clear the connection, by typing
clearconv
and press the Enter key.
Example of a system response:
SESSION TERMINATED.
Connection closed by foreign host.
- 21 You have completed this procedure.

How to correlate carrier information from the MAPCI, to the GWC, and Media Gateway 15000/7400

Use this task to correlate carrier information from the maintenance and administration position command interface (MAPCI) to the Gateway Controller (GWC) and the Media Gateway 15000/7400.

Correlating carrier information from MAPCI to GWC, and Media Gateway 15000/7400

Finding carrier provisioning information

- 1 To obtain carrier provisioning information for Media Gateway 15000/7400, see *Nortel Networks Media Gateway 7480/15000 Technology Fundamentals*, NN10600-780.
- 2 To obtain general carrier provisioning information for GWC, you can use the Trunk Maintenance Manager (TMM). For additional information on using TMM to view provisioning information, see *ATM/IP Fault Management*, NN10325-900.
- 3 To obtain carrier provisioning information at the CS 2000 MAPCI, access table TRKMEM by typing

```
> table trkmem
```

and press the Enter key.

- 4 Position on the tuple of interest by typing

```
pos <clli> <extrknum>
```

and press the Enter key.

where

<clli>

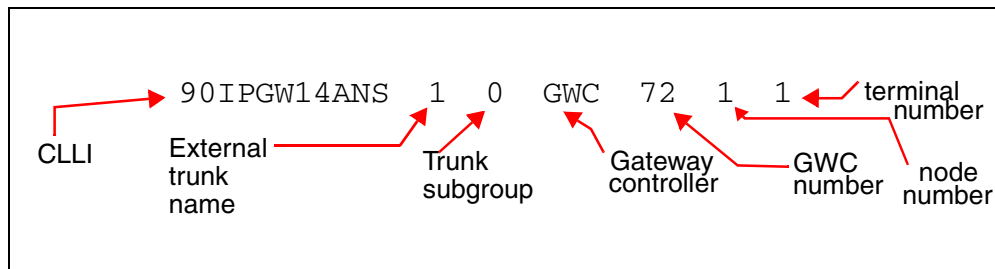
is the common language location identifier code of the trunk group to which the trunk is a member

<extrknum>

is the external trunk number (0-9999) that is assigned to the trunk

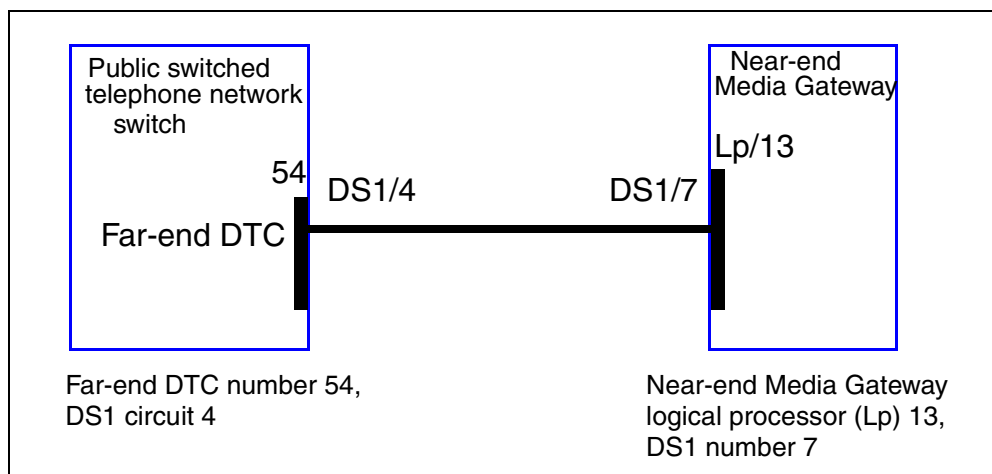
Example

```
pos 90IPW15ANS 1
```

Example of a system response

- 5 With the information from [step 4](#), use your customer database to determine the far-end peripheral module, and the near-end Media Gateway that terminate the carrier on which you are working.

Example of the carrier information available in the customer database



- 6 Access the carrier level of the MAPCI by typing
- ```
>mapci;mtc;trks;carrier
```
- and press the Enter key.
- 7 Post the carrier you are working on using the far-end information you obtained in [step 4](#) by typing
- ```
> post <pm> <pm_number> <carrier_circuit_num>
```
- where
- <pm>** is the peripheral module that terminates the far-end trunk
 - <pm_number>** is the peripheral module number that terminates the far-end trunk

<carrier_circuit_num>

is the circuit number of the carrier

Example

post pdtc 54 4

Example of a system response

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL			
POST												
0 Quit_		CLASS	ML	OS	ALRM	SYSB	MANB	UNEQ	OFFL	CBSY	FBSY	INSV
2 Post_		TRUNKS	0	0	0	0	0	0	0	0	0	1004
3		HSCARR	0	0	0	0	0	0	0	0	0	1004
4		DS1										
5 Loop_		N CLASS	SITE	PDTC	CK	D	ALRM	SLIP	FRME	BER	ES	SES STATE
6 Tst_		0 TRUNKS	HOST	54	4	C						INSV
7 Bsy_												
8 RTS_												
9 Offl_												
10 DispOpt_												
11 Disp_												
12 Next												
13												
14 Detail_												
15												
16												
17												
18												

Time 10: 58 >■

PDTC 54 Carrier 4

If the DS1 on the Passport PVG is up, then the state is INSV

- 8** To view GWC and Media Gateway endpoint information from the CS 2000 Management Tools Trunk Maintenance Manager (TMM) perform the following steps:

- From the CS 2000 Management Tools common launch page, launch the Trunk Maintenance Manager by clicking on the appropriate link (see the following figure).

Example of the CS 2000 Management Tools common launch page

NORTEL NETWORKS

Application Launch Point

Web based applications available on this server (47.142.130.70)

- . Trunk Maintenance Manager
- . CS2000 Management Tools
- . Line Maintenance Manager
- . Batch Configuration Monitor
- . CS2000 SAM21 Manager
- . Network Patch Manager

[Click on this link](#)

Example of a system response

- b** Select the **Mtc By Trunk CLLI** menu item in the Maintenance action field (see the previous figure).
- c** Enter the CLLI, a Trunk Range value (or use the default value of zero), and select **Post Trunks** from the Maintenance Action drop-down menu, then click on the **Go** button. (see the following figure).

Example of a TMM screen

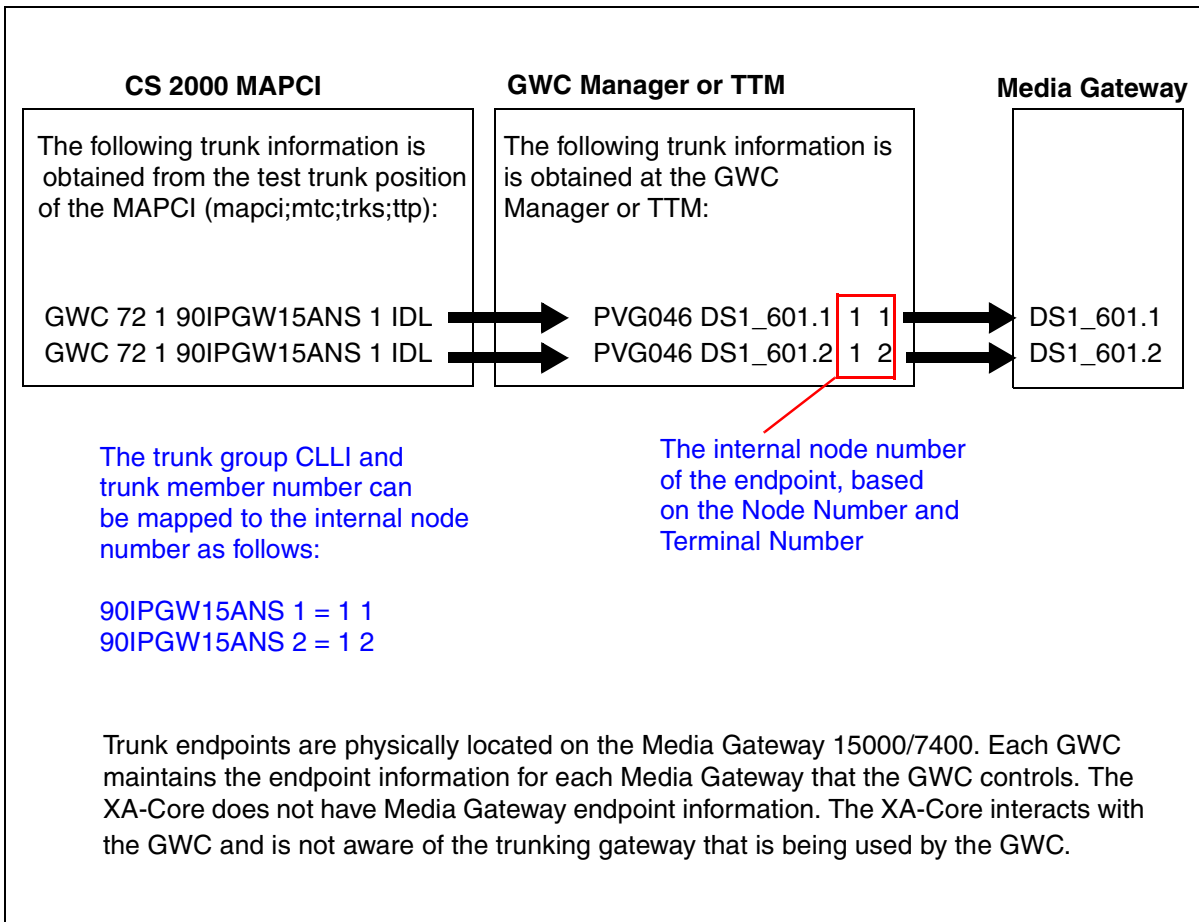
- d** The Trunk Maintenance Manager software displays the GWC, and endpoint information that is associated with the trunk group CLLI that you have specified (see the following figure).

Example of a TMM screen

Maintenance Action. Mtc by Gateway Name . Get TrkCLLIs by GW Name . Mtc by Trunk CLLI . D-Channel Maintenance . ICOT Test . Properties. CM CLLI . Auto-Refresh Rate . ☐ Auto-Refresh . Home .		Trunk Maintenance Manager Maintenance Actions Trunk CLLI: 90IPGW14ANS Trunk Range: 0- Maintenance Action: Post Trunks Go CM CLLI: NDPX TRUNK CLLI: 90IPGW14ANS First Member: 1 Group Size: 24	

Number	State	Direction	Signaling	PM Type	PM Number	Node #	Terminal #	Gateway Name	Endpoint Name
1	IDL	2W	S7 S7	GWC NODE	72	1	1	PVG046	DS1_601.1
2	IDL	2W	S7 S7	GWC NODE	72	1	2	PVG046	DS1_601.2
3	IDL	2W	S7 S7	GWC NODE	72	1	3	PVG046	DS1_601.3
4	IDL	2W	S7 S7	GWC NODE	72	1	4	PVG046	DS1_601.4
5	IDL	2W	S7 S7	GWC NODE	72	1	5	PVG046	DS1_601.5
6	IDL	2W	S7 S7	GWC NODE	72	1	6	PVG046	DS1_601.6
6	IDL	2W	S7 S7	GWC NODE	72	1	7	PVG046	DS1_601.7
8	IDL	2W	S7 S7	GWC NODE	72	1	8	PVG046	DS1_601.8

- 9 You likely now have enough information to map carrier information from the MAPCI to a specific trunk endpoint (see the following figure).



10 You have completed this procedure.

Checking for Media Gateway logs

Media Gateway 15000/7400 alarm logs can be viewed in switch control center 2 (SCC2) format at your operations support system (OSS). The Preside MDM software collects alarm and log data from the Media Gateway 15000/7400. This data is, in turn, forwarded to the CS 2000 Core Manager. The CS 2000 Core Manager Log Streamer application converts the Media Gateway logs into SCC2 format. The CS 2000 Core Manager, then transmits the logs to the OSS.

Alternatively, you can view Media Gateway alarms by using applications on the Preside MDM. For information on viewing Media Gateway alarms on the Preside MDM, see *Preside MDM Fault Management User Guide*, 241-6001-011.

Checking for CS 2000 or CS 2000-Compact logs

Use this procedure to check for CS 2000 logs of type XAC, MS, NET, IOD, EXT, and APPL. using LOGUTIL (at the MAP). You can also use this procedure to check for CS 2000-Compact call processing logs of type IOD, EXT, or APPL.

Note: The XAC, MS, and NET logs do not apply to the CS 2000-Compact.

To view CS 2000-Compact logs that are generated by the Call Agent hardware and software platform, use the Call Agent Manager, see

To view CS 2000-Compact logs that are generated by the STORage Management (STORM), see

Checking for CS 2000 or CS 2000-Compact logs

At the MAP terminal

- 1 Access the log utility (LOGUTIL), by typing

```
> logutil
```

and press the Enter key.
System response:
LOGUTIL
- 2 View the most recent CS 2000 (or CS 2000-Compact) logs of a specific type, by typing

```
> open <log_name>
```

and press the Enter key.
where

```
<log_name>
```

is name of a group of logs, for example: XAC, IOD, MS, NET, EXT, or APPL
Example

```
> open xac
```

The switch responds with the most recent XAC log.
- 3 View the entire log buffer of logs of a specific type, by typing

```
> dumplogs <log_name>
```

and press the Enter key.
where

<log_name>

is name of a group of logs, for example: XAC, IOD, MS, NET, EXT, or APPL

Example

> dumplogs xac

Note: The switch dumps the entire log buffer of XAC logs.

- 4 You have completed this procedure.

Passport 8600 Ethernet port configuration, and 100Base-T cable replacement

This document provides you with references to the Passport 8600 documents you need to consult for configuration of Ethernet ports, and 100Base-T cabling.

Configuring Ethernet ports on Passport 8600

For information on configuring a Passport 8600 Ethernet port, see *Configuring Network Management and Diagnostics*, 314723A, on this compact disk. Refer to the chapter on port configuration and graphing.

100Base-T cabling

For information on verifying and replacing 100Base-T cabling that connects the CS 2000 GWC to the Passport 8600, see *Installing and Maintaining the 8010co Chassis and Components*, 312746C, on this compact disk.

View carrier provisioning data for a GWC node

Purpose of this procedure

Use this procedure to view carrier (endpoint group) provisioning data for a selected Gateway Controller (GWC) node.

Note: Starting in SN07, this procedure supports viewing carriers provisioned on H.323 gateways.

When to use this procedure

Use this procedure when you require specific provisioning information about carriers associated with a specific GWC node.

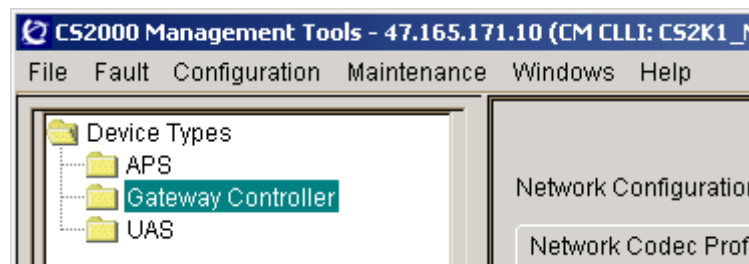
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

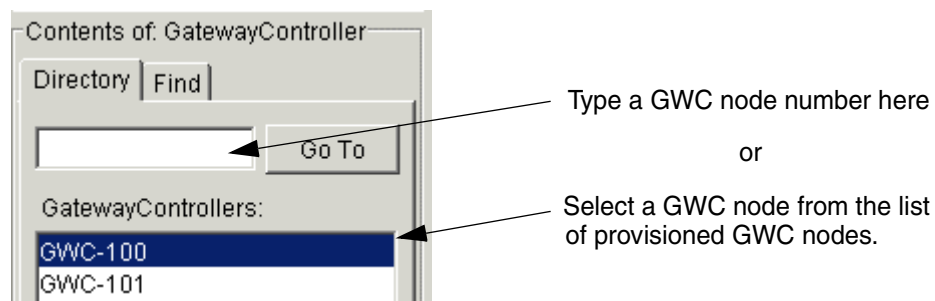
Action

At the CS 2000 GWC Manager client

- 1 At the CS2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



- 2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.



- 3 Click the **Provisioning** tab.
- 4 Click the **Controller** tab to view general provisioning information for the GWC node selected.

The screenshot shows the 'Provisioning' tab selected in the top navigation bar. Below it, the 'Controller' sub-tab is also selected. The interface is divided into several sections:

- IP Addresses:** Active: 47.142.128.60, Inactive: 47.142.128.61, Unit 0: 47.142.128.62, Unit 1: 47.142.128.63.
- Element Manager:** IP address: 47.142.128.94, SNMP port: 161, Trap port: 162.
- Profile:** Current: SMALL_LINENA, with a 'Change...' button.
- Call Agent:** Node number: 44.
- Capacity Table:**

Capability	Capacity	Units
Lines	6400	ports
Dynamic Quality of...	20	connections
Small Gateways	6400	gateways
IP Security		
Kerberos		
- Exec Lineup Table:**

Exec Lineup	Term Type
POTSEX	POTS
KSETEX	KEYSET
- Bearer Network and Codec Profile:** Bearer network: NET_IP, Bearer fabric type: IP, Codec Profile: com5, with a 'Change...' button.
- General:** ☐ Enable Location Identification reporting.
- GWC Statistics Data:** with a 'Statistics' button.

- 5 Click the **Carriers** tab to view information related to carriers (endpoint groups) belonging to gateways associated with the GWC node selected previously.

Select the edge of any tab to adjust the display.

Note: For H.323 carriers, the existing auto-generated carrier names from release SN06.2 also appear in release SN08. Any new H.323 carriers assigned in SN08 are added manually based on the naming convention for H.323 carriers.

1 Retrieval criteria:

2 Limit results: 25

3 ☒ Replace List ☐ Append to List

4 Retrieve

Retrieve All

Carrier List

5

Name	Gateway	Node Num...	Start Term	Num Ports	V5.2 I/F ID	V5.2 Link ID	V5 UA Link...	PRI I/F ID
EPG_001	BCMY2	120	25	4				0
AUTOGEN_EPG_001	BCM_RTPG	120	1	24				1
EPG_001	M1_Y1	120	29	672				0

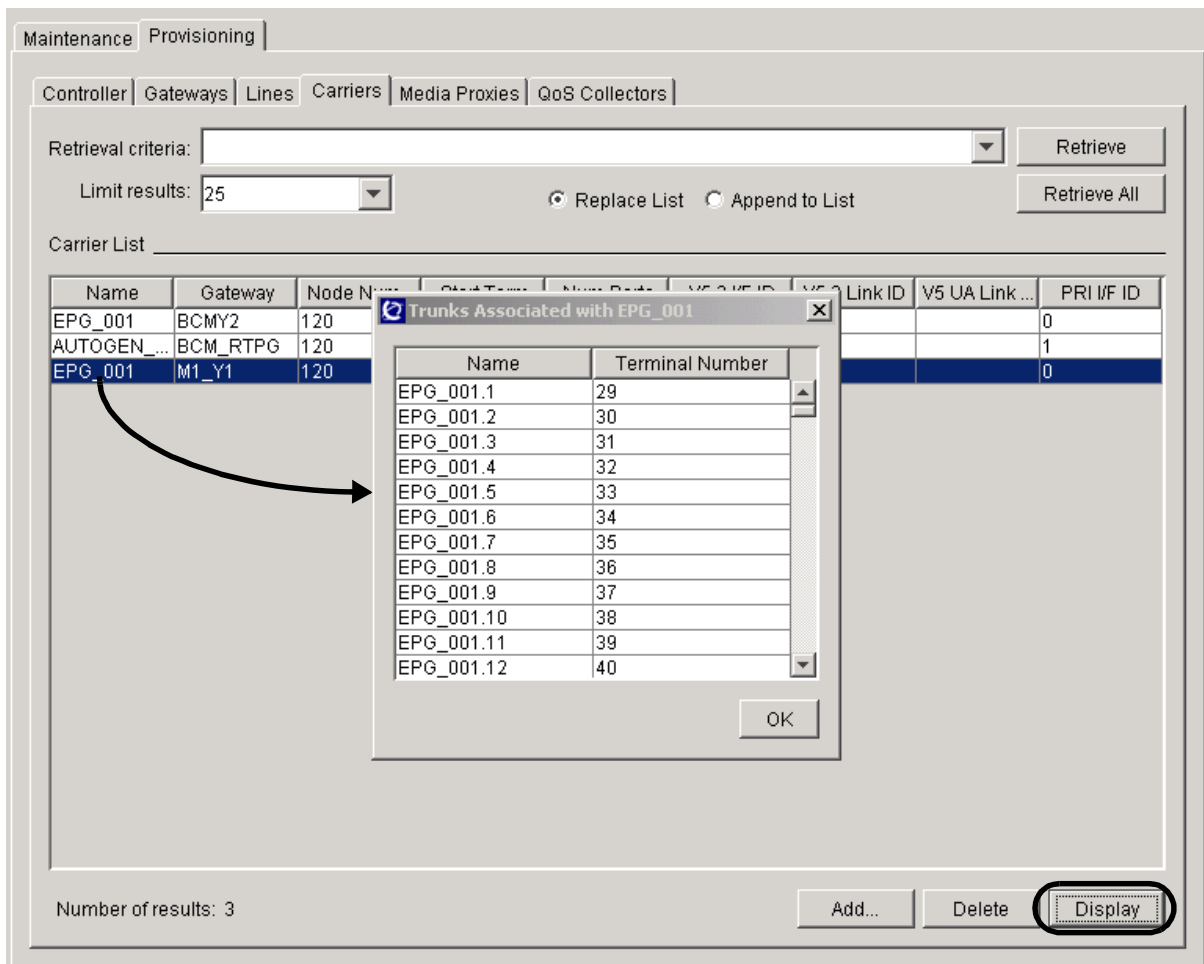
Number of results: 3

Add... Delete **6** Display

- 6 Click the **Retrieve All** button to view carrier endpoint data.

Note: The table [Description of carrier endpoint search criteria functions on page 617](#) contains information about the search functions (see the numbers in the figure above).

- 7 If you wish to view the trunk endpoints and terminal numbers associated with a specific carrier, click the carrier entry and click the **Display** button.



- 8 Repeat this procedure as required for carrier endpoints you wish to view on this or other GWC nodes.
- 9 The procedure is complete.

The following table describes the carrier endpoint search criteria functions.

Description of carrier endpoint search criteria functions (Sheet 1 of 3)

Step	Menu component	Description
①	Retrieval criteria: selection box and drop-down list	Enter a search criteria string in this field. Up to 20 search strings are saved during the session. Previous search strings can be recalled by selecting from the drop-down list. Refer to the table Examples of carrier search criteria on page 619 at the end of this procedure for more details about using search strings.
②	Limit results: selection box and drop-down list	Select a value from the drop-down list. This value limits the number of matching entries returned in response to the query. Valid values are as follows: 25, 50, 100, 250, 500, 1000, and "no limit". Note: The "no limit" value is still itself limited by the maximum number of entries currently downloadable, which is 4094.
③	Replace List radio button	Deselect this option if you do not want the query results to replace previously existing data displayed in the table. The default selection is to replace the existing data.
	Append to List radio button	Select this option if you want the query results to be appended to the existing data displayed in the table.

Description of carrier endpoint search criteria functions (Sheet 2 of 3)

Step	Menu component	Description
④	Retrieve button	This selection retrieves data from the CS 2000 GWC Manager server database matching the specified search retrieval criteria. The data presented is a “snapshot” of the CS 2000 GWC Manager database based on the currently provisioned data. The view is not updated in real time. Note: Newly added or deleted data will not be added to or deleted from the displayed table view except when there is a deletion of endpoints. If an carrier endpoint is selected from the table and deleted using the Delete button, then the endpoint will be removed from the table if deletion was successful. Endpoint deletion using this interface is limited to carrier endpoints only. Line endpoints are added automatically when you provision lines to a GWC. For instructions on how to add or delete lines, refer to the <i>CS 2000 Configuration Management</i> NTP applicable to your solution.
	Retrieve All button	This selection retrieves all the gateway or endpoint data, up to the maximum of 4094 entries. Values in the “Retrieval criteria” and “Limit results” are ignored.
⑤	Carrier List table	This is the tables where the search results are displayed. By clicking on a column header, you can sort the rows in ascending order, based on the values in that column. By clicking on the column header a second time, you can sort the rows in descending order. Note: The data is not preserved once another GWC node is selected; however, the retrieval criteria are maintained in the drop-down list so the same search can be reexecuted.

Description of carrier endpoint search criteria functions (Sheet 3 of 3)

Step	Menu component	Description
⑥	Display	Highlight a carrier name and click this button if you wish to view the endpoints trunk and terminal numbers associated with a specific carrier.
Note 1: Use the Add button to add carriers (endpoint groups). For more information, refer to procedure "Add carriers to a GWC" in <i>Gateway Controller Configuration Management</i>, NN10205-511. Note 2: Use the Delete button to delete carriers. For more information, refer to procedure "Delete carriers from a GWC" in <i>Gateway Controller Configuration Management</i>, NN10205-511. Note 3: Line endpoints are added automatically when you provision lines on a GWC. For instructions on how to add or delete lines, refer to procedures in the <i>CS 2000 Configuration Management NTP</i> for your solution.		

Examples of carrier search criteria (Sheet 1 of 2)

Examples of carrier search criteria	
The gateway and endpoint panels use the same search functionality. The functionality is similar to that available in web search engines. - One or more strings can be entered in the Retrieval Criteria: box, separated by space(s). - Each string in the criteria is compared with the value in each column. If a match is found in any column, the record will be returned. - Each string in the criteria is automatically wildcard at the beginning and end of the string. (For example, the string "gate" will match "MYGATEWAY" and "GATEWAY1".) - Two special characters are supported as modifiers: the plus "+" and minus "-" signs. The "+" plus character prefixed to the string (for example, "+gate") means the value must match. The "-" character prefixed to the string (for example, "-gate") means the value must not match. The "+" character is assumed, and therefore is not typically used. - The search is not case sensitive. A string using "gate" will return records where the following strings are found: "MYGATEWAY", "MyGateway", or "mygateway". <i>Example Retrieval Criteria: "DS3"</i> Expected Results: Returns all records where the string is found in any column. A match for the example string will only be found in the Gateway name column.	

Examples of carrier search criteria (Sheet 2 of 2)*Example Retrieval Criteria: "aspen"*

Expected Results: Returns all records where the string is found, in any column. A match for the example string could be found in the Protocol column.

Retrieval Criteria: "47.108.2 -aspen"

Expected Results: Returns all records where the string "47.108.2" is found in any column and the string "aspen" is not found. The search will return the records of gateways where the subnet equals "47.108.2" and the protocol is not Aspen.

View media proxy configuration data for a GWC node

Purpose of this procedure

Use this procedure to view media proxy configuration data for a selected GWC node.

When to use this procedure

Use this procedure when you require specific configuration information about media proxies associated with a specific GWC node.

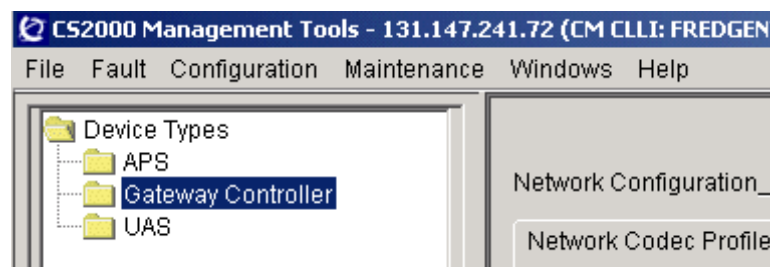
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

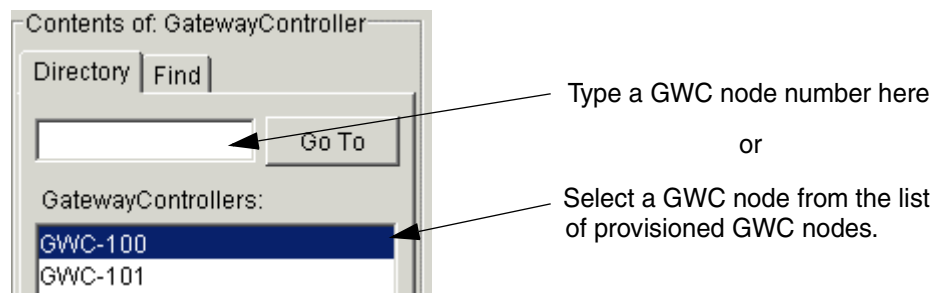
Action

At the CS 2000 GWC Manager client

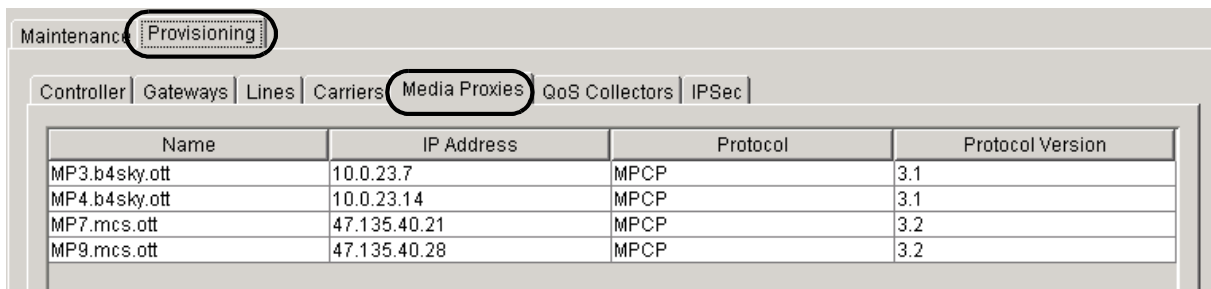
- 1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



- 2 From the Contents of: Gateway Controller frame, select the GWC node that has a media proxy you wish to view.



- 3 Click the **Provisioning** tab in the GWC node view.
If necessary, click the **Controller** tab to view general node provisioning information for the GWC node.
- 4 Click the **Media Proxies** tab in the Provisioning panel to view information about media proxies associated with the selected GWC node.



Name	IP Address	Protocol	Protocol Version
MP3.b4sky.ott	10.0.23.7	MPCP	3.1
MP4.b4sky.ott	10.0.23.14	MPCP	3.1
MP7.mcs.ott	47.135.40.21	MPCP	3.2
MP9.mcs.ott	47.135.40.28	MPCP	3.2

- 5 The procedure is complete.

Take a manual GWC software image

Purpose of this procedure

This procedure describes how to save a software image to the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM).

Note: A procedure also exists to enable the auto-imaging of a GWC software load once daily. Refer to “Enable or disable GWC software auto-imaging” in *Gateway Controller Configuration Management*, NN10205-511.

When to use this procedure

Use this procedure as a part of upgrading GWC software for an office or as a part of maintenance activity.

Take an image after all patches have been applied to GWC software. Refer to your site operating procedures for information about soak time and how many patches to apply before taking an image. In the absence of this information, Nortel Networks recommends taking an image immediately after applying R or P status patches.



CAUTION

Do not invoke the Save Image function during patching activities. Doing so can cause an invalid or incomplete image to be taken.

Prerequisites

This procedure has no prerequisites.

Action

At the CS 2000 Core Manager or CBM console

- 1 Log in to the CS 2000 Core Manager or CBM as the root user.
- 2 Change directory to the GWC software directory.

Example
cd /swd/gwc

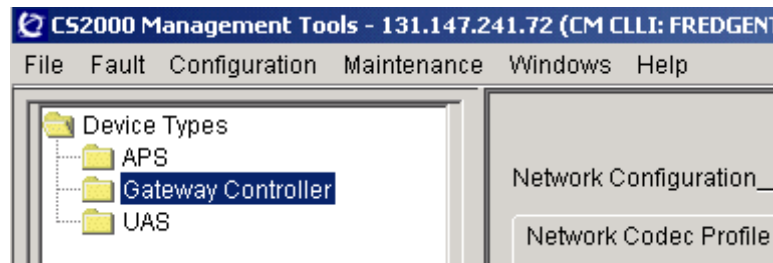
- 3 Copy the existing GWC software load file to a backup.

Example
cp pgc06as.imag pgc06as.imag.bak

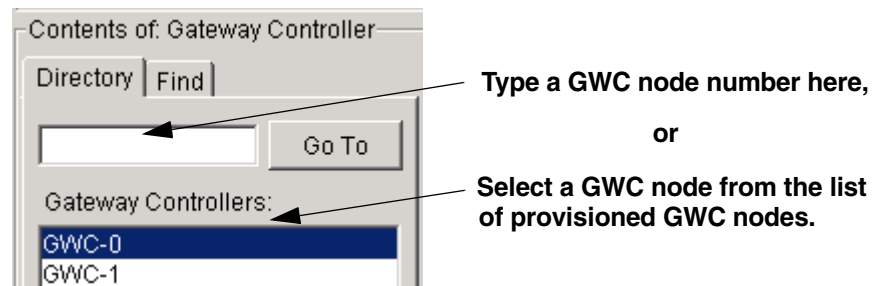
Note: You can use any name for the backup file name.

At the CS 2000 GWC Manager client

- 4 At the CS 2000 Management Tools window, click on the Gateway Controller folder from the Device Types directory tree in the far left frame.



- 5 From the Contents of: Gateway Controller frame, select the appropriate GWC node from which you wish to take an image.



- 6 Select the **Maintenance** tab to view the Maintenance panel.

- 7 In the Maintenance panel, identify the GWC card in the node that has an upgraded load already installed.
 - a Click the **Save Image** button for that card to save the software image back to the CS 2000 Core Manager or CBM.

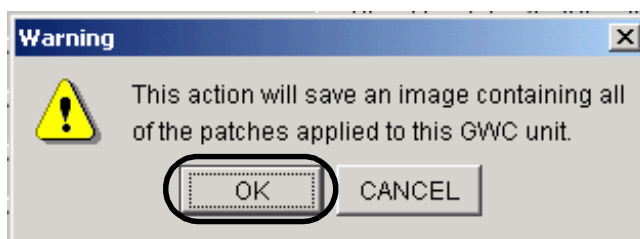
GWC-3-UNIT-1

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	hotStandby(1)
Activity state:	standby(2)	Swact state:	manualSwActWarm(1)
Isolation state:	notIsolated(2)	Alarm state:	00 00 00 00
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	GIBOPVG		

Save Image Busy (Disable) RTS (Enable) Card View

☐ Force Warm Swact Cold Swact

- b At the following warning message, click **OK** to continue with saving the GWC card's software image on the CS 2000 Core Manager. To stop the operation, click **Cancel**.



Note: The Save Image command overwrites the existing GWC software load file on the CS 2000 Core Manager or CBM. If the load file name is a link on the file system, the link is replaced with a file of the same name. Nortel Networks does not support using links to load files.



CAUTION

Do not invoke the Save Image function during patching activities. Doing so can cause an invalid or or corrupt image to be saved.

- 8 This procedure is complete.

Note 1: To return to the Overall GWC upgrade procedure, refer to “Overall upgrade process - manual” in *Upgrading the Gateway Controller*, NN10196-461.

Note 2: To return to the Overall GWC downgrade procedure, refer to “Roll back a software upgrade on a GWC node” in *Upgrading the Gateway Controller*, NN10196-461.

Troubleshooting

The /swd/gwc directory needs to have privileges set to read, write, execute for world access.

At the CS 2000 Core Manager or CBM console

- 1 Log in to the CS 2000 Core Manager or CBM as the root user.
- 2 Change directory to the /swd directory by typing
cd /swd
and pressing the Enter key.
- 3 Change the permissions for the gwc directory and its file contents by typing
chmod 777 gwc/*
and pressing the Enter key.
- 4 This procedure is complete.

Posting a trunk member

Application

Use this procedure to post trunk members by CLLI code.

Note: The Trunk Maintenance Manager (TMM) only supports ISUP and PRI trunks in Succession. Other trunk types can work, but they are not explicitly supported. Maintenance on those trunks, such as UAS and SIP-T trunks, needs to be performed using the CS 2000 XA-Core MAPCI interface.

Prerequisites

You need the CLLI code for the trunk you want to post. Refer to procedure [Displaying trunk CLLI codes by gateway](#) in this document, if required.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications](#), if required.

At the TMM GUI

- 2 Click **Mtc By Trunk CLLI**.
- 3 Enter the trunk CLLI name and optionally a Trunk Range value (or use the default [0-] value for all trunk members), then select **Post Trunks** from the **Maintenance Action** drop down menu, and click **Go**.

The trunk members are displayed as shown in the following example.

CM CLLI:	Trunk CLLI:	First Member:	Group Size:
RTPS	P3D0IBNT2	1	24

Number	State	Connected To	Direction	Signaling	PM Type	PM Number	Node #	Terminal #	Gateway Name	Endpoint Name
1	IDL		2W	S7 S7	GWC_NODE	1	13	1057	PVG193	STS/6/0/3/VT15/2/1/3/1
2	IDL		2W	S7 S7	GWC_NODE	1	13	1058	PVG193	STS/6/0/3/VT15/2/1/3/2
3	IDL		2W	S7 S7	GWC_NODE	1	13	1059	PVG193	STS/6/0/3/VT15/2/1/3/3
4	IDL		2W	S7 S7	GWC_NODE	1	13	1060	PVG193	STS/6/0/3/VT15/2/1/3/4
5	IDL		2W	S7 S7	GWC_NODE	1	13	1061	PVG193	STS/6/0/3/VT15/2/1/3/5
6	IDL		2W	S7 S7	GWC_NODE	1	13	1062	PVG193	STS/6/0/3/VT15/2/1/3/6
7	IDL		2W	S7 S7	GWC_NODE	1	13	1063	PVG193	STS/6/0/3/VT15/2/1/3/7
8	IDL		2W	S7 S7	GWC_NODE	1	13	1064	PVG193	STS/6/0/3/VT15/2/1/3/8
9	IDL		2W	S7 S7	GWC_NODE	1	13	1065	PVG193	STS/6/0/3/VT15/2/1/3/9

4 You have completed this procedure.

Returning a trunk member to service

Application

Use this procedure to return one or more trunk members to service (RTS) by CLLI code.

Note: The Trunk Maintenance Manager (TMM) only supports ISUP and PRI trunks in Succession. Other trunk types can work, but they are not explicitly supported. Maintenance on those trunks, such as UAS and SIP-T trunks, needs to be performed using the CS 2000 XA-Core MAPCI interface.

Prerequisites

You must first post the trunk you want to return to service. Refer to procedure [Posting a trunk member](#) in this document, if required.

The trunk members must be in a maintenance busied (MB) state or in other proper states such as CPD.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications](#), if required.

At the TMM GUI

- 2 Click **Mtc By Trunk CLLI**.
- 3 Enter the trunk CLLI name and optionally a Trunk Range value (or use the default [0-] value for all trunk members), then select **Return Trunks to Service (RTS)** from the **Maintenance Action** drop down menu, and click **Go**.

Trunk Maintenance Manager

Maintenance Action

[Mtc By Gateway Name](#)

[Get TrkCLIs by GW Name](#)

Mtc By Trunk CLLI

[D-Channel Maintenance](#)

[ICOT Test](#)

Properties

[CM CLli](#)

[Auto-Refresh Rate](#)

☐ Auto-Refresh

☒ Need Confirmation

[Home](#)

Maintenance Actions

Trunk CLLI: Trunk Range:

Maintenance Action:

Return Trunks to Service (RTS)

Post Trunks

Busy Trunks (BSY)

Return Trunks to Service (RTS)

Force Release Trunks (FRLS)

Installation Busy Trunks (BSY INB)

- 4 Observe that the selected trunk members are in the idle (IDL) state as shown in the following example.

CM CLLI:

RTPS

Trunk CLLI:

AL7ITICS7

First Member:

0

Group Size:

4

Number	State	Connected To	Direction	Signaling	PM Type	PM Number	Node #	Terminal #	Gateway Name	Endpoint Name
0	IDL		IC	S7	GWC_NODE	1	13	627	PVG190	DS3/02/0/27/3
1	IDL		IC	S7	GWC_NODE	1	13	628	PVG190	DS3/02/0/27/4
2	IDL		IC	S7	GWC_NODE	1	13	629	PVG190	DS3/02/0/27/5
3	IDL		IC	S7	GWC_NODE	1	13	630	PVG190	DS3/02/0/27/6

Last Refreshed: Wed Sep 24 13:42:27 EDT 2003

- 5 You have completed this procedure.

Reconfigure NTP service

Use this procedure to change the network time protocol (NTP) source for all the cards in the SAM21 shelf to a new NTP server. Reconfiguring the NTP server does not affect timing for call processing or signaling, the intent is to synchronize the timestamps on log reports.



CAUTION

Possible service interruption

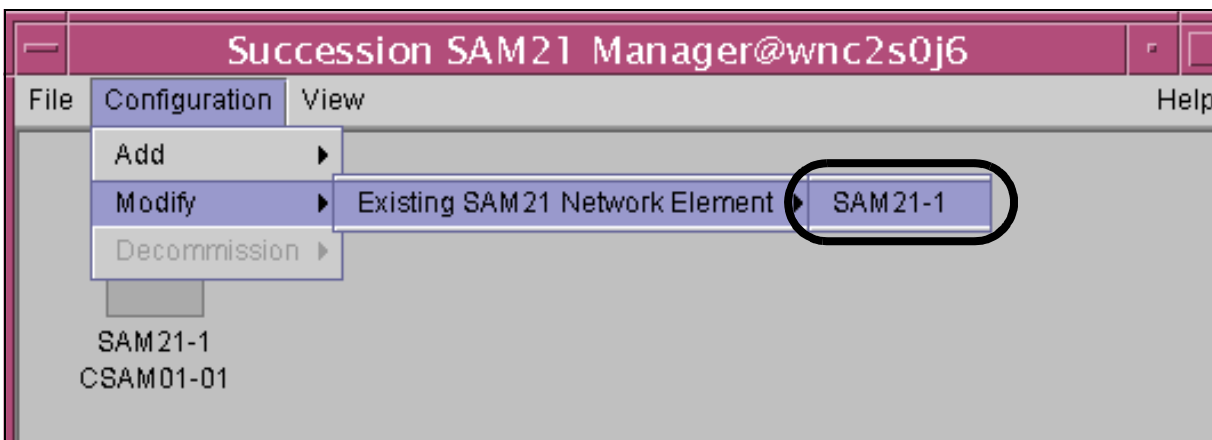
Reconfiguring the NTP service requires locking and unlocking the cards in the shelf. Locking and unlocking the Shelf Controllers does not affect service, but locking and unlocking non-system slot (NSS) cards can disrupt service.

Gateway Controllers (GWC) do not require locking and unlocking to update the NTP server information. GWCs require a Warm Swact. Refer to “Invoking a manual protection switch (warm swact)” in *Gateway Controller Security and Administration*, NN10213-611.

For information about updating the NTP service on the Call Agents, refer to “Reconfigure NTP service” in *Call Agent Configuration Management*, NN10111-511.

At the CS 2000 SAM21 Manager client

- 1 Select the shelf to modify from the Subnet View.



- 2 Replace the value in the Primary and Secondary NTP fields with the new NTP server addresses.

Reprovision SAM21-1

General

Name: Number:

CSAM number: Shelf Position:

Primary NTP: Secondary NTP:

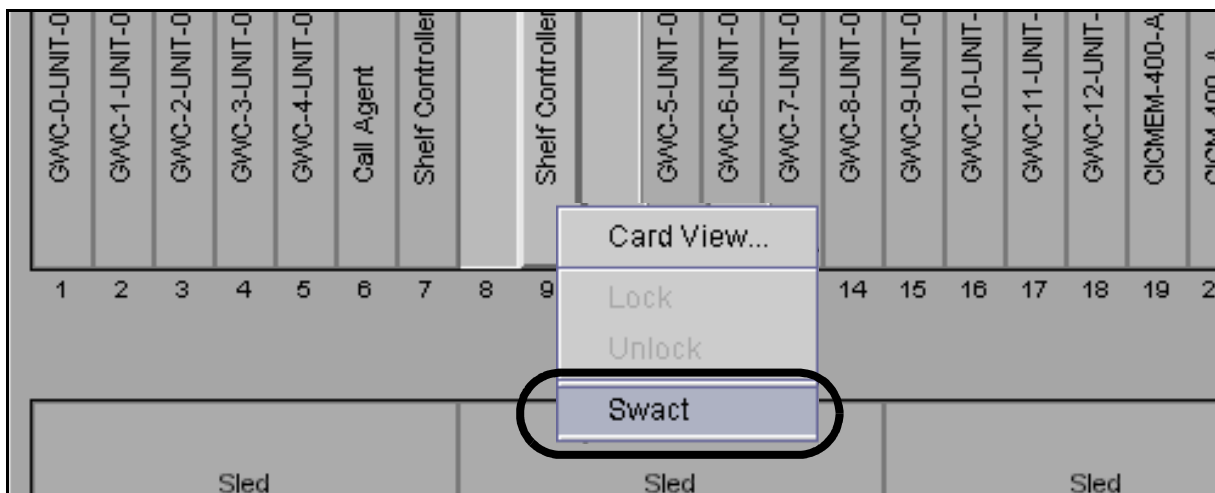
Timezone Offset: SNMP Community:

- 3 Lock and unlock the inactive Shelf Controller.

Note 1: Two critical alarms are raised after the lock and clear after the unlock.

Note 2: If the Shelf Controllers are provisioned with ATM interfaces, verify that the inactive Shelf Controller does not carry the active ATM link. If necessary, switch link activity at the far end node.

- 4 Switch activity by selecting Swact from the card context menu. If the Shelf Controllers are provisioned with ATM interfaces, perform the Swact during a low traffic period.



- 5 Lock and unlock the newly inactive Shelf Controller.

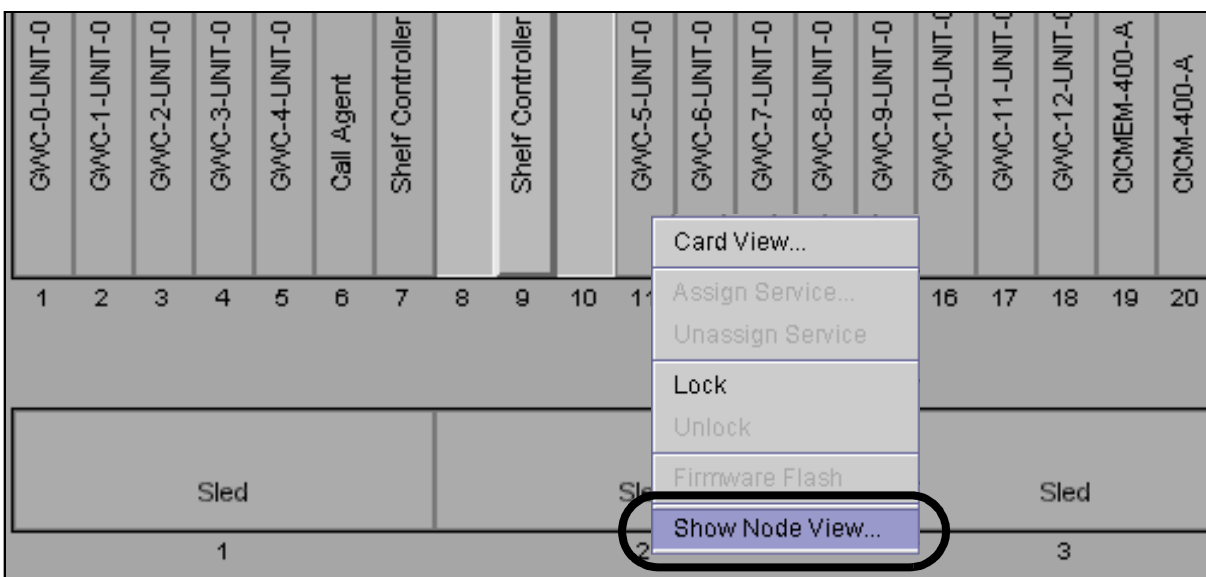
- 6 Lock and unlock each of the cards in the SAM21 shelf. For GWCs, open the GWC Manager. Refer to [Additional information](#).
Before locking any card, refer to the documentation for the card type and determine any precautions to take before locking the card.
- 7 This procedure is complete.

Additional information

Some network components require different maintenance activities to update the NTP server information.

Gateway Controller

To update the NTP server information in a GWC, warm swact one unit of the GWC node and then warm swact again to update the second unit in the node. Open the GWC Manager by selecting Show Node View from the Shelf View.



Once the GWC Manager opens, use the WarmSwact button on the maintenance tab to update the NTP information. Warm Swact the GWC

node twice so that both GWC units are updated. Perform these Warm Swacts for all GWC nodes in the SAM21 shelf.

UNIT-1

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	hotStandby(1)
Activity state:	standby(2)	Swact state:	noSwAct(0)
Isolation state:	notIsolated(2)	Alarm state:	00 00 00 00
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	PGC09AN		

Save Image Busy (Disable) RTS (Enable) Card View

☐ Force **Warm Swact** Cold Swact

After any unlock, RTS, or Swact to a Gateway Controller (GWC), the GWC makes its first NTP requests to the primary NTP server. If the service is unavailable, the GWC makes a final NTP service request to the CS 2000 Management Tools server. For the SN06 release, the secondary NTP server is ignored.

STORage Management

For offices with a CS 2000 - Compact, this procedure does not change the NTP source for STORage Management (STORM) units that are on the SAM-XTS hardware platform (STORM-IA).

Using the table editor to delete a tuple from a table

To delete certain provisioned entities in the XA-Core component of the CS 2000, you must use the table editor to delete tuples from tables. This procedure tells how to delete a tuple from a table.

Note 1: For detailed information on table-editor commands, see *DMS-100 Family Basic Translations Tools Guide*, 297-1001-360.

Note 2: For detailed information on the tables that contain the provisioning values, see:

- in the North American market, see *North American DMS-100 Customer Data Schema Reference Manual*, 297-8001-351
- in the international market, see *DMS-100 MMP Customer Data Schema Reference Manual*, 297-9051-351

This procedure assumes that you need to delete a tuple from a table in order to delete the provisioned entity that the tuple specifies.

Some tables are write-protected because deleting tuples can (or will) have a drastic effect on service. Exercise caution when deleting tuples.

Interval

Perform this procedure as required.

Prerequisites

None.

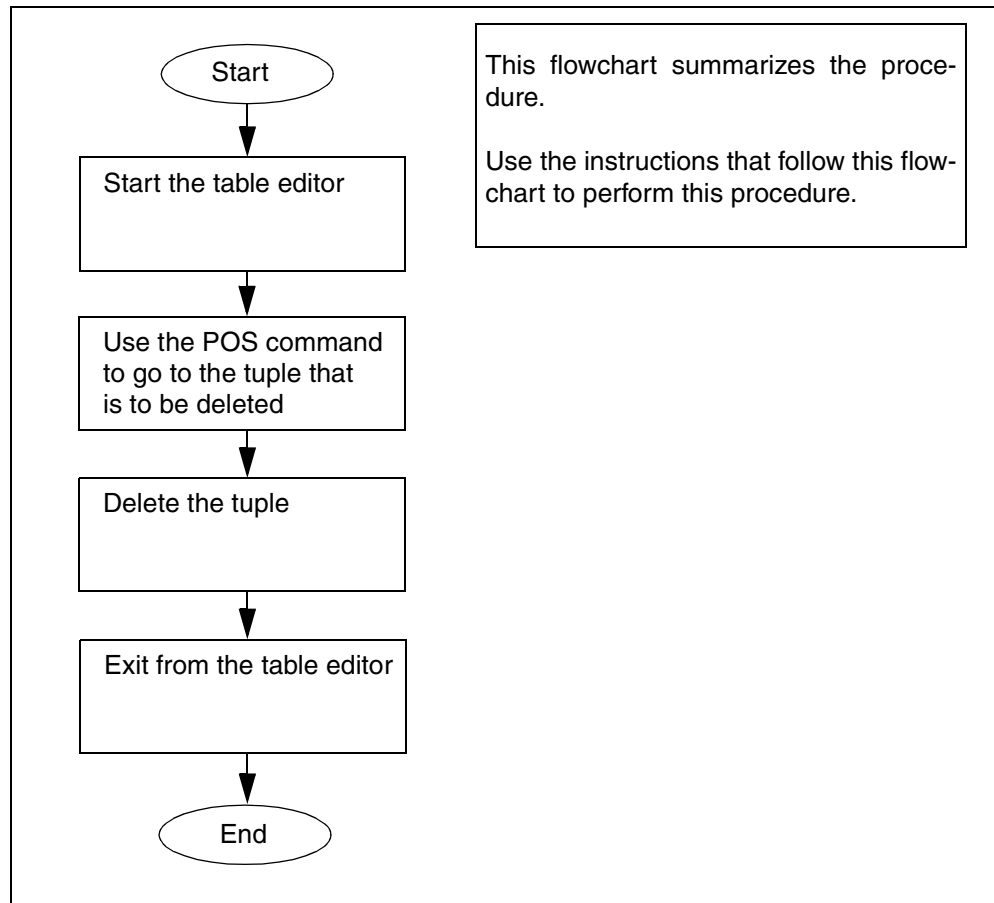
Common procedures

This procedure does not refer to any common procedures.

Action

The following flowchart summarizes this procedure.

Using the table editor to delete a tuple from a table



Using the table editor to delete a tuple from a table

At the MAP terminal

- 1 Start the table editor. At the user interface prompt on any MAP screen type.

>TABLE <table-name>

and press the Enter key

where

<table-name> is the name of the table from which you want to delete a tuple

Example of system response, assuming you use table-name CLLI:

TABLE: CLLI

- 2 Use the POS command to move to the tuple that you want to delete. Type
>POS <key-value>
and press the Enter key
where
<key-value> is the key value identifying the tuple
For example, if you wanted to delete the INCOMING_TRUNK tuple from table CLLI, you would enter
>POS INCOMING_TRUNK
Example of system response, continuing the example:
INCOMING_TRUNK 250 10 INCOMING_IT
where
250, 10, and INCOMING_IT are the values of the fields that compose a tuple in the CLLI table: ADNUM, TRKGRSIZ, and ADMININF.
- 3 Delete the tuple. Type
>DEL
and press the Enter key.
Example of system response:
TUPLE TO BE DELETED:
INCOMING_TRUNK 250 10 INCOMING_IT
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
- 4 Confirm the deletion. Type
>Y
and press the Enter key.
Example of system response:
TUPLE DELETED:
WRITTEN TO JOURNAL FILE AS JF NUMBER 567
- 5 Exit from the table editor. Type
>QUIT
and press the Enter key.
- 6 You have completed the procedure.

Deleting a line

Here is a high-level view of the sequence of activities for deleting a line on the CS 2000:

- You delete the line using one of the following methods:
 - You establish a telnet connection to OSSGate and enter a SERVORD command.
 - You use an operations support system (OSS), which must be purchased separately. The OSS has its own user interface. The OSS acts as the intermediary between you and OSSGate.

Note: An OSS must be purchased separately.

This procedure explains how to delete a line by telnetting to OSSGate and entering SERVORD commands one by one. If you have an OSS, see the documentation provided with the OSS for information on provisioning lines.

Interval

Perform this procedure as required.

Prerequisites

Prerequisites for line deletion are as follows:

- You must have the telnet application.
- You must know either the host name or the IP address of the server on which OSSGate is running. If in doubt, ask the local network administrator.
- You must know the number of the port used by OSSGate. If in doubt, ask the local network administrator.
- You must know the names of the media gateways that will be used, and you must know the endpoint names that the gateway controller element manager has allocated to those gateways.
- You must know how to format the values that you will enter in the media gateway endpoint name field in the OUT command (the SERVORD command that removes service from a line). You can find information on the formatting rules in the following list.

Here are the formatting rules for the values that you enter in the media gateway endpoint name field in a SERVORD command.

Names for media gateway endpoints on cable MTA gateways

The format for media gateway endpoint names is as follows:

<media-gateway-name> <endpoint-name>

where

- <media-gateway-name> is in the form of a fully qualified domain name including the hostname of the device and suitable for lookup using Directory Name Service (DNS). The name must contain a period (.).

Example

cust34671.rdu.attcable.net

- <endpoint-name> has the following format: **aa1n/<n>** where n is an integer in the range 1 to n, where n is the number of the voice port on the MTA.

Note: In the format, there is a space between <media-gateway-name> and <endpoint-name>.

Names for media gateway endpoints on MG 9000 H.248 gateways

The format for media gateway endpoint names is as follows:

<media-gateway-name> <endpoint-name>

where

- <media-gateway-name> has the following format:

<site><frame>-<logical-frame>-<shelf>

where

- <site> is the value previously datafilled in table SITE. The value is one to four alphanumeric characters.
- <frame> is a three-digit integer in the range 000 to 511, indicating the frame number within the office.
- <logical-frame> is an integer in the range 0 to 7, indicating the logical frame number within the physical MG.
- <shelf> is an integer in the range 0 to 3 indicating the shelf number within the frame.

- <endpoint-name> has the following format: **tp/<card>/<circuit>**

where

- <card> is a two-digit integer in the range 02 to 09 or in the range 14 to 21, indicating the card number.
- <circuit> is a two-digit integer in the range 00 to 31, indicating the circuit number.

Note: In the format, there is a space between <media-gateway-name> and <endpoint-name>.

For example, the following name conforms to the naming format for media gateway endpoints on an MG 9000 H.248 gateway:

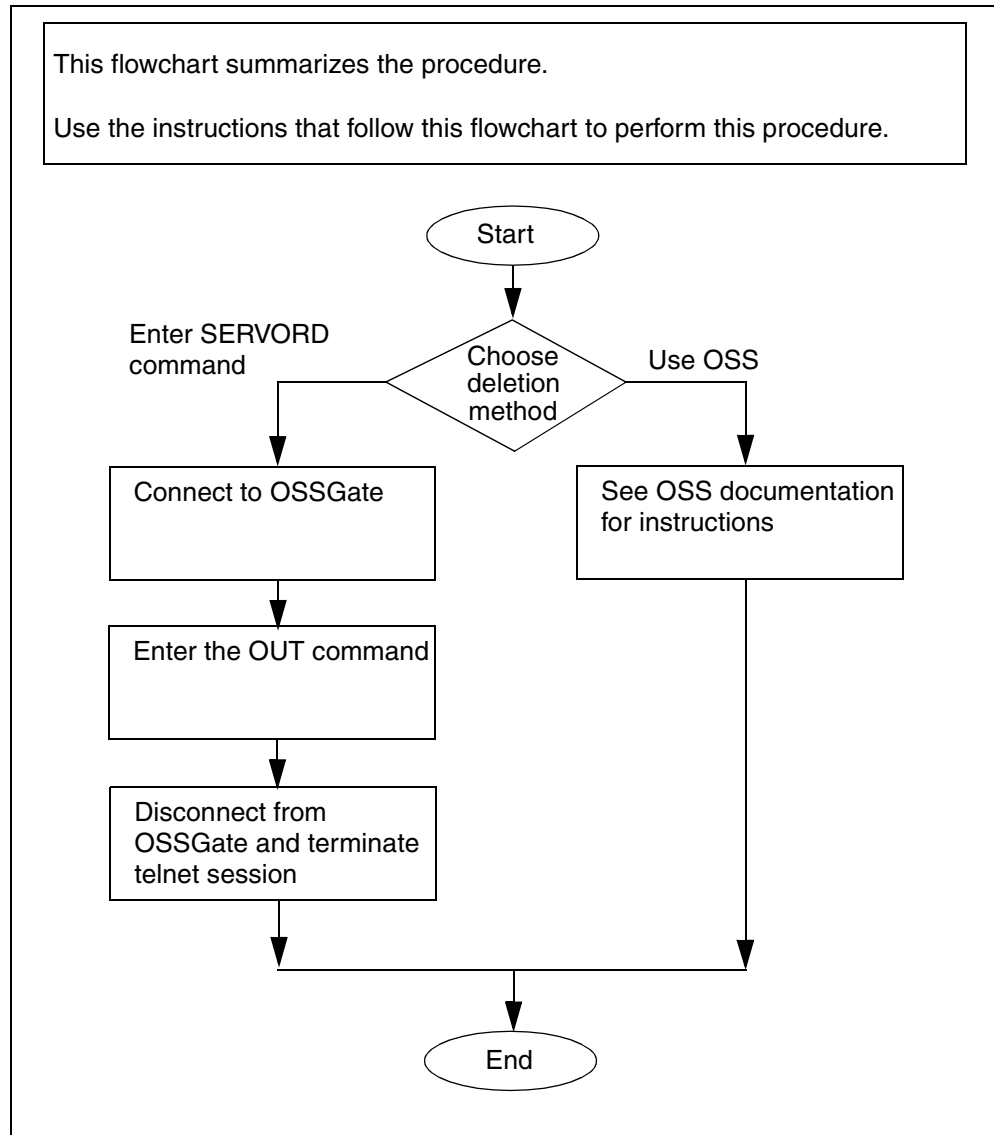
ABCD511-7-3 tp/21/31

Common procedures

This procedure does not refer to any common procedures.

Action

The following flowchart summarizes this procedure.

Deleting a line

**CAUTION****Loss of service**

When deleting lines, use only the user interfaces referred to in this procedure. Do not use the MAP interface to modify any of the data-schema tables directly. Modifying these tables directly via the MAP will result in service-impacting corruption that will require Nortel assistance to resolve.

Deleting a line***At the PC connected to the CS LAN*****1**

If you intend to delete the line by	Do
telnetting to OSSGate and entering a SERVORD command	step 2
using an operations support system (OSS)	step 9

2

Initiate a telnet session to OSSGate. Type the following command at the system prompt

telnet <OSSGate-server-name> <port-number>

and press the Enter key

where

- <OSSGate-server-name> is one of the following:
 - the host name of the server on which OSSGate is running
 - the IP address of the server on which OSSGate is running
- <port-number> is the server port used by OSSGate

Note 1: The default port number is 10023.

Note 2: If in doubt regarding the OSSGate-server-name or the port-number, ask the local network administrator.

For example, type

telnet wcn0s5jk 10023

and press the Enter key.

Example of system response:

Trying 47.142.94.80...

Connected to wcn0s5jk.

Escape character is '^]'.
Enter username and password

- 3** Enter your username and password. Type

<username> <password>

and press the Enter key.

For example, type

user1 passwd

and press the Enter key.

Example of system response:

user1 logged in on 2002/2/2 at 11:51:55.

** **

** 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. **

** **

>

- 4** You have connected to OSSGate, so the system is displaying a prompt, the ">" character, in the telnet window on your screen. Now you put the telnet session into CI mode.

Proceed as follows.

- a Hold down the control key and type B.

Example of system response:

?

- b At the question-mark prompt, type
mode ci

and press the Enter key.

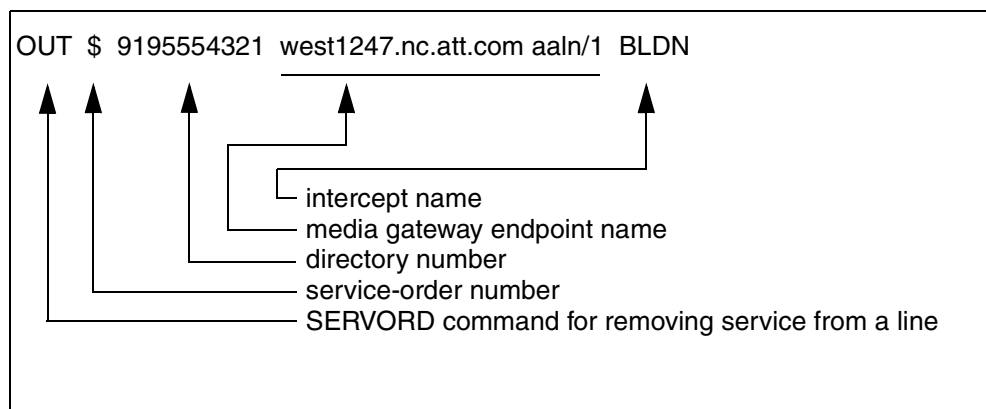
Example of system response:

Mode is CI.

>

- 5 Delete a line by entering the OUT command at the ">" prompt.
The following figure shows an example of the OUT command.

Example of the OUT command



Use the proper format for the media gateway endpoint name in the OUT command. The formatting rules are listed in the prerequisites to this procedure.

When the system processes the OUT command, it deletes the line from table LNINV, and cancels service on the line equipment number (LEN). It also deletes the endpoint from the gateway controller.

Note: For detailed information about SERVORD commands, see the *SERVORD Reference Manual*, 297-8001-808 in the North American market, or 297-9051-808 in the international market.

- 6 Disconnect from OSSGate. Proceed as follows.
 - a Hold down the control key and type B.
Example of system response:
?
 - b At the question-mark prompt, type **logout**
and press the Enter key.
Example of system response:
user1 logged out.

>
- 7 Terminate the telnet session. Proceed as follows.
 - a Hold down the control key and type B.
Example of system response:
?
 - b At the question-mark prompt, type **clearconv**
and press the Enter key.
Example of system response:
SESSION TERMINATED.

Connection closed by foreign host.
- 8 Go to [step 12](#).
- 9 If you are going to use an operations support system (OSS) to delete a line, ask your system administrator for the following:
 - instructions for accessing the OSS
 - information about the OSS interface
- 10 Access the OSS following the instructions of your system administrator.
- 11 Delete the line using the OSS interface.
- 12 You have completed this procedure.

View and troubleshoot GWC service alarms

Purpose of this procedure

Use this procedure to access service-related alarms that are currently active on the GWC application. The Alarm Manager displays alarms as they occur (in real time). This option also permits alarm display filtering based on GWC unit and alarm category.

Refer to section [Troubleshooting GWC service alarms on page 652](#) at the end of this procedure for details about GWC alarm types. Table [Troubleshooting GWC service alarms on page 652](#) contains appropriate actions to diagnose and resolve the alarm condition.

Note: The alarm manager option provides access to UAS and APS device alarms, as well as to other alarms that are not specific to any Carrier VoIP network component.

Access to platform-related alarms is provided in procedure [View GWC platform hardware alarms on page 665](#).

When to use this procedure

Use this procedure as a primary source for fault diagnostic information related to GWC services.

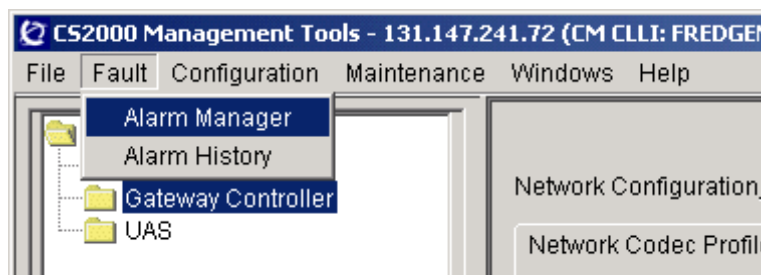
Prerequisites

This procedure has no prerequisites.

Action

At the CS 2000 GWC Manager client

- 1 At the CS 2000 Management Tools window, click the **Fault** menu and select **Alarm Manager** to open the Alarm Manager window.



- 2 From the Alarm Manager window, review the alarms displayed.
The colors to the left of the alarm display provide a visual indication of alarm severity:
 - yellow - warning,
 - orange - minor
 - red - major and criticalRefer to section [Troubleshooting GWC service alarms on page 652](#) at the end of this procedure for details about the alarm types displayed, including appropriate actions to diagnose and resolve the alarm condition. Table [Troubleshooting GWC service alarms on page 652](#) specifically contains the alarm information.
- 3 Click **Refresh List** to update the alarm list.

4 Click the **Details** button to review specific details about an alarm.

Nortel Networks - Alarm Manager - Connected to: 131.147.241.72

File Actions

Raw Alarm List

Network Element	Category	Alarm Time	Sever...	Probable Cause
fdh_uas_01_l.nd.net	Equipment Error	15:03:35 17-Jun-20...	Minor	Equipment malfunction
GWC-5-UNIT-0	Communications	04:14:47 07-Jun-20...	Minor	LAN error
GWC-5-UNIT-0	Communications	05:14:26 07-Jun-20...	Major	Communications sub...
GWC-5-UNIT-0	Communications	23:48:35 08-Jun-20...	Major	Communications sub...
fdh_uas_01_l.nd.net	Communications	14:46:05 26-May-20...	Minor	LAN error
fdh_uas_01_l.nd.net	Equipment Error	15:03:39 17-Jun-20...	Minor	Equipment malfunction
GWC-4-UNIT-0	Communications	03:43:31 09-Jun-20...	Minor	LAN error
GWC-4-UNIT-0	Communications	10:37:34 09-Jun-20...	Major	Communications sub...
GWC-2-UNIT-0	Communications	03:31:50 09-Jun-20...	Minor	LAN error
GWC-2-UNIT-0	Communications	10:36:49 09-Jun-20...	Major	Communications sub...
GWC-9-UNIT-1	Communications	03:51:20 23-Jun-20...	Major	Communications sub...
GWC-11-UNIT-0	Communications	12:59:08 02-Jul-200...	Minor	LAN error
GWC-11-UNIT-0	Communications	12:58:53 02-Jul-200...	Major	Underlying resource un...
Audit	Processing Error	10:28:29 28-Jun-20...	Critical	Corrupt data
SNMP_NE_Poller	Communications	11:08:35 02-Jul-200...	Major	Communications sub...
GWC-11-UNIT-0	Communications	12:58:53 02-Jul-200...	Major	Underlying resource un...
SNMP_NE_Poller	Communications	09:17:36 28-Jun-20...	Major	Communications sub...
GWC-11-UNIT-1	Communications	11:08:34 02-Jul-200...	Major	LAN error
GWC-11-UNIT-0	Communications	12:58:53 02-Jul-200...	Major	Underlying resource un...
GWC-6-UNIT-0	Communications	06:01:52 05-Jul-200...	Minor	LAN error
Audit	Processing Error	04:34:58 23-Jun-20...	Critical	Corrupt data
GWC-5-UNIT-0	Communications	07:05:57 24-Jun-20...	Minor	LAN error

Show alarms: ☒ Critical ☒ Major ☒ minor ☐ warning

New Alarms: 18 C 33 M 13 m 0 w

64 alarms at 10:57:47 05-Jul-2004 EDT

Advanced Filters

Refresh List

Details

Log Name: GWC 307 Component ID: GWC=GWC-5-UNIT-0;Ve

NE Name: GWC-5-UNIT-0 NODEMTC

Alarm Level: Major Alarm Description: Element Manager comm

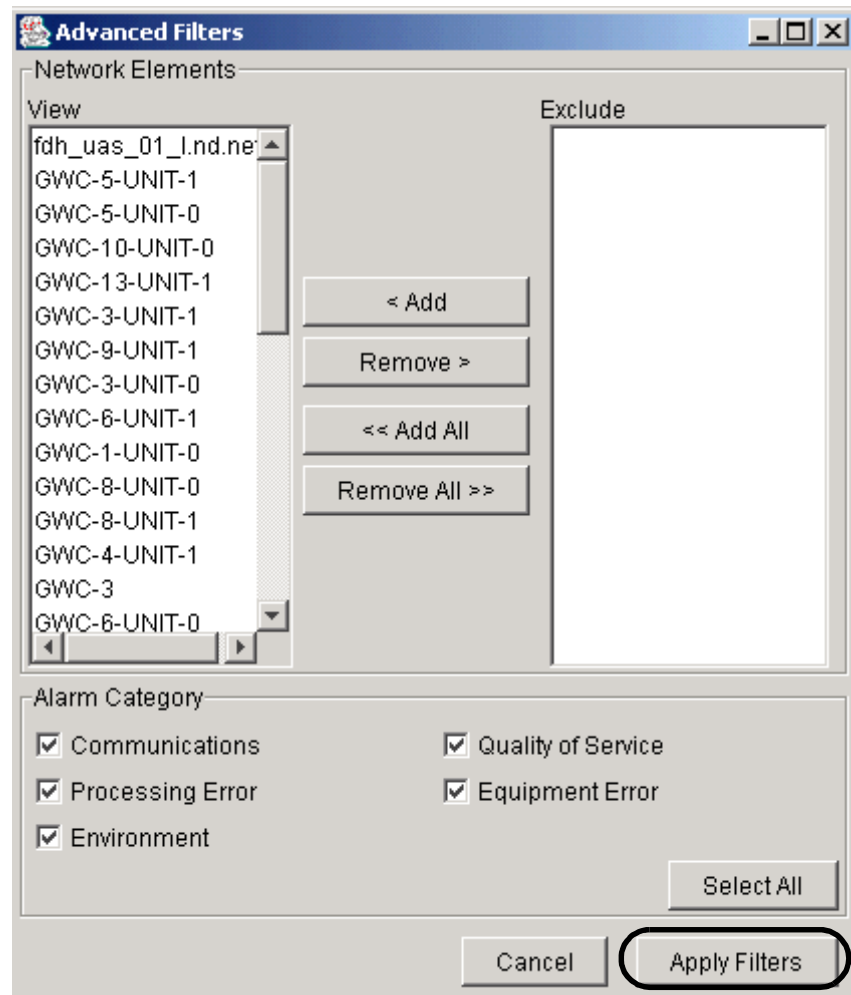
Category: Communications

Alarm Time: 05:14:26 07-Jun-2004 EDT

Probable Cause: Communications subsystem failure Specific Problem: EM indicates provisione

System Uptime: 1 hours, 0 minutes, 11 seconds.

- 5 To filter the alarm display for specific GWC units by excluding the display of certain alarm types, click the **Advanced Filters** button to filter alarms based on selected alarm categories.

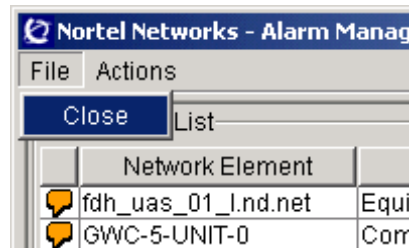


Perform the following steps at the Advanced filters dialog box:

- a In the view list, select the GWC units to be excluded (filtered). You can press and hold the <Shift> key to select multiple GWC units.
- b Click the **Remove >** button to place the selected GWC units in the Exclude (filtered) list. Click the **Remove All >>** button to place all GWC units in the Exclude (filtered) list.

If necessary, select GWC units in the Exclude list. Then, click the **< Add** button to place the selected GWC units in the View (unfiltered) list. Click the **<< Add All** button to place all GWC units in the View (unfiltered) list.

- c De-select the Alarm Category check boxes to exclude (filter) an alarm type for the GWC units in the Exclude list. Any alarm categories that remain selected will be included (will not be filtered) for the GWC units in the Exclude list.
 - d After you have selected the filter criteria click the **Apply Filters** button.
- 6 When you are finished with the Alarm Manager, click the **File** menu and select **Close**.



- 7 This procedure is complete.

Troubleshooting GWC service alarms

Table [Troubleshooting GWC service alarms on page 652](#) contains details about GWC alarm types, and includes appropriate actions to diagnose and resolve the alarm condition.

Note: An alarm ID code for each alarm appears in the first column of the table under the alarm description. You can also find these logs with the alarm ID code in the following locations:

- The syslog Customerlog files in the /var/log directory on the CS 2000 Management Tools server. For example, see the file customerlog.1.

For information on how to open these Syslog log files and search for alarm codes, refer to procedure [View GWC logs in syslog files on page 693](#) in this NTP.

- These logs may also be available in syslog format in custlog files in the /var/adm directory on the CS 2000 Core Manager or Core and Billing Manager (CBM). The CS 2000 Management Tools server must be configured to send the syslog logs to the CS 2000 Core Manager or CBM.
- Switch Control Center (SCC2) or Nortel Networks STD log formats available on the customer's Operations Support System (OSS) interface.

Conversion to these log formats must be activated at the CS 2000 Core Manager or CBM. For information on configuring log

delivery to the customer's OSS, refer to the Fault Management NTP for the CS 2000 Core Manager or CBM.

Troubleshooting GWC service alarms (Sheet 1 of 10)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
Recovery alarm GCEM301	Critical 	A GWC recovery process has terminated early, and the GWC remains out of service. This alarm is generated by the CS 2000 GWC Manager rather than the GWC.	Check IP communications from OAM system to the GWC. Check the CS 2000 Management Tools server logs for additional information, and BSY/RTS the affected GWC unit.
Active unit disabled GWC300	Critical 	Specific problem: Indicates that a unit is out of service: Service is not available. Probable cause: the lack of availability of the underlying resource.	This alarm reports that the unit is not in service (Operational state of "disabled"). If the Administrative state is "unlocked" and the Usage state is "busy" this indicates the unit is trying to recover itself to an in service state. Note: When both units are out of service, the active unit must recover before the standby unit will. Check the following: 1- Whether the unit is manually locked out of service (Administrative state of "locked"). 2- Alarms that may indicate a problem on the unit preventing it from returning to service. 3- Other state indicators which may indicate problems, such as - Isolation state of "isolated" - Availability state of "offLine" 4- Logs which may also indicate a failure of a step in the process of recovering the unit.
		Specific problem: Indicates that a unit has invalid GWC Profile Data: Service is not available. Probable cause: A configuration or customization error.	Check the profile data for the unit and do one of the following: - Change to another profile. - Reconfigure the GWC unit software or CS 2000 GWC Manager software to remove the incompatibility. Then RTS the unit.

Troubleshooting GWC service alarms (Sheet 2 of 10)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
Standby unit disabled GWC301	Major 	Specific problem: Unit is out of service - Service is not available. Probable cause: The lack of availability of the underlying resource.	This alarm reports that the unit is not in service (Operational state of “disabled” and Administrative state is “unlocked”). The unit is system busy (SysB). If the Administrative state is “unlocked” and the Usage state is “busy” this indicates the unit is trying to recover itself to an in service state. Note: When both units are out of service, the active unit must recover before the standby unit will. Check the following: 1 - Alarms that may indicate a problem on the unit preventing it from returning to service. 2 - Other state indicators which may indicate problems, such as - Isolation state of “isolated” - If it is the standby unit, Availability state of “degraded” - Availability state of “offLine” 3- Logs which may also indicate a failure of a step in the process of recovering the unit.

Troubleshooting GWC service alarms (Sheet 3 of 10)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
Standby unit disabled GWC301	Minor 	- Specific problem: Unit is out of service - Service is not available. - Probable cause: The lack of availability of the underlying resource.	This alarm reports that the unit is not in service (Operational state of “disabled” and Administrative state is “locked”). The unit is manually busy (ManB). If the Administrative state is “unlocked” and the Usage state is “busy” this indicates the unit is trying to recover itself to an in service state. Note: When both units are out of service, the active unit must recover before the standby unit will. Check the following: 1- Alarms that may indicate a problem on the unit preventing it from returning to service. 2- Other state indicators which may indicate problems, such as - Isolation state of “isolated” - If it is the standby unit, Availability state of “degraded” - Availability state of “offLine” 3- Logs which may also indicate a failure of a step in the process of recovering the unit.
		- Specific problem: Unit out of service - invalid GWC Profile Data. - Probable cause: Configuration or customization error.	Check the profile data for the unit and do one of the following: - Change to another profile. - Reconfigure the GWC unit software or CS 2000 GWC Manager software to remove the incompatibility. Then, RTS the unit.
Core communication lost GWC302	Major 	Specific problem: No response received to Core heartbeat messages from active GWC unit. Probable cause: LAN error.	Clears automatically after a Core or network outage clears. Otherwise, verify that the node number and Core Side IP address is correct for the GWC to communicate with the Core.

Troubleshooting GWC service alarms (Sheet 4 of 10)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
Core communication lost GWC302	Minor 	Specific problem: No response received to Core heartbeat messages from inactive GWC unit. Probable cause: LAN error.	Clears automatically after a Core or network outage clears. Otherwise, verify that the node number and Core Side IP address is correct for the GWC to communicate with the Core.
Mate unit communication lost GWC303	Minor 	Specific problem: No response received to mate unit heartbeat messages. Probable cause: LAN error.	Cleared by restoring communication from the CS 2000 GWC Manager to the GWC unit. Do this by unlocking the GWC at the CS 2000 SAM21 Manager. Also, verify that the Ethernet cable is connected, and that the GWC is setup to use the correct node number.
Communication with a gateway is down GWC304	Major 	Specific problem: Communication with gateway <Gatewayname> is down. Probable cause: The underlying resource is not available. Note: 'Gateway' is defined as large gateway or audio gateway (e.g. PVG, H.323 gateway with 64 or more endpoints, MG 9000, UAS).	Cleared by restoring communication to the managed gateway. Do this by verifying the availability of the gateway, and comparing the configuration data at the gateway and the CS 2000 GWC Manager (IP address, protocol/version, etc.).
This is a test alarm generated from pmdebug interface GWC305	Minor 	Specific problem: A test alarm generated to log in to notilog table - not sent to manager. Probable cause: Unspecified reason.	Cleared from pmdebug command (not a customer interface) or with a GWC reload.
This is a test alarm generated from pmdebug interface GWC305	Any (critical, major, or minor)	Specific problem: Alarms test from debug interface. Probable cause: Unspecified reason.	Cleared from pmdebug command (not a customer interface) or with a GWC reload.

Troubleshooting GWC service alarms (Sheet 5 of 10)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
DQoS/COPS connection failure GWC306	Major 	Specific problem: A DQoS connection <ConnName> has failed - attempting recovery. Probable cause: Communications subsystem failure. See Note 2 on page 662 for details about what happens when a DQoS connection fails.	The DQoS connection loss alarm is cleared by DCCNXMGR (using DCALARM) when the connection is reestablished or the connection is deleted by provisioning.
Element Manager communication failure GWC307	Major 	- Specific problem: CS 2000 GWC Manager indicates provisioned data mismatched in this unit. Probable cause: Communications subsystem failure - Specific problem: CS 2000 GWC Manager not responding, provisioned data loaded from local Flash. Probable cause: Communications subsystem failure	Cleared with a Busy/RTS of GWC unit. Restore communication with the CS 2000 GWC Manager. Determine if the CS 2000 GWC Manager is down and or disconnected. Determine if the GWC has been setup to use the wrong IP address for the CS 2000 GWC Manager at the CS 2000 SAM21 Manager.
Flash memory error GWC308	Minor 	Specific problem: Erase of flash sector failed. Probable cause: Equipment malfunction. Flash life span exceeded; the number of writes to flash has exceeded the recommended or intended limit.	Cleared with hardware replacement.
SA_PERCENTAGE _USAGE GWC309 Note: This alarm does not apply to the Wireline Universal Packet Access (UA-AAL1) solution.	Minor 	Specific problem: The number of IPSec security associations (that is, secure connections) reached the maximum supported number. Probable cause: Resource at or nearing capacity	This is an information alarm. Report this alarm with details to your next level of support. Note that the alarm clears automatically as SA usage decreases.

Troubleshooting GWC service alarms (Sheet 6 of 10)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
Provisioned GWC Profile not yet activated GWC311	Warning 	Specific problem: GWC profile loaded into Flash will activate on the next reload. A New GWC Profile has been loaded to GWC FLASH by the CS 2000 GWC Manager, but the GWC is still using the old Profile. Probable cause: Configuration or customization error.	Cleared with a GWC reload.
QoS collection application (QCA) connection failure GWC312	Major (partial outage) 	Specific problem: QCA connection <ConnName> has failed - attempting recovery. Probable cause: Communications subsystem failure.	Note: No reports are lost since a back up server is collecting them. Check the following: 1- Ensure that the QCA contains the correct properties (port, IP address...). Check that the QCA is properly provisioned using the CS 2000 Management Tools. 2- Use the ping command to see if you can reach the QCA server. If you cannot reach the server, there may be a problem in the network. 3- Verify that there is no memory exhaustion on the QCA server. 4- Restart the QCA application on the server to bring up the links. 5- Try connecting to a QCA on another CS 2000 Management Tools server.

Troubleshooting GWC service alarms (Sheet 7 of 10)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
QCA connection failure GWC312	Critical (total outage) 	Specific problem: QCA connection <ConnName> has failed - attempting recovery. Probable cause: Communications subsystem failure.	Check the following: 1- Ensure that the QCA contains the correct properties (port, IP address...). Check that the QCA is properly provisioned using the CS 2000 Management Tools. 2- Use the ping command to see if you can reach the QCA server. If you cannot reach the server, there may be a problem in the network. 3- Verify that there is no memory exhaustion on the QCA server. 4- Restart the QCA application on the server to bring up the links. 5- Try connecting to a QCA on another CS 2000 Management Tools server.
RMGC overloaded GWC313	Major 	Specific problem: RMGC can't process all incoming requests. Probable cause: Resource at or nearing capacity.	The RMGC is temporarily overloaded. The alarm will clear itself once the RMGC is able to process requests again. Gateways keep sending requests until they get a response. So, once the overload clears, gateways will be able to register without any further intervention. If this alarm is seen regularly or does not clear, then this is an indication that there is insufficient RMGC processing capacity in the office. Consider commissioning another RMGC.
Location ID reporting connection failure GWC314	Major 	Specific problem: Location ID reporting connection <IP address> has failed - attempting to recover. Probable cause: Communications subsystem failure - destination not available.	Clear the alarm condition using one of the following approaches: - Reestablish the connection to the location recipient. - Disable the location ID reporting application. - Busy/RTS the GWC unit.

Troubleshooting GWC service alarms (Sheet 8 of 10)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
External host interface signal loss GWC315	Critical (>50% loss) Major (>20% loss) Minor (any signal loss)	Specific problem: Small GWs in disabled state Probable cause: Signal loss - alarm based on number of GWs out of service compared with number of GWs provisioned	Logs (GWC502) indicate a small line GW going out of service and coming back into service. GWs are considered to be out of service when heartbeat messages between the GW and GWC are lost. 1. Use the new small gateway OMs to check how many small line GWs are out of service. 2. Use the logs to identify which GWs need attention.
External host interface signal loss GWC315	Major (both links down) Minor (one link down)	Specific problem: USP SS7 paths disabled Probable cause: Signal loss	This alarm is based on the number of USP connections that are out of service, compared with the number of paths (maximum two) checked in a 5-minute polling period. The link paths are considered to be out of service when heartbeat messages between the GWC and USP are lost. Check the USP connections.
External host interface signal loss GWC315	Critical (>50% loss) Major (>20% loss) Minor (any signal loss)	Specific problem: Peer connections failed during interval Probable cause: Signal loss	This alarm is based on the number of call setups failed, compared with the number of calls attempted in a 5-minute polling period. 1. Use the new peer messaging OMs to check the number of calls failed over a longer period. 2. Check the Ethernet link between the GWC and the remote host or peer GWCs.

Troubleshooting GWC service alarms (Sheet 9 of 10)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
External host interface configuration error GWC315	Warning (non-service affecting)	Specific problem: DNS failed GW discovery Probable cause: Configuration or customization error	This alarm is based on the number of gateways that failed DNS lookup in a 5-minute polling period. 1. Use the new DNS OMs to check the number of gateways not discovered, and the number of gateways discovered using RSIP. Note: RSIP discovery does not survive a cold SwAct on the GWC, which may cause long outages. 2. Check the DNS server entries for every gateway.
External host interface protocol error GWC315	Major (both links not active) Minor (one link not active)	Specific problem: USP SS7 path not active Probable cause: Communications protocol error	This alarm is based on the number of USP connections that have heartbeat messages but are not active in a 5-minute polling period. A major alarm affects some call processing; a minor alarm causes a redundancy error. Check the USP configuration to the GWC.
External communication interface GWC315	Critical (>50% proxies disabled) Major (>20% proxies disabled) Minor (any media proxies disabled)	Specific problem: Media proxies in disabled state Probable cause: Signal loss - alarm based on number of media proxies out of service compared with number of media proxies provisioned	Media proxies are considered to be out of service when they fail to respond to messages sent from the GWC, and returned to service when the GWC receives the regular RSIP message. The alarm is raised as a media proxy goes out of service, and cleared when it comes back into service. 1. Use the media proxy OMs to check how many media proxies are out of service in any 5-minute polling period. 2. Use the RTP Portal EM to identify which media proxies need attention. Note: This alarm and the associated OMs give the GWC view of calls, as opposed to the media proxy view.

Troubleshooting GWC service alarms (Sheet 10 of 10)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
Communication with a gateway is down GWC501	Major 	Specific problem: Gateway failed to respond to heartbeat/audit Probable cause: The underlying resource is not available. Note: 'Gateway' is defined as small gateway (e.g. Askey/Medatrix line gateway, Arris/Motorola gateway, H.323 gateway with less than 64 endpoints).	Cleared by restoring communication to the managed gateway. Do this by verifying the availability of the gateway, and comparing the configuration data at the gateway and the CS 2000 GWC Manager (IP address, protocol/version, etc.).
Note 1: An alarm ID code for each alarm appears in the first column of the table under the alarm description. You can also find these logs with the alarm ID code in the following locations: - The syslog Customerlog files in the /var/log directory on the CS 2000 Management Tools server. For example, see the file customerlog.1. For information on how to open these Syslog log files and search for alarm codes, refer to procedure View GWC logs in syslog files on page 693 in this NTP. - These logs may also be available in syslog format in custlog files in the /var/adm directory on the CS 2000 Core Manager or Core and Billing Manager (CBM). The CS 2000 Management Tools server must be configured to send the syslog logs to the CS 2000 Core Manager or CBM. - Switch Control Center (SCC2) or Nortel Networks STD log formats available on the customer's Operations Support System (OSS) interface. Conversion to these log formats must be activated at the CS 2000 Core Manager or CBM. For information on configuring log delivery to the customer's OSS, refer to the Fault Management NTP for the CS 2000 Core Manager or CBM. Note 2: When a dynamic quality of service (DQoS) connection is down between the CS 2000 and a CMTS, the CS 2000 will allow new calls hosted by that CMTS to proceed without DQoS. The behavior of the Multimedia Terminal Adapter (MTA) and CMTS determines whether new calls are attempted using best-effort service or whether they are torn down: - Some MTA vendors allow calls to proceed as a data call (best-effort) and do not send a data-over-cable service interface specification (DOCSIS) authorization block to the CMTS. In this case, the CMTS cannot recognize the call as a voice call and so it proceeds without managed quality of service. - Other MTA vendors send the DOCSIS authorization block to the CMTS with no authorization key or gate-id. When this happens, the CMTS decides whether or not to allow calls to proceed. When the DQoS connection is up, but the CS 2000 does not receive a DQoS gate-id from the CMTS, the CS 2000 will tear down a call.			

Troubleshooting faults in a DQoS network

Refer to section “GWC fault management in a DQoS network” in *Gateway Controller Fault Management*, NN10202-911 for information specific to troubleshooting faults in a dynamic quality of service (DQoS) network.

View GWC platform hardware alarms

Purpose of this procedure

This procedure provides access to platform related alarms such as communication over Ethernet, operating system resource availability, and hardware faults.

When to use this procedure

Use this procedure as a part of alarm clearing at the CS 2000 SAM21 Manager or as a secondary source of diagnostic information for GWC application (service) alarms.

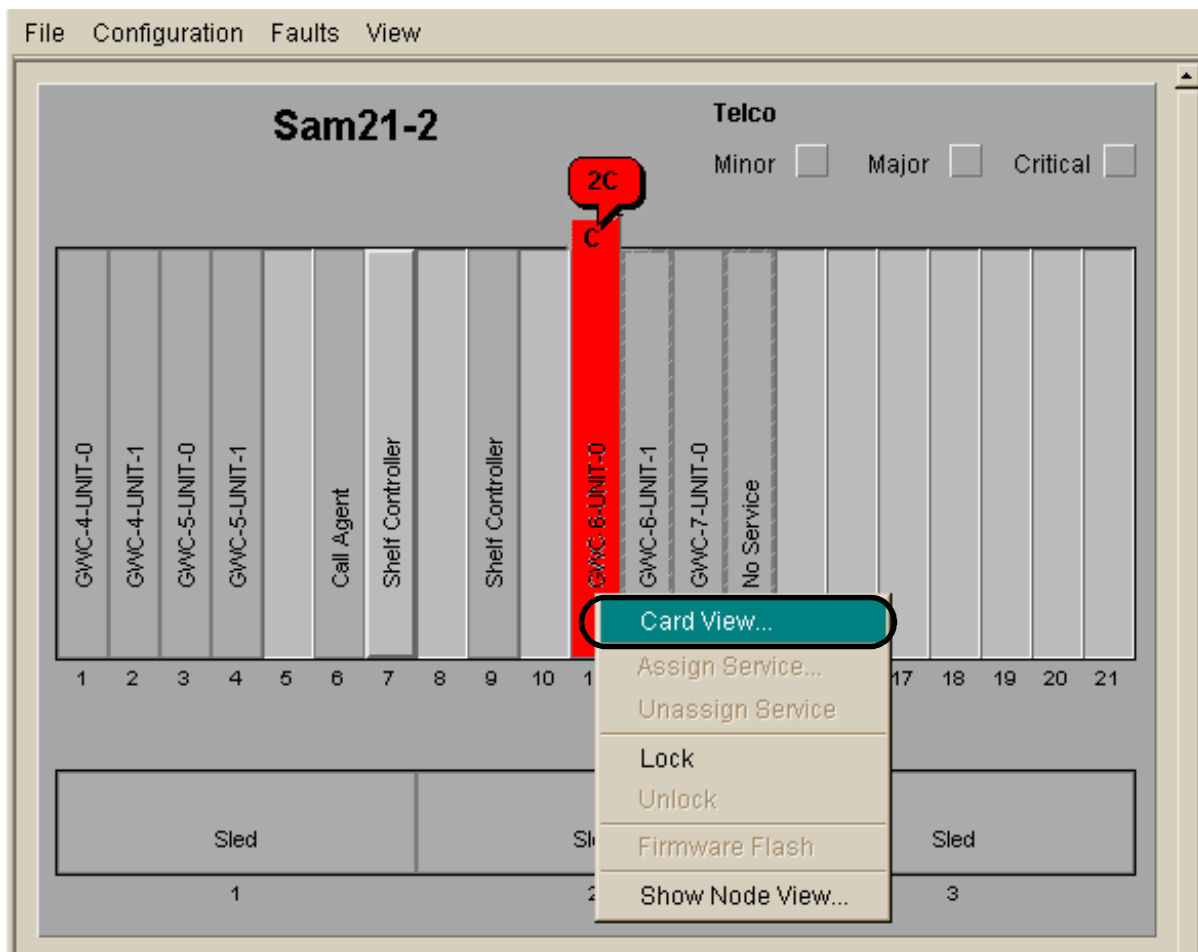
Prerequisites

This procedure has no prerequisites.

Action

At the CS 2000 SAM21 Manager client

- 1 Open the Card View for the card in an alarm condition by right-clicking the card and selecting **Card View** from the pop-up menu.



2 Select the **Alarms** tab in the Card View window.

Sam21-2 : Slot 11

Alarms | Equip | States | Diags | Provisioning

Summary

Critical	Major	Minor
0	1	0

Details

Equip.	ID	Time	Type	Severity	Reason
Card (4)	15	Fri May 17 15:26:31 EDT 2002	ProblemTypeNull	Major	Diagnostic failed at test case

GWC-6-UNIT-0

11

- Refer to the SAM21 Fault Management NTP, NN10089911 for details about the various alarms generated by the SAM21 platform.
- For details about individual alarms related to the NSS cards (including the GWC card) in the SAM21 Shelf, refer to CS 2000 Management Tools information in the ATM/IP Solution-level Fault Management NTP, NN10408-900.

3 This procedure is complete.

Diagnose problems with a GWC card that cannot be booted

Purpose of this procedure

Use this procedure to diagnose problems with a GWC card that cannot be booted and does not appear in the CS 2000 SAM21 Manager shelf view.

When to use this procedure

Use this procedure when a GWC card is installed in the SAM21 shelf but does not appear on the CS 2000 SAM21 Manager shelf view.

Prerequisites

You must have root user access to the CS 2000 Core Manager or Core and Billing Manager (CBM) console.

Action

At the CS 2000 Core Manager or Core and Billing Manager (CBM) console

- 1 Login to the CS 2000 Core Manager or CBM as the root user.
- 2 Start the CS 2000 Core Manager or CBM maintenance interface application by typing

#sdmmtc

or

#cbmmtc

and pressing the enter key.

- 3** Access the applications (APPL) level of the CS 2000 Core Manager or CBM maintenance interface and verify that the Bootp Loading Service and File Transfer Service applications are in service (.) by typing

>appl

and pressing the enter key.

```

SDM      CON      512      NET      APPL      SYS      HW      CLI: OFFC
.         .         .         .         .         .         .      Host: sdmname
                        . .                        Fault Tolerant

Appl
0 Quit
2          # Application                               State
3          1 OM Delivery                               .
4 Logs     2 OSS Comms Svcs                             .
5          3 OSS and Application Svcs                   .
6          4 Base Maintenance Interface                 .
7 Bsy      5 Generic Data Delivery                     .
8 RTS      6 File Transfer Service                     .
9 OffL     7 BOOTP Loading Service                     .
10         8 Enhanced Terminal Access                  .
11         9 SDM Corba Framework                       .
12 Up      10 Table Access Service                      .
13 Down    11 OM Access Service                        .
14 QuerySDM                                     Applications showing: 1 to 11 of 15
15 Locate
16

```

- 4** If these applications are not in service, first BSY then RTS the applications. If these applications are in service (.), then check for bootpd and tftpd messages in the /var/adm/syslog and /var/adm/daemon.log. Refer to the CS 2000 Core Manager or Core and Billing Manager (CBM) Security and Administration NTP for details on busying applications and returning them to service.

Note: Unless log entries have been generated relating to application problems, no log file exists for daemon.log.

At the SAM21 frame

- 5 Verify that the GWC card has power by looking for the lighted yellow or green LEDs on its faceplate.
- 6 Use a VT100 terminal or a PC with terminal application software to connect to the DB9 serial port on the faceplate of the GWC card.
Note: Use a standard straight through serial cable, rather than a null modem cable.
- 7 Configure the PC software to set the PC serial port to 9600 baud, 8 bits, no parity, 1 stop bit.
- 8 Start the terminal application and select a direct connection from COM1.
- 9 Press and hold the reset button on the faceplate of the GWC card for 5 seconds.
- 10 Monitor the boot process on the terminal. If the boot fails, check for the error number and reference it to the following list of error IDs.

(Sheet 1 of 2)

Error ID	Reason text
0500	TFTP retry time out. The following problems could exist: • network has too much traffic • the CS 2000 Core Manager or CBM is busy • the tftp daemon is not running • the load name was entered incorrectly
0600	BOOTP retry time out. The following problems could exist: • network has too much traffic • the CS 2000 Core Manager or CBM is busy • the bootp daemon is not running • the /etc/bootptab file is incorrectly configured

(Sheet 2 of 2)

Error ID	Reason text
8100	The load file on the CS 2000 Core Manager or CBM has the wrong path, the wrong permissions, or the wrong load name.
0020	Message CRC errors. The network could be busy and causing traffic errors.
0017	10baseT link failure. Verify that the Ethernet cable is fully seated in the faceplate and the router.

11 This procedure is complete.

Restart or reboot a GWC card

Purpose of this procedure

Use this procedure to stop all software processes on the GWC card, performs a hardware reset, and reloads the GWC card software from the CS 2000 Core Manager or Core and Billing Manager (CBM).

To restart software applications only, refer to procedure “Enable (RTS) GWC card services” in document *Gateway Controller Security and Administration*, NN10213-611.

When to use this procedure

Use this procedure when you need to reboot a GWC card and force a GWC to download and execute a software load from the The CS 2000 Core Manager or CBM.

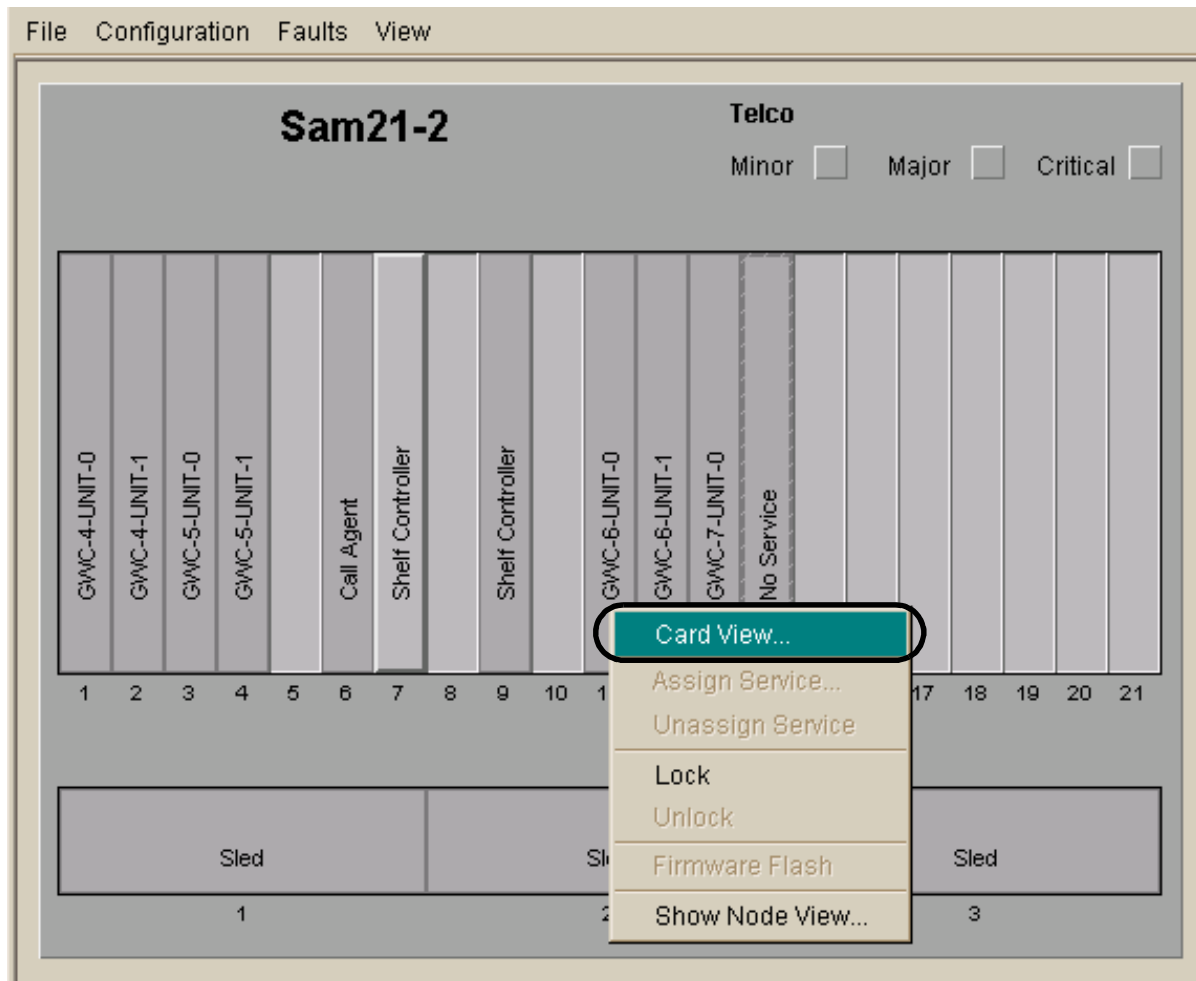
Prerequisites

To reduce the risk of service interruption, you can first busy the GWC applications on specific GWC nodes using the CS 2000 GWC Manager. Refer to the *Gateway Controller Security and Administration* NTP, NN10213-611, for these procedures.

Action

At the CS 2000 SAM21 Manager client

- 1 From the Shelf View, right-click the GWC card you want to reboot and select **Card View** from the context menu.



- 2 At the Card View, select the **States** tab.

The screenshot shows the 'Sam21-2 : Slot 11' window with the 'States' tab selected. The 'Summary' section displays three columns: Critical, Major, and Minor, each with a value of 0. The 'Details' section shows a table with columns: Equip., ID, Time, Type, Severity, and Reason. A sidebar on the left shows a list of units, with 'GWC-6-UNIT-0' selected and '11' highlighted below it.

Critical	Major	Minor
0	0	0

Equip.	ID	Time	Type	Severity	Reason

- 3 Click the **Lock** button to lock the card.

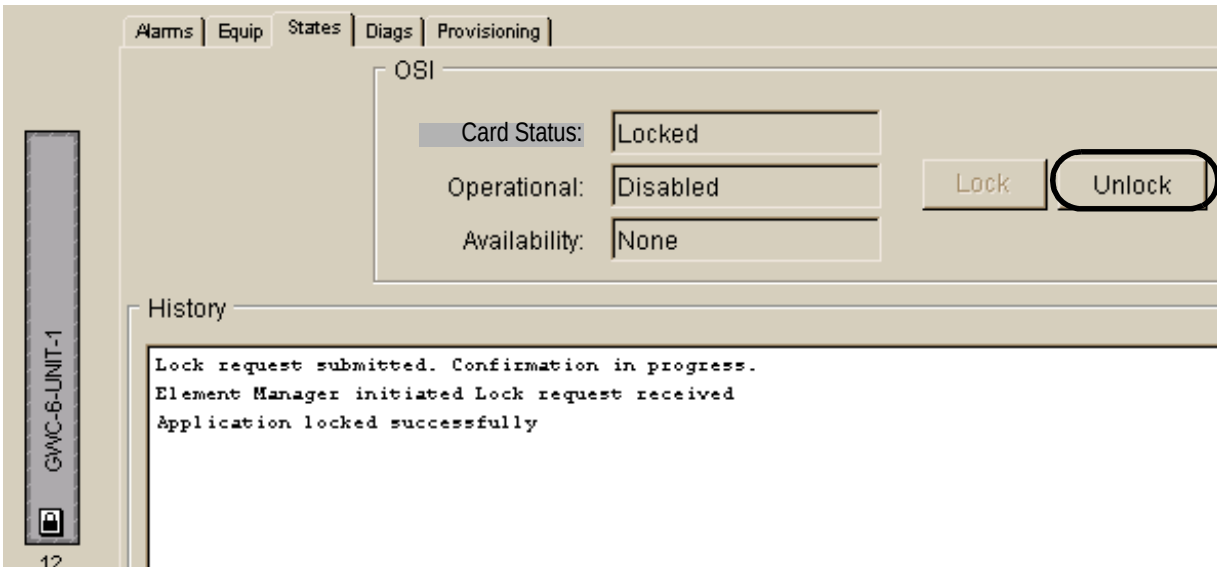
Note: The card must be busy (disabled) before you can lock it. Refer to the procedure “Disable (Busy) GWC card services” in the Gateway Controller Security and Administration NTP, NN10213-611.

The screenshot shows the 'Sam21-2 : Slot 12' window with the 'States' tab selected. The 'OSI' section displays three fields: Card Status (Unlocked), Operational (Enabled), and Availability (None). To the right of these fields are 'Lock' and 'Unlock' buttons. The 'History' section is visible below. A sidebar on the left shows a list of units, with 'GWC-6-UNIT-1' selected and '11' highlighted below it.

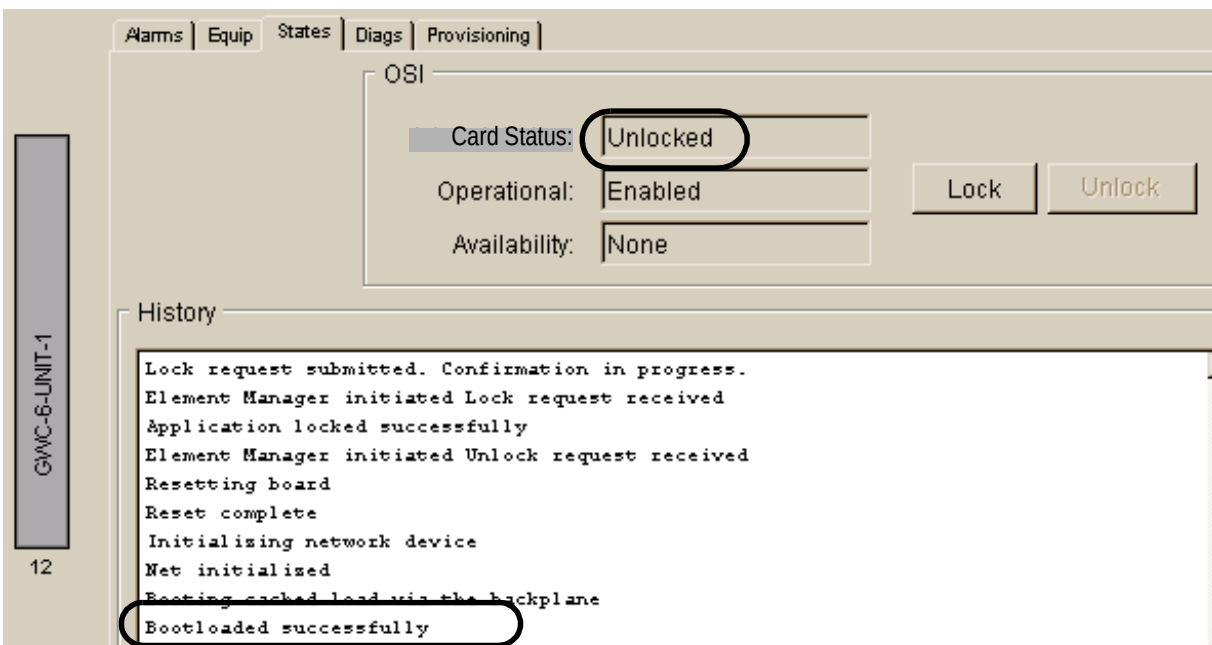
Card Status:	Operational:	Availability:
Unlocked	Enabled	None

Lock Unlock

- 4 Wait until the Card Status is Locked and the History window indicates “Application locked successfully”. Then, click the **Unlock** button.



- 5 Monitor the reboot process. Wait until the Card Status is “Unlocked” and the History window indicates “Bootloaded successfully”.



- 6 This procedure is complete.

View GWC PM logs

Purpose of this procedure

Use this procedure to access service-related Peripheral Module (PM) logs generated by the GWC and forwarded to the core.

Note: For specific information about the logs, and any actions required, refer to the PM log descriptions in this NTP.

When to use this procedure

Use this procedure as a part of scheduled maintenance and as a secondary source of diagnostic information.

Prerequisites

This procedure has no prerequisites.

Action

At the MAPCI interface

- 1 Type **logutil** and press **Enter**.
- 2 Type **open pm** and press **Enter** to retrieve the latest PM log.

```
CI:
>logutil
Current MODE setting is: EXTENDED

LOGUTIL:
>open pm
Done.
RTPS03BD      *    PM185 SEP10 09:07:49 0000 TBL   PM TRAP
                GWC 21 Unit 1 : Act
                Trap message received from the XPM. But unable
                to get trap data because either LOGON not allowed
                or unable to talk to the XPM.

>
```

Note: For reference information about PM logs related to GWC activities, refer to the appropriate PM log description in this NTP.

- 3 For more information about commands available in logutil, type **print logutildir** and press **Enter**.
- 4 This procedure is complete.

Troubleshoot with GWC fault logs

Purpose of this procedure

This procedure is used to perform troubleshooting activities on the GWC or a related component in response to a particular fault log.

When to use this procedure

Use this procedure when the log presented requires action by the craftsperson or service person to resolve, or when other faults with associated components can be involved.

Prerequisites

Before executing this procedure ensure that you have executed procedure [View GWC PM logs](#) in this NTP.

Description

There are various log types that are specific to GWCs, which are described below.

- GWC Return To Service Error Logs
- Communication Problem Logs
 - Communication Loss Detection
 - Communication Loss Confirmation
- State Mismatch Logs
 - State Mismatch Detection Log
 - State Mismatch Resolution Log

Action

Troubleshooting for log PM181

- 1 Use the table following the steps in this procedure to review the details of the log type displayed by your log utility and formulate the appropriate actions to diagnose and repair the problem condition.
- 2 This procedure is complete.

Troubleshooting activities related to log PM181 (Sheet 1 of 4)

Log type; Problem logged	Reason of failure	Action to take
PM181 fault logs are issued for a number of different events, not many of which have to do with communications issues. Most are state changes or steps in a process for the GWC, such as SysB to InSv transition (RTS), or static data loaded.		
GWC Return To Service Error Log; No reply from Peripheral Module	The communication path between the core and the GWC is faulty. Most commonly, recently datafilled GWCs can encounter this problem if the SRVRADDR IP address is incorrect in table SRVRINV on the core, or the Call Server IP number or node number is incorrect on the GWC.	Verify the GWC is datafilled correctly and that the ethernet links and Passport 8600 are connected and working properly.
Communication Loss Detection; Detecting communication loss between core and GWC	A packet may have been intermittently lost, there could be a problem with the GWC such that it is not sending a heartbeat message, (if the core detects that the GWC has not sent a heartbeat in the expected heartbeat interval, a communication loss detection log is generated) or the communication link between the GWC could be broken. If the core detects that the GWC has not sent a heartbeat in the expected heartbeat interval, a communication loss detection log is generated.	If the log is printed only once then there was likely an intermittent packet loss in the network and no action is required If the log is printed periodically then there is likely a problem with the network path between the GWC and the core and packets are being dropped periodically. In this case the network needs to be examined to reduce packet loss.

Troubleshooting activities related to log PM181 (Sheet 2 of 4)

Log type; Problem logged	Reason of failure	Action to take
Communication Loss Confirmation; Communication loss between core and GWC has been confirmed	The GWC may have stopped sending heartbeat messages without notifying the core that it is going out of service. This can occur if the GWC is rebooted without first being taken out of service, or an autonomous restart due to severe failures on the GWC. Note: If the heartbeat is not sent consistently for three time intervals in a row, then the XA-core will determine that communication between the XA-core and GWC has been lost and will print the log entry. The XA-core will also transition the core status of the GWC to SYSB which will cause all call processing on the core side to be cleared.	If the GWC is in service at the time these logs are printed then there is likely a network fault and the network needs to be examined to locate the broken communication path.
State Mismatch Detection Log; A GWC state discrepancy has been detected.	The state mismatch detection log is printed when the GWC reports a state that is not the same as the XA-core recorded state. This can occur if a state transition message sent from the GWC to the XA-core is lost.	A transient log seen once is of no concern. If these logs are seen periodically then there can be an internal software problem, or problem with the network if communication loss logs are also seen. Refer also to the log type "Communication Loss Detection" in this table.

Troubleshooting activities related to log PM181 (Sheet 3 of 4)

Log type; Problem logged	Reason of failure	Action to take
State Mismatch Resolution Log; The GWC state discrepancy is being resolved.	A state mismatch occurred consistently. If a state mismatch has been consistently detected (varies depending on the type of mismatch), then the core will take action to resolve the mismatch and synchronize the GWC and XA-core states as well as any related call processing. Note: This can involve sending the GWC a message which will cause the GWC to go out of service and then back in service, constituting a call processing outage.	The XA-core will resolve the mismatch automatically. However, the circumstances surrounding the mismatch needs to be investigated by your next level of support.
GWC unit timed out on recovery. Ensure datafilled GWC is communicating with the core.	Whenever the core goes through a restart cycle, during the restart the core sends all GWC units a message indicating that the core restarted. The GWC will in turn send a reply message to the core indicating its state. The core uses this information to ensure the recorded state of the GWC on the core database matches the actual state of the GWC. The log is generated for any GWC unit that does not respond to the core restart message during a core restart (warm, cold, or reload). The log is to alert the customer that the GWC unit did not respond.	-For a simplex GWC configuration (where the GWC node is made up of only one GWC card rather than two cards), this log can be ignored if it flags the inactive unit. The lack of an inactive card unit causes this log to be produced because a simplex GWC node only has one real hardware card unit. Currently, the core cannot be made to realize this and so the log cannot be avoided. -For duplex (redundant) GWC nodes ensure the identified GWC unit (unit 0 or 1) is operating correctly and communicating with the core.

Troubleshooting activities related to log PM181 (Sheet 4 of 4)

Log type; Problem logged	Reason of failure	Action to take
Note: Do not datafill GWCs on the core if there is no real GWC corresponding to the datafill, as any datafilled GWC consumes core resources. For GWC recovery over core restart reload, extra datafilled GWCs with no corresponding physical GWC connected can lead to an undesirable increase to overall system recovery. GWC node timed out on recovery. Ensure datafilled GWC is communicating with the core.		
	Normally this log is seen for a GWC that is datafilled, but no physical GWC exists. This log can also be seen if a GWC goes busy over a core restart reload, but never comes back into service.	- Delete datafill for GWCs that do not really exist. - For a GWC that fails to recover troubleshoot the GWC. Likely there is something wrong with it preventing it from going into service. Check other PM logs that can indicate communication failures or data download failures.

Perform a CS 2000 data integrity audit

Purpose of this procedure

Use this procedure to perform an on-demand data integrity audit of the CS 2000 GWC Manager database.

The audit compares the GWC Manager database with the CS 2000 XA Core database and flags any mismatches between the two databases. The XA Core is considered to hold the 'master' database. This procedure uses the audit system data integrity tool to perform the audit, view the results and take corrective action.

Note: You can also schedule a CS 2000 data integrity audit using this tool. Refer to procedure "Configure a recurring data integrity audit" in the Gateway Controller Configuration Management NTP, NN10205-511.

Remedial actions offered are likely to involve deletion of inconsistent data. However, where possible the option to repair data inconsistencies will be given.

Note: Starting in SN07, the CS 2000 data integrity audit compares the following data to highlight inconsistencies:

- On the CS 2000 Management Tools server:
 - Bearer network fabric type of each GWC node
 - The network instance of each GWC node
- On the XA-Core:
 - The network instance and fabric type contained in the BEARNETS table
 - The bearer network type for each GWC node contained in the SERVINV table.

If the audit detects any inconsistencies in this data, you will have the option to attempt to repair them.

When to use this procedure

Use this procedure when you are receiving logs or alarms in the CS 2000 XA Core or at the CS 2000 SAM21 Manager client indicating a possible provisioning error with a GWC card or node.

Note 1: When the audit is running, suitable locks are in place that disable provisioning operations.

Note 2: The audit application keeps no record of problems that it has raised an alarm for. Therefore, if a problem is detected during an audit and not corrected, an alarm will be generated in the alarm manager for the same problem the next time the audit is run.

Note 3: If you have scheduled data integrity audits, remember that a maximum of one CS 2000 data integrity audit can be in progress at a time. An in-progress CS 2000 audit blocks all attempts to run CS 2000 audits. If you run an on-demand CS 2000 audit, and if that audit is still in progress at the start time of a scheduled CS 2000 audit, the scheduled audit will not occur.

Prerequisites

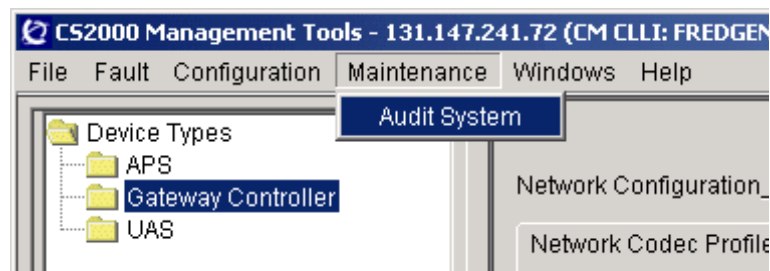
Ensure that no provisioning activities are scheduled to take place during the audit.

Unlike the line and trunk audits, the CS 2000 data integrity audit does not provide an option to save the audit report to a file on the local disk.

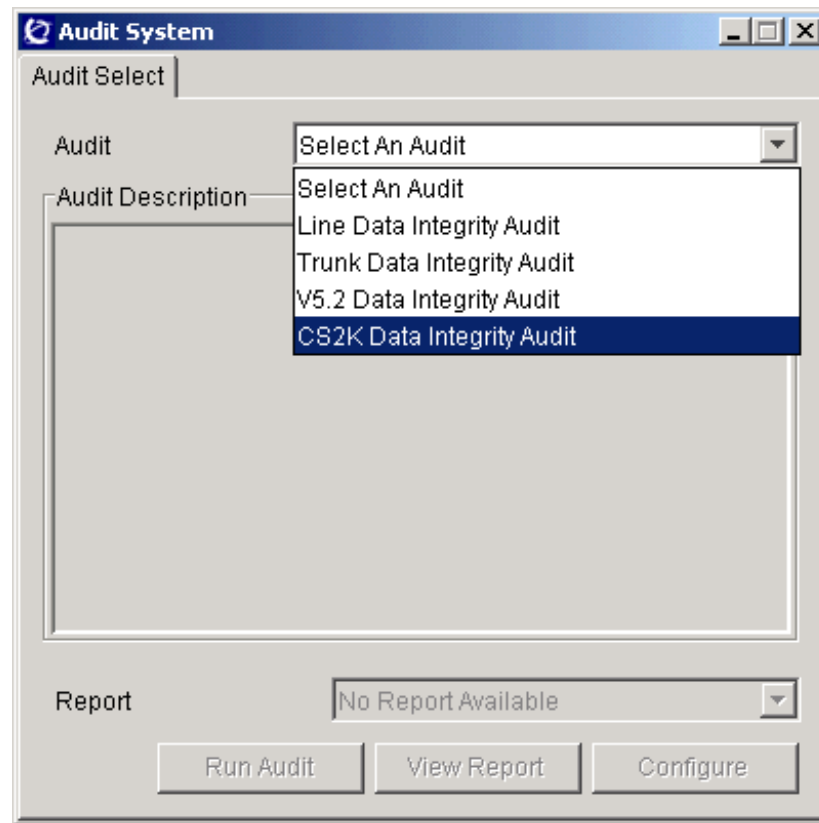
Action

At the CS 2000 GWC Manager client

- 1 At the CS 2000 Management Tools window, select **Maintenance**, and then **Audit System**.



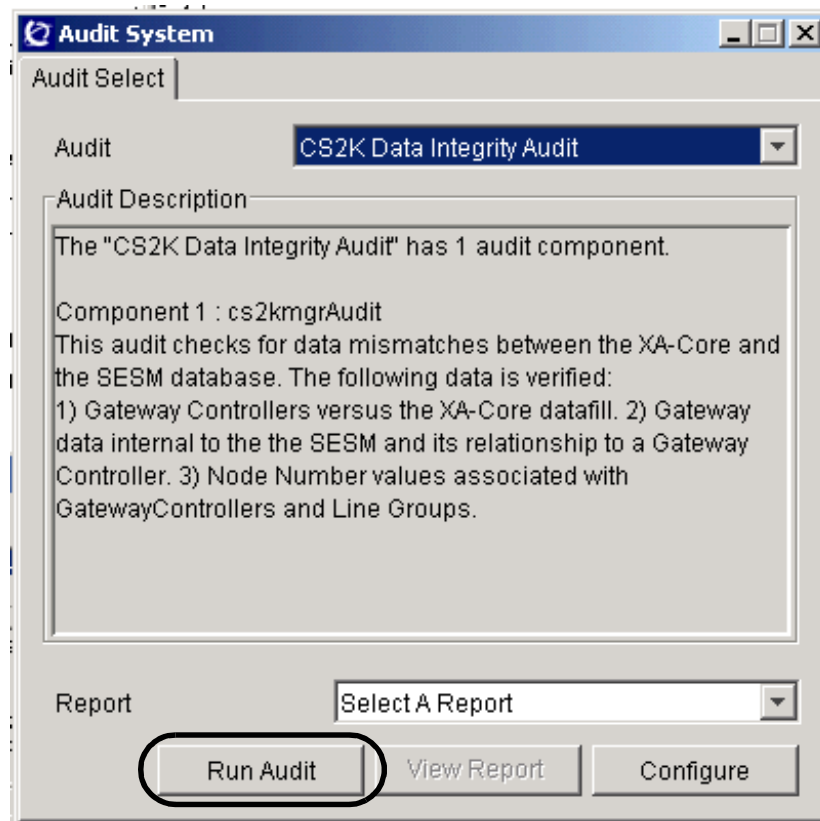
- 2 At the Audit System dialog box, select **CS2K Data Integrity Audit** from list of audits displayed in the drop-down menu.



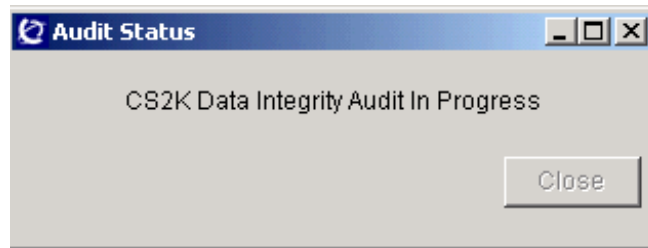
- 3 Select the next step as follows.

If you want to	Do
perform a CS 2000 audit and view the results of the audit	step 4 and complete the procedure
view the results of a CS 2000 audit that has finished running and resolve problems	step 6 and complete the procedure

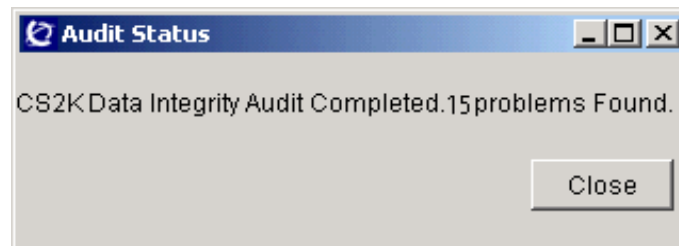
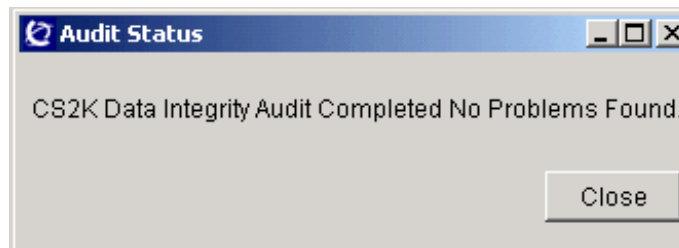
- 4 Click the **Run Audit** button to start the audit.



During a CS 2000 audit, the system displays the following message:



The audit may take a few minutes to complete. When the audit is successfully completed, the system displays one of two types of messages as follows:



Note: If the audit does not execute successfully, the message "CS2K Data Integrity Audit Failed to Complete" is displayed with an error message indicating the reason. Contact your next level of support to resolve the problem.

- 5 Click the **Close** button to close the Audit Status pop-up window.
- 6 To view a CS 2000 audit report, proceed as follows:
 - a Ensure that you have selected **CS2K Data Integrity Audit** from the Audit field drop-down menu at the top of the Audit System dialog box.

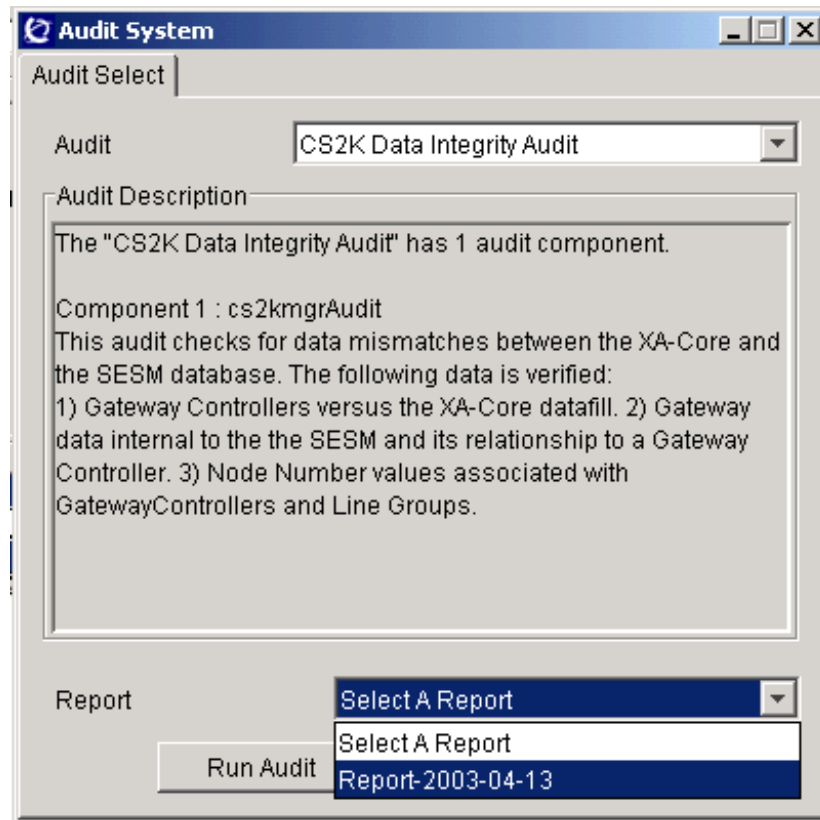
- b Select **Report** <date> from the drop-down menu in the Report field at the bottom of the dialog box.

The file name has the following format:

Report-<date>

where

<date> is the date in yyyy-mm-dd format, for example, 2003-02-15.



- c Click the **View Report** button.



The system displays the selected report. If no problems were discovered, the report will be empty. Here is an example of a report containing problems:

CS2K Data Integrity Audit Report

File Last Audit Date: 2002-07-29 14:58:22

Index	Problem Description	Current Status
0	GWC-9 at IP 172.17.40.64 is only datafilled in XA-Core	Problem Exists
1	GWC-10 at IP 172.17.40.68 is only datafilled in XA-Core	Problem Exists
2	GWC-11 at IP 172.17.40.72 is only datafilled in XA-Core	Problem Exists
3	GWC-12 at IP 172.17.40.76 is only datafilled in XA-Core	Problem Exists
4	GWC-13 at IP 172.17.40.80 is only datafilled in XA-Core	Problem Exists
5	GWC-14 at IP 172.17.40.84 is only datafilled in XA-Core	Problem Exists
6	GWC-15 at IP 172.17.40.88 is only datafilled in XA-Core	Problem Exists
7	GWC-16 at IP 172.17.40.96 is only datafilled in XA-Core	Problem Exists
8	GWC-17 at IP 172.17.40.100 is only datafilled in XA-Core	Problem Exists
9	GWC-18 at IP 172.17.40.104 is only datafilled in XA-Core	Problem Exists
10	GWC-19 at IP 172.17.40.108 is only datafilled in XA-Core	Problem Exists
11	GWC-20 at IP 172.17.40.112 is only datafilled in XA-Core	Problem Exists
12	GWC-21 at IP 172.17.40.116 is only datafilled in XA-Core	Problem Exists
13	GWC-22 at IP 172.17.40.120 is only datafilled in XA-Core	Problem Exists
14	GWC-100 at IP 172.17.46.244 is only datafilled in XA-Core	Problem Exists

Problem Detail:

Problem Number: 0

Problem Description: GWC-9 at IP 172.17.40.64 is only datafilled in XA-Core

Current Status: Problem Exists

Possible Actions

Actions: Please Select An Action

Description:

Take Action

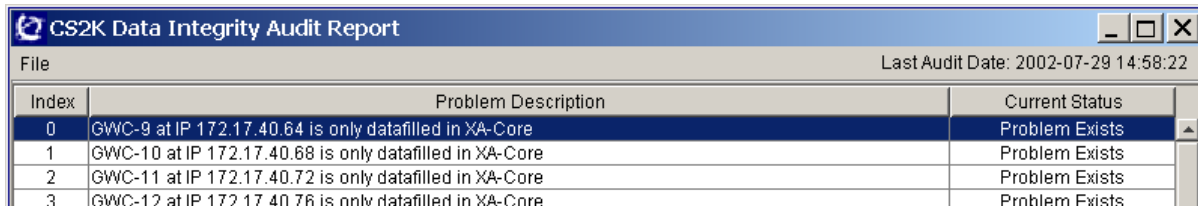
Note 1: The CS 2000 Management Tools server retains the most recent CS 2000 audit report. When a new audit occurs, the server deletes the previous report.

Note 2: The system places the audit report in the following directory on the CS 2000 Management Tools server: /opt/nortel/ptm/current/M12/apps/Audit.

Note 3: The CS 2000 GWC Manager does not provide an option to save a CS 2000 data audit report to local disk.

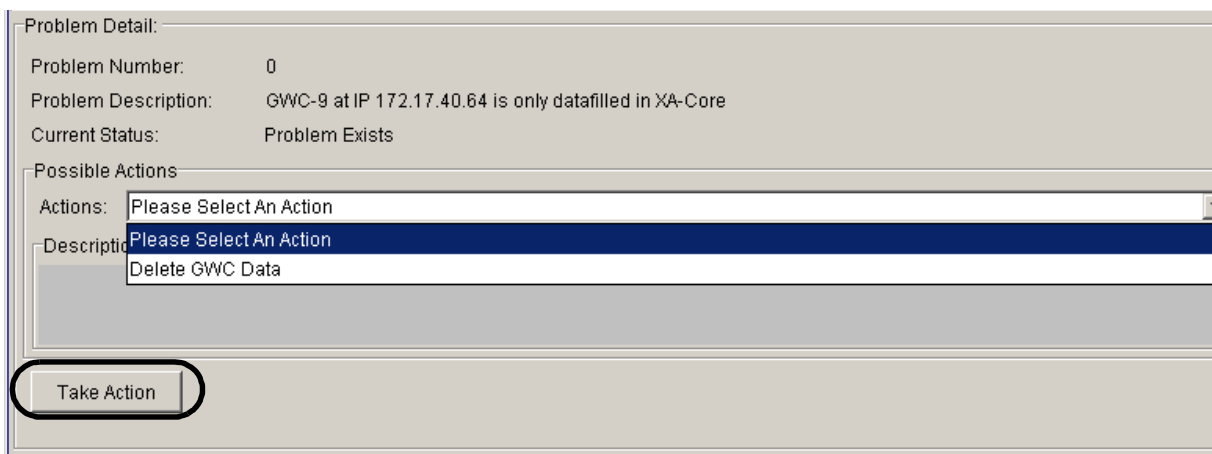
- 7 Review the results of the audit and select a problem to resolve.

Note: If necessary, resize the entire window to completely view the Problem Description field.



Index	Problem Description	Current Status
0	GWC-9 at IP 172.17.40.64 is only datafilled in XA-Core	Problem Exists
1	GWC-10 at IP 172.17.40.68 is only datafilled in XA-Core	Problem Exists
2	GWC-11 at IP 172.17.40.72 is only datafilled in XA-Core	Problem Exists
3	GWC-12 at IP 172.17.40.76 is only datafilled in XA-Core	Problem Exists

- 8 Evaluate actions to resolve a problem and take action.
- Click and hold on the Action drop-down menu near the bottom of the screen to assess any possible actions.
 - If appropriate, select an action. Read the description of the action and ensure that you observe any recommended steps or cautions.



Problem Detail:

Problem Number: 0

Problem Description: GWC-9 at IP 172.17.40.64 is only datafilled in XA-Core

Current Status: Problem Exists

Possible Actions

Actions: Please Select An Action

Description: Please Select An Action

Delete GWC Data

Take Action

- c Click the **Take Action** button

Note: If you see the message “Correction Failed”, please contact your next level of support.

- 9 Return to [step 7](#) to review another problem.
- 10 This procedure is complete.

View GWC logs in syslog files

Purpose of this procedure

This procedure provides access to GWC logs stored in the syslog files on the CS 2000 Management Tools server. Instructions are also provided for searching specific entries in the syslog files. The logs mentioned in this procedure contain information on the GWC.

For a list of syslog logs that contain information on the GWC, refer to section [Syslog files relevant to the GWC on page 695](#).

Note: This NTP contains descriptions of GWC series logs.

When to use this procedure

Use this procedure as a part of scheduled maintenance and as a secondary source of diagnostic information.

Prerequisites

This procedure has no prerequisites.

Action

At the CS 2000 Management Tools client

- 1 Access the directory level where the syslog files reside by typing
\$ cd /var/log
and pressing the enter key.

- 2 List the directory content by typing
\$ ls
and pressing the enter key.

The system displays a list of different log files, such as, customerlog, securitylog, and so on. These files are appended with numbers, for example "customerlog.0". The files with the lower numbers are the newer files.

Note: For a list of files relevant to the GWC, refer to table [Syslog logs containing GWC entries on page 695](#).

- 3 Use the following table to determine your next step.

If you want to view	Do
the entire content of a log file	step 4
specific content of a log file	step 6

- 4 Display the entire content of a log file by typing

```
$ cat <log_filename> |more
```

and pressing the enter key.
where
log_filename
is the name of the log file you want to display. See the first table below for specific examples.
Example

```
$ cat customerlog.0 |more
```

Press the space bar to scroll through the file if it is larger than the screen can display.
- 5 Continue with [step 7](#).
- 6 Search and display specific content of a log file by typing

```
$ cat <log_filename> |grep <search_string>
```

and pressing the enter key.
where
search_string
is the text you want to search for, for example KRB (to search for logs associated with the Kerberos application)
Example

```
cat customerlog.0 |grep GWC309
```

or

```
cat securitylog.1 |grep KRB_LOG
```
- 7 To print the contents of this file, contact your site system administrator for assistance with using UNIX print commands and with locating a printer connected to your network.
- 8 This procedure is complete.

Syslog files relevant to the GWC

The following table describes the syslog logs in the /var/log directory that contain entries relevant to the GWC.

Syslog logs containing GWC entries

Log type	Description	Examples of log file names
Audit log	Records the actions taken by users on the system, including some of the parameters they used.	auditlog auditlog.0 auditlog.1
Customer log	Records all alarms the system has received.	customerlog customerlog.0 customerlog.1
Debug log	Records debug information for CS 2000 Management Tools network components to help detect an underlying problem.	debuglog debuglog.0
PTM log	Contains a record of all the SNMP traps received by the system.	ptmlog ptmlog.1 ptmlog.2
Security log	Records failed actions taken by users on the system. Securitylog file also includes fault related logs for the Kerberos application.	securitylog securitylog.0

Use the following table to interpret the syslog application logs on the redirecting media gateway controller (RMGC).

GWC syslog application logs

Application log description	Cause or condition	Action
RMGC: Successful Count: x Failed Count: y	The RMGC application produces a syslog performance report once an hour. (See the debug log in /var/log.) It contains the counts of the number of RSIPs processed successfully (x) and the number failed (y). The counts are cumulative, so that to calculate the number of successful/failed RSIPs, it is not necessary to parse each and every log but just to subtract the counts from the previous log to derive the counts between the current log and the previous.	No action is required.

Retrieve and correlate GWC logs in customer log files

Purpose of this procedure

This procedure provides access to the customer log files, one of the syslog log-types on the CS 2000 Management Tools server. Instructions are provided for searching specific log entries in customer log files. The log entries described in this procedure contain information on the GWC.

Note: For more information on syslog logs in general, refer to [View GWC logs in syslog files on page 693](#).

When to use this procedure

Use this procedure as a part of scheduled maintenance and as a secondary source of diagnostic information.

Prerequisites

This procedure has no prerequisites.

Action

At the CS 2000 Management Tools client

- 1 Access the directory level where the customer log files reside by typing

```
>cd /var/log
```

and pressing the enter key.

If you want to	Do
look at the contents of the whole customer log file	step 2
search for specific text in the customer log file	step 4

- 2 Review the contents of customer log file by typing

```
>cat <log_filename> |more
```

and pressing the enter key.

where

log_filename

is the name of the customer log file you want to display.

Example

```
cat customerlog.1 |more
```

Press the space bar to scroll through the file if it is larger than the screen can display.

- 3 Go to [step 5](#).
- 4 Search for specific text in a customer log file by typing

```
>cat <log_filename> |grep <search_string>
```

and pressing the enter key.
where
search_string
is the text you want to search for.
Example
cat customerlog.0 |grep GWC307
- 5 To print the contents of this file, contact your site system administrator for assistance with using UNIX print commands and with locating a printer connected to your network.
- 6 This procedure is complete.

GWC log reference

The customer log file contains a record of all GWC alarms the system has received and also includes several GWC logs that are not raised as alarms. For reference information about these GWC logs, refer to the appropriate GWC log description in this NTP.

GWC300

Log report GWC300 indicates an “Active unit disabled.” Unit Out of Service: Service is not available or Invalid GWC Profile Data. The alarm severity is Critical.

Format

The format for log report GWC300 is as follows:

```
COMPACT2 *** GWC300 JUN30 11:01:55 0580 TBL GWC Fault
  Location: GWC-0-UNIT-0
  NotificationID: 1
  State: Raise
  Category: Quality of Service
  Cause: Underlying resource unavailable
  Time: Jun 30 11:09:16 2003
  Component Id: GWC-0-UNIT-0
  Specific Problem: Unit Out of Service: Service is not available
  Description: Active unit disabled.
```

Selected field descriptions

This log report has no selected fields.

Action

See the following table:

Specific problem Probable cause	Action
Specific problem: Indicates that a unit is out of service: Service is not available. Probable cause: the lack of availability of the underlying resource.	This log reports that the unit is not in service (Operational state of "disabled"). If the Administrative state is "unlocked" and the Usage state is "busy" this indicates the unit is trying to recover itself to an in service state. Note that when both units are out of service, the active unit must recover before the standby unit will. Check the following: 1- Whether the unit is manually locked out of service (Administrative state of "locked"). 2- Alarms that may indicate a problem on the unit preventing it from returning to service. 3- Other state indicators which may indicate problems, such as - Isolation state of "isolated" - If it is the standby unit, Availability state of "degraded" - Availability state of "offLine" 4- Logs which may also indicate a failure of a step in the process of recovering the unit.
Specific problem: Indicates that a unit has invalid GWC Profile Data: Service is not available. Probable cause: A configuration or customization error	Check the profile data for the unit and do one of the following: - Change to another profile. - Reconfigure the GWC unit software or CS 2000 GWC Manager software to remove the incompatibility. Then, RTS the unit.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC301

Log report GWC301 indicates a "Standby unit disabled." Unit Out of Service: Service is not available or Invalid GWC Profile Data. The alarm severity is Minor or Major.

Format

The format for log report GWC301 is as follows:

```
COMPACT2 * GWC301 JUN30 11:02:44 0588 TBL GWC Fault
Location: GWC-0-UNIT-1
NotificationID: 1
State: Raise
Category: Quality of Service
Cause: Underlying resource unavailable
Time: Jun 30 10:54:34 2003
Component Id: GWC-0-UNIT-1
Specific Problem: Unit Out of Service: Service is not available
Description: Standby unit disabled.
```

Selected field descriptions

This log report has no selected fields.

Action

See the following table:

Specific problem Probable cause	Action
Specific problem: Indicates that a unit is out of service: Service is not available. Probable cause: the lack of availability of the underlying resource.	This log reports that the unit is not in service (Operational state of "disabled"). If the Administrative state is "unlocked" and the Usage state is "busy" this indicates the unit is trying to recover itself to an in service state. Note that when both units are out of service, the active unit must recover before the standby unit will. If the Operational state "disabled" and Administrative state is "unlocked", the unit is system busy (SysB) - the alarm is major. If the Operational state "disabled" and Administrative state is "locked", the unit is manually busy (ManB) - the alarm is minor. Check the following: 1- Alarms that may indicate a problem on the unit preventing it from returning to service. 2- Other state indicators which may indicate problems, such as - Isolation state of "isolated" - Availability state of "offLine" 3- Logs which may also indicate a failure of a step in the process of recovering the unit.
Specific problem: Indicates that a unit has invalid GWC Profile Data: Service is not available. Probable cause: A configuration or customization error	Check the profile data for the unit and do one of the following: - Change to another profile. - Reconfigure the GWC unit software or CS 2000 GWC Manager software to remove the incompatibility. Then, RTS the unit.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC302

Log report GWC302 indicates a Major for active unit; Minor for inactive unit. "Core communication lost." No response received to Core heartbeat messages.

Format

The format for log report GWC302 is as follows:

```
COMPACT06BT * GWC302 JUL1 15:02:21 0055 TBL GWC Fault
  Location: GWC-2-UNIT-0
  NotificationID: 3
  State: Raise
  Category: Communications
  Cause: LAN error
  Time: Jul 01 15:02:27 2003
  Component Id: GWC=GWC-2-UNIT-0;Version=PGC91AQ;Unit=unit_0;
    Software=NODE MTC
  Specific Problem: No response received to Core heartbeat messages.
  Description: Core communication lost.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log clears automatically after a Core or network outage clears. Otherwise, verify that the node number and Core Side IP address is correct for the GWC to communicate with the Core.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC303

Log report GWC303 indicates a "Mate unit communication lost." No response received to mate heartbeat messages. The alarm severity is Minor.

Format

The format for log report GWC303 is as follows:

```
COMPACT2 * GWC303 JUN30 11:02:47 0589 TBL GWC Fault
  Location: GWC-0-UNIT-0
  NotificationID: 4
  State: Raise
  Category: Communications
  Cause: LAN error
  Time: Jun 30 11:10:08 2003
  Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
  Software=NODE MTC
  Specific Problem: No response received to mate heartbeat messages.
  Description: Mate unit communication lost.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by restoring communication from the CS 2000 GWC Manager to the GWC unit. Do this by unlocking the GWC at the CS 2000 SAM21 Manager. Also, verify that the Ethernet cable is connected, and that the GWC is setup to use the correct node number.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC304

Log report GWC304 indicates that communication with a gateway is down. The alarm severity is Major.

Note: 'Gateway' is defined as large gateway or audio gateway (for example, PVG, H.323 gateway with 64 or more endpoints, MG 9000, UAS).

Format

The format for log report GWC304 is as follows:

```
COMPACT2 ** GWC304 JUL2 01:25:58 0619 TBL GWC Fault
Location: GWC-1-UNIT-1
NotificationID: 78
State: Raise
Category: Communications
Cause: Underlying resource unavailable
Time: Jul 02 01:21:20 2003
Component Id: GWC=GWC-1-UNIT-1;Version=PGT09BL;
Unit=unit_1;Software=SSC
Specific Problem: TESTPVG
Description: Communication with a gateway is down.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by restoring communication to the managed gateway. Do this by verifying the availability of the gateway, and comparing the configuration data at the Gateway and the CS 2000 GWC Manager (IP address, protocol/version, etc).

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC305

Log report GWC305 indicates that a test alarm is generated from pmdebug interface to log in to the notilog table. May be any level.

Format

The format for log report GWC305 is as follows:

```
COMPACT2 *** GWC305 JUL10 09:56:30 0671 TBL GWC Fault
  Location: GWC-0-UNIT-0
  NotificationID: 12
  State: Raise
  Category: Communications
  Cause: Unspecified reason
  Time: Jul 10 10:07:23 2003
  Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
    Software=DEBUG
  Specific Problem: Alarms test from debug interface
  Description: This is a test alarm generated from pmdebug interface.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by using the pmdebug command (not a customer interface) or with a GWC reload.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC306

Log report GWC306 indicates a DQoS/COPS connection failure. The alarm severity is major.

Format

The format for log report GWC306 is as follows:

```
COMPACT2 ** GWC306 JUL10 09:56:31 0672 TBL GWC Fault
  Location: GWC-0-UNIT-0
  NotificationID: 13
  State: Raise
  Category: Communications
  Cause: Communications subsystem failure
  Time: Jul 10 10:07:24 2003
  Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
    Software=DQOS MTC
  Specific Problem: DQoS connection CMTS065 has failed - attempting
    recovery.
  Description: DQoS/COPS connection failure.
```

Selected field descriptions

This log report has no selected fields.

Action

The DQoS connection loss alarm is cleared by DCCNXMGR (using DCALARM) when the connection is reestablished or the connection is deleted from provisioning.

Associated OM registers

This log report has no associated OM registers.

Additional information

When a dynamic quality of service (DQoS) connection is down between the CS 2000 and a CMTS, the CS 2000 will allow new calls hosted by that CMTS to proceed without DQoS. The behavior of the multimedia terminal adapter (MTA) and CMTS determines whether new calls are attempted using best-effort service or whether they are torn down:

- Some MTA vendors allow calls to proceed as data calls (best-effort) and do not send a data-over-cable service interface specification (DOCSIS) authorization block to the CMTS. In this case, the CMTS

cannot recognize the call as a voice call and so it proceeds without managed quality of service.

- Other MTA vendors send the DOCSIS authorization block to the CMTS with no authorization key or gate-id. When this happens, the CMTS decides whether or not to allow calls to proceed.

When the DQoS connection is up, but the CS 2000 does not receive a DQoS gate-id from the CMTS, the CS 2000 will tear down a call.

GWC307

Log report GWC307 indicates an "Element Manager communication failure." EM indicates provisioned data mismatched in this unit, or EM is not responding, provisioned data loaded from local Flash. The alarm severity is Major.

Format

The format for log report GWC307 is as follows:

```
COMPACT06BT ** GWC307 JUL1 10:45:47 0028 TBL GWC Fault
  Location: GWC-3-UNIT-1
  NotificationID: 10
  State: Raise
  Category: Communications
  Cause: Communications subsystem failure
  Time: Jul 01 10:45:51 2003
  Component Id: GWC=GWC-3-UNIT-1;Version=PGC91AQ;Unit=unit_1;
  Software=NODE MTC
  Specific Problem: EM indicates provisioned data mismatched in this
  unit
  Description: Element Manager communication failure.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared with a Busy/RTS of GWC unit.

Restore communication with the CS 2000 GWC Manager. Determine if the CS 2000 GWC Manager is down and or disconnected. Determine if the GWC has been setup to use the wrong IP address for the CS 2000 GWC Manager at the CS 2000 SAM21 Manager.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC308

Log report GWC308 indicates a "Flash memory error." Erase of Flash sector failed. The alarm severity is Minor

Format

The format for log report GWC308 is as follows:

```
COMPACT2 * GWC308 JUL10 09:56:37 0675 TBL GWC Fault
  Location: GWC-0-UNIT-0
  NotificationID: 16
  State: Raise
  Category: Equipment
  Cause: Equipment Malfunction Time: Jul 10 10:07:23 2003
  Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
    Software=FLASH
  Specific Problem: Erase of Flash sector failed
  Description: Flash memory error.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by replacing the hardware.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC309

Log report GWC309 indicates that the number of the security associations (SA) that the system can support has been exceeded. The associated alarm severity is Minor.

Format

The format for log report GWC309 is as follows:

```
GWC309 AUG10 14:15:09 0674 TBL GWC Fault
  Location: GWC-12-UNIT-0
  Component ID: GWC=GWC-12-UNIT-0;Version=GN070BV;Unit=unit_0;
                Software=Signalling security
  Alarm Level: Minor
  Alarm Description: Security SAs are nearing capacity
  Category: Processing Error
  Alarm Time: 14:05:10 10-Aug-2004 EDT
  Probable Causes: Resource at or nearing capacity
  Specific Problem: SA nearing capacity
  System Uptime: 1 hours, 0 minutes, 45 seconds
```

Selected field descriptions

This log report has no selected fields.

Action

This log is associated with a minor information alarm. Report this alarm with details to your next level of support. Note that the alarm clears automatically as SA usage decreases.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC310

Log report GWC310 indicates "Excessive Security SA failures." The alarm severity is Major.

Format

The format for log report GWC310 is as follows:

```
COMPACT2 ** GWC310 JUL10 09:56:35 0673 TBL GWC Fault
  Location: GWC-0-UNIT-0
  NotificationID: 14
  State: Raise
  Category: Processing Error Cause: Underlying resource unavailable
  Time: Jul 10 10:07:23 2003
  Component Id: GWC=GWC-0-UNIT-
0;Version=PGT09BL;Unit=unit_0;Software=Signalling security
  Specific Problem: Excessive SA failures.
  Description: Excessive Security SA failures.
```

Selected field descriptions

This log report has no selected fields.

Action

Contact your next level of support. The alarm condition associated with this log clears automatically as SA failures decrease.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC311

Log report GWC311 indicates a Warning. "Provisioned GWC Profile not yet activated." The GWC Profile loaded into Flash will activate on the next reload.

Format

The format for log report GWC311 is as follows:

```
COMPACT06BT GWC311 JUL1 10:39:56 0022 TBL GWC Fault
Location: GWC-3-UNIT-0
NotificationID: 12
State: Raise
Category: Quality of Service
Cause: Configuration or customization error
Time: Jul 01 10:40:03 2003
Component Id: GWC=GWC-3-UNIT-0;Version=PGC91AQ;Unit=unit_0;
Software=CONFIG
Specific Problem: GWC Profile loaded into Flash will activate on
next reload.
Description: Provisioned GWC Profile not yet activated.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by reloading the GWC.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC312

Log report GWC312 indicates a QCA connection failure, either a major alarm (partial outage) or a critical alarm (total outage).

Format

The format for log report GWC312 is as follows:

```
COMPACT2 *** GWC312 JUN30 11:02:37 0586 TBL GWC Fault
  Location: GWC-0-UNIT-0
  NotificationID: 3
  State: Raise
  Category: Communications
  Cause: Communications subsystem failure
  Time: Jun 30 11:09:58 2003
  Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
  Software=QCAMTC
  Specific Problem: QCA connection <qca_47.142.130.70 Port # 20000> has
    failed - attempting recovery.
  Description: QCA connection failure
```

Selected field descriptions

This log report has no selected fields.

Action

No reports are lost since they are collected on a backup server.

- Ensure that the QCA contains the correct properties (port, IP address, etc). Check that the QCA is properly provisioned using the CS 2000 Management Tools.
- Use the ping command to see if you can reach the QCA server. If you cannot reach the server, there may be a problem in the network.
- Verify that there is no memory exhaustion on the QCA server.
- To bring up the links, restart the QCA application on the server.
- Try connecting to a QCA on another CS 2000 Management Tools server.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC398

Log report GWC398 is generated when the Management Tool server cannot communicate with a Gateway Controller card.

Format

The format for log report GWC398 is as follows:

```
MSH10_I06BR *** GWC398 JUN10 17:03:57 9872 TBL GWC Fault
Location: GWC-3-UNIT-1
NotificationID: 0
State: Raise
Category: Communications
Cause: Communications subsystem failure
Time: Jun 10 17:03:57 2003
Component Id: GatewayController
Specific Problem: SNMP Timeout
Description: CMT Unable to communicate with managed device
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC399

Log report GWC399 clears all other GWC logs.

Note: In the case of H.323 GWCs, this log report is generated only for H.323 gateways that contain 64 endpoints or greater.

Format

The format for log report GWC399 is as follows:

```
MSH10_IO6BR      GWC399 MAY26 13:38:30 0529 INFO GWC Fault
Location: GWC-2-UNIT-1
NotificationID: 6
State: Clear
Time: May 26 13:38:40 2003
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC501

Log report GWC501 indicates that there has been a connection fault between the GWC and the gateway which requires investigation.

Note: 'Gateway' is defined as small gateway (for example, Askey/Mediatrix line gateway, Arris/Motorola gateway, H.323 gateway with less than 64 endpoints).

Format

The format for log report GWC501 is as follows:

```
RTP4 GWC34      GWC501 JUN21 09:36:02 4767 PBSY GWC34_OrigGW35.rtp4.net
Reason: GW failed to respond to HeartBeat/Audit
```

Selected field descriptions

This log report has no selected fields.

Action

Verify the availability of the gateway and compare the configuration data at the gateway and the CS 2000 GWC Manager (IP address, protocol/version, etc).

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC502

Log report GWC502 indicates that service has been restored to the referenced gateway.

Format

The format for log report GWC502 is as follows:

```
RTP4 GWC34      GWC502 JUN21 09:36:11 4852 RTS      GWC34_OrigGW27.rtp4.net
Connection to remote gateway restored: GWC34_OrigGW27.rtp4.net
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC503

Log report GWC503 indicates that the gateway has requested that service become interrupted because of a fault condition on the gateway.

Format

The format for log report GWC503 is as follows:

```
RTP4 GWC32      GWC503 JUN21 10:41:56 9371 OFFL GWC32_OrigGW99.rtp4.net
Connection drop initiated by remote gateway: GWC32_OrigGW99.rtp4.net
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC600

Log report GWC600 is an information log for an H.323 failure. The log entry identifies the specific problem and describes the reason for the failure.

This log report recommends a set of actions that depend on the specific problem and reason for the problem.

Format

The format for log report GWC600 is as follows:

```
RTPG GWC11 GWC600 MAY21 14:54:47 <sequence number> INFO GWC Protocol Event
Category: Communication
Component Id: GWC=<GWC node/unit>;LINK=<gateway name>
Specific Problem: <specific problem>
Description: <reason for problem>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
sequence number	0000-9999	Four digit sequence number identifying a specific log entry.
GWC node / unit	Alpha-numeric text label	Identifies the GWC node and unit affected by the failure. Example: GWC-11-UNIT-0
gateway name	Alpha-numeric text label	Identifies the gateway connected to the GWC card affected by the failure condition. Example: BCM_RTPG1
specific problem	Text description	Identifies the H.323 failure condition.
reason for problem	Text description	Describes the specific reason for the failure.

Action

The following table describes the actions the user takes when an H.323 failure condition occurs.

Note:

GRQ = Gatekeeper request

RRQ = Registration request

ARQ = Admission request

URQ = Unregistration request

DRQ = Disengage request

RAS = Registration, admission and status

Actions associated with an H.323 failure (Sheet 1 of 4)

Specific problem	Description	Action
H323 GRQ rejected	Gateway Name Not Provisioned Note: A log with same description is generated for RRQ received with invalid GW name.	Ensure that the H.323 gateway name provisioned on the CS 2000 GWC Manager matches exactly with the gateway name provisioned using the H323 GW provisioning tool.
H323 GRQ rejected	Gateway IP Address Invalid Note: A log with same description is generated for RRQ received with an invalid source gateway IP address. In this case, the source IP address is the IP address in the ethernet frame. So, for gateways behind the NAT, the source IP address will be the NAT IP address. The RAS IP address is not part of the H.323 payload. If the H.323 gateway is not behind a NAT, the source IP will be the IP address of the H.323 gateway.	If the H.323 gateway is behind the NAT: - Ensure that the H.323 gateway IP address provisioned on the CS 2000 GWC Manager matches exactly the IP address of the NAT box. If the H.323 Gateway is not behind a NAT box: - Ensure that the H.323 gateway IP address provisioned on the CS 2000 GWC Manager matches exactly the IP address of the H323 gateway.

Actions associated with an H.323 failure (Sheet 2 of 4)

Specific problem	Description	Action
H323 GRQ rejected	Gateway Port Invalid Note: A log with same description is generated for an RRQ received with an invalid source gateway port. In this case, the source port is the source port address in the ethernet frame. So, for gateways behind a NAT, the source port is the port entry of the static bind at the enterprise NAT for the H323 gateway. It is not the RAS port which is part of the H323 payload. If the H323 Gateway is not behind a NAT, the source port will be the RAS port of the H323 gateway.	If the H.323 gateway is behind the NAT: - Ensure that the H.323 gateway port provisioned on the CS 2000 GWC Manager matches exactly the port entry of the static bind at the enterprise NAT for the H323 gateway. If the H.323 Gateway is not behind a NAT box: - Ensure that the H.323 gateway IP address provisioned on the CS 2000 GWC Manager matches exactly the IP address of the H323 gateway.
H323 GRQ rejected	Missing Mandatory RAS Address	No action needed. This log report is for information only.
H323 RRQ rejected	Incorrect Endpoint Identifier Syntax	No action needed. This log report is for information only.
H323 keepAlive RRQ rejected	Incorrect Endpoint Identifier Syntax	No action needed. This log report is for information only.
H323 RRQ rejected	Invalid Endpoint Identifier	No action needed. This log report is for information only.
H323 ARQ rejected	Invalid Endpoint Identifier	No action needed. This log report is for information only.
H323 RRQ rejected	D-Channel Not Provisioned	Ensure that the trunk datafill is provisioned correctly on the CS 2000 XA-Core and CS 2000 GWC Manager.

Actions associated with an H.323 failure (Sheet 3 of 4)

Specific problem	Description	Action
H323 RRQ rejected	D-Channel Out Of Service	Ensure that the D-channel associated with the H.323 gateway is in LO state at mapci, mtc, ttp, trks, pradch level on the CS 2000 Core before the H.323 gateway registers. This log can be cleared with a BSY/RTS of the D-channel associated with the H.323 gateway on the CS 2000 Core. Note: Trunk logs are also generated which are similar to PRI trunk logs. For example, H.323 gateway "BCM_RTPG" appears on the XA-Core as trunk name "RTPG_BCM_LOCAL" Refer to section Additional information on page 742 for examples of XA-Core logs.
H323 RRQ rejected	Table LTDATA Needs H323 Option	Check the datafill in Table LTDATA on the CS 2000 Core. The option PRI_IP_PROT H323 should be present for the D-channel associated with the H.323 gateway.
H323 RRQ rejected	Max Gateways Registered	No action needed. This log report is for information only. The CS 2000 GWC has reached the maximum limit for the number of H.323 gateways it can have registered simultaneously.
H323 ARQ rejected	B-Channel Resource Unavailable	Ensure that B-channels associated with the gateway are idle (IDL) at mapci, mtc, ttp, trks level on the CS 2000 XA-Core. This log can be cleared with a BSY/RTS of the B-channels associated with the H.323 gateway on the CS 2000 XA-Core. If all the B-channels associated with the H.323 gateway are call processing busy (CPB) at mapci, mtc, ttp, trks level on the CS 2000 XA-Core, then no action is needed. There is no B-channel available for the call. This log report is for information.

Actions associated with an H.323 failure (Sheet 4 of 4)

Specific problem	Description	Action
H323 RRQ rejected	No GWC Unit Active Running Note: A log with the same description will be generated if any RAS message (GRQ, RRQ, ARQ, URQ, DRQ) is received when the GWC unit is not active running. This log can be cleared with a BSY/RTS of GWC unit.	Ensure that the CS 2000 GWC is in active running state. This log can be cleared with a BSY/RTS of GWC unit.
H323 DRQ rejected	Request to Drop Non Existent Call	No action needed. This log report is for information only. This reports a disengage request for a call which is not active or non-existent.
H323 URQ rejected	Endpoint Not Registered	A RAS request is received from a H.323 gateway which is not registered on the CS 2000 GWC. Verify that the H.323 gateway is provisioned on the CS 2000 GWC.
H323 Call rejected	Codec Mismatch With CS2K	Ensure that at least one of the codecs provisioned on the H323 gateway matches the codec for the CS 2000 provisioned at the CS 2000 GWC Manager.
H323 Call rejected	Codec / Payload Mismatch With CS2K	Ensure that at least one of the codecs provisioned on the H323 gateway matches the codec for the CS 2000 provisioned at the CS 2000 GWC Manager. Ensure that the payload (packetization) time on the H323 gateway matches the payload (packetization) for the CS 2000 provisioned at the CS 2000 GWC Manager.
H323 Call rejected	H245 Tunneling Not Enabled On Gateway	Ensure that H.245 tunneling is enabled on the H.323 gateway.

Associated OM registers

This log report has no associated OM registers.

Additional information

This section provides examples of XA-Core logs relevant to

- Specific problem: H323 RRQ rejected
- Description: D-Channel Out Of Service.

Examples of XA-Core logs when the D-channel is manually busied (BSY):

```
RTPG * ISDN105 JUN16 21:45:44 2311 FLT PRA Sync Loss  
ISP = 0 GWC 11 PORT 0 CHNL 0
```

```
RTPG *** ISDN112 JUN16 21:45:44 2412 INFO PRA D-CHANNEL  
CRITICAL ALARM RTPG_BCM_LOCAL DCH=GWC 11 120 1 : OOS
```

```
RTPG *** TRK103 JUN16 21:45:49 2917 FLT GROUP_ALARM  
RTPG_BCM_LOCAL 100% BUSY
```

Examples of XA-Core logs when the D-channel is returned to service (RTS) and the gateway registers with GWC:

RTPG ISDN118 JUN16 21:46:52 6654 INFO PRA Sync Established
ISP = 0 GWC 11 Port 0 Chnl 0

RTPG TRK104 JUN16 21:46:56 7462 INFO GROUP OK
RTPG_BCM_LOCAL

PM180

Log report PM180 appears when the system encounters a software exception. A software exception occurs when software is not used correctly. Operating company personnel use log report PM180 to identify and correct software errors. A software exception that relates to hardware can also generate log report PM180.

The PM subsystem generates this report when a software condition occurs. This software condition affects normal operation of the DMS or the peripherals of the DMS. Formats 3 and 4 supply information on a PM EXCEPTION REPORT. Format 5 identifies software exceptions in the remote line concentrating module with extended distance capability (RLCM-EDC) and the universal edge 9000 (UE9000).

Format

The format for log report PM180 is as follows:

```
PM180 mmmdd hh:mm:ss ssdd TBL PM EXCEPTION REPORT
      pmid UNIT n: acttxt
      TASKID : taskid, TIME: hhhhhhhh, COMID: comid
      TEXT: swerrtxt hh hh hh hh hh hh hh
      CONTEXT TERMINAL: TID=(nodenum,termnum), EXTBYTE=n,
      AGENT=CKT trkid
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
TBL PM EXCEPTION REPORT	Constant	Indicates a PM exception report.
pmid	Symbolic text	Identifies the affected PM
UNIT	Integer (0 or 1)	Identifies the PM unit that generates the report
acttxt	Act	Indicates that the PM unit is active (Act). Not provided for digital line module (DLM).
	Inact	Indicates that the PM unit is inactive (Inact). Not provided for DLM.
TASKID	Symbolic text	Provides identification for suspect task

Field	Value	Description
TIME	Hex (0000-FFFF)	Indicates time that exception occurred
COMID	Hex (0000-FFFF), Character string	Provides communication port identification. Not provided for DLM.
swerrtxt	Character string	Provides the reason for the exception.
hhhh	Hex (0000-FFFF)	The 14 hexadecimal characters display contents of process status word for DLMs. The hexadecimal characters display more than 14 characters in the hhhh format to display the following: • contents of process status word • different registers • other information used in troubleshooting
CONTEXT TERMINAL	Constant	Indicates the information that follows applies to the terminal involved in the transaction that produced the exception condition. Not provided for DLM.
TID	Integers	Provides the node number and terminal number for terminal identification. Not provided for DLM.
EXTBYTE5000	0 or 1	Identifies the extension byte of the call involved in the exception condition. Electronic business sets use the extension byte to distinguish directory number (DN) keys. For 500 series and 2500 series sets and for trunks, the field does not apply and is set to zero. Not provided for DLM.
AGENT	Symbolic text	Provides identification for context terminal equipment. Not provided for DLM.
TEXT	CMR CARD TROUBLE	Indicates the system detected a problem on the CLASS modem resource (CMR) card. The system attempts to reset the card. Report that this log occurred.
	Character string or blank	Provides additional information for operating company personnel to isolate problems
hhhh	Hex (0000-FFFF)	Provides a dump of information for operating company personnel to use
Text string	Alphabetic	Provides the reason of the exception

Field	Value	Description
Software Exception	Character string	Provides the reason for the log
Processor ID	MP, CP, or PP	Indicates that the processor in the RLCM-EDC or the UE9000 that generates the report is one of the following: • master processor • control side (C-side) • peripheral processor (P-side)
Task ID	Symbolic text	Identifies the ID of the RLCM-EDC or the UE9000 task that generated the log
Time	00 00-2359	Indicates the RLCM-EDC or the UE9000 time of exception
Data	Hex (0000-FFFF)	Identifies the type of hardware exception
site	0000-ZZZZ	Identifies the site to the ILDR
frame	0 through 99	Identifies the line concentrating module (LCM) frame number
drawer	0 through 19	Identifies the ILDR drawer number in the LCM
swerrdata	Character string	Provides the exception data from the software error text (swerrtxt)

Action

Attempt to interpret swerrdata character string to determine the cause of the exception. If you are not able to interpret swerrdata, contact the next level of support.

If the system indicates a hardware problem, perform diagnostic and maintenance procedures on the suspect equipment.

If the character string indicates a software error, retain the log report for trend analysis. There is no action required.

For formats 3 and 4, save all reports generated during the 5 min before the subsystem generated log report PM180 report. Contact the next level of support.

For format 5, save all reports generated during the 6 h before the subsystem generated log report PM180. Contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

PM185

Log report PM185 gives the trace back of the last trap that caused a peripheral to start again.

Format

The format for log report PM185 is as follows:

```
PM185 date time seqnbr TBL PM TRAP pmtyp pmnbr
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
pmtyp	alphabetic	The peripheral module type.
pmnbr	0000-9999	The peripheral module number.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

PM777

Log report PM777 is generated when the software detects a hardware defect. This log indicates the source of the defect.

Format

The format for log report PM777 is as follows:

```
PM777 mmmdd hh:mm:ss ssdd INFO SUSPECTED H/W FAULT pmid
unit no.
PP TIME: hh:mm:sshs
ERROR STATE: xxxxxxxxxxxxxxxxxxxx
SUSPECTED CARD(S):
SITE FLR RPOS BAY ID SHF DESCRIPTION SLOT EQPEC
host fl# row# bay id sh# frame# slot# cardid
DATA: xx xx xx xx xx xx xx
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
INFO SUSPECTED H/W FAULT	Symbolic text	Indicates the PM with the suspected hardware defect.
unit no.	Integers	Indicates the unit number.
PP TIME	Integers	Indicates the time of the defect.
ERROR STATE	Symbolic text	Indicates the error state.
SUSPECTED CARD(S)	Numeric	Indicates the suspect cards.
DATA	Alphanumeric	Indicates more information about the defect.

Action

Follow standard maintenance procedures.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

Troubleshooting APS login problems

This procedure enables you to identify and solve the following common problems that prevent you from logging in to the APS:

- URL in the browser address window is incorrect
- keyboard “Caps Lock” is on
- Oracle database is down
- web server is not running
- APS application software was removed or is not installed

Troubleshooting APS login problems

At your console

- 1 Verify that the URL in your browser address window is correct. The URL will be of the format: `http://<hostname or IP address of the APS>:8080/aps/`

If	Do
the URL is correct	step 3
the URL is incorrect	Correct the URL entry in the browser. Go to step 2

- 2 Try to log in to the APS.

If	Do
you are able to log in to the APS	step 28
you are unable to log in to the APS	step 3

- 3 Ensure that “Caps Lock” is not enabled on your keyboard.

If	Do
“Caps Lock” is enabled	Press the “Caps Lock” key on your keyboard. Go to step 4
“Caps Lock” is not enabled	step 5

- 4 Try to log in to the APS.

If	Do
you are able to log in to the APS	step 28
you are unable to log in to the APS	step 5

In a telnet connection to the APS server

5 Open an xterm window and log in using the “maint” login and password.

6 Become the “root” user by entering:

```
su - root
```

7 Determine whether the APS login page is accessible.

If	Do
the APS login page is accessible	step 8
the APS login page is not accessible	step 19

8 Ensure that the Oracle database is online by entering the following command:

```
/opt/servman/bin/servman query -status -g  
DATABASE -v
```

The display will indicate that the Oracle processes, listed at the end of the display (that is, entries in the display that begin with “oracle <pid>”), are running.

If	Do
the displayed Oracle processes are not running	step 9
the displayed Oracle processes are running	step 13

9 Restart the Oracle database by entering the following command:

```
/opt/servman/bin/servstart DATABASE
```

10 Kill the APS server process and let the server restart automatically, by entering the following command:

```
/opt/uas/aps/scripts/killDbServer.sh
```

A message eventually displays indicating that the server is restarting.

11 Enter the following command to check the status of the database:

```
/opt/servman/bin/servman query -status -g  
DATABASE -v
```

The display will indicate that the Oracle processes, listed at the end of the display (that is, entries in the display that begin with “oracle <pid>”), are running.

If	Do
the displayed Oracle processes are running	step 12
the displayed Oracle processes are not running	step 27

12 Try to log in to the APS.

If	Do
you are able to log in to the APS	step 28
you are unable to log in to the APS	step 13

13 Ensure that you can connect to the Oracle database by entering the following command:

sql

An “sql” prompt will display.

If	Do
the sql prompt does not display	step 14
the sql prompt does display	step 26

14 Determine whether you already restarted the Oracle database once before during this procedure.

If	Do
you have already restarted the database once before	step 27
you have not already restarted the database once before	step 15

15 Restart the Oracle database by entering the following command:

/opt/servman/bin/servstart DATABASE

16 Kill the APS server process and let the server restart automatically, by entering the following command:

/opt/uas/aps/scripts/killDbServer.sh

A message eventually displays indicating that the server is restarting. This may take from 2 to 5 minutes.

- 17** Enter the following command to check the status of the database:
- ```
/opt/servman/bin/servman query -status -g DATABASE -v
```
- The display will indicate that the Oracle processes, listed at the end of the display (that is, entries in the display that begin with "oracle <pid>"), are running.*
- | If                                             | Do                      |
|------------------------------------------------|-------------------------|
| the displayed Oracle processes are running     | step <a href="#">18</a> |
| the displayed Oracle processes are not running | step <a href="#">27</a> |
- 18** Try to log in to the APS.
- | If                                  | Do                      |
|-------------------------------------|-------------------------|
| you are able to log in to the APS   | step <a href="#">28</a> |
| you are unable to log in to the APS | step <a href="#">27</a> |
- 19** If the correct IP address of the APS server is entered in the browser address window, but the login page is not accessible, an Application Launch Point page will display.
- | If                                                 | Do                      |
|----------------------------------------------------|-------------------------|
| the Application Launch Point page displays         | step <a href="#">21</a> |
| the Application Launch Point page does not display | step <a href="#">20</a> |
- 20** Enter the following command to start the Apache server:
- ```
/opt/servman/bin/servstart WEBSERVICES
```
- Messages that indicate the Apache server has started display.*
- 21** Verify that the APS software packages have been installed by entering the following command:
- ```
pkginfo | grep aps
```
- | If                                                            | Do                                                                                  |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------|
| a list of the required APS software packages displays         | step <a href="#">22</a>                                                             |
| a list of the required APS software packages does not display | You will need to install the required APS packages. Go to step <a href="#">27</a> . |



- 22** Enter the following command to check the status of the database:
- ```
/opt/servman/bin/servman query -status -g DATABASE -v
```
- The display will indicate that the Oracle processes, listed at the end of the display (that is, entries in the display that begin with "oracle <pid>"), are running.*
- | If | Do |
|--|-------------------------|
| the displayed Oracle processes are running | step 26 |
| the displayed Oracle processes are not running | step 23 |
- 23** Restart the Oracle database by entering the following command:
- ```
/opt/servman/bin/servstart DATABASE
```
- 24** Kill the APS server process and let the server restart automatically, by entering the following command:
- ```
/opt/uas/aps/scripts/killDbServer.sh
```
- A message eventually displays indicating that the server is restarting. This may take from 2 to 5 minutes.*
- 25** Enter the following command to check the status of the database:
- ```
/opt/servman/bin/servman query -status -g DATABASE -v
```
- The display will indicate that the Oracle processes, listed at the end of the display (that is, entries in the display that begin with "oracle <pid>"), are running.*
- | If                                             | Do                      |
|------------------------------------------------|-------------------------|
| the displayed Oracle processes are running     | step <a href="#">26</a> |
| the displayed Oracle processes are not running | step <a href="#">27</a> |
- 26** Try to log in to the APS.
- | If                                  | Do                                                                        |
|-------------------------------------|---------------------------------------------------------------------------|
| you are able to log in to the APS   | step <a href="#">28</a>                                                   |
| you are unable to log in to the APS | It may be necessary to reboot the server. Go to step <a href="#">27</a> . |

- 27**    Contact your next level of support.
- 28**    You have completed this procedure.

---

## Changing the APS Oracle account password

---

When the APS is installed, a default password is assigned to the Oracle account. This procedure enables you to change the default password, for added system security.

### Changing the APS Oracle account password

#### *In a telnet connection to the APS server*

- 1 Open an xterm window and log in using the “root” login and password.
- 2 If you are unsure whether the password has been changed, obtain the current password by entering the following command:

```
getNTDBpasswd.ksh
```

*The system displays the current Oracle account password.*

- 3 Become the “Oracle” user by entering the following command:

```
su - oracle
```

- 4 Perform the following steps to change the Oracle account password:

- a Enter the following command to run the script that enables you to change the password:

```
/usr/ntdb/uas/scripts/setNTDBpasswd.ksh
```

- b At the prompt, enter the current APS Oracle account password.

**Note:** This is the password that you displayed in step 2.

- c At the prompt, enter the new APS Oracle account password.

- d At the prompt, reenter the new APS Oracle account password.

*The system changes the password in UNIX and in the Oracle database.*

- e Enter the following command to exit from the Oracle user account:

```
exit
```

*This causes you to become the “root” user again.*

- 5 Restart the APS processes by entering the following command:

```
/opt/uas/aps/scripts/killDbServer.sh
```

*A message eventually displays indicating that the server is restarting.*

- 6** Enter the following commands to complete the password change:

```
cd /
```

```
. /etc/profile
```

```
. ./profile
```

- 7** You can now check the password change you have made by entering the following command:

```
getNTDBpasswd.ksh
```

*The system displays the current Oracle account password.*

- 8** You have completed this procedure.

## Increasing the size of a logical volume

### Purpose

Use this procedure to allocate more disk space to a logical volume.

### Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display other information about a user or role group, review the procedures in the following table.

#### Procedures related to this procedure

| Procedure                                         | Document                                                              |
|---------------------------------------------------|-----------------------------------------------------------------------|
| Logging in to the CS 2000 Core Manager            | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |
| Displaying information about a user or role group | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |

### Application

**DANGER**

**Increasing the size of a logical volume can limit future software upgrade capability**

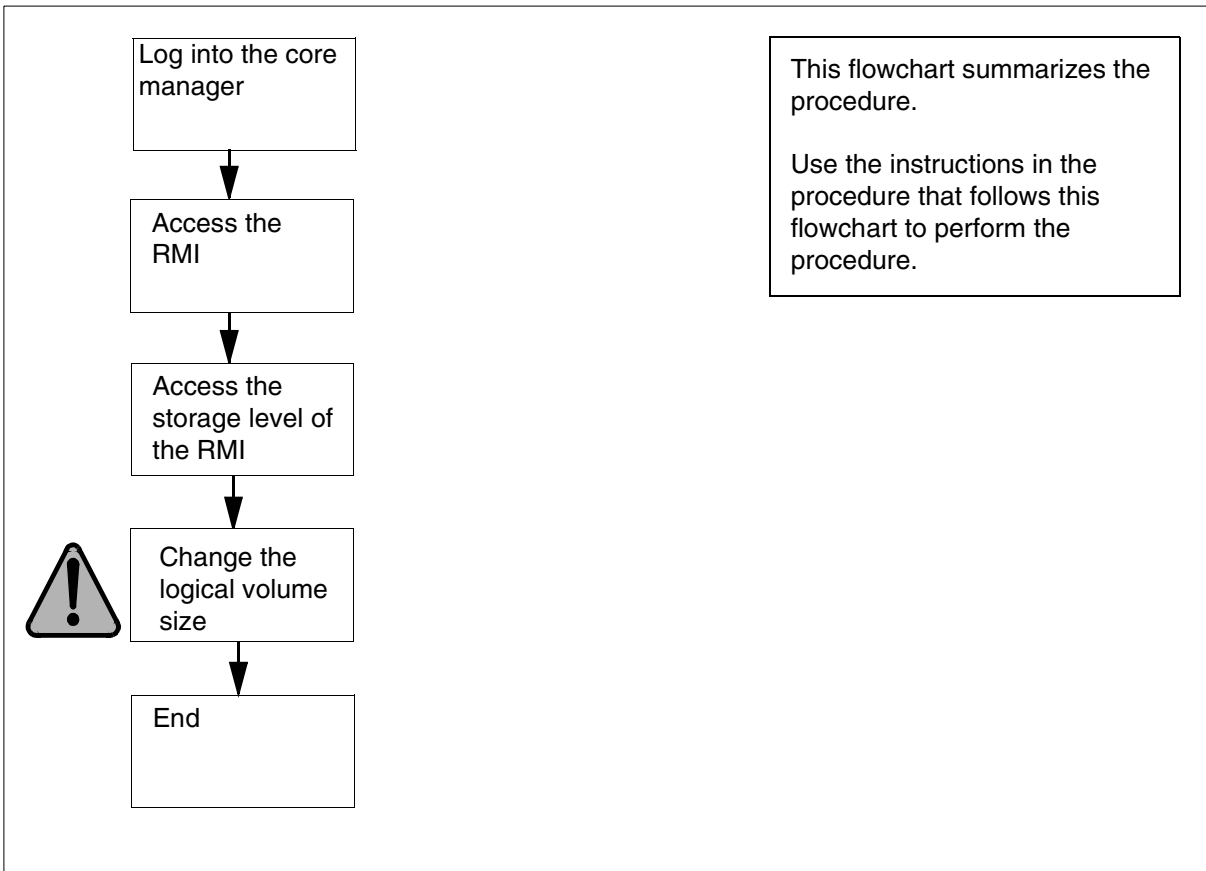
core manager logical volumes are pre-engineered to sizes that are adequate for Nortel customers. Do not increase the size of a logical volume unless absolutely necessary.

If you need to change the size of a logical volume, do so only with the assistance of Nortel Technical Assistance and Support. Failure to follow this warning may jeopardize future software upgrade capability.

### Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the tasks.

## Summary of increasing the size of a logical volume



### Increasing the size of a logical volume

#### *At the local VT100 console*

- 1 Log into the core manager as a user authorized to perform config-admin actions.
- 2 Access the top menu level of the remote maintenance interface (RMI):  
**# sdmmtc**
- 3 Access the system (Sys) menu level of the RMI:  
**> sys**
- 4 Access the storage menu level of the RMI:  
**> storage**

*Example response:*

```

Volume Group Status Free (MB)
rootvg mirrored 1932
datavg mirrored 7760

Logical Volume Location Size (MB) %
full/threshold 1 / rootvg 88
11/ 80
2 /usr rootvg 600 28/ 90
3 /var rootvg 200 7/ 70
4 /tmp rootvg 24 5/ 90
5 /home rootvg 304 11/ 90
6 /sdm rootvg 504 23/ 90
7 /data datavg 208
6/ 80

```

Logical volumes showing: 1 to 7 of 7

**Note:** The example response only shows part of the information displayed at the storage menu level of the RMI.

- 5 Determine if there is un-allocated disk space that can be used to increase a logical volume.

| If there is           | Do                      |
|-----------------------|-------------------------|
| enough disk space     | step <a href="#">6</a>  |
| not enough disk space | step <a href="#">10</a> |

- 6 Identify the logical volume to increase in size. Record the volume name of the logical volume on the left of the System menu of the RMI.

7

**ATTENTION**

A logical volume on the core manager must never reach 100% full. System behavior cannot be predicted when a logical volume reaches 100% full.

Change the size of the logical volume:

**> change lv /<logical\_vol> <Mbyte>**

where

**<logical\_vol>**

is the name of the logical volume

**<Mbyte>**

is the size in Mbytes to be added to the logical volume. The size must be less than the amount of un-allocated disk space.

*Example input:*

**> change lv /home 48**

*Example response:*

Expanding Volume /home

Expanding Volume /home - Command complete

**Note:** The core manager can round the new size to the nearest 8-, or 16-Mbyte increment.

- 8** For a 4 Gbyte disk, add 8- or 16-Mbyte multiples. When the logical volume is created, the operating system determines the multiple that has to be used.
- 9** If the occupancy level of the specified logical volume has exceeded its alarm threshold, contact your system administrator to assess the current condition of the logical volume.
- 10** You have completed this procedure.



---

## Configuring the SESM server application

---

### Application

Use this procedure to configure the SESM server application.

#### ATTENTION

Only perform this procedure if you installed an HTTPS certificate after the CS2M software was installed or upgraded.

### Prerequisites

Prior to performing this procedure, obtain the following information:

- the IP address of the CS 2000 Management Tools server
- the market for which you are configuring this application (North America or International)

**Note:** Only the root user can perform this procedure.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Telnet to the server by typing  
    > **telnet <server>**  
    and pressing the Enter key.  
    where  
        **server**  
        is the IP address or host name of the CS 2000  
        Management Tools 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 Execute the configuration script by typing  
`# configure`  
and pressing the Enter key.

*Example response*

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 -

- 6 Enter the number next to the "SESM common configuration" option in the menu.

*Example response*

SESM common configuration

SDM IP : 47.123.456.78

CM CLLI : OFFICE3

- 7 When prompted, enter the IP address of the CS 2000 Management Tools server, or press the Enter key to accept the default if one is specified.
- 8 When prompted, enter the number next to the market for which you are configuring the SESM server application.  
The system displays the information you entered for confirmation.

- 9 When prompted, confirm the information by typing  
**y**  
and pressing the Enter key.  
The system executes the command, and returns you to the  
SESM configuration main menu.
- 10 Exit “SESM configuration” by typing  
`select - x`  
and pressing the Enter key.
- 11 You have completed this procedure.



---

## Viewing SESM configuration settings

---

### Application

Use this procedure to view the configuration settings for the Succession Element and Subelement Manager (SESM) server application and determine what the current setting for the CM CLI is.

### Prerequisites

You need the root user ID and password to log in to the server where the CS 2000 Management Tools reside.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Telnet to the server where the CS 2000 Management Tools reside by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the server where the CS 2000 Management Tools reside
- 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 Change directory by typing  

```
cd /opt/nortel/NTsesm/admin/bin
```

and pressing the Enter key.

- 6** Execute the configuration script by typing

```
./configure
```

and pressing the Enter key.

*Response*

```
SESM configuration
```

```
1 - SESM common configuration (IP addresses,
Market, CM CLLI)
```

```
2 - SESM database tools
```

```
3 - SESM related applications configuration
(MG9K, LMM)
```

```
4 - SESM provisioning configuration
```

```
5 - SESM logging configuration (syslog, sesm
debug log)
```

```
6 - view sesm configuration settings
```

```
X - exit
```

```
select -
```

- 7** Select the “view sesm configuration settings” option by typing

```
select - 6
```

and pressing the Enter key.

- 8** Take note of the CM CLLI. If you need to change it, refer to procedure “Setting the CS 2000 CLLI on the Sun server” in the ATM/IP solution-level Configuration Management document, NN100409-500, if required.

- 9** Exit SESM configuration by typing

```
select - x
```

and pressing the Enter key.

- 10** You have completed this procedure.

---

## Setting the CS 2000 CLI on an SSPFS-based server

---

### Application

The CM CLI is automatically retrieved from the Communication Server 2000 (CS 2000) through the SDM IP address. Use this procedure to rediscover the CM CLI on a Succession Server Platform Foundation Software (SSPFS)-based server when the SDM IP has already been configured. The steps to configure the SDM IP are also provided in the event it has not already been configured.

**Note:** The CM CLI can be configured or unconfigured on an SSPFS-based server that hosts the Core Billing Manager (CBM), but cannot be configured or unconfigured on an SSPFS-based server that hosts the following components:

- CS 2000 Management Tools and Audio Provisioning Server (APS)
- CS 2000 Management Tools, Integrated Element Management System (EMS), or both
- Media Gateway 9000 Manager

To set the CM CLI on an SSPFS-based server that hosts the CBM, refer to the CBM Configuration Management document, NN10353-511.

### Prerequisites

Have the SDM IP address on hand in the event it is not already configured.

### Action

Perform the following steps to complete this procedure.

#### ***At your workstation***

- 1 Log in to the server by typing  
    `> telnet <server>`  
    and pressing the Enter key.  
    where  
        **server**  
        is the IP address or host name of the SSPFS-based server on which you are setting the CS 2000 CLI
- 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.

*Response*

Command Line Interface

- 1 - View
- 2 - Configuration
- 3 - Other

X - exit

select -

- 6 Enter the number next to the "Configuration" option in the menu.

*Example response*

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 -



- 7 Enter the number next to the “OAMP Application Configuration” option in the menu.

*Example response*

```
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-discover 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 -

- 8 Enter the number next to the “cmClli\_rediscovery” option in the menu.

*Example response*

```
=== Executing "cmClli_rediscovery"
```

```
Retrieve CM CLLI by SDM IP <ip address>. Please
wait.....
```

```
CM CLLI old value: TESTCLLI
CM CLLI new value: TESTCLLI
CM CLLI has not changed.
```

```
=== "cmClli_rediscovery" completed successfully
```

| If the system response                 | Do                      |
|----------------------------------------|-------------------------|
| provides the CM CLLI value             | step <a href="#">12</a> |
| indicates the SDM IP is not configured | step <a href="#">9</a>  |

- 9 Enter the number next to the “sdm\_conf” option in the menu.

*Example response*

```
Enter the ip address of the SDM []
```

- 10** When prompted, enter the SDM IP address.

*Example response*

Retrieving CM CLLI. Please wait.....

SDM IP: 45.123.456.89

CM CLLI: TESTCLLI

Enter "ok" to commit changes

Enter "quit" to exit

Enter anything else to re-enter settings

- 11** When prompted, commit the changes if acceptable by typing

**ok**

and pressing the Enter key.

- 12** 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.

- 13** Log out and log back in to the server to reflect the CLLI environment changes as follows:

- a** Exit the root user level by typing

# **exit**

and pressing the Enter key.

- b** Exit the maint user level by typing

\$ **exit**

and pressing the Enter key.

- c** Log in to the server by typing

> **telnet <server>**

and pressing the Enter key.

where

**server**

is the IP address or host name of the SSPFS-based server

- d When prompted, enter your user ID and password.

**Note:** If the Network Patch Manager (NPM) server application is running on this SSPFS-based server, you must stop it and start it now. If required, refer to procedures “Stopping the NPM server application” and “Starting the NPM server application” in the document titled *ATM/IP Security and Administration*, NN10402-600.

- 14 You have completed this procedure.



---

## Changing the Oracle user password on an SSPFS-based server

---

### Application

Use this procedure to change the default Oracle passwords on a Succession Server Platform Foundation Software (SSPFS)-based server.

**Note:** Refer to procedure [Changing the APS Oracle account password on page 759](#), to change the default password.

#### ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SSPFS-based server  
**Note:** In a two-server configuration, log in to the active server using its physical IP address.
- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing  
`$ su -`  
and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change to the Oracle user by typing  
`# su - oracle`  
and pressing the Enter key.
- 6 Change the password by typing  
`$ /opt/nortel/sspfs/db/pfsora_set_pwd <userID>`  
and pressing the Enter key.

Where

**userID**

is the user ID of the Oracle user

Example response:

Enter new password for user SYSTEM:

- 7 When prompted, enter the new password for the system.

*Example response:*

Re-enter new password:

- 8 When prompted, enter the password a second time to confirm the password.

*Example response:*

Please wait...

Successfully changed password for Oracle user  
SYSTEM

**Note:** The command takes approximately 15 to 20 seconds to execute.

You have completed this procedure.

# Powering up the network

---

## Purpose of this procedure

### ATTENTION

If your network uses a Geographically Survivable configuration, refer to “Geographic survivability” in *Carrier Voice Over IP Disaster Recovery Procedures*, Nn10450-900.

This procedure details the sequence of steps necessary to power up all of the network elements in the office. Not all network elements covered in this procedure will apply to your office. The following network elements are covered by this procedure:

- XA-Core
- 3rd Party Core
- Message Switch
- ENET
- Ethernet Routing Switch 8600
- LPP
- SDM, CS 2000 Core Manager, or Core and Billing Manager
- Integrated EMS
- CS 2000 Management Tools
- MG 9000 Manager
- RTP Media Portal Manager
- SAM21 shelf and cards
- CICM
- USP
- Media Gateway 15000/7400 or Multiservice Switch 15000/7400
- MDM workstation
- SPM, MG 4000, IW-SPM, DPT-SPM
- MCS servers
- RTP Media Portal
- MS 2000 Series or UAS

- Packet Media Anchor
- MG 9000

### **When to use this procedure**

Use this procedure in the event of a power outage. This outage may have been planned or unplanned.

### **Prerequisites**

This procedure has the following prerequisites:

- This task requires more than one person to perform, as some steps are performed in parallel.
- The power recovery sequence can only be started when the AMP reading on SPDC-0 reaches 0.

### **Action**

This procedure contains a summary flowchart and a list of steps. Use the flowchart to review the procedure. Follow the steps to perform the recovery task.



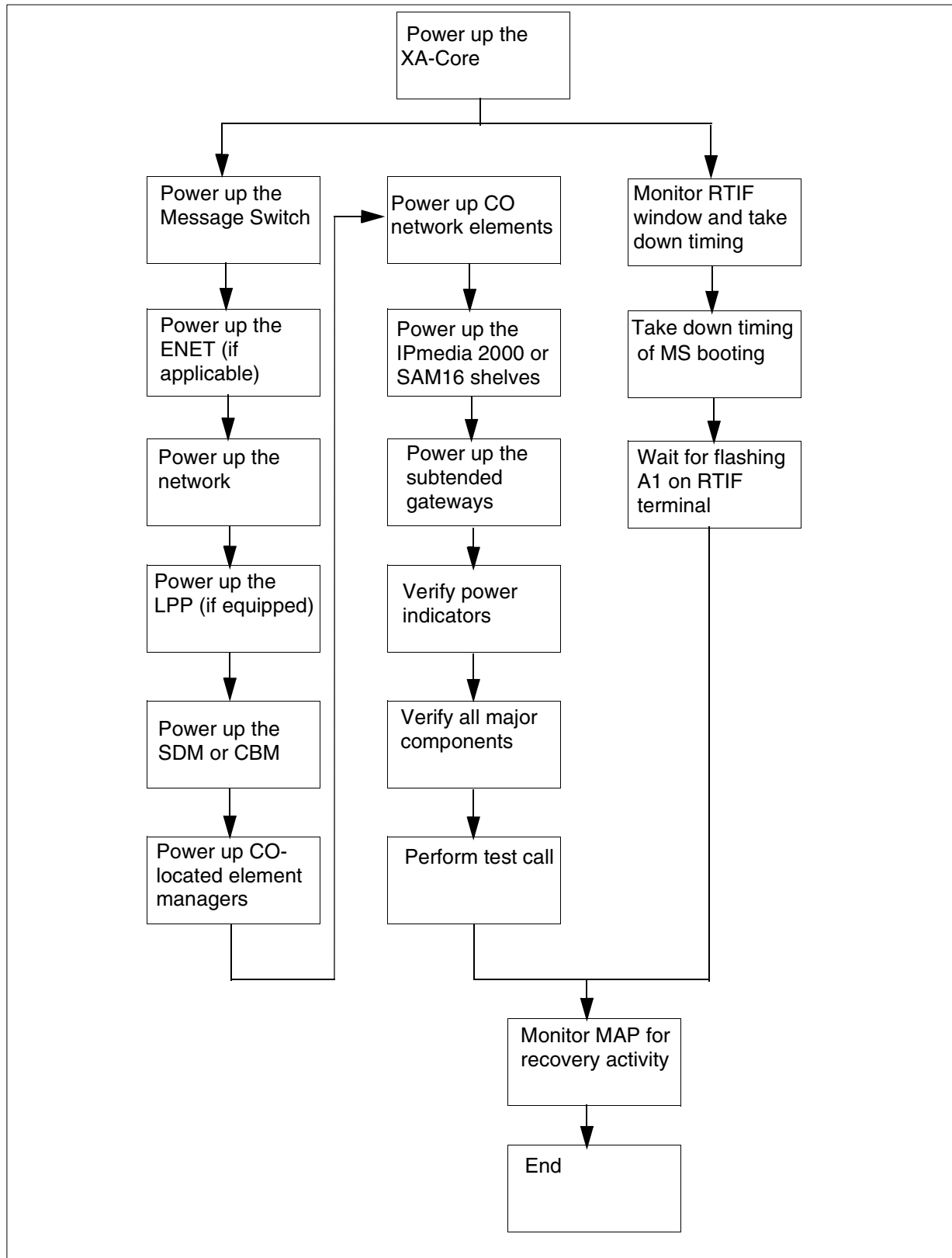
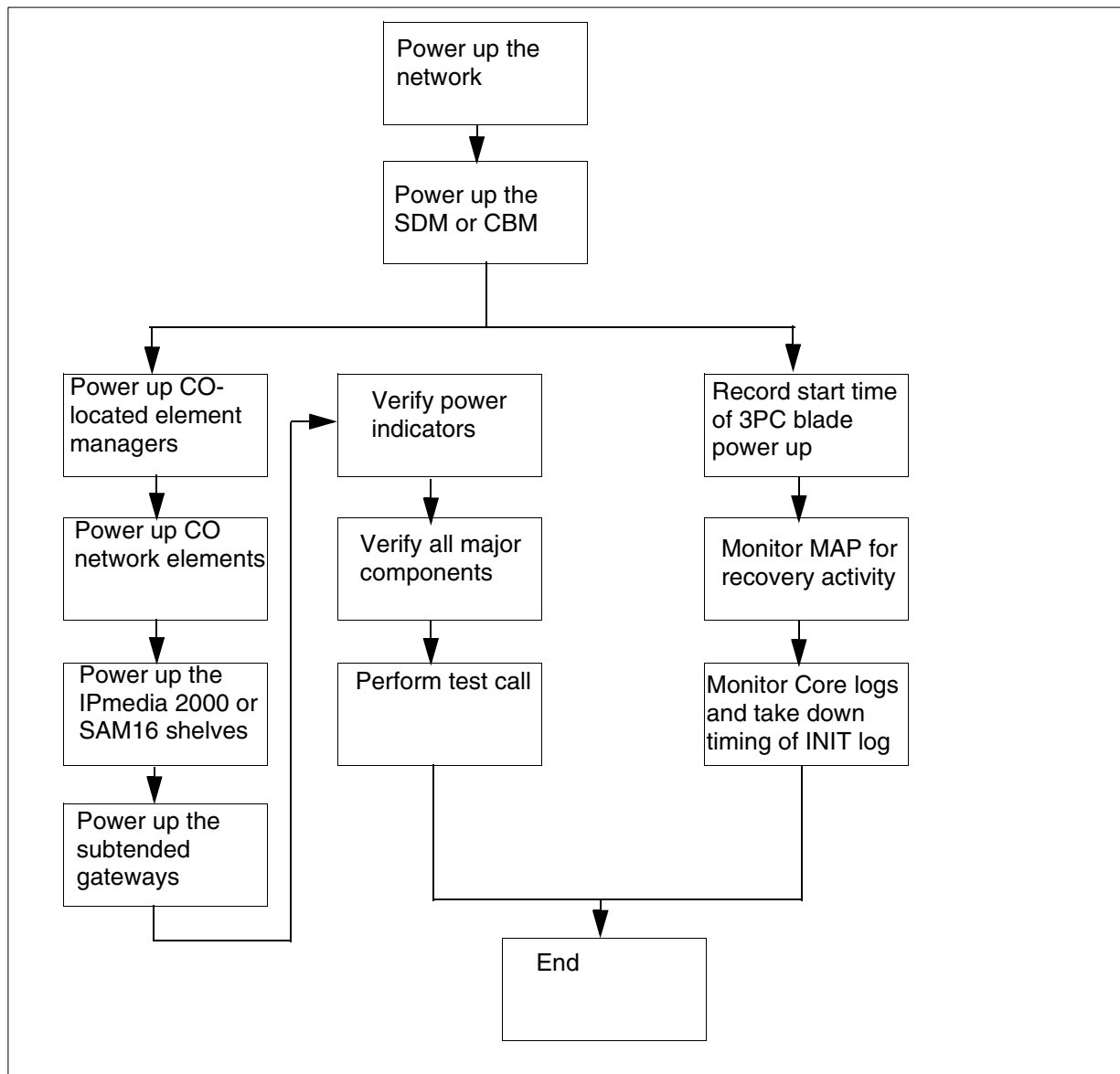
**Figure 1 Summary of procedure for an XA-Core-based office**

**Figure 2 Summary of procedure for a CS 2000-Compact-based office*****In the network office***

- 1 Determine if you are powering up a CS 2000 or CS 2000-Compact-based office.

| <b>If you are powering up a</b> | <b>Do</b>              |
|---------------------------------|------------------------|
| CS 2000-based office            | step <a href="#">2</a> |
| CS 2000-Compact-based office    | step <a href="#">9</a> |

- 2 Power up the XA-Core. Refer to [Powering up the XA-Core on page 789](#).
- 3 Perform steps 4 and 5 in parallel.
- 4 Power up the network elements and element managers.
  - a Power up the Message Switch and ENET (if equipped).  
Refer to [Powering up the Message Switch on page 817](#) and [Powering up the Enhanced Network on page 823](#).
  - b Power up the IP network, including the Ethernet Routing Switch 8600 and the IP Switches.  
Refer to [Powering up a Ethernet Routing Switch 8600 on page 837](#).
  - c Power up the LPP (if equipped).  
Refer to [Powering up the Link Peripheral Processors on page 839](#).
  - d Power up the SDM or CBM.  
For the SDM, refer to [Powering up the SDM on page 859](#). For the CBM, refer to [Powering up a T1400 or N240 server on page 861](#).
  - e If equipped, power up the DNS server. Refer to the hardware documentation for your server for detailed instructions.
  - f

**ATTENTION**

Wait at least 5 minutes between each step from [f](#) to [k](#).

Power up the CO located element managers, such as the Integrated EMS, CS 2000 Management Tools, and MG 9000 Manager.

Refer to [Powering up a T1400 or N240 server on page 861](#)

- g If equipped, power up the RTP Media Portal Manager.  
Refer to [Powering up the RTP Media Portal Manager on page 863](#).
- h Power up the CO network elements, including the SAM21 SCs, GWCs, Session Server, Policy Controller, CICM, USP, Multiservice Switch 15000/7400, Media Gateway 15000/7400, and SPMs.

Refer to the following procedures:

- [Powering up the SAMF frame on page 865](#)
- [Powering up a USP on page 893](#)
- [Powering up a Media Gateway/Multiservice Switch 15000 on page 907](#)
- [Powering up a Media Gateway/Multiservice Switch 7400 on page 909](#)
- [Powering up the MDM workstation on page 911](#)
- [Powering up an SPM device on page 913](#)

- i If equipped, power up the MCS servers and/or RTP Media Portal.

Refer to [Powering up the MCS servers on page 915](#) and [Powering up an RTP Media Portal on page 919](#).

- j Power up the shelves that house the MS 2000 Series/UAS devices and Packet Media Anchor.

If your system uses an MS 2000 Series device or Packet Media Anchor, refer to [Powering up the IPmedia 2000 shelves on page 921](#). If your system uses a UAS, refer to [Powering up the SAM16 shelves on page 923](#).

- k Power up the subtended gateways, such as the MG 9000 and MTA.

For the MG 9000, refer to [Powering up an MG 9000 device on page 925](#).

For other third party devices, refer to the documentation for your hardware.

- l Proceed to step [6](#) after completing this step and step [5](#).

**5** Collect XA-Core dead office recovery data.

- a During the power up sequence, monitor the RTIF window until Core booting is complete. Take down the timing.
- b MS booting should start next. Allow the booting to complete before proceeding to the next step. Take down the timing.
- c Restart reload should start. Wait until you see the flashing A1 on the RTIF terminal before proceeding.
- d Proceed to step [6](#) after completing this step and step [4](#).

**6** From the operator terminal, type

```
>priority on; mapci;mtc;srstatus
```

and press the Enter key.

Check the MAP banner and monitor recovery activity. They should have critical alarms that indicate the autonomous Network Elements recovery.

- 7 Reverify all the power indicators on the Network Elements.
- 8 Go to step [15](#).
- 9 Power up the IP network, including the Ethernet Routing Switch 8600 and the IP switches.  
Refer to [Powering up a Ethernet Routing Switch 8600 on page 837](#).
- 10 Power up the SDM or CBM.  
For the SDM, refer to [Powering up the SDM on page 859](#). For the CBM, refer to [Powering up a T1400 or N240 server on page 861](#).
- 11 If equipped, power up the DNS server. Refer to the hardware documentation for your server for detailed instructions.
- 12 Perform steps [13](#) and [14](#) in parallel.
- 13 Power up the remaining network elements by performing the following steps.

**a**

**ATTENTION**

Wait at least 5 minutes between each step from [a](#) to [f](#).

Power up the CO located element managers, such as the Integrated EMS, CS 2000 Management Tools, and MG 9000 Manager.

Refer to [Powering up a T1400 or N240 server on page 861](#)

- b** If equipped, power up the RTP Media Portal Manager.

Refer to [Powering up the RTP Media Portal Manager on page 863](#).

- c** Power up the CO network elements, including the SAM21 SC, 3PC cards, GWCs, Session Server, CICM, USP, IW-SPM, Multiservice Switch 15000/7400, Media Gateway 15000/7400, and SPMs.

Refer to the following procedures:

- [Powering up the Call Control Frame on page 869](#)
- [Powering up a USP on page 893](#)

- [Powering up a Media Gateway/Multiservice Switch 15000 on page 907](#)
  - [Powering up a Media Gateway/Multiservice Switch 7400 on page 909](#)
  - [Powering up the MDM workstation on page 911](#)
  - [Powering up an SPM device on page 913](#)
- d If equipped, power up the MCS servers and/or RTP Media Portal.
- Refer to [Powering up the MCS servers on page 915](#) and [Powering up an RTP Media Portal on page 919](#).
- e Power up the shelves that house the MS 2000 Series/UAS devices and Packet Media Anchor.
- If your system uses an MS 2000 Series device or Packet Media Anchor, refer to [Powering up the IPmedia 2000 shelves on page 921](#). If your system uses a UAS, refer to [Powering up the SAM16 shelves on page 923](#).
- f Power up the subtended gateways, such as the MG 9000 and MTA.
- For the MG 9000, refer to [Powering up an MG 9000 device on page 925](#).
- For other third party devices, refer to the documentation for your device.
- g Verify all the power indicators after the outage once all the above steps are completed.
- h Verify all the major components after power up via Integrated EMS (or other managers if not equipped with Integrated EMS).
- i Proceed to step [15](#) after completing this step and step [14](#).
- 14 Collect dead office recovery data by performing the following steps.
- a Record the start time of the 3PC blades powering up.
  - b While the 3PC is rebooting, attempt to login to the Call Agent Application level through the SDM, CBM, or CS 2000 Management Tools server. As soon as available, type  
**# priority on;mapci;mtc;srstatus**  
and press the Enter key.
  - c Check the MAP banner. There should be critical alarms indicating the autonomous Network Elements recovery.

- d Take down the timings for the Trks, Lns, CCS, and PM alarms when they are cleared.
- e Start logutil and monitor core logs for recovery activities. Take down the timing of the INIT log by typing

```
logutil;open INIT
```

**15** You have completed this procedure.





## Powering up the XA-Core

### Application

Use this procedure to power up a dead switch that has an eXtended Architecture Core (XA-Core). The switch can be a DMS SuperNode or SuperNode SE switch. The switch is dead if the complete switch is without power. The power loss results from a loss or interruption of A and B dc power feeds to the power distribution center (PDC).

### Action

#### How to recover a dead XA-Core DMS switch

**CAUTION****Call ETAS or your next level of support**

In the event of a dead system, call the Emergency Technical Assistance Services (ETAS) of Nortel Networks. Also call your next level of support before you perform this procedure.

**DANGER****Risk of electrocution**

Do not touch the cabinet wiring. Connections with unshielded cabinet wiring can result in electric shock. Only qualified power maintenance personnel can perform the voltage measurements in step [3](#).

#### At the PDC

- 1 When possible after detection of the power outage, remove all the fuse holders for the following:
  - line concentrating equipment (LCE) talk batteries
  - trunk module equipment (TME) talk batteries
  - PDC filter fuses from the correct PDCs

**Note:** The location of the fuse holders in the fuse panel can vary, depending on your office configuration. For help in locating the fuse holders, refer to the fuse assignment diagram for your office. Also call your next level of support to help you locate the fuses.

- 2 The next step depends on if the switch power is a -48 V dc feed or by a -60 V dc feed.

---

| If the switch power is | Do                     |
|------------------------|------------------------|
| -48 V dc               | <a href="#">step 3</a> |
| -60 V dc               | <a href="#">step 4</a> |

---

- 3 Continue when you know of restored power at the power plant for your office. Power maintenance personnel must check for restored power at each PDC. At the rear of each PDC, measure the dc voltage across the A feed bus and the battery return plate. Repeat the dc voltage measurement for the B feed bus. Power is correct when the voltage on each feed is -48 V dc.

**Note:** Power can be at a nominal potential of -48 V dc. Under conditions that are not normal, the operating voltage can range from -43.75 V dc to -55.8 V dc. A not normal condition is a commercial power failure

---

| If the switch has  | Do                     |
|--------------------|------------------------|
| power retrieval    | <a href="#">step 6</a> |
| no power retrieval | <a href="#">step 5</a> |

---

- 4 Continue when you know of restored power at the power plant for your office. Request power maintenance personnel to check for restored power at each PDC. At the rear of each PDC, measure the dc voltage across the A feed bus and the battery return plate. Repeat the dc voltage measurement for the B feed bus. Power is correct when the voltage on each feed is -60 V dc.

**Note:** Power can be at a nominal potential of -60 V dc. Under conditions that are not normal, the operating voltage can range from -57.4 V dc to -67.7 V dc. A not normal condition is a commercial power failure.

---

| If power has       | Do                     |
|--------------------|------------------------|
| power retrieval    | <a href="#">step 6</a> |
| no power retrieval | <a href="#">step 5</a> |

---

### ***At the power room***

- 5 For help in restoring power to the PDC, call the personnel responsible for maintenance of power at your site.
- When power restores to the PDC, return to this point.

**At the PDC**

- 6** Inspect the alarm indication fuses for the XA-Core and the network cabinets.

| <b>If uses that blew are</b> | <b>Do</b>               |
|------------------------------|-------------------------|
| present                      | <a href="#">step 7</a>  |
| not present                  | <a href="#">step 14</a> |

- 7** Replace the blown cartridge fuse in the rear of the fuse holder. Make sure that the amperage of the replacement cartridge fuse matches the amperage marked on the PDC.

- 8** Remove the blown alarm-indication fuse from the front of the fuse holder.

- 9** Re-insert the fuse holder, with the alarm-indication fuse removed, into the PDC.

- 10** Get an alarm-indication fuse for replacement.

- 11** Insert the alarm-indication fuse that is for replacement into the fuse holder.

- 12** Continue as follows:

| <b>If the replacement fuse is</b>   | <b>Do</b>               |
|-------------------------------------|-------------------------|
| not successful and blows repeatedly | <a href="#">step 13</a> |
| successful                          | <a href="#">step 14</a> |

- 13** Call your next level of support for help.

Continue when you complete replacement of all blown fuses and restored power to the XA-Core and network cabinets. Continue this procedure at [step 14](#).

- 14** If a second person is available to help in the recovery, continue this procedure with two sets of tasks. Request the second person to restore power from the pdc to the peripheral module frames. The second person restores power by use of steps [56](#) through [71](#) of this procedure. While the second person restores power, you recover the core and network by completion of steps [15](#) through [43](#). If one person is available, recover the core and network first.

- 15** Determine if the switch has a remote oscillator shelf.

| <b>If the switch has</b>  | <b>Do</b>               |
|---------------------------|-------------------------|
| a remote oscillator shelf | <a href="#">step 16</a> |

| <b>If the switch has</b>   | <b>Do</b>               |
|----------------------------|-------------------------|
| no remote oscillator shelf | <a href="#">step 17</a> |

**At the remote oscillator shelf**

- 16** Turn on the power converters for the shelf.

**At the XA-Core cabinet**

- 17** Determine if the switch is a SuperNode switch or a SuperNode SE switch.

| <b>If the switch is</b> | <b>Do</b>               |
|-------------------------|-------------------------|
| a SuperNode switch      | <a href="#">step 18</a> |
| a SuperNode SE switch   | <a href="#">step 21</a> |

- 18** Turn on circuit breakers for shelf interface module (SIM) A. Turn on the three switches for circuit breakers A1, A2, and A3. The SIM A card is in slot 3R of the XA-Core shelf.
- 19** Turn on circuit breakers for shelf interface module (SIM) B. Turn on the three switches for circuit breakers B1, B2, and B3. The SIM B card is in slot 16R of the XA-Core shelf.
- 20** Go to [step 23](#)
- 21** Turn on circuit breakers for shelf interface module (SIM) A. Turn on the two switches for circuit breakers A1 and A2. The SIM A card is in slot 3R of the XA-Core shelf.
- 22** Turn on circuit breakers for shelf interface module (SIM) B. Turn on the two switches for circuit breakers B1 and B2. The SIM B card is in slot 16R of the XA-Core shelf.
- 23** Determine if all the power converters have power. You know that all the power converters have power when all the Converter Off lights go off.

| <b>If all the power converters have</b> | <b>Do</b>               |
|-----------------------------------------|-------------------------|
| power                                   | <a href="#">step 26</a> |
| not power                               | <a href="#">step 24</a> |

- 24** To power up the frame perform the procedure, "Clearing an Ext FSP DPCC cabinet major alarm" in *Alarm Clearing and Performance Monitoring Procedures*, 297-8001-543 (North American market) or 297-9051-543 (International market).  
When you completed the procedure, return to this point.

- 25 Go to [step 17](#)

**At the XA-Core reset terminal**

- 26 Monitor the XA-Core reset terminal to determine if the switch has booted.

When the switch boots, the XA-Core reset terminal displays a response to indicate a boot in progress. The response also displays different diagnostic messages and alphanumeric addresses. When the switch has completely booted, an A1 appears on the RTIF display.

| If the response has              | Do                       |
|----------------------------------|--------------------------|
| an A1                            | <a href="#">step 27</a>  |
| no A1 after approximately 15 min | <a href="#">step 111</a> |

**At the MAP terminal**

- 27



**CAUTION**

**Extended service interruption**

The exact log in procedure can vary, depending on your office configuration. If you need additional help, call the personnel responsible for the next level of support.

Determine if you have to log in.

**Note:** The log in message indicates that you have to manually log in. An automatic log in can occur if the office parameters have automatic log in.

*Example of a MAP response*

Please Login.

| If the log in is | Do                      |
|------------------|-------------------------|
| not automatic    | <a href="#">step 28</a> |
| automatic        | <a href="#">step 32</a> |

- 28 Press the break key.

*Example of a MAP response*

?

- 29 To log in to the MAP terminal, type:

**>LOGIN**

and press the enter key.

*Example of a MAP response*

Enter User Name

- 30 To enter the user name, type:

**>user\_name**

and press the enter key.

where

user\_name is the name of the user for the account

*Example of a MAP response*

Enter Password

- 31 To enter the password, type:

**>password**

and press the enter key.

where

password is the name of the password for the account

*Example of a MAP response*

SuperNode1 Logged in on 1997/01/15 at 20:37:17

- 32



#### **CAUTION**

**All customers must follow the sequence of steps set out in this procedure.**

Do not interrupt this procedure at this point to clear an alarm. If a TOD critical alarm appears under the APPL level in the alarm banner, and if the system uses Network Time Protocol (NTP), you must complete all steps in the sequence shown. You will clear the TOD critical alarm by completing [step 39](#). (For information on NTP, see [step 39](#).)

To turn on priority, type:

**>PRIORITY ON**

and press the enter key.

*Example of a MAP response*

```
Pref>
```

- 33** To determine if the system time is correct, type:

**>TIME**

and press the enter key.

*Example of a MAP response*

```
Time is 14:55:50
```

| If the system time is | Do                      |
|-----------------------|-------------------------|
| correct               | <a href="#">step 36</a> |
| not correct           | <a href="#">step 34</a> |

- 34** To enter the correct time (by use of the 24 hour clock), type:

**>SETTIME hh mm**

and press the enter key.

where

hh is the hour (00 to 23)

mm is the minute (00 to 59)

*Example of a MAP response*

```
Warning: There is an automated TOD clock
change
request scheduled on:
1997/10/15 at 1:00 (see table DSTTABLE).
Do you want to proceed with this request?
Please confirm ("YES", "Y", "NO", or "N")
```

- 35** To confirm the command, type:

**>YES**

and press the enter key.

*Example of a MAP response*

```
Time is 20:40:00 on WED 1997/10/15.
```

- 36** Determine if the system date is correct.

| If the system date is | Do                      |
|-----------------------|-------------------------|
| correct               | <a href="#">step 40</a> |

- |  | If the system date is | Do                      |
|--|-----------------------|-------------------------|
|  | not correct           | <a href="#">step 37</a> |
- 37** To enter the correct date, type:
- >SETDATE dd mm yyyy**
- and press the enter key.
- where
- dd is the day (01 to 31)
- mm is the month (01 to 12)
- yyyyy is the year
- Example of a MAP response*
- Warning: There is an automated TOD clock change request scheduled on:  
1997/10/15 at 1:00 (see table DSTTABLE).  
Do you want to proceed with this request?  
Please confirm ("YES", "Y", "NO", or "N")
- 38** To confirm the command, type:
- >YES**
- and press the enter key.
- Example of a MAP response*
- Date is WED. 15/OCT/1997 00:00:00
- 39** If the system uses Network Time Protocol (NTP) as the timing reference, and if a TOD critical alarm is displayed under the APPL level in the alarm banner, perform the procedure titled "How to check and adjust the XA-Core TOD" in the *XA-Core Maintenance Manual*, 297-8991-510. By performing that procedure, you will clear the TOD critical alarm. Return to this point when finished.
- Note:** In the German market only, switches can use Network Time Protocol (NTP) as the timing reference for the time-of-day clock. The system uses Network Time Protocol if the value of the SNTP\_CLIENT office parameter in table OFCENG has been set to Y. For information on the office parameter, see the chapter titled "XA-Core data schema overview" in the *XA-Core Reference Manual*, 297-8991-810.



**At the MAP terminal**

- 40** To access the NET level of the MAP display, type:

**>NET**

and press the enter key.

*Example of a MAP response*

```

NET
 11111 11111 22222
22222 33
Plane 01234 56789 01234 56789 01234
56789 01
 0 0000
 1 0000
JNET

```

- 41** To manually busy the network module for return to service, type:

**>BSY plane\_no pair\_no**

and press the enter key.

where

plane\_no is the network plane number (0 or 1)

pair\_no is the network plane pair number (0 to 31)

- 42** To return the network module to service, type:

**>RTS plane\_no pair\_no**

and press the enter key.

where

plane\_no is the network plane number (0 or 1)

pair\_no is the network plane pair number (0 to 31)

- 43** Repeat steps [41](#) through [42](#) for each JNET shelf.

When all JNET shelves recover, continue this procedure at step [44](#).

- 44** Determine if there are additional input output controller (IOC) and maintenance and administration position (MAP) terminals to recover.

---

| <b>If recover of additional<br/>IOCs and MAP terminals is</b> | <b>Do</b>               |
|---------------------------------------------------------------|-------------------------|
| not complete                                                  | <a href="#">step 45</a> |
| complete                                                      | <a href="#">step 56</a> |

---

- 45 Restore power to all remaining power inverters in the office.

**At the IOC**

- 46 Locate the IOC for recovery.

| If recovery is for | Do                      |
|--------------------|-------------------------|
| an IOC             | <a href="#">step 47</a> |
| an IOM             | <a href="#">step 51</a> |

- 47 Turn on the power converters on the IOC.

**Note:** The version of IOC determines if the IOC has one or two power converters.

- 48 While you press the reset button on one of the IOC power converters, lift the related circuit breaker to turn on the FSP.

- 49 Release the reset button.

- 50 Repeat steps [46](#) through [49](#) for each IOC for recovery, then continue this procedure at [step 51](#).

- 51 To access the input output device (IOD) level of the MAP display, type:

**>IOD**

and press the enter key.

- 52 To access the IOC level of the MAP display for the IOC for recovery, type:

**>BSY ioc\_no**

and press the enter key.

where

ioc\_no is the number of the IOC or IOM

- 53 To return the IOC or IOM to service, type:

**>RTS ioc\_no**

and press the enter key.

where

ioc\_no is the number of the IOC or IOM

- 54 Repeat steps [52](#) through [53](#) for each IOC or IOM for recovery, then continue this procedure at [step 55](#).

- 55 Log in to additional MAP terminals as required.

**Note:** Steps [28](#) through [31](#) describe how to log in to the MAP terminal.

**At the PDC**

- 56** Steps [57](#) through [71](#) describe how to restore power from the PDC to Series I and Series II peripheral module frames. Continue as follows:

---

|                                                   |           |
|---------------------------------------------------|-----------|
| <b>If the PDC power to the PM frames restores</b> | <b>Do</b> |
|---------------------------------------------------|-----------|

---

|           |                         |
|-----------|-------------------------|
| correctly | <a href="#">step 72</a> |
|-----------|-------------------------|

|               |                         |
|---------------|-------------------------|
| not correctly | <a href="#">step 57</a> |
|---------------|-------------------------|

---

- 57** Get one of the following capacitor charging tools:
- a 100-W, 120-V light bulb installed into a socket that has pigtail leads
  - tool number T000655 (CPC number NTA0600512), that has a fuse holder-style connector instead of pigtail leads for easier insertion

**58**

**WARNING**

**Possible equipment damage or extended service interruption**

Use correct fuses. When you return fuses to the PDC, make sure that the amperage of the fuses is correct. The fuse amperage must match the amperage marked on the PDC.

At the first empty fuse slot in the PDC, connect the leads of the capacitor charging tool. Connect the leads across the contacts for the fuse holder until the lamp decreases brightness. If you use a charging tool with a fuse holder-style connector, insert the connector into the slot. Insert the connector until the lamp decreases brightness.

- 59** Remove the capacitor charging tool and immediately insert again the correct fuse holder into the slot.
- 60** Repeat steps [58](#) and [59](#) for all the LCE talk battery, TME talk battery, and PDC filter fuse holders you removed in step 1. When all fuses restore to the PDCs, continue with this procedure.

- 61 Determine if any alarm-indicating fuses blew.

**Note:** The fuse alarm-indicator lamp lights when an alarm-indicating fuse blows.

| If any alarm-indicating fuses have | Do                      |
|------------------------------------|-------------------------|
| blown                              | <a href="#">step 62</a> |
| not blown                          | <a href="#">step 72</a> |

- 62 Locate a fuse holder with a blown alarm-indicating fuse.

**Note:** You can replace blown fuses in any order.

- 63 The cartridge fuse in the fuse holder has blown. Remove the fuse holder from the PDC.
- 64 Replace the blown cartridge fuse in the rear of the fuse holder. Make sure that the amperage of the replacement cartridge fuse matches the amperage marked on the PDC.
- 65 Remove the blown alarm-indicating fuse from the front of the fuse holder.
- 66 Insert again the fuse holder, with the alarm-indicating fuse removed, into the PDC.
- 67 Get a replacement alarm-indicating fuse.
- 68 Insert the replacement alarm-indicating fuse into the fuse holder.
- 69 Determine if the alarm-indicating fuse blows.

**Note:** The fuse alarm indicator lamp lights when an alarm-indicating fuse blows.

| If the alarm-indicating fuse is | Do                       |
|---------------------------------|--------------------------|
| blown                           | <a href="#">step 111</a> |
| not blown                       | <a href="#">step 70</a>  |

- 70 Determine if you replaced all the blown alarm-indicating fuses.

| If you have                                       | Do                      |
|---------------------------------------------------|-------------------------|
| replaced all the blown alarm-indicating fuses     | <a href="#">step 71</a> |
| not replaced all the blown alarm-indicating fuses | <a href="#">step 62</a> |

- 71** Determine if the fuse alarm indicator lamp lit.

| <b>If the fuse alarm indicator lamp lit</b> | <b>Do</b>                |
|---------------------------------------------|--------------------------|
| yes                                         | <a href="#">step 111</a> |
| no                                          | <a href="#">step 72</a>  |

**At the PM frames**

- 72** Select a peripheral module (PM) frame to power up.

**Note:** The PM frames can power up in any order.

- 73** Locate the frame supervisory panel (FSP) and the power converters on the frame.

- 74** Determine if the FSP for the frame has fuses or circuit breakers.

| <b>If the FSP has</b> | <b>Do</b>               |
|-----------------------|-------------------------|
| fuses                 | <a href="#">step 75</a> |
| circuit breakers      | <a href="#">step 80</a> |

- 75** Determine if the power converters have Power Reset buttons or Power Reset switches.

| <b>If the power converters have</b> | <b>Do</b>               |
|-------------------------------------|-------------------------|
| Power Reset buttons                 | <a href="#">step 76</a> |
| Power Reset switches                | <a href="#">step 78</a> |

- 76** To turn on each power converter press and hold its Power Reset button for 2 s.

**Note:** The Converter Fail light goes off when the power converter turns on.

- 77** Determine if all the power converters turn on correctly, indicated by all the Converter Fail lights going off.

| <b>If all the Converter Fail lights are</b> | <b>Do</b>               |
|---------------------------------------------|-------------------------|
| off                                         | <a href="#">step 82</a> |
| not off                                     | <a href="#">step 83</a> |

- 78** To turn on each power converter pull out the power switch and toggle it to the Power Reset position.

**Note:** The Converter Fail light goes off when the power converter turns on.

- 79** Determine if all the power converters turns on correctly, indicated by all the Converter Fail lights are off.

---

**If all the Converter Fail lights are**

**Do**

---

off

[step 82](#)

not off

[step 83](#)

---

- 80** Turn on each power converter as follows:

- Toggle the circuit breaker to the ON position.
- Press and hold the Power Reset button for 2 s.
- Release the circuit breaker and the Power Reset button.

**Note:** The Converter Fail light goes off when the power converter turns on.

- 81** Determine if all the power converters turn on correctly, indicated by all the CONVERTER FAIL lights are off.

---

**If all the Converter Fail lights are**

**Do**

---

off

[step 82](#)

not off

[step 83](#)

---

- 82** Determine if all PM frames turn on.

---

**If all the PM frames turn on**

**Do**

---

yes

[step 87](#)

no

[step 83](#)

---

- 83** Determine if a try made to power up the remaining PM frames.

---

**If power up has**

**Do**

---

not tried

[step 84](#)

tried and failed

[step 86](#)

---

- 84** Power up the next PM frame.

- 85** Go to [step 73](#).

- 86** To power up the remaining PM frames perform the correct procedures in *Alarm Clearing and Performance Monitoring Procedures*, 297-8001-543 (North American market) or 297-9051-543 (International market).

**At the MAP terminal**

- 87** To access the SRSTATUS level of the MAP display, type:

**>MAPCI;MTC;SRSTATUS**

and press the enter key.

*Example of a MAP response*

```
SRSTATUS
0 Quit OVERALL STATUS Pend: 0% Inprg: 0%
Comp: 100% Fail: 0%
2 View_ View: SYSTEM
14:08:30
3 List_ Pend InPrg Comp Fail Pend
InPrg Comp Fail
4 MS 0 0 2 0 IOD
5 5 30 2
5 NET 0 0 6 0 Other
21 3 13 3
6 SER1 0 41 0 0
7 SER2 0 39 0 0
8 SER3 0 0 37 0
9
10 MTC :
11 STATUS:
```

- 88** From the MAP display, determine the recovery status of the Series I and II PMs.

**Note:** Series I PM recovery status displays to the right of the word “SER1” in the MAP display. Series II PM recovery status displays to the right of the word “SER2” in the MAP display. Recovery status can be one of pending, in progress, complete, or failed.

| If the recovery status is | Do                      |
|---------------------------|-------------------------|
| zero                      | <a href="#">step 91</a> |
| not zero                  | <a href="#">step 89</a> |

- 89** Determine from office records or other office personnel which PMs to manually recover first.
- 90** To manually recover the PMs in the required order, perform the correct alarm clearing procedures in *Alarm Clearing and Performance Monitoring Procedures*, 297-8001-543 (North American market) or 297-9051-543 (International market).

91

**CAUTION****Loss of billing data**

Different billing systems than automatic message accounting (AMA) or additional billing system, can be in your office configuration. Call your next level of support to determine if other billing systems are in your office, and if you require recovery action.

To access the device independent recording package (DIRP) level of the MAP, type:

**>IOD;DIRP**

and press the enter key.

**92** To determine the state of the recording volumes for the billing system, type:

**>QUERY subsystem ALL**

and press the enter key.

where

subsystem is the name of the DIRP system used for the billing system

*Example of a MAP response*

```
SSNAME SSNO SEQNO ROTATES POOLNO PARLPOOL EMERGENCY
AMA 0 1 6 9 62 ***YES***
REGULAR
FILE(S) STATE VOLUME RECCOUNT BLOCK E V V_B VLID FNUM FRN#
ACTIVE NONEg
STANDBY1 NONE
PARALLEL
FILE STATE VOLUME BLOCK E V V_B VLID
FNUM FRN#
 NONE
REGULAR VOLUME(S)
VOL# VOLNAME STATE IOC CARD VOL FSEG ROOM
VLID FILES
REGULAR SPACE
```

---

**If the state of the recording volumes for the billing system has** **Do**

---

no volumes allocated, as indicated by the word NONE  
under the state header on the MAP display

[step 94](#)

---



---

| If the state of the recording volumes for the billing system has | Do |
|------------------------------------------------------------------|----|
|------------------------------------------------------------------|----|

---

|                                                                                            |                         |
|--------------------------------------------------------------------------------------------|-------------------------|
| any volume is IN ERROR, as indicated under the REGULAR VOLUME(S) header on the MAP display | <a href="#">step 93</a> |
|--------------------------------------------------------------------------------------------|-------------------------|

|                                                                                           |                         |
|-------------------------------------------------------------------------------------------|-------------------------|
| all volumes are READY, as indicated under the REGULAR VOLUME(S) header on the MAP display | <a href="#">step 95</a> |
|-------------------------------------------------------------------------------------------|-------------------------|

---

**Note:** Different billing systems than automatic message accounting (AMA) or additional billing system, can be in your office configuration. Call your next level of support to determine if other billing systems are in your office, and if you require recovery action.

93 To reset any volumes that are IN ERROR, type:

>**RSETVOL vol\_name**

and press the enter key.

where

vol\_name is the name of the volume to reset

---

| If the volumes reset has | Do |
|--------------------------|----|
|--------------------------|----|

---

|        |                         |
|--------|-------------------------|
| passed | <a href="#">step 95</a> |
|--------|-------------------------|

|        |                          |
|--------|--------------------------|
| failed | <a href="#">step 111</a> |
|--------|--------------------------|

---

94 Perform the procedure, "Allocating recording volumes in the DIRP utility" in *Routine Maintenance Procedures*, 297-8001-546 (North American market) or 297-9051-546 (International market). When you complete the procedure, return to this point.

95 To determine the state of the DLOG recording volumes, type:

>**QUERY DLOG ALL**

and press the enter key.

*Example of a MAP response*

```

SSNAME SSNO SEQNO ROTATES POOLNO PARLPOOL EMERGENCY
DLOG 2 1 102 10 NONE ****YES***
.
REGULAR
FILE(S) STATE VOLUME RECCOUNT BLOCK E V V_B VLID FNUM FRN#
ACTIVE AVAIL S01DDLOG 6 6 0 22 NO 8447 0013 204D
STANDBY1 AVAIL S00DDLOG 0 0 0 23 NO 8408
0014 309B
.
REGULAR VOLUME(S)
VOL# VOLNAME STATE IOC CARD VOL FSEG ROOM
VLID FILES
 22 S01DDLOG READY N/A N/A 7 5 18
8447 A
 23 S00DDLOG READY N/A N/A 8 4 18
8408 S1
REGULAR SPACE
VOL# VOLNAME STATE SEGS EXP UNEXP TOTAL
 22 S01DDLOG READY 5 13 0 18
 23 S00DDLOG READY 4 14 0 18

```

**If the state of DLOG  
recording volumes is****Do**

no allocated volumes, as indicated  
by the word NONE under the state  
header on the MAP display

[step 97](#)

any volume is IN ERROR, as  
indicated under the REGULAR  
VOLUME(S) header on the MAP  
display

[step 96](#)

all volumes are READY, as  
indicated under the REGULAR  
VOLUME(S) header on the MAP  
display

[step 98](#)

**Note:** Different billing systems than automatic message accounting (AMA) or additional billing system, can be in your office configuration. Call your next level of support to determine if other billing systems are in your office, and if you require recovery action.

- 96 To reset any volumes that are IN ERROR, type:

**>RSETVOL vol\_name**

and press the enter key.

where

vol\_name is the name of the volume to reset

---

| If the volumes reset has | Do |
|--------------------------|----|
|--------------------------|----|

---

|        |                         |
|--------|-------------------------|
| passed | <a href="#">step 98</a> |
|--------|-------------------------|

|        |                          |
|--------|--------------------------|
| failed | <a href="#">step 111</a> |
|--------|--------------------------|

---

- 97 Perform the procedure, "Allocating recording volumes in the DIRP utility" in *Routine Maintenance Procedures*, 297-8001-546 (North American market) or 297-9051-546 (International market). When you complete the procedure, return to this point.

- 98 Determine from your next level of support if you need to recover other DIRP systems (for example, JF, OM).

---

| If you need to recover other DIRP systems | Do |
|-------------------------------------------|----|
|-------------------------------------------|----|

---

|     |                         |
|-----|-------------------------|
| yes | <a href="#">step 99</a> |
|-----|-------------------------|

|    |                          |
|----|--------------------------|
| no | <a href="#">step 103</a> |
|----|--------------------------|

---

- 99 Perform the correct procedures in *Alarm Clearing and Performance Monitoring Procedures*, 297-8001-543 (North American market) or 297-9051-543 (International market). When you complete the procedures, return to this point.

- 100 To determine if DIRP logs generated, type:

**>LOGUTIL;OPEN DIRP**

and press the enter key.

---

| If DIRP log generated | Do |
|-----------------------|----|
|-----------------------|----|

---

|     |                          |
|-----|--------------------------|
| yes | <a href="#">step 101</a> |
|-----|--------------------------|

|    |                          |
|----|--------------------------|
| no | <a href="#">step 103</a> |
|----|--------------------------|

---

- 101 Refer to the *Log Report Reference Manual*, 297-8001-840 (North American market) or 297-9051-840 (International market), and take the correct action.

When you complete the log report activities, return to this point.

- 102 To turn off priority, type:

**>PRIORITY OFF**

and press the enter key.

**103** To access the SRSTATUS level of the MAP display, type:

**>MAPCI;MTC;SRSTATUS**

and press the enter key.

*Example of a MAP response*

SRSTATUS

0 Quit OVERALL STATUS Pend: 0% Inprg: 0%

Comp: 100% Fail: 0%

2 View\_ View: SYSTEM

14:08:30

3 List\_ Pend InPrg Comp Fail Pend

InPrg Comp Fail

4 MS 0 0 2 0 IOD

5 5 30 2

5 NET 0 0 6 0 Other

21 3 13 3

6 SER1 0 0 41 0

7 SER2 0 0 39 0

8 SER3 0 0 37 0

9

10 MTC:

11 STATUS:

- 104** Determine the status of the switch recovery.

---

| <b>If the status of the switch recovery is</b> | <b>Do</b> |
|------------------------------------------------|-----------|
|------------------------------------------------|-----------|

---

|                                         |                          |
|-----------------------------------------|--------------------------|
| any Series III PMs that failed recovery | <a href="#">step 105</a> |
|-----------------------------------------|--------------------------|

|                                             |                          |
|---------------------------------------------|--------------------------|
| any Series I or II PMs that failed recovery | <a href="#">step 107</a> |
|---------------------------------------------|--------------------------|

|                                                             |                          |
|-------------------------------------------------------------|--------------------------|
| any IODs or other devices and services that failed recovery | <a href="#">step 110</a> |
|-------------------------------------------------------------|--------------------------|

|                                          |                          |
|------------------------------------------|--------------------------|
| that the system has completely recovered | <a href="#">step 112</a> |
|------------------------------------------|--------------------------|

---

- 105** To manually recover the PMs, perform the procedure, "Recovering Link Peripheral Processors" in *Recovery Procedures*, 297-8001-545 (North American market) or 297-9051-545 (International market).

When you complete the procedure, return to this point.

- 106** Go to [step 103](#).

- 107** Determine from office records or other office personnel which PMs you can recover first.

- 108** To manually recover the PMs in the required order perform the correct alarm clearing procedures in *Alarm Clearing and Performance Monitoring Procedures*, 297-8001-543 (North American market) or 297-9051-543 (International market).

When you complete the procedure, return to this point.

- 109** Go to [step 103](#).

- 110** To manually recover IODs and other devices and services, perform the correct procedure in this document. Also you can refer to your site-related operating procedures.

- 111** For additional help, call the personnel responsible for the next level of support.

- 112** You have completed this procedure.

















---

## Powering up the Message Switch

---

### Application

Use this procedure to power up the Message Switch (MS) when recovering from a power outage.

### Action

#### Powering up the MS

##### *At the XA-Core frame*

- 1 Locate the NT9X31 and NT9X30 power converters for message switch 0 (MS 0) in slots 33F and 36F on the MS 0 shelf.
- 2 Turn on the NT9X31 and NT9X30 power converters in slots 33F and 36F of the MS 0 shelf at the same time. Lift and release the power switches located on the faceplates of the converters.
- 3 Locate the NT9X31 and NT9X30 power converters for MS 0 in slots 1F and 4F on the MS 0 shelf.
- 4 Turn on the NT9X31 and NT9X30 power converters in slots 1F and 4F of the MS 0 shelf at the same time. Lift and release the power switches located on the faceplates of the converters.
- 5 Locate the NT9X31 and NT9X30 power converters for message switch 1 (MS 1) in slots 33F and 36F on the MS 1 shelf.
- 6 Turn on the NT9X31 and NT9X30 power converters in slots 33F and 36F of the MS 1 shelf at the same time. Lift and release the power switches located on the faceplates of the converters.
- 7 Locate the NT9X31 and NT9X30 power converters for MS 1 in slots 1F and 4F on the MS 01shelf.
- 8 Turn on the NT9X31 and NT9X30 power converters in slots 1F and 4F of the MS 1 shelf at the same time. Lift and release the power switches located on the faceplates of the converters.

##### *At the MAP terminal*

- 9 To access the SRSTATUS level of the MAP, type:

**>MAPCI;MTC;SRSTATUS**

and press the enter key.

*Example of a MAP response*

```
SRSTATUS
0 Quit OVERALL STATUS Pend: 0% Inprg: 0%
Comp: 100% Fail: 0%
```

```

2 View_ View: SYSTEM
14:08:30
3 List_ Pend InPrG Comp Fail Pend
InPrG Comp Fail
4 MS 0 0 2 0 IOD
5 5 30 2
5 NET 0 0 6 0 Other
21 3 13 3
6 SER1 0 41 0 0
7 SER2 0 39 0 0
8 SER3 0 37 0 0
9
10 MTC:
11 STATUS:

```

**10** Determine the recovery status of the MSs.

**Note:** MS recovery status displays to the right of the word “MS” in the MAP display. Recovery status for each MS can be one of pending, in progress, complete, or failed.

| If the recovery status is                                | Do                      |
|----------------------------------------------------------|-------------------------|
| either MS failed recovery                                | <a href="#">step 15</a> |
| either MS continues to have pending recovery             | <a href="#">step 11</a> |
| another status different from failed or pending recovery | <a href="#">step 12</a> |

**11** Wait until both MSs are either in recovery development or have completed recovery.

When neither MS continues to have pending recovery, go to step [10](#)

**12** To access the MS Clock level of the MAP display, type:

**>MAPCI;MTC;MS;CLOCK**

and press the enter key.

**13** To synchronize the clocks, type:

**>SYNC**

and press the enter key.

| If the SYNC command is | Do                      |
|------------------------|-------------------------|
| successful             | <a href="#">step 16</a> |
| failed                 | <a href="#">step 14</a> |

- 14** Record the reason for synchronization failure, as shown in the MAP response. Repeat the try to synchronize the MS clocks later, after networks and PMs are in service.
- 15** For additional help, call the personnel responsible for the next level of support.
- 16** You have completed this procedure.









## Powering up the Enhanced Network

### Application

Use this procedure to manually power up the enhanced network (ENET) in the event of a power failure.

### Action

#### Powering up the ENET

##### *At the ENET frames*

- 1 Locate the NT9X31 power converters in slots 1F and 33F on the ENET shelves.
- 2 To turn on the NT9X31 power converters lift and release the power switches located on the faceplates of the converters.
- 3 Locate the NT9X30 power converters in slots 4F and 36F on the ENET shelves.
- 4 Turn on the NT9X30 power converters lift and release the power switches located on the faceplates of the converters.
- 5 Determine if all the converters have power. Power is indicated by all the Converter Off lights going off.

---

|                                         |           |
|-----------------------------------------|-----------|
| <b>If all the power converters have</b> | <b>Do</b> |
|-----------------------------------------|-----------|

---

|       |                        |
|-------|------------------------|
| power | <a href="#">step 7</a> |
|-------|------------------------|

|           |                        |
|-----------|------------------------|
| not power | <a href="#">step 6</a> |
|-----------|------------------------|

---

- 6 To power up the ENET frame perform the procedure, "Clearing an Ext FSP DPCC cabinet major alarm", in the document, *Alarm and Performance Monitoring Procedures*, 297-8021-543.  
When you complete the procedure, return to this point.

##### *At the MAP terminal*

- 7 To access the SRSTATUS level of the MAP display, type:  
**>MAPCI;MTC;SRSTATUS**  
and press the enter key.

*Example of a MAP response*

```
SRSTATUS
0 Quit OVERALL STATUS Pend: 0% Inprg: 0%
Comp: 100% Fail: 0%
```

```

2 View_ View: SYSTEM
14:08:30
3 List_ Pend InPrg Comp Fail Pend
InPrg Comp Fail
4 MS 0 0 2 0 IOD
5 5 30 2
5 NET 0 0 6 0 Other
21 3 13 3
6 SER1 0 41 0 0
7 SER2 0 39 0 0
8 SER3 0 37 0 0
9
10 MTC:
11 STATUS:

```

- 8** From the MAP display, determine the recovery status of the network.

**Note:** Network recovery status displays to the right of the word “NET” in the MAP display. Recovery status can be one of pending, in progress, complete, or failed.

---

**If the status of any network element is**

**Do**

failed

[step 11](#)

pending

[step 9](#)

another status

[step 13](#)

---

- 9** Continue when there are no network elements that continue to be pending recovery.
- 10** Go to [step 8](#).
- 11** To manually recover the ENET perform the procedure, “Recovering the Enhanced Network” in *Recovery Procedures*, 297-8021-545.
- 12** Go to [step 7](#).
- 13** You have completed this procedure.





























---

## Powering up a Ethernet Routing Switch 8600

---

### Purpose of this procedure

Use the following procedure to power up a Ethernet Routing Switch 8600.

### When to use this procedure

Use this procedure when it is necessary to power up a Ethernet Routing Switch 8600.

### Prerequisites

None

### Action

#### Powering up a Ethernet Routing Switch 8600

##### *At the Ethernet Routing Switch 8600 frame*

- 1 Turn the DC input power source on or reset the power source circuit breaker to provide power to the power supply.
- 2 Turn the power supply switch for all three DC power supplies to the on position.

**Note:** You must turn on two of the power supply units within 2 seconds of each other. If you wait longer to turn on the second power supply, one of the power supplies could shut down. To correct this condition, turn off both power supplies, wait at least 30 seconds, and then turn on both power supplies again within 2 seconds.

- 3 You have completed this procedure.



---

## Powering up the Link Peripheral Processors

---

### Application

Use this procedure to power up the Link Peripheral Processors (LPP) or fiberized LPPs (FLPPs) in the event of a power failure.

**Note:** Throughout this procedure, LPP is used to refer to both the LPP and FLPP.

### Action

#### Recovering LPPs

##### At the PDC

- 1 Determine if PDC has power restored to the LPP(s).

| If PDC has                     | Do                     |
|--------------------------------|------------------------|
| power restored to the LPPs     | <a href="#">step 5</a> |
| not power restored to the LPPs | <a href="#">step 2</a> |

- 2 Check the PDC fuses that supply the LPP.

| If there are           | Do                     |
|------------------------|------------------------|
| blown fuses            | <a href="#">step 3</a> |
| no blown fuses visible | <a href="#">step 4</a> |

- 3 Replace the blown fuses.

**Note:** If fuses blow repeatedly, call your next level of support for help.

When PDC power restores to the LPPs, continue this procedure at [step 5](#).

- 4 Call the personnel responsible for maintaining power at your site, or refer to your next level of support for help.

When PDC power restores to the LPPs, continue this procedure at [step 5](#).

- 5 Locate the LPPs for recovery.

**At the LPP cabinet****6****WARNING****Static electricity damage**

Wear a wrist strap connected to the wrist-strap grounding point of a frame supervisory panel (FSP). Also a wrist strap can connect to a modular supervisory panel (MSP). Wear a wrist strap when you handle circuit cards. A wrist strap protects the cards against damage caused by static electricity.

Locate the NT9X74 cards in all link interface shelves (LIS).

**Note:** NT9X74 cards are in shelf position 7F and 32F on all LISs.

- 7** To unseat each NT9X74 card, release the locking levers and carefully pull the card towards you about 25 mm (1 in.).
- 8** Locate the NT9X30 power converters in slots 4F and 36F of the link interface module (LIM) unit shelf.
- 9** To turn on the power converters of the LIM unit shelf, toggle the switch each NT9X30 card.
- 10** Locate the NT9X30 or NTDX16 power converters for each LIS.  
**Note:** NT9X30 power converters are in slots 4F and 36F for each LIS. NTDX16 power converters can be in slots 1F, 4F, 33F, and 36F for each LIS.
- 11** To turn on the LIS power converters, toggle the switch on each NT9X30 or NTDX16 card.
- 12** Determine if all the power converters turned on power correctly. All the CONVERTER OFF lights go off when power turns on correctly.

| If all the CONVERTER OFF lights are | Do                      |
|-------------------------------------|-------------------------|
| off                                 | <a href="#">step 15</a> |
| not off                             | <a href="#">step 13</a> |

- 13** To power up the frame, perform the procedure, "Clearing an Ext FSP LPP cabinet major alarm" in *Alarm Clearing and Performance Monitoring Procedures*, 297-8001-543 (North American market) or 297-9051-543 (International market).

When you complete the procedure, return to this point.

- 14 Go to [step 8](#).
  - 15 Put in position all NT9X74 cards as follows:
    - Carefully slide each NT9X74 card back into the LIS.
    - Push on the upper and lower edges of each faceplate. Make sure that the card is completely in the slot of the shelf.
    - Close the locking levers on each card.
  - 16 Repeat steps [5](#) through [15](#) for each LPP in your office.
- When power restores to all LPPs, continue this procedure at step [17](#).
- 17 To access the SRSTATUS level of the MAP display, type:

**>MAPCI;MTC;SRSTATUS**

and pressing the Enter key.

*Example of a MAP response*

```
SRSTATUS
0 Quit OVERALL STATUS Pend: 0% Inprg: 0%
Comp: 100% Fail: 0%
2 View_ View: SYSTEM
14:08:30
3 List_ Pend InPrgr Comp Fail Pend
InPrgr Comp Fail
4 MS 0 0 2 0 IOD
5 5 30 2
5 NET 0 0 6 0 Other
21 3 13 3
6 SER1 0 41 0 0
7 SER2 0 39 0 0
8 SER3 0 37 0 0
9
10 MTC:
11 STATUS:
```

- 18 From the MAP display, determine the recovery status of the Series III PMs.

**Note:** Series III PM recovery status displays to the right of the word “SER3” in the MAP display. Recovery status can be one of pending, in progress, complete, or failed.

| If the Series 3 PMs are | Do                      |
|-------------------------|-------------------------|
| zero                    | <a href="#">step 20</a> |

| If the Series 3 PMs are | Do                      |
|-------------------------|-------------------------|
| not zero                | <a href="#">step 19</a> |

- 19** To manually recover the PMs, perform the procedure, "Recovering Link Peripheral Processors, in *Recovery Procedures*, 297-8021-545.
- When you complete the procedure, return to this point.
- 20** You have completed this procedure.





































---

## Powering up the SDM

---

### Purpose of this procedure

Use the following procedure to power up the SuperNode Data Manager (SDM) that houses the CS 2000 Core Manager.

### When to use this procedure

Use this procedure when it is necessary to power up the SDM hardware.

### Prerequisites

None

### Action

#### Powering up the SDM

##### *At the SDM frame*

- 1 Turn on the two top breakers at the top of the SDM frame.
- 2 Wait a few moments until the green lights on each card are steady.

##### *At the VT100 terminal*

- 3 Login as root and type  
`# sdmmtc`  
and press the Enter key.
- 4 Verify that all hardware is in service.
- 5 Verify that *rootvg* and *datavg* logical volumes are mirrored at the storage level.

**Note:** There will likely be alarms at the connection and application levels. The general status of the SDM will be in-service trouble (IsTb).

- 6 You have completed this procedure.





---

## Powering up a T1400 or N240 server

---

### Purpose of this procedure

Use the following procedure to power up a Netra™ T1400 or N240 server. Powering up the N240 server will, in turn, supply power for the following applications:

- Integrated EMS
- Core and Billing Manager
- CS 2000 Management Tools applications
- MG 9000 Manager

### When to use this procedure

Use this procedure when it is necessary to power up the Netra™ T1400 or duplex N240 servers.

### Prerequisites

None

### Action

#### Powering up a Netra™ T1400 or N240 server

- 1 To bring the T1400 server into service, turn on the circuit breakers. The T1400 should recover on its own.
- 2 To bring the duplex N240 servers into service, turn on the circuit breakers. To help with recovery, turn the power on to what was the active server first. If there is no record of this, turn on the Unit 0 server before the Unit 1 server.  
  
Once power is restored to the server they will recover on their own.
- 3 You have completed this procedure.



---

## Powering up the RTP Media Portal Manager

---

### Purpose of this procedure

Use the following procedure to power up the RTP Media Portal Manager. The RTP Media Portal Manager is installed on a Sun Netra 240 (N240).

### When to use this procedure

Use this procedure when it is necessary to power up the Sun N240 server that houses the RTP Media Portal Manager.

### Prerequisites

None

### Action

#### Powering up the RTP Media Portal Manager

##### *At the frame housing the RTP Media Portal Manager*

- 1 For DC powered shelves, switch the circuit breakers at the EBIP that provide power to the servers being powered to the *ON* position. The breaker will have the 'I' side (top) of the breaker depressed.  
  
**Note:** The DC powered N240 does not have a Power ON/OFF switch and can only be powered ON/OFF from the breaker at the EBIP.
- 2 For AC powered shelves, push the rocker located on the top of the AC outlet to apply power to the servers. It should be switched to the "I" position.
- 3 Once the breakers are switched *ON* at the power source, power up the servers by switching the breakers on the back of the chassis to the *ON* position.
- 4 Verify the system is powered up correctly by observing the LEDs on the front of the N240.
- 5 You have completed this procedure.



---

## Powering up the SAMF frame

---

### Purpose of this procedure

Use the following procedure to power up the SAMF frame. Powering up the SAMF frame allows the SAM21 hardware cards, the Policy Controller unit, and the Session Server unit to return to service.

### When to use this procedure

Use this procedure when it is necessary to power up the SAMF frame.

### Prerequisites

None

### Action

#### Powering up the SAMF frame

##### *At the SAMF frame*

- 1 Power up the SAMF BIP breakers. At the top of the cabinet, turn on the breakers that supply power to the two SAM21 shelves and the Session Server (if equipped).

##### *At the CS 2000 SAM21 Manager*

- 2 If necessary, unlock the previously active Shelf Controller (SC). Refer to [Unlocking a SAM21 Shelf Controller on page 875](#).
- 3 If necessary, unlock the previously inactive SC. Refer to [Unlocking a SAM21 Shelf Controller on page 875](#).
- 4 If necessary, unlock any remaining locked cards on the SAM21 other than the GWC cards.

##### *At the CS 2000 GWC Manager*

- 5 If necessary, unlock all previously active GWC cards. Refer to [Unlock a GWC card on page 881](#).
- 6 If necessary, unlock all previously inactive GWC cards. Refer to [Unlock a GWC card on page 881](#).

##### *At the Policy Controller unit*

- 7 Determine which physical or logical unit you want to become active and power that unit up first by executing procedure

“Power-On and boot a Policy Controller unit” in *Policy Controller Security and Administration*, NN10434-611.

- 8 Once the active unit has begun call processing, power up the mate unit by executing procedure “Power-On and boot a Policy Controller unit” in *Policy Controller Security and Administration*, NN10434-611.

#### **At the Session Server unit**

- 9 Determine which physical or logical unit you want to become active and power that unit up first by executing procedure “Power-On and boot a Session Server unit” in *Session Server Security and Administration*, NN10346-611.
- 10 Log onto the active unit to monitor the status of the SIP Gateway application using procedure “View the operational status of the SIP Gateway application” in *Session Server Security and Administration*, NN10346-611. Verify that the Administrative state of the SIP Gateway application becomes Unlocked and the Operational state becomes Enabled.

If the active unit comes up in any state other than Unlocked:Enabled, refer to *Session Server Security and Administration*, NN10346-611, and complete one or both of the following procedures:

- complete procedure *Unsuspend the SIP gateway application*
  - complete procedure *Unlock the SIP gateway application*
- 11 Once the active unit has begun call processing, power up the mate unit by executing procedure “Power-On and boot a Session Server unit” in *Session Server Security and Administration*, NN10346-611.
  - 12 From the active unit, verify that the SIP Gateway application databases on the both units have synchronized using procedure “Verify synchronization status of Session Server units” in *Session Server Security and Administration*, NN10346-611
  - 13 Monitor the system for an appropriate period per your site guidelines.

If you experience problems with call processing, refer to *Session Server Security and Administration*, NN10346-611, and perform the following tasks in order:

- complete procedure Invoke a maintenance SwAct of the Session Server platform
- complete procedure Inhibit a system SwAct (Jam)
- contact your next level of support or Nortel GNPS

**14** The procedure is complete.





---

## Powering up the Call Control Frame

---

### Purpose of this procedure

Use the following procedure to power up the Call Control Frame (CCF).

Powering up the CCF allows the SAM21 hardware cards and the STORM disk array to return to service.

### When to use this procedure

Use this procedure when it is necessary to power up the CCF.

### Prerequisites

None

### Action

#### Powering up the Call Control Frame

##### *At the CCF*

- 1 Determine the configuration of your CCF.

---

| If the CCF configuration includes | Do |
|-----------------------------------|----|
|-----------------------------------|----|

---

|                                                                |                        |
|----------------------------------------------------------------|------------------------|
| a STORM disk array and two STORM cards in the Call Agent shelf | <a href="#">step 2</a> |
|----------------------------------------------------------------|------------------------|

|                         |                        |
|-------------------------|------------------------|
| two STORM SAM-XTS units | <a href="#">step 3</a> |
|-------------------------|------------------------|

---

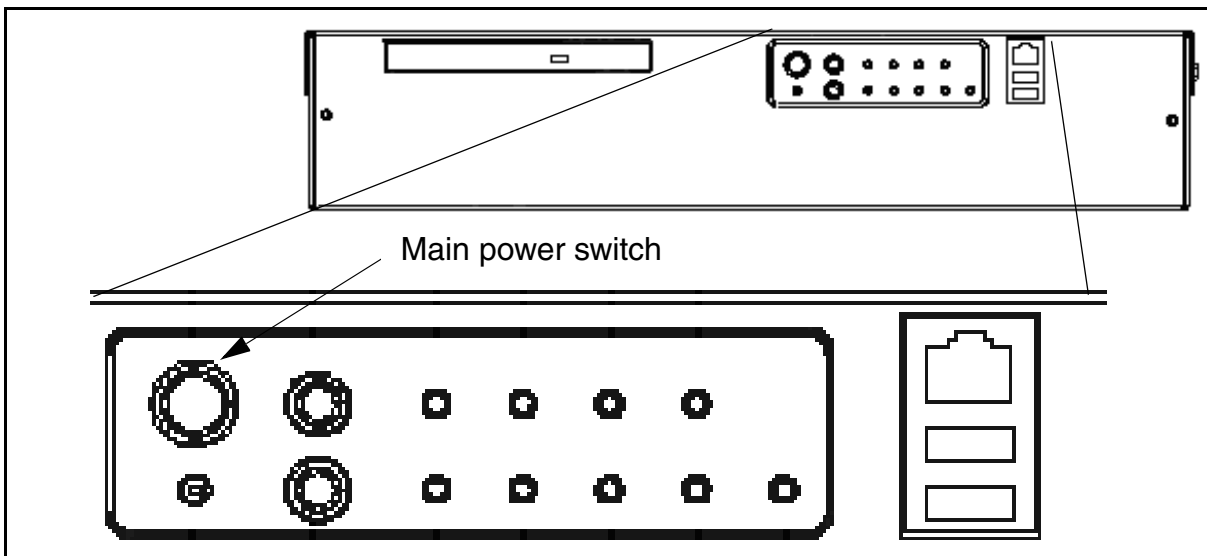
- 2 Power up the CCF BIP breakers. At the top of the cabinet, turn on the breakers that supply power to the STORM disk array and the two SAM21 shelves.

Go to [step 6](#)

- 3 Power up the CCF BIP breakers. At the top of the cabinet, turn on the breakers that supply power to the two SAM21 shelves and the STORM SAM-XTS units.

##### *At the front panel of the STORM SAM-XTS units*

- 4 If necessary, power on the STORM SAM-XTS units using the main power switch located on the front panel.



- 5 At the console, monitor the boot progress of the unit until booting is complete.

***At the CS 2000 SAM21 Manager***

- 6 If necessary, unlock the previously active Shelf Controller (SC).  
Refer to [Unlocking a SAM21 Shelf Controller on page 875](#).
- 7 If necessary, unlock the previously inactive SC.  
Refer to [Unlocking a SAM21 Shelf Controller on page 875](#).
- 8 If necessary, unlock the previously active Compact Call Agent (CCA) card.  
Refer to [Unlocking the Call Agent on page 879](#).
- 9 If necessary, unlock the previously inactive CCA card.  
Refer to [Unlocking the Call Agent on page 879](#).
- 10 If necessary, unlock the previously active USP-lite card.
- 11 If necessary, unlock the previously inactive USP-lite card.
- 12 If necessary, unlock any remaining locked cards on the SAM21 other than the GWC cards.

***At the CS 2000 GWC Manager***

- 13 If necessary, unlock all previously active GWC cards.  
Refer to [Unlock a GWC card on page 881](#).
- 14 If necessary, unlock all previously inactive GWC cards.

Refer to [Unlock a GWC card on page 881](#).

**15** You have completed this procedure.





# SAM21 Shelf Controller Security and Administration

---

## What's new for SN08

The SAM21 Shelf Views have been updated to reflect the shelf configuration in the NTRX51TA Call Control Frame (CCF). In the NTRX51TA CCF, the SAM21 shelf does not contain a STORage Management (STORM) card. A redundant pair of SAM-XTS servers, referred to as the STORM Integrated Array (STORM-IA), support STORM functionality. For more information, refer to the following documents:

- *SAM21 Shelf Controller Basics*, NN10025-111
- *STORM Basics*, NN10024-111

## What's new for SN07

Logins are allowed from console access and secure shell (ssh) clients. Direct root login is not available on those interfaces though. To gain super user privilege, login as a maintenance level user, and then use the **su** command to gain super user privilege. Trying to log in as the root user on network and console interfaces is rejected. The SAM21 Shelf Controllers allow logins from the CS 2000 Core Manager and the CS 2000 Management Tools host.

## What's new for SN06

Even though local logins to the SAM21 Shelf Controllers are not needed for operations, maintenance, administration or provisioning (OAM&P), security of logins to the SAM21 Shelf Controller operating system is improved. Access is denied from all hosts except the mate SAM21 Shelf Controller, the CS 2000 Core Manager, and the host that provides the CS 2000 Management Tools. Access requires the use of the secure shell (ssh). Remote shell (rsh) access is permitted from the mate SAM21 Shelf Controller.

Local passwords are enabled. Once logged in, password changes are enabled with the **passwd** command. However, password changes do

not persist after locking the SAM21 Shelf Controller. Contact your Nortel account representative for information about passwords.

Since login access to the SAM21 Shelf Controller is not needed to perform OAM&P, this document only discusses the OAM&P operations available from the CS 2000 SAM21 Manager client.

## Security and administration strategy

Security for the SAM21 Shelf Controllers is implemented according to the items in the following list:

- physical security of the client workstation
- physical security of the SAM21 shelf
- security mechanisms available through the client workstation operating system
- SAM21 Shelf Controllers only allow login connections from the CS 2000 Core Manager, the host that provides the CS 2000 Management Tools, and the mate SAM21 Shelf Controller

## Tools and utilities

There are no tools or utilities for security. The CS 2000 SAM21 Manager client is the interface for administration of the SAM21 Shelf Controllers.

**Note:** If a Card View window is opened and a task or maintenance is completed, close the window rather than minimize the window. Memory consumption is kept to a minimum, but several unused and open Card View windows can consume memory on the CS 2000 SAM21 Manager client workstation.

## User administration

The SAM21 Shelf Controllers do not implement any custom security features. The CS 2000 SAM21 Manager client authenticates users when the application is started.

### Adding a user

The SAM21 Shelf Controllers do not provide user administration. The CS 2000 SAM21 Manager provides authentication, but not user administration. For procedures on how to add a user to the CS 2000 SAM21 Manager client workstation, contact your system administrator or refer to the operating system reference documentation.

### Setting privileges

The SAM21 Shelf Controllers and the CS 2000 SAM21 Manager client do not implement user privilege administration.

### Removing a user

To prevent user access to the CS 2000 SAM21 Manager client, contact your system administrator to disable the user account on the workstation.

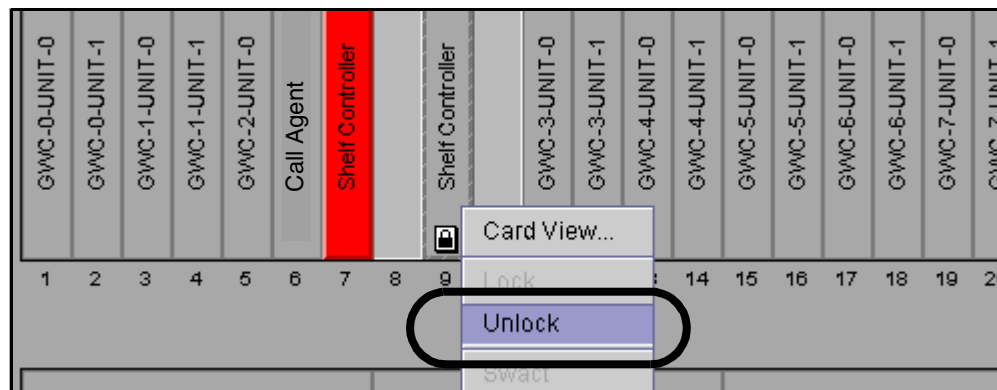
## Device administration

Administration of the SAM21 Shelf Controllers is done through the CS 2000 SAM21 Manager client.

### Unlocking a SAM21 Shelf Controller

#### *At the CS 2000 SAM21 Manager client workstation*

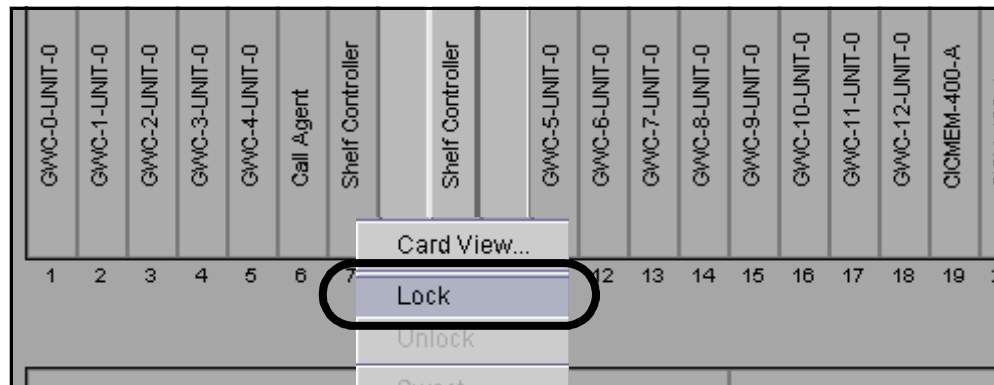
- 1 From the Shelf View, right click on the SAM21 Shelf Controller and select Unlock from the context menu.



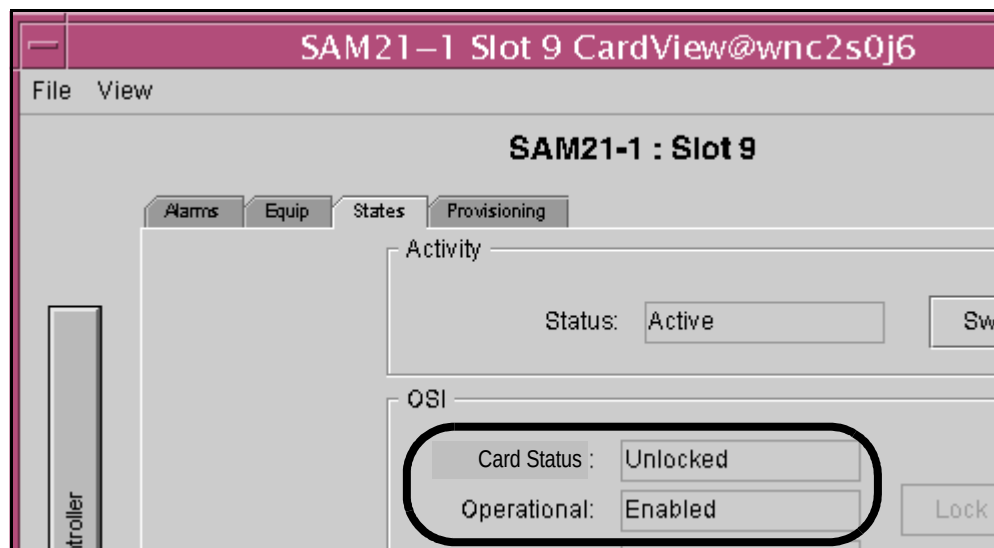
## Locking a SAM21 Shelf Controller

### *At the CS 2000 SAM21 Manager client workstation*

- 1 From the Shelf View, right click on the SAM21 Shelf Controller and select Lock from the context menu.



**Note:** Only lock a circuit pack that is in service. If a SAM21 Shelf Controller is unlocked and then relocked before the SAM21 Shelf Controller boots, flash memory can be corrupted and require a replacement SAM21 Shelf Controller. Check that a SAM21 Shelf Controller is Unlocked and Enabled from the Status tab of the Card View window.



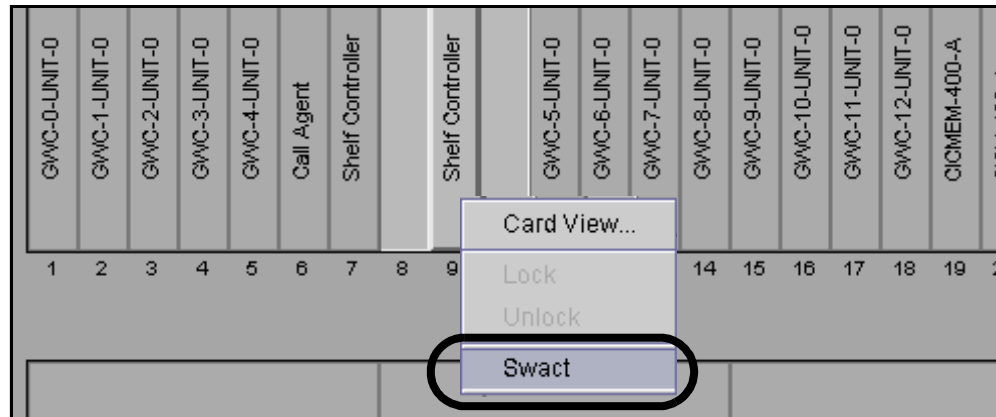


## Invoking manual protection switch

### *At the CS 2000 SAM21 Manager client workstation*

- 1 From the Shelf View, right click on the SAM21 Shelf Controller and select Swact from the context menu.

**Note:** Swact is available on the active SAM21 Shelf Controller only.



## Replacing air filters

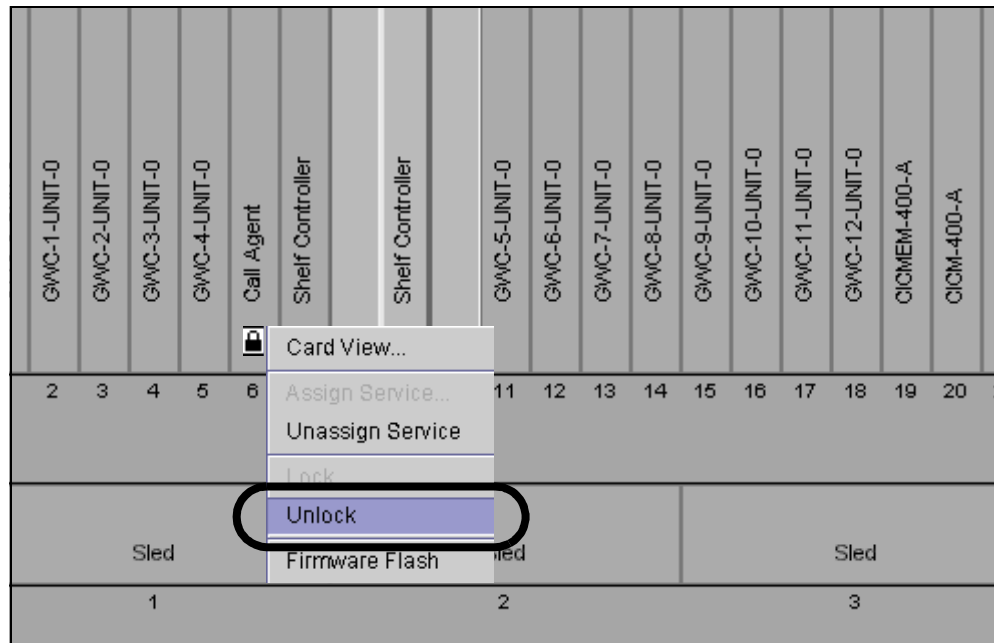
Replace the three air filters from the front of the fan sleds on the SAM21 shelf with part number A0828397. This part number includes three air filters. Replace these air filters every 10 000 hours. When performing the replacement, replace one air filter at a time and do not leave a fan uninserted for more than one minute.



## Unlocking the Call Agent

### *At the CS 2000 SAM21 Manager client*

- 1 From the Shelf View, right click on the card and select Unlock from the context menu.



**Note:** Unlock is also available from the States tab of the Card View window.

The card resets, downloads software, and reboots.

- 2 Wait for the lock icon to disappear.  
**Note:** Do not perform any patching activities on the Call Agent until ten minutes have passed.
- 3 This procedure is complete.



---

## Unlock a GWC card

---

### Purpose of this procedure

This procedure initiates a reboot of the GWC card causing the card to download its software from the CS 2000 Core Manager and to restart its call processing services and applications software.

### When to use this procedure

Use this procedure:

- after replacing a GWC card.
- as part of a fault clearing activity.
- when a new software load is available.
- when you have completed reprovisioning a GWC card or GWC node (a node is made up of unit 0 and unit 1 GWC cards) and you would like the card or node to begin using the new provisioning values.
- when you have applied or removed a patch to the GWC software using the Network Patch Manager (NPM) and have saved a new GWC software image to the CS 2000 Core Manager.

**Note:** For more information about upgrading or patching GWC software, refer to the *Upgrading the Gateway Controller* NTP, NN10196-461.

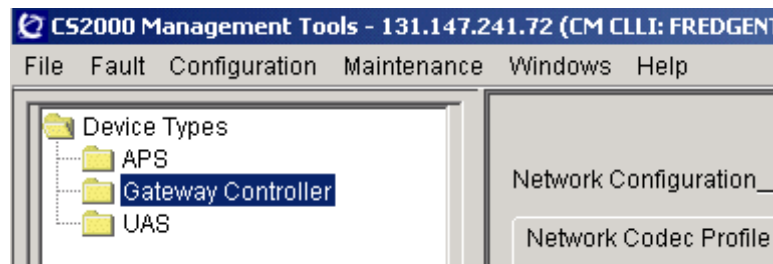
### Prerequisites

The GWC card must be locked. The procedure [Lock a GWC card on page 887](#) in this NTP provides instruction on how to lock a GWC card.

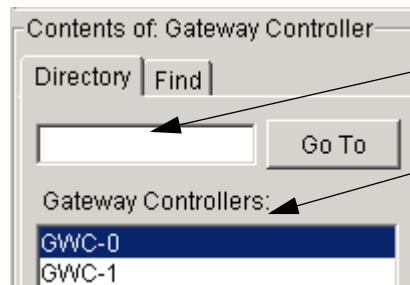
## Action

### *At the CS 2000 GWC Manager client*

- 1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



- 2 From the Contents of: GatewayController frame, select the GWC node that contains the card you want to unlock.



Type a GWC node name here,  
or

Select a GWC node from the list  
of provisioned GWC nodes.

- 3 Select the **Maintenance** tab to display maintenance information about the node.

GWC-6 Unit 0: 47.104.41.54  
Unit 1: 47.104.41.55

**Maintenance** | Provisioning

GWC-6-UNIT-0

|                       |                |                 |                     |
|-----------------------|----------------|-----------------|---------------------|
| Administrative state: | unlocked(1)    | Usage state:    | idle(1)             |
| Operational state:    | enabled(1)     | Stand by state: | providingService(3) |
| Activity state:       | active(1)      | Swact state:    | noSwAct(0)          |
| Isolation state:      | notisolated(2) | Alarm state:    | 00 00 00 00         |
| Available state:      | 00 00 00 00    | Fault state:    | none(0)             |
| Loadname:             | GI080BJ        |                 |                     |

- 4 Click the **Card View** button for the card you want to unlock. This action opens the CS 2000 SAM21 Manager.

**Note:** If a card is currently locked, all fields display the value <unknown>.

GWC-6-UNIT-1

|                       |           |                 |           |
|-----------------------|-----------|-----------------|-----------|
| Administrative state: | <unknown> | Usage state:    | <unknown> |
| Operational state:    | <unknown> | Stand by state: | <unknown> |
| Activity state:       | <unknown> | Swact state:    | <unknown> |
| Isolation state:      | <unknown> | Alarm state:    | <unknown> |
| Available state:      | <unknown> | Fault state:    | <unknown> |
| Loadname:             |           |                 |           |

Save Image Busy (Disable) RTS (Enable) **Card View**

☐ Force Warm Swact Cold Swact

**At the CS 2000 SAM21 Manager**

- 5 In the card view, select the **States** tab.

**Note:** If you want to display the status of all cards in the shelf, select the **Shelf View** from the **View** menu.

The screenshot shows the 'States' tab selected for 'Sam21-2 : Slot 12'. The interface includes a sidebar with 'GWC-6-UNIT-1' and '12'. The main area has tabs for 'Alarms', 'Equip', 'States', 'Diags', and 'Provisioning'. Below the tabs is a 'Summary' section with a table showing counts for Critical, Major, and Minor states, all currently at 0. Below that is a 'Details' section with a table header for Equip., ID, Time, Type, Severity, and Reason.

| Critical | Major | Minor |
|----------|-------|-------|
| 0        | 0     | 0     |

| Equip. | ID | Time | Type | Severity | Reason |
|--------|----|------|------|----------|--------|
|--------|----|------|------|----------|--------|

- 6 In the States display, click the **Unlock** button to unlock the card.

The screenshot shows the 'States' tab selected for 'Sam21-2 : Slot 12'. The interface includes a sidebar with 'GWC-6-UNIT-1' and '12'. The main area has tabs for 'Alarms', 'Equip', 'States', 'Diags', and 'Provisioning'. Below the tabs is an 'OSI' section with fields for 'Card Status' (Locked), 'Operational' (Disabled), and 'Availability' (None). To the right of these fields are 'Lock' and 'Unlock' buttons, with the 'Unlock' button highlighted. Below the OSI section is a 'History' section with a scrollable area.

|               |          |
|---------------|----------|
| Card Status:  | Locked   |
| Operational:  | Disabled |
| Availability: | None     |

Lock Unlock



- 7 Observe the system response in the History window.  
The card is unlocked when you see the text “Application unlocked successfully”.

The screenshot displays a web-based management interface for a Nortel network device. On the left, a vertical sidebar identifies the selected unit as 'GWC-6-UNIT-1' and shows the slot number '12'. The main content area features a top navigation bar with tabs for 'Alarms', 'Equip', 'States', 'Diags', and 'Provisioning'. The 'States' tab is active, showing the 'OSI' (Operational State Information) section. This section contains three status fields: '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' window with a scrollable text area showing the following sequence of events: 'Element Manager initiated Unlock request received', 'Resetting board', 'Reset complete', 'Initializing network device', 'Net initialized', 'Booting cached load via the backplane', 'Bootloaded successfully', and 'Application unlocked successfully'. At the bottom of the History window are 'Save' and 'Clear' buttons.

| Alarms                                            | Equip | States                                                                    | Diags | Provisioning |
|---------------------------------------------------|-------|---------------------------------------------------------------------------|-------|--------------|
| <b>OSI</b>                                        |       |                                                                           |       |              |
| Card Status:                                      |       | Unlocked                                                                  |       |              |
| Operational:                                      |       | Enabled                                                                   |       |              |
| Availability:                                     |       | None                                                                      |       |              |
|                                                   |       | <input type="button" value="Lock"/> <input type="button" value="Unlock"/> |       |              |
| <b>History</b>                                    |       |                                                                           |       |              |
| Element Manager initiated Unlock request received |       |                                                                           |       |              |
| Resetting board                                   |       |                                                                           |       |              |
| Reset complete                                    |       |                                                                           |       |              |
| Initializing network device                       |       |                                                                           |       |              |
| Net initialized                                   |       |                                                                           |       |              |
| Booting cached load via the backplane             |       |                                                                           |       |              |
| Bootloaded successfully                           |       |                                                                           |       |              |
| Application unlocked successfully                 |       |                                                                           |       |              |
|                                                   |       | <input type="button" value="Save"/> <input type="button" value="Clear"/>  |       |              |

- 8 Return to [step 2](#) and repeat this procedure for the next GWC card until all the GWC cards have been unlocked and brought into service. Remember, each GWC node has two GWC cards.
- 9 The procedure is complete.



---

## Lock a GWC card

---

### Purpose of this procedure

This procedure locks a single GWC card, stopping the services, applications, and platform software running on the GWC card.

### When to use this procedure

Use this procedure:

- when you are removing the card from service
- along with procedure [Unlock a GWC card on page 881](#) to reboot a GWC and force a software download
- as part of fault clearing activity to determine if a problem is temporary or persistent
- when you have applied or removed a patch to the GWC software using the Network Patch Manager (NPM) and have created a new GWC software image on the CS 2000 Core Manager.
- when you are removing a GWC node from the CS 2000 GWC Manager database

### Prerequisites

If the card you want to lock is currently active, you need to switch call processing to its mate card in the node. This places the card in standby mode. Refer to procedure “Invoke a manual protection switch (warm swact)” in document *Gateway Controller Security and Administration*, NN10213-611.

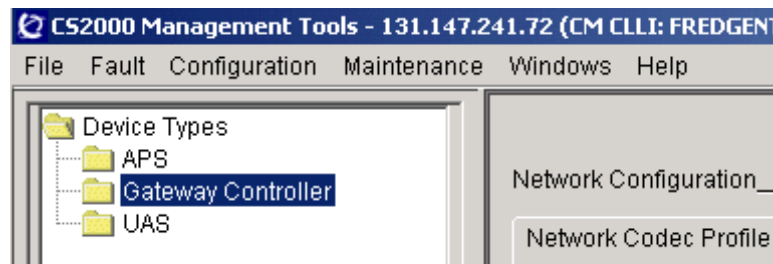
When the card is standby, you need to disable (busy) services on the card. Refer to the procedure “Disable (Busy) GWC card services” in document *Gateway Controller Security and Administration*, NN10213-611.

Once services on a standby card have been disabled, you can proceed with locking the card.

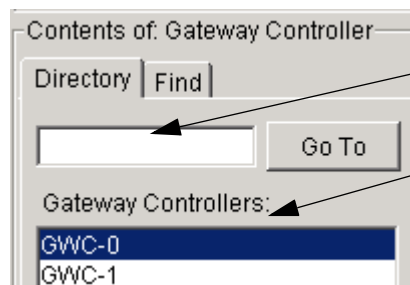
## Action

### *At the CS 2000 GWC Manager client*

- 1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



- 2 From the Contents of: GatewayController frame, select the GWC node that contains the card you want to lock.



Type a GWC node name here,  
or

Select a GWC node from the list  
of provisioned GWC nodes.

- 3 Select the **Maintenance** tab to display maintenance information about the node.

GWC-1 Unit 0: 10.66.17.42  
Unit 1: 10.66.17.43

**Maintenance** Provisioning

GWC-1-UNIT-0

|                       |                |                 |               |
|-----------------------|----------------|-----------------|---------------|
| Administrative state: | unlocked(1)    | Usage state:    | idle(1)       |
| Operational state:    | enabled(1)     | Stand by state: | hotStandby(1) |
| Activity state:       | standby(2)     | Swact state:    | noSwAct(0)    |
| Isolation state:      | notIsolated(2) | Alarm state:    | 00 00 00 00   |
| Available state:      | 00 00 00 00    | Fault state:    | none(0)       |
| Loadname:             | GN080BI        |                 |               |

Save Image Busy (Disable) RTS (Enable) Card View

- 4 Click the **Card View** button for the card you want to lock.

GWC-1-UNIT-1

|                       |                |                 |                                   |
|-----------------------|----------------|-----------------|-----------------------------------|
| Administrative state: | unlocked(1)    | Usage state:    | idle(1)                           |
| Operational state:    | enabled(1)     | Stand by state: | providingService(3)               |
| Activity state:       | active(1)      | Swact state:    | noSwAct(0)                        |
| Isolation state:      | notIsolated(2) | Alarm state:    | critical(1) , alarmOutstanding(4) |
| Available state:      | 00 00 00 00    | Fault state:    | none(0)                           |
| Loadname:             | GN080BI        |                 |                                   |

Save Image Busy (Disable) RTS (Enable) **Card View**

**At the CS 2000 SAM21 Manager client**

- 5 In the card view, select the **States** tab.

The screenshot shows the 'Sam21-2 : Slot 12' window with the 'States' tab selected. The 'Summary' section displays three columns: Critical, Major, and Minor, each with a value of 0. The 'Details' section shows a table with headers: Equip., ID, Time, Type, Severity, and Reason. A sidebar on the left indicates 'GWC-6-UNIT-1' and '12'.

| Critical | Major | Minor |
|----------|-------|-------|
| 0        | 0     | 0     |

| Equip. | ID | Time | Type | Severity | Reason |
|--------|----|------|------|----------|--------|
|--------|----|------|------|----------|--------|

- 6 In the States display, click the **Lock** button to lock the card.

The screenshot shows the 'Sam21-2 : Slot 12' window with the 'States' tab selected. The 'OSI' section displays three fields: Card Status: Unlocked, Operational: Enabled, and Availability: None. The 'Lock' button is highlighted. The 'History' section is empty. A sidebar on the left indicates 'GWC-6-UNIT-1' and '12'.

| Card Status:  | Unlocked |
|---------------|----------|
| Operational:  | Enabled  |
| Availability: | None     |

**Lock** **Unlock**

- 7 Observe the system response in the History window.

The card is locked when you see the text “Application locked successfully” in the History display. The lock icon (circled in the screen shot below) should also be present on the card graphic at the left of the screen:



- 8 If necessary, return to [step 2](#) and repeat this procedure for the next GWC card in the node.
- 9 The procedure is complete.





---

## Powering up a USP

---

### Purpose of this procedure

Use the following procedure to power up a Universal Signaling Processor (USP).

### When to use this procedure

Use this procedure when it is necessary to power up the USP. USP RTC-12 will initially be used to get the shelf back in service.

### Prerequisites

The CS 2000 Core and USP ABS server must be in-service.

### Action

#### Powering up a USP

##### *At the USP shelf*

- 1 Ensure all cards are seated in the USP shelf with the exception of the RTC-15 (slot 15) front panel card on the Control shelf.
- 2 Power up both A/B buttons on the control and extension shelves.
- 3 RTC-12 should SCSI boot and it should come into service within 1-2 minutes of being powered up.

##### *At the USP Manager*

- 4 Once RTC-12 is up, use the USP Manager to uninhibit and activate all links, where applicable. Refer to [Configuring Links on page 895](#).
- 5 Verify logs and alarms to ensure no unexpected problems and perform test calls.
- 6 Verify that all cards on all shelves are up and running with the exception of RTC-15.
- 7 Ensure that the System Date/Time is set to the current local time, if not using SNTP. Refer to [Administration: Date and Time on page 905](#).

##### *At the USP frame*

- 8 Once all cards are up and properly running, reseal RTC-15. RTC-15 should SCSI boot and perform a database synchronization with RTC-12. RTC-15 should come into service in approximately 5-7 minutes.

***At the USP Manager***

- 9 Verify that RTC-15 is in-service and inactive.
- 10 Verify logs and alarms again to ensure no unexpected or undesired events and perform test calls.
- 11 Verify that the USP can communicate with the ABS. From the USP Manager main menu, click on the Administration button and select ABS Settings.
- 12 Select the Test button to initiate a series of tests to ensure the USP can properly communicate with the ABS.
- 13 Check the USP logs for the test results. Troubleshoot ABS connectivity in the event that the tests fail.  
  
**Note:** To assist with troubleshooting, the Logs message will include the nature of the test failure.
- 14 Take a snapshot of the USP, and copy the snapshot to the ABS using the File Manager.
- 15 Using the ABS CM GUI, modify the site information to point to the new snapshot.
- 16 You have completed this procedure.

---

## Configuring Links

---

Links provide the physical connection between two adjacent signaling points in a network. You can add new links and change or delete existing ones.

### Adding Links

To add new links, perform the following steps:

#### *At the OAMP workstation*

- 1 Click **Configuration>mtp>link**.
- 2 Select the **link-type** for this link from the drop down box. Supported link types include:
  - ss7iplink: IP High Speed Link using M2PA, M2UA-SAAL, M2UA-MTP2, or M3UA
  - atmhslink: ATM High Speed Link over T1 or E1 interfaces
  - chanlslink: Channelized links supporting up to 8 channel over E1 or T1.
  - lslink: Low speed link, V.35 or DS0A.
  - Virtuallink: used to connect 2 System Identities on the same USP.
  - mtp2hslink: MTP L2 High Speed Link.
- 3 Click the **system-id** list and select the system identity to be associated with this link.
- 4 Select a linkset from the **linkset-name** list.
- 5 Assign an unused SLC for this link by entering one in the **SLC** box. This code is a logical representation (0 to 15) of a physical link and is agreed upon with the far end node.

An SLC can only be used once per linkset.
- 6 Select a shelf, slot, and port for the link. Click the... button to display a list of available nodes.
- 7 Indicate whether the system should periodically perform signal link testing (SLT). Click the **periodic-slt-option** check box to change the test status (defaults to unchecked, no test).

Click the check box to toggle between checked and unchecked.

- 8 Use the table below to determine the next step, based on the type of link that you are adding.

| If you are provisioning: | Do:                                  |
|--------------------------|--------------------------------------|
| an SS7iplink             | complete step <a href="#">9</a> .    |
| an atmhslink             | proceed to step <a href="#">10</a> . |
| a chanslink              | proceed to step <a href="#">11</a> . |
| an lslink                | proceed to step <a href="#">12</a> . |
| an mtp2hslink            | proceed to step <a href="#">13</a> . |

- 9 For SS7iplink, complete the following steps:
- Click the **protocol** list and select a protocol for this link.
  - Enter the far end destination IP address in the **dest-ipaddress** box.
 

**Note:** The provisioned IP address becomes the primary IP address if the peer is multi-homed. In addition to the primary address, each association on the USP accepts up to four multi-homed IP addresses from the far end.
  - If the protocol for this link is M2UA-SAAL or M2UA-MTP2, enter an interface identifier in the **IID** box.
 

**Note:** The interface identifier needs to match the peer interface identifier for the link.
  - In the **local-port** box, enter the number of the local port. For M3UA links, the port is 2905.
  - In the **remote-port** box, enter the number of the remote port.
  - Click the **sctp-operation-mode** list and select an operation for the link. If you select **server**, the connection starts. If you select **client**, the client establishes the connection.
 

**Note 1:** If client mode is selected, then **sctp-checksum** must be set (the choices are **adler** and **crc32**).

**Note 2:** If the transport protocol is **m2ua** or **m3ua**, then you must set the checksum to **crc32**.
  - Click the **sctp-parms-index** list and select an SCTP parameter index number to associate with this link.
  - Proceed to step [14](#).
- 10 For ATM High-speed Links, complete the following steps:

- a Enter a **port** value of 0 for atmhslinks.
  - b To enable MTP3b, select the **MTPb-option** checkbox.  
*Note:* MTP3b support is introduced in USP10.0 to enable the full ATM HSL functionality. Users must select a high-speed link that is capable of transporting MTP3b messages because not all ATM HSL or terminating nodes support MTP3b.
  - c Enter a VCC value in the **vcc** box. The value must be between 0 and 15 for atmhslinks.
  - d Enter a VPI in the **vpi** box. The default is 0.
  - e Enter a VCI in the **vci** box. The default is 5.
  - f Select a SAAL parameter index from the **saal-param-index** list.  
*Note:* There is no default SAAL parameter index.
  - g Select a SAAL timer index from the **saal-timer-index** list.  
*Note:* There is no default SAAL timer index.
  - h Proceed to step [14](#).
- 11 For channelized links, complete the following steps:
- a Enter a **port** value of 0 for chanlslinks.
  - b Enter a channel in the channel box.
  - c Select a provisioned MTP link timer index from the **l2-timer-index** list.  
The default index is the first available index.  
*Note:* A system-id must be selected prior to selecting the l2-timer-index or a multiple timer list with the same index is displayed.
  - d Select a provisioned MTP link SLT timer index from the **slt-timer-index** list.  
The default index is the first available index.
  - e Indicate whether the system should perform preventive cyclic retransmission (PCR) on the link using the **pcr-option** check box. PCR is recommended for all satellite links, and intercontinental links where the one-way propagation delay is greater than 15 ms. Both the transmitting and receiving

terminal units of the link must use the same error correction method.

**Note:** The default value is unchecked. If PCR is not enabled, the link uses basic error correction at MTP level 2.

- i Select a value between 5 and 20 (representing tenths of a second) in the **l2-t7-timer** box. This value represents the excessive delay of acknowledgement timer. PCR continually re-transmits unacknowledged MSUs until an acknowledgement is received or the T7 timer expires, at which point the link is taken down.

**Note 1:** The default value for the T7 timer is 600 ms.

**Note 2:** Changing the T7 timer value on this screen will not change the T7 timer value for the provisioned timer index. If PCR is selected, the value in the T7 timer box is used for the excessive delay of acknowledgement. If PCR is not selected, the value for T7 in the timer index is used for the excessive delay of acknowledgement.

- ii Select a value between 1 and 50 (representing tenths of a second) in the **pcr-delay** box. This value represents the round trip propagation delay for the link in milliseconds.

The default value is 10, or 1000 ms.

- f Proceed to step [14](#).

## 12 For low-speed link, complete the following steps:

- a Enter a **port** value of 0-3 for Islinks.
- b Select a provisioned MTP link timer index from the **l2-timer-index** list.

The default index is the first available index.

**Note:** A system-id must be selected prior to selecting the l2-timer-index or a multiple timer list with the same index will be displayed.

- c Select a provisioned MTP link SLT timer index from the **slt-timer-index** list.

The default index is the first available index.

- d Indicate whether the system should perform preventive cyclic retransmission (PCR) on the link using the **pcr-option** check box. PCR is recommended for all satellite links, and intercontinental links where the one-way propagation delay is greater than 15 ms. Both the transmitting and receiving

terminal units of the link must use the same error correction method.

**Note:** The default value is unchecked. If PCR is not enabled, the link will use basic error correction at MTP level 2.

- i Select a value between 5 and 20 (representing tenths of a second) in the **l2-t7-timer** box. This value represents the excessive delay of acknowledgement timer. PCR continually re-transmits unacknowledged MSUs until an acknowledgement is received or the T7 timer expires, at which point the link is taken down.

**Note 1:** The default value for the T7 timer is 600 ms.

**Note 2:** Changing the T7 timer value on this screen will not change the T7 timer value for the provisioned timer index. If PCR is selected, the value in the T7 timer box is used for the excessive delay of acknowledgement. If PCR is not selected, the value for T7 in the timer index is used for the excessive delay of acknowledgement.

- ii Select a value between 1 and 50 (representing tenths of a second) in the **pcr-delay** box. This value represents the round trip propagation delay for the link in milliseconds.

The default value is 10, or 1000 ms.

- e Proceed to step [14](#).

**13** For MTP2 High Speed links, complete the following steps:

- a Enter a **port** value of 1 for mtp2hslinks.
- b Select a provisioned MTP link timer index from the **l2-timer-index** list.

The default index is the first available index.

**Note:** A system-id must be selected prior to selecting the l2-timer-index or a multiple timer list with the same index is displayed.

- c Select a provisioned MTP link SLT timer index from the **slt-timer-index** list.

The default index is the first available index.

- d Proceed to step [14](#).

**14** Click **Add**. A confirmation dialog box appears.

**15** Click **Yes** to confirm the change.

## Modifying Links

To edit links, perform the following steps:

### *At the OAMP workstation*

- 1 Click **Configuration>mtp>link**.
- 2 Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to modify. Double click the link to open it in the administration panel and edit active fields as required.
- 3 Click **Modify** to save these link changes. A confirmation dialog box appears.
- 4 Click **Yes** to confirm the change.

## Deleting Links

To delete existing links, perform the following steps:

### *At the OAMP workstation*

- 1 Click **Configuration>mtp>link**.
- 2 Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to delete. Double click the link to open it in the administration panel.
- 3 Click **Delete**. A confirmation dialog box appears.
- 4 Click **Yes** to confirm the change.

## Inhibiting and Uninhibited Links

Inhibit differs from deactivate because an inhibit command does not disrupt traffic. The system finds another link within the linkset before taking the inhibited link down.

To inhibit or uninhibited links, perform the following steps.

### *At the OAMP workstation*

- 1 Click **Configuration>mtp>link**.
- 2 Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to Inhibit. Double click the link to open it in the administration panel.
- 3 Click **Uninhibit** to uninhibit the displayed link, or click **Inhibit** to inhibit the displayed link. A confirmation dialog box appears.



When you uninhibit or inhibit a link, several boxes are updated in the Link Status.

When you successfully uninhibit a link, the **local-inhibit-state** box changes to Uninhibited.

When you successfully inhibit a link, the **local-inhibit-state** box changes to Local Inhibit.

- 4 Click **Yes** to confirm the change.

## Activating and Deactivating Links

You can stop traffic on a link by changing its status to inactive. You can allow traffic on a link by changing its status to active.

To activate or deactivate links, perform the following steps

### *At the OAMP workstation*

- 1 Click **Configuration>mtp>link**.
- 2 Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to activate or deactivate. Double click the link to open it in the administration panel.
- 3 Click **Activate** to activate the displayed link, or click **Deactivate** to deactivate the displayed link. A confirmation dialog box appears

When you activate or deactivate a link, several boxes are updated in the Operational Data section of this window.

- 4 Click **Yes** to confirm the change.

## Understanding Link States

The information displayed in the l3-link-status, activation-state, remote-block-status, local-inhibit-state, remote-inhibit-state, congestion-level, discard-level and level-2-status report information on your links. The system updates all SS7 states once per second.

### **l3-link-status**

The l3-link-status box shows the availability of the link: available or unavailable

### **activation-state**

The activation-state box shows you if the link is active. Possible states are inactive, act-restoring, active, failed, suspended-t17, suspended-card-out-of-service, and initializing.

**remote-inhibit-status**

The remote-inhibit-status refers to links that are inhibited by the far-end node of this link. The remote-inhibit-status box displays the remote inhibit status: remote-inhibit or uninhibited.

**remote-block-state**

The local-block-state refers to links that are inhibited locally. The local-block-state box displays the local inhibit state: remote-blocked or unblocked.

**local-inhibit-state**

The local-inhibit-state refers to links that are inhibited by the near-end node of this link. The local-inhibit-state box displays the local inhibit state: local-inhibit or uninhibited.

**discard-level**

The discard-level ranges from 0 (lowest) through 3 (highest). All messages are assigned a discard priority level. Any messages with a priority level less than the currently displayed discard level are discarded.

**congestion-level**

Measurement of link congestion differs, depending on the protocol used by your system. If your system identity is ANSI-based, link congestion is measured in four levels: 0 (lowest) through 3 (highest). If your system identity is ITU 14-bit based, link congestion is measured in two levels: 0 (lowest) and 1 (highest).

The congestion levels provide a way for the USP to manage messages during times of elevated congestion. Each SS7 message is assigned a congestion priority level. Messages with high priority levels are more likely to be sent, even when congestion is high.

Any messages with a priority level lower than the currently displayed congestion level result in the following actions:

- The system generates a signaling network management (SNM) transfer control message (TFC) to notify the senders of the messages in the network of the congestion status.
- The system checks the discard level.

If the congestion level continues to remain above 0 for an extended period of time, you may need to add a link.

**level-2-status**

The level 2 status for a link appears in the level-2-status box. Possible states are idle, in-service, out-of-service, initial-alignment, aligned-not-ready, aligned-ready, processor-outage, not-aligned, proving, aligned, monitoring, local-processor-outage, remote-processor-outage, both-processor-outage, l2-congestion and unknown.



---

## Administration: Date and Time

---

If your user account has administrative privileges, you can set the date and time information for a system. The date and time information includes month-day-year, hour-minute-second, and time zone data. In addition, you can configure the system to automatically adjust the clock settings when daylight savings time begins and ends.

You need to manually reset the date/time information if both of the RTC system nodes should go offline at the same time for any length of time. This usually occurs for one of the following reasons:

- if you perform a restore operation
- if you perform a complete office recovery (COR) on your system
- if your system is booted from an alternate boot data snapshot

You can set your USP to use the simple network time protocol (SNTP) to query a network time protocol server. Each time the USP queries the network time protocol server, the USP resets its time accordingly. The SNTP protocol enables the USP to obtain the accurate time of day and keep the same time as other elements in the network.

**Note:** If SNMP is not enabled for your system, verify the time settings for your system weekly to ensure that the system time is synchronized with the time on your OAMP workstation.

### Setting Date/Time information

#### *At the OAMP workstation*

- 1 Click **Administration>Date/Time** window. The current date and time settings for the system appear.
- 2 Determine if you want your USP to use the simple network time protocol (SNTP).

| If: | Do:                                 |
|-----|-------------------------------------|
| No  | Proceed to <a href="#">step 3</a> . |

|    | If:                                                                                                                                                                                        | Do:                                                                                                                                                                                                                                                        |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | Yes, user defined                                                                                                                                                                          | Check Enable SNTP Time Sync (User defined) in the SNTP portion of the window. Add an IP address for the SNTP server in the SNTP Server Address field. The information in the Time portion of the window is greyed out. Proceed to <a href="#">step 5</a> . |
| 3  | To set the date, click the calendar icon and highlight the day corresponding to today's date.                                                                                              |                                                                                                                                                                                                                                                            |
| 4  | To set the time of day, click the clock icon. Use the spin boxes to set hour, minutes and seconds.                                                                                         |                                                                                                                                                                                                                                                            |
| 5  | To set the local time zone, click the <b>Time Zone</b> drop-down menu. A world-wide list of time zones appears. Select the time zone listing that matches the local time zone.             |                                                                                                                                                                                                                                                            |
|    | <b>Note:</b> The daylight savings time boxes are unavailable when the time zone you select does not use daylight savings time.                                                             |                                                                                                                                                                                                                                                            |
| 6  | To enable or disable the automatic system clock adjustment for daylight savings time, click the <b>Adjust clock for daylight savings changes</b> box.                                      |                                                                                                                                                                                                                                                            |
|    | <b>Note:</b> If you are enabling the automatic system clock adjustment for daylight savings time for the first time, make sure you perform steps <a href="#">7</a> to <a href="#">13</a> . |                                                                                                                                                                                                                                                            |
| 7  | Set the starting month for daylight savings time, click <b>dst-start-month</b> . Select the month in which daylight savings time starts.                                                   |                                                                                                                                                                                                                                                            |
| 8  | Set the starting day in the <b>dst-start-day</b> spinbox.                                                                                                                                  |                                                                                                                                                                                                                                                            |
| 9  | Set the starting hour in the <b>dst-start-hour</b> spinbox.                                                                                                                                |                                                                                                                                                                                                                                                            |
| 10 | Set the ending month for daylight savings time, click <b>dst-end-month</b> . Select the month in which daylight savings time ends.                                                         |                                                                                                                                                                                                                                                            |
| 11 | Set the ending day in the <b>dst-end-day</b> spinbox.                                                                                                                                      |                                                                                                                                                                                                                                                            |
| 12 | Set the ending hour in the <b>dst-end-hour</b> spinbox.                                                                                                                                    |                                                                                                                                                                                                                                                            |
| 13 | Click <b>OK</b> .                                                                                                                                                                          |                                                                                                                                                                                                                                                            |

---

## Powering up a Media Gateway/Multiservice Switch 15000

---

### Purpose of this procedure

Use the following procedure to power up a Media Gateway/Multiservice Switch 15000.

### When to use this procedure

Use this procedure when it is necessary to power up a Media Gateway/Multiservice Switch 15000.

### Prerequisites

None

### Action

#### Powering up a Media Gateway/Multiservice Switch 15000

##### *At the chassis*

- 1 Breaker interface panels (BIPs) are located at the top of the chassis. Switch on the breakers on each BIP. The system should come up on its own.  
  
**Note:** In the event that the CP card or its disk becomes unserviceable, the backup-up provisioning data and software will be downloaded from the MDM backup copy and SDS site, respectively.
- 2 You have completed this procedure.





---

## Powering up a Media Gateway/Multiservice Switch 7400

---

### Purpose of this procedure

Use the following procedure to power up a Media Gateway/Multiservice Switch 7400.

### When to use this procedure

Use this procedure when it is necessary to power up a Media Gateway/Multiservice Switch 7400.

### Prerequisites

All power supply switches must be in the standby position.

### Action

#### Powering up a Media Gateway/Multiservice Switch 7400

##### *At the chassis*

- 1 Disengage all processor cards from the backplane of the shelf.
- 2 Engage the minimum number of processor cards required, based on the number of power supplies in the shelf.
  - If you have one power supply, engage a CP in slot 0 and at least one FP.  
  
Do not engage more than seven FPs. Ensure that all other processors are disengaged.
  - If you have two power supplies, engage at least one CP and two FPs. Or, engage two CPs and at least one FP.
- 3 Turn on the circuit breakers for the outlets that supply power to your switch.
- 4 Verify that the LEDs on all power supplies are red.
- 5 Apply power to one of the power supplies by setting its power switch to the on position. Verify that the power supply LED is green.  
  
Normal operation is not guaranteed if there are no processor cards in the shelf. If you have not installed any processor cards before you switch on a power supply, the system does not supply power to the shelf and the power supply LED remains red.
- 6 Verify that the cooling unit LED is green and is operational. You should be able to hear the fans start to rotate.

- 7** If necessary, apply power to a second and third power supply by setting their power switches to the on position. Verify that the LED for each power supply is green.

If you install eight or more FPs, you must use a second power supply. If your system contains fewer than eight FPs, the system uses the second power supply for redundancy.
- 8** If necessary, engage the remaining processor cards.
- 9** Verify the LED color on each FP is appropriate.
- 10** Verify that the appropriate LEDs are illuminated on termination panels.
- 11** You have completed this procedure.

---

## Powering up the MDM workstation

---

### Purpose of this procedure

Use the following procedure to power up the MDM Sun Fire™ V480 workstation.

### When to use this procedure

Use this procedure when it is necessary to power up the MDM workstation.

### Prerequisites

An MDM user account is required.

### Action

#### Powering up the MDM workstation

##### *At the workstation*

- 1 Switch the workstation on.
- 2 Once the workstation has started, login with an MDM user account and ensure that the MDM toolset is available.
- 3 You have completed this procedure.



---

## Powering up an SPM device

---

### Purpose of this procedure

This procedure details the sequence of steps necessary to power up a Spectrum Peripheral Module (SPM), Media Gateway 4000 (MG 4000), Interworking Spectrum Peripheral Module (IW-SPM), or Dynamic Packet Trunking Spectrum Peripheral Module (DPT-SPM).

### When to use this procedure

Use this procedure when it is necessary to power up the SPM/MG 4000/IW-SPM/DPT-SPM.

### Prerequisites

None.

### Action

#### *At the MAP terminal*

- 1 Restore power to the frame and re-insert the fuses.
- 2 Reseat the SIM cards if they were unseated and turn them on one at a time using the switches on the front.
- 3 Reseat any unseated cards in the shelves.
- 4 Post the SPM/MG 4000/IW-SPM/DPT-SPM by typing  
**>MAPCI;MTC;PM;POST SPM <spm\_no>**  
and pressing the Enter key.  
where  
**spm\_no**  
is the number of the SPM/MG 4000/IW-SPM/DPT-SPM
- 5 Select and RTS the CEMs by typing  
**>SELECT CEM ALL;BSY ALL; LOADMOD ALL;RTS ALL**  
and pressing the Enter key.
- 6 Select and RTS the SRM, OC3 RMs, ATM RMs, and/or GEM RMs by typing  
**>QUIT;SELECT <rm\_type> ALL;BSY ALL;LOADMOD ALL;RTS ALL**  
and pressing the Enter key.  
where

**rm\_type**

is either SRM, OC3, ATM, or GEM

**Note:** To RTS the ATM, use the BSY FORCE and RTS FORCE commands.

- 7 Bring the carriers into service by typing

```
>QUIT ALL;MAPCI;MTC;TRKS;CARRIER;POST SPM
<spm_no>;BSY ALL;RTS ALL
```

and pressing the Enter key.

where

**spm\_no**

is the number of the SPM/MG 4000/IW-SPM/DPT-SPM

- 8 Post and recover the trunks on the SPM at the TTP level by typing

```
>QUIT ALL;MAPCI;MTC;TRKS;TTP;PRADCH;POST AD SPM
<spm_no>;BSY ALL;RTS ALL
```

and pressing the Enter key, followed by typing

```
>QUIT ALL;MAPCI;MTC;TRKS;TTP;POST D SPM
<spm_no>;BSY ALL;RTS ALL
```

and pressing the Enter key.

where

**spm\_no**

is the number of the SPM/MG 4000/IW-SPM/DPT-SPM

- 9 Return to the PM level and post the SPM by typing

```
>QUIT ALL;MAPCI;MTC;PM;POST SPM <spm_no>
```

and pressing the Enter key.

where

**spm\_no**

is the number of the SPM/MG 4000/IW-SPM/DPT-SPM

- 10 Select and RTS the remaining RMs by typing

```
>SELECT <rm_type> ALL;BSY ALL;LOADMOD ALL;RTS
ALL
```

and pressing the Enter key.

where

**rm\_type**

is DLC, DSP, VSP, and ALM

- 11 You have completed this procedure.

---

## Powering up the MCS servers

---

### Purpose of this procedure

This procedure details the steps needed to power up the 8 MCS servers. The database server should be brought into service before any other servers. If other servers come up first, restart the management server.

### When to use this procedure

Use this procedure to power up and recover the MCS servers from a power outage.

### Prerequisites

None

### Action

#### *At the frame housing the MCS servers*

1

#### **ATTENTION**

The following shows the preferred order, which is not the way the system comes up if all servers are powered on at the same time.

Power on the database server by turning on the circuit breakers that provide power to the servers. It takes from 5 to 8 minutes for the server to boot and load Oracle.

2

After the DBSvr powers on, telnet to the box and run a spot check to make sure it is ready.

- a Make sure Oracle is loaded. The best way is to telnet to the database. Type: **sqlplus** and fill in the username and password (in other words, log in as *user*, not *root*). If Oracle is running, you should receive the `SQL>` command prompt. Type **quit** to exit from sqlplus.
- b Verify that the snmp service is running on the database box. Type: **ps -ef | grep snmp**. You should see three snmp processes:

```
/usr/local/sbin/snmpd -f udp:161
```

```
/bin/sh
```

```
/opt/app/oracle/product/9.2.0/bin/dbsnmpwd
```

```
/opt/app/oracle/product/9.2.0/bin/dbsnmp
```

The snmp processes are not critical to getting the system up. However, if any of the snmp processes are not running, you will not be able to see accurate reporting of this box on the System Management Console.

- c To stop or start oracle, telnet to the database as sysadmin and then su to root. Go to the following directory: `/etc/init.d`. The stop command is **`./dbora stop`**. The start command is **`./dbora start`**. These commands will severely affect service.
- 3 Verify that the SysMgr processes on the MgmtSvr/AcctMgr box are running in order to control the MCS components from the System Management Console. Telnet to the MgmtSvr/AcctMgr box as *nortel*.

- a Make sure that the SysMgr processes are running by typing: **`meinit -p`**. You should see three processes running. If any of these processes are not running, you will not be able to launch the System Management Console:

```
Rel2.0 NTme_pids mgmtsvr mgmtsvr.3
```

```
Rel2.0 NTme_pids tsscma tsscma.5
```

```
Rel2.0 NTme_pids tssfpma tssfpma.6
```

- b To stop or start the SysMgr, go to the following directory: `IMS/mgmtsvr/bin/mgmtsvr/` and type: **`./MgmtSvrShutdown.pl`**. This will kill any (or all) of the SysMgr processes.
  - c To start the SysMgr, stay in the same directory and type: **`MgmtSvrConfigSetup.pl`**. This will try to start all three processes. You will see a messages on the telnet session that say something like “starting tsscma waiting 30 seconds.” The tssfpma process will start next, followed by the mgmtsvr processes.
  - d If you want to watch the SysMgr startup logs, after performing step b above, go to the following directory: `/var/Rel2.0/mgmtsvr`. Then type: **`tail -f mgmtsvr.3.log`**.
  - e Verify that the snmp process is running on the MgmtSvr/AcctMgr box by typing: **`ps -ef | grep snmp`**.  
You should see one process running:  
`/usr/local/sbin/snmpd -f udp:161`. If this process is not running or you get an alarm from the System Management Console that there is a problem with the





- e Restart the Provisioning component. The best way to see if the Provisioning Module is behaving properly is to log in to the ProvClient. Launch a web browser to the IP address of the box where the Provisioning Module is deployed, such as <http://192.168.0.10/prov>. Log in as admin/admin and attempt any of the List options in the navigation tree, for example, List Devices or List Users. If the browser doesn't respond properly, then restart the Provisioning Module by right clicking on the Provisioning component in the System Management Console and select **Restart**. Confirm the request.
- f Restart the WebClientMgr component. Log in to the Personal Agent through your browser, such as <http://192.168.0.10/pa>. Log in as a subscriber, such as myusername@mydomain.com, and enter the subscriber's password. The Personal Agent should appear for that subscriber. If it does not, or the interface does not seem to respond correctly, restart the Provisioning Module described in 4e above. (If you've already restarted it once and the ProvClient interface seems ok, but the Personal Agent interface is still not working correctly, it is probably a configuration issue.
- g Launch the WebClient GUI from inside a subscriber's Personal Agent page. Attempt to log in to the WebClient when the System Management Console completes loading.

---

## Powering up an RTP Media Portal

---

### Purpose of this procedure

Use the following procedure to power up an RTP Media Portal. The RTP Media Portal shelves are powered from either a PDU or EBIP located at the top of the frame depending on if the frame is AC or DC powered.

### When to use this procedure

Use this procedure when it is necessary to power up the chassis that houses the RTP Media Portal.

### Prerequisites

None

### Action

#### Powering up the RTP Media Portal

##### *At the frame housing the RTP Media Portal*

- 1 For DC powered shelves, switch the circuit breakers at the EBIP that provide power to the shelf being powered to the *ON* position. The breaker will have the '1' side (top) of the breaker depressed.
- 2 For AC powered shelves, push the rocker located on the top of the AC outlet to apply power to the chassis. It should be switched to the "I" position.
- 3 Once the breaker are switched *ON* at the power source, power up the shelf by switching the breaker on the back of the chassis to the *ON* position.
- 4 Observe the System, Power/Fan, Slot (filled) and Host Card LEDs as the unit is being powered. Once power on is complete, the should all have a steady green color.
- 5 You have completed this procedure.



---

## Powering up the IPmedia 2000 shelves

---

### Purpose of this procedure

Use the following procedure to power up the IPmedia 2000 shelves that house the MS 2000 series devices and the Packet Media Anchor. The IPmedia 2000 shelves reside in either a SAMF frame or CCF, depending on whether or not your solution uses the CS 2000 or CS 2000-Compact.

### When to use this procedure

Use this procedure when it is necessary to power up the IPmedia 2000 shelves.

### Prerequisites

None

### Action

#### Powering up the Media Server 2000 servers

##### *At the CCF or SAMF frame*

- 1 Open the front door of the CCF/SAMF frame.
- 2 At the EBIP at the top of the frame, turn the breaker associated the Media Server to the ON position.
- 3 Ensure that the Green Power LED on the front of the Nortel Media Server 2000 is on (right hand side of the card).  
After 1 to 2 minutes, the Green LED on the left hand side of the card lights.
- 4 Verify the status of the LEDs on the front of the Nortel Media Server 2000:
  - Red Fail LED is off (left hand side of the board).
  - ACT LED is on (left hand side of the board).

**Note:** It may take up to 60 seconds for the ACT LED to light up.

- Blue LED does not remain on (right hand side of the board).
- PWR LED is on (right hand side of the board).
- Both Ethernet Link LEDs are on (middle of the board).

**Note:** The Ethernet LEDs are Green when indicating a connection, and Orange when indicating activity.

**Note:** Check the Media Server 2000 to make sure it is set to an unlocked state.

- 5 You have completed this procedure.

---

## Powering up the SAM16 shelves

---

### Purpose of this procedure

Use the following procedure to power up the SAM16 shelves that house the UAS devices. The SAM16 shelves reside in either a SAMF frame or CCF, depending on whether or not your solution uses the CS 2000 or CS 2000-Compact.

### When to use this procedure

Use this procedure when it is necessary to power up the SAM16 shelves.

### Prerequisites

None

### Action

#### Powering up the SAM16 shelves

##### *At the CCF or SAMF frame*

- 1 Open the front door of the CCF/SAMF frame.
- 2 At the EBIP at the top of the frame, turn the breakers associated the SAM16 to the ON position.
- 3 You have completed this procedure.





---

## Powering up an MG 9000 device

---

### Purpose of this procedure

Use the following procedure when power to the MG 9000 has been lost.

### When to use this procedure

Use this procedure when it is necessary to power up the MG 9000 frame.

### Prerequisites

None

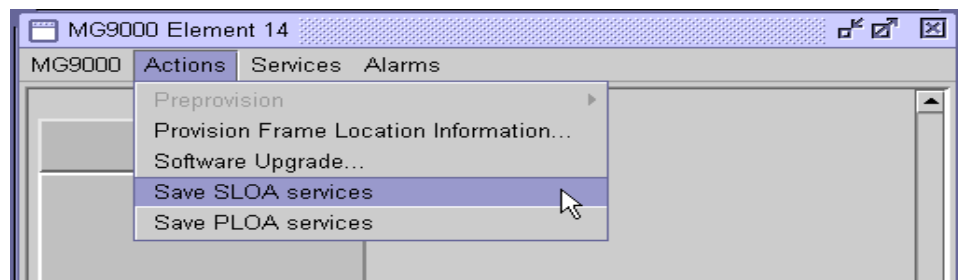
### Action

#### Recovering an MG 9000 that has lost power and cannot communicate with the MG 9000 Manager

##### *At the MG 9000 Manager*

- 1 At the Subnet View of the MG 9000 Manager, select the MG 9000 to be re-commissioned. A warning window indicating that your connection to the gateway is down may appear. This will not block the saving of services information.
- 2 Save a copy of the MG 9000 Manager SLoA provisioning data as follows (you'll be re-entering this data later):
  - a To Save the SLoA services provisioning data, at the Frame (Element) view, select the "Save SLOA services" option from the Actions menu.

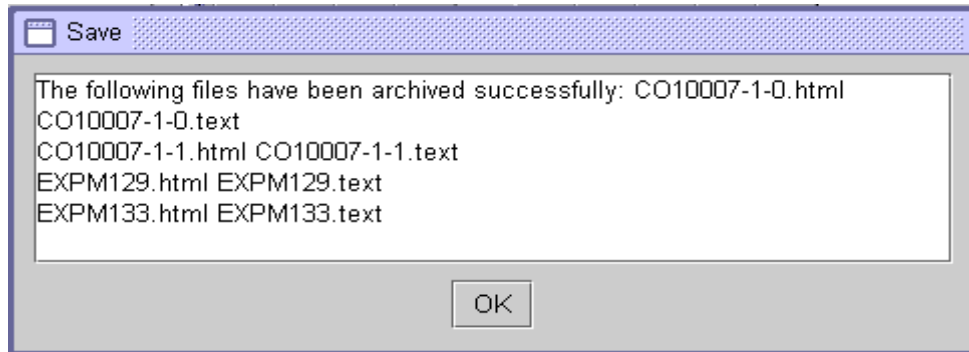
##### Frame View



An acknowledgment window appears in response to this request. The acknowledgment window contains the name of the two files (with .html and .text suffixes) where your data had been stored on the MG 9000 Manager.

- b** Record the file name provided in the Save acknowledgement window for later use.

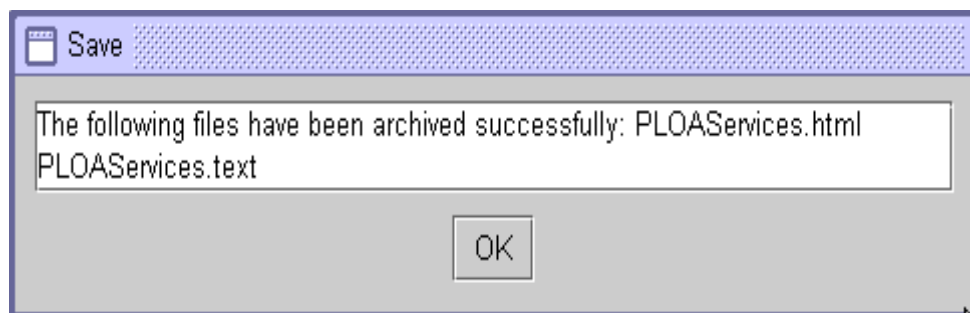
## Save acknowledgement message for SLoA



- 3** Save a copy of the MG 9000 Manager PLoA provisioning data as follows (you'll be re-entering this data later):
  - a** To save the PLoA services provisioning data, at the Frame (Element) view, select the “Save PLOA services” option from the Actions menu.

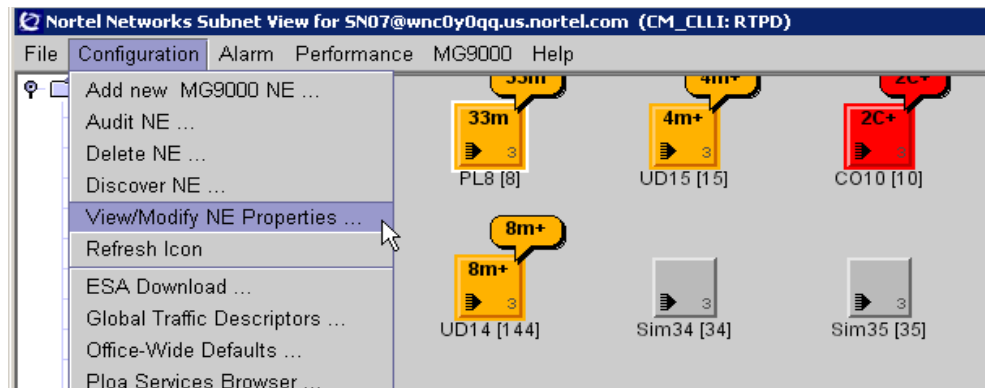
An acknowledgment window appears in response to this request. The acknowledgment window contains the name of the files where your data had been stored on the MG 9000 Manager.
  - b** Record the file name provided in the Save acknowledgement window for later use.

## Save acknowledgement message for PLoA



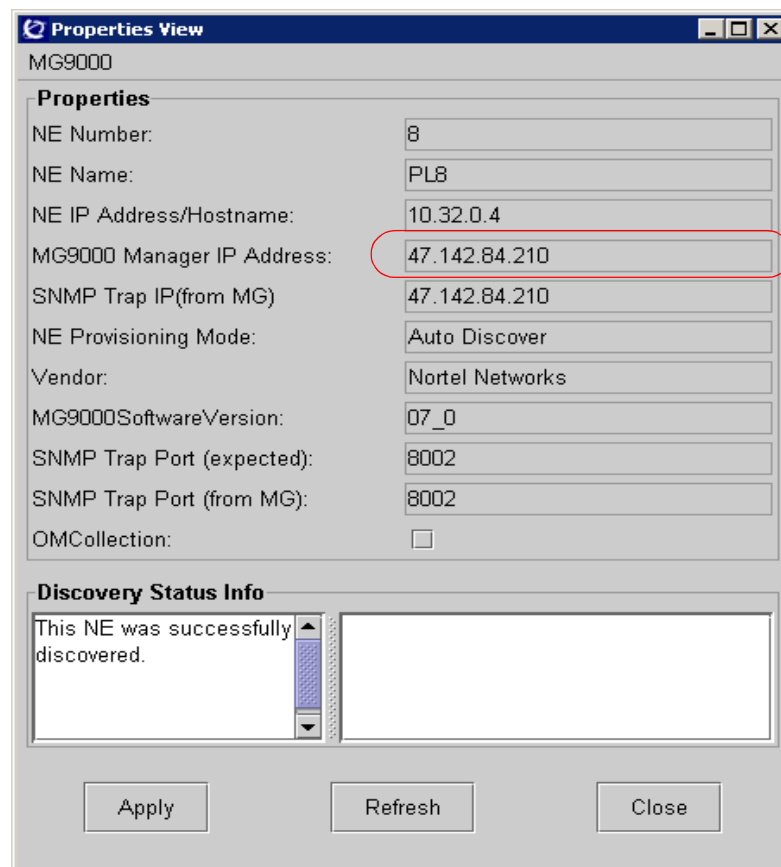
- 4 Obtain the IP address of the MG 9000 Manager server (not the mid-tier or client). At the Subnet View, select Configuration->View/Modify NE Properties from the menu bar.

## Subnet View accessing Configuration ->View/Modify NE Properties



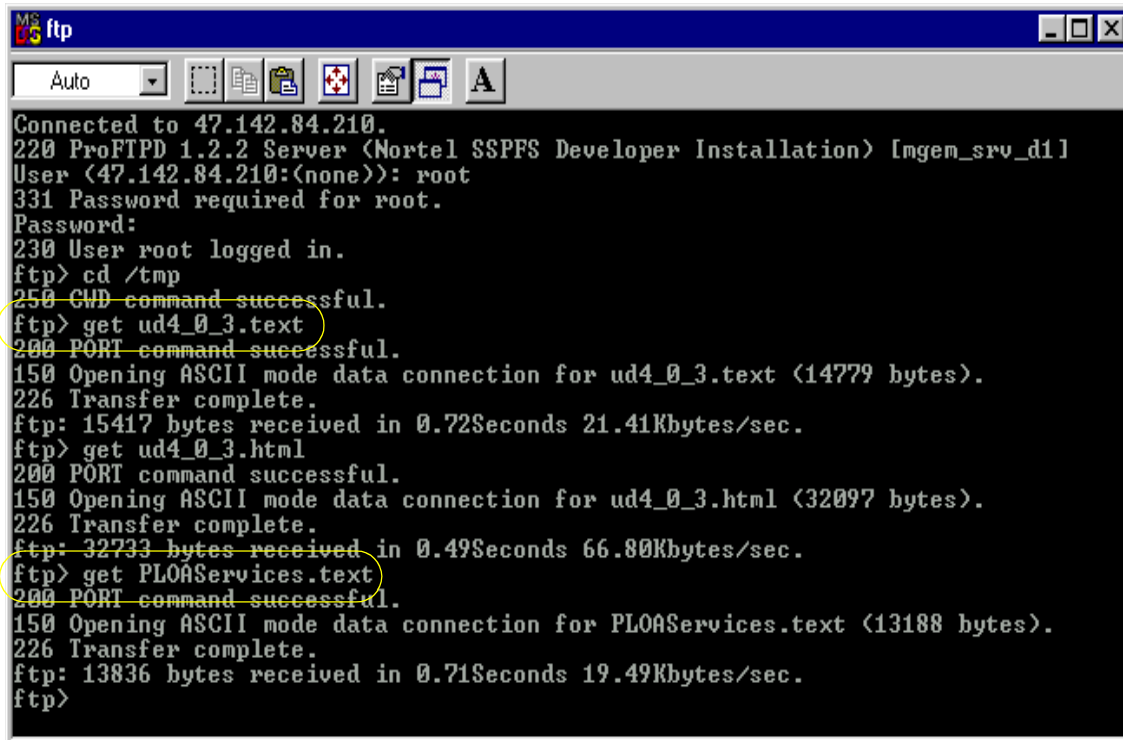
- 5 Record the IP address in the MG 9000 Manager IP Address field.

## Properties View



- 6 FTP to the address recorded in step 5 and copy the files in the /tmp directory to a secure location, such as your desktop or permanent server before proceeding.

## FTP files to secure location



The screenshot shows a Windows-style window titled "ftp" with a standard toolbar. The command prompt inside the window displays the following text:

```
Connected to 47.142.84.210.
220 ProFTPD 1.2.2 Server (Nortel SSPFS Developer Installation) [mgem_srv_d1]
User (47.142.84.210:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> get ud4_0_3.text
200 PORT command successful.
150 Opening ASCII mode data connection for ud4_0_3.text (14779 bytes).
226 Transfer complete.
ftp: 15417 bytes received in 0.72Seconds 21.41Kbytes/sec.
ftp> get ud4_0_3.html
200 PORT command successful.
150 Opening ASCII mode data connection for ud4_0_3.html (32097 bytes).
226 Transfer complete.
ftp: 32733 bytes received in 0.49Seconds 66.80Kbytes/sec.
ftp> get PLOAServices.text
200 PORT command successful.
150 Opening ASCII mode data connection for PLOAServices.text (13188 bytes).
226 Transfer complete.
ftp: 13836 bytes received in 0.71Seconds 19.49Kbytes/sec.
ftp>
```

### *At the MG 9000 frame*

- 7 Power up the shelves in the frame by reinstalling the fuse modules on the IBIP. Restore all fuses left to right in the frame.
- 8 Connect a laptop PC to the active DCC card and launch the local craft interface (LCI).
- 9 Wait for the restart to complete and for all cards initialize, typically takes 5 minutes. The Administrative State of all common cards will be Locked.
- 10 From the LCI, Unlock the active DCC OC-3/DS1 IMA card by selecting the Admin. State Unlock radio button. Wait for the status at the LCI to change to Enabled, Online, and Unlocked.
- 11 From the LCI continue to unlock the common cards in the following order until all are unlocked and online:
  - active ITX
  - active ITP
  - OC-3 carriers on the active OC-3 DCC card
  - inactive DCC

- inactive ITX
- inactive ITP
- OC-3 carriers on the inactive OC-3 DCC card
- DS1 cards (if provisioned)
- ABI cards (if provisioned)

**12** Initiate rediscovery by sending a cold start trap from the LCI.

***At the MG 9000 Manager***

**13** Monitor the MG 9000 network element and wait until the discovery process is complete.

**14** Wait for the network element to show it is operational, then check for dial tone.

**15** This procedure is complete.



## CS 2000 Management Tools fault procedures

The fault procedures available for the CS 2000 Management Tools are listed under the following categories:

- [Alarms on page 931](#)
- [Audit on page 932](#)
- [Line maintenance on page 932](#)
- [Trunk maintenance on page 932](#)
- [Logs on page 933](#)
- [Hardware on page 933](#)
- [Communications on page 934](#)
- [CS 2000 Management Tools server and SSPFS on page 934](#)
- [Downgrading the CS 2000 Management Tools software on page 935](#)

### Alarms

The table below lists the available procedures related to alarms.

#### Alarms procedures

| Procedure                                                          | Page |
|--------------------------------------------------------------------|------|
| <a href="#">CS 2000 Management Tools fault management overview</a> | 937  |
| <a href="#">Accessing the Alarm Manager</a>                        | 943  |
| <a href="#">Retrieving details about an alarm</a>                  | 951  |
| <a href="#">Accessing the Alarm History</a>                        | 955  |
| <a href="#">Filtering alarms</a>                                   | 957  |
| <a href="#">Resetting the filters for alarms</a>                   | 961  |
| <a href="#">Defining alarms using the NPM</a>                      | 963  |
| <a href="#">Enabling and disabling alarms using the NPM</a>        | 971  |

## Audit

The table below lists the available procedures related to the audit.

### Audit procedures

| Procedure                           | Page |
|-------------------------------------|------|
| <a href="#">Performing an audit</a> | 973  |

## Line maintenance

The table below lists the available procedures related to line maintenance using the Line Maintenance Manager (LMM).

### Line maintenance procedures

| Procedure                                                          | Page |
|--------------------------------------------------------------------|------|
| <a href="#">Posting a line by directory number</a>                 | 995  |
| <a href="#">Posting a line by gateway</a>                          | 997  |
| <a href="#">Busying a line</a>                                     | 1001 |
| <a href="#">Installation busying a line</a>                        | 1003 |
| <a href="#">Force releasing a line</a>                             | 1005 |
| <a href="#">Returning a line to service</a>                        | 1007 |
| <a href="#">Clearing one or more posted lines from the display</a> | 1009 |
| <a href="#">Retrieving line properties</a>                         | 1011 |
| <a href="#">Querying line gateways in a trouble state</a>          | 1013 |

## Trunk maintenance

The table below lists the available procedures related to trunk maintenance using the Trunk Maintenance Manager (TMM).

### Trunk maintenance procedures

| Procedure                                                                        | Page |
|----------------------------------------------------------------------------------|------|
| <a href="#">Performing trunk maintenance using the Trunk Maintenance Manager</a> | 1019 |
| <a href="#">Posting PRI Group D-channels</a>                                     | 1041 |



## Trunk maintenance procedures

| Procedure                                              | Page |
|--------------------------------------------------------|------|
| <a href="#">Displaying trunk CLLI codes by gateway</a> | 1045 |
| <a href="#">Performing an ISUP Continuity Test</a>     | 1047 |

## Logs

The table below lists the available procedures and information related to logs.

**Note:** For details on the logs that can be generated, refer to the Carrier Voice over IP Fault Management Logs Reference document, NN10275-909.

## Logs procedures

| Procedure                                                        | Page |
|------------------------------------------------------------------|------|
| <a href="#">Routing customer logs to a remote host</a>           | 1049 |
| <a href="#">Configuring log reporting</a>                        | 1053 |
| <a href="#">Viewing debug logs</a>                               | 1057 |
| <a href="#">Viewing OMPUSH logs</a>                              | 1059 |
| <a href="#">Viewing customer logs on an SSPFS-based server</a>   | 1061 |
| <a href="#">Disabling local logging of SSPFS platform faults</a> | 1063 |

## Hardware

The table below lists the available procedures related to hardware.

## Hardware procedures

| Procedure                                                                         | Page |
|-----------------------------------------------------------------------------------|------|
| <a href="#">Replacing one or more failed disk drives on an SSPFS-based server</a> | 1067 |
| <a href="#">Replacing a DVD drive on an SSPFS-based server</a>                    | 1079 |
| <a href="#">Cleaning the DAT drive on the Netra T1400</a>                         | 1083 |

## Communications

The table below lists the available procedures related to communications.

### Communications procedures

| Procedure                                                                                                                         | Page |
|-----------------------------------------------------------------------------------------------------------------------------------|------|
| <a href="#">Re-establishing the connection between the NPM GUI and the server</a>                                                 | 1085 |
| <a href="#">Restoring SSH communication between the CS 2000 Management Tools server and the core manager</a>                      | 1087 |
| <a href="#">Correcting a CORBA configuration issue between the CS 2000 Management Tools server and the MG 9000 Manager server</a> | 1091 |

## CS 2000 Management Tools server and SSPFS

The table below lists the available procedures related to the CS 2000 Management Tool server and the Succession Server Platform Foundation Software (SSPFS).

### CS 2000 Management Tools server and SSPFS procedures

| Procedure                                                                   | Page |
|-----------------------------------------------------------------------------|------|
| <a href="#">Verifying the state of a cluster</a>                            | 1101 |
| <a href="#">Initiating a manual failover on a Sun Netra 240 server pair</a> | 1107 |
| <a href="#">Querying the state of the SSPFS platform</a>                    | 1109 |
| <a href="#">Rebooting an SSPFS-based server</a>                             | 1113 |
| <a href="#">Shutting down an SSPFS-based server</a>                         | 1115 |
| <a href="#">Executing a fallback during an SSPFS-based server upgrade</a>   | 1119 |

## Downgrading the CS 2000 Management Tools software

The table below lists the available procedures related to downgrading the CS 2000 Management Tool software on an SSPFS-based server

### Downgrading the CS 2000 Management Tools software

| Procedure                                                                    | Page |
|------------------------------------------------------------------------------|------|
| <a href="#">Downgrading the CS 2000 Management Tools software</a>            | 325  |
| <a href="#">Performing a full system restore on an SSPFS-based server</a>    | 331  |
| <a href="#">Restoring the oracle data on an SSPFS-based server</a>           | 337  |
| <a href="#">Restoring NPM patch files</a>                                    | 1123 |
| <a href="#">Performing a restore of APS audio files from tape</a>            | 343  |
| <a href="#">Performing a restore of APS audio files from CD</a>              | 345  |
| <a href="#">Performing an APS-only Data Base Restore from a 4mm DAT</a>      | 1129 |
| <a href="#">Performing an APS-only Database restore from a CD</a>            | 1131 |
| <a href="#">Cloning the image of one node in a cluster to the other node</a> | 351  |



---

## CS 2000 Management Tools fault management overview

---

### Fault management strategy

The Succession Server Platform Foundation Software (SSPFS) on the CS 2000 Management Tools server consists of several common components, including a fault management sub-system. The network elements forward their alarms to the fault management sub-system using standard SNMP traps. The alarm sub-system consolidates the alarms from the network elements and provides the user with the ability to monitor both active and historical alarms.

The SSPFS platform also has a fault detection and reporting mechanism for a power supply failure, disk failure, file system over usage, memory over usage, CPU load over usage, swap space over usage, fan failure, network connectivity failure, and high temperature. The SSPFS fault detection and reporting mechanism is integrated with the alarm utility, which has the following capabilities:

- keeps track of alarms on the platform
- lights a light when an alarm is raised and extinguishes the light when the alarm is cleared (if no other alarms are present)
- writes a customer log that corresponds to the state of an alarm
- stores information about all the alarms on the system in its database, which can be queried by a user at any time

### User interface

A user can perform fault management using one of the following interfaces:

- A user can view and filter NE alarms through the CS2000 Management Tools GUI.
- A user can use the Integrated Element Management System (EMS) GUI, which provides a consolidated historical and a real-time view of the events that have occurred in a CS 2000 central office. For details on the Integrated EMS, refer to the Fault Management section of the Integrated EMS User Guide, NN10329-111.
- A user can view SNMP-based traps that arrive from Succession Element Sub-network Manager (SESM)-based managed devices into the “/var/log/ptmlog” file.
- A user can query the SSPFS platform alarms through the SSPFS command line interface (CLI) tool.

## CS2000 Management Tools GUI

The CS2000 Management Tools GUI provides both an Alarm Manager and an Alarm History window for viewing and filtering alarms. Active alarms are typically viewed with the Alarm Manager, while the Alarm History window provides both active and inactive alarms. Both provide information on alarms in a tabular format. There are methods for filtering alarms to show only alarms for a particular network element, of a particular severity or alarm category.

### Alarm severity color codes

Based on alarm severity, each alarm has an associated color code as shown in figure [Alarm Severity Color Codes](#).

- Critical and major - red
- Minor - amber
- Warning - yellow

### Alarm Severity Color Codes

|                                                                                     |       |                  |                     |          |                |
|-------------------------------------------------------------------------------------|-------|------------------|---------------------|----------|----------------|
|    | UAS-S | Processing Error | 2001-08-31 18:17:11 | Minor    | Software Error |
|    | UAS-S | Processing Error | 2001-09-11 08:31:33 | Critical | Software Error |
|   | UAS-S | Processing Error | 2001-09-11 08:31:33 | Major    | File Error     |
|  | UAS-S | Processing Error | 2001-09-11 08:31:33 | Minor    | Software Error |
|  | UAS-S | Processing Error | 2001-09-11 08:31:33 | Warning  | Software Error |

### Alarm totals

The Alarm Manager provides an alarm summary of the total number of active alarms, as well as the specific number of alarms for each severity (for example, Critical, Major, Minor, and Warning). This summary is located in the lower left-hand corner of the alarm manager below the "Raw Alarm List". The Alarm History browser provides the total number of alarms, but does not show the number of alarms for any severity. In addition, both the Alarm Manager and the Alarm History windows include the time the display was last updated.

## Raw Alarm List

| File Actions                                                                      |                 |                |                      |          |                           |
|-----------------------------------------------------------------------------------|-----------------|----------------|----------------------|----------|---------------------------|
| Raw Alarm List                                                                    |                 |                |                      |          |                           |
|                                                                                   | Network Element | Category       | Alarm Time           | Sever... | Probable Cause            |
|  | GWC-32-UNIT-1   | Communications | 22:18:58 04-二月-20... | Major    | Underlying resource un... |
|  | GWC-32-UNIT-1   | Communications | 22:18:58 04-二月-20... | Major    | Underlying resource un... |
|  | SNMP_NE_Poller  | Communications | 15:24:41 18-二月-20... | Major    | Communications subsy...   |
|  | GWC-64-UNIT-1   | Communications | 14:48:22 10-二月-20... | Minor    | LAN error                 |
|  | GWC-32-UNIT-0   | Communications | 19:17:56 05-二月-20... | Major    | Underlying resource un... |
|  | GWC-32-UNIT-0   | Communications | 19:17:56 05-二月-20... | Major    | Underlying resource un... |
|  | GWC-32-UNIT-0   | Communications | 19:18:24 05-二月-20... | Minor    | LAN error                 |
|  | GWC-44-UNIT-0   | Communications | 20:03:40 18-二月-20... | Major    | Communications subsy...   |
|  | SNMP_NE_Poller  | Communications | 15:25:56 18-二月-20... | Major    | Communications subsy...   |
|  | SNMP_NE_Poller  | Communications | 15:25:56 18-二月-20... | Major    | Communications subsy...   |
|  | SNMP_NE_Poller  | Communications | 15:25:56 18-二月-20... | Major    | Communications subsy...   |

### Syslog traplogger interface

The SESM server application on the CS 2000 Management Tools server uses UNIX syslog to store SNMP traps that arrive from network elements into the CS 2000 Management Tools server. The CS 2000 Management Tools server sends messages to the UNIX daemon syslogd, which logs messages into a set of files described by the configuration file /etc/syslog.conf. The file containing SNMP traps is /var/log/ptmlog.

**Note:** Log entries in the ptmlog file are not forwarded to any external systems, such as the OSS. These logs are intended as a local tool to maintain a record of all incoming traps from devices managed by the SESM server application.

The syslog traplogger interface is automatically set up by scripts and is started when the SESM server application is started or restarted. There are currently three configuration parameters for the syslog traplogger interface:

- the maximum file size
- the hour when file rotation backup occurs
- the minute when file rotation backup occurs

The parameters mentioned above can be configured using the “configure” tool on the CS 2000 Management Tools server. Refer to procedure [Configuring log reporting on page 1053](#) in this document.

### SESM server application debug logs

These are debug log files residing on the CS 2000 Management Tools server that are produced by the SESM server application. Optionally, the maximum size, maximum number of files, default debug levels, log file name, and other options can be configured using the “configure” tool on the CS 2000 Management Tools server. Refer to procedure [Configuring log reporting on page 1053](#) in this document.

There are three debug log file name extensions: mi2, misc, and pa. The “mi2” log files (for example, ptmdebuglog1.mi2) contains logs from the SESM server application. This is typically the largest and most significant log file. The “pa” logs files (for example, ptmdebuglog1.pa) are produced by the Proxy Agent which is a different application that is also part of the SESM server application. The “misc” log files (for example, ptmdebuglog1.misc) are produced by miscellaneous parts of the SESM server application. The “misc” file could contain critical errors such as startup errors in the SESM server application processes or OutOfMemory errors.



The logs are located in the /opt/nortel/NTsesm/admin/logs directory and should not be erased. They rotate when necessary, such that the file size or number of log files remains manageable. Display the log files using the UNIX command "ls -alt" in this directory. The newest logs will have a "1" in the title (assuming a default rotation) such as ptmdebuglog1.mi2. Older files that have been rotated may be named ptmdebuglog2.mi2 or ptmdebuglog3.mi2. The oldest file, for example ptmdebuglog7.mi2, is deleted during the next rotation.

The /opt/nortel/NTsesm/admin/logs directory contains the createDB\_<date>.log file created during the installation of the SESM server application. This file contains debug information from the initial creation of the SESM server application data base schema. This log file does not persist across upgrades of the SESM software.

### CS 2000 Management Tools logs

The default northbound alarm feed for the SESM-based applications on the CS 2000 Management Tools server, is Corba notifications to the Integrated Element Management System (EMS).

**Note:** The SESM syslog alarm feed is disabled by default to avoid duplication of the alarm logs. Procedure [Configuring log reporting on page 1053](#) in this document, is available to enable or disable the SESM syslog alarm feed when required.

The CS 2000 SAM21 Manager, QoS Collector Application (QCA), and Network Patch Manager (NPM) applications on the CS 2000 Management Tools server, use the SSPFS logging Application Program Interface (API) to record their logs. This API also provides the customer log feed to the OSS Fault Collector. The API supports five severity levels of custlogs: critical, major, minor, warning, and none.

The SSPFS logging API includes the following types of log files located in “/var/log”:

- customerlog (alarms and other customer visible elements)
- auditlog (user actions taken)
- authlog (authentication events)
- securitylog (security events)
- debuglog (software or hardware errors)
- sspfslog (platform events)
- ptmlog (SNMP traps received by the system)

**Note:** Syslog has built-in capabilities to forward logs to another IP address. This functionality is used to send the logs in the SSPFS custlog feed to the OSS Fault Collector.

The logs in “/var/log” rotate when necessary, such that the file size or number of log files remains manageable. After rotation, the following log files are compressed by the gzip compression program: customerlog, auditlog, securitylog, debuglog, and sspfslog. Log files fs.log and lv.log in “/var/log/filesys”, are also compressed.

Syslog forwarding is configured using the Syslog Configuration option at the SSPFS command line interface (CLI). This option modifies the syslog.conf text file (a standard syslog file) which dictates how syslog operates. It can define whether to record the logs on the local machine, send them to another machine (such as the OSS Fault Collector), or both. Syslogs are controlled on a log-level basis, such that critical logs can be handled one way and warning logs another way. See procedure [Routing customer logs to a remote host on page 1049](#) in this document.

In general, the only logs that will be forwarded are customer logs which contain alarm logs. Although, this can be customized using Syslog Configuration.

The default northbound fault feed for the SSPFS platform-specific faults is SNMP. However, when local logging is enabled (default), the SSPFS platform alarm logs are sent over both the syslog (custlog) and SNMP (alarmd) interfaces to the Integrated Element Management System (EMS) causing duplication of alarm logs. To avoid this duplication, disable local logging using procedure [Disabling local logging of SSPFS platform faults on page 1063](#) in this document.

## Accessing the Alarm Manager

### Application

This procedure provides access to service-related alarms on the hardware application. The Alarm Manager provides information on the fields described in the following table:

#### Alarm Manager field details

| Field Name           | Description                                                                                                                                                      |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Element name | Provides the name of the Network Element for which the selected alarm is being raised.                                                                           |
| Category             | Represents the alarm problem category values (ITU-T X.733):<br>“Communications”<br>“Quality of Service”<br>“Processing Error”<br>“Equipment Error” “Environment” |
| Alarm Time           | Represents the time that the alarm was raised in the following format:<br><br>HH:MM:SS day-Month-year                                                            |
| Severity             | Provides the associated severity of the alarm being raised. The range of values is as follows:<br>“Critical”<br>“Major”<br>“Minor”<br>“Warning”                  |

**Alarm Manager field details**

| Field Name     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Probable Cause | Provides the probable cause of the particular alarm (X.733 Probable Cause):<br>“Adapter Error”<br>“Non-Repudiation Failure”<br>“Bandwidth Reduced”<br>“Call Establishment Error”<br>“Communications Protocol Error”<br>“Communications Subsystem Error”<br>“Configuration or Customization Error”<br>“Congestion”<br>“Corrupt Data”<br>“CPU Cycles Limit Exceeded”<br>“Data Set or Modem Error”<br>“Degraded Signal”<br>“DTE DCE Interface Error”<br>“Enclosure Door Open”<br>“Equipment Malfunction”<br>“Excessive Vibration”<br>“File Error”<br>“Fire Detected”<br>“Flood Detected” |

**Alarm Manager field details**

| Field Name | Description                                       |
|------------|---------------------------------------------------|
|            | "Framing Error"                                   |
|            | "Heating, Ventilation, or Cooling System Problem" |
|            | "Humidity Unacceptable"                           |
|            | "Input Output Device Error"                       |
|            | "Input Device Error"                              |
|            | "LAN Error"                                       |
|            | "Leak Detected"                                   |
|            | "Local Node Transmission Error"                   |
|            | "Loss of Frame"                                   |
|            | "Loss of Signal"                                  |
|            | "Material Supply Exhausted"                       |
|            | "Multiplexer Problem"                             |
|            | "Out of Memory"                                   |
|            | "Output Device Error"                             |
|            | "Performance Degraded"                            |
|            | "Power Problem"                                   |
|            | "Pressure Unacceptable"                           |
|            | "Pump Failure"                                    |
|            | "Queue Size Exceeded"                             |
|            | "Receive Failure"                                 |
|            | "Remote Node Transmission Error"                  |
|            | "Resource At or Nearing Capacity"                 |
|            | "Response Time Excessive"                         |

**Alarm Manager field details**

| Field Name | Description                              |
|------------|------------------------------------------|
|            | "Retransmission Rate Excessive"          |
|            | "Software Error"                         |
|            | "Software Program Abnormally Terminated" |
|            | "Software Program Error"                 |
|            | "Storage Capacity Problem"               |
|            | "Temperature Unacceptable"               |
|            | "Threshold Crossed"                      |
|            | "Timing Problem"                         |
|            | "Toxic Leak Detected"                    |
|            | "Transmit Failure"                       |
|            | "Transmitter Failure"                    |
|            | "Underlying Resources Unavailable"       |
|            | "Version Mismatch"                       |
|            | "Authentication Failure"                 |
|            | "Breach of Confidentiality"              |
|            | "Cable Tamper"                           |
|            | "Delayed Information"                    |
|            | "Denial of Service"                      |
|            | "Duplicate Information"                  |
|            | "Information Modification Detected"      |
|            | "Information Missing"                    |
|            | "Information Out of Sequence"            |

**Alarm Manager field details**

| Field Name | Description                        |
|------------|------------------------------------|
|            | "Intrusion Detection"              |
|            | "Key Expired"                      |
|            | "Non-Repudiation Failure"          |
|            | "Out of Hours Activity"            |
|            | "Out of Service"                   |
|            | "Procedural Error"                 |
|            | "Unauthorized Access Attempt"      |
|            | "Unexpected Information"           |
|            | "Unspecified Reason"               |
|            | "Probable Cause Conversion Failed" |

To avoid using too much memory to display the alarms, only 1000 alarms are displayed at any given time. Alarms that are no longer displayed on the Alarm Manager can be viewed using the Alarm History window, which uses paging to minimize the size to the GUI.

**Prerequisites**

None

**Action**

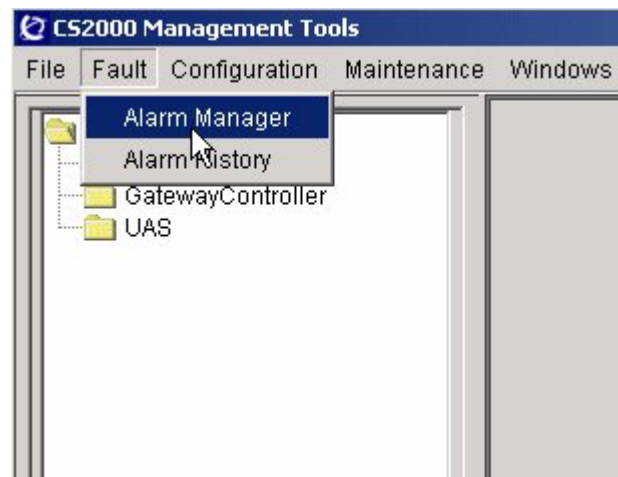
Perform the following steps to complete this procedure.

***At your workstation***

- 1 Launch the CS2000 Management Tools GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications.](#) in this document, if required.

***At the CS2000 Management Tools GUI***

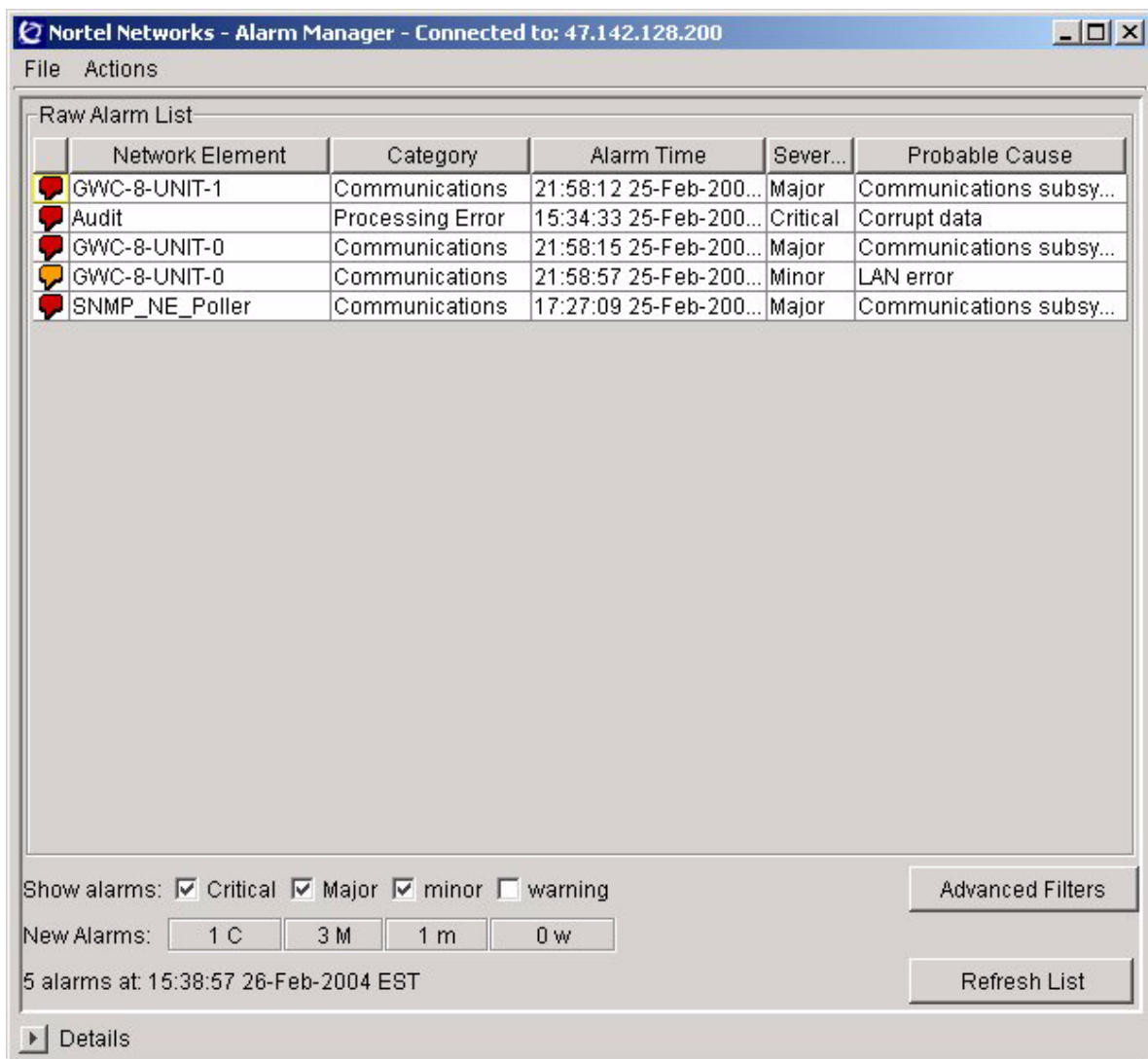
- 2 On the **Fault** menu, click **Alarm Manager**.



The Alarm Manager window, similar to following, appears.



## Alarm Manager window



**3** You have completed this procedure.



## Retrieving details about an alarm

### Application

Use this procedure to display detailed information about service-related alarms on the managed network elements. The detailed view provides information on the items in the following table:

#### Alarm details fields

| Field Name     | Description                                                                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NE Name        | Provides the name of the Network Element for which the selected alarm is being raised.                                                                                                                                   |
| Alarm Level    | Provides the associated severity of the alarm being raised. The range of values is as follows:<br>“Critical”<br>“Major”<br>“Minor”<br>“Warning”                                                                          |
| Category       | Represents the alarm problem category values (ITU-T X.733):<br>“Communications”<br>“Quality of Service”<br>“Processing Error”<br>“Equipment Error” “Environment”                                                         |
| Alarm Time     | Represents the time that the alarm was raised in the following format:<br><br>HH:MM:SS day-Month-year                                                                                                                    |
| Probable Cause | Provides the probable cause of the particular alarm (X.733 Probable Cause).<br><br>See the procedure <a href="#">Accessing the Alarm Manager on page 943</a> for a list of possible entries in the Probably Cause field. |

**Alarm details fields**

| Field Name        | Description                                                                                                                                                                                                                  |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System uptime     | Represents the time since the network element was last re-initialized. Here is an example of how system uptime is displayed:<br><br>2 hours, 10 minutes, 30 seconds                                                          |
| Component ID      | Represents the distinguished name (DN) (refer X.720) of the component object against which the particular alarm is raised.<br><br>Example:<br><br>GWC=GWC-3-UNIT-1;Version=PGC91AFZ;Unit=unit_1;Software=NODEMTC             |
| Alarm Description | Provides the description text for the particular alarm. (X.733 Additional text)<br><br>Example:<br><br>Element Manager communication failure.                                                                                |
| Specific Problem  | Provides the specific problem data (ITU-T X.733) to further qualify the probable cause of the particular alarm. (X.733 Specific Problem)<br><br>Example:<br><br>EM not responding, provisioned data loaded from local Flash. |

**Prerequisites**

This procedure has no prerequisites.

**Action**

Perform the following steps to complete this procedure.

***At your workstation***

- 1 Launch the CS2000 Management Tools GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#) in this document if required.

**At the CS2000 Management Tools application GUI**

- 2 On the **Fault** menu, click **Alarm Manager**.

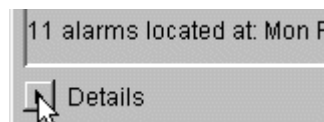


The Alarm Manager window opens.

- 3 Select an alarm in the Alarm Manager window.

| Raw Alarm List |                 |                |                      |          |                         |
|----------------|-----------------|----------------|----------------------|----------|-------------------------|
|                | Network Element | Category       | Alarm Time           | Severity | Probable Cause          |
|                | GWC 7 Unit 0    | Communications | 10:03:47 14-Feb-2002 | Critical | Communications subsv... |
|                | GWC 7 Unit 1    | Communications | 10:03:47 14-Feb-2002 | Critical | Communications subsv... |
|                | sam16_4a        | Communications | 10:03:47 14-Feb-2002 | Critical | Communications subsv... |
|                | GWC 9 Unit 1    | Communications | 12:53:15 17-Feb-2002 | Minor    | LAN error               |
|                | aps05           | Communications | 10:03:47 14-Feb-2002 | Critical | Communications subsv... |
|                | GWC 100 Unit 0  | Communications | 10:03:47 14-Feb-2002 | Critical | Communications subsv... |

- 4 Click **Details**.



Detailed information about the alarm is displayed.

**Alarm details**

|                    |                                 |
|--------------------|---------------------------------|
| <b>Details</b>     |                                 |
| NE Name:           | GWC 9 Unit 1                    |
| Alarm Level:       | Minor                           |
| Category:          | Communications                  |
| Alarm Time:        | 12:53:15 17-Feb-2002            |
| Probable Cause:    | LAN error                       |
| Acknowledged at:   | Not Yet                         |
| ComponentID:       | GWC;Unit=unit_1;Software=NODEMT |
| Alarm Description: | Mate unit communication lost.   |
| Specific Problem:  | No response received to mate    |

- 5 You have completed this procedure.



---

## Accessing the Alarm History

---

### Application

Use this procedure to access the Alarm History window, which provides a list of active and inactive alarms.

### Prerequisites

None

### Action

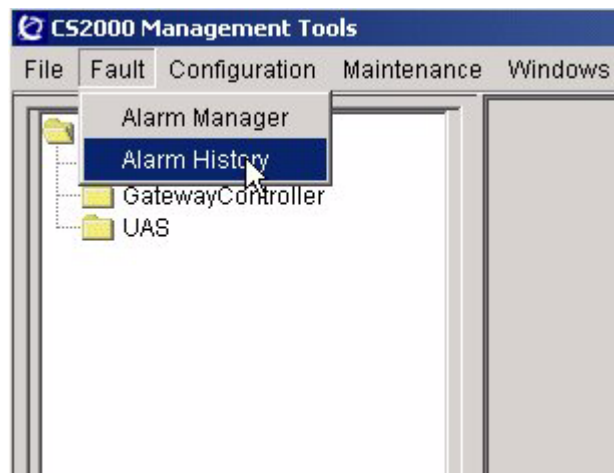
Perform the following steps to complete this procedure.

#### *At your workstation*

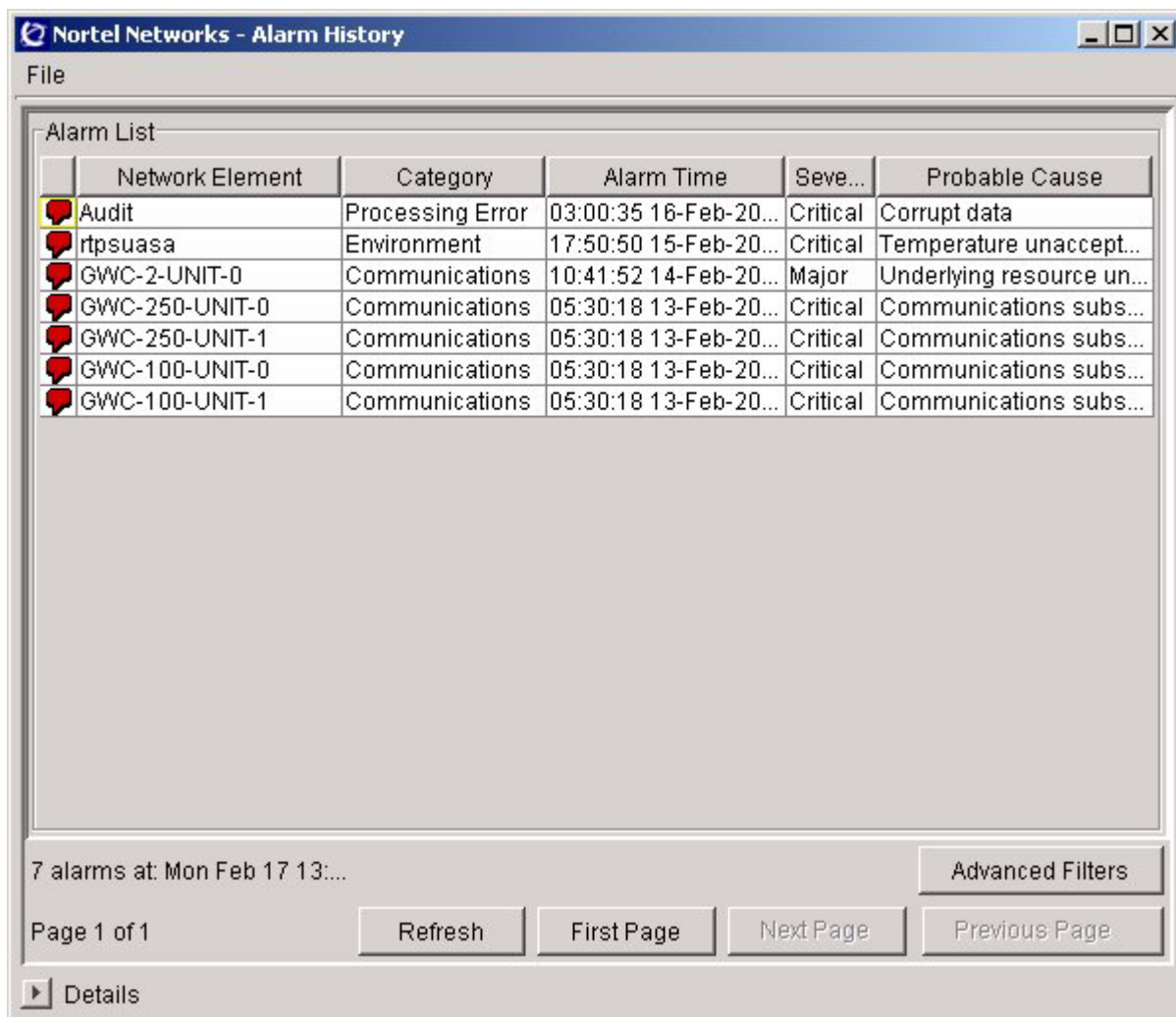
- 1 Launch the CS2000 Management Tools GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#) in this document if required.

#### *At the CS2000 Management Tools GUI*

- 2 On the **Fault** menu, click **Alarm History**.



The Alarm History window, similar to following, appears.



**3** You have completed this procedure.



## Filtering alarms

### Application

Use this procedure to filter the alarms you want to view. You can filter by alarm severity, network element and type of alarm (alarm category).

**Note:** This procedure provides the steps to filter alarms in the Alarm Manager, but similar filtering capabilities are also available in the Alarm History.

### Prerequisites

None

### Action

#### *At your workstation*

- 1 Launch the CS2000 Management Tools GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#) in this document if required.

#### *At the CS2000 Management Tools GUI*

- 2 On the **Fault** menu, click **Alarm Manager**.



The Alarm Manager window opens.

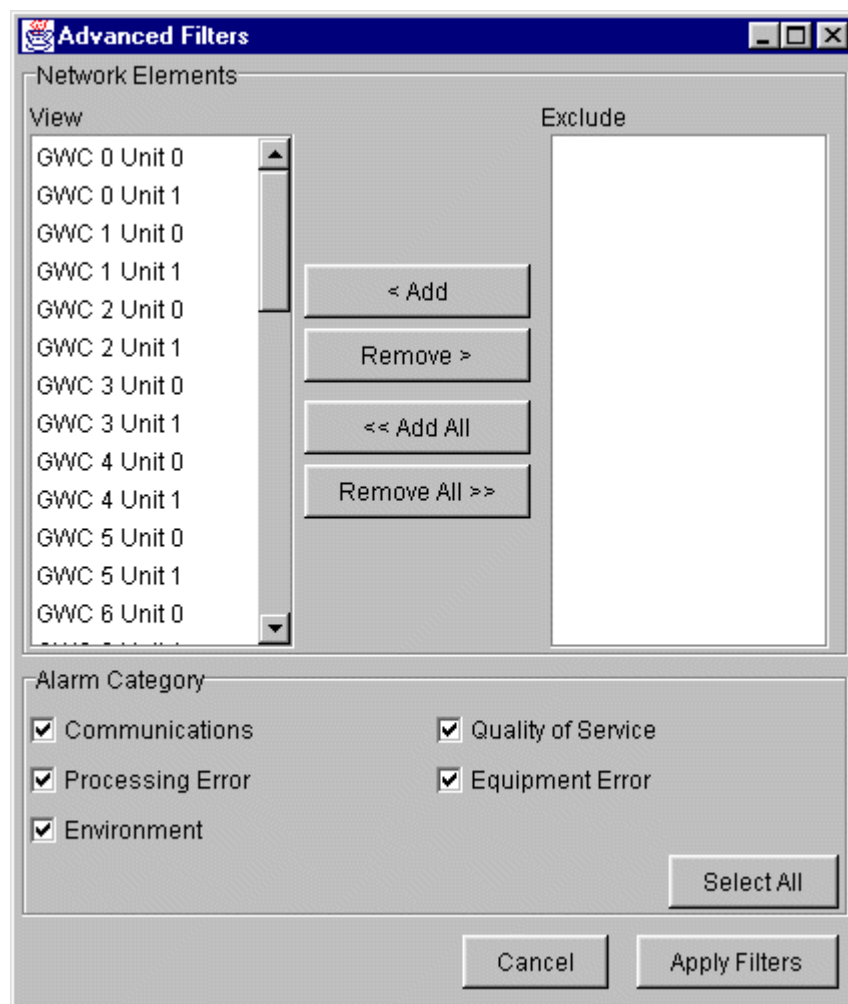
A screenshot of the 'Nortel Networks - Alarm Manager' window. It displays a 'Raw Alarm List' table with columns for Network Element, Category, Alarm Time, Severity, and Probable Cause. The table contains six rows of alarm data.

|   | Network Element | Category       | Alarm Time            | Seve...  | Probable Cause           |
|---|-----------------|----------------|-----------------------|----------|--------------------------|
| 🔴 | GW-C-100-UNIT-1 | Communications | 05:30:18 13-Feb-20... | Critical | Communications subs...   |
| 🔴 | GW-C-100-UNIT-0 | Communications | 05:30:18 13-Feb-20... | Critical | Communications subs...   |
| 🔴 | GW-C-250-UNIT-1 | Communications | 05:30:18 13-Feb-20... | Critical | Communications subs...   |
| 🔴 | GW-C-250-UNIT-0 | Communications | 05:30:18 13-Feb-20... | Critical | Communications subs...   |
| 🔴 | rtpsusa         | Environment    | 17:50:50 15-Feb-20... | Critical | Temperature unaccept...  |
| 🔴 | GW-C-2-UNIT-0   | Communications | 10:41:52 14-Feb-20... | Major    | Underlying resource u... |

- 3 Use the following table to determine your next step.

| If you want to filter by          | Do                     |
|-----------------------------------|------------------------|
| network element or alarm category | step <a href="#">4</a> |
| severity                          | step <a href="#">5</a> |

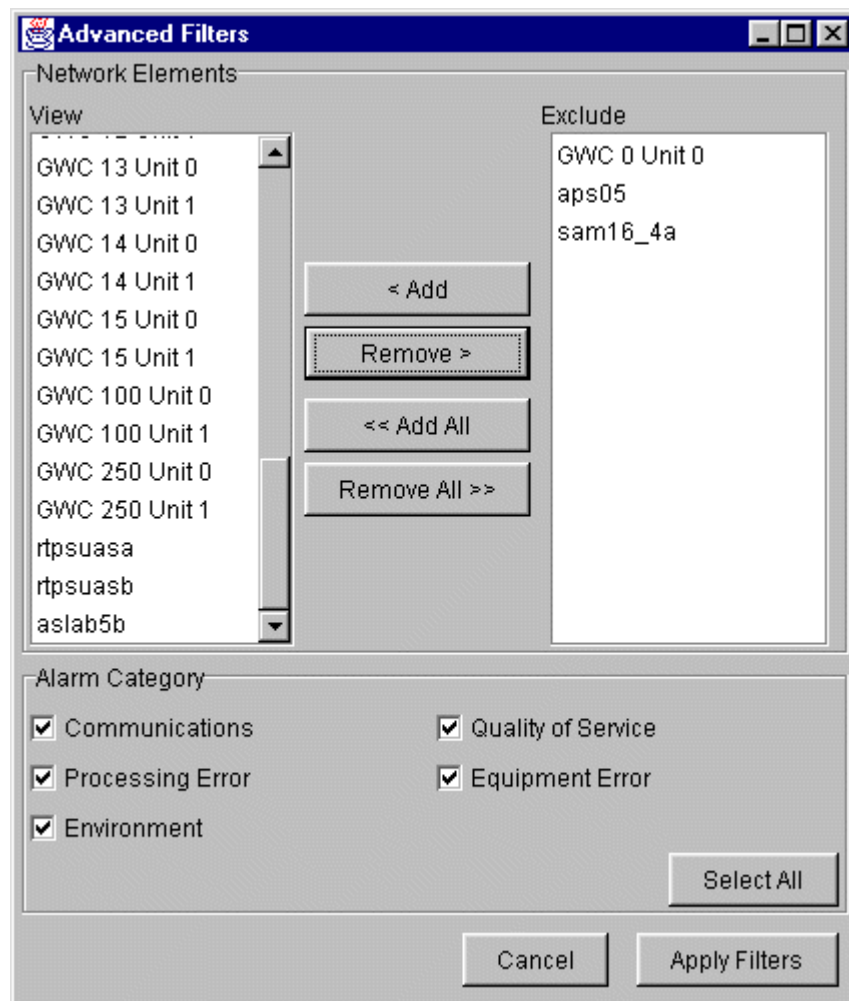
- 4 Filter by network element or alarm category as follows:
- a In the **Alarm Manager** window, click **Advanced Filters**.  
The Advanced Filters window opens.



- b Select the network elements you want to exclude from the viewable alarms in the View column, then click **Remove**.

The network elements you have selected move to the **Exclude** column.

**Note:** If you move all Network Elements to the **Exclude** column, the filters based on Network Element node names will be deactivated. As a result, the alarm manager will display alarms from all managed devices and alarms from internal Call server applications (for example, Call Server Data Audit).



- c Under **Alarm Category**, check the box next to the type of alarms you want to view for the network elements, then click **Apply filters**.

- 5 Filter by severity as follows:
  - a If checked, uncheck the severity type(s) you want to filter.



Show alarms: ☒ Critical ☒ Major ☐ minor ☐ warning

New Alarms:

- b Click **Refresh List** to refresh the alarm list.  
The alarms of the unchecked severity type(s) no longer appear in the **Alarm Manager** window.
- 6 You have completed this procedure.

## Resetting the filters for alarms

### Application

Use this procedure to reset the filters for service-related alarms at the Alarm Manager. This applies only for alarm severity.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Launch the CS2000 Management Tools GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#) in this document if required.

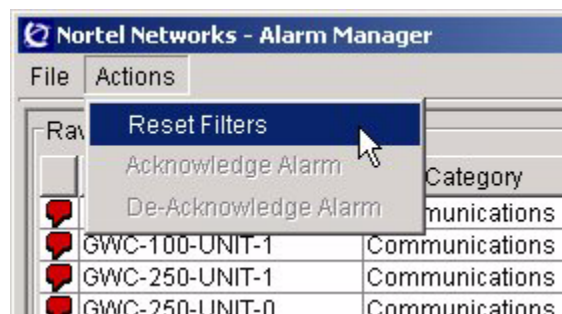
#### *At the CS2000 Management Tools GUI*

- 1 On the **Fault** menu, click **Alarm Manager**.



The Alarm Manager window opens.

- 2 On the **Actions** menu, click **Reset Filters**.



- 3 Click **Refresh List** to refresh the alarm list.  
The alarms of the previous default severity types appear in the Alarm Manager window.
- 4 You have completed this procedure.

---

## Defining alarms using the NPM

---

### Application

Use this procedure to define your own alarms to match your specific criteria using the Network Patch Manager (NPM). You can define alarms using one of the following two NPM interfaces:

- [Using the NPM CLUI on page 964](#)
- [Using the NPM GUI on page 965](#)

The NPM is initially configured with the following system-defined alarms:

- PFRSGETPATCH: PFRS GETPATCH task has failed
- DEVICE\_ONLHOLD: Devices on hold
- PFRSGENREPORT: PFRS GENREPORT task has failed
- DNR\_NOT\_APP: Do Not Remove (DNR)-type patches not applied
- ACT\_NOT\_APP: Activatable patches not applied
- OBE\_NOT\_REMOVED: Obsolete Emergency (OBE)-type patches not removed
- OBS\_NOT\_REMOVED: Obsolete (OBS)-type patches not removed
- DEBUG\_APP: Debug patches applied
- DEVICE\_AUDIFAIL: Devices which have failed or not executed audits since registration
- ACT\_NOT\_ACT: Activatable patches not activated
- PATCH\_ONLHOLD: Patches on hold
- ENABLED\_REMOVED: Patches that are removed but enabled
- REMOVED\_PATCHES: Removed patches which are not category OBS, OBE, or DBG
- EMG\_NOT\_APP: Emergency (EMG)-type patches not applied
- GEN\_NOT\_APP: General (GEN)-type patches at V (verification) status, not applied
- REL\_GEN\_NOT\_APP: General (GEN)-type patches at R (released) status, not applied

- DISABLED\_APPLIED: Patches that are applied but disabled
- LTD\_NOT\_APP: Limited (LTD) patches not applied

**Note:** You can enable or disable system-defined alarms, and you can view, but not modify, the definition of system-defined alarms.

## Prerequisites

None

## Action

Perform the steps under [Using the NPM CLUI](#) or [Using the NPM GUI](#) to complete this procedure.

### Using the NPM CLUI

#### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 1151](#).

#### *At the NPM CLUI*

- 2 Define an alarm by typing

```
npm> addalarm <alarm_name> <alarm_enable>
<alarm_severity> "<alarm_pd> <alarm_criteria>"
'<alarm_desc>'
```

and pressing the Enter key.

where

**alarm\_name**

is the name of the alarm being defined

**alarm\_enable**

identifies whether the alarm will be enabled initially (Y, N)

**alarm\_severity**

identifies the alarm severity (NONE, MINOR, MAJOR, or CRITICAL)

**alarm\_pd**

identifies whether the alarm is from a patch or device (PATCH, DEVICE)

**alarm\_criteria**

is the SQL statement that defines the alarm condition



**alarm\_desc**

is a brief description of the alarm

**Example**

```
addalarm PATCHUNAVAIL Y CRITICAL "PATCH where
PATCH.FILEAVAILABLE='FALSE'" 'No patch file
available'
```

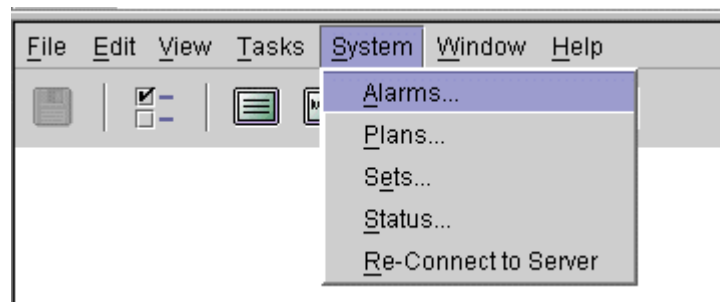
You have completed this procedure.

**Using the NPM GUI*****At your workstation***

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#).

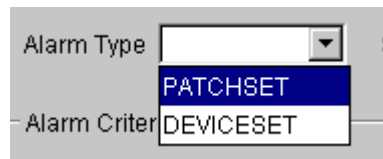
***At the NPM GUI***

- 2 On the **System** menu, click **Alarms...**

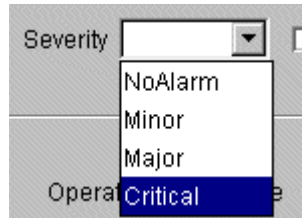


The Alarms window opens.

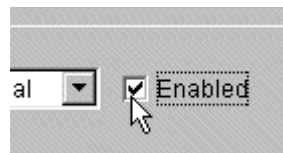
- 3 Select an alarm type from the **Alarm Type** list.



- 4 Select a severity level from the **Severity** list.



- 5 Click the **Enabled** checkbox to enable the alarm.



- 6 In the **Alarm Criteria** panel, enter the criteria for the alarm.

**If you want to enter the alarm criteria**

**Do**

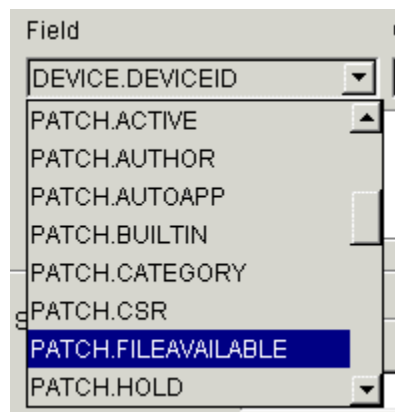
using the boxes

step [7](#)

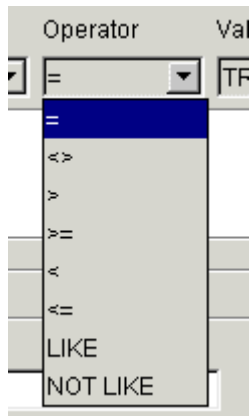
using a command string

step [8](#)

- 7 Using the boxes, specify the alarm criteria as follows:
- a Select the field from the **Field** list.



- b Select the operator from the **Operator** list.



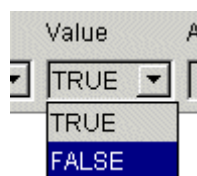
The table below lists the supported operators and their meaning.

#### Supported operators

| Operator | Meaning                                 |
|----------|-----------------------------------------|
| =        | Equal                                   |
| <>       | Not equal                               |
| >        | Greater than                            |
| >=       | Greater than or equal                   |
| <        | Less than                               |
| <=       | Less than or equal                      |
| LIKE     | Matches string with wildcard (%)        |
| NOT LIKE | Does not match string with wildcard (%) |

- c Select the value from the **Value** list, or enter the value.

**Note:** The data type for **Value** will change depending on the data type of the field. For alphanumeric data, enter the value. For boolean data, select the value.



- d To combine multiple criteria statements, select the AND or the OR options from the **And/Or** box.
  - e Go to step 9.
- 8 Using a command string, specify the alarm criteria in the text area.
- Note:** Parenthesis “( )” may be inserted to define precedence for multiple criteria statements.

| Field                         | Operator |
|-------------------------------|----------|
| DEVICE.DEVICEID               | =        |
| PATCH.FILEAVAILABLE = 'FALSE' |          |

- 9 Enter a unique name for the alarm in the **Alarm Name** box.

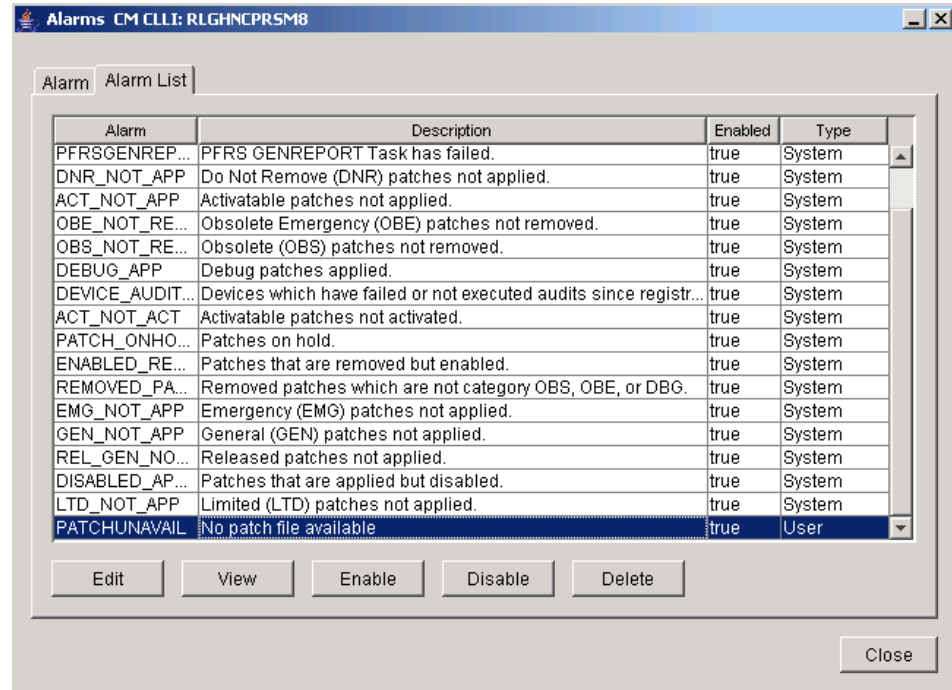
| Save Alarm         |              |
|--------------------|--------------|
| Alarm Name:        | PATCHUNAVAIL |
| Alarm Description: |              |
| <div>Save</div>    |              |

- 10 Optionally enter a description for the alarm in the **Alarm description** box.

| Save Alarm         |                         |
|--------------------|-------------------------|
| Alarm Name:        | PATCHUNAVAIL            |
| Alarm Description: | No patch file available |
| <div>Save</div>    |                         |

# 11 Click **Save** to save the alarm.

The new alarm will be displayed in the Alarm List once the NPM Server has saved the alarm.



You have completed this procedure.



---

## Enabling and disabling alarms using the NPM

---

### Application

Use this procedure to enable or disable an alarm using the Network Patch Manager (NPM). You can enable or disable alarms using one of the following two NPM interfaces:

- [Using the NPM CLUI on page 971](#)
- [Using the NPM GUI on page 972](#)

### Prerequisites

None

### Action

Perform the steps under [Using the NPM CLUI](#) or [Using the NPM GUI](#) to complete this procedure.

#### Using the NPM CLUI

##### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 1151](#).

##### *At the NPM CLUI*

- 2 Enable or disable an alarm by typing  
`npm> alarm <alarm_name> <alarm_option>`  
and pressing the Enter key.  
where

**alarm\_name**

is the name of the alarm

**alarm\_option**

indicates what is to be done to the alarm (enable, disable, delete, matches)

*Example for enabling an alarm:*

```
npm> alarm DEVICE_ONHOLD enable
```

*Example for disabling an alarm:*

```
npm> alarm DEVICE_ONHOLD disable
```

You have completed this procedure.

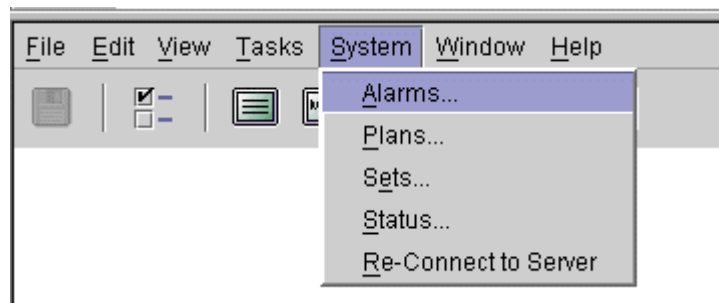
## Using the NPM GUI

### At your workstation

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#).

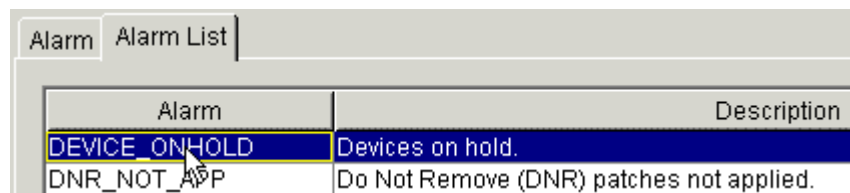
### At the NPM GUI

- 2 On the **System** menu, click **Alarms....**

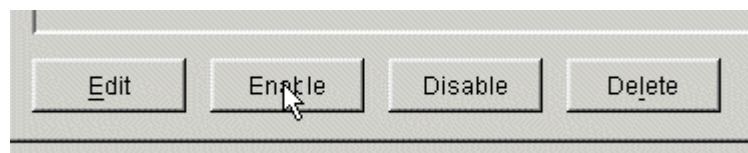


The Alarms window opens.

- 3 Click the **Alarm List** tab to display a list of all defined alarms.
- 4 Select the alarm you want to enable or disable from the alarm list.



- 5 Click **Enable** or **Disable**.



You have completed this procedure.



---

## Performing an audit

---

### Application

Use this procedure to manually perform a line, trunk, V5.2 interface, or CS 2000 (CS2K) data audit.

**Note:** The V5.2 audit is only available in the international version of the software and not in the North American.

You can set the audit to run automatically at a specific time on a daily or a weekly basis. Refer to procedure “Configuring an audit schedule” in the ATM/IP Solution-level Configuration Management document, NN10409-500.

#### CS 2000 data audit

For a CS2K data audit, the system compares the GWC element manager database (part of the CS 2000 GWC Manager database) with the CS 2000 XA-Core database and flags any mismatches between the two databases. The XA-Core is considered to hold the ‘master’ database.

Remedial actions offered are likely to involve deletion of inconsistent data. However, where possible, the option to repair data inconsistencies will be given.

#### Line audit

For a line audit, the system compares the ENDPOINTENTRY area in the CS 2000 GWC Manager database with the following tables in the CS 2000 XA-Core database:

- DNINV
- LGRPINV
- LNINV
- LNENDPT (if DQOS gateway has been provisioned)
- HUNTMEM (if hunt groups have been provisioned)
- MDNMEM (if MADN groups have been provisioned)

The system writes the results of the audit into two files, one containing a list of valid data and the other containing a list of problem data. The files are stored on the CS 2000 Management Tools server.

**Trunk audit**

For a trunk audit, the system compares the ENDPOINTENTRY area in the CS 2000 GWC Manager database with the following tables in the CS 2000 XA-Core database:

- SERVRINV
- TRKMEM
- LTMAP
- TRKSGRP

The system writes the results of the audit into two files, one containing a list of valid data and the other containing a list of problem data. The files are stored on the CS 2000 Management Tools server.

**V5.2 audit**

For a V5.2 data integrity audit, the system compares data in the following databases and flags any mismatches:

- V5.2 interface data stored in the Network View database
- V5.2 endpoint data stored in the CS 2000 GWC Manager database
- V5.2 interface data stored in the table GPPTRNSL in the CS 2000 XA-Core database

Remedial actions offered are likely to involve deletion of inconsistent data. However, where possible, the option to repair data inconsistencies will be offered.

**Prerequisites**

It is recommended to run only one audit at a time, therefore, ensure your manual audit does not conflict with another scheduled audit. Running multiple audits at the same time may cause some unexpected errors.

You must be assigned to user group “mgcadm” to run an audit. If required, refer to procedure “Setting up users on a Sun server” in the ATM/IP Administration and Security document, NN10281-600.

## Action

Perform the following steps to complete this procedure.

### *At your workstation*

- 1 Launch the CS2000 Management Tools GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#) in this document if required.

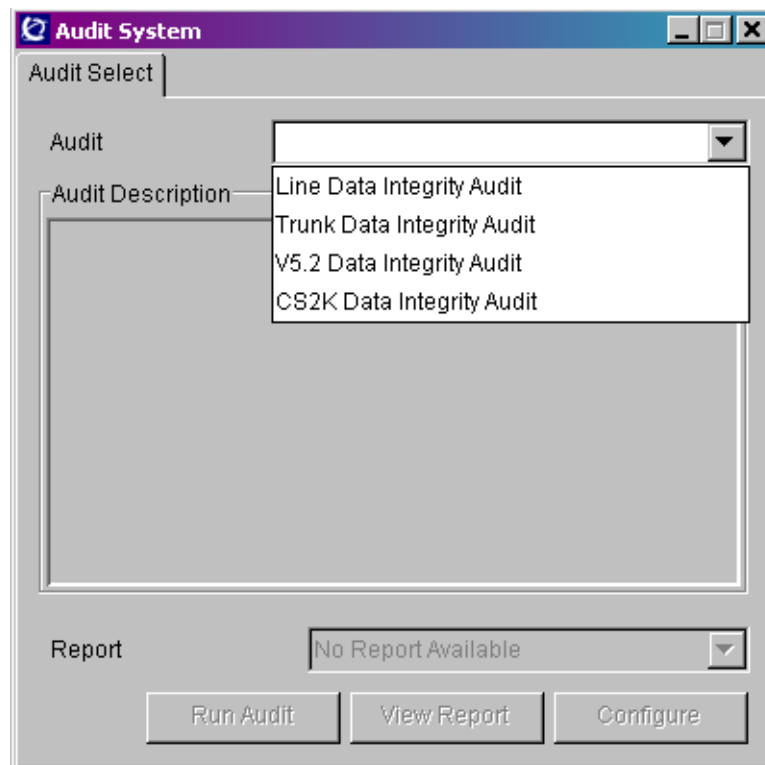
### *At the CS2000 Management Tools GUI*

- 2 On the **Maintenance** menu, click **Audit System**.

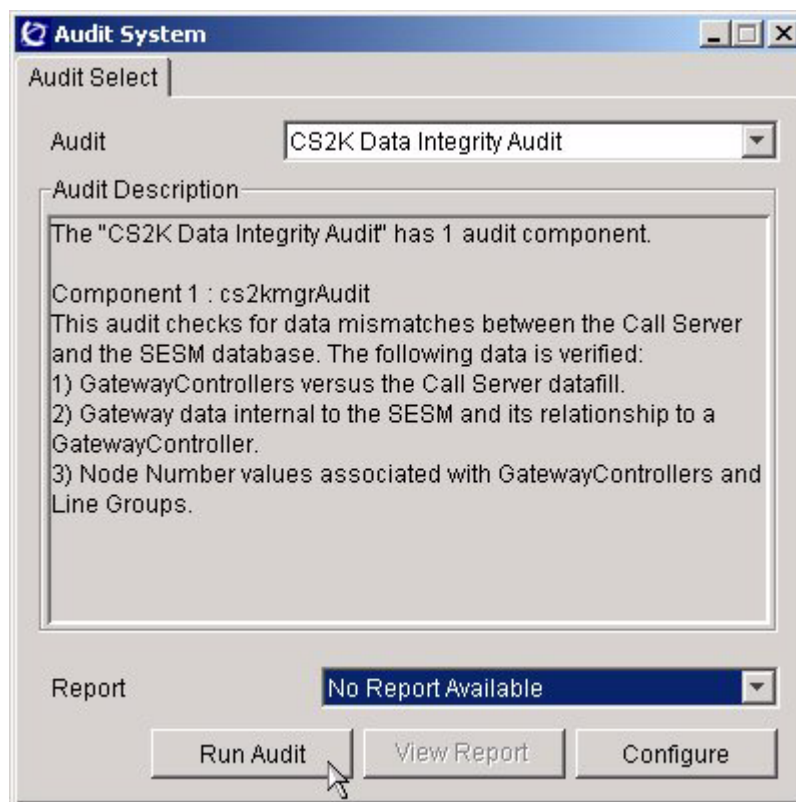


The Audit System window opens.

- 3 In the **Audit** list, click the type of audit you want to perform.



4 Click **Run Audit**.



During the audit, an Audit Status window is displayed to indicate the audit is in progress. The Audit Status window indicates when the audit is complete.

**Note:** If the audit does not execute successfully, the Audit Status window indicates that the audit failed and provides the reason. Contact your next level of support to resolve the problem if required.

- 5 Once the audit completes, click **Close** to close the Audit Status window.
- 6 Use the following table to determine your next step.

| If you performed a         | Do                      |
|----------------------------|-------------------------|
| CS2K Data Integrity Audit  | step <a href="#">7</a>  |
| Line Data Integrity Audit  | step <a href="#">11</a> |
| Trunk Data Integrity Audit | step <a href="#">14</a> |
| V5.2 Data Integrity Audit  | step <a href="#">17</a> |

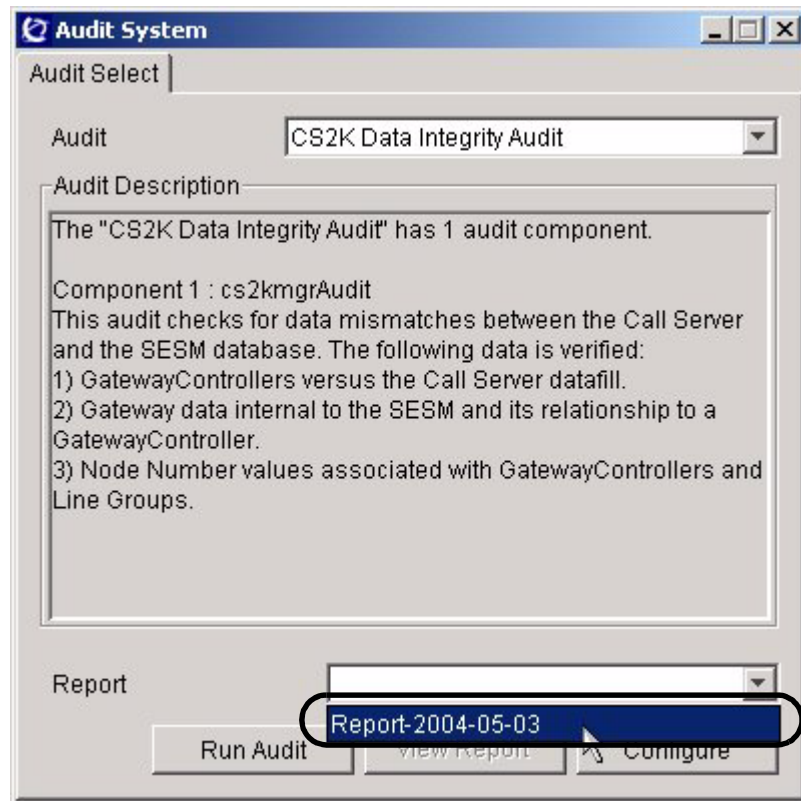
- 7 Proceed as follows for a CS2K Data Integrity Audit:
  - a Ensure that you have selected **CS2K Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.
  - b Select **Report <date>** from the pull-down menu in the Report field at the bottom of the dialog box.

The file name has the following format:

Report-<date>

where

<date> is the date in yyyy-mm-dd format, for example, 2003-02-15.



- c Click the **View Report** button.



The system displays the selected report. If no problems were discovered, the report will be empty. Here is an example of a report containing problems:

**CS2K Data Integrity Audit Report**

File Last Audit Date: 2002-07-29 14:58:22

| Index | Problem Description                                       | Current Status |
|-------|-----------------------------------------------------------|----------------|
| 0     | GWC-9 at IP 172.17.40.64 is only datafilled in XA-Core    | Problem Exists |
| 1     | GWC-10 at IP 172.17.40.68 is only datafilled in XA-Core   | Problem Exists |
| 2     | GWC-11 at IP 172.17.40.72 is only datafilled in XA-Core   | Problem Exists |
| 3     | GWC-12 at IP 172.17.40.76 is only datafilled in XA-Core   | Problem Exists |
| 4     | GWC-13 at IP 172.17.40.80 is only datafilled in XA-Core   | Problem Exists |
| 5     | GWC-14 at IP 172.17.40.84 is only datafilled in XA-Core   | Problem Exists |
| 6     | GWC-15 at IP 172.17.40.88 is only datafilled in XA-Core   | Problem Exists |
| 7     | GWC-16 at IP 172.17.40.96 is only datafilled in XA-Core   | Problem Exists |
| 8     | GWC-17 at IP 172.17.40.100 is only datafilled in XA-Core  | Problem Exists |
| 9     | GWC-18 at IP 172.17.40.104 is only datafilled in XA-Core  | Problem Exists |
| 10    | GWC-19 at IP 172.17.40.108 is only datafilled in XA-Core  | Problem Exists |
| 11    | GWC-20 at IP 172.17.40.112 is only datafilled in XA-Core  | Problem Exists |
| 12    | GWC-21 at IP 172.17.40.116 is only datafilled in XA-Core  | Problem Exists |
| 13    | GWC-22 at IP 172.17.40.120 is only datafilled in XA-Core  | Problem Exists |
| 14    | GWC-100 at IP 172.17.46.244 is only datafilled in XA-Core | Problem Exists |

**Problem Detail:**

Problem Number: 0

Problem Description: GWC-9 at IP 172.17.40.64 is only datafilled in XA-Core

Current Status: Problem Exists

**Possible Actions**

Actions: Please Select An Action

Description:

Take Action

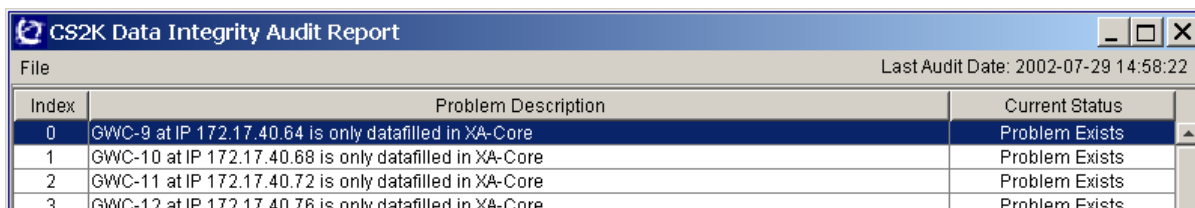
**Note 1:** The CS 2000 Management Tools server retains the most recent CS 2000 audit report. When a new audit occurs, the server deletes the previous report.

**Note 2:** The system places the audit report in the following directory on the CS 2000 Management Tools server: /opt/nortel/ptm/current/M12/apps/Audit.

**Note 3:** The CS 2000 GWC Manager does not provide an option to save a CS 2000 data audit report to local disk.

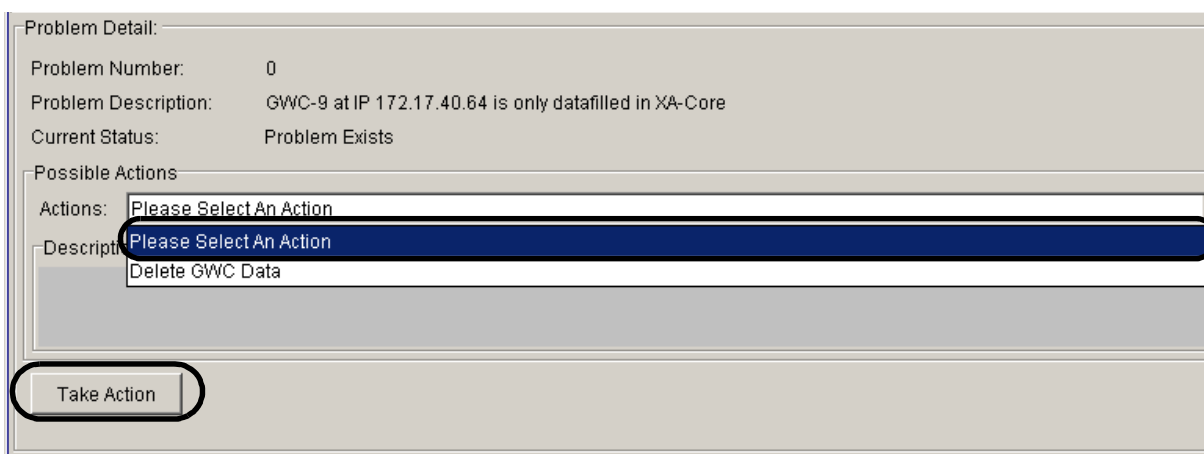
- 8 Review the results of the audit and click on a problem to resolve.

**Note:** If necessary, resize the entire window to completely view the Problem Description field.



| Index | Problem Description                                     | Current Status |
|-------|---------------------------------------------------------|----------------|
| 0     | GWC-9 at IP 172.17.40.64 is only datafilled in XA-Core  | Problem Exists |
| 1     | GWC-10 at IP 172.17.40.68 is only datafilled in XA-Core | Problem Exists |
| 2     | GWC-11 at IP 172.17.40.72 is only datafilled in XA-Core | Problem Exists |
| 3     | GWC-12 at IP 172.17.40.76 is only datafilled in XA-Core | Problem Exists |

- 9 Evaluate actions to resolve a problem and take action.
- Click and hold on the Action pull-down menu near the bottom of the screen to assess any possible actions.
  - If appropriate, select an action. Read the description of the action and ensure that you observe any recommended steps or cautions.



Problem Detail:

Problem Number: 0

Problem Description: GWC-9 at IP 172.17.40.64 is only datafilled in XA-Core

Current Status: Problem Exists

Possible Actions

Actions: Please Select An Action

Describe: Please Select An Action

Delete GWC Data

Take Action

- c Click the **Take Action** button.

**Note:** If you see the message “Correction Failed”, please contact your next level of support.

- 10 Return to [step 8](#) to review another problem.
- 11 Proceed as follows for a Line Data Integrity Audit:

| If you want to view          | Do                      |
|------------------------------|-------------------------|
| the line valid-data report   | step <a href="#">12</a> |
| the line problem-data report | step <a href="#">13</a> |

- 12 View the line valid-data report as follows:
  - a Ensure that you have selected **Line Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.
  - b Select **ValidLineData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ValidLineData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

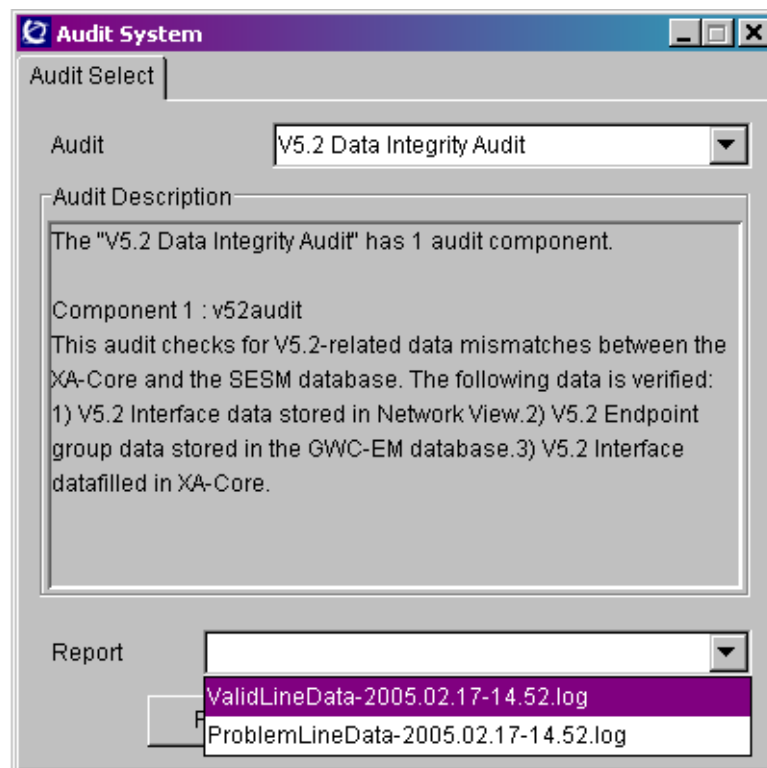
The file name has the following format:

ValidLineData-<date>-<time>.log

where

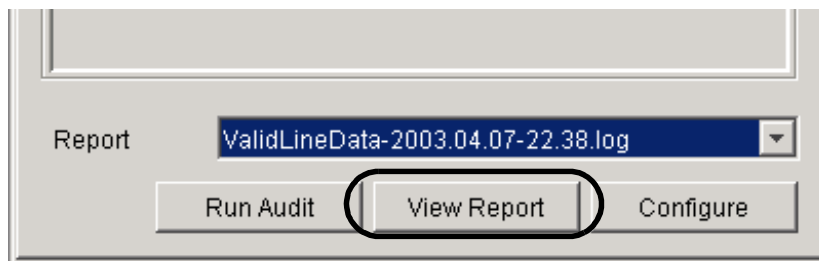
<date> is the date in yyyy.mm.dd format, for example, 2003.02.15.

<time> is the time in hh.mm format, for example 17.30.





**c Click View Report.**



The system displays the selected report. Here is an example of a “ValidLineData” report.

ta-2005.02.17-14.52.log

Go to page

|               |         |     |        |                        |
|---------------|---------|-----|--------|------------------------|
| LG 00 2 02 41 | LG 00 2 | 242 | GWC-44 | mg1kr1013.nortel.com   |
| LG 00 2 02 42 | LG 00 2 | 243 | GWC-44 | mg1kr1013.nortel.com   |
| LG 00 2 02 43 | LG 00 2 | 244 | GWC-44 | mg1kr1013.nortel.com   |
| LG 00 2 02 44 | LG 00 2 | 245 | GWC-44 | mg1kr1013.nortel.com   |
| LG 00 2 02 45 | LG 00 2 | 246 | GWC-44 | mg1kr1013.nortel.com   |
| LG 00 2 02 46 | LG 00 2 | 247 | GWC-44 | mg1kr1013.nortel.com   |
| LG 00 2 02 48 | LG 00 2 | 249 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 49 | LG 00 2 | 250 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 50 | LG 00 2 | 251 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 51 | LG 00 2 | 252 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 52 | LG 00 2 | 253 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 53 | LG 00 2 | 254 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 54 | LG 00 2 | 255 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 55 | LG 00 2 | 256 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 56 | LG 00 2 | 257 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 57 | LG 00 2 | 258 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 58 | LG 00 2 | 259 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 59 | LG 00 2 | 260 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 60 | LG 00 2 | 261 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 61 | LG 00 2 | 262 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 62 | LG 00 2 | 263 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 2 02 63 | LG 00 2 | 264 | GWC-44 | mg1kr1014.nortel.com   |
| LG 00 8 04 17 | LG 00 8 | 418 | GWC-44 | ambit16p002.nortel.com |
| LG 00 2 02 31 | LG 00 2 | 232 | GWC-44 | mg1kr1012.nortel.com   |

or Event Messaing Supported Line Data Integrity)

| GWC     | GW NAME               | EP NAME |
|---------|-----------------------|---------|
| GWC-100 | isplab3ncs.nortel.com | aaln/1  |
| GWC-100 | isplab3ncs.nortel.com | aaln/2  |
| GWC-100 | isplab3ncs.nortel.com | aaln/3  |
| GWC-100 | isplab3ncs.nortel.com | aaln/4  |

Prev

Next

Save as

Exit

**Note 1:** The CS 2000 Management Tools server retains the six most recent “ValidLineData” reports. When a new line audit occurs, the server deletes the oldest report.

**Note 2:** The system places valid data audit reports in the following directory on the CS 2000 Management Tools

server:

/opt/nortel/ptm/current/www/Audit/LineDataIntegrityAudit/.

- d** If you want to retain one of these reports for a longer time, or if you want to print a report, click the **Save as** button at the bottom of the screen. Then, save the report under a file name of your choice.
- e** To print a report you have saved, open the file using a text editor and print the file.
- f** After viewing the valid-data report, click the **Exit** button at the bottom of the screen.

**13** View the line problem-data report as follows:

- a** Ensure that you have selected **Line Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.
- b** Select **ProblemLineData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ProblemLineData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

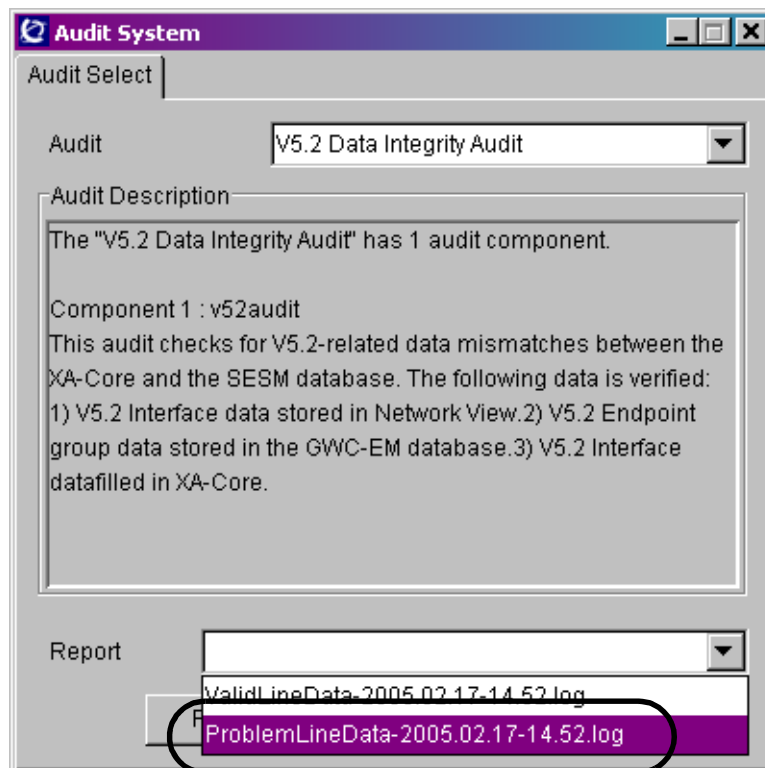
The file name has the following format:

ProblemLineData-<date>-<time>.log

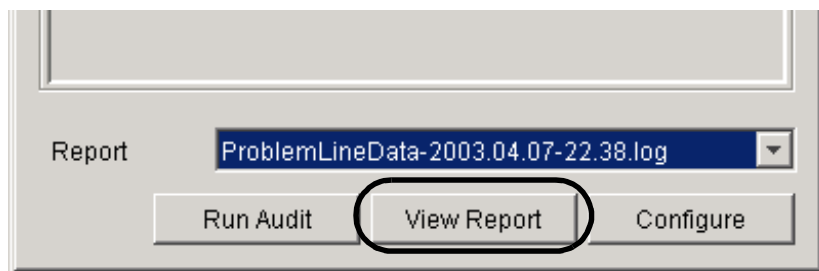
where

<date> is the date in yyyy.mm.dd format, for example, 2003.02.15.

<time> is the time in hh.mm format, for example 17.30.



c Click the **View Report** button.



The system displays the selected report.

If the audit found no problems, the “Problem” report contains a message stating that no problems were found.

The “Problem” report produced by a line audit can contain messages in the following formats:

- DN <DN> for LEN <len> has no associated Endpoint on <GWC ID>.
- Endpoint <endpointname> on gateway <gatewayname> on GWC <GWCname> has no associated DN/LEN on CM.

Here is an example of a “ProblemLineData” report:



Page: 1/1

Go to

```

EndPoint aaln/48 on Gateway mgikv2007.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/5 on Gateway mgikv2007.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/6 on Gateway mgikv2007.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/7 on Gateway mgikv2007.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/8 on Gateway mgikv2007.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/9 on Gateway mgikv2007.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/2 on Gateway mindytest.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/3 on Gateway mindytest.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/1 on Gateway natl.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/2 on Gateway natl.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/3 on Gateway natl.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/4 on Gateway natl.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/1 on Gateway natla.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/10 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/11 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/3 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/4 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/5 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/6 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/7 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/8 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/9 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/1 on Gateway ambitlp4217nat.nortel.com on GWC GWC-116 has no associated LEN on CM

```

## Invalid Data (For Event Messaing Supported Line Data Integrity)

```

EndPoint aaln/1 on Gateway isp33199.nortel.com on GWC GWC-100 has no event messaging associated LEN on CM
EndPoint aaln/2 on Gateway isp33199.nortel.com on GWC GWC-100 has no event messaging associated LEN on CM
LEN LG 00 0 08 56 for EndPoint aaln/1 on Gateway moto2pl.nortel.com has no associated endpoint on GWCEM
LEN LG 00 0 08 57 for EndPoint aaln/2 on Gateway moto2pl.nortel.com has no associated endpoint on GWCEM
LEN LG 00 0 10 17 for EndPoint aaln/1 on Gateway hobdqos.gdnt.com has no associated endpoint on GWCEM
LEN LG 00 1 03 50 for EndPoint aaln/1 on Gateway HOBDQOS1 has no associated endpoint on GWCEM
LEN LG 00 1 03 51 for EndPoint aaln/2 on Gateway HOBDQOS1 has no associated endpoint on GWCEM
LEN LG 00 1 03 52 for EndPoint aaln/3 on Gateway HOBDQOS1 has no associated endpoint on GWCEM
LEN LG 00 1 03 53 for EndPoint aaln/4 on Gateway HOBDQOS1 has no associated endpoint on GWCEM
LEN LG 00 1 03 64 for EndPoint aaln/1 on Gateway HOBDQOS2 has no associated endpoint on GWCEM
LEN LG 00 1 03 65 for EndPoint aaln/2 on Gateway HOBDQOS2 has no associated endpoint on GWCEM
LEN LG 00 1 03 66 for EndPoint aaln/3 on Gateway HOBDQOS2 has no associated endpoint on GWCEM
LEN LG 00 1 03 67 for EndPoint aaln/4 on Gateway HOBDQOS2 has no associated endpoint on GWCEM
LEN LG 00 9 00 67 for EndPoint aaln/1 on Gateway lab3ncsgw2.nortel.com has no associated endpoint on GWCEM
LEN LG 00 9 00 68 for EndPoint aaln/2 on Gateway lab3ncsgw2.nortel.com has no associated endpoint on GWCEM

```

Prev

Next

Save as

Exit

**Note 1:** The CS 2000 Management Tools server retains the six most recent “ProblemLineData” reports. When a new audit occurs, the server deletes the oldest report.

**Note 2:** The system places problem data audit reports in the following directory on the CS 2000 Management Tools server:

/opt/nortel/ptm/current/www/Audit/LineDataIntegrityAudit/.

- d If you want to retain one of these reports for a longer time, or print a report, click the **Save as** button at the bottom of the screen. Then, save the report under a new file name.

- e To print a report you have saved, open the file using a text editor and print the file.
- f To correct the problems, refer to the printed copy of the report. You will need to delete and then reprovision the listed lines.
- g After viewing the problem-data report, click the **Exit** button at the bottom of the viewer screen.

**14** Proceed as follows for a Trunk Data Integrity Audit:

| If you want to view           | Do                      |
|-------------------------------|-------------------------|
| the trunk valid-data report   | step <a href="#">15</a> |
| the trunk problem-data report | step <a href="#">16</a> |

**15** View the trunk valid-data report as follows:

- a Ensure that you have selected **Trunk Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.
- b Select **ValidTrunkData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ValidTrunkData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

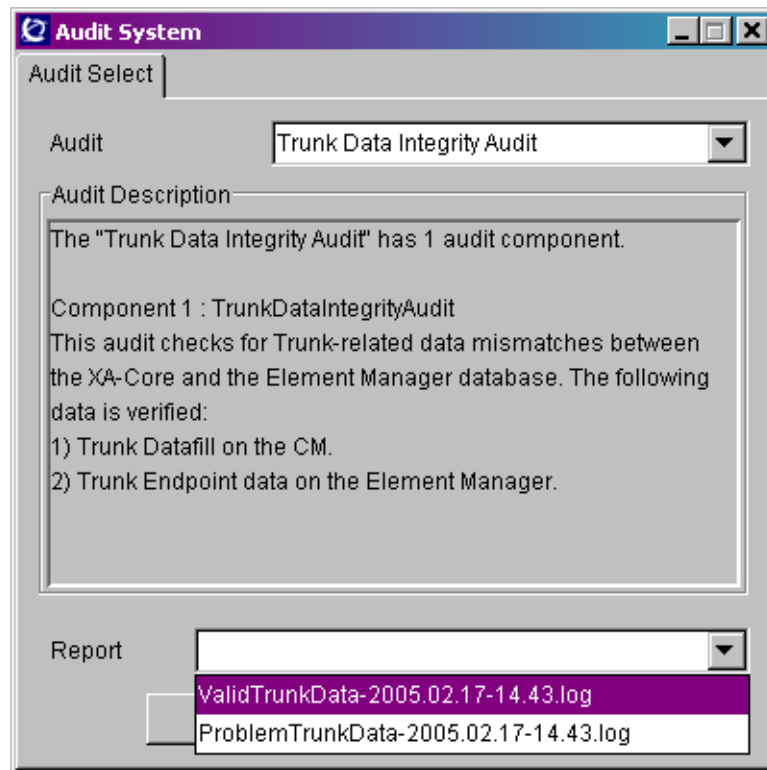
The file name has the following format:

ValidTrunkData-<date>-<time>.log

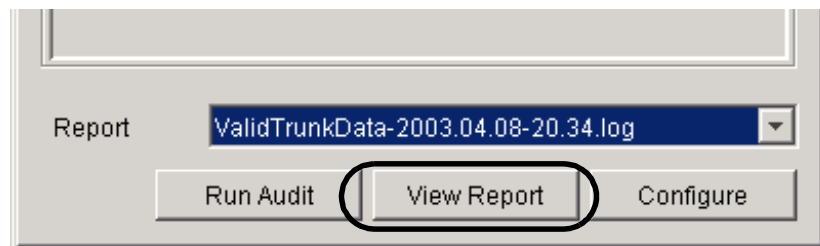
where

<date> is the date in yyyy.mm.dd format, for example, 2003.02.15.

<time> is the time in hh.mm format, for example 17.30.



c Click **View Report**.



The system displays the selected report. Here is an example of a "ValidTrunkData" report.

ValidTrunkData-2003.09.23-11.32.log

Page: 1/1

Go to page:

| CLLI    | TRK# | GWC   | NODE | TN | GW_NAME | EP_NAME     |
|---------|------|-------|------|----|---------|-------------|
| KOUPRI1 | 1    | GWC-1 | 15   | 1  | PVG190  | DS3_20.1.1  |
| KOUPRI1 | 2    | GWC-1 | 15   | 2  | PVG190  | DS3_20.1.2  |
| KOUPRI1 | 3    | GWC-1 | 15   | 3  | PVG190  | DS3_20.1.3  |
| KOUPRI1 | 4    | GWC-1 | 15   | 4  | PVG190  | DS3_20.1.4  |
| KOUPRI1 | 5    | GWC-1 | 15   | 5  | PVG190  | DS3_20.1.5  |
| KOUPRI1 | 6    | GWC-1 | 15   | 6  | PVG190  | DS3_20.1.6  |
| KOUPRI1 | 7    | GWC-1 | 15   | 7  | PVG190  | DS3_20.1.7  |
| KOUPRI1 | 8    | GWC-1 | 15   | 8  | PVG190  | DS3_20.1.8  |
| KOUPRI1 | 9    | GWC-1 | 15   | 9  | PVG190  | DS3_20.1.9  |
| KOUPRI1 | 10   | GWC-1 | 15   | 10 | PVG190  | DS3_20.1.10 |
| KOUPRI1 | 11   | GWC-1 | 15   | 11 | PVG190  | DS3_20.1.11 |
| KOUPRI1 | 12   | GWC-1 | 15   | 12 | PVG190  | DS3_20.1.12 |
| KOUPRI1 | 13   | GWC-1 | 15   | 13 | PVG190  | DS3_20.1.13 |
| KOUPRI1 | 14   | GWC-1 | 15   | 14 | PVG190  | DS3_20.1.14 |
| KOUPRI1 | 15   | GWC-1 | 15   | 15 | PVG190  | DS3_20.1.15 |
| KOUPRI1 | 16   | GWC-1 | 15   | 16 | PVG190  | DS3_20.1.16 |
| KOUPRI1 | 17   | GWC-1 | 15   | 17 | PVG190  | DS3_20.1.17 |
| KOUPRI1 | 18   | GWC-1 | 15   | 18 | PVG190  | DS3_20.1.18 |
| KOUPRI1 | 19   | GWC-1 | 15   | 19 | PVG190  | DS3_20.1.19 |
| KOUPRI1 | 20   | GWC-1 | 15   | 20 | PVG190  | DS3_20.1.20 |
| KOUPRI1 | 21   | GWC-1 | 15   | 21 | PVG190  | DS3_20.1.21 |
| KOUPRI1 | 22   | GWC-1 | 15   | 22 | PVG190  | DS3_20.1.22 |
| KOUPRI1 | 23   | GWC-1 | 15   | 23 | PVG190  | DS3_20.1.23 |
| KOUPRI2 | 25   | GWC-1 | 15   | 25 | PVG190  | DS3_20.2.1  |
| KOUPRI2 | 26   | GWC-1 | 15   | 26 | PVG190  | DS3_20.2.2  |
| KOUPRI2 | 27   | GWC-1 | 15   | 27 | PVG190  | DS3_20.2.3  |
| KOUPRI2 | 28   | GWC-1 | 15   | 28 | PVG190  | DS3_20.2.4  |
| KOUPRI2 | 29   | GWC-1 | 15   | 29 | PVG190  | DS3_20.2.5  |
| KOUPRI2 | 30   | GWC-1 | 15   | 30 | PVG190  | DS3_20.2.6  |
| KOUPRI2 | 31   | GWC-1 | 15   | 31 | PVG190  | DS3_20.2.7  |

Prev Next Save as Exit

**Note 1:** The CS 2000 Management Tools server retains the six most recent “ValidTrunkData” reports. When a new trunk audit occurs, the server deletes the oldest report.

**Note 2:** The system places trunk audit reports in the following directory on the CS 2000 Management Tools server:

/opt/nortel/ptm/current/www/Audit/TrunkDataIntegrityAudit/.

- d If you want to retain one of these reports for a longer time, or if you want to print a report, click **Save as** at the bottom of the screen. Then, save the report under a file name of your choice.
- e To print a report you have saved, open the file using a text editor and print the file.
- f After viewing the valid-data report, click **Exit** at the bottom of the screen.

- 16 View the trunk problem-data report as follows:
- Ensure that you have selected **Trunk Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit system dialog box.
  - Select **ProblemTrunkData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ProblemTrunkData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

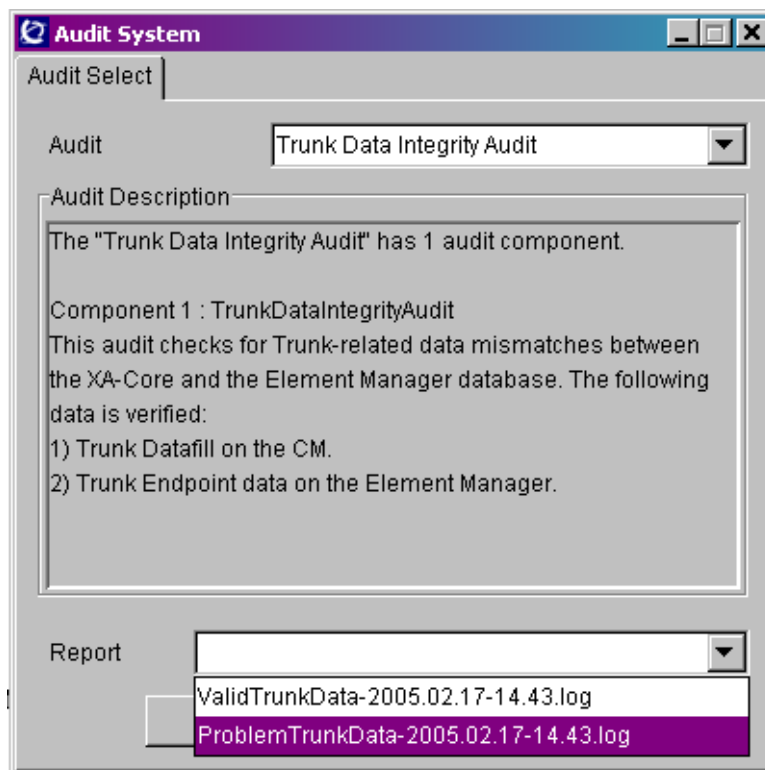
The file name has the following format:

ProblemTrunkData-<date>-<time>.log

where

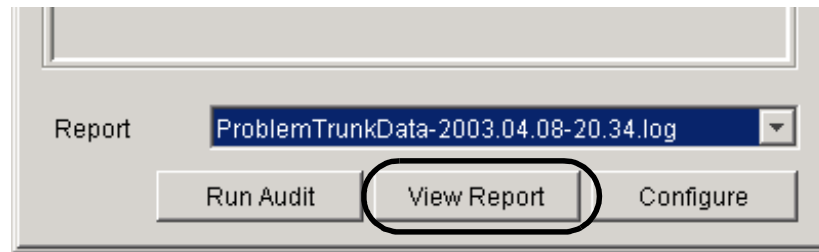
<date> is the date in yyyy.mm.dd format, for example, 2003.02.15.

<time> is the time in hh.mm format, for example 17.30.



- Click the **View Report** button.





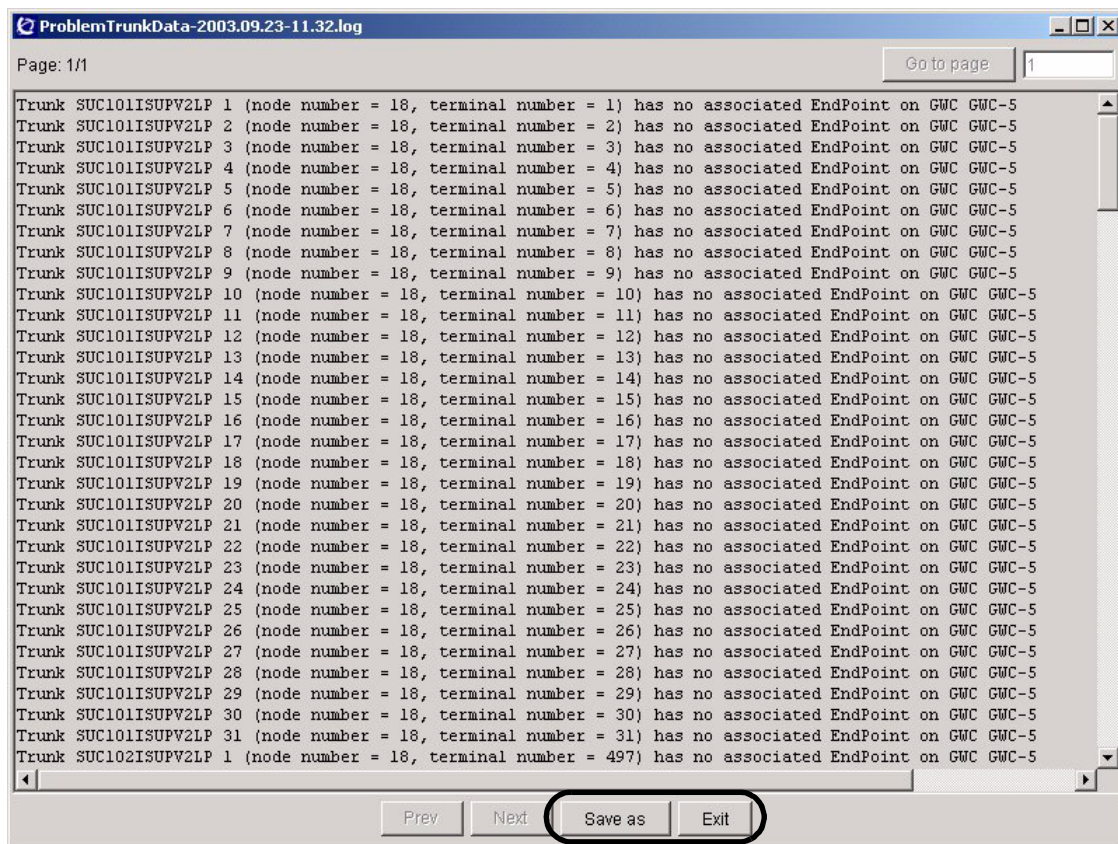
The system displays the selected report.

If the audit found no problems, the “Problem” report contains a message stating that no problems were found.

The “Problem” report produced by a trunk audit can contain messages in the following formats:

- Trunk <trunk name> (node number = <NODE>, terminal number = <TID>) has no associated Endpoint on GWC <GWC ID>.
- Endpoint <EP NAME> on gateway <GW NAME> (terminal number = <TID>) on GWC <GWC ID> has no associated trunk member datafilled on the CM.

Here is an example of a “ProblemTrunkData” report:



**Note 1:** The CS 2000 Management Tools server retains the six most recent “ProblemTrunkData” reports. When a new audit occurs, the server deletes the oldest report.

**Note 2:** The system places trunk audit reports in the following directory on the CS 2000 Management Tools server:

/opt/nortel/ptm/current/www/Audit/TrunkDataIntegrityAudit/.

- d If you want to retain one of these reports for a longer time, or print a report, click **Save as** at the bottom of the screen. Then, save the report under a file name of your choice.
- e To print a report you have saved, open the file using a text editor and print the file.



**c Click View Report.**

The system displays the selected report. If no problems were discovered, the report will be empty. Here is an example of a report in which two problems were discovered:

A screenshot of the 'V5.2 Data Integrity Audit Report' window. The window title is 'V5.2 Data Integrity Audit Report'. The menu bar includes 'File'. The status bar shows 'Last Audit Date: 2003-04-11 16:50:33'. The main content area contains a table with the following data:

| Index | Problem Description                                                                                                        | Current Status |
|-------|----------------------------------------------------------------------------------------------------------------------------|----------------|
| 0     | A V5.2 Link with Interface ID 23456 and Link ID 1 is datafilled in GPPTRNLS table but there is no matching entry in GWC-EM | Problem Exists |
| 1     | A V5.2 Link with Interface ID 23456 and Link ID 2 is datafilled in GPPTRNLS table but there is no matching entry in GWC-EM | Problem Exists |

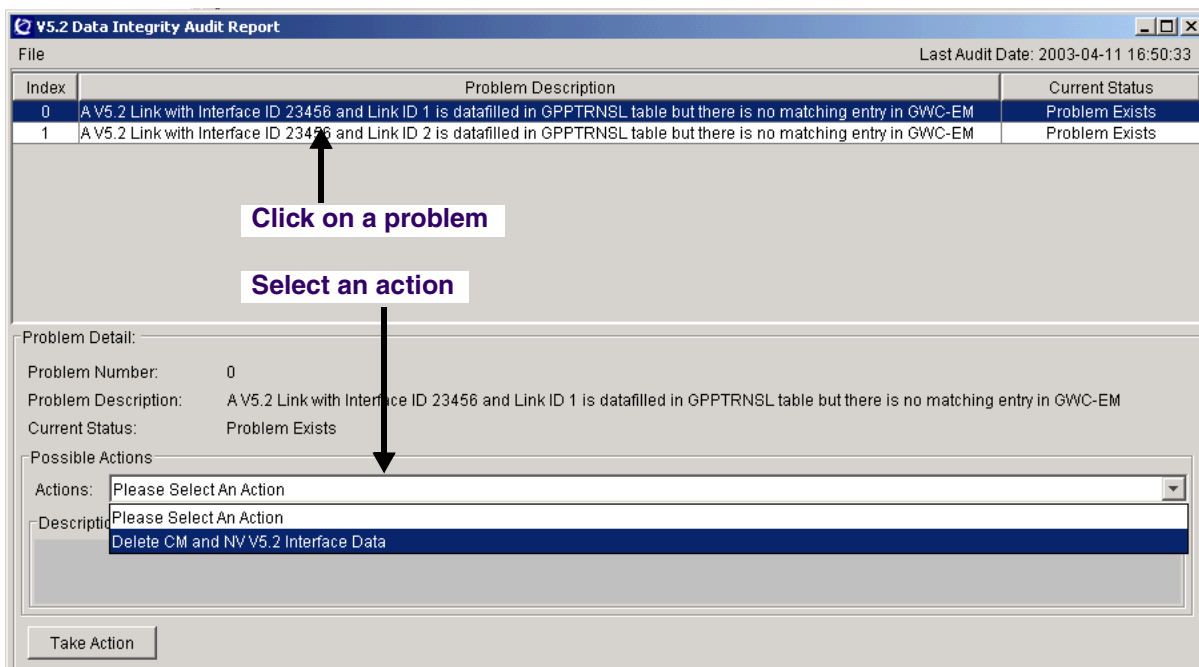
Below the table is a section titled 'Problem Detail:' with fields for 'Problem Number:', 'Problem Description:', and 'Current Status:'. There is also a 'Possible Actions' section with an 'Actions:' dropdown menu and a 'Description' text area. At the bottom left is a 'Take Action' button.

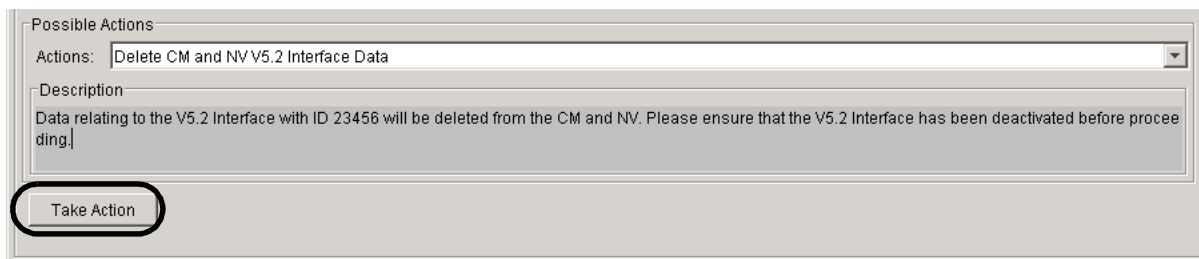
**Note 1:** The CS 2000 Management Tools server retains the most recent V5.2 audit report. When a new audit occurs, the server deletes the previous report.

**Note 2:** The system places the audit report in the following directory on the CS 2000 Management Tools server: /opt/nortel/ptm/current/MI2/apps/Audit.

**Note 3:** The CS 2000 GWC Manager does not provide an option to save a V5.2 audit report to local disk.

- 18 Review the results of the audit and click on a problem to resolve.  
**Note:** If necessary, resize the entire window to completely view the Problem Description field.
- 19 Evaluate actions to resolve a problem and take action.
  - a Click and hold on the Action pull-down menu near the bottom of the screen to assess any possible actions.
  - b If appropriate, select an action. Read the description of the action and ensure that you observe any recommended steps or cautions.



**c Click Take Action.**

Possible Actions

Actions: Delete CM and NV V5.2 Interface Data

Description

Data relating to the V5.2 Interface with ID 23456 will be deleted from the CM and NV. Please ensure that the V5.2 Interface has been deactivated before proceeding.

Take Action

**Note:** If you see the message “Correction Failed”, please contact your next level of support.

- 20 Return to [step 18](#) to review another problem.
- 21 You have completed this procedure.

---

## Posting a line by directory number

---

### Application

Use this procedure to post a line by its directory number (DN) so you can perform maintenance on the line.

### Restrictions

V5.2 line maintenance is not supported using the Line Maintenance Manager (LMM). V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface.

Since the CS 2000 supports both legacy DMS TDM lines as well as Succession lines, TDM lines can be posted on LMM and maintenance operations like BSY/RTS/FRLS/INB can be performed; however, the CS Line State column will not be displayed accurately. The Endpoint State column will show "Legacy Line" and the GW Profile column and all properties not applicable to TDM lines will display as "Not Available".

When using hunt groups, you can only post the primary DN using the Line Maintenance Manager. You cannot perform line maintenance operations on all members of a hunt group using the LMM. If you need to perform line maintenance on all members of a hunt group, use the CS 2000 XA-Core MAPCI interface. For details, refer to the DMS-100 Family National ISDN BRI Service Implementation Guide, 297-2401-201.

### Prerequisites

All Line Maintenance Manager (LMM) status fields must be Green (OK) in order to post lines.



### Action

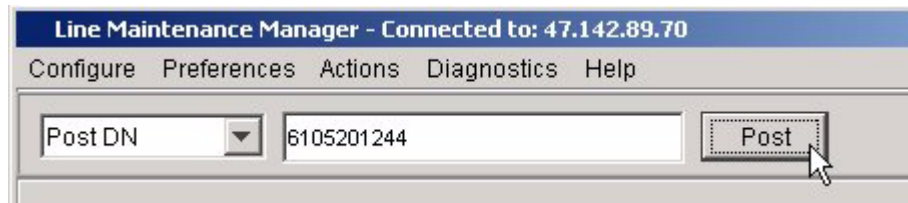
Perform the following steps to complete this procedure.

#### ***At your workstation***

- 1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#) in this document, if required.

***At the LMM GUI***

- 2 Select **Post DN**, enter the directory number, and click **Post**.



- 3 You have completed this procedure.



---

## Posting a line by gateway

---

### Application

Use this procedure to post one or more lines by their associated gateway so you can perform maintenance on the lines.

Use this procedure after adding a gateway and before performing maintenance on that gateway.

### Restrictions

V5.2 line maintenance is not supported using Line Maintenance Manager (LMM). V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

Only line gateways can be posted.

### Prerequisites

The following prerequisites apply to posting one or more lines by gateway:

- The associated gateway must be provisioned with endpoints in the CS 2000 GWC Manager database
- All LMM status fields must be Green (OK) in order to post lines.



### Action

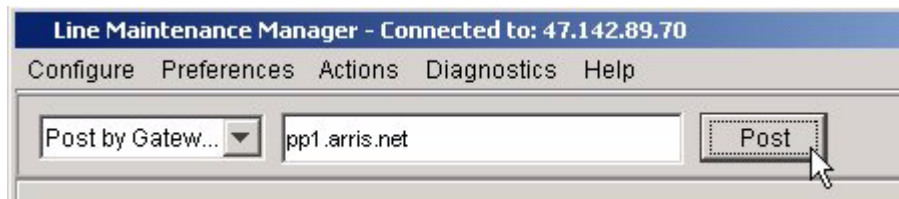
Perform the following steps to complete this procedure.

#### ***At your workstation***

- 1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#) in this document, if required.

**At the LMM GUI**

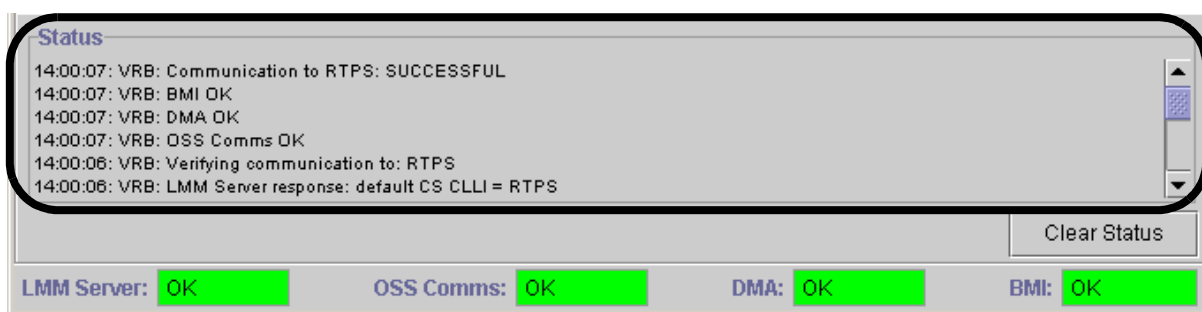
- 2 Select **Post by Gateway**, enter the name of the gateway and its path, then click **Post**.



- 3 You have completed this procedure.

**Additional information**

When post-by-gateway is selected on the LMM GUI, the line state at the CM is displayed. A on-demand audit to identify the state of the endpoint on the gateway is also done through the CS 2000 GWC Manager and the endpoint state is displayed at the LMM GUI Endpoint State field. This audit is done in a protocol independent manner by the LMM. Any errors produced during the posting activity will be displayed on the status panel shown below.



A list of currently supported LMM GUI error codes with descriptions is shown in the following table.

| Error Code | LMM client text displayed in status panel | Description                               |
|------------|-------------------------------------------|-------------------------------------------|
| 1000       | OK                                        | Audit response received from endpoint     |
| 1010       | Wait_GW_response                          | GWC waiting for gateway audit response    |
| 1020       | GW_Protocol_Unsupported                   | Unsupported gateway protocol              |
| 1100       | GWC_Unavailable                           | GWC not available for endpoint query      |
| 1200       | IP_Unavailable                            | Unable to retrieve IP address for gateway |
| 2000       | SNMP_exception                            | SNMP error between LMM and GWC            |

| Error Code | LMM client text displayed in status panel | Description                                     |
|------------|-------------------------------------------|-------------------------------------------------|
| 2010       | EP_Not_Found                              | Endpoint status expired in GWC before retrieval |
| 2020       | Invalid_EP                                | Endpoint does not exist in GWC                  |
| 3000       | GWC_LoadName_error                        | Incompatible GWC load version detected          |
| 3010       | Unsupported_GWC_Load                      | GWC is running an unknown or unsupported load   |
| 4000       | Decode_Failure                            | Error decoding Gateway IP address               |
| 4010       | Unknown_Endpoint                          | LMM could not get endpoint state                |



---

## Busying a line

---

### Application

Use this procedure to busy (BSY) a line and put it into a maintenance busy (MB) state. Once busied, the line cannot perform call processing.

Use this procedure during maintenance or alarm clearing activities.

### Restrictions

V5.2 line maintenance is not supported using Line Maintenance Manager. V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

### Prerequisites

The line must be posted. Refer to procedures [Posting a line by gateway on page 997](#) or [Posting a line by directory number on page 995](#) in this document, if required.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#) in this document, if required.

#### *At the LMM GUI*

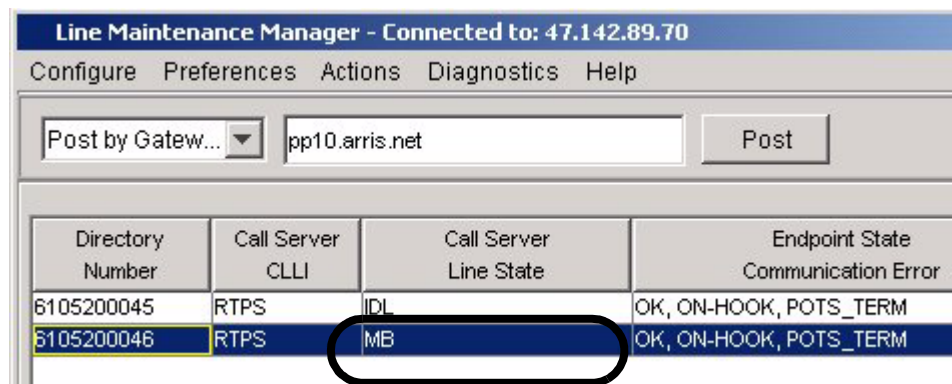
- 2 Select the DN you want to busy, then on the **Actions** menu, click **BSY**, or right-click on the selected DN then click **BSY**.

**Note:** You can perform this operation on one or more posted lines at the same time. You can use the **Shift** key to select multiple lines consecutively, or the **Ctrl** key to select multiple lines non-consecutively.



- 3 Observe that the selected DN(s) are put into a maintenance busy (MB) state as shown below.

**Note:** The line state will be CPD if the original line state was CPB prior to Busy.



- 4 You have completed this procedure.

---

## Installation busying a line

---

### Application

Use this procedure to set a line to the installation busy (INB) state.

Use this procedure during maintenance and fault clearing activities.

### Restrictions

V5.2 line maintenance is not supported using Line Maintenance Manager. V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

### Prerequisites

The line must be posted. Refer to procedures [Posting a line by gateway on page 997](#) or [Posting a line by directory number on page 995](#) in this document, if required.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications](#) in this document, if required.

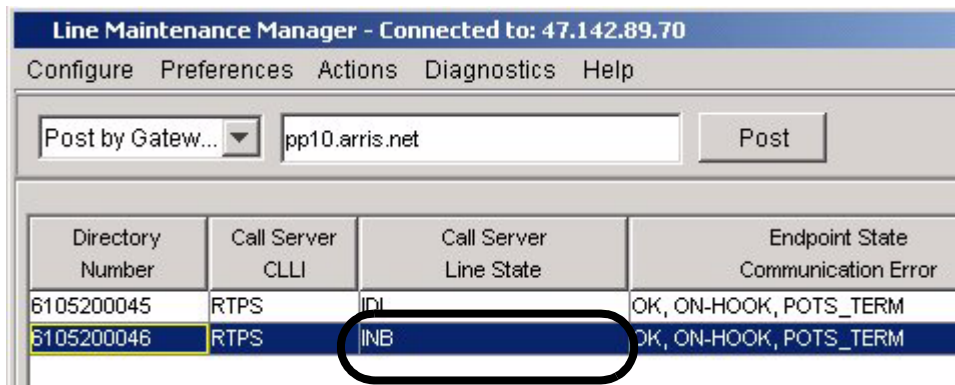
#### *At the LMM GUI*

- 2 Select the DN you want to installation busy, then on the **Actions** menu, click **INB**, or right-click on the selected DN then click **INB**.

**Note:** You can perform this operation on one or more posted lines at the same time. You can use the **Shift** key to select multiple lines consecutively, or the **Ctrl** key to select multiple lines non-consecutively.



- 3 Observe that the selected DN(s) are put into an installation busy (INB) state as shown below.



- 4 You have completed this procedure.



---

## Force releasing a line

---

### Application

Use this procedure to force release (FRLS) a line, putting it into a maintenance busy (MB) state.

Use this procedure if Nortel Networks support personnel indicate its use.

### Restrictions

V5.2 line maintenance is not supported using Line Maintenance Manager. V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

### Prerequisites

The line must be posted. Refer to procedures [Posting a line by gateway on page 997](#) or [Posting a line by directory number on page 995](#) in this document, if required.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#) in this document, if required.

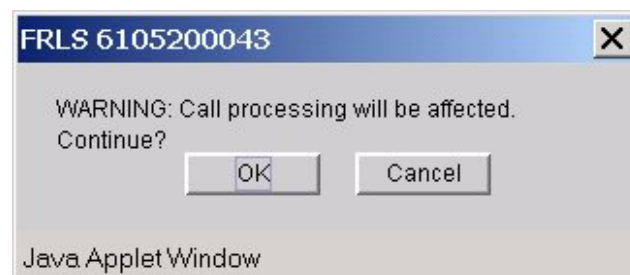
#### *At the LMM GUI*

- 2 Select the DN you want to force a release on, then on the **Actions** menu, click **FRLS**, or right-click on the selected DN then click **FRLS**.

**Note:** You can perform this operation on one or more posted lines at the same time. You can use the **Shift** key to select multiple lines consecutively, or the **Ctrl** key to select multiple lines non-consecutively.

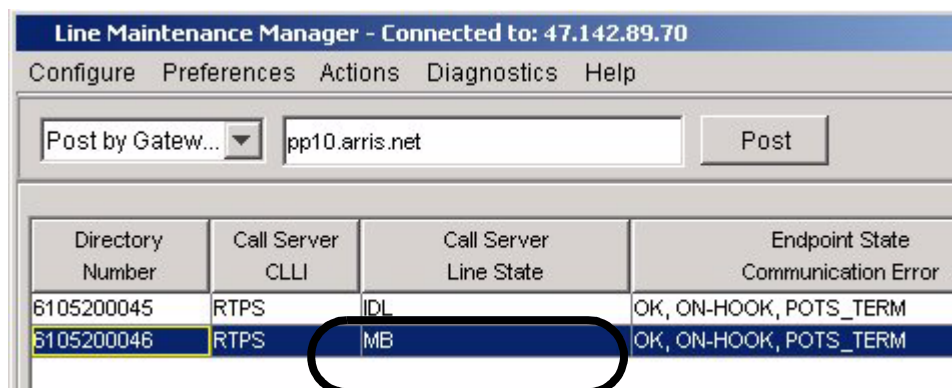


- 3 Click **OK** to confirm the force release of the line(s).



**Note:** The call will be dropped if there was a call on the selected DN.

- 4 Observe that the selected DN(s) are put into an maintenance busy (MB) state as indicated in the following figure.



- 5 You have completed this procedure.

---

## Returning a line to service

---

### Application

Use this procedure to return a busied line to service (RTS). Once returned to service, the line can then perform call processing.

Use this procedure after maintenance has been performed on a busied line.

### Restrictions

V5.2 line maintenance is not supported using Line Maintenance Manager. V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

### Prerequisites

The line must be in a maintenance busy (MB) state. Refer to procedure [Busying a line on page 1001](#) in this document, if required.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#) in this document, if required.

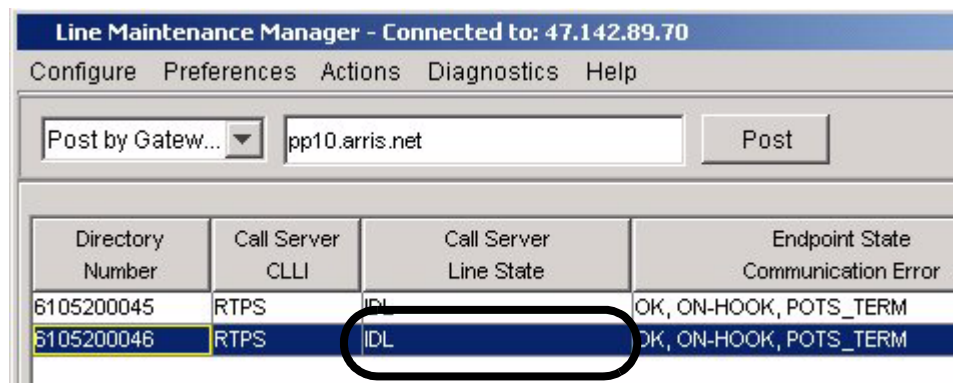
#### *At the LMM GUI*

- 2 Select the DN you want to return to service, then on the **Actions** menu, click **RTS**, or right-click on the selected DN then click **RTS**.

**Note:** You can perform this operation on one or more posted lines at the same time. You can use the **Shift** key to select multiple lines consecutively, or the **Ctrl** key to select multiple lines non-consecutively.



- 3 Observe that the state of the selected DN(s) is changed from maintenance busy (MB) to idle (IDL) as shown below.



- 4 You have completed this procedure.

---

## Clearing one or more posted lines from the display

---

### Application

Use this procedure to remove a directory number (DN) from the list of posted DNs.

Use this procedure before performing maintenance on a posted set of lines or when the posted lines no longer need to be monitored.

### Restrictions

V5.2 line maintenance is not supported using Line Maintenance Manager. V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

### Prerequisites

The line must be posted. Refer to procedures [Posting a line by gateway on page 997](#) or [Posting a line by directory number on page 995](#) in this document, if required.

### Action

Perform the following steps to complete this procedure.

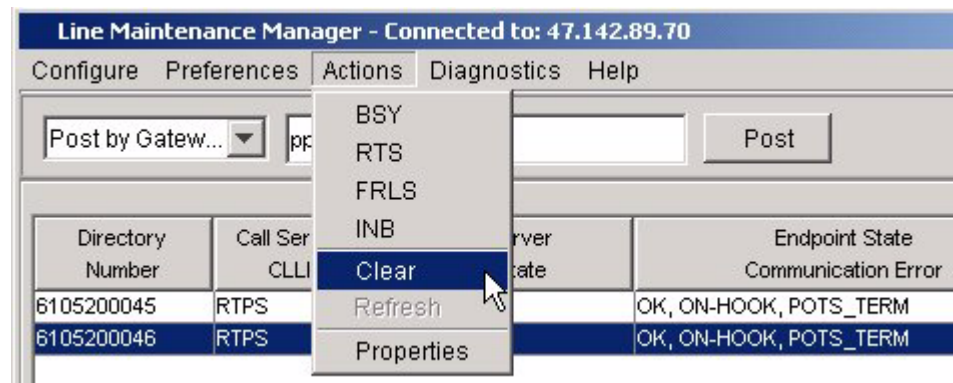
#### *At your workstation*

- 1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#) in this document, if required.

#### *At the LMM GUI*

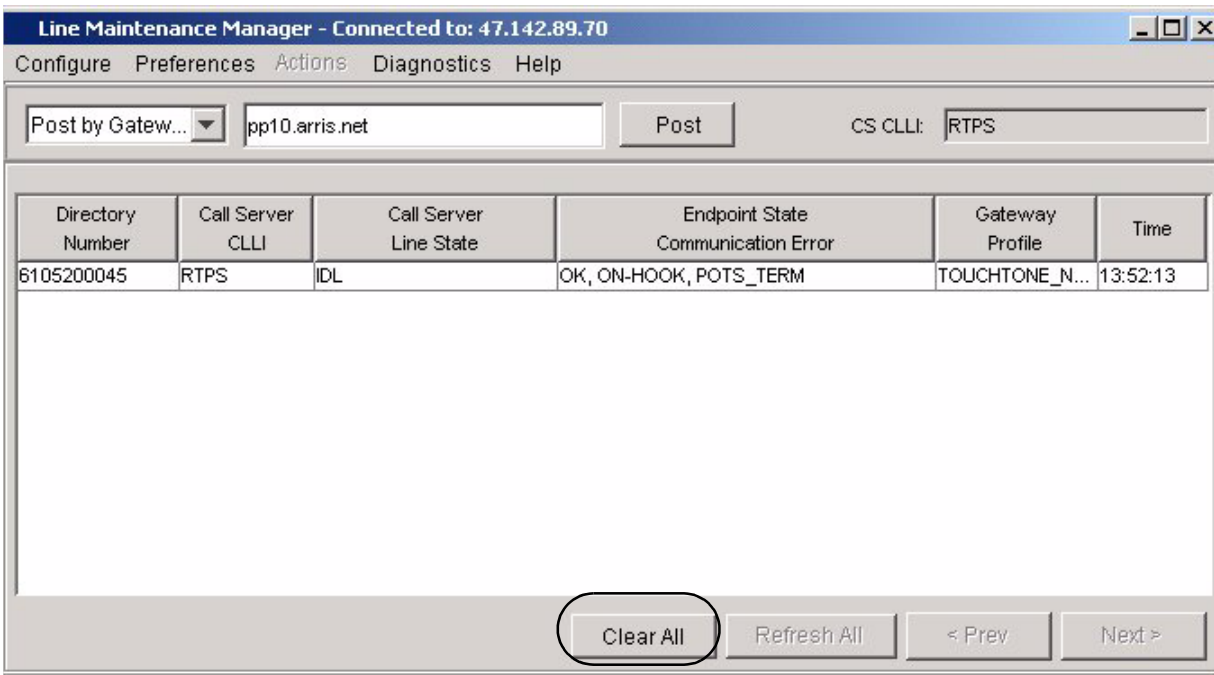
- 2 Select the DN you want to remove from the display of posted lines, then on the **Actions** menu, click **Clear**, or right-click on the selected DN then click **Clear**.

**Note:** You can perform this operation on one or more posted lines at the same time. You can use the **Shift** key to select multiple lines consecutively, or the **Ctrl** key to select multiple lines non-consecutively.



- 3 Observe that the selected DN(s) are cleared from the list as shown below.

**Note:** To clear all posted DN, click **Clear All**.



- 4 You have completed this procedure.

---

## Retrieving line properties

---

### Application

Use this procedure to retrieve and display the line properties for a selected directory number (DN) or group of DNs.

Use this procedure as a part of fault clearing activities.

### Restictions

V5.2 line maintenance is not supported using Line Maintenance Manager. V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

### Prerequisites

The line must be posted. Refer to procedures [Posting a line by gateway on page 997](#) or [Posting a line by directory number on page 995](#) in this document, if required.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#) in this document, if required.

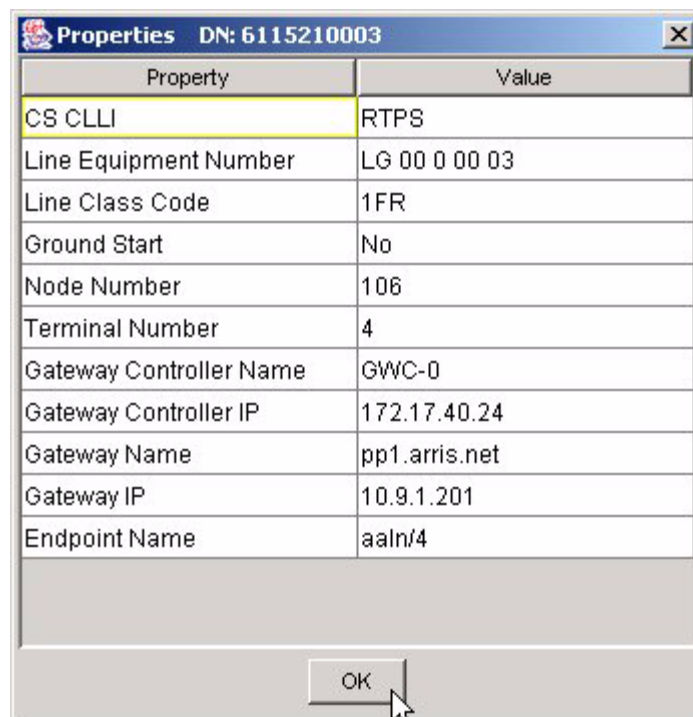
#### *At the LMM GUI*

- 2 Select the DN you want to view the properties for, then on the **Actions** menu, click **Properties**, or right-click on the selected DN then click **Properties**.

**Note:** You can perform this operation on one or more posted lines at the same time. You can use the **Shift** key to select multiple lines consecutively, or the **Ctrl** key to select multiple lines non-consecutively.



The Properties window, similar to the following, opens.



**Note:** If a gateway was provisioned with IP address 0.0.0.0 (Discovery), the IP address shown in the Properties window will indicate the current Dynamic IP address of the gateway as reflected in the Gateway Controller.

- 3 Click **OK** to close the Properties window.
- 4 You have completed this procedure.



## Querying line gateways in a trouble state

### Application

This procedure describes how to perform a query on line gateways in a trouble state, and view reports.

**Note:** You can configure a query to run on a daily or weekly basis at a specific time. Refer to procedure “Configuring a query for line gateways in a trouble state” in the ATM/IP Solution-level Configuration Management document, NN10409-500.

Use this procedure to troubleshoot line gateways.

### Prerequisites

All Line Maintenance Manager (LMM) status fields must be Green (OK) in order to perform a query.



### Action

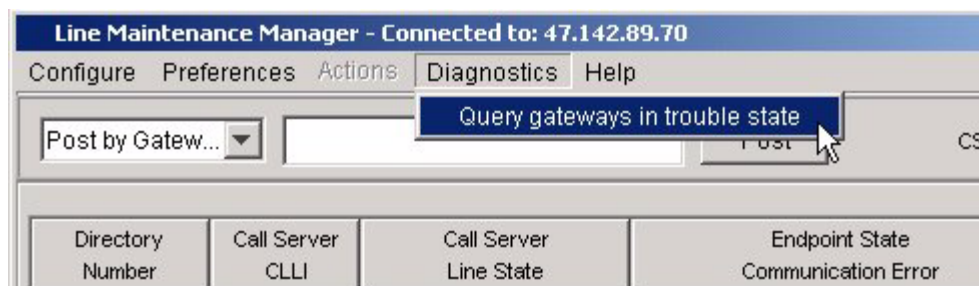
Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Launch the Line Maintenance Manager (LMM) GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#).

#### *At the LMM GUI*

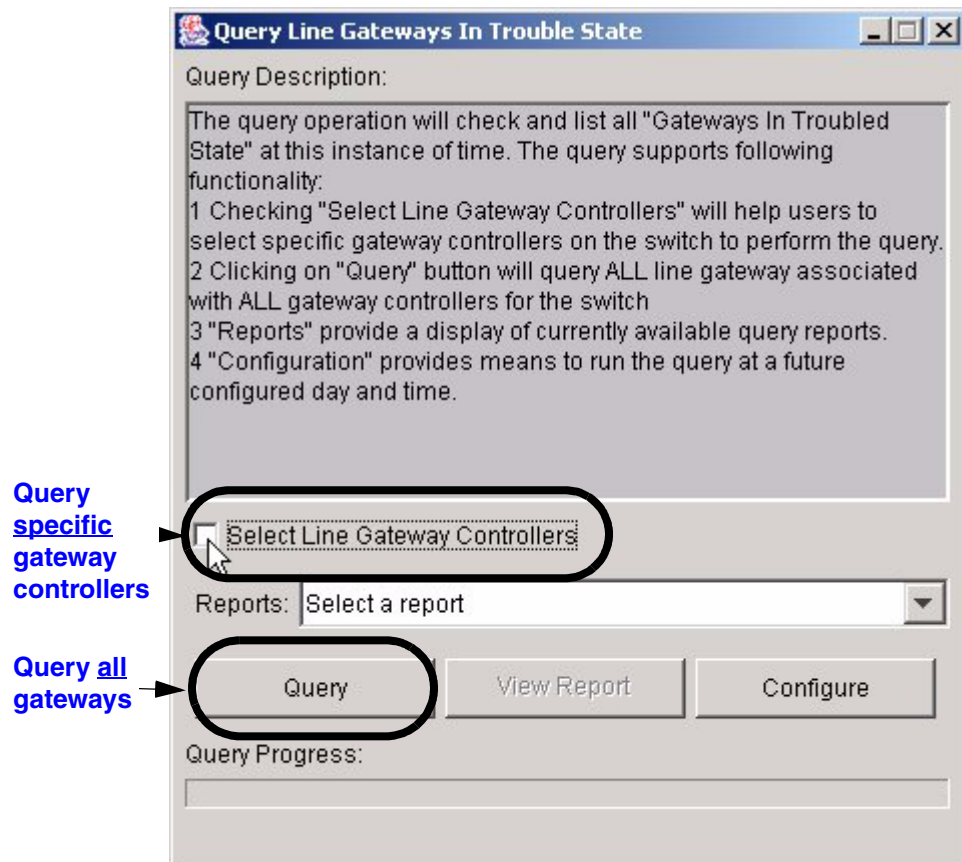
- 2 On the **Diagnostics** menu, click **Query gateways in trouble state**.



- 3 Use the following table to determine your next step.

| If you want to  | Do                     |
|-----------------|------------------------|
| perform a query | step <a href="#">4</a> |
| view reports    | step <a href="#">8</a> |

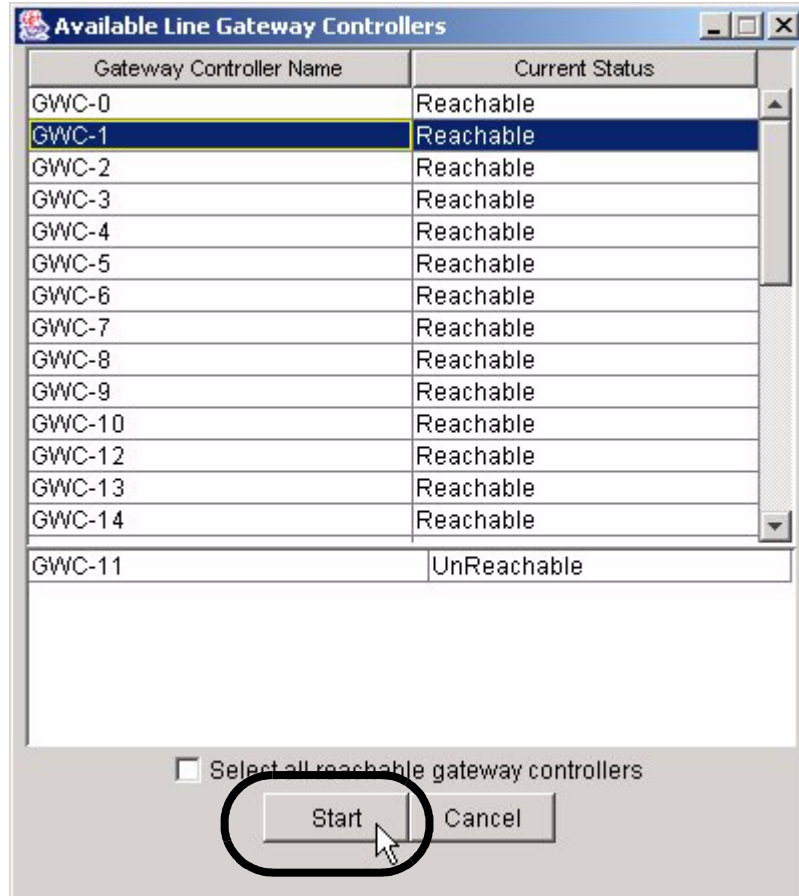
- 4 Click **Query** to query all line gateways associated with all gateway controllers for the switch, or click the **Select line gateway controllers** check box to query all line gateways associated with specific gateway controllers .



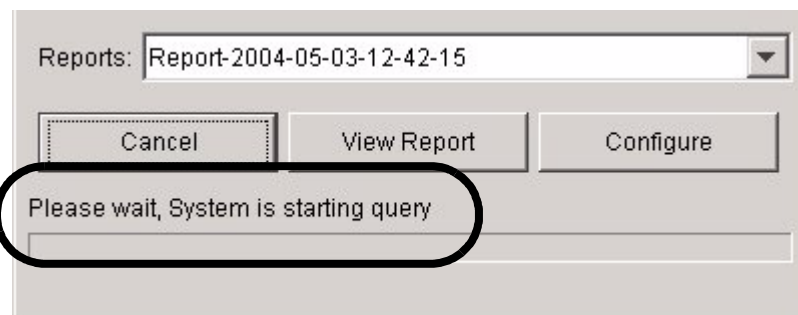
- 5 Use the following table to determine your next step.

| If you are querying          | Do                     |
|------------------------------|------------------------|
| specific gateway controllers | step <a href="#">6</a> |
| all gateways                 | step <a href="#">7</a> |

- 6 Select the reachable gateway controller(s) of your choice, press **Ctrl+a**, or click the **Select all reachable gateway controllers** check box, then click **Start**.

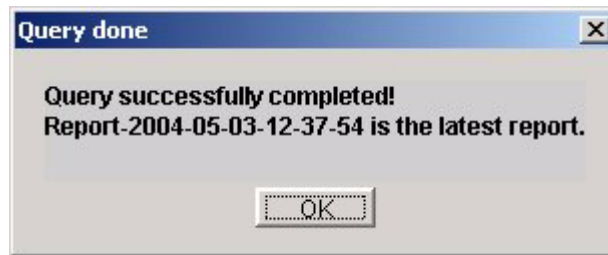


The system starts the query.

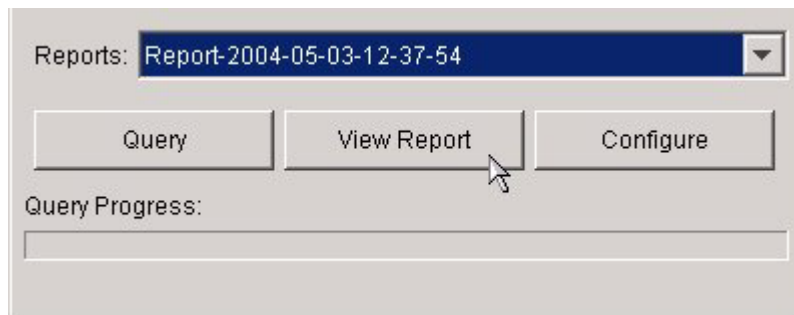


**Note:** Click **Cancel** at any time to cancel the query.

- 7 Click **OK** once the query completes.



- 8 Select a report from the list and click **View Report**. If you just performed a query, the report is the one displayed in the **Reports:** box.



**Note:** The system maintains a maximum number of seven reports for each gateway controller.

- 9 Click on the gateway controller of your choice to display the associated gateways and their trouble state information.

| Query Report - Report-2003-09-11-15-30 |              |                    |                    |             |
|----------------------------------------|--------------|--------------------|--------------------|-------------|
| Report-2003-09-11-15-30                |              |                    |                    |             |
| Gateway Controller Name                | Query Result | Number of Gateways | Gateway Name       |             |
| GWCC-8                                 | Successful   | 580                | GWCC08_OrigGW1 ... | GW DISABLED |
|                                        |              |                    | GWCC08_OrigGW1 ... | GW DISABLED |
|                                        |              |                    | GWCC08_OrigGW1 ... | GW DISABLED |
|                                        |              |                    | GWCC08_OrigGW1 ... | GW DISABLED |
|                                        |              |                    | GWCC08_OrigGW1 ... | GW DISABLED |

The gateway can be in any one of the following states:

- GW OK
- GW introuble
- GW inservice trouble
- GW disabled

The “GW disabled” state has security details appended to it to quickly determine if security is causing the gateway disabled condition. The security details are as follows:

| State                              | Meaning                                                              |
|------------------------------------|----------------------------------------------------------------------|
| GW DISABLED; SECURE:200 (0,0)      | gateway has secure policy (policy ID = 200), but no SAs              |
| GW DISABLED; FLEX-secure:400 (0,0) | gateway has flex policy (policy ID = 400) in secure mode, but no SAs |
| GW DISABLED; FLEX-non-secure:400   | gateway has flex policy (policy ID = 400) in non-secure mode         |

| State                                                 | Meaning                                                                                   |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------|
| GW DISABLED; FLEX-unknown:400                         | gateway has flex policy (policy ID = 400), IP known, but security mode not yet discovered |
| GW DISABLED; BYPASS:default                           | gateway has bypass policy                                                                 |
| GW DISABLED; BYPASS:1000                              | gateway has bypass policy (policy ID = 1000)                                              |
| GW DISABLED; DISCARD:2000                             | gateway has discard policy (policy ID = 2000)                                             |
| <b>Note:</b> The policy ID numbers are only examples. |                                                                                           |

If the security details indicate a SECURE or FLEX-secure policy without Security Associations (SAs), that is "0,0", which represents the count of incoming and outgoing SAs respectively, then security is likely involved and needs to be verified. If a discard policy is provisioned, this will cause all messaging to or from the gateway to be discarded, and will cause the disabled state. If the gateway uses Dynamic Host Configuration Protocol (DHCP), and it has not yet discovered its IP address, the state of the gateway will be disabled with no security details.

- 10 As required, you can select other reports from the **Query Report** window. You can scroll through the list of gateways using the **Prev** (previous) and **Next** buttons.

You have completed this procedure.

---

## Performing trunk maintenance using the Trunk Maintenance Manager

---

### Application

Use this procedure to perform maintenance operations on trunks using the Trunk Maintenance Manager (TMM). This procedure provides the steps to perform maintenance operations on trunks using any one of the following methods:

- [Maintenance by carrier on page 1020](#)
- [Maintenance by Gateway Name on page 1027](#)
- [Maintenance by trunk CLLI on page 1034](#)

The maintenance operations available, are as follows:

- post - posts trunk for maintenance activities
- busy - removes trunk from service and makes it unavailable for call processing
- installation busy - busies trunk from the MB (manual busy) or NEQ (not equipped) state for provisioning or test purposes
- return to service - returns trunk to service and makes it available for call processing
- force release - forces trunk already involved in call processing, out of service, and makes it unavailable for call processing

You can also query carrier and endpoint states using methods [Maintenance by carrier on page 1020](#) or [Maintenance by Gateway Name on page 1027](#) respectively.

Maintenance operations using the Trunk Maintenance Manager (TMM) are supported on ISUP, PRI (Carrier Voice over IP only), and PTS trunks.

### Prerequisites

None

### Action

Perform the steps under one of the following methods to complete this procedure:

- [Maintenance by carrier](#)
- [Maintenance by Gateway Name](#)
- [Maintenance by trunk CLLI](#)

## Maintenance by carrier

### At your workstation

- 1 Launch the Trunk Maintenance Manager (TMM) GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#).

### At the TMM GUI

- 2 Click **Maintenance By Carrier**.

A window similar to the following, is displayed.

**Trunk Maintenance Manager**

**Maintenance Actions**

Maintenance Action

Maintenance By Gateway Name •

Maintenance By Carrier •

Get Trunk CLLI by GW Name •

Maintenance By Trunk CLLI •

D-Channel Maintenance •

ICOT Test •

**Properties**

CM CLLI •

Auto-Refresh Rate •

☐ Auto-Refresh •

☒ Need Confirmation •

On-line Help •

Home •

Gateway Name: No Gateway Selection

Endpoint Range: 0-

Maintenance Action: Query Carrier State

When Querying, Show: All States

Carrier Names: Add >> << Del

Go

Show Details: ☐

NORTEL NETWORKS

- 3 Enter the request criteria as follows:
  - a Select a gateway from the **Gateway Name** list.
  - b Optionally enter an endpoint range value, or use the default (0-) value to display all endpoints.
  - c Optionally select the state for the endpoints you want displayed, or use the default (All States) value to display endpoints in all states.
  - d Optionally select one or more carriers from the **Carrier Names** list, and click **Add** to add the selected carriers to the request input, or use the default (All Carriers) value for all carriers.



- e Optionally click the **Show Details** check box if you want to display additional details about the carriers, otherwise, only a summary of the carriers will be displayed.

4 Use the following table to determine your next step.

| If you want to            | Do                          |
|---------------------------|-----------------------------|
| Query carrier state       | step <a href="#">a</a> only |
| Post carrier              | step <a href="#">b</a> only |
| Busy carrier              | step <a href="#">c</a> only |
| Return carrier to service | step <a href="#">d</a> only |
| Force release carrier     | step <a href="#">e</a> only |
| Installation busy carrier | step <a href="#">f</a> only |

- a Select **Query Carrier State** from the **Maintenance Action** list, and click **Go**.

Following is an example of the response with **Show Details** checked:

|                         |                    |                           |                       |
|-------------------------|--------------------|---------------------------|-----------------------|
| Gateway Name:<br>PVG190 | Node Number:<br>13 | Filtered by State:<br>ALL | Endpoint Range:<br>0- |
|-------------------------|--------------------|---------------------------|-----------------------|

| Summary of Endpoints |     |
|----------------------|-----|
| Total Endpoints      | 672 |
| IDL                  | 289 |
| UNKNOWN              | 138 |
| RMB                  | 5   |
| INB                  | 227 |
| MB                   | 5   |

| Endpoint Number | State |
|-----------------|-------|
| 1               | IDL   |
| 2               | IDL   |
| 3               | IDL   |

Proceed to step [5](#)

- b Select **Post Carrier** from the **Maintenance Action** list, and click **Go**.

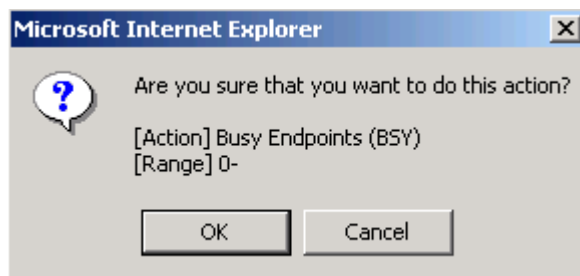
Following is an example the response with **Show Details** checked:

|                                                                                                                                                                        |       |                    |           |                           |          |                       |               |            |              |            |             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------------------|-----------|---------------------------|----------|-----------------------|---------------|------------|--------------|------------|-------------|
| Gateway Name:<br>PVG190                                                                                                                                                |       | Node Number:<br>13 |           | Filtered by State:<br>ALL |          | Endpoint Range:<br>0- |               |            |              |            |             |
| <div><div>Summary of Endpoints</div><div><div>Total Endpoints672</div><div>IDL289</div><div>UNKNOWN150</div><div>RMB5</div><div>INB223</div><div>MB5</div></div></div> |       |                    |           |                           |          |                       |               |            |              |            |             |
| Endpoint Number                                                                                                                                                        | State | Connected To       | Direction | Signaling                 | PM Type  | PM Number             | Endpoint Name | Trunk CLLI | Trunk Member | PM Carrier | PM TimeSlot |
| 1                                                                                                                                                                      | IDL   |                    | 2W        | S7 S7                     | GWC_NODE | 1                     | DS3_20.1.1    | POP0ITOG   | 1            | 0          | 1           |
| 2                                                                                                                                                                      | IDL   |                    | 2W        | S7 S7                     | GWC_NODE | 1                     | DS3_20.1.2    | POP0ITOG   | 2            | 0          | 1           |

Proceed to step [5](#)

- c Select **Busy Carrier (BSY)** from the **Maintenance Action** list, and click **Go**.

If you attempted to busy more than one carrier and the **Need Confirmation** check box is checked, you need to confirm the busy action as shown below.



If it is acceptable to busy more than one carrier, click **OK**.

Following is an example of the response:

Observe that the selected carriers are manual busy (MB).

|                          |  |                    |  |                          |  |                       |  |
|--------------------------|--|--------------------|--|--------------------------|--|-----------------------|--|
| Gateway Name:<br>PVG-190 |  | Node Number:<br>13 |  | Filtered by State:<br>MB |  | Endpoint Range:<br>0- |  |
|--------------------------|--|--------------------|--|--------------------------|--|-----------------------|--|

| Summary of Endpoints |     |
|----------------------|-----|
| Total Endpoints      | 672 |
| IDL                  | 289 |
| UNKNOWN              | 150 |
| RMB                  | 5   |
| INB                  | 223 |
| MB                   | 5   |

| Endpoint Number | State | Connected To | Direction | Signaling | PM Type  | PM Number | Endpoint Name | Trunk CLLI      | Trunk Member | PM Carrier | PM TimeSlo |
|-----------------|-------|--------------|-----------|-----------|----------|-----------|---------------|-----------------|--------------|------------|------------|
| 618             | MB    |              | 2W        | S7 S7     | GWC_NODE | 1         | DS3_20.26.18  | AL17IBNT2S7CGA0 | 2            | 0          | 1          |
| 619             | MB    |              | 2W        | S7 S7     | GWC_NODE | 1         | DS3_20.26.19  | AL17IBNT2S7CGA0 | 4            | 0          | 1          |
| 620             | MB    |              | 2W        | S7 S7     | GWC_NODE | 1         | DS3_20.26.20  | AL17IBNT2S7CGA0 | 6            | 0          | 1          |

Proceed to step [5](#)

- d Select **Return Carrier to Service (RTS)** from the **Maintenance Action** list, and click **Go**.

Following is an example of the response:

Observe that the selected carriers are idle (IDL).

Gateway Name:

PVG190

Node Number:

13

Filtered by State:

IDL

Endpoint Range:

0-

Summary of Endpoints

|                 |     |
|-----------------|-----|
| Total Endpoints | 672 |
| IDL             | 289 |
| UNKNOWN         | 150 |
| RMB             | 5   |
| INB             | 223 |
| MB              | 5   |

| Endpoint Number | State | Connected To | Direction | Signaling | PM Type  | PM Number | Endpoint Name | Trunk CLLI | Trunk Member | PM Carrier | PM TimeSlot |
|-----------------|-------|--------------|-----------|-----------|----------|-----------|---------------|------------|--------------|------------|-------------|
| 1               | IDL   |              | 2W        | S7 S7     | GWC_NODE | 1         | DS3_20.1.1    | POP0ITOG   | 1            | 0          | 1           |
| 2               | IDL   |              | 2W        | S7 S7     | GWC_NODE | 1         | DS3_20.1.2    | POP0ITOG   | 2            | 0          | 1           |
| 3               | IDL   |              | 2W        | S7 S7     | GWC_NODE | 1         | DS3_20.1.3    | POP0ITOG   | 3            | 0          | 1           |

Proceed to step [5](#)

- e Select **Force Release Carrier (FRLS)** from the **Maintenance Action** list, and click **Go**.

Following is an example of the response:

Observe that the selected carriers are manual busy (MB).

|                         |  |                    |  |                          |  |                       |  |
|-------------------------|--|--------------------|--|--------------------------|--|-----------------------|--|
| Gateway Name:<br>PVG190 |  | Node Number:<br>13 |  | Filtered by State:<br>MB |  | Endpoint Range:<br>0- |  |
|-------------------------|--|--------------------|--|--------------------------|--|-----------------------|--|

| Summary of Endpoints |     |
|----------------------|-----|
| Total Endpoints      | 672 |
| IDL                  | 289 |
| UNKNOWN              | 150 |
| RMB                  | 5   |
| INB                  | 223 |
| MB                   | 5   |

| Endpoint Number | State | Connected To | Direction | Signaling | PM Type  | PM Number | Endpoint Name | Trunk CLLI      | Trunk Member | PM Carrier | PM TimeSlot |
|-----------------|-------|--------------|-----------|-----------|----------|-----------|---------------|-----------------|--------------|------------|-------------|
| 618             | MB    |              | 2W        | S7 S7     | GWC_NODE | 1         | DS3_20.26.18  | AL17IBNT2S7CGA0 | 2            | 0          | 1           |
| 619             | MB    |              | 2W        | S7 S7     | GWC_NODE | 1         | DS3_20.26.19  | AL17IBNT2S7CGA0 | 4            | 0          | 1           |
| 620             | MB    |              | 2W        | S7 S7     | GWC_NODE | 1         | DS3_20.26.20  | AL17IBNT2S7CGA0 | 6            | 0          | 1           |

Proceed to step [5](#)

- f Select **Installation Busy Carrier (BSY INB)** from the **Maintenance Action** list, and click **Go**.

Following is an example of the response:

Observe that the selected carriers are installation busy (INB).

Gateway Name:

PVG190

Node Number:

13

Filtered by State:

INB

Endpoint Range:

0-

Summary of Endpoints

|                 |     |
|-----------------|-----|
| Total Endpoints | 672 |
| IDL             | 287 |
| UNKNOWN         | 150 |
| RMB             | 5   |
| CPB             | 2   |
| INB             | 223 |

| Endpoint Number | State | Connected To | Direction | Signaling | PM Type | PM Number | Endpoint Name | Trunk CLLI | Trunk Member | PM Carrier | PM TimeSlot |
|-----------------|-------|--------------|-----------|-----------|---------|-----------|---------------|------------|--------------|------------|-------------|
| 14              | INB   |              | 2W        | S7 S7     | GWCODE  | 1         | DS3_20.1.14   | PPATCOG    | 2            | 0          | 1           |
| 38              | INB   |              | 2W        | S7 S7     | GWCODE  | 1         | DS3_20.2.14   | PPEANTIC   | 2            | 0          | 1           |
| 149             | INB   |              | 2W        | S7 S7     | GWCODE  | 1         | DS3_20.7.5    | SAITTPVG   | 1            | 0          | 1           |

- 5 Use the following table to determine your next step.

| If you                                | Do                                |
|---------------------------------------|-----------------------------------|
| want to perform another action        | step <a href="#">4</a>            |
| do not want to perform another action | you have completed this procedure |

## Maintenance by Gateway Name

### At your workstation

- 1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#), if required.

### At the TMM GUI

- 2 Click **Maintenance By Gateway Name**.  
A window similar to the following, is displayed.

**Trunk Maintenance Manager**

**Maintenance Actions**

Gateway Name      Endpoint Range      Show When Querying, Show Details

No Gateway Selection      0-      ☐      All States

Maintenance Action:

Query Endpoint State

Go

**Maintenance Action**

- Maintenance By Gateway Name
- Maintenance By Carrier
- Get Trunk CLLIs by GW Name
- Maintenance By Trunk CLLI
- D-Channel Maintenance
- ICOT Test
- Properties**
- CM CLLI
- Auto-Refresh Rate
- ☐ Auto-Refresh
- ☒ Need Confirmation
- On-line Help
- Home

NORTEL NETWORKS

- 3 Enter the request criteria as follows:
  - a Select a gateway from the **Gateway Name** list.
  - b Optionally enter an endpoint range value, or use the default (0-) value to display all endpoints.
  - c Optionally click the **Show Details** check box if you want to display additional details about the endpoints, otherwise, only a summary of the endpoints will be displayed.
  - d Optionally select the state for the endpoints you want displayed, or use the default (All States) value to display endpoints in all states.

- 4 Use the following table to determine your next step.

| If you want to              | Do                          |
|-----------------------------|-----------------------------|
| Query endpoint state        | step <a href="#">a</a> only |
| Post endpoints              | step <a href="#">b</a> only |
| Busy endpoints              | step <a href="#">c</a> only |
| Return endpoints to service | step <a href="#">d</a> only |
| Force release endpoints     | step <a href="#">e</a> only |
| Installation busy endpoints | step <a href="#">f</a> only |

- a Select **Query Endpoint State** from the **Maintenance Action** list, and click **Go**.

Following is an example of the response with **Show Details** checked:

| Gateway Name:                                                                                                                                                     | Node Number: | Filtered by State: | Endpoint Range: |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|--------------------|-----------------|
| PVG190                                                                                                                                                            | 13           | ALL                | 0-              |
| <div> <div>Summary of Endpoints</div> <div>Total Endpoints 672</div> <div>STB 1</div> <div>INB 8</div> <div>CPB 6</div> <div>DMB 69</div> <div>INS 6</div> </div> |              |                    |                 |
| Endpoint Number                                                                                                                                                   | State        |                    |                 |
| 1                                                                                                                                                                 | IDL          |                    |                 |
| 2                                                                                                                                                                 | IDL          |                    |                 |
| 3                                                                                                                                                                 | IDL          |                    |                 |

Proceed to step [5](#)



- b Select **Post Endpoints** from the **Maintenance Action** list, and click **Go**.

Following is an example of the response with **Show Details** unchecked:

|                      |                     |                           |                        |
|----------------------|---------------------|---------------------------|------------------------|
| <b>Gateway Name:</b> | <b>Node Number:</b> | <b>Filtered by State:</b> | <b>Endpoint Range:</b> |
| PVG190               | 13                  | ALL                       | 0-                     |

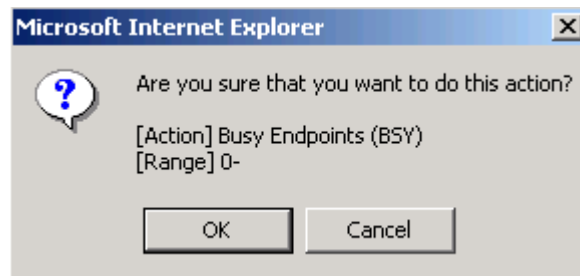
**Summary of Endpoints**  
Total Endpoints 672  
CFL 37  
IDL 377  
LO 12  
DMB 69  
UNKNOWN 172

Last Refreshed: Fri Sep 26 09:41:42 EDT 2003

Proceed to step [5](#)

- c Select **Busy Endpoints (BSY)** from the **Maintenance Action** list, and click **Go**.

If you attempted to busy more than one endpoint and the **Need Confirmation** check box is checked, you need to confirm the busy action as shown below.



If it is acceptable to busy more than one endpoint, click **OK**.

Following is an example of the response with **Show Details** checked:

Observe that the selected trunk endpoints are manual busy (MB).

|                                |                           |                                  |                               |
|--------------------------------|---------------------------|----------------------------------|-------------------------------|
| <b>Gateway Name:</b><br>PVG190 | <b>Node Number:</b><br>13 | <b>Filtered by State:</b><br>ALL | <b>Endpoint Range:</b><br>1-2 |
|--------------------------------|---------------------------|----------------------------------|-------------------------------|

**Summary of Endpoints**  
Total Endpoints 2  
MB 2

| Endpoint Number | State |
|-----------------|-------|
| 1               | ME    |
| 2               | ME    |

Last Refreshed: Fri Sep 26 09:54:53 EDT 2003

Proceed to step [5](#)

- d Select **Return Endpoints to Service (RTS)** from the **Maintenance Action** list, and click **Go**.

Following is an example of the response with **Show Details** checked:

Observe that the selected trunk endpoints are idle (IDL).

|               |              |                    |                 |
|---------------|--------------|--------------------|-----------------|
| Gateway Name: | Node Number: | Filtered by State: | Endpoint Range: |
| PVG190        | 13           | ALL                | 1-2             |

Summary of Endpoints

Total Endpoints 2

IDL 2

| Endpoint Number | State |
|-----------------|-------|
| 1               | IDL   |
| 2               | IDL   |

Last Refreshed: Fri Sep 26 10:04:35 EDT 2003

Proceed to step [5](#)

e

**CAUTION****Call loss**

If you force release trunk endpoints already involved in call processing, the endpoints will transition to manual busy (MB) and the calls in progress will be dropped.

Select **Force Release Endpoints (FRLS)** from the **Maintenance Action** list, and click **Go**.

Following is an example of the response with **Show Details** checked:

Observe that the selected trunk endpoints are manual busy (MB).

|                                |                           |                                  |                               |
|--------------------------------|---------------------------|----------------------------------|-------------------------------|
| <b>Gateway Name:</b><br>PVG190 | <b>Node Number:</b><br>13 | <b>Filtered by State:</b><br>ALL | <b>Endpoint Range:</b><br>1-2 |
|--------------------------------|---------------------------|----------------------------------|-------------------------------|

**Summary of Endpoints**  
Total Endpoints 2  
MB 2

| Endpoint Number | State |
|-----------------|-------|
| 1               | MB    |
| 2               | MB    |

Last Refreshed: Fri Sep 26 09:54:53 EDT 2003

Proceed to step [5](#)

- f Select **Installation Busy Endpoints (BSY INB)** from the **Maintenance Action** list, and click **Go**.

Following is an example of the response with **Show Details** checked:

Observe that the selected trunk endpoints are installation busy (INB).

|                                |                           |                                  |                               |
|--------------------------------|---------------------------|----------------------------------|-------------------------------|
| <b>Gateway Name:</b><br>PVG190 | <b>Node Number:</b><br>13 | <b>Filtered by State:</b><br>ALL | <b>Endpoint Range:</b><br>1-2 |
|--------------------------------|---------------------------|----------------------------------|-------------------------------|

**Summary of Endpoints**  
Total Endpoints 2  
INB 2

| Endpoint Number | State |
|-----------------|-------|
| 1               | INB   |
| 2               | INB   |

Last Refreshed: Fri Sep 26 10:12:56 EDT 2003

- 5 Use the following table to determine your next step.

| If you                                | Do                                |
|---------------------------------------|-----------------------------------|
| want to perform another action        | step <a href="#">4</a>            |
| do not want to perform another action | you have completed this procedure |

## Maintenance by trunk CLLI

### At your workstation

- 1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#), if required.

### At the TMM GUI

- 2 Click **Maintenance By Trunk CLLI**.

A window similar to the following, is displayed.

**Trunk Maintenance Manager**

**Maintenance Actions**

Trunk CLLI:

Trunk Range:

Maintenance Action:

**Maintenance Action**

- [Maintenance By Gateway Name](#)
- [Maintenance By Carrier](#)
- [Get Trunk CLLIs by GW Name](#)
- [Maintenance By Trunk CLLI](#)**
- [D-Channel Maintenance](#)
- [ICOT Test](#)

**Properties**

- [CM CLLI](#)
- [Auto-Refresh Rate](#)
- ☐ Auto-Refresh
- ☒ Need Confirmation
- [On-line Help](#)
- [Home](#)

NORTEL NETWORKS

- 3 Enter the request criteria as follows:
  - a Enter the trunk CLLI name under **Trunk CLLI**.
  - b Optionally enter a trunk range value, or use the default (0-) value to display all trunk members.

- 4 Use the following table to determine your next step.

| If you want to           | Do                          |
|--------------------------|-----------------------------|
| Post trunks              | step <a href="#">a</a> only |
| Busy trunks              | step <a href="#">b</a> only |
| Return trunks to service | step <a href="#">c</a> only |
| Force release trunks     | step <a href="#">d</a> only |
| Installation busy trunks | step <a href="#">e</a> only |

- a Select **Post Trunks** from the **Maintenance Action** list, and click **Go**.

Following is an example of the response:

|                  |                          |                    |                   |
|------------------|--------------------------|--------------------|-------------------|
| CM CLLI:<br>RTPS | Trunk CLLI:<br>P3D0IBNT2 | First Member:<br>1 | Group Size:<br>24 |
|------------------|--------------------------|--------------------|-------------------|

| Number | State | Connected To | Direction | Signaling | PM Type  | PM Number | Node # | Terminal # | Gateway Name | Endpoint Name          |
|--------|-------|--------------|-----------|-----------|----------|-----------|--------|------------|--------------|------------------------|
| 1      | IDL   |              | 2W        | S7 S7     | GWC_NODE | 1         | 13     | 1057       | PVG193       | STS/6/0/3/VT15/2/1/3/1 |
| 2      | IDL   |              | 2W        | S7 S7     | GWC_NODE | 1         | 13     | 1058       | PVG193       | STS/6/0/3/VT15/2/1/3/2 |
| 3      | IDL   |              | 2W        | S7 S7     | GWC_NODE | 1         | 13     | 1059       | PVG193       | STS/6/0/3/VT15/2/1/3/3 |
| 4      | IDL   |              | 2W        | S7 S7     | GWC_NODE | 1         | 13     | 1060       | PVG193       | STS/6/0/3/VT15/2/1/3/4 |
| 5      | IDL   |              | 2W        | S7 S7     | GWC_NODE | 1         | 13     | 1061       | PVG193       | STS/6/0/3/VT15/2/1/3/5 |
| 6      | IDL   |              | 2W        | S7 S7     | GWC_NODE | 1         | 13     | 1062       | PVG193       | STS/6/0/3/VT15/2/1/3/6 |
| 7      | IDL   |              | 2W        | S7 S7     | GWC_NODE | 1         | 13     | 1063       | PVG193       | STS/6/0/3/VT15/2/1/3/7 |
| 8      | IDL   |              | 2W        | S7 S7     | GWC_NODE | 1         | 13     | 1064       | PVG193       | STS/6/0/3/VT15/2/1/3/8 |
| 9      | IDL   |              | 2W        | S7 S7     | GWC_NODE | 1         | 13     | 1065       | PVG193       | STS/6/0/3/VT15/2/1/3/9 |

Proceed to step [5](#).

- b Select **Busy Trunks (BSY)** from the **Maintenance Action** list, and click **Go**.

If you attempted to busy more than one trunk member and the **Need Confirmation** check box is checked, you need to confirm the busy action as shown below.



If it is acceptable to busy more than one trunk member, click **OK**.

Following is an example of the response:

Observe that the selected range of trunk members are manual busy (MB).

| CM CLI: |       |              | Trunk CLI:  |           |          | First Member: |        |            | Group Size:  |               |  |
|---------|-------|--------------|-------------|-----------|----------|---------------|--------|------------|--------------|---------------|--|
| RTPS    |       |              | RTP5IBNT2OG |           |          | 1             |        |            | 4            |               |  |
| Number  | State | Connected To | Direction   | Signaling | PM Type  | PM Number     | Node # | Terminal # | Gateway Name | Endpoint Name |  |
| 1       | MB    |              | 2W          | S7 S7     | GWC_NODE | 1             | 13     | 365        | PVG190       | DS3/02/0/16/5 |  |
| 2       | MB    |              | 2W          | S7 S7     | GWC_NODE | 1             | 13     | 366        | PVG190       | DS3/02/0/16/6 |  |
| 3       | MB    |              | 2W          | S7 S7     | GWC_NODE | 1             | 13     | 367        | PVG190       | DS3/02/0/16/7 |  |
| 4       | MB    |              | 2W          | S7 S7     | GWC_NODE | 1             | 13     | 368        | PVG190       | DS3/02/0/16/8 |  |

Last Refreshed: Wed Sep 24 13:46:10 EDT 2003

Proceed to step [5](#).



- c Select **Return Trunks to Service (RTS)** from the **Maintenance Action** list, and click **Go**.

Following is an example of the response:

Observe that the selected trunk members are idle (IDL).

| CM CLLI: |  | Trunk CLLI: |  | First Member: |  | Group Size: |  |
|----------|--|-------------|--|---------------|--|-------------|--|
| RTPS     |  | AL7ITICS7   |  | 0             |  | 4           |  |

| Number | State | Connected To | Direction | Signaling | PM Type  | PM Number | Node # | Terminal # | Gateway Name | Endpoint Name |
|--------|-------|--------------|-----------|-----------|----------|-----------|--------|------------|--------------|---------------|
| 0      | IDL   |              | IC        | S7        | GWC_NODE | 1         | 13     | 627        | PVG190       | DS3/02/0/27/3 |
| 1      | IDL   |              | IC        | S7        | GWC_NODE | 1         | 13     | 628        | PVG190       | DS3/02/0/27/4 |
| 2      | IDL   |              | IC        | S7        | GWC_NODE | 1         | 13     | 629        | PVG190       | DS3/02/0/27/5 |
| 3      | IDL   |              | IC        | S7        | GWC_NODE | 1         | 13     | 630        | PVG190       | DS3/02/0/27/6 |

Last Refreshed: Wed Sep 24 13:42:27 EDT 2003

Proceed to step [5](#).

d

**CAUTION****Call loss**

If you force release a trunk already involved in call processing, the trunk will transition to manual busy (MB) and the calls in progress will be dropped.

Select **Force Release Trunks (FRLS)** from the **Maintenance Action** list, and click **Go**.

Following is an example of the response:

Observe that the selected range of trunk members are manual busy (MB).

**CM CLLI:**  
RTPS

**Trunk CLLI:**  
RTP5IBNT2OG

**First Member:**  
1

**Group Size:**  
4

| Member | State | Connected To | Direction | Signaling | PM Type  | PM Number | Node # | Terminal # | Gateway Name | Endpoint Name |
|--------|-------|--------------|-----------|-----------|----------|-----------|--------|------------|--------------|---------------|
| 1      | MB    |              | 2W        | S7 S7     | GWC_NODE | 1         | 13     | 365        | PVG190       | DS3/02/0/16/5 |
| 2      | MB    |              | 2W        | S7 S7     | GWC_NODE | 1         | 13     | 366        | PVG190       | DS3/02/0/16/6 |
| 3      | MB    |              | 2W        | S7 S7     | GWC_NODE | 1         | 13     | 367        | PVG190       | DS3/02/0/16/7 |
| 4      | MB    |              | 2W        | S7 S7     | GWC_NODE | 1         | 13     | 368        | PVG190       | DS3/02/0/16/8 |

Last Refreshed: Wed Sep 24 13:46:10 EDT 2003

Proceed to step [5](#).

- e Select **Installation Busy Trunks (BSY INB)** from the **Maintenance Action** list, and click **Go**.

Following is an example of the response:

Observe that the selected range of trunk members are installation busy (INB).

| CM CLLI: |  | Trunk CLLI: |  | First Member: |  | Group Size: |  |
|----------|--|-------------|--|---------------|--|-------------|--|
| COMPACT2 |  | KOUISUP26   |  | 121           |  | 24          |  |

| Number | State | Connected To | Direction | Signaling | PM Type  | PM Number | Node # | Terminal # | Gateway Name | Endpoint Name |
|--------|-------|--------------|-----------|-----------|----------|-----------|--------|------------|--------------|---------------|
| 121    | INB   |              | 2W        | S7 S7     | GWC_NODE | 1         | 15     | 1081       | PVG190       | DS3_22.6.1    |
| 122    | INB   |              | 2W        | S7 S7     | GWC_NODE | 1         | 15     | 1082       | PVG190       | DS3_22.6.2    |
| 123    | INB   |              | 2W        | S7 S7     | GWC_NODE | 1         | 15     | 1083       | PVG190       | DS3_22.6.3    |
| 124    | INB   |              | 2W        | S7 S7     | GWC_NODE | 1         | 15     | 1084       | PVG190       | DS3_22.6.4    |
| 125    | INB   |              | 2W        | S7 S7     | GWC_NODE | 1         | 15     | 1085       | PVG190       | DS3_22.6.5    |
| 126    | INB   |              | 2W        | S7 S7     | GWC_NODE | 1         | 15     | 1086       | PVG190       | DS3_22.6.6    |
| 127    | INB   |              | 2W        | S7 S7     | GWC_NODE | 1         | 15     | 1087       | PVG190       | DS3_22.6.7    |
| 128    | INB   |              | 2W        | S7 S7     | GWC_NODE | 1         | 15     | 1088       | PVG190       | DS3_22.6.8    |

- 5 Use the following table to determine your next step.

| If you                                | Do                                |
|---------------------------------------|-----------------------------------|
| want to perform another action        | step <a href="#">4</a>            |
| do not want to perform another action | you have completed this procedure |



---

## Posting PRI Group D-channels

---

### Application

Use this procedure to display statistics about the D-channels for a selected PRI trunk and perform maintenance operations.

This procedure can only be performed on Carrier Voice over IP PRI trunks.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### ***At your workstation***

- 1 Launch the Trunk Maintenance Manager (TMM) GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#).

#### ***At the TMM GUI***

- 2 Click **D-Channel Maintenance**.  
A window similar to the following, is displayed.

- 3 Enter the trunk CLLI name, then select **Post Group D-Channel** from the **Maintenance Action** drop down menu, and click **Go**.
- 4 Observe that the selected range of PRI trunk D-channel is displayed as shown in the following example.

CM CLLI:  
RTPS

Trunk CLLI:  
VSP3PRA250\_1

| Maint Operation    | State | Direction | Signaling | PM Type  | PM Number | Node # | Terminal # | Gateway Name | Endpoint Name |
|--------------------|-------|-----------|-----------|----------|-----------|--------|------------|--------------|---------------|
| Select Operation ▼ | INS   | 2W        | ISD ISD   | GWC_NODE | 1         | 13     | 744        | PVG193       | SS_6003_VT15_ |
| Select Operation ▼ | STB   | 2W        | ISD ISD   | GWC_NODE | 1         | 13     | 816        | PVG193       | SS_6003_VT15_ |

Last Refreshed: Fri Sep 26 10:34:30 EDT 2003

- 5 Select the desired maintenance operation as shown in the following example.

| CM CLI:          |       |           |           |          | Trunk CLI:   |        |            |              |                   |
|------------------|-------|-----------|-----------|----------|--------------|--------|------------|--------------|-------------------|
| RTPS             |       |           |           |          | VSP3PRA250_1 |        |            |              |                   |
| Maint Operation  | State | Direction | Signaling | PM Type  | PM Number    | Node # | Terminal # | Gateway Name | Endpoint Name     |
| Select Operation | INS   | 2W        | ISD ISD   | GWC_NODE | 1            | 13     | 744        | PVG193       | SS_6003_VT15_0113 |
| Select Operation | STB   | 2W        | ISD ISD   | GWC_NODE | 1            | 13     | 816        | PVG193       | SS_6003_VT15_0122 |
| Busy D-Channel   |       |           |           |          |              |        |            |              |                   |
| RTS D-Channel    |       |           |           |          |              |        |            |              |                   |
| INB D-Channel    |       |           |           |          |              |        |            |              |                   |

Last Refreshed: Fri Sep 26 10:34:30 EDT 2003

You have completed this procedure.





## Displaying trunk CLLI codes by gateway

### Action

Use this procedure to retrieve a list of trunk CLLI codes associated with a specific trunk gateway.

### Prerequisites

None

### Action

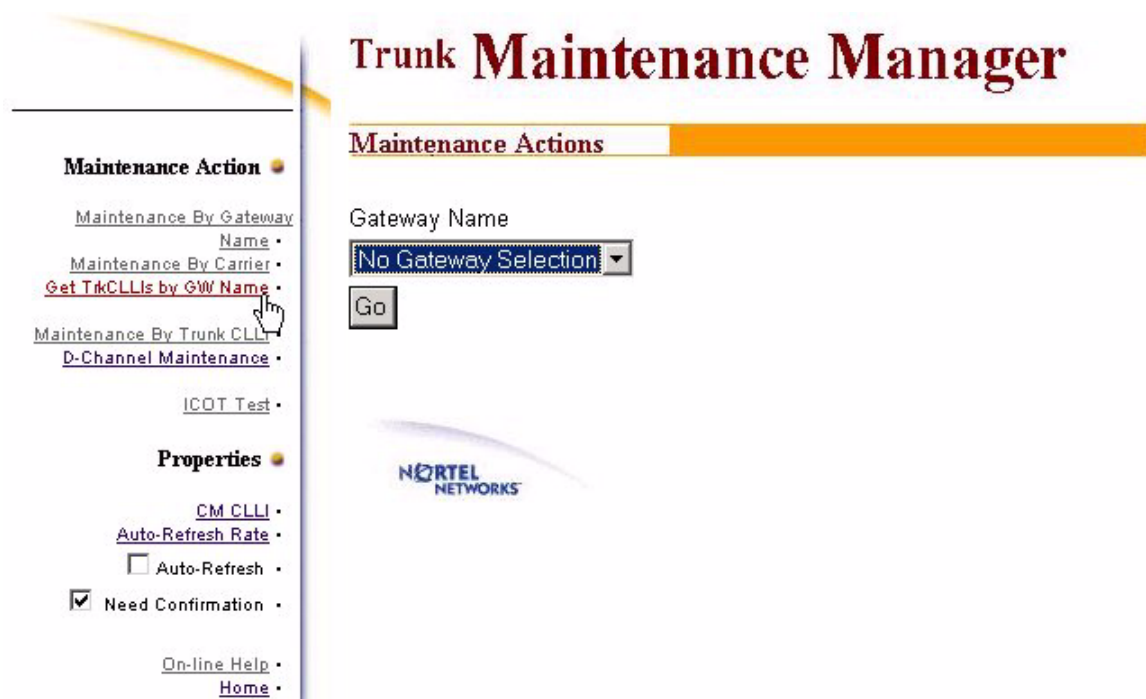
Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Launch the Trunk Maintenance Manager (TMM) GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#).

#### *At the TMM GUI*

- 2 Click **Get TrkCLLIs by GW Name**.  
A window similar to the following, is displayed.



- 3 From the **Gateway Name** list, select a gateway, then click **Go**.

The trunk CLLI codes associated with the trunk gateway are displayed as shown in the following example.

| Trunk Clli   |
|--------------|
| P0D0RTPQE911 |
| AL10ATCICS7  |
| S5EANTATCPVG |
| P0D0ITOGH    |
| P0D0ATCOG    |

Last Refreshed: Fri Sep 26 10:46:16 EDT 2003

You have completed this procedure.

---

## Performing an ISUP Continuity Test

---

### Application

Use this procedure to perform an ISUP (Integrated Services Digital Network User Part) continuity test (ICOT) on a single trunk member for a specific CLLI.

This test can only be performed on outgoing or 2-way ISUP trunks.

### Prerequisites

The trunk must be in a maintenance busy (MB) state. Refer to procedure [Performing trunk maintenance using the Trunk Maintenance Manager on page 1019](#) in this document, if required.

### Action

Perform the following steps to complete this procedure.

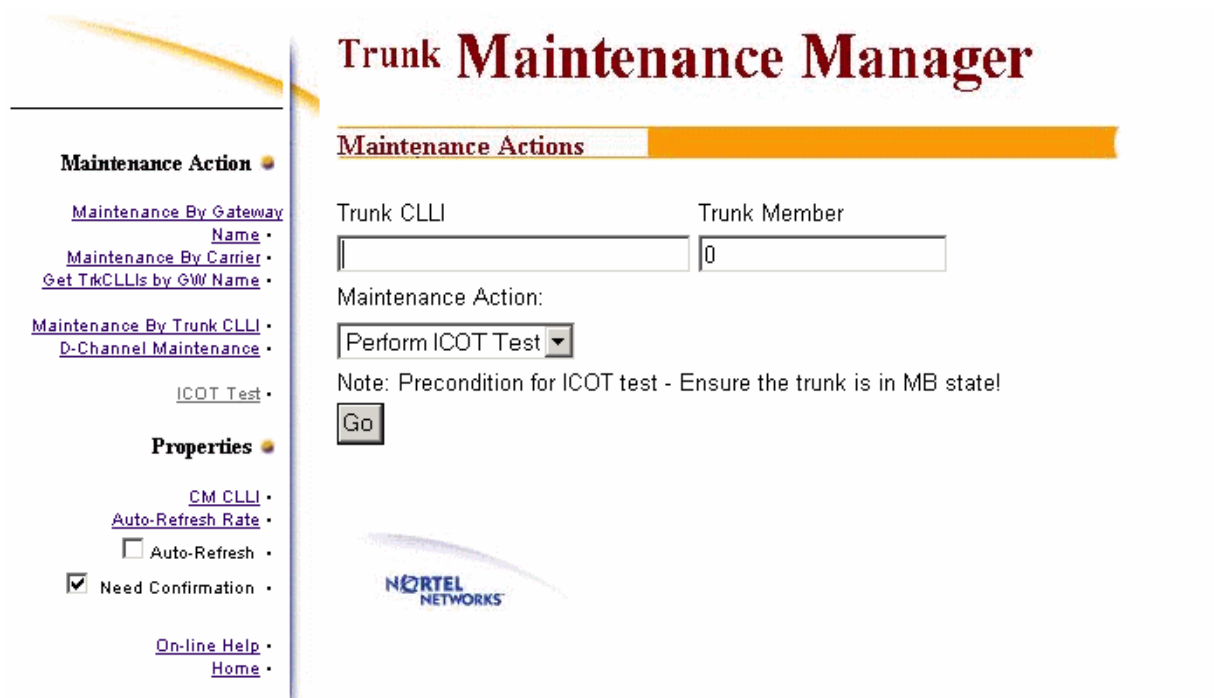
#### ***At your workstation***

- 1 Launch the Trunk Maintenance Manager (TMM) GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#).

#### ***At the TMM GUI***

- 2 Click **ICOT Test**.

A window similar to the following, is displayed.



## Trunk Maintenance Manager

### Maintenance Actions

Trunk CLLI      Trunk Member

Maintenance Action:

Note: Precondition for ICOT test - Ensure the trunk is in MB state!

**Maintenance Action**

- [Maintenance By Gateway Name](#)
- [Maintenance By Carrier](#)
- [Get Trunk CLLIs by GW Name](#)
- [Maintenance By Trunk CLLI](#)
- [D-Channel Maintenance](#)
- [ICOT Test](#)

**Properties**

- [CM CLLI](#)
- [Auto-Refresh Rate](#)
- ☐ Auto-Refresh
- ☒ Need Confirmation
- [On-line Help](#)
- [Home](#)

NORTEL NETWORKS

- 3 Enter the trunk CLLI name and member number.
- 4 Select **Perform ICOT Test** from the **Maintenance Action** list, and click **Go**.
- 5 Observe that the test results and continuity conditions for the trunk number are displayed as shown in the example below.  
If you encounter any unexpected errors such as “test failed”, review any details and determine a solution, or contact your next level of support.

| CM CLLI:<br>RTPS |             | Trunk CLLI:<br>POP0ITOG |                 |
|------------------|-------------|-------------------------|-----------------|
| Number           | Test Result | Continuity Condition    | Additional Info |
| 1                | TEST_PASSED |                         |                 |

You have completed this procedure.

---

## Routing customer logs to a remote host

---

### Application

Use this procedure to route customer logs to a remote host such as the core manager.

### Prerequisites

You must have the IP address of the remote host.

### Action

Perform the following steps to complete this procedure.

#### ***At your workstation***

- 1 Log in to the server by typing  
    > **telnet <IP address>**  
    and pressing the Enter key.  
    where  
        **IP address**  
        is the IP address of the SSPFS-based server where the  
        CS 2000 Management Tools reside
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  
    \$ **su -**  
    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 - exit

select -
```

- 6** Enter the number next to the “Configuration” option in the menu.

*Example response*

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 -

- 7** Enter the number next to the “Syslog Configuration” option in the menu.

*Example response*

Syslog Configuration

- 1 - list\_syslog (List a system's syslog configuration)
- 2 - add\_syslog (Add a syslog configuration entry)
- 3 - del\_syslog (Remove a syslog configuration entry)
- 4 - route\_syslog\_on (Route syslog to remote host)
- 5 - route\_syslog\_off (Turn off syslog re-direction to a remote host)

X - exit

select -

- 8** Enter the number next to the “route\_syslog\_on” option in the menu.
- 9** When prompted, enter the facility to be routed, for example, “local1.notice”.
- 10** When prompted, enter the IP address of the remote host.
- 11** Exit each menu level of the command line interface to eventually return to the command prompt, by typing

select - **x**

and pressing the Enter key.

You have completed this procedure.





---

## Configuring log reporting

---

### Application

Use this procedure to configure log reporting, which consists of configuring SESM syslog and SESM debug log, and enabling or disabling SESM syslog alarm logging.

**Note:** As of the SN07 release, the default northbound alarm feed is Corba notifications to the Integrated Element Management System (EMS). The SESM syslog alarm feed is disabled by default to avoid duplication of the alarm logs. Step [10](#) in this procedure allows you to enable or disable the SESM syslog alarm feed when required.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Telnet to the CS 2000 Management Tools server by typing  

```
> telnet <IP address>
```

and pressing the Enter key.  
where  
**IP address**  
is the IP address of the CS 2000 Management Tools 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 Change directory to where the configuration script is located by typing  

```
cd /opt/nortel/NTsesm/admin/bin
```

and pressing the Enter key.

**6** Execute the configuration script by typing

```
./configure
```

and pressing the Enter key.

*Example response*

```
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 -
```

**7** Enter the number next to the “SESM logging configuration” option in the menu.*Example response*

```
SESM Logging Configuration
```

- 1 - SESM Syslog configuration
- 2 - SESM Debug Log configuration
- 3 - SESM Alarm Logging configuration
- 4 - SESM Alarm GUI configuration

```
X - exit
```

```
select -
```

**8** Configure syslog as follows:

- a** Enter the number next to the “SESM Syslog configuration” option in the menu.
- b** When prompted, enter the maximum file size (in megabytes) of SESM Syslog, or press the Enter key to accept the default value of “3 meg”.
- c** When prompted, enter the SESM Syslog Backup Hour (for daily file rotation, or press the Enter key to accept the default value of “3” hours.

- d When prompted, enter the SESM Syslog Backup Minute, or press the Enter key to accept the default value of “0” minutes.  
The system sets the values you selected and returns you to the SESM Logging Configuration menu.
- 9 Configure debug log as follows:
  - a Enter the number next to the “SESM Debug Log configuration” option in the menu.
  - b When prompted, enter the maximum file size of SESM Debug Log, or press the Enter key to accept the default value of “20560 KB”.
  - c When prompted, enter the maximum number of SESM Debug Log files, or press the Enter key to accept the default value of “7”.
  - d When prompted, enter the MI2 default log level, or press the Enter key to accept the default value of “MNR”.
  - e When prompted, enter the Proxy Agent default log level, or press the Enter key to accept the default value of “CRT”.
  - f When prompted, enter the SESM log file name, or press the Enter key to accept the default value of “ptmdebuglog”.
  - g When prompted, enter the log file rotation method, or press the Enter key to accept the default value of “Size based”.  
The system sets the values you selected and returns you to the SESM Logging Configuration menu.
- 10 Enable or disable syslog alarm logging as follows:
  - a Enter the number next to the “SESM Alarm Logging configuration” option in the menu.
  - b When prompted, enter Y if you want to enable syslog alarm logging, or N if you want to disable syslog alarm logging.  
The system returns you to the SESM Logging Configuration menu.
- 11 Exit SESM Logging Configuration by typing  
`select - x`  
and pressing the Enter key.
- 12 Exit SESM configuration by typing  
`select - x`  
and pressing the Enter key.
- 13 You have completed this procedure.



---

## Viewing debug logs

---

### Application

Use this procedure to view debug logs.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Telnet to the CS 2000 Management Tools server by typing  
`> telnet <IP address>`  
and pressing the Enter key.  
where  
**IP address**  
is the IP address of the CS 2000 Management Tools 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 Display the debug logs by typing  
`# ptmctl display <log_type>`  
and pressing the Enter key.  
where  
**log\_type**  
is MI2, PA, or MISC
- 6 You have completed this procedure.



## Viewing OMPUSH logs

### Application

Use this procedure to view OMPUSH logs.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Telnet to the Sun server by typing  

```
> telnet <IP address>
```

and pressing the Enter key.  
where  
**IP address**  
is the IP address of the Sun server where OMPUSH resides
- 2 When prompted, enter your user ID and password.
- 3 Use the following table to determine your next step.

| If you want to                             | Do                     |
|--------------------------------------------|------------------------|
| monitor the OMPUSH syslog stream           | step <a href="#">a</a> |
| view the OMPUSH history log file           | step <a href="#">b</a> |
| save the OMPUSH history log file to a file | step <a href="#">c</a> |

- a Monitor the OMPUSH syslog stream by typing  

```
tail -f /var/adm/messages |grep -i ompush
```

and pressing the Enter key.
- b View the OMPUSH history log file by typing  

```
cat /var/adm/messages |grep -i ompush
```

and pressing the Enter key.

- c Save the OMPUSH history log file to a file by typing

```
cat /var/adm/messages |grep -i ompush >
<filename>
```

and pressing the Enter key.

Where

**filename**

is the name you want to give to the OMPUSH history log file you are saving

- 4 You have completed this procedure.



---

## Viewing customer logs on an SSPFS-based server

---

### Application

Use this procedure to view customer logs for the following components:

- Succession Element and Sub-element Manager (SESM)
- Gateway Controller (GWC)
- Media Gateway 9000 (MG 9000)
- Succession Server Platform Foundation Software (SSPFS)

Customer logs reside in directory /var/log on the server. For details on customer logs, refer to the Carrier Voice over IP Fault Management Log Reference document, NN10275-909.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Telnet to the server by typing  

```
> telnet <IP address>
```

  
and pressing the Enter key.  
where  
**IP address**  
is the IP address of the SSPFS-based server
- 2 When prompted, enter your user ID and password.
- 3 Access the directory where the customer log files reside by typing  

```
$ cd /var/log
```

  
and pressing the Enter key.
- 4 List the directory content by typing  

```
$ ls
```

  
and pressing the Enter key.

The customer log files are appended with numbers, for example "customerlog.0". The files with the lower numbers are the newer files.

- 5 Use the following table to determine your next step.

| If you want to                        | Do                             |
|---------------------------------------|--------------------------------|
| view the entire content of a log file | substep <a href="#">a</a> only |
| view specific content of a log file   | substep <a href="#">b</a> only |

- a** View the entire content of a log file by typing

```
$ cat <log_filename> |more
```

and pressing the Enter key.

*where*

**log\_filename**

is the name of the customer log file you want to view.

**Example**

```
$ cat customerlog.0 |more
```

- b** View specific content of the log file by typing

```
cat <log_filename> |grep <search_string>
```

and pressing the Enter key.

*where*

**search\_string**

is the text you want to search for.

**Example**

```
$ cat customerlog.0 |grep SPFS350
```

- 6 To print the contents of this file, contact your site system administrator for assistance with using UNIX print commands and with locating a printer connected to your network.
- 7 You have completed this procedure.

---

## Disabling local logging of SSPFS platform faults

---

### Application

Use this procedure to disable local logging of the Succession Server Platform Foundation Software (SSPFS) platform alarm logs. Local logging is enabled by default and when enabled, the SSPFS platform alarm logs are sent over both the syslog (custlog) and SNMP (alarmd) interfaces to the Integrated Element Management System (IEMS) causing duplication of alarm logs. To avoid this duplication, disable local logging.

### Prerequisites

You must have root user privileges.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Log in to the server by typing  
    `> telnet <IP address>`  
and pressing the Enter key.  
where  
    **IP address**  
    is the IP address or host name of the SSPFS-based server  
    you want to query
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  
    `$ su -`  
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 - exit

select -

**6** Enter the number next to the “Configuration” option in the menu.*Example response*

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 -

- 7** Enter the number next to the “Succession Element Configuration” option in the menu.

*Example response:*

```
Succession Element Configuration
1 - SESM Application Configuration
2 - SAM21EM Application Configuration
3 - NPM Application Configuration
4 - DDMSProxy Application Configuration
5 - OMPUSH Application Configuration
6 - PSE Application Configuration
7 - RESMON Application Configuration
```

```
X - exit
```

```
select -
```

- 8** Enter the number next to the “RESMON Application Configuration” option in the menu.

*Example response*

```
RESMON Application Configuration
1 - settrapdest (Set location for IEMS traps)
2 - queryFaults (Query all faults on the box)
3 - enableLocalLogs (Enable Local Logging Of
 Faults)
4 - disableLocalLogs (Disable Local Logging Of
 Faults)
```

```
X - exit
```

```
select -
```

- 9** Enter the number next to the “DisableLocalLogs” option in the menu.

*Example response*

```
===Executing "DisableLocalLogs"
```

```
=== "DisableLocalLogs" completed successfully
```

```
RESMON Application Configuration
```

- 1 - settrapdest (Set location for IEMS traps)
- 2 - queryFaults (Query all faults on the box)
- 3 - enableLocalLogs (Enable Local Logging Of Faults)
- 4 - disableLocalLogs (Disable Local Logging Of Faults)

```
X - exit
```

```
select -
```

- 10** Exit each menu level of the command line interface to eventually return to the command prompt, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

---

## Replacing one or more failed disk drives on an SSPFS-based server

---

### Application

Use this procedure to replace one or more failed disk drives on a Succession Server Platform Foundation Software (SSPFS)-based server (a Netra t1400 or a Netra 240 server). Also use this procedure if a disk drive was pulled out by mistake. Simply re-inserting the disk is not sufficient to recover.

Disk failures will appear as IO errors or SCSI errors from the Solaris kernel. These messages will appear in the system log and on the console terminal. To indicate a disk failure, log SPFS310 is generated, and an alarm light is illuminated on the front panel. After the disk is replaced, the alarm light will go off within a few minutes.

Systems installed with SSPFS use disk mirroring. With mirrored hot-swap disks, a single failed disk can be replaced without interrupting the applications running on the server. Thus, a single disk can be replaced while the system is in-service. Follow one of the links below for a view of the disks on a Netra t1400 and Netra 240:

- [Netra t1400 on page 1068](#)
- [Netra 240 on page 1069](#)

The steps to replace a failed drive are to identify the failed drive, replace it physically, and replace it logically.

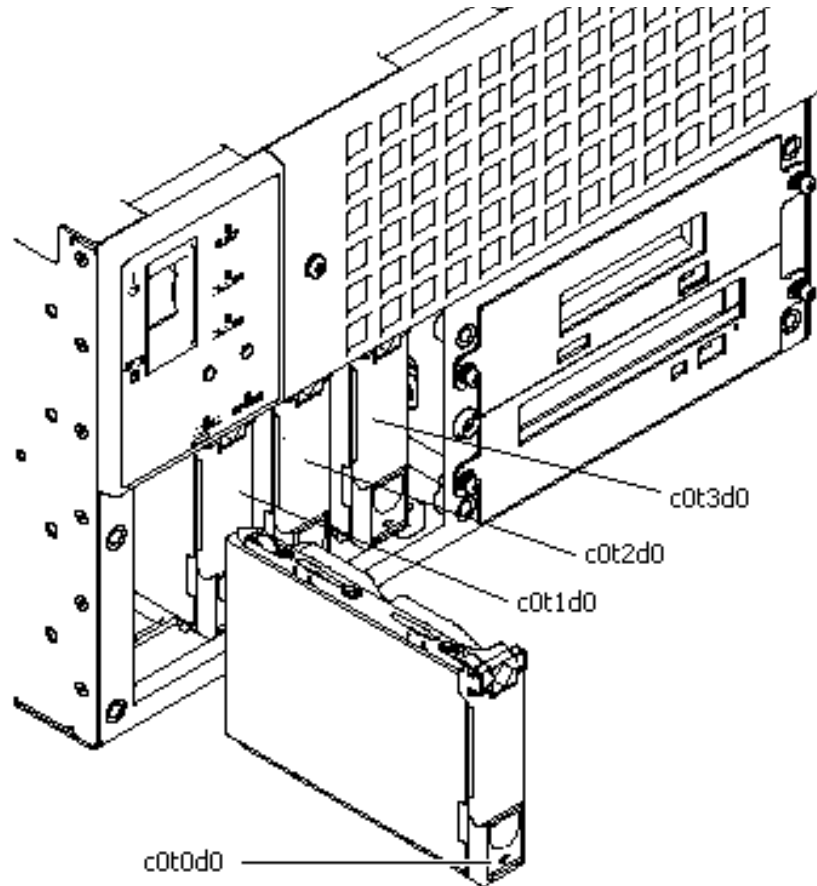
Follow one of the links below according to your office configuration to replace the failed disk drives:

- [Replacing failed disks on a Netra t1400 on page 1070](#)
- [Replacing failed disks on a Netra 240 simplex on page 1073](#)
- [Replacing failed disks on a Netra 240 cluster \(two-server\) on page 1075](#)

**Netra t1400**

Each Netra t1400 is equipped with four hot-swap drives: “c0t0d0”, “c0t1d0”, “c0t2d0”, and “c0t3d0”. Each physical drive is divided into slices, which are named based on the physical disk and a slice number. For example, “c0t0d0s0” is the first slice of the physical disk “c0t0d0”.

The following figure identifies the disk drives of the Netra t1400.

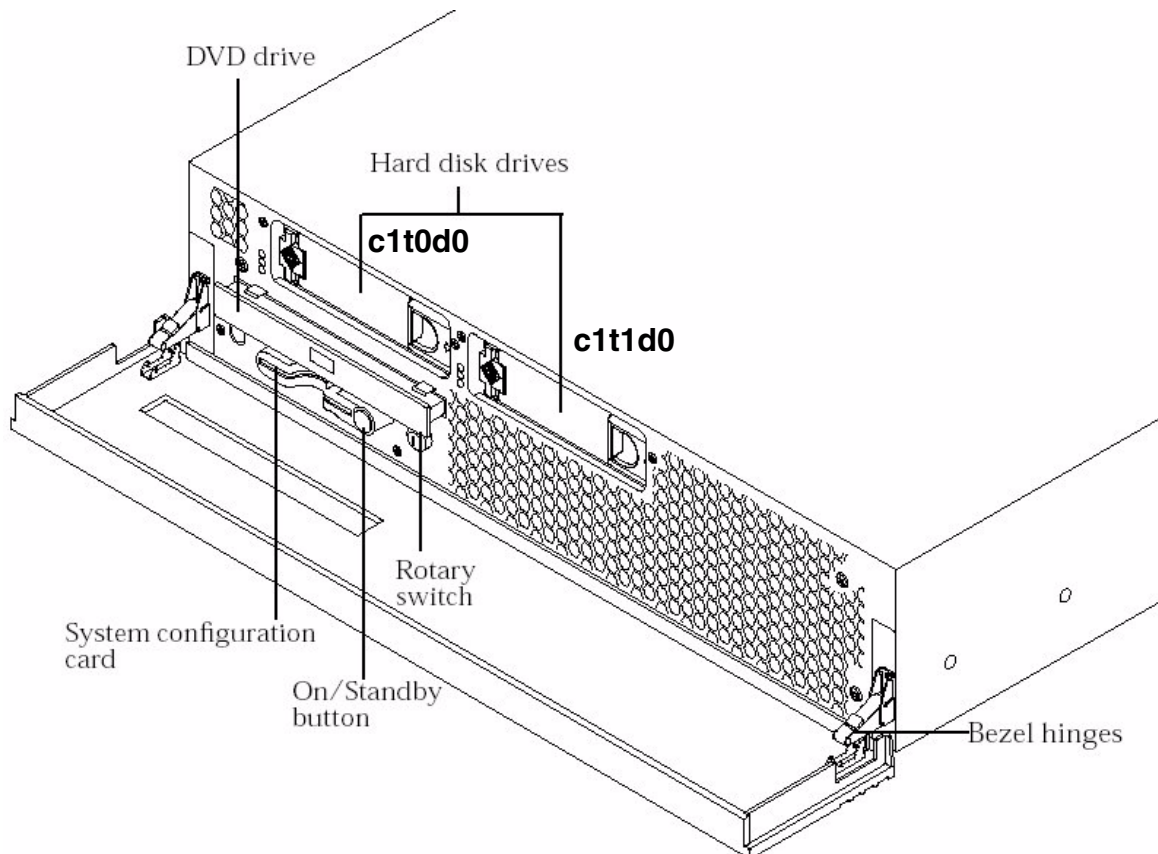
**Netra t1400 disk drives**



**Netra 240**

Each Netra 240 is equipped with two hot-swap drives: “c1t0d0”, and “c1t1d0”.

The following figure identifies the disk drives of the Netra 240.

**Netra 240 disk drives****Prerequisites**

You have a replacement disk.

## Action

Perform the following steps to complete this procedure.

### Replacing failed disks on a Netra t1400

#### *At the server*

- 1 Locate the failed disk(s) using figure [Netra t1400 disk drives on page 1068](#).
- 2 Physically replace the disk using the documentation for the Netra t1400. When complete, proceed with step [3](#) in this procedure to logically replace the disk.

**Note:** If more than one disk needs to be replaced, physically replace one disk and return to this procedure to logically replace the disk (step [3](#)), before you proceed to physically replace the next failed disk.

#### *At your workstation*

- 3 Logically replace the disk you just physically replaced.

| If you physically replaced | Do                     |
|----------------------------|------------------------|
| c0t0d0                     | step <a href="#">a</a> |
| c0t1d0                     | step <a href="#">b</a> |
| c0t2d0                     | step <a href="#">c</a> |
| c0t3d0                     | step <a href="#">d</a> |

- a** Logically replace disk “c0t0d0” by entering the following sequence of commands:

```
metadb -d c0t0d0s7
prtvtoc -h /dev/rdisk/c0t1d0s2 | fmthard -s
- /dev/rdisk/c0t0d0s2
metadb -a c0t0d0s7
metareplace -e d2 c0t0d0s1
metareplace -e d5 c0t0d0s0
metareplace -e d8 c0t0d0s3
metareplace -e d11 c0t0d0s4
metareplace -e d100 c0t0d0s5
```

Proceed to step [4](#)

- b** Logically replace disk “c0t1d0” by entering the following sequence of commands.

```
metadb -d c0t1d0s7
prtvtoc -h /dev/rdisk/c0t0d0s2 | fmthard -s
- /dev/rdisk/c0t1d0s2
metadb -a c0t1d0s7
metareplace -e d2 c0t1d0s1
metareplace -e d5 c0t1d0s0
metareplace -e d8 c0t1d0s3
metareplace -e d11 c0t1d0s4
metareplace -e d100 c0t1d0s5
```

Proceed to step [4](#)

- c** Logically replace disk “c0t2d0” by entering the following sequence of commands.

```
metadb -d c0t2d0s7
prtvtoc -h /dev/rdisk/c0t3d0s2 | fmthard -s
- /dev/rdisk/c0t2d0s2
metadb -a c0t2d0s7
metareplace -e d100 c0t2d0s0
```

Proceed to step [4](#)

- d Logically replace disk “c0t3d0” by entering the following sequence of commands.

```
metadb -d c0t3d0s7
prtvtoc -h /dev/rdisk/c0t2d0s2 | fmthard -s
- /dev/rdisk/c0t3d0s2
metadb -a c0t3d0s7
metareplace -e d100 c0t3d0s0
```

Proceed to step [4](#)

- 4 Use the following table to determine your next step.

| If you                                         | Do                     |
|------------------------------------------------|------------------------|
| have another disk to physically replace        | step <a href="#">1</a> |
| do not have another disk to physically replace | step <a href="#">5</a> |

- 5 Use the following table to determine your next step.

| If you replaced                                                                         | Do                                |
|-----------------------------------------------------------------------------------------|-----------------------------------|
| 1 disk                                                                                  | you have completed this procedure |
| 2 non-mirrored disks (i.e. c0t0d0 and c0t2d0 or c0t3d0, or c0t1d0 and c0t2d0 or c0t3d0) | you have completed this procedure |
| 2 mirrored disks (i.e. c0t0d0 and c0t1d0, or c0t2d0 and c0t3d0)                         | step <a href="#">6</a>            |
| 3 disks                                                                                 | step <a href="#">6</a>            |
| 4 disks                                                                                 | step <a href="#">6</a>            |

- 6 Restore the file systems and oracle data. If required, refer to procedure “Performing a full system restore on a Sun server - SN06.2 or greater” in the ATM/IP Security and Administration document, NN10402-600.

**Note:** As long as one disk from each pair is good, the data in the system is intact. When both disks in a pair fail, the data needs to be restored.

You have completed this procedure.

## Replacing failed disks on a Netra 240 simplex

### At the server

- 1 Locate the failed disk(s) using figure [Netra 240 disk drives on page 1069](#).
- 2 Physically replace the disk using the documentation for the Netra 240. When complete, proceed with step [3](#) in this procedure to logically replace the disk.

**Note:** If both disks need to be replaced, physically replace one disk and return to this procedure to logically replace the disk (step [3](#)), before you proceed to physically replace the other failed disk.

### At your workstation

- 3 Logically replace the disk you just physically replaced.

| If you physically replaced | Do                     |
|----------------------------|------------------------|
| c1t0d0                     | step <a href="#">a</a> |
| c1t1d0                     | step <a href="#">b</a> |

- a Logically replace disk “c1t0d0” by entering the following sequence of commands:

```
metadb -d c1t0d0s7
prtvtoc -h /dev/rdisk/c1t1d0s2 | fmthard -s
- /dev/rdisk/c1t0d0s2
metadb -a c1t0d0s7
metareplace -e d2 c1t0d0s1
metareplace -e d5 c1t0d0s0
metareplace -e d8 c1t0d0s3
metareplace -e d11 c1t0d0s4
metareplace -e d100 c1t0d0s5
```

Proceed to step [4](#)

- b Logically replace disk “c1t1d0” by entering the following sequence of commands:

```
metadb -d c1t1d0s7
prtvtoc -h /dev/rdisk/c1t0d0s2 | fmthard -s
- /dev/rdisk/c1t1d0s2
metadb -a c1t1d0s7
metareplace -e d2 c1t1d0s1
metareplace -e d5 c1t1d0s0
metareplace -e d8 c1t1d0s3
metareplace -e d11 c1t1d0s4
metareplace -e d100 c1t1d0s5
```

Proceed to step [4](#)

- 4 Use the following table to determine your next step.

| If you                              | Do                     |
|-------------------------------------|------------------------|
| have another disk to replace        | step <a href="#">1</a> |
| do not have another disk to replace | step <a href="#">5</a> |

- 5 Use the following table to determine your next step.

| If you replaced | Do                                |
|-----------------|-----------------------------------|
| 1 disk          | you have completed this procedure |
| both disks      | step <a href="#">6</a>            |

- 6 Restore the file systems and oracle data. If required, refer to procedure “Performing a full system restore on a Sun server - SN06.2 or greater” in the ATM/IP Security and Administration document, NN10402-600.

**Note:** As long as one disk is good, the data in the system is intact. When both disks fail, the data needs to be restored.

You have completed this procedure.

## Replacing failed disks on a Netra 240 cluster (two-server)

### *At the server*

- 1 Locate the failed disk(s) using figure [Netra 240 disk drives on page 1069](#).
- 2 Use the following guidelines to determine the steps you need to do, and do only those steps in the order they appear:
  - **to replace one disk on one unit**
    - physically replace the disk (step [3](#))
    - logically replace this disk (step [4](#))
  - **to replace one disk on each unit**
    - physically replace the disk on the Active unit first (step [3](#))
    - logically replace this disk (step [4](#))
    - physically replace the disk on the other unit (step [3](#))
    - logically replace this disk (step [4](#))
  - **to replace both disks on a unit**
    - physically replace one disk on the unit (step [3](#))
    - logically replace this disk (step [4](#))
    - physically replace the other disk on this unit (step [3](#))
    - logically replace this disk (step [4](#))
    - clone the image from the Active unit onto this unit (step [6](#))
  - **to replace three disks**
    - physically replace the disk on the Active unit first (step [3](#))
    - logically replace this disk (step [4](#))
    - physically replace one disk on the other unit (step [3](#))
    - logically replace this disk (step [4](#))
    - physically replace the other disk on this same unit (step [3](#))
    - logically replace this disk (step [4](#))
    - clone the image from the Active unit onto this unit (step [6](#))

- **to replace four disks**
    - physically replace one disk on the unit with the most recent backup (step [3](#))
    - logically replace this disk (step [4](#))
    - physically replace the other disk on this same unit (step [3](#))
    - logically replace this disk (step [4](#))
    - restore the file systems and oracle data on this unit (step [5](#))
    - physically replace one disk on the other unit (step [3](#))
    - logically replace this disk (step [4](#))
    - physically replace the other disk on this same unit (step [3](#))
    - logically replace this disk (step [4](#))
    - clone the image from the Active unit onto this unit (step [6](#))
- 3** Physically replace the disk using the documentation for the Netra 240. When complete, proceed with step [4](#) in this procedure to logically replace the disk.

***At your workstation***

- 4** Logically replace the disk you just physically replaced.

| If you physically replaced | Do                     |
|----------------------------|------------------------|
| c1t0d0                     | step <a href="#">a</a> |
| c1t1d0                     | step <a href="#">b</a> |



- a Logically replace disk “c1t0d0” by entering the following sequence of commands:

```
metadb -d c1t0d0s7
prtvtoc -h /dev/rdisk/c1t1d0s2 | fmthard -s
- /dev/rdisk/c1t0d0s2
metadb -a c1t0d0s7
metareplace -e d2 c1t0d0s1
metareplace -e d5 c1t0d0s0
metareplace -e d8 c1t0d0s3
metareplace -e d11 c1t0d0s4
metareplace -e d100 c1t0d0s5
```

- b Logically replace disk “c1t1d0” by entering the following sequence of commands:

```
metadb -d c1t1d0s7
prtvtoc -h /dev/rdisk/c1t0d0s2 | fmthard -s
- /dev/rdisk/c1t1d0s2
metadb -a c1t1d0s7
metareplace -e d2 c1t1d0s1
metareplace -e d5 c1t1d0s0
metareplace -e d8 c1t1d0s3
metareplace -e d11 c1t1d0s4
metareplace -e d100 c1t1d0s5
```

- 5 Restore the file systems and oracle data. If required, refer to procedure “Performing a full system restore on a Sun server - SN06.2 or greater” in the ATM/IP Security and Administration document, NN10402-600.

**Note:** As long as one disk is good, the data in the system is intact. When both disks fail, the data needs to be restored.

- 6 Clone the data from the Active unit. If required, refer to procedure “Cloning the image of one node in a cluster to the other node” in the ATM/IP Security and Administration document, NN10402-600.

You have completed this procedure.



## Replacing a DVD drive on an SSPFS-based server

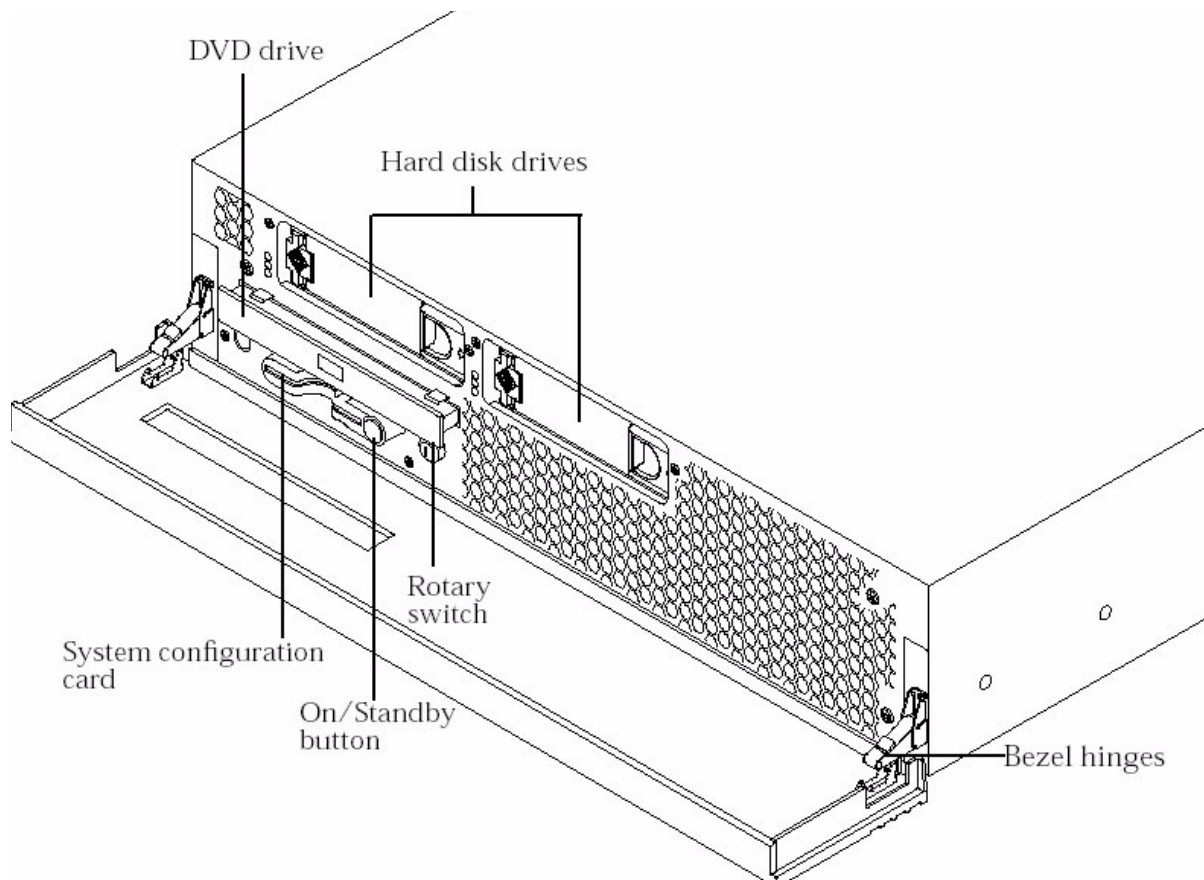
### Application

Use this procedure to replace a DVD drive on a Netra 240 server. This procedure applies to simplex and high-availability (HA) systems. An HA system refers to a Sun Netra 240 server pair.

#### ATTENTION

The DVD drive is not hot-swappable. The server must be powered down. Therefore, ensure the server can be powered down before you proceed with the procedure.

The following figure shows the location of the DVD drive on the Netra 240.



Use one of the methods below according to your office configuration:

- [Simplex configuration \(one server\)](#)
- [High-availability configuration \(two servers\)](#)

## Prerequisites

None.

## Action

### Simplex configuration (one server)

#### *At your workstation*

- 1 Power down the server. Refer to procedure [Shutting down an SSPFS-based server on page 1115](#) if required.
- 2 Physically replace the DVD drive using the Sun documentation for the Netra 240.
- 3 Once the new DVD drive is in place, restore power to the server by turning on the power at the circuit breaker panel of the frame. The server recovers on its own once power is restored.
- 4 You have completed this procedure.

### High-availability configuration (two servers)

#### *At your workstation*

- 1 Use the following table to determine your first step.

| If you are replacing the DVD drive on the | Do                     |
|-------------------------------------------|------------------------|
| active server                             | step <a href="#">2</a> |
| inactive server                           | step <a href="#">3</a> |

- 2 Initiate a manual failover. Refer to procedure [Initiating a manual failover on a Sun Netra 240 server pair on page 1107](#) if required.
- 3 Once the active server acquires the status of standby (inactive), power down the server. Refer to procedure [Shutting down an SSPFS-based server on page 1115](#) if required.
- 4 Physically replace the DVD drive using the Sun documentation for the Netra 240.
- 5 Once the new DVD drive is in place, restore power to the server by turning on the power at the circuit breaker panel of the frame. The server recovers on its own once power is restored.

**6** You have completed this procedure.



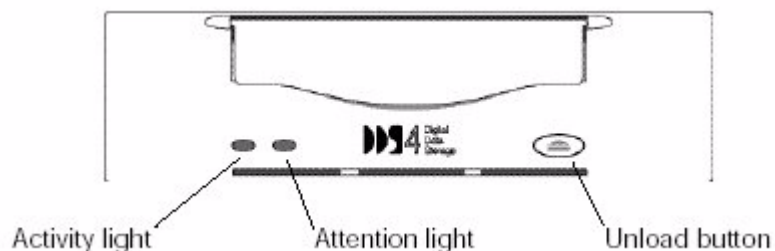
## Cleaning the DAT drive on the Netra T1400

### Application

Use this procedure to clean the digital audio tape (DAT) drive on the Netra T1400.

The DAT drive has an Activity light and an Attention light on the front panel as shown below.

#### DAT drive



The Activity light flashes green to show activity (loading, unloading, reading, and writing). It is a steady green when a tape is loaded and the DAT drive is ready to begin operations.

The Attention light flashes amber to indicate that a tape is near the end of its life, or that the DAT drive needs cleaning. It is a steady amber when there is a hardware fault.

When the Attention light flashes amber, clean the DAT drive as described in this procedure.

### Schedule

The table below provides the recommended cleaning interval.

| Number of tapes used each day | Cleaning interval |
|-------------------------------|-------------------|
| 1 or less                     | 8 weeks           |
| 2                             | 4 weeks           |
| 3                             | 3 weeks           |
| 4 or more                     | weekly            |

To clean the DAT drive, use an appropriate DAT drive cleaning tape. Nortel recommends the Maxell cleaning tape (HS-4/CL or equivalent). Refer to the documentation that accompanies the cleaning tape for additional information about its use, and the life expectancy of the cleaning tape.

## Prerequisites

None

## Action

Perform the following steps to complete this procedure

### ***At the front of the Netra T1400***

- 1 Obtain a cleaning tape (Maxell HS-4/CL or equivalent).
- 2 If a tape is already in the DAT drive, press the Unload button on the DAT drive to eject the tape.
- 3 Insert the cleaning tape into the DAT drive. Cleaning begins automatically. When cleaning is complete, the tape is automatically ejected.  
  
**Note:** The Attention light should go off. If the Attention light is still flashing amber after cleaning the DAT drive. Repeat the operation with a different cleaning tape.
- 4 Remove the cleaning tape from the DAT drive.
- 5 If you removed a tape in step 2, reinsert the tape. If the Attention light flashes amber, the tape is nearing the end of its life. Copy the data onto a new tape and discard the old one.
- 6 You have completed this procedure.



## Re-establishing the connection between the NPM GUI and the server

### Application

Use this procedure to re-establish the connection between the Network Patch Manager (NPM) GUI and the Sun server where the Network Patch Manager (NPM) software resides. The NPM GUI loses server connectivity when the server goes out of service. Once the server returns to service you need to reconnect.

### Prerequisites

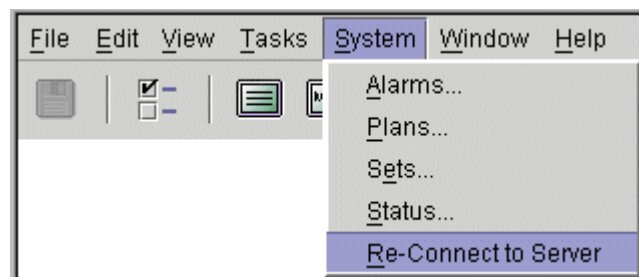
The server where the NPM software resides must be in service.

### Action

Perform the following steps to complete this procedure.

#### *At the NPM GUI*

- 1 On the **System** menu, click **Re-Connect to Server**.



When the connection is successful, a response similar to the one below is displayed.



When the connection fails, a response similar to the one below is displayed.



When the connection fails, try to reconnect at a later time. If the connection failure persists, contact your next level of support.

- 2 You have completed this procedure.

---

## Restoring SSH communication between the CS 2000 Management Tools server and the core manager

---

### Application

Use this procedure to re-establish SSH communication between the CS 2000 Management Tools server and the core manager if either one undergoes a fresh install after the CS 2000 SAM21 Manager has been migrated from the core manager to the CS 2000 Management Tools server.

### Prerequisites

None

### Action

Perform the steps in one of the following procedures depending on which platform underwent a fresh install:

- [Re-establishing SSH communication after a core manager fresh install on page 1087](#)
- [Re-establishing SSH communication after an SSPFS fresh install on page 1090](#)

#### Re-establishing SSH communication after a core manager fresh install

##### *At the SDM*

- 1 Log in to the core manager.
- 2 Access the SWIM level of the maintenance interface by typing  
`# sdmmtc swim`  
and pressing the Enter key.
- 3 Access the Details level by typing  
`> details`  
and pressing the Enter key.
- 4 Ensure the following filesets are applied.
  - OpenSSH
  - Bootp Loading Service

**Note:** Use the up/down commands to scroll through the list of applications if required.

**At the CS 2000 Management Tools server (SSPFS)**

- 5 Log in to the CS 2000 Management Tools server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the CS 2000 Management Tools server
- 6 When prompted, enter your user ID and password.
- 7 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 8 When prompted, enter the root password.
- 9 Change to the CS 2000 SAM21 Manager user by typing  

```
su - sam21em
```

and pressing the Enter key.
- 10 Remove the existing entry for the SDM in file  
“/export/home/sam21em/.ssh/known\_hosts”.
- 11 Secure-append the public key to the authorized key’s list that  
resides on the core manager by typing  

```
$ cat .ssh/id_rsa.pub | ssh root@$SDM_IP 'cat >>
/home/swld/.ssh/authorized_keys2'
```

and pressing the Enter key.

**Example response:**

```
The authenticity of host '47.142.128.16
(47.142.128.16)' can't be established. RSA key
fingerprint is
21:cb:c6:7f:df:05:f8:4a:2f:23:e9:09:c8:37
bc:1e sam21em@znc0s0j6
Are you sure you want to continue connecting
(yes/no)?
```

- 12** When prompted, confirm you want to continue connecting by typing

# **yes**

and pressing the Enter key.

*Example response:*

```
Warning: Permanently added '47.142.128.16'
(RSA) to the list of known hosts.
root@47.142.128.16's password:
```

- 13** When prompted, enter the password for the SDM root user.
- 14** Ensure the “authorized\_keys2” file has the proper ownership on the SDM by typing

```
$ ssh root@$SDM_IP chown swld:swld
/home/swld/.ssh/authorized_keys2
```

and pressing the Enter key.

*Example response:*

```
root@47.142.128.16's password:
```

- 15** When prompted, enter the password for the SDM root user.
- 16** Propagate the SDM's bootptab file with the entries from SSPFS by typing

```
$ /usr/bin/scp -q
/data/sspfs/etc/bootp/bootptab
$root@{SDM_IP}:/etc/bootptab
```

and pressing the Enter key.

When prompted, enter the password for the SDM root user.

```
$ /usr/bin/ssh -q -l ${SDM_USER}
${SDM_USER}@{SDM_IP} /sdm/swld/loadtab
```

and pressing the Enter key.

You have completed this procedure.

## Re-establishing SSH communication after an SSPFS fresh install

### *At the SDM*

- 1 Log in to the core manager.
- 2 Access the SWIM level of the maintenance interface by typing  
`# sdmmtc swim`  
and pressing the Enter key.
- 3 Access the Details level by typing  
`> details`  
and pressing the Enter key.
- 4 Ensure the OpenSSH fileset is applied.  
**Note:** Use the up/down commands to scroll through the list of applications if required.
- 5 Perform procedure “Setting up the BootP file on SSPFS” in the Voice over IP Network Upgrade document, NN10440-450.  
You have completed this procedure.

---

## Correcting a CORBA configuration issue between the CS 2000 Management Tools server and the MG 9000 Manager server

---

### Application

Use this procedure when you are unable to provision MG 9000 lines or asynchronous digital subscriber lines (ADSLs) through OSSGate, or provision virtual media gateways (VMGs) from the MG 9000 Manager graphical user interface (GUI).

This procedure provides the steps to configure the naming service between the CS 2000 Management Tools server and the server where the MG 9000 Manager resides.

You must configure the naming service on both servers using the steps under

- [Configuring the naming service on the CS 2000 Management Tools server on page 1092](#)
- [Configuring the naming service on the server where the MG 9000 Manager resides on page 1096](#)

Once you have configured the naming service on both servers, you can verify the naming service is set up correctly using the steps under [Verifying the naming service is configured correctly on page 1099](#).

### Prerequisites

None

## Action

Perform the following steps to complete this procedure.

### **Configuring the naming service on the CS 2000 Management Tools server**

#### ***At your workstation***

- 1 Telnet to the CS 2000 Management Tools server by typing  
`> telnet <server>`  
and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the CS 2000 Management Tools 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 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 - exit

select -



- 6** Enter the number that corresponds to the “Configuration” option in the menu.

*Example response*

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 -

- 7** Enter the number that corresponds to the “CORBA Configuration” option in the menu.

*Example response*

CORBA Configuration

- 1 - nsmirror (CORBA Naming Context Mirroring)

X - exit

select -

- 8 Enter the number that corresponds to the “nsmirror” option in the menu.

*Example response*

===Executing “nsmirror”

- 1 - Add CORBA Naming Context Mirror
- 2 - Remove CORBA Naming Context Mirror
- 3 - Display Current Configuration
- 4 - Exit

Configuraton

file:/opt/corba/rcscripts/NamingServiceMirrors.cfg

Please enter selection (1, 2, 3 or 4):

- 9 Enter the number that corresponds to the “Add CORBA Naming Context Mirror” option in the menu.
- 10 When prompted, enter the Application Name for the Succession Element and Sub-Network Manager by typing

**sesm**

and pressing the Enter key.

- 11 When prompted, enter the Host Name or IP address of the server where the MG 9000 resides.

- 12 When prompted, enter the Context Path by typing

**NameService/Subnet\_<release>**

and pressing the Enter key.

Where

**release**

is the current release of the software, for example 07 for (I)SN07

**Note:** The command is case sensitive.

- 13** When prompted, enter the Context Name by typing  
**Subnet\_<release>**  
and pressing the Enter key.  
Where  
**release**  
is the current release of the software, for example 07 for (I)SN07  
**Note:** The command is case sensitive.
- 14** When prompted, press the Enter key to accept the default value (2001) for the Local Port.
- 15** When prompted, press the Enter key to accept the default value (2001) for the Remote Port.
- Example response:*
- You have selected to bind the remote naming context as follow:
- ```
Application Name      :SESM
Host Name             :47.142.89.70
Context Path          :NameService/Subnet_07
Context Name          :Subnet_07
Local Port            :2001
Remote Port           :2001
```
- Continue with configuration? (default:Y[Y/N/Q])
- 16** When prompted, confirm the configuration by typing.
y
and pressing the Enter key.
- 17** 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.
- 18** You have completed this procedure. Proceed to [Configuring the naming service on the server where the MG 9000 Manager resides on page 1096](#).

Configuring the naming service on the server where the MG 9000 Manager resides

At your workstation

- 1 Telnet to the server where the MG 9000 Manager resides by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server

is the IP address or host name of the server where the MG 9000 Manager resides

- 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 - exit
```

```
select -
```

- 6** Enter the number that corresponds to the “Configuration” option in the menu.

Example response

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 -

- 7** Enter the number that corresponds to the “CORBA Configuration” option in the menu.

Example response

CORBA Configuration

- 1 - nsmirror (CORBA Naming Context Mirroring)

X - exit

select -

- 8** Enter the number that corresponds to the “nsmirror” option in the menu.

Example response

```
===Executing "nsmirror"
```

```
1 - Add CORBA Naming Context Mirror
2 - Remove CORBA Naming Context Mirror
3 - Display Current Configuration
4 - Exit
```

Configuraton

```
file:/opt/corba/rcscripts/NamingServiceMirrors.cfg
```

Please enter selection (1, 2, 3 or 4):

- 9** Enter the number that corresponds to the “Add CORBA Naming Context Mirror” option in the menu.
- 10** When prompted, enter the Application Name for the MG 9000 Manager by typing

mgems

and pressing the Enter key.

- 11** When prompted, enter the Host Name or IP address of the CS 2000 Management Tools server where the SESM resides.

- 12** When prompted, enter the Context Path by typing

NameService/Nortel

and pressing the Enter key.

Note: The command is case sensitive.

- 13 When prompted, enter the Context Name by typing
Nortel
and pressing the Enter key.
Note: The command is case sensitive.
- 14 When prompted, press the Enter key to accept the default value (2001) for the Local Port.
- 15 When prompted, press the Enter key to accept the default value (2001) for the Remote Port.

Example response:

You have selected to bind the remote naming context as follow:

```
Application Name      :MGEMS
Host Name             :47.142.85.56
Context Path          :NameService/Nortel
Context Name          :Nortel
Local Port            :2001
Remote Port           :2001
```

Continue with configuration? (default:Y[Y/N/Q])

- 16 When prompted, confirm the configuration by typing.
y
and pressing the Enter key.
- 17 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.
- 18 You have completed this procedure. Proceed to [Verifying the naming service is configured correctly on page 1099](#).

Verifying the naming service is configured correctly

At your workstation

- 1 Close all GUIs and OSSGate telnet sessions if any.
- 2 Restart the SESM server application. Refer to procedure “Starting the SESM server application” in the ATM/IP Security and Administration document, NN10402-600, if required.

- 3** Restart the MG 9000 Manager server application. Refer to the corresponding procedure in the MG 9000 Security and Administration document, NN10162-611, if required.
- 4** Start OSSgate client and provision one or more lines or ADSLs. Refer to the OSSgate User Guide, if required.
- 5** Access the MG 9000 Manager and provision a VMG. Refer to the corresponding procedure in the MG 9000 Security and Administration document, NN10162-611, if required.

Verifying the state of a cluster

Application

Use this procedure to verify the state of a cluster, which involves verifying the status of replicated disk volumes, the cluster indicator, and the cluster configuration. A cluster refers to a Sun Netra 240 server pair.

ATTENTION

Perform this procedure to determine the state of the cluster rather than rely on the presence of the ClusterOutOfSync file in the root directory. The ClusterOutOfSync file does not give the definitive state of the cluster.

When a cluster node is out of sync, log SPFS310 is generated.

For more information on logs, refer to *Carrier Voice over IP Networks Fault Management Logs Reference*, NN10275-909. For information on how to configure log reporting, route customer logs to a remote host and view customer logs, refer to *ATM/IP Fault Management*, NN10408-900.

Prerequisites

You need the root user ID and password for the inactive server.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Establish a login session to the inactive server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- 2 Log in to the server using telnet (unsecure) as follows:
 - a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the physical IP address of the inactive server
 - b When prompted, enter your user ID and password.
 - c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.
 - d When prompted, enter the root password.
Note: Ensure you are on the right server by typing ubmstat. You must be on the inactive server and the response must be *ClusterIndicatorSTBY*.
Proceed to step [4](#).
- 3 Log in using ssh (secure) as follows:
 - a Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.
where
server
is the physical IP address of the inactive server
Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter *yes* at the prompt.
 - b When prompted, enter the root password.
Note: Ensure you are on the right server by typing ubmstat. You must be on the inactive server and the response must be *ClusterIndicatorSTBY*.

- 4 Ensure you are logged in to the inactive server by typing
ubmstat
and pressing the Enter key.
- | If | Do |
|--|------------------------|
| the system response is
ClusterIndicatorSTBY | step 6 |
| otherwise | step 5 |
- 5 Log out of the active server and return to step [1](#) to log in to the inactive server.
- 6 Verify the status of replicated disk volumes by typing
udstat
and pressing the Enter key.
- | If | Do |
|--|------------------------|
| the system response is
STANDBY normal UP
clean | step 7 |
| otherwise | step 8 |
- 7 Verify the status of the cluster configuration by typing
CheckConfiguration
and pressing the Enter key.
- | If | Do |
|--|---|
| the system response is
Cluster configuration
validated. All
cluster node
configurations in
sync | the cluster is in a good state
and you can proceed to
step 13 |
| otherwise | step 8 |

- 8** Reboot the inactive server by typing

init 6

and pressing the Enter key.

If	Do
the problem persists	step 9
otherwise	the cluster is in a good state and you can proceed to step 13

- 9** Capture SSPFS file and logs for debugging purposes. 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 - exit

select -

- 10** Enter the number next to the Other option in the menu.

Example response

Other

- 1 - Log Rotation
- 2 - capt_files (Capture Various SSPFS Files/Logs For Debugging Purposes)
- 3 - sun_explorer (Execute the Sun Explorer Data Gathering Tool)
- 4 - mount_image (Mount A Generic Iso Image To the SSPFS Unit)
- 5 - umount_image (Un-Mount A Generic Iso Image From the SSPFS Unit)
- 6 - disp_sspfspatch (Display the patching status of the SSPFS unit)

x - exit

select -

- 11** Enter the number next to the capt_files option in the menu.
Example response
Executing "capt_files"
- 12** Provide the debugging data to your next level of support for analysis before you proceed.
- 13** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Initiating a manual failover on a Sun Netra 240 server pair

Application

Use this procedure to initiate a manual failover on a Sun Netra 240 server pair. Initiating a manual failover can be required in the following situations:

- general maintenance
- software update without a data schema or configuration change

The failover causes the standby (inactive) server to take over and start providing OAM&P services as the new active server.

ATTENTION

During an automatic or manual failover, the high-availability (HA) cluster takes approximately 5 minutes to failover and bring up the standby node to Active state.

Prerequisites

You must perform this procedure on the active node.

Action

Perform the following steps to complete this procedure.

ATTENTION

Perform the steps that follow on the Active server.

At the active node console

- 1 Log in to the active node through the console (port A) using the root user ID and password.

Note: Ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server in the pair. The response must display `ClusterIndicatorACT`, which indicates you are on the Active server.

- 2 Initiate the manual failover by typing

swact

and pressing the Enter key.

Example response

Are you sure you want to initiate a cluster failover? [Y/N]

- 3 If it is acceptable to initiate a manual failover, indicate you want the failover to occur by typing

y

and pressing the Enter key.

You have completed this procedure.

Querying the state of the SSPFS platform

Application

Use this procedure to query the state of the system (all monitors registered with AlarmD or just those that have alarms against them).

Prerequisites

You must have root user privileges.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Telnet to the Sun server by typing
 `> telnet <IP address>`
 and pressing the Enter key.
 where
 IP address
 is the IP address of the Sun server you want to query
- 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 - exit

select -
```

- 6** Enter the number next to the “Configuration” option in the menu.

Example response

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 -

- 7** Enter the number next to the “Succession Element Configuration” option in the menu.

Example response:

Succession Element Configuration

- 1 - SESM Application Configuration
- 2 - SAM21EM Application Configuration
- 3 - NPM Application Configuration
- 4 - PSE Application Configuration
- 5 - RESMON Application Configuration
- 6 - OMPUSH Application Configuration

X - exit

select -

- 8** Enter the number next to the “RESMON Application Configuration” option in the menu.

Example response

```
RESMON Application Configuration
 1 - settrapdest (Set location for IEMS traps)
 2 - queryFaults (Query all faults on the box)
 3 - enableLocalLogs (Enable Local Logging Of
    Faults)
 4 - disableLocalLogs (Disable Local Logging Of
    Faults)

X - exit

select -
```

- 9** Enter the number next to the “queryFaults” option in the menu.

Example response

```
===Executing “queryFaults”
```

The Log Information is

```
*SPFS350 Current filesystem usage = 77%
  Filesystem is filling up
  iemscs2k=wrxrpz0xy;NODE=wrxrpz0xy;CLASS=SYS
  SYSTYP=FSMon;FSMonName=FSUsage;FSName=/
  Wed Jun 30 14:54:36 2004
```

```
===“queryFaults” completed successfully
```

```
RESMON Application Configuration
 1 - settrapdest (Set location for IEMS traps)
 2 - queryFaults (Query all faults on the box)
 3 - enableLocalLogs (Enable Local Logging Of
    Faults)
 4 - disableLocalLogs (Disable Local Logging Of
    Faults)

X - exit

select -
```

- 10** If log information is displayed, refer to the *Carrier Voice over IP Fault Management Logs Reference* document, NN10275-909, for more information.

- 11 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.
- 12 You have completed this procedure.

Rebooting an SSPFS-based server

Application

Use this procedure to reboot a Succession Server Platform Foundation Software (SSPFS)-based server, which may be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core and Billing Manager (CBM)

ATTENTION

The SSPFS-based server may be hosting more than one of the above components, therefore, ensure it is acceptable to reboot the server.

Prerequisites

You must have root user privileges.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Telnet to the Sun server by typing
 > **telnet <IP address>**
 and pressing the Enter key.
 where
 IP address
 is the IP address of the SSPFS-based server you want to reboot
- 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 Reboot the server by typing
shutdown -i 6 -y
and pressing the Enter key.
- 6 You have completed this procedure.

Shutting down an SSPFS-based server

Application

Use this procedure to shut down a Succession Server Platform Foundation Software (SSPFS)-based server, which may be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

ATTENTION

The SSPFS-based server may be hosting more than one of the above components, therefore, ensure it is acceptable to shut down the server.

Prerequisites

You must have root user privileges.

Action

Use one of the following procedures according to your office configuration:

- [One-server configuration on page 1116](#)
- [Two-server \(cluster\) configuration on page 1117](#)

One-server configuration

At your workstation

- 1 Log in to the server by typing
 `> telnet <IP address>`
 and pressing the Enter key.
 where
 IP address
 is the IP address of the SSPFS-based server you want to power down
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing
 `$ su -`
 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Shut down the server by typing
 `# init 0`
 and pressing the Enter key.
 The server shuts down gracefully, and the telnet connection is closed.
- 6 If required, turn off the power to the server at the circuit breaker panel of the frame.
 You have completed this procedure.
 To bring the server back up, turn on the power to the server at the circuit breaker panel of the frame. The server recovers on its own once power is restored.

Two-server (cluster) configuration

At your workstation

- 1 Log in to the Inactive server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

IP address

is the physical IP address of the Inactive SSPFS-based server in the cluster you want to power down (unit 0 or unit 1)

- 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.

Note: Ensure you are on the Inactive server by typing `ubmstat`. If *ClusterIndicatorACT* is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorSTBY*, which indicates you are on the Inactive server.

- 5 Shut down the Inactive server by typing

```
# init 0
```

and pressing the Enter key.

The server shuts down gracefully, and the telnet connection is closed.

- 6 If required, turn off the power to the Inactive server at the circuit breaker panel of the frame. You have completed a partial power down (one server).

If you want to perform a full power down (both servers), proceed to step [7](#), otherwise, you have completed this procedure.

7

ATTENTION

Only perform the remaining steps if you want to perform a full power down, which involves powering down both servers in the cluster.

Telnet to the Active server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

IP address

is the physical IP address of the Active SSPFS-based server in the cluster you want to power down

8 When prompted, enter your user ID and password.

9 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

10 When prompted, enter the root password.

11 Shut down the Active server by typing

```
# init 0
```

and pressing the Enter key.

The server shuts down gracefully, and the telnet connection is closed.

12 If required, turn off the power to the servers at the circuit breaker panel of the frame. You have completed a full power down (two servers).

You have completed this procedure.

To bring the servers back up, turn on the power to the servers at the circuit breaker panel of the frame. The servers recover on their own once power is restored.

Executing a fallback during an SSPFS-based server upgrade

Application

Use this procedure to rollback to the state prior to the upgrade.

ATTENTION

Only use this procedure when directed to do so.

Prerequisites

You must perform this procedure on the newly upgraded server.

Action

Perform the steps under one of the headings that follow to complete this procedure.

- [One-server configuration on page 1119](#)
- [Two-server configuration on page 1120](#)

One-server configuration

At the server console

- 1 Log in to the server through the console (port A) using the root user ID and password if not already logged in.
- 2 Rollback to the state prior to the upgrade by typing
`# /SSPFS_Upgrade.fallback`
and pressing the Enter key.
- 3 Use the following table to determine your next step.

If your server is hosting the	Do
Core Billing Manager (CBM)	you have completed this procedure
CS 2000 Management Tools, Media Gateway 9000 Manager, or Integrated Element Management System (IEMS)	step 4

- 4 Restore the oracle data on the server. If required, refer to procedure “Restoring the oracle data on an SSPFS-based server” in the ATM/IP Security and Administration document, NN10402-600

You have completed this procedure.

Two-server configuration

At the server console

- 1 Log in to the server server that has the new software on it through the console (port A) using the root user ID and password if not already logged in.
- 2 Rollback to the state prior to the upgrade by typing
/SSPFS_Upgrade.fallback
and pressing the Enter key.
- 3 Use the following table to determine your next step.

If your server is hosting the	Do
Core Billing Manager (CBM)	step 7
CS 2000 Management Tools, Media Gateway 9000 Manager, or Integrated Element Management System (IEMS)	step 4

- 4 Connect to the console port of the other server that has the previous software on it.
- 5 Boot the server by typing
OK boot
and pressing the Enter key.
- 6 Log in using the root user ID and password.
- 7 Verify both servers are present by typing
GetRunningClusterNodeNames
and pressing the Enter key.

If the system response returns	Do
one server	step 8
two servers	step 9

- 8 Wait for one minute and repeat step [7](#). If after the second time, only one server is displayed, contact your next level of support before proceeding with this fallback.

- 9 Verify the status of replicated disk volumes by typing

udstat

and pressing the Enter key.

If	Do
all the file systems are ACTIVE normal UP clean	step 10
otherwise	contact your next level of support

- 10 Clone the image of the active server onto the other server. If required, refer to procedure [Cloning the image of one node in a cluster to the other node on page 351](#).

Once the clone is complete, the cluster is restored as it was before the upgrade.

You have completed this procedure.

Restoring NPM patch files

Application

Use this procedure to restore NPM patch files on the server. This procedure provides the following instructions:

- [Restoring NPM patch files from tape \(Sun Netra t1400 only\) on page 1123](#)
- [Restoring NPM patch files from CD/DVD \(Sun Netra 240 only\) on page 1126](#)

Note: NPM patch files saved to a location on disk are preserved over an upgrade. However, if for some reason you need to restore those patch files, contact your next level of support.

Prerequisites

This procedure has the following prerequisites:

- for a Sun Netra t1400, you need the NPM patch file archive tape
- for a Sun Netra 240, you need the NPM patch file archive CD or DVD

Action

Perform the steps using one of the following methods to complete this procedure:

- [Restoring NPM patch files from tape \(Sun Netra t1400 only\)](#)
- [Restoring NPM patch files from CD/DVD \(Sun Netra 240 only\)](#)

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

Restoring NPM patch files from tape (Sun Netra t1400 only)

At your workstation

- 1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server

is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step [4](#).

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server

is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter `yes` at the prompt.

- b** When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

- 4** Stop the NPM server application if it is running. If required, refer to procedure “Stopping the NPM server application” in document *ATM/IP Security and Administration*, NN10402-600.
- 5** Re-initialize the NPM database. If required, refer to procedure “Initializing the NPM database” in document *ATM/IP Security and Administration*, NN10402-600.
- 6** Insert the NPM patch file archive tape into the drive.
- 7** Rewind the tape by typing

```
# mt rewind
```

and pressing the Enter key.
- 8** Access the NPM patch file directory by typing

```
# cd /data/npm/Au
```
- 9** Restore the NPM patch files to the `/data/npm/Au` directory by typing

```
# tar tvf /dev/rmt/0
```

and pressing the Enter key.
- 10** Rewind and eject the tape by typing

```
# mt offline
```

and pressing the Enter key.
- 11** Remove the tape from the drive.
- 12** Start the NPM server application. If required, refer to procedure “Starting the NPM server application” in document *ATM/IP Security and Administration*, NN10402-600.
- 13** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Restoring NPM patch files from CD/DVD (Sun Netra 240 only)**At your workstation**

- 1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- 2 Log in to the server using telnet (unsecure) as follows:
 - a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration
 - b When prompted, enter your user ID and password.
 - c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.
 - d When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the active server.

Proceed to step [4](#).

- 3 Log in using ssh (secure) as follows:
 - a Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration
Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter *yes* at the prompt.
 - b When prompted, enter the root password.
Note: In a two-server configuration, ensure you are on the active server by typing *ubmstat*. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.
- 4 Stop the NPM server application if it is running. If required, refer to procedure “Stopping the NPM server application” in document *ATM/IP Security and Administration*, NN10402-600.
- 5 Re-initialize the NPM database. If required, refer to procedure “Initializing the NPM database” in document *ATM/IP Security and Administration*, NN10402-600.
- 6 Insert the NPM patch file archive CD/DVD into the drive.
- 7 Copy the NPM patch files to the /data/npm/Au directory by typing

```
# cp /cdrom/patches/*.ptch* /data/npm/Au/
```

and pressing the Enter key.
- 8 Eject the CD or DVD from the drive as follows:
 - a Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

b Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.

c Remove the CD or DVD from the drive.

- 9** Start the NPM server application. If required, refer to procedure “Starting the NPM server application” in document *ATM/IP Security and Administration*, NN10402-600.
- 10** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Performing an APS-only Data Base Restore from a 4mm DAT

Use this procedure to restore the APS DB from an APS DB tape backup in a 4mm DAT drive.

Prerequisites

This procedure is for sites with a SUN t1400 server equipped with a 4mm DAT drive.

Note: This procedure is not for sites with a SUN v240 and the CD-DVD drive.

At the APS server

- 1 Become the root user by entering the following command and then entering the "root" password when prompted.

```
su - root
```

- 2 Ensure the 4mm DAT tape in the drive is a write-protected.
- 3 Start the DB restore from the tape by typing the following command.

```
$ ips_export_db.sh -t /dev/rmt/0 -restore
```

This command restores the APS DB from the tape to the following directory.

```
/audio_files/aps_db_backup/*.dmp
```

- 4 Restore the APS audio files to the file system if not already performed.
- 5 You have completed this procedure.

Performing an APS-only Database restore from a CD

Use this procedure on a SUN v240 server with a CD drive.

Prerequisites

This procedure is for sites with a SUN v240 and the CD-DVD drive.

Note: This procedure is not for sites with a SUN t1400 server equipped with a 4mm DAT drive.

At the APS server

- 1 Become the root user by entering the following command and then entering the "root" password when prompted.

`su - root`
- 2 Load the backup CD into the CD drive on the server.
- 3 Change to the aps backup directory on the server by typing the following command.

`cd /audio_files/aps_db_backup`
- 4 Copy the dmp files on the CD to this directory by typing the following command.

`$ cp /cdrom/cdrom0/* ./`
- 5 Verify the dmp files were copied from CD to the destination directory by typing the following command and then viewing the command output.

`$ ls -l *`


```
-rwxrwsrwx 1 root other 54272 May 13 11:11  
ips_db_audit.dmp  
  
-rwxrwsrwx 1 root other 4096 May 13 11:11  
ips_node_config.dmp  
  
-rwxrwsrwx 1 root other 2048 May 13 11:11  
ips_prov_prg_grp.dmp  
  
-rwxrwsrwx 1 root other 2048 May 13 11:11  
ips_prov_set.dmp  
  
-rwxrwsrwx 1 root other 3072 May 13 11:11  
ips_user.dmp  
  
-rwxrwsrwx 1 root other 3072 May 13 11:11  
ips_user_perm_group.dmp  
  
-rwxrwsrwx 1 root other 71 May 13 11:11 README
```

```
-rwxrwsrwx 1 root other 4096 May 13 11:11
sys_parms.dmp
. . . . .
-rwxrwsrwx 1 root other 44032 May 13 11:11
uas_segments.dmp
-rwxrwsrwx 1 root other 6144 May 13 11:11
uas_selector_relation.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_selector_type.dmp
-rwxrwsrwx 1 root other 7168 May 13 11:11
uas_selector_value.dmp
-rwxrwsrwx 1 root other 5120 May 13 11:11
uas_sequences.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_set_content.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_set_definition.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_user_perms.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_var_start_seg_id.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11
uas_variables.dmp
#
```

- 6** Start the DB restore from the disk files by typing the following command.

```
$ . ips_export_db.sh -diskonly -restore
```

This command restores the APS DB from the disk files to the directory shown below.

```
/audio_files/aps_db_backup/*.dmp
```

- 7** Restore the APS audio files to the file system if not already performed.
- 8** You have completed this procedure.

Starting the SESM server application

Application

Use this procedure to start the Succession Element and Subelement Manager (SESM) server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the Active server.

At your workstation

- 1 Log in to the server by typing

> **telnet <server>**

and pressing the Enter key.

where

server

is the IP address or host name of the CS 2000 Management Tools server

Note: In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

- 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.

Note: In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the Active server.

- 5 Verify the status of the SESM server application by typing

```
# servman query -status -group SESMService
```

If SESMService is	Do
not running	step 6
running	you have completed this procedure

- 6 Start the SESM server application by typing

```
# servstart SESMService
```

and pressing the Enter key.

- 7 Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to start.

Note: Starting SESM for the first time after an upgrade from a pre-SN07 release, can take up to 90 minutes depending on the number of GWs provisioned in the office. This is a one-time event that occurs during an upgrade to facilitate better topological management of data.

- 8 Verify the SESM server application started by typing
servman query -status -group SESMSERVICE
and pressing the Enter key.

Example response:

```
Executing: /opt/servman/bin/servquery -status -  
group SESMSERVICE
```

```
Succession CS2K Management Tools VERSION:  
SESM_8_019_0
```

Current status of the CS2K Management Tools:

```
LMM is running  
TMM is running  
GWCEM is running  
UASEM is running  
OSS Gate is running
```

You have completed this procedure.

Launching CS 2000 Management Tools and NPM client applications

Application

Use this procedure to launch any one of the following client applications:

- Trunk Maintenance Manager (TMM)
- CS2000 Management Tools
- Line Maintenance Manager (LMM)
- SAM21 Element Manager
- Batch Configuration Monitor
- Network Patch Manager (NPM), when installed and enabled on the same server as the CS 2000 Management Tools

Note: The NPM also has a command line user interface (CLUI). Refer to procedure [Accessing the Network Patch Manager CLUI on page 1151](#).

This procedure provides the following four methods to launch a CS 2000 Management Tools client application:

- [Launching applications from a web browser on page 1139](#). You must use this method when launching an application for the first time.
- [Launching applications from the JWS Application Manager on page 1142](#).

Note: You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- [Launching applications from a desktop icon or Start menu \(Windows only\) on page 1145](#).

Note: You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- [Launching specific applications using a URL on page 1148](#).

Note: You can also launch applications from the Integrated Element Management System (IEMS) when the IEMS is present in the office. Refer to the Integrated Element Management System Basics document, NN10329-111.

Prerequisites

Ensure the client workstation meets the minimum requirements. Refer to section "Client workstation requirements" under "CS 2000 Management Tools" in the Basics document, NN10320-100 (ATM solution) or NN10300-100 (IP solution).

ATTENTION

If you have an ATI Raedon 7000 series graphics card installed on your desktop computer, or an ATI Mobility graphics chip installed in your laptop computer, you can experience the "blue screen of death" in your Windows environment. You can obtain information on this issue at the following website:

<http://developer.java.sun.com/developer/bugParade/bugs/4713003.html>

A workaround for this issue is to download the latest ATI graphics driver from the following web site:

<http://mirror.ati.com/support/driver.html>

Contact your IT support team if you need assistance.

You need the IP address or host name of the server where the CS 2000 Management Tools are installed, and a valid user name and password to launch an application.

Note: Users of the CS 2000 Management Tools client applications must belong to the primary user group "succssn" for login access, and to one or more secondary user groups, which specify the operations a user is authorized to perform. If required, refer to procedure "Setting up local user accounts on a Sun server" in the ATM/IP Security and Administration document, NN10402-600.

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2_05 and Java™ Web Start (JWS) version 1.2.0_02 installed to launch the following applications:

- CS2000 Management Tools
- Line Maintenance Manager
- CS2000 SAM21 Manager
- Network Patch Manager

Note: JWS 1.2.0_02 is included as part of JRE 1.4.2_05.

Action

Launching applications from a web browser

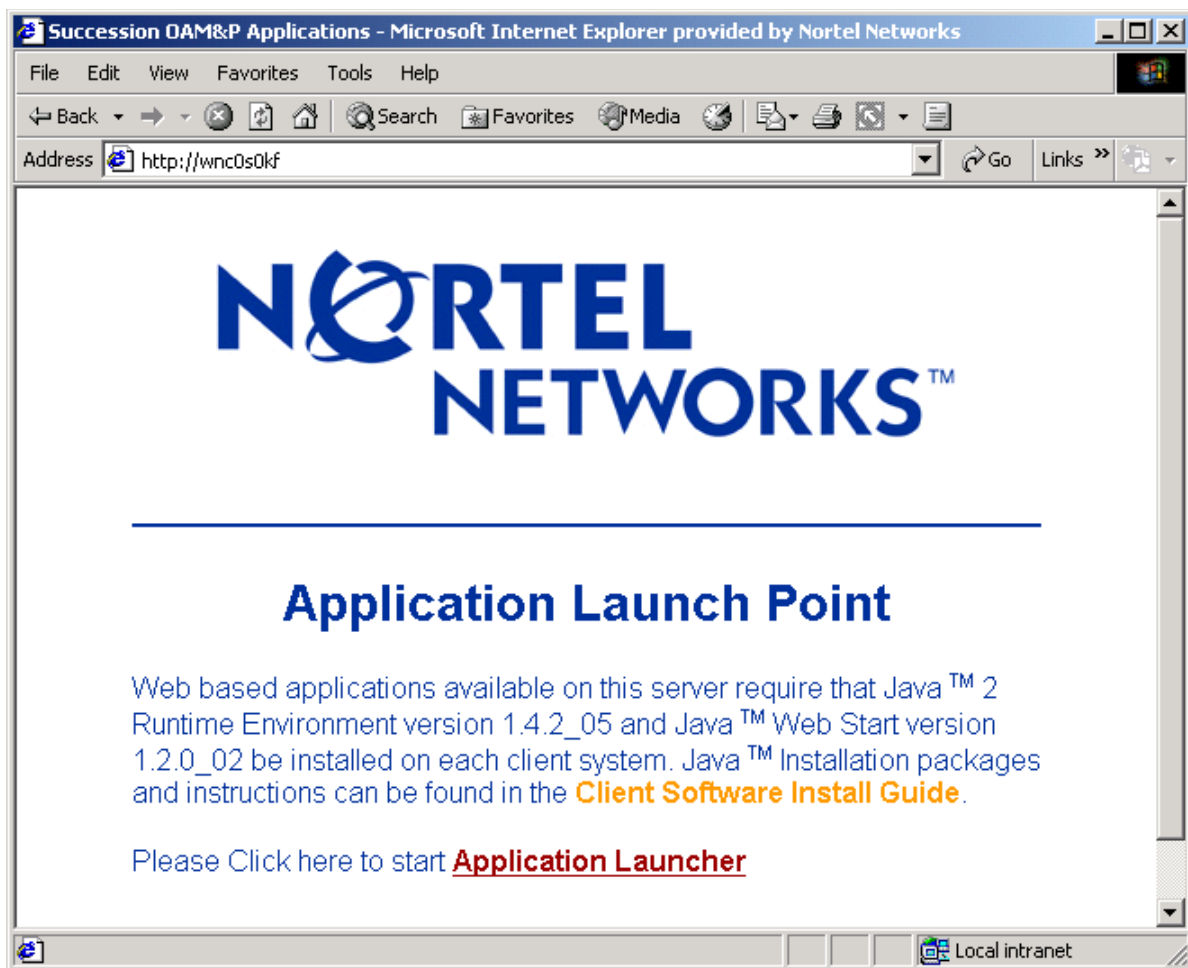
At your workstation

- 1 Launch your web browser.
- 2 In the Address field, enter the name or IP address of the CS 2000 Management Tools server.

Example

<http://47.142.89.70>

The “Application Launch Point” page appears.



- 3 Refer to the following table to determine your next step.

If	Do
you have JRE 1.4.2_05 and JWS 1.2.0_02 installed	step 9
you do not have JRE 1.4.2_05 and JWS 1.2.0_02 installed	step 4
you do not know which version of JRE and JWS you have	step 4

- 4 Click **Client Software Install Guide** and follow the instructions under *How to check version* to verify your client setup.

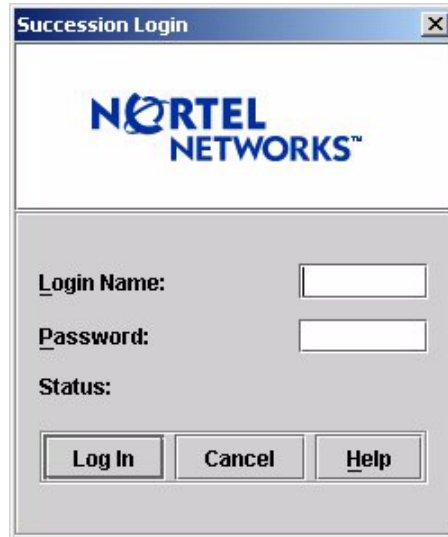
If	Do
you have JRE 1.4.2_05 and JWS 1.2.0_02 installed	step 8
you do not have JRE 1.4.2_05 and JWS 1.2.0_02 installed	step 5

- 5 Click **Java 2 Runtime Environment Install Guide** under *Microsoft Windows* or *Sun Solaris* for system requirements and installation instructions.
- 6 Once you have read through the Java 2 Runtime Environment Install Guide, click the **Back** button to return to the Client Software Installation page.
- 7 Click **Java 2 Runtime Environment Software Download** under *Microsoft Windows* or *Sun Solaris* to download and install the software.

Note: You must have administrative privileges to install the software on the workstation.

- 8 Click the **Back** button to return to the Application Launch Point.

- 9 Click **Application Launcher**.
The Login window appears.

A screenshot of a web browser window titled "Succession Login". The window has a blue header bar with the title and a close button. Below the header is the Nortel Networks logo. The main content area is a light gray box containing three labels: "Login Name:", "Password:", and "Status:". Each label is followed by a text input field. At the bottom of the gray box are three buttons: "Log In", "Cancel", and "Help".

Succession Login

NORTEL NETWORKS™

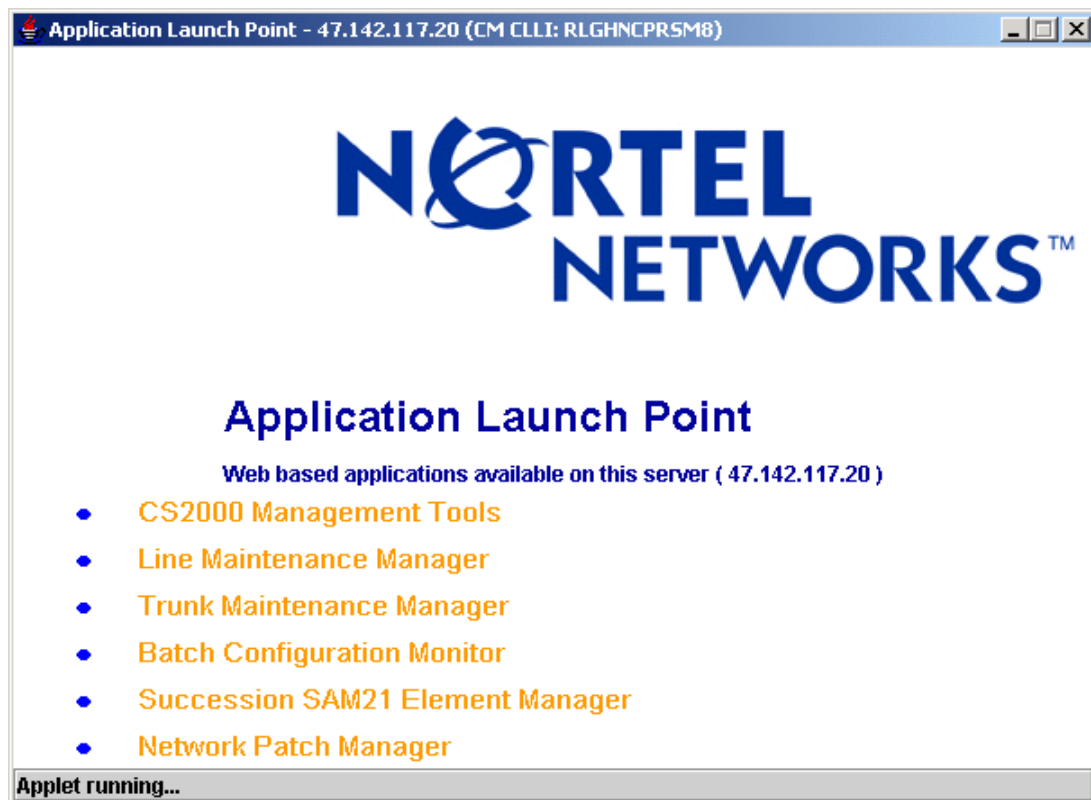
Login Name:

Password:

Status:

Log In Cancel Help

- 10 Enter your user name and password, then click **Log In**.
The Application Launch Point, similar to following, appears.

A screenshot of a web browser window titled "Application Launch Point - 47.142.117.20 (CM CLI: RLGHNCP5M8)". The window has a blue header bar with the title and standard window controls. The main content area is white and features the Nortel Networks logo at the top. Below the logo is the title "Application Launch Point" in blue. Underneath is the text "Web based applications available on this server (47.142.117.20)". A bulleted list of applications follows: "CS2000 Management Tools", "Line Maintenance Manager", "Trunk Maintenance Manager", "Batch Configuration Monitor", "Succession SAM21 Element Manager", and "Network Patch Manager". At the bottom of the window is a status bar that says "Applet running...".

Application Launch Point - 47.142.117.20 (CM CLI: RLGHNCP5M8)

NORTEL NETWORKS™

Application Launch Point

Web based applications available on this server (47.142.117.20)

- CS2000 Management Tools
- Line Maintenance Manager
- Trunk Maintenance Manager
- Batch Configuration Monitor
- Succession SAM21 Element Manager
- Network Patch Manager

Applet running...

- 11 Click the link for the application you want to launch.

The interface for the application you launched, is displayed.

Note: If you delay clicking an application link by 5 minutes or more after you log in, the login window will appear requiring you to log in again.

You have completed this procedure.

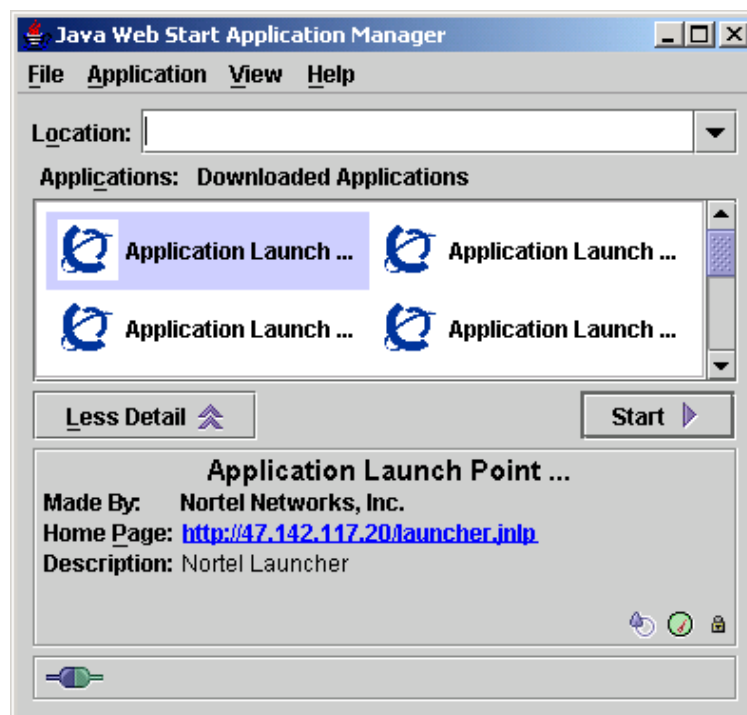
Launching applications from the JWS Application Manager

ATTENTION

You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

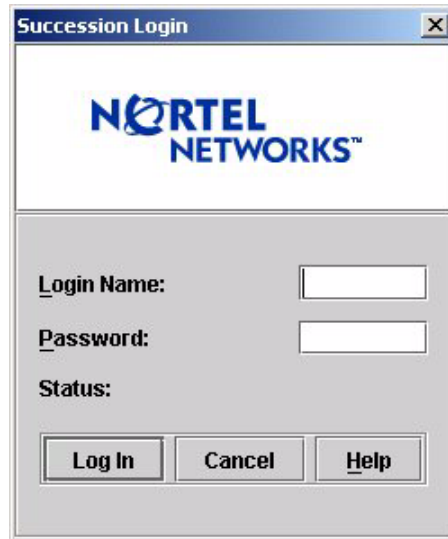
At your workstation

- 1 Launch the Java Web Start Application Manager.

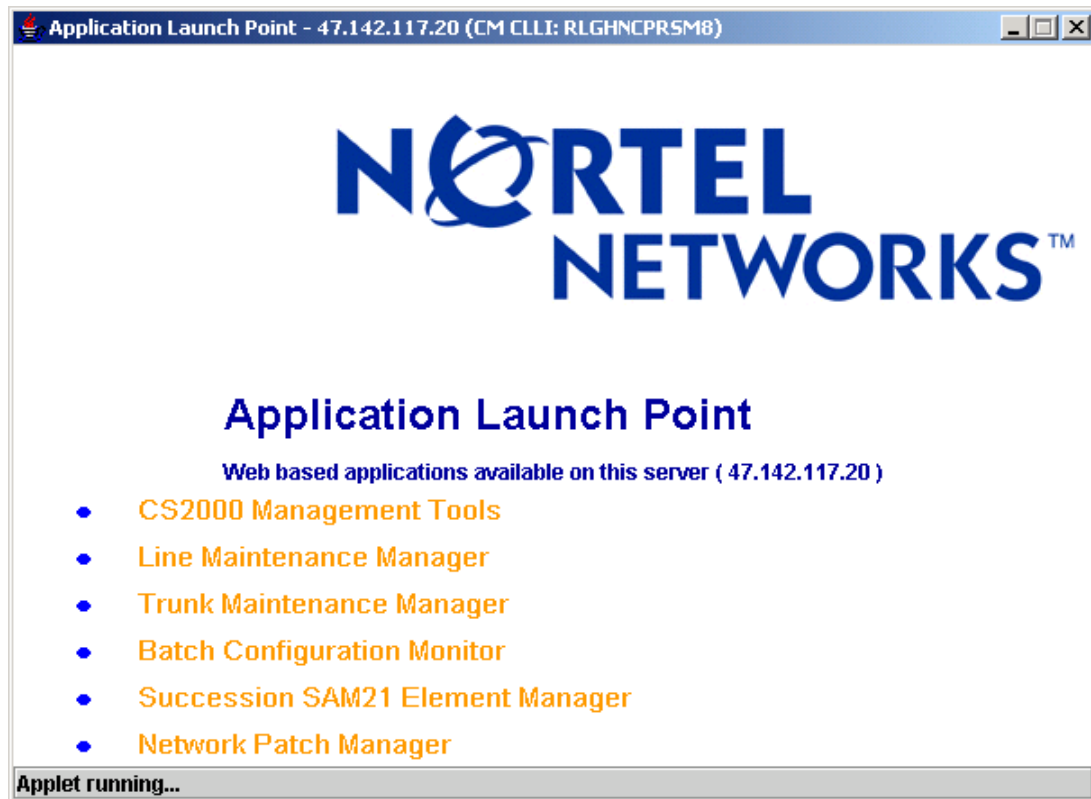


Note: If you do not see the downloaded applications as shown in the example above, on the **View** menu, click **Downloaded Applications**.

- 2 Double click on the Application Launch Point you want to access, or select the Application Launch Point and click **Start**.
The Login window appears.
- 3 Enter your user name and password, then click **Log In**.



The Application Launch Point, similar to following, appears.



- 4 Click the link for the application you want to launch.
The interface for the application you launched, is displayed.
You have completed this procedure.

Launching applications from a desktop icon or Start menu (Windows only)

ATTENTION

You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

At your workstation

- 1 Perform [step a](#) to launch an application from a desktop icon, or [step b](#) to launch an application from the Start menu.
 - a To launch a CS 2000 Management Tools client application from a desktop icon, locate the short-cut icon on your desktop, and double click on it to start the application.

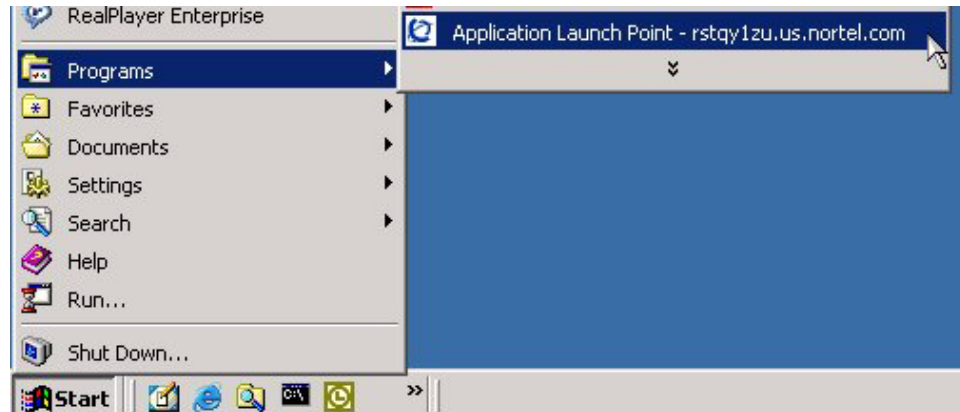
Note: For short-cut icons to be present on your desktop, you must have the right settings under the Shortcut Options tab, which is accessed through **File->Preferences** in the JWS Application Manager.



The Login window appears.

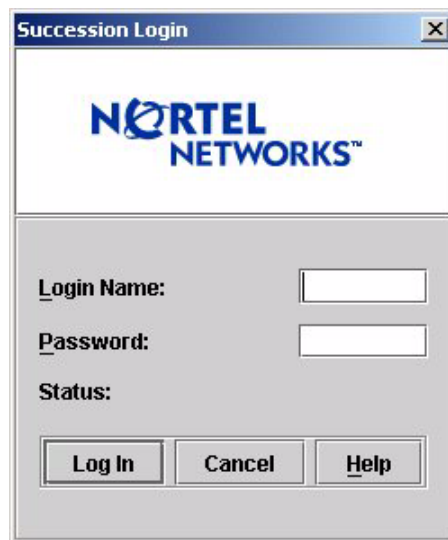
Proceed to [step 2](#).

- b To launch a CS 2000 Management Tools client application from the Start menu, click **Start->Programs**, then click the CS 2000 Management Tools client application you want to launch.



The Login window appears.

- 2 Enter your user name and password, then click **Log In**.



The Application Launch Point, similar to following, appears.



- 3 Click the link for the application you want to launch.
The interface for the application you launched, is displayed.
You have completed this procedure.

Launching specific applications using a URL

ATTENTION

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2_05 and Java™ Web Start (JWS) version 1.2.0_02 installed to launch the applications. If this is the first time you are launching an application, use the first method provided in this procedure [Launching applications from a web browser on page 1139](#).

At your workstation

- 1 Launch your web browser.
- 2 In the Address field, enter one of the following URLs for the application you want to launch:

Application	URL
CS2000 Management Tools	http://<host>:8080/launch/servlet/Launch?app=sesm
Line Maintenance Manager	http://<host>:8080/launch/servlet/Launch?app=lmm
Trunk Maintenance Manager	http://<host>/sesm/tmm.html
Batch Configuration Monitor	http://<host>/sesm/bpt.html
CS2000 SAM21 Manager	http://<host>:8080/launch/servlet/Launch?app=sam21em
Network Patch Manager	http://<host>:8080/launch/servlet/Launch?app=npm

Where

host

is the host name or IP address of the server where the application resides

The Login window appears.

- 3 Enter your user name and password, then click **Log In**.



The interface for the application you launched, is displayed.
You have completed this procedure.

Additional information

The GUI-based client applications (CS2000 Management Tools, Line Maintenance Manager, Network Patch Manager, and SAM21 Element Manager) connect to their corresponding server-side application through a Socks proxy.

Note: The Trunk Maintenance Manager (TMM) and Batch Configuration Monitor do not use a Socks proxy.

If, when you launch a client application that connects through a Socks proxy, you receive an error message indicating that the Socks connection to the server has failed, the server is down and needs to be rebooted. Once the server has rebooted, you can relaunch the client application.

Accessing the Network Patch Manager CLUI

Application

Use this procedure to access the Network Patch Manager (NPM) command line user interface (CLUI).

Note 1: You can also access the NPM CLUI from the Integrated Element Management System (EMS) when the Integrated EMS is present in the office. Refer to the Integrated EMS Basics document, NN10329-111.

Note 2: The Network Patch Manager also has a graphical user interface (GUI). Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 1137](#).

Prerequisites

You must have a valid user ID and password to access the NPM interface. In addition, you must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on an SSPFS-based server” in the ATM/IP Security and Administration document, NN10402-600.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SSPFS-based server where NPM resides
- 2 When prompted, enter your user ID and password.
- 3 Start the NPM CLUI by typing

```
$ npm
```

and pressing the Enter key.

- 4 When prompted, enter your user ID and password.

Example response:

```
Entering shell mode: Enter 'npm' commands, help  
or quit to exit.
```

```
npm>
```

You have completed this procedure.