



Carrier VoIP

Nortel ATM/IP Solution-level Fault Management

Document status: Standard
Document version: 04.04
Document date: 20 October 2006

Copyright © 2006, Nortel Networks
All Rights Reserved.

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.

Nortel ATM/IP Solution-level Fault Management

New in this release

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

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.

(I)SN09U ATM/IP features

Feature descriptions
CS 2000 features ACD Call Recording Phase I (ATM, UA-IP, PT-IP, IAC, IAW, CHS, TDM) This feature provides trunk information in the ICM (Intelligent Call Management) protocol to facilitate call recording functionality in a TDM environment. UUI NI-2 PRI over SCAI (ATM, UA-IP, PT-IP, IAC, IAW, CHS, TDM) This feature provides PRI User-to-User Signalling (UUS) supplementary service which enables a user to send/receive a limited amount of information to/from another user. This information is passed transparently without modification of content through the network over the signalling channel in association with the call. MG 9000 features MG9K PKI development (UA-IP) This design feature addresses the reception, installation and use of digital certificate authenticate nodes attempting to establish an IPSec session. MG 9000 Manager features MG9KEM SN09.1 CPR robustness (UA-AAL1, UA-IP)

Feature descriptions

This feature is supported for MG9Ks with version SN091 and greater and will support all the types of NEs present in subnet (e.g. discovered and undiscovered). The following will be supported for this feature:

The craftsperson will be able to initiate an LCI session directly from the MG9K EM subnet screen for all the nodes.

The craftsperson will be able to launch a 'clear persist and discover' operation from the MG9K EM for all the nodes.

Geographic Survivability features

Compact Call Agent: GEO support for GIGE (PT-IP, UA-AAL1, UA-IP, IAW, IAC, intl IAW, intl IAC, intl PT-IP, intl UA-IP, CHS)

This feature enables synchronization of data between two Compact Call Agent (CCA) blades over a Gigabit Ethernet link. The current design uses Fiber Channel (FC) for keeping data synchronized. This feature will provide an additional option of synchronization over Gigabit Ethernet (GigE) depending on the customers' needs.

SPFS features

Disabling non-secure network services in SPFS

This activity provides some configuration tools to assist customer in configuring the server based on their security policy. Upon completion of the fresh system installation or upgrade, the customer (security administrator) has the possibility to apply the security policy on the server via a command line interface.

SDM/CBM features

Pass phrase protected keys for SSH (CHS)

This feature enhances the existing secure outbound file transfer functionality by introducing the key-based (public key) authentication.

The key-based authentication mechanism is provided as an additional option for the user. Hence, the user can select to use either the password-based or the key-based authentication while adding and changing the secure file transfer schedules in the SBA (billmtc) or OMDD (omui) user interface programs.

Session Server features

Enhanced Network Centrex and RES services (CHS)

This activity enables support of DISA service on SIP Lines.

Feature descriptions

Session Server Fault Handling Enhancements (CHS)

This activity extends the coverage of hardware faults handled by the Session Server NCGL Platform Manager software and thus increases the reliability of the Session Server platform. This activity involves the detection and reporting of hardware faults in the following areas:

- Power Supplies
- Fan Speeds
- System Temperature
- System Voltage
- Miscellaneous Hardware Elements

Fault management strategy

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

- ["Fault Delivery" \(page 5\)](#)
- ["Testing and Diagnostics" \(page 6\)](#)
- ["OSS interface" \(page 34\)](#)

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
- MG 9000 testing

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 which 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.

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.

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

Command	Description
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)

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.

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

Command	Description
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 1: Additional equipment is required.

Note 2: This is available for both TDM and DPT-SPM/MG 4000 trunk types

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

Note: Additional equipment is required.

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" \(page 198\)](#) 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.

DPT trunk testing with the DPT-SPM and MG 4000

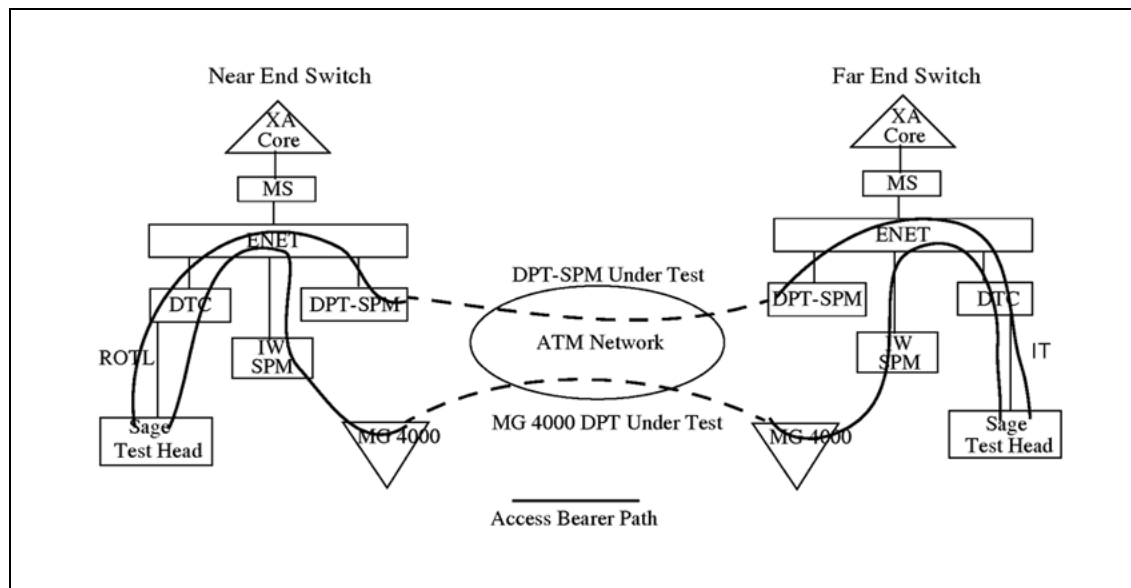
ATTENTION

This section applies only to the North American PT-AAL1.

Digital Remote Office Test Line (ROTL) is a DMS feature to remotely test trunks via a digital, four wire, E&M trunk. This CAS trunk interface permits a test head to be connected to the CS 2000 and, via a maintenance dial plan, select an outgoing trunk to be tested. A test head is connected to the CS 2000 by a T1, on which several channels are provisioned with a ROTL trunk type. Test calls can then be outpulsed from the test head over the ROTL trunk members using a defined maintenance dial plan which instructs the CS 2000 software to select an outgoing trunk circuit and generate a test call to the far-end switch. A connection is then established between the test equipment and the trunk circuit being tested. Once all connections have been made the test head conducts the desired trunk test.

The Digital ROTL functionality has been enhanced to permit test connections over DPTs hosted by an DPT-SPM or MG 4000. The customer can directly select the DPT group, node and TID to test.

The following figure illustrates the configuration of the Digital ROTL functionality on the DPT-SPM and MG 4000.



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

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

Both solutions offer the ability to conduct testing on Media Gateway (MG) TDM trunk circuits at the DS-0 level.

Developed for the PT-IP (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 trunk circuits. This solution takes advantage of the TDM to IP bridge capabilities of the IW-SPM, to provide connectivity between the MG TDM trunk under test and the test hardware located in the ISM.

Developed for the AAL2 (ATM) and AAL5 (PT-IP) switch configurations that do not contain an ENET or ISM, the solution utilizes the 3rd party test equipment 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 following list is not supported for MG PTS trunk circuits. The applicable Nortel documentation reference is provided for each MAPCI level.

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.

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

Command	Description
LOSS	Manually measures transmission loss

Command	Description
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)

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.

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

Command	Description
Bertime	Sets the length of time a BERT will run

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

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 trunk circuits via the MAPCI TTP level and ATT level interfaces. Trunk test functionality is provided by either the Media Server 2000 series products, MS 2010 (PT-IP [AAL5]) and MS 2020 (AAL2) or by the Universal Audio Server in conjunction with the

SAGE 945RTS test unit. Except for the MWTSwap command, the following list is not supported for MG PTS trunk circuits. The applicable Nortel documentation reference is provided for each MAPCI level.

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

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
MWTSwap	Permits the ability to send and receive a 1004 Hz test tone and measure transmission loss on the received test tone Note 1: Command supported on MS 2000 series only. Note 2: Command supported on ISUP and PTS ES/OP trunk types only.
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) • T904 (originating and terminating) Note: T105 termination on the MS 2000 series supports only the LSC, L, NSC, RN, N, and NT subtests.

Command	Description

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.

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.

Trunk testing with the UAS 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) from SN06 and for ATM (AAL2) from 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). **T105 termination on the MS 2000 series supports only the LSC, L, NSC, RN, N, and NT subtests.
- TL904 which provides two-way signal loss at 800 Hz. (International test trunk utilized in the Israeli telephone network.)
- MWTSwap, which permits the ability to send and receive a 1004 Hz test tone and measures transmission loss on the received 1004 Hz test tone.

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 from (I)SN06.2 and for ATM (AAL2) is the MS 2020 from (I)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 for SPM nodes 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

REX testing for the MG 9000 Routine Exercise (REX) of intelligent card pairs performs the diagnostics of the inactive card. During REX, the inactive card of a card pair will be diagnosed. Followed by the inactive card, REX is executed on the active card. This occurs after a SWACT is initiated on the active card, which now becomes inactive.

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

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

- REX on an NE can be scheduled for a particular day and time from the GUI or can be executed immediately. Scheduling of REX is similar to that of Audit.
- An option is provided to remove an NE for which REX is already scheduled. When removing the NE, if the REX is in progress, it would be suspended.
- User can suspend the already scheduled REX.
- User can resume the suspended REX.
- User can view the results/progress details of REX executed on the selected NE.

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

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:

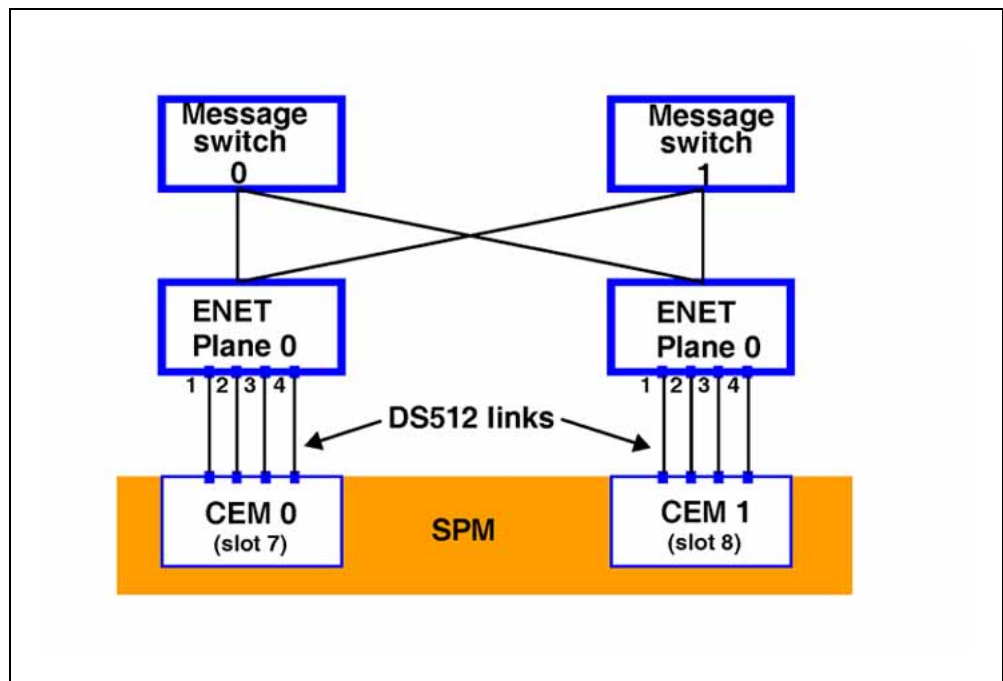
- Links from ENET plane 0 must terminate on CEM 0 (of the SPM) and links from ENET plane 1 must terminate on CEM 1.

- 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.

"Correct method of connecting DS512 links" (page 21) shows the correct way to connect DS512 links from the ENET to the CEM ports of an SPM.

Correct method of connecting DS512 links

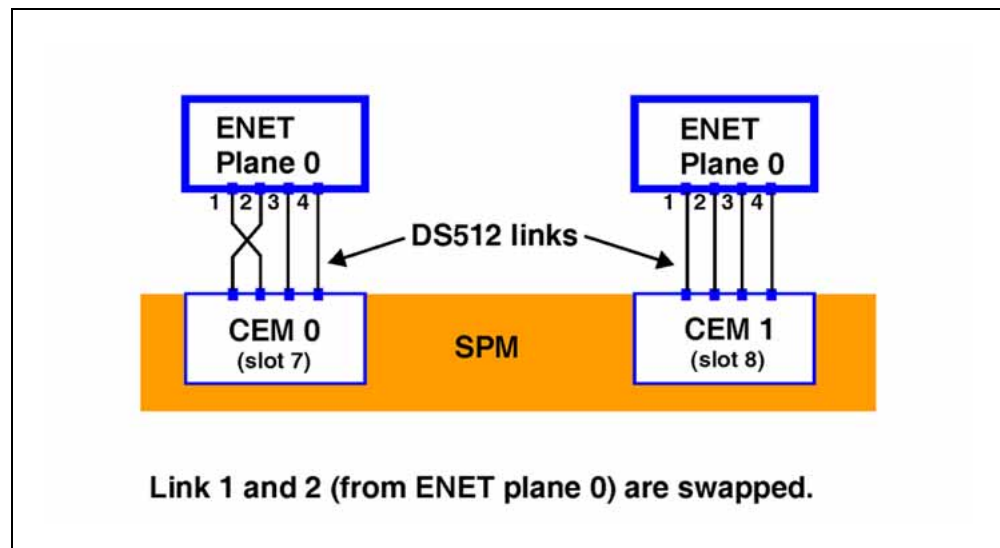


"Misconnection of DS512 links within a CEM" (page 22) shows an example of an improper method of connecting DS512 links from the ENET to the CEMs of an SPM. In this case, link 1 and 2, from ENET plane 0, to CEM 0 are swapped. Although this is an incorrect method of connecting DS512 links, in this example, 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 "Misconnection of DS512 links within a CEM" (page 22), 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.

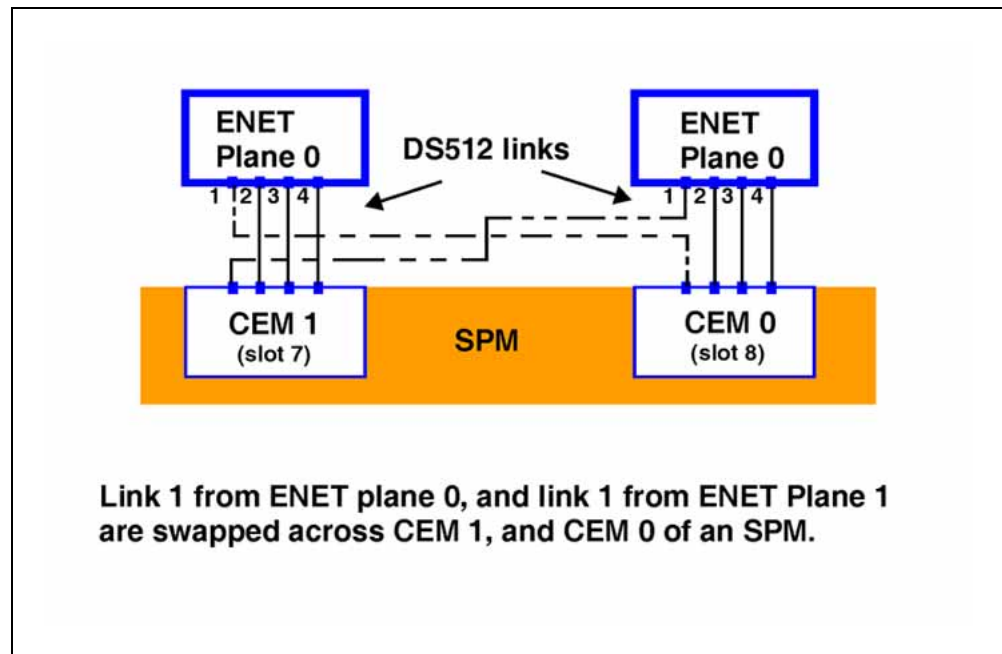
Misconnection of DS512 links within a CEM



"Misconnection of DS512 links across CEMs (software is swapped)" (page 23) 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.

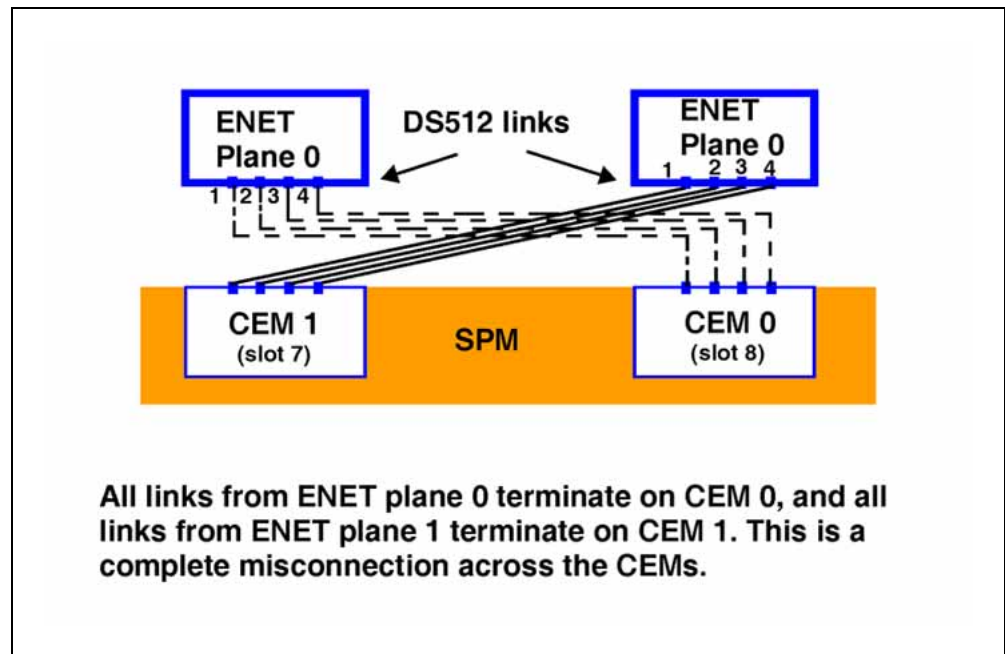
In the example in "Misconnection of DS512 links across CEMs (software is swapped)" (page 23), the misconnected link 1 from ENET plane 0, and ENET plane 1 (to the CEMs) remains in service. Links 2, 3, and 4 to CEM 0 and CEM 1 remain in-service. The MS ports associated with links 2, 3, and 4 are out-of-service. 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.

Misconnection of DS512 links across CEMs (software is swapped)

"Complete misconnection of DS512 links" (page 24) 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.

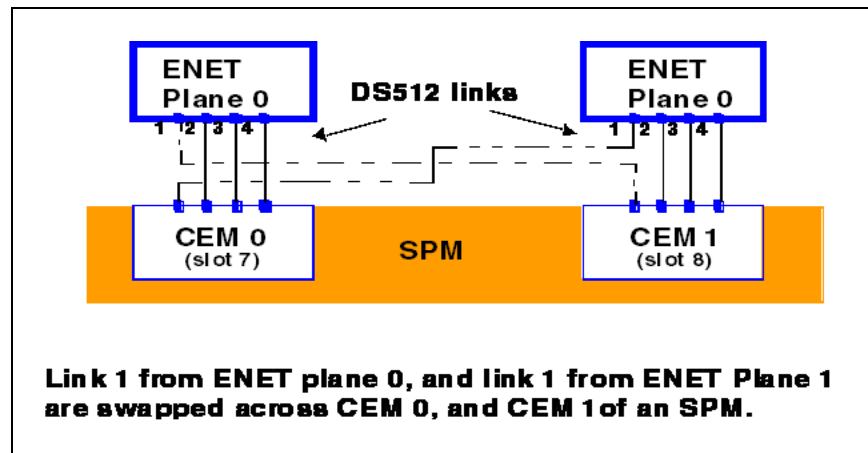
In this example in "Complete misconnection of DS512 links" (page 24), all four misconnected links from ENET plane 0 to CEM 1, and all four links from ENET plane 1 to CEM 0 remain in service. The MS port associated with each of the misconnected links remains in service. The system generates Link 300 logs for each link that is swapped and misconnected across the CEMs. The system does not generate a log when the fault clears.

Complete misconnection of DS512 links

"Misconnection of DS512 links across CEMs (software is not swapped)" (page 25) 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 "Misconnection of DS512 links across CEMs (software is not swapped)" (page 25), 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.

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.

"Connection paths" (page 25) lists the connection paths that you can troubleshoot using the Multiservice Switch/I.610 Loopback feature.

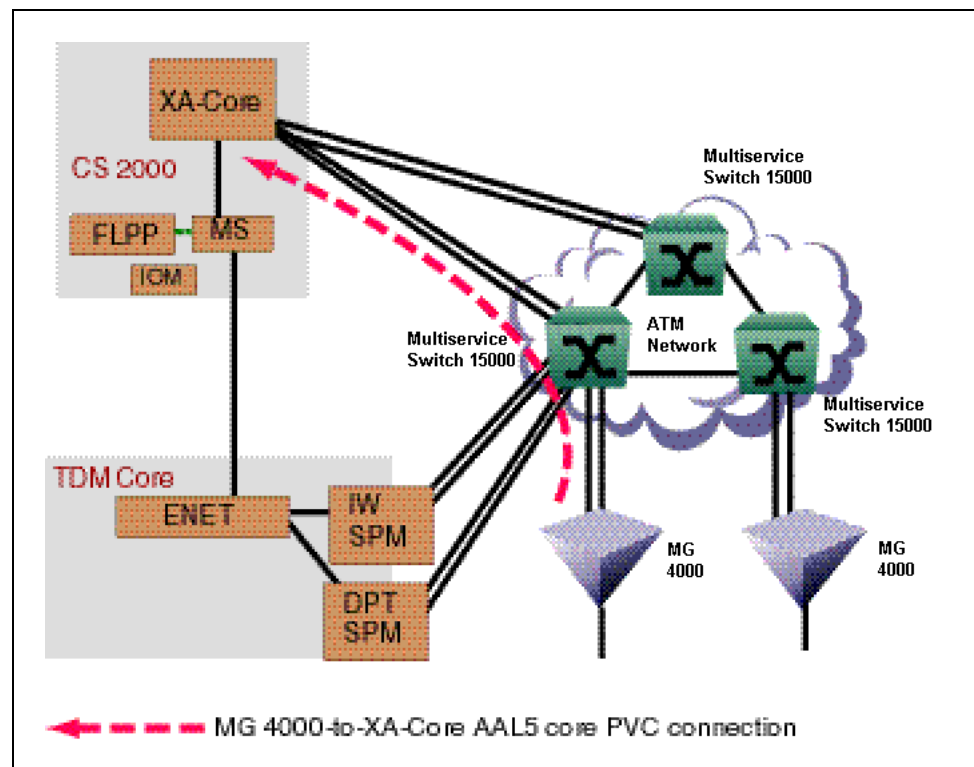
Connection paths

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

MAP level	Source of trace	Destination of trace	Signal Type	Circuit Type
ATMconn/BearConn	MG 4000	IW SPM	AAL1	SVC
ATMconn/BearConn	IW SPM	MG 4000	AAL1	SVC

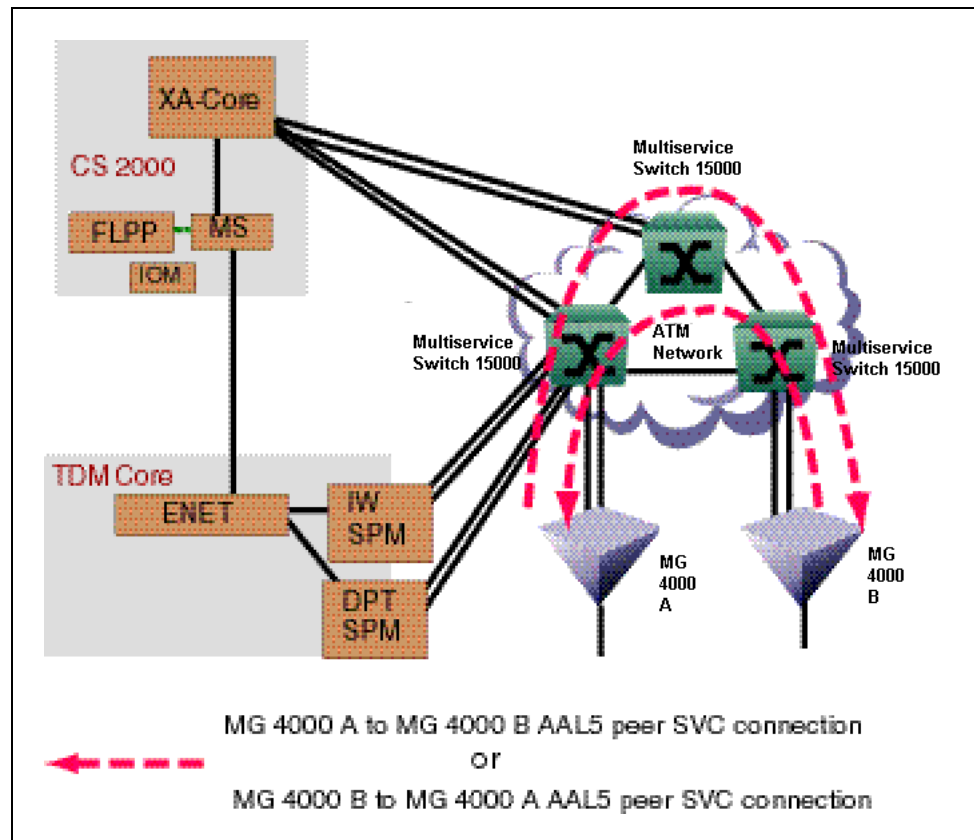
"MG 4000 to XA-Core connection" (page 26) shows an MG 4000 to XA-Core AAL5 PVC (permanent virtual circuit) messaging connection.

MG 4000 to XA-Core connection



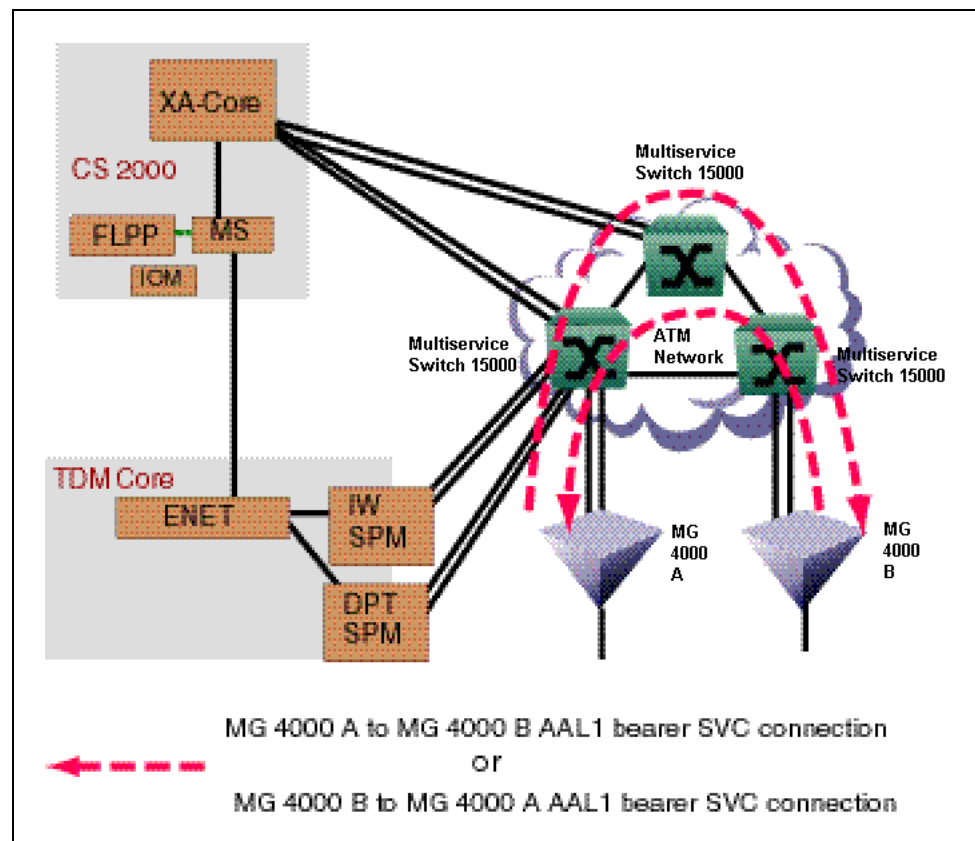
"MG 4000-to-MG 4000 peer AAL5 messaging connection" (page 27) shows a peer SVC AAL5 messaging connection between two MG 4000s.

MG 4000-to-MG 4000 peer AAL5 messaging connection



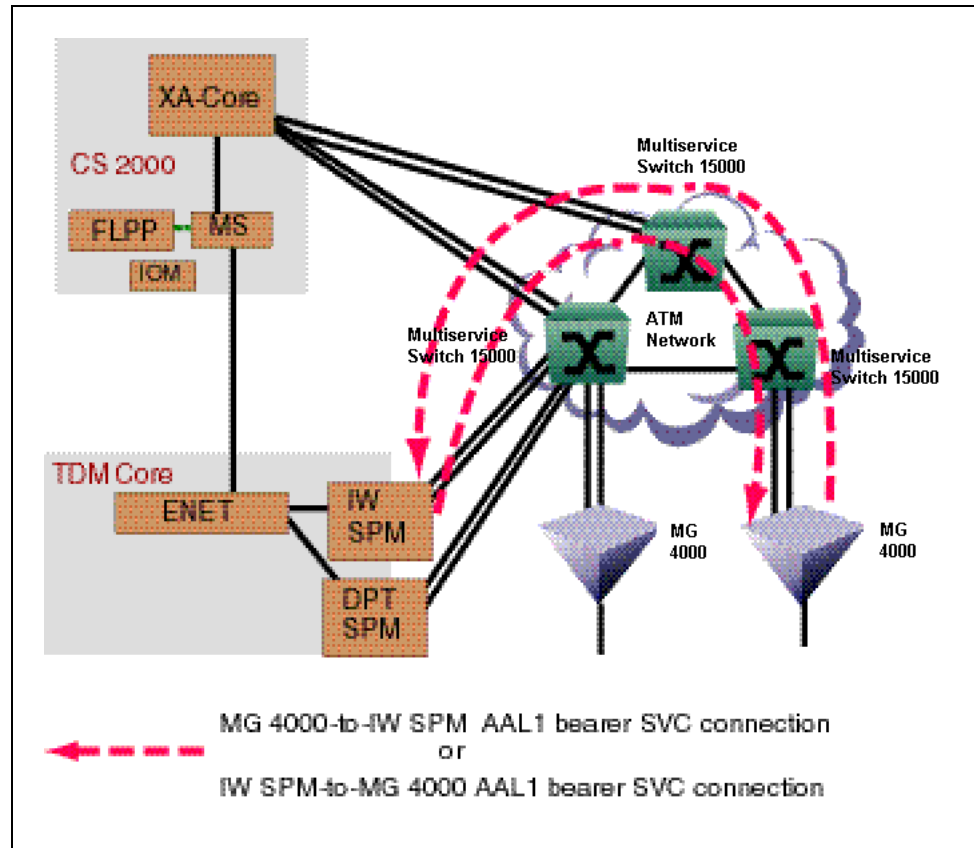
"MG 4000-to-MG 4000 AAL1 bearer connection" (page 28) shows an SVC AAL1 bearer connection between two MG 4000s.

MG 4000-to-MG 4000 AAL1 bearer connection



"MG 4000-to-IW SPM AAL1 bearer connection" (page 29) shows an SVC AAL1 bearer connection between an MG 4000 and an IW SPM.

MG 4000-to-IW SPM AAL1 bearer connection



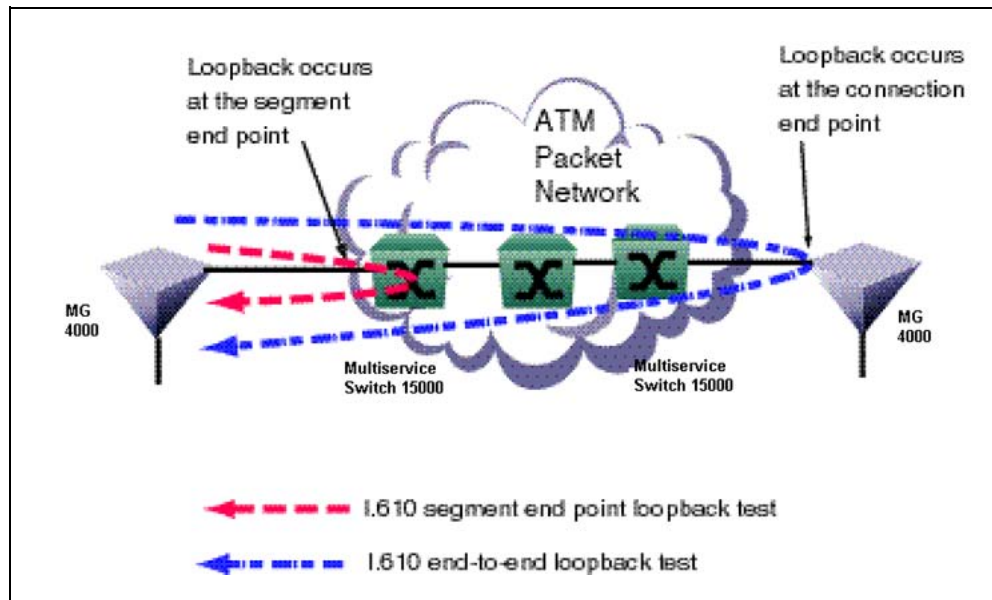
The Multiservice Switch/I.610 Loopback feature displays the results of both proprietary and standards-based ATM loopback queries. The four types of queries are as follows:

- 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)

"[I.610 end-to-end loopback test and, I.610 segment end point loopback test](#)" (page 30) 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

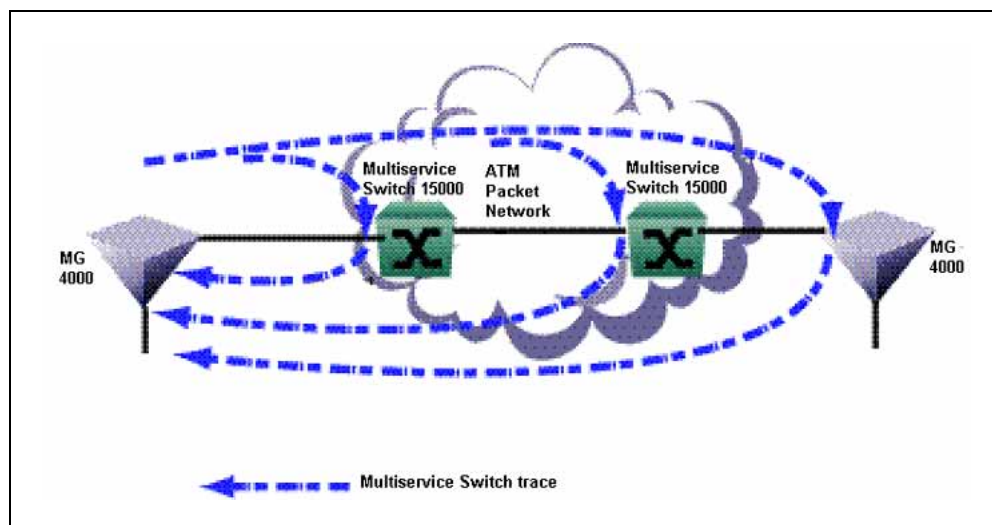
segment-end-point. In "i.610 end-to-end loopback test and, I.610 segment end point loopback test" (page 30), the end points are shown as MG 4000s and the ATM switches as Multiservice Switch 15000s.

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



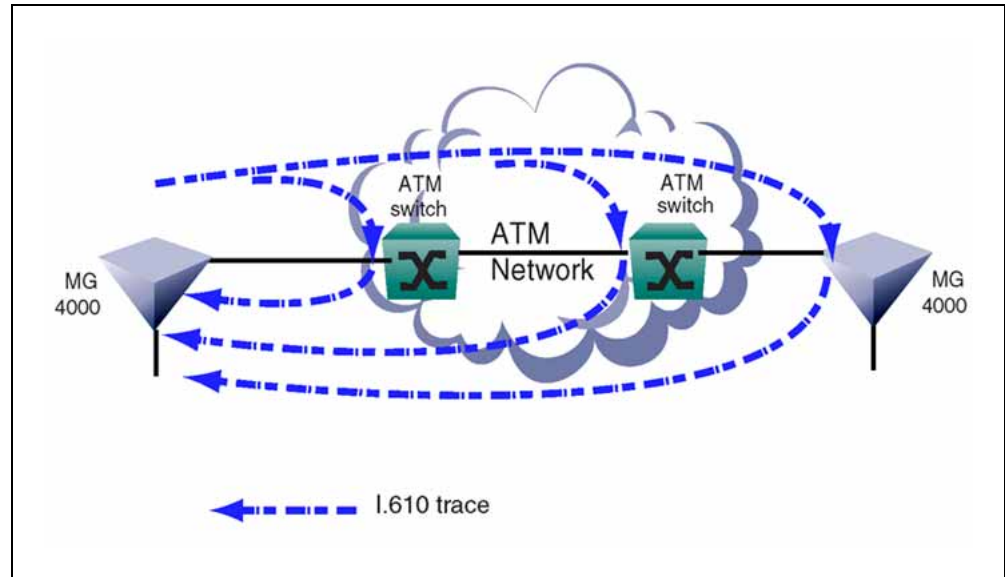
"Multiservice Switch trace" (page 30) shows an example of the Multiservice Switch trace. You would only use the Multiservice Switch trace on Multiservice Switch 15000 ATM switches. During the trace, the system software forwards a loopback cell from one Multiservice Switch 15000 to the next. Each Multiservice 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.

Multiservice Switch trace



"I.610 trace" (page 31) 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 (in other words, ATM switches that are not Multiservice Switch 15000s).

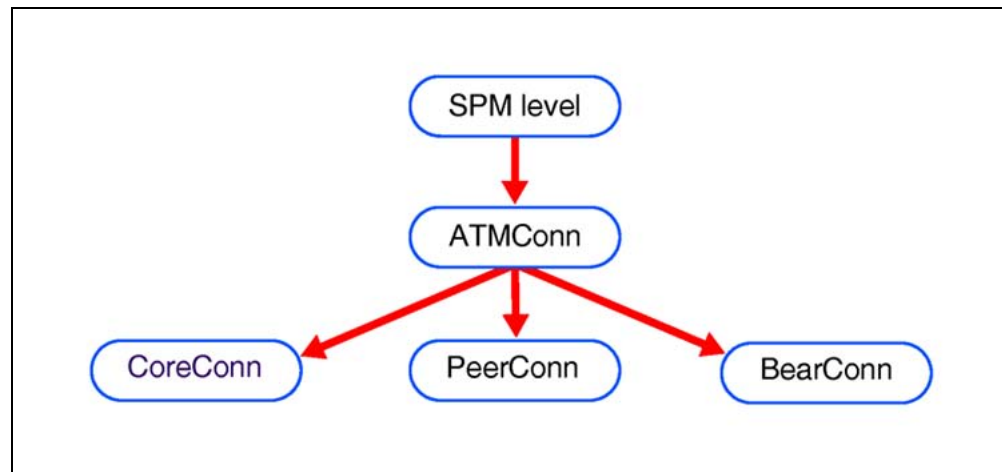
I.610 trace



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.

"MAPCI levels used for Multiservice Switch/I.610 Loopback feature" (page 32) shows the MAPCI hierarchy for the ATMConn directory.

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 Spectrum Peripheral Module (SPM) 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 Switched Virtual Circuit (SVC) 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*, NN10076-911 on this disk. To perform a Multiservice Switch/I.610 Loopback test or trace that originates from a IW SPM, see *IW SPM-ATM Fault Management*, NN10077-911.

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.

MAP-based MG 9000 testing

MAP-based line testing for the MG 9000 is supported on Intl UA-IP solutions. It uses the legacy DMS MTM/ISM hardware or RMM hardware for remote sites and software along with the MG 9000 Line Test System to perform MG 9000 line testing from the Maintenance and Administration Position (MAP) terminal.

MG 9000 native lines in the central office are tested by using MTM/ISM hardware. MG 9000 native lines in the remote side are tested by using RMM hardware.

ABI lines are tested using MTM/ISM hardware in the Central office. ABI lines in the remote site are tested using RMM hardware. To test ABI lines, the Core sends the MAP-based line test request to the Gateway Control (GWC). The GWC encapsulates this test request into an H.248 package and sends the gateway of the MG 9000. the MG 9000 receives the MAP-based line test request from H.248 package and then sends it to the LGC. After testing, test results are sent to Core with same route.

OSS interface

Fault aggregation can be performed by the IEMS. 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, SPFS 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, SPFS Platform, UAS, APS, and MG 9000.

Note: The CS 2000 Core Manager also supports alarm reporting. See ["Alarm Reporting" \(page 45\)](#)

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 (IEMS)
- 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 (IEMS)
- 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 (IEMS)
- 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 (IEMS)
- 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 (IEMS)
- 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 (IEMS)
- 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 (IEMS)
- 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

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

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

The IEMS 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 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 IEMS. The alarms have one of the following severities:

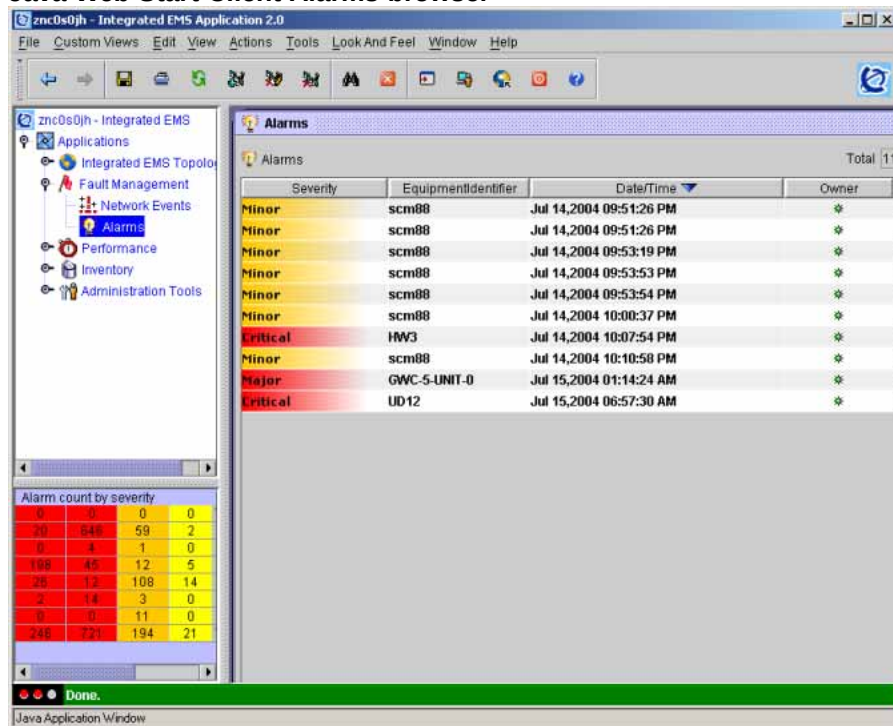
- Critical
- Major
- Minor
- Warning

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
Orange	Major
Yellow	Minor
Light Yellow	Warning

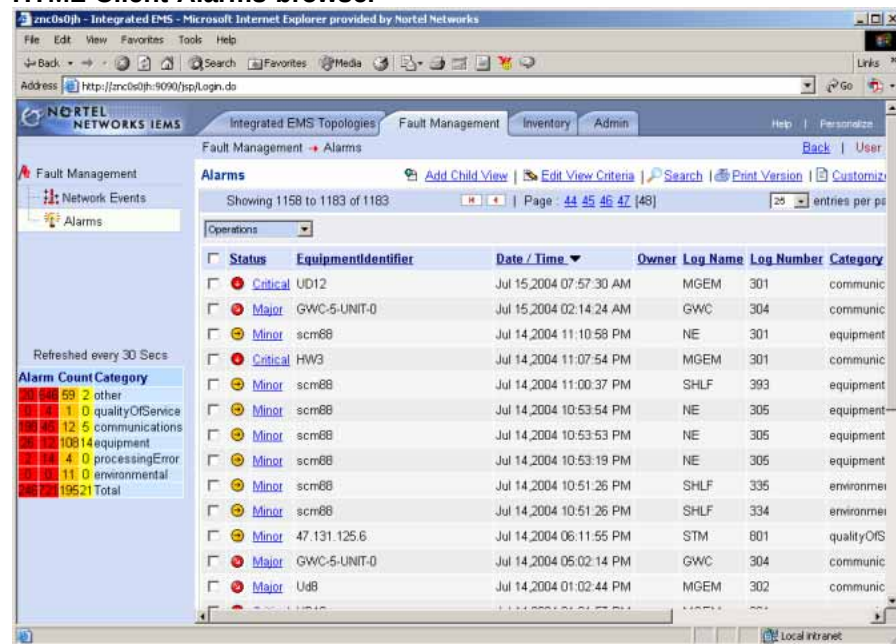
To access the Java Web Start Client Alarms browser, select the Alarms node (sub-node of Fault Management) in the IEMS tree. The following figure illustrates the Java Web Start Client Alarms browser.

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.

HTML Client Alarms browser



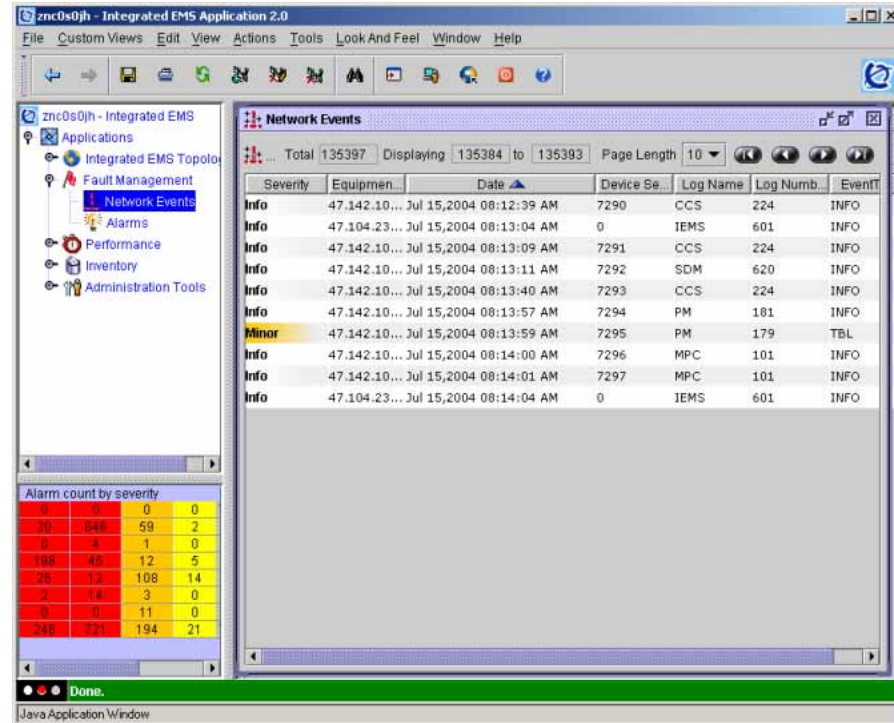
For additional information, refer to *IEMS Fault Management*, NN10334-911.

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

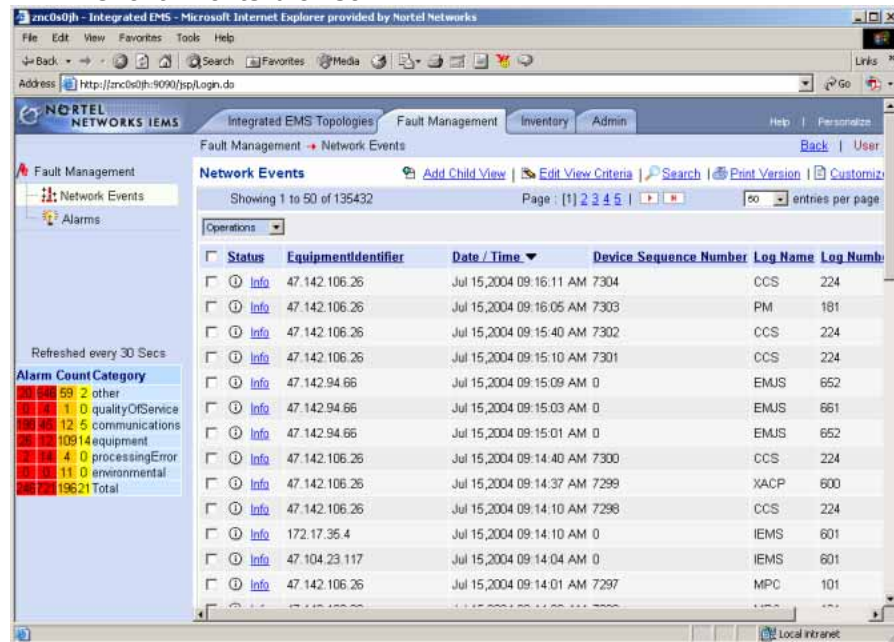
The IEMS event browser provides a consolidated historical and real-time view of the events that have occurred in a CS 2000 central office. Event browser is a tool to view the events from the Nortel EMSs, NEs, platforms, and applications in a common GUI. The event browser serves as a key tool that enables 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 IEMS tree. The following figure illustrates the Java Web Start Client Event browser.

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.

HTML Client Events browser

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

Configuring Northbound fault feeds

The IEMS 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 IEMS 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 office.

For additional information, refer to *IEMS 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

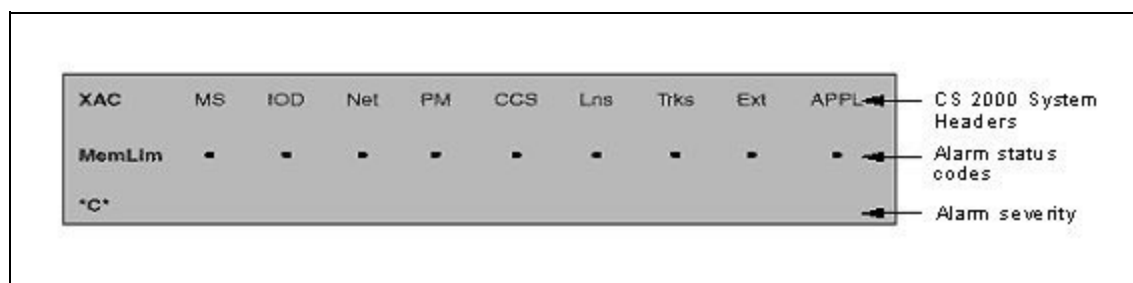
company personnel clears the alarm condition. The alarm system includes audible notification and visual display through warning lights and the MAP terminal.

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 ["MAP alarm banner" \(page 46\)](#).

MAP alarm banner



For information on the alarm banner, refer to ["MAP alarm banner summary field" \(page 46\)](#).

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 ["Alarm severity conditions" \(page 47\)](#).

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.
"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 ["XA-Core MAP subsystem and status summary field" \(page 47\)](#).

XA-Core MAP subsystem and status summary field

SM	FE	IO	PKLT	
.	.	.	.	Subsystem headers
0	0	0	0	Hardware Alarm codes
				OOS CP / Packet count

["MAP subsystem and status summary field" \(page 47\)](#) 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.

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.

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

"Log with SCC2 header format" (page 49) 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).

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
	SM	SYSB	HOST 01	A00	DPCC:00	00 07F

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

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.

"ATM300 log with SCC2 header format" (page 50) 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.

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
  
```

"Comparison of an ATM log with and without enhanced text" (page 51) shows the ATM300 log in both NT Standard and SCC2 log formats. In addition "Comparison of an ATM log with and without enhanced text" (page 51) 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 "Comparison

of an ATM log with and without enhanced text" (page 51)). 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.

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

"CCMT501 log with SCC2 header format" (page 52) 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, IWBMM, and SPM logs, the location and type field and the fabric field (see arrow 2) only appears in the (I)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 (I)SN06 or later display the location and type fields by default, regardless of the value of SPM_ENHANCED_OUTPUT.

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

```

"Comparison of an ATM log with and without enhanced text" (page 51) shows the CCMT501 log in both NT Standard and SCC2 log formats. In addition "Comparison of an ATM log with and without enhanced text" (page 51) 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 "Comparison of an ATM log with and without enhanced text" (page 51)). 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.

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

Log Format		Two variations of the CCMT501 log
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

"SPM-related logs that have the optional location and type fields" (page 53) 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).

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

Log number	Description
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
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

Log number	Description
SPM301	Clock Range
SPM310	Suspend Echo Canceller 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
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

Log number	Description
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 the following:

- *MG 4000 Operational Configuration*, NN10098-511
- *IW SPM (ATM) Operational Configuration*, NN10099-511
- *IW SPM (IP) Operational Configuration*, NN10100-511,
- *DPT SPM (ATM) Operational Configuration*, NN10102-511

For additional information on the Enhanced Logs feature, see *the following*:

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

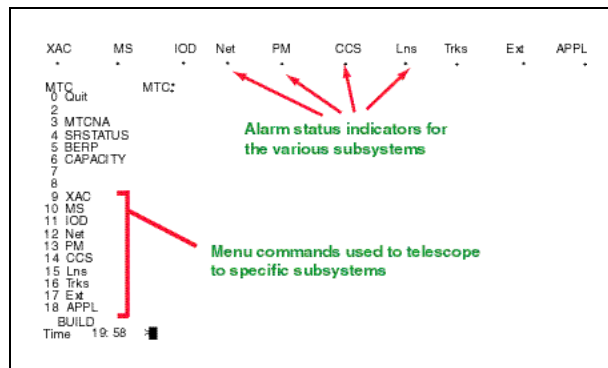
Logging in to the Map and accessing the maintenance level

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.

After logging in to the maintenance level of the MAP, the alarm status indicators along the top status area will be seen (see "[Example screen showing the maintenance level of the MAP](#)" (page 57)). 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 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.

Example screen showing the maintenance level of the MAP



Navigating to the appropriate subsystem of the MAP

"Example MAP display of the XAC subsystem" (page 58) shows an example of the MAP maintenance level for the XAC subsystem and "Example MAP display of the PM subsystem" (page 58) 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 ATM 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 "DPTRKS level of MAPCI" (page 59). 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 to 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, 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.

A list of alarms can be displayed at the PM level of the MAP by using the ListAlm (list alarms) and Disp_ (display alarms) commands. Current logs can be viewed 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.

Example MAP display of the XAC subsystem

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
XAC									
0 Quit		Front : 111111111		Rear : 111111	SM	PE	IO	PKLT	
2 Card		123456789012345678		456789012345		0	0	0	
3 XAC/Mtc	Sta								
4 SM	Dep								
5 PE	XAC:								
6 IO									
7 CMIC									
8 RTIF									
9 Disk									
10 Tape									
11 AMDI									
12 ETHR									
13									
14 Alarm									
15									
16									
17 Indicat_									
18 Query_									
BUILD									
Time 20:04									

System status information
that is specific to the XAC subsystem

"Example MAP display of the PM subsystem" (page 58) shows an example of the MAP maintenance level for the PM (peripheral module) subsystem.

Example MAP display of the PM subsystem

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
PM									
0 Quit		PM		SysB	ManB	OffL	CBey	ISTB	InSv
2 Post_	POST:			0	0	0	0	0	24
3	PM:								
4 SCAITCP									
5									
6									
7									
8									
9									
10									
11 Disp_									
12									
13 Status									
14 IPML									
15 PES									
16 FMT									
17									
18									
BUILD									
Time 19:58									

System status information that is
specific to 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

"DPTRKS level of MAPCI" (page 59).) In "DPTRKS level of MAPCI" (page 59), 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 Configuration Management*, 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.

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		CKT	TYPE	COM	LANG	STATE	RANGE		
2 Post_		2W	ISP	DPTEANLOOP		INSV	30 000		32046
3									
4									
5 BSY_		IDL:	0						
6 RTS_		CPB:	0						
7 OP		MTC:	2046						
8 FRLS		PV:	0	FE BLK:	2046	FE UNEQ:	0		
9 Rese_		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 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, 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 DMS (digital multiplex system) switch running a CVoIP (I)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 Configuration Management*, NN10201-511.

Assuming the far-end switch is a DMS running (I)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

The erase flash (ERASEFL) command can be used 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, refer to the following component documentation:

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

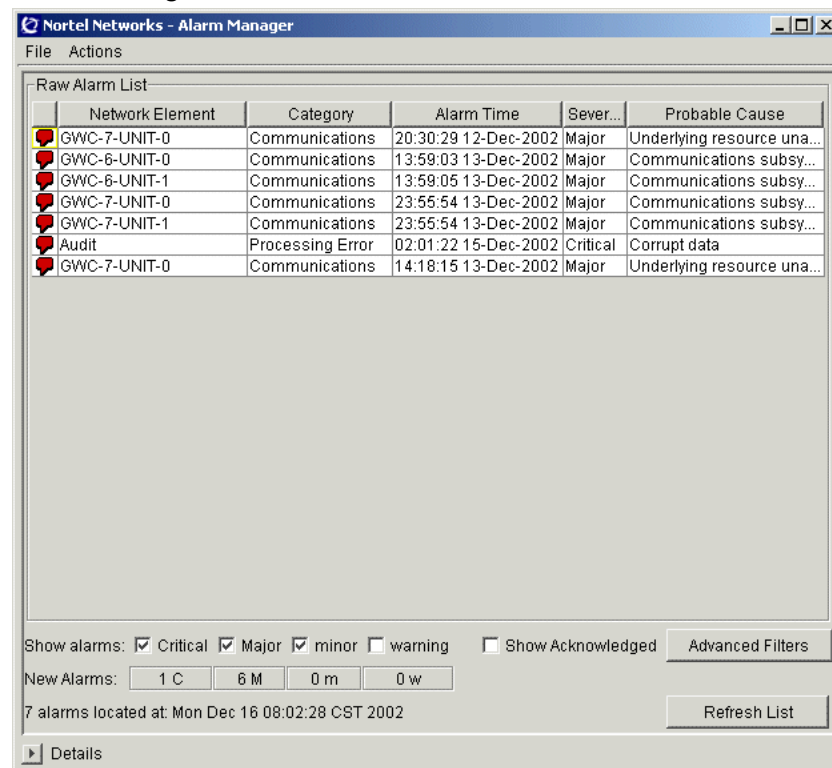
The user can view the alarms and the status of hardware components through the CS 2000 Gateway Controller Manager which also supports the following activities:

- 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. ["Alarm Manager without details" \(page 66\)](#) shows the Alarm Manager without details.

Alarm Manager without details



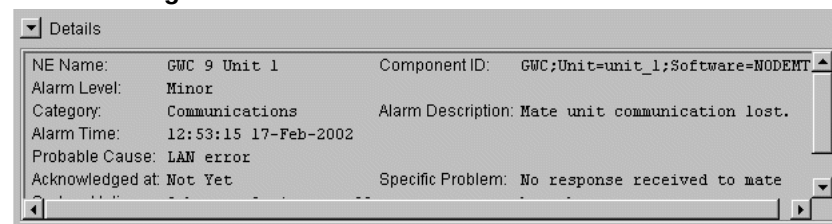
After the browser pops up, the user has the ability to filter for severity and acknowledgement state. Alarms are displayed in the center alarm table panel. The headers for the center alarm table panel are Network Element Name, Alarm Level, Category, Alarm Time, Probable Cause, Acknowledge Time, System 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. "[Alarm Manager details](#)" (page 67) shows the Details panel of the Alarm Manager window.

Alarm Manager details



The screenshot shows a window titled "Details" with a scrollable area containing the following information:

NE Name:	GWC 9 Unit 1	Component ID:	GWC;Unit=unit_1;Software=NODEMT
Alarm Level:	Minor		
Category:	Communications	Alarm Description:	Mate unit communication lost.
Alarm Time:	12:53:15 17-Feb-2002		
Probable Cause:	LAN error		
Acknowledged at:	Not Yet	Specific Problem:	No response received to mate

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. "[Alarm History without details](#)" (page 68) shows the alarm history without details.

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" \(page 65\)](#).

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.

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.

Session Server logs web page

The Customer Logs panel does not update automatically! Datestamp of last update: Friday April 30th 2004 01:10:13 PM EST	
Customer Logs	
Apr 29 11:06:51 loopback alarmd: XTS391 MINOR INIT Array Rebuilding	NCGL=localhost; Array: 'dev/md1' (ntvg) Status: The array is currently being rebuilt.
Apr 29 06:08:38 sp2k-2 alarmd: XTS336 CRIT FLT Network Connectivity NCGL=sp2k-2;Unit=1 Link0: INSV, mateCon: AVAIL, netCon: UNAVAIL; Link1: INSV, mateCon: AVAIL, netCon: UNAVAIL; PTPLink: INSV, mateCon: AVAIL;	
Apr 29 11:08:39 sp2k-2 logman: XTS655 NONE INFO Release Jam on Inactive unit Unit Number : 1, UNDETERMINED Description : Inactive not JAMMED	
Apr 29 11:08:39 sp2k-2 logman: XTS651 NONE INFO Mate Communication Restored Unit Number : 1, UNDETERMINED Description : Mate unit is available.	
Apr 29 11:08:39 sp2k-2 logman: XTS601 NONE INFO CPU Alarm Cleared Unit Number : 1, UNDETERMINED Description : 1 minute load average is less than 10.00; no threshold reached.	
Apr 29 11:08:39 sp2k-2 logman: XTS600 NONE INFO Memory Alarm Cleared Unit Number : 1, UNDETERMINED Description : Available memory is greater than the minor threshold value of 150MB	
Apr 29 11:08:40 sp2k-2 logman: XTS602 NONE INFO Disk Alarm Cleared Unit Number : 1, UNDETERMINED Description : Percentage of root free disk space is greater than 15.00.	
Apr 29 11:08:40 sp2k-2 logman: XTS603 NONE INFO Zombie Process Alarm Cleared Unit Number : 1, UNDETERMINED Description : Zombie process is not running.	

Note: The body of log formats shown in this document are the formats for Session Server logs if viewed from the IEMS. 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"](#) (page 65).

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 IEMS system in the network. The MS 2000 server must be added to IEMS 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 IEMS 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.

APS alarm fields

Field	Description
severity	warning, minor, major, or critical

Field	Description
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 SPFS-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.

"Default state to color mapping" (page 77) shows default state to color mapping.

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

"Default alarm severity to color mapping" (page 77) shows default alarm severity to color mapping.

Default alarm severity to color mapping

Alarm Severity	State
Unknown	Light blue
Warning	Dark blue
Minor	Yellow

Alarm Severity	State
Major	Orange
Critical	Reg

Network status bar The MDM tool provides a high-level view of all network element alarms in the network ("MDM Network Status bar" (page 78)). 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

MDM Network Status bar



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.

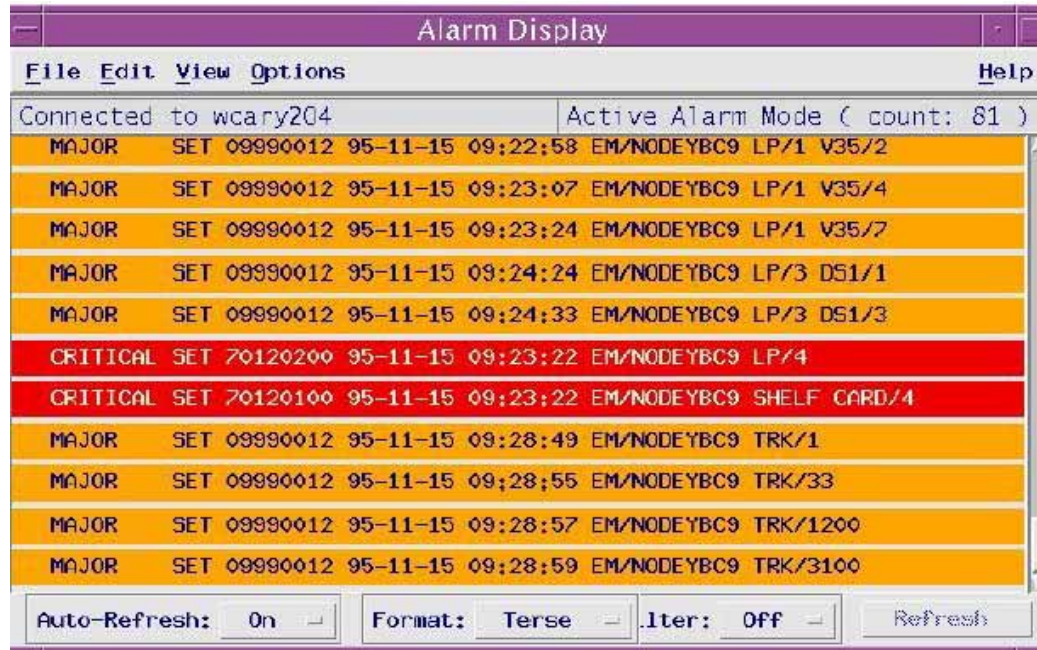
Short-term Historical Alarm Reporting provides the ability to query old alarms and supports the following various search criteria:

- 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. ["Query results from Short-term Historical Alarm Reporting" \(page 80\)](#) shows the Historical Alarm reporting tool.

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 ("[MDM Alarm Display](#)" (page 81)). 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).

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

"Example of a Multiservice Switch/Media Gateway SCC2 alarm log" (page 82) 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.

Example of a Multiservice Switch/Media Gateway SCC2 alarm log

```

*C35 P15K025 4790 TBL arIfProbableCause.42 Lp/5 Sonet/2
managedObjectInstance: 1030:MDMFmRmMoa, 1028:EM/P15KE, 11004:Lp/5 Sonet/2
notificationID: 67109941
perceivedSeverity: Critical
logRecordID:
CLFI:
eventTime:20010306153519Z
eventType: 5002
equipmentType:
managedObjectClass: 11004
NETypeID: 138
specificProblems: 70115202
probableCause: arIfProbableCause.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 (xAlsAlarm).

```

Determining a Multiservice Switch/Media Gateway log

"Example SCC2 log identifying Multiservice Switch 15000/Media Gateway 15000 major alarm" (page 83) shows an example of an SCC2 log. In "Example SCC2 log identifying Multiservice Switch 15000/Media Gateway 15000 major alarm" (page 83), 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

Also note (in "Example SCC2 log identifying Multiservice Switch 15000/Media Gateway 15000 major alarm" (page 83)) the value of the managedObjectInstance field which is EM/15K COL/LOG SP/\$ (see field 2), the NetTypeID which is 138 (see field 3) and the specificProblems code which is 70030002 (shown in field 4).

If the log name, on the SCC2 log, does not match one of the two Multiservice Switch/Media Gateway log names, then the log is not a Multiservice Switch/Media Gateway log and must be a log associated with the CS 2000 Core Manager, CS 2000, MG 4000, or IW SPM.

Example SCC2 log identifying Multiservice Switch 15000/Media Gateway 15000 major alarm

```

1234567890123456789012345678901234567890123456789012345678901234567890
1  **54 F15X162 0002 TBL arfProbableCause.17 SP/$
2  managedObjectInstance: 1038:EM/15X.1038:COL/LOG,1038:SP/$
3  notificationID: 49
4  perceivedSeverity: Major
5  logRecordID: 4
6  CLFI:
7  eventTime: 20010111005410Z
8  eventType: 5010
9  equipmentType:
10 managedObjectClass: 1004
11 NETypeID: 138
12 specificProblem: 70030002
13 probableCause: arfProbableCause.17
14 correlatedNotifications:
15 trendIndication:
16 thresholdInfo:
17 activeStatus: TRUE
18 unknownStatus: FALSE
19 alarmDisplayInfo: SubcomponentID=COL/LOG SP,NEUserLabel=EM/15X,NENumbe
19a r=138
20 vendorSpecificInfo:
21 technologySpecificInfo:
22 additionalText: Probable Cause: fileError - Received notification that t
    he file system is not available. Spooling is stopped.

```

Logging in to the MDM and accessing the Component Information Viewer

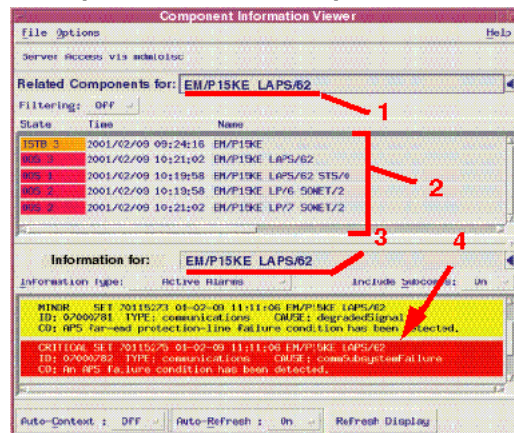
After logging in to the MDM, launch the Component Information Viewer tool from the MDM Toolset (see ["Example view of the Component Information Viewer"](#) (page 84)). Then, input the network element information (EM/P15E LP/5 Sonet/2) from the SCC2 log into the field called Related Components for (see field 1). As a result of this action the related components will be displayed in field 2.

Next, input EM/P15E LP/5 Sonet/2 into the Information For field (see field 3 in ["Example view of the Component Information Viewer"](#) (page 84)) to obtain a list of alarms for this component. Select the required alarm (choose the highest priority first) from the list (see field 4) and right click the mouse to launch the Alarm Help utility in the Web browser.

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 Fault Management Tools*, 241-6001-011.

Example view of the Component Information Viewer

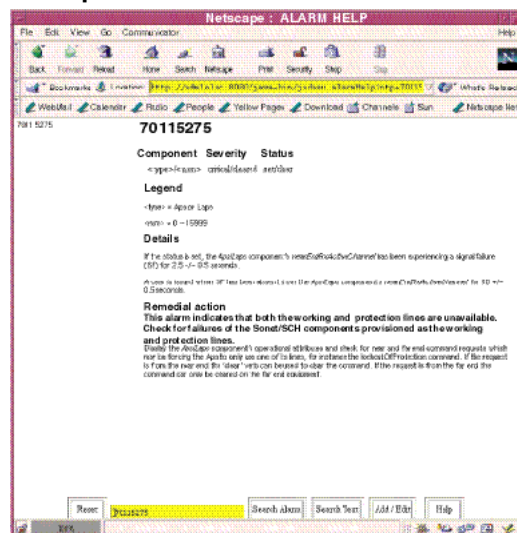


Obtaining remedial action for a Multiservice Switch alarm

The Alarm Help utility can be used to obtain specific information for Multiservice Switch alarms (see "Example alarm information from the Alarm Help utility" (page 84)). 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 "Example alarm information from the Alarm Help utility" (page 84) does not relate to the SCC2 alarm log shown earlier.

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. The MDM Advisor

Performance Viewer tool is used 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 the 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 to be examined. 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: Multiservice Switch 15000 fault management tasks can only be carried out using MDM tools. Multiservice Switch 15000 fault management tasks cannot be carried out through the OSS interface.

Note 2: For more information on these Multiservice Switch 15000 tests, see *MSS 15000*, *MG 15000* & *MDM Basics (PT-AAL1/UA-AAL1/UA-IP)*, NN10028-111.

Multiservice Switch 15000 Control processor test This test is performed following a control processor fault or failure using the MDM Advisor Command Console. 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 These diagnostics are used following control processor disk fault or failure, and use the MDM Advisor Command Console. Disk tests verify the integrity of the disk. Test a disk only when a fault is suspected in the disk hardware. The disk cannot be tested on the active control processor. If the disk to be tested is currently active, switch control between the active and the standby control processors.

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

Multiservice Switch 15000 function processor lock and unlock Perform this test prior to replacing a function processor using the MDM Advisor Command Console.

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

Multiservice Switch 15000 function processor loopback port test 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 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. Use remote tests to verify the full length of the transmission facility.

Manual loopback port test 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 the operator 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

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 (ERS 8600) through a Graphical User Interface (GUI). Configurations on the ERS 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 ERS 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, RMON alarms can be set that relate to specific events or variables simply by selecting these variables from a drop-down menu. 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
 - 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 ERS 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
 - 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
 - Use port mirroring to specify a destination port on which mirrored traffic can be seen 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. 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 and can only be used when consulting with Nortel support personnel.
- Enabling the system log

- 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
 - Use the system log-messaging feature of the ERS to manage switch event messages on any UNIX-based management platform. The ERS 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 ["Call Agent Manager MAPCI" \(page 90\)](#).

Call Agent Manager MAPCI

	IOD	CCS	Lns	Trks	APPL
	.	.	.	.	.
CAPACITY					
0 Quit	CATMP/HR	CCOVRID	IDLE		
2 Parm	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 "[STORM Manager Alarm Screen](#)" (page 91).

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 "STORM Manager Log Screen" (page 91).

STORM Manager Log Screen

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

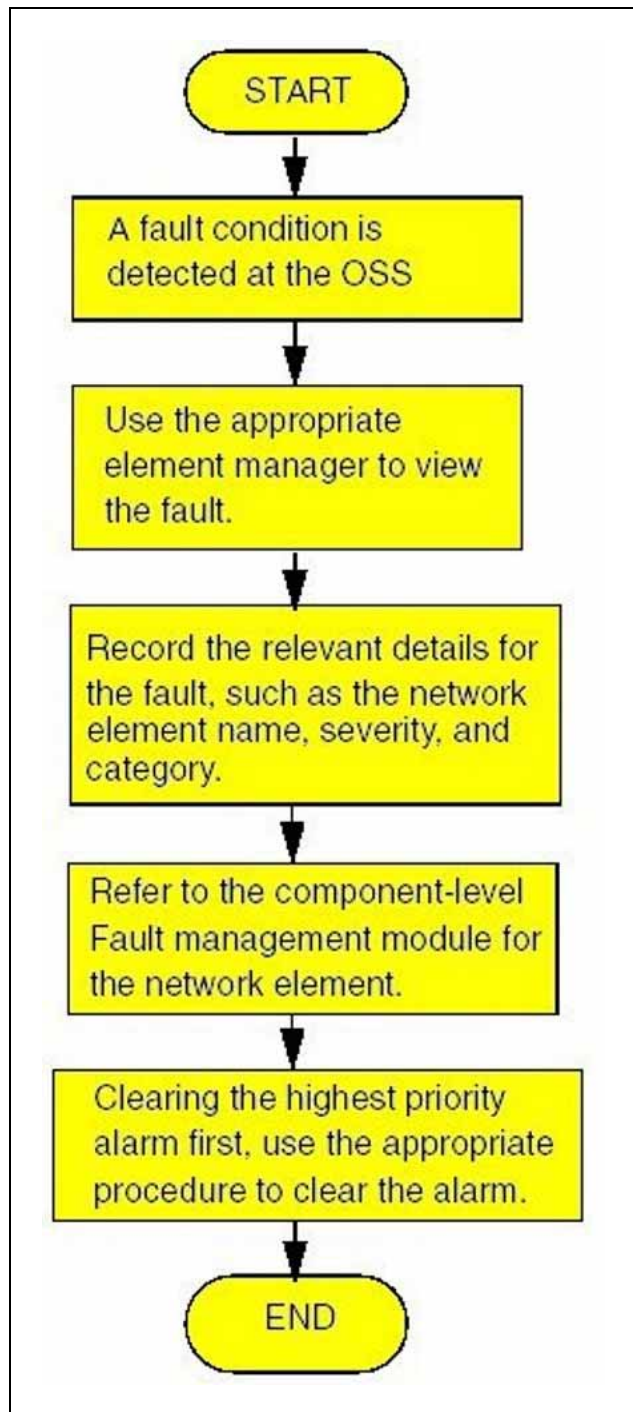
For information on HP OpenView, refer to the ORCA BTX-Series Software Manual or the BTX System Overview.

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). ["Fault Management task flow" \(page 93\)](#) displays this sequence of actions in the form of a flow chart.

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

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.

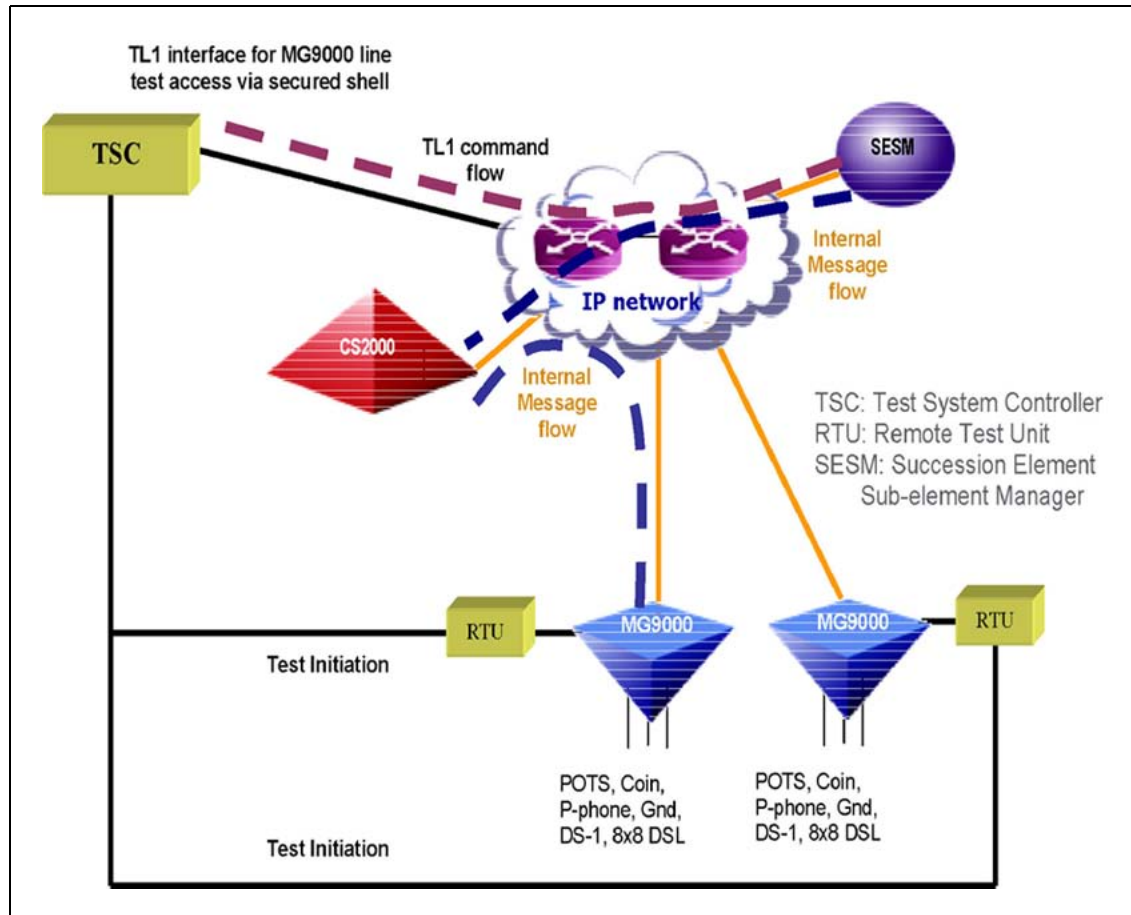
TL1 line test interface for MG 9000 lines

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 must be obtained by the third party line test controller vendor to implement the TL1 interface. Contact your Nortel 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

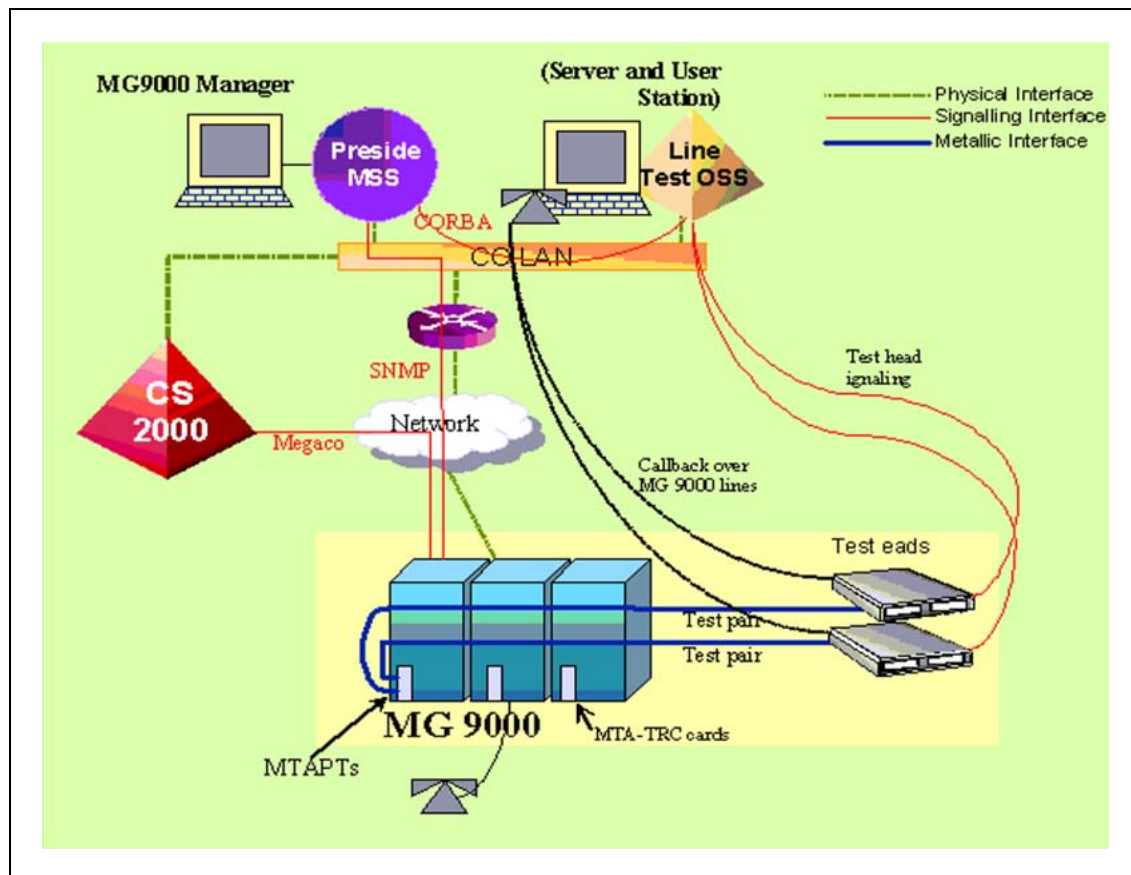
Metallic access through a network interface

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](#)" (page 102) figure. The line and loop test features provided by this configuration are dependent on the vendor.



- **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 the desired state. Internally to the call server, there is a messaging interface between XACore and the GWC.
- **MG 9000 Manager and MG 9000** - The MG 9000 Manager generates SNMP transactions for MTAPT provisioning. This must be done using

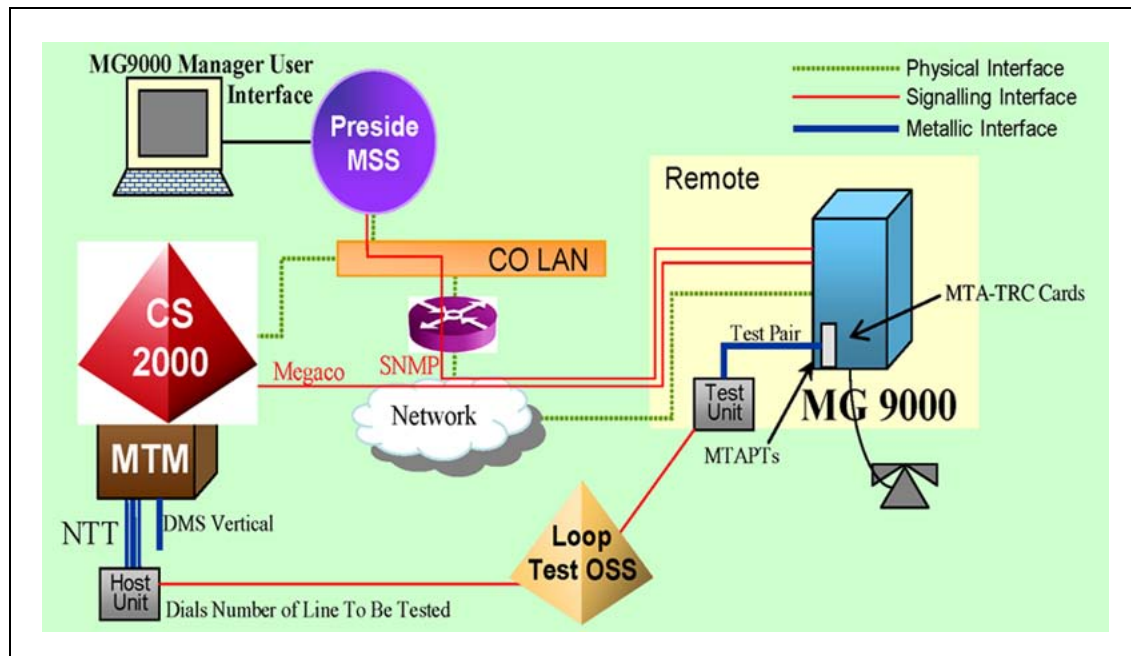
the MTAPT Provisioning screen, to indicate which MTAPTs have been connected to a DMS-100 Vertical or to a test head.

MTAPT provisioning data is written to the MG 9000 on startup if needed, and when there are modifications to the line test configuration.

How a loop test over NTT works

NTT test heads depend on DMS-100 legacy line test equipment. The test head initiates a loop connection by seizing the NTT trunk. When the CS 2000 acknowledges, the test head dials the directory number of the line to be tested. Please refer to the following figure.

System view, NTT support, split connect and test



The XA Core recognizes that the number belongs to an MG 9000 line. It uses provisioning data in tables LGRPINV and MTAVERT to determine how to set up a connection to the MG 9000, and which 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.

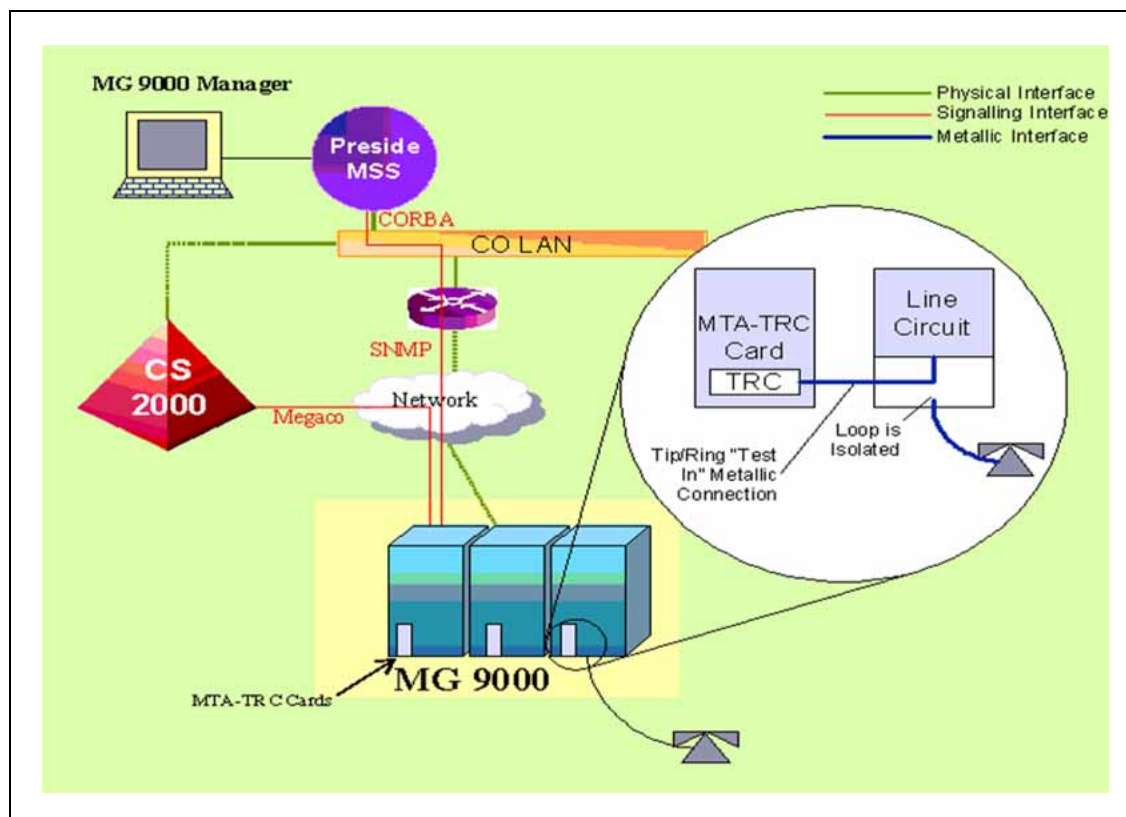
The end result is a tip/ring metallic connection from the test head's NTT trunk to the loop. The connection traverses NTT, through the NT2X90 card to a DMS-100 horizontal, which is connected through an NT3X09 card to a vertical which corresponds to an MG 9000 MTAPT. From here, it is routed through the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

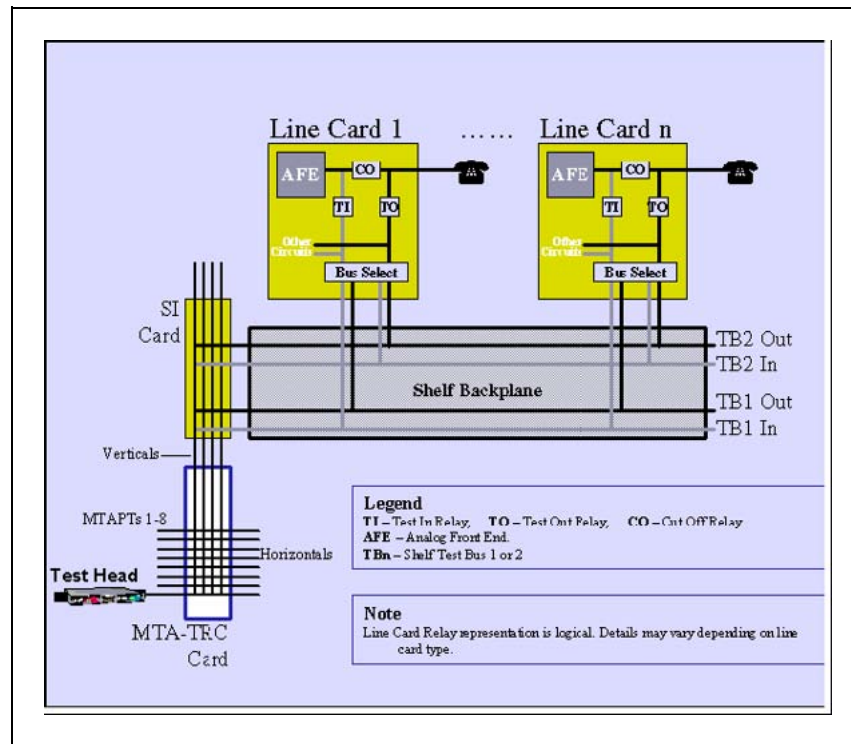
MG 9000 hardware components and configurations

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

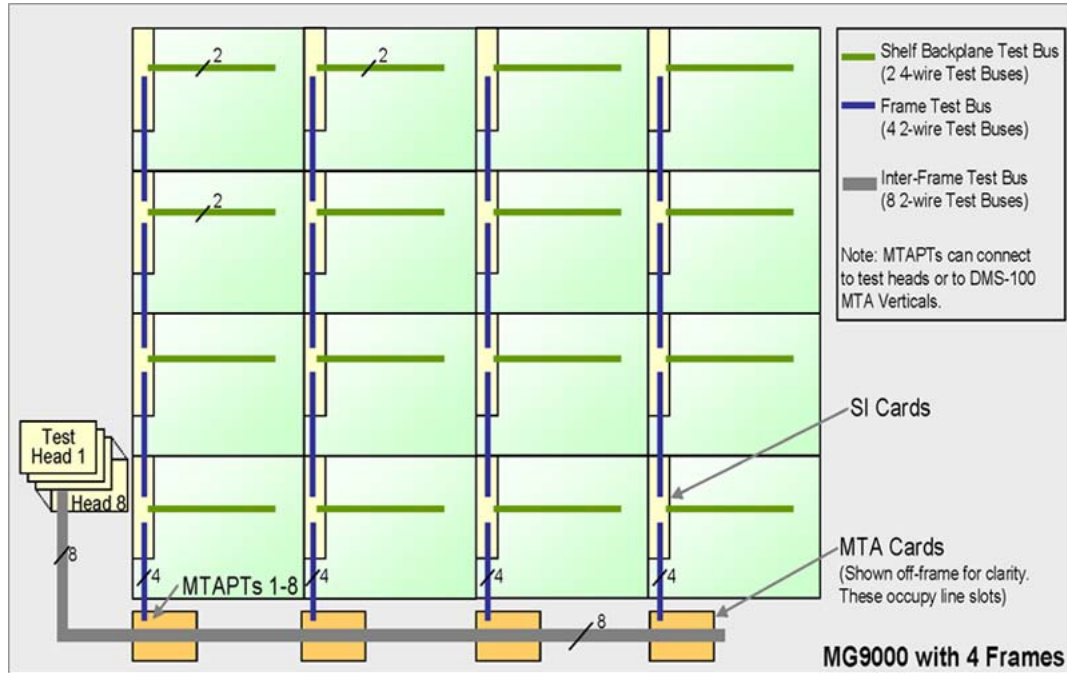
The MG 9000 components providing metallic connections are described in this section. Refer to the following figure.

MG 9000 metallic test access components

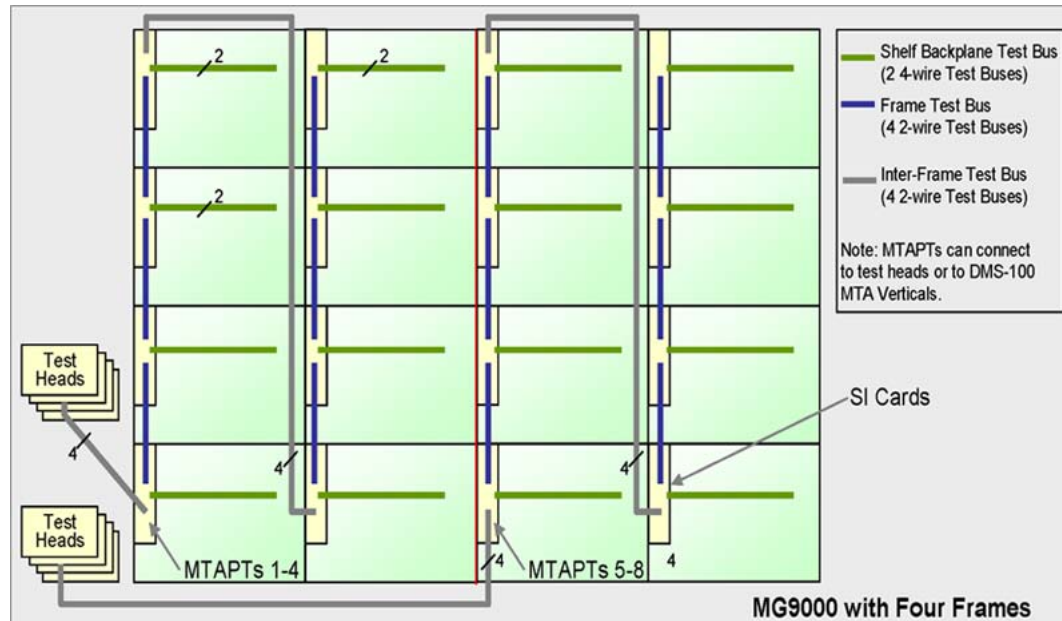


- MG 9000 nodes with MTA-TRC cards (typical) - Each MTA-TRC card has a metallic relay matrix that can connect eight tip/ring horizontals to four tip/ring verticals. Verticals are connected to the SIC card for shelf access. The eight possible MTAPTs (metallic test access points) for test head connections 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](#)" (page 107). 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 bar 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" \(page 109\)](#) have been followed, and that all MTA-TRC cards are on line and unlocked.

With the answers to the questions in ["Provisioning MTAPTs" \(page 110\)](#) 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" \(page 110\)](#) 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

Step	Action

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.

—End—

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	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.
No Ringing		Line is PLO or IDL	Perform the "General line testing - loop test" (page 112)
		Line is out of service (such as SB, LMB).	Perform the "General line testing - loop test" (page 112)
Phone rings, but can't receive calls	Perform the Loop Test in "General line testing - loop test" (page 112)		
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

Step	Action						
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.						
	<table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>the loop test passes</td><td>Perform the line circuit test</td></tr> <tr> <td>the loop test fails</td><td>Perform the "General line testing - customer premise equipment test" (page 113)</td></tr> </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" (page 113)
If	Do						
the loop test passes	Perform the line circuit test						
the loop test fails	Perform the "General line testing - customer premise equipment test" (page 113)						
3	This procedure is complete.						
—End—							

General line testing - customer premise equipment test

Step	Action

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.

—End—

General line testing - line equipment test

Step	Action

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" (page 114)

- 3 This procedure is complete.

—End—

General line testing - line circuit test**Step Action****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" (page 114)

- 3 This procedure is complete.

—End—

General line testing - line card default diagnostic**Step Action****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" (page 115)
the circuit passes (EBS)	Perform the "Next level debugging, generic - perform a continuous loop test" (page 119)

- 3 This procedure is complete.

—End—

General line testing - service verification test

Step	Action

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" (page 118)
the circuit passes but a dial tone problem is revealed	Perform the "Next level debugging, generic - perform a continuous loop test" (page 119)
the circuit passes but another problem is revealed	Return to symptom "Problem not solved" line in "Line circuit troubleshooting guide" (page 112)

- 3 This procedure is complete.

—End—

Speech test - speech test

Step	Action

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" (page 116)

- 4 This procedure is complete.

—End—

Speech test - subscriber premise equipment test

Step Action

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" (page 116)

- 3 This procedure is complete.

—End—

Speech test - check the last phone

Step Action

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 " (page 117)

- 3 This procedure is complete.

—End—

Speech test - check the transmission equipment

Step Action

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 " (page 118)
PCM or Packet Component Alarms or failures are present	Dispatch MG 9000 repair and retest.

- 4 This procedure is complete.

—End—

Speech test - check the network**Step Action*****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" (page 119)
transmission alarms or failures are observed	Dispatch network repair and retest.

- 3 This procedure is complete.

—End—

Next level debugging, ringing problem on POTS and Coin lines - check subscriber phone**Step Action*****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" (page 119)

- 3 This procedure is complete.

—End—

Next level debugging, generic - perform a continuous loop test

Step Action

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.

—End—

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.

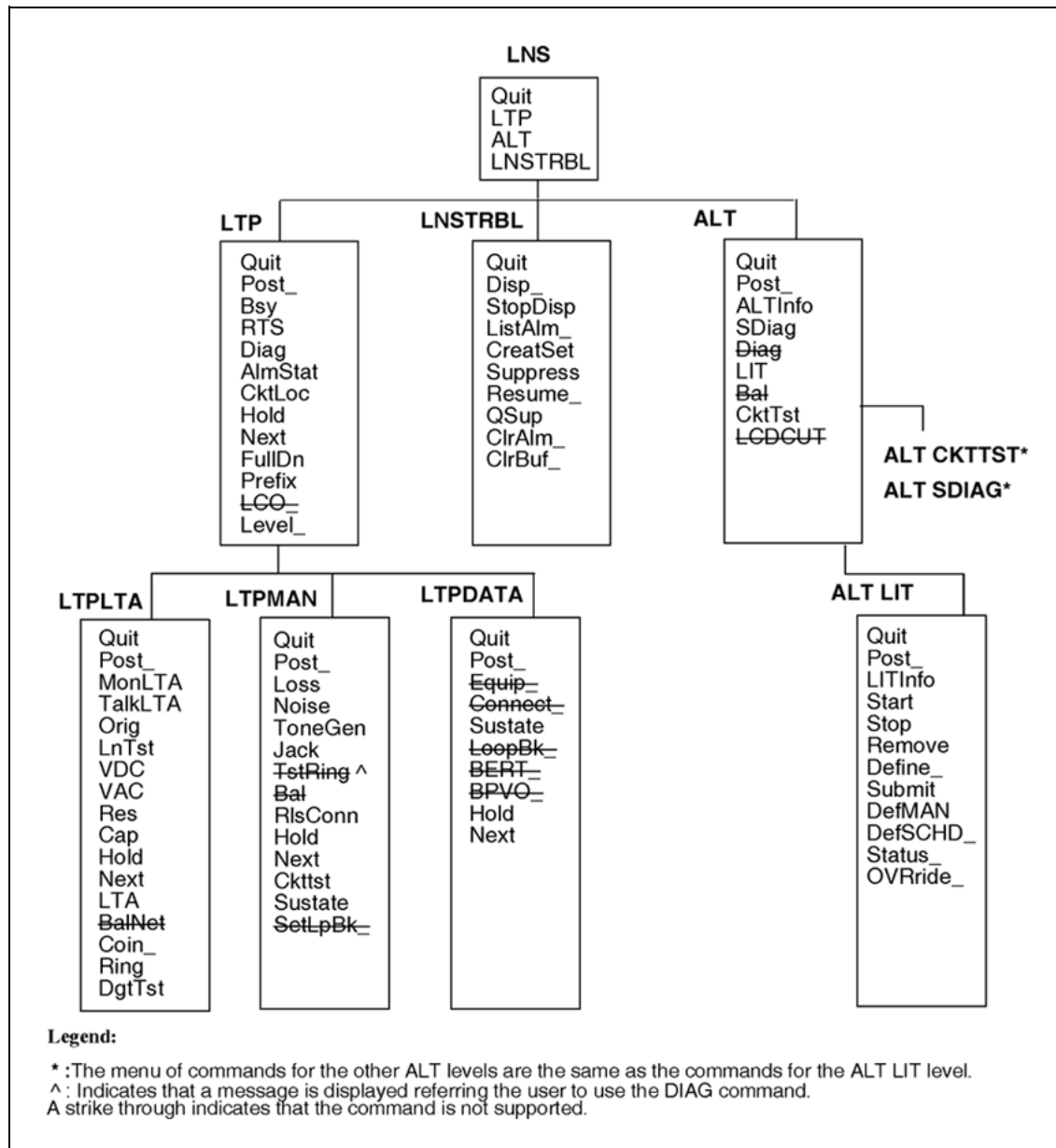
The following figure lists the line maintenance commands and their respective levels that support native MG 9000 lines. The unsupported commands are indicated by a strikethrough. The legend in the figure provides additional clarification.

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, RDTCON, or RDTEBS lines.

Line maintenance commands



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 Ô00' for the Floor and ÔA00' for the Row position. The Bay ID consists of frame type, which is displayed as ÔMG9F' and the frame number. LEN information stored in table LNINV is also displayed.
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

Command	Description
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
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	Uses a metallic loop
	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.	
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

Command	Description	Metallic and non-metallic information
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	Uses a metallic loop
	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.	
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

Command	Description	Metallic and non-metallic information
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
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.	
RIConn	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

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
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)

Command	Description
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)

Command	Description
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.
DefSCHD_	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.

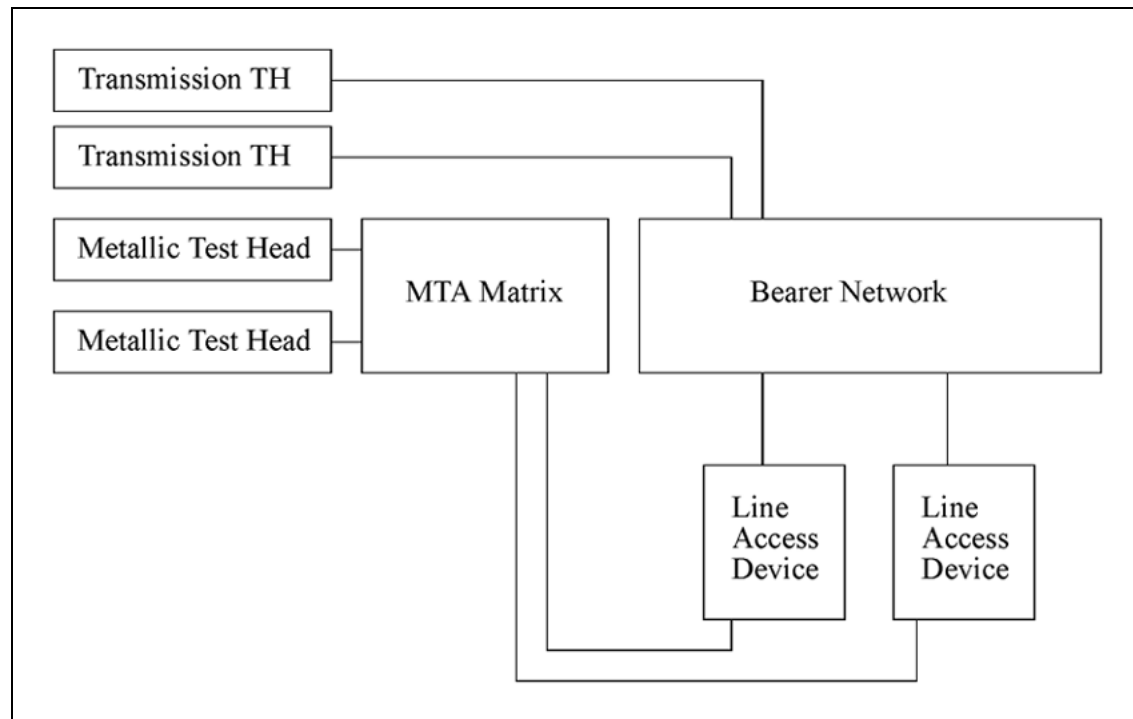
Test configurations

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](#)" (page 130), the transmission test heads have access to the bearer network. The test heads are connected to the line access devices through the bearer network.

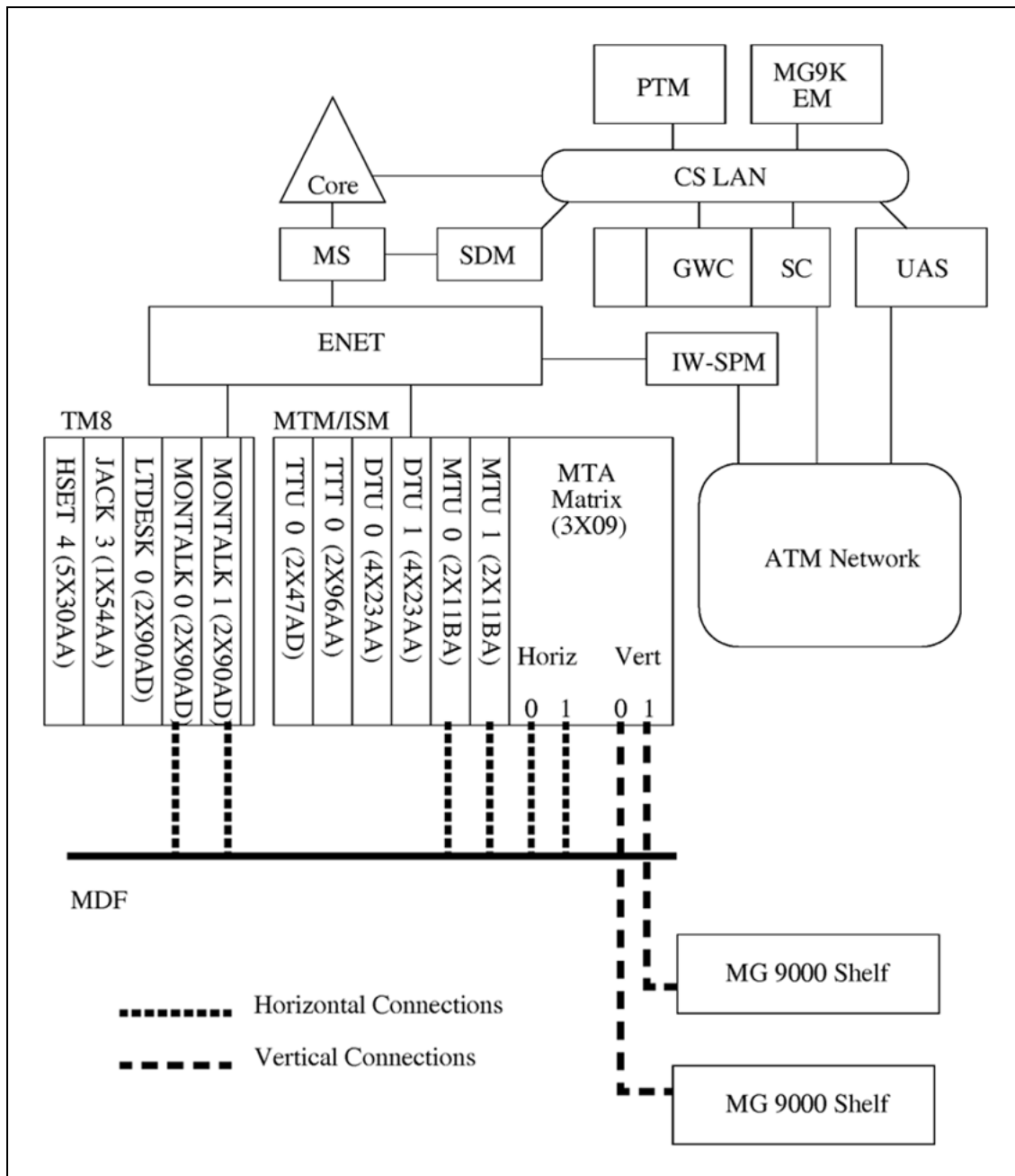
The metallic test heads are connected to horizontal leads on the MTA matrix. The line access devices are connected to the vertical leads on the MTA matrix. In this configuration, any metallic test head can be cross-connected to any line on any line access device.

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 LGRPOPTS

CARY 77 1 GWC 5 S (MTSTAPT CARY (0 1) \$)\$

CARY 40 2 GWC 5 S (MTSTAPT CARY (1 1) \$)\$

TABLE: MTAVERT

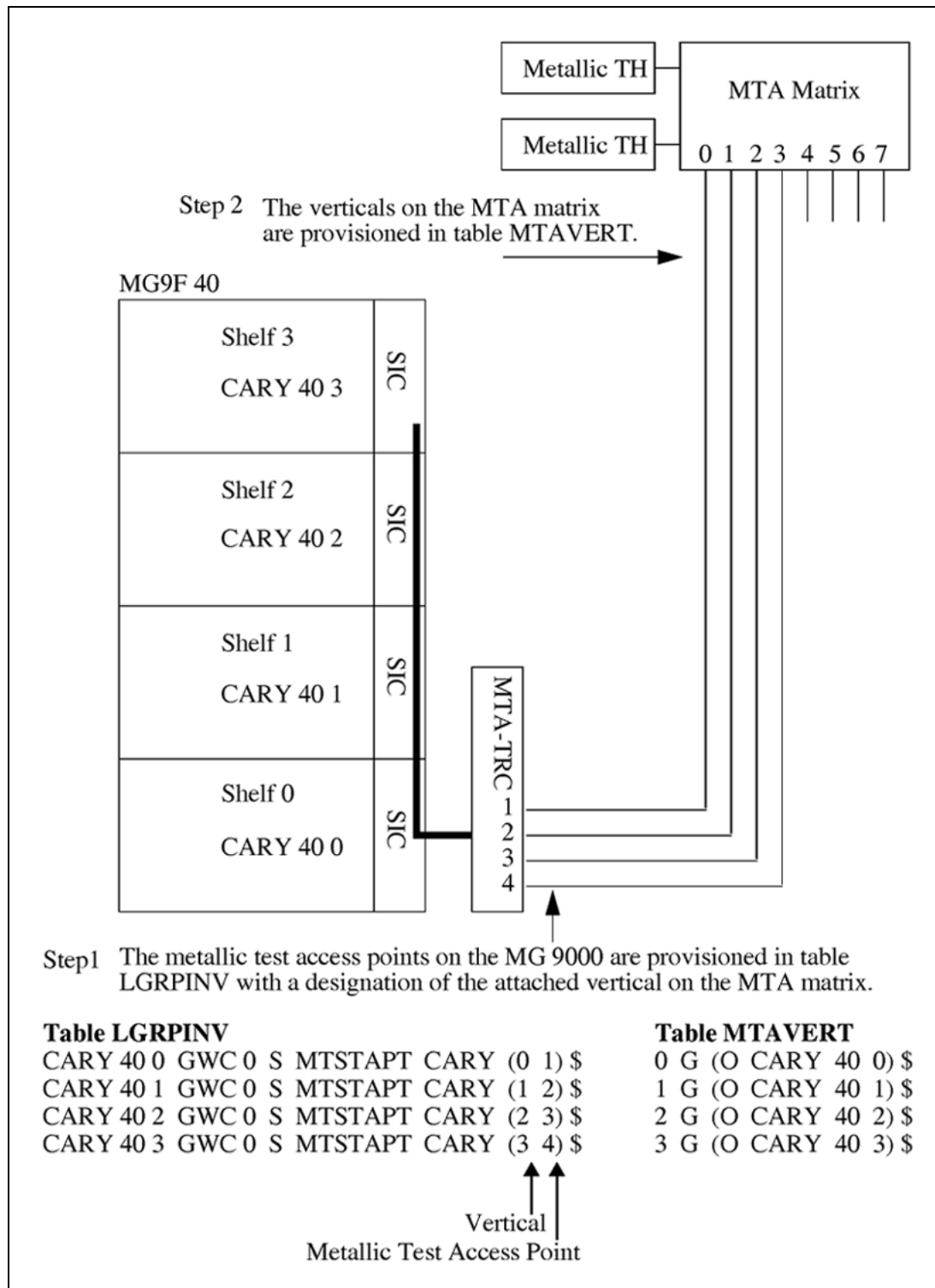
VERT VERTCONN

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 MTAVERTTable MTAVERT



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 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 (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
-----

```

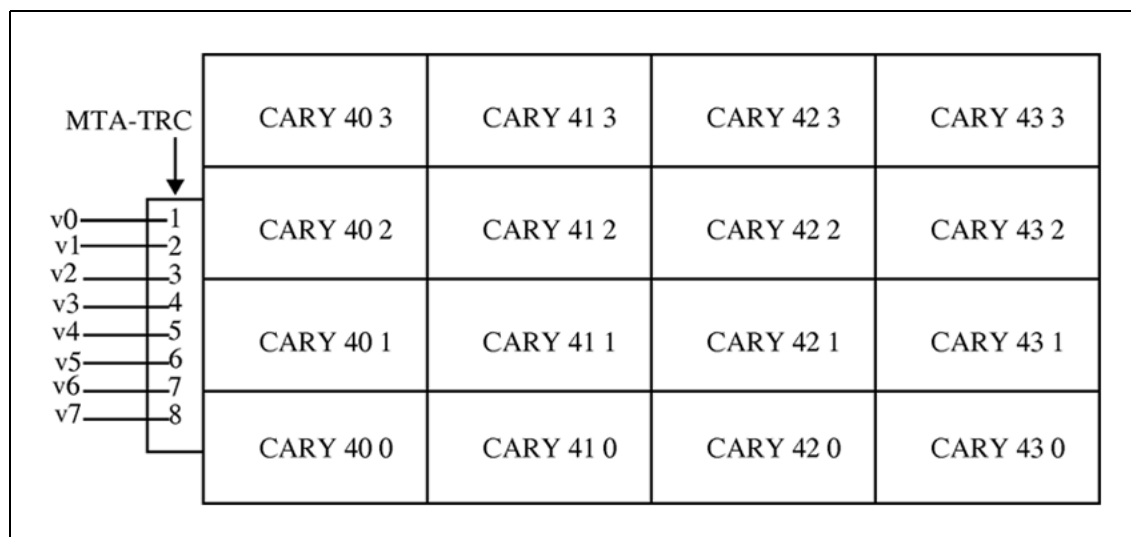
```

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 LGRPOPTS

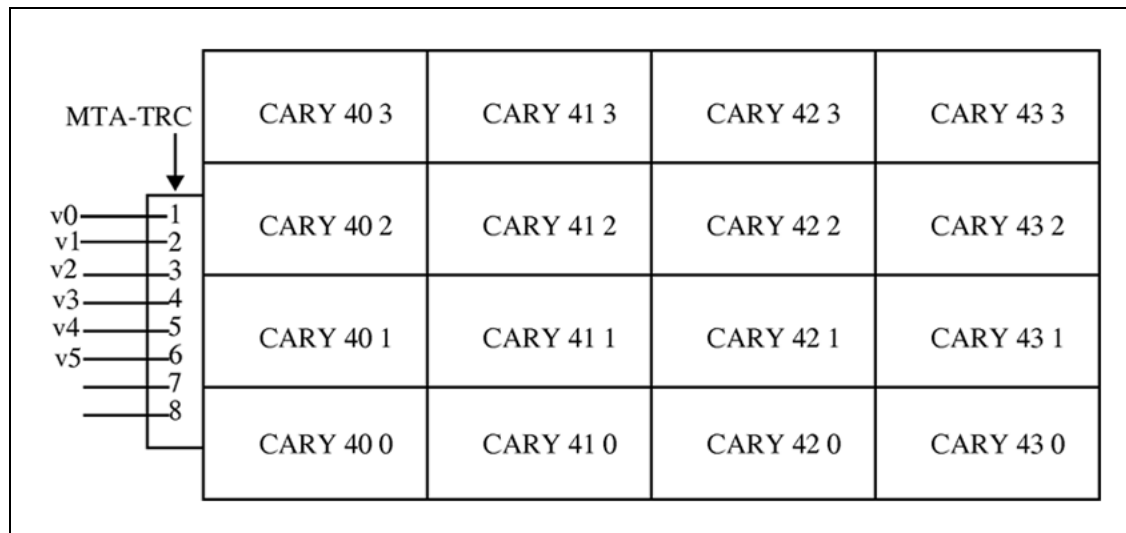
```
-----
CARY 40 0 GWC 0 S (MTSTAPT CARY (0 1) $ ) $
CARY 40 1 GWC 0 S (MTSTAPT CARY (1 2) $ ) $
CARY 40 2 GWC 0 S (MTSTAPT CARY (2 3) $ ) $
CARY 40 3 GWC 0 S (MTSTAPT CARY (3 4) $ ) $
CARY 41 0 GWC 0 S (MTSTAPT CARY (4 5) $ ) $
CARY 41 1 GWC 0 S (MTSTAPT CARY (5 6) $ ) $
CARY 41 2 GWC 0 S (MTSTAPT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

Line state	Meaning	Applicable to MG 9000 lines?
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
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

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.

State	Information
Operational	• Unlocked indicates the circuit has not been manually taken out of service. Shows the current service state. The values can be enabled or disabled.
Fault	• Enabled indicates the circuit is in the working state. • Disabled indicates the circuit is not in the working state. 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.
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
Ringing	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
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 In 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 TYPERTLSG
```

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;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;lms;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;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

Replace the line circuit or move the subscriber to another circuit.

Single-party ringing failure

Log example

```
RTP206BH ***+LINE101 MAR05 14:55:55 6900 FAILLN_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 DN6195200000  
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;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

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 -.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;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

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"](#) (page 147).

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"](#) (page 190).
- 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.

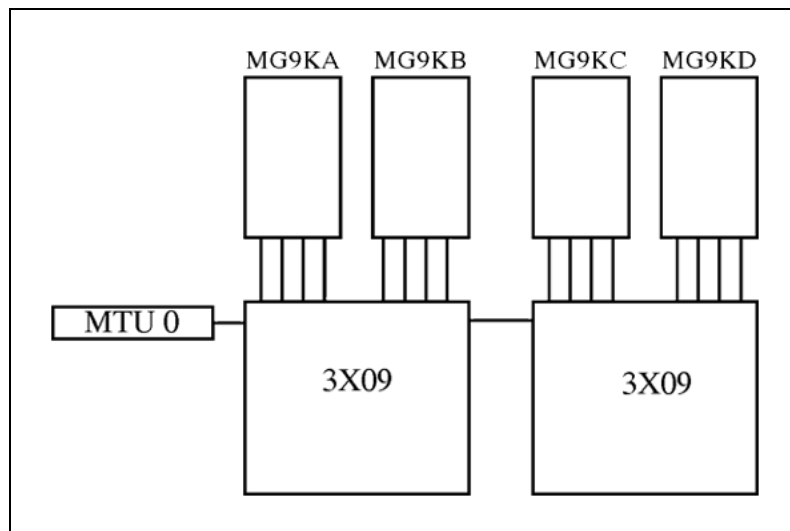
ALT LIT requires an MTU to test the subscriber loop. ALT uses the dedicated MTUs in the switch.

There are two test configuration options for MG 9000 lines:

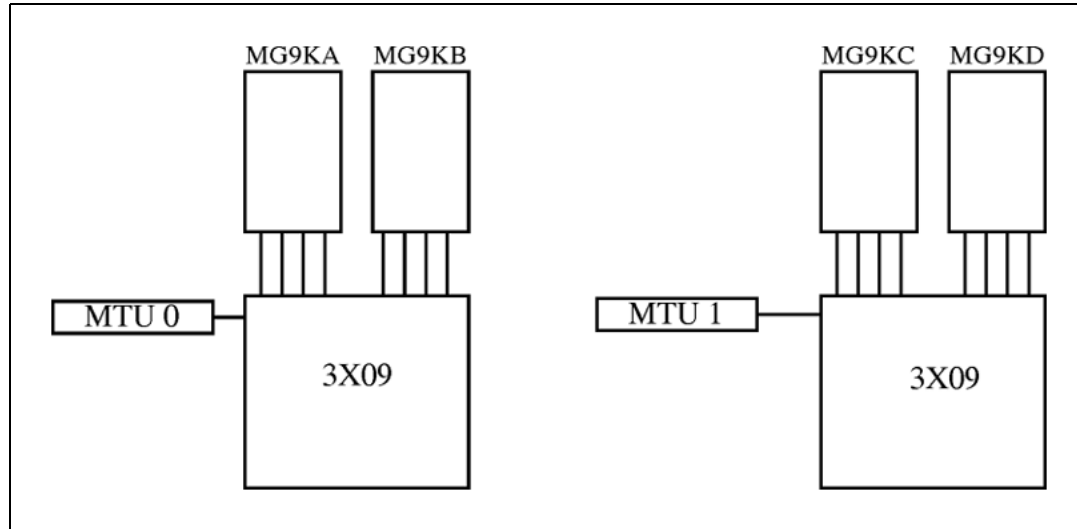
- Single dedicated MTU for a pair of NT3X09s - If you use the Wide band Test Access (WTA) panel, there will be a single dedicated MTU for a pair of NT3X09s.
- Dedicated MTU for each NT3X09 - If you wire the test equipment together through the main distribution frame (MDF), a dedicated MTU can be assigned 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.

DSCKT

The DSCKT 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

Step	Action

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.

—End—

Poor speech quality

Procedure 2

Troubleshooting poor speech quality

Step	Action

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.

—End—

Line does not ring

Procedure 3

Troubleshooting a line that does not ring

Step	Action

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.

—End—

Call not completed correctly

Procedure 4

Troubleshooting a call not completed correctly

Step	Action

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.

—End—

P-phone lines not functioning correctly

Procedure 5

Troubleshooting P-phone lines

Step	Action

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	Do
the problem is resolved	step 4
the problem cannot be isolated	Escalate to the next level of support. Go to step 4.

- 4 You have completed this procedure.

—End—

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

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 (I)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    OFFICE

OFFICE OFFICE
                                CURRENT  MINOR

MAJOR  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 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

Multiple alarms	Cutoff (CUT)	Diagnostic failure (DF)	Hazard (HAZ)	Permanent signal partial dial (PSPD)	System busy (SYSB)
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      0
2 Post_     LGRP    2      0      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 OFFL 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  SysB  ManB  OffL
CBsy  ISTb  InSv
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

```

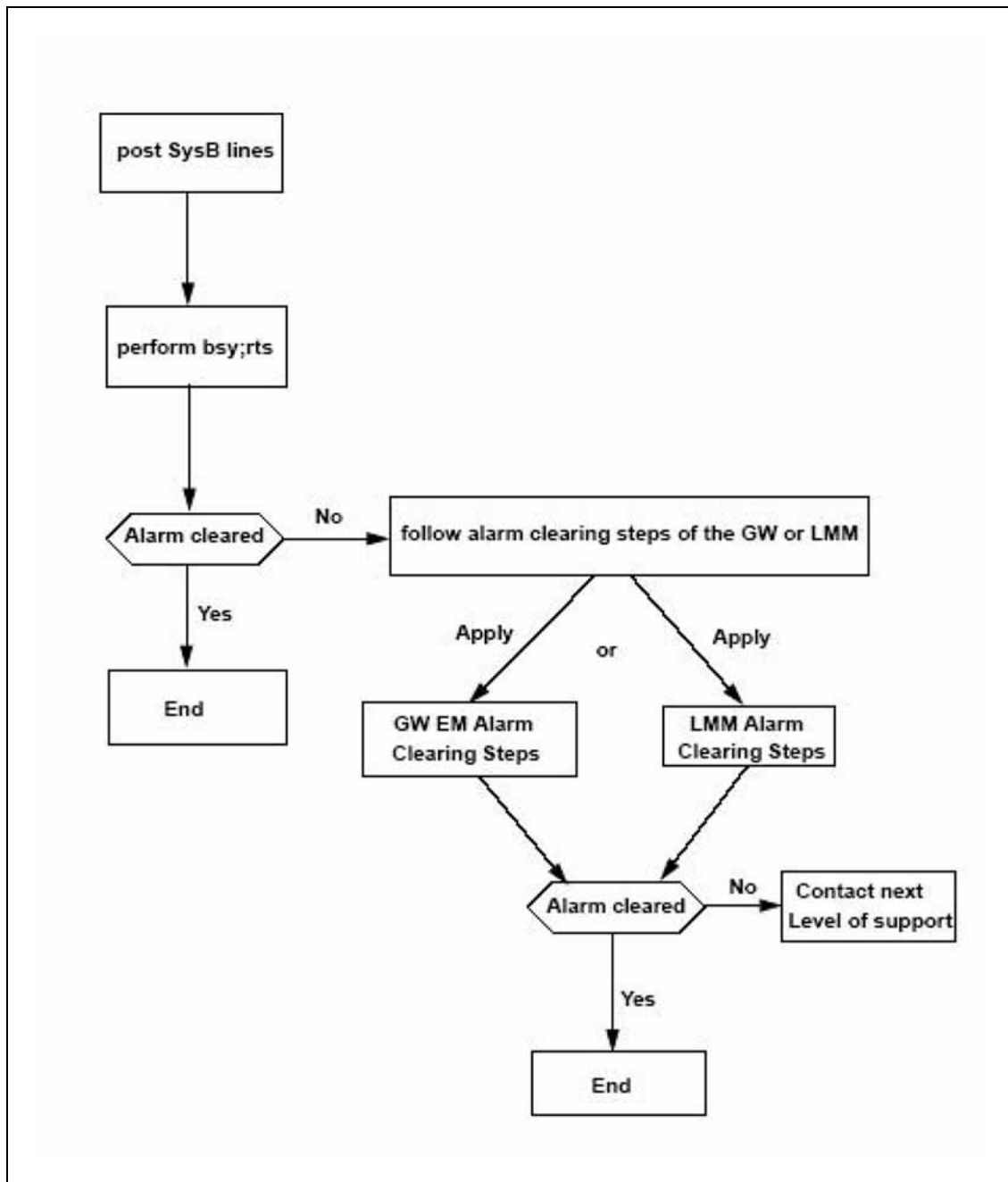
YD

Time 14:50 >

Clearing a SysB Lns 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:

- (I)SN07 to (I)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.					

- (I)SN06 to (I)SN07 - In (I)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 test 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:
LNS:
LTP:
>nff start sfdev diag1
>diag
RTD ***+LINE100 OCT30 08:52:43 1200 PASS LN_DIAG
      UD17 05 3 02 00      DN 6136211701
      DIAGNOSTIC RESULT    Card Diagnostic OK
      ACTION REQUIRED      None
      CARD TYPE            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	LGRPPTS

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>) É

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).

Logging in to an SPFS-based server

Application

Use this procedure to log into a Server Platform Foundation Software (SPFS) server. This procedure provides the steps to establish a login session using SSH, which is secure, or telnet, which is not secure.

Some tasks will require that you log in to the server through the console (port A) using the root user ID and password.

Prerequisites

This procedure requires the following information:

- the IP address or host name of the server
In a two-server configuration, you need the physical IP address of the active or inactive server.
- a valid user id and password
- the root password if you need to perform a task on the server that requires root user privileges

Action

Perform the steps under one of the following headings to complete this procedure.

- Logging in using SSH
- Logging in using Telnet
- Logging in through the console

Logging in using SSH

Step	Action

At your workstation

- 1 Establish an SSH session.

If you have access to a workstation which supports the ssh command (Linux, for example) then proceed with [step a](#).

Otherwise, connect to the server using an SSH client and proceed to [step 2](#).

- a. Establish an SSH session to the server by typing

```
> ssh -l <user_id> <server>
```

where

user_id is root or your user id

server is the IP address or host name of the SPFS-based server, or the physical IP address of the active or inactive server as required, in a two-server configuration

- 2 Use the following table to determine your next step.

If you receive	Do
a message indicating a host authentication issue and a request to continue the connection	step 3
a prompt for a password	step 4

ATTENTION

The prompt indicates SSH is verifying whether the server is a trusted host for the workstation. SSH performs the verification the first time SSH is run on a workstation.

- 3 Continue the connection by typing
`y`
 and pressing the Enter key.
- 4 Enter the password for root or your user id and press the Enter key.
- 5 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 9
two-server configuration	step 6

- 6 Ensure you are on the correct server by typing
`# ubmstat`
 and pressing the Enter key.
- 7 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 8
inactive server and the response is ClusterIndicatorACT	step 8

If you need to be on the	Do
active server and the response is ClusterIndicatorACT	step 9
inactive server and the response is ClusterIndicatorSTBY	step 9

- 8 You are logged in to the wrong server. Return to [step 1](#) to log in to the other server.
- 9 You have completed this procedure.
If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Logging in using Telnet

Step	Action

At your workstation

- 1 Establish a telnet session to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server is the IP address or hostname of the SPFS-based server, or the physical IP address of the active or inactive server in a two-server configuration

- 2 When prompted, enter your userid.

ATTENTION

You cannot log in using the root userid at this step.

- 3 When prompted, enter your password.
- 4 Use the following table to determine your next step.

If	Do
you need to log in as root	step 5
otherwise	step 7

- 5 Change to the root user by typing


```
$ su -
```

and pressing the Enter key.

6 When prompted, enter the root password.

7 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 11
two-server configuration	step 8

8 Ensure you are on the correct server by typing

```
# ubmstat
```

and pressing the Enter key.

9 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 10
inactive server and the response is ClusterIndicatorACT	step 10
active server and the response is ClusterIndicatorACT	step 11
inactive server and the response is ClusterIndicatorSTBY	step 11

10 You are logged in to the wrong server. Log out of this server and return to [step 1](#) to log in to the other server.

11 You have completed this procedure.
If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Logging in through the console

Step	Action

At the console connected to the server

- 1 Log in to the server through the console (port A) using the root user ID and password. In a two-server configuration, log in to the active or inactive server as required.
- 2 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 6
two-server configuration	step 3

- 3 Ensure you are on the correct server by typing

```
# ubmstat
```

and pressing the Enter key.

- 4 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 5
inactive server and the response is ClusterIndicatorACT	step 5
active server and the response is ClusterIndicatorACT	step 6
inactive server and the response is ClusterIndicatorSTBY	step 6

- 5 You are logged in to the wrong server. Log out of this server and return to [step 1](#) to log in to the other server.
- 6 You have completed this procedure.
If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Fault management trunk testing

The following section of fault management deals with trunk 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.

The solution is 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.

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 in the trunk.
Ckt	Connects a specified circuit to a trunk.
StkSdr	Allows access to the Stuck Sender feature, which identifies trunks with outpulsing problems.

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

Command	Description
LOSS	Manually measures transmission loss. For additional information, refer to "TGEN, LOSS, and CKTMON Command additional information" (page 204)
TGEN	Manually generates a tone of desired frequency and level. For additional information, refer to "TGEN, LOSS, and CKTMON Command additional information" (page 204)
Noise	Manually measures transmission noise.
OP	Permits the ability to seize and outpulse a set of desired digits over a trunk.

Command	Description
TDet	Manually measures the presence of an incoming tone.
HSet	Executes a bit signaling test on a trunk.
SGNL	Connects an available headset to a trunk.
TST	Permits the user to run a number of supported tests, including the following: • "ISUP continuity test (ICOT)" (page 218) • T100 (originating and terminating) • T102 (originating and terminating) • T104 (originating and terminating) • T105 (originating and terminating)

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

Command	Description
MonPost	Provides the user the ability to monitor a trunk circuit in a posted position.
MonLink	Provides the user the ability to monitor a trunk circuit in a 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 the 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.

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 the trunk.
QrySig	Queries the signaling availability and the state of a trunk.

Command	Description
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.

Supported Tests

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 1: Additional equipment is required.

Note 2: This is available for both TDM and DPT-SPM/MG 4000 trunk types.

- 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 \(AAL5 IP only\)" \(page 200\)](#)
- ["Non-hybrid/CS 2000-Compact solution \(AAL2 and AAL5\)" \(page 200\)](#)

Hybrid switch solution (AAL5 IP only)

Developed for the AAL5 hybrid switch configuration 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 the test and the test hardware located in the ISM.

Non-hybrid/CS 2000-Compact solution (AAL2 and AAL5)

Developed for the AAL2 and AAL5 switch configurations that do not contain an ENET or ISM, this solution utilizes the 3rd party Media Server 2000 Series as a limited replacement for the ISM. The AMS 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 TEM trunks via the MAPCI TTP level and ATT level interfaces. The applicable Nortel documentation reference is provided for each MAPCI level.

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 in the trunk.
Ckt	Connects a specified circuit to a trunk.
StkSdr	Allows access to the Stuck Sender feature, which identifies trunks with outpulsing problems.

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

Command	Description
LOSS	Manually measures transmission loss. For additional information, refer to "TGEN, LOSS, and CKTMON Command additional information" (page 204)
TGEN	Manually generates a tone of desired frequency and level. For additional information, refer to "TGEN, LOSS, and CKTMON Command additional information" (page 204)
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	Executes a bit signaling test on a trunk.

Command	Description
SGNL	Connects an available headset to a trunk.
TST	Permits the user to run a number of supported tests, including the following: • "ISUP continuity test (ICOT)" (page 218) • T100 (originating and terminating) • T102 (originating and terminating) • T104 (originating and terminating) • T105 (originating and terminating)

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 the 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.

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.

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 the trunk.
QrySig	Queries the signaling availability and the state of a trunk.

Command	Description
RouteSet	Displays the route set CLLI of a CCS7 trunk.
CIC	Displays the circuit identification code of a trunk.

Trunk Type	Start Signaling Type	Pulse Type	Card Type
OP	Wink	MF	DSISIG
ES	Wink	MF	DSISIG
ATC	Wink	MF	DSISIG
IT	Wink	MF	DSISIG
CELL	Wink	MF	DSISIG
IBNT2	Wink	MF, DP	DSISIG
IBNTO	Wink	MF, DP	DSISIG
IBNTI	Wink	MF, DP	DSISIG

The SGNL command support on MG15000 PTS trunks has the following qualifications:

- No international trunk variants are supported.
- Delay Dial and Immediate start signaling types are not supported.
- Not supported in the IAC solution which employs PTS trunk variants OP and ES hosted on TGCP protocol based trunk gateways.
- Current MG15000 based PTS trunk architecture does not support onhook signal reporting during digit collection. If the user is executing the SGNL command whose far-end trunk is a MG15000 based PTS trunk, the following procedure applies:
 - User posts supported PTS trunk circuit and executes the SGNL 'onoffhk' command
 - Far-end MG15000 PTS trunk connects to an available digit receiver and outputs a Wink signal reply
 - Upon successful reporting of Wink signal, user releases posted PTS trunk circuit trunk via the available RLS release command
 - User waits for far-end trunk digit receiver timer to expire. Upon expiration, far-end trunk returns to its idle state.

TGEN, LOSS, and CKTMON Command additional information

The TGEN, LOSS, and CKTMON commands support the following North American PTS trunk variants which use the standard /TDM PTS call model for the H.248 based protocol.

Trunk Type	Start Signaling Type	Pulse Type	Card Type
OP	Wink	MF	DSISIG
ES	Wink	MF	DSISIG
ATC	Wink	MF	DSISIG
IT	Wink	MF	DSISIG
CELL	Wink	MF	DSISIG
IBNT2	Wink, DT, IM	MF, DP, DD	DSISIG
IBNTO	Wink, DT, IM	MF, DP, DD	DSISIG
IBNTI	Wink, DT, IM	MF, DP, DD	DSISIG

TGEN, LOSS, and CKTMON commands support on MG15000 PTS trunks has the following qualifications:

- No international trunk variants are supported.
- Not supported in the IAC solution which employs PTS trunk variants OP and ES hosted on TGCP protocol based trunk gateways.
- The LOSS command line option "E" for the echo test is not supported.
- The CKTMON command resides on the MAPCI TTP Monitor level. No physical hardware connections will be attempted upon entry of MAPCI TTP Monitor level. Monitor level commands MonPost, MonLink, MonBoth, and MonTalk are not 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.

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 in the trunk.
StkSdr	Allows access to the Stuck Sender feature, which identifies trunks with outpulsing problems.

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.
MWTSwap	Permits the ability to send and receive a 1004 Hz test tone and measure transmission loss on the received tone.
SGNL	Connects an available headset to a trunk.
TST	Permits the user to run a number of supported tests, including the following: • • T100 (originating and terminating) • T102 (originating and terminating) • T104 (originating and terminating) • T105 (originating and terminating) Note: T105 termination on the MS2000 series supports only the LSC, L, NSC, RN, N, and NT subtests.

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

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

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 the 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.

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

Step	Action

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.

—End—

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

Step	Action

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.

—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

Step	Action

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.

—End—

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

Step	Action

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.

—End—

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. "TL105 Test combination description" (page 212) lists the designation codes and associated tests.

TL105 Test combination description

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 0 dBm 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 –16 dB, 1004 Hz. C-notched filter).
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.

Code	Tests	Description
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.
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 0 dB and 1004 Hz. Noise measurement (C-message filter). Return loss measurement.
T50L	L, ERL, SRLLO, SHI	Loss measurement at 0 dB 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.

Code	Tests	Description
T5LB	L4,10, L28, ERL, SRLLO, SHI	Loss measurement at –16 dB and 404, 1004 2804 Hz. Return loss measurement.
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. ["Test and layer format description" \(page 214\)](#) 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 ["TL105 Test combination description" \(page 212\)](#) and ["Test and layer format description" \(page 214\)](#) for tests that use these filters.

Test and layer format description

Test	Layer	MF digit	MF Frequency	Test description
ERL	2	C	700/1700	Echo return loss measurement with quiet termination
ERLS C	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.
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.

Test	Layer	MF digit	MF Frequency	Test description
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.
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

Step	Action

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.

—End—

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 T108 Terminating Test Line test is a method for accessing the dialed non-inverting loopback on trunks features known as TRKLPBK. T108 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.

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

Performing a TL108 trunk test

The following procedure outlines the test sequence for the TL108 trunk test.

Originating a TL108 trunk test

Step	Action

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 1 kHz 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.

—End—

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

Step	Action

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
```

—End—

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

Step	Action

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.
```

—End—

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

Step	Action

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
```

—End—

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

Step	Action

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
```

—End—

Logs and operational measurements supported by CEM

Logs

For logs generated by the core and sent to the CEM and then to the IEMS, see the following table.

Log numbers	Documentation reference
ESA120, ESA121	<i>North American DMS-100 Log Report Reference Manual</i> , 297-8021-840
ATM300, ATM301, ATM501, ATM600, ATM605	<i>North American DMS-100 Log Report Reference Manual</i> , 297-8021-840
XPKT806, XPKT807	<i>Carrier VoIP Fault Management Logs Reference</i> , NN10275-909
BITS300, BITS310, BITS500, BITS600, BITS601, BITS610	<i>Carrier VoIP Fault Management Logs Reference</i> , NN10275-909
BOOT101	<i>North American DMS-100 Log Report Reference Manual</i> , 297-8021-840
C7UP104, C7UP109, C7UP113, C7UP114, C7UP120, C7UP130, C7UP310	<i>CDMA/TDMA Logs Reference Manual</i> , 411-2131-510
CARR300, CARR310, CARR320, CARR330, CARR331, CARR340, CARR341, CARR500, CARR501, CARR510, CARR511, CARR512, CARR800, CARR801, CARR811	<i>CDMA/TDMA Logs Reference Manual</i> , 411-2131-510
CCMT301, CCMT501, CCMT502, CCMT601	<i>North American DMS-100 Log Report Reference Manual</i> , 297-8021-840
DPTM500, DPTM501, DPTM502, DPTM503, DPTM504, DPTM550, DPTM560, DPTM700, DPTM701	<i>North American DMS-100 Log Report Reference Manual</i> , 297-8021-840
ENET308, ENET311	<i>North American DMS-100 Log Report Reference Manual</i> , 297-8021-840
EXT102, EXT108	<i>North American DMS-100 Log Report Reference Manual</i> , 297-8021-840

Log numbers	Documentation reference
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>
QCA201, QCA202, QCA203, QCA300, QCA301, QCA302, QCA305, QCA310, QCA315, QCA322, QCA399	<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>
SDMB300, SDMB310, SDMB315, SDMB316, SDMB320, SDMB321, 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, NN10275-909</i>
SOS701, SOS702, SOS703	<i>XA-Core Reference Manual, 297-8991-810</i>

Log numbers	Documentation reference
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, NN10275-909</i>
TMN301, TMN302, TMN304, TMN303, TMN304, TMN309, TMN311, TMN600, TMN601, TMN604, TMN605	<i>Carrier VoIP Fault Management Logs Reference, NN10275-909</i>
TRK882	<i>North American DMS-100 Log Report Reference Manual, 297-8021-840</i>
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, 297-8991-810</i>
XACP300, XACP500, XACP600	<i>XA-Core Reference Manual, 297-8991-810</i>

Log reports CSEM300 and CSEM600

Log reports CSEM300 and CSEM600 address a change of format for northbound events on the log feeds of IEMS 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 IEMS 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	Carrier VoIP Fault Management Logs Reference, 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, see "Specifying the logs delivered from the CM to the core manager" in *CS 2000 Core Manager Configuration*, NN10104-511.

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" (page 227)
- "Tasks to be performed weekly" (page 228)
- "Tasks to be performed monthly" (page 229)
- "Tasks to be performed per office schedule or as required" (page 229)
- "Backup and restore" (page 231)

Tasks to be performed daily

Component	Task	Document	Notes
GWC	Monitor for alarms and check that functions continue without interruptions	<i>GWC Fault Management</i> , NN10202-911	
Media Server 2000 series	Monitor alarms	<i>Media Server 2000 Series Fault Management</i> , NN10328-911	
Ethernet Routing Switch 8600	Monitor alarms and LEDs	<i>Ethernet Routing Switch 8010co Chassis hardware components</i> , 312746-*	
Multiservice Switch/Media Gateway 7400/15000	Monitor alarms	<i>Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting</i> , NN10600-520	
Multiservice Switch/Media Gateway 15000	Monitoring equipment status LEDs	<i>Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade</i> , NN10600-130	
Multiservice Switch 7400/15000	Monitoring ATM services	<i>Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management</i> , NN10600-715	

Component	Task	Document	Notes
Multiservice Switch/Media Gateway 15000 or 7400	Using status indicator LEDs and sounds	<i>Nortel 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> , NN10202-911	

Component	Task	Document	Notes
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-*	perform immediately upon completion of the configuration or when changes are made to the configuration/firmware are
Contivity VPN Switch	Performing file maintenance	<i>Reference for the Contivity VPN Switch</i> , 311643-*	perform immediately upon completion of the configuration or when changes are made to the configuration/firmware are
Contivity VPN Switch	Creating a recovery disk	<i>Reference for the Contivity VPN Switch</i> , 311643-*	perform immediately upon completion of the configuration or when changes are made to the configuration/firmware are
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

Component	Task	Document	Notes
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</i> , NN10205-511	includes Line, Trunk, V5.2, and CS 2000 data integrity audits
GWC	Take a manual software image	<i>GWC Upgrades</i> , NN10196-461	should be taken after patches have been applied
GWC	Retrieve GWC services alarm history	<i>GWC Fault Management</i> , NN10202-911	
GWC	Retrieve and correlate GWC PM logs	<i>GWC Fault Management</i> , NN10202-911	
GWC	Retrieve and correlate Syslog logs	<i>GWC Fault Management</i> , NN10202-911	
MDM	Clean up accumulated log files	<i>Multiservice Data Manager Customization and Server Administration</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

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> , NN10202-911	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 to *ATM/IP Solution-level Security and Administration*, NN10402-600.

Upgrade rollbacks

For information on software rollback procedures for the Ethernet Routing Switch 8600 and the CS 2000 Management Tools see *Upgrading the Carrier Voice over IP Network*, NN10440-450.

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 \(I\)SN07" \(page 233\)](#)
- ["Downgrading to \(I\)SN08" \(page 234\)](#)

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)SN07

Follow the link according to your office configuration.

- ["Rollback on Sun Netra t1400 or Sun Netra 240 one-sever configuration" \(page 233\)](#)
- ["Rollback on Sun Netra 240 two-server configuration" \(page 233\)](#)

Rollback on Sun Netra t1400 or Sun Netra 240 one-sever configuration

Use the table below as a checklist during the rollback of the SPFS and CS 2000 Management Tools software to (I)SN07. 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)SN07

Activities	√	Procedures
1 Restore the file systems and Oracle data from backup media.		Refer to procedure "Routing customer logs to a remote host" (page 818) .
2 Clear the Java TM Web Start (JWS) cache on the client workstation.		Refer to procedure Clearing the JWS cache on a client workstation.

Restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN09.

Rollback on Sun Netra 240 two-server configuration

Follow the link according to whether only one server in the cluster was upgraded to (I)SN09, or both servers in the cluster were upgraded to (I)SN09.

- ["Downgrading the only upgraded server in the cluster" \(page 234\)](#)
- ["Downgrading both upgraded servers in the cluster" \(page 234\)](#)

Downgrading the only upgraded server in the cluster

Use the table below as a checklist during the rollback of the SPFS and CS 2000 Management Tools software to (I)SN07 on the only upgraded server. Place a check (✓) in the ✓ column as you complete each procedure.

Downgrading the only upgraded server to (I)SN07

Activities	✓	Procedures
1 Clone the image of the server with the (I)SN07 software onto the other (upgraded) server.		Refer to procedure "Disabling local logging of SPFS platform faults" (page 830).

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)SN09.

Downgrading both upgraded servers in the cluster

Use the table below as a checklist during the rollback of the SPFS and CS 2000 Management Tools software to (I)SN07 on both upgraded servers. Place a check (✓) in the ✓ column as you complete each procedure.

Downgrading both upgraded servers to (I)SN07

Activities	✓	Procedures
1 Restore the file systems and Oracle data from backup media on one of the servers.		Refer to procedure "Routing customer logs to a remote host" (page 818).
2 Clone the image of the server you just downgraded to (I)SN07, onto the other server.		Refer to procedure "Disabling local logging of SPFS platform faults" (page 830).
3 Clear the Java TM Web Start (JWS) cache on the client workstation.		Refer to procedure Clearing the JWS cache on a client workstation .

Restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN09.

Downgrading to (I)SN08

Follow the link according to your office configuration.

- ["Rollback on Sun Netra t1400 or Sun Netra 240 one-server configuration"](#) (page 235)
- ["Rollback on Sun Netra 240 two-server configuration"](#) (page 235)

Rollback on Sun Netra t1400 or Sun Netra 240 one-server configuration

Use the table below as a checklist during the rollback of the SPFS and CS 2000 Management Tools software to (I)SN08. 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)SN08

Activities	✓	Procedures
1 Restore the file systems and Oracle data from backup media.		Refer to procedure "Routing customer logs to a remote host" (page 818) .
2 Clear the Java TM Web Start (JWS) cache on the client workstation.		Refer to procedure Clearing the JWS cache on a client workstation .

Restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN09.

Rollback on Sun Netra 240 two-server configuration

Follow the link according to whether only one server in the cluster was upgraded to (I)SN09, or both servers in the cluster were upgraded to (I)SN09.

- ["Downgrading the only upgraded server in the cluster" \(page 235\)](#)
- ["Downgrading both upgraded servers in the cluster" \(page 236\)](#)

Downgrading the only upgraded server in the cluster

Use the table below as a checklist during the rollback of the SPFS and CS 2000 Management Tools software to (I)SN08 on the only upgraded server. Place a check (✓) in the ✓ column as you complete each procedure.

Downgrading the only upgraded server to (I)SN08

Activities	✓	Procedures
1 Clone the image of the server with the (I)SN08 software onto the other (upgraded) server.		Refer to procedure "Disabling local logging of SPFS platform faults" (page 830) .

Cloning the image of the (I)SN08 server onto the server that was upgraded, restores the server as it was before the upgrade to (I)SN09.

Downgrading both upgraded servers in the cluster

Use the table below as a checklist during the rollback of the SPFS and CS 2000 Management Tools software to (I)SN08 on both upgraded servers.

Place a check (√) in the √ column as you complete each procedure.

Downgrading both upgraded servers to (I)SN08

Activities	√	Procedures
1 Restore the file systems and Oracle data from backup media on one of the servers.		Refer to procedure " Routing customer logs to a remote host " (page 818).
2 Clone the image of the server you just downgraded to (I)SN08, onto the other server.		Refer to procedure " Disabling local logging of SPFS platform faults " (page 830).
3 Clear the Java TM Web Start (JWS) cache on the client workstation.		Refer to procedure Clearing the JWS cache on a client workstation.

Restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN09.

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, if you replaced the Inactive unit or if you executed a reverse restore (switched unit 0 and 1)

ATTENTION

Ensure that no provisioning activities are in progress, or are scheduled to take place during this procedure.

Action

Perform the following steps to complete this procedure.

Step	Action						
At your workstation							
1	Establish a login session to the Active node using one of the following methods:						
<table border="1"> <thead> <tr> <th>If using</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>telnet (unsecure)</td> <td>step 2</td> </tr> <tr> <td>ssh (secure)</td> <td>step 7</td> </tr> </tbody> </table>		If using	Do	telnet (unsecure)	step 2	ssh (secure)	step 7
If using	Do						
telnet (unsecure)	step 2						
ssh (secure)	step 7						
2	Log in to the Active node using telnet (unsecure) by typing <code>> telnet <server></code> and pressing the Enter key. where server is the cluster IP address, which automatically defaults to the Active node in the cluster						
3	When prompted, enter your user ID and password.						

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 7

- 2 Log in to the Active node using telnet (unsecure) 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
- 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 Proceed to step 9.
- 7 Log in using ssh (secure) 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

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.

- 8 When prompted, enter the root password.
- 9 Verify the status of replicated disk volumes by typing
`# udstat`
 and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 10
not ACTIVE	contact your next level of support

- 10 Determine the server profile. 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 - exits
select -
```

- 11 Enter the number next to the View option in the menu.

Example response

```

View
  1 - SPFS_soft (Display Software      Installation
Level Of SPFS)
  2 - chk_SPFS (Check SPFS 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 -

```

- 12** Enter the number next to the SPFS_soft option in the menu.

Example response

```

=== Executing "SPFS_soft"
SPFS version:  08.0 Build:  200508421 Server Profile:
cbm850
=="SPFS_soft" completed successfully

```

- 13** Determine the Server Profile.

If the Server Profile is	Do
cbm850	step 28
anything else	step 14

- 14** 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
SESMSservice                           RUNNING
CORBA                                  RUNNING
ORA_ARCHIVE_ROTATOR                    RUNNING
OMPUSH                                 RUNNIN
GBOOTP  RUNNING
WEBSERVICES                            RUNNING
ORA_AUTO_BACKUP                        RUNNING
APS                                    RUNNING

```

NPM

RUNNING

- 15 Use the following table to determine your next step.

If	Do
all applications are running	step 18
one or more applications are not running	step 16

- 16 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

- 17 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 18

- 18 Use the following table to determine your next step.

If this server is	Do
running the NPM software	step 19
not running the NPM software	step 21

The Network Patch Manager (NPM) software is running on this server if NPM appeared in the response from step 14.

- 19 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 21
not running	step 20

- 20 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 21

- 21 Use the following table to determine your next step.

If this server is	Do
running the CS 2000 Management Tools software	step 22
not running the CS 2000 Management Tools software	step 28

- 22 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
```

- 23 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 24

- 24 Deconfigure NDS replication before cloning the node by typing

```
#cp /etc/nsswitch.files /etc/nsswitch.conf
```

and pressing the Enter key.

- 25 Type

```
#cp /etc/pam.conf.orig /etc/pam.conf
```

and press the Enter key.

26 Type

```
#cd /opt/nortel/applications/security/current_slisext
/swmgmt/bin
```

and press the Enter key.

27 Type

```
#./configure_slisext.sh -replica disable
```

and press the Enter key.

28 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 29
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 36

29 Use the following table to determine your next step.

If you	Do
know the Ethernet address of the Inactive unit	step 34
do not know the Ethernet address of the Inactive unit	step 30

At the console connected to the inactive node

30 Determine the Ethernet address of the Inactive node. Log in to the inactive node through the console (port A) using the root user ID and password.

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.

- 31** Bring the system to the OK prompt by typing
`# init 0`
 and pressing the Enter key.
- 32** 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.
```

Ethernet address formats can vary from machine to machine. The fields in an Ethernet address may contain one alphanumeric character or two alphanumeric characters, both are acceptable formats.

- 33** Record the Ethernet address that is displayed.

At your workstation (login session to the Active node)

- 34** 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
- 35** Proceed to step 37
- 36** Start the cloning process by typing
`# startb`
 and press the Enter key.
- 37** Use the following table to determine your next step.

If the system	Do
prompts you to enter the command "boot net - image"	step 38
does not prompt you to enter the command "boot net - image"	step 42

- 38** Connect to the console port of the Inactive node.

If the console displays	Do
the OK prompt	step 41
the login prompt	step 39

At the console connected to the inactive node

- 39** Log in using the root user ID and password.
- 40** Bring the system to the OK prompt by typing
`# init 0`
 and pressing the Enter key.
- 41** 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.
 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)

- 42** 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
```

- 43** 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)

- 44** Verify the status of replicated disk volumes by typing

```
# udfstat
```

and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 45
not ACTIVE	contact your next level of support

At your workstation

- 45** Establish a login session to the Inactive node using one of the following methods:

If using	Do
telnet (unsecure)	step 46
ssh (secure)	step 51

- 46** Log in to the Inactive node using telnet (unsecure) by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the physical IP address of the Inactive node in the cluster

- 47** When prompted, enter your user ID and password.

- 48** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

49 When prompted, enter the root password.

50 Proceed to step 53.

51 Log in to the 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

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.

52 When prompted, enter the root password.

53 Verify the status of replicated disk volumes by typing

```
# udfstat
```

and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 54
not ACTIVE	contact your next level of support

At your workstation (login session to the Active node)

54 Complete the cloning process by typing

```
# finishb
```

and pressing the Enter key.

Sessions on both the Active and Inactive nodes

55 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
```

and pressing the Enter key.

56 Type

```
#cp /etc/pam.conf.is /etc/pam.conf
```

and press the Enter key.

- 57** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Migrating the SAM21 network elements back to the CS 2000 SAM21 Manager on the core manager

Application

Use this procedure to migrate the SAM21 network element back to the CS 2000 SAM21 Manager on the core manager.

Prerequisites

None

Action

Launch the CS 2000 SAM21 Manager client that resides on the core manager

Step	Action

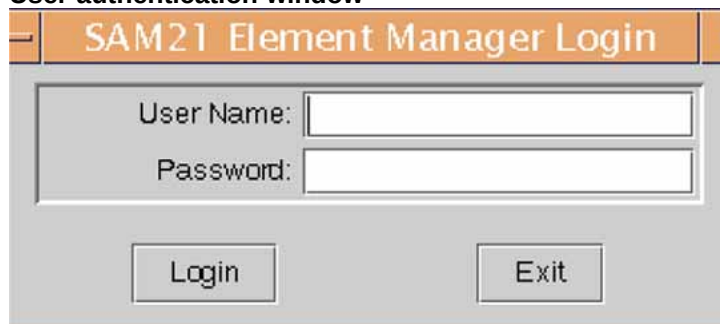
At the client workstation

- 1 Log on the client workstation using the correct user ID and password. Do not log on as the root user.
- 2 Launch the SAM21 Manager client application that resides on the core manager by typing

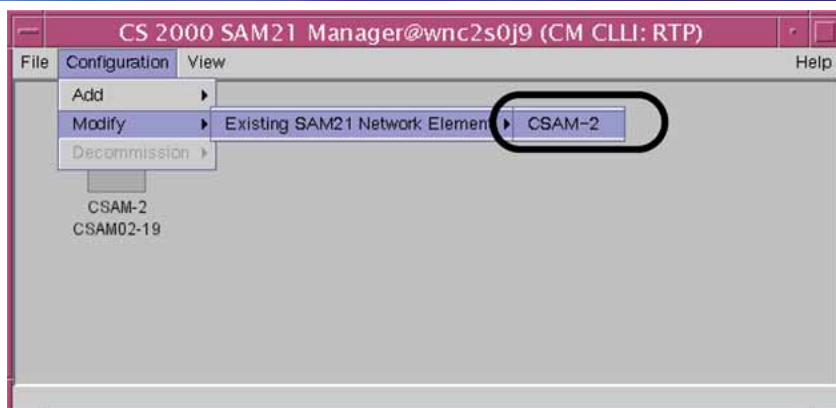
```
# /sdm/bin/sam21gui
```

and pressing the Enter key.
The user authentication window appears.

User authentication window



- 3 Enter a valid user name and password, and click the "Login" button.
- 4 Reprovision each SAM21 network element (NE) as follows:
 - a. Use the Configuration menu to modify a SAM21 NE.



The Reprovision window for the SAM21NE you selected, opens.

- b. Replace the existing IP address with the IP address of the core manager, and click Save.

An SNMP message is sent to both SAM21 NEs with the IP and port of the core manager. Within approximately 1 minute, the SAM21 NE recovers from isolation on the CS 2000 SAM21 Manager that resides on the core manager. Within approximately 2 minutes, the SAM21 NE is isolated on the CS 2000 SAM21 Manager that resides on the CS 2000 Management Tools server.

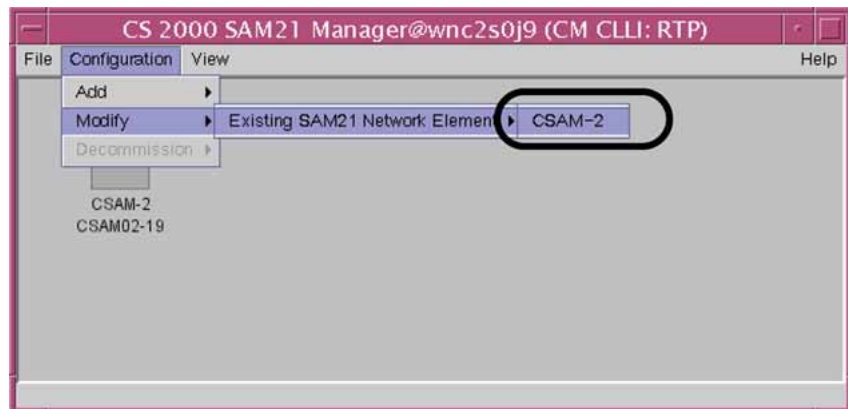
—End—

Launch the CS 2000 SAM21 Manager client that resides on the CS 2000 Management Tools server

Step	Action

At your workstation

- 1 Launch the SAM21 Manager client application that resides on the CS 2000 Management Tools server. Refer to procedure Launching CS 2000 Management Tools and NPM client applications in this document, if required.
- 2 Reprovision each SAM21 network element (NE) as follows:
 - a. Use the Configuration menu to modify a SAM21 NE.



The Reprovision window for the SAM21NE you selected, opens.

- b. Replace the existing IP address with the IP address of the core manager, and click Save.

Reprovision SAM21-1

General

Name: SAM21 Number: 1

CSAM number: 01 Shelf Position: 01

Primary NTP: 172.16.1.205 Secondary NTP: 172.16.1.210

Timezone Offset: -5.0 SNMP Community: *****

BootP Provisioning

SC: Slot 7 SC: Slot 9

IP: 172.16.1.26 IP: 172.16.1.27

MAC: 08003e2d7921 MAC: 08003e2d790f

Gateway IP and Subnet Mask

IP: 172.16.1.1 Mask: 255.255.255.0

SAM21 EM Server

IP: 172.16.1.212 Port: 9560

Load Info

Server IP: 172.16.1.20

Server Path: /swd/sam21

Server Load: 10.0.x.0310290845

Clear Save Cancel Details...

All non-isolated shelves are communicating with the CS 2000 SAM21 Manager on the core manager.

3 You have completed this procedure.

—End—

Roll back the Shelf Controller software

ATTENTION

If the office supports CS 2000 - Compact, roll back the Call Agent software before rolling back the SAM21 Shelf Controller software. If you do not roll back the Call Agent software first, a reset loop may occur on the next unlock or REXtst of the Call Agent.

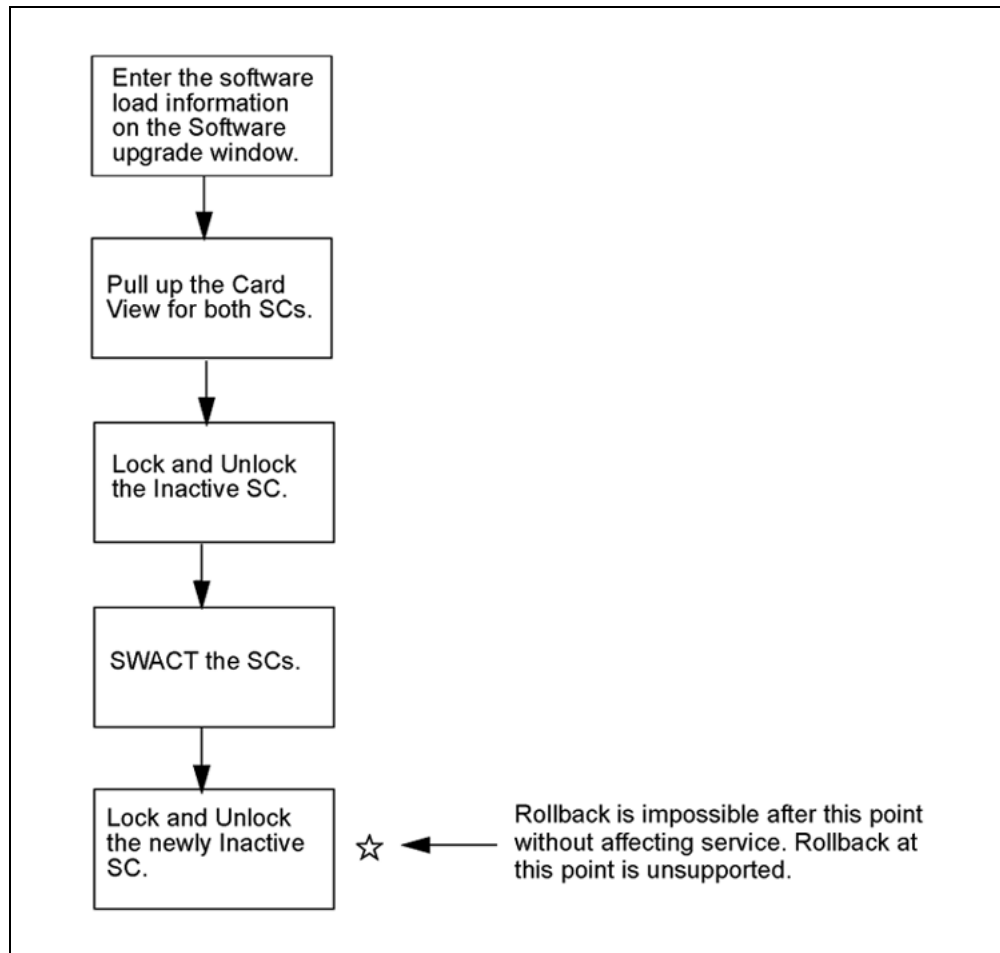
Purpose of this procedure

This procedure enables you to restore the previous Shelf Controller software load following an unsuccessful upgrade.

The following figure summarizes the upgrade procedure. Rollback is available until the second SAM21 Shelf Controller is unlocked and upgraded to the new software load. This point is indicated with the star.

The following figure summarizes the upgrade procedure. Use the step-by-step instructions that follow the figure to perform the procedure.

Note: Rollback is available until the second SAM21 Shelf Controller is unlocked and upgraded to the new software load. This point is indicated with the star.



When to use this procedure

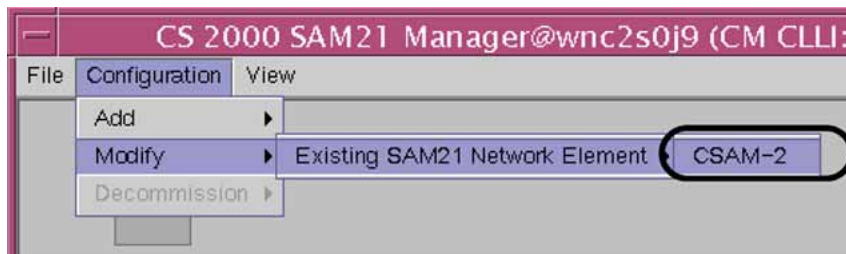
Use this procedure if problems occurred during the upgrade (automated or manual), and the upgrade was terminated.

Prerequisites

This procedure has no prerequisites.

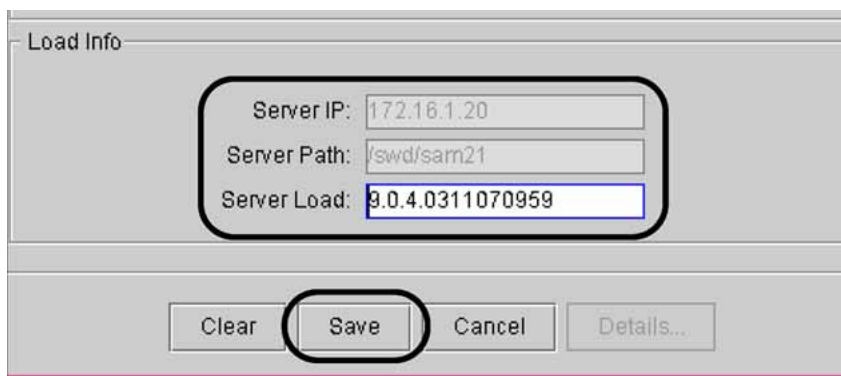
Action

Step	Action
<i>At the CS 2000 SAM21 Manager client (Java Web Start client)</i>	
1	From the Subnet View, select Configuration->Modify->Existing SAM21 Network Element and the SAM21 shelf with the SAM21 Shelf Controllers that need a software rollback..



- 2 In the Reprovision window, enter the name of the old software load in the Server Load field.

If you upgraded from 9.0.4.0311070959 to 10.0.0.0301120523, enter 9.0.4.0311070959 as the name of the old software load



- 3 Click Save.
- 4 Open the Shelf View of the SAM21 Shelf with the SAM21 Shelf Controllers that need a software rollback.
- 5 Double-click the card icon of a SAM21 Shelf Controller that needs a software rollback..
- 6 In the Card View window, click the States tab and check the Status of the SAM21 Shelf Controller.
- 7 Use the following table to determine your next step.

If the SAM21 Shelf Controller is:	Do
active	step 9
inactive	step 14

- 8 Close the Card View window.
- 9 Right-click on the card icon of the active SAM21 Shelf Controller and select Swact from the menu.

- 10 Wait for completion of the switch of activity.
- 11 Double-click the card icon of the SAM21 Shelf Controller.
- 12 In the Card View window, click the States tab and make sure the Status is Inactive.
- 13 Close the Card View window.
- 14 Right click on the card icon of inactive SAM21 Shelf Controller and select Lock from the menu.
- 15 Wait for the lock icon to appear on the inactive SAM21 Shelf Controller.
- 16 Right-click on the card icon of the inactive SAM21 Shelf Controller and select Unlock from the menu.
- 17 Wait for the hashed outline to disappear from the inactive SAM21 Shelf Controller.
- 18 Right-click on the card icon of the active SAM21 Shelf Controller and select Swact from the menu.
- 19 Wait for completion of the switch of activity.
- 20 Use the following table to determine your next step:

If you	Do
need to rollback software on the other SAM21 Shelf Controller	step 14
do not need to rollback software on the other SAM21 Shelf Controller	step 21

- 21 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Performing a rollback of the CS 2000 SAM21 Manager

Application

Use this procedure to rollback the CS 2000 SAM21 Manager from the CS 2000 Management Tools server to the core manager.

ATTENTION

This procedure deletes all provisioned data for the CS 2000 SAM21 Manager from the database on the CS 2000 Management Tools server.

Prerequisites

None

Action

Step	Action

At the CS 2000 Management Tools server

- 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 hostname 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 Stop the SAM21 Manager server application by typing
`# servstop SAM21EM`
 and pressing the Enter key.
- 6 Change directory by typing
`# cd /opt/nortel/sam21em/bin/migration`
 and pressing the Enter key.

- 7 Run the SAM21 Manager rollback script by typing

```
# ./sam21emRollback.sh
```

and pressing the Enter key.

Example response:

```
SAM21 Element Manager Server Persistent Data Migration  
Rollback
```

```
=====
```

```
This script should only be executed to rollback from  
the SPFS SAM21 EM to the CS2E SAM21 EM.
```

```
WARNING: This script deletes all provisioned data from  
the SAM21 EM database.
```

```
Do you wish to proceed?
```

```
Please confirm ("YES", "Y", "NO", "N")
```

- 8 Confirm that you want to proceed with the rollback by typing

```
# y
```

and pressing the Enter key.

Example response:

```
Retrieving Oracle SAM21 EM Password...
```

```
Clearing the SAM21EM Database Tables...
```

```
SAM21 Element Manager Persistent data migration  
rollback successful.
```

- 9 You have completed this procedure.

—End—

Performing a full system restore on an SPFS-based server

Application

Use this procedure to perform a full system restore from backup media on a Server Platform Foundation Software (SPFS)-based server (Sun Netra t1400 or Sun Netra 240).

A full system restore consists of reverting to the previous release of SPFS, restoring the file systems, and restoring the oracle data.

ATTENTION

After performing a full system restore on IEMS you must also perform a subsequent central server restore. Refer to: *Restoring the Central Security Server* in *IEMS Administration and Security*, NN10336-611

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)

Restoring the oracle data is not applicable to the CBM as it does not use an oracle database.

ATTENTION

System logs indicating application and database errors, will be generated until the file systems and oracle data are restored on the system using this procedure and procedure ["Restoring the oracle data on an SPFS-based server"](#) (page 264). No database errors will be generated on the CBM as it does not use an oracle database.

Prerequisites

This procedure has the following prerequisites:

- you need SPFS CD disk #1 for the release you are reverting to
- you need the tape or DVD on which you backed up the file systems
- you need the tape or DVD on which you backed up the oracle data

Action

Use one of the following methods according to your office configuration.

- "Simplex configuration (one server)" (page 259)
- "High-availability configuration (two servers)" (page 261)

Only the "Simplex configuration (one server)" (page 259) is applicable to perform a full system restore from tape on a Sun Netra t1400 server.

Simplex configuration (one server)

Step	Action

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 SPFS CD disk#1 into the drive.
- 4 Use the following table to determine your next step.

If restoring from	Do
tape	step 5
DVD	step 6

- 5 Insert the tape on which you backed up the 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 the restore process fails at this point due to one or more disks not being labeled, which is reported as 'Bad Magic Number in Disk Label', refer to procedure 'Labelling disks on an SPFS-based server'.

If restoring from DVD, you will be prompted to insert Volume 1 of the backup DVD into the drive. Insert the 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 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.

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 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 DVD by typing

```
# eject cdrom
```

and pressing the Enter key.

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 backup DVD from the drive.

9 Use the following table to determine your next step.

If the server is hosting	Do
this SPFS-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 dbs or oinstall dbs data	step 12
oinstall dba data	step 11

- 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 SPFS-based server" \(page 264\)](#). Once the data restore is complete, execute step 13 of this procedure.
- 13 Reboot the server by typing

```
# init 6
```

 and pressing the Enter key.
- 14 Ensure the node is active by typing

```
# cd/opt/nortel/sspfs/ha
```

```
# ./ActivateNode
```

—End—

High-availability configuration (two servers)

Step	Action

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 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

- 5 Insert SPFS DVD 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 DVD on which you backed up the file systems, into the drive.

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.

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 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 DVD by typing

```
# eject cdrom
```

and pressing the Enter key.

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 backup CD or DVD from the drive.

- 10 Use the following table to determine your next step.

If the server is hosting	Do
this SPFS-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 dba data	step 13
oinstall data dbs or oinstall dbs data	step 12

- 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 SPFS-based server" \(page 264\)](#). Once the data restore is complete, execute steps 14 and 15 of this procedure.

- 14 Reboot the server by typing

```
# init 6
```

and pressing the Enter key.

- 15 Ensure the node is active by typing

```
# cd/opt/nortel/sspfs/ha
```

```
# ./ActivateNode
```

- 16 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" \(page 237\)](#).

You have completed this procedure.

—End—

Restoring the oracle data on an SPFS-based server

Application

Use this procedure to restore the oracle data from a backup tape or DVD on a Server Platform Foundation Software (SPFS)-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)

Restoring the oracle data is not applicable to the MG 9000 Manager or the CBM as they do not use an oracle database.

Prerequisites

You need the tape or DVD on which you backed up the oracle data. If the data was backed up by the backup restore manager, you need the name of the file located in directory /data/bkresmgr/backup.

Action

Perform the following steps to complete this procedure.

Step	Action

<i>At the server</i>	

- 1 Use the following table to determine how to start this procedure.

If	Start at step
restoring from tape or DVD	step 2
restoring from a file	step 3

- 2 Insert the tape or DVD on which you backed up the oracle data, into the drive. If restoring the data from a file, start at [step 3](#).

At your workstation

- 3 Log in to the server.

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server on which you are performing the data restore

- 4 When prompted, enter your user ID and password.

- 5 Change to the root user.

```
$ su -
```

and press the Enter key.

- 6 When prompted, enter the root password.

- 7 Verify the permissions on the restore log directory (bkslog).

```
# ls -alrt /var/opt/nortel
```

and press 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 9
are not drwxrwxrwt	step 8

- 8 Change the permissions of bkslog.

```
# chmod 1777 /var/opt/nortel/bkslog
```

and press the Enter key.
- 9 Determine if server applications have been stopped.

```
# servquery -status all
```

and press the Enter key.
- 10 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 "Starting the SAM21 Manager server application" (page 562) "Stopping the NPM server application" (page 560)
MG 9000 Manager and mid-tier server applications	ATM/IP Security and Administration, NN10402-600 MG 9000 Security and Administration, NN10162-611, if required
IEMS server application	IEMS Security and Administration, NN10336-611, if required

- 11 Verify the permissions, owner and group of /data/oradata by typing:

```
#ls -l /data
```

and pressing the Enter key.

Example response:

```
drwxr-xr-x  7 oracle    oinstall    512 Oct
16 18:13 oradata
```

- 12** Use the following table to determine the next step:

If	Go to
permission is "drwxr-xr-x" owner is "oracle" and group is "oinstall" as shown in the example in the previous step	step 14
values do not match the example in the previous step	step 13

- 13** Change the permission, owner and group of /data/oradata by typing:

```
#chmod 755 /data/oradata
```

and pressing the Enter key

```
#chown oracle /data/oradata
```

and pressing the Enter key

```
#chgrp oinstall /data/oradata
```

and pressing the Enter key

- 14** Verify the permissions, owner and group of /data/oradata/arch by typing:

```
#ls -l /data/oradata
```

and pressing the Enter key.

Example response:

```
drwxr-xr-x  4 oracle  oinstall    512
Oct 16 18:36 arch
```

- 15** Use the following table to determine the next step:

If	Go to
permission is "drwxr-xr-x" owner is "oracle" and group is "oinstall" as shown in the example in the previous step	step 17
values do not match the example in the previous step	step 16

- 16** Change the permission, owner and group of /data/oradata/arch by typing:

```
#chmod 755 /data/oradata/arch
```

and pressing the Enter key

```
#chown oracle /data/oradata/arch
```


and pressing the Enter key

```
#chgrp oinstall /data/oradata/arch
```

and pressing the Enter key

- 17** Use the following table to determine your next step.

If	Do
restoring from tape or DVD	step 18
restoring from a file	step 20

- 18** Restore the database from backup tape or DVD.

```
$ /opt/nortel/SPFS/bks/rsdata
```

and press the Enter key.

- 19** Remove the tape from the drive, or eject the DVD from the drive as follows:

- a. Ensure you are at the root directory level.

```
# cd /
```

and press the Enter key.

- b. Eject the DVD.

```
# eject cdrom
```

and press the enter key.

If the DVD drive tray does 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
```

Press the eject button located on the front of the DVD drive.

- c. Remove the DVD from the drive.

Proceed to [step 21](#).

- 20** Restore the database from the backup file.

```
$ /opt/nortel/SPFS/bks/rsdata -f /data/bkresmgr/backup /<filename>
```

and press the Enter key.

Variable	Value
<filename>	is the name of the backup file created by the backup restore manager

- 21** Verify that the database restored properly.

```
# queryAllFaults
```

and press the Enter key.

If an alarm appears like the following, the database was not restored properly:

```
*** SPFS330 Import of Oracle data caused corruption
ORA-22337: Error importing Oracle data cs2kaps=rtp6ba
ckupsesm;NODE=rtp6backupsesm;CLASS=SW;SWTYPE=Database
Fri Jun 10 15:48:59 2005
```

- 22** Use the information in the following table to determine the next step.

If	Do
no alarm appears	step 23
alarm appears	contact Nortel
the database did not restore properly	contact Nortel

- 23** Use the following table to determine your next step.

If	Do
WebPKProxy is configured	step 24
WebPKProxy is not configured	step 27

- 24** Restore the WebPKProxy.

```
# ls /data/pkclient/certificates
```

and press the Enter key.

- 25 Use the following table to determine your next step.

If	Do
the following files are associated with this machine: • CA1_Cert.pem • CA2_Cert.pem • TRUSTED_Cert.pem	step 26
the above files do not exist	step 27

- 26 Reconfigure WebPKProxy as follows:

- a. From the CLI, select Configuration ---> Security Services Configuration ---> Certificate Manager Certificate Installation ---> install_certs.

Wait for the script to complete. Verify that no errors displayed.

- b. From the CLI, select Configuration ---> Security Services Configuration ---> WebPKProxy/PKClient---> register_pkclient.

- c. Enter the host name of the Certificate Manager.

The Certificate Manager box must be fully functional for this step to succeed.

Wait for the script to complete. Verify that no errors displayed.

- 27 Start the server applications that run on the server.

For	Refer to
CS 2000 Management Tools server applications	Stopping the SESM server application "Starting the SAM21 Manager server application" (page 562) "Stopping the NPM server application" (page 560) ATM/IP Security and Administration, NN10402-600
MG 9000 Manager and mid-tier server applications	the MG 9000 Security and Administration document, NN10162-611, if required
IEMS server application	the IEMS Security and Administration document, NN10336-611, if required

If one or more applications do not start, contact Nortel for assistance.
You have completed this procedure.

—End—

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

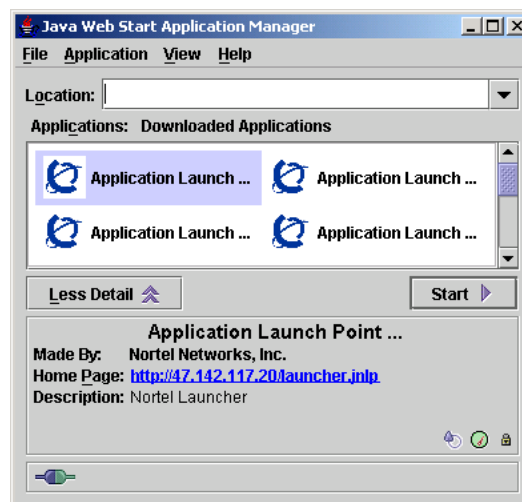
Action

Perform the following steps to complete this procedure.

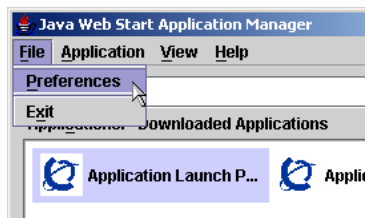
Step	Action

At your workstation

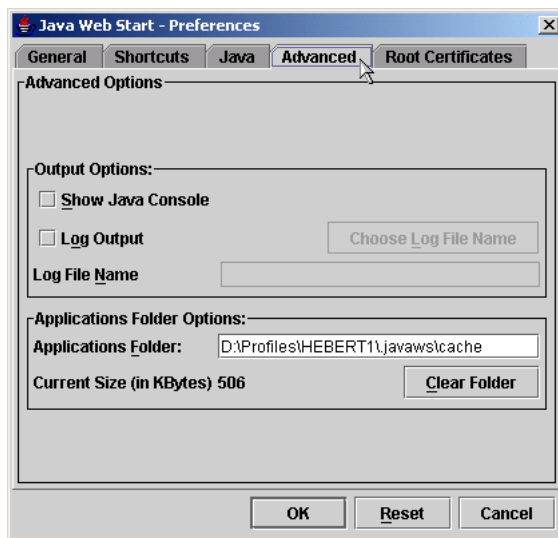
- 1 Access the Java Web Start Application Manager.



- 2 Click **File->Preferences** to access the Preferences window.



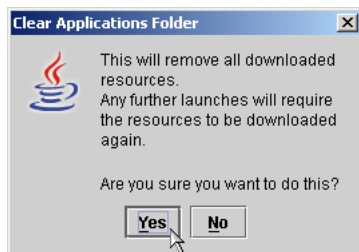
- 3 Click the **Advanced** tab to access the Advanced window.



- 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.

—End—

Removing a breaker module

Application

Remove a breaker module to replace it due to a failure or to ensure safe removal of the breaker interface panel (BIP).

The following frames contain an alarm module:

- Services Application module Frame (SAMF) for CS 2000 and CS 2000 Compact
- Cabinetized Operations Administration and Maintenance (COAM) frame for CS 2000 and CS 2000 Compact
- Call Control Frame (CCF) for CS 2000 Compact only
- Ethernet Routing Switch (ERS) 8600 Carrier Voice over IP Frame, which is also referred to as the CS LAN Frame, for CS 2000 and CS 2000 Compact
- Universal Signaling Point (USP), which can be one of USP Compact CCF, USP Frame with a Control Application Module (CAM) shelf, or USP in a COAM

Interval

Remove a breaker module when the module fails.

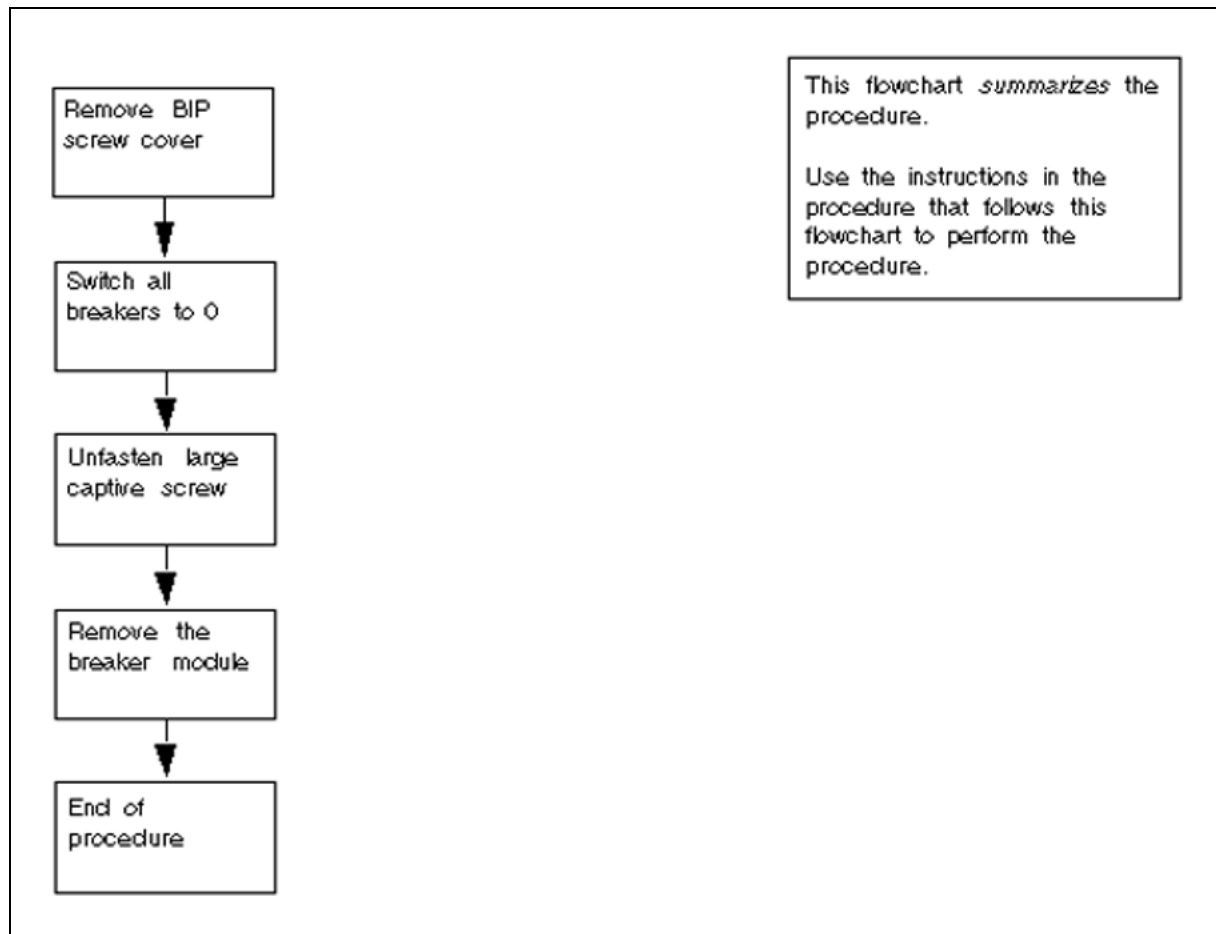
Common procedures

You must be familiar with the safety considerations and best practices for your location.

Action

This procedure contains a summary flowchart as an summary of the procedure. Follow the exact steps to perform this procedure.

Removing a breaker module



WARNING

Make sure that you have protection against electrostatic discharge (ESD). Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP).



CAUTION

Read and make sure you thoroughly understand the instructions in this procedure before removing the BIP alarm module. While the module is removed, alarm reporting is temporarily suspended.

Step Action

At the front of the BIP

- 1 Grasp the BIP screw cover and pull it out of the BIP chassis.

- 2 Switch all breakers to 0.
- 3 Unfasten the large captive screw of the breaker module.
- 4 While pinching the lower front lip of the module with your thumb and finger tips, pull gently but firmly straight out until the alarm disengages. Stop pulling when the front of the module is past the front of the BIP.

**DANGER**

Allow 15 seconds before removing the breaker module. Capacitors on the breaker module must be allowed to discharge.

- 5 Pull the module straight out of the BIP.
- 6 This procedure is complete.

—End—

Replacing a breaker module

Application

Use this procedure to replace a breaker module in the breaker interface panel (BIP).

The following frames contain an alarm module:

- Services Application module Frame (SAMF) for CS 2000 and CS 2000 Compact
- Cabinetized Operations Administration and Maintenance (COAM) frame for CS 2000 and CS 2000 Compact
- Call Control Frame (CCF) for CS 2000 Compact only
- Ethernet Routing Switch (ERS) 8600 Carrier Voice over IP Frame, which is also referred to as the CS LAN Frame, for CS 2000 and CS 2000 Compact
- Universal Signaling Point (USP), which can be one of USP Compact CCF, USP Frame with a Control Application Module (CAM) shelf, or USP in a COAM

Interval

Replace a breaker module when the module fails.

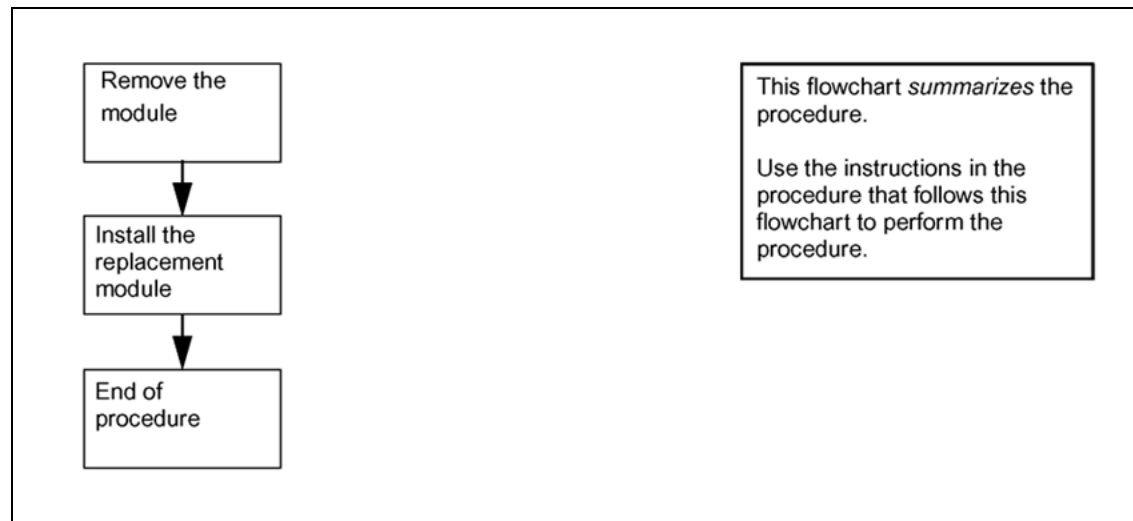
Common procedures

You must be familiar with the safety considerations and best practices for your location.

Action

This procedure contains a summary flowchart as an summary of the procedure. Follow the exact steps to perform this procedure.

Replacing a breaker module



WARNING

Make sure that you have protection against electrostatic discharge (ESD). Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP).



CAUTION

Read and make sure you thoroughly understand the instructions in this procedure before replacing the BIP alarm module. While the module is removed, alarm reporting is temporarily suspended.

Step	Action

At the front of the BIP

1	Remove the failed breaker module. To remove the breaker module, use the procedure "Removing a BIP alarm module" (page 275) . When the module has been removed, proceed to step 2 of this procedure.
2	Install the replacement breaker module. To replace the module, use the procedure "Installing a BIP alarm module" (page 280) .
3	This procedure is complete.

—End—

Installing a BIP alarm module

Application

The BIP alarm module indicates hardware alarms, drives the alarm light-emitting diode (LED) board and monitors the state of the power breakers.

The following frames contain an alarm module:

- Services Application module Frame (SAMF) for CS 2000 and CS 2000 Compact
- Cabinetized Operations Administration and Maintenance (COAM) frame for CS 2000 and CS 2000 Compact
- Call Control Frame (CCF) for CS 2000 Compact only
- Ethernet Routing Switch (ERS) 8600 Carrier Voice over IP Frame, which is also referred to as the CS LAN Frame, for CS 2000 and CS 2000 Compact
- Universal Signaling Point (USP), which can be one of USP Compact CCF, USP Frame with a Control Application Module (CAM) shelf, or USP in a COAM

Interval

Install a BIP alarm module as part of a replacement or initial installation task.

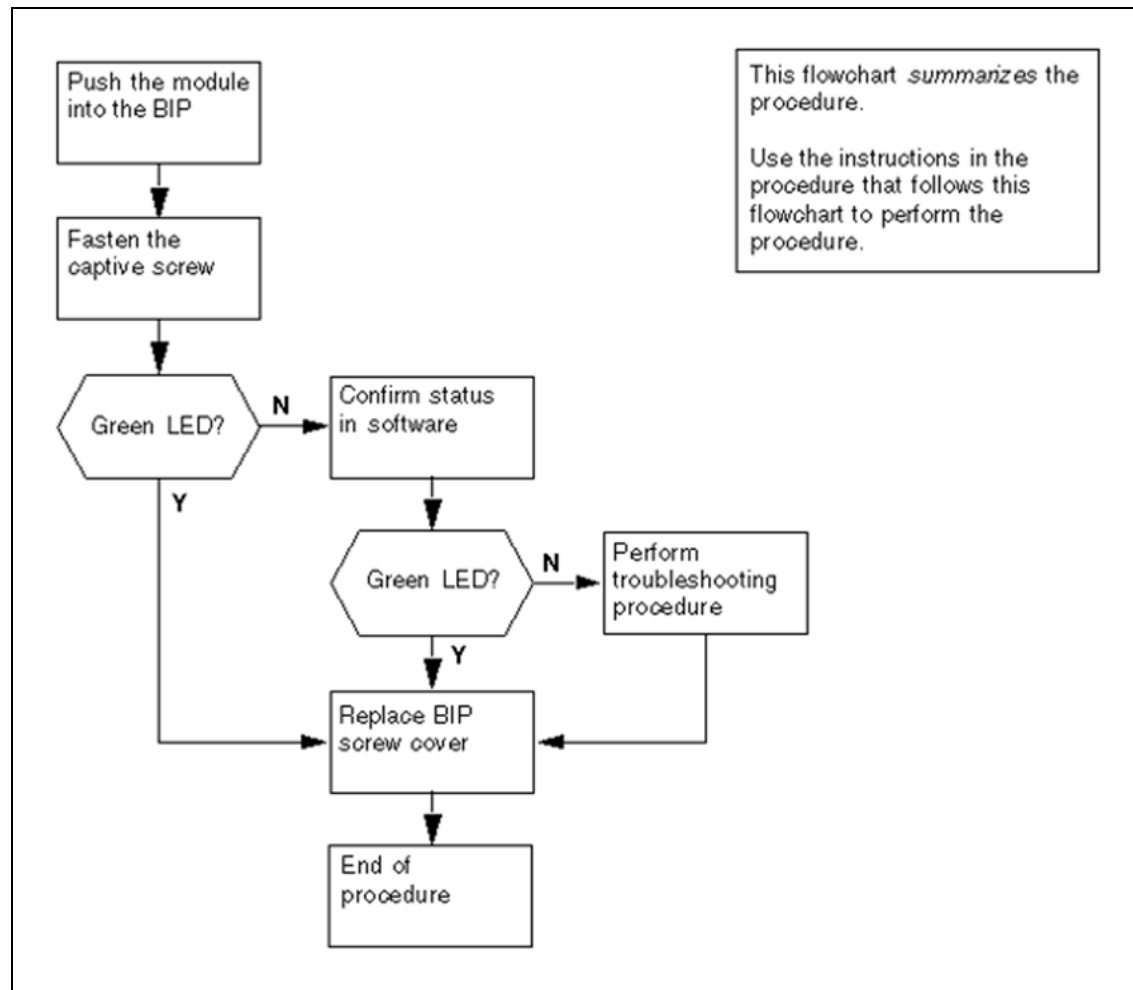
Common procedures

You must be familiar with the safety considerations and best practices for your location.

Action

This procedure contains a summary flowchart as an summary of the procedure. Follow the exact steps to perform this procedure.

Installing a BIP alarm module

**CAUTION****Risk of static electricity damage**

Make sure that you have protection against electrostatic discharge (ESD). Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP).

**CAUTION****Loss of service**

Read and make sure you thoroughly understand the instructions in this procedure before removing the BIP alarm module. To minimize the effect of removing an alarm module, insert the replacement immediately. Once the alarm module is installed, software alarms stop.

Installing a BIP alarm module

Step	Action

At the front of the BIP

- 1 Get a BIP alarm module PEC NTRX51HC.
- 2 Grip the replacement alarm module with the fingers and thumb of one hand on the lower front lip (the screw end) and use the other hand to align the rear of the module with the opening in the BIP.
- 3 Push the module gently but firmly straight in until it engages. Stop pushing when the front of the module is flush with the front of the BIP.
- 4 Engage and fasten the large slotted captive screw of the alarm module. Do not strip the threads or the hole because the module cannot seat properly.
- 5 Check the alarm module status LEDs.

If the color is	Do
green	step 7
other than green	step 6

- 6 Have the network operator confirm the status in the software.

If the color is	Do
green	step 7
other than green	Perform troubleshooting procedures to clear the problem, and continue to step 7 .

- 7 Replace the BIP screw cover by aligning the screw cover with the BIP chassis and pushing it into place. The BIP screw cover snaps into the snap-in posts.
- 8 This procedure is complete.

—End—

Removing a BIP alarm module

Application

Remove a BIP alarm module to replace it due to a failure or to ensure safe removal of the BIP.

The following frames contain an alarm module:

- Services Application module Frame (SAMF) for CS 2000 and CS 2000 Compact
- Cabinetized Operations Administration and Maintenance (COAM) frame for CS 2000 and CS 2000 Compact
- Call Control Frame (CCF) for CS 2000 Compact only
- Ethernet Routing Switch (ERS) 8600 Carrier Voice over IP Frame, which is also referred to as the CS LAN Frame, for CS 2000 and CS 2000 Compact
- Universal Signaling Point (USP), which can be one of USP Compact CCF, USP Frame with a Control Application Module (CAM) shelf, or USP in a COAM

Interval

Remove a BIP alarm module when the module fails.

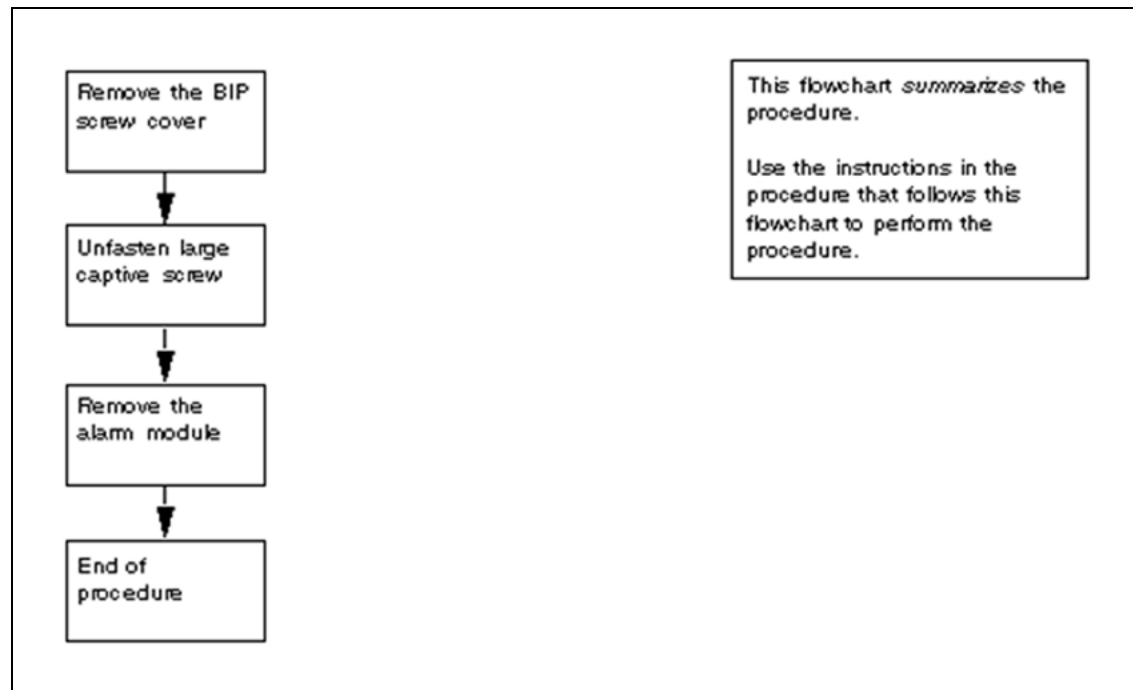
Common procedures

You must be familiar with the safety considerations and best practices for your location.

Action

This procedure contains a summary flowchart as an summary of the procedure. Follow the exact steps to perform this procedure.

Removing a BIP alarm module



CAUTION

Risk of static electricity damage

Make sure that you have protection against electrostatic discharge (ESD). Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP).



CAUTION

Loss of service

Read and make sure you thoroughly understand the instructions in this procedure before removing the BIP alarm module. While the module is removed, alarm reporting is temporarily suspended.

Removing a BIP alarm module

Step	Action

At the front of the BIP

1	Grasp the BIP screw cover and pull it out of the snap-in posts on the BIP chassis.
2	Unfasten the large captive screw of the BIP alarm module.
3	While pinching the lower front lip of the module with your thumb and finger tips, pull gently but firmly straight out until the alarm

disengages. Stop pulling when the front of the module is past the front of the BIP.

**DANGER****Risk of electric shock**

Allow 15 seconds before removing the breaker module. Capacitors on the breaker module must be allowed to discharge.

- 4 Pull the module straight out of the BIP.
- 5 This procedure is complete.

—End—

Replacing a BIP alarm module

Application

Use this procedure to replace a breaker interface panel (BIP) alarm module.

The following frames contain an alarm module:

- Services Application module Frame (SAMF) for CS 2000 and CS 2000 Compact
- Cabinetized Operations Administration and Maintenance (COAM) frame for CS 2000 and CS 2000 Compact
- Call Control Frame (CCF) for CS 2000 Compact only
- Ethernet Routing Switch (ERS) 8600 Carrier Voice over IP Frame, which is also referred to as the CS LAN Frame, for CS 2000 and CS 2000 Compact
- Universal Signaling Point (USP), which can be one of USP Compact CCF, USP Frame with a Control Application Module (CAM) shelf, or USP in a COAM

Interval

Replace a BIP alarm module when the module fails.

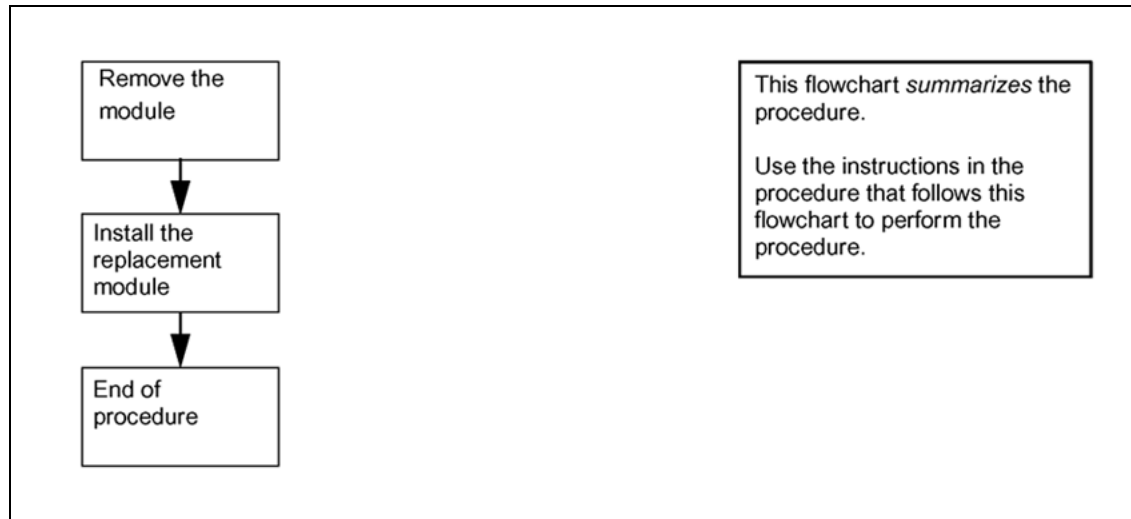
Common procedures

You must be familiar with the safety considerations and best practices for your location.

Action

This procedure contains a summary flowchart as an summary of the procedure. Follow the exact steps to perform this procedure.

Replacing a BIP alarm module



CAUTION

Risk of static electricity damage

Make sure that you have protection against electrostatic discharge (ESD). Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP).



CAUTION

Loss of service

Read and make sure you thoroughly understand the instructions in this procedure before replacing the BIP alarm module. While the module is removed, alarm reporting is temporarily suspended.

Replacing a BIP alarm module

Step	Action

At the front of the BIP

1	Remove the failed BIP alarm module. To remove the module, use the procedure " Removing a BIP alarm module " (page 275). When the module has been removed, proceed to step 2 of this procedure.
2	Install the replacement BIP alarm module. To replace the module, use the procedure " Installing a BIP alarm module " (page 280).
3	This procedure is complete.

—End—

CVoIP Solution Troubleshooting

Use this document to isolate and resolve certain network faults for the CVoIP 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 CVoIP solutions. The table 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

Troubleshooting task
CS 2000 problems "Troubleshooting multiple DS1 carriers in a Carrier Fail Loss (CFL) state" (page 292) "Troubleshooting DS1 carriers in an intermittent Carrier Fail Loss (CFL) state" (page 295) "Troubleshooting DS0s trunks that are in a Carrier Fail Loss (CFL) state" (page 298) "Troubleshooting DS0s trunks that are in a peripheral manual busy (PMB) state" (page 300) "Troubleshooting DS0s trunks that are in a System Busy (SB) state" (page 301) "Troubleshooting DS0 trunks that are in a lock out (LO) state" (page 302) "Troubleshooting DS0s trunks that are in a remote manual busy (RMB) state" (page 303) "Troubleshooting line(s) in a permanent lock out (PLO) state" (page 304) "Troubleshooting line(s) in a manual busy (MB) state" (page 306) "Troubleshooting line(s) in a system busy (SB) state" (page 307) GWC problems "Troubleshooting a GWC that continuously initializes and fails to return to service (RTS)" (page 308) "Troubleshooting a GWC that fails to boot" (page 310) "Troubleshooting a GWC that has a poor call completion rate" (page 311) "Troubleshooting PRI trunks that remain in a lockout state" (page 312) "Troubleshooting a failed attempt to create a GWC image" (page 314) "Troubleshooting alarms generated on a GWC" (page 317) "Troubleshooting GWC peripheral module log reports" (page 318)

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" (page 321)

"Troubleshooting a failure to add or delete a GWC" (page 323)

"Troubleshooting when an OSSGate session fails to launch from a PC" (page 324)

"Troubleshooting a connection failure when adding a GWC node" (page 325)

"Troubleshooting a failure of the CS 2000 Management Tools alarm manager to properly set alarm date a" (page 330)

"Troubleshooting small gateway IP addresses that are reset to 0.0.0.0 in the CS 2000 Management Tools" (page 332)

"Troubleshooting a failure to RTS a DMS Maintenance Application that is IsTb" (page 334)

"Troubleshooting a failure to add a fourth Media Gateway 15000 to a GWC" (page 335)

"Troubleshooting a failure to perform maintenance actions while using the CS 2000 Management Tools" (page 337)

"Troubleshooting a failure to launch CS 2000 SAM21 Manager, CS 2000 Management Tools GUI, or Network " (page 339)

"Troubleshooting problems arising when an SSL certificate is changed and the CM hostname is new or ch" (page 341)

"Procedure for troubleshooting combined failures to start SESM server application, to apply a patch t" (page 342)

"Troubleshooting a failure to delete a line from a media gateway in the IAC or Intl IAC solution" (page 344)

"Troubleshooting a failed attempt to input the SDNA command in OSSGate" (page 346)

"Troubleshooting a failure to add an endpoint to a GWC during line provisioning of the IAC or Intl IA" (page 347)

"Troubleshooting combined CS 2000 Management Tools failures" (page 342)

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

Detailed procedure
"How to correlate carrier information from the MAPCI, to the GWC, and Media Gateway 15000/7400" (page 375) View GWC PM logs "Checking for Media Gateway logs" (page 381) "Checking for MSC Server 1000 XACoreCS 2000 logs" (page 382) View and troubleshoot GWC service alarms View GWC platform hardware alarms "Troubleshooting a provisioning error with a GWC card or node" (page 319) "How to correlate line information from the MAPCI to the GWC and line gateway" (page 368) "Ethernet Routing Switch 8600 Ethernet port configuration, and 100Base-T cable replacement" (page 384) "Viewing SESM configuration settings" (page 552) Diagnose problems with a GWC card that cannot be booted Restart or reboot a GWC card View media proxies associated with a GWC node Setting the CS 2000 MSC Server 1000 CLLI on an SPFS-based server View and troubleshoot GWC service alarms View GWC platform hardware alarms View GWC logs in syslog files View GWC PM logs Perform a CS 2000 data integrity audit "Take a manual GWC software image" (page 418) (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" (page 350) "Pinging the CS 2000 Core Manager" (page 351) "Ensuring that the OSS Comms Svcs and OSS and Application Svcs are in service" (page 354) "Checking the status of the DDMS proxy" (page 357) "Stopping and starting the DDMS proxy" (page 554)

Detailed procedure

["Starting the SESM server application" \(page 548\)](#)

Configuring a Timing Provider on an SPFS-Based Server

Reconfigure NTP service

["Adding the CS 2000 Management Tools Server as a DDMS client of the CS 2000 Core Manager" \(page 358\)](#)

["Restarting the Apache Web server" \(page 361\)](#)

Configuring the SESM server application

["Checking the occupancy of the /opt/ directory on the CS 2000 Management Tools server" \(page 362\)](#)

Changing the Oracle user password on an SPFS-based server

["Adding LEN information back into the XA-Core" \(page 364\)](#)

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

Step	Action						
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" (page 375).						
2	Determine if the DS1 carriers (in the CFL state) span more than one GWC. <table> <tr> <th>If the DS1 carriers</th><th>Do</th></tr> <tr> <td>span more than one GWC</td><td>step 3</td></tr> <tr> <td>do not span more than on GWC</td><td>step 4</td></tr> </table>	If the DS1 carriers	Do	span more than one GWC	step 3	do not span more than on GWC	step 4
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 <i>GWC Fault Management</i>, 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. <table> <tr> <th>If all the DS1 carriers in the CFL state are</th><th>Do</th></tr> <tr> <td>on a single GWC</td><td>step 5</td></tr> <tr> <td>not on a single GWC</td><td>step 7</td></tr> </table>	If all the DS1 carriers in the CFL state are	Do	on a single GWC	step 5	not on a single GWC	step 7
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 <i>GWC Fault Management</i>, 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 <i>GWC Fault Management</i>, 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
If 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 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.

—End—

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

Step	Action						
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" (page 375).						
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. <table> <tr> <th>If there are</th><th>Do</th></tr> <tr> <td>GWC PM logs being generated</td><td>step 3</td></tr> <tr> <td>no GWC PM logs being generated</td><td>step 5</td></tr> </table>	If there are	Do	GWC PM logs being generated	step 3	no GWC PM logs being generated	step 5
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 <i>GWC Fault Management</i>, 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. <table> <tr> <th>If the problem</th><th>Do</th></tr> <tr> <td>has been resolved</td><td>step 18</td></tr> <tr> <td>has not been resolved</td><td>step 5</td></tr> </table>	If the problem	Do	has been resolved	step 18	has not been resolved	step 5
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 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 CS2000-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, and SAM21 logs, refer to *CVoIP 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.

—End—

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.

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

Step	Action						
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" (page 375).						
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 <table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>there are GWC PM logs being generated</td><td>step 2</td></tr> <tr> <td>there are no GWC PM logs being generated</td><td>step 5</td></tr> </table>	If	Do	there are GWC PM logs being generated	step 2	there are no GWC PM logs being generated	step 5
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" (page 319).						
4	Determine if the original DS0 problem has been resolved. <table> <tr> <th>If the problem</th><th>Do</th></tr> <tr> <td>has been resolved</td><td>step 8</td></tr> <tr> <td>has not been resolved</td><td>step 5</td></tr> </table>	If the problem	Do	has been resolved	step 8	has not been resolved	step 5
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.

—End—

Troubleshooting DS0s trunks that are in a peripheral manual busy (PMB) state

Use this task to troubleshoot one or more DS0 trunks that are in a peripheral 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

Step	Action						
1	A GWC is not accessible, with the result that one or more DS0s are in a PMB state. Check XA-Core logs for the occurrence of a PM181 log. Refer to <i>GWC Fault Management</i> , NN10202-911, to fix the problem.						
2	Determine if you have fixed the problem. <table><tr><th>If the problem</th><th>Do</th></tr><tr><td>has been corrected</td><td>step 4</td></tr><tr><td>has not been corrected</td><td>step 3</td></tr></table>	If the problem	Do	has been corrected	step 4	has not been corrected	step 3
If the problem	Do						
has been corrected	step 4						
has not been corrected	step 3						
3	Contact your next level of support.						
4	You have completed this procedure.						
—End—							

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

Step	Action						
1	There is a status mismatch between the MSC Server 2000 Call Agent 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: • <i>MSC Server 1000 Fault Management</i>, NN20000-222 • <i>XA-Core Reference Manual</i>, 297-8991-810 • <i>CVoIP Fault Management Logs Reference</i>, NN10275-909 • <i>GWC Fault Management</i>, NN10202-911 • <i>DMS-MTX Logs Reference Manual</i>, 411-2131-510						
2	Determine if you have fixed the problem and are able to return the DS0 links to service. <table> <tr> <th>If the problem</th><th>Do</th></tr> <tr> <td>has been resolved</td><td>step 4</td></tr> <tr> <td>has not been resolved</td><td>step 3</td></tr> </table>	If the problem	Do	has been resolved	step 4	has not been resolved	step 3
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.						
—End—							

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

Step	Action						
1	There is an SS7 problem. Check for logs and alarms to isolate the problem. Refer to the following documents for more information: • <i>Communication Server 2000 Fault Management</i>, NN10083-911 • <i>XA-Core Reference Manual</i>, 297-8991-810 • <i>CVoIP Fault Management Logs Reference</i>, NN10275-909 • <i>USP Fault Management</i>, NN10071-911						
2	Determine if you have fixed the SS7 problem and are able to return the DS0 trunks to service. <table> <tr> <th>If the problem</th><th>Do</th></tr> <tr> <td>has been fixed</td><td>step 4</td></tr> <tr> <td>has not been fixed</td><td>step 3</td></tr> </table>	If the problem	Do	has been fixed	step 4	has not been fixed	step 3
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.						
—End—							

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

Step	Action
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.
—End—	

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

Step	Action						
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" (page 368).						
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. <table> <tr> <th>If the device</th><th>Do</th></tr> <tr> <td>can be reached</td><td>step 8</td></tr> <tr> <td>cannot be reached</td><td>step 3</td></tr> </table>	If the device	Do	can be reached	step 8	cannot be reached	step 3
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. <table> <tr> <th>If the device</th><th>Do</th></tr> <tr> <td>can be reached</td><td>step 8</td></tr> <tr> <td>cannot be reached</td><td>step 4</td></tr> </table>	If the device	Do	can be reached	step 8	cannot be reached	step 4
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 Ethernet Routing Switch 8600. Use the Device Manager and the appropriate Ethernet Routing Switch 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.

—End—

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

Step	Action
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.
—End—	

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

Step	Action
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 <i>MG 9000 Fault Management</i>, 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.

—End—

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

Step	Action
1	Determine the setting of the ethernet port on the Ethernet Routing Switch 8600. Refer to "Ethernet Routing Switch 8600 Ethernet port configuration, and 100Base-T cable replacement" (page 384).
2	Ensure the Ethernet port settings on the Ethernet Routing Switch 8600 have Auto Negotiation set to True . Refer to "Ethernet Routing Switch 8600 Ethernet port configuration, and 100Base-T cable replacement" (page 384).
3	Determine that you are able to successfully return the GWC to service.

If able to return the GWC to service	Do
able to return the GWC to service	step 11
unable to return the GWC to service	step 5

- 4 Determine if the IP addressing scheme for the GWC is correct.
Refer to View media proxies associated with a GWC node.

If the IP addressing scheme	Do
is correct	step 6
is incorrect	step 5

- 5 Assign four consecutive IP addresses to the GWC. The first IP address must be divisible by 4. For more information, refer to *GWC Configuration Management*, 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 Ethernet Routing Switch 8600 router is correctly installed and fully functional.

Refer to "[Ethernet Routing Switch 8600 Ethernet port configuration, and 100Base-T cable replacement](#)" (page 384).

If the cabling	Do
is functional	step 10
not functional	step 8

- 8 Replace the cabling between the GWC and the Ethernet Routing Switch 8600 router with cabling that supports 100Mb/s bandwidth.

Refer to "[Ethernet Routing Switch 8600 Ethernet port configuration, and 100Base-T cable replacement](#)" (page 384).

- 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.

—End—

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

Step	Action						
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. <table><tr><th>If you are</th><th>Do</th></tr><tr><td>able to boot the GWC successfully</td><td>step 4</td></tr><tr><td>unable to boot the GWC successfully</td><td>step 3</td></tr></table>	If you are	Do	able to boot the GWC successfully	step 4	unable to boot the GWC successfully	step 3
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.						
—End—							

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

Step	Action						
1	Determine the setting of the ethernet port on the Ethernet Routing Switch 8600. Refer to "Ethernet Routing Switch 8600 Ethernet port configuration, and 100Base-T cable replacement" (page 384). <table> <tr> <th>the Ethernet Routing Switch 8600 is set to</th><th>Do</th></tr> <tr> <td>100Base-T Half Duplex Auto Negotiate = N</td><td>step 2</td></tr> <tr> <td>anything else</td><td>step 4</td></tr> </table>	the Ethernet Routing Switch 8600 is set to	Do	100Base-T Half Duplex Auto Negotiate = N	step 2	anything else	step 4
the Ethernet Routing Switch 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 Ethernet Routing Switch 8600 to 100Base-T Half Duplex Auto Negotiate = N. Refer to "Ethernet Routing Switch 8600 Ethernet port configuration, and 100Base-T cable replacement" (page 384).						
3	Determine if the GWC call completion rate is acceptable. <table> <tr> <th>the GWC call completion rate is</th><th>Do</th></tr> <tr> <td>acceptable</td><td>step 5</td></tr> <tr> <td>unacceptable</td><td>step 4</td></tr> </table>	the GWC call completion rate is	Do	acceptable	step 5	unacceptable	step 4
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.						
—End—							

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

Step	Action						
1	Determine if the Media Gateway hostname matches the gateway name that is datafilled in the CS 2000 Management Tools software.						
	<table> <tr> <th>the Media Gateway hostname</th><th>Do</th></tr> <tr> <td>matches the gateway name</td><td>step 2</td></tr> <tr> <td>does not match the gateway name</td><td>step 5</td></tr> </table>	the Media Gateway hostname	Do	matches the gateway name	step 2	does not match the gateway name	step 5
the Media Gateway hostname	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 " (page 350).						
	<table> <tr> <th>the carrier endpoint name</th><th>Do</th></tr> <tr> <td>contains a leading zero</td><td>step 7</td></tr> <tr> <td>does not contain a leading zero</td><td>step 3</td></tr> </table>	the carrier endpoint name	Do	contains a leading zero	step 7	does not contain a leading zero	step 3
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 <i>Nortel Networks Media Gateway 7480/15000 Technology Fundamentals</i> , NN10600-780, to fix the problem.						
4	Determine if you have eliminated the PRI trunk lockout state.						
	<table> <tr> <th>the PRI trunk lockout state</th><th>Do</th></tr> <tr> <td>has been eliminated</td><td>step 8</td></tr> <tr> <td>has not been eliminated</td><td>step 7</td></tr> </table>	the PRI trunk lockout state	Do	has been eliminated	step 8	has not been eliminated	step 7
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.

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.

—End—

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

Step	Action								
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.								
<table> <tr> <th>If the RC value equals</th><th>Do</th></tr> <tr> <td>-4</td><td>step 3</td></tr> <tr> <td>-9</td><td>step 5</td></tr> <tr> <td>any other value</td><td>step 7</td></tr> </table>		If the RC value equals	Do	-4	step 3	-9	step 5	any other value	step 7
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" (page 418) (the last page of the procedure).								
4	Determine if you are able to correct the problem and successfully create a GWC image.								
<table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>you are able to create a GWC image</td><td>step 10</td></tr> <tr> <td>you are unable to create a GWC image</td><td>step 9</td></tr> </table>		If	Do	you are able to create a GWC image	step 10	you are unable to create a GWC image	step 9		
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.

—End—

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

Step	Action						
1	Determine if there are logs or alarms generated indicating a possible GWC card or node provisioning problem.						
	<table> <tr> <th>If there are</th><th>Do</th></tr> <tr> <td>alarms or logs generated</td><td>step 2</td></tr> <tr> <td>no alarms or logs generated</td><td>step 4</td></tr> </table>	If there are	Do	alarms or logs generated	step 2	no alarms or logs generated	step 4
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 procedurePerform a CS 2000 data integrity audit Then perform the actions necessary to fix the problem.						
3	Determine if you have corrected the provisioning error associated with the GWC card.						
	<table> <tr> <th>If the provisioning error is</th><th>Do</th></tr> <tr> <td>corrected</td><td>step 5</td></tr> <tr> <td>not corrected</td><td>step 4</td></tr> </table>	If the provisioning error is	Do	corrected	step 5	not corrected	step 4
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.						
—End—							

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](#)" (page 314) 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

Step	Action						
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 " (page 552).						
<table><tr><th>If the CM CLLI is configured</th><th>Do</th></tr><tr><td>correctly</td><td>step 5</td></tr><tr><td>incorrectly</td><td>step 3</td></tr></table>		If the CM CLLI is configured	Do	correctly	step 5	incorrectly	step 3
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 MSC Server 1000 CLLI on an SPFS-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.						
<table><tr><th>If</th><th>Do</th></tr><tr><td>you have corrected the problem</td><td>step 6</td></tr><tr><td>you have not corrected the problem</td><td>step 5</td></tr></table>		If	Do	you have corrected the problem	step 6	you have not corrected the problem	step 5
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.

—End—

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

Step	Action						
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.						
	<table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>you are able to add or delete a GWC successfully</td><td>step 5</td></tr> <tr> <td>you are unable to add or delete a GWC successfully</td><td>step 4</td></tr> </table>	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
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.						
—End—							

Troubleshooting when an OSSGate session fails to launch from a PC

Use this task to troubleshoot an OSSGate session that fails to launch from 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

Step	Action						
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. <pre>'Incomplete login information supplied'</pre> 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. <table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>you were able to launch OSSGate</td><td>step 4</td></tr> <tr> <td>you were unable to launch OSSGate</td><td>step 3</td></tr> </table>	If	Do	you were able to launch OSSGate	step 4	you were unable to launch OSSGate	step 3
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.						
—End—							

Troubleshooting a connection failure when adding a GWC node

Use this task to troubleshoot a connection failure when adding a GWC node.

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

Step	Action						
1	Determine if you received the following message when attempting to add the GWC node: <pre>'An error has been detected while trying to connect to the Server. Please close the current session and restart the client.'</pre> <table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>you received the message</td><td>step 2</td></tr> <tr> <td>you did not receive the message</td><td>step 12</td></tr> </table>	If	Do	you received the message	step 2	you did not receive the message	step 12
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" (page 351). <table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>you were able to ping the CS 2000 Core Manager</td><td>step 4</td></tr> <tr> <td>you were unable to ping the CS 2000 Core Manager</td><td>step 3</td></tr> </table>	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
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 OSS Comms 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"](#) (page 354).

- 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"](#) (page 357).

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"](#) (page 554).

- 10 Restart the SESM server application.
Refer to "Starting the SESM server application" (page 548).
- 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.

—End—

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

Step	Action						
1	If the SESM server fails to start, determine if you have received the following CS 2000 Management Tools server database error message: <pre>java.sql.SQLException: ORA-01034:ORACLE not available ORA-27101:shared memory realm does not exist SVR4 Error 2: No such file or directory</pre> <table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>you received the message</td><td>step 2</td></tr> <tr> <td>you did not receive the message</td><td>step 5</td></tr> </table>	If	Do	you received the message	step 2	you did not receive the message	step 5
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. <table> <tr> <th>If the Oracle server</th><th>Do</th></tr> <tr> <td>is running</td><td>step 5</td></tr> <tr> <td>is not running</td><td></td></tr> </table>	If the Oracle server	Do	is running	step 5	is not running	
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.

—End—

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

Step	Action						
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. <table border="1"> <thead> <tr> <th>If</th><th>Do</th></tr> </thead> <tbody> <tr> <td>you received the problem indicators</td><td>step 2</td></tr> <tr> <td>did not receive the problem indicators</td><td>step 5</td></tr> </tbody> </table>	If	Do	you received the problem indicators	step 2	did not receive the problem indicators	step 5
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.

—End—

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

Step	Action						
1	Determine if the IP addresses of all six 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.						
	<table> <tr> <th>If both cases</th><th>Do</th></tr> <tr> <td>are true</td><td>step 2</td></tr> <tr> <td>are not true</td><td>step 6</td></tr> </table>	If both cases	Do	are true	step 2	are not true	step 6
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.						
	<table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>you have a backup</td><td>step 4</td></tr> <tr> <td>you do not have a backup</td><td>step 6</td></tr> </table>	If	Do	you have a backup	step 4	you do not have a backup	step 6
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 <i>ATM/IP Solution-level Security and Administration</i> , 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.

—End—

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

Step	Action
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 You access the DMA500 log in the directory <code>/var/adm/custlog</code> on the CS 2000 Core Manager console. You see the SDM303 log by logging in to the CS 2000 Core Manager as a maint or root user, accessing the <code>sdmmtc;mtc</code> level, and inputting the <code>querysdm flt</code> command.
2	Contact your next level of support.
3	You have completed this procedure.
—End—	

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

Step	Action						
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. <table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>you are able to add the fourth Media Gateway 15000</td><td>step 4</td></tr> <tr> <td>you are unable to add the fourth Media Gateway 15000</td><td>step 3</td></tr> </table>	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
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.

—End—

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

Step	Action						
1	Determine if there is any response from the XA-Core.						
	<table> <tr> <th>If the XA-Core</th><th>Do</th></tr> <tr> <td>responds</td><td>step 5</td></tr> <tr> <td>does not respond</td><td>step 2</td></tr> </table>	If the XA-Core	Do	responds	step 5	does not respond	step 2
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 MSC Server 1000 CLLI on an SPFS-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" (page 358).						
4	Determine if you are now able to perform maintenance activities using the CS 2000 Management Tools and that the XA-Core responds. <table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>you are able to perform maintenance activities and the XA-Core responds</td><td>step 6</td></tr> <tr> <td>you are unable to perform maintenance activities or the XA-Core does not respond</td><td>step 5</td></tr> </table>	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
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.

—End—

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

Step	Action						
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 <table><tr><th>If</th><th>Do</th></tr><tr><td>you received one of the messages</td><td>step 2</td></tr><tr><td>you did not receive one of the messages</td><td>step 4</td></tr></table>	If	Do	you received one of the messages	step 2	you did not receive one of the messages	step 4
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 " (page 361).						

- 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
you are unable to launch the GUIs	step 4

- 4 Contact your next level of support.

- 5 You have completed this procedure.

—End—

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

Step	Action

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.

—End—

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

Step	Action						
1	Determine if the <code>/opt/</code> directory on the CS 2000 Management Tools server is full. Refer to "Checking the occupancy of the <code>/opt/</code> directory on the CS 2000 Management Tools server" (page 362). <table> <tr> <th>If the <code>/opt/</code> directory</th><th>Do</th></tr> <tr> <td>is full</td><td>step 2</td></tr> <tr> <td>is not full</td><td>step 4</td></tr> </table>	If the <code>/opt/</code> directory	Do	is full	step 2	is not full	step 4
If the <code>/opt/</code> directory	Do						
is full	step 2						
is not full	step 4						
2	The <code>/opt/</code> 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 SPFS-based server.						
3	Determine if the original problem has been corrected. <table> <tr> <th>If the problem</th><th>Do</th></tr> <tr> <td>has been corrected</td><td>step 5</td></tr> <tr> <td>has not been corrected</td><td>step 4</td></tr> </table>	If the problem	Do	has been corrected	step 5	has not been corrected	step 4
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.

—End—

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 'OMG 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

Step	Action
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" \(page 364\)](#).

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.

—End—

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

Step	Action						
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. <table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>you are able to input the command</td><td>step 4</td></tr> <tr> <td>you are unable to input the command</td><td>step 3</td></tr> </table>	If	Do	you are able to input the command	step 4	you are unable to input the command	step 3
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.						
—End—							

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

Step	Action
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.
—End—	

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 the ["Troubleshooting" \(page 420\)](#) 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).

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

Step	Action

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 CLI                  : 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.

—End—

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

Step	Action

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.

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 Host: wcary2p3 Fault Tolerant
0 Q	■	■	■	■	■	■	■	
1								
2								
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.

—End—

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

Step	Action

At your workstation

1	Telnet to the CS 2000 Management Tools server by typing <code>> telnet <ip_address></code> and press the Enter key. where <code><ip_address></code> 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 <code>\$ su - root</code> and press the Enter key.
4	When prompted, enter the root password.
5	Determine if the DDMS proxy is running, by typing <code># /etc/init.d/ddmsproxy status</code>
6	Note whether the DDMS proxy is running or not running.
7	You have completed this procedure.

—End—

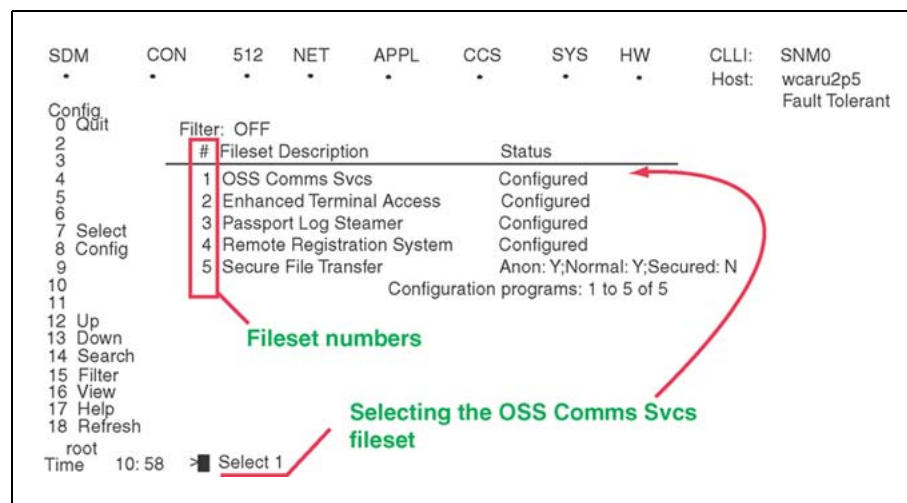
Adding the CS 2000 Management Tools Server as a DDMS client of the CS 2000 Core Manager

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

Step	Action
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 # <code>sdmmtc</code> and press the Enter key.
2	Access the Config level by typing # <code>config</code> and press the Enter key.

Example of a screen showing the Config level on the CS 2000 Core Manager



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
```

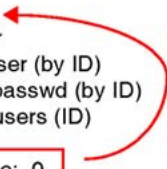
- 6 Advance to the CM User Setup screen by pressing the Enter key.

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

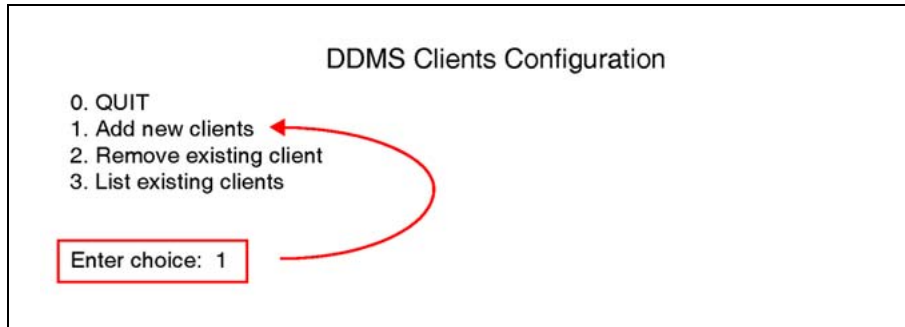


- 7 Advance to the DDMS Clients Configuration screen by typing:

0

and pressing the Enter key.

Example of the DDMS Clients Configuration screen



- 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.

—End—

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 Server Platform Foundation Software (SPFS) which in turn is a software package included in the CS 2000 Management Tools suite of software.

Restart the Apache Web server

Step	Action

At the local or remote VT100 console

1	Telnet to the CS 2000 Management Tools server by typing <code>> telnet <server></code> and pressing the Enter key. where <code><server></code> 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 <code>\$ su - root</code> and pressing the Enter key.
4	When prompted, enter your root password.
5	Restart the Apache Web server by typing <code># /etc/init.d/apache restart</code> and pressing the Enter key.
6	If the restart fails, contact your next level of support.
7	You have completed this procedure.

—End—

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

Step	Action
At your workstation	
1	Telnet to the CS 2000 Management Tools server by typing <pre>> telnet <server></pre> 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 <pre>\$ df -k</pre> Example of a screen showing occupancy of the /opt/ directory at 98%
4	You have completed this procedure.

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

—End—

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

Step	Action

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.

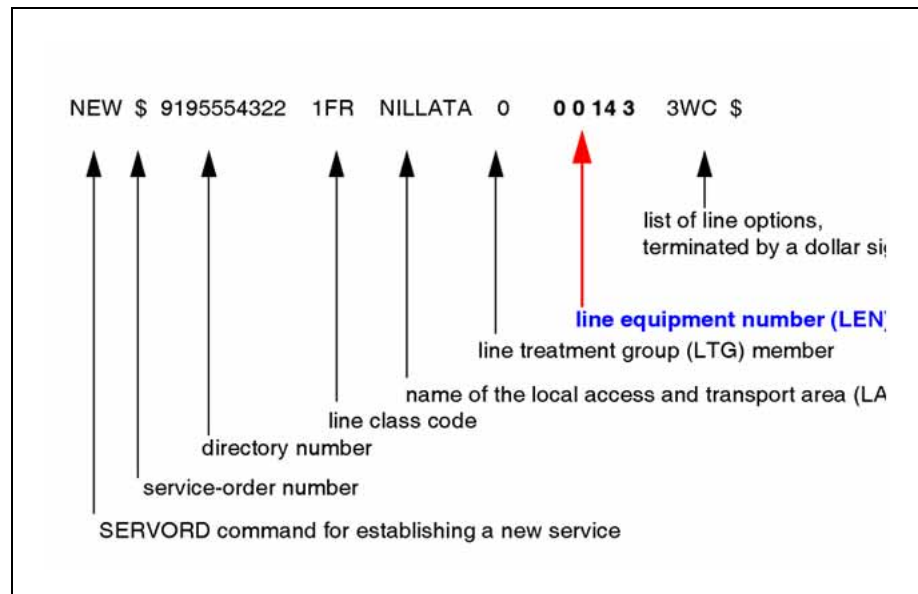
Example of system response:

```
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.

—End—

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 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

Step	Action

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;lns;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
2 LEN MG9A 01 3 05 00
3 Post_
4 LCC PTY RNG
5 IBN
6 DN 613 748 9898 SB
7
8
9 AlmStat
10 CktLoc
11 Hold
12 Next
13
14
15 FullDn
16 Prefix
17 LCO_
18 Level

POST SB DELQ
BUSYQ
PREFIX
STA F S LTA TE RESULT

Post s sb

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
PM TERMINAL 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.

—End—

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

Step	Action

Finding carrier provisioning information

1 To obtain carrier provisioning information for Media Gateway 15000/7400, see *Nortel 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 Solution-level Fault Management*, NN10408-900.

3 To obtain carrier provisioning information at the CS 2000MAPCI, 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

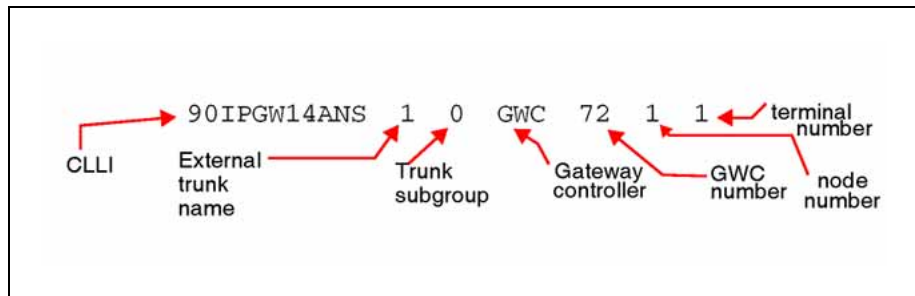
<clli> is the common language location identifier code of the trunk group to which the trunk is a member

<extrknum> is the external trunk number (0-9999) that is assigned to the trunk

Example

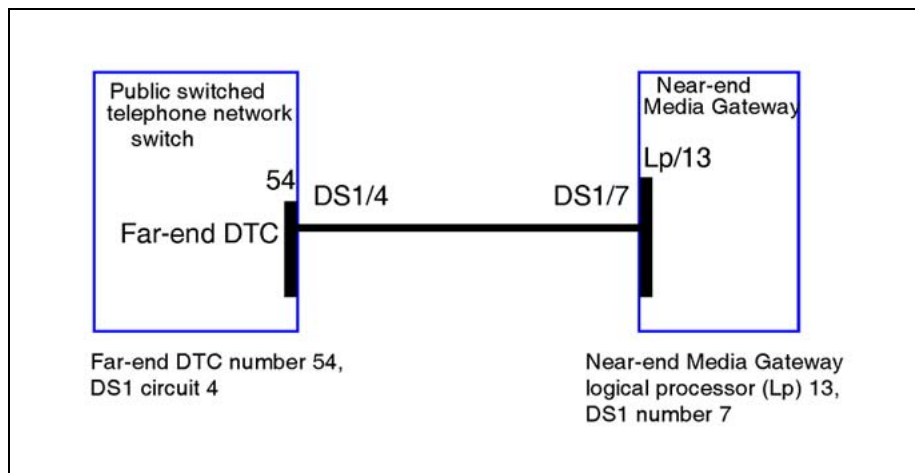
```
pos 90IPW15ANS 1
```

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_		SIZE OF POSTED SET : 1										
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

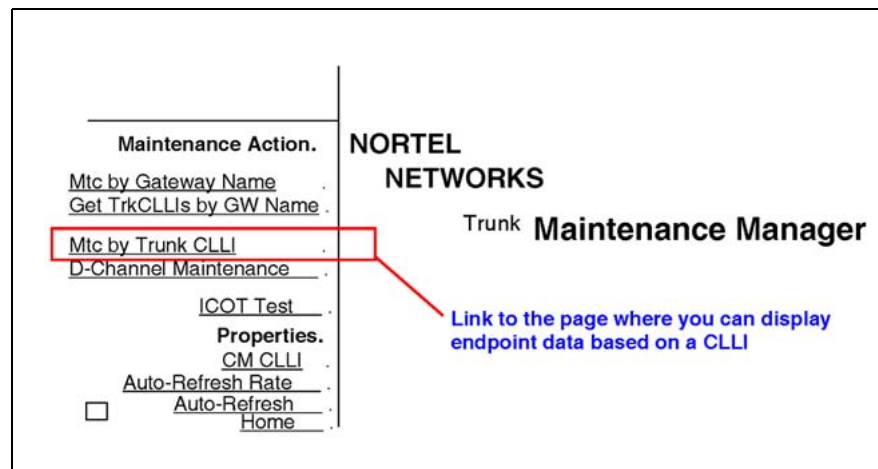
NORTEL NETWORKS

Application Launch Point

Web based applications available on this server (47.142.130.70)

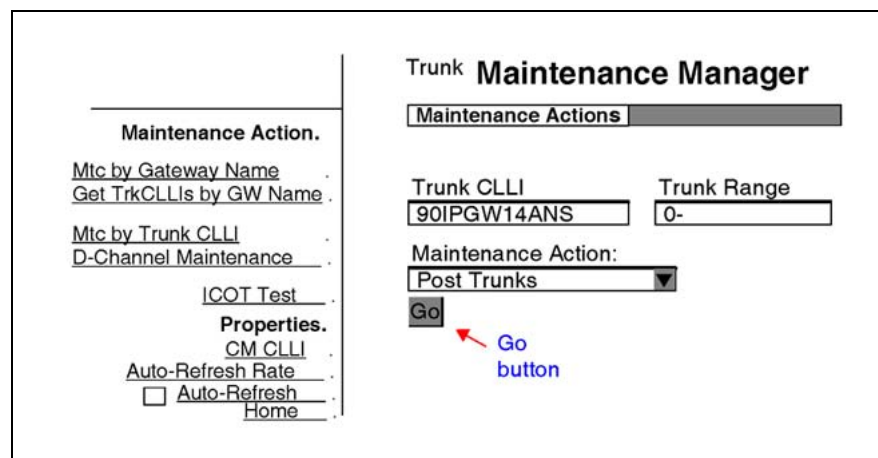
- . Trunk Maintenance Manager
- . CS2000 Management Tools
- . Line Maintenance Manager
- . Batch Configuration Monitor
- . CS2000 SAM21 Manager
- . Network Patch Manager

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: Trunk Range:

Maintenance Action:

CM CLLI: NDPX

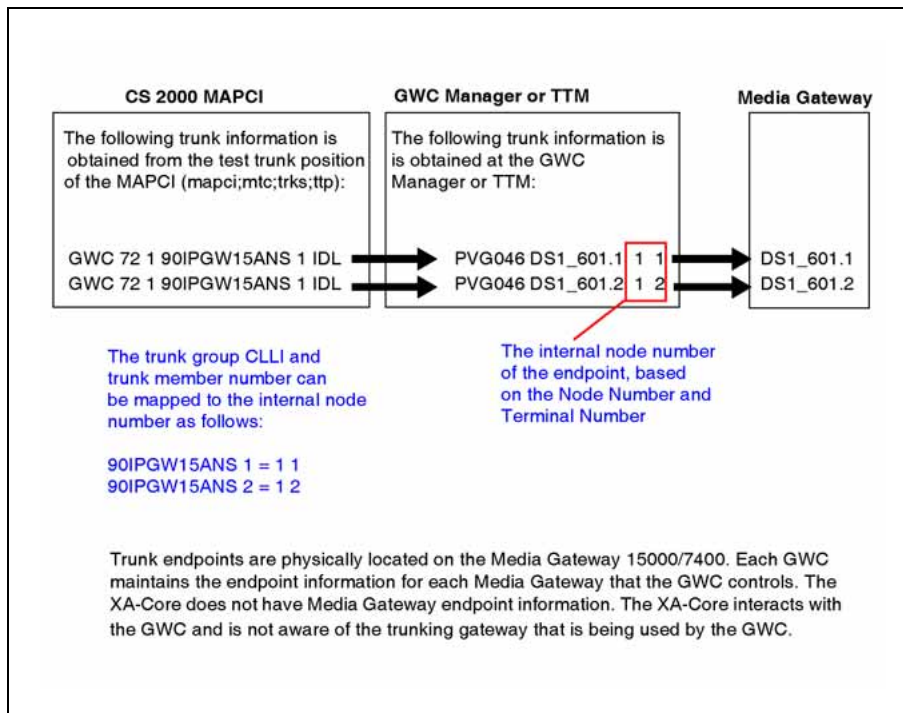
TRUNK CLLI: 90IPGW14ANS

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.

—End—

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 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 MDM. For information on viewing Media Gateway alarms on the MDM, see *Multiservice Data Manager Fault Management Tools*, 241-6001-011.

Media Gateway alarms can be viewed by using applications on the Nortel MDM. For information on viewing Media Gateway alarms on the Nortel MDM, see *Nortel 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.

The XAC, MS, and NET logs do not apply to the CS 2000-Compact.

Checking for CS 2000 or CS 2000-Compact logs

Step	Action
At the MAP terminal	
1	Access the log utility (LOGUTIL), by typing <code>> logutil</code> and press the Enter key. <i>System response:</i> LOGUTIL
2	View the most recent CS 2000(or CS 2000-Compact) logs of a specific type, by typing <code>> open <log_name></code> and press the Enter key. where <code><log_name></code> is name of a group of logs, for example: XAC, IOD, MS, NET, EXT, or APPL Example <code>> open xac</code> <i>The switch responds with the most recent XAC log.</i>
3	View the entire log buffer of logs of a specific type, by typing <code>> dumplogs <log_name></code> and press the Enter key. where <code><log_name></code> is name of a group of logs, for example: XAC, IOD, MS, NET, EXT, or APPL Example <code>> dumplogs xac</code>

The switch dumps the entire log buffer of XAC logs.

- 4 You have completed this procedure.

—End—

Ethernet Routing Switch 8600 Ethernet port configuration, and 100Base-T cable replacement

This document provides you with references to the Ethernet Routing Switch 8600 documents you need to consult for configuration of Ethernet ports, and 100Base-T cabling.

Configuring Ethernet ports on Ethernet Routing Switch 8600

For information on configuring a Ethernet Routing Switch 8600 Ethernet port, see *Configuring Network Management*, 314723C, 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 ERS 8600, see *Installing and Maintaining the 8010co Chassis and Components*, 312746C, on this compact disk.

Delete carriers from a GWC

Purpose of this procedure

Use this procedure to delete (remove) carriers from a Gateway Controller (GWC) node.

When to use this procedure

Use this procedure when carriers must be removed or changed.

Line endpoints are removed automatically when lines are removed (de-provisioned) from a GWC. To de-provision lines, see the *CS 2000 Configuration Management* NTP supporting your solution.

Carriers for all other gateway types must also be removed manually.

Prerequisites and guidelines

All carriers on a gateway must be in one of the following states before they can be removed:

- INB (Installation Busy)
- UNKNOWN (core datafill is missing)

To place trunk groups on the Core in a state of INB, follow procedure "Performing trunk maintenance using the Trunk Maintenance Manager" in *Nortel ATM/IP Solution-level Fault Management* (NN10408-900).

Additional Core table datafill may need to be removed in order to remove all trunk and line endpoint data from all databases.

You must delete one carrier at a time.

Do not remove V5.2 carriers using this procedure. If required, see procedure "Delete V5.2 interfaces" in *Gateway Controller Configuration Management* (NN10205-511).

Action

Step	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 you wish to view.
- 3 Click the **Provisioning** tab.
- 4 Click the **Carriers** tab.
- 5 Click the **Retrieve All** button to retrieve all carriers on the specified GWC node.
- 6 From the Carrier List, select the carrier you wish to delete.
Your selection is highlighted.
You can delete only one carrier at a time.
- 7 Click the **Delete** button at the bottom screen.

Maintenance | **Provisioning** | Controller | Gateways | Lines | **Carriers** | Media Proxies | QoS Collectors | IPSec

Retrieval criteria: Retrieve

Limit results: 25 **Retrieve All**

Carrier List

Name	Gateway	GW Domain	Node Num	Start Term	Num Ports	PRI/DPNSS IID
ds/ds1-2	nuerabb0-1.car...		97	49	24	
ds/ds1-5	nuerabb0-1.car...		97	25	24	
ds/ds3-1/ds1-1	bt4k1.car3c.ott		97	1	24	
ds/ds3-1/ds1-12	bt4k1.car3c.ott		97	268	24	
ds/ds3-1/ds1-13	bt4k1.car3c.ott		97	436	24	
ds/ds3-1/ds1-2	bt4k1.car3c.ott		97	100	24	
ds/ds3-1/ds1-3	bt4k1.car3c.ott		97	73	24	
ds/ds3-1/ds1-4	bt4k1.car3c.ott		97	124	24	
ds/ds3-1/ds1-5	bt4k1.car3c.ott		97	148	24	
ds/ds3-1/ds1-6	bt4k1.car3c.ott		97	172	24	
ds/ds3-1/ds1-7	bt4k1.car3c.ott		97	196	24	
ds/ds3-1/ds1-8	bt4k1.car3c.ott		97	220	24	
ds/ds3-1/ds1-9	bt4k1.car3c.ott		97	244	24	
ds/ds1-1	TGCPzmer0rb....		97	292	24	
ds/ds1-2	TGCPzmer0rb....		97	316	24	
ds/ds1-3	TGCPzmer0rb....		97	340	24	
ds/ds1-4	TGCPzmer0rb....		97	364	24	
ds/ds1-5	TGCPzmer0rb....		97	388	24	
ds/ds1-6	TGCPzmer0rb....		97	412	24	

Number of results: 19 **Delete**



CAUTION

Possible partial service disruption

If endpoints associated with a carrier are deleted from the GWC and not from the Core, you will encounter call processing problems. See the *CS 2000 Configuration Management* NTP for your solution to remove corresponding trunk data from the Core tables.

- 8 At the confirmation box, click **Yes** to confirm that you wish to delete the carrier.

The carrier list is automatically updated following a successful deletion.

- 9 Repeat this procedure for other carriers you wish to delete on this GWC node.
- 10 The procedure is complete.

—End—

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.

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

Step	Action
<i>At the CS 2000 GWC Manager client</i>	
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, then the Controller tab to view general provisioning information for the GWC node selected.

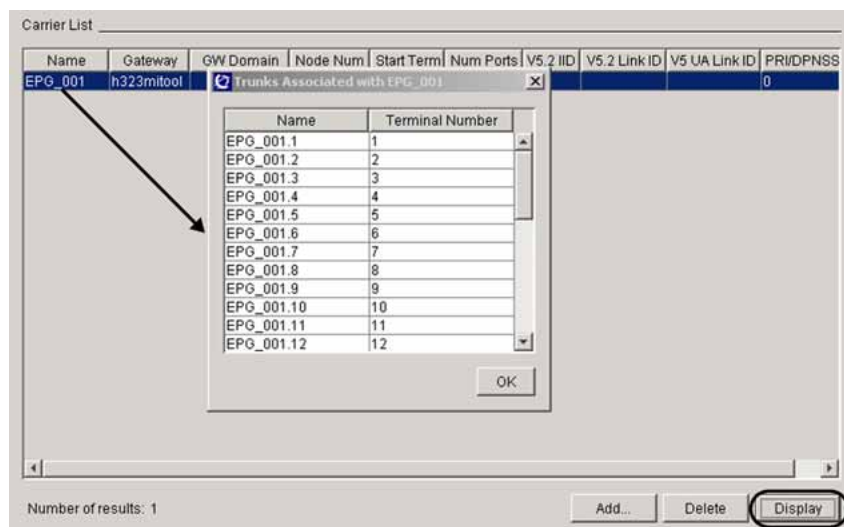
- 4 Click the **Carriers** tab to view information related to carriers (endpoint groups) belonging to gateways associated with the GWC node selected previously.

Select the edge of any tab to adjust the display.

- 5 Click the **Retrieve All** button to view carrier endpoint data.

Table "Description of carrier endpoint search criteria functions" (page 390) contains information about the search functions (see the numbers in the preceding figure).

- 6 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.



- 7 Repeat this procedure as required for carrier endpoints you wish to view on this or other GWC nodes.
- 8 The procedure is complete.
- The following table describes the carrier endpoint search criteria functions.

—End—

Description of carrier endpoint search criteria functions

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. For more information about using search string, see table "Examples of carrier search criteria" (page 392) at the end of this procedure.

Step	Menu component	Description
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". The "no limit" value is still itself limited by the maximum number of entries currently downloadable.
3	Replace List radio button Append to 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. Select this option if you want the query results to be appended to the existing data displayed in the table.
4	Retrieve button Retrieve All 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. 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 information about how to add or delete lines, see the <i>CS 2000 Configuration Management</i> NTP applicable to your solution. This selection retrieves all the gateway or endpoint data. 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.

Step	Menu component	Description
		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 re-executed.
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.

Examples of carrier search criteria

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".

Example Retrieval Criteria: "DS3"

Expected Results: Returns all records where the string is found in any column.

Add carriers to a GWC

Purpose of this procedure

Use this procedure to add carriers (endpoint groups) and their endpoints to a gateway associated with a GWC node.

Carrier endpoints are usually provisioned in groups representing E1 and DS1 levels allowing access to all timeslots for service provisioning. Services supported include ISUP trunking, PRI, DPNSS trunking.

The section "[Carrier and endpoint naming](#)" (page 398) contains a table of carrier formats to be used for different media gateway profiles.

Line carriers

Line endpoints are added automatically when you provision lines to a GWC. For information about how to provision lines, see the *CS 2000 Configuration Management NTP* for your solution.

In a Carrier VoIP environment, the allocation of line equipment numbers (LEN) for new lines is done by the system. This is because the LEN is no longer directly associated with physical hardware and its location as it was in legacy networks. In Carrier VoIP networks, LENs act as an internal map to a gateway endpoint pair. Use of LEN has been replaced with the implementation of the gateway endpoint to designate actual termination points in the network. This mapping is done by the system and is not intended to be determined manually at provisioning time. Since the data needs to reside in multiple locations and retain synchronization in the network, the line provisioning system acts as a single point of entry for this data to ensure it is named and assigned consistently across all network elements.

H.323 carriers

To permit greater flexibility in carrier provisioning, H.323 carriers are added manually using this procedure. Any new H.323 carriers assigned are added manually based on the naming convention for H.323 carriers.

For details related to H.323 carrier provisioning, see section "[H.323 carrier provisioning](#)" (page 412).

After an H.323 gateway is added to the CS 2000 GWC Manager database, additional provisioning of terminal identifiers (TID) that are mapped to endpoints must be manually added to the Core. For information about how to perform this task, see the *CS 2000 Configuration Management NTP* applicable to your solution.

DPNSS carriers (international market)

Starting in (I)SN09, international markets can use the Nortel Media Gateway 3200 (MG 3200) to provide direct interconnection between Private Branch Exchange (PBX) gateways and the CS 2000 network. The Digital Private Network Signaling System (DPNSS) protocol carried over E1 carrier is used to send messages between the MG3200 and the CS 2000.

When to use this procedure

Use this procedure after you have associated specific media gateways with a GWC node.

Prerequisites and guidelines

You must first associate a media gateway with a GWC node before you can add carriers (endpoint groups) to the gateway.

You need to be familiar with the names of the media gateways associated with the GWC node.

To determine the naming convention for your gateway profile type, see ["Carrier and endpoint names" \(page 399\)](#).

Do not add V5.2 carriers using this procedure. See procedure "Add V5.2 interfaces in *Gateway Controller Configuration Management* (NN10205-511)

After you have completed this procedure, see the *CS 2000 Configuration Management* NTP for your solution to specify the trunks to provision by adding tuple datafill to table TRKMEM.

**CAUTION****Possible partial service disruption**

If you are adding carrier endpoints after having previously removed them from the same gateway, you will have terminal identifier (TID) mismatches. Contact your next level of support for instructions on how to avoid TID mismatches.

Action

Step	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 you wish to view.
- 3 Click the **Provisioning** tab, then the **Carriers** tab

The screenshot shows the 'Provisioning' tab selected in the 'Maintenance' window. Within this tab, the 'Carriers' sub-tab is active. The interface includes a 'Retrieval criteria' dropdown, a 'Limit results' dropdown set to 25, and buttons for 'Retrieve', 'Retrieve All', 'Replace List', and 'Append to List'. Below these is a 'Carrier List' table with the following data:

Name	Gateway	GW Domain	Node Num	Start Term	Num Ports	V5.2 IID	V5.2 Link ID	V5 UA Link ID	PRI/DPNSS IID
01/01	GCPSPAT		89	1	31				
01/02	GCPSPAT		89	32	31				

At the bottom of the window, there are buttons for 'Add...', 'Delete', and 'Display', along with a status bar indicating 'Number of results: 2'.

- 4 Click the **Add** button at the bottom of the screen to display the Add Carrier dialog box.

The 'Add Carrier' dialog box is shown. It contains the following fields and options:

- Carrier name: [Text Field]
- Gateway name: [Text Field]
- Start terminal number: [Text Field]
- Number of ports: [Text Field]
- ☐ H.323
- ☐ PRI/DPNSS IID: [Text Field]
- Buttons: OK, Cancel

- a. In the Carrier name: field, type the name (an alphanumeric character string) of the carrier that you want to add.

The carrier name is based on the media gateway type (the gateway profile name). For naming conventions applicable to specific media gateways, see ["Carrier and endpoint names" \(page 399\)](#).

For DPNSS carriers, this name must match the name configured for the Physical Name Pattern field when configuring the MG 3200 gateway using the Web Server Interface. For more information, see *Media Gateway 3200 H.248 User's Manual* (LTRT-72704).

- b. In the Gateway name: field, type the name (an alphanumeric character string) of the gateway to which you are adding carriers.

The name of the gateway is selected when associating a media gateway with a GWC node.

- c. If desired, in the Start terminal number: field, type a number representing the starting point of a contiguous block of endpoints or terminal identifiers (TID).

This field is optional. If you do not type a number in this field, the system will automatically define which TIDs are used and how they map to the carrier.

For any gateway other than an H.323 gateway, the contiguous block of endpoints will be either 24 (North American market) or 32 (International market). Note that 31 endpoints will be added for International PRI. The system automatically identifies the number of endpoints included in the block based on the configuration of the CS 2000 Management Tools server.

For gateways supporting H.323, the number of endpoints in the contiguous block is defined by the value in the Number of ports: field (see [step f](#)). If no value is entered in the Number of ports: field, then the default of 24 (NA market) or 32 (International market) endpoint will be used.

Ensure that a contiguous range of endpoints are available on your gateway to fulfill your requirements when you perform the following tasks:

- assign a value in the Start terminal number: field
- change the size of your carrier block

- d. Determine your next step using the following table.

If you are adding carriers to	Do
an H.323 gateway	go to step e

If you are adding carriers to	Do
a non-H.323 gateway and PRI trunks are provisioned in the carrier group	go to step g
a non-H.323 gateway and PRI trunks are not provisioned in the carrier group	go to step i
a gateway to support DPNSS signaling (international market)	go to step h

- e. If you are adding carriers to an H.323 gateway, select the H.323 check box.

The Number of ports: field is activated.

You must select the H.323 check box to add carriers to an H.323 gateway.

- f. If desired, in the Number of ports: field, type a number defining the size of the H.323 virtual carrier block you are adding.

A range of 4 to 672 endpoints (inclusive) is supported.

For examples of how to take advantage of carrier block flexibility when provisioning H.323 gateways, see "[H.323 carrier provisioning](#)" (page 412).

The Number of ports: field is optional for H.323 gateways. If you do not type a number in this field, the system allocates the default block of endpoints for your system, either 24 (NA) or 32 (International).

The total sum of values entered in the Number of ports: field for all carriers assigned to an H.323 gateway must be less than, or equal to, the value entered in the Reserved terminations: field of the Associate Media Gateway dialog box. See procedure "Associate an H.323 media gateway" in *Gateway Controller Configuration Management* (NN10205-511).

Continue with [step i](#).

- g. Select the PRI/DPNSS check box, if applicable, and enter a PRI Interface ID (IID) value within the range of 0 to 31 (inclusive).

The IID value is not used in international PRI. Therefore, for offices using international PRI, select the PRI check box and set the value to 0.

For PRI in the North American market, the IID value is used in the non-facility associated signaling (NFAS) configuration in which multiple DS1 trunks are controlled by one D-channel. In this case, the IID value must match the IID value provisioned at the far-end switch.

Do not select this check box if

- PRI trunks are not provisioned in the carrier group;
- you are adding carriers to a gateway supporting H.323.

Continue with [step i](#).

- h. For DPNSS carriers, select the PRI/DPNSS check box and enter an integer Interface ID (IID:) value within the range of 0 to 63.

This IID must be unique for each gateway and must match the value specified for this particular carrier when configuring the MG 3200 gateway. For more information, see the *Media Gateway 3200 H.248 User's Manual*, LTRT-72704.

- i. Click **OK** to accept the input to the Add Carrier dialog box.

If the add carrier operation is successful, a dialog box is displayed. Click **OK** to continue.

If the add carrier operation fails, an error message will be displayed. Click the **Show Details** button for more information. An error message will also appear in the status bar at the bottom of the screen.

- 5 To verify your changes, click the **Retrieve All** or the **Retrieve** button to update the Carrier List.
- 6 Repeat this procedure as required for other carriers you wish to add to a media gateway.
- 7 See the *CS 2000 Configuration Management* NTP applicable to your solution to provision the trunks that correspond to the carriers.
- 8 The procedure is complete.

—End—

Carrier and endpoint naming

This section provides a table containing the naming conventions for carriers (endpoint groups) and endpoints. This table is organized based on the gateway profile name selected when associating a media gateway with a GWC node.

This table references the following signaling protocols:

- H.248/Megaco
- Media Gateway Control Protocol (MGCP)
- Trunk Gateway Control Protocol (TGCP)

- H.323

Carrier and endpoint names

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
AMBIT line gateways	aaln/<n> where <n> is a number: 1-16 depending on the model and market (specified when choosing the media gateway profile)
ARRIS_TOUCHSTONE line gateways	aaln/<n> where <n> is a number: 1-4 depending on the MTA model and market (specified when choosing the media gateway profile)
ASKEY_LINE Integrated Access Devices (IAD) gateways	aaln/<n> where <n> is a number: 1-30 depending on the model and market (specified when choosing the media gateway profile)
AUDCDSMG32LN	p/<nnn> where p is lower case <nnnn> is an endpoint number: 1 to 384
AUDICODES (Nortel Media Gateway 3200 and 3500)	Carrier or gateway endpoints are provisioned in groups representing E1 and DS1 levels. Provisioning at this level gives access to all timeslots for service provisioning. Carrier names are case sensitive and must be entered in upper case. The following descriptions include both endpoint groups and individual endpoint descriptions. Services can be applied at the DS1/E1 timeslot level. DS1 DS1/<h2>/<g> (H.248/Megaco) where <h2> is the DS1 (two digit) port or span number: 01-04 <g> is the channel number: 1-24 (no leading 0), assigned by the system Example: Carrier name: DS1/03 Carrier Endpoint name (timeslot): DS1/03/1

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
AUDIOCODES_6310_TRUNK (Nortel Media Gateway 3500 using TP-6310 card and configured as trunk gateway)	Carrier or gateway endpoints are provisioned in groups representing E1 and DS1 levels. Carrier names are case sensitive and must be entered in upper case. The following descriptions include both endpoint groups and individual endpoint descriptions. Services can be applied at the DS1/E1 timeslot level. DS1 DS1/<h2>/<g_optional> (H.248/Megaco) where <h2> is the DS1 (two digit) port or span number: 01-84 <g> is optional PRI IID: 0 to 31 (32 to 63 range is not supported). This value must be unique for each gateway. Example: Carrier name: DS1/03 Each DS1 carrier supports 24 terminations and the appropriate number of terminations must be reserved in advance. A fully equipped gateway with DS1 carriers requires 84 x 24=2016 terminations. E1 E1/<h2>/<g_optional> (H.248/Megaco) where <h2> is a number: 1 to 63 <g> is optional PRI IID: 0 to 63 Example: Carrier name: E1/03 Each E1 carrier supports 31 terminations and the appropriate number of terminations must be reserved in advance. A fully equipped gateway with E1 carriers requires 63 x 31=1953 terminations.
CALIX_C7	tp/<TT><tt> where tp is lower case <TT> is a number: 00-10 <tt> is a number: 00-99 (except <TT> is 10, in which case <tt> is limited to the range 00-22); for a maximum of 1022 terminations allowed for each gateway Example: tp/1013

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
CICM	tp/<vmg>/<nnnn> where tp is lower case <vmg> is a number: 0 - 2 <nnnn> is a number: 0001 - 1022; always zero padded Example: tp/1/0002 Each endpoint appears as a virtual media gateway (VMG). For more information, see <i>CICM Basics</i> (NN10044-111).
CISCO_2600 CISCO_3600 CISCO_AS5300 CISCO_H323_IOS Supporting H.323 signaling protocol	EPG_<n> where <n> is a number: 000 - 999 The underscore character "_" is required and the number must include three digits (it must be zero-padded). Duplicate carrier names on different media gateways are permitted. Example: EPG_001
CVX-600 CVX-1800	<gateway Name>.<E1 carrier>_<W0>.<Y1>.<Z1> where <W0> is the slot number on the CVX chassis: 1-18 <Y1> is the E1 port number on the Digital Access Card: 0-99 <Z1> is the E1 timeslot/channel number: 0-31 Example: CVX1.E1_17.2.19 Provisioning of the endpoints is same for both RAS and VOIP setup.
H323_PROXY	EPG_<n> where <n> is a number: 000 - 999 The underscore character "_" is required and the number must include three digits (it must be zero-padded). Duplicate carrier names on different media gateways are permitted. Example: EPG_001

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
KEYMILE_UMUX	POTS table entry: p/nnn where p is lower case <nnnn> is an endpoint number: 1 to 480; not padded (no leading zeros for padding to three digits) This value should match the terminal number. Example: p/24 Third-party media gateways support flexible allocation of the LEN circuit number and the endpoint terminal number, independently of the endpoint name. The circuit number allocated for an endpoint must be unique and in the range of 1 to 480. This value identifies the LEN that the system creates. Nortel recommends that the circuit number is equal to: <nnn> - 1. For example, if the endpoint is p/1, the associated LEN is: <LGRP> 00 00. Nortel recommends that you create the endpoints as blocks of 30 contiguous endpoints to align with the configuration of the Keymile UMUX cards.
MEDIATRIX Integrated Access Device (IAD) gateways	aaln/<n> where <n> is a number: 1-4 or 1-24 depending on the model and market (specified when choosing the media gateway profile).
MGCP line gateway MGCP_IAD_40 line gateway	aaln/<n> where <n> is a number: 1-40 depending on the configuration of the gateway.
MOTOROLA MTA line gateways	aaln/<n> where <n> is a number: 1-4 depending on the MTA model and market (specified when choosing the media gateway profile)
NORTEL_BCM Supporting H.323 signaling protocol	EPG_<n> where <n> is a number: 000 - 999 The underscore character "_" is required and the number must include three digits (it must be zero-padded). Duplicate carrier names on different media gateways are permitted. Example: EPG_001

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
NUERA_BT4K	The gateway profile name NUERA_BT4K supports the Nuera BT4K gateway, which allows provisioning of six DS3 interfaces. DS3 (with channelized DS1 levels) There are 24 DS0 channels for each DS1 interface for a total of 4032 DS0 channels for each BT4K gateway. ds/ds3-<u1>/ds1-<u2>/<c> where <u1> is a decimal value referring to the particular instance of ds3: 1-6 <u2> is a decimal value referring to the particular instance of ds1: 1-28 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy: 1-24 Example: Carrier name: ds/ds3-2/ds1-3 Carrier Endpoint name (timeslot): ds/ds3-2/ds1-3/1
NUERA_GX	Carrier or gateway endpoints are provisioned in groups representing E1 and DS3 levels. Provisioning at this level gives access to all timeslots for service provisioning. Supported services include ISUP trunking and PRI trunking. Carrier names are case sensitive and must be entered in upper case. The following descriptions include both endpoint groups and individual endpoint descriptions. Services can be applied at the DS1/E3 timeslot level. E1/<h1>/<h2>/<g> (H.248/Megaco) where <h1> is the two-digit LP (logical processor) number (or slot) of the E1: 1-15 <h2> is the E1 (two digit) port number: 01-32 <g> is the channel number: 1-31 (no leading 0), assigned by the system H.248/Megaco example: Carrier name: E1/03/05 Carrier Endpoint name (timeslot): E1/05/05/1

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
	DS3/DS1 DS1 carriers are provisioned using the same endpoint naming as DS3. DS3/<h1>/<h2>/<g> (H.248/Megaco) where <h1> is the LP (logical processor) number or slot of the DS3: 1-15 (2-5 recommended) <h2> is the DS3 port number <g> is the channel number in the DS3: 1-24, assigned by the system H.248/Megaco example: Carrier name: DS3/03/05 Carrier Endpoint name (timeslot): DS3/05/05/1
PVG7K, PVG15K PVG15K_1000 PVG15K_PARTIAL	Carrier or gateway endpoints are provisioned in groups representing E1 and DS3 levels. Provisioning at this level gives access to all timeslots for service provisioning. Supported services include ISUP trunking and PRI trunking. Carrier names are case sensitive and must be entered in upper case. The following descriptions include both endpoint groups and individual endpoint descriptions. Services can be applied at the DS3/E1 timeslot level. ATTENTION Starting in (I)SN09, all PVG ASPEN profiles are obsolete. These profiles are still present in the GWC Manager GUI but are not supported. Do not use these profiles. Instead, use the PVG_MEGACO profiles. E1 e1/<h1>/<h2>/<g> (H.248/Megaco) where <h1> is the two-digit LP (logical processor) number or slot of the E1: 1-15 (no leading 0) <h2> is the E1 (two digit) port number: 01-32 <g> is the channel number: 1-31 (no leading 0), assigned by the system H.248/Megaco example: Carrier name: e1/03/05 Carrier Endpoint name (timeslot): e1/03/05/1

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
	DS3 DS3/<h1>/<h2>/<g> (H.248/Megaco) where <b1> is the LP (logical processor) number or slot of the DS3: 1-15 (2-5 recommended) <b2> is the DS3 (single digit) port number: 0-1 <c> is the DS3 number: 1-28 <d> is the channel number in the DS3: 1-24, assigned by the system H.248/Megaco example: Carrier name: DS3/03/05 Carrier Endpoint name (timeslot): DS3/05/05/1 STM-1 STM/<lp>/<p>/1/VC4VC12/1/<k>/<l>/<m>/<e> (H.248/Megaco) where <lp> is the LP (logical processor) number or slot of the STM-1 interface: 2-15 (slots 2-5 are recommended) <pp> is the two-digit port number: 00-03 <p> is the one-digit port number: 0-3 <k> is the one-digit TUG-3 number within a VC4: 1-3 <l> is the one-digit TUG-2 number within a TUG-3: 1-7 <m> is the one-digit TU number within a TU: 1-3 <e> is the VC12 channel/timeslot: 1-31 (no leading 0) Hard-coded values 1/VC4VC12/1 (H.248) indicate the STM carrier type, multiplexing within the STM-1 frame, and the AUG within the STM-1 frame. H.248/Megaco example: Carrier name: STM/2/1/1/VC4VC12/1/3/6/1 Carrier Endpoint name (timeslot): STM/2/1/1/VC4VC12/1/3/6/1/1 OC-3 STS/<lp>/<p>/3/VT15/<t>/<l>/<m>/<e> (H.248/Megaco) where <lp> is the LP (logical processor) number or slot of the OC-3 interface: 1-15 (recommended slots 2-5) <pp> is the (two digit) port number: 00-03 <p> is the (one digit) port number: 0-3 <jj> is the (two digit) STS-1 number within the STS-3: 01-03 <l> is the (one digit) VT group number within STS-1: 1-7 <m> is the (one digit) VT number within a VT: 1-4 <t> is the (one digit) STS-1 number within the STS-3: 0-3

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
	<e> is the VT1.5 channel/timeslot: 1-24 (no leading 0) Hardcoded value /3/VT15/ (H.248) indicates the STS carrier type and the multiplexing within the OC-3 carrier. H.248/Megaco example: Carrier name: STS/2/1/3/VT15/1/6/1 Carrier Endpoint name (timeslot): STS/2/1/3/VT15/1/6/1/1
PVG_VSP4E	STM/<l>/<p>/1/VC4VC12/1/<t>/<u>/<v> where <1> is the LP (logical processor) number or slot of the STM interface: 2-15 <p> is the one-digit port number: 0-3 <t> is the one-digit TUG-3 number within a VC4: 1-3 <u> is the one-digit TUG-2 number within a TUG-3: 1-7 <v> is the one-digit TU number within a TU: 1-3 The maximum capacity is 31 endpoints. Hard-coded value of 1/VC4VC12/1 indicates the STM carrier type, multiplexing within the STM-1 frame, and the AUG within the STM-1 frame. Example: Carrier name: STM/2/1/1/VC4VC12/1/3/6/1 Carrier Endpoint name (timeslot): STM/2/1/1/VC4VC12/1/3/6/1 STS/<l>/<p>/3/VT15/<t>/<v>/<w> where <1> is the LP (logical processor) number or slot of the STS interface: 1-15 <p> is the port number: 0-3 <t> is the STS-1 number: 1-3 <v> is the VT group number: 1-7 <w> is the VT number: 1-4 The maximum capacity is 24 endpoints. Hard-coded value of 3/VT15 indicates the STS carrier type. Example: Carrier name: STS/2/1/3/VT15/1/3/4 Carrier Endpoint name (timeslot): STS/2/1/3/VT15/1/3/4

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
SIPVOICE	/<SITE>/<FFF>/<G>/<TT tt> where <SITE> is a name defined in table SITE configured on the Core <FFF> is a frame number: 0 - 511 <G> is a group number: 0 - 9 <TT tt> is a terminal number: 00 00 - 1023 Example: /ABCD/10/9/01 20
SUCCESSION_1000 Supporting H.323 signaling protocol	EPG_<n> where <n> is a three-digit number: 000 - 999 The underscore character "_" is required and the number must include three digits (it must be zero-padded). Duplicate carrier names on different media gateways are permitted. Example: EPG_001
TGCP	GWCs support TGCP media gateways with • DS1 interfaces • DS1 interfaces within a logical processor or slot • OC3 interfaces with channelized DS3 and DS1 levels • OC3 interfaces with channelized DS3 and DS1 levels within a logical processor or slot • DS3 interfaces with a channelized DS1 level within a logical processor or slot DS3 interfaces without DS1 framing • DS3 interfaces with a channelized DS1 level • E1 interfaces The following abbreviations are used in TGCP carrier and endpoint formats: • u = unit number • c = channel number The gateway profile name TGCP supports third party media gateways using TGCP signaling protocol.

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
	DS1 ds/ds1-<u><u>/<c></u> where <u><u></u> is a decimal value referring to the particular instance of ds1: 1-68 <u><c></u> is a decimal value indicating the channel number at the lowest level in the hierarchy: 1-24 Example: Carrier name: ds/ds1-1 Carrier Endpoint name (timeslot): ds/ds1-1/1 DS1 (within a logical processor or slot) ds/s-<u><u1>/ds1-<u><u2>/<c></u></u> where <u><u1></u> is a decimal value referring to the particular instance of s (slot): 1-28 <u><u2></u> is a decimal value referring to the particular instance of ds1: 1-28 <u><c></u> is a decimal value indicating the channel number at the lowest level in the hierarchy: 1-24 Example: Carrier name: ds/s-2/ds1-1 Carrier Endpoint name (timeslot): ds/s-2/ds1-1/1 OC3 (with DS3 and DS1 levels) ds/oc3-<u><u1>/ds3-<u><u2>/ds1-<u><u3>/<c></u></u></u> where <u><u1></u> is a decimal value referring to the particular instance of oc3: 1-28 <u><u2></u> is a decimal value referring to the particular instance of ds3: 1-28 <u><u3></u> is a decimal value referring to the particular instance of ds1: 1-28 <u><channel #></u> is a decimal value indicating the channel number at the lowest level in the hierarchy: 1-24 Example: Carrier name: ds/oc3-2/ds3-3/ds1-1 Carrier Endpoint name (timeslot): ds/oc3-2/ds3-3/ds1-1/1

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
TGCP (continued)	OC3 (with DS3 and DS1 levels within a logical processor or slot) ds/s-<u1>/oc3-<u2>/ds3-<u3>/ds1-<u4>/<c> where <u1> is a decimal value referring to the particular instance of s (slot): 1-28 <u2> is a decimal value referring to the particular instance of oc3: 1-28 <u3> is a decimal value referring to the particular instance of ds3: 1-28 <u4> is a decimal value referring to the particular instance of ds1: 1-28 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy: 1-24 Example: Carrier name: ds/s-2/oc3-2/ds3-3/ds1-1 Carrier Endpoint name (timeslot): ds/s-2/oc3-2/ds3-3/ds1-1/1
	DS3 (with a DS1 level within a logical processor or slot) ds/s-<u1>/ds3-<u2>/ds1-<u3>/<c> where <u1> is a decimal value referring to the particular instance of s (slot): 1-28 <u2> is a decimal value referring to the particular instance of ds3: 1-28 <u3> is a decimal value referring to the particular instance of ds1: 1-28 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy:1-24 Example: Carrier name: ds/s-2/ds3-3/ds1-1 Carrier Endpoint name (timeslot): ds/s-2/ds3-3/ds1-1/1

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
TGCP (continued)	DS3 (without DS1 framing) ds/s-<u1>/ds3-<u2>/<c> where <u1> is a decimal value referring to the particular instance of s (slot): 1-28 <u2> is a decimal value referring to the particular instance of ds3: 1-28 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy: 1-24 Example: Carrier name: ds/s-2/ds3-3/ Carrier Endpoint name (timeslot): ds/s-2/ds3-3/1
	DS3 (with channelized DS1 levels) ds/ds3-<u1>/ds1-<u2>/<c> where <u1> is a decimal value referring to the particular instance of ds3: 1-28 <u2> is a decimal value referring to the particular instance of ds1: 1-28 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy:1-24 Example: Carrier name: ds/ds3-2/ds1-3 Carrier Endpoint name (timeslot): ds/ds3-2/ds1-3/1
TGCP (continued)	E1 ds/e1-<u1> /<c> where <u1> is a decimal value referring to the particular instance of e1: 1-68 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy: 1-31 Example: Carrier name: ds/e1-1 Carrier Endpoint name (timeslot): ds/e1-1/1

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
TOUCHTONE_NN line gateways	aaln/<n> where <n> is a number: 1-4 depending on the MTA model and market (specified when choosing the media gateway profile).
UAS Audio servers (including Nortel Media Server 2000 Series)	Endpoints are not specified during provisioning of audio servers.
UE9000MG (Media Gateway 9000)	<i>For non-ABI (access bridge interface) lines:</i> tp/<slot>/<circuit> where tp is lower case <slot> is a number: 2-9 <circuit> is a number: 14-21 Example: tp/2/14 Each endpoint appears as a virtual media gateway (VMG). The <slot> and <circuit> values constitute the SLOT and the CIRCUIT part of the line equipment number (LEN) for the gateway. <i>For MG 9000 ABI lines:</i> tp/channel/<channelID> where tp is lower case <channelID> is a number between 000 and 511
WESTELL Supporting H.323 signaling protocol	EPG_<n> where <n> is a three-digit number: 000 - 999 The underscore character "_" is required and the number must include three digits (it must be zero-padded). Duplicate carrier names on different media gateways are permitted. Example: EPG_001

H.323 carrier provisioning

This section compares the various limits associated with carrier provisioning of GWCs supporting H.323 signaling protocol between Carrier VoIP releases. This section also provides two examples of carrier provisioning on a GWC node supporting H.323. One example uses many small gateways, and the other uses one large gateway.

The following table describes the rules that apply to provisioning carriers on GWCs supporting H.323.

H.323 carrier provisioning limits and ranges

Parameter	Maximum
Number of endpoints supported on a GWC node	1032 - NA 1024 - Intl
Number of endpoints supported on a media gateway	1032 - NA 1024 - Intl (all supported gateways)
Number of media gateways supported on a GWC node	254
Number of endpoints in a carrier (size of a carrier block)	4 - 672 (virtual carrier - user provisionable within this range)
More than one carrier (D-channel) can be supported on a single media gateway. Therefore, more than one trunk group on the Core can be mapped to the endpoints (TID) provisioned on the GWC.	
For a provisioning example of this feature, see "Example 2: One large gateway provisioned on a GWC node" (page 413)	

Example 1: Many gateways provisioned on a GWC node

This example demonstrates how to take advantage of the flexible carrier size for small gateways with relatively few endpoints on each gateway.

In this example, a GWC node supporting H.323 protocol is provisioned as follows:

- 254 NORTEL_BCM media gateways are associated with 1 GWC node.
- 253 of the gateways are provisioned with 1 carrier containing 4 endpoints each.
- One gateway is provisioned with 1 carrier containing 20 endpoints.

In this example, the total number of endpoints used on the GWC node is 1032.

Example 2: One large gateway provisioned on a GWC node

This example demonstrates how to take advantage of the fact that more than one carrier (or D-channel) can be mapped to a single gateway.

In this example, a GWC node supporting H.323 protocol is provisioned as follows:

- One SUCCESSION_1000 media gateway is associated with one GWC node.
- The gateway is provisioned with two carriers containing 515 endpoints each.

In this example, the total number of endpoints used on the GWC node is 1032. Each carrier group maps to a trunk group on the Core.

View media proxy associations

Purpose of this procedure

This procedure describes how to check all current associations of the selected media proxy. A media proxy can be associated as a default media proxy with one or more Gateway Controllers (GWC) or can belong to one or more preferred media proxy groups, or both.

When to use this procedure

Use this procedure when you wish to view the list of all GWCs and all preferred media proxy groups with which the selected media proxy is currently associated.

Prerequisites and guidelines

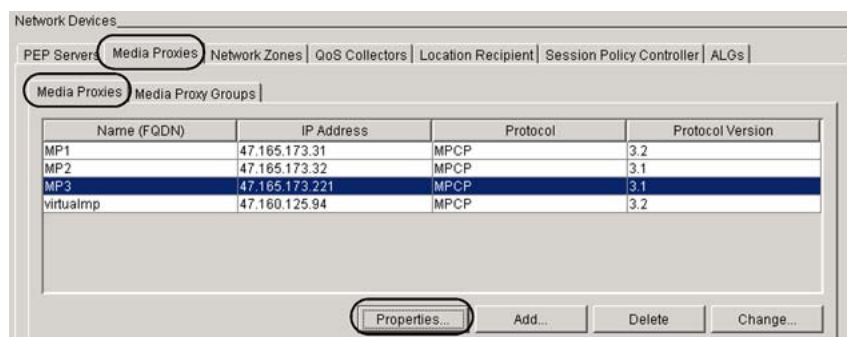
There are no prerequisites or guidelines for procedure.

Action

Step	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 Network Devices panel click the Media Proxies tab, then click the newly displayed Media Proxies tab.
3	Select the proxy you wish to view. Your selection is highlighted.
4	Click the Properties button.
The Media Proxy Description dialog box displays all the preferred media proxy groups to which the selected media proxy belongs and all GWCs with which the proxy is associated.	

At the CS 2000 GWC Manager client

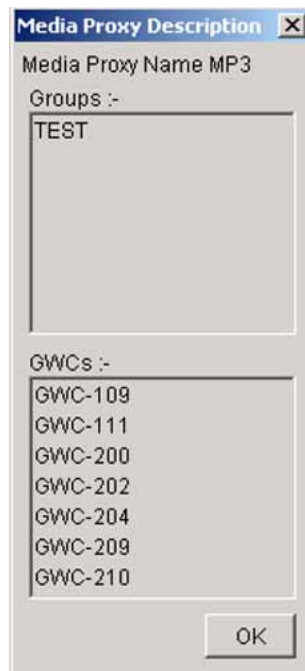
- At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
- From the Network Devices panel click the **Media Proxies** tab, then click the newly displayed **Media Proxies** tab.



- Select the proxy you wish to view. Your selection is highlighted.

- Click the **Properties** button.

The Media Proxy Description dialog box displays all the preferred media proxy groups to which the selected media proxy belongs and all GWCs with which the proxy is associated.



- 5 Click **OK** to close the dialog box.
- 6 The procedure is complete.

—End—

View media proxies associated with a GWC node

Purpose of this procedure

Use this procedure to view configuration data for media proxies currently associated with a selected Gateway Controller (GWC) node.

The same media proxies can also belong to preferred media proxy groups. To view the list of all media proxy groups and GWCs with which the selected media proxy is associated, see procedure ["View media proxy associations" \(page 414\)](#).

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

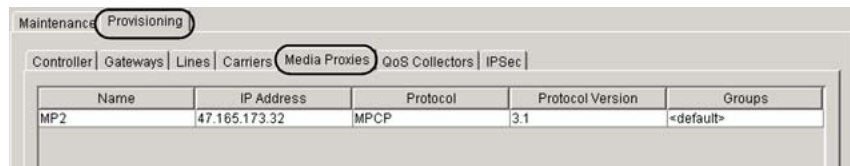
There are no prerequisites or guidelines for this procedure.

Action

Step	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.
4	Click the Media Proxies tab. The displayed table lists the following information about media proxies currently associated with the selected GWC node:
	- the name - the IP address - the protocol and protocol version

At the CS 2000 GWC Manager client

- At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
- From the Contents of: Gateway Controller frame, select the GWC node that has a media proxy you wish to view.
- Click the **Provisioning** tab in the GWC node view.



Name	IP Address	Protocol	Protocol Version	Groups
MP2	47.165.173.32	MPCP	3.1	<default>

- Click the **Media Proxies** tab. The displayed table lists the following information about media proxies currently associated with the selected GWC node:
 - the name
 - the IP address
 - the protocol and protocol version

- the groups associated with the selected GWC to which the selected media proxy belongs. The <default> entry means that the selected media proxy is one of the default media proxies for the selected GWC.

If you wish to view all GWCs and all media proxy groups with which a particular media proxy is currently associated, see procedure ["View media proxy associations" \(page 414\)](#).

5 The procedure is complete.

—End—

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 or Core and Billing Manager (CBM).

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 *Upgrading the Gateway Controller*, NN10196-461.

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 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

Step	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.

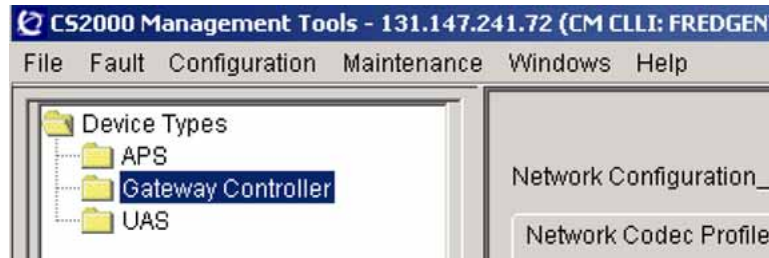
Example

```
# cp pgc06as.imag pgc06as.imag.bak
```

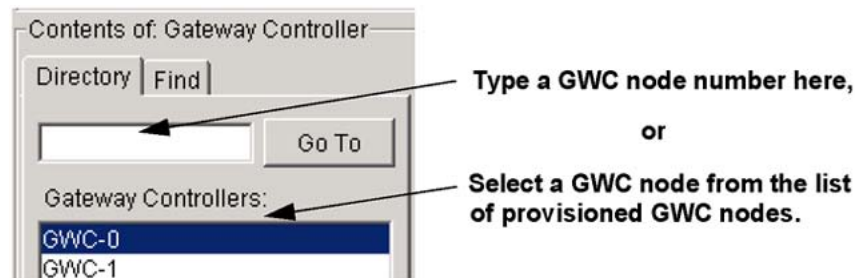
You can use any name for the backup file name.

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 want 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. Click the Save Image button for that card to save the software image back to the CS 2000 Core Manager or CBM.

The Save Image command overwrites the existing GWC software load file on the CS 2000 Core Manager or CBM.



CAUTION

Do not invoke the Save Image function during patching activities. Doing so can cause an invalid or corrupt image to be saved.



- 8 At the following warning message, click OK to continue with saving the GWC card's software image on the CS 2000 Core Manager. To abort the operation, click Cancel.



ATTENTION

If the load file name is a link on the file system, the link is replaced with a file of the same name. Nortel does not support using links to load files.

- 9 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure. To return to the Overall GWC upgrade procedure, refer to Overall GWC upgrade process - manual. To return to the Overall GWC downgrade procedure, refer to Roll back a software upgrade on a standby GWC node.

—End—

Troubleshooting

The /swd/gwc directory needs to have privileges set to read, write, execute for world access.

Step	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 /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	Log out of the CS 2000 Core Manager or CBM.

- 5 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Reconfiguring 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.

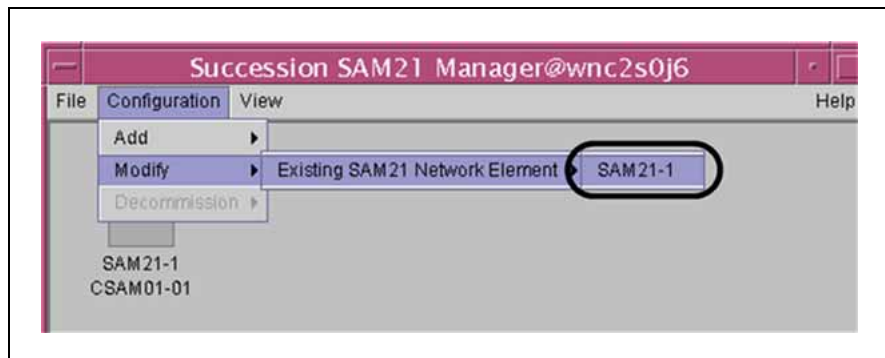
Gateway Controllers (GWC) do not require locking and unlocking to update the NTP server information. GWCs require a Warm Swact. Refer to "Invoking a manual protection switch (warm swact)" in *Gateway Controller Security and Administration*, NN10213-611.

For information about updating the NTP service on the Call Agents, refer to "Reconfigure NTP service" in *Call Agent Configuration Management*, NN10111-511.

Step	Action
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.

At the CS 2000 SAM21 Manager client

- 1 Select the shelf to modify from the Subnet View.



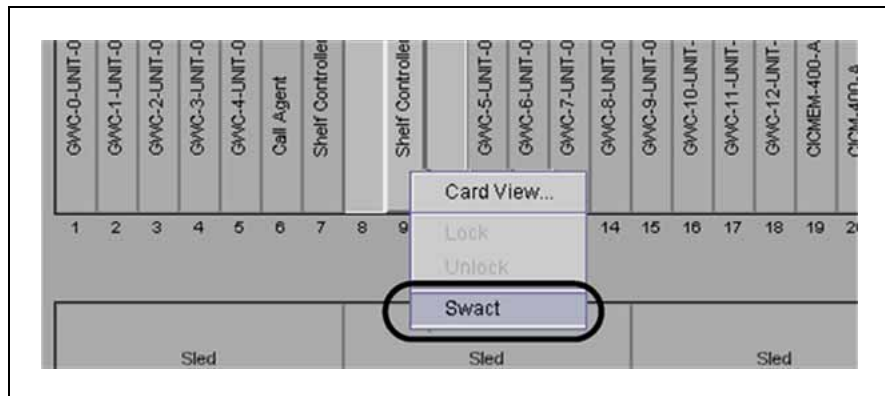
- 2 Replace the value in the Primary and Secondary NTP fields with the new NTP server addresses.

- 3 Lock and then unlock the inactive Shelf Controller.

Two critical alarms are raised after the lock operation. The alarms clear after the unlock operation.

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" \(page 424\)](#)
- 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.

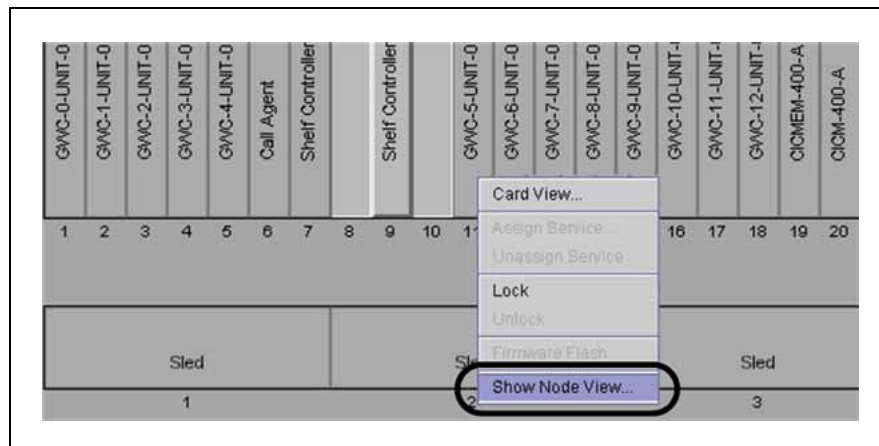
—End—

Additional information

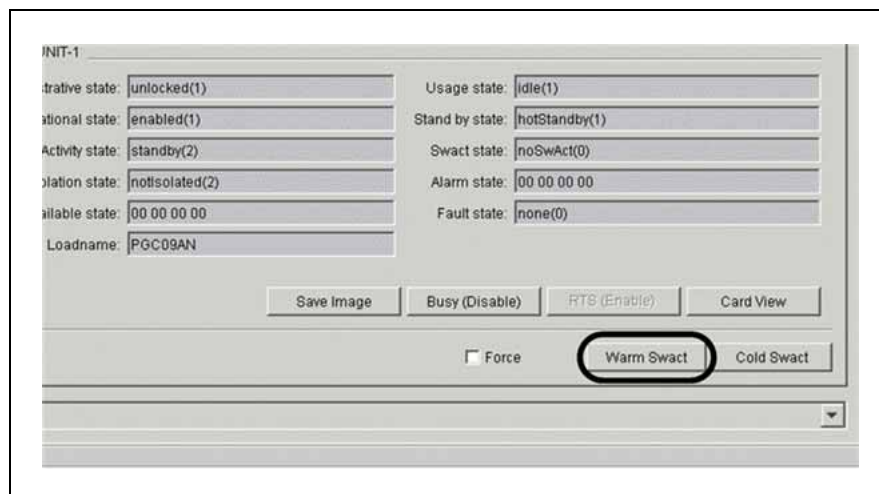
Some network components require different maintenance activities to update the NTP server information.

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.



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.

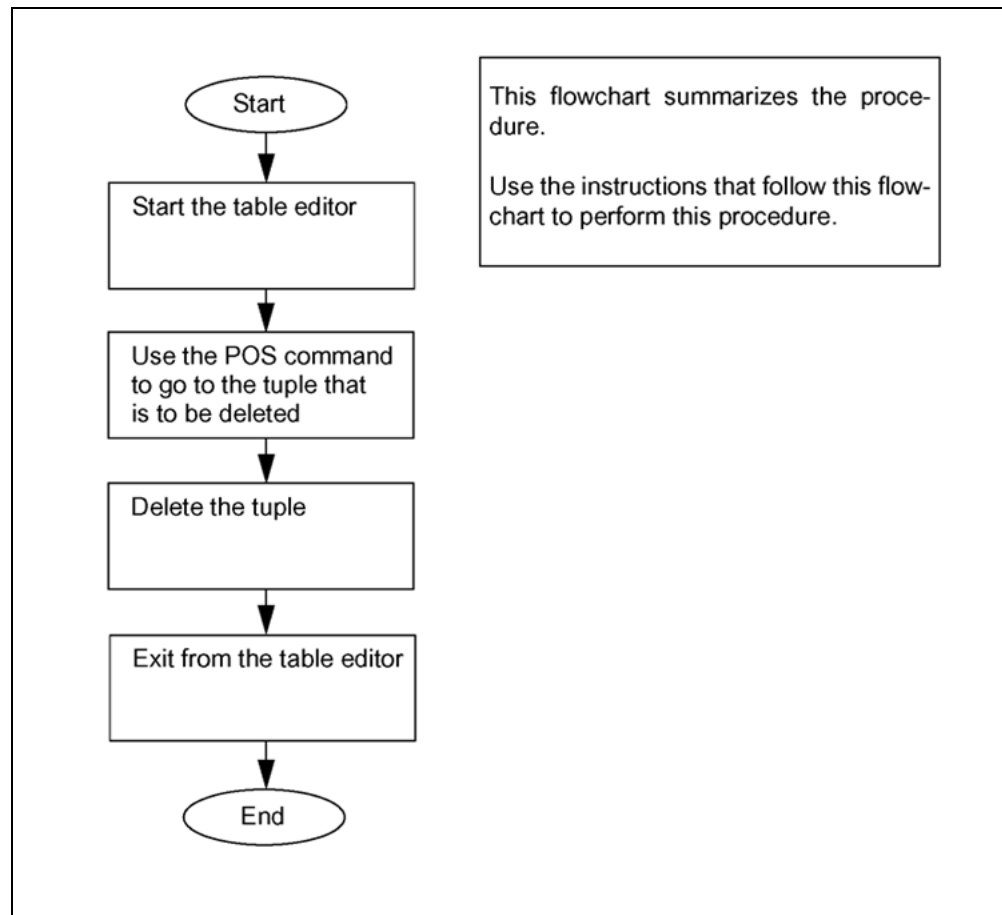
Common procedures

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

Step	Action

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.

—End—

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.

Note 1: SERVORD+ commands are the subset of SERVORD commands that can be entered by way of the OSSGate interface.

Note 2: For detailed information about SERVORD commands, see *SERVORD Reference Manual* (297-8001-808) in the North American market, or 297-9051-808 in the international market.

- 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:

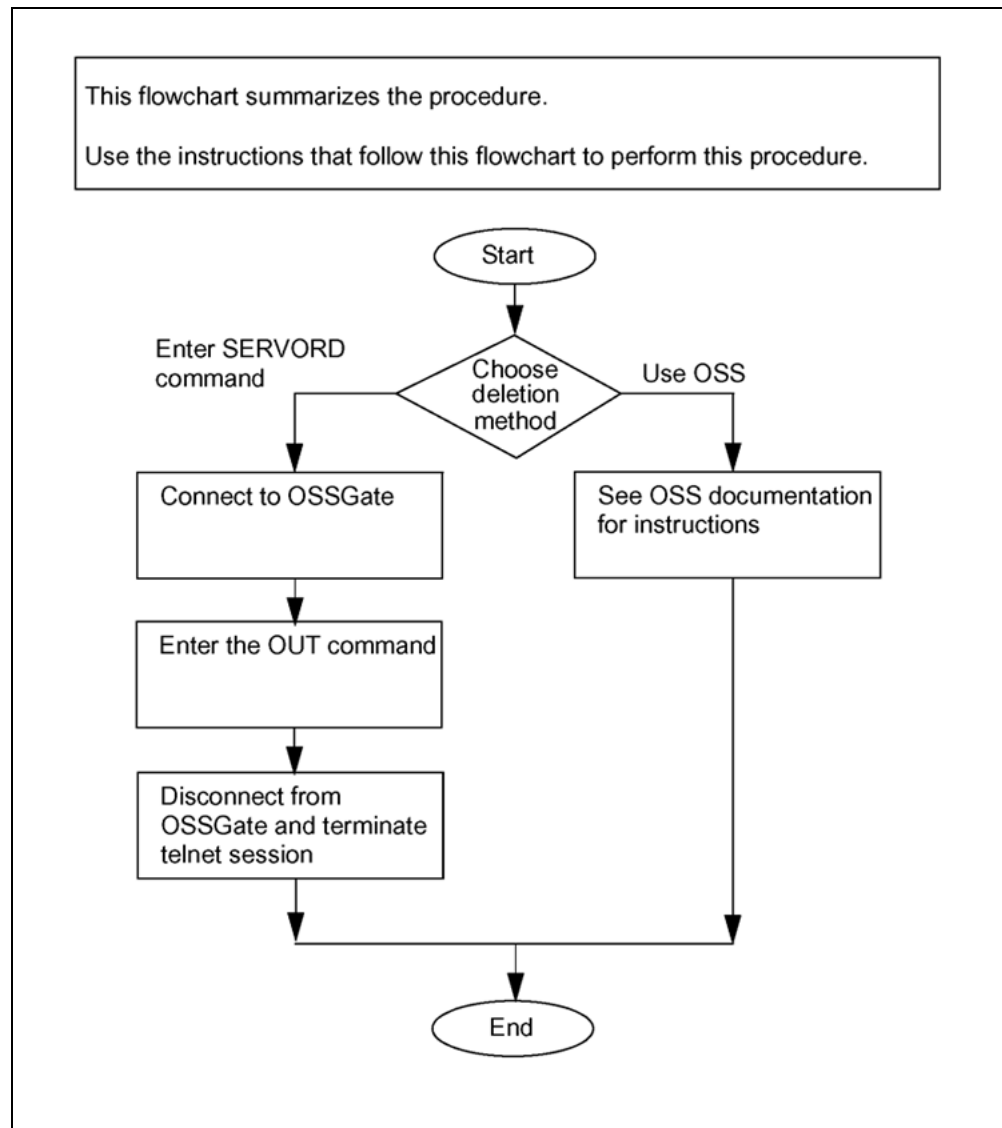
- You must have the telnet application.
- You must know either the host name or the IP address of the server on which OSSGate is running. If in doubt, ask the local network administrator.
- You must know the number of the port used by OSSGate. If in doubt, ask the local network administrator.

Common procedures

This procedure does not refer to any common procedures.

Action

The following flowchart summarizes this procedure.

Deleting a line**CAUTION**

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**Step Action**

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 14
- 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:*

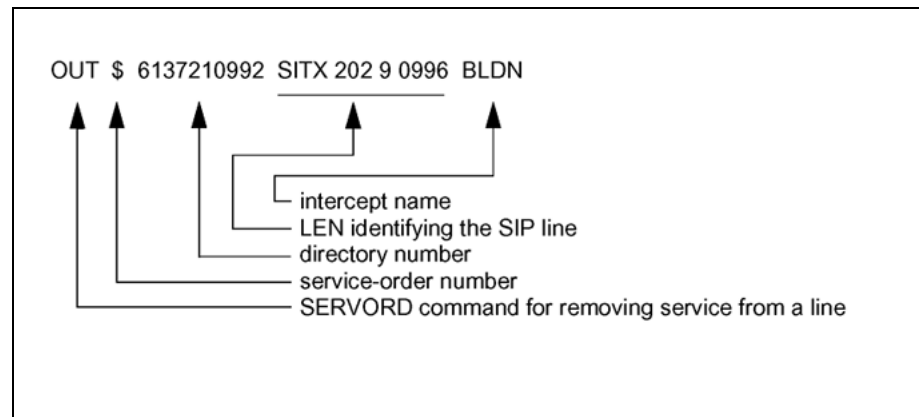
```
Mode is CI.
```

```
>
```

- 5 Select the next step as follows:

| If you are deleting                                      | Do                      |
|----------------------------------------------------------|-------------------------|
| a SIP lin                                                | <a href="#">step 6</a>  |
| a line on a CICM gateway                                 | <a href="#">step 8</a>  |
| a line other than a SIP line or a line on a CICM gateway | <a href="#">step 10</a> |

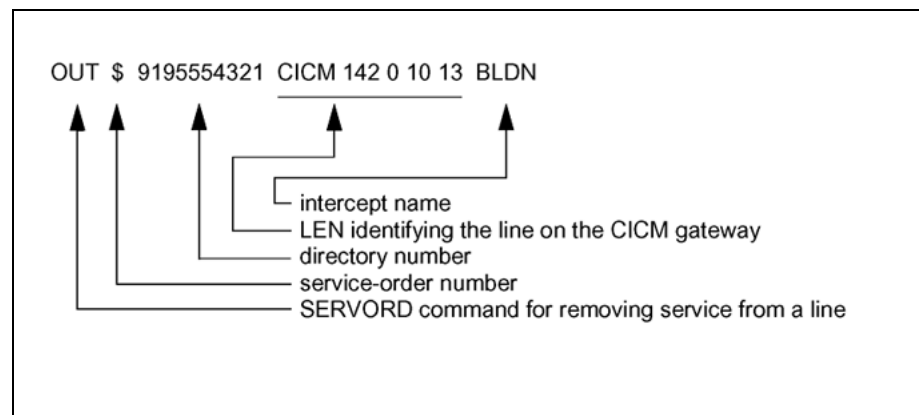
- 6 Delete the SIP line by entering the OUT command at the ">" prompt. The following figure shows an example of the OUT command to delete a SIP line.

**Example of the OUT command to delete a SIP line**

**Note:** For detailed information on the format of the LEN identifying a SIP line, see the module that tells how to provision SIP lines. That module will be available if your solution supports SIP lines.

- 7 Go to [step 11](#).
- 8 Delete the line on the CICM gateway by entering the OUT command at the ">" prompt.

The following figure shows an example of the OUT command to delete a line on a CICM gateway.

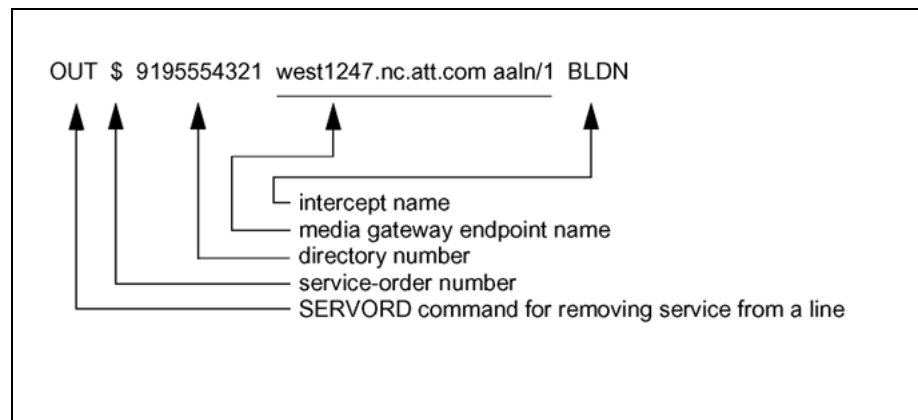
**Example of the OUT command to delete a line on a CICM gateway**

**Note:** For detailed information on the format of the LEN identifying a line on a CICM gateway, see the module that tells how to provision lines on CICM gateways. That module will be available if your solution supports lines on CICM gateways.

- 9 Go to [step 11](#).
- 10 Delete the line by entering the OUT command at the ">" prompt.

The following figure shows an example of the OUT command.

**Example of the OUT command**



**Note:** For detailed information on the format of the media gateway endpoint name in the OUT command, see ["Media gateway endpoint names"](#) (page 435) in this module.

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.

**11** 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.

>

**12** 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.
```

- 13 Go to [step 17](#).
- 14 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
- 15 Access the OSS following the instructions of your system administrator.
- 16 Delete the line using the OSS interface.
- 17 You have completed this procedure.

---

—End—

---

**Media gateway endpoint names**

This section contains information on the format of the media endpoint gateway name used in the OUT command that deletes certain lines.

This information is not relevant to SIP lines, and is not relevant to lines on CICM gateways. For those types of lines, you do not use the media endpoint gateway name in the OUT command; instead, you use the line equipment number (LEN) to identify the line.

**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
```

**Note:** If a gateway is associated with a GWC for which a default gateway domain name has been provisioned, do not use the default gateway domain name as part of the <media-gateway-name> in any SERVORD+



command. SERVORD+ commands are the subset of SERVORD commands that can be entered by way of the OSSGate interface.

- <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

---

## Fault management strategy

---

The Gateway Controller (GWC) uses self-testing, automated diagnostics and reporting systems to support maintenance and manage faults. These systems raise alarms and generate log reports when the following types of hardware or software events occur:

- a fault or failure condition
- correction of a fault or failure condition
- a threshold is crossed and the GWC is operating at a degraded level or has exceeded a defined operating capacity level
- a condition occurs that is transient or cannot be repaired.

### GWC alarms

Alarms provide notification that a system hardware or software-related event has occurred that requires attention. Alarms are generated by the GWC or a related component, such as a gateway, when problems or conditions are detected that can change the performance or operating state of a GWC node and its connections. Administration of the network elements requires monitoring for alarms and checking that functions continue without interruption.

The GWC is provisioned with a set of pre-defined alarms installed. You cannot remove or modify these alarms, although you can disable them. By default, all system alarms are enabled.

Alarm management for the GWC is separated into two categories: hardware faults and service and application faults. Hardware fault management activities are carried out using the CS 2000 SAM21 Manager. Service and application fault management activities are carried out using the CS 2000 GWC Manager.

Fault clearing depends on the timely resolution of alarms. Alarms provide notification of problems or conditions that can change the performance or working state of the GWC, the CS 2000 or other related network components.

### Alarm severity codes

Alarm severity codes indicate the impact of events on the GWC or other network elements. There are four levels of alarm severity:

- Critical alarm - This severity level indicates that a service affecting condition has occurred and an immediate corrective action is required. For example, a critical alarm occurs when a managed element is out of service and its capability must be restored.

- **Major alarm** - This severity level indicates a service affecting condition that requires an urgent corrective action. For example, a major alarm occurs when there is a severe degradation in the capability of the managed element, such as loss of fault tolerance, and its full capability must be restored.
- **Minor alarm** - This severity level indicates a non-service affecting fault condition. Corrective action should be taken in order to prevent a more serious fault that might affect service. A minor alarm occurs when an alarm condition exists that does not degrade the capacity of the managed element.
- **Warning Alarm** - This severity level indicates the detection of a potential or impending service affecting fault, before there is any significant effect. Action should be taken to further diagnose and correct the problem to prevent it from becoming a more serious service affecting fault.

Based on alarm severity, each alarm has a specific color. Critical and major alarms are red, minor alarms are orange and warnings are yellow. For an example of the alarm severity color codes, see the following figure.

|                                                                                     | Network Element | Category         | Alarm Time             | Sever... | Probable Cause          |
|-------------------------------------------------------------------------------------|-----------------|------------------|------------------------|----------|-------------------------|
|    | GWC-222-UNIT-0  | Communications   | 11:36:20 30-Jun-200... | Minor    | LAN error               |
|   | GWC-222-UNIT-0  | Communications   | 12:10:36 30-Jun-200... | Major    | Communications subsy... |
|  | gwcem           | Processing Error | 08:27:06 01-Jul-200... | Critical | Corrupt data            |
|  | SNMP_NE_Poller  | Communications   | 08:22:53 01-Jul-200... | Major    | Communications subsy... |
|  | GWC-222         | Communications   | 11:36:20 30-Jun-200... | Minor    | LAN error               |

## Alarm acknowledgement

It is possible to acknowledge or silence existing GWC service related alarms, although any new alarms cannot be silenced. Starting in (I)SN07, you can no longer acknowledge GWC alarms or view acknowledged GWC alarms using the CS 2000 GWC Manager. Procedures to perform this activities are removed from this NTP.

Use the Integrated Element Management System (IEMS) to perform these functions. For information about alarm acknowledgement, see *IEMS Fault Management* (NN10334-911).

## GWC logs

A log report is a record of a message that your system or component generates whenever a significant event has occurred on the switch, one of its peripherals or a network element such as the GWC. Log reports include status and activity reports, as well as reports on hardware or software faults, test results, changes in state and other temporary events or conditions likely to affect the performance of the system. A system action or a manual action can generate a log report.

When software code traps are generated by faults in the software code running on the GWC, service related PM logs are generated by the GWC to the Core. These logs can be accessed using the logutil application at a maintenance and administration position (MAP) terminal.

When fault events occur on the GWC, a simple network management protocol (SNMP) trap is sent to the common SNMP agent that resides on the CS 2000 Management Tools server. The trap is logged using the syslog UNIX logger. The text file output of syslog is saved to a default file location on the CS 2000 Management Tools server.

Alarm information is sent to:

- the alarm browser in the CS 2000 GWC Manager
- the Operations Support System (OSS) interface for presentation to an OSS application (e.g. Micro Muse)
- the CS 2000 Management Tool server syslog storage for logs.

For syslog storage, the alarm is converted into syslog format before storing. It is possible to disable syslog alarm logging to prevent CS 2000 Management Tools alarms (including the GWC alarms) from being written to the customer log files. You may want to avoid the duplication of these alarms if your system is reporting them using another tool.

For information about how to configure alarm logging, see CS 2000 Management Tools sections in *Nortel ATM/IP Solution-level Fault Management* (NN10408-900).

Event log information is sent to:

- the alarm browser in the CS 2000 GWC Manager
- the CS 2000 Management Tool server syslog storage for logs.

GWC log information, included in syslog logs found in the /var/log directory on the CS 2000 Management Tools server, can also be forwarded to the customer's OSS interface for analysis. The following items must be in place for the GWC logs to be forwarded to the OSS:

- The syslog client and the CS 2000 GWC Manager must reside on the same host (typically the CS 2000 Management Tools server).
- The Solaris log host on the CS 2000 Management Tools server must be configured to accept remote logs from multiple log sources.

For more information about syslog, and for instructions about syslog forwarding in a network containing the Integrated Element Management System (IEMS), see the CS 2000 Management Tools sections in *Nortel ATM/IP Solution-level Fault Management* (NN10408-900).

For more information about how to access the GWC syslog logs, see procedure ["View GWC logs in syslog files"](#) (page 487) in this NTP.

For GWC log report descriptions, see *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909).

## Logs and alarms associated with IPSec

Use the following logs and alarms to monitor and manage faults and other events associated with IPSec:

- logs GWC309, GWC320, GWC400

For more information, see *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909).

- Kerberos logs
- IPSec and IKE security logs
- alarm SA\_PERCENTAGE\_USAGE (minor)
- GWC320 alarms (various specific problems)

For alarms information, see procedure ["View and troubleshoot GWC service alarms"](#) (page 444).

## View GWC service alarm history

### Purpose of this procedure

This procedure provides access to service-related alarms that have occurred on the GWC application.

The alarm history option allows you to query the GWC alarms that have already occurred, and permits alarm display filtering based on GWC unit, alarm severity, alarm category and date / time.

Access to platform-related alarms is provided in procedure "[View GWC platform hardware alarms](#)" (page 461).

### When to use this procedure

Use this procedure as a part of scheduled maintenance and as a primary source of fault diagnostic information for GWC services.

### Prerequisites

This procedure has no prerequisites.

### Action

| Step | Action |
|------|--------|
|------|--------|

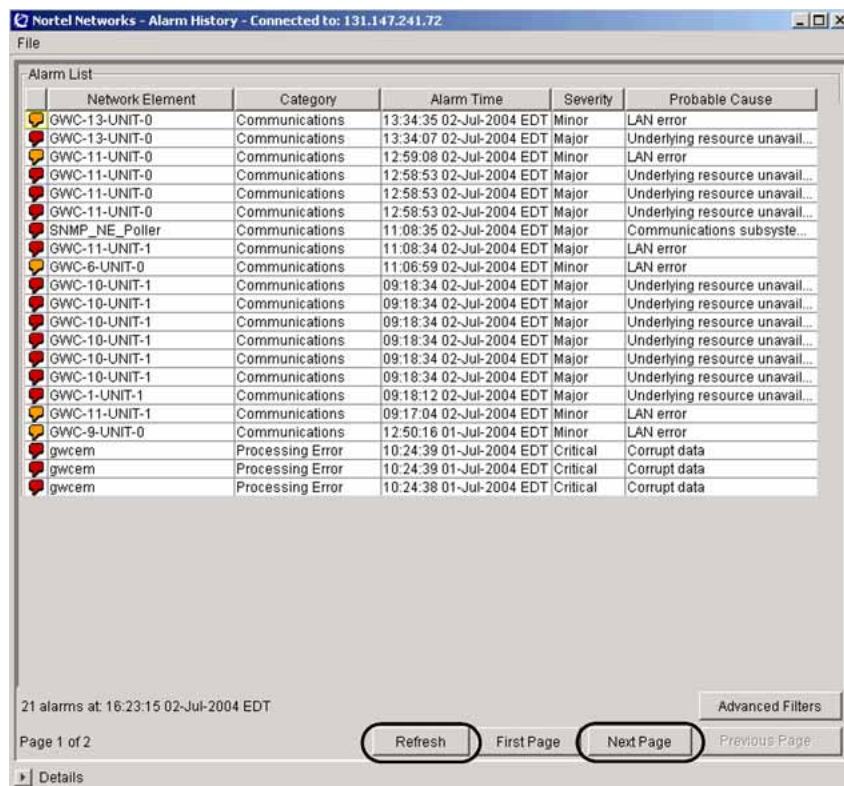
#### *At the CS 2000 GWC Manager client*

- 1 From the CS2000 Management Tools window menu, select the **Fault** menu and then **Alarm History**.

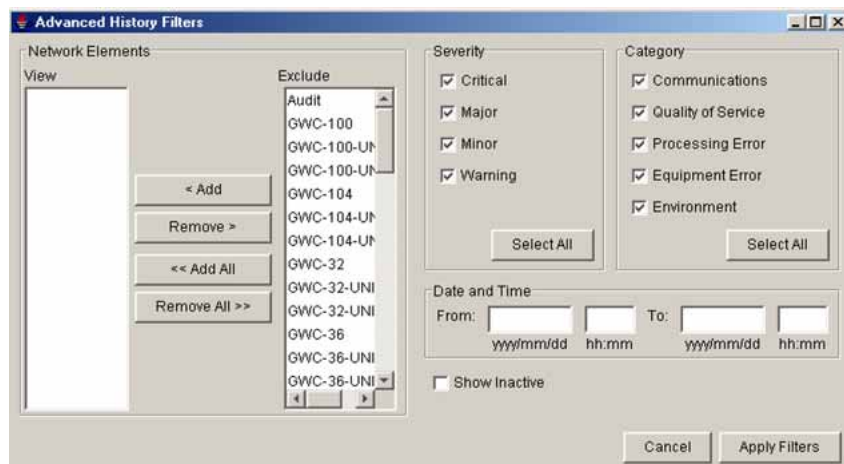


- 2 Review the alarms displayed.  
The colors to the left of the alarm display provide a visual indication of alarm severity:
  - yellow - warning
  - orange - minor
  - red - major and critical
- 3 Click **Refresh** to update the alarm list.

- 4 Click **Next Page** (if applicable) to view more alarms.



- 5 Click the **Advanced Filters** button to filter alarms based on selected criteria.



- 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 Severity check boxes to exclude (filter) an alarm type for the GWC units in the Exclude list. Any alarm severities that remain selected will be included (will not be filtered) for the GWC units in the Exclude list. If necessary, click the **Select All** button to select all alarm severity check boxes.
  - d. 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. If necessary, click the **Select All** button to select all alarm category check boxes.
  - e. If you wish to filter according a specific range of dates, type the date range in the format, yyyy/mm/dd.
  - f. If you wish to filter according a specific time frame, type the time frame in the format, hh:mm.
  - g. After you have selected the filter criteria, click the **Apply Filters** button.
- 6 If necessary, click the **Advanced Filters** button again to further modify the filter criteria, then click the **Apply Filters** button.
  - 7 When you are finished with the Alarm History, click the **File** menu at the top of the screen and select **Close**.
  - 8 This procedure is complete.

---

—End—

---



## 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.

Access to platform-related alarms is provided in procedure "[View GWC platform hardware alarms](#)" (page 461).

### 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

| Step | 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 critical



See section "Troubleshooting GWC service alarms" (page 447) 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" (page 448) 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

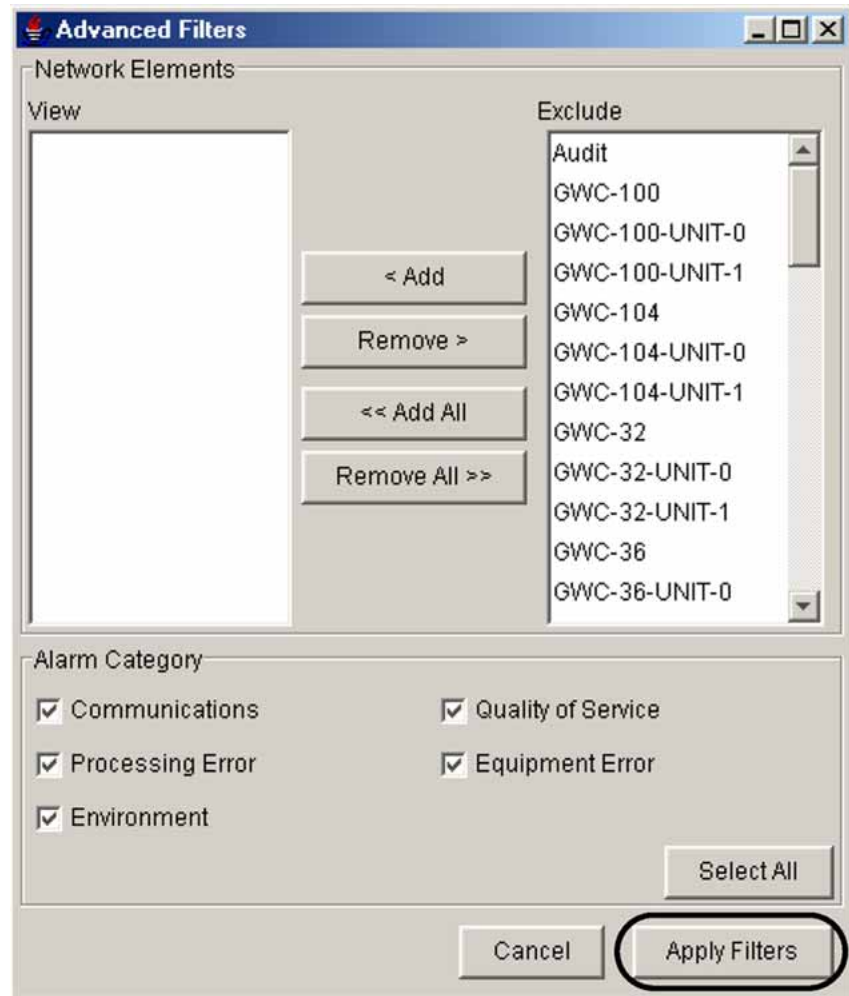
Refresh List

Details

Log Name: GWC 307  
 NE Name: GWC-5-UNIT-0  
 Alarm Level: Major  
 Category: Communications  
 Alarm Time: 05:14:26 07-Jun-2004 EDT  
 Probable Cause: Communications subsystem failure  
 System Uptime: 1 hours, 0 minutes, 11 seconds.

Component ID: GWC=GWC-5-UNIT-0;Ve  
 NODEMTC  
 Alarm Description: Element Manager comm  
 Specific Problem: EM indicates provisioner

- 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 at the top of the screen and select **Close**.
- 7 This procedure is complete.

---

—End—

---

## Troubleshooting GWC service alarms

The following table contains details about GWC alarm types, and includes appropriate actions to diagnose and resolve the alarm condition.

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 about how to open these Syslog log files and search for alarm codes, see procedure ["View GWC logs in syslog files"](#) (page 487) 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 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 about configuring log delivery to the customer's OSS, see the Fault Management NTP for the CS 2000 Core Manager or CBM.

The following table lists GWC service alarms.

#### Troubleshooting GWC service alarms

| Alarm description<br>Alarm ID code<br>Severity           | Specific problem<br>Probable cause                                                                                                                                                                                                                                                                                                                            | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recovery alarm<br><b>GWCEM301</b><br><i>Critical</i>     | 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<br><b>GWC300</b><br><i>Critical</i> | <p>Specific problem:<br/>Indicates that a unit is out of service: Service is not available.</p> <p>Probable cause:<br/>the lack of availability of the underlying resource.</p> <p>Specific problem:<br/>Indicates that a unit has invalid GWC Profile Data: Service is not available.</p> <p>Probable cause:<br/>A configuration or customization error.</p> | <p>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.</p> <p>When both units are out of service, the active unit must recover before the standby unit will.</p> <p>Check the following:</p> <ul style="list-style-type: none"> <li>• Whether the unit is manually locked out of service (Administrative state of "locked").</li> <li>• Alarms that may indicate a problem on the unit preventing it from returning to service.</li> <li>• Other state indicators which may indicate problems, such as: <ul style="list-style-type: none"> <li>— Isolation state of "isolated"</li> <li>— Availability state of "offLine"</li> </ul> </li> <li>• Logs which may also indicate a failure of a step in the process of recovering the unit.</li> </ul> <p>Check the profile data for the unit and do one of the following:</p> <ul style="list-style-type: none"> <li>- Change to another profile.</li> <li>- Reconfigure the GWC unit software or CS 2000 GWC Manager software to remove the incompatibility.</li> </ul> <p>Then RTS the unit.</p> |

| Alarm description<br>Alarm ID code<br>Severity         | Specific problem<br>Probable cause                                                                                                                     | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Standby unit disabled<br><b>GWC301</b><br><i>Major</i> | Specific problem:<br>Unit is out of service - Service is not available.<br><br>Probable cause:<br>The lack of availability of the underlying resource. | <p>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.</p> <p>When both units are out of service, the active unit must recover before the standby unit will.</p> <p>Check the following:</p> <ul style="list-style-type: none"> <li>alarms that may indicate a problem on the unit preventing it from returning to service</li> <li>other state indicators which may indicate problems, such as: <ul style="list-style-type: none"> <li>isolation state of "isolated"</li> <li>for the standby unit, availability state of "degraded"</li> <li>availability state of "offLine"</li> </ul> </li> <li>logs which may also indicate a failure of a step in the process of recovering the unit</li> </ul> |
| Standby unit disable<br><b>GWC301</b><br><i>Minor</i>  | Specific problem:<br>Unit is out of service - Service is not available.<br><br>Probable cause:<br>The lack of availability of the underlying resource. | <p>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.</p> <p>When both units are out of service, the active unit must recover before the standby unit will.</p> <p>Check the following:</p> <ul style="list-style-type: none"> <li>alarms that may indicate a problem on the unit preventing it from returning to service</li> </ul>                                                                                                                                                                                                                                                                                                                                                                 |

| Alarm description<br>Alarm ID code<br>Severity                | Specific problem<br>Probable cause                                                                                                            | Action                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                               |                                                                                                                                               | <ul style="list-style-type: none"> <li>other state indicators which may indicate problems, such as:               <ul style="list-style-type: none"> <li>isolation state of "isolated"</li> <li>for the standby unit, availability state of "degraded"</li> <li>availability state of "offLine"</li> </ul> </li> <li>logs which may also indicate a failure of a step in the process of recovering the unit</li> </ul> |
|                                                               | <p>Specific problem:<br/>Unit out of service - invalid GWC Profile Data.</p> <p>Probable cause:<br/>Configuration or customization error.</p> | <p>Check the profile data for the unit and do one of the following:</p> <ul style="list-style-type: none"> <li>- Change to another profile.</li> <li>- Reconfigure the GWC unit software or CS 2000 GWC Manager software to remove the incompatibility.</li> </ul> <p>Then, RTS the unit.</p>                                                                                                                          |
| Core communication lost<br><b>GWC302</b><br><i>Major</i>      | <p>Specific problem:<br/>No response received to Core heartbeat messages from active GWC unit.</p> <p>Probable cause:<br/>LAN error.</p>      | 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.                                                                                                                                                                                                                                       |
| Core communication lost<br><b>GWC302</b><br><i>Minor</i>      | <p>Specific problem:<br/>No response received to Core heartbeat messages from inactive GWC unit.</p> <p>Probable cause:<br/>LAN error.</p>    | 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<br><b>GWC303</b><br><i>Minor</i> | <p>Specific problem:<br/>No response received to mate unit heartbeat messages.</p> <p>Probable cause:<br/>LAN error.</p>                      | 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.                                                                                                                                                               |



| Alarm description<br>Alarm ID code<br>Severity                                                             | Specific problem<br>Probable cause                                                                                                                                                                                                                                          | Action                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Communication with a gateway is down<br><b>GWC304</b><br><i>Major</i>                                      | Specific problem:<br>Communication with gateway <Gatewayname> is down.<br><br>Probable cause:<br>The underlying resource is not available.<br><br>'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<br><b>GWC305</b><br><i>Minor</i>                     | Specific problem:<br>A test alarm generated to log in to notilog table - not sent to manager.<br><br>Probable cause:<br>Unspecified reason.                                                                                                                                 | Cleared from pmdebug command (not a customer interface) or with a GWC reload.                                                                                                                                                          |
| This is a test alarm generated from pmdebug interface<br><b>GWC305</b><br><i>Critical, Major, or Minor</i> | Specific problem:<br>Alarms test from debug interface.<br><br>Probable cause:<br>Unspecified reason.                                                                                                                                                                        |                                                                                                                                                                                                                                        |
| DQoS/COPS connection failure<br><b>GWC306</b><br><i>Major</i>                                              | Specific problem:<br>A DQoS connection <ConnName> has failed - attempting recovery.<br><br>Probable cause:<br>Communications subsystem failure.<br><br>See GWC fault management in a DQoS network 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<br><b>GWC307</b><br><i>Major</i>                                     | Specific problem:<br>CS 2000 GWC Manager indicates provisioned data mismatched in this unit.<br><br>Probable cause:<br>Communications subsystem failure                                                                                                                     | Cleared with a Busy/RTS of GWC unit.                                                                                                                                                                                                   |



| Alarm description<br>Alarm ID code<br>Severity                                                                                                    | Specific problem<br>Probable cause                                                                                                                                                                                                                                                   | Action                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                   | <p>Specific problem:<br/>CS 2000 GWC Manager not responding, provisioned data loaded from local Flash.</p> <p>Probable cause:<br/>Communications subsystem failure</p>                                                                                                               | Restore communication with the CS 2000 GWC Manager. Determine if the CS 2000 GWC Manager is down or disconnected, or both. 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<br><b>GWC308</b><br><i>Minor</i>                                                                                               | <p>Specific problem:<br/>Erase of flash sector failed.</p> <p>Probable cause:<br/>Equipment malfunction.<br/>Flash life span exceeded; the number of writes to flash has exceeded the recommended or intended limit.</p>                                                             | Cleared with hardware replacement.                                                                                                                                                                                                                   |
| SA_PERCENTAGE_USAGE<br><b>GWC309</b><br><i>Minor</i><br><br>This alarm does not apply to the Wireline Universal Packet Access (UA-AAL1) solution. | <p>Specific problem:<br/>The number of IPSec security associations (that is, secure connections) reached the maximum supported number.</p> <p>Probable cause:<br/>Resource at or nearing capacity</p>                                                                                | 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.                                                                                          |
| Provisioned GWC Profile not yet activated<br><b>GWC311</b><br><i>Warning</i>                                                                      | <p>Specific problem:<br/>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.</p> <p>Probable cause:<br/>Configuration or customization error.</p> | Cleared with a GWC reload.                                                                                                                                                                                                                           |

| Alarm description<br>Alarm ID code<br>Severity                                                        | Specific problem<br>Probable cause                                                                                                           | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| QoS collection application (QCA) connection failure<br><b>GWC312</b><br><i>Major (partial outage)</i> | Specific problem:<br>QCA connection <ConnName> has failed - attempting recovery.<br><br>Probable cause:<br>Communications subsystem failure. | No reports are lost since a back up server is collecting them.<br><br>Check the following: <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>3. Verify that there is no memory exhaustion on the QCA server.</li> <li>4. Restart the QCA application on the server to bring up the links.</li> <li>5. Try connecting to a QCA on another CS 2000 Management Tools server.</li> </ol> |
| QCA connection failure<br><b>GWC312</b><br><i>Critical (total outage)</i>                             | Specific problem:<br>QCA connection <ConnName> has failed - attempting recovery.<br><br>Probable cause:<br>Communications subsystem failure. | Check the following: <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>3. Verify that there is no memory exhaustion on the QCA server.</li> <li>4. Restart the QCA application on the server to bring up the links.</li> <li>5. Try connecting to a QCA on another CS 2000 Management Tools server.</li> </ol>                                                                       |

| Alarm description<br>Alarm ID code<br>Severity                                                                                                          | Specific problem<br>Probable cause                                                                                                                                                             | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RMGC overloaded<br><b>GWC313</b><br><i>Major</i>                                                                                                        | Specific problem:<br>RMGC can't process all incoming requests.<br><br>Probable cause:<br>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.<br><br>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<br><b>GWC314</b><br><i>Major</i>                                                                               | Specific problem:<br>Location ID reporting connection <IP address> has failed - attempting to recover.<br><br>Probable cause:<br>Communications subsystem failure - destination not available. | Clear the alarm condition using one of the following approaches: <ul style="list-style-type: none"> <li>• Reestablish the connection to the location recipient.</li> <li>• Disable the location ID reporting application.</li> <li>• Busy/RTS the GWC unit.</li> </ul>                                                                                                                                                                                                    |
| External host interface signal loss<br><b>GWC315</b><br><i>Critical (&gt;50% loss)</i><br><i>Major (&gt;20% loss)</i><br><i>Minor (any signal loss)</i> | Specific problem:<br>Small GWs in disabled state<br><br>Probable cause:<br>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.<br><br>Use the new small gateway OMs to check how many small line GWs are out of service.<br><br>Use the logs to identify which GWs need attention.                                                                                                                            |
| External host interface signal loss<br><b>GWC315</b><br><i>Major (both links down)</i><br><i>Minor (one link down)</i>                                  | Specific problem:<br>USP SS7 paths disabled<br><br>Probable cause:<br>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.<br><br>Check the USP connections.                                                                                                                                                        |

| Alarm description<br>Alarm ID code<br>Severity                                                                                                    | Specific problem<br>Probable cause                                                                          | Action                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| External host interface signal loss<br><b>GWC315</b><br><i>Critical</i> (>50% loss)<br><i>Major</i> (>20% loss)<br><i>Minor</i> (any signal loss) | Specific problem:<br>Peer connections failed during interval<br><br>Probable cause:<br>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.<br><br>Use the new peer messaging OMs to check the number of calls failed over a longer period.<br><br>Check the Ethernet link between the GWC and the remote host or peer GWCs.                                                                  |
| External host interface configuration error<br><b>GWC315</b><br><i>Warning</i> (non-service affecting)                                            | Specific problem:<br>DNS failed GW discovery<br><br>Probable cause:<br>Configuration or customization error | This alarm is based on the number of gateways that failed DNS lookup in a 5-minute polling period.<br><br>Use the new DNS OMs to check the number of gateways not discovered, and the number of gateways discovered using RSIP.<br><br>RSIP discovery does not survive a cold SwAct on the GWC, which may cause long outages.<br><br>Check the DNS server entries for every gateway. |
| External host interface protocol error<br><b>GWC315</b><br><i>Major</i> (both links not active)<br><i>Minor</i> (one link not active)             | Specific problem:<br>USP SS7 path not active<br><br>Probable cause:<br>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.<br><br>A major alarm affects some call processing; a minor alarm causes a redundancy error.<br><br>Check the USP configuration to the GWC.                                                                                                        |

| Alarm description<br>Alarm ID code<br>Severity                                                                                                                                    | Specific problem<br>Probable cause                                                                                                                                                                                                                                                                                                                                                                                 | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| External communication interface<br><b>GWC315</b><br><i>Critical</i> (>50% proxies disabled)<br><i>Major</i> (>20% proxies disabled)<br><i>Minor</i> (any media proxies disabled) | Specific problem:<br>Media proxies in disabled state<br><br>Probable cause:<br>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.<br><br>Use the media proxy OMs to check how many media proxies are out of service in any 5-minute polling period.<br><br>Use the RTP Portal EM to identify which media proxies need attention.<br><br>This alarm and the associated OMs give the GWC view of calls, as opposed to the media proxy view. |
| PreSwact audit failure<br><b>GWC317</b><br><i>Major</i>                                                                                                                           | Specific problem:<br>PreSwact audit failed for two consecutive cycles<br><br>Probable cause: <ul style="list-style-type: none"> <li>monitored base resource reaches the threshold level</li> <li>monitored application resource reaches the threshold level</li> <li>data synchronization mismatch (SESM, GWC flash, GWC RAM)</li> <li>standby unit is jammed and prevented from taking up the activity</li> </ul> | Check the alarm text to see which component has failed.<br>The alarm clears when you clear the error condition.<br><br>If required, you can use Swact force to force a manual warm Swact.                                                                                                                                                                                                                                                                                                                                                                                                         |

The preSwact audit runs at a frequency of 40 seconds and with priority 6.

A second occurrence of the same error condition does not raise an alarm.

No alarm is raised if the preSwact audit fails while patching is in progress in the inactive unit.

| Alarm description<br>Alarm ID code<br>Severity                                                                                                                                             | Specific problem<br>Probable cause                                                                                                                                                                                                                                                                                                                                            | Action                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Autonomous<br>SWACT initiated<br><br><b>GWC318</b><br><br><i>Critical</i>                                                                                                                  | Specific problem:<br>(Element Name>: No communication with associated media gateway(s)<br><br>Probable cause: Underlying resource unavailable.<br><br>This alarm indicates that the system attempts to restore communication with the associated media gateways.                                                                                                              | Check the related network component managers to identify failures within the network.<br><br>The alarm clears automatically when a manual SWACT back to the original active unit is performed.<br><br>You can also manually clear this alarm once the problem on the original active unit is solved. Follow procedure Clear the GWC318 critical alarm manually.                                                          |
| GWC communication loss with associated media gateway(s)<br><br><b>GWC319</b><br><br><i>Critical</i>                                                                                        | Specific problem:<br>(Element Name>: No communication with associated media gateway(s)<br><br>Probable cause: Underlying resource unavailable.                                                                                                                                                                                                                                | Check the related network component managers to identify failures within the network.<br><br>This alarm clears when the GWC detects communication with at least one associated gateway. It also clears when the GWC automatically or manually switches activity, but it is raised again on the newly active unit if communication is still lost with all associated gateways.                                            |
| IKE/IPSec<br><br><b>GWC320</b>                                                                                                                                                             | GWC320 alarms indicate an IKE/IPSec-related problems. See the Specific Problem: field to check the reason for generating this alarm.<br><br>Each specific alarm may have an associated security log, which provides additional details about the problem. For the description of all IKE and IPSec security logs, see procedure IPSec and IKE security logs.                  |                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>GWC320</b><br><br><i>Critical</i> - certificate expires within 5 days<br><br><i>Major</i> - certificate expires within 15 days<br><br><i>Minor</i> - certificate expires within 30 days | Specific problem:<br>One or more certificates in set number <x> are expiring. An outage may occur if an IKE connection policy is using these certificates. At the GWCEM, please verify the expiry dates for certificates in set number <x><br>-- <GWC_IP_address><br>where<br><br><x> is the set number of the [IKE certificates] panel<br><br>Probable cause:<br>Key expired | This alarm indicates that an IKE certificate is expiring soon and the GWC Manager has not obtained a new certificate from the Certificate Manager. Service disruption may occur when the certificate expires.<br><br>For information about how to clear this alarm, see procedure "Recovery of the GWC320 certificate expiry alarm" in <i>Nortel CVoIP IPSec Security Service Implementation Overview</i> (NN10453-100). |

| Alarm description<br>Alarm ID code<br>Severity | Specific problem<br>Probable cause                                                                                                                                                                                                                                                                                                                                                                       | Action                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>GWC320</b><br><i>Critical</i>               | <p>Specific problem:<br/>One or more certificates in set number &lt;x&gt; are expired. An outage will occur if an IKE connection policy is using these certificates. At the GWCEM, please verify the expiry dates for certificates in set number &lt;x&gt; -- &lt;GWC_IP_address&gt; where</p> <p>&lt;x&gt; is the set number of the [IKE certificates] panel</p> <p>Probable cause:<br/>Key expired</p> | <p>This alarm indicates that an IKE certificate is expired and the GWC Manager has not obtained a new certificate from the Certificate Manager. Service disruption will occur when the certificate expires.</p> <p>For information about how to clear this alarm, see procedure "Recovery of the GWC320 certificate expiry alarm" in <i>Nortel CVoIP IPSec Security Service Implementation Overview</i> (NN10453-100).</p> |
| <b>GWC320</b><br><i>Major</i>                  | <p>Specific problem:<br/>Phase 1 SA failure -- &lt;remote_gateway_IP_address&gt;</p> <p>Probable cause:<br/>Underlying resource unavailable</p>                                                                                                                                                                                                                                                          | <p>This alarm indicates that a Phase 1 negotiation failed. This alarm is the result of an outage.</p> <p>To clear this alarm, complete procedure Clear the GWC320 Phase 1 SA failure alarm.</p>                                                                                                                                                                                                                            |
| <b>GWC320</b><br><i>Major</i>                  | <p>Specific problem:<br/>Phase 2 SA failure -- &lt;remote_gateway_IP_address&gt;</p> <p>Probable cause: Underlying resource unavailable</p>                                                                                                                                                                                                                                                              | <p>This alarm indicates that a Phase 2 negotiation failed. This alarm is the result of an outage.</p> <p>To clear this alarm, complete procedure Clear the GWC320 Phase 2 SA failure alarm.</p>                                                                                                                                                                                                                            |
| <b>GWC320</b><br><i>Critical</i>               | <p>Specific problem:<br/>GWC certificate in set number &lt;x&gt; doesn't match private key -- &lt;GWC_IP_address&gt;</p> <p>Probable cause:<br/>Unexpected Information</p>                                                                                                                                                                                                                               | <p>This alarm may indicate an outage.</p> <p>Contact your next level of support.</p> <p>There are no security logs associated with this specific problem.</p>                                                                                                                                                                                                                                                              |

| Alarm description<br>Alarm ID code<br>Severity                                                                                                                      | Specific problem<br>Probable cause                                                                                                                                                                                          | Action                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>GWC320</b><br><i>Critical</i>                                                                                                                                    | Specific problem:<br>Invalid Subject Alternative Name in GWC certificate set number <x> -- <GWC_IP_address><br>where<br><x> - is the set number of the [IKE certificates] panel<br>Probable cause:<br>unexpectedInformation | This alarm indicates that the Subject Alternative Name in the GWC certificate does not match the provisioned IP address for the GWC certificate. This may indicate a data or communication problem between the GWC and the GWC Manager.<br>Contact your next level of support. |
| Ethernet/IP Errors<br><b>GWC321</b><br><i>Major</i>                                                                                                                 | Specific problem:<br>Auto-negotiation disabled on ethernet link.<br>Probable cause:<br>Configuration or customization error                                                                                                 | Enable the auto-negotiation capability on the Ethernet Routing Switch 8600. If required, see the Ethernet Routing Switch 8600 configuration documentation.                                                                                                                     |
| A subsystem overloaded<br><b>GWC322</b><br><i>Minor</i> - SNMP message rate crossed the Panic Level<br><i>Warning</i> - SNMP message rate crossed the Warning Level | Specific problem:<br>• for major alarms:<br>SNMP message rate exceeded recommended maximum<br>• for warning alarms:<br>SNMP message rate is close to recommended maximums<br>Probable cause:<br>Threshold crossed           | Reduce the SNMP traffic level.                                                                                                                                                                                                                                                 |
| Communication with a gateway is down                                                                                                                                | Specific problem:<br>Gateway failed to respond to heartbeat/audit                                                                                                                                                           | Cleared by restoring communication to the managed gateway. Do this by verifying the availability of the gateway, and comparing                                                                                                                                                 |



| Alarm description<br>Alarm ID code<br>Severity                      | Specific problem<br>Probable cause                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Action                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>GWC501</b><br><i>Major</i>                                       | <p>Probable cause:<br/>The underlying resource is not available.</p> <p>'Gateway' is defined as small gateway<br/>(e.g. Askey/Medatrix line gateway, Arris/Motorola gateway, H.323 gateway with less than 64 endpoints).</p>                                                                                                                                                                                                                                                          | the configuration data at the gateway and the CS 2000 GWC Manager (IP address, protocol/version, etc.).                                                                                                                                                         |
| Data inconsistency between GWCEM and Session Server<br><i>Minor</i> | <p>Specific problem:<br/>Data inconsistency between GWCEM and Session Server</p> <p>Probable cause:<br/>Depends on the condition that caused the alarm.</p> <p>Examples: "Data Audit run but data not fully synchronized", "Setting the Call Agent ID has resulted in data changes, which need to be propagated to the Session Server. Run the CS2KSS EM Data Integrity Audit", "Failed to rollback 'add zone' command from Database", "Failed to rollback 'delete zone' command.</p> | For all cases other than when the Data Audit fails, run the CS2KSS Data Integrity Audit. If the data audit fails, investigate the reason (for example, connection failure, problem with the data on the CS2KSS EM, and so on) and manually correct the problem. |

# 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.

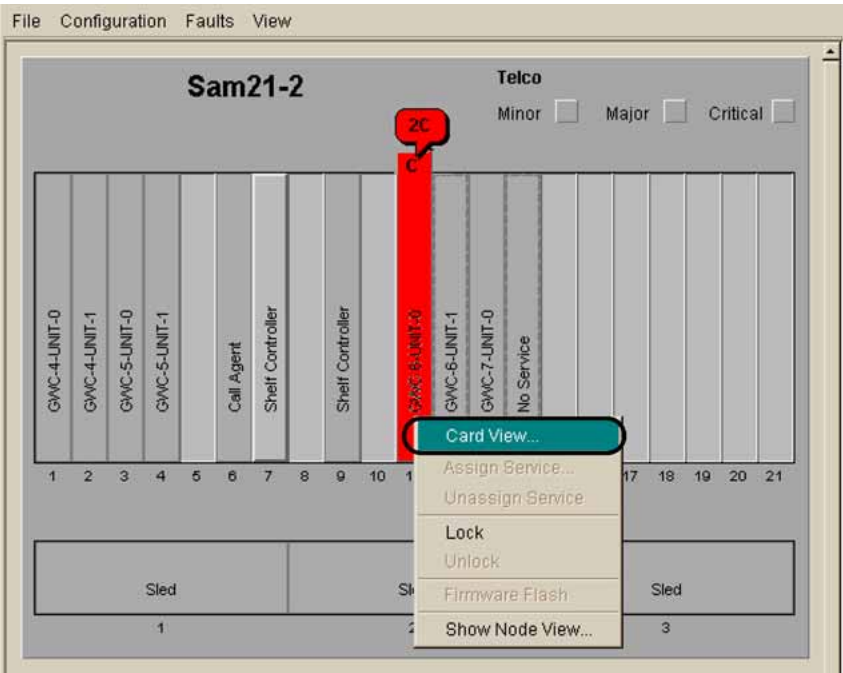
## Prerequisites

This procedure has no prerequisites.

## Action

| Step                                       | Action |
|--------------------------------------------|--------|
| <i>At the CS 2000 SAM21 Manager client</i> |        |

- 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

- For information about various alarms generated by the SAM21 platform, see *SAM21 Shelf Controller Fault Management* (NN10089-911).
- For information about individual alarms related to the NSS cards (including the GWC card) in the SAM21 Shelf, see the CS 2000 Management Tools sections in *Nortel ATM/IP Solution-level Fault Management* (NN10408-900).

In wireless markets, see *Packet MSC Fault Management* (NN-20000-212).

- 3 This procedure is complete.

---

—End—

---

## 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

| Step                                                                                | Action                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b><i>At the CS 2000 Core Manager or Core and Billing Manager (CBM) console</i></b> |                                                                                                                                                                                                                                                                                                                    |
| 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 by typing<br><br><code>#sdmmtc</code><br><br>or<br><br><code>#cbmmtc</code><br><br>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<br><br><code>&gt;appl</code><br><br>and pressing the enter key.<br><br><i>Example system response:</i> |

```

SDM CON 512 NET APPL SYS HW CLLI: 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 Enhanced Terminal Access .
9 OffL 7 SDM Corba Framework .
10 8 Table Access Service .
11 9 OM Access Service .
12 Up 10 Bootpd and tftpd .
13 Down
14 QuerySDM
15 Locate
16

Applications showing: 1 to 10 of 15

```

In SDM, the application "Bootpd and tftpd" is an optional application and may not be installed on your system. In this case it would not be visible in the APPL level menu. In CBM, "Bootpd and tftpd" does not have a presence on the maintenance interface APPL level.

- 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. For information about busying applications and returning them to service, see the CS 2000 Core Manager or Core and Billing Manager (CBM) Security and Administration NTP.

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.  
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.

| Error ID | Reason text                                                                                                                                                                                                                                                                                             |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0500     | TFTP retry time out.<br>The following problems could exist: <ul style="list-style-type: none"> <li>• network has too much traffic</li> <li>• the CS 2000 Core Manager or CBM is busy</li> <li>• the tftp daemon is not running</li> <li>• the load name was entered incorrectly</li> </ul>              |
| 0600     | BOOTP retry time out.<br>The following problems could exist: <ul style="list-style-type: none"> <li>• network has too much traffic</li> <li>• the CS 2000 Core Manager or CBM is busy</li> <li>• the bootp daemon is not running</li> <li>• the /etc/bootptab file is incorrectly configured</li> </ul> |
| 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** You have completed this procedure.

—End—

## View and interpret the operational status of a GWC node

### Purpose of this procedure

Use this procedure to determine the operational status of a selected Gateway Controller (GWC) node using the CS 2000 GWC Manager.

### When to use this procedure

Use this procedure as a primary source of information about the operational status of a GWC card or GWC node.

### Prerequisites or guidelines

This procedure has no prerequisites or guidelines.

### Action

| Step | 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 you wish to view.
- 3 Click the **Maintenance** tab.  
The GUI displays the Maintenance panel with two independent status views, one for each of the GWC cards in the node.

- 4 See table ["CS 2000 GWC Manager status fields"](#) (page 468) following this procedure to interpret the GWC card (unit) status fields.  
If the selected GWC loses communication with the GWC Manager, the client does not provide an accurate status of the GWC node. You can verify the call processing status of a GWC node using the MAPCI interface. If required, follow procedure ["Verify the call processing status of a GWC node"](#) (page 467).
- 5 Repeat this procedure for other cards that you wish to view.
- 6 The procedure is complete.

---

—End—

---

## Verify the call processing status of a GWC node

| Step | Action |
|------|--------|
|------|--------|

### At the MAPCI interface

- 1 Enter the peripheral module maintenance level by typing  
`>MAPCI;MTC;PM`  
and pressing the Enter key.



- 2 Post the desired GWC node in the control position by typing  
`>post GWC <node_number>`  
 and pressing the Enter key.  
 where  
`node_number` is the node number of the GWC that you selected
- 3 The system displays both GWC units and their current states. Verify the current state of the selected GWC node.  
 The GWC node can be in one of the following states:
  - InSv (in service)  
 If one or both units are in an InSv state, the GWC is capable of performing call processing.
  - SysB (system busy) or ManB (manual busy)  
 If both units are in SysB or ManB state, the GWC is not capable of performing call processing.
- 4 Go back to [step 5](#) in the main procedure.

---

—End—

---

The following table describes the GWC card (unit) status fields.

#### CS 2000 GWC Manager status fields

| Status field          | Possible values | Meaning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrative state: | locked          | The unit is prohibited, administratively, from providing service to users.<br><br>A status of "locked" on the CS 2000 GWC Manager indicates that the software application on the card is no longer performing its primary call processing function, but the card is still running. (The call processing function has been "busied", but underlying maintenance and communications activities are still functioning.)<br><br>A status of "locked" on the CS 2000 SAM21 Manager indicates that the hardware is locked to ROM level, and the software application is no longer running. |
|                       | unlocked        | The unit is permitted, administratively, to provide service to users.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Operational state:    | enabled         | The unit is partially or fully providing service to users.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Status field     | Possible values                     | Meaning                                                                                                                                                                                                                                                       |
|------------------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | disabled                            | The unit is not operating or providing service to users. If the Administrative state for this unit is "locked", then the unit has been manually busied. If the Administrative state for this unit is "unlocked", then the unit has been busied by the system. |
| Activity state:  | active                              | The unit is currently providing end user services. This is the state of the node as seen by other network elements.                                                                                                                                           |
|                  | standby                             | The unit is not providing end user services but can be switched to Active at any time if the active (mate) unit fails.                                                                                                                                        |
| Isolation state: | isolated                            | The unit is not communicating with the Core.                                                                                                                                                                                                                  |
|                  | notisolated                         | The unit is communicating with the Core.                                                                                                                                                                                                                      |
| Available state: | offLine(3)                          | The unit has not received its configuration data from the CS 2000 GWC Manager. The unit cannot provide service until it is booted and receives configuration data.                                                                                            |
|                  | degraded(6)                         | The unit does not have heartbeat communication with its mate and it is operating without fault-tolerant redundancy.                                                                                                                                           |
|                  | offLine(3), degraded(6)             | The unit has both: offline and degraded conditions.                                                                                                                                                                                                           |
|                  | 00 00 00 00                         | The unit does not have either of the preceding conditions.                                                                                                                                                                                                    |
| Loadname:        | <string_of_alphanumeric_characters> | This is the name of the load file that the unit currently boots from. The file is located on the CS 2000 Core Manager or Core and Billing Manager (CBM) disk drive.                                                                                           |
| Usage state:     | idle                                | The GWC maintenance system is not currently working on a request, such as a Return to Service (RTS). The unit is available for maintenance requests.                                                                                                          |
|                  | busy                                | Maintenance is in progress on this unit and no further requests are accepted.                                                                                                                                                                                 |
| Stand by state:  | providingService                    | The unit is the active unit and is providing service.                                                                                                                                                                                                         |
|                  | hotStandby                          | The unit is the standby unit - ready to provide service.                                                                                                                                                                                                      |

| Status field | Possible values     | Meaning                                                                                                                                                                                                     |
|--------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | coldStandby         | The unit is synchronizing with the active unit (not providing redundancy). After completion of synchronization, the status changes to hotStandby when the Operational state is enabled.                     |
| Swact state: |                     | This field indicates the last switch of activity for the unit.                                                                                                                                              |
|              | manualSwActWarm     | Last switch of activity was due to a manual warm SwAct. Requested by a user, a warm SwAct causes no service interruption to stable calls, but calls in the setup processes can be lost.                     |
|              | manualSwActCold     | Last switch of activity was due to a manual cold SwAct. Requested by a user, a cold SwAct temporarily takes both units out of service and takes down all calls.                                             |
|              | autonomousSwActWarm | Last switch of activity was due to a system warm SwAct. These SwActs are automatically performed by the device in response to faults or failures. Established calls are preserved. Calls in setup are lost. |
|              | autonomousSwActCold | Last switch of activity was due to a system cold SwAct. These SwActs are automatically performed by the device in response to faults or failures. All calls are lost.                                       |
|              | noSwAct             | No switch of activity has occurred.                                                                                                                                                                         |
| Alarm state: |                     | This field indicates the severity of the currently raised alarms.                                                                                                                                           |
|              | 00 00 00 00         | There are no alarms raised on the GWC card unit.                                                                                                                                                            |
|              | critical(1)         | If present, indicates that one or more critical alarms have been raised.                                                                                                                                    |
|              | major(2)            | If present, indicates that one or more major alarms have been raised.                                                                                                                                       |
|              | minor(3)            | If present, indicates that one or more minor alarms have been raised.                                                                                                                                       |
|              | alarmOutstanding(4) | If present, indicates that at least one or a combination of different alarms has been raised.                                                                                                               |
| Fault state: | none(0)             | This field is not used.                                                                                                                                                                                     |

---

## 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, follow procedure ["Restart GWC card services"](#) (page 474).

### 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 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. Follow procedure "Disable (Busy) GWC card services" in *Gateway Controller Security and Administration* (NN10213-611).

### Action

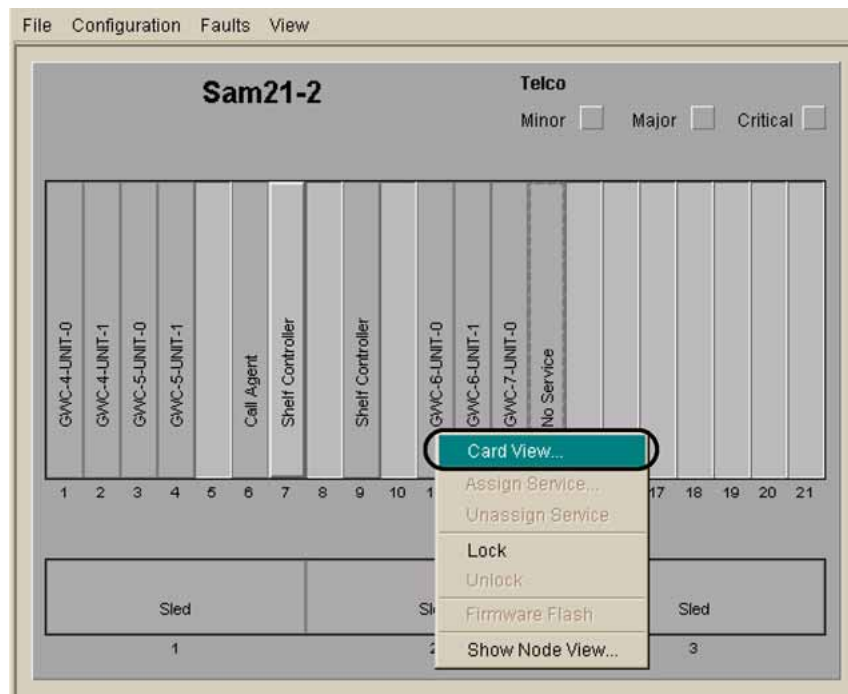
---

| Step | Action |
|------|--------|
|------|--------|

---

*At the CS 2000 SAM21 Manager client*

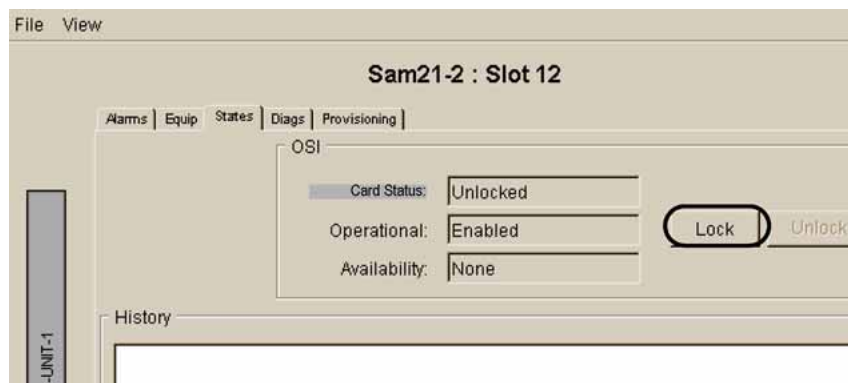
- |   |                                                                                                                     |
|---|---------------------------------------------------------------------------------------------------------------------|
| 1 | From the Shelf View, right-click the GWC card you want to reboot and select <b>Card View</b> from the context menu. |
|---|---------------------------------------------------------------------------------------------------------------------|



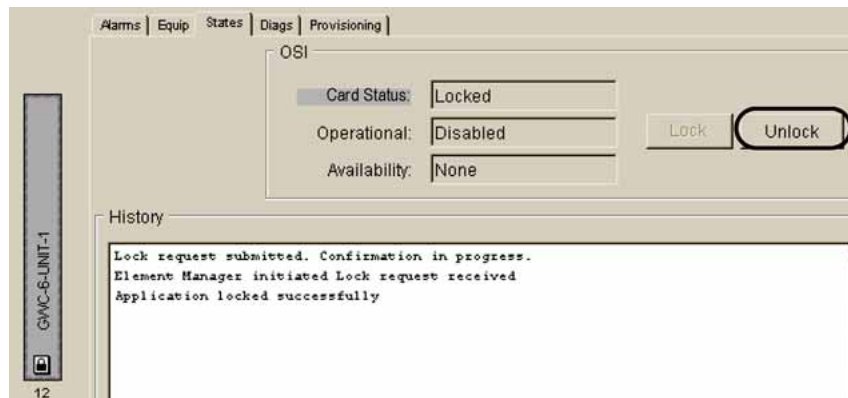
2 At the Card View, select the **States** tab.

3 Click the **Lock** button to lock the card.

The card must be busy (disabled) before you can lock it. If required, see procedure "Disable (Busy) GWC card services" in *Gateway Controller Security and Administration* (NN10213-611).



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.

---

—End—

---

## Restart GWC card services

### Purpose of this procedure

Use this procedure to stop and restart call processing and network services on a standby GWC card.

To restart the hardware and software on an individual GWC card, follow procedure "[Restart or reboot a GWC card](#)" (page 471).

### When to use this procedure

Use this procedure on a GWC card to determine if a known fault is temporary or persistent and if the fault is limited to the GWC card in question.

### Prerequisites

To reduce the risk of service interruption, ensure that the card you are about to restart is in standby status. Otherwise, perform a call processing switch activity (SWACT) to change the card state from active to standby. If required, see procedure "Invoke a manual protection switch (warm SWACT)" in *Gateway Controller Security and Administration* (NN10213-611).

### Action

| Step | Action |
|------|--------|
|------|--------|

*At the CS 2000 GWC Manager client*

- |   |                                                                                                                                                    |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | At the main 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: Gateway Controller frame, select the appropriate GWC node you wish to restart.                                               |
| 3 | Click the <b>Maintenance</b> tab.                                                                                                                  |
| 4 | Locate the Activity State field for the GWC unit and determine which unit (card) is active (either unit 0 or unit 1) and which is in standby mode. |
| 5 | Click the <b>Busy (Disable)</b> button for the GWC unit on standby.                                                                                |

Maintenance | Provisioning

GWC-7-UNIT-0

|                       |                |                 |                |
|-----------------------|----------------|-----------------|----------------|
| Administrative state: | unlocked(1)    | Usage state:    | idle(1)        |
| Operational state:    | enabled(1)     | Stand by state: | coldStandby(2) |
| 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:             | GI070BN        |                 |                |

Save Image Busy (Disable) RTS (Enable) Card View

GWC-7-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:    | 00 00 00 00         |
| Available state:      | 00 00 00 00    | Fault state:    | none(0)             |
| Loadname:             | GI070BN        |                 |                     |

Save Image Busy (Disable) RTS (Enable) Card View

☐ Force Warm Swact Cold Swact

- 6 At the confirmation box, click **OK** to busy the standby GWC unit. Wait for the CS 2000 GWC Manager screen to update the Operational state of the card to disabled(2). This indicates that the card has been busied
- 7 Click the **RTS (Enable)** button to return the card to service.

GWC-7-UNIT-0

|                       |                |                 |                               |
|-----------------------|----------------|-----------------|-------------------------------|
| Administrative state: | locked(2) ←    | Usage state:    | idle(1)                       |
| Operational state:    | disabled(2) ←  | Stand by state: | coldStandby(2)                |
| Activity state:       | standby(2)     | Swact state:    | noSwAct(0)                    |
| Isolation state:      | notisolated(2) | Alarm state:    | minor(3), alarmOutstanding(4) |
| Available state:      | 00 00 00 00    | Fault state:    | none(0)                       |
| Loadname:             | GI070BN        |                 |                               |

Save Image Busy (Disable) RTS (Enable) Card View

GWC-7-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:    | 00 00 00 00         |
| Available state:      | 00 00 00 00    | Fault state:    | none(0)             |
| Loadname:             | GI070BN        |                 |                     |

☐ Force Warm Swact Cold Swact

After 30 seconds, the Administrative state field changes to unlocked and the Operational state field changes to enabled.



|                       |              |
|-----------------------|--------------|
| Administrative state: | unlocked (1) |
| Operational state:    | enabled (1)  |
| Activity state:       | standby (2)  |

The state change is automatic. However, if necessary, you can refresh the screen. At the top of the CS 2000 GWC Manager screen, click the **Windows** menu and select **Refresh GWC Status**.



8 This procedure is complete.

---

—End—

---

## 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.

For specific information about the logs, and any actions required, see the PM log descriptions in *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909).

### 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

| Step                                                                                                                                                                                                                                                                                                | Action                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>At the MAPCI interface</b>                                                                                                                                                                                                                                                                       |                                                                                                                 |
| 1                                                                                                                                                                                                                                                                                                   | Type <b>logutil</b> and press <b>Enter</b> .                                                                    |
| 2                                                                                                                                                                                                                                                                                                   | Type <b>open pm</b> and press <b>Enter</b> to retrieve the latest PM log.                                       |
| <pre> CI: &gt;logutil Current MODE setting is: EXTENDED  LOGUTIL: &gt;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. &gt; </pre> |                                                                                                                 |
| 3                                                                                                                                                                                                                                                                                                   | For more information about commands available in logutil, type <b>print logutildir</b> and press <b>Enter</b> . |
| 4                                                                                                                                                                                                                                                                                                   | This procedure is complete.                                                                                     |



For information about PM logs related to GWC activities, see the appropriate PM log description in the *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909).

---

—End—

---

---

## 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 Gateway Controller (GWC) Manager database.

The audit compares the GWC Manager database with the CS 2000 Core or the Session Server Manager database, or both and flags any mismatches between the databases. The 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.

You can also use this tool to schedule a CS 2000 data integrity audit. For instructions, see procedure "Configure a recurring data integrity audit" in *Gateway Controller Configuration Management* (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.

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 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.

If your network configuration includes a Session Server for SIP Lines functionality, the audit can also compare the IP-VPN(NAT) network zones configuration data in the GWC Manager and the Session Server Manager databases. This data must be consistent to allow the insertion of Media Proxies for SIP lines. For information about the Session Server Lines virtual gateway, see procedure "Associate a Session Server virtual gateway for SIP Lines" in *Gateway Controller Configuration Management* (NN10205-511).

For the Session Server Lines configuration information, see *Session Server Lines Fundamentals* (NN10437-111).

## When to use this procedure

Use this procedure when you are receiving logs or alarms in the CS 2000 Core or at the CS 2000 SAM21 Manager client indicating a possible provisioning errors or data inconsistencies.

When the audit is running, suitable locks are in place that disable provisioning operations.

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.

### ATTENTION

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 and guidelines

The following guidelines apply to this procedure:

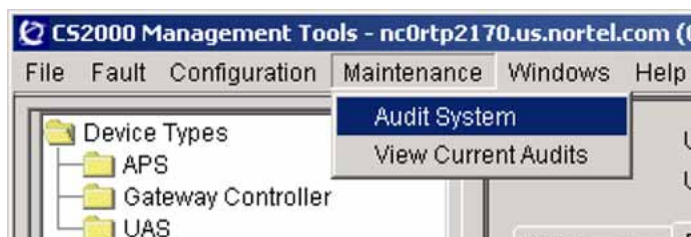
- Ensure that no provisioning activities are scheduled to take place during the audit.
- Unlike the line and trunk audits, the CS 2000 data integrity audit does not provide an option to save the audit report to a file on the local disk.
- You can access and view audit reports only on the GWC unit that was active during the audit. If a switch of activity (SWACT) occurs after the audit, the new active unit will not display any reports. To access audit reports, you need to run the audit again or perform another SWACT.

## Action

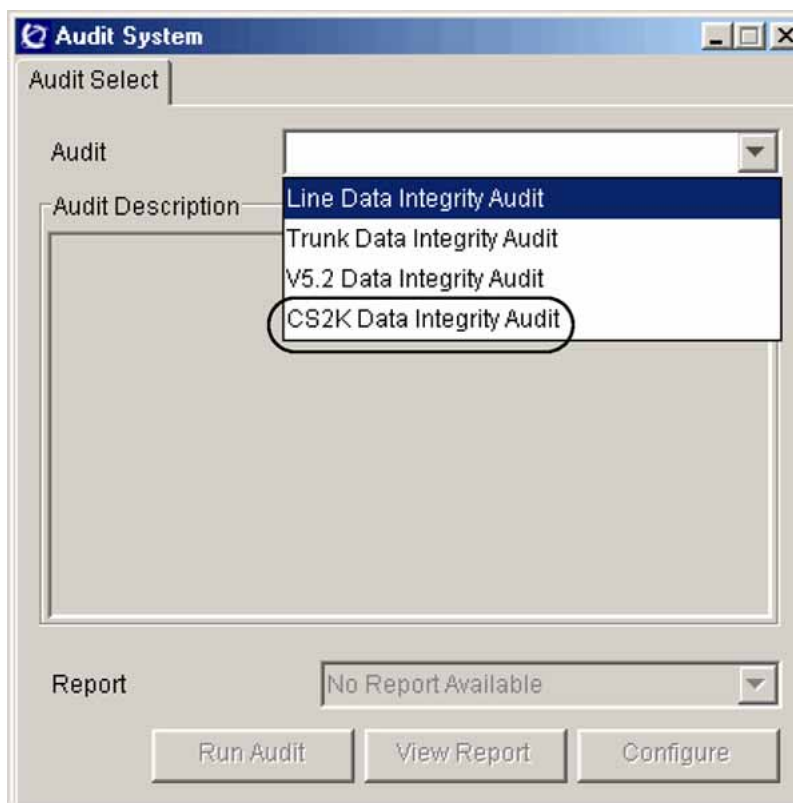
| Step | Action |
|------|--------|
|------|--------|

### *At the CS 2000 GWC Manager client*

- |   |                                                                                                |
|---|------------------------------------------------------------------------------------------------|
| 1 | At the CS 2000 Management Tools window, select <b>Maintenance</b> , then <b>Audit System</b> . |
|---|------------------------------------------------------------------------------------------------|



- 2 At the Audit System dialog box, select **CS2K Data Integrity Audit** from the list of audits displayed in the drop-down menu.



- 3 Use the following table to determine your next step.

| If you want to                                                              | Do                           |
|-----------------------------------------------------------------------------|------------------------------|
| perform an on-demand CS 2000 audit, then view the results of the audit      | go to <a href="#">step 4</a> |
| view the results of an audit that has finished running and resolve problems | go to <a href="#">step 8</a> |

- 4 At the Audit System dialog box, click the **Run Audit** button to display the CS2K Data Integrity Audit Configuration dialog box.

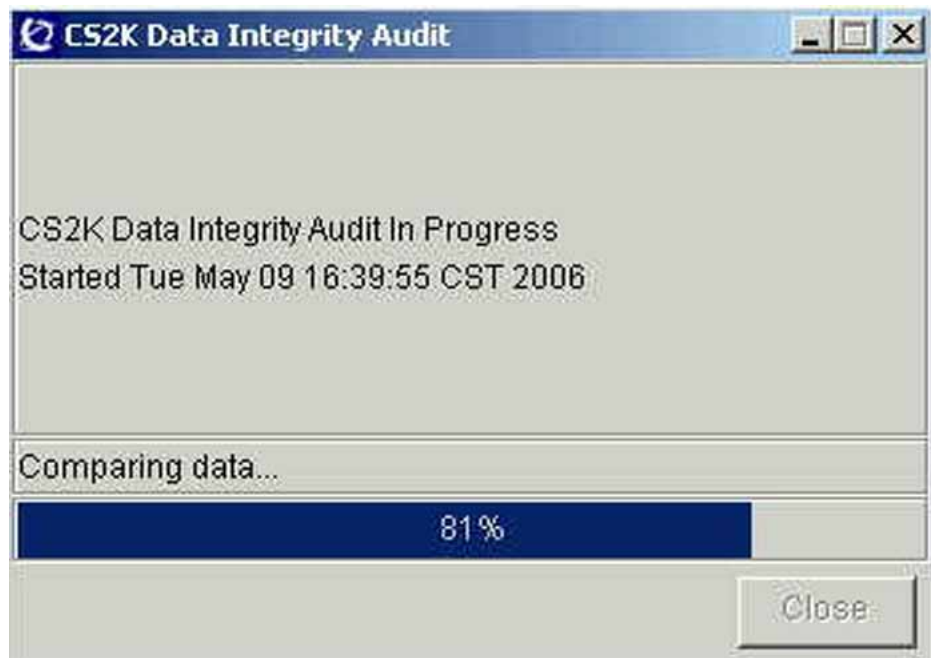


- 5 Select the CS 2000 component that you wish to audit:
- Select the CS2KSS EM Data Integrity Audit check box - if you wish to verify that the network zones configuration data in the GWC Manager and the Session Server Manager databases match.
  - Select the CS2K Call Server Data Integrity Audit check box - if you wish to verify that the data held by the GWC Manager database and the CS 2000 Call Server Core match.
  - Select both check boxes - if you wish to audit both components.
- If there is no Session Server Manager configured on the CS 2000, the CS2KSS EM Data Integrity Audit check box is disabled.

- 6 Click the **Run Audit** button to start the audit.

If you wish to cancel the process, click the **Close** button.

During a CS 2000 audit, the system displays the following message:



The audit may take a few minutes to complete. When the audit ends successfully, the system displays the following message:



If the audit does not execute successfully, the system displays the message "CS2K Data Integrity Audit Failed to Complete", with an error message indicating the reason. Contact your next level of support to resolve the problem.

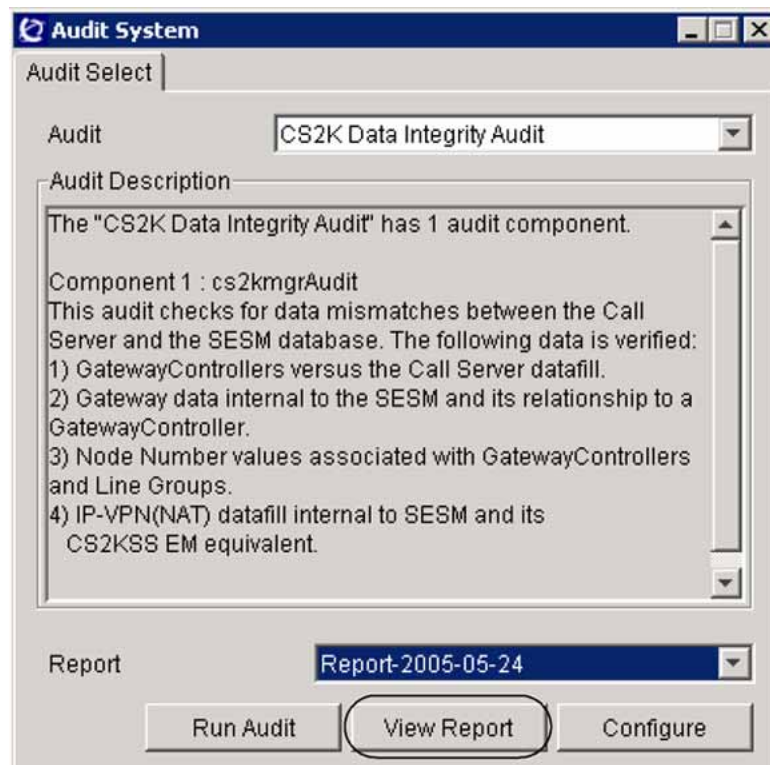
- 7 Click the **Close** button to close the Audit Status window.
- 8 To view a CS 2000 audit report, complete the following sub-steps.

#### **ATTENTION**

You can view the audit reports only on the GWC unit that was active during the audit. If a switch of activity (SWACT) occurred after the audit, the new active unit will not display any reports. To access audit reports, you need to run the audit again or perform another SWACT.

- a. Ensure that you have the **CS2K Data Integrity Audit** option selected from the Audit field drop-down menu at the top of the Audit System dialog box.





- b. From the drop-down menu in the Report field at the bottom of the dialog box, select the report that you want to view.

The file name has the following format:

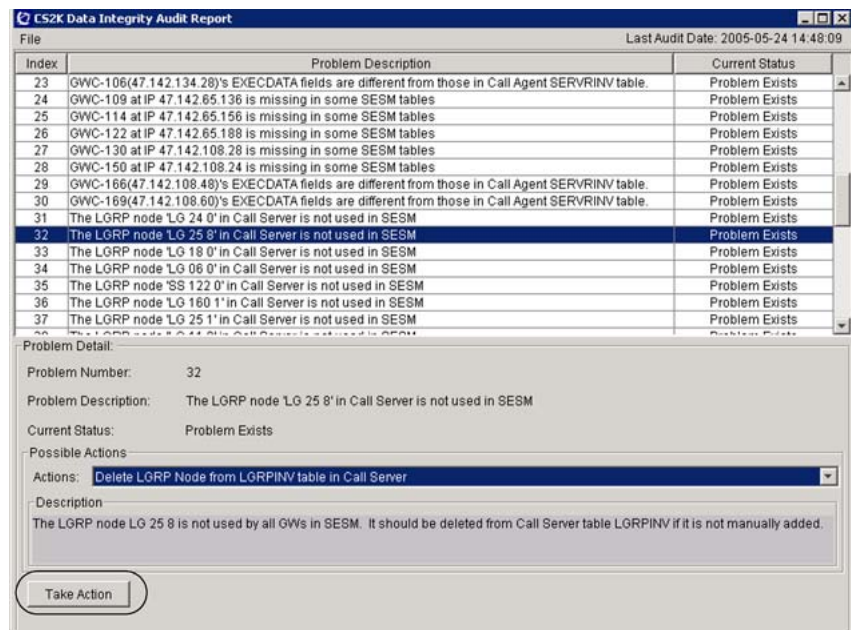
Report-<date>

where

<date> is the date in yyyy-mm-dd format, for example, 2005-05-24.

- c. Click the **View Report** button.

The system displays the selected report. If no problems were discovered, the report is empty. The following example of a report lists various problems.



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.

The system places the audit report in the following directory on the CS 2000 Management Tools server:  
/opt/nortel/ptm/current/MI2/apps/Audit.

The CS 2000 GWC Manager does not provide an option to save a CS 2000 data audit report to local disk.

The CS2KSS EM Data Integrity Audit attempts to automatically correct all data mismatches found. The problems listed in the report are typically corrected and are displayed for information only. If any mismatch correction fails, manual action may be required or the system re-attempts the audit, or both.

- 9 Review the results of the audit and select a problem to resolve.  
If necessary, resize the entire window to completely view the Problem Description field.
- 10 Click the Actions: field and from the drop-down menu, select an appropriate action.
- 11 Read the description of the action and ensure that you observe any recommended steps or cautions.
- 12 Click the **Take Action** button.

If you see the message *Correction Failed*, contact your next level of support.

**13** Return to [step 9](#) if you wish to review another problem.

**14** You have completed this procedure.

---

—End—

---

## 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 about the GWC.

For a list of GWC syslog logs, see section ["Syslog files relevant to the GWC" \(page 490\)](#).

This procedure describes how to access syslog files by logging into the CS 2000 Management Tools server using telnet or ssh. You can also access syslog files using the Integrated Element Management System (IEMS) GUI. If required, see the IEMS procedure "Viewing audit and security logs".

### When to use this procedure

Use this procedure as a part of scheduled maintenance and as a secondary source of diagnostic information.

### Prerequisites

You need the root user ID and password to log in to the CS 2000 Management Tools server.

### Action

| Step                       | Action                                                                                                                                                                                                 |          |    |                   |                              |              |                              |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----|-------------------|------------------------------|--------------|------------------------------|
| <i>At your workstation</i> |                                                                                                                                                                                                        |          |    |                   |                              |              |                              |
| 1                          | Establish a login session to the CS 2000 Management Tools server using one of the following methods:                                                                                                   |          |    |                   |                              |              |                              |
|                            | <table> <tr> <th>If using</th><th>Do</th></tr> <tr> <td>telnet (unsecure)</td><td>go to <a href="#">step 2</a></td></tr> <tr> <td>ssh (secure)</td><td>go to <a href="#">step 3</a></td></tr> </table> | If using | Do | telnet (unsecure) | go to <a href="#">step 2</a> | ssh (secure) | go to <a href="#">step 3</a> |
| If using                   | Do                                                                                                                                                                                                     |          |    |                   |                              |              |                              |
| telnet (unsecure)          | go to <a href="#">step 2</a>                                                                                                                                                                           |          |    |                   |                              |              |                              |
| ssh (secure)               | go to <a href="#">step 3</a>                                                                                                                                                                           |          |    |                   |                              |              |                              |
| 2                          | Complete the following sub-steps to log in using telnet.                                                                                                                                               |          |    |                   |                              |              |                              |
|                            | a. Log in to the server by typing<br><code>&gt; telnet &lt;server&gt;</code><br>and pressing the Enter key.<br>where                                                                                   |          |    |                   |                              |              |                              |

**server** is the hostname or IP address of the server

b. When prompted, enter you 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.

Continue with [step 4](#).

**3** Complete the following sub-steps to log in using ssh (secure).

Use the following command only if your workstation platform supports ssh. Otherwise, the command fails.

a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

**server** is the hostname or IP address of the server

b. When prompted, enter the root password.

#### ***At the CS 2000 Management Tools client***

**4** Access the directory level where the syslog files reside by typing

```
$ cd /var/log
```

and pressing the enter key.

**5** 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.

**6** If the file that you want to view is zipped (has an extention .gz), unzip it using the following command. Otherwise, go to the next step.

Unzip the file by typing

```
$ gunzip <log_filename.gz>
```

and pressing the enter key.

where

`log_filename.gz` is the name of the log file you want to unzip

**Example**

```
$ gunzip securitylog.1.gz
```

The file changes to a readable file securitylog.1.

- 7 Use the following table to determine your next step.

| If you want to view              | Do                            |
|----------------------------------|-------------------------------|
| the entire content of a log file | go to <a href="#">step 8</a>  |
| specific content of a log file   | go to <a href="#">step 10</a> |

- 8 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.  
For specific examples, see table "[Syslog logs containing GWC entries](#)" (page 490).

**Example**

```
$ cat customerlog.0 |more
```

Press the space bar to scroll through the file if it is larger than the screen can display.

- 9 Continue with [step 11](#).

- 10 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
```

- 11 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.

12 This procedure is complete.

---

—End—

---

## 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<br>auditlog.0<br>auditlog.1          |
| Customer log | Records all alarms the system has received.                                                                                                 | customerlog<br>customerlog.0<br>customerlog.1 |
| Debug log    | Records debug information for CS 2000 Management Tools network components to help detect an underlying problem.                             | debuglog<br>debuglog.0                        |
| PTM log      | Contains a record of all the SNMP traps received by the system.                                                                             | ptmlog<br>ptmlog.1<br>ptmlog.2                |
| Security log | Records failed actions taken by users on the system. Securitylog file also includes fault-related logs for Kerberos and IKE/IPSec security. | securitylog<br>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<br>Count: x<br>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 required |



## 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                                         |
|---------------------------------------------------|
| Logging in to the CS 2000 Core Manager            |
| Displaying information about a user or role group |

### Application



#### **DANGER**

#### **Increasing the size of a logical volume can limit future software upgrade capability**

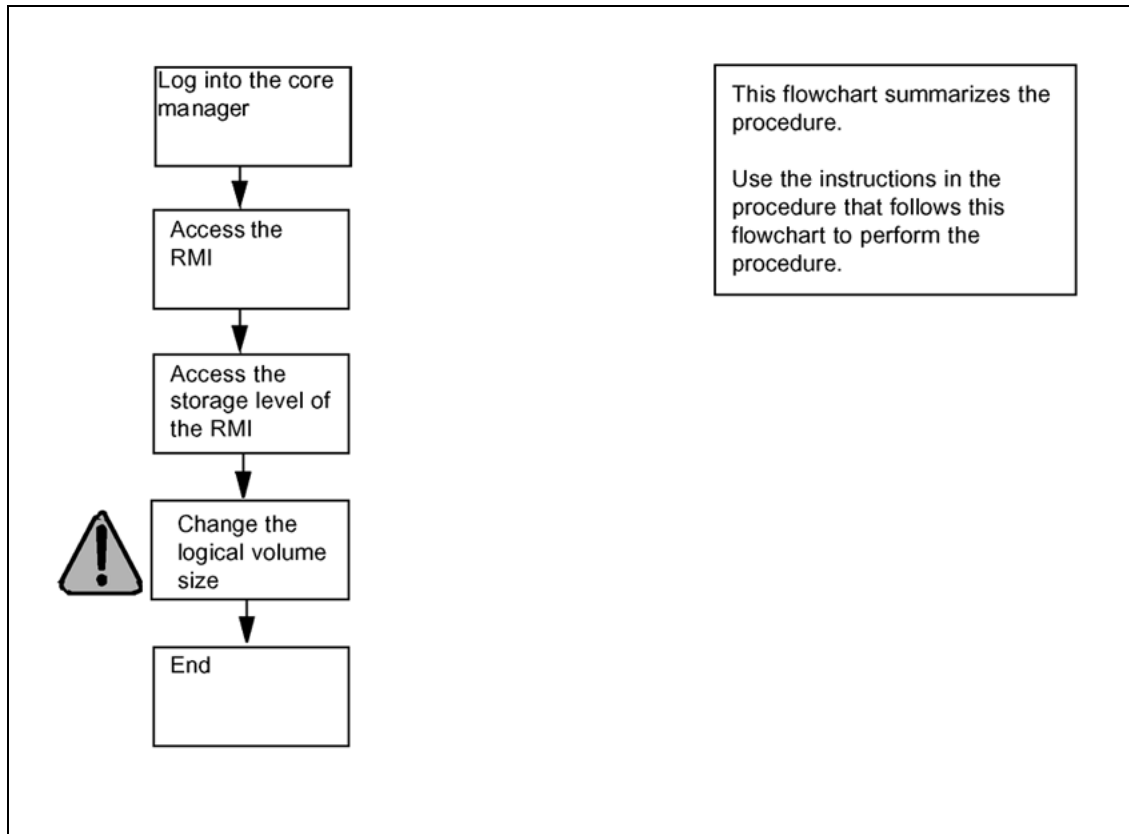
core manager logical volumes are pre-engineered to sizes that are adequate for Nortel customers. Do not increase the size of a logical volume unless absolutely necessary.

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

| Step | Action |
|------|--------|
|------|--------|

**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 /
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 6  |
| not enough disk space | step 10 |

- 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.

---

—End—

---

---

## Replacing an I/O module in an ERS 8600 in a carrier CS-LAN

---

The following procedure provides the steps you need to replace an I/O module in an Ethernet Routing Switch (ERS) 8600 that supports the Communication Server LAN (CS-LAN). When applicable, a reference that contains the detailed steps is provided.

In a CS-LAN environment most devices are cabled across two ERS 8600s. In some instances, it may be required to groom the traffic off of the I/O module to another I/O module located within the same chassis or on the alternate ERS 8600.

The following document is referenced in this procedure: *Installing Ethernet Routing Switch 8600 Modules (312749-K)*.

### Prerequisites

Ensure you have a replacement I/O module.

Make sure you use READ/WRITE/ALL (RWA) login privileges, password privileges or both when performing this procedure. For more information about RWA privileges, refer to Passport Documentation in the Nortel website.

Access the ERS 8600s using the serial (console) port. You can use a direct serial connection and a terminal program from an attached PC or a TELNET connection to an appropriately configured IP address on a terminal server connected to the console port.

### Task list

Complete each task in the following list to replace an I/O module in an ERS 8600.

1. Verify that console access is available to the ERS 8600 switch where the I/O module is being replaced. This is to ensure that out-of-band access to the switch is available in the event that in-band access is lost when the module is removed.
2. If using a Compact Call Agent (CCA) Core, ensure there are no alarms on the call agent.
3. Save the original boot and runtime configuration files to flash memory and copy to pcmcia using the following commands. Enter **y** when prompted.

```
save config backup /pcmcia/config.cfg
```

```
save bootconfig backup /pcmcia/boot.cfg
```

4. Identify the devices connected to the I/O module being replaced and what equipment is being hosted by each of the ports, see procedure ["Identifying the devices connected to the I/O module being replaced"](#) (page 499).
5. If using a CCA Core, ensure that the active call agent subtends to the ERS 8600 switch that does not contain the I/O module being replaced, and the inactive call agent subtends to the ERS 8600 switch that does contain the I/O module being replaced.
6. If any of the following devices are connected to the I/O module being replaced, ensure that it has a unit subtending to the other ERS 8600 switch:
  - Border Control Point (BCP) 7100
  - Media Gateway (MG) 7000 or MG 15000

**Note:** Only if the I/O card is an 8672

  - Gateway Controller (GWC)
  - High performance Input/Output Processor (HIOP)
  - USP/USP Compact
  - STORM-IA
  - Shelf Controller (SC)
7. Select the next step as follows:

| If any of the following devices are connected to the I/O module being replaced | Do                                                                                      |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| BCP 7100                                                                       | "Shutting down the Border Control Point 7100 connected to chassis X" (page 500)         |
| MG 7000 or MG 15000                                                            | "Offloading PVG traffic from the ERS 8600" (page 502)                                   |
| <b>Note:</b> Only if the I/O card is an 8672                                   |                                                                                         |
| GWC                                                                            | "Disabling GWCs that subtend the slave Ethernet Routing Switch 8600" (page 512)         |
| HIOP                                                                           | "Disabling the Ethernet links between an XA-Core and HIOPs and the ERS 8600" (page 516) |

| If any of the following devices are connected to the I/O module being replaced | Do                                                                                   |
|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| USP Compact                                                                    | "Locking the USP-Compact" (page 517)                                                 |
| USP                                                                            | "Taking down the paths to the ERS 8600 chassis X" (page 524)                         |
| STORM-IA                                                                       | "Determining if STORM devices require rotating, demounting and busying" (page 526)   |
| SC                                                                             | "Locking the inactive Shelf Controller (SC) blade connected to chassis X" (page 530) |

8. Ensure all cables are properly labeled.
9. Busy all ports on the I/O module being replaced using the following command:  

```
config ether x/y-x/z state disable
```
10. Replace the I/O module using procedure "Installing and replacing a module" in the document *Installing Ethernet Routing Switch 8600 Modules* (312749-K).
11. Enable all the ports on the replacement I/O module using the following command:  

```
config ether x/y-x/z state enable
```
12. Clear port stats and ensure there are no errors on the new module using the following commands:  

```
clear ports stats
```

Wait five minutes, then enter the following:  

```
show ports error show-all
```

If errors are encountered, check that cables are properly plugged in. If you still encounter errors, contact technical support.

13. Select the next step as follows:

| If any of the following devices were connected to the module replaced | Do                                                                            |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------|
| BCP 7100                                                              | "Unlocking the Border Control Point 7100" (page 534)                          |
| SC                                                                    | "Unlocking the inactive SC" (page 536)                                        |
| USP Compact                                                           | "Unlocking the USP-Compact" (page 536)                                        |
| USP                                                                   | "Returning the paths to the ERS 8600 chassis X to service" (page 543)         |
| HIOP                                                                  | "Enabling the Ethernet links between the XA-Core and the ERS 8600" (page 543) |

14. Verify that existing functionality is working properly. If you encounter any problems, contact technical support.

## Procedures

The procedures that follow are the detailed procedures referenced in the task list. Refer to the ["Task list" \(page 496\)](#), which provides the task sequence to replace an I/O module in an ERS 8600.

### Identifying the devices connected to the I/O module being replaced

| Step                      | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>At the workstation</i> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>1</b>                  | <p>Enter the following command to identify connections to the I/O module being replaced:</p> <pre>show port info name</pre> <p>In the following sample output, it is clear that this I/O module has connections to the following devices: CS 2000 management tools, CBM, USP, MDM, SDM, MG 3500 EM server, MG 9000 EM server, XA-Core HIOP, SSLM, and SSLI.</p> <p>This module also has two GBIC ports. Port 1/33 as an MLT port and port 1/34 is used to connect to ERS-03</p> |



| Port Name |                                  |             |        |       |       |        |
|-----------|----------------------------------|-------------|--------|-------|-------|--------|
| PORT      | OPERATE OPERATE OPERATE          |             |        |       |       |        |
| NUM       | NAME                             | DESCRIPTION | STATUS | DUPLX | SPEED | VLAN   |
| 1/1       | CS2000 Mgmt Tools                | 100BaseTX   | up     | full  | 100   | Access |
| 1/2       | Reserved for CBM                 | 100BaseTX   | down   | half  | 0     | Access |
| 1/3       | 15 / 0 USP (RTC_15)              | 100BaseTX   | up     | full  | 100   | Access |
| 1/4       | MDM_1                            | 100BaseTX   | up     | full  | 100   | Access |
| 1/5       | Rear 13 / 0 SDM (13R)            | 100BaseTX   | down   | full  | 0     | Access |
| 1/6       | Reserved for CBM                 | 100BaseTX   | down   | full  | 0     | Access |
| 1/7       | MG3500 EM server #1              | 100BaseTX   | down   | full  | 0     | Access |
| 1/8       | MG9000 EM Server #1              | 100BaseTX   | up     | full  | 100   | Access |
| 1/9       | Rear 14 / 0 XA-Core HIOP (14R)   | 100BaseTX   | up     | full  | 100   | Access |
| 1/10      | Rear 15 / 0 SDM (15R)            | 100BaseTX   | up     | full  | 100   | Access |
| 1/11      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/12      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/13      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/14      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/15      | 14 / 0 USP (IP Link System Card) | 100BaseTX   | up     | full  | 100   | Access |
| 1/16      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/17      | SSLM, unit 0 eth B               | 100BaseTX   | up     | full  | 100   | Access |
| 1/18      | SSLM, unit 1 eth B               | 100BaseTX   | up     | full  | 100   | Access |
| 1/19      | SSLI, unit 0 eth B               | 100BaseTX   | up     | full  | 100   | Access |
| 1/20      | SSLI, unit 1 eth B               | 100BaseTX   | up     | full  | 100   | Access |
| 1/21      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/22      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/23      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/24      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/25      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/26      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/27      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/28      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/29      |                                  | 100BaseTX   | down   | half  | 0     | Access |
| 1/30      | TekServer TA1100                 | 100BaseTX   | up     | full  | 100   | Access |
| 1/31      | ISG2000 Secondary Slot 3 Port 2  | 100BaseTX   | down   | full  | 0     | Access |
| 1/32      | csnettxk1n104 - 5                | 100BaseTX   | up     | half  | 10    | Access |
| 1/33      | ERS8600-00 Slot 1 Port 33        | GbicSx      | up     | full  | 1000  | Tagged |
| 1/34      | ERS8600 03 Slot 1 Port 34        | GbicSx      | up     | full  | 1000  | Access |

---

—End—

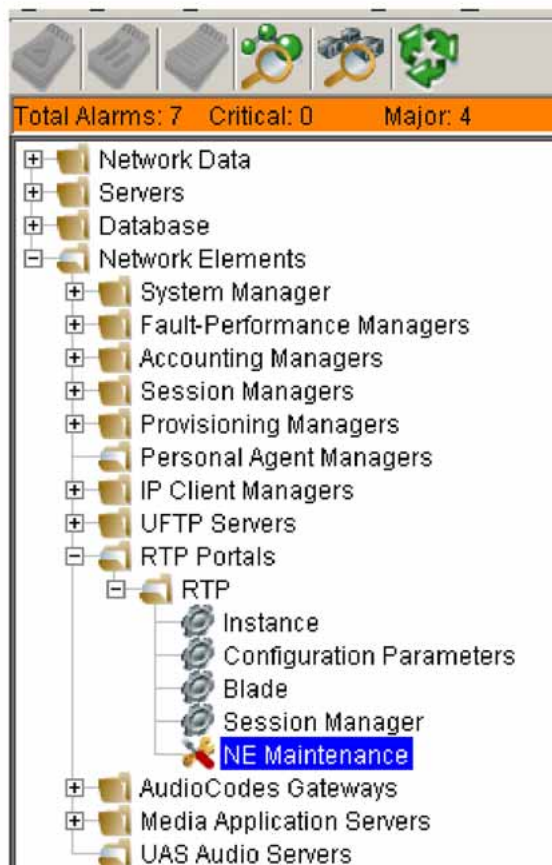
---

## Shutting down the Border Control Point 7100 connected to chassis X

| Step | Action |
|------|--------|
|------|--------|

Where chassis X is the chassis containing the I/O module to be replaced.  
At the System Management Console

- 1 Ensure that direct connectivity has been established according to the instructions in bulletin SEB-08-01-009.
- 2 From the System tree, click the plus sign next to **Network Elements** to expand the view of the folder.

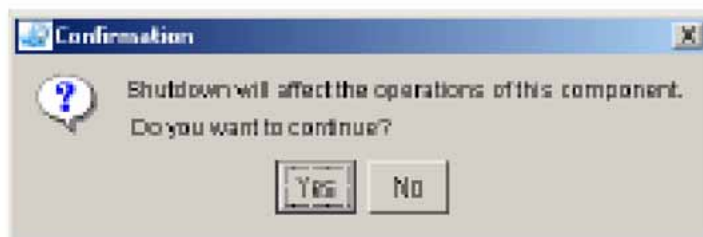
**Expanding BCP 7100 window**

- 3 Next, click the plus sign next to **RTP Portals** to expand the view of the folder. The contents of this folder lists all BCP 7100s and BCP 7200s configured for the site.
- 4 Continue to expand the view of folders until the target BCP 7100 is selected. Do not modify the state of any BCP 7200s.
- 5 Click the **NE Maintenance** option. A new window opens.
- 6 Click the **Stop** button to initiate shut down.

**BCP 7100 shutdown**

The Stop button shuts down the system. The Kill button locks the BCP 7100, and the Restart button stops and starts the system.

- 7 A confirmation window appears. Click **Yes** to continue.

**BCP 7100 shutdown confirmation**

- 8 The BCP 7100 component shuts down gracefully and eventually goes into an inactive state when the last active media session ends (as seen in the General Information Area of the System Management Console).
- 9 You have completed this procedure. Return to ["Task list" \(page 496\)](#) to determine your next task.

---

—End—

---

**Offloading PVG traffic from the ERS 8600****Step Action**

*Use the PVG CLI to determine the PVG IP addresses*

- 1 Check the provisioning information for the VSPs, NSTA, and VGS subcomponents as follows:

- a. Enter the following command to display media and signaling gateway IP addresses.

```
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/\*" portion 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. Enter the following command to display the IPmcon IP address.

```
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" portion 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 ERS 8600 CLI to verify that the PVGs are set up redundantly*

- 2 Enter the following command on each ERS 8600 chassis to check the VLAN configuration file.

```
sho config module vlan
```

This command outputs all VLANs provisioned on the ERS 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
```

**Note:** Both ERS 8600s display the identical PVG VLAN configuration. The "vlan <#> ports add" entry identifies each VSP ATM Sonet connection. This information is required in [step 8](#).

**3** Check the routing table information for each ERS 8600 chassis as follows:

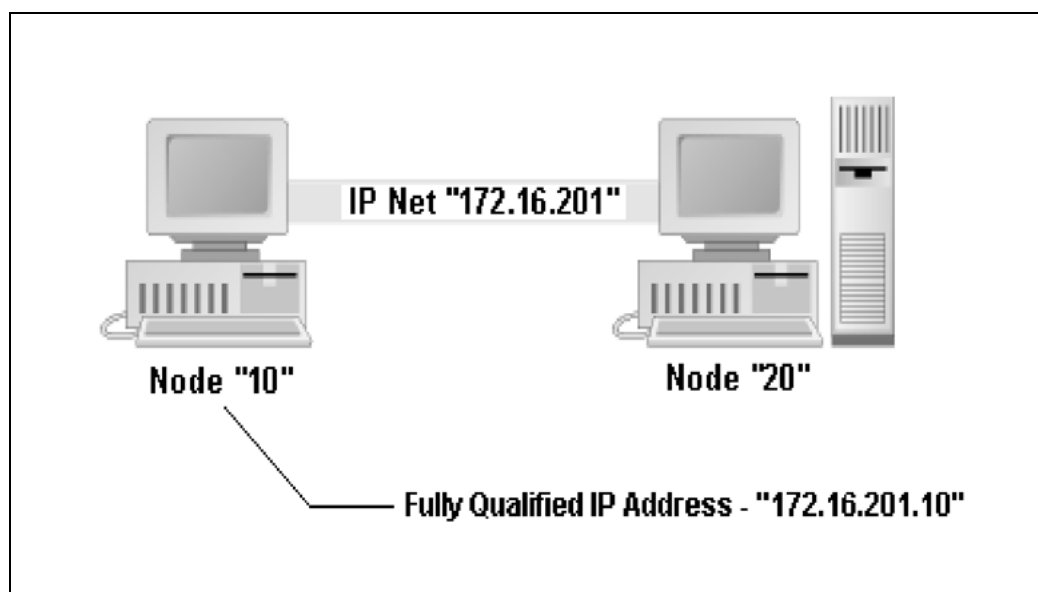
- a. Enter the following command to display IP route information.

```
sho ip route info ip x.y.z
```

where

**x.y.z** specifies the IP Net address provided at [step 1](#)

**Note:** Specifying the x.y.z octets limits the command output to those nodes served by the specified IP Net.



The following list provides an example for the command output for one of the ERS 8600s.

```
=====
Ip Route
=====
DSTMASKNEXTCOSTVLANPORTPROTAGETYPEPEPRF

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.
```

The following list provides an example for the command output for the other ERS 8600 chassis.

```
=====
Ip Route
=====
DSTMASKNEXTCOSTVLANPORTPROTAGETYPEPEPRF

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.
```

**ATTENTION**

The routing information under the PROT column heading must indicate either VSP subnet LOC or OSPF.

If both ERS 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 X (chassis containing module to be replaced) of the ERS 8600 must be OSPF (LOC for chassis Y). See [step 10](#) for details on forcing compliance to this requirement.

- b. Repeat [substep 3a](#) for each VSP VLAN on the ERS 8600 chassis X.

where

**chassis X** is chassis containing module to be replaced.

- c. Repeat [substep 3a](#) and [3b](#) for ERS 8600 chassis Y.

where

**chassis Y** is chassis not containing module to be replaced.

*Use the PVG CLI to verify the correct provisioning of each VSP*

- 4 Check the SPVCAP subcomponent of each VSP VGS Ctrl/<mg.sg> and IPmcon as follows:

- a. Enter the following command to display the provisioning information for each VSP.

```
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. Enter the following command to display IPmcon information.

```
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
```

- 5 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.

- 6 Enter the following command to check the ATMIF UNI addresses provisioned as primary and alternate.

```
1 atmif/* uni addr/*
```

A sample of the command output for the ATMIFs present on the PVG shelf follows.

```
Atmif/141Uni
Addr/45613512123400002F000000010020480D008D00,pri-
mary
```

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 ERS 8600s*

- 7 Determine which ATMIF the VSP VGS Ctrl/<mg,sg> and IPmcon ATMCON subcomponents point to as follows:

- a. Enter the following command to display the VGS Ctrl/<mg,sg> ATMCON subcomponent for all VSPs.

```
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 6](#). If they do not match, contact your next level of support.

- b. Enter the following command to display the NSTA VGS IPmcon ATMCON subcomponent for the VSPs.

```
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 6](#). If they do not match, contact your next level of support.

- 8 Check the physical connections between each PVG ATM interface and their related ERS 8600.

**Note:** See [step 2](#) for the ERS 8600 local route tables for the VSPs to be offloaded and verify the fiber connectivity between the PVGs and ERS 8600s. Refer to your engineering guidelines for additional information.

*Use the PVG CLI to disable the ATM interface to the ERS 8600 undergoing the I/O module replacement*

- 9 Select the next step as follows (refer to [step 3](#)):

| If all VSP VLANs for ERS 8600 chassis X are | Do                      |
|---------------------------------------------|-------------------------|
| OSPF (see Note)                             | <a href="#">step 16</a> |
| Anything except OSPF                        | <a href="#">step 10</a> |

**Note:** OSPF routing does not require manual maintenance to reduce the risk of call processing outage, as the link redundancy on PVGs fails over nearly immediately.

- 10 Disable the ATM interface for each VSP as follows:

- a. Enter the following command to identify the ATM interfaces and Sonet layer.

```
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
applicationFramename = Atmif/141
txPathTrace= ""
expectedReceivePathTrace= ""
concatNumber= 0
customerIdentifier= 0
ifAdminStatus= up
ifIndex= 6
Lp/15 Sonet/1 Sts/0
applicationFramename = Atmif/151
txPathTrace= ""
expectedReceivePathTrace= ""
concatNumber= 0
customerIdentifier= 0
ifAdminStatus= up
ifIndex= 472
```

- b. Enter the following command to lock all Sonet layer connections related to the ATM ports connected to ERS 8600 chassis X.

```
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.

**11** Confirm the ATM (software) connection switchover is successful as follows:

a. Enter the following command to display the VGS Ctrl/<mg,sg>ATMCON subcomponent for the VSPs.

```
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 7](#)) 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. Enter the following command to display the VGS IPmcon ATMCON subcomponent for the VSPs.

```
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 7](#)) to AtmIf/151.

```
+=====+-----+-----+-----+-----+
|Nsta | nextHop |state |Response
+=====+-----+-----+-----+-----+
| 7|AtmIf/151 Vcc/7.10 |connec|
```

Use the ERS 8600 CLI to verify the IP route table for the offloaded VSP VLANs

**12** Enter the following command to display the routing table for both ERS 8600s.

```
sho ip route info ip x.y.z
```

where

**x.y.z** is the IP Net address (see [step 3](#))

**Note:** The routing information under the PROT column heading must indicate OSPF for all VSP VLANs on ERS 8600 chassis X.

- 13 Select the next step as follows:

| If switchover of all VSPs is                     | Do                      |
|--------------------------------------------------|-------------------------|
| incomplete (that is, not all VSPs switched over) | <a href="#">step 10</a> |
| complete (that is, all switched over)            | <a href="#">step 14</a> |

*Use the PVG CLI to re-enable all disabled ATM ports*

- 14 Enter the following command to unlock all Sonet ports locked at [step 10](#).

```
unlock lp/<slot> sonet/<sonetif>
```

where

<slot> is the slot number of the ATMIF blade

<sonetif> is the Sonet interface on the ATM blade

*Use the ERS 8600 CLIs to check the IP route tables*

- 15 Enter the following command to make sure all VSP VLANs remain OSPF on ERS 8600 chassis X, and LOC on ERS 8600 chassis Y.

```
sho ip route info ip 172.16.201
```

The routing information under the PROT column heading must indicate OSPF for all VSP VLANs on ERS 8600 chassis X. If it does not, contact your next level of support.

- 16 You have completed this procedure. Return to ["Task list" \(page 496\)](#) to determine your next task.

---

—End—

---

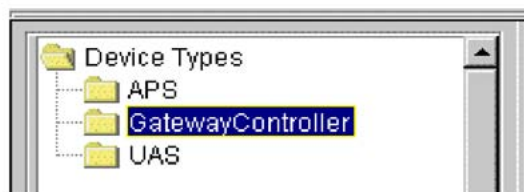
## Disabling GWCs that subtend chassis X

| Step | Action |
|------|--------|
|------|--------|

*Using your web browser*

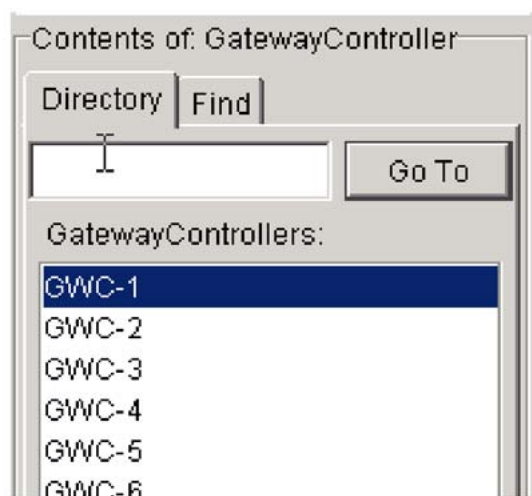
- |   |                                                                                                                                                                                                                      |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Launch CS 2000 Management Tools from your web browser.                                                                                                                                                               |
| 2 | Access the Maintenance information for the GWCs as follows: <ol style="list-style-type: none"> <li>Select <b>GatewayController</b> from the <b>Device Types</b> field of the CS2000 Management Tools GUI.</li> </ol> |

The **GatewayController** folder in the **Device Types** field is highlighted.



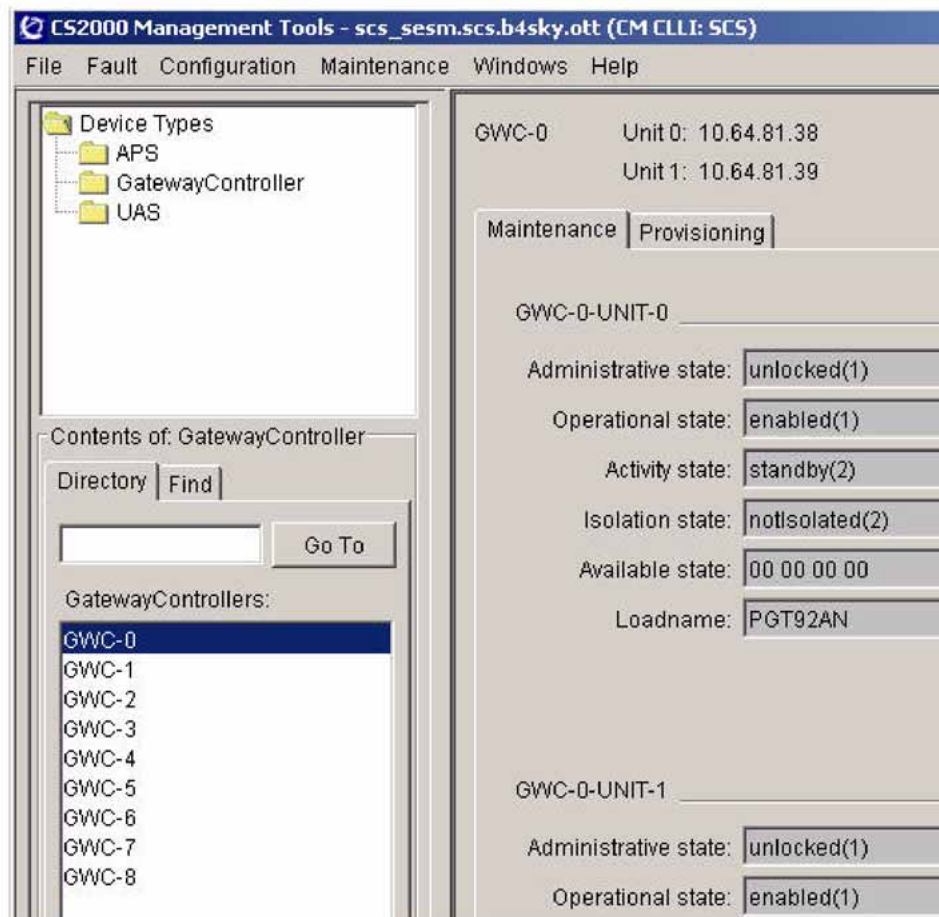
- b. Select the **Directory** tab under **Contents of: Gateway Controller**.

The list of Gateway Controllers (GWC) appears.



- c. Select the first GWC in the list.

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 displayed.

### 3 Make all GWCs inactive on ERS 8600 chassis X.

where

**chassis X** is chassis containing module to be replaced.

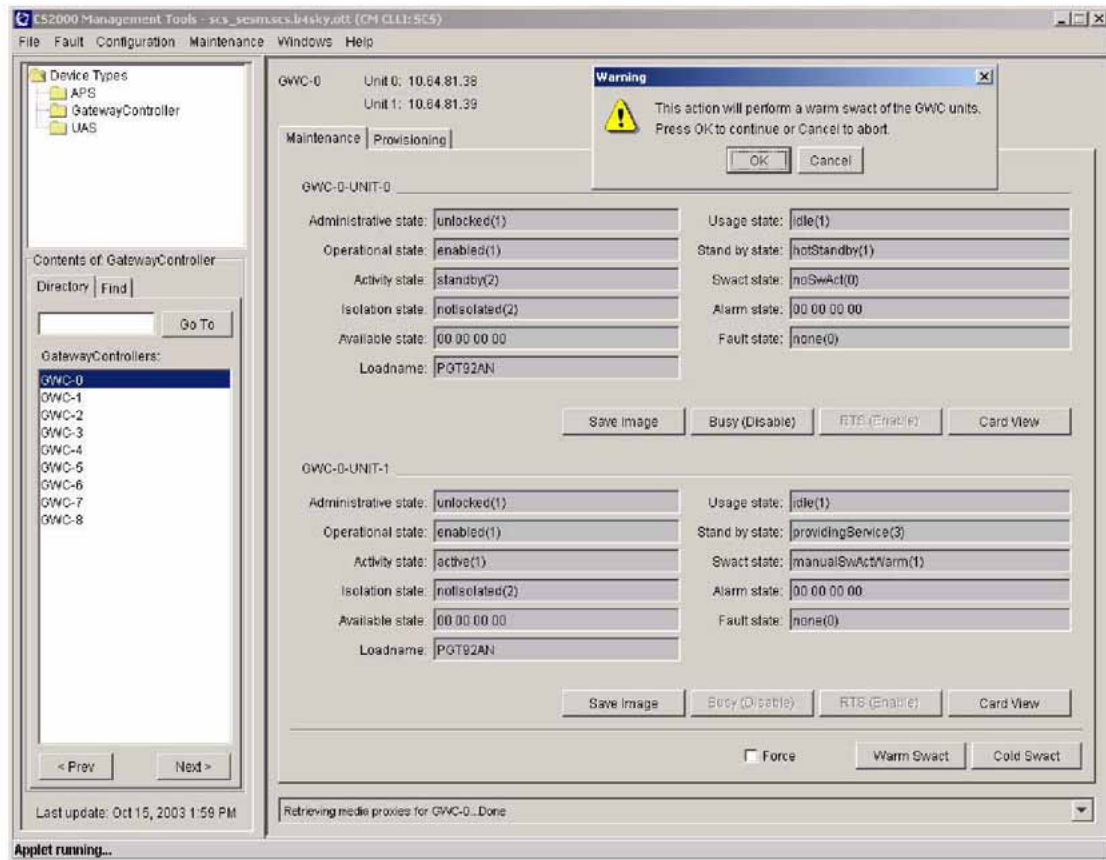
- a. Check the Activity State field for GWC Unit N to determine which unit is active and which is standby

| If the Activity State field is | Do                      |
|--------------------------------|-------------------------|
| active                         | <a href="#">step 3b</a> |
| standby, instead of inactive   | <a href="#">step 3d</a> |

- b. Click **WarmSwact**.

A warning window appears

Click **OK** to continue or **Cancel** to abort.



- c. Click **OK**, and wait for the activity change to complete.

The selected GWC undergoes a change of activity. The change of activity can take approximately 2 minutes.

- d. Select the next GWC in the list, and repeat these substeps until the **Activity State** field for **Unit: N Status is standby** for all GWCs.

- 4 You have completed this procedure. Return to "Task list" (page 496) to determine your next task.

—End—



## Disabling the Ethernet links between an XA-Core and HIOPs and the ERS 8600

| Step | Action |
|------|--------|
|------|--------|

*At the XA-Core MAP terminal*

- 1 Enter the following command to access the ETHR level of the MAP display.

```
>MAPCI;MTC;XAC;ETHR
```

The following is a sample MAP display for the ETHR level.

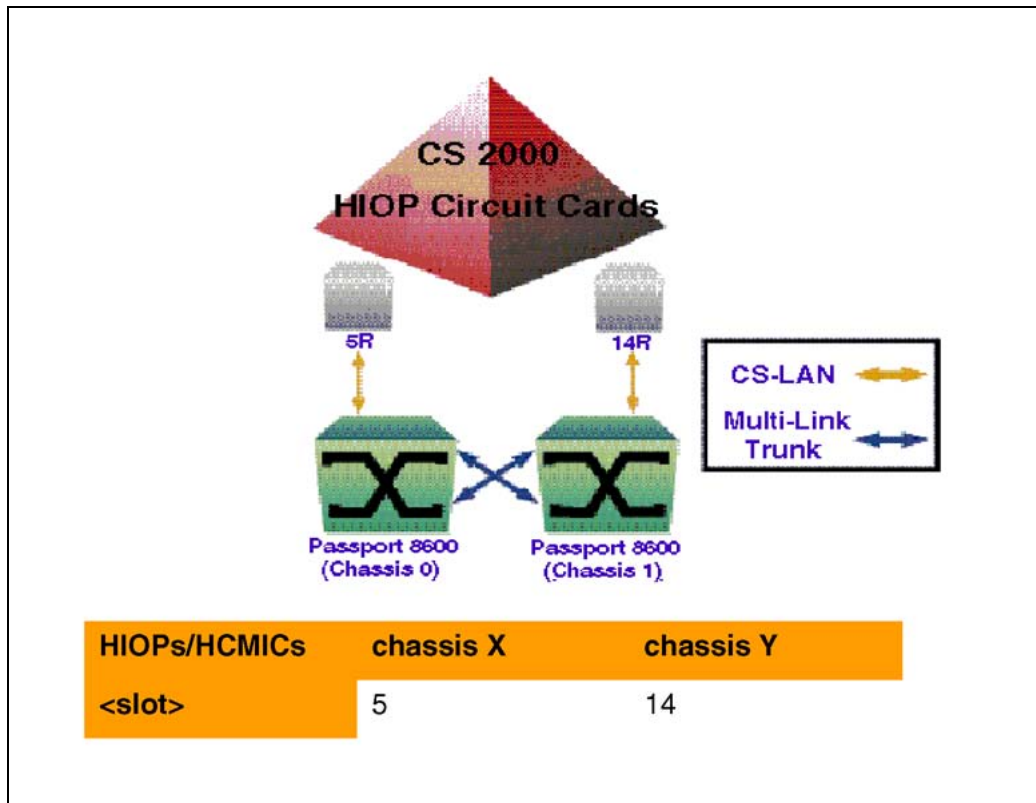
| XAC        | MS | IOD | Net | PM | CCS | Lns | Trks | Ext | APPL |
|------------|----|-----|-----|----|-----|-----|------|-----|------|
| ETHR       |    |     |     |    |     |     |      |     |      |
| 0 Quit     |    |     |     |    |     |     |      |     |      |
| 2          |    |     |     |    |     |     |      |     |      |
| 3          |    |     |     |    |     |     |      |     |      |
| 4          |    |     |     |    |     |     |      |     |      |
| 5          |    |     |     |    |     |     |      |     |      |
| 6 Tst_     |    |     |     |    |     |     |      |     |      |
| 7 Bsy_     |    |     |     |    |     |     |      |     |      |
| 8 RTS_     |    |     |     |    |     |     |      |     |      |
| 9          |    |     |     |    |     |     |      |     |      |
| 10 LoadFW_ |    |     |     |    |     |     |      |     |      |
| 11         |    |     |     |    |     |     |      |     |      |
| 12 Uneq_   |    |     |     |    |     |     |      |     |      |
| 13         |    |     |     |    |     |     |      |     |      |
| 14 Alarm_  |    |     |     |    |     |     |      |     |      |
| 15 Cntrs_  |    |     |     |    |     |     |      |     |      |
| 16         |    |     |     |    |     |     |      |     |      |
| 17 Indic_  |    |     |     |    |     |     |      |     |      |
| 18 Query_  |    |     |     |    |     |     |      |     |      |

- 2 Refer to the figure and table that follow. Enter the following command to disable the XA-Core to ERS 8600 chassis X (chassis containing I/O module to be replaced) Ethernet link.

```
bsy <slot> r link force
```

Accept the state change by typing Y

Executing this command produces an alarm indicating that the port is down. Ignore this alarm.



**Note:** In the previous configuration, one HIOP is connected to each ERS 8600.

- 3 You have completed this procedure. Return to ["Task list" \(page 496\)](#) to determine your next task.

—End—

## Locking the USP-Compact

### Step Action

At the USP Compact (USPc) GUI

#### ATTENTION

Prior to adhering to [step 2](#) to [step 17](#), ensure that the slave USPc blade is being addressed.

Determine the USPc blade-to-ERS 8600 connectivity. The slave USPc blade must connect to ERS 8600 chassis X (chassis containing I/O module to be replaced); master USPc blade to chassis Y (chassis not containing I/O module to be replaced).

**1** Preparing the slave USPc blade for locking consists of the following tasks:

- inhibiting all SS7 links on the slave USPc blade

**Note:** If only one link is available on a linkset, it cannot be inhibited. If there are other links on the linkset, ensure at least one of the links is available before attempting to inhibit the link.

- deactivating all SS7 links on the slave USPc blade
- bringing down all IPS7 paths on the slave USPc blade
- locking the slave USPc blade from the USPc GUI

**Note:** Both USPc blades carry traffic and are in service.

**2** Launch the USPc GUI.

**3** Select **Configuration --> platform --> Node**.

The following window displays.

The screenshot shows the USPc GUI with the following sections:

- Provisioning Data:**
  - slot-type: [dropdown]
  - slot-name: [text field]
  - slot-description: [text field]
  - shelf: [text field]
  - slot: [text field]
  - front-pec: [dropdown]
  - tm-pec: [dropdown]
  - tm-type: [text field]
- Operational Data:**
  - operational-state: [text field]
  - administrative-state: [text field]
  - procedural-state: [text field]
  - availability-state: [text field]
- Boot Data:**
  - status-message: [text field]
  - running-image: [text field]
  - boot-image: [dropdown]

The top toolbar includes buttons for New, Add, Modify, Delete, Lock, Unlock, Load, Offline, Swact, and Restart. The bottom status bar shows "loading complete" and a progress indicator.

**4** Select the **Search** tab and click **Retrieve**.

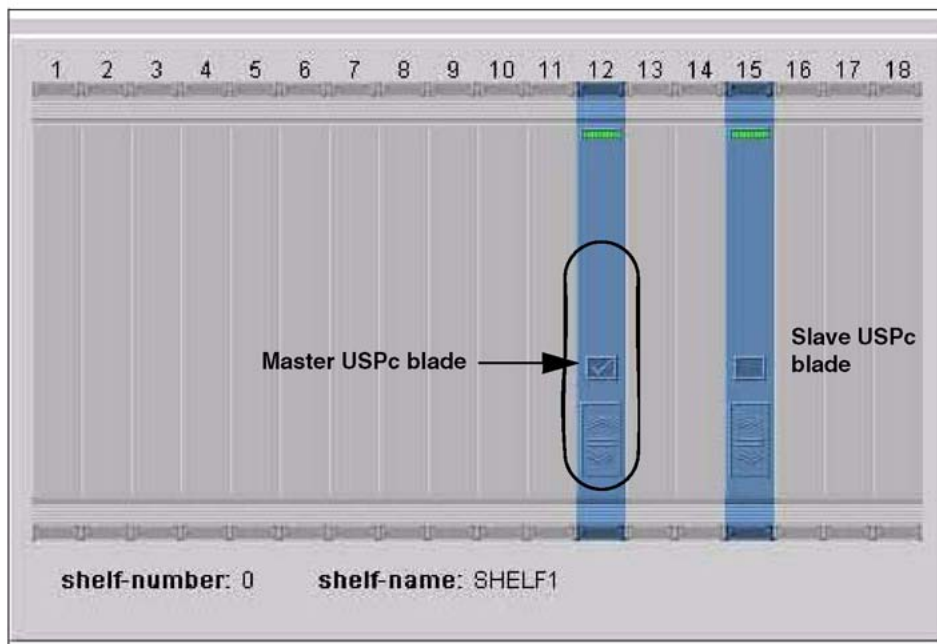
- 5 From the list of USP-Compact cards, select the row corresponding to the card to be locked and click **Post**.

The screenshot shows a web-based interface for managing USP-Compact cards. The top toolbar includes buttons for New, Add, Modify, Delete, Lock, Unlock, Load, Offline, Swact, and Restart. The 'Search' tab is active, displaying 'Retrieval Criteria' with fields for Field, Condition, Value, and Records (set to 100). Below this, 'Retrieval Results - 2 record(s) retrieved' are shown in a table.

| shelf | slot | slot-name | slot-description | slot-type  | operational-state | administrative-state | procedural-state | avail |
|-------|------|-----------|------------------|------------|-------------------|----------------------|------------------|-------|
| 0     | 12   | USP0      | USP-Compact #0   | usp-com... | enabled           | unlocked             | null             | null  |
| 0     | 15   | USP1      | USP-Compact #1   | usp-com... | enabled           | unlocked             | null             | null  |

At the bottom, there is an 'auto refresh' checkbox (unchecked), a timestamp 'Last Updated: Thu Oct 05 11:43:38 EDT 2006', and buttons for 'Post', 'Clear', and 'Get Next'. A status bar at the very bottom shows 'retrieve complete' and a page number '1'.

- 6 Verify the master and slave USPc blade-to-ERS 8600 connectivity by selecting the **Graphical View** tab.
- The following figure displays the Graphical View of the USPc blades.

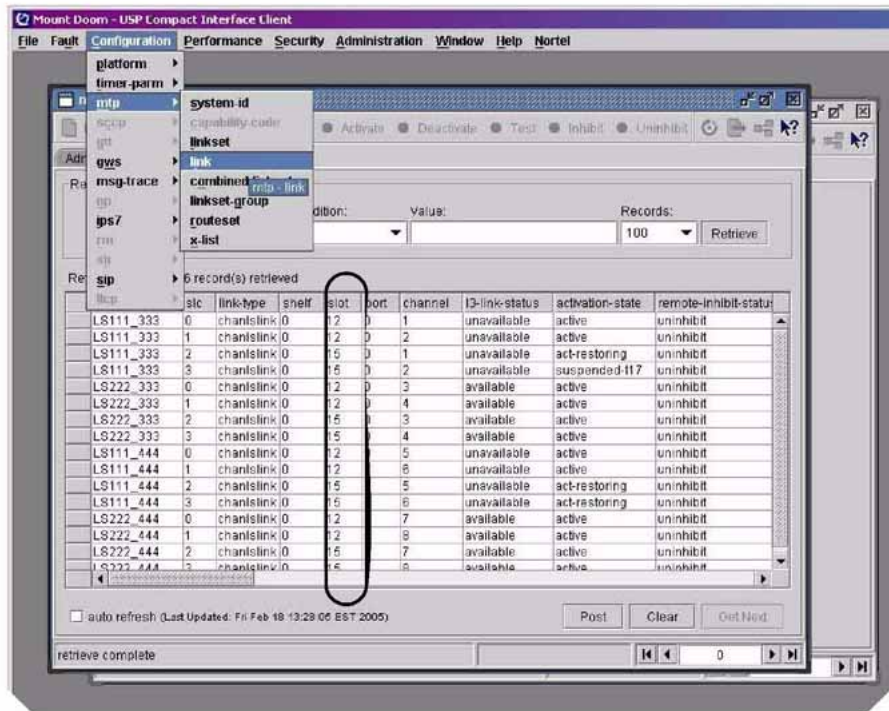


The icon with a checkmark identifies the master USPc blade. Slot 12 contains the master USPc blade. Slot 15 contains the slave USPc blade.

- 7 Select the next step as follows.

| If the slave USPc blade is                 | Do                     |
|--------------------------------------------|------------------------|
| not connected to chassis X of the ERS 8600 | <a href="#">step 8</a> |
| connected to chassis X of the ERS 8600     | <a href="#">step 9</a> |

- 8 In the Administration tab, click **Swact** to perform a SWACT on the two USPc blades.
- 9 Turn down the paths and the links associated with the slave blade to be locked.  
 Select **Configuration --> MTP --> Link** from the pull-down menu.  
 Select **Search->Retrieve**.  
 The following screen appears.



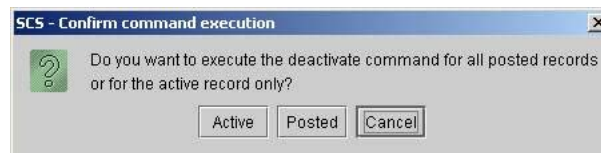
- 10 Refer to the Slot column to verify the SS7 links against the USPC blades. Select any SS7 links that are against the slave USPC blade. Post the link.

Click **Inhibit** to inhibit the links that apply to the slave USPC blade.

The following prompt displays.

The inhibit command will be executed for all posted records. Are you sure you want to continue?

- 11 Click **Yes** to execute the command on the selected links.
- 12 Using the same screen, reselect the links, and click **Deactivate**. The following window displays.

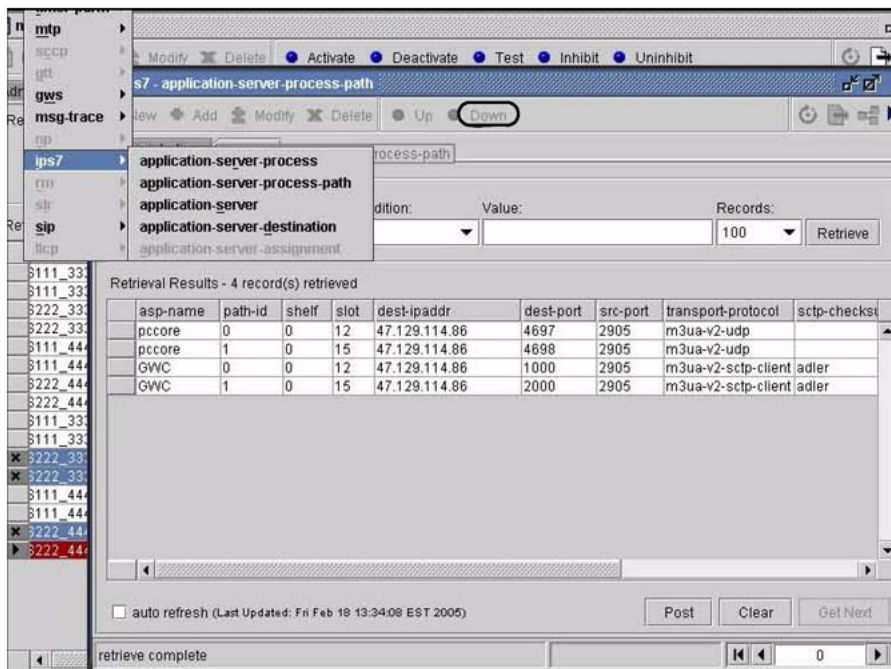


- 13 Click **Posted** to execute the command on the selected links.
- 14 Post the IPS7 paths that use the slave USPC blade.

Select **Configuration --> ips7 --> application-server-process-path**.

Select **Search->Retrieve**.

The following screen appears.



- 15** Post the IPS7 paths against the slave USPc blade.

Select all the IPS7 paths against the slave USPc blade, and click **Down**.

The down command will be executed for all posted records. Are you sure you want to continue?

- 16** Click **Yes** to execute the command on the IPS7 paths on the slave USPc blade.

The IPS7 paths and SS7 links against the slave USPc blade have been deactivated.

- 17** Lock the slave USPc blade.

Select **Configuration --> platform --> Node**.

The Administration tab redisplay.

- 18** Click **Lock**.

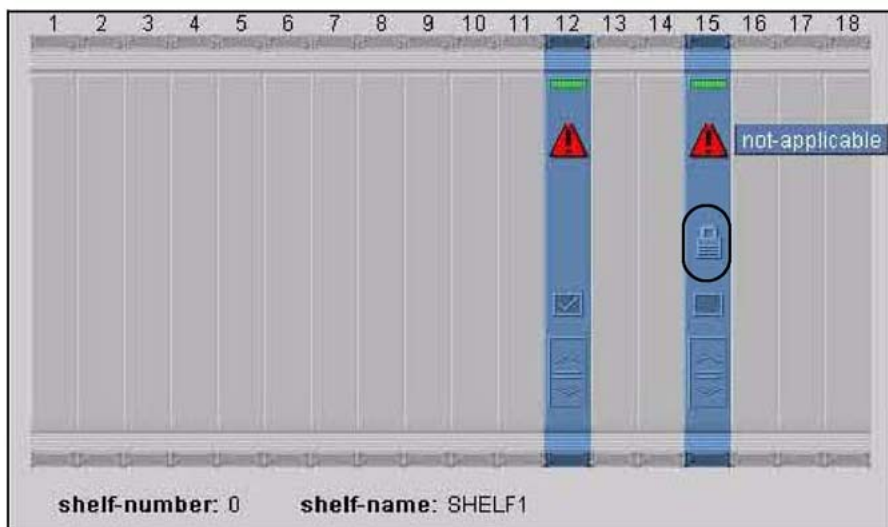
The following prompt displays:

The node lock command will impact the last in-service link in at least 1 linkset and cause at least 1 routeset to become inaccessible which may impact network traffic. Do you want to continue?

- 19** 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.

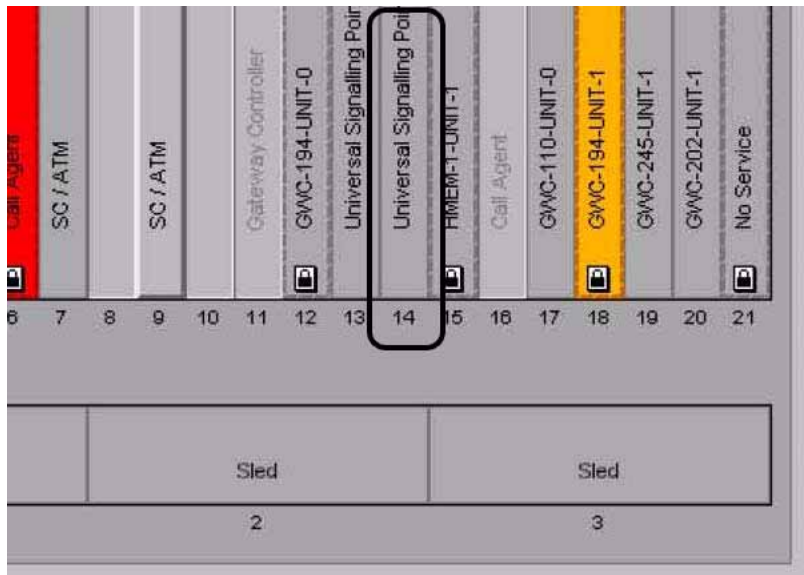


*Use the SAM21 Manager to lock the USPc blade*

- 20** Access the SAM21 Element Manager.
- 21** Select the SAM21 shelf by double-clicking on its icon.

The following figure shows an example of a shelf which contains a slave USPc blade residing on slot 14.





- 22** Right-click on the icon that corresponds to where the slave USPc blade resides.

A sub-window appears with the Card View and Lock selections enabled.

- 23** 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 can cause a system outage.

**Note 2:** An alternative method to lock the blade from the SAM21 Manager is to first open the card by double-clicking on it. Then click Lock in the States tab.

- 24** You have completed this procedure. Return to ["Task list" \(page 496\)](#) to determine your next task.

---

—End—

---

## Taking down the paths to the ERS 8600 chassis X

| Step | Action |
|------|--------|
|------|--------|

*At the USP GUI*

- |          |                     |
|----------|---------------------|
| <b>1</b> | Launch the USP GUI. |
|----------|---------------------|

Taking down the paths to the ERS 8600 chassis X consists of the following tasks:

- identifying all IP cards in the USP, and noting which Ethernet Routing Switch chassis they are connected to
- ensuring that for each path, there is an alternate in-service path through chassis Y
- taking down all IPS7 paths using chassis X

where

**chassis X** is the chassis containing the I/O module to be replaced.

**chassis Y** is the chassis not containing the I/O module to be replaced.

- 2 Select **Configuration->platform->node->Search**.
- 3 Click **retrieve**, and look for all records that have a slot-type of iplink.
- 4 Note the following information for each IP link card:
  - Shelf
  - Slot
  - IP Address
  - ERS8600 unit it is connected to
- 5 Select **Configuration->ips7->application-server-process-path->Search**.
- 6 Click **retrieve**, and look for all paths on the cards noted in [step 4](#), that are connected to chassis X.
- 7 Click on the **asp-name** column to sort the table, and confirm that for each path connected to a card using chassis X, there is an alternate path using chassis Y that has a path-state of up. Refer to the information you noted in [step 4](#).



#### CAUTION

##### Potential service interruption

If the alternate path to any destination is not in service, performing the step that follows will result in a service interruption.

- 8 Select each path connected to chassis X, and click Post, then confirm that only the paths associated with the cards connected to chassis X, are selected. Refer to the information you noted in [step 4](#).

- 9 Click Down to take the posted paths out of service.
- 10 Click Yes to confirm the command execution on the IPS7 paths associated with the cards connected to chassis X.
- 11 You have completed this procedure. Return to ["Task list" \(page 496\)](#) to determine your next task.

---

—End—

---

## Determining if STORM devices require rotating, demounting and busying

| Step | Action |
|------|--------|
|------|--------|

### ATTENTION

Before proceeding with the following STORM-related steps, consider if other applications will be affected by the loss of STORM disk volumes.

- 1 Select the next step as follows

| If                                                                                                                                                                                                                                                      | Do                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| STORM uses a Dothill device                                                                                                                                                                                                                             | <a href="#">step 2</a>  |
| STORM IA (SAM-XTS) device <sub>1</sub>                                                                                                                                                                                                                  | <a href="#">step 15</a> |
| 1. The SAM-XTS configuration uses dual-homed split multilink trunks (SMLT). Both STORM volumes are recognized by both ERS 8600 routers. Therefore, taking down one router in an SAM-XTS configuration does not affect the STORM volume being addressed. |                         |

- 2 Select the next step as follows.

| If                                                                                                                                                                                                                                                                                                                                          | Do                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| the volumes on any STORM disk (for example, sd01) are actively mounted in Device Independent Recording Package (DIRP) <sub>1</sub>                                                                                                                                                                                                          | <a href="#">step 3</a>  |
| the volumes on the STORM disk are not actively mounted DIRP <sub>2</sub>                                                                                                                                                                                                                                                                    | <a href="#">step 15</a> |
| 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 "INERROR," resulting in permanent loss of data.<br>2. Regardless of whether DIRP volumes are mounted, the procedure can result in an unavailable STORM disk and associated volumes. |                         |

- 3 If needed, enter the following command to check which STORM device is connected to the ERS 8600. If configured properly, XTS0 should have a lower IP address than XTS1.

```
sho ip arp info <STORM_address>
```

where

<STORM\_address> is the IP address of the STORM device

- 4 Login to the Call Agent as a maintenance user.
- 5 Enter the DF command to map the STORM volumes to XTS IP addresses.

```
$ df
```

Example response

```
Filesystem 1k-blocks Used Available Use% Mounted on
tmpfs 51200 36352 14848 71% /
10.102.16.112:/nfsserv/3pc/mtc/tape1
 1019200 14216 1004984 2% /TAPE1
10.102.16.111:/nfsserv/3pc/mtc/tape0
 1019200 239004 780196 24% /TAPE
10.102.16.112:/nfsserv/3pc/cs/sd01
 8187200 1972256 6214944 25% /3PC/sd01
10.102.16.111:/nfsserv/3pc/cs/sd00
 8187200 2196124 5991076 27% /3PC/sd00
10.102.16.112:/nfsserv/3pc/mtc/log1
 1019200 14216 1004984 2% /var/log_mate
10.102.16.111:/nfsserv/3pc/mtc/log0
 1019200 239004 780196 24% /var/log
```

- 6 Based on the responses of [step 3](#) and [step 5](#), determine which XTS volume (SD00 or SD01) corresponds with the STORM.
- 7 Logout of the Call Agent.
- 8 From the Core MAP command line, enter the following command to list all available DIRP subsystems (field SYSSNAME in table DIRPSSYS) for the Core.

```
>table dirpssys; lis all
```

- 9 Enter the following command to access the DIRP level in SOS.

```
>mapci nodisp;mtc;iod;dirp
```

- 10** Enter the following command to query all volumes associated with the subsystem.

```
>query <subsystem> all
```

where

**<subsystem>** is from the list of available subsystems executed in [step 8](#).

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
```

- 11** Enter the following command to rotate the active volume for each subsystem if it is located on a STORM blade connected to the ERS 8600. Manually rotate all subsystems until the active files reside on STORM volumes connected to the other ERS 8600 chassis.

```
>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:** The volume associated with the slave ERS 8600 must not be active. Ensure that no volume is active in each pass which is prefixed with sd0M.

where

**M** = 0 or 1, depending on which volume is connected to the ERS 8600, determined in [step 6](#).

(Rotate each subsystem with volumes prefixed with sd0M 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
```

**12** Repeat [step 11](#) to ensure that all volumes needing rotating have been rotated successfully.

**13** Enter the following command to demount all DIRP volumes connected to the ERS 8600 chassis that contains the CPU to be replaced.

```
>dmnt <subsystem> <volume> <variable>
```

where

**<volume>** is the volume on the STORM determined in [step 6](#)

**<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.

- 14** Enter the following command to busy all STORM volumes connected to the ERS 8600 chassis that contains the CPU to be replaced

```
>diskadm sd0M; bsy all
```

where

**sd0M** is the STORM volume defined in [step 6](#)

**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.

- 15** You have completed this procedure. Return to "Task list" ([page 496](#)) to determine your next task.

---

—End—

---

## Locking the inactive Shelf Controller (SC) blade connected to chassis X

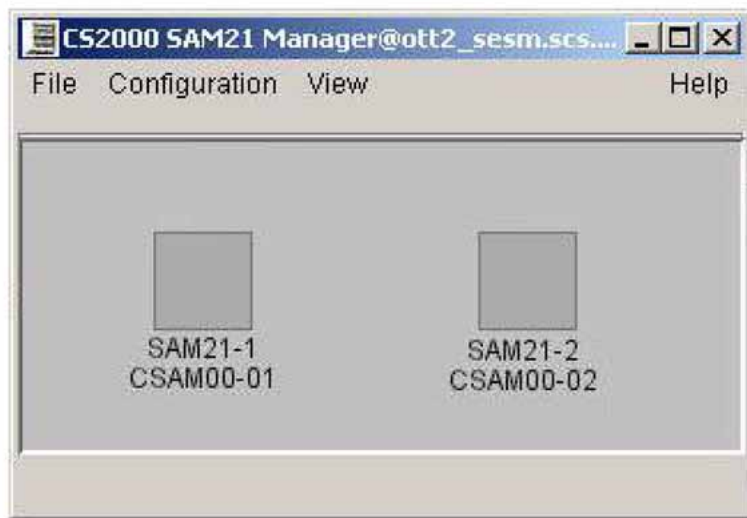
| Step                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Action                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>At the SAM21 Manager</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                  |
| <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: center;"><b>ATTENTION</b></p> <p>During a SWACT on the SCs, flapping (that is, rapid enabling and disabling of the router port connected to an SC) can result in temporary loss of Ethernet connectivity. This can cause ongoing failures on the newly active SC following the SWACT.</p> <p>To prevent the possibility of an outage from this condition, monitor ongoing or recent logs for Ethernet instability on the router ports that are associated with the SCs.</p> <p>Do not SWACT the SCs until all network problems involving flapping are addressed</p> </div> |                                                                                                                                                                                                                                                                  |
| <b>1</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Confirm that SC unit 0s (in slot 7) subtend ERS 8600 chassis 0, and SC unit 1s (in slot 9) subtend ERS 8600 chassis 1 for all SAM21 shelves. If the SAM21 shelf varies from this recommendation, adjust this procedure accordingly.                              |
| <b>2</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Lock the inactive SAM21 SC blade for each SAM21 shelf in turn as follows: <ol style="list-style-type: none"> <li>a. Launch the SAM21 Manager.</li> </ol> <p style="margin-left: 40px;">The SAM21 Manager GUI appears with the related shelf icons displayed.</p> |





- a. Launch the SAM21 Manager.

The SAM21 Manager GUI appears with the related shelf icons displayed.



- b. Use the cursor to select the shelf icon for the first SAM21 shelf displayed.

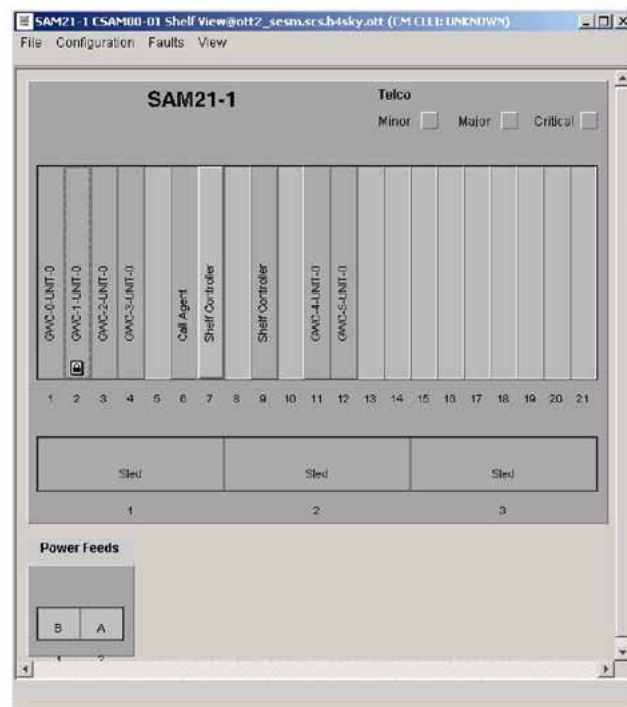
**Example**

The first shelf in the preceding figure is SAM21-1 CSAM00-01

- c. Double-click the selected shelf icon.

The SAM21 Manager shelf view for the selected shelf appears.





- d. Right-click on the icon for the SC blade associated with the inactive ERS 8600 chassis.

A sub-window appears with the Card View and Lock selections enabled.



- e. Click **Card View**.

The SC Card View appears.

The screenshot shows the SAM21 Manager interface with the 'States' tab selected. The 'Activity' section displays 'Status: Active' and a 'Swact' button. The 'OSI' section displays 'Administrative: Unlocked', 'Operational: Enabled', and 'Availability: None', with 'Lock' and 'Unlock' buttons. The 'History' section is empty. 'Save' and 'Clear' buttons are at the bottom.

- f. Select the **States** tab and make sure the SC is inactive.  
If the SC state is **Active**, click **Swact** 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 can cause a system outage.
- j. Close the **Shelf View**.  
The SAM21 Manager view reappears.

- k. Select the next step as follows

| If the (inactive) SC cards are | Do                                                               |
|--------------------------------|------------------------------------------------------------------|
| locked on all SAM21 shelves    | Proceed to <a href="#">step 3</a>                                |
| not all locked                 | select the next SAM21 Shelf and go to <a href="#">substep 2c</a> |

---

**Note:** Repeat [substep 2c](#) through [substep 2j](#) until the inactive SCs are all locked.

- 3** You have completed this procedure. Return to "[Task list](#)" ([page 496](#)) to determine your next task.

---

—End—

---

## Unlocking the Border Control Point 7100

---

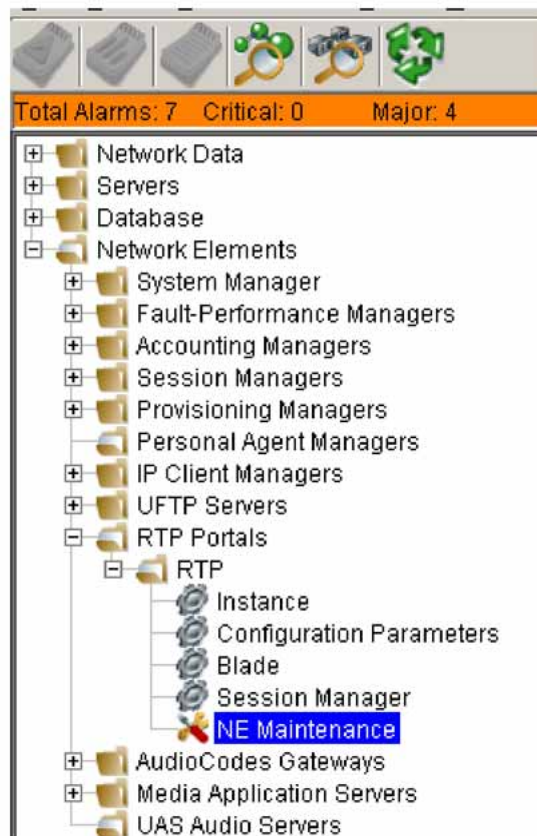
| Step | Action |
|------|--------|
|------|--------|

---

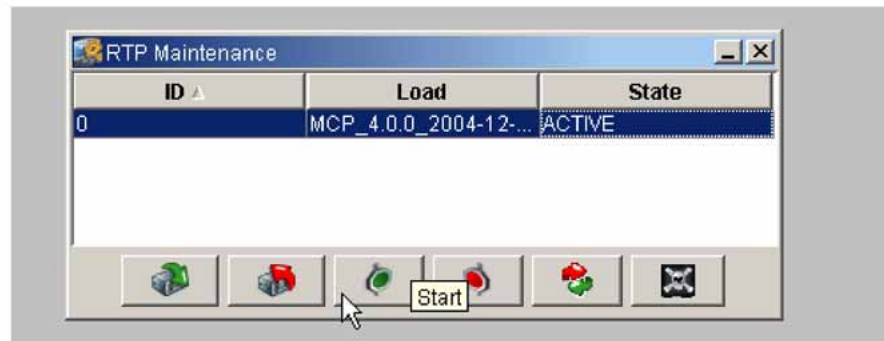
*Use the System Management Console to start the Border Control Point 7100 connected to chassis X*

- |          |                                                                                                             |
|----------|-------------------------------------------------------------------------------------------------------------|
| <b>1</b> | From the System tree, click the plus sign next to <b>Network Elements</b> to expand the view of the folder. |
|----------|-------------------------------------------------------------------------------------------------------------|

## Expanding BCP 7100 windows



- 2 Next, click the plus sign next to RTP Portals to expand the view of the folder. The contents of this folder lists all BCP 7100s and BCP 7200s configured for the site.
- 3 Continue to expand the view of folders until the target BCP 7100 is selected. Do not modify the state of any BCP 7200s.
- 4 Click the **NE Maintenance** option. A new window opens.
- 5 Click the **Start** button to restart the previously shut down BCP 7100.

**Start the BCP 7100**

- 6 You have completed this procedure. Return to ["Task list" \(page 496\)](#) to determine your next task.

---

—End—

---

**Unlocking the inactive SC**


---

**Step Action**


---

*At the SAM21 Manager*

- 1 Launch the SAM21EM client.  
The SAM21 Manager GUI appears.
- 2 Unlock each locked SC blade as follows:
  - a. Right-click on each locked SC blade.
  - b. Select Unlock from the drop-down menu that appears.
  - c. Repeat [substep a](#) and [substep b](#) until all units are unlocked.

**Note:** A padlock icon identifies locked SC blades.
- 3 You have completed this procedure. Return to ["Task list" \(page 496\)](#) to determine your next task.

---

—End—

---

**Unlocking the USP-Compact**


---

**Step Action**


---

*At the SAM21 Manager*

- 1 Re-access the SAM21 Manager. Unlock the locked slave USPc blade.

**Note 1:** Unlocking the slave USPc blade from the SAM21 Manager enables the USPc GUI.

**Note 2:** An alternative method to unlock the blade from the SAM21 Manager is to open the card by double-clicking on it. Click **Unlock** in the States tab

*At the USPc GUI*

- 2 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.

- 3 Select **Configuration --> platform --> Node**.

The window opens as follows:

The screenshot shows the USPc GUI interface. At the top, there is a toolbar with buttons: New, Add, Modify, Delete, Lock, Unlock, Load, Offline, Swact, Restart, and a help icon. Below the toolbar are three tabs: Administration, Search, and Graphical View. The main area is divided into three sections: Provisioning Data, Operational Data, and Boot Data. The Provisioning Data section includes fields for slot-type, slot-name, slot-description, shelf, slot, front-pec, tm-pec, and tm-type. The Operational Data section includes fields for operational-state, administrative-state, procedural-state, and availability-state. The Boot Data section includes fields for status-message, running-image, and boot-image. At the bottom, there is a status bar with the text 'loading complete' and a progress indicator showing 0.

- 4 Select the **Search** tab and click **Retrieve**.

The screenshot shows a web-based interface for Nortel ATM/IP Solution-level Fault Management. The top menu bar includes options: New, Add, Modify, Delete, Lock, Unlock, Load, Offline, Swact, and Restart. Below this is a tabbed interface with 'Administration', 'Search', and 'Graphical View'. The 'Search' tab is active, displaying a 'Retrieval Criteria' section with fields for Field, Condition, Value, and Records (set to 100), and a 'Retrieve' button. Below the criteria is a 'Retrieval Results - 2 record(s) retrieved' section containing a table with the following data:

|  | shelf | slot | slot-name | slot-description | slot-type  | operational-state | administrative-state | procedural-state | avail |
|--|-------|------|-----------|------------------|------------|-------------------|----------------------|------------------|-------|
|  | 0     | 12   | USP0      | USP-Compact #0   | usp-com... | enabled           | unlocked             | null             | null  |
|  | 0     | 15   | USP1      | USP-Compact #1   | usp-com... | enabled           | unlocked             | null             | null  |

Below the table is a large empty area for additional results. At the bottom of the interface, there is a status bar showing 'retrieve complete' and a progress indicator with a value of 0. A status message at the bottom left reads 'auto refresh (Last Updated: Thu Oct 05 11:43:38 EDT 2006)'. Buttons for 'Post', 'Clear', and 'Get Next' are located at the bottom right of the results area.

- 5 From the list of USP-Compact cards, select the row corresponding to the card to be unlocked and click **Post**.

The screenshot shows a web-based interface for network management. At the top, there is a toolbar with buttons: New, Add, Modify, Delete, Lock, Unlock, Load, Offline, Swact, and Restart. Below the toolbar are three tabs: Administration (selected), Search, and Graphical View. The main area is titled 'Retrieval Criteria' and contains a form with fields for Field, Condition, Value, and Records (set to 100). A 'Retrieve' button is next to the Records field. Below the form, it says 'Retrieval Results - 2 record(s) retrieved'. A table displays the results:

|   | shelf | slot | slot-name | slot-description | slot-type  | operational-state | administrative-state | procedural-state | avail |
|---|-------|------|-----------|------------------|------------|-------------------|----------------------|------------------|-------|
| ✖ | 0     | 12   | USP0      | USP-Compact#0    | usp-com... | enabled           | unlocked             | null             | null  |
|   | 0     | 15   | USP1      | USP-Compact#1    | usp-com... | enabled           | unlocked             | null             | null  |

Below the table is a large empty area. At the bottom of the interface, there is a status bar with 'retrieve complete' on the left and navigation buttons (back, forward, etc.) on the right. A checkbox for 'auto refresh (Last Updated: Thu Oct 05 11:43:38 EDT 2006)' is also present.

- 6 Select the **Administration** tab.  
The Administration tab displays.



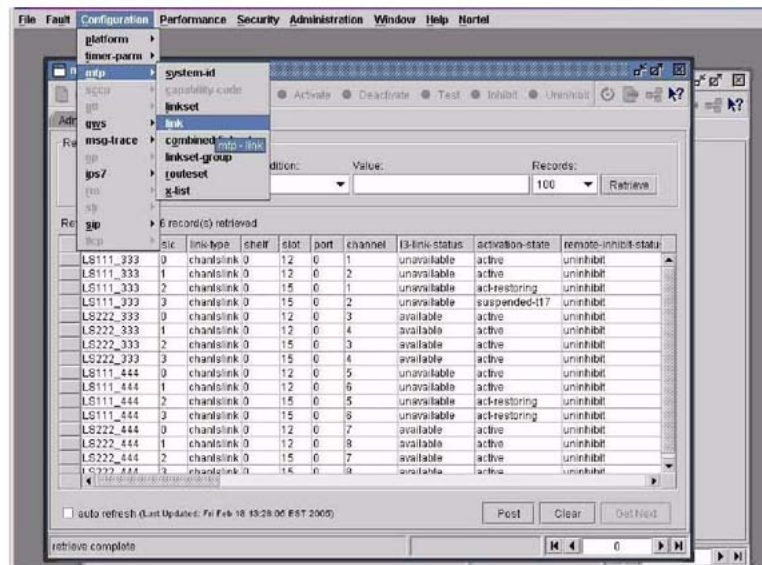
The screenshot shows the Nortel ATM/IP Solution-level Fault Management interface. The top toolbar contains buttons for New, Add, Modify, Delete, Lock, Unlock, Load, Offline, Swact, and Restart. The 'Unlock' button is circled in red. Below the toolbar are tabs for Administration, Search, and Graphical View. The main area is divided into three sections: Provisioning Data, Operational Data, and Boot Data. The Provisioning Data section includes fields for slot-type, slot-name, slot-description, shelf, slot, t1-e1-mode, ext-ip-address, ext-subnet-mask, ext-gateway, and front-pec. The Operational Data section includes fields for operational-state, administrative-state, procedural-state, availability-state, activity-state, and rex-status. The Boot Data section includes fields for status-message, running-image, ha-running-image, running-snapshot, boot-image, ha-boot-image, boot-snapshot, snapshot-description, snapshot-date, and snapshot-version. The status bar at the bottom shows 'retrieve complete' and '1 of 1'.

7 Click **Unlock** to unlock the slave USPc blade.

8 Reactivate the SS7 links and the paths associated with the slave USPc blade.

From the Administration tab, select **Configuration --> MTP --> Link** from the pull-down menu.

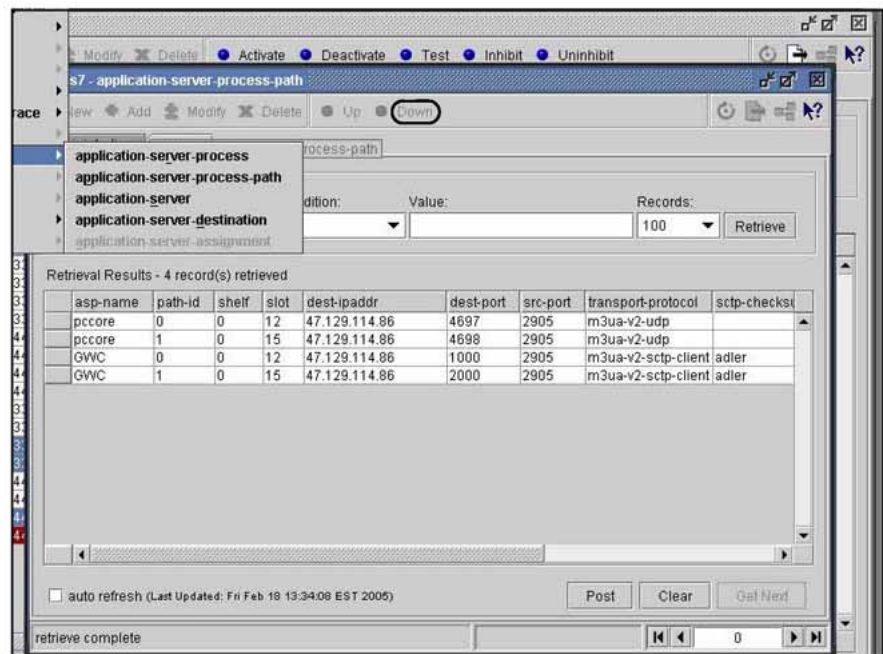
The following screen appears.



- 9 Select any SS7 links displayed in the form that are against the slave blade, and click **Activate**.
- 10 Select Yes to execute the command on the selected links.
- 11 Using the same screen, reselect the links, and click **Uninhibit**.
- 12 Select Yes to execute the command on the selected links.
- 13 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 screen appears.



- 14 Select all the IPS7 paths against the slave USPc blade, and click **Up**.

The following prompt displays:

```
execute ips7 application-serverprocess-path up command
?
```

- 15 Select Yes to execute the command on the IPS7 paths on the slave USPc blade.

- 16 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 3](#). Press the Swact button in the upper-right portion of the screen.

- 17 Select the next step as follows:

| If your office is                             | Do                      |
|-----------------------------------------------|-------------------------|
| in a Geographic Survivability environment     | <a href="#">step 18</a> |
| not in a Geographic Survivability environment | <a href="#">step 20</a> |

*Use the SAM21 Manager to unlock the inactive slave USP Compact blade*

- 18 Launch the SAM21EM client.  
The SAM21 Manager GUI appears.
- 19 Unlock each locked USPc blade as follows:
  - a. Right-click on each locked USPc blade.
  - b. Select **Unlock** from the drop-down menu that appears.
  - c. Repeat [substep a](#) and [substep b](#) until all units are unlocked.

**Note:** A padlock icon identifies locked USPc blades.
- 20 You have completed this procedure. Return to ["Task list" \(page 496\)](#) to determine your next task.

---

—End—

---

### Returning the paths to the ERS 8600 chassis X to service

| Step | Action |
|------|--------|
|------|--------|

*At the USP GUI*

- |   |                                                                                                                                                                  |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Post the IPS7 paths that use nodes connected to chassis X by selecting <b>Configuration-&gt;ips7-&gt;application-server-process-path</b>                         |
| 2 | Select each path connected to chassis X and click <b>Post</b> , then confirm that only the paths associated with the cards connected to chassis X, are selected. |
| 3 | Click <b>Up</b> to bring the posted paths back into service.                                                                                                     |
| 4 | Click <b>Yes</b> to confirm the command execution on the IPS7 paths associated with the cards connected to chassis X.                                            |
| 5 | You have completed this procedure. Return to <a href="#">"Task list" (page 496)</a> to determine your next task.                                                 |

---

—End—

---

### Enabling the Ethernet links between the XA-Core and the ERS 8600

| Step | Action |
|------|--------|
|------|--------|

*At the MAP display*

- |   |                                                                          |
|---|--------------------------------------------------------------------------|
| 1 | Enter the following command to access the ETHR level of the MAP display. |
|---|--------------------------------------------------------------------------|

```
>MAPCI;MTC;XAC;ETHR
```

- 2 Refer to the following tables and enable the Ethernet link between the XA-Core and ERS 8600 chassis X by executing substep 2a or 2b, as appropriate.

- a. If the XA-Core uses HIOPs or HCMICs, enter the following command to enable the link (otherwise execute substep 2b):

```
rts <slot> r link
```

| HIOPs/HCMICs | chassis X | chassis Y |
|--------------|-----------|-----------|
| <slot>       | 5         | 14        |

Go to [step 3](#).

- b. If the XA-Core uses IOPs with ETHR packets, enter the following command to enable the link:

```
rts <slot1> r 1 link
```

Wait for the command to complete, then enter the following command:

```
rts <slot2> r 1 link
```

| IOP with ETHRs | chassis X | chassis Y |
|----------------|-----------|-----------|
| <slot1>        | 5         | 6         |
| <slot2>        | 13        | 14        |

- 3 You have completed this procedure. Return to the ["Task list"](#) (page 496) to determine your next task.

---

—End—

---

# Configuring the SESM Server Application

## Application

Use this procedure to configure the Succession Element and Sub-element Manager (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)
- the CLLI name of the office (CM CLLI), and the IP address of the SDM (CS 2000 Core Manager)Packet SDMX (XA-Core manager) associated with the CLLI
- the IP address of the Media Gateway 9000 Manager if present in the network

### ATTENTION

Only the root user can perform this procedure.

## Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

### *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
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.

- 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.

- 9 When prompted, enter the CLLI name of the office (CM CLLI), or press the Enter key to accept the default if one is specified.

- 10 When prompted, enter the IP address of the SDM (CS 2000 Core Manager)Packet SDMX (XA-Core manager) associated with the CM CLLI, or press the Enter key to accept the default if one is specified.  
The system displays the information you entered for confirmation.

- 11 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.

- 12 Exit "SESM configuration" by typing  
`select - x`  
and pressing the Enter key.
- 13 You have completed this procedure.

---

—End—

---



## Starting the SESM server application

### Application

Use this procedure to start the Succession Element and Subelement Manager (SESM) server application on the SPFS-based server.

### Prerequisites

None

### Action

Perform the steps that follow to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

***At your workstation***

- Establish a connection to the server that is hosting the CS 2000 Management Tools through telnet or SSH, and log in using the root user ID and password.  
  
In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the ubmstat command.  
  
For detailed steps, refer to procedure "Logging in to an SPFS-based server".
- Verify the status of the SESM server application by typing  
  
`# servman query -status -group SESMService`  
  
and pressing the Enter key.

| If the response indicates | Do                     |
|---------------------------|------------------------|
| not running               | <a href="#">step 3</a> |
| running                   | <a href="#">step 6</a> |

- Start the SESM server application by typing  
  
`# servstart SESMService`  
  
and pressing the Enter key.
- Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to start.
- Verify the SESM server application started as follows:

- a. Verify the SESM services started by typing

```
servman query -status -group SESMSERVICE
```

and pressing the Enter key.

*Example response:*

```
CS2K Management Tools are running
```

- b. Verify the SESM applications started by typing

```
ptmctl status
```

and pressing the Enter key.

*Example response:*

```
SESM STATUS -----
 COMPONENT STATUS

Proxy Agent RUNNING
RMI Regisry RUNNING
Snmpfactory RUNNING
MI2 Server RUNNING
Current number of SESM processes running: 4 (of 4)
SESM APPLICATION STATUS: All Applications Ready
```

- 6** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

—End—

---

## Stopping the SESM server application

### Application

Use this procedure to stop the Succession Element and Subelement Manager (SESM) server application on the CS 2000 Management Tools server.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

***At your workstation***

- Establish a connection to the server that is hosting the CS 2000 Management Tools through telnet or SSH, and log in using the root user ID and password.  
  
In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the `ubmstat` command.  
  
For detailed steps, refer to procedure "Logging in to an SPFS-based server".
- Verify the status of the SESM server application by typing  
  
`# servman query -status -group SESMSservice`  
  
and pressing the Enter key.

| If the response indicates | Do                     |
|---------------------------|------------------------|
| running                   | <a href="#">step 3</a> |
| not running               | <a href="#">step 6</a> |

- Stop the SESM server application by typing  
  
`# servstop SESMSservice`  
  
and pressing the Enter key.
- Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to stop.
- Verify the SESM server application stopped as follows:

- a. Verify the SESM services stopped by typing

```
servman query -status -group SESMSERVICE
```

and pressing the Enter key.

*Example response:*

```
CS2K Management Tools are not running
```

- b. Verify the SESM applications stopped by typing

```
ptmctl status
```

and pressing the Enter key.

*Example response:*

```
SESM STATUS -----
COMPONENT STATUS

Proxy Agent NOT RUNNING
RMI Regisry NOT RUNNING
Snmpfactory NOT RUNNING
MI2 Server NOT RUNNING
Current number of SESM processes running: 0 (of 4)
SESM APPLICATION STATUS: No Applications are ready
```

- 6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

—End—

---

## 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 CLLI 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.

| Step | Action |
|------|--------|
|------|--------|

#### *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.

---

—End—

---

## Stopping and starting the DDMS proxy

### Application

#### ATTENTION

Use this procedure only if you have been directed here from the Optional post-upgrade tasks in *Core Manager Upgrades*, NN10060-461, after a software upgrade.

Use this procedure to stop and start the DDMS proxy on the CS 2000 Management Tools server. The DDMS proxy enables communication between the CS 2000 Management Tools server and the core.

### Prerequisites

There are no prerequisites for this procedure.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *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 - 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 server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

**server** is the physical IP address of the inactive server

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 Use the following table to determine your next step.

| If you upgraded the CS 2000 Core Manager from |  | Do     |
|-----------------------------------------------|--|--------|
| SN07                                          |  | step 5 |
| SN08                                          |  | step 8 |

5 Stop the DDMS proxy by typing

```
/opt/nortel/NTsesm/admin/scripts/ddmsproxy stop
```

and pressing the Enter key.

6 Start the DDMS proxy by typing

```
/opt/nortel/NTsesm/admin/scripts/ddmsproxy start
```

and pressing the Enter key.

7 Proceed to step 14.

8 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 -

- 9** Enter the number next to the "Configuration" option in the menu.

*Example response*

Configuration

1 - NTP Configuration  
2 - Apache Proxy Configuration  
3 - OAMP Application Configuration  
4 - CORBA Configuration  
5 - IP Configuration  
6 - DNS Configuration  
7 - Syslog Configuration  
8 - Remote Backup Configuration  
9 - Database Configuration  
10 - NFS Configuration  
11 - Bootp Configuration  
12 - Restricted Shell Configuration  
13 - Security Services Configuration  
14 - Disk Drive Upgrade  
15 - Login Session  
16 - Location Configuration  
17 - Cluster Configuration  
18 - Succession Element Configuration  
19 - snmp\_poller (SNMP Poller Configuration)  
20 - backup\_config (Backup Configuration)  
X - exit  
Select -

- 10** Enter the number next to the "Succession Element Configuration" option in the menu.

*Example response:*

Succession Element Configuration

1 - NPM Application Configuration  
2 - SESM Application Configuration  
3 - SAM21EM Application Configuration  
4 - PSE Application Configuration  
5 - RESMON Application Configuration  
6 - OMPUSH Application Configuration  
7 - DDMSProxy Application Configuration  
X - exit  
select -

- 11** Enter the number next to the "DDMSProxy Application Configuration" option in the menu.

*Example response*

DDMSProxy Application Configuration

1 - ddmsproxy\_query (query the status of  
ddmsproxy service)

```
2 - ddmsproxy_stop (stop the ddmsproxy service)
3 - ddmsproxy_start (start the ddmsproxy
 service)
X - exit
select -
```

- 12** Enter the number next to the "ddmsproxy\_stop" option in the menu.

*Example response*

```
===Executing "ddmsproxy_stop"
ddmsproxy service stopping
=== "ddmsproxy_stop" completed successfully
```

- 13** Enter the number next to the "ddmsproxy\_start" option in the menu.

*Example response*

```
===Executing "ddmsproxy_start"
ddmsproxy service starting
=== "ddmsproxy_start" completed successfully
```

- 14** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

—End—

---

## Stopping the SAM21 Manager server application

### Application

Use this procedure to stop the SAM21 Manager server application on the SPFS-based server that is hosting the CS 2000 Management Tools.

### Prerequisites

None

### Action

Perform the steps that follow to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

*At your workstation*

- Establish a login session to the server, using one of the following methods  
  
In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the `ubmstat` command.  
  
For detailed steps, refer to procedure "Logging in to an SPFS-based server".
- Verify the status of the SAM21 Manager server application by typing  
`# servman query -status -group SAM21EM`  
and pressing the Enter key.

| If SAM21EM is | Do                     |
|---------------|------------------------|
| running       | <a href="#">step 3</a> |
| not running   | <a href="#">step 5</a> |

- Stop the SAM21EM server application by typing  
`# servstop SAM21EM`  
and pressing the Enter key.
- Verify the SAM21EM server application stopped by typing  
`# servman query -status -group SAM21EM`  
and pressing the Enter key.

*Example response:*

```
Executing: /opt/servman/bin/servquery -status - group
SAM21EM
Succession SAM21 Element Manager version: SAM21EM_9
_020_0
Current status of the Succession SAM21 Element Manager:
 SNMP Access Gateway is not running.
 SAM21 Element Manager Server is not running.
```

- 5 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

—End—

---

## Stopping the NPM server application

### Application

Use this procedure to stop the Network Patch Manager (NPM) server application on a Server Platform Foundation Software (SPFS)-based server.

### Prerequisites

You need root user privileges to perform this procedure.

It is recommended that all users exit the NPM CLUI and GUI before stopping the NPM server application.

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the Active server.

| Step | Action |
|------|--------|
|------|--------|

#### *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 SPFS-based server where the NPM server application resides  
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.  
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 NPM server application by typing

```
servman query -status -group NPM
```

and pressing the Enter key.

| If the NPM server application is | Do                                |
|----------------------------------|-----------------------------------|
| running                          | step 6                            |
| not running                      | you have completed this procedure |

- 6 Stop the NPM server application by typing

```
servstop NPM
```

and pressing the Enter key.

- 7 Verify the NPM server application is no longer running by typing

```
servman query -status -group NPM
```

and pressing the Enter key.

You have completed this procedure.

---

—End—

---

## Starting the SAM21 Manager server application

### Application

Use this procedure to start the SAM21 Manager server application on the SPFS-based server that is hosting the CS 2000 Management Tools.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

*At your workstation*

- Establish a connection to the server that is hosting the CS 2000 Management Tools through telnet or SSH, and log in using the root user ID and password.  
  
In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.  
  
For detailed steps, refer to procedure "Logging in to an SPFS-based server".
- Verify the status of the SAM21 Manager server application by typing  
**# servman query -status -group SAM21EM**  
and pressing the Enter key.

| If SAM21EM is | Do                     |
|---------------|------------------------|
| not running   | <a href="#">step 3</a> |
| running       | <a href="#">step 5</a> |

- Start the SAM21EM server application by typing  
**# servstart SAM21EM**  
and pressing the Enter key.
- Verify the SAM21EM server application started by typing  
**# servman query -status -group SAM21EM**  
and pressing the Enter key.

*Example response:*

```
Executing: /opt/servman/bin/servquery -status - group
SAM21EM
Succession SAM21 Element Manager version: SAM21EM_9
_020_0
Current status of the Succession SAM21 Element Manager:
 SNMP Access Gateway is running.
 SAM21 Element Manager Server is running.
```

- 5** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure

---

**—End—**

---



## Starting the NPM server application

### Application

Use this procedure to start the Network Patch Manager (NPM) server application on a Server Platform Foundation Software (SPFS)-based server.

### Prerequisites

You need root user privileges to perform this procedure, and CORBA must be running in order for the NPM to come up.

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the Active server.

| Step | Action |
|------|--------|
|------|--------|

#### *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 SPFS-based server where the NPM server application resides  
 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.  
 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 NPM server application by typing
- ```
# servman query -status -group NPM
```
- and pressing the Enter key.

If the NPM server application is	Do
not running	step 6
running	you have completed this procedure

- 6 Start the NPM server application by typing
- ```
servstart NPM
```
- and pressing the Enter key.
- 7 Verify the NPM server application is running by typing
- ```
# servman query -status -group NPM
```
- and pressing the Enter key.
- You have completed this procedure.

—End—

Starting and stopping CInotifier

Use the CInotifier application to notify network users that remote connectivity is running.

ATTENTION

When you start CInotifier and then delete the GWC manager node, all client GWCs auto-refresh their GWCEM lists. However, when you stop CInotifier the GWCEM lists do not refresh.

Prerequisites

This procedure has the following prerequisites:

- You must be logged in to your work station

Procedure steps

Step	Action

1	Start CInotifier using <code>servstop CINOTIFIER</code> .

2	Stop CInotifier using <code>servstop CINOTIFIER</code> .

—End—	

Setting the MSC Server 1000 CLLI on the Sun server

Application

The SDM IP address automatically retrieves the CM CLLI from the Communication Server 2000 (CS 2000).

Use this procedure to rediscover the CM CLLI on a Server Platform Foundation Software (SPFS) based server when the SDM IP has already been configured.

ATTENTION

The steps to configure the SDM IP are also provided in the event it has not already been configured. The CM CLLI can be configured or unconfigured on an SPFS-based server that hosts the Core and Billing Manager (CBM), but cannot be configured or unconfigured on an SPFS-based server that hosts the following components:

- CS 2000 Management Tools and Audio Provisioning Server (APS)
- CS 2000 Management Tools, Integrated Element Management System (IEMS), or both
- Media Gateway 9000 Manager

To set the CM CLLI on an SPFS-based server that hosts the CBM, refer to the CBM Configuration Management document (NN10353-511). Use this procedure to set the CLLI for the MSC Server 1000 XA-Core (CM CLLI) on a server that uses Server Platform Foundation Software (SPFS). You can also use this procedure to remove the MSC Server 1000 CLLI from the server.

Make sure your system is patch-current before performing this procedure. If the system is not patch-current, changing or unconfiguring the CM CLLI can cause loss of configuration data on the system. If you are not sure whether the patch that corrects this issue is applied, contact your next level of support before you proceed.

Prerequisites

- Be prepared to configure the SDM IP address in the event the address is not already configured.
- You must have the CLLI for the CS 2000 that is associated with the SPFS-based server on which you are setting the CLLI.

ATTENTION

The CS 2000 CLLI is listed in table OFCENG.

Action

Perform the following steps to complete this procedure.

Step	Action

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 SPFS-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- OAMP Application Configuration
4- CORBA Configuration
5- IP Configuration
6- DNS Configuration
7- Syslog Configuration
8- Remote Backup Configuration
9 - Database Configuration
```

```

10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
Select -

```

- 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 12
...indicates the SDM IP is not configured	step 9

- 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.

Example response

You must log out and log back in to the new SDM environment settings to take place.

SDM IP and CM CLLI have been successfully configured.

- 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 maintenance 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 SPFS-based server

- d. When prompted, enter your user ID and password.

ATTENTION

If the Network Patch Manager (NPM) server application is running on this SPFS-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) .

You have completed this procedure.

—End—

Changing the Oracle user password on an SPFS-based server

Application

Use this procedure to change the default Oracle passwords on a Server Platform Foundation Software (SPFS)-based server.

Refer to procedure Changing the APS Oracle account password, to change the Oracle account 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.

Step	Action

At your workstation

- 1 Log in to the Active server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server is the IP address or host name of the SPFS-based server
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/SPFS/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

The command takes approximately 15 to 20 seconds to execute.
You have completed this procedure.

—End—

Powering up the network

Purpose of this procedure

ATTENTION

If your network uses a Geographically Survivable configuration, refer to "[Geographic survivability](#)" (page 582).

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
- IEMS
- CS 2000 Management Tools
- MG 9000 Manager
- Border Control Point 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
- Border Control Point
- 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

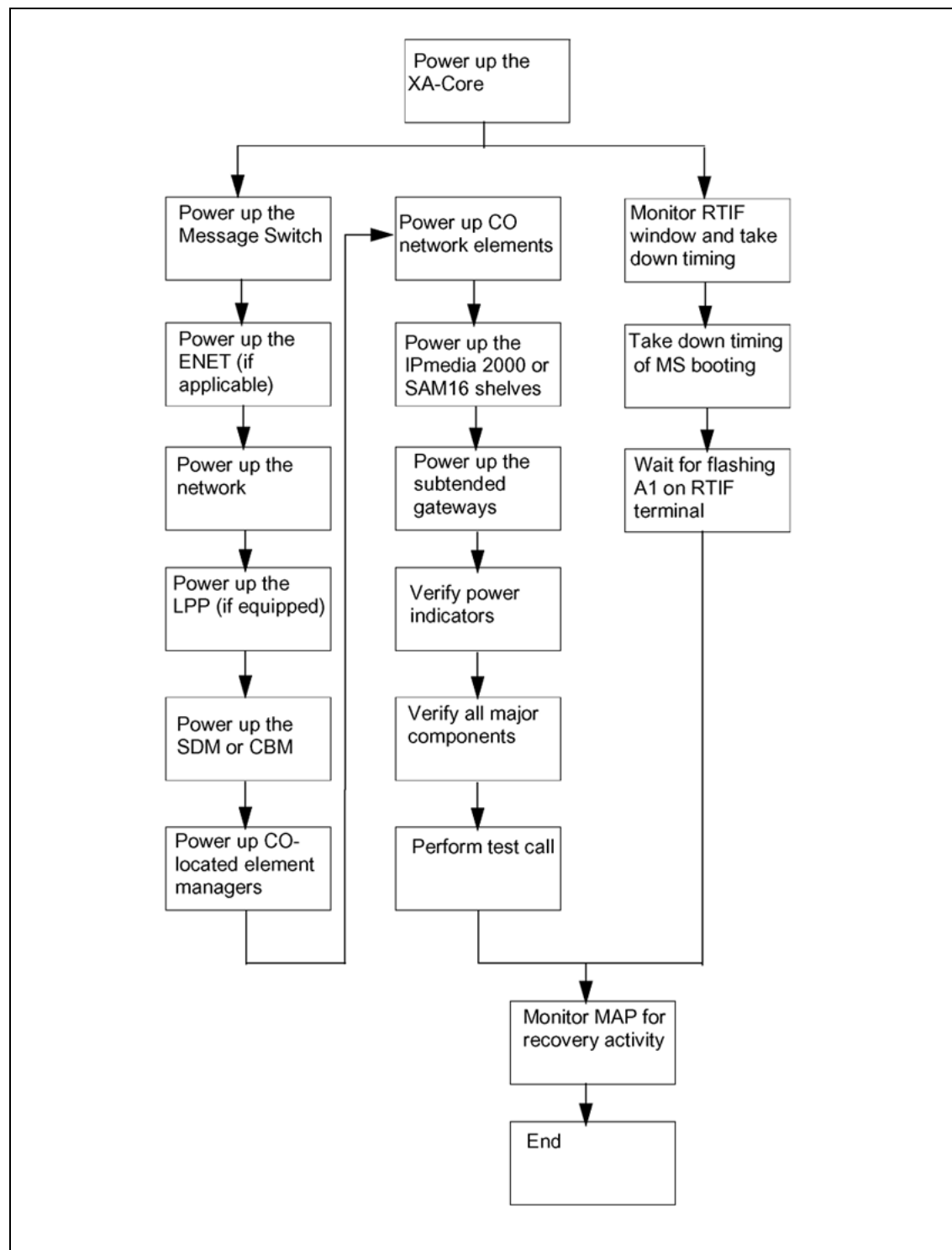
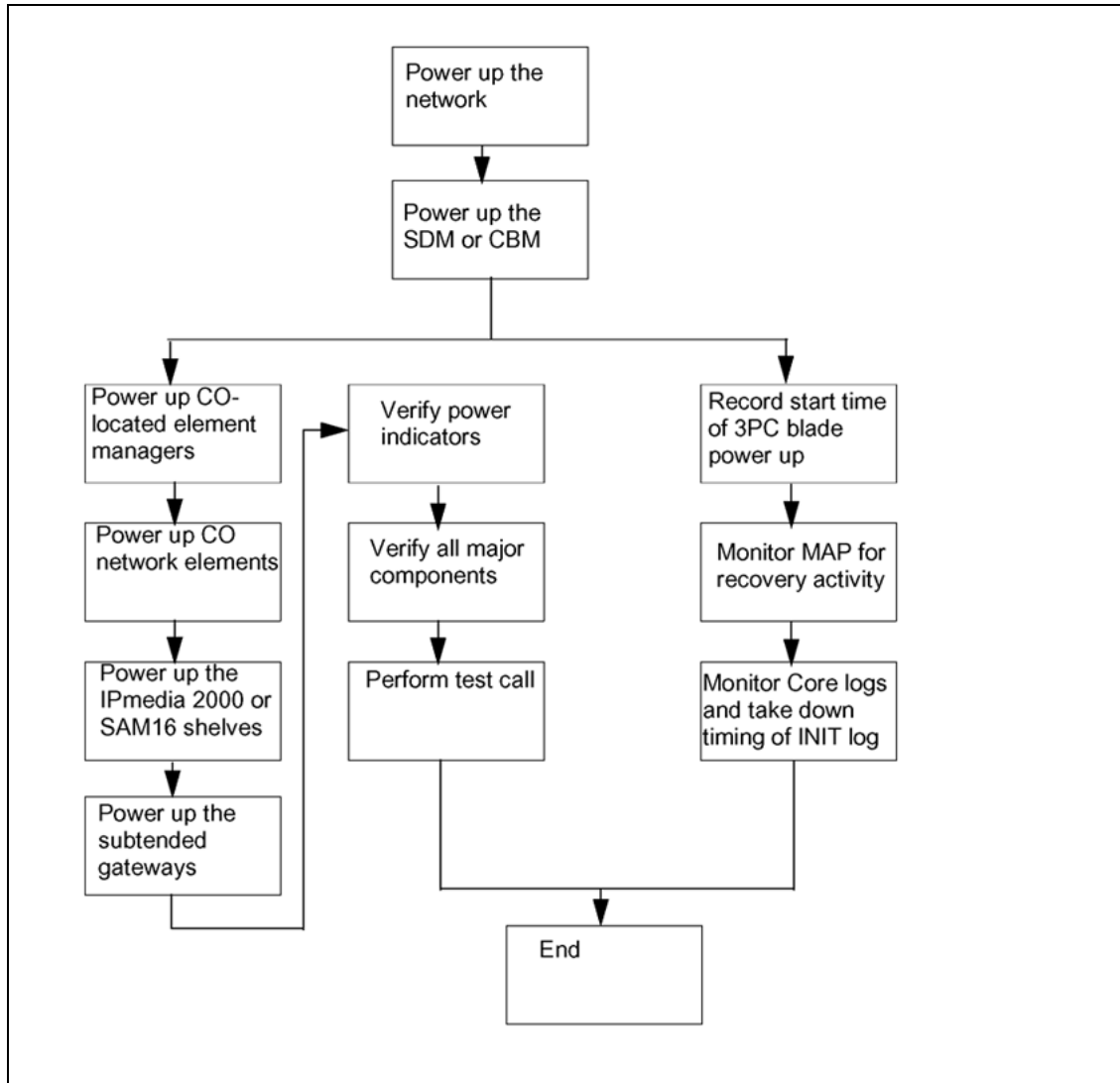


Figure 2
Summary of procedure for a CS 2000-Compact-based office



Step	Action

In the network office

- 1 Determine if you are powering up a CS 2000 or CS 2000-Compact-based office.

If you are powering up a	Do
CS 2000-based office	step 2
CS 2000-Compact-based office	step 9

- 2 Power up the XA-Core. Refer to Powering up the XA-Core.

- 3 Perform [step 4](#) and [step 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 and Powering up the Enhanced Network.
 - 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.
 - c. Power up the LPP (if equipped).
Refer to Powering up the Link Peripheral Processors.
 - d. Power up the SDM or CBM.
For the SDM, refer to Powering up the SDM. For the CBM, refer to Powering up a T1400 or N240 server.
 - e. If equipped, power up the DNS server. Refer to the hardware documentation for your server for detailed instructions.

ATTENTION

Wait at least 5 minutes between each step from [step 4f](#) to [step 4k](#).

- f. Power up the CO located element managers, such as the IEMS, CS 2000 Management Tools, and MG 9000 Manager.
Refer to Powering up a T1400 or N240 server.
- g. If equipped, power up the RTP Media Portal Manager.
Refer to Powering up the RTP Media Portal Manager.
- 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
 - Powering up a USP
 - Powering up a Media Gateway/Multiservice Switch 15000
 - Powering up a Media Gateway/Multiservice Switch 7400
 - Powering up the MDM workstation
 - Powering up an SPM device
- i. If equipped, power up the MCS servers and/or RTP Media Portal.

Refer to Powering up the MCS servers and Powering up an RTP Media Portal.

- 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. If your system uses a UAS, refer to Powering up the SAM16 shelves.

- 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.

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.

10 Power up the SDM or CBM.

For the SDM, refer to Powering up the SDM. For the CBM, refer to Powering up a T1400 or N240 server.

- 11 If equipped, power up the DNS server. Refer to the hardware documentation for your server for detailed instructions.
- 12 Perform [step 13](#) and [step 14](#) in parallel.
- 13 Power up the remaining network elements by performing the following steps.

ATTENTION

Wait at least 5 minutes between each step from [step 13a](#) to [step 13f](#).

- a. Power up the CO located element managers, such as the IEMS, CS 2000 Management Tools, and MG 9000 Manager.
Refer to Powering up a T1400 or N240 server
- b. If equipped, power up the RTP Media Portal Manager.
Refer to Powering up the RTP Media Portal Manager.
- 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
 - Powering up a USP
 - Powering up a Media Gateway/Multiservice Switch 15000
 - Powering up a Media Gateway/Multiservice Switch 7400
 - Powering up the MDM workstation
 - Powering up an SPM device
- d. If equipped, power up the MCS servers and/or Border Control Point.
Refer to Powering up the MCS servers and Powering up an RTP Media Portal.
- 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. If your system uses a UAS, refer to Powering up the SAM16 shelves.
- 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.

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 IEMS (or other managers if not equipped with IEMS).
- 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.

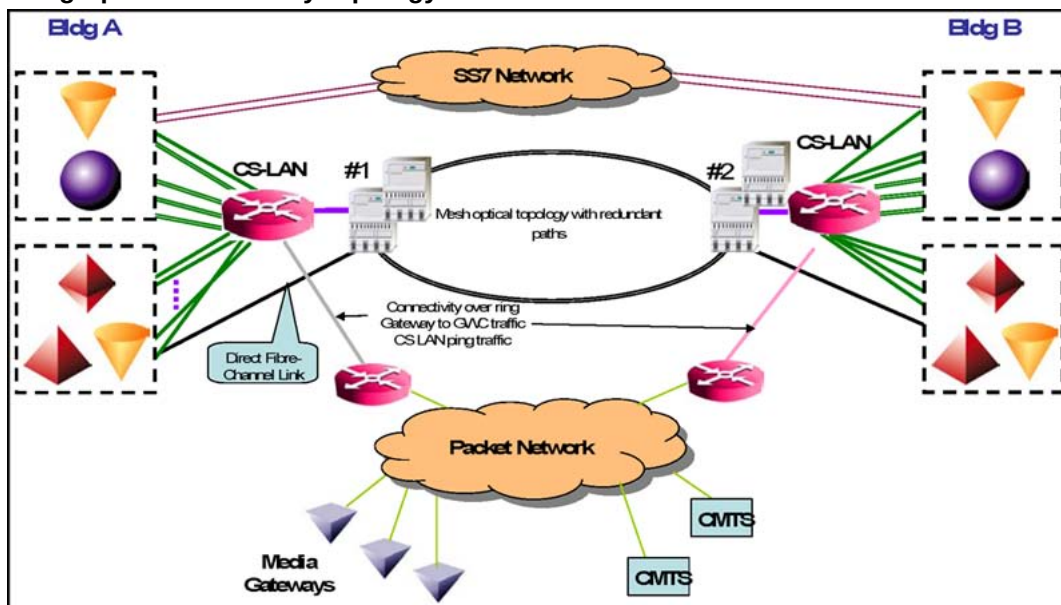
—End—

Geographic survivability

Geographic survivability is the distribution of components across a geographic area to ensure services continue in the event of a disaster. A disaster can include fire, flood, tropical storm, or act of terrorism. Geographic survivability includes the distribution of hardware across multiple locations.

The following figure shows the topology for CS 2000 - Compact support for geographic survivability.

Geographic survivability topology



The CS 2000 - Compact supports geographic survivability through the fail-over and sparing functionality of individual nodes. The configuration for the CS 2000 Management Tools (CMT) and Integrated Element Management System (IEMS) servers and the Core and Billing Manager (CBM) 850 is as follows:

- Site A is configured with the CMT and IEMS high-availability (HA) server pairs
- Site B is configured with the CBM 850 HA server pairs (referred to as CBM 850 HA u0 and u1)
- Site A is configured with an additional CBM in to be used in the event of disaster at Site B (referred to as CBM 850 standby u0)
- Site B is configured with an additional server for the CMT and IEMS in the event of disaster at Site A

For a communication server, geographic survivability requires that redundant components (other than OAM components) must reside at different sites (referred to as Site A and Site B).

For OAM components, the Automatic Backup and Accelerated restore feature (known as remote backup) remotely backs up all data on the target unit. This provides a standby backup system ready to provide service should the primary system or cluster be unavailable for an extended period of time (for example, catastrophic site loss). The remote backup can assume the identity of the target system with data and files accurate to the last sync and will be located at a different site from the target system. Remote backup performs the backup via TCP/IP connection and stores an exact copy on the standby server which can be quickly and remotely activated. This remote backup copies all files in each file system marked for backup using the same behavior as a full system backup.

A remote backup configuration tool is provided to set the necessary parameters and schedule for automatic backup which can be scheduled to automatically occur from once a day to four times per day. This tool also provides a facility for manually initiating a backup and monitoring its progress. The standby server has an identical copy of files from the last backup, so it can become the primary system via changing the boot pointer and rebooting. When the primary site is again available, the remote backup feature can be reused to transfer current system configuration back to the primary site and system.

ATTENTION

If configuration, provisioning, patching or other “write”-type operations occurred since the last remote backup, the remote backup system can be out of sync compared to the data in network elements and/or the primary OAM system

When initiating a switchover to a remote backup OAM server, do not execute configuration, provisioning, patching or other “write”-type operations through the remote backup OAM system until out-of-sync conditions are cleared.

Take actions before initiating the switchover to a remote backup OAM server (that is, response to a geographic or other prolonged outage of the primary OAM system) to halt or prevent “write”-type operations by OSSs and operations personnel until an in-sync status is achieved.

If a site outage is imminent (for example, threatening severe weather conditions), consider precautionary preparations to discontinue “write”-type operations. Make manual backups to the remote backup OAM servers to ensure data synchronization of the remote OAM server before performing a switchover.

Apply similar precautions when initiating a recovery back to the primary cluster. In this more controlled scenario, “write”-type operations must be discontinued before initiating this procedure

Site failure in a geographic survivable configuration

There are two scenarios for recovery of a geographic survivable network configuration:

- "Site A failure" (page 584)
- "Site B failure" (page 584)

Site A failure

A loss of Site A would include a loss of the CS 2000 Management Tools and IEMS servers. This loss would result in the following losses of functionality:

- all OAM&P functions of the CS 2000 Management Tools and Integrate EMS, including GUI access, element management, alarms, and non-Core logs
- access to the CS 2000-Compact Core Manager on the CBM 850

The responsive action in this scenario is to initiate a switchover to the standby CMT and IEMS servers at Site B.

Site B failure

A loss of Site B would include a loss of the CBM 850 servers. This loss would result in the following losses of functionality:

- transfer of billing records from the Core to the CBM 850
- billing records resident in the CBM 850 that had not been offloaded to an OSS
- ability to receive scheduled Core OM's and logs (resulting in them being discarded)
- access to the CS 2000-Compact Core Manager
- backup bootp load repository

The responsive action in this scenario is to initiate a switchover to the standby CMT and IEMS servers at Site A.

Fresh pre-install of CBM 850 cold u0

To reduce the duration of downtime during an outage, it is recommended that the CBM 850 cold u0 be pre-installed. Contact your next level of support for this task.

Maintaining sites in a geographic survivable configuration

The following procedures contain information for OA&M auto backup and accelerated restore capability:

- "Installing the remote backup server" (page 603)
- "Scheduling automatic backups on the remote server" (page 608)

- "Viewing configuration information for remote server backups" (page 611)
- "Performing a manual backup of the target server" (page 613)
- "Viewing logs from a remote backup" (page 615)
- "Initiating a recovery back to the cluster" (page 616)
- "Initiating a switch over to the remote backup server" (page 618)

Geographical Survivability impacts to CS 2000-Compact

The Geographic Survivability feature allows services to continue in the event of a natural or man-made disaster. A sub-panel to the Call Agent Card View Provisioning panel (tab) allows you to enable or disable the feature. The following figure shows an example configuration with Geographic Survivability enabled.

Call Agent Card View Provisioning panel: Geographic Survivability enabled

OTT4 CA-1 : Slot 6

Alarms Equip States Diags **Provisioning**

General

IP: 10.72.17.22 Gateway IP: 10.72.16.1

Subnet Mask: 255.255.240.0 FW Version: RM03-2.4

MAC Address: 0001AF12AFA0 MAC 2: 0001AF12AF9F

NTP

Primary NTP: 47.135.43.193 Secondary NTP: 47.135.43.196

Load Info

Server IP: 47.135.43.193

Path: /3pc

Load: ncgl_cca_image_7.02.1.0 Get Load Files

☒ FW Flash Enable

Geographical Survivability

Geographical CS 2000 Compact

☒ Enable

Backup Path:

GEO UNIT 0 IP: 10.72.0.12 Mask: 255.255.255.248

GEO UNIT 1 IP: 10.72.0.20 Mask: 255.255.255.248

Modify Save Clear Cancel Details... Help

Failure scenarios

The following table provides summaries of system responses during various failure scenarios when Geographical Survivability is enabled. The scenarios assume redundant configurations are located in two separate sites.

System response summaries

Scenario	Response
Ethernet Routing Switch 8600 failure at one site	<i>At the site with the failed routing switch:</i> - All nodes lose mate connectivity via Ethernet. - The Call Agent loses WAN backup connectivity.

Scenario	Response
	• FC or GigE call data sync link remains up until the Call Agent resets. • The Call Agent resets itself approximately 1 minute after losing network connectivity and tries to boot from the network. The Call Agent keeps trying to boot until the network recovers and the boot is successful. • The Call Agent detects IST loss, but cannot disable ERS 8600 routing. • USPC detects isolation and takes down SS7 links at the site with the 8600 failure. <i>At the site with the in-service routing switch:</i> • The Call Agent remains active if it is already active. No outage occurs. If the Call Agent was not active, it takes activity within 2 seconds. • SOS goes through a warm or restart (approximately 20 seconds for the NTRX51HZ card with the MCPN905 processor and 30 seconds for the NTRX51GZ card with the MPCN765 processor). • Other nodes go active and follow the Call Agent example after losing mate connectivity. • If Site B has the in-service router, the standby CMT server must be brought into service. Consider using this option based on the estimated time to recover the fault or failure of the CS LAN versus time and effort to bring up the cold standby system and recover the high availability (HA) pair afterward. For example, if the time to recover the CS LAN is estimated to be 10 hours, it might not be worth activating the cold standby CMT server or CBM. • If Site A has the in-service router, the standby CBM must be brought into service. See procedure <i>Initiating a switchover to the remote backup server.</i>

Scenario	Response
Optical frame failure at one site	<i>At the site with the failed optical frame:</i> • All nodes lose mate connectivity via Ethernet. • Call Agent FC or GigE call data link connectivity is lost. • WAN backup remains up. • The active Call Agent remains active, but without sync. No outage occurs <i>The remainder of this scenario assumes the active Call Agent is at this site.</i> • If not already active, other nodes co-located with the active Call Agent are expected to go active after losing mate connectivity. If not already inactive, other nodes co-located with the inactive Call Agent are expected to go inactive after losing mate connectivity. (Done without mate connectivity.) <i>At the site with the in-service optical frame:</i> • The inactive Call Agent detects IST loss. For an ERS 8600 CS LAN using OSPF, the Call Agent disables OSPF. For an ERS 8600 CS LAN using Border Gateway Protocol (BGP) or for a third-party CS LAN using either OSPF or BGP, execute manual action to disable routing at the site with the inactive Call Agent. <i>See section Disabling Border Gateway Protocol (BGP) for instructions of disabling and enabling BGP.</i> • Other nodes go inactive and follow the Call Agent example after losing mate connectivity. (Done without mate connectivity.) • USPC detects isolation from the active Call Agent, and takes down SS7 links at the site with the inactive USP. • If Site B has the failed optical frame, the standby CBM must be brought into service at Site A. • If Site A has the failed optical frame, the standby CMT must be brought into service at Site B. Consider using this option based on the estimated time to recover the fault or failure of the CS LAN versus time and effort to bring up the standby system and recover the HA pair afterward. For example, if the time to recover the CS LAN is estimated to be 10 hours, it might not be worth activating the cold standby CMT server or CBM.

Scenario	Response
One site is destroyed in a catastrophic event	<i>At the site that is destroyed:</i> • There is no activity. • The SS7 network takes down the links to the destroyed building. <i>At the site that is not destroyed:</i> • All nodes lose mate connectivity. • The Call Agent loses all mate connectivity, including the backup WAN link, and drops sync. • If the Call Agent is active, it remains active. No outage occurs. If the Call Agent is not active, it takes activity within 2 seconds. • If the Call Agent is inactive, it takes activity within 2 seconds followed by a warm or SOS restart (approximately 20 seconds for the NTRX51HZ card with the MCPN905 processor, and 30 seconds for the NTRX51GZ card with the MCPN765 processor). • Other nodes go active, and follow the Call Agent example after losing mate connectivity. • If Site B was destroyed, initiate a switchover to the standby CBM at Site A. • If Site A was destroyed, initiate a switchover to the standby CMT at Site B.
Active Call Agent card fails at one site	<i>At the site with the failed Call Agent:</i> • All nodes at the site can communicate with their mates. <i>At the site with the mate Call Agent:</i> • All nodes in the site can communicate with their mates. • The (inactive) Call Agent detects loss of connectivity with the mate, detects local and WAN connectivity, takes activity, and restarts the SOS. • Other nodes experience disconnection from the SOS for approximately 20 seconds for the NTRX51HZ card with the MCPN905 processor, and 30 seconds for the NTRX51GZ card with the MCPN765 processor (normal restart behavior)

Scenario	Response
Inactive Call Agent card fails at one site	At the site with the failed inactive Call Agent: - All nodes in the site can communicate with their mates. At the site with the mate Call Agent: - All nodes in the site can communicate with their mates. - The (active) Call Agent detects loss of connectivity with the mate, detects local and WAN connectivity, and stays active. - No SWACT or restart is required.
Recovery from isolation split brain (Active/Inactive)	At both sites: - Once the Call Agents can communicate with their mates, they recognize that both are active. The Call Agent that was inactive backs down, leaving the other Call Agent active. The fallout is to force Unit 0 active and Unit 1 inactive. - Other nodes can communicate with their mates, negotiate activity, and resume normal operations.

System impact of failures

Failures could cause the following system impacts:

- When negotiating activity, the Call Agent preference is always to remain on the same side, if that side supports activity.
- If failover of the Call Agent is necessary, the Call Agent switches activity in less than 2 seconds. When the Callp Application performs a restart, call processing is interrupted for approximately 20 seconds for the NTRX51HZ card with the MCPN905 processor, and 30 seconds for the NTRX51GZ card with the MCPN765 processor (normal restart behavior). Failovers of other Callp nodes follow the Call Agent failover within 2 seconds.
- In Enterprise-only configurations where the solution contains Message Controller (MC) cards connected to Message Switches (MS), ENET and TDM peripherals, the MC and MS cards are co-located in one of the main geographically redundant sites.
- During site isolation, when determining the appropriate master site, preference is given to the site that contains the MC cards. This assumes that the site is able to take activity. If necessary, activity is switched to this side during the activity negotiation.

Recovery scenarios

The following table provides a summary of system responses during recovery.

System response summary

Scenario	Response
Recovery from isolation split brain (Active/Inactive)	- When Call Agents can communicate with their mates, they recognize that both are active. The Call Agent that was inactive before the failure backs down, leaving the other Call Agent active. The fallout is to force Unit 0 active, and Unit 1 inactive. - Other nodes can communicate with their mates, negotiate activity and resume normal operations.
General recovery behavior	All elements: - continually monitor connections with their mates, and with other network elements with which they normally communicate. When connectivity is not present, they continue to monitor the connections for restored connectivity. (The elements continue monitoring regardless of their activity state.) - negotiate activity and services when connectivity recovers, and resume normal operations.

System impact of recovery

Recovery could cause the following system impacts:

- When negotiating activity, the Call Agent preference is always to leave activity on the same side. When recovering to a full system configuration, activity remains on the same unit, without impact.
- During recovery from a split system (caused by incorrect message routing), node activity resolves in a few seconds. Call processing could require up to 15 minutes to recover completely.
- If an inactive call agent is not in service when the IST goes down, OSPF on the Ethernet Routing Switch 8600 is not disabled on the site of the inactive call agent, potentially resulting in failed calls due to misdirected messages. This condition can occur on site recovery after the Ethernet Routing Switch 8600 returns to service and the optical ring is still recovering. In the event that this outage occurs, manually disable OSPF on the Ethernet Routing Switch 8600 or disconnect the links to the WAN on the site of the inactive call agent until it returns to its operational state.

Disabling Border Gateway Protocol (BGP)

This section applies only to CS-LAN routers configured with Ethernet Routing Switch 8600s using BGP.

Similar to protocols OSPF and IS-IS, but providing more scalability and reliability, BGP serves as an interdomain protocol to distribute routing information between endpoints in an Geographic Survivability configuration.

Recall that the CS-LAN consists of dual Ethernet Routing Switch 8600s running as layer 2/3 switches. For redundancy, a pair of upstream routers must be deployed on the Core network edge as the entrance to the CS-LAN.

Nortel supports a square CS-LAN topology configuration, in which each Ethernet Routing Switch 8600 is connected to one of two upstream routers. Each Ethernet Routing Switch 8600 includes two BGP neighbors. One BGP neighbor is the eBGP peer to the wide area network (WAN) Core router. The other BGP neighbor is the iBGP peer to its Ethernet Routing Switch 8600 mate.

Routing policies

The following routing policies control the way in which the CS-LAN routers advertise CS-LAN prefixes to the BGP peers.

- one policy is used during normal operations
- one policy is used during a failure condition

When the system detects a communication failure condition, the routing policy to the external peer (that is, the eBGP peer) changes to control which prefixes are advertised.

A third policy could be required if BGP is used as the routing protocol between the network operations center (NOC) and the CS-LAN.

Nortel recommends using command network to advertise the backup path prefix.

Example

```
ip bgp network 172.30.242.169/29 add
```

Normal operations policy A policy is used on each Ethernet Routing Switch 8600 to redistribute all locally connected subnets to its peers: the iBGP peer (that is, the other Ethernet Routing Switch 8600) and the eBGP peer (the WAN router).

All prefixes to be redistributed are defined in a prefix list. The routing policy uses and applies the prefix list to the BGP peer. On any Ethernet Routing Switch 8600, a routing policy contains the prefix for the default route and other prefix that was advertised originally by the other Ethernet Routing Switch 8600.

Nortel recommends setting the name of the normal operations policy to "RoutesToDistribute."

Normal operations policy example The following example shows entries in a typical normal operations policy prefix list:

Example

```
ip prefix-list "LocalPrefixes: add-prefix 0.0.0.0/0
ip prefix-list "LocalPrefixes: add-prefix 172.16.0.0/20
```

The following example shows a typical definition of a routing policy to be applied to the WAN eBGP peer:

Example

```
ip route-policy "RoutesToDistribute" seq 30 create
ip route-policy "RoutesToDistribute" seq 30 enable
ip route-policy "RoutesToDistribute" seq 30 action permit
ip route-policy "RoutesToDistribute" seq 30 match-network
"LocalPrefixes"
```

Failure condition policy When a failure condition interrupts connectivity between two halves of the CS-LAN, the system must react and change the routing policy. On each Ethernet Routing Switch 8600, a policy is applied to redistribute only the prefix for the backup path to the eBGP peer (that is, the WAN router).

As with the normal operations policy, all prefixes are redistributed and defined in a prefix list. The routing policy uses and applies the prefix list to the BGP peer.

Nortel recommends setting the name of the failure condition policy to "GeoBackupPath."

Failure condition policy example The following example shows an entry in a typical failure condition policy prefix list:

Example

```
ip prefix-list "GeoBackupPath" add-prefix 172.30.242.168
/29
```

The following example shows a typical definition of a routing policy to be applied to the WAN eBGP peer during a failure condition:

Example

```
ip route-policy "GeoBackupPath" seq 30 create
ip route-policy "GeoBackupPath" seq 30 enable
ip route-policy "GeoBackupPath" seq 30 action permit
ip route-policy "GeoBackupPath" seq 30 match-network
"GeoBackupPath"
```

Manual actions to disable and re-enable BGP When a failure occurs at the site with the in-service optical frame, adhere to the following sections to disable and re-enable routing at the site with the inactive call agent.

Disabling BGP during a failure condition When two call control agents (CCA) lose communication with one another through fiber channel/multi-link trunking (MLT), the CCA that does not assume mastership changes the redistribution policy (that is, from "RoutesToDistribute" to "GeoBackupPath"). Only the backup path prefix is advertised to the next hop WAN router.

Enter the following commands to advertise only the backup path prefix to the WAN router:

```
ip bgp neighbor 172.30.252.1 route-policy out "GeoBackupPath"
add
```

```
ip bgp neighbor 172.30.252.1 restart soft-reconfiguration out
```

This action results in a new policy replacing the existing policy. Execute a soft restart of the peering session for this action to take effect.

Re-enabling BGP during a system recovery When the optical outage has been addressed and the master CCA recognizes that communication has been re-established with the backup CCA through fiber channel/MLTs, the backup CCA reverts the routing policy to normal steady-state (that is, from "GeoBackupPath" to "RoutesToDistribute").

Enter the following commands to advertise all CS-LAN prefixes to the WAN router:

```
ip bgp neighbor 172.30.252.1 route-policy out "RoutesToDistribute"
add
```

```
ip bgp neighbor 172.30.252.1 restart soft-reconfiguration out
```

This action results in a new policy replacing the existing policy. Execute a soft restart of the peering session for this action to take effect

Limitations and restrictions

The following limitations and restrictions apply to the Geographic Survivability feature:

- The physical distance between active and standby sites is limited to 120 KM/75 miles.
- Geographic survivability requires the USP - Compact.
- Each site must have a single Ethernet Routing Switch 8600 with dual switch fabric and CPU blades or third-party equivalent.

- Synchronization of data between two CCA blades over GigE links applies to the CS 2100 market with reduced capabilities. This configuration applies just to Enterprise solutions.
- In Enterprise hybrid configurations (with TDM equipment homed at one site), the TDM equipment is not geographically redundant. In determining the master site, preference is given to the TDM side only when either side can support Callp. If necessary, perform a SWACT to the TDM side to allow Callp on that side.
- Because the Call Agent interacts with the Ethernet Routing Switch 8600, the feature requires that each site have only one routing switch and IST links configured between sites. Dual ERS 8600s at each site and SMLT links between sites are not supported. Interactions between the Call Agent and the CS LAN are supported to prevent split brain scenarios (by disabling OSPF) when the ERS 8600s are used for the CS LAN. Upgrades from previous releases in an Enterprise geographic survivable configuration (which have dual ERS 8600's at each site) require that the dual ERS 8600s be migrated to a single ERS 8600 site.
- When a total loss of communication between sites occurs (that is, all three master links are down), the two Call Agents cannot negotiate activity decision. The decision is based on connectivity check from each site the WAN network.
 - While unlikely, it could be possible to have an active/active (split brain) scenario, or an inactive/inactive scenario (no processing).
 - The WAN backup path mitigates the risk of optical ring failure. The WAN connection check helps resolve activity when the backup path is down.
- CS 2000 - Compact supports only a single time zone setting. If the two physical sites are in different time zones, Nortel recommends that the time zone be set to either GMT or the time zone of one of the sites.
- Both Session Server units of a pair are located at the same site. For offices with Message Controllers, Nortel recommends that the Session Servers be located at the same site as the TDM components.
- For maximum redundancy, the WAN backup path must be configured separately from the optical network, as follows:
 - special vlans configured on Ethernet Routing Switch 8600 for backup path use only
 - vlans route over the WAN network instead of over the optical ring
 - vlans are not disabled with OSPF disable
 - alarm generated for lack of connectivity

- Gateways and services node components of CS 2000 - Compact are single units, and are not geographically redundant. Where the nodes are located and how they are connected to the network affects whether they survive a failure. Although the same nodes are supported in configurations with and without Geographic Survivability, there is no change in configuration or connection in the configuration with the Geographic Survivability configuration.

Disabling Ethernet Routing Switch 8600 WAN Edge routing

Purpose

ATTENTION

Perform this procedure immediately after a site failure occurs to limit effects to Call Processing.

This procedure is required to workaround a deficiency in the architecture when the active in-service and SYSB (out of service) GWC send messages to a gateway provisioned off the GWC causing mismatches in the gateway resulting in loss of call processing.

This procedure will impact every element sitting off the ERS 8600.

There are two options for this procedure. The first option will disable all dynamic routing on the chassis and no traffic will be able to leave or enter the VLANs configured on that chassis when using Open Shortest Path First (OSPF). Static routes and Local communication is still possible.

The second option will disable the WAN Edge Interface. All traffic, whether through dynamic or static routes will not be able to leave or enter the chassis.

Prerequisites

None

Procedure

Disabling Ethernet Routing Switch 8600 WAN Edge routing

Step	Action						
<i>At the Ethernet Routing Switch 8600 Workstation</i>							
1	Determine which option you will use.						
	<table border="1"> <thead> <tr> <th>you will use</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>option 1</td> <td>step 2</td> </tr> <tr> <td>option 2</td> <td>step 4</td> </tr> </tbody> </table>	you will use	Do	option 1	step 2	option 2	step 4
you will use	Do						
option 1	step 2						
option 2	step 4						
2	Disable OSPF by typing <code>#config ip ospf disable</code>						

At the Ethernet Routing Switch 8600 Workstation

- Determine which option you will use.

you will use	Do
option 1	step 2
option 2	step 4

- Disable OSPF by typing
`#config ip ospf disable`

and pressing the Enter key.

3 Go to [step 7](#).

4 Identify the WAN Edge VLAN ID by typing

```
#show vlan info basic
```

and pressing the Enter key.

Example response

Vlan Basic						
VLAN ID	NAME	TYPE	STG ID	PROTOCOLID	SUBNETADDR	SUBNETMASK
1	Default	byPort	1	none	N/A	N/A
2	SmartBits4Alteon	byPort	1	none	N/A	N/A
9	FP8600-MLT	byPort	1	none	N/A	N/A
10	IST	byPort	1	none	N/A	N/A
11	OM3500-RPR-cards	byPort	1	none	N/A	N/A
12	WAN-Jun-00	byPort	1	none	N/A	N/A
14	toRTFS-1	byPort	1	none	N/A	N/A
18	Backup Path	byIpSubnet	1	none	172.30.242.168	255.255.255.248
19	Alteon6614	byPort	1	none	N/A	N/A
20	RTF4-NGSS	byPort	1	none	N/A	N/A
50	MCS-CallP	byPort	1	none	N/A	N/A

5 Identify the ports used for WAN Edge connectivity by typing

```
#show vlan info ports <vlan_id>
```

and pressing the Enter key.

where

vlan_id is the VLAN ID obtained in [step 4](#)

Example response

Vlan Port			
VLAN ID	PORT MEMBER	ACTIVE MEMBER	STATIC MEMBER
12	1/2	1/2	

6 Disable the ports used for WAN Edge connectivity by typing

```
#config ethernet <port_range_1> state disable
```

```
#config ethernet <port_range_2> state disable
```

...

```
#config ethernet <port_range_n> state disable
```

and pressing the Enter key.

where

port_range_1 is a range of ports used for WAN Edge (example: 3/1-3/48)

`port_range_2` is a second range of ports used for WAN Edge
(example: 4/1-4/48)

`port_range_n` is the final range of ports used for WAN Edge

7 You have completed this procedure.

—End—

Disabling and re-enabling the router ports on the Ethernet Routing Switch 8600

Purpose

Use this procedure when a failure occurs, such that Sites A and B are isolated from each other, to disable and re-enable the Ethernet Routing Switch 8600 router ports that are connected to the GWC in the inactive site.

Prerequisites

Know the list of router ports connected to the GWCs.

Procedure

Disabling the router ports on the Ethernet Routing Switch 8600

Step	Action

At the Ethernet Routing Switch 8600 Workstation

- 1 Confirm which site has the active Call Agent.
- 2 Confirm that the GWCs in the active site are active.
- 3 Disable the ports to the GWC units on the inactive site by typing


```
#config ethernet <port_range_1> state disable
#config ethernet <port_range_2> state disable
...
#config ethernet <port_range_n> state disable
```

 and pressing the Enter key.
 where
`port_range_1` is a range of ports connected to the GWC
 (example: 3/1-3/48)
`port_range_2` is a second range of ports connected to the
 GWC (example: 4/1-4/48)
`port_range_n` is the final range of ports connected to the GWC
- 4 If you disabled OSPF in the procedure Disabling Ethernet Routing Switch 8600 WAN Edge routing on page 205, re-enable it by typing


```
#config ip ospf enable
```

 and pressing the Enter key.

- 5 If you disabled the ports used for WAN Edge connectivity, re-enable those ports by typing


```
#config ethernet <port_range_1> state enable
#config ethernet <port_range_2> state enable
...
#config ethernet <port_range_n> state enable
```

 and pressing the Enter key.

where

port_range_1 is a range of ports used for WAN Edge obtained in step 5 of the procedure Disabling Ethernet Routing Switch 8600 WAN Edge routing

port_range_2 is a second range of ports used for WAN Edge obtained in step 5 of the procedure Disabling Ethernet Routing Switch 8600 WAN Edge routing

port_range_n is the final range of ports used for WAN Edge obtained in step 5 of the procedure Disabling Ethernet Routing Switch 8600 WAN Edge routing
- 6 Check the time by typing


```
#date
```

 and pressing the Enter key.

Example response

```
local time:  THU MAR 31 17:32:57 2005 EST
hardware time: THU MAR 31 22:32:57 2005 UTC
```
- 7 Allow at least one minute to pass to ensure that internal GWC audits set the units to inactive.
- 8 Check the time by typing


```
#date
```

 and pressing the Enter key.

Example response

```
local time:  THU MAR 31 17:33:59 2005 EST
hardware time: THU MAR 31 22:33:59 2005 UTC
```
- 9 If the inactive building is accessible, verify the inactive GWC units have gone inactive.
 - a. Connect the terminal to the console port on the GWC.
 - b. Enter PMDEBUG and perform the 'T', 'N', and 'A' commands.
 - c. Confirm that the state is inactive. If not, repeat [step 3](#) through [step 8](#) on those ports.

- 10** Re-enable the ports to the GWC units in the inactive site by typing
- ```
#config ethernet <port_range_1> state enable
#config ethernet <port_range_2> state enable
...
#config ethernet <port_range_n> state enable
```
- and pressing the Enter key.
- where
- port\_range\_1** is a range of ports connected to the GWC  
(example: 3/1-3/48)
- port\_range\_2** is a second range of ports connected to the  
GWC (example: 4/1-4/48)
- port\_range\_n** is the final range of ports connected to the GWC
- 11** You have completed this procedure.

---

—End—

---

## Installing the remote backup server

### Target

Use this procedure to install the remote backup server for Geographic Survivability. Backing up the remote server provides a standby backup system which is ready to provide service if the primary system is unavailable for an extended period of time. The remote server can assume the identity of the primary server with data and files accurate to the last synchronization.

### Prerequisites

You must have the root user ID and password to perform this procedure.

Use the following table to ensure that you have the information ready for input during this procedure.

| System Variable                                                                                                       | Actual value |
|-----------------------------------------------------------------------------------------------------------------------|--------------|
| Hostname                                                                                                              |              |
| IP address (remote backup server)                                                                                     |              |
| Netmask                                                                                                               |              |
| Router (default gateway IP)                                                                                           |              |
| DNS (Yes, No)                                                                                                         |              |
| Unit 0 IP address (IP of primary cluster unit 0)                                                                      |              |
| Daily backup (up to four) in format: <b>HH:MM</b><br>where<br><b>HH</b> = hours (00-23)<br><b>MM</b> = minute (00-59) |              |
| DNS domain                                                                                                            |              |
| IP address (DNS server[s])                                                                                            |              |
| DNS search domain(s)                                                                                                  |              |

DNS variables apply only when a DNS server has been configured.



**Action****Installing the remote backup server on a Geographic Survivability standby server****At your workstation or the remote server console****Step Action**

- 1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server.

| If you want to log in by means of | Do                                                                                                 |
|-----------------------------------|----------------------------------------------------------------------------------------------------|
| ssh                               | Type <code>ssh -l root &lt;server&gt;</code> and press the Enter key. Go to <a href="#">step 2</a> |
| telnet                            | Type <code>telnet &lt;server&gt;</code> and press the Enter key. Go to <a href="#">step 2</a>      |
| the remote server console         | <a href="#">step 2</a>                                                                             |

where

**server** is the name of the N240 server.

- 2 Log in to the server through the console (port A) and when prompted, enter the root user ID and password.
- 3 Bring the system to the {0} OK prompt by typing:  

```
init 0
```
- 4 Enter the following command to verify that the auto-boot option is set to true.  

```
{0} ok printenv auto-boot?
```

If it is set to false, enter the following command.  

```
{0} ok setenv auto-boot?=true
```
- 5 Insert disk 1 of the SPFS0\*\* (090) CD set into the DVD drive on the standby unit.
- 6 Install the remote backup server for Geographic Survivability.  

```
{0} OK boot cdrom - rbackup
```
- 7 Type OK and press Enter to acknowledge restriction on your use of the software.
- 8 Select the rbackup server profile for the system.
- 9 Enter no to not select the default settings. The N240 server must be connected to the network and must have access to the default

gateway. This allows you to enter the server's settings for the installation.

- 10** Enter site-specific information in response to the following prompts. (Refer to the information entered in the table at the beginning of this procedure.)

Enter the hostname for this system.  
 Enter the IP address for the remote backup server.  
 Enter the subnet mask for this network.  
 Enter the IP address for this network's router.  
 Enter the timezone for this system.

The default timezone is US/Eastern. Enter ? for a list of supported time zones.

Will this system use DNS?

- 11** Enter yes or no. If you answer yes, you are prompted for the DNS domain name, name server IP addresses, and the search domains. You can enter several name servers and search domains. To stop entry, enter a blank line

- 12** Enter OK to accept current settings.

The installation of the first CD takes approximately 25 minutes. No action is required until the following system response displays:

Media:

1. CD/DVD
2. Network File System
3. Skip

Media[1]:

- 13** Enter 1 and then press Enter to select CD/DVD as the Media type for the installation of Solaris 9.

The system ejects disk 1 CD automatically.

- 14** Remove SPFS disk 1 CD from the server.

- 15** Insert SPFS disk 2 CD (the second SPFS CD in the set of 3 disks) into the DVD drive and then press Enter.

This step takes approximately 15 minutes to complete.

- 16** Enter 2 to continue with the installation.

- 17** Press Enter to reboot the system.

The installation of the Solaris Patches starts after the system reboots.

- 18** The installation of the second CD takes approximately 20 minutes. No action is required until the system prompts you to enter the third CD.
- Done Installing Solaris Patches...  
Insert SSPFS Deadstart CD ROM Disk 3 in the Drive.  
Type "ok" when Ready.
- 19** Remove SPFS disk 2 CD from the server.
- 20** Insert SPFS disk 3 CD (the third SPFS CD in the set of 3 disks) into the DVD drive.
- 21** Enter OK and then press Enter to start the installation of the third CD. The installation of the third CD takes approximately 50 minutes. You could be required to press Enter to reprint the login prompt to the screen after the reboot.
- <Hostname> console login:
- 22** Log in to the server using the root user ID and password.
- 23** Remove SPFS disk 3 CD from the server.
- `eject cdrom`
- 24** Enter the command line interface (CLI) tool.
- `cli`
- 25** Enter the number next to the Configuration option in the menu.
- 26** Enter the number next to the Succession Element Configuration option in the menu.
- 27** Enter the number next to the PSE Application Configuration option in the menu.
- 28** Enter the number next to the Configure PSE option in the menu.
- 29** Enter the primary/cluster IP address of CS 2000 Management Tools server. This is the address of the NPM server.
- 30** Enter Y to confirm the IP address.
- Ignore the following error message if it displays.  
Can't configure PSE on remote backup unit to enable NPM
- 31** Enter X to exit each level until you have exited from the cli tool.
- 32** Start the PSE server.
- `# pse start`

- 33** Verify that the server has started. If the server does not start, contact your next level of support.
- # pse status**
- 34** If an SPFS MNCL CD is to be installed, refer to the documentation included with the CD for complete installation instructions.
- 35** Enter NPM on the CS 2000 Management Tools server and follow patching procedures to apply all relevant patches.

---

**—End—**

---

## Scheduling automatic backups on the remote server

### Target

Use this procedure to schedule automatic backups to the remote server. Backing up the primary server provides a standby backup system which is ready to provide service if the primary system is unavailable for an extended period of time. The remote server can assume the identity of the primary server with data and files accurate to the last synchronization.

#### ATTENTION

This procedure is for use with Geographic Survivability only.

### Action

#### Scheduling automatic backups of the remote server

##### At your workstation or the remote server console

| Step | Action                                                                                                    |
|------|-----------------------------------------------------------------------------------------------------------|
| 1    | Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server. |



| If you want to log in by means of | Do                                                                            |
|-----------------------------------|-------------------------------------------------------------------------------|
| ssh                               | Type ssh -l <server> and press the Enter key.<br>Go to <a href="#">step 2</a> |
| telnet                            | Type telnet <server> and press the Enter key.<br>Go to <a href="#">step 2</a> |
| the remote server console         | <a href="#">step 2</a>                                                        |

where

**server** is the name of the N240 server.

- 2 When prompted, enter the root password.
- 3 Start the command line interface tool by entering:  
`cli`
- 4 Select the Configuration menu.  
The system displays the Configuration menu.
- 5 Select the Remote Backup option.

Response:

Remote Backup Configuration

```

1 - rbackup_display (Display Remote Backup Configurati
on)
2-rbackup_config (Remote Backup Configuration)
3-rbackup_exec (Execute Remote Backup Now)
4 - rbackup_cancel (Cancel Running Remote Backup)
X-exit

```

**6** Select:

```
2-rbackup_config (Remote Backup Configuration)
```

The system responds with the IP address of the primary server that is currently configured as the remote server, and the times that are currently configured for automatic backups.

**7** Enter the unit 0 IP address of the primary server to be backed up.

```
<nnn.nnn.nnn.nnn> is alive
```

where

**nnn.nnn.nnn.nnn** is the IP address that you entered.

**8** Use the following table to determine your next step.

| If the system                             | Do                                      |
|-------------------------------------------|-----------------------------------------|
| prompts you to accept the ssh key         | Enter yes. Go to <a href="#">step 9</a> |
| does not prompt you to accept the ssh key | Go to <a href="#">step 9</a>            |

```
Enter a time for a daily backup to occur (HH:MM):
```

where

**HH** is hours. Valid values are 00 to 23.

**MM** are minutes. Valid values are 00 to 59.

**9** Enter the first time for a daily backup to occur

You can configure up to four times for daily backup to occur.

Response:

```
Enter a second time for a daily backup to occur (HH:MM)
or enter "x" to stop provisioning backup times:
```

**10** Use the following table to determine your next step

| If you                                                         | Do                                                                             |
|----------------------------------------------------------------|--------------------------------------------------------------------------------|
| want to enter another time for a remote backup to occur        | Enter a second time for a daily backup to occur. Go to <a href="#">step 11</a> |
| do not want to enter another time for a remote backup to occur | Enter x. Go to <a href="#">step 13</a>                                         |

**11** Use the following table to determine your next step

| If you                                                         | Do                                                                            |
|----------------------------------------------------------------|-------------------------------------------------------------------------------|
| want to enter another time for a remote backup to occur        | Enter a third time for a daily backup to occur. Go to <a href="#">step 12</a> |
| do not want to enter another time for a remote backup to occur | Enter x. Go to <a href="#">step 13</a>                                        |

**12** Use the following table to determine your next step

| If you                                                         | Do                                                                             |
|----------------------------------------------------------------|--------------------------------------------------------------------------------|
| want to enter another time for a remote backup to occur        | Enter a fourth time for a daily backup to occur. Go to <a href="#">step 13</a> |
| do not want to enter another time for a remote backup to occur | Enter x. Go to <a href="#">step 13</a>                                         |

**13** Use the following table to determine your next step

| If you want to    | Do                                                                 |
|-------------------|--------------------------------------------------------------------|
| commit changes    | Go to <a href="#">step 14</a>                                      |
| exit              | Enter quit. Go to <a href="#">step 15</a>                          |
| re-enter settings | Enter anything other than ok or quit. Go to <a href="#">step 9</a> |

**14** Enter

ok

=== "rbackup\_config" completed successfully

**15** Exit the Remote Backup Configuration level.

x

—End—

## Viewing configuration information for remote server backups

### Target

Use this procedure to view the current configuration information for remote server backups. The system displays the IP address of the target system and the times in which automatic backups of the target system will occur.

#### ATTENTION

This procedure is for use with Geographic Survivability only.

### Action

#### Viewing configuration information for remote server backups

##### At your workstation or the remote server console

| Step | Action                                                                                                    |
|------|-----------------------------------------------------------------------------------------------------------|
| 1    | Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server. |



| If you want to log in by means of | Do                                                                                               |
|-----------------------------------|--------------------------------------------------------------------------------------------------|
| ssh                               | Type <code>ssh -l &lt;server&gt;</code> and press the Enter key.<br>Go to <a href="#">step 2</a> |
| telnet                            | Type <code>telnet &lt;telnet&gt;</code> and press the Enter key.<br>Go to <a href="#">step 2</a> |
| the remote server console         | <a href="#">step 2</a>                                                                           |

where

**server** is the name of the N240 server.

- 2 Start the command line interface tool by entering:

```
cli
```

The system responds by displaying a menu.

- 3 Select the Configuration menu.

The system displays the Configuration menu.

- 4 Select the Remote Backup option.

Response:

```
Remote Backup Configuration
```

```
1-rbackup_display (Display Remote Backup Configuration)
```



```
2-rbackup_config (Remote Backup Configuration)
3-rbackup_exec (Execute Remote Backup Now)
4 - rbackup_cancel (Cancel Running Remote Backup)
X-exit
```

**5**      **Select**

```
1-rbackup_display (Display Remote Backup Configuration)
```

**Response:**

Current settings:

Target system is: <nnn.nnn.nnn.nnn>

Back up times are: <Time 1>...<Time n>

where

<nnn.nnn.nnn.nnn> is the IP address of the remote server

where

<Time 1>...<Time n> is the set of times at which automated backups occur.

**6**      **Exit the Remote Backup Configuration level by typing:**

**x**

---

**—End—**

---

## Performing a manual backup of the target server

### Target

Use this procedure to perform a manual backup of the primary server. Backing up the primary server provides a standby backup system which is ready to provide service if the primary system is unavailable for an extended period of time. The remote server can assume the identity of the primary server with system configuration data and files accurate to the last synchronization.

#### ATTENTION

This procedure is for use with Geographic Survivability only.

### Action

#### Performing a manual backup of the remote server

##### At your workstation or the remote server console

| Step | Action                                                                                                    |
|------|-----------------------------------------------------------------------------------------------------------|
| 1    | Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server. |



| If you want to log in by means of | Do                                                                                                 |
|-----------------------------------|----------------------------------------------------------------------------------------------------|
| ssh                               | Type <code>ssh -l root &lt;server&gt;</code> and press the Enter key. Go to <a href="#">step 2</a> |
| telnet                            | Type <code>telnet &lt;server&gt;</code> and press the Enter key. Go to <a href="#">step 2</a>      |
| the remote server console         | <a href="#">step 2</a>                                                                             |

where

**server** is the name of the N240 server.

- When prompted, enter the root password.
- Start the command line interface tool.  
`cli`  
The system responds by displaying a menu.
- Select the Configuration menu.  
The system displays the Configuration menu.
- Select the Remote Backup option.

Remote Backup Configuration

1-rbackup\_display (Display Remote Backup Configuration)  
2-rbackup\_config (Remote Backup Configuration)  
3-rbackup\_exec (Execute Remote Backup Now)  
4 - rbackup\_cancel (Cancel Running Remote Backup)  
X-exit

**6** Select

3-rbackup\_exec (Execute Remote Backup Now)

**7** An automatic backup is made.

Pressing 4 during execution of the backup halts the process and performs necessary clean-up operations.

**8** Exit the Remote Backup Configuration level.

x

---

—End—

---

## Viewing logs from a remote backup

### Target

Use this procedure to view logs associated with a backup of the remote server. Logs are created during automatic and manual backups of the remote server.

### Action

#### Viewing logs from a remote backup

##### At your workstation or the remote server console

| Step | Action                                                                                                    |
|------|-----------------------------------------------------------------------------------------------------------|
| 1    | Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server. |



| If you want to log in by means of | Do                                                                                               |
|-----------------------------------|--------------------------------------------------------------------------------------------------|
| ssh                               | Type <code>ssh -l &lt;server&gt;</code> and press the Enter key.<br>Go to <a href="#">step 2</a> |
| telnet                            | Type <code>telnet &lt;server&gt;</code> and press the Enter key.<br>Go to <a href="#">step 2</a> |
| the remote server console         | <a href="#">step 2</a>                                                                           |

where

**server** is the name of the N240 server.

- 2 Enter:  
`less /var/adm/messages`  
The system responds by displaying the contents of the log file.
- 3 The procedure is complete.

---

—End—

---

## Initiating a recovery back to the cluster

### Prerequisites

It is expected that the primary server is in the shut-down mode.

If the server was previously a CBM and contains billing files not already sent to a down-stream billing server, using the cluster server, these files should be copied to a downstream server prior to performing ["Installing the remote backup server" \(page 604\)](#). Otherwise these files and the billing records will be lost. Contact next level of support for assistance

### Target

When completed, this procedure will restore the HA cluster and backup server.

### Action

#### Initiating a recovery back to the cluster At your workstation

##### Initiating a recovery back to the cluster

| Step | Action                                                                                                                                                                                                                                                                                      |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Follow the <a href="#">"Installing the remote backup server" (page 604)</a> procedure.<br><br>In this case, the unit0 server of the cluster is used as a remote backup server. Use the same hostname and IP address that was used to configure the remote backup server in the first place. |
| 2    | Follow the <a href="#">"Scheduling automatic backups on the remote server" (page 608)</a> procedure.<br><br>Use only one automated schedule and make sure to select a time that will not be invoked shortly.                                                                                |
| 3    | Follow the <a href="#">"Performing a manual backup of the target server" (page 613)</a> procedure.                                                                                                                                                                                          |
| 4    | Bring down the machine currently active by following the procedure 'Two-server (cluster) configuration' in chapter 'Shutting down an SPFS-based server' in the document <i>ATM/IP Solution-level Fault Management</i> NN10408-900.                                                          |
| 5    | Follow the <a href="#">"Initiating a switch over to the remote backup server" (page 618)</a> procedure to bring the services back to unit0 of the cluster.                                                                                                                                  |

- 6 Follow the 'Cloning the image of one server in a cluster to the other server' procedure in the document *ATM/IP Solution-level Security and Administration* NN10402-600.
- 7 If the server was previously a CBM and contains billing files not already sent to a down-stream billing server, using the remote backup server, these files MUST be copied to a downstream server prior to performing "[Installing the remote backup server](#)" (page 604). Otherwise these files and the billing records will be lost. Contact next level of support for assistance.
- 8 Reinstall the backup server following the "[Installing the remote backup server](#)" (page 604) procedure.
- 9 Reconfigure the backup server following the "[Scheduling automatic backups on the remote server](#)" (page 608) procedure.
- 10 The procedure is complete.

---

—End—

---

## Initiating a switch over to the remote backup server

### Prerequisites

Prior to starting this procedure, shut down the Cluster machine.

Refer to section *Two-server (cluster) configuration* in chapter *Shutting down an SPFS-based server* in document *ATM/IP Solution-level Fault Management* NN10408-900.

The user must be logged in as the root user in order to initiate the switch command.



#### CAUTION

If configuration, provisioning, patching or other “write”-type operations occurred since the last remote backup, the remote backup system can be out of sync compared to the data in network elements and/or the primary OAM system.

Take actions before initiating the switchover to a remote backup OAM server (that is, response to a geographic or other prolonged outage of the primary OAM system) to halt or prevent “write”-type operations by OSSs and operations personnel until an in-sync status is achieved.

When initiating a switchover to a remote backup OAM server, do not execute configuration, provisioning, patching or other “write”-type operations through the remote backup OAM system until out-of-sync conditions are cleared.

### Target

When completed, this procedure reboots the remote backup server as the unit0 of the cluster.

### Action

#### Initiating a switch over to the remote backup server

##### At your workstation

| Step | Action |
|------|--------|
|------|--------|

- |   |                                                                                                                             |
|---|-----------------------------------------------------------------------------------------------------------------------------|
| 1 | <p>Log in to the server by typing</p> <pre>&gt; telnet &lt;server&gt;</pre> <p>and pressing the Enter key.</p> <p>where</p> |
|---|-----------------------------------------------------------------------------------------------------------------------------|

**server** is the IP address or host name of the SPFS-based remote backup server.

- 2 When prompted, enter your user ID and password.
- 3 Change to the root user.  
`su - root`
- 4 When prompted, enter the root password.
- 5 Invoke the switch by typing:  
`$ /opt/sspfs/rbks/switch`
- 6 When ready, indicate you want to proceed by typing:  
`OK`

---

—End—

---



## Communication Server 2000 Management Tools Geographic Survivability

### Overview

The Communication Server 2000 (CS 2000) Management Tools configuration for Geographic Survivability for the SN08 release consists of two CS 2000 Management Tools active servers at site A which are commissioned as a local HA cluster and one CS 2000 Management Tools (hitherto referred to as CKMT) server at site B which acts as a standby. The standby server is brought into service using a recovery procedure if there is a catastrophic site outage at site A. This section contains the CS 2000 Management Tools manual recovery procedure for disaster recovery by switching activity between sites in the event of a catastrophic fault condition on the CKMT cluster.

### Terminology

The following table defines the terms used in the CKMT Geographic Survivability procedures:

| Term          | Definition                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CKMT HA       | The high-availability CKMT product which consists of two Sun Netra 240 servers both commissioned with the CKMT SSPFS profile, and installed with cluster=ON.                                                                                                                                                                                                                          |
| CKMT for GS   | An additional standby server located at a different physical location. This unit is prepared for implementation of the manual recovery procedure in the event of a catastrophic fault condition at the local, main CKMT HA site.                                                                                                                                                      |
| Cluster       | Two interconnected redundant units. One unit is active, and the other is inactive. The active unit has applications in-service (INSV), and ensures that the inactive unit replicated filesystems are updated in real-time. In the event of an automatic cluster failover, the currently inactive unit becomes the active unit and the formerly active unit becomes the inactive unit. |
| Sites A and B | The two geographic survivability sites. Each site has duplicate configured hardware, with the exception of the CBM 850 and CKMT units.                                                                                                                                                                                                                                                |
| CKMT HA u0    | Unit 0 of the CKMT cluster at site A. One half of the cluster configuration formed by units A0 and A1. This unit is the mate of CKMT HA u1.                                                                                                                                                                                                                                           |
| CKMT HA u1    | Unit 1 of the CKMT cluster at site A. One half of the cluster configuration formed by units A0 and A1. This unit is the mate of CKMT HA u0.                                                                                                                                                                                                                                           |

| Term               | Definition                                                                                                                                                                |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CKMT u0            | The single standby CKMT server at site B. Although clustering is configured on this unit because it will be restored from CKMT HA u0 or u1, it does not have a mate unit. |
| Active CKMT unit   | The CKMT HA unit at site A (either CKMT HA u0 or CKMT HA u1) which has the application states as in-service (INSV).                                                       |
| Inactive CKMT unit | The CKMT HA unit at site A (either CKMT HA u0 or CKMT HA u1) which has the application states as STANDBY.                                                                 |

### Distribution of OAMP platform

The components in an OAMP platform are distributed as follows: The scenarios assume redundant configurations are located in two separate buildings:

- CKMT HA - The CKMT and Integrated Element Management Systems (IEMS) high-availability (HA) server pairs are located at site A.
- CBM 850 HA - The Core and Billing Manager (CBM) high-availability server pair are located at site B.
- Standby Sun servers - In the event of a catastrophic fault condition at one site, the standby Sun servers are brought into service through the manual recovery procedure. The Sun servers are positioned as follows:
  - The CBM 850 standby server is located in the Centralized Operations Administration and Maintenance (COAM) frame at site A.
  - The CS 2000 Management Tools/IEMS standby server is located in the COAM frame at site B.
  - The standby server is brought into service using a manual recovery procedure if there is a total loss of connectivity at the other site.

All three servers need to be able to connect to the OAMP LAN. However, if the servers at both site locations are permitted to function on the OAMP LAN at the same time, networks problems with clustering and duplicate IP addresses will occur.

### Required backups on the CKMT servers

There are two types of required backups needed to restore the standby server to functionality following a catastrophic fault condition:

- a full filesystem backup that makes a copy of all the filesystems on the server with the exception of the Oracle filesystem. The OS and third party software application configuration data is captured on DVD-RW discs. The amount of data on the server determines the number of DVD-RW discs required to complete the backup.

- a data-only backup for the data stored in the Oracle database and other application-specific data.

## Prerequisites

Adhering to the prerequisites in this section and the subsequent procedures will help ensure successful completion of geographical survivability manual recovery while holding the maximum out-of-service time for the failover to approximately four hours.

If the documented procedures are not adhered to strictly, longer restoration times will result. Failure to perform the following tasks properly will result in problems:

- full filesystem backup and data backup on the CKMT cluster
- full filesystem restore and data restore to the standby CKMT/IEMS server
- ensuring the CKMT cluster at site A (CKMT HA u0 and u1) and the standby CKMT unit in site B (CKMT u0) are not on-line at the same time

Nortel recommends that you perform a full filesystem backup before and after every install, upgrade, or patch application to the CKMT server. The application data in the Oracle database is not automatically backup up, therefore, Nortel recommends daily backups of this data for the best recovery outcomes.

## Communication Server 2000 Management Tools geographic survivability

The following procedures contain information for OA&M auto backup and accelerated restore capability:

- ["Installing the remote backup server" \(page 603\)](#)
- Scheduling automatic backups on the remote server
- ["Viewing configuration information for remote server backups" \(page 611\)](#)
- ["Performing a manual backup of the target server" \(page 613\)](#)
- ["Viewing logs from a remote backup" \(page 615\)](#)
- Initiating a recovery back to the cluster
- ["Initiating a switch over to the remote backup server" \(page 618\)](#)

## 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

| Step              | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>At the PDC</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 1                 | <p>When possible after detection of the power outage, remove all the fuse holders for the following:</p> <ul style="list-style-type: none"> <li>line concentrating equipment (LCE) talk batteries</li> <li>trunk module equipment (TME) talk batteries</li> <li>PDC filter fuses from the correct PDCs</li> </ul> <p><b>Note:</b> 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.</p> |



#### 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. 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.

- 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               | step 3 |
| -60 V dc               | step 4 |

- 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    | step 6 |
| no power retrieval | step 5 |

- 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    | step 6 |
| no power retrieval | step 5 |

### ***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.

| If uses that blew are | Do                      |
|-----------------------|-------------------------|
| 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:

| If the replacement fuse is          | Do                      |
|-------------------------------------|-------------------------|
| 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.

| If the switch has          | Do                      |
|----------------------------|-------------------------|
| a remote oscillator shelf  | <a href="#">step 16</a> |
| 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.

| If the switch is      | Do                      |
|-----------------------|-------------------------|
| 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.

| If all the power converters have | Do                      |
|----------------------------------|-------------------------|
| 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**



**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.

- 27 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



**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](#).)

- 32** 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> |
| 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)  
 yyyy 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.
- | If recover of additional IOCs and MAP terminals is | Do      |
|----------------------------------------------------|---------|
| not complete                                       | step 45 |
| complete                                           | step 56 |
- 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             | step 47 |
| an IOM             | step 51 |
- 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:

| If the PDC power to the PM frames restores | Do      |
|--------------------------------------------|---------|
| correctly                                  | step 72 |
| not correctly                              | step 57 |

- 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

**WARNING****Possible equipment damage or extended service interruption**

Use correct fuses. When replacing fuses in the PDC, make sure that the amperage of the fuses is correct. The fuse amperage must match the amperage marked on the PDC.

- 58** 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

[step 62](#)

not blown

[step 72](#)

- 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.

| If the fuse alarm indicator lamp lit | Do                       |
|--------------------------------------|--------------------------|
| 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.

| If the FSP has   | Do      |
|------------------|---------|
| fuses            | step 75 |
| circuit breakers | step 80 |

- 75 Determine if the power converters have Power Reset buttons or Power Reset switches.

| If the power converters have | Do      |
|------------------------------|---------|
| Power Reset buttons          | step 76 |
| Power Reset switches         | step 78 |

- 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.

| If all the Converter Fail lights are | Do      |
|--------------------------------------|---------|
| off                                  | step 82 |
| not off                              | step 83 |

- 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                                  | <a href="#">step 82</a> |
| not off                              | <a href="#">step 83</a> |

- 82** Determine if all PM frames turn on.

| If all the PM frames turn on | Do                      |
|------------------------------|-------------------------|
| yes                          | <a href="#">step 87</a> |
| no                           | <a href="#">step 83</a> |

- 83** Determine if a try made to power up the remaining PM frames.

| If power up has  | Do                      |
|------------------|-------------------------|
| not tried        | <a href="#">step 84</a> |
| tried and failed | <a href="#">step 86</a> |

- 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).



#### 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.

- 91** 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 | <a href="#">step 94</a> |
| 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 | <a href="#">step 97</a> |

| If the state of DLOG recording volumes is                                                  | Do                      |
|--------------------------------------------------------------------------------------------|-------------------------|
| any volume is IN ERROR, as indicated under the REGULAR VOLUME(S) header on the MAP display | <a href="#">step 96</a> |
| all volumes are READY, as indicated under the REGULAR VOLUME(S) header on the MAP display  | <a href="#">step 98</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.

- 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.

| If the status of the switch recovery is                     | Do                       |
|-------------------------------------------------------------|--------------------------|
| 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.

---

—End—

---

## 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

| Step | Action |
|------|--------|
|------|--------|

##### *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_
InPrG Comp Fail Pend InPrG Comp Fail Pend
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                                | step 111                |
| 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.

---

—End—

---

---

## 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

---

| Step | Action |
|------|--------|
|------|--------|

---

##### *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. |
|---|------------------------------------|

---

—End—

---

# 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

| Step | Action |
|------|--------|
|------|--------|

*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.

| If all the power converters have | Do                     |
|----------------------------------|------------------------|
| 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_
InPrG Comp Fail Pend InPrG Comp Fail Pend
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.

| the status of any network element is | Do                      |
|--------------------------------------|-------------------------|
| failed                               | <a href="#">step 11</a> |
| pending                              | <a href="#">step 9</a>  |
| another status                       | <a href="#">step 13</a> |

- 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.

---

—End—

---

## 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

| Step                                                                                                                                                                                                                                                                       | Action                                                                                                              |              |    |                            |                        |                                |                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|--------------|----|----------------------------|------------------------|--------------------------------|------------------------|
| <b>At the PDC</b>                                                                                                                                                                                                                                                          |                                                                                                                     |              |    |                            |                        |                                |                        |
| 1                                                                                                                                                                                                                                                                          | Determine if PDC has power restored to the LPP(s).                                                                  |              |    |                            |                        |                                |                        |
| <table border="1"> <thead> <tr> <th>If PDC has</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>power restored to the LPPs</td> <td><a href="#">step 5</a></td> </tr> <tr> <td>not power restored to the LPPs</td> <td><a href="#">step 2</a></td> </tr> </tbody> </table> |                                                                                                                     | 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> |
| 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.                                                                            |              |    |                            |                        |                                |                        |
| <table border="1"> <thead> <tr> <th>If there are</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>blown fuses</td> <td><a href="#">step 3</a></td> </tr> <tr> <td>no blown fuses visible</td> <td><a href="#">step 4</a></td> </tr> </tbody> </table>                      |                                                                                                                     | If there are | Do | blown fuses                | <a href="#">step 3</a> | no blown fuses visible         | <a href="#">step 4</a> |
| 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.                                                                                            |              |    |                            |                        |                                |                        |
| <p><b>Note:</b> If fuses blow repeatedly, call your next level of support for help.</p> <p>When PDC power restores to the LPPs, continue this procedure at <a href="#">step 5</a>.</p>                                                                                     |                                                                                                                     |              |    |                            |                        |                                |                        |
| 4                                                                                                                                                                                                                                                                          | Call the personnel responsible for maintaining power at your site, or refer to your next level of support for help. |              |    |                            |                        |                                |                        |
| <p>When PDC power restores to the LPPs, continue this procedure at <a href="#">step 5</a>.</p>                                                                                                                                                                             |                                                                                                                     |              |    |                            |                        |                                |                        |
| 5                                                                                                                                                                                                                                                                          | Locate the LPPs for recovery.                                                                                       |              |    |                            |                        |                                |                        |
| <b>At the LPP cabinet</b>                                                                                                                                                                                                                                                  |                                                                                                                     |              |    |                            |                        |                                |                        |

**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 handling circuit cards. A wrist strap protects the cards against damage caused by static electricity.

- 6 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 [step 5](#) through [step 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 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:
```

**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> |
| 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.

---

**—End—**

---

## 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

| Step                         | Action                                                                                                                                                                                                                                      |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>At the SDM frame</i>      |                                                                                                                                                                                                                                             |
| 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.                                                                                                                                                                          |
| <i>At the VT100 terminal</i> |                                                                                                                                                                                                                                             |
| 3                            | Login as root and type<br># <code>sdmmtc</code><br>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.<br><br><b>Note:</b> 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.                                                                                                                                                                                                          |
| —End—                        |                                                                                                                                                                                                                                             |

---

## 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:

- IEMS
- 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

| Step  | Action                                                                                                                                                                                                                                                                                                                    |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.<br><br>Once power is restored to the server they will recover on their own. |
| 3     | You have completed this procedure.                                                                                                                                                                                                                                                                                        |
| —End— |                                                                                                                                                                                                                                                                                                                           |

## Powering up the Border Control Point Manager

### Purpose of this procedure

Use the following procedure to power up the Border Control Point Manager. The Border Control Point 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 Border Control Point Manager.

### Prerequisites

None

### Action

#### Powering up the Border Control Point Manager

| Step | Action |
|------|--------|
|------|--------|

##### *At the frame housing the Border Control Point 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.

—End—

## 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

| Step                                        | Action                                                                                                                                                           |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b><i>At the SAMF frame</i></b>             |                                                                                                                                                                  |
| 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). |
| <b><i>At the CS 2000 SAM21 Manager</i></b>  |                                                                                                                                                                  |
| 2                                           | If necessary, unlock the previously active Shelf Controller (SC).<br>Refer to Unlocking a SAM21 Shelf Controller.                                                |
| 3                                           | If necessary, unlock the previously inactive SC.<br>Refer to Unlocking a SAM21 Shelf Controller.                                                                 |
| 4                                           | If necessary, unlock any remaining locked cards on the SAM21 other than the GWC cards.                                                                           |
| <b><i>At the CS 2000 GWC Manager</i></b>    |                                                                                                                                                                  |
| 5                                           | If necessary, unlock all previously active GWC cards.<br>Refer to Unlock a GWC card.                                                                             |
| 6                                           | If necessary, unlock all previously inactive GWC cards.<br>Refer to Unlock a GWC card.                                                                           |
| <b><i>At the Policy Controller unit</i></b> |                                                                                                                                                                  |

- 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"](#) (page 659).
- 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"](#) (page 659).

**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 - Trunks unit](#).
- 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](#). 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 - Trunks unit](#).
- 12 From the active unit, verify that the SIP Gateway application databases on the both units have synchronized using procedure [Verify synchronization status](#)
- 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.

---

—End—

---



## Power-On and boot a Policy Controller unit

### Purpose of this procedure

This procedure is used to power on a Policy Controller unit that has been installed as a replacement, or was shutdown for any other reason.

This procedure may be used as a standalone task or as part of a higher level activity such as part of a dead office recovery activity or software upgrade activity.

### Limitations and restrictions

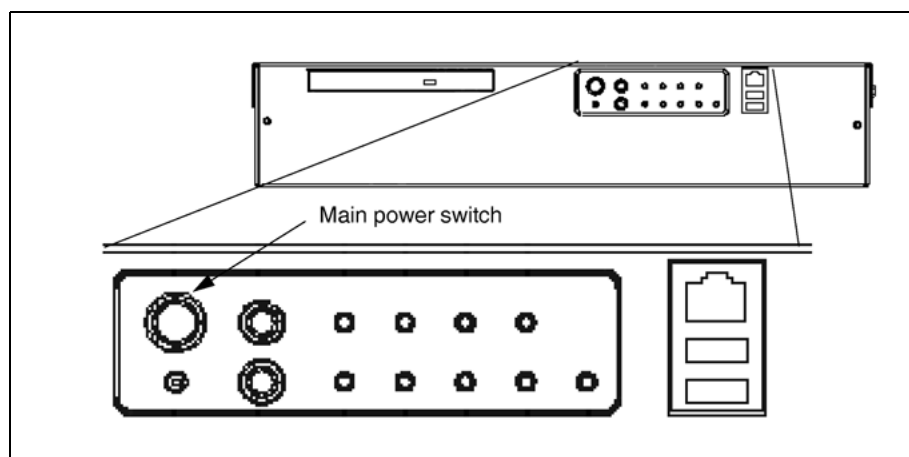
There are no restrictions on using this procedure.

### Prerequisites

If the unit was a replacement unit recently installed, ensure that all power cabling connections have been properly installed and secured at the rear of the chassis and SAM-F frame.

### Action

| Step                                                           | Action                                                                                               |
|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b><i>At the front panel of the Policy Controller unit</i></b> |                                                                                                      |
| 1                                                              | If necessary, power on the Policy Controller using the main power switch located on the front panel. |
| 2                                                              | If desired, at the Policy Controller console, monitor the boot progress of the unit.                 |
| 3                                                              | The procedure is complete.                                                                           |





---

—End—

---

## Powering on and booting an SST unit

### Purpose of this procedure

This procedure is used to power on an SST unit that has been installed as a replacement, or was shutdown for any other reason.

This procedure may be used as a standalone task or as part of a higher level activity such as part of a dead office recovery activity or software upgrade activity.

### Limitations and restrictions

There are no restrictions on using this procedure.

### Prerequisites

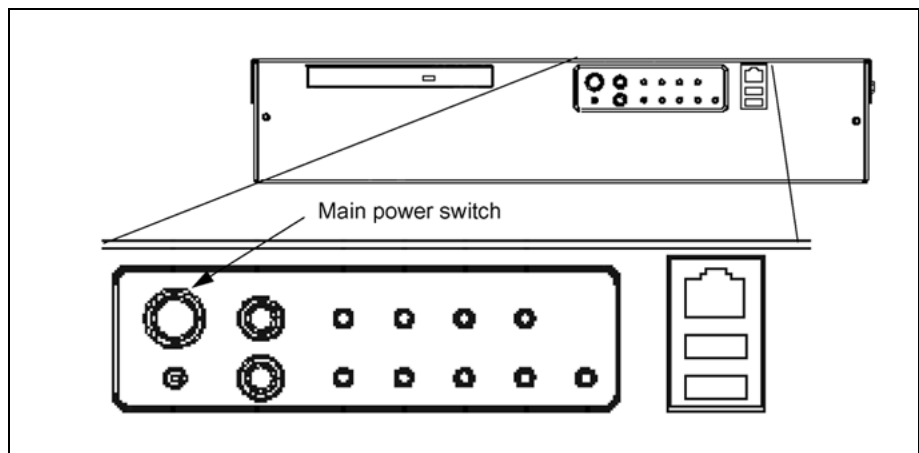
If the unit was a replacement unit recently installed, ensure that all power cabling connections have been properly installed and secured at the rear of the chassis and SAM-F frame.

### Action

| Step                                                                                 | Action                                                                                 |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <b>At the front panel of the SST unit</b>                                            |                                                                                        |
| 1                                                                                    | If necessary, power on the SST using the main power switch located on the front panel. |
|  |                                                                                        |
| 2                                                                                    | If desired, at the SST console, monitor the boot progress of the unit.                 |
| —End—                                                                                |                                                                                        |

#### At the front panel of the SST unit

- 1 If necessary, power on the SST using the main power switch located on the front panel.



- 2 If desired, at the SST console, monitor the boot progress of the unit.

—End—

## Viewing the operational status of the SIP Gateway application

### Purpose of this procedure

Use the following procedure to view the service status of the SIP Gateway application.

### Limitations and restrictions

This procedure provides instructions for determining the service status of the SIP Gateway application software only.

### Prerequisites

There are no prerequisites for this procedure.

### Action

| Step | Action |
|------|--------|
|------|--------|

#### *At the CS 2000 Session Server Manager or IEMS client*

- 1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu.



- 3 Monitor the status of the SIP Gateway application from this view:

| Session Server Status - Connected to Unit #1 |                |                   |
|----------------------------------------------|----------------|-------------------|
| Unit Number                                  | Activity State | Operational State |
| 0                                            | Inactive       | Enabled           |
| 1                                            | Active         | Enabled           |

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| UnLocked             | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

Refresh QueryInfo

Last Performed Operation: Refresh

Result: Passed

SIP Cold SwAct

This page updates automatically every 10 seconds!

Last update: Thu Jun 10 13:04:20 EDT 2004

10 sec Refresh Rate

This view is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the Refresh Rate button or manually refresh the page by clicking the Refresh button.

- 4 See ["Interpreting SIP Gateway application status and maintenance fields"](#) (page 665) to review the description of the various fields of this view.

For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section "Interpreting SIP Gateway application states" in *Session Server Trunks Security and Administration* (NN10346-611).

- 5 The following service affecting actions are available:
- Lock the SIP Gateway application
  - Unlock the SIP Gateway application
  - Suspend the SIP Gateway application
  - Unsuspend the SIP Gateway application
  - Cold SwAct the SIP Gateway application
- 6 To view the number of active calls currently being handled by the application and the synchronization status of the units, click QueryInfo.

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| UnLocked             | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |
| Refresh                                                | QueryInfo                               |

- 7 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

—End—

---

## Interpreting SIP Gateway application status and maintenance fields

Use the following table to assist you in interpreting information displayed in the Status area:

### Node status field descriptions

| Field                      | Description                                                                                                                                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unit Connection Status Bar | Indicates which unit in the node the CS 2000 Session Server Manager is connected to.                                                                                                                            |
| Unit Number                | Identifies the two units in the node, labeled 0 and 1.                                                                                                                                                          |
| Activity State             | Indicates which unit is Active and which is Inactive (standby). Also acts as an indirect indicator of fault-tolerant status; when both units have an Operational status of Enabled, the node is fault-tolerant. |
| Operational State          | Indicates the service status of each unit, Enabled or Disabled.                                                                                                                                                 |

Use the following table to assist you in interpreting information displayed in the SIP Gateway status area:

### SIP Gateway application Status field descriptions

| Field                | Indication                        |
|----------------------|-----------------------------------|
| Administrative State | Locked, Unlocked, or ShuttingDown |
| Operational State    | Enabled or Disabled               |
| Procedural Status    | Terminating or -                  |
| Control Status       | Suspended or -                    |

Use the following table to assist you in interpreting the SIP Gateway area's CCITT X.731-style and related DMS-style status indicators:

### SIP Gateway Maintenance field descriptions and interpretation of service states

| Administrative State                         | Operational State | Procedural Status | Control Status | DMS style Service States          |
|----------------------------------------------|-------------------|-------------------|----------------|-----------------------------------|
| Locked                                       | Disabled          | -                 | Suspended      | Offline (OFFL)                    |
| Locked                                       | Enabled           | -                 | -              | Manual Busy(M ANB)                |
| Locked                                       | Enabled           | Terminating       | -              | Manual Busy Transitioning(M ANBP) |
| Unlocked                                     | Enabled           | -                 | -              | In Service(INSV)                  |
| A dash (-) indicates a status of in-service. |                   |                   |                |                                   |

| Administrative State                         | Operational State | Procedural Status | Control Status | DMS style Service States    |
|----------------------------------------------|-------------------|-------------------|----------------|-----------------------------|
| Unlocked                                     | Disabled          | -                 | -              | System Busy(SY SB)          |
| Shutting Down                                | Enabled           | -                 | -              | Going out of service(INSVD) |
| A dash (-) indicates a status of in-service. |                   |                   |                |                             |

## Verifying synchronization status

### Purpose of this procedure

Use this procedure to determine the synchronization status of the two units.

### Limitations and restrictions

There are no restrictions for performing this procedure.

### Prerequisites

There are no prerequisites for performing this procedure.

### Action

| Step                                                        | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>At the CS 2000 Session Server Manager or IEMS client</i> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 1                                                           | Select <b>Carrier VoIP Communication Server 2000 Session Server Manager</b> from the launch point menu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                                                             |  <p>Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.</p> <p>Please select one of the following management interfaces:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Succession Communication Server 2000 NCGL Platform Manager</a></li> <li>▪ <a href="#">Succession Communication Server 2000 Session Server Manager</a></li> </ul> |
| 2                                                           | Select <b>Session Server &gt; Maintenance &gt; Application &gt; SIP Gateway</b> from the left side menu:                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                                             |  <p>The screenshot shows a tree view of the management interface. The path 'Session Server &gt; Maintenance &gt; Application &gt; SIP Gateway' is highlighted. The 'SIP Gateway' item is circled in red.</p>                                                                                                                                                                                                                                                                                  |
| 3                                                           | At the bottom of the SIP Gateway Maintenance panel, locate and click the <b>QueryInfo</b> button.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

*At the CS 2000 Session Server Manager or IEMS client*

- 1 Select **Carrier VoIP Communication Server 2000 Session Server Manager** from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select **Session Server > Maintenance > Application > SIP Gateway** from the left side menu:



- 3 At the bottom of the SIP Gateway Maintenance panel, locate and click the **QueryInfo** button.



| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| UnLocked             | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |
| Refresh                                                | QueryInfo                               |

- 4 The synchronization status of the units is displayed at the bottom of the query results panel.

If the units are not in sync, check for alarm conditions.

|                                                 |
|-------------------------------------------------|
| Last Performed Operation: Query Number of Calls |
| Result: Passed                                  |
| Number Of Active Calls: 0                       |
| SIP Gateway is: In Sync                         |
| SIP Gateway Cold SwAct                          |

- 5 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

## 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

| Step | Action |
|------|--------|
|------|--------|

##### *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> |
|-------------------------|------------------------|

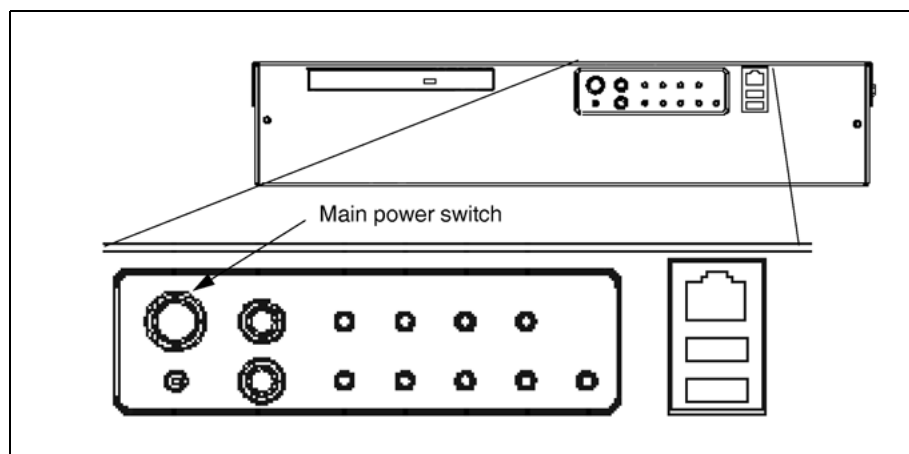
- 2 Power up the CCF BIP breakers. At the top of the cabinet, turn on the breakers that supply power to the STORM disk array and the two SAM21 shelves.

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.
- 7 If necessary, unlock the previously inactive SC.  
Refer to Unlocking a SAM21 Shelf Controller.
- 8 If necessary, unlock the previously active Compact Call Agent (CCA) card.  
Refer to Unlocking the Call Agent.
- 9 If necessary, unlock the previously inactive CCA card.  
Refer to Unlocking the Call Agent.
- 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.
- 14 If necessary, unlock all previously inactive GWC cards.  
Refer to Unlock a GWC card.
- 15 You have completed this procedure.

---

—End—

---

## **SAM21 Shelf Controller Security and Administration**

---

### **New in this release**

#### **Feature changes**

All the feature changes are associated with activity A00015879.

We have added a procedure for changing the password of a SAM21 shelf controller card, Changing the password of a SAM21 shelf controller card.

We have added three procedures explaining how to reset the password of a SAM21 shelf controller card to its default value. You will have to do this if you set the password and subsequently forget it. The password-reset procedures are as follows.

- If the SAM21 shelf contains two SAM21 shelf controller cards, and one or more passwords on each of the cards have been forgotten, use the procedure Resetting SAM21 shelf controller card passwords (I).
- If the SAM21 shelf contains two SAM21 shelf controller cards, and one or more passwords on one of the cards have been forgotten, use the procedure Resetting SAM21 shelf controller card passwords (II).
- If the SAM21 shelf contains one SAM21 shelf controller card, and one or more passwords on that card have been forgotten, use the procedure Resetting SAM21 shelf controller card passwords (III).

#### **Other changes**

There are no other changes.

### **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.

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

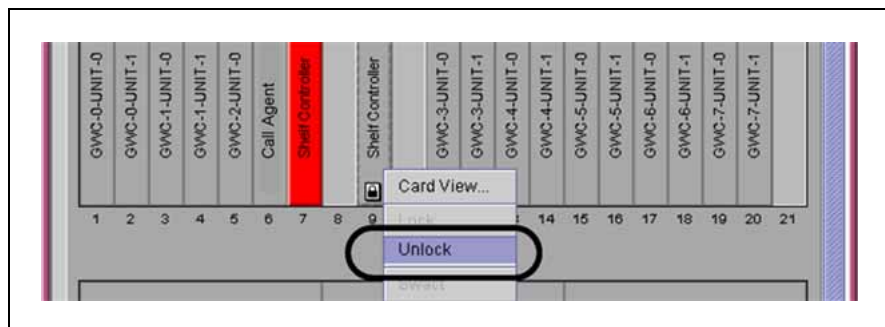
Administration of the SAM21 shelf controllers is done through the CS 2000 SAM21 Manager client.

### Unlocking a SAM21 shelf controller

| Step | Action |
|------|--------|
|------|--------|

#### *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.

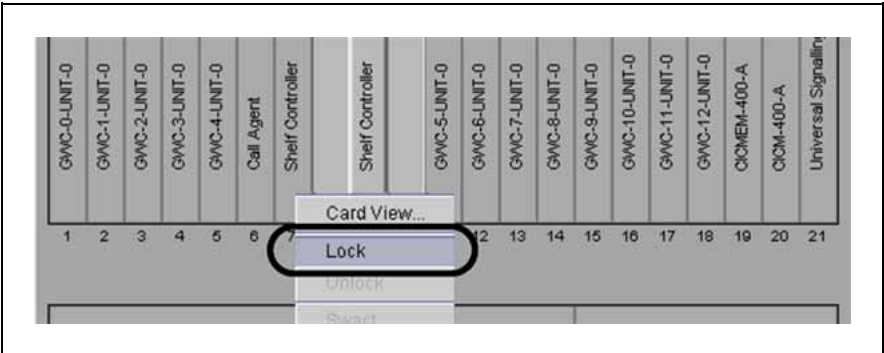


—End—

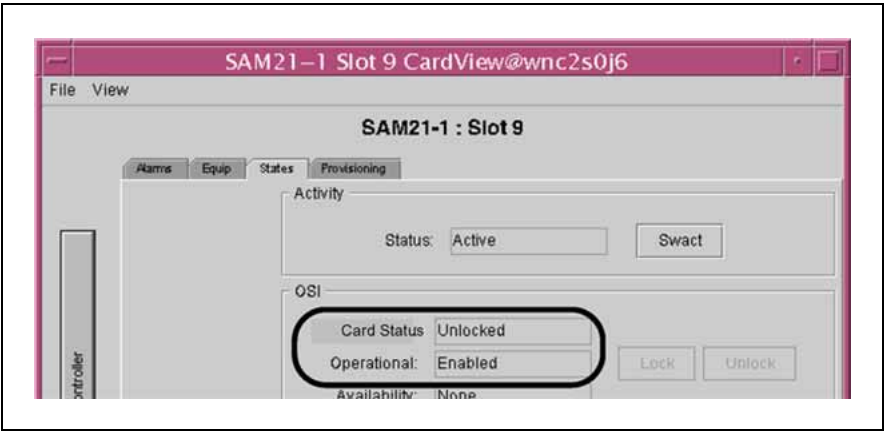
Locking a SAM21 shelf controller

| Step                                                   | Action |
|--------------------------------------------------------|--------|
| <i>At the CS 2000 SAM21 Manager client workstation</i> |        |

- 1 From the Shelf View, right click on the SAM21 shelf controller and select Lock from the context menu.



Only lock a circuit pack that is in service. If a SAM21 shelf controller is unlocked and then re-locked 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.



—End—

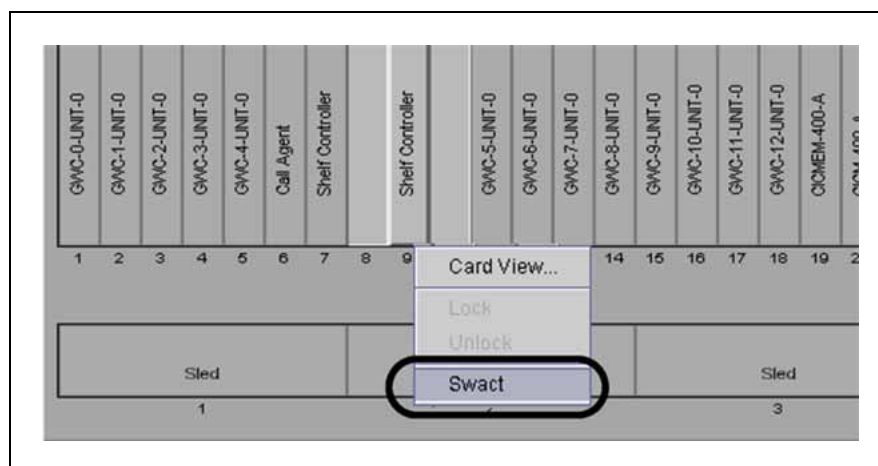
## Invoking manual protection switch

| Step | Action |
|------|--------|
|------|--------|

**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.

Swact is available on the active SAM21 shelf controller only.



—End—

## 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 not inserted for more than one minute.



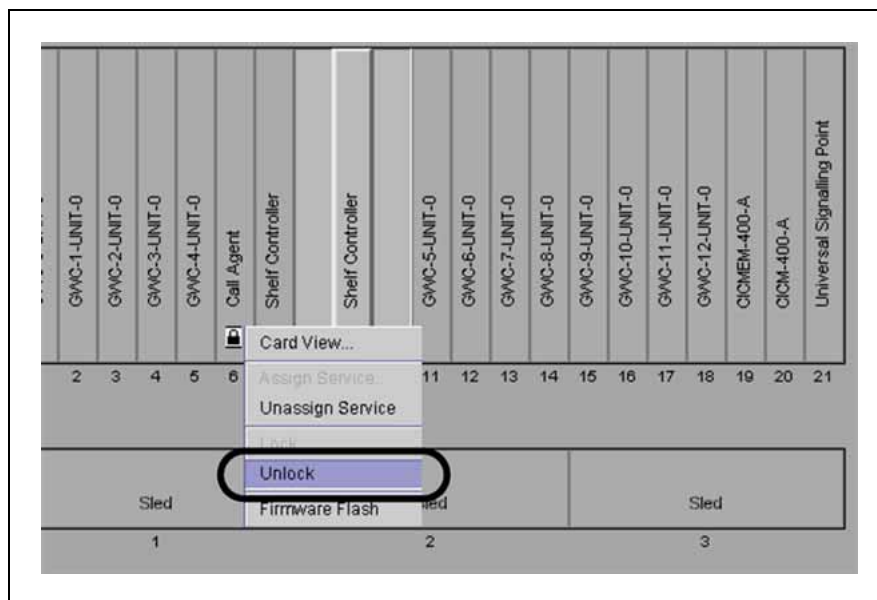
## Unlocking the Call Agent

### Unlocking the Call Agent

| Step | Action |
|------|--------|
|------|--------|

*At the CS 2000 SAM21 Manager client*

- 1 From the Shelf View, right click on the card and select Unlock from the context menu.



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.  
Do not perform any patching activities on the Call Agent until ten minutes have passed.
- 3 This procedure is complete.

—End—

## 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.

### Prerequisites

The GWC card must be locked. The procedure ["Lock a GWC card"](#) (page 680) provides instruction on how to lock a GWC card.

If the IP addresses for the card that you want to unlock and its mate are not contiguous, you cannot unlock the card. You must correct these addresses using procedure ["Manually re-provision GWC cards"](#) in the *Gateway Controller Configuration Management* (NN10205-511) before attempting to unlock the card.

### Action

| Step | 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.                           |

- 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:             | GI091BK (MCPN750) |                 |               |

Save Image Busy (Disable) RTS (Enable) **Card View**

- 4 Click the **Card View** button for the card you want to unlock. This action opens the CS 2000 SAM21 Manager.
- If a card is currently locked, all fields display the value <unknown>.

**At the CS 2000 SAM21 Manager**

- 5 In the card view, select the **States** tab.
- If you want to display the status of all cards in the shelf, select **Shelf View** from the **View** menu.

File View

**Sam21-2 : Slot 12**

Alarms | Equip | **States** | Diags | Provisioning

Summary

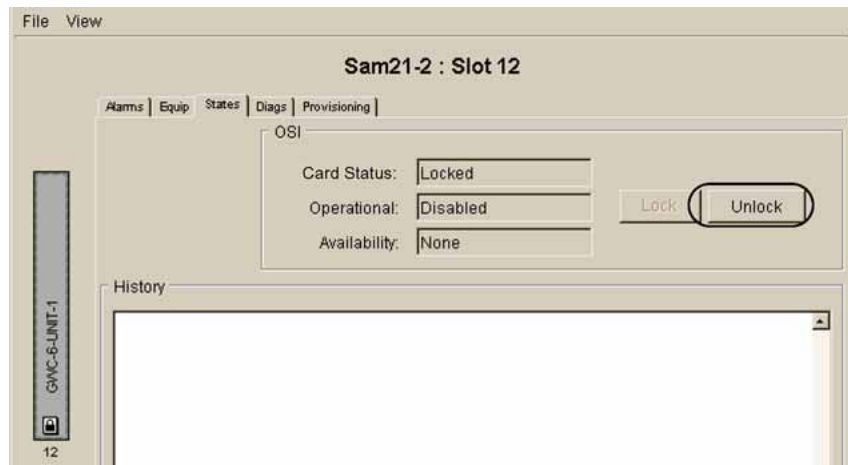
| Critical | Major | Minor |
|----------|-------|-------|
| 0        | 0     | 0     |

Details

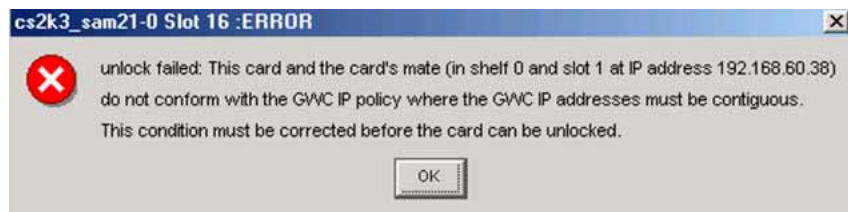
| Equip. | ID | Time | Type | Severity | Reason |
|--------|----|------|------|----------|--------|
|        |    |      |      |          |        |

GWC-6-UNIT-1  
12

- 6 In the States display, click the **Unlock** button to unlock the card.



If the IP addresses for the selected card and its mate are not contiguous, the system displays the following error message:



Follow procedure "Manually re-provision GWC cards" in *Gateway Controller Configuration Management* (NN10205-511) to correct these addresses, then repeat this procedure.

- 7 Observe the system response in the History window.  
The card is unlocked when you see the text "Application unlocked successfully".
- 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.

---

—End—

---

## 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](#)" (page 677) 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
- when replacing or upgrading hardware

### Prerequisites

If the card that 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. If required, follow procedure "Invoke a manual protection switch (warm SWACT)" in *Gateway Controller Security and Administration* (NN10213-611).

When the card is standby, you need to disable (busy) services on the card. Follow procedure "Disable (Busy) GWC card services" in *Gateway Controller Security and Administration* (NN10213-611).

Once services on a standby card have been disabled, you can proceed with locking the card.

### Action

| Step | Action |
|------|--------|
|------|--------|

|                                                 |  |
|-------------------------------------------------|--|
| <b><i>At the CS 2000 GWC Manager client</i></b> |  |
|-------------------------------------------------|--|

- 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.
- 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: G1091BK (MCPN750)       |                               |

Save Image Busy (Disable) RTB (Enable) Card View

- 4 Click the **Card View** button for the card you want to lock.

**At the CS 2000 SAM21 Manager client**

- 5 In the card view, select the **States** tab.

File View

Sam21-2 : Slot 12

Alarms Equip States Diags Provisioning

Summary

| Critical | Major | Minor |
|----------|-------|-------|
| 0        | 0     | 0     |

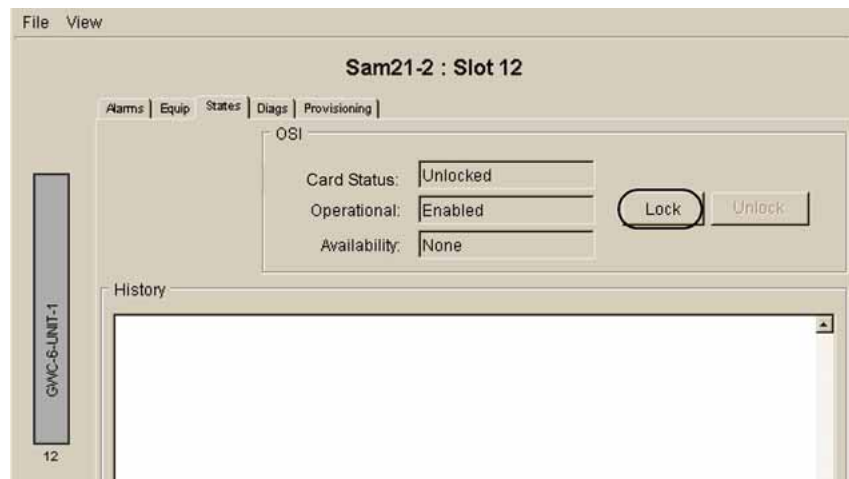
Details

| Equip. | ID | Time | Type | Severity | Reason |
|--------|----|------|------|----------|--------|
|        |    |      |      |          |        |

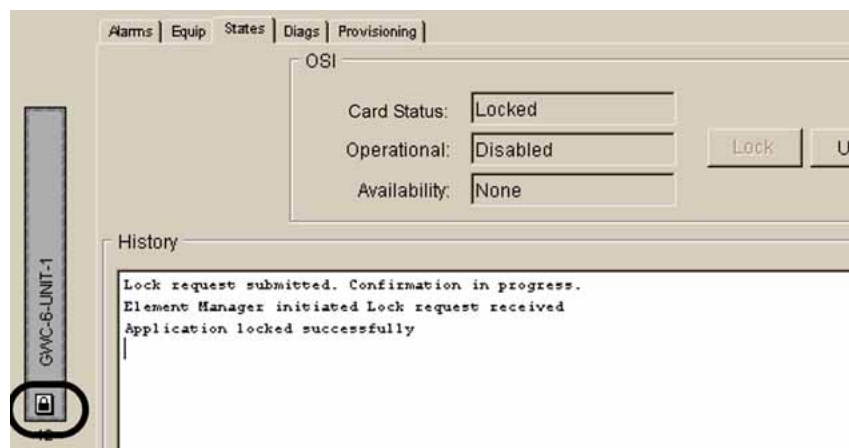
GWC-6-UNIT-1

12

- 6 In the States display, click the **Lock** button to lock the card.



- 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 following figure) 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.

---

—End—

---

## Manually re-provision GWC cards

### Purpose of this procedure

Use this procedure to manually change the basic provisioning information for a set of Gateway Controller (GWC) cards, including IP addresses, port addresses, gateway addresses, and load paths.

### When to use this procedure

Use this procedure when it is necessary to change GWC card-related provisioning information in the CS 2000 SAM21 Manager database.

### Prerequisites and guidelines

This procedure does not provide instructions on how to make provisioning changes to GWC services in the CS 2000 GWC Manager database (such as changing a service profile for a GWC node).

You must first busy the GWC node services using the CS 2000 GWC Manager before re-provisioning any cards in the node. Follow procedure "Busy a GWC node" in *Gateway Controller Configuration Management* (NN10205-511).

When re-provisioning IP addresses for GWC cards, you must use a block of four contiguous IP addresses for each card pair (node).



#### CAUTION

##### Partial service disruption

Changes to the IP addresses or other configuration values of a GWC card can cause inconsistencies with the CS 2000 GWC Manager database.

### Action

| Step | 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 Select or type the name of the GWC node to re-provision.
- 3 Complete procedure "Busy a GWC node" in *Gateway Controller Configuration Management* (NN10205-511) to make the card resources unavailable for call processing activities.



- 4 Click the **Card View** button for the card you busied in the preceding step. This action opens the CS 2000 SAM21 Manager.

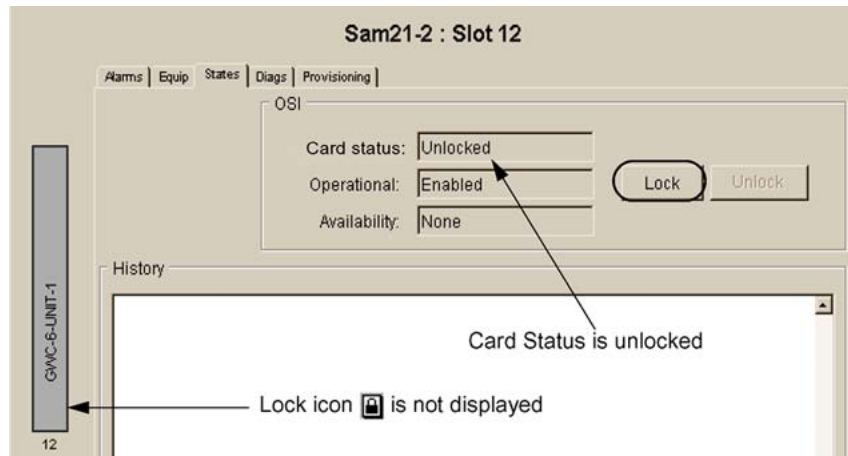
### At the CS 2000 SAM21 Manager

- 5 Select the **States** tab to view the states window.

- 6 If the card is already locked, go to the next step.

If the card is not locked, click the **Lock** button.

You can determine if the card is locked by looking at the card graphic at the left of the screen. If the lock icon is present, the card is locked. If the lock icon is not present, the card is not locked. The Card Status also indicates whether the card is locked.



*System response:*

Application locked Successfully.

If you are denied your first attempt to lock the card, you can override the lock request denial and force the card to lock. Use the CS 2000 GWC Manager to interpret the various states of the card. Follow procedure ["View and interpret the operational status of a GWC node"](#) (page 466).

A card has accepted a lock request if it has the following states:

- Card Status: locked
- Operational state: disabled

- 7 Select the **Provisioning** tab.
- 8 Click the **Modify** button to make changes to the provisioning datafill.

The screenshot shows the 'Provisioning' tab for 'Sam21-1 : Slot 13'. The interface includes a sidebar with 'GWC-3-UNIT-0' and '13'. The main area has several sections: 'General' with fields for IP (47.104.41.42), Gateway IP (47.104.41.1), Subnet Mask (255.255.255.128), FW Version (RM05), MAC Address (0001AF080CC7), and GWC Number (3); 'NTP' with Primary and Secondary NTP (172.25.15.1); 'GWC-EM' with Host IP (47.104.41.4); 'Load Info' with Server IP (47.104.41.3), Path (/swd/gwc), Load (pgc09av.imag), and a checkbox for FW Flash Enable; and 'Domain Servers' with Primary, 1st Alt, and 2nd Alt (all 0.0.0.0). At the bottom are buttons for Modify, Save, Clear, Cancel, and Details...

| Section        | Field           | Value                    |
|----------------|-----------------|--------------------------|
| General        | IP              | 47.104.41.42             |
|                | Gateway IP      | 47.104.41.1              |
|                | Subnet Mask     | 255.255.255.128          |
|                | FW Version      | RM05                     |
|                | MAC Address     | 0001AF080CC7             |
| NTP            | Primary NTP     | 172.25.15.1              |
|                | Secondary NTP   | 172.25.15.1              |
| GWC-EM         | Host IP         | 47.104.41.4              |
| Load Info      | Server IP       | 47.104.41.3              |
|                | Path            | /swd/gwc                 |
|                | Load            | pgc09av.imag             |
|                | FW Flash Enable | <input type="checkbox"/> |
| Domain Servers | Primary         | 0.0.0.0                  |
|                | 1st Alt         | 0.0.0.0                  |
|                | 2nd Alt         | 0.0.0.0                  |

- 9 Enter the new or changed provisioning data as described in the following list.

File View

Sam21-2 : Slot 12

Alarms Equip States Diags Provisioning

General

IP: 47.104.41.55 Gateway IP: 47.104.41.1

Subnet Mask: 255.255.255.128 FW Version: RM04

MAC Address: 0001AF07A6A0 GWC Number: 6

NTP

Primary NTP: 172.25.15.1

Secondary NTP: 172.25.15.1

GWC-EM

Host IP: 47.104.41.4

Load Info

Server IP: 47.104.41.3

Path: /swd/gwc

Load: pgc09ar.imag Get Load Files

☐ FW Flash Enable

Domain Servers

Primary: 0.0.0.0 1st Alt: 0.0.0.0

2nd Alt: 0.0.0.0

Modify Save Clear Cancel Details

In most cases, when pre-provisioning a GWC, use the default values indicated. Otherwise, obtain and enter the following values:

- IP: <GWC\_unit\_0\_IP\_address> or  
IP: <GWC\_unit\_1\_IP\_address>

A contiguous block of four IP addresses is required. If the IP addresses for the GWC card and its mate are not contiguous and you save your settings, the system displays a warning message. The message explains that you must correct the IP addresses; otherwise, you will not be able to unlock the card. If necessary, repeat this procedure to make sure that the IP addresses are contiguous.

If any of the four IP addresses for the new card is already used by another card, the system displays an error message. Contact your site system administrator to identify the IP addresses you must use.

- Gateway IP: default\_router or gateway\_IP\_address
- Subnet Mask: subnet\_mask
- FW Version: firmware version of the GWC load

- Host IP: CS 2000 Management Tools\_Server\_IP\_Address
  - Server IP: IP address of the CS 2000 Core Manager or Core and Billing Manager (CBM)
  - Path: /swd/gwc/ - on the CS 2000 Core Manager or CBM
  - Load: name of the GWC load image file;  
example: pgc08bg.imag  
Click the **Get Load Files** button and select the required load from the drop-down list.
  - If available, select the **FW Flash Enable** check box if you wish to flash the card firmware with a new firmware version
  - Primary Domain Server: server\_IP\_address
  - 1st Alternate Domain Server: server\_IP\_address
  - 2nd Alternate Domain Server: server\_IP\_address
- 10** When you are finished entering changes, click the **Save** button.
- 11** Return to [step 2](#) and repeat the steps for each GWC node you are re-provisioning.
- 12** Re-provisioning does not take effect until the card is unlocked and rebooted. For information about how to unlock GWC cards, see procedure "[Unlock a GWC card](#)" (page 677).
- 13** The procedure is complete.

---

—End—

---

## 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

| Step | Action |
|------|--------|
|------|--------|

##### *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 109.
- 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 40.

##### *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.

---

—End—

---

## 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:

| Step | Action |
|------|--------|
|------|--------|

**At the OAMP workstation**

- |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Click <b>Configuration&gt;mtp&gt;link</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 2 | <p>Select the <b>link-type</b> for this link from the drop down box. Supported link types include:</p> <ul style="list-style-type: none"> <li>• ss7iplink: IP High-speed Link using M2PA, M2UA-SAAL, M2UA-MTP2, or M3UA</li> <li>• atmhslink: ATM High-speed Link over T1 or E1 interfaces</li> <li>• chanslink: Channelized links supporting up to 8 channel over E1 or T1.</li> <li>• lslink: Low-speed link, V.35 or DS0A.</li> <li>• Virtuallink: used to connect 2 System Identities on the same USP.</li> <li>• mtp2hslink: MTP L2 High-speed Link.</li> </ul> |
| 3 | Click the <b>system-id</b> list and select the system identity to be associated with this link.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 4 | Select a linkset from the <b>linkset-name</b> list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |



#### CAUTION

When USP connects to third party M3UA peer and the link-type is selected as ss7iplink, you must provision only one link into one linkset of which the protocol-type is M3UA. Provisioning multiple links in the same linkset will result in incorrect M3UA handling.

- 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: | Go to    |
|--------------------------|----------|
| an SS7iplink             | step 9.  |
| an atmhslink             | step 10. |
| a chanlslink             | step 11. |
| an lslink                | step 12. |
| an mtp2hslink            | step 13. |

- 9 For SS7iplink, complete the following steps:
  - a. Click the **protocol** list and select a protocol for this link.
  - b. Enter the far end destination IP address in the **dest-ipaddress** box.  
  
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.
  - c. If the protocol for this link is M2UA-SAAL or M2UA-MTP2, enter an interface identifier in the **IID** box.

#### ATTENTION

The interface identifier needs to match the peer interface identifier for the link.

- d. In the **local-port** box, enter the number of the local port. For M3UA links, the port is 2905.
- e. In the **remote-port** box, enter the number of the remote port.
- f. 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.

**ATTENTION**

If client mode is selected, then **sctp-checksum** must be set (the choices are adler and crc32).

If the transport protocol is m2ua or m3ua, then you must set the checksum to crc32.

- g. Click the **sctp-parms-index** list and select an SCTP parameter index number to associate with this link.
- h. 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.

**ATTENTION**

MTP3b support was introduced in USP 10.0 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-parm-index** list.  
There is no default SAAL parameter index.
- g. Select a SAAL timer index from the **saal-timer-index** list.  
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.

**ATTENTION**

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.

#### ATTENTION

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 retransmits unacknowledged MSUs until an acknowledgement is received or the T7 timer expires, at which point the link is taken down.

#### ATTENTION

The default value for the T7 timer is 600 ms.

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.

**ATTENTION**

A system-id must be selected prior to selecting the I2-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.

**ATTENTION**

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 **I2-t7-timer** box. This value represents the excessive delay of acknowledgement timer. PCR continually retransmits unacknowledged MSUs until an acknowledgement is received or the T7 timer expires, at which point the link is taken down.
- 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 **I2-timer-index** list.

The default index is the first available index.

**ATTENTION**

A system-id must be selected prior to selecting the I2-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.

---

—End—

---

## Modifying Links

To edit links, perform the following steps:

| Step | Action |
|------|--------|
|------|--------|

*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.

---

—End—

---

## Deleting Links

To delete existing links, perform the following steps:

| Step | Action |
|------|--------|
|------|--------|

*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.

---

—End—

---

## 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.

---

| Step | Action |
|------|--------|
|------|--------|

---

***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 uninhibited 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.

---

—End—

---

## 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

---

| Step | Action |
|------|--------|
|------|--------|

---

***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.

---

—End—

---

## Understanding Link States

The information displayed in the I3-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.

### I3-link-status

The I3-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 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.

### ATTENTION

If simple network management protocol (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

| Step | Action |
|------|--------|
|------|--------|

### *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 SNTP.

| If:               | Do:                                                                                                                                                                                                                                                        |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No                | Proceed to <a href="#">step 3</a> .                                                                                                                                                                                                                        |
| 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 **Time Zone** drop-down menu. A world-wide list of time zones appears. Select the time zone listing that matches the local time zone.  
  
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 **Adjust clock for daylight savings changes** box.  
  
If you are enabling the automatic system clock adjustment for daylight savings time for the first time, make sure you perform [step 7](#) to [step 13](#).
- 7 Set the starting month for daylight savings time, click **dst-start-month**. Select the month in which daylight savings time starts.
- 8 Set the starting day in the **dst-start-day** spinbox.
- 9 Set the starting hour in the **dst-start-hour** spinbox.
- 10 Set the ending month for daylight savings time, click **dst-end-month**. Select the month in which daylight savings time ends.
- 11 Set the ending day in the **dst-end-day** spinbox.
- 12 Set the ending hour in the **dst-end-hour** spinbox.
- 13 Click **OK**.

---

—End—

---

## 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

| Step | Action |
|------|--------|
|------|--------|

*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. |
|---|------------------------------------|

—End—

# 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

| Step | Action |
|------|--------|
|------|--------|

#### *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. <ul style="list-style-type: none"> <li>If you have one power supply, engage a CP in slot 0 and at least one FP.</li> </ul> <p>Do not engage more than seven FPs. Ensure that all other processors are disengaged.</p> <ul style="list-style-type: none"> <li>If you have two power supplies, engage at least one CP and two FPs. Or, engage two CPs and at least one FP.</li> </ul> |
| 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. <p>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.</p>                                                                                             |

- 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.

---

—End—

---

---

## 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

---

| Step | Action |
|------|--------|
|------|--------|

---

#### *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.                                                                             |
- 

—End—

---

## 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

| Step                       | Action                                                                                                                                                                                                     |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>At the MAP terminal</b> |                                                                                                                                                                                                            |
| 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<br><pre>&gt;MAPCI;MTC;PM;POST SPM &lt;spm_no&gt;</pre> and pressing the Enter key.<br>where<br><b>spm_no</b> is the number of the SPM/MG 4000/IW-SPM/DPT-SPM |
| 5                          | Select and RTS the CEMs by typing<br><pre>&gt;SELECT CEM ALL;BSY ALL; LOADMOD ALL;RTS ALL</pre> and pressing the Enter key.                                                                                |
| 6                          | Select and RTS the SRM, OC3 RMs, ATM RMs, and/or GEM RMs by typing<br><pre>&gt;QUIT;SELECT &lt;rm_type&gt; ALL;BSY ALL;LOADMOD ALL;RTS ALL</pre> 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.

---

—End—

---



## 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

| Step | Action |
|------|--------|
|------|--------|

#### *At the frame housing the MCS servers*

#### **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.

- 1 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. To observe 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 MgmtSvr/AcctMgr's snmp, then kill the process. The process will automatically restart in about 30 seconds.
- f. Restart the AcctMgr process. If any of the components send an alarm in the System Management Console indicating that the component cannot communicate with the primary or backup

CAM, then again restart the AcctMgr process. Right click on the Accounting component in the System Management Console and select Restart. Confirm the request. A progress box will pop up and then disappear when the restart has begun. While the Accounting module is rebooting, the other MCS component will throw alarms to the System Management Console, but those will go away when the Acct component is fully operational.

- 4 Now verify the state of the other machines and the MCS components on them. Launch the System Management Console as you normally would. Expand the navigation tree fully so that each component is fully exposed.
  - a. Restart the AppSvr. If the clients are having trouble communicating with the AppSvr, then restart the AppSvr. Right click on the AppSvr component in the System Management Console and select **Restart**. Confirm the request. You should see a progress window and it disappears after the restart has begun. To view AppSvr startup logs, telnet to the AppSvr box (we recommend that you telnet as *nortel*) and go to the following directory: `/var/Rel2.0/appsvr`. Type: **`tail -f appsvr.0.log`**.
  - b. Verify that the AppSvr's snmp process is running. This step is the same as 3e above.
  - c. Restart the IPCM. If the i2004 phones are not responding to client registers, the hollow blinking icons in the i2004 display, then restart the IPCM component. Right click on the IPCM component in the System Management Console and select **Restart**. Confirm the request. You see a progress window that will disappear after the restart has begun. To view IPCM startup logs, telnet to the IPCM box (recommend as *nortel*) and go to the following directory: `/var/Rel2.0/esm`. Type: **`tail -f esm.1.log`**.
  - d. Verify that the IPCM's snmp process is running. This step is the same as 3e above. Most likely, the Provisioning Module and the WebClient Module are deployed on the same box as the IPCM. Therefore, you only need to verify the snmp service on the box once.
  - 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](mailto: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.

---

—End—

---

---

## Powering up a Border Control Point

---

### Purpose of this procedure

Use the following procedure to power up a Border Control Point. The Border Control Point 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 Border Control Point.

### Prerequisites

None

### Action

#### Powering up the Border Control Point

---

| Step | Action |
|------|--------|
|------|--------|

---

##### *At the frame housing the Border Control Point*

- 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.

---

—End—

---

## 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

| Step                            | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>At the CCF or SAMF frame</i> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 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).<br><br>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: <ul style="list-style-type: none"> <li>• Red Fail LED is off (left hand side of the board).</li> <li>• ACT LED is on (left hand side of the board).</li> </ul> <p><b>Note:</b> It may take up to 60 seconds for the ACT LED to light up.</p> <ul style="list-style-type: none"> <li>• Blue LED does not remain on (right hand side of the board).</li> <li>• PWR LED is on (right hand side of the board).</li> <li>• Both Ethernet Link LEDs are on (middle of the board).</li> </ul> |

**Note 1:** The Ethernet LEDs are Green when indicating a connection, and Orange when indicating activity.

**Note 2:** Check the Media Server 2000 to make sure it is set to an unlocked state.

5 You have completed this procedure.

---

—End—

---

---

## 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

| Step                            | Action                                                                                          |
|---------------------------------|-------------------------------------------------------------------------------------------------|
| <i>At the CCF or SAMF frame</i> |                                                                                                 |
| 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.                                                              |
| —End—                           |                                                                                                 |



## 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

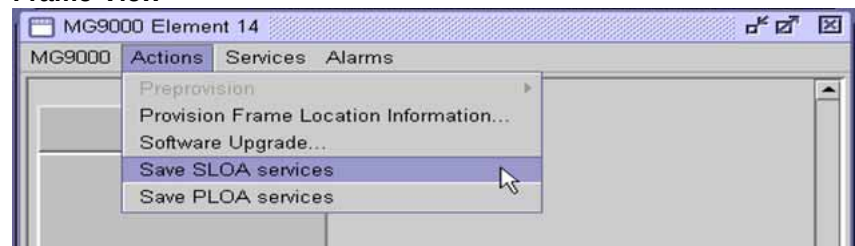
#### Recovering an MG 9000 that has lost power and cannot communicate with the MG 9000 Manager

| Step | Action |
|------|--------|
|------|--------|

##### *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**



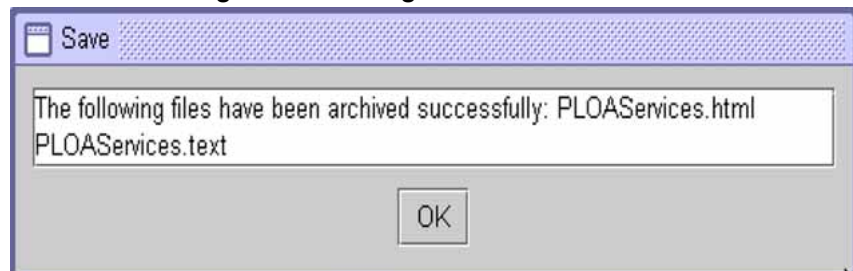
- 3 Save a copy of the MG 9000 Manager PLoA provisioning data as follows (you'll be re-entering this data later):

- 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.

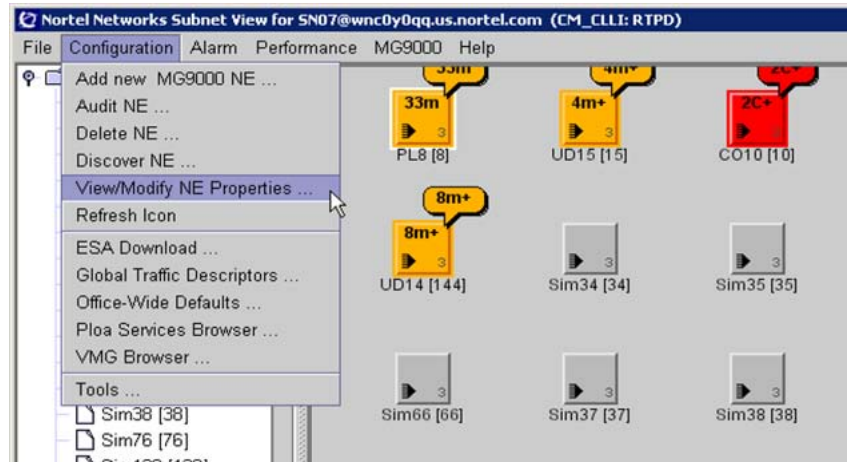
- b. Record the file name provided in the Save acknowledgement window for later use.

**Save acknowledgement message for PLoA**



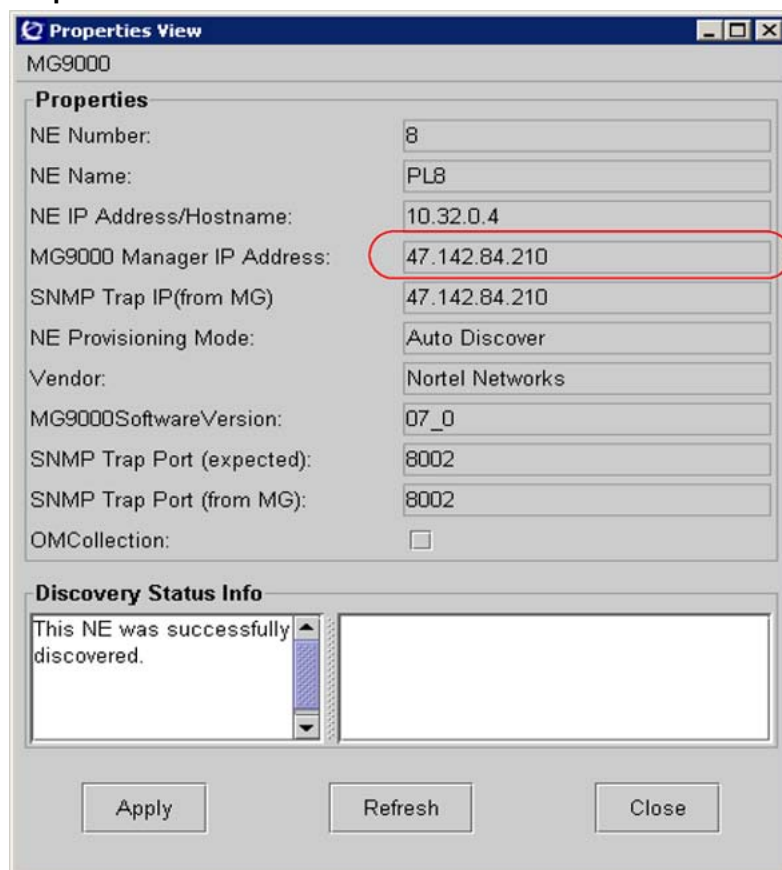
- 4 Obtain the IP address of the MG 9000 Manager server (not the mid-tier or client). At the Subnet View, select Configuration->View/Modify NE Properties from the menu bar.

## 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

```

ftp
Auto
Connected to 47.142.84.210.
220 ProFTPD 1.2.2 Server (Nortel SSPFS Developer Installation) [ngen_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: 32732 bytes received in 0.49Seconds 66.80Kbytes/sec.
ftp> get PLOSservices.text
200 PORT command successful.
150 Opening ASCII mode data connection for PLOSservices.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** You have completed this procedure.

---

**—End—**

---

## CS 2000 Management Tools fault procedures

The fault procedures available for the CS 2000 Management Tools are listed under the following categories:

- "Alarms" (page 721)
- "Audit" (page 721)
- "Trunk maintenance" (page 722)
- "Logs" (page 722)
- "Hardware" (page 723)
- "Communications" (page 723)
- "CS 2000 Management Tools fault procedures" (page 721)

### Alarms

The following table lists the available procedures related to alarms.

#### Alarms procedures

| Procedure                                                                       |
|---------------------------------------------------------------------------------|
| <a href="#">"CS 2000 Management Tools fault management overview" (page 725)</a> |
| <a href="#">"Accessing the Alarm Manager" (page 730)</a>                        |
| <a href="#">"Retrieving details about an alarm" (page 736)</a>                  |
| <a href="#">"Accessing the Alarm History" (page 740)</a>                        |
| <a href="#">"Filtering alarms" (page 742)</a>                                   |
| <a href="#">"Resetting the filters for alarms" (page 746)</a>                   |
| <a href="#">"Defining alarms using the NPM" (page 748)</a>                      |

### Audit

The following table lists the available procedures related to the audit.

#### Audit procedures

| Procedure                                        |
|--------------------------------------------------|
| <a href="#">"Performing an audit" (page 754)</a> |

## Line maintenance

The following table lists the available procedures related to line maintenance using the Line Maintenance Manager (LMM).

| Procedure                                                       |
|-----------------------------------------------------------------|
| "Posting a line by directory number" (page 775)                 |
| "Posting a line by gateway" (page 777)                          |
| "Busying a line" (page 780)                                     |
| "Installation busying a line" (page 782)                        |
| "Force releasing a line" (page 784)                             |
| "Returning a line to service" (page 786)                        |
| "Clearing one or more posted lines from the display" (page 788) |
| "Retrieving line properties" (page 790)                         |
| "Querying line gateways in a trouble state" (page 793)          |

## Trunk maintenance

The following table lists the available procedures related to trunk maintenance using the Trunk Maintenance Manager (TMM).

### Trunk maintenance procedures

| Procedure                                                                     |
|-------------------------------------------------------------------------------|
| "Performing trunk maintenance using the Trunk Maintenance Manager" (page 798) |
| "Posting PRI Group D-channels" (page 812)                                     |
| "Displaying trunk CLLI codes by gateway" (page 814)                           |
| "Performing an ISUP Continuity Test" (page 816)                               |

## Logs

The following table lists the available procedures and information related to logs.

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                                           |
|-----------------------------------------------------|
| "Routing customer logs to a remote host" (page 818) |
| "Configuring log reporting" (page 821)              |
| "Viewing debug logs" (page 825)                     |

**Procedure**

"Viewing OMPUSH logs" (page 826)  
 "Viewing customer logs on an SPFS-based server" (page 828)  
 "Disabling local logging of SPFS platform faults" (page 830)

**Hardware**

The following table lists the available procedures related to hardware.

**Hardware procedures****Procedure**

"Replacing one or more failed disk drives on an SPFS-based server" (page 833)  
 "Replacing a DVD drive on an SPFS-based server " (page 842)  
 "Cleaning the DAT drive on the Netra T1400" (page 848)

**Communications**

The following table lists the available procedures related to communications.

**Communications procedures****Procedure**

"Re-establishing the connection between the NPM GUI and the server" (page 850)  
 "Restoring SSH communication between the CS 2000 Management Tools server and the core manager" (page 852)  
 "Correcting a CORBA configuration issue between the CS 2000 Management Tools server and the MG 9000 Manager server " (page 856)

**CS 2000 Management Tools server and SPFS**

The following table lists the available procedures related to the CS 2000 Management Tool server and the Server Platform Foundation Software (SPFS).

**CS 2000 Management Tools server and SPFS procedures****Procedure**

"Verifying the state of a cluster" (page 864)  
 "Initiating a manual failover on a Sun Netra 240 server pair" (page 868)  
 "Querying the state of the SPFS platform" (page 870)  
 "Rebooting an SPFS-based server" (page 873)



**Procedure**

"Shutting down an SPFS-based server" (page 875)

"Recovering from having two inactive servers in a cluster" (page 880)

**Downgrading the CS 2000 Management Tools software**

The following table lists the available procedures related to downgrading the CS 2000 Management Tool software on an SPFS-based server.

| Procedure                                                                  |
|----------------------------------------------------------------------------|
| "Downgrading the CS 2000 Management Tools software " (page 233)            |
| "Performing a full system restore on an SPFS-based server " (page 258)     |
| "Restoring the oracle data on an SPFS-based server " (page 264)            |
| "Restoring NPM patch files " (page 884)                                    |
| "Performing a restore of APS audio files from tape " (page 890)            |
| "Performing a restore of APS audio files from CD " (page 892)              |
| Performing an APS-only Data Base Restore from a 4mm DAT                    |
| Performing an APS-only Database restore from a CD                          |
| "Cloning the image of one node in a cluster to the other node " (page 237) |
| "Executing a fallback during an SPFS-based server upgrade " (page 897)     |

---

## CS 2000 Management Tools fault management overview

---

### Fault management strategy

The Server Platform Foundation Software (SPFS) 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 simple network management protocol (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 SPFS 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 SPFS 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 (IEMS) 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 IEMS, refer to the Fault Management section of the IEMS User Guide, NN10329-111.

### 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 the following figure.

- 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 subse...   |
|  | 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 subse...   |
|  | SNMP_NE_Poller  | Communications | 15:25:56 18-二月-20... | Major    | Communications subse...   |
|  | SNMP_NE_Poller  | Communications | 15:25:56 18-二月-20... | Major    | Communications subse...   |
|  | SNMP_NE_Poller  | Communications | 15:25:56 18-二月-20... | Major    | Communications subse...   |

## 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. All traps managed by SESM are stored in pa log files in the /opt/nortel/NTsesm/admin/logs directory. The number of pa log files is determined manually using the CLI and the SESM logging and debug log configuration options available from the configuration script.

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 preceding parameters can be configured using the "configure" tool on the CS 2000 Management Tools server. Refer to procedure ["Configuring log reporting" \(page 821\)](#) 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" \(page 821\)](#) 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 (IEMS) .

The SESM syslog alarm feed is disabled by default to avoid duplication of the alarm logs. Procedure ["Configuring log reporting" \(page 821\)](#) 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 SPFS 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 SPFS 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)
- SPFSlog (platform events)
- ptmlog (SNMP traps received by the system)

Syslog has built-in capabilities to forward logs to another IP address. This functionality is used to send the logs in the SPFS 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 SPFSlog. 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 SPFS 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" \(page 818\)](#) 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 SPFS platform-specific faults is SNMP. However, when local logging is enabled (default), the SPFS 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 using procedure ["Disabling local logging of SPFS platform faults" \(page 830\)](#) 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><br>"Communications"<br><br>"Quality of Service"<br><br>"Processing Error"<br><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><br>"Critical"<br><br>"Major"<br><br>"Minor"<br><br>"Warning"                  |
| Probable Cause       | Provides the probable cause of the particular alarm (X.733 Probable Cause):<br><br>"Adapter Error"                                                                               |

| Field Name | Description                                       |
|------------|---------------------------------------------------|
|            | "Non-Repudiation Failure"                         |
|            | "Bandwidth Reduced"                               |
|            | "Call Establishment Error"                        |
|            | "Communications Protocol Error"                   |
|            | "Communications Subsystem Error"                  |
|            | "Configuration or Customization Error"            |
|            | "Congestion"                                      |
|            | "Corrupt Data"                                    |
|            | "CPU Cycles Limit Exceeded"                       |
|            | "Data Set or Modem Error"                         |
|            | "Degraded Signal"                                 |
|            | "DTE DCE Interface Error"                         |
|            | "Enclosure Door Open"                             |
|            | "Equipment Malfunction"                           |
|            | "Excessive Vibration"                             |
|            | "File Error"                                      |
|            | "Fire Detected"                                   |
|            | "Flood Detected"                                  |
|            | "Framing Error"                                   |
|            | "Heating, Ventilation, or Cooling System Problem" |



| Field Name | Description                                     |
|------------|-------------------------------------------------|
|            | "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"                       |

| 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"                       |

| Field Name | Description                        |
|------------|------------------------------------|
|            | "Information Out of Sequence"      |
|            | "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.

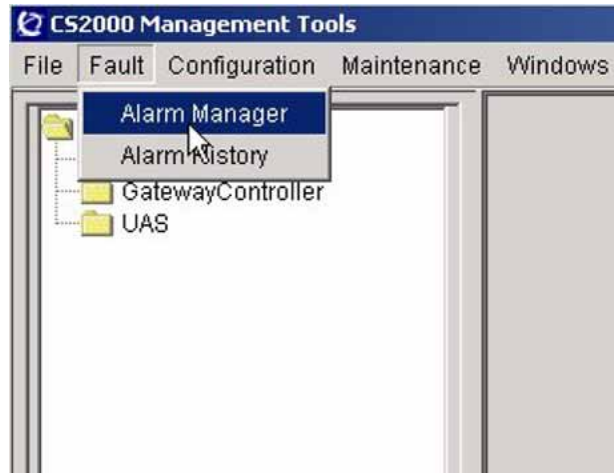
| Step | Action |
|------|--------|
|------|--------|

### *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.

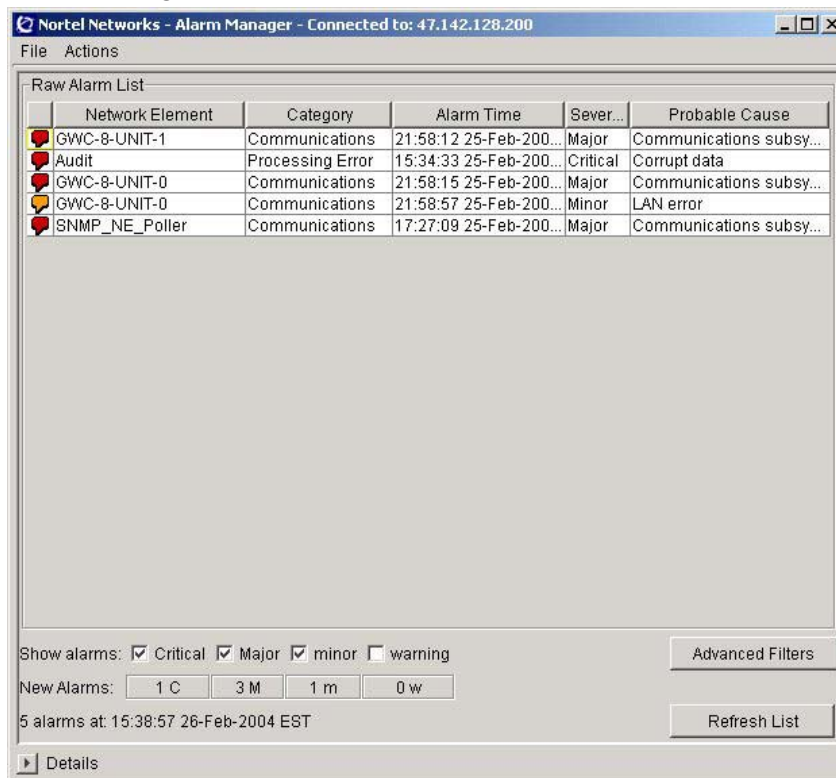
### *At the CS2000 Management Tools GUI*

- 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.

—End—

## 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><br>"Critical"<br><br>"Major"<br><br>"Minor"<br><br>"Warning"                  |
| Category    | Represents the alarm problem category values (ITU-T X.733):<br><br>"Communications"<br><br>"Quality of Service"<br><br>"Processing Error"<br><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                                                                            |

| Field Name        | Description                                                                                                                                                                                                                  |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Probable Cause    | Provides the probable cause of the particular alarm (X.733 Probable Cause).<br><br>See the procedure View and troubleshoot GWC service alarms for a list of possible entries in the Probably Cause field.                    |
| 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.

| Step | Action |
|------|--------|
|------|--------|

**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 application GUI**

- 2 On the **Fault** menu, click **Alarm Manager**.

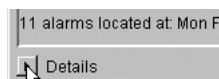


The Alarm Manager window opens.

- 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**

|                  |                      |                    |                                 |
|------------------|----------------------|--------------------|---------------------------------|
| ▼ Details        |                      |                    |                                 |
| NE Name:         | GWC 9 Unit 1         | Component ID:      | GWC;Unit=unit_1;Software=NODEMT |
| Alarm Level:     | Minor                |                    |                                 |
| Category:        | Communications       | Alarm Description: | Mate unit communication lost.   |
| Alarm Time:      | 12:53:15 17-Feb-2002 |                    |                                 |
| Probable Cause:  | LAN error            |                    |                                 |
| Acknowledged at: | Not Yet              | Specific Problem:  | No response received to mate    |

- 5 You have completed this procedure.

---

—End—

---



## 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.

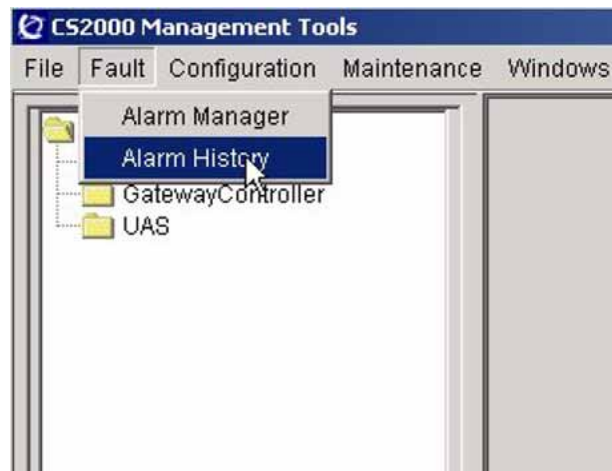
| Step | Action |
|------|--------|
|------|--------|

**At your workstation**

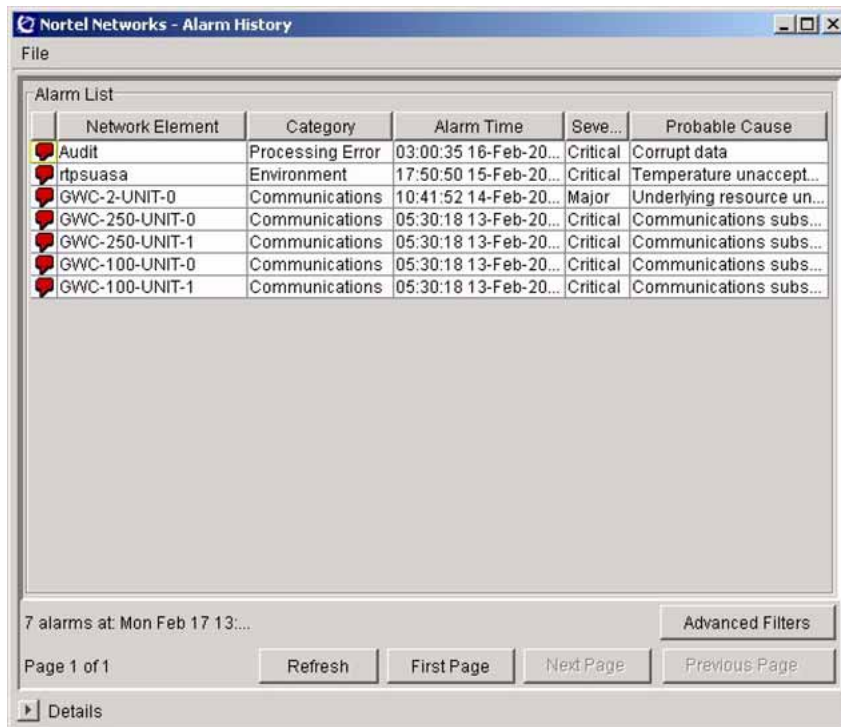
- 1 Launch the CS2000 Management Tools GUI. Refer to procedure Launching CS 2000 Management Tools and NPM client applications in this document if required.

**At the CS2000 Management Tools GUI**

- 2 On the **Fault** menu, click **Alarm History**.



The Alarm History window, similar to following, appears.



**3** You have completed this procedure.

—End—

## 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).

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

| Step | Action |
|------|--------|
|------|--------|

***At your workstation***

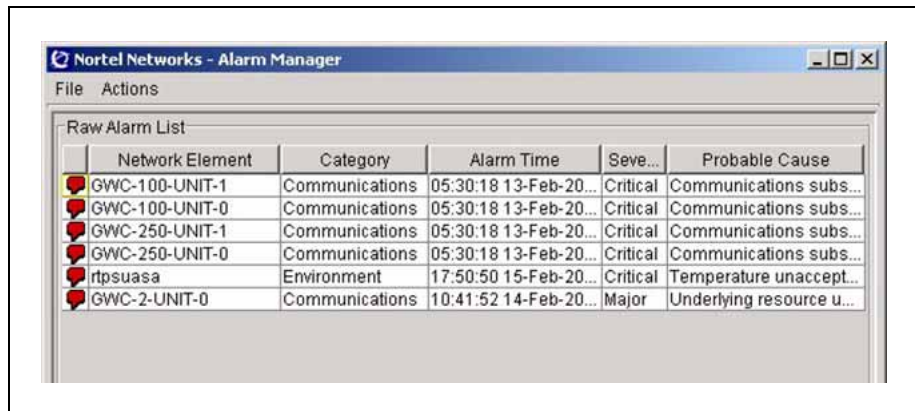
- 1 Launch the CS2000 Management Tools GUI. Refer to procedure Launching CS 2000 Management Tools and NPM client applications in this document if required.

***At the CS2000 Management Tools GUI***

- 2 On the **Fault** menu, click **Alarm Manager**.



The Alarm Manager window opens.



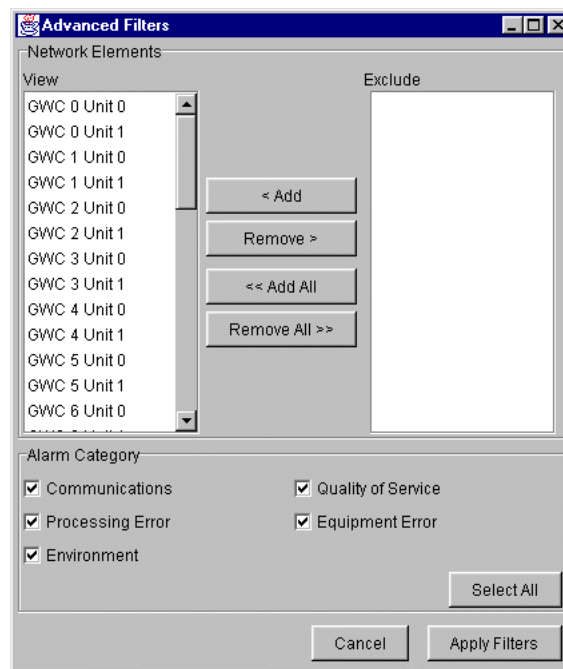
3 Use the following table to determine your next step.

| If you want to filter by          | Do     |
|-----------------------------------|--------|
| network element or alarm category | step 4 |
| severity                          | step 5 |

4 Filter by network element or alarm category as follows:

a. In the **Alarm Manager** window, click **Advanced Filters**.

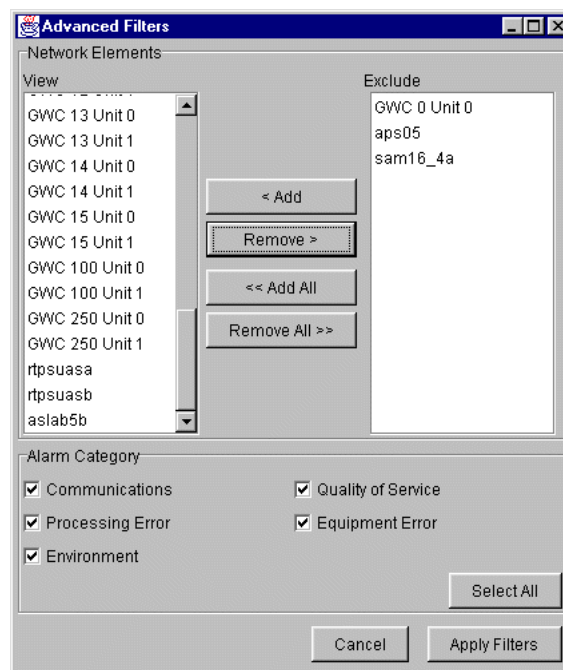
The Advanced Filters window opens.



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.

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.



- 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.

---

—End—

---



## 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.

| Step | Action |
|------|--------|
|------|--------|

*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.

—End—

| Step | Action |
|------|--------|
|------|--------|

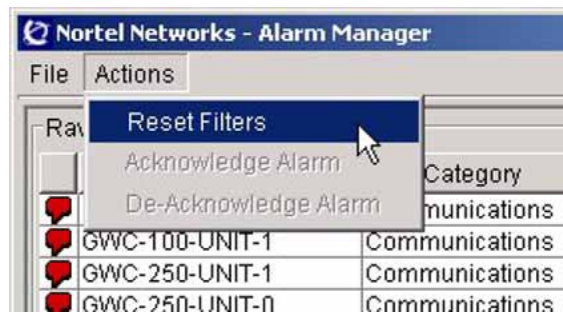
*At the CS2000 Management Tools GUI*

- 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.

---

—End—

---



---

## 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" \(page 749\)](#)
- ["Using the NPM GUI" \(page 750\)](#)

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

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" (page 749) or "Using the NPM GUI" (page 750) to complete this procedure.

### Using the NPM CLUI

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure Accessing the Network Patch Manager CLUI.

#### *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.

---

—End—

---

## Using the NPM GUI

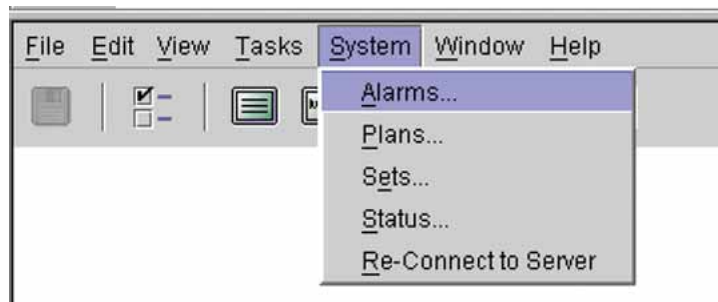
| Step | Action |
|------|--------|
|------|--------|

### *At your workstation*

- 1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications.

### *At the NPM GUI*

- 2 On the **System** menu, click **Alarms....**

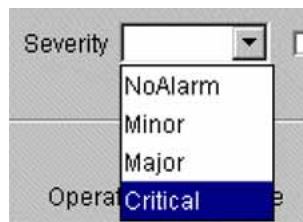


The Alarms window opens.

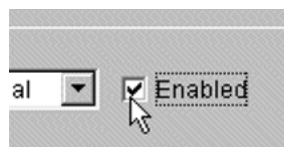
- 3 Select an alarm type from the **Alarm Type** list.



- 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 following table lists the supported operators and their meaning.

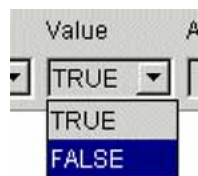
#### Supported operators

| Operator | Meaning   |
|----------|-----------|
| =        | Equal     |
| <>       | Not equal |

| Operator | Meaning                                 |
|----------|-----------------------------------------|
| >        | 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 (%) |

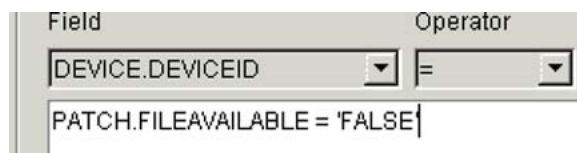
- c. Select the value from the **Value** list, or enter the value.

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. Parenthesis "(" may be inserted to define precedence for multiple criteria statements.



- 9 Enter a unique name for the alarm in the **Alarm Name** box.

 A screenshot of a 'Save Alarm' dialog box. It has two input fields: 'Alarm Name' with the text 'PATCHUNAVAIL' and 'Alarm Description' which is empty. There is a 'Save' button to the right of the 'Alarm Name' field.

- 10 Optionally enter a description for the alarm in the **Alarm description** box.



Save Alarm

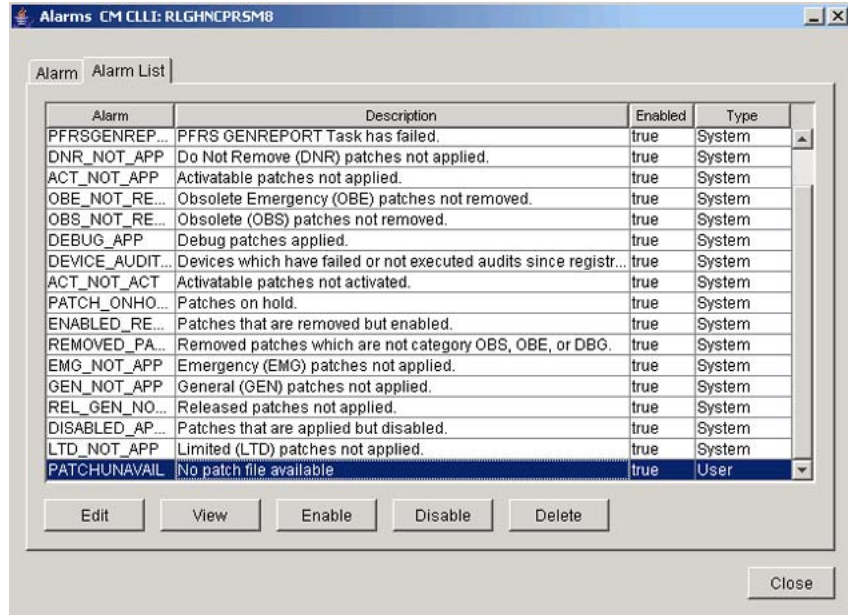
Alarm Name: PATCHUNAVAIL

Alarm Description: No patch file available

Save

- 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.



Alarms CM CLI: RLGHNCPR5M8

Alarm Alarm List

| Alarm           | Description                                                       | Enabled | Type   |
|-----------------|-------------------------------------------------------------------|---------|--------|
| PFRSGENREP...   | PFRS GENREPORT Task has failed.                                   | true    | System |
| DNR_NOT_APP     | Do Not Remove (DNR) patches not applied.                          | true    | System |
| ACT_NOT_APP     | Activatable patches not applied.                                  | true    | System |
| OBE_NOT_RE...   | Obsolete Emergency (OBE) patches not removed.                     | true    | System |
| OBS_NOT_RE...   | Obsolete (OBS) patches not removed.                               | true    | System |
| DEBUG_APP       | Debug patches applied.                                            | true    | System |
| DEVICE_AUDIT... | Devices which have failed or not executed audits since registr... | true    | System |
| ACT_NOT_ACT     | Activatable patches not activated.                                | true    | System |
| PATCH_ONHO...   | Patches on hold.                                                  | true    | System |
| ENABLED_RE...   | Patches that are removed but enabled.                             | true    | System |
| REMOVED_PA...   | Removed patches which are not category OBS, OBE, or DBG.          | true    | System |
| EMG_NOT_APP     | Emergency (EMG) patches not applied.                              | true    | System |
| GEN_NOT_APP     | General (GEN) patches not applied.                                | true    | System |
| REL_GEN_NO...   | Released patches not applied.                                     | true    | System |
| DISABLED_AP...  | Patches that are applied but disabled.                            | true    | System |
| LTD_NOT_APP     | Limited (LTD) patches not applied.                                | true    | System |
| PATCHUNAVAIL    | No patch file available                                           | true    | User   |

Edit View Enable Disable Delete

Close

You have completed this procedure.

—End—

## Performing an audit

---

### Application

Use this procedure to manually perform a line, trunk, V5.2 interface, or CS 2000 (CS2K) data audit.

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 *ATM/IP Configuration Management*, NN10409-500.

### CS 2000 data audit

For a CS2K data audit, the system compares the GWC element manager (EM) database (part of the CS 2000 GWC Manager database) with the CS 2000 XA-Core database and flags any mismatches between the two databases. You need to take action in order to correct a data mismatch. The XA-Core is considered to hold the 'master' database. The system also audits IP-VPN (NAT) datafill internal to Succession Element and Sub-element Manager (SESM) and its CS2KSS EM equivalent. This audit attempts to automatically correct the datafill on CS2K SS EM when a problem is detected. Whether the audit succeeded or failed to correct the problem is indicated in the problem report.

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 GPPTNSL in the CS 2000 XA-Core database

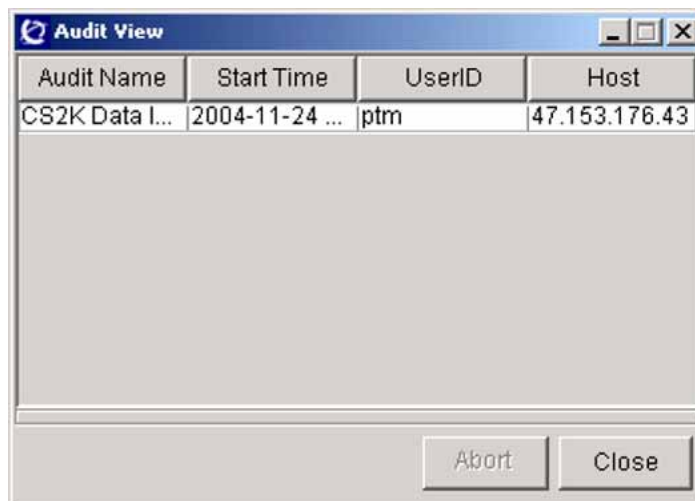
Remedial actions offered are likely to involve deletion of inconsistent data. However, where possible, the option to repair data inconsistencies will be offered.

### **Aborting audits**

All four types of audits can be aborted when running by selecting the View Current Audits option from the Maintenance menu of the CS 2000 Management Tools GUI.

Select the audit you want from the Audit View window and click Abort in order to end an audit currently in progress.





## 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 local user accounts on an SPFS-based server" in *ATM/IP Security and Administration*, NN10402-600.

## Action

Perform the following steps to complete this procedure.

---

### Step Action

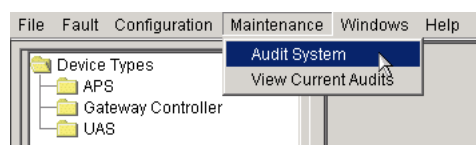
---

#### *At your workstation*

- 1 Launch the CS2000 Management Tools GUI. If required, refer to procedure "[Launching CS 2000 Management Tools and NPM Client Applications](#)" (page 901).

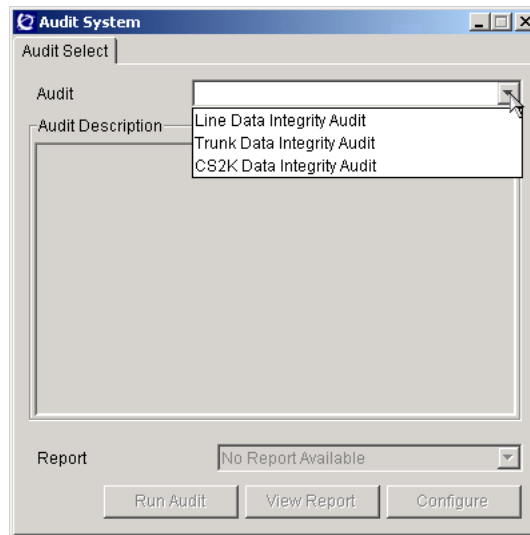
#### *At the CS2000 Management Tools GUI*

- 2 On the **Maintenance** menu, click **Audit System**.



The Audit System window opens.

- 3 In the **Audit** list, select the type of audit you want to perform.
-



In addition to the audit types shown in the preceding example, the international version of the software also contains the V5.2 audit.

- 4 Use the following table to determine your next step.

| If you selected the        | Do      |
|----------------------------|---------|
| CS2K Data Integrity Audit  | step 5  |
| Line Data Integrity Audit  | step 9  |
| Trunk Data Integrity Audit | step 13 |
| V5.2 Data Integrity Audit  | step 13 |

- 5 Click **Run Audit**.
- 6 Select the type of CS2K audit to be run by clicking one or both of the check boxes.



The CS2KSS EM Data Integrity Audit option is only available when the CS2KSS EM is provisioned with SESM.

Choosing the first option runs an audit that compares the GWC manager with the CS 2000 XA-Core database and flags mismatches. Choosing the second option runs an audit that compares the IP-VPN (NAT) datafill internal to SESM and its CS2KSS EM equivalent. Both options can be selected at the same time as well.

**7 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.

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.

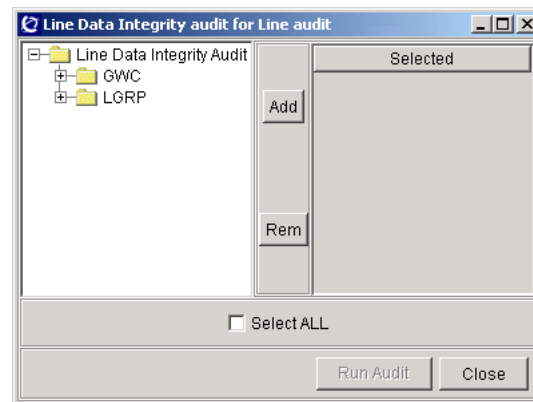
**8 Proceed to step 14.**

**9 Click Run Audit.**

**10 Select the elements you want audited and click Add, or click the Select ALL checkbox to audit the entire call server.**

You cannot select GWCs and LGRPs for the same audit.

The ALL audit (by checking the "Select ALL" checkbox) is not comprised of granular audits (by selecting some GWCs or LGRPs separately). The ALL audit checks line-related data mismatches between XA-Core and the Element Manager database bidirectionally. The granular audit only compares the line-related data in the Element Manager database with XA-Core and not vice versa. The ALL audit and granular audit are implemented in different ways, so there may be some audit result discrepancies between them.



The Line Data Integrity Audit list on the left displays all the small and large line GWCs and the associated gateways, as well as the logical line groups of these small line or large line gateways.

**11** 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.

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.

**12** Proceed to step 14.**13** Click **Run Audit**.**14** Click **Close** to close the Audit Status window once the audit completes.**15** Use the following table to determine your next step.

| If you performed a         | Do      |
|----------------------------|---------|
| CS2K Data Integrity Audit  | step 16 |
| Line Data Integrity Audit  | step 20 |
| Trunk Data Integrity Audit | step 23 |
| V5.2 Data Integrity Audit  | step 26 |

**16** Proceed as follows for a CS2K Data Integrity Audit:

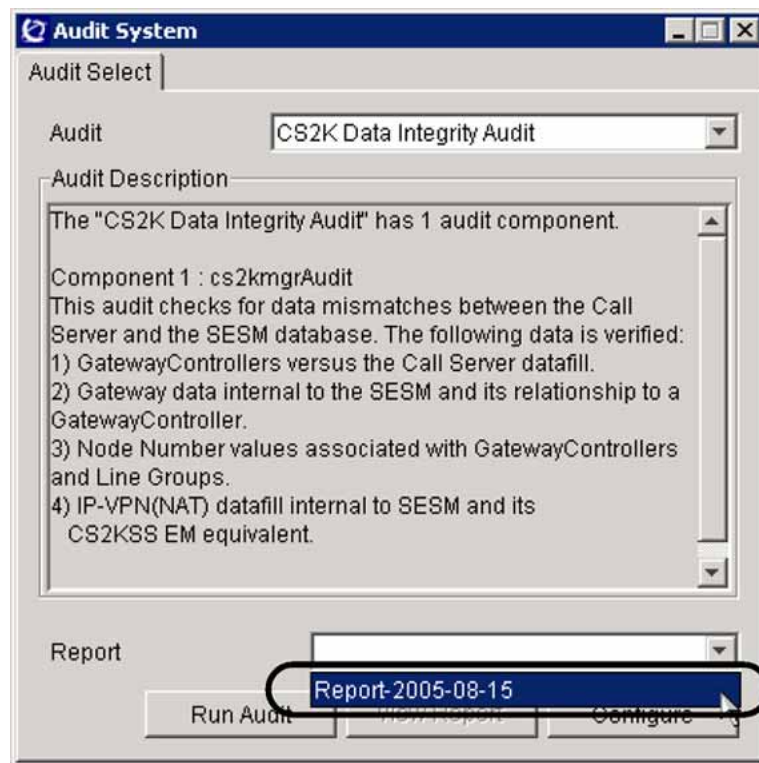
- a. Ensure that you have selected **CS2K Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.
- b. Select **Report** <date> from the pull-down menu in the Report field at the bottom of the dialog box.

The file name has the following format:

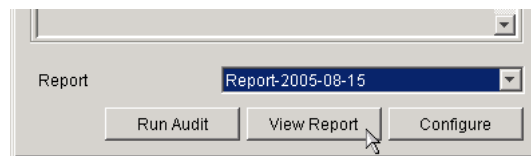
Report- <date>

where

<date> is the date in yyyy-mm-dd format, for example, 2005-07-14.



- 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 containing problems:

The screenshot shows the 'CS2K Data Integrity Audit Report' window. At the top, it says 'Last Audit Date: 2005-08-11 14:24:17'. Below this is a table with three columns: Index, Problem Description, and Current Status. The table lists 30 items. Items 16 through 28 have a status of 'Problem Exists'. Items 29 and 30 have a status of 'Problem Corrected'. Below the table is a 'Problem Detail' section with fields for Problem Number, Problem Description, Current Status, Possible Actions, and a list of Actions with a description. A 'Take Action' button is at the bottom.

| Index | Problem Description                                          | Current Status    |
|-------|--------------------------------------------------------------|-------------------|
| 16    | The LGRP node 'LGRP 00 0' in Call Server is not used in SESM | Problem Exists    |
| 17    | The LGRP node 'MG9K 00 3' in Call Server is not used in SESM | Problem Exists    |
| 18    | The LGRP node 'KEYM 06 0' in Call Server is not used in SESM | Problem Exists    |
| 19    | The LGRP node 'PTGM 00 0' in Call Server is not used in SESM | Problem Exists    |
| 20    | The LGRP node 'KEYM 00 0' in Call Server is not used in SESM | Problem Exists    |
| 21    | The LGRP node 'KEYM 01 0' in Call Server is not used in SESM | Problem Exists    |
| 22    | The LGRP node 'KEYM 02 0' in Call Server is not used in SESM | Problem Exists    |
| 23    | The LGRP node 'MG9K 00 1' in Call Server is not used in SESM | Problem Exists    |
| 24    | The LGRP node 'MUXS 00 0' in Call Server is not used in SESM | Problem Exists    |
| 25    | The LGRP node 'REM1 00 0' in Call Server is not used in SESM | Problem Exists    |
| 26    | The LGRP node 'PHNX 00 0' in Call Server is not used in SESM | Problem Exists    |
| 27    | The LGRP node 'PLG 00 0' in Call Server is not used in SESM  | Problem Exists    |
| 28    | The LGRP node 'KEYM 04 0' in Call Server is not used in SESM | Problem Exists    |
| 29    | Network Zone deneme2 not present on Session Server           | Problem Corrected |
| 30    | Wrong ID for Network Zone deneme on Session Server           | Problem Corrected |

This example report is the result of the user running both the CS2K Call Server Data Integrity Audit and CS2KSS EM Data Integrity Audit. The problems labelled with the status of 'Problem Corrected' were automatically corrected as part of the CS2KSS EM Data Integrity Audit.

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.

The system places the audit report in the following directory on the CS 2000 Management Tools server:  
/opt/nortel/ptm/current/MI2/apps/Audit.

The CS 2000 GWC Manager does not provide an option to save a CS 2000 data audit report to local disk.

- 17 Review the results of the audit and click on a problem with the status of 'Problem Exists' that needs to be resolved.

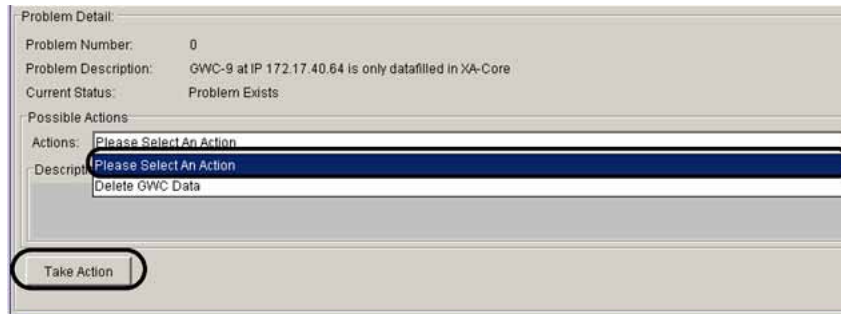
If necessary, resize the entire window to completely view the Problem Description field.

The screenshot shows the 'CS2K Data Integrity Audit Report' window. At the top, it says 'Last Audit Date: 2002-07-29 14:58:22'. Below this is a table with three columns: Index, Problem Description, and Current Status. The table lists 4 items, all with a status of 'Problem Exists'.

| 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 |

- 18 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**.

If you see the message "Correction Failed", please contact your next level of support.

- 19 Return to [step 17](#) to review another problem.
- 20 Proceed as follows for a Line Data Integrity Audit:

| If you want to view          | Do                          |
|------------------------------|-----------------------------|
| the line valid-data report   | step <a href="#">Step 8</a> |
| the line problem-data report | step <a href="#">22</a>     |

- 21 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.

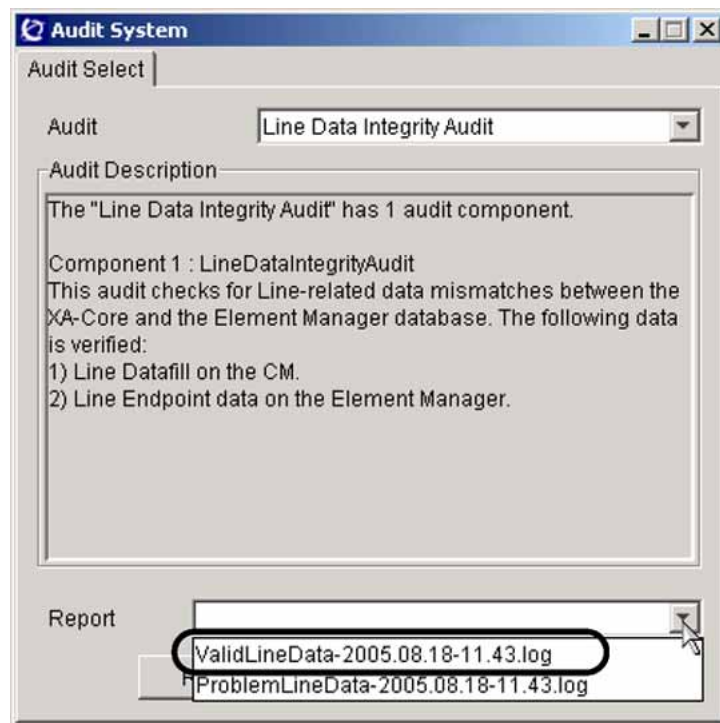
The file name has the following format:

ValidLineData-<date>-<time>.log

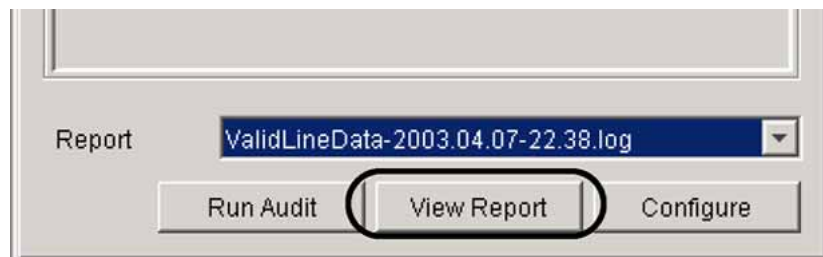
where

<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 | nglkr1013.nortel.com   |
| LG 00 2 02 42 | LG 00 2 | 243 | GWC-44 | nglkr1013.nortel.com   |
| LG 00 2 02 43 | LG 00 2 | 244 | GWC-44 | nglkr1013.nortel.com   |
| LG 00 2 02 44 | LG 00 2 | 245 | GWC-44 | nglkr1013.nortel.com   |
| LG 00 2 02 45 | LG 00 2 | 246 | GWC-44 | nglkr1013.nortel.com   |
| LG 00 2 02 46 | LG 00 2 | 247 | GWC-44 | nglkr1013.nortel.com   |
| LG 00 2 02 48 | LG 00 2 | 249 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 49 | LG 00 2 | 250 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 50 | LG 00 2 | 251 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 51 | LG 00 2 | 252 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 52 | LG 00 2 | 253 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 53 | LG 00 2 | 254 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 54 | LG 00 2 | 255 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 55 | LG 00 2 | 256 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 56 | LG 00 2 | 257 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 57 | LG 00 2 | 258 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 58 | LG 00 2 | 259 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 59 | LG 00 2 | 260 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 60 | LG 00 2 | 261 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 61 | LG 00 2 | 262 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 62 | LG 00 2 | 263 | GWC-44 | nglkr1014.nortel.com   |
| LG 00 2 02 63 | LG 00 2 | 264 | GWC-44 | nglkr1014.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 | nglkr1012.nortel.com   |

or Event Messaging Supported Line Data Integrity)

| GWC     | GWC NAME               | EP NAME |
|---------|------------------------|---------|
| GWC-100 | isplab3nccs.nortel.com | aaln/1  |
| GWC-100 | isplab3nccs.nortel.com | aaln/2  |
| GWC-100 | isplab3nccs.nortel.com | aaln/3  |
| GWC-100 | isplab3nccs.nortel.com | aaln/4  |

Prev Next Save as Exit

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.

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.

## 22 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.

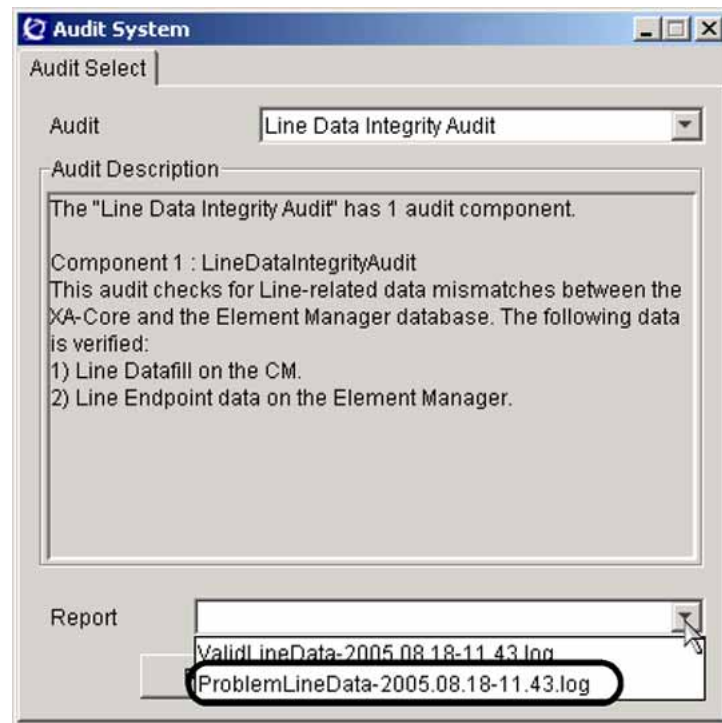
The file name has the following format:

ProblemLineData-<date>-<time>.log

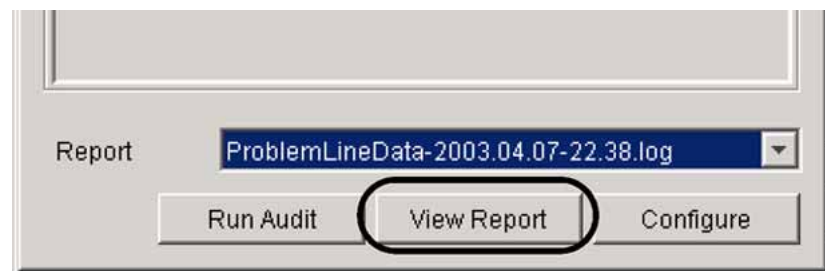
where

<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.

Following is an example of a "ProblemLineData" report:

```

ProblemLineData-2005.02.17-14.52.log
Page: 1/1
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 ambtlp4217nat.nortel.com on GWC GWC-116 has no associated LEN on CM

Invalid Data (For Event Messaging 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 HOBDAQOS1 has no associated endpoint on GWCEM
LEN LG 00 1 03 51 for EndPoint aaln/2 on Gateway HOBDAQOS1 has no associated endpoint on GWCEM
LEN LG 00 1 03 52 for EndPoint aaln/3 on Gateway HOBDAQOS1 has no associated endpoint on GWCEM
LEN LG 00 1 03 53 for EndPoint aaln/4 on Gateway HOBDAQOS1 has no associated endpoint on GWCEM
LEN LG 00 1 03 64 for EndPoint aaln/1 on Gateway HOBDAQOS2 has no associated endpoint on GWCEM
LEN LG 00 1 03 65 for EndPoint aaln/2 on Gateway HOBDAQOS2 has no associated endpoint on GWCEM
LEN LG 00 1 03 66 for EndPoint aaln/3 on Gateway HOBDAQOS2 has no associated endpoint on GWCEM
LEN LG 00 1 03 67 for EndPoint aaln/4 on Gateway HOBDAQOS2 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

```

The CS 2000 Management Tools server retains the six most recent "ProblemLineData" reports. When a new audit occurs, the server deletes the oldest report.

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/.

- 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.
- 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.

**23** Proceed as follows for a Trunk Data Integrity Audit:

| If you want to view           | Do      |
|-------------------------------|---------|
| the trunk valid-data report   | step 24 |
| the trunk problem-data report | step 25 |

**24** 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.

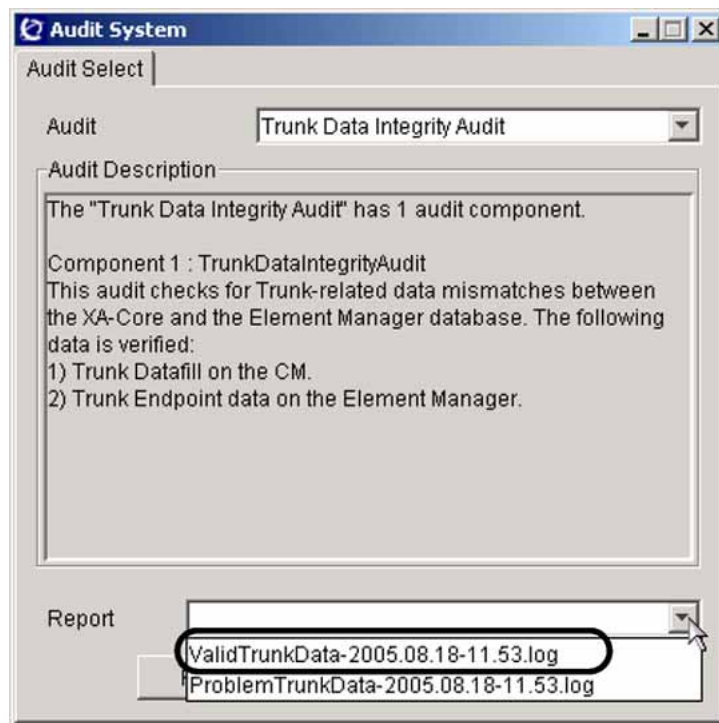
The file name has the following format:

ValidTrunkData-<date>-<time>.log

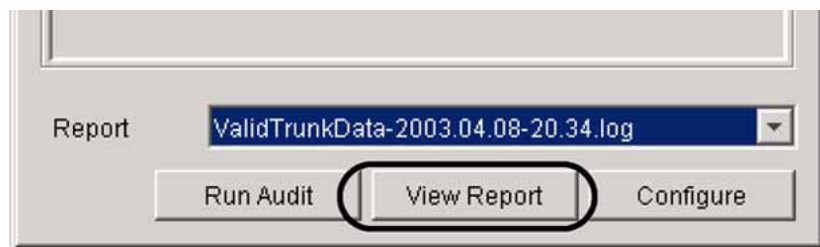
where

<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

Goto page:

| CLLI    | TRK# | GWC   | NODE | TN | GW NAME | EF 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

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.

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.

## 25 View the trunk problem-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 **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:

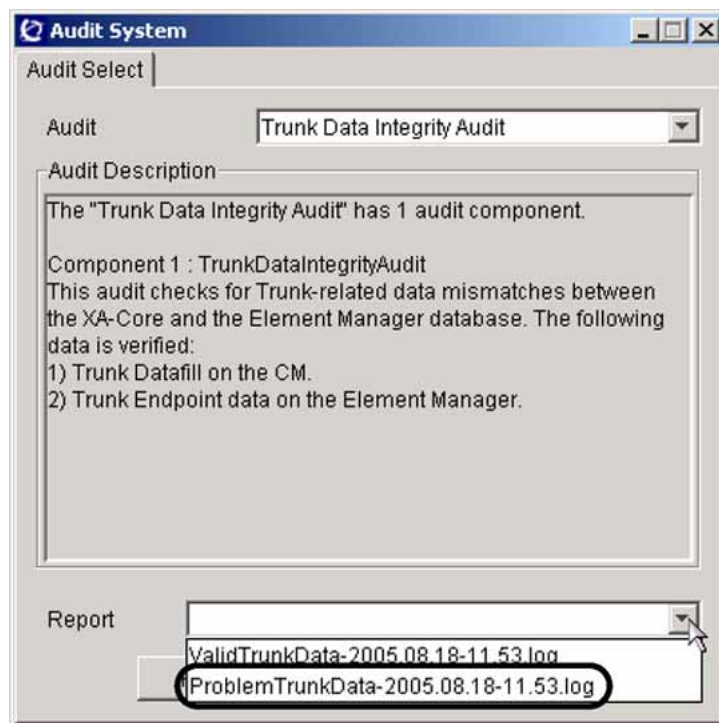


ProblemTrunkData-<date>-<time>.log

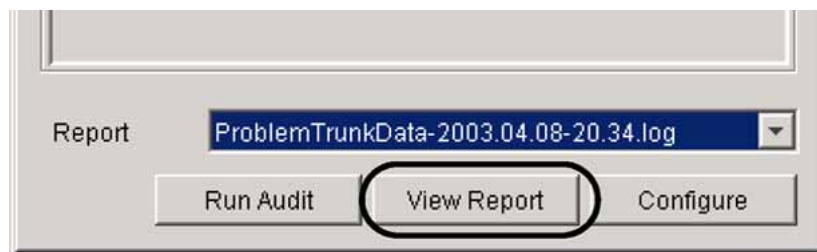
where

<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.



- c. Click the **View Report** button.



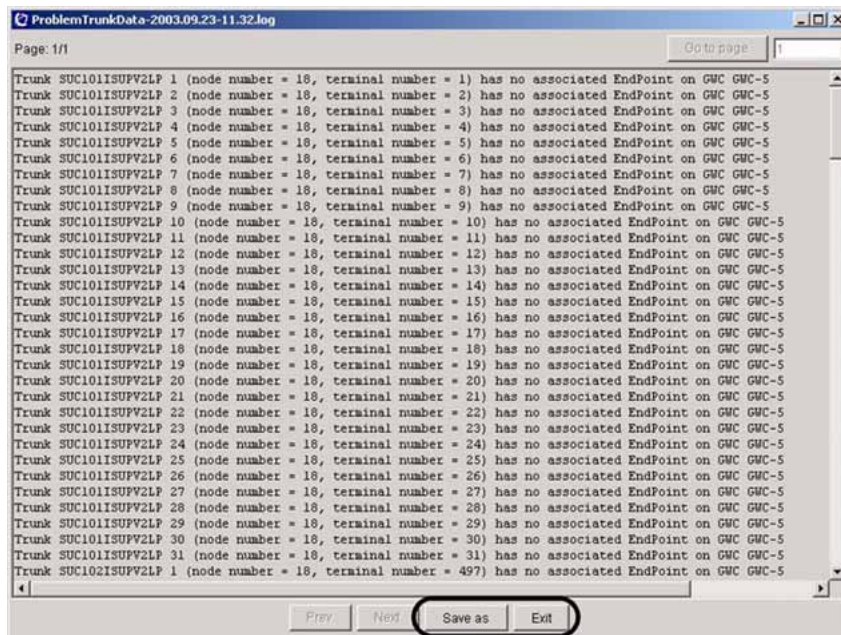
The system displays the selected report.

If the audit found no problems, the "Problem" report contains a message stating that no problems were found.

The "Problem" report produced by a 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 datafiled on the CM.

Here is an example of a "ProblemTrunkData" report:



The CS 2000 Management Tools server retains the six most recent "ProblemTrunkData" reports. When a new audit occurs, the server deletes the oldest report.

The system places trunk audit reports in the following directory on the CS 2000 Management Tools server:  
/opt/nortel/ptm/current/www/Audit/TrunkDataIntegrityAudit/.

- 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.
- To print a report you have saved, open the file using a text editor and print the file.
- To correct the problems, refer to the printed copy of the report. You will need to delete and then reprovision the listed trunks.



- g. After viewing the problem-data report, click **Exit** at the bottom of the viewer screen.

**26** View a V5.2 audit report as follows:

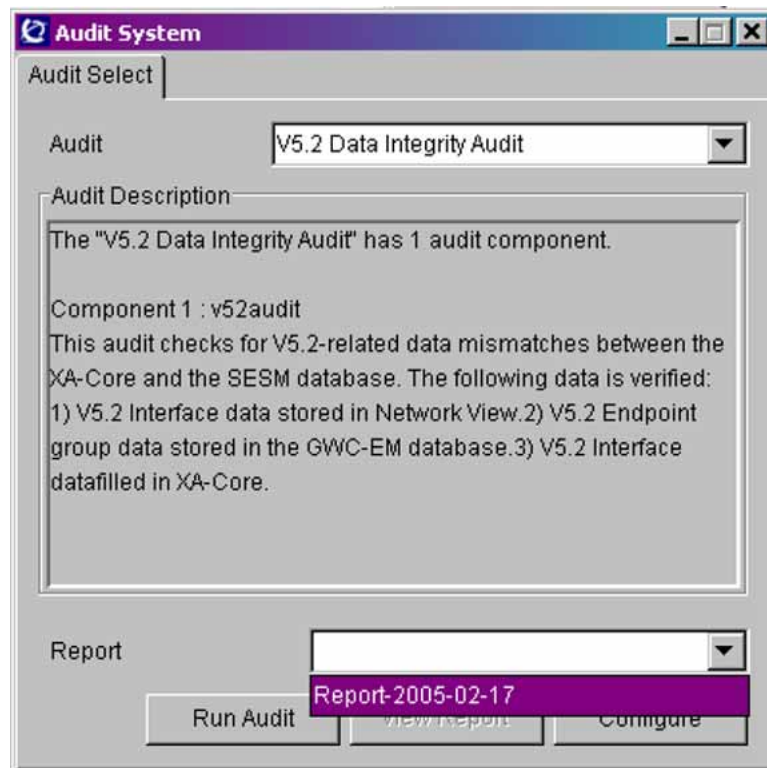
- a. Ensure that you have selected **V5.2 Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.
- b. Select **Report** <date> from the pull-down menu in the Report field at the bottom of the dialog box.

The file name has the following format:

Report-<date>

where

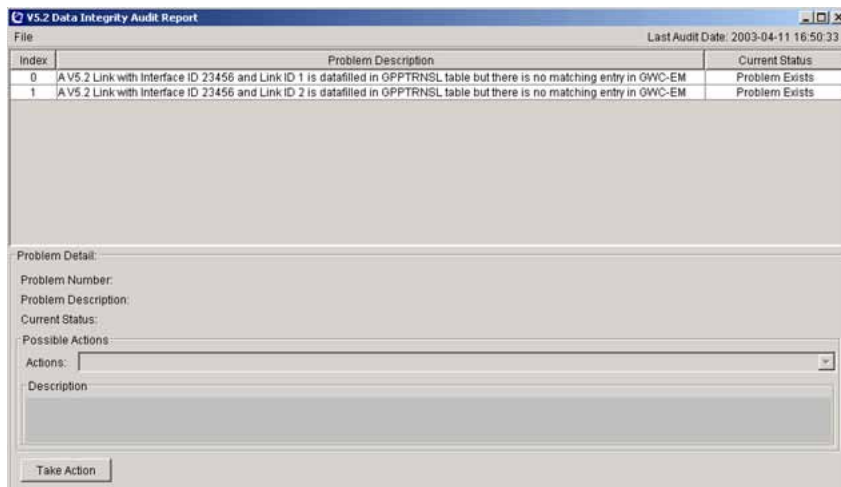
<date> is the date in yyyy-mm-dd format, for example, 2003-02-15.



- c. Click **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:



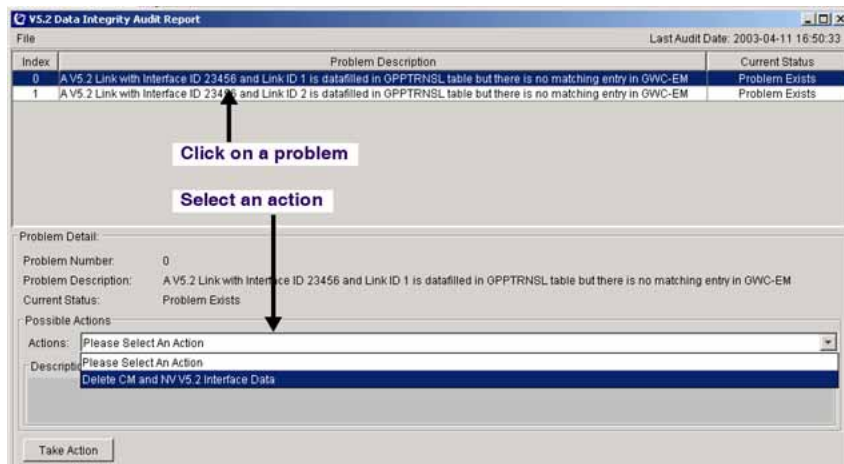
The CS 2000 Management Tools server retains the most recent V5.2 audit report. When a new audit occurs, the server deletes the previous report.

The system places the audit report in the following directory on the CS 2000 Management Tools server:  
/opt/nortel/ptm/current/MI2/apps/Audit.

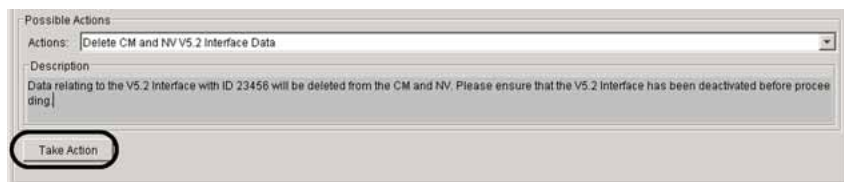
The CS 2000 GWC Manager does not provide an option to save a V5.2 audit report to local disk.

- 27 Review the results of the audit and click on a problem to resolve.  
If necessary, resize the entire window to completely view the Problem Description field.
- 28 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**.



If you see the message "Correction Failed", please contact your next level of support.

- 29** Return to Step 9 to review another problem.

You have completed this procedure.

—End—

## 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 CVoIP 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.

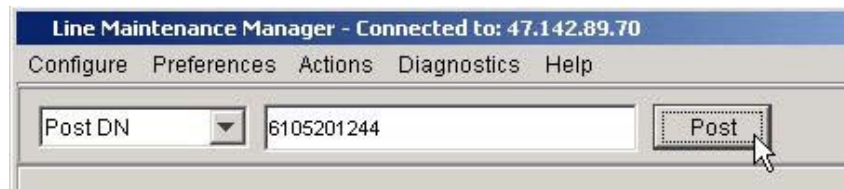
| Step | Action |
|------|--------|
|------|--------|

#### *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 **Post DN**, enter the directory number, and click **Post**.



**3** You have completed this procedure.

---

—End—

---

## 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.

| Step | Action |
|------|--------|
|------|--------|

#### *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 **Post by Gateway**, enter the name of the gateway and its path, then click **Post**.



**3** You have completed this procedure.

—End—

## 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                  |
| 2010       | EP_Not_Found                              | Endpoint status expired in GWC before retrieval |
| 2020       | Invalid_EP                                | Endpoint does not exist in GWC                  |

| Error Code | LMM client text displayed in status panel | Description                                   |
|------------|-------------------------------------------|-----------------------------------------------|
| 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"](#) (page 777) or ["Posting a line by directory number"](#) (page 775) in this document, if required.

### Action

Perform the following steps to complete this procedure.

| Step                       | Action                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>At your workstation</b> |                                                                                                                                                                                                                                                                                                                                                                              |
| 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.                                                                                                                                                                                                              |
| <b>At the LMM GUI</b>      |                                                                                                                                                                                                                                                                                                                                                                              |
| 2                          | Select the DN you want to busy, then on the <b>Actions</b> menu, click <b>BSY</b> , or right-click on the selected DN then click <b>BSY</b> .<br><br>You can perform this operation on one or more posted lines at the same time. You can use the <b>Shift</b> key to select multiple lines consecutively, or the <b>Ctrl</b> 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.

The line state will be CPD if the original line state was CPB prior to Busy.



- 4 You have completed this procedure.

—End—

---

## 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" \(page 777\)](#) or ["Posting a line by directory number" \(page 775\)](#) in this document, if required.

### Action

Perform the following steps to complete this procedure.

---

| Step | Action |
|------|--------|
|------|--------|

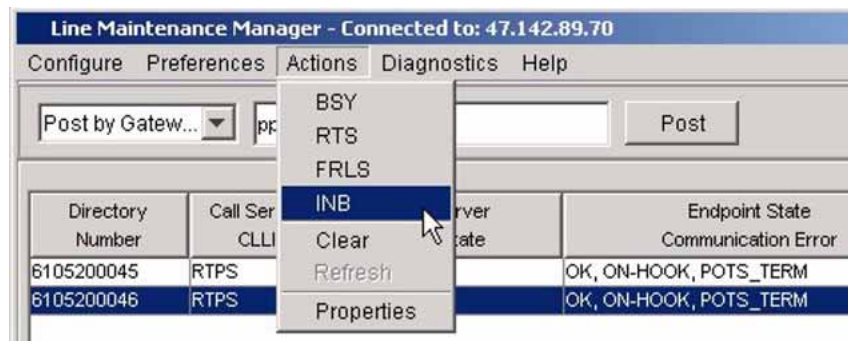
---

#### *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**.  
  
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.

—End—

## 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 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" \(page 777\)](#) or ["Posting a line by directory number" \(page 775\)](#) in this document, if required.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *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 force a release on, then on the **Actions** menu, click **FRLS**, or right-click on the selected DN then click **FRLS**.  
  
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.

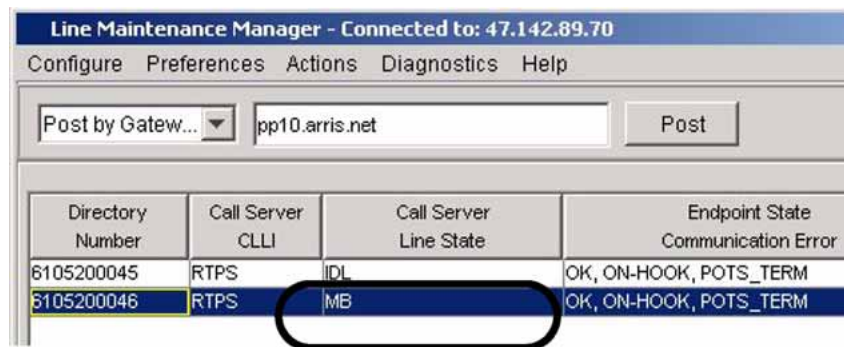


- 3 Click **OK** to confirm the force release of the line(s).



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.

—End—

## 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"](#) (page 780) in this document, if required.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

***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 return to service, then on the **Actions** menu, click **RTS**, or right-click on the selected DN then click **RTS**.  
  
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.

—End—



---

## 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"](#) (page 777) or ["Posting a line by directory number"](#) (page 775) in this document, if required.

### Action

Perform the following steps to complete this procedure.

---

| Step | Action |
|------|--------|
|------|--------|

---

#### *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*

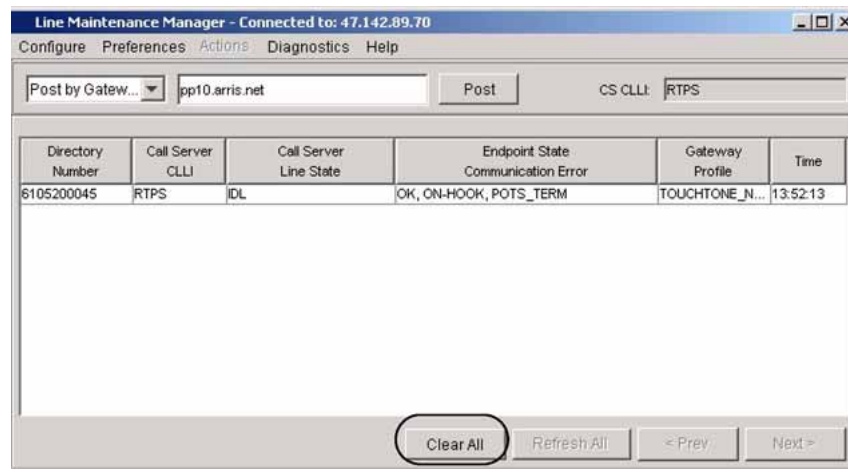
- 2 Select the DN you want to remove from the display of posted lines, then on the **Actions** menu, click **Clear**, or right-click on the selected DN then click **Clear**.

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.

To clear all posted DN, click **Clear All**.



- 4 You have completed this procedure.

—End—

## 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" \(page 777\)](#) or ["Posting a line by directory number" \(page 775\)](#) in this document, if required.

### Action

Perform the following steps to complete this procedure.

---

| Step | Action |
|------|--------|
|------|--------|

---

#### *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.

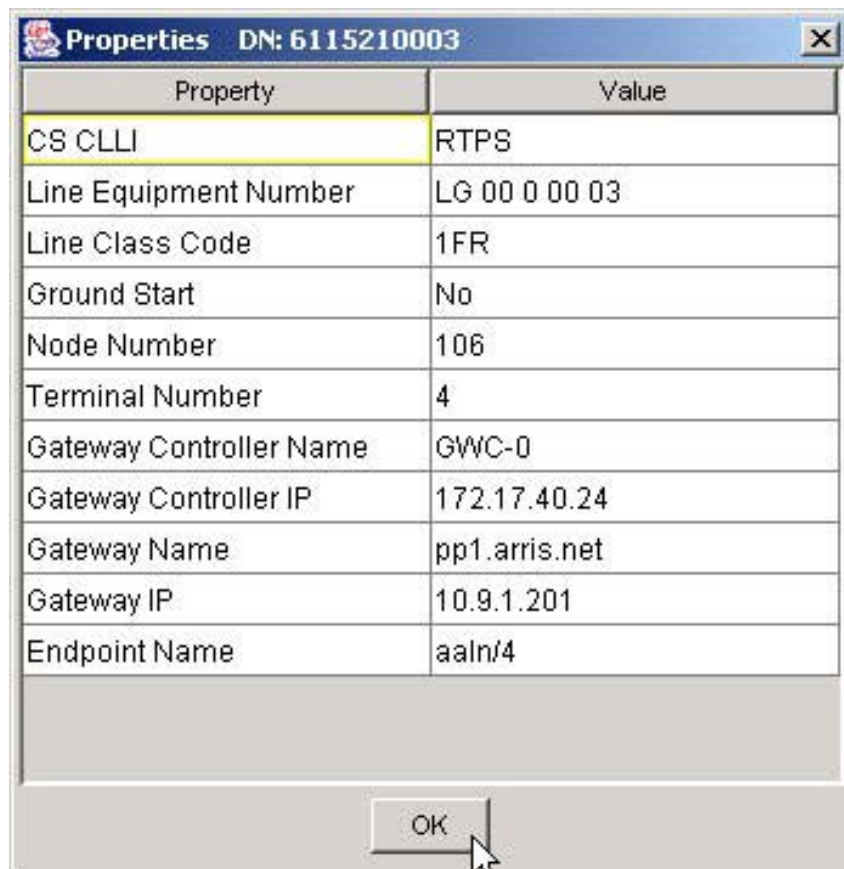
#### *At the LMM GUI*

- 2 Select the DN you want to view the properties for, then on the **Actions** menu, click **Properties**, or right-click on the selected DN then click **Properties**.

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.



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.

---

—End—

---

## 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.

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 *ATM/IP Solution-level Configuration Management*, 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.

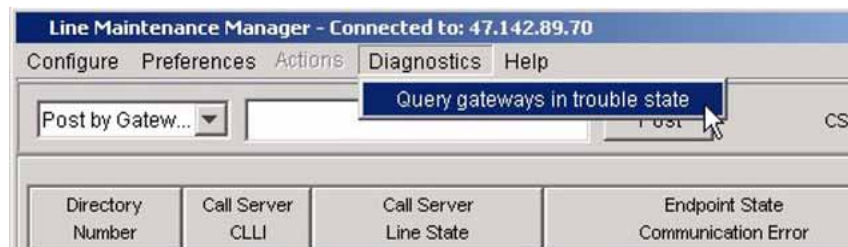
| Step | Action |
|------|--------|
|------|--------|

#### *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.

#### *At the LMM GUI*

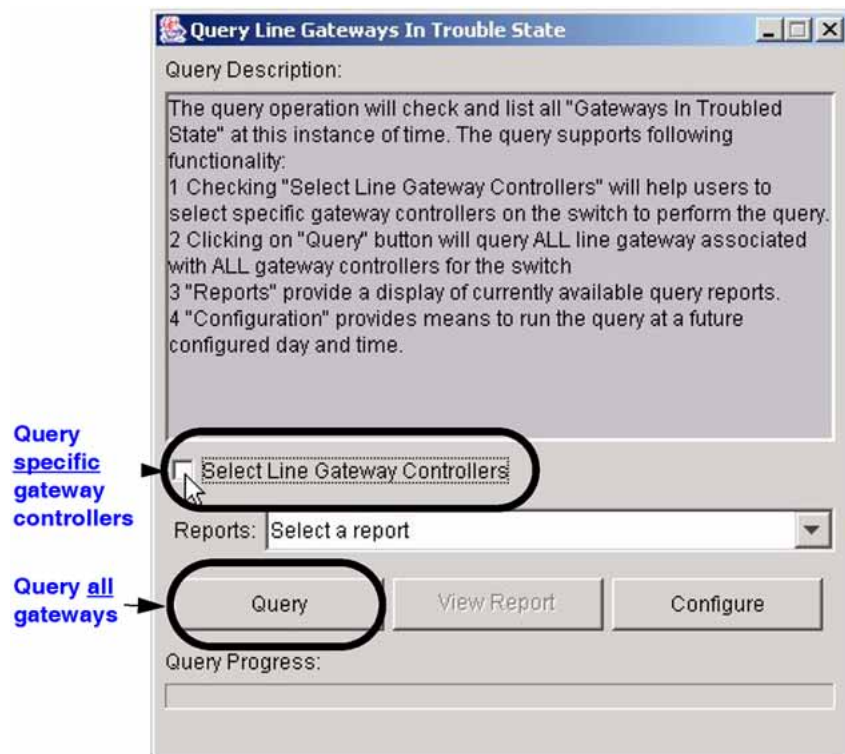
- 2 On the **Diagnostics** menu, click **Query gateways in trouble state**.



- 3 Use the following table to determine your next step.

| If you want to  | Do     |
|-----------------|--------|
| perform a query | step 4 |
| view reports    | step 8 |

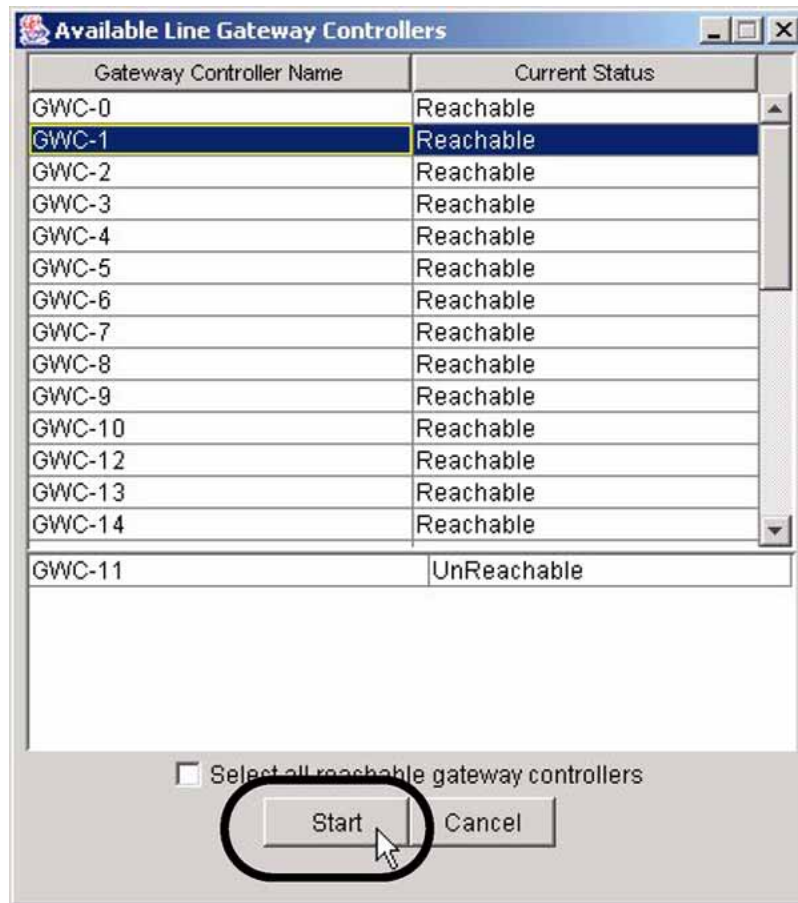
- 4 Click **Query** to query all line gateways associated with all gateway controllers for the switch, or click the **Select line gateway controllers** check box to query all line gateways associated with specific gateway controllers .



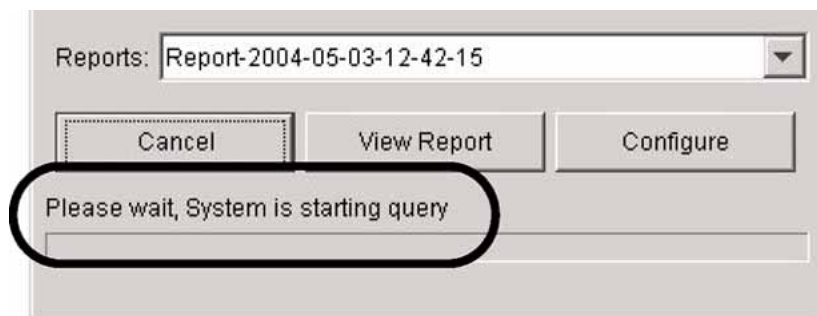
- 5 Use the following table to determine your next step.

| If you are querying          | Do     |
|------------------------------|--------|
| specific gateway controllers | step 6 |
| all gateways                 | step 7 |

- 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.



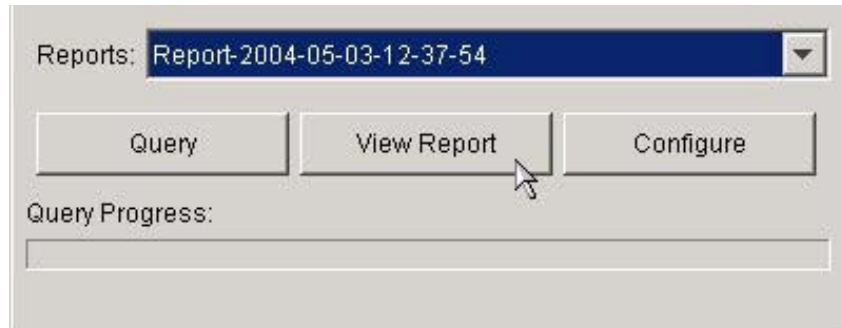
Click **Cancel** at any time to cancel the query.

- 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.



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      |             |
| GWC-B                                  | Successful   | 580                | GWC08_OrigGW1 ... | GW DISABLED |
|                                        |              |                    | GWC08_OrigGW1 ... | GW DISABLED |
|                                        |              |                    | GWC08_OrigGW1 ... | GW DISABLED |
|                                        |              |                    | GWC08_OrigGW1 ... | GW DISABLED |
|                                        |              |                    | GWC08_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                              |
| 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)                                             |
| 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.

---

—End—

---

## 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" \(page 799\)](#)
- ["Maintenance by Gateway Name" \(page 803\)](#)
- ["Maintenance by trunk CLLI" \(page 808\)](#)

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" \(page 799\)](#) or ["Maintenance by Gateway Name" \(page 803\)](#) 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" \(page 799\)](#)
- ["Maintenance by Gateway Name" \(page 803\)](#)

- "Maintenance by trunk CLLI" (page 808)

## Maintenance by carrier

| Step | Action |
|------|--------|
|------|--------|

### 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.

### At the TMM GUI

- 2 Click **Maintenance By Carrier**.

A window similar to the following is displayed:

- 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.  
  
The Force Release Endpoints (FRLS) maintenance action does not support a range of endpoints. Individual endpoints must be specified, or listed with a comma between them for multiple endpoints (eg, 1,3,5,10).
  - 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- |                      |  |  |                 |     |  |     |     |  |         |     |  |     |   |  |     |     |  |    |   |  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------|-----------------------|----------------------|--|--|-----------------|-----|--|-----|-----|--|---------|-----|--|-----|---|--|-----|-----|--|----|---|--|
| <table><tr><th colspan="2">Summary of Endpoints</th><td></td></tr><tr><td>Total Endpoints</td><td>672</td><td></td></tr><tr><td>IDL</td><td>289</td><td></td></tr><tr><td>UNKNOWN</td><td>138</td><td></td></tr><tr><td>RMB</td><td>5</td><td></td></tr><tr><td>INB</td><td>227</td><td></td></tr><tr><td>MB</td><td>5</td><td></td></tr></table> |                    |                           |                       | Summary of Endpoints |  |  | Total Endpoints | 672 |  | IDL | 289 |  | UNKNOWN | 138 |  | RMB | 5 |  | INB | 227 |  | MB | 5 |  |
| 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- |               |            |              |            |             |                      |  |  |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------------------|-----------|---------------------------|----------|-----------------------|---------------|------------|--------------|------------|-------------|----------------------|--|--|-----------------|--|-----|-----|--|-----|---------|--|-----|-----|--|---|-----|--|-----|----|--|---|
| <table><tr><th colspan="2">Summary of Endpoints</th><td></td></tr><tr><td>Total Endpoints</td><td></td><td>672</td></tr><tr><td>IDL</td><td></td><td>289</td></tr><tr><td>UNKNOWN</td><td></td><td>150</td></tr><tr><td>RMB</td><td></td><td>5</td></tr><tr><td>INB</td><td></td><td>223</td></tr><tr><td>MB</td><td></td><td>5</td></tr></table> |       |                    |           |                           |          |                       |               |            |              |            |             | Summary of Endpoints |  |  | Total Endpoints |  | 672 | IDL |  | 289 | UNKNOWN |  | 150 | RMB |  | 5 | INB |  | 223 | MB |  | 5 |
| 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           |                      |  |  |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |

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 in the following figure.



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>PVG190                                                                                                                                                                                                                                                                                                                           |       | Node Number:<br>13 |           | Filtered by State:<br>MB |          | Endpoint Range:<br>0- |               |                      |              |            |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------------------|-----------|--------------------------|----------|-----------------------|---------------|----------------------|--------------|------------|-----------------|--|-----|-----|--|-----|---------|--|-----|-----|--|---|-----|--|-----|----|--|---|
| <table><tr><th colspan="2">Summary of Endpoints</th><td></td></tr><tr><td>Total Endpoints</td><td></td><td>672</td></tr><tr><td>IDL</td><td></td><td>289</td></tr><tr><td>UNKNOWN</td><td></td><td>150</td></tr><tr><td>RMB</td><td></td><td>5</td></tr><tr><td>INB</td><td></td><td>223</td></tr><tr><td>MB</td><td></td><td>5</td></tr></table> |       |                    |           |                          |          |                       |               | Summary of Endpoints |              |            | Total Endpoints |  | 672 | IDL |  | 289 | UNKNOWN |  | 150 | RMB |  | 5 | INB |  | 223 | MB |  | 5 |
| 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  | AL17IBNT2S7CGAD      | 2            | 0          | 1               |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| 619                                                                                                                                                                                                                                                                                                                                               | MB    |                    | 2W        | S7 S7                    | GWC_NODE | 1                     | DS3_20.26.19  | AL17IBNT2S7CGAD      | 4            | 0          | 1               |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| 620                                                                                                                                                                                                                                                                                                                                               | MB    |                    | 2W        | S7 S7                    | GWC_NODE | 1                     | DS3_20.26.20  | AL17IBNT2S7CGAD      | 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:<br>PV0190                                                                                                                                                                                                                                                                                                                                             |        | Node Number:<br>13 |           | Filtered by State:<br>IDL |          | Endpoint Range:<br>0- |               |            |              |            |             |                      |  |  |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|--------------------|-----------|---------------------------|----------|-----------------------|---------------|------------|--------------|------------|-------------|----------------------|--|--|-----------------|--|-----|-----|--|-----|---------|--|-----|-----|--|---|-----|--|-----|----|--|---|
| <table><tr><th colspan="2">Summary of Endpoints</th><th></th></tr><tr><td colspan="2">Total Endpoints</td><td>672</td></tr><tr><td colspan="2">IDL</td><td>269</td></tr><tr><td colspan="2">UNKNOWN</td><td>150</td></tr><tr><td colspan="2">RMB</td><td>5</td></tr><tr><td colspan="2">INB</td><td>223</td></tr><tr><td colspan="2">MB</td><td>5</td></tr></table> |        |                    |           |                           |          |                       |               |            |              |            |             | Summary of Endpoints |  |  | Total Endpoints |  | 672 | IDL |  | 269 | UNKNOWN |  | 150 | RMB |  | 5 | INB |  | 223 | MB |  | 5 |
| Summary of Endpoints                                                                                                                                                                                                                                                                                                                                                |        |                    |           |                           |          |                       |               |            |              |            |             |                      |  |  |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| Total Endpoints                                                                                                                                                                                                                                                                                                                                                     |        | 672                |           |                           |          |                       |               |            |              |            |             |                      |  |  |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| IDL                                                                                                                                                                                                                                                                                                                                                                 |        | 269                |           |                           |          |                       |               |            |              |            |             |                      |  |  |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| UNKNOWN                                                                                                                                                                                                                                                                                                                                                             |        | 150                |           |                           |          |                       |               |            |              |            |             |                      |  |  |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| RMB                                                                                                                                                                                                                                                                                                                                                                 |        | 5                  |           |                           |          |                       |               |            |              |            |             |                      |  |  |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| INB                                                                                                                                                                                                                                                                                                                                                                 |        | 223                |           |                           |          |                       |               |            |              |            |             |                      |  |  |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| MB                                                                                                                                                                                                                                                                                                                                                                  |        | 5                  |           |                           |          |                       |               |            |              |            |             |                      |  |  |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| Endpoint Number                                                                                                                                                                                                                                                                                                                                                     | Status | 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**.

The Force Release Endpoints (FRLS) maintenance action does not support a range of endpoints. Individual endpoints must be specified, or listed with a comma between them for multiple endpoints (eg, 1,3,5,10).

Following is an example of the response:

Observe that the selected carriers are manual busy (MB).

| Gateway Name:<br>PV0190                                                                                                                                                                                                                                                                                                                           |        | Node Number:<br>13 |           | Filtered by State:<br>MB |          | Endpoint Range:<br>0- |               |                      |              |            |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|--------------------|-----------|--------------------------|----------|-----------------------|---------------|----------------------|--------------|------------|-----------------|--|-----|-----|--|-----|---------|--|-----|-----|--|---|-----|--|-----|----|--|---|
| <table><tr><th colspan="2">Summary of Endpoints</th><th></th></tr><tr><td>Total Endpoints</td><td></td><td>672</td></tr><tr><td>IDL</td><td></td><td>269</td></tr><tr><td>UNKNOWN</td><td></td><td>150</td></tr><tr><td>RMB</td><td></td><td>5</td></tr><tr><td>INB</td><td></td><td>223</td></tr><tr><td>MB</td><td></td><td>5</td></tr></table> |        |                    |           |                          |          |                       |               | Summary of Endpoints |              |            | Total Endpoints |  | 672 | IDL |  | 269 | UNKNOWN |  | 150 | RMB |  | 5 | INB |  | 223 | MB |  | 5 |
| Summary of Endpoints                                                                                                                                                                                                                                                                                                                              |        |                    |           |                          |          |                       |               |                      |              |            |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| Total Endpoints                                                                                                                                                                                                                                                                                                                                   |        | 672                |           |                          |          |                       |               |                      |              |            |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| IDL                                                                                                                                                                                                                                                                                                                                               |        | 269                |           |                          |          |                       |               |                      |              |            |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| UNKNOWN                                                                                                                                                                                                                                                                                                                                           |        | 150                |           |                          |          |                       |               |                      |              |            |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| RMB                                                                                                                                                                                                                                                                                                                                               |        | 5                  |           |                          |          |                       |               |                      |              |            |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| INB                                                                                                                                                                                                                                                                                                                                               |        | 223                |           |                          |          |                       |               |                      |              |            |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| MB                                                                                                                                                                                                                                                                                                                                                |        | 5                  |           |                          |          |                       |               |                      |              |            |                 |  |     |     |  |     |         |  |     |     |  |   |     |  |     |    |  |   |
| Endpoint Number                                                                                                                                                                                                                                                                                                                                   | Status | 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:<br>PV0190                                                                                                                                                                                                                                           |       | Node Number:<br>13 |           | Filtered by State:<br>INB |          | Endpoint Range:<br>0- |               |            |              |            |            |     |   |     |   |     |     |  |  |
| <div>Summary of Endpoints</div> <table><tr><td>Total Endpoints</td><td>672</td></tr><tr><td>IDL</td><td>287</td></tr><tr><td>UNKNOWN</td><td>150</td></tr><tr><td>RMB</td><td>5</td></tr><tr><td>CPB</td><td>2</td></tr><tr><td>INB</td><td>223</td></tr></table> |       |                    |           |                           |          | Total Endpoints       | 672           | IDL        | 287          | UNKNOWN    | 150        | RMB | 5 | CPB | 2 | INB | 223 |  |  |
| 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 TimeSta |     |   |     |   |     |     |  |  |
| 14                                                                                                                                                                                                                                                                | INB   |                    | 2W        | S7 S7                     | GWC_NODE | 1                     | DS3_20.1.14   | PPATCOG    | 2            | 0          | 1          |     |   |     |   |     |     |  |  |
| 38                                                                                                                                                                                                                                                                | INB   |                    | 2W        | S7 S7                     | GWC_NODE | 1                     | DS3_20.2.14   | PPEANTIC   | 2            | 0          | 1          |     |   |     |   |     |     |  |  |
| 140                                                                                                                                                                                                                                                               | INB   |                    | 2W        | S7 S7                     | GWC_NODE | 1                     | DS3_20.7.4    | SEITIDV2   | 1            | 0          | 1          |     |   |     |   |     |     |  |  |

- 5 Use the following table to determine your next step.

| If you                                | Do                                |
|---------------------------------------|-----------------------------------|
| want to perform another action        | step 4                            |
| do not want to perform another action | you have completed this procedure |

—End—

## Maintenance by Gateway Name

### Step Action

#### 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 **Maintenance By Gateway Name**.

A window similar to the following, is displayed.



- 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-              |

| Summary of Endpoints |  |
|----------------------|--|
| Total Endpoints 672  |  |
| STB 1                |  |
| INB 8                |  |
| CPB 6                |  |
| DMB 69               |  |
| INS 6                |  |

| 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:

| Gateway Name: | Node Number: | Filtered by State: | Endpoint Range: |
|---------------|--------------|--------------------|-----------------|
| PVG190        | 13           | ALL                | 0-              |

| Summary of Endpoints |  |
|----------------------|--|
| Total Endpoints 672  |  |
| CFL 37               |  |
| IDL 377              |  |
| LO 12                |  |
| DMB 69               |  |
| UNK/MO/MN 173        |  |

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 in the following figure.



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).

|               |              |                    |                 |
|---------------|--------------|--------------------|-----------------|
| Gateway Name: | Node Number: | Filtered by State: | Endpoint Range: |
| PVG190        | 13           | ALL                | 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

- 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



### 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.

- e. Select **Force Release Endpoints (FRLS)** from the **Maintenance Action** list, and click **Go**.

The Force Release Endpoints (FRLS) maintenance action does not support a range of endpoints. Individual endpoints must be specified, or listed with a comma between them for multiple endpoints (eg, 1,3,5,10).

Following is an example of the response with **Show Details** checked:

Observe that the selected trunk endpoints are manual busy (MB).

|                         |                    |                           |                        |
|-------------------------|--------------------|---------------------------|------------------------|
| Gateway Name:<br>PVG190 | Node Number:<br>13 | Filtered by State:<br>ALL | Endpoint Range:<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).

|                         |                    |                           |                        |
|-------------------------|--------------------|---------------------------|------------------------|
| Gateway Name:<br>PVG190 | Node Number:<br>13 | Filtered by State:<br>ALL | Endpoint Range:<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 4                            |
| do not want to perform another action | you have completed this procedure |

—End—

## Maintenance by trunk CLLI

### Step Action

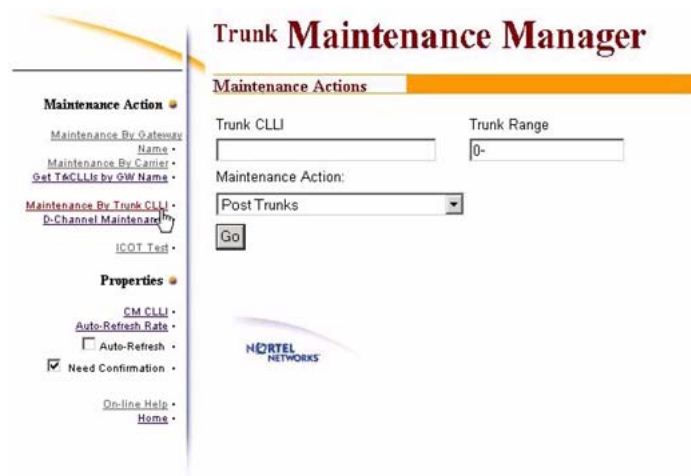
#### At your workstation

- 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 **Maintenance By Trunk CLLI**.

A window similar to the following, is displayed.



- 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 <b>a</b> only |
| Busy trunks              | step <b>b</b> only |
| Return trunks to service | step <b>c</b> only |
| Force release trunks     | step <b>d</b> only |
| Installation busy trunks | step <b>e</b> 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/6/03/VT15/2/1/3/1 |
| 2                | IDL   |                          | 2W        | S7 S7              | GWC_NODE | 1                 | 13     | 1058       | PVG193       | STS/6/03/VT15/2/1/3/2 |
| 3                | IDL   |                          | 2W        | S7 S7              | GWC_NODE | 1                 | 13     | 1059       | PVG193       | STS/6/03/VT15/2/1/3/3 |
| 4                | IDL   |                          | 2W        | S7 S7              | GWC_NODE | 1                 | 13     | 1060       | PVG193       | STS/6/03/VT15/2/1/3/4 |
| 5                | IDL   |                          | 2W        | S7 S7              | GWC_NODE | 1                 | 13     | 1061       | PVG193       | STS/6/03/VT15/2/1/3/5 |
| 6                | IDL   |                          | 2W        | S7 S7              | GWC_NODE | 1                 | 13     | 1062       | PVG193       | STS/6/03/VT15/2/1/3/6 |
| 7                | IDL   |                          | 2W        | S7 S7              | GWC_NODE | 1                 | 13     | 1063       | PVG193       | STS/6/03/VT15/2/1/3/7 |
| 8                | IDL   |                          | 2W        | S7 S7              | GWC_NODE | 1                 | 13     | 1064       | PVG193       | STS/6/03/VT15/2/1/3/8 |
| 9                | IDL   |                          | 2W        | S7 S7              | GWC_NODE | 1                 | 13     | 1065       | PVG193       | STS/6/03/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 in the following figure.



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 CLLI:  
RTPS

Trunk CLLI:  
RTP5BNT20G

First Member:  
1

Group Size:  
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:  
RTPS

Trunk CLLI:  
AL7MICS7

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

Proceed to step 5.



### 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.

- d. Select **Force Release Trunks (FRLS)** from the **Maintenance Action** list, and click **Go**.

The Force Release Endpoints (FRLS) maintenance action does not support a range of endpoints. Individual endpoints must be specified, or listed with a comma between them for multiple endpoints (eg, 1,3,5,10).

Following is an example of the response:



Observe that the selected range of trunk members are manual busy (MB).

CM CLI:

RTPS

Trunk CLI:

RTP5IBNT20G

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 CLI:  |       | Trunk CLI:   | 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 4                            |
| do not want to perform another action | you have completed this procedure |

—End—



## 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.

| Step | Action |
|------|--------|
|------|--------|

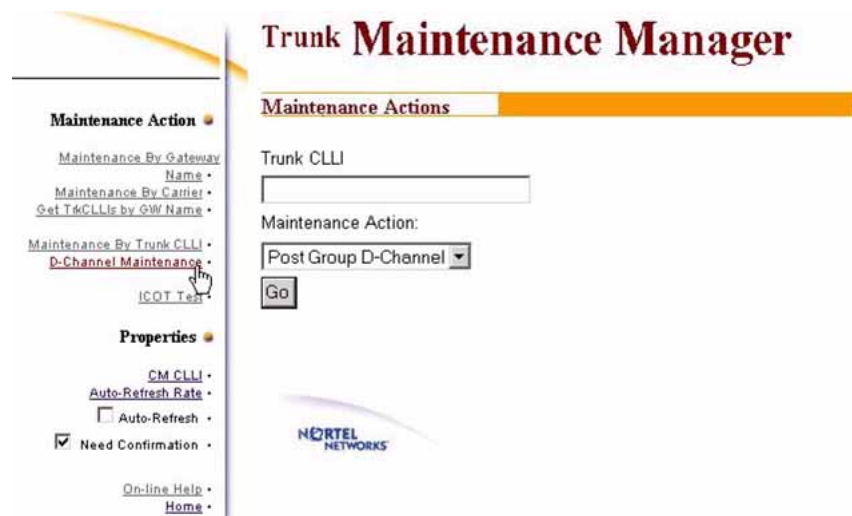
#### *At your workstation*

- 1 Launch the Trunk Maintenance Manager (TMM) GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications.

#### *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:<br>RTPS |       |           |           |          | Trunk CLLI:<br>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 CLLI:<br>RTPS |       |           |           |          | Trunk CLLI:<br>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_0123 |

Last Refreshed: Fri Sep 26 10:34:30 EDT 2003

You have completed this procedure.

—End—

## 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.

| Step | Action |
|------|--------|
|------|--------|

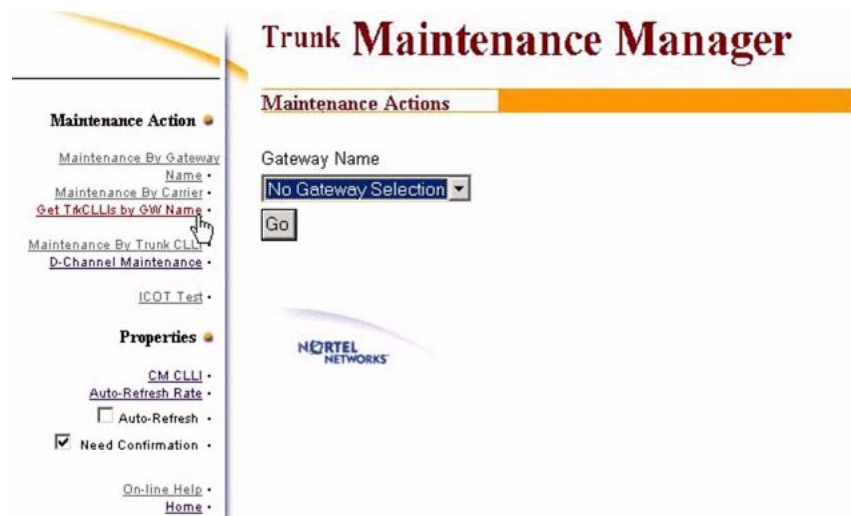
#### *At your workstation*

- 1 Launch the Trunk Maintenance Manager (TMM) GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications.

#### *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.

—End—

## 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"](#) (page 798) in this document, if required.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *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](#).

#### *At the TMM GUI*

- 2 Click **ICOT Test**.

A window similar to the following, is displayed.



- 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 following example.  
  
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>P0P0ITOG |                 |
|------------------|-------------|-------------------------|-----------------|
| Number           | Test Result | Continuity Condition    | Additional Info |
| 1                | TEST_PASSED |                         |                 |

You have completed this procedure.

---

—End—

---

## 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.

| Step | Action |
|------|--------|
|------|--------|

*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 SPFS-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 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Disk Drive Upgrade
16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20- snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)
X - exit
Select -

```

- 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.

---

**—End—**

---

# 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.

As of the SN07 release, the default northbound alarm feed is Corba notifications to the Integrated Element Management System (IEMS). 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.

| Step | Action |
|------|--------|
|------|--------|

***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 CLI)
2 - SESM database tools
3 - SESM related applications configuration
 (MG9K, LMM, CICM)
4 - SESM provisioning configuration
5 - SESM logging configuration (syslog, sesm
 debug log)
6 - view sesm configuration settings
7 - SESM refresh properties
X - exit
select -
```

**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:

The status of the SESM syslog fault feed on the CMT SPFS server is determined by the value of "Alarm Syslog Enabled" configuration attribute. The default option for this setting is FALSE, meaning the SESM syslog alarm logging does not occur unless you specify otherwise.

- 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.

---

—End—

---

## Viewing debug logs

### Application

Use this procedure to view debug logs.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

*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.

—End—

## Viewing OMPUSH logs

### Application

Use this procedure to view OMPUSH logs.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

| Step                       | Action                                                                                                                                                                                                           |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>At your workstation</b> |                                                                                                                                                                                                                  |
| 1                          | Telnet to the Sun server by typing<br><code>&gt; telnet &lt;IP address&gt;</code><br>and pressing the Enter key.<br>where<br><code>IP address</code> is the IP address of the Sun server where<br>OMPUSH resides |
| 2                          | When prompted, enter your user ID and password.                                                                                                                                                                  |
| 3                          | Use the following table to determine your next step.                                                                                                                                                             |

- 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 |
| view the OMPUSH history log file           | step b |
| save the OMPUSH history log file to a file | step c |

- 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.

---

—End—

---



## Viewing customer logs on an SPFS-based server

### Application

Use this procedure to view customer logs for the following components:

- Succession Element and Sub-element Manager (SESM)
- Gateway Controller (GWC)
- Server Platform Foundation Software (SPFS)

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.

| Step | Action |
|------|--------|
|------|--------|

***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 SPFS-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.

---

—End—

---

## Disabling local logging of SPFS platform faults

### Application

Use this procedure to disable local logging of the Server Platform Foundation Software (SPFS) platform alarm logs. Local logging is enabled by default and when enabled, the SPFS 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.

| Step | Action |
|------|--------|
|------|--------|

#### *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 SPFS-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 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
Select -

```

- 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 -

```

Only two options are available for the Core and Billing Manager (CBM). Please see the following CBM example response:

- 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.

---

—End—

---

## Replacing one or more failed disk drives on an SPFS-based server

### Application

Use this procedure to replace one or more failed disk drives on a Server Platform Foundation Software (SPFS)-based server (a Netra t1400 or a Netra 240 server). Also use this procedure if a disk drive was pulled out by mistake. Simply reinserting 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 SPFS 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 these links for a view of the disks on a Netra t1400 and Netra 240:

- ["Netra t1400" \(page 833\)](#)
- ["Netra 240" \(page 834\)](#)

The steps to replace a failed drive are to identify the failed drive, replace it physically, and replace it logically.

#### ATTENTION

The steps contained within these procedures change depending on whether the SPFS platform has previously been upgraded. If you are working on an upgraded platform, be sure to pay special attention to the associated notes during the disk replacement procedures.

Follow one of these links according to your office configuration to replace the failed disk drives:

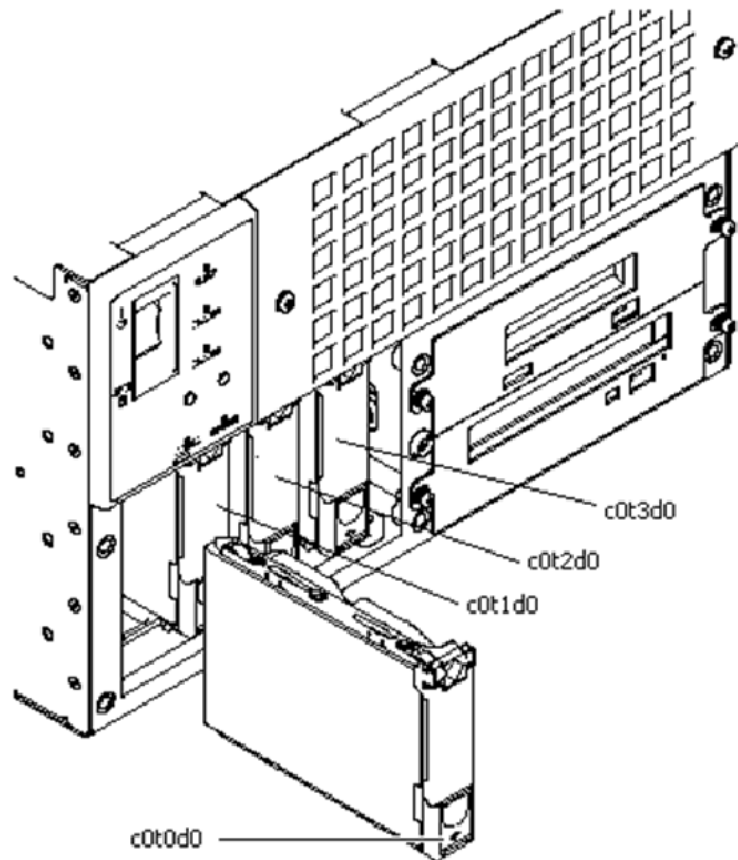
- [Replacing failed disks on a Netra t1400](#)
- [Replacing failed disks on a Netra 240](#)

### 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.

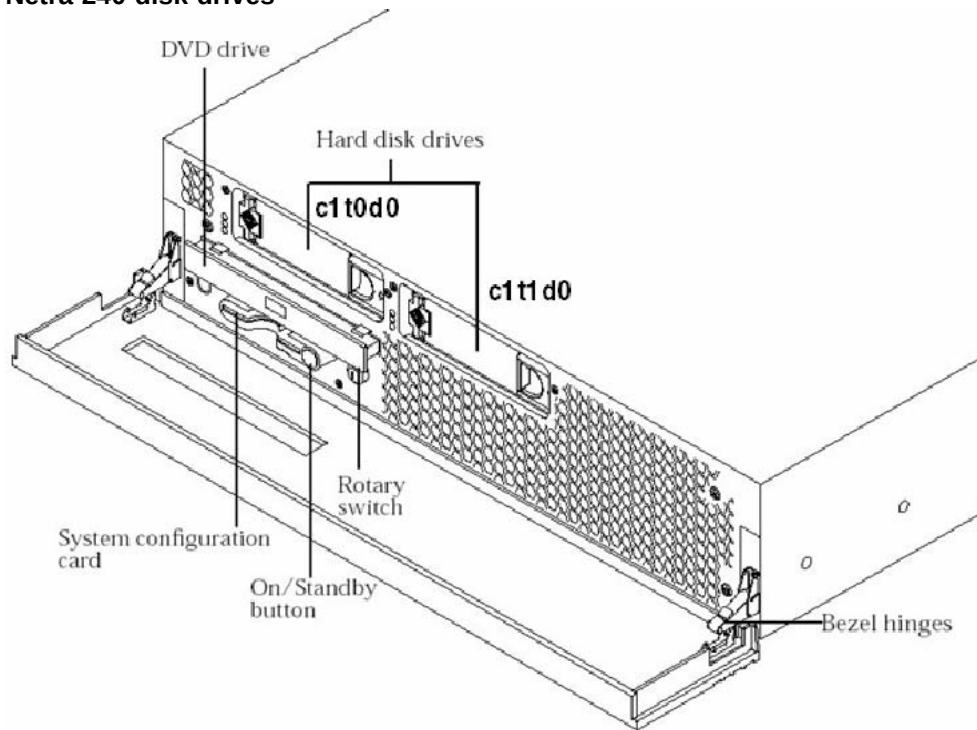
### Netra t1400 disk drives



### 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**

This procedure has the following prerequisites:

- The root user ID and password to log into the server.
- Physical access to the server.
- A replacement hard drive of the of the same size as the hard drive being replaced.
- No other maintenance procedure, such as upgrade, or patch application are currently being executed.
- A Phillips screwdriver, if the system is a Netra t1400/t1405.

**Prerequisites for Core and Billing Manager 850**

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform fault-admin actions.
- You must obtain non-restricted shell access.



For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

#### Related procedures

| Procedure                                                | Document                                                                      |
|----------------------------------------------------------|-------------------------------------------------------------------------------|
| Logging in to the CBM                                    | <i>Core and Billing Manager 850 Security and Administration</i> , NN10358-611 |
| Requesting non-restricted shell access                   | <i>Core and Billing Manager 850 Security and Administration</i> , NN10358-611 |
| Displaying actions a role group is authorized to perform | <i>Core and Billing Manager 850 Security and Administration</i> , NN10358-611 |

## Action

Perform the following steps to complete this procedure.

### Replacing failed disks on a Netra t1400

#### Step Action

##### *At your workstation*

- 1 Log in to the system that is reporting disk or disk mirroring errors as the root user using the system physical IP address.

- 2 Start the CLI tool by typing "cli" at the shell console.

```
cli
```

and press the Enter key.

##### *Example response*

```
Command Line Interface
```

```
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

- 3 Enter the number next to the "Configuration" option in the menu.

##### *Example response*

```
Configuration
```

```
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - OAMP Application Configuration
...
14 - Disk Drive Upgrade
15 - Disk Drive Replacement
...
```

```
X - exit
select -
```

- 4 Enter the number next to the "Disk Drive Replacement" option in the menu.

*Example response*

```
Disk Drive Replacement
1 - disk_drive_replace (Perform Faulty Disk Drive
Replacement)
X - exit
select -
```

- 5 Select the number next to the "disk\_drive\_replace" option in the menu.

*Example response*

```
=== Executing "disk_drive_replace" ===
INFO: Once the disk replacement is complete, it could
take several hours until full disk redundancy is
restored since all file systems on the new drive must
resync. Are you sure you want to continue [y,n]?:
```

- 6 Enter **y** if you want to continue with the disk replacement procedure.

The output provided by the disk replacement utility after specifying **y** will depend on the current status of the system's disks and their configuration which, in turn, depends on many factors. Therefore, the response will probably look different from the following example.

*Example response*

```
INFO: Initializing disk data: Success.
INFO: Determining this system's disk configuration
variant: Success.
INFO: Configuration status for disks: Results:
- Status for "disk" on "clt0d0", on "wcars2yh-unit0",
at level "INFO": - Disk size = 73GB.
- Status for "disk" on "clt1d0", on "wcars2yh-unit0",
at level "INFO": - Disk size = 73GB.
- Status for "metadisk" on "clt1d0", on "wcars2yh-un
it0", at level "WARNING":
- Missing metadb replicas on slice "clt1d0s7".
- Slice "clt1d0s5" of submirror "d102" of mirror "d100"
is in "Maintenance" state.
- Slice "clt1d0s1" of submirror "d1" of mirror "d2" is
in "Maintenance" state.
- Slice "clt1d0s3" of submirror "d7" of mirror "d8" is
in "Maintenance" state.
- Submirror "d4" is not attached to mirror "d5".
- Submirror "d10" is not attached to mirror "d11".
- Possible orphaned submirror "d10".
```

Which disk would you like to replace ("c1t0d0",  
"c1t1d0", "exit"):

- 7 If you would like to abort the disk replacement procedure, enter **exit** otherwise, enter the disk you would like to replace.

*Example response*

Analyzing system state to determine if disk replacement can proceed:

INFO: Disk replacement can proceed.

Details:

Warnings exist, but they are recoverable.

Do you want to continue with the disk replacement procedure [y,n]?:

- 8 If the disk analysis detects:
- A situation that prevents the disk replacement from proceeding, then it will automatically abort this procedure. Call second level support.
  - That disk replacement can continue, then confirm that you would like to continue by entering **y** and pressing the Enter key. The disk replacement utility will take a couple minutes to finish this step.

*Example response*

INFO: Ensuring the mate disk configuration is sane.

Results:

- Status for "metadisk" on "c1t0d0", on "wcars2yh-unit0", at level "INFO":
- Configured the MetaDisk for target disk: c1t0d0

INFO: Deconfiguring the target disk "c1t1d0". Results:

- Status for "disk" on "c1t1d0", on "wcars2yh-unit0", at level "INFO":
- Deconfigured disk "c1t1d0".
- Status for "metadisk" on "c1t1d0", on "wcars2yh-unit0", at level "INFO":
- Removed metadb replicas from slice "c1t1d0s7", on target disk: "c1t1d0".
- Deleted the concatenation or stripe "d10" defined on disk "c1t1d0".
- Deleted the concatenation or stripe "d1" defined on disk "c1t1d0".
- Deleted the concatenation or stripe "d4" defined on disk "c1t1d0".
- Deleted the concatenation or stripe "d102" defined on disk "c1t1d0".
- Deleted the concatenation or stripe "d7" defined on disk "c1t1d0".

Go to the next step in the procedure "Replacing one or more failed disk drives on an SSPFS-based server" in the document "NN10408-900" for the necessary steps to physically replace the faulty hard drive with the new hard drive.

Enter "y" when you have completed physically replacing the faulty hard drive to continue with the configuration of the new hard drive:

Generally, if any status is provided at "ERROR" level, then there is a disk configuration or health issue that the disk replacement utility cannot resolve, and the disk replacement procedure must be halted.

If the "ERROR" is that a file system is currently in "Resync" state then you must wait until the file system has finished resynchronizing. This may take a couple hours and depends on the size of the file system being resynchronized as well as system load. You can retry this disk replacement procedure after the file systems are resynchronized.

If any status is provided at "WARNING" level, then there is a disk configuration or health issue but most likely the disk replacement utility can resolve the issue(s), depending on the combination of warnings that it has detected. This analysis step will let you know if the disk replacement can continue.

If there is one warning that states that a file system is in "Maintenance" state, and another warning that states that a file system is in "Last Erred" state, then the disk with the file system in "Maintenance" state must be replaced first and its file systems resynchronized before replacing the hard drive with the file system in "Last Erred" state.

If status is only provided at "INFO" level or if there is no status information, then both disk configuration and health are in good condition.

## 9 Physically replace the failed disk.

Messages similar to the following might be displayed at the console or in the system logs while replacing the hard drive:

### *Message 1.*

Apr 21 11:39:47 wcars2yh unix: MAJOR ALARM is set  
SC Alert: MAJOR ALARM is set

### *Message 2.*

SC Alert: DISK @ HDD0 has been removed.  
Apr 27 16:24:44 wcars2yh unix: DISK @ HDD0 has been inserted.  
SC Alert: DISK @ HDD0 has been inserted.

*Message 3.*

Apr 21 11:39:47 wcars2yh root:

/opt/resmon/Hardware/disk\_check.ksh: Disk or disk mirroring errors:  
See system alarms for details

a. Procedure for Netra 240:

1. Ensure that you are properly grounded before removing the drive.
2. Open the front panel of the Netra 240 (refer to figure "[Netra 240 disk drives](#)" (page 835)).
3. Unlatch the hard drive with the blue light lit to its left.
4. Use the latch as a lever to start removing the hard drive.
5. Pull the drive the rest of the way out of the SCSI bay.
6. Ensure the latch on the replacement hard drive is open.
7. Insert the replacement hard drive completely into the vacant SCSI bay as far as it will go.
8. Close the latch on the replacement hard drive.
9. Close the front panel of the Netra 240.

b. Procedure for Netra t1400/t1405:

1. Ensure that you are properly grounded before removing the drive.
2. Open the front panel of the Netra t1400/t1405. You will need a phillips screwdriver.
3. Determine the correct hard drive to replace by referring to the figure "[Netra t1400 disk drives](#)" (page 834). While facing the front of the t1400, the hard drives are, from left to right: c0t0d0, c0t1d0, c0t2d0, and c0t3d0.
4. Unlatch the hard drive identified in the previous step.
5. Use the latch as a lever to start removing the hard drive.
6. Pull the drive the rest of the way out of the SCSI bay.
7. Ensure the latch on the replacement hard drive is open.
8. Insert the replacement hard drive completely into the vacant SCSI bay as far as it will go.
9. Close the latch on the replacement hard drive.
10. Close the front panel of the Netra t1400/t1405. You will need a Phillips screwdriver.

- 10** Complete the configuration of the new drive by entering y at the prompt. It will take the disk replacement utility a couple minutes to complete this step.

INFO: Configuring new hard drive.

Results:

- Status for "disk" on "c1t1d0", on "wcars2yh-unit0", at level "INFO":

Configured target disk "c1t1d0".

- Status for "metadisk" on "c1t1d0", on "wcars2yh-unit0", at level "INFO":

- Created metadb replicas on target disk: c1t1d0

- Configured concatenation or stripe "d102" defined on target disk "c1t1d0".

- Configured mirror "d100".

- Configured concatenation or stripe "d1" defined on target disk "c1t1d0".

- Configured mirror "d2".

- Configured concatenation or stripe "d7" defined on target disk "c1t1d0".

- Configured mirror "d8".

- Configured concatenation or stripe "d4" defined on target disk "c1t1d0".

- Configured mirror "d5".

- Configured concatenation or stripe "d10" defined on target disk "c1t1d0".

- Configured mirror "d11".

- Configured the MetaDisk for target disk: c1t1d0

INFO: The disk replacement procedure has completed successfully.

=== "disk\_drive\_replace" completed successfully

- 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.

It will take several hours for the file systems on the new hard drive to synchronize. The "SPFS310" alarm will clear in about a minute.

You have completed this procedure.

---

—End—

---

## Replacing a DVD drive on an SPFS-based server

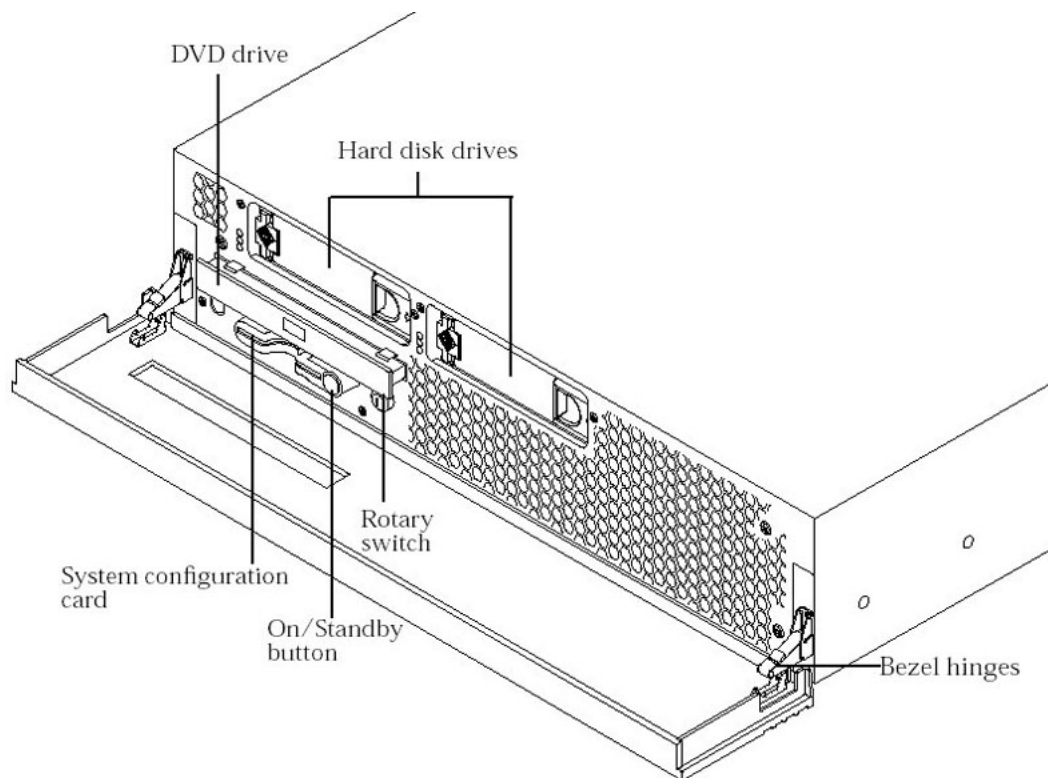
### Application

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 following methods according to your office configuration:

- "Simplex configuration (one server)" (page 843)
- "High-availability configuration (two servers)" (page 843)

### Prerequisites

None.

## Action

### Simplex configuration (one server)

| Step | Action |
|------|--------|
|------|--------|

*At your workstation*

- 1 Power down the server. Refer to procedure ["Shutting down an SPFS-based server" \(page 875\)](#) 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.

---

—End—

---

### High-availability configuration (two servers)

| Step | Action |
|------|--------|
|------|--------|

*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 2 |
| inactive server                           | step 3 |

- 2 Initiate a manual failover. Refer to procedure ["Initiating a manual failover on a Sun Netra 240 server pair" \(page 868\)](#) if required.
- 3 Once the active server acquires the status of standby (inactive), power down the server. Refer to procedure ["Shutting down an SPFS-based server" \(page 875\)](#) 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.

---

—End—

---

---

## Replacing a failed SPFS-based server

---

### Application

Use the following procedure when an SPFS-based server has failed and you need to replace it. This procedure provides the instructions for a one-server configuration or a two server configuration.

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 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager (NPM)
- Core Billing Manager (CBM)

### Prerequisites

You must have a replacement server.

#### **ATTENTION**

Ensure that no provisioning activities are in progress, or scheduled to take place during this procedure.

You must have the root user ID and password to log into the system.

### **Prerequisites for Core and Billing Manager 850**

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform fault-admin actions.
- You must obtain non-restricted shell access.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

#### Related procedures

| Procedure                                                | Document                                                                      |
|----------------------------------------------------------|-------------------------------------------------------------------------------|
| Logging in to the CBM                                    | <i>Core and Billing Manager 850 Security and Administration</i> , NN10358-611 |
| Requesting non-restricted shell access                   | <i>Core and Billing Manager 850 Security and Administration</i> , NN10358-611 |
| Displaying actions a role group is authorized to perform | <i>Core and Billing Manager 850 Security and Administration</i> , NN10358-611 |

## Action

Perform the steps under one of the headings that follow to complete this procedure.

- ["Replacing an SPFS-based server \(one-server configuration\)" \(page 846\)](#)
- ["Replacing one server in an HA configuration" \(page 847\)](#)
- ["Replacing both servers in an HA configuration" \(page 847\)](#)

### Replacing an SPFS-based server (one-server configuration)

---

#### Step Action

---

##### *At the COAM frame*

- 1 Disconnect and remove the failed server.
- 2 Connect and power up the replacement server.
- 3 Restore the file systems and oracle data from backup media. If required, refer to procedure ["Routing customer logs to a remote host" \(page 818\)](#).

Restoring the oracle data does not apply to the CBM as it does not use an oracle database.

You have completed this procedure.

---

—End—

---

## Replacing one server in an HA configuration

| Step | Action |
|------|--------|
|------|--------|

### *At the COAM frame*

- |   |                                                                                                                                                                                                                         |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Disconnect and remove the failed server.                                                                                                                                                                                |
| 2 | Connect and power up the replacement server.                                                                                                                                                                            |
| 3 | Clone the image of the active server onto the server you just replaced. If required, refer to procedure <a href="#">"Routing customer logs to a remote host" (page 818)</a> .<br><br>You have completed this procedure. |

---

—End—

---

## Replacing both servers in an HA configuration

| Step | Action |
|------|--------|
|------|--------|

### *At the COAM frame*

- |   |                                                                                                                                                                                                                                                                                                     |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Disconnect and remove one failed server.                                                                                                                                                                                                                                                            |
| 2 | Connect and power up the replacement server.                                                                                                                                                                                                                                                        |
| 3 | Restore the file systems and oracle data from backup media on the server you just replaced. If required, refer to procedure <a href="#">"Routing customer logs to a remote host" (page 818)</a> .<br><br>Restoring the oracle data does not apply to the CBM as it does not use an oracle database. |
| 4 | Disconnect and remove the other failed server.                                                                                                                                                                                                                                                      |
| 5 | Connect and power up the replacement server.                                                                                                                                                                                                                                                        |
| 6 | Clone the image of the active server onto the server you just replaced. If required, refer to procedure <a href="#">"Routing customer logs to a remote host" (page 818)</a> .<br><br>You have completed this procedure.                                                                             |

---

—End—

---

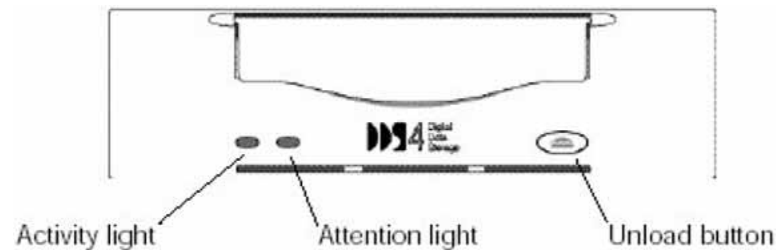
## Cleaning the DAT drive on the Netra T1400

### 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

---

| Step | Action |
|------|--------|
|------|--------|

---

***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.  
  
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.

---

—End—

---

## 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.

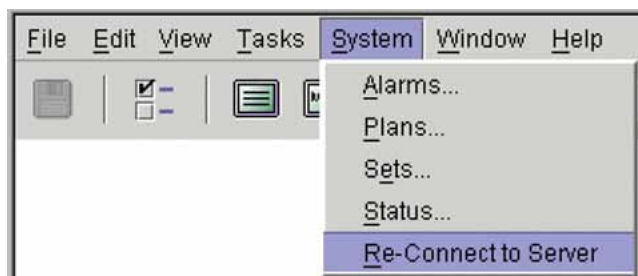
### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

*At the NPM GUI*

- 1 On the **System** menu, click **Re-Connect to Server**.



When the connection is successful, a response similar to the following one is displayed.



When the connection fails, a response similar to the following one 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.

---

—End—

---



---

## 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" \(page 852\)](#)
- ["Re-establishing SSH communication after an SPFS fresh install" \(page 854\)](#)

#### Re-establishing SSH communication after a core manager fresh install

| Step                                                                             | Action                                                                                                                               |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>At the SDM</b>                                                                |                                                                                                                                      |
| 1                                                                                | Log in to the core manager.                                                                                                          |
| 2                                                                                | Access the SWIM level of the maintenance interface by typing<br><code># sdmmtc swim</code><br>and pressing the Enter key.            |
| 3                                                                                | Access the Details level by typing<br><code>&gt; details</code><br>and pressing the Enter key.                                       |
| 4                                                                                | Ensure the following filesets are applied. <ul style="list-style-type: none"><li>• OpenSSH</li><li>• Bootp Loading Service</li></ul> |
| Use the up/down commands to scroll through the list of applications if required. |                                                                                                                                      |

**At the CS 2000 Management Tools server (SPFS)**

- 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:le 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 SPFS by typing

```
$ /usr/bin/scp
-q /data/SPFS/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.

---

—End—

---

## Re-establishing SSH communication after an SPFS fresh install

| Step | Action |
|------|--------|
|------|--------|

### *At the SDM*

- |   |                                                                                                                              |
|---|------------------------------------------------------------------------------------------------------------------------------|
| 1 | Log in to the core manager.                                                                                                  |
| 2 | Access the SWIM level of the maintenance interface by typing<br><br># <b>sdmmntc swim</b><br><br>and pressing the Enter key. |
| 3 | Access the Details level by typing<br><br>> <b>details</b>                                                                   |

and pressing the Enter key.

- 4** Ensure the OpenSSH fileset is applied.

Use the up/down commands to scroll through the list of applications if required.

- 5** Perform procedure "Setting up the BootP file on SPFS" in the Voice over IP Network Upgrade document, NN10440-450.

You have completed this procedure.

---

**—End—**

---

## 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" (page 856)
- "Configuring the naming service on the server where the MG 9000 Manager resides " (page 859)

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](#)" (page 862).

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### **Configuring the naming service on the CS 2000 Management Tools server**

| Step | Action |
|------|--------|
|------|--------|

##### ***At your workstation***

- |   |                                                                                                                                                      |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | <p>Telnet to the CS 2000 Management Tools server by typing</p> <pre>&gt; telnet &lt;server&gt;</pre> <p>and pressing the Enter key.</p> <p>where</p> |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------|

**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 - Remote Backup Configuration
```

```
10 - Database Configuration
```

```
11 - NFS Configuration
```

```
12 - Bootp Configuration
```

```
13 - Restricted Shell Configuration
```

```
14 - Security Services Configuration
```

```
15 - Disk Drive Upgrade
```

```
16 - Login Session
```

```
17- Location Configuration
```

```
18 - Cluster Configuration
```

```
19 - Succession Element Configuration
```

```
20 - snmp_poller (SNMP Poller Configuration)
```

```
21 - backup_config (Backup Configuration)
```

```
X - exit
Select -
```

- 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

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

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"](#) (page 859).

---

—End—

---

## **Configuring the naming service on the server where the MG 9000 Manager resides**

---

| <b>Step</b> | <b>Action</b> |
|-------------|---------------|
|-------------|---------------|

---

***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 - Remote Backup Configuration  
10 - Database Configuration  
11 - NFS Configuration  
12 - Bootp Configuration  
13 - Restricted Shell Configuration  
14 - Security Services Configuration  
15 - Disk Drive Upgrade  
16 - Login Session  
17 - Location Configuration

```
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)
X - exit
Select -
```

- 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.

The command is case sensitive.

- 13** When prompted, enter the Context Name by typing

**Nortel**

and pressing the Enter key.

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" \(page 862\)](#).

---

—End—

---

## Verifying the naming service is configured correctly

| Step | Action |
|------|--------|
|------|--------|

### *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.

---

**—End—**

---

## Verifying the state of a cluster

### Application

#### 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.

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.

### Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access.

- You must be a user in the role group authorized to perform config-admin functions.
- You must obtain non-restricted shell access

For CBM 850, root user ID and password are not required. If logging in using telnet, [step 2c](#) and [step 2d](#) of this procedure are therefore not required. If logging in using ssh you can use your own user ID in [step 3](#) of this procedure.

For more information on how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

#### Related procedures

| Procedure             | Document                                                                      |
|-----------------------|-------------------------------------------------------------------------------|
| Logging in to the CBM | <i>Core and Billing Manager 850 Security and Administration</i> , NN10358-611 |

| Procedure                                                | Document                                                                     |
|----------------------------------------------------------|------------------------------------------------------------------------------|
| Requesting non-restricted shell access                   | <i>Core and Billing Manager 850 Security and Administration, NN10358-611</i> |
| Displaying actions a role group is authorized to perform | <i>Core and Billing Manager 850 Security and Administration, NN10358-611</i> |

This is only applicable to the CBM and not any other SPFS-based server.

## Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

### *At your workstation*

- 1 Establish a login session to the inactive server, using one of the following methods:

| If using          | Do                          |
|-------------------|-----------------------------|
| telnet (unsecure) | step <a href="#">step 2</a> |
| ssh (secure)      | step <a href="#">step 3</a> |

- 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.
 

Ensure you are on the right server by typing `ubmstat`. You must be on the inactive server and the response must be `ClusterIndicatorSTBY`.
- 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

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.

Ensure you are on the right server by typing `ubmstat`. You must be on the inactive server and the response must be *ClusterIndicatorSTBY*.

- 4 Determine your next action based on the system response to the `ubmstat` command.

| If                                                          | Do                     |
|-------------------------------------------------------------|------------------------|
| the system response is<br><code>ClusterIndicatorSTBY</code> | <a href="#">step 6</a> |
| otherwise                                                   | <a href="#">step 5</a> |

- 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 for each<br>filesystem is <code>STANDBY normal</code><br><code>UP clean</code> | <a href="#">step 7</a> |
| otherwise                                                                                          | <a href="#">step 8</a> |

- 7 Verify the status of the cluster configuration by typing

```
CheckConfiguration
```

and pressing the Enter key.

| If                                                                        | Do                                                                           |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------|
| the system response is Checking local configuration against unit0-priv0 # | the cluster is in a good state and you can proceed to <a href="#">step 9</a> |
| otherwise                                                                 | <a href="#">step 8</a>                                                       |

There will be some discrepancy between the (I)SN07/(I)SN08 response to the CheckConfiguration command and the (I)SN09 response. In (I)SN09, the system returns an additional response if the verification passes and the cluster nodes are in sync. This response is not returned in (I)SN07 or (I)SN08. This discrepancy is normal.

**8** Reboot the inactive server by typing

```
init 6
```

and pressing the Enter key.

| If                       | Do                                                                           |
|--------------------------|------------------------------------------------------------------------------|
| you identified a problem | Contact your next level of support.                                          |
| otherwise                | the cluster is in a good state and you can proceed to <a href="#">step 9</a> |

**9** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

—End—

---



## 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.

| Step | Action |
|------|--------|
|------|--------|

#### *At the active node console*

- 1 Log in to the active node through the console (port A) using the root user ID and password.  
  
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.

---

—End—

---

## Querying the state of the SPFS 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.

| Step | Action |
|------|--------|
|------|--------|

*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 - OAMP Application Configuration
4 - CORBA Configuration
5 - IP Configuration
6 - DNS Configuration
7 - Syslog Configuration
8 - Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
Select -

```

- 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=wxrpz0xy;NODE=wxrpz0xy;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.

—End—

Rebooting an SPFS-based server

Application

Use this procedure to reboot a Server Platform Foundation Software (SPFS)-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)
- Multiservice Data Manager (MDM)

MDM when installed on SPFS-based servers is not configured as a two-server cluster but as two distinct one-server configurations.

ATTENTION

The SPFS-based server may be hosting more than one of the preceding 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.

Step	Action

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 SPFS-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.

—End—

Shutting down an SPFS-based server

Application

Use this procedure to shut down a Server Platform Foundation Software (SPFS)-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)
- Multiservice Data Manager (MDM)

MDM when installed on SPFS-based servers is not configured as a two-server cluster but as two distinct one-server configurations.

ATTENTION

The SPFS-based server may be hosting more than one of the preceding components, therefore, ensure it is acceptable to shut down the server.

Prerequisites

You must have root user privileges.

Perform this procedure from a console only.

Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform fault-admin actions. Therefore, [Step 3](#) and [Step 9](#) are not required.
- You must obtain non-restricted shell access.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	<i>Core and Billing Manager 850 Security and Administration</i> , NN10358-611
Requesting non-restricted shell access	<i>Core and Billing Manager 850 Security and Administration</i> , NN10358-611
Displaying actions a role group is authorized to perform	<i>Core and Billing Manager 850 Security and Administration</i> , NN10358-611

Action

Use one of the following procedures according to your office configuration:

- ["One-server configuration" \(page 876\)](#)
- ["Two-server \(cluster\) configuration" \(page 877\)](#)

One-server configuration

Step	Action

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 SPFS-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.

—End—

Two-server (cluster) configuration

Step	Action

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 SPFS-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.
 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.

ATTENTION

Only perform the remaining steps if you want to perform a full power down, which involves powering down both servers in the cluster.

- 7** 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 SPFS-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.

—End—

Recovering from having two inactive servers in a cluster

Application

Use this procedure to make one server active when both servers in the cluster are inactive.

When there is no active server, log SPFS330 is generated.

For more information on logs, refer to the *Carrier Voice over IP Networks Fault Management Logs Reference document*, NN10275-909.

Prerequisites

You need the root user ID and password.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

- 1 Determine which server has the most recent application data as follows:
 - a. Telnet to one server of the cluster by typing


```
> telnet <IP address>
```

 and pressing the Enter key.
 where
IP address is the physical IP address of the server
 - b. When prompted, enter your user ID and password.
 - c. Access the "/data" directory by typing


```
> cd /data
```

 and pressing the Enter key.
 - d. List the files in the "/data" directory with their detailed information by typing


```
> ls -l
```

 and pressing the Enter key.
 - e. Note the timestamp on each of the files.

- f. Exit the `/data` directory by typing
`> cd`
and pressing the Enter key.
 - g. Telnet to the other server of the cluster by typing
`> telnet <IP address>`
and pressing the Enter key.
where
`IP address` is the physical IP address of the server
 - h. When prompted, enter your user ID and password.
 - i. Access the `/data` directory by typing
`> cd /data`
and pressing the Enter key.
 - j. List the files in the `/data` directory with their detailed information by typing
`> ls -l`
and pressing the Enter key.
 - k. Note the timestamp on each of the files.
 - l. Exit the `/data` directory by typing
`> cd`
and pressing the Enter key.
- 2 On the server that has the most recent application data, change to the root user by typing
`$ su - root`
and pressing the Enter key.
 - 3 When prompted, enter the root password.
 - 4 Make this server the Active server by typing
`# ActivateNode`
and pressing the Enter key.
 - 5 When prompted, confirm you want to make this server the Active server by typing
`# yes`
and pressing the Enter key.

- 6 Verify the status of file systems on this server by typing

udstat

and pressing the Enter key.

If the file systems are	Do
ACTIVE normal UP clean	step 7
not ACTIVE normal UP clean	contact your next level of support

- 7 Verify the cluster indicator by typing

ubmstat

and pressing the Enter key.

If the system response is	Do
"ClusterIndicatorACT"	step 8
not "ClusterIndicatorACT"	contact your next level of support

- 8 Telnet to the other server in the cluster by typing

> **telnet <IP address>**

and pressing the Enter key.

where

IP address is the physical IP address of the server

- 9 When prompted, enter your user ID and password.

- 10 Change to the root user by typing

\$ **su - root**

and pressing the Enter key.

- 11 When prompted, enter the root password.

- 12 Verify the status of file systems on this server by typing

udstat

and pressing the Enter key.

If the file systems are	Do
STANDBY normal UP clean	step 13
not STANDBY normal UP clean	contact your next level of support

- 13 Verify the cluster indicator by typing

ubmstat

and pressing the Enter key.

If the system response is	Do
"ClusterIndicatorSTBY"	the cluster is in a good state and you have completed this procedure
not "ClusterIndicatorSTBY"	contact your next level of support

14 You have completed this procedure.

—End—

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)" (page 884)
- "Restoring NPM patch files from CD/DVD (Sun Netra 240 only)" (page 886)

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)" (page 884)
- "Restoring NPM patch files from CD/DVD (Sun Netra 240 only)" (page 886)

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)

Step	Action						
At your workstation							
1	Establish a login session to the server, using one of the following methods:						
	<table border="1"> <thead> <tr> <th>If using</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>telnet (unsecure)</td> <td>step 2</td> </tr> <tr> <td>ssh (secure)</td> <td>step 3</td> </tr> </tbody> </table>	If using	Do	telnet (unsecure)	step 2	ssh (secure)	step 3
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 SPFS-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.

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 SPFS-based server, or the physical IP address of the active server in a two-server configuration

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.

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.

—End—

Restoring NPM patch files from CD/DVD (Sun Netra 240 only)

Step	Action

<i>At your workstation</i>	

- 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 SPFS-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.

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 SPFS-based server, or the physical IP address of the active server in a two-server configuration

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.

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.
```

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.

—End—

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 Server Platform Foundation Software (SPFS)-based server (Sun t1400) running the SN06.2 or greater release of the SPFS.

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 tape" \(page 890\)](#).

Prerequisites

You need the tape on which you backed up the APS audio files.

Step	Action
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 <code>> telnet <server></code> and pressing the Enter key. where <code>server</code> is the IP address or host name of the SPFS-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 <code>\$ su - root</code> and pressing the Enter key.
5	When prompted, enter the root password.
6	Change directory to the root file system by typing <code># cd /</code> 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.

—End—

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 Server Platform Foundation Software (SPFS)-based server (Sun Netra 240) running the SN06.2 or greater release of the SPFS.

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" \(page 890\)](#).

Prerequisites

You need the CD or DVD on which you backed up the APS audio files.

Step	Action
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 <code>> telnet <server></code> and pressing the Enter key. where <code>server</code> is the IP address or host name of the SPFS-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 <code>\$ su - root</code> and pressing the Enter key.
5	When prompted, enter the root password.
6	Change directory to the root file system by typing <code># cd /</code> 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.

—End—

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.

Step	Action
At the APS server	
1	Become the root user by entering the following command and then entering the "root" password when prompted. <code>su - root</code>
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. <code>\$ ips_export_db.sh -t /dev/rmt/0 -restore</code> This command restores the APS DB from the tape to the following directory. <code>/audio_files/aps_db_backup/*.dmp</code>
4	Restore the APS audio files to the file system if not already performed.
5	You have completed this procedure.
—End—	

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.

Step	Action
<i>At the APS server</i>	
1	Become the root user by entering the following command and then entering the "root" password when prompted. <pre>su - root</pre>
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. <pre>cd /audio_files/aps_db_backup</pre>
4	Copy the dmp files on the CD to this directory by typing the following command. <pre>\$ cp /cdrom/cdrom0/* ./</pre>
5	Verify the dmp files were copied from CD to the destination directory by typing the following command and then viewing the command output. <pre>\$ ls -l *</pre> <pre>-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_prgrp.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_permissions_group.dmp -rwxrwsrwx 1 root other 71 May 13 11:11 README -rwxrwsrwx 1 root other 4096 May 13 11:11 sys_parms.dmp</pre>

```

. . . . .
-rwxrwsrwx 1 root other 44032 May 13 11:11 uas_segmen
ts.dmp
-rwxrwsrwx 1 root other 6144 May 13 11:11 uas_select
or_relation.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11 uas_select
or_type.dmp
-rwxrwsrwx 1 root other 7168 May 13 11:11 uas_selecto
r_value.dmp
-rwxrwsrwx 1 root other 5120 May 13 11:11 uas_sequenc
es.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11 uas_set_con
tent.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11 uas_set_def
inition.dmp
-rwxrwsrwx 1 root other 3072 May 13 11:11 uas_user_p
erms.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_variabl
es.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.

—End—

Executing a fallback during an SPFS-based server upgrade

Application

Use this procedure to roll back (fall back) to the state prior to the upgrade. One or more of the following components can be hosted on the server:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

ATTENTION

Only use this procedure when directed to do so.

Prerequisites

You can only perform this procedure on the newly upgraded node.

Action

Perform the steps under one of the headings that follow to complete this procedure.

- ["One-server configuration" \(page 897\)](#)
- ["Two-server configuration" \(page 898\)](#)

One-server configuration

Step	Action

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 <pre># /SSPFS_Upgrade.fallback</pre> and pressing the Enter key.

- 3 Use the following table to determine your next step. If server is hosting the:

If your server is hosting the	Do
Core Billing Manager (CBM) or MG 9000 Element Manager	step 5
CS 2000 Management Tools 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 SPFS-based server" in *ATM/IP Security and Administration*, NN10402-600.
- 5 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Two-server configuration

Step Action

At the server console

- 1 Log in to the 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

If	Do
server is hosting the MG 9000 EM Server	step 10

- 11

If	Do
server is hosting the IEMS or CS2M	refer to procedure "Restoring the oracle data on an SPFS-based server" in <i>ATM/IP Security and Administration</i> , NN10402-600

- 12**
- | If | Do |
|---------------------------|-------------------------|
| server is hosting the NPM | step 13 |
| otherwise | step 10 |
- 13** Download the NPM database file (old_npm_db.tar) made in step 44 of Saving user-defined NPM data using the NPM in NN10440-450 to the /data/npm directory on the NPM server if not already carried out.
- 14** telnet to server running previous software and su to root where NPM is resident and erase existing NPM database by typing:
- ```
cd/data/npm/database
rm -Rf*
```
- 15** Now stage the old NPM database by typing:
- ```
# cd/data/npm  
# tar-xvf old_npm_db.tar
```
- 16** servstart NPM
- 17** Clone the image of the active server onto the other server. If required, refer to procedure "[Routing customer logs to a remote host](#)" (page 818).
- 18** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

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 (CMT)
- Line Maintenance Manager (LMM)
- SAM21 Element Manager (SAM21 EM)
- Batch Configuration Monitor (BCM)
- Network Patch Manager (NPM)

ATTENTION

This only applies when the NPM is installed and enabled on the same SPFS-based server as CS 2000 Management Tools.

The NPM also has its own command line user interface (CLUI). Refer to procedure "[Accessing the network patch manager CLUI](#)" (page 912).

This procedure provides the following four methods to launch a CS 2000 Management Tools client application:

1. "[Launch applications from a web browser](#)" (page 903).

ATTENTION

You must use method one to launch an application for the first time.

You cannot use launch methods two through four to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

2. "[Launch applications from the JWS Application Manager](#)" (page 905).
3. "[Launch applications from a desktop icon or Start menu \(Windows only\)](#)" (page 907)
4. "[Launch specific applications using a URL](#)" (page 909).

You can also launch applications from the Integrated Element Management System (IEMS) when the IEMS is present in the office. Refer to document *IEMS Basics* (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 for your solution.
-
- Make sure the client workstation meets the minimum requirements.



CAUTION

If you have an ATI Radeon 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/bugPatches/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 SPFS-based server where the CS 2000 Management Tools are installed, and a valid user name and password to launch an application.

ATTENTION

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 an SPFS-based server" in *ATM/IP Security and Administration* (NN10402-600)

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2_08 and Java™ Web Start (JWS) version 1.4.2_08 installed to launch the following applications:

- CS 2000 Management Tools
- Line Maintenance Manager
- CS 2000 SAM21 Manager
- Network Patch Manager

Action

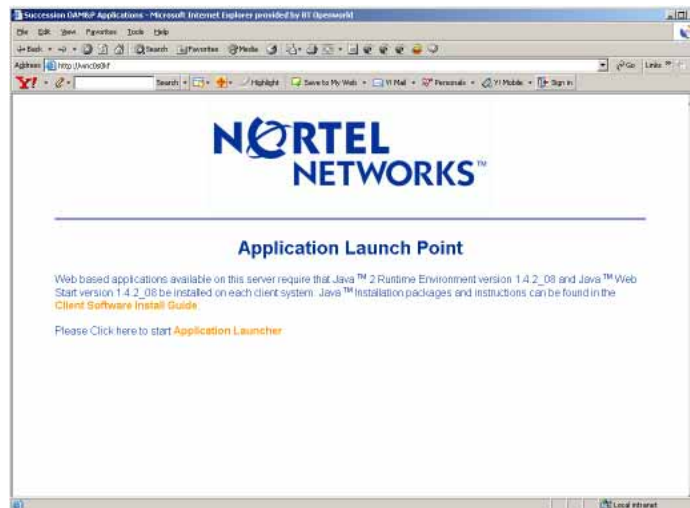
Launch applications from a web browser

Step	Action

At your workstation

- 1 Launch your web browser.
- 2 In the Address field, enter the name or IP address of the SPFS-based server where the CS 2000 Management Tools are installed.

The Application Launch Point page appears.



- 3 Use the following table to determine your next step.

If	Do
you have JRE 1.4.2_08 and JWS 1.4.2_08 installed	step 9
you do not have JRE 1.4.2_08 and JWS 1.4.2_08 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_08 and JWS 1.4.2_08 installed	step 8
you do not have JRE 1.4.2_08 and JWS 1.4.2_08 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 **Back** 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.

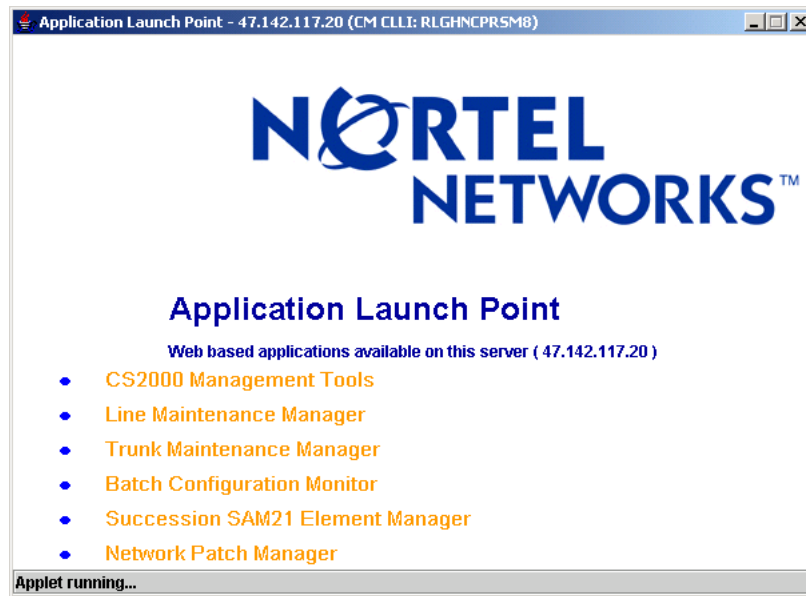
ATTENTION

You must have administrative privileges to install the software on the workstation.

- 8 Click **Back** to return to the Application Launch Point.
- 9 Click **Application Launcher**.
The Login window appears.



- 10 Enter your user name and password, then click **Log In**.
The Application Launch Point, similar to following, appears.



- 11 Click the link for the application you want to launch.
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.
The interface for the application you launched, is displayed.
- 12 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Launch applications from the JWS Application Manager

Step	Action

At your workstation

- 1 Launch the Java Web Start Application Manager.

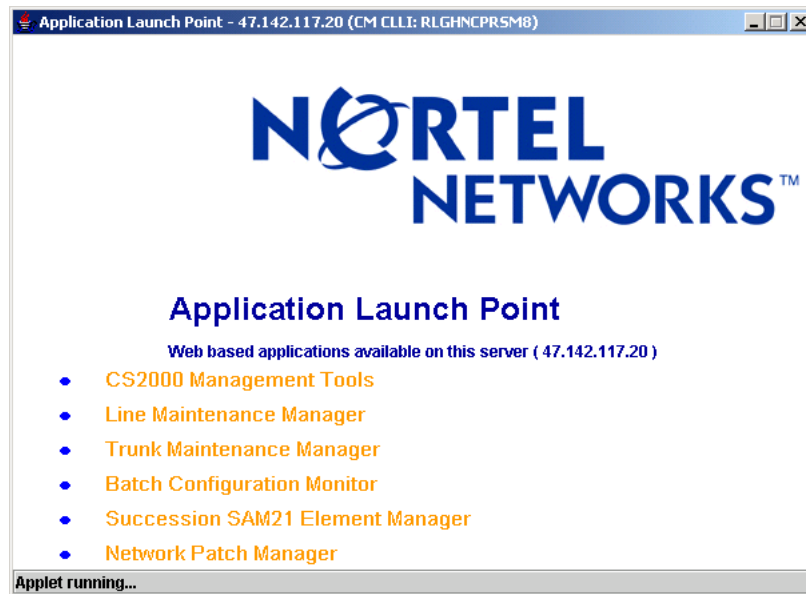


- 2 If you do not see the downloaded applications as shown in the previous figure, then on the View menu click **Downloaded Applications**. Otherwise, skip to the next step.
- 3 Double-click the Application Launch Point you want to access, or select the Application Launch Point and click Start.

The Login window appears.



- 4 Enter your user name and password, then click Log In. The Application Launch Point, similar to following, appears.



- 5 Click the link for the application you want to launch.
The interface for the application you launched, is displayed.
- 6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

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.

—End—

Launch applications from a desktop icon or Start menu (Windows only)

Step Action

At your workstation

- 1 Use the following table to determine your next step.

If you want to launch an application from ...	Do
... a desktop icon	step 2
... the Start menu	step 4

- 2 To launch a CS 2000 Management Tools client application from a desktop icon, locate the short-cut icon on your desktop, and double-click it to start the application.

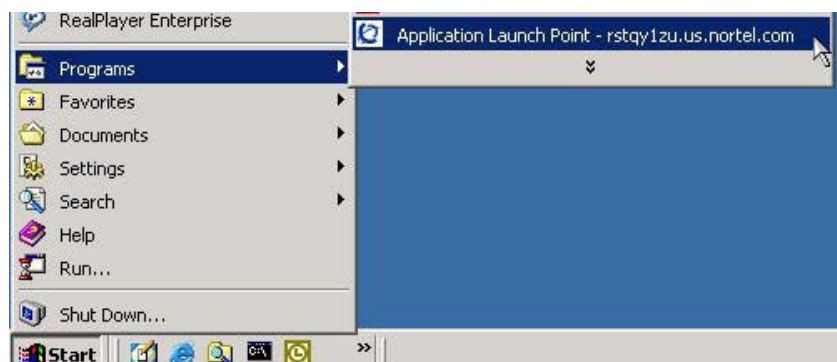
ATTENTION

For short-cut icons to be present on your desktop, you must have the correct settings under the Shortcut Options tab. Access the Shortcut Options tab through File->Preferences in the JWS Application Manager.



The Login window appears.

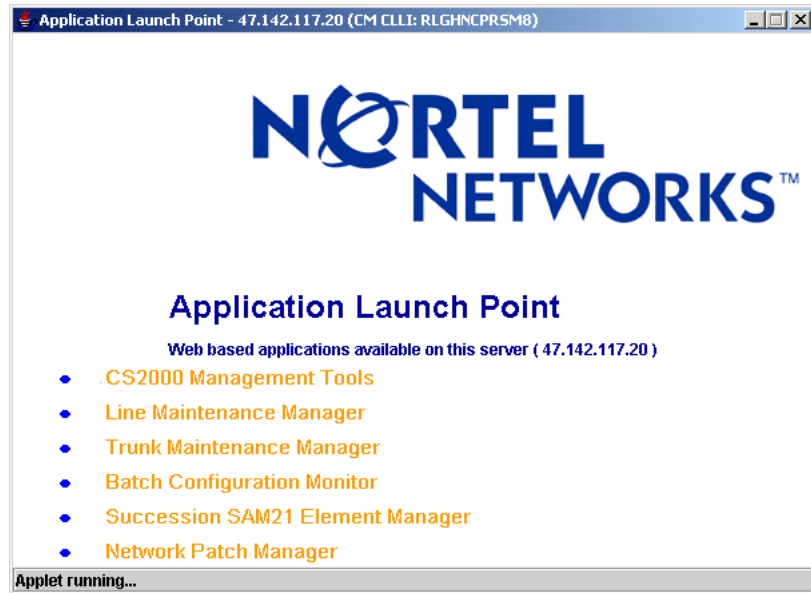
- 3 Proceed to step 5.
- 4 To launch a CS 2000 Management Tools client application from the Start menu, click Start->Programs, then click the CS 2000 Management Tools client application you want to launch.



The Login window appears.

- 5 Enter your user name and password, then click **Log In**.

The Application Launch Point, similar to following, appears.



- 6 Click the link for the application you want to launch.

The interface for the application you launched, is displayed.

- 7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

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.

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2_08 and Java™ Web Start (JWS) version 1.4.2_08 installed to launch the applications. If this is the first time you are launching an application, use the first method provided in the "[Launch applications from a web browser](#)" (page 903) procedure.

—End—

Launch specific applications using a URL

Step Action

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=imm
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 SPFS-based 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.
- 4 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Additional information

The GUI-based client applications (CS2000 Management Tools, Line Maintenance Manager, Network Patch Manager, and SAM21 Manager) connect to their corresponding server-side application through a Socks proxy.

The Trunk Maintenance Manager (TMM) and Batch Configuration Monitor do not use a Socks proxy.

When you launch a client application that connects through a Socks proxy, you can 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).

You can also access the NPM CLUI from the Integrated Element Management System (IEMS) when the IEMS is present in the office. Refer to *IEMS Basics*, NN10329-111.

The Network Patch Manager also has a graphical user interface (GUI). Refer to procedure "[Launching CS 2000 Management Tools and NPM Client Applications](#)" (page 901) .

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 SPFS-based server" in *ATM/IP Security and Administration*, NN10402-600.

Action

Perform the following steps to complete this procedure.

Step	Action						
At your workstation							
1	Establish a login session to the server, using one of the following methods:						
<table border="1"> <thead> <tr> <th>If using</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>telnet (unsecure)</td> <td>step 2</td> </tr> <tr> <td>ssh (secure)</td> <td>step 3</td> </tr> </tbody> </table>		If using	Do	telnet (unsecure)	step 2	ssh (secure)	step 3
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 <pre>> telnet <server></pre> and pressing the Enter key. where <pre>server</pre> is the IP address or host name of the SPFS-based server							

At your workstation

- Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- Log in to the server using telnet (unsecure) as follows:

- 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 SPFS-based server

- b. When prompted, enter your user ID and password.
Proceed to step 4.
- 3 Log in using ssh (secure) as follows:
 - a. Log in to the server by typing

```
> ssh -l <userID> <server>
```

and pressing the Enter key.
where
server is the IP address or host name of the SPFS-based server

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 your password.
- 4 Start the NPM CLUI by typing

```
$ npm
```

and pressing the Enter key.
- 5 When prompted, enter your user ID and password.
Example response:
Entering shell mode: Enter npm' commands, help or quit to exit.
npm>
- 6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Carrier VoIP

Nortel ATM/IP Solution-level Fault Management

Copyright © 2006, Nortel Networks
All Rights Reserved.

Publication: NN10408-900
Document status: Standard
Document version: 04.04
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

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

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.

