Gateway Controller Fault Management

What’s new in SN07

The following release SN07 changes are documented in this NTP:

- A00003575 - Security productization. Added the following log descriptions:
  - — GWC400 information log
  - — Kerberos logs
  - — IKE logs

  Removed alarm GWC310 “Excessive securitySA failures”. Modified alarm GWC309 and log GWC309, now “SA_PERCENTAGE_USAGE”.
- A00007211 - H.323 GWC600 to adhere to OSS requirements. GWC600 log description updated to reflect changes.
- CR Q00712225 - Additions to log PM181.
- CR Q00952413 - H.323 Flex carrier: too many alarms. New log reports GWC506 and GWC507 included in NTP. Changes made to alarm and log GWC304 as well as log reports GWC399 and GWC600.
- Consolidated procedure “Abort GWC hardware diagnostics” into procedure “Perform GWC hardware diagnostics”.
- Consolidated procedures “Retrieve and correlate GWC syslog logs” and “Retrieve and correlate GWC logs in customer log files” into one procedure “View GWC logs in syslog files”.
- Consolidated the contents of procedure “Troubleshoot with GWC fault logs” into log description “PM181”.
- Incorporated alarm changes as a result of SN07 features in procedure “View and troubleshoot GWC service alarms”.
- Simplified and improved the usabilty of procedures “View and interpret GWC service states”, “Filter GWC service alarms” and “Perform GWC hardware diagnostics”.

- The capability to acknowledge alarms and view acknowledged alarms is removed from the CS 2000 GWC Manager in SN07. As a result the following procedures are removed from this NTP:
  - “Acknowledge GWC service alarms”
  - “View acknowledged GWC alarms”

  In SN07, these tasks can be performed using the Integrated Element Management System (EMS).
- Updated examples of logs GWC501, GWC502, and GWC503. Added an action to log description GWC501.
- Update to procedure “Perform a CS 2000 data integrity audit” as a result of feature A00003948 - Tri-modal server support on CS 2000 Management Tools and CS 2000 GWC Manager.

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 logs 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.

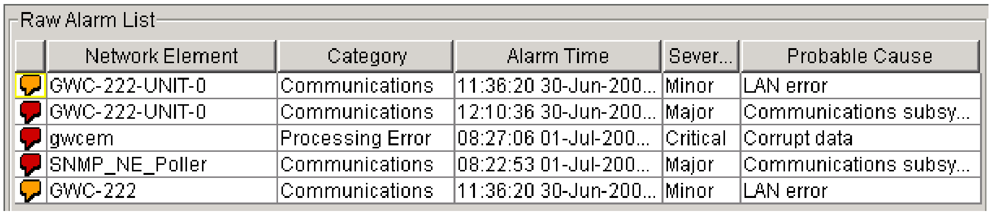
Fault clearing depends on the timely resolution of alarms. Alarms provide notification of problems or conditions that can change the performance or working state of the GWC, the CS 2000 or other related network components.

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. Refer to the following figure for an example of the alarm severity color codes.



Raw Alarm List

	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 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 Manager System (EMS) to perform these functions. For details on alarm acknowledgement, refer to the Integrated EMS Fault Management NTP, 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 XA-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.

Note 1: For syslog storage, the alarm is converted into syslog format before storing.

Note 2: 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 details on how to configure alarm logging, refer to CS 2000 Management Tools information in the ATM/IP Solution-level Fault Management NTP, 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 on syslog, and for instructions on syslog forwarding in a network containing the Integrated Element Management System (EMS), refer to the CS 2000 Management Tools information in the ATM/IP Solution-level Fault Management NTP, NN10408-900.

For more information on how to access the GWC syslog logs, refer to procedure View GWC logs in syslog files on page 54 in this NTP.

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 and GWC400

  For more information, refer to the appropriate log description in this NTP.

- logs for the Kerberos and IKE key management systems

  Logs for the Kerberos and IKE systems are stored in the securitylog files in directory /var/log on the CS 2000 Management Tools server. Refer to procedure View GWC logs in syslog files on page 54 for instructions on how to access these logs.

  For the description of Kerberos logs, refer to Kerberos logs on page 249.

  For the description of IKE logs, refer to IKE logs on page 255.

- alarm SA_PERCENTAGE_USAGE (minor)

  For more information, refer to procedure View and troubleshoot GWC service alarms on page 21.

Tools and utilities overview

Three interfaces may be used to manage fault that occur on the GWC:

- Use the maintenance and administration position (MAP) terminal to access the logutil application on the XA-core to retrieve PM logs.
- If the fault is related to a service that the GWC performs, such as a trunk or line service, use the CS 2000 GWC Manager to clear the fault.
- If the fault is related to the hardware state of the GWC card, then use the CS 2000 SAM21 Manager to clear the fault.

For information on how to access the CS 2000 GWC Manager and the CS 2000 SAM21 Manager, refer to the CS 2000 Management Tools information in the ATM/IP Solution-level Security and Administration NTP, NN10402-600.

Comparing the CS 2000 element managers

The SAM21 Shelf Controllers do not associate Non System Slot (NSS) cards, such as GWCs, as mated pairs and do not monitor application redundancy on GWC cards. For example, a hardware failure resulting in the loss of communication between the element managers and a GWC card in the node is handled as follows:

- The CS 2000 GWC Manager places the card in an “unknown” state and displays a minor alarm.

  Any service alarms which were raised by the CS 2000 GWC Manager when the GWC card failed are persisted by the alarm manager, and will continue to be displayed until card service is restored.

- The Shelf Controller attempts to recover the card and return it to service.

  Although no alarm is raised on the CS 2000 SAM21 Manager, logs are generated indicating that a card has failed.

Integrated Element Management System

Many FCAPS activities may now be performed using the Integrated Element Management System (EMS). In addition, access to the CS 2000 GWC Manager and the CS 2000 SAM21 Manager is now provided using the Integrated EMS. For more information, refer to the Integrated EMS Basics NTP, NN10329-111.

To launch the CS 2000 GWC Manager or the CS 2000 SAM21 Manager, refer to the following procedures in the Integrated EMS Basics NTP, NN10329-111:

- “Launching GWC Manager”
- “Launching SAM21 Manager”

Note: If you wish to acknowledge alarms, refer to the Integrated EMS Fault Management NTP, NN10334-911.

GWC fault management in a DQoS network

In a network using dynamic quality of service (DQoS) implemented for a cable solution, there exist TCP connections between the GWCs and cable modem termination system (CMTS) devices used for authorizing allocation of network resources for each call or connection. A DQoS common open policy service (COPS) connection is a TCP/IP connection used to allow the GWC or policy decision point (PDP) to send call authorizations to the CMTS or PEP. If one of these connections should fail, the gateways associated with the CMTS and controlled by the GWC may still be able to make calls.

> ***Note:*** When a dynamic quality of service (DQoS) connection is down between the CS 2000 and a CMTS, the CS 2000 will allow new calls hosted by that CMTS to proceed without DQoS. The behavior of the multimedia terminal adapter (MTA) and CMTS determines whether new calls are attempted using best-effort service or whether they are torn down:
>
> - Some MTA vendors allow calls to proceed as data calls (best-effort) and do not send a data-over-cable service interface specification (DOCSIS) authorization block to the CMTS. In this case, the CMTS cannot recognize the call as a voice call and it proceeds without managed quality of service.
> - Other MTA vendors send the DOCSIS authorization block to the CMTS with no authorization key or gate-id. When this happens, the CMTS decides whether or not to allow calls to proceed.
>
> When the DQoS connection is up, but the CS 2000 does not receive a DQoS gate-id from the CMTS, the CS 2000 will tear down a call.

Some CMTS devices are capable of terminating more than the 6400 lines supported on a GWC node. It is therefore important that the customer be alerted to any connection failures between the GWC and CMTS devices. Such connection failures will be reported to the CS 2000 GWC Manager alarm panel.

DQoS COPS alarm description

If a CMTS connection fails on a GWC, a major alarm will be raised using an SNMP trap to the alarm manager. The alarm will automatically be cleared in the same manner when the connection is restored. A DQoS connection alarm will be asserted by the GWC node for each of its connections if:

- the connection fails 3 or more times during the 15 second alarm reporting interval
- the connection fails for more than 5 seconds

A DQoS connection alarm is cleared if:

- the connection failed less than 3 times during the 15 second alarm reporting interval
- the connection is up and initialized
- the connection has been removed by provisioning activity

The alarm text displays “DQoS/COPS connection failure” with specific alarm text “DQoS connection <cmts_name> has failed - attempting recovery.” Since the GWC automatically attempts to re-establish any connection, the connection may be recovered before the alarm is actually reported. In this case, the alarm is cleared during the next alarm reporting interval (approximately 15 seconds).

> ***Note:*** If a connection cannot be recovered and the CMTS appears to be functioning normally, call Nortel Support to investigate the problem.

All DQoS connections are managed in the GWC software to remain up at all times. If a connection fails, the GWC automatically recovers the connection by reconnecting to the CMTS. When a connection fails, the connection is retried almost immediately. If the retry fails, retries continue at a fixed interval until the connection is successfully established or until the provisioning is removed.

DQoS connection alarms are reported at least every 15 seconds and at most every 30 seconds after the fault is detected. A connection is considered to be in alarm status if it fails 3 or more times within the 15 second reporting window, or if it is down for more than 5 seconds total during the reporting window. A connection failure that occurs between two reporting windows, such that 2 seconds of outage occur in one window and 3 seconds occur in the next window, is reported in the second window. None of these intervals are customer configurable.

Troubleshooting DQoS/COPS connection failures

In the event of a COPS connection failure that does not quickly recover, perform the following activities:

- Verify that the CMTS specified in the alarm is operational and running a DQoS-capable software version. Look for fault indications on the CMTS that may have led to a failure of the DQoS/COPS server on the CMTS.
- Verify that the PEP server IP address can be pinged from the GWC IP address. This rules out cable cuts and network problems.

- Look for alarms and logs generated by the CMTS to the CS 2000 GWC Manager alarm browser or the OSS (if applicable to your solution).
- Verify that the PEP server IP address configured in the CS 2000 GWC Manager is correct. The PEP IP address is normally the address assigned to the ethernet interface on the CMTS chassis.
- Verify that the network is functioning between the GWC that raised the alarm and the CMTS specified in the alarm. This can be done using ping, tracert or similar operating system-level networking tools.

If the problem cannot be resolved, contact your next level of support for assistance.

GWC card auto-recovery and boot auditing

In the event of an application failure on a GWC card, the card will go through an auto-recovery sequence to automatically bring the application back into service.

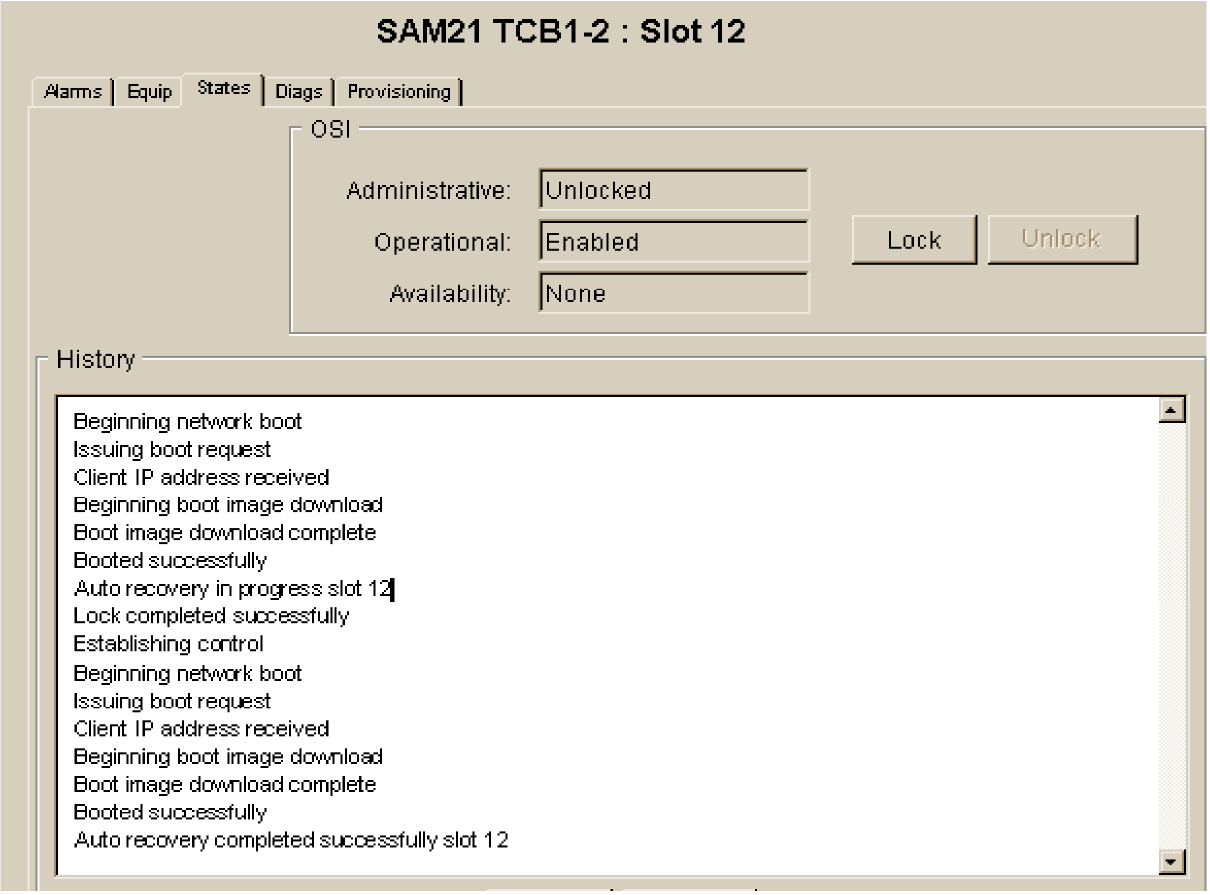
> ***Note:*** When an application failure occurs, the card will be "unlocked-enabled" in the CS 2000 SAM21 Manager, but disabled at the card application level in the CS 2000 GWC Manager.

There are two stages recover from an application failure:

1. The Motorola firmware on the GWC card will perform a network autoboot of the card, forcing the card to attempt to boot a software image from the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM).
2. If the network autoboot fails, the SAM21 shelf controller will then perform a boot of the card in a backup attempt to bring the application into service. This boot audit occurs routinely across the entire shelf.

   For more information, refer to the SAM21 Shelf Controller Fault Management NTP, NN10089-911.

A sample of the auto-recovery progress text displayed in the "History" window is shown below.



Administrative: Unlocked

Operational: Enabled

Availability: None

```
Beginning network boot
Issuing boot request
Client IP address received
Beginning boot image download
Boot image download complete
Booted successfully
Auto recovery in progress slot 12
Lock completed successfully
Establishing control
Beginning network boot
Issuing boot request
Client IP address received
Beginning boot image download
Boot image download complete
Booted successfully
Auto recovery completed successfully slot 12
```

During the boot audit the user will see the GWC card transition from “unlocked-enabled” to “locked-disabled” to “unlocked-disabled” to “unlocked-enabled” in the Card States panel. At the same time, text in the History window of the Card States panel will display an “Auto-recovery in Progress” message followed by the boot recovery sequence messages.

> ***Note:*** The GWC boot audit recovery sequence is also captured in the NSS_boot_audit logs on the shelf controller, as follows:

```
Apr 29 19:36:03: Slot 12 (MCPN750-8): Reset SNMP.1.3.6.1.4.1.562.28.0.1.5.1.2.10
Apr 29 19:36:03: Slot 12 (MCPN750-8): Received MAC address: 08003E2D46D8
Apr 29 19:36:03: Slot 12 (MCPN750-8): Attempting to recover board
Apr 29 19:36:04: Slot 12 (MCPN750-8): Rebooting board
Apr 29 19:36:19:Slot 12 (MCPN750-8): It took 60s to download boot file.
Apr 29 19:36:04: Slot 12 (MCPN750-8): FW_FLASH_VALUE=1
Apr 29 19:40:30: Slot 12 (MCPN750-8): Recovery attempt completed
```

Routine maintenance

To prevent faults from occurring, perform the following routine maintenance activities at the specified time intervals:

- Replace the three air filters from the front of the fan sleds on the SAM21 shelf using the following guidelines:
  - — Replace these air filters once every 10,000 hours (approximately one year and seven weeks) of service.
  - — When replacing the air filters, replace one air filter at a time and do not leave a fan uninserted for more than one minute.

  The Nortel part number for the three air filters is A0828397.
- 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.

Perform this task once weekly. Refer to the figure on the next page for details.

The following LEDs appear on the front of a GWC card:

— BFL (Board failure) LED (yellow) - Lights when a system failure occurs on the card.

— CPU activity LED (green) - Lights when the card's processor is currently active.

— Hot swap status LED (blue) - Lights when it is permissible to remove the card from the shelf.

In addition to the LEDs, there is also an ABT/RST (abort / reset) button on the front of GWC card. Press this button briefly (for less than three seconds) to abort the CPU's current process. Press and hold this button (for more than three seconds) to reset the card.

- Check and secure the cables and connectors for all GWC cards using the following guidelines:

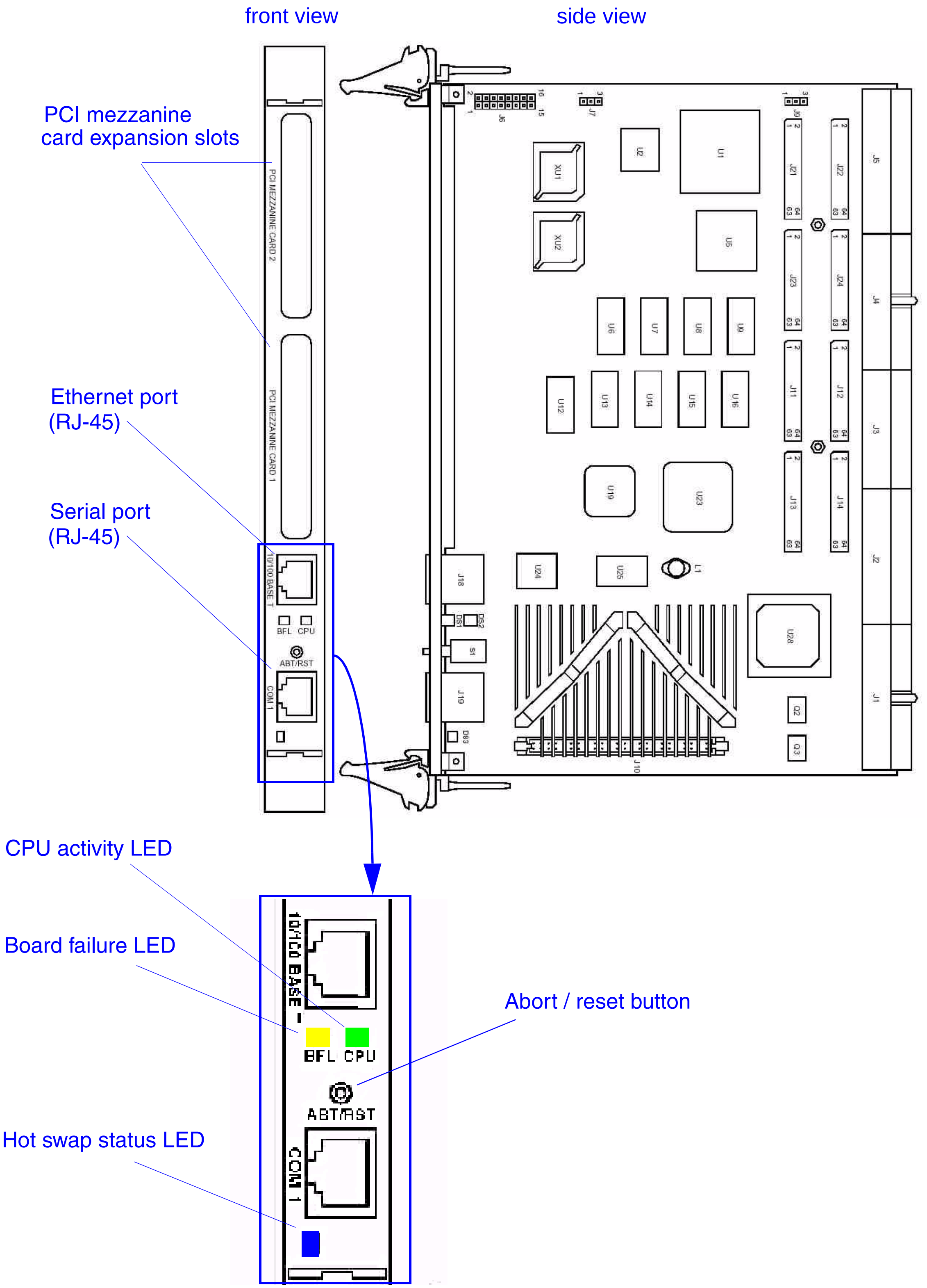
— Check the routing of the cables and how they are secured.

— Ensure that the data and power cables are routed separately.

— Inspect the integrity of all cabling to ensure there is no frayed wiring. Perform these tasks once weekly.

The following figure shows the connectors and slots on the front of a GWC card. The Ethernet port is the card's main network connection. The peripheral component interconnect (PCI) mezzanine card expansion slots are currently not used on a GWC card.

Note: Consult your Nortel installation staff for proper maintenance practices.


front view
side view
PCI mezzanine card expansion slots
Ethernet port (RJ-45)
Serial port (RJ-45)
PCI MEZZANINE CARD 2
PCI MEZZANINE CARD 1
10/100 BASE T
BFL
CPU
ABT/RST
COM 1
CPU activity LED
Board failure LED
Abort / reset button
Hot swap status LED
U1
U2
U5
XU1
XU2
U6
U7
U8
U9
U12
U13
U14
U15
U16
U19
U23
U24
U25
U28
L1
J1
J2
J3
J4
J5
J6
J7
J9
J10
J11
J12
J13
J14
J18
J19
J21
J22
J23
J24
DS1
DS2
DS3
S1
Q2
Q3

List of fault management procedures

This section lists the procedures available in this NTP by general fault management category.

Alarm surveillance and reporting procedures

The following table lists the alarm surveillance and reporting procedures available in this NTP:

Alarm surveillance and reporting procedures
• View GWC service alarm history on page 17
• View and troubleshoot GWC service alarms on page 21
• View GWC platform hardware alarms on page 35
• View and interpret the operational status of a GWC node on page 38
• Filter GWC service alarms on page 43

Test invocation procedures

The following table lists the test invocation procedures available in this NTP:

Test invocation procedures
• Perform GWC hardware diagnostics on page 47
• Access and print GWC diagnostic results on page 52
• Perform a GWC line data integrity audit on page 102
• Perform a GWC trunk data integrity audit on page 114

Log collection configuration and review

The following table lists the log collection configuration and review procedures available in this NTP:

Log collection configuration and review procedures
• View GWC PM logs on page 53
• View GWC logs in syslog files on page 54
• Access the debug log to view GWC auto-image events on page 58
• View and troubleshoot GWC auto-image error logs on page 61
• For international markets using a cable solution, Review GWC V5.2 audit logs and investigate problems on page 142

Fault correction procedures

The following table lists the fault correction procedures available in this NTP:

Fault correction procedures
• Re-provision a GWC card automatically on page 71
• Restart or reboot a GWC card on page 80
• Restart GWC card services on page 84
• Diagnose problems with a GWC card that cannot be booted on page 88
• Replace and re-provision a GWC card on page 92
• Perform a GWC V5.2 data integrity audit on page 134
• Perform a CS 2000 data integrity audit on page 126

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.

Note 1: The alarm history option provides access to UAS and APS device alarms, as well as to other alarms that are not specific to any Carrier Voice over IP (VoIP) component.

Note 2: Access to platform-related alarms is provided in procedure View GWC platform hardware alarms on page 35.

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.

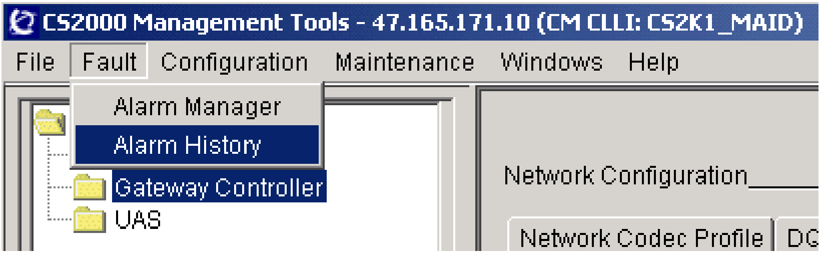
Prerequisites

This procedure has no prerequisites.

Action

At the CS 2000 GWC Manager client

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



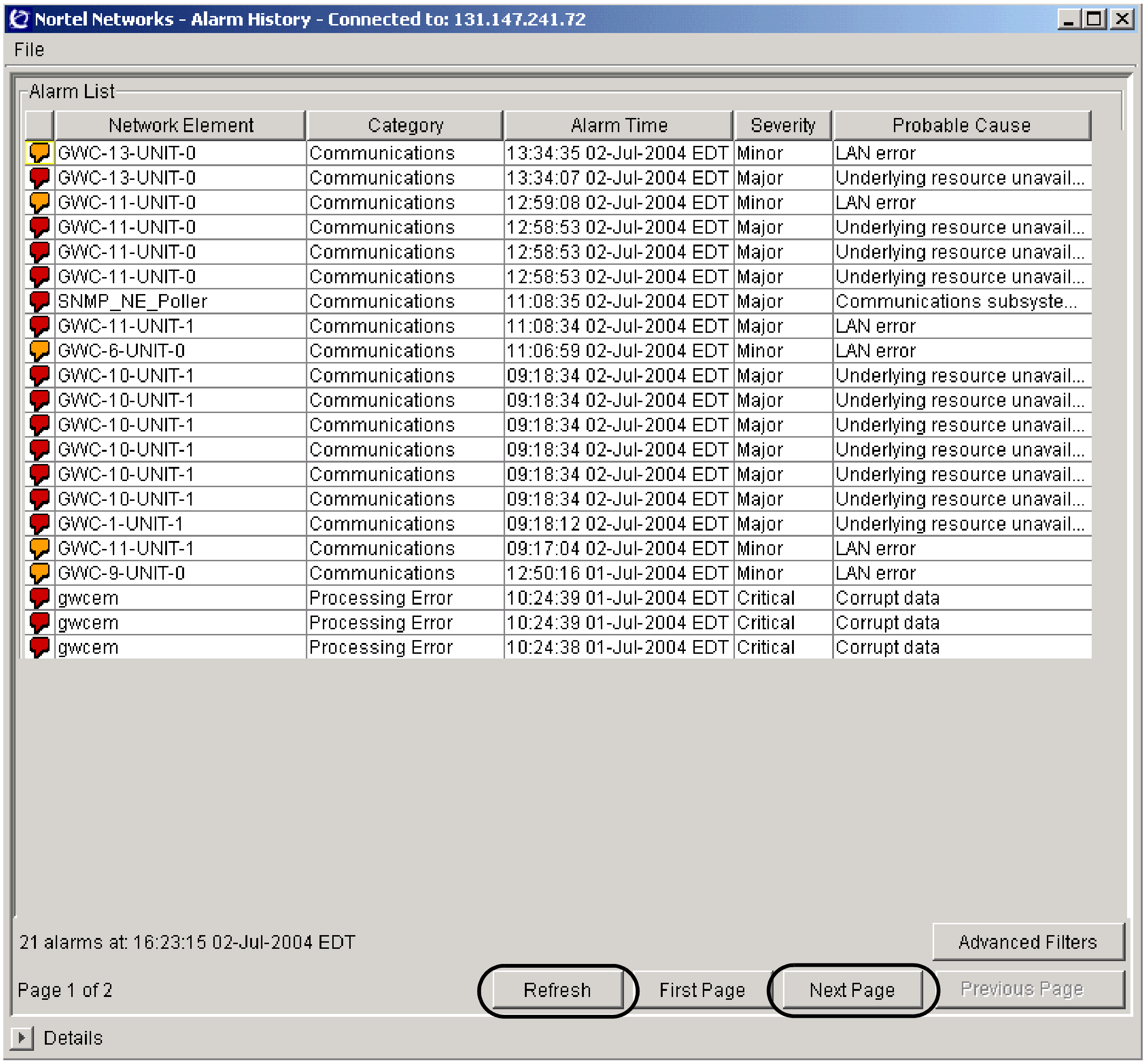
2 Review the alarms displayed.

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.

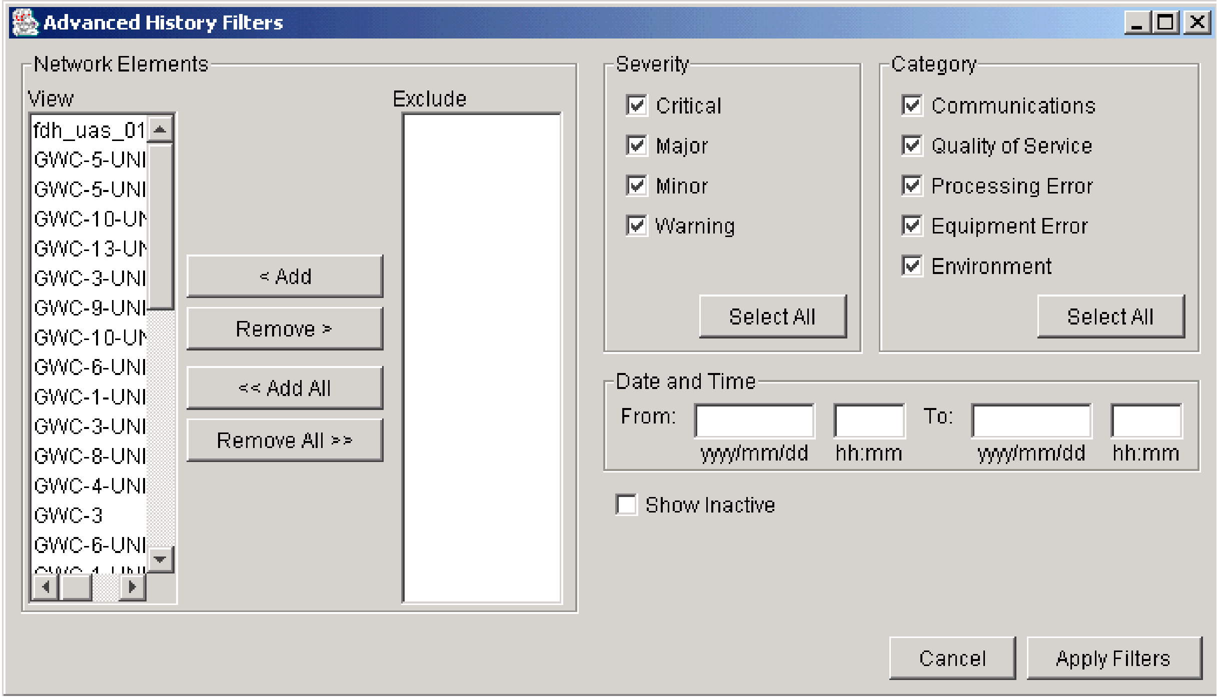

Nortel Networks - Alarm History - Connected to: 131.147.241.72
File
Alarm List

	Network Element	Category	Alarm Time	Severity	Probable Cause
🟧	GWC-13-UNIT-0	Communications	13:34:35 02-Jul-2004 EDT	Minor	LAN error
🟥	GWC-13-UNIT-0	Communications	13:34:07 02-Jul-2004 EDT	Major	Underlying resource unavail...
🟧	GWC-11-UNIT-0	Communications	12:59:08 02-Jul-2004 EDT	Minor	LAN error
🟥	GWC-11-UNIT-0	Communications	12:58:53 02-Jul-2004 EDT	Major	Underlying resource unavail...
🟥	GWC-11-UNIT-0	Communications	12:58:53 02-Jul-2004 EDT	Major	Underlying resource unavail...
🟥	GWC-11-UNIT-0	Communications	12:58:53 02-Jul-2004 EDT	Major	Underlying resource unavail...
🟥	SNMP_NE_Poller	Communications	11:08:35 02-Jul-2004 EDT	Major	Communications subsyste...
🟥	GWC-11-UNIT-1	Communications	11:08:34 02-Jul-2004 EDT	Major	LAN error
🟧	GWC-6-UNIT-0	Communications	11:06:59 02-Jul-2004 EDT	Minor	LAN error
🟥	GWC-10-UNIT-1	Communications	09:18:34 02-Jul-2004 EDT	Major	Underlying resource unavail...
🟥	GWC-10-UNIT-1	Communications	09:18:34 02-Jul-2004 EDT	Major	Underlying resource unavail...
🟥	GWC-10-UNIT-1	Communications	09:18:34 02-Jul-2004 EDT	Major	Underlying resource unavail...
🟥	GWC-10-UNIT-1	Communications	09:18:34 02-Jul-2004 EDT	Major	Underlying resource unavail...
🟥	GWC-10-UNIT-1	Communications	09:18:34 02-Jul-2004 EDT	Major	Underlying resource unavail...
🟥	GWC-10-UNIT-1	Communications	09:18:34 02-Jul-2004 EDT	Major	Underlying resource unavail...
🟥	GWC-1-UNIT-1	Communications	09:18:12 02-Jul-2004 EDT	Major	Underlying resource unavail...
🟧	GWC-11-UNIT-1	Communications	09:17:04 02-Jul-2004 EDT	Minor	LAN error
🟧	GWC-9-UNIT-0	Communications	12:50:16 01-Jul-2004 EDT	Minor	LAN error
🟥	gwcem	Processing Error	10:24:39 01-Jul-2004 EDT	Critical	Corrupt data
🟥	gwcem	Processing Error	10:24:39 01-Jul-2004 EDT	Critical	Corrupt data
🟥	gwcem	Processing Error	10:24:38 01-Jul-2004 EDT	Critical	Corrupt data

21 alarms at: 16:23:15 02-Jul-2004 EDT

Page 1 of 2

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



Advanced History Filters

Network Elements

View

fdh_uas_01
GWC-5-UNI
GWC-5-UNI
GWC-10-UN
GWC-13-UN
GWC-3-UNI
GWC-9-UNI
GWC-10-UN
GWC-6-UNI
GWC-1-UNI
GWC-3-UNI
GWC-8-UNI
GWC-4-UNI
GWC-3
GWC-6-UNI

Exclude

Severity

☑ Critical
☑ Major
☑ Minor
☑ Warning

Category

☑ Communications
☑ Quality of Service
☑ Processing Error
☑ Equipment Error
☑ Environment

Date and Time

From: ____ yyyy/mm/dd ____ hh:mm To: ____ yyyy/mm/dd ____ hh:mm

☐ Show Inactive

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.

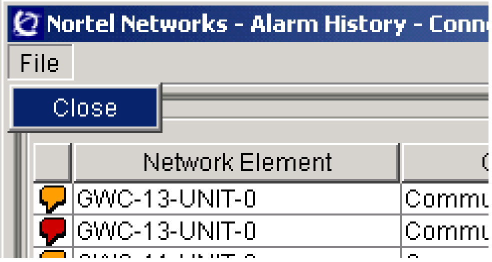
c De-select the alarm Severity check boxes to exclude (filter) an alarm type for the GWC units in the Exclude list. Any alarm severities that remain selected will be included (will not be filtered) for the GWC units in the Exclude list. If necessary, click the **Select All** button to select all alarm 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.

View and troubleshoot GWC service alarms

Purpose of this procedure

Use this procedure to access service-related alarms that are currently active on the GWC application. The Alarm Manager displays alarms as they occur (in real time). This option also permits alarm display filtering based on GWC unit and alarm category.

Refer to section Troubleshooting GWC service alarms on page 26 at the end of this procedure for details about GWC alarm types. Table Troubleshooting GWC service alarms on page 27 contains appropriate actions to diagnose and resolve the alarm condition.

> ***Note:*** The alarm manager option provides access to UAS and APS device alarms, as well as to other alarms that are not specific to any Carrier VoIP network component.

Access to platform-related alarms is provided in procedure View GWC platform hardware alarms on page 35.

When to use this procedure

Use this procedure as a primary source for fault diagnostic information related to GWC services.

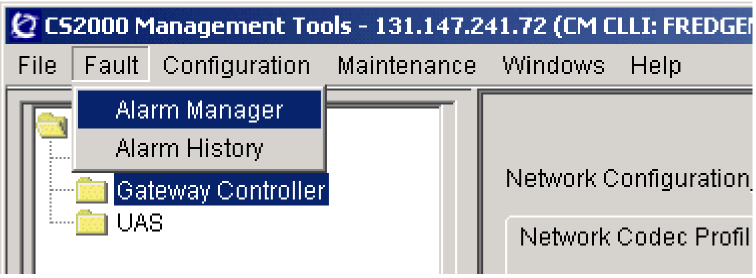
Prerequisites

This procedure has no prerequisites.

Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the **Fault** menu and select **Alarm Manager** to open the Alarm Manager window.



2 From the Alarm Manager window, review the alarms displayed.

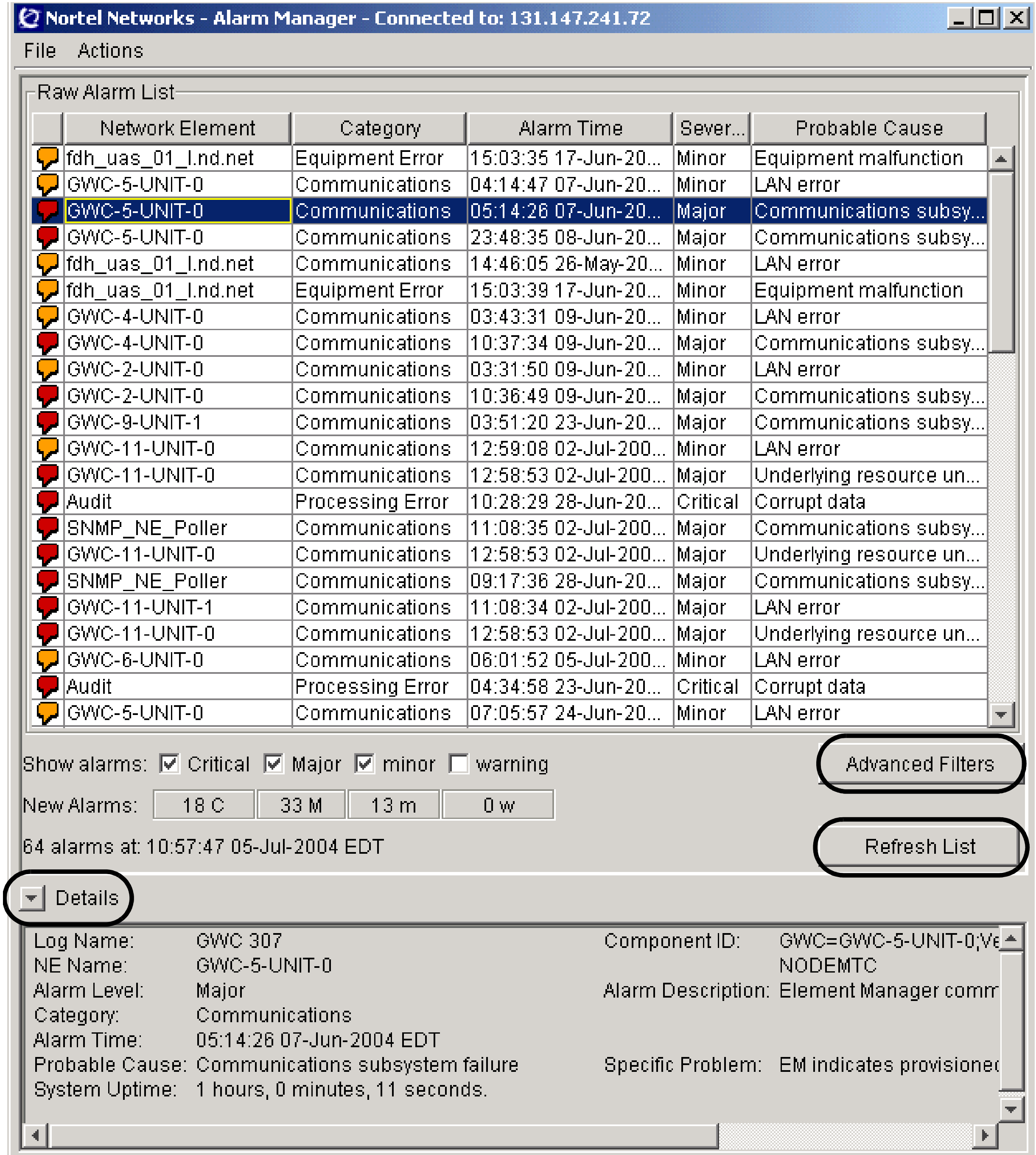
The colors to the left of the alarm display provide a visual indication of alarm severity:

- yellow - warning,
- orange - minor
- red - major and critical

Refer to section Troubleshooting GWC service alarms on page 26 at the end of this procedure for details about the alarm types displayed, including appropriate actions to diagnose and resolve the alarm condition. Table Troubleshooting GWC service alarms on page 27 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 subsy...
🟥	GWC-5-UNIT-0	Communications	23:48:35 08-Jun-20...	Major	Communications subsy...
🟧	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 subsy...
🟧	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 subsy...
🟥	GWC-9-UNIT-1	Communications	03:51:20 23-Jun-20...	Major	Communications subsy...
🟧	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 subsy...
🟥	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 subsy...
🟥	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

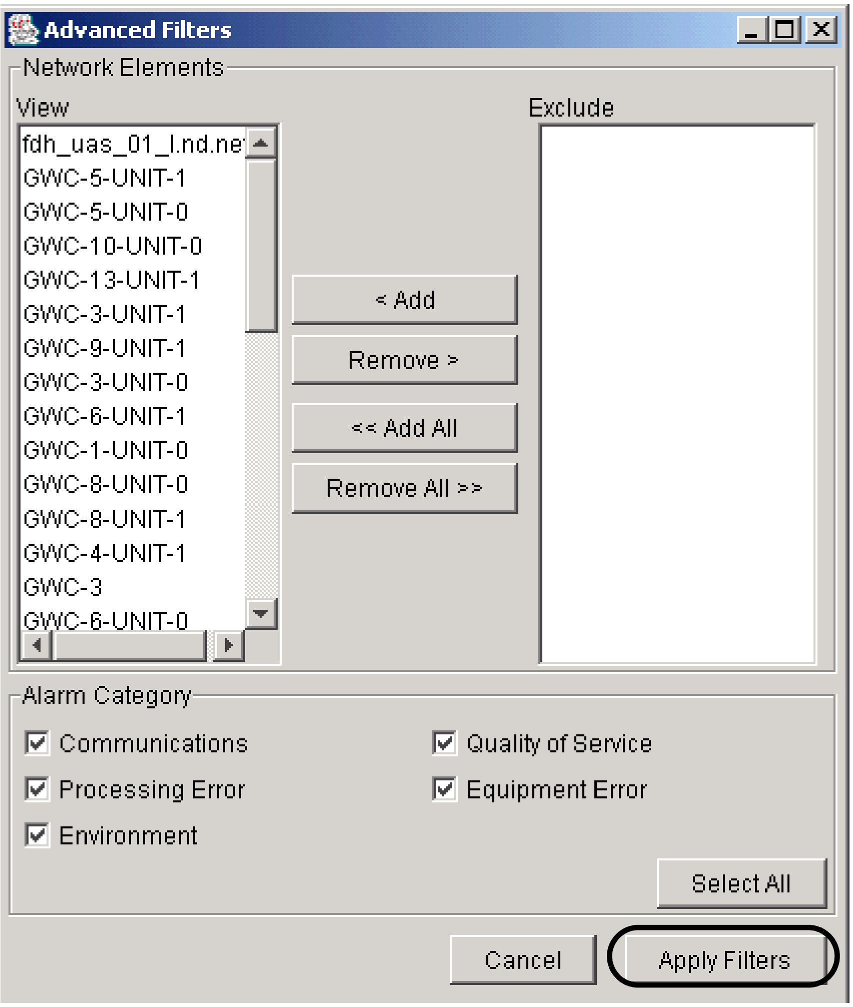
New Alarms: 18 C 33 M 13 m 0 w

64 alarms at: 10:57:47 05-Jul-2004 EDT

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 provisioned

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.



fdh_uas_01_l.nd.ne
GWC-5-UNIT-1
GWC-5-UNIT-0
GWC-10-UNIT-0
GWC-13-UNIT-1
GWC-3-UNIT-1
GWC-9-UNIT-1
GWC-3-UNIT-0
GWC-6-UNIT-1
GWC-1-UNIT-0
GWC-8-UNIT-0
GWC-8-UNIT-1
GWC-4-UNIT-1
GWC-3
GWC-6-UNIT-0

☑ Communications
☑ Quality of Service
☑ Processing Error
☑ Equipment Error
☑ Environment

Perform the following steps at the Advanced filters dialog box:

a In the view list, select the GWC units to be excluded (filtered). You can press and hold the <Shift> key to select multiple GWC units.

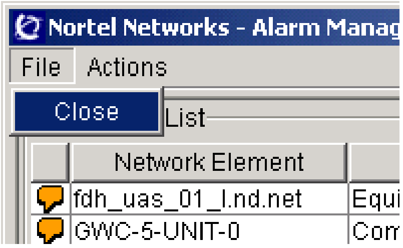
b Click the **Remove** > button to place the selected GWC units in the Exclude (filtered) list. Click the **Remove All** >> button to place all GWC units in the Exclude (filtered) list.

If necessary, select GWC units in the Exclude list. Then, click the **< Add** button to place the selected GWC units in the View (unfiltered) list. Click the **<< Add All** button to place all GWC units in the View (unfiltered) list.

c De-select the Alarm Category check boxes to exclude (filter) an alarm type for the GWC units in the Exclude list. Any alarm categories that remain selected will be included (will not be filtered) for the GWC units in the Exclude list.

d After you have selected the filter criteria click the **Apply Filters** button.

6 When you are finished with the Alarm Manager, click the **File** menu and select **Close**.



	Network Element	
	fdh_uas_01_l.nd.net	Equi
	GWC-5-UNIT-0	Com

7 This procedure is complete.

Troubleshooting GWC service alarms

Table Troubleshooting GWC service alarms on page 27 contains details about GWC alarm types, and includes appropriate actions to diagnose and resolve the alarm condition.

> ***Note:*** An alarm ID code for each alarm appears in the first column of the table under the alarm description. You can also find these logs with the alarm ID code in the following locations:
>
> - The syslog Customerlog files in the /var/log directory on the CS 2000 Management Tools server. For example, see the file customerlog.1.
>
>   For information on how to open these Syslog log files and search for alarm codes, refer to procedure View GWC logs in syslog files on page 54 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 (SDM) or Core and Billing Manager (CBM). The CS 2000 Management Tools server must be configured to send the syslog logs to the CS 2000 Core Manager or CBM.
> - Switch Control Center (SCC2) or Nortel Networks STD log formats available on the customer's Operations Support System (OSS) interface.
>
>   Conversion to these log formats must be activated at the CS 2000 Core Manager or CBM. For information on configuring log

delivery to the customer’s OSS, refer to the Fault Management NTP for the CS 2000 Core Manager (SDM) or CBM.

Troubleshooting GWC service alarms (Sheet 1 of 8)

Alarm description **Alarm ID code**	**Severity**	**Specific problem** **Probable cause**	**Action**
Recovery alarm GCEM301	Critical 💬	A GWC recovery process has terminated early, and the GWC remains out of service. This alarm is generated by the CS 2000 GWC Manager rather than the GWC.	Check IP communications from OAM system to the GWC. Check the CS 2000 Management Tools server logs for additional information, and BSY/RTS the affected GWC unit.
Active unit disabled GWC300	Critical 💬	• Specific problem: Indicates that a unit is out of service: Service is not available. Probable cause: the lack of availability of the underlying resource.	This alarm reports that the unit is not in service (Operational state of "disabled"). If the Administrative state is “unlocked” and the Usage state is “busy” this indicates the unit is trying to recover itself to an in service state. Note that when both units are out of service, the active unit must recover before the standby unit will. Check the following: 1- Whether the unit is manually locked out of service (Administrative state of “locked”). 2- Alarms that may indicate a problem on the unit preventing it from returning to service. 3- Other state indicators which may indicate problems, such as - Isolation state of “isolated” - Availability state of “offLine” 4- Logs which may also indicate a failure of a step in the process of recovering the unit.
		• Specific problem: Indicates that a unit has invalid GWC Profile Data: Service is not available. Probable cause: A configuration or customization error.	Check the profile data for the unit and do one of the following: - Change to another profile. - Reconfigure the GWC unit software or CS 2000 GWC Manager software to remove the incompatibility. Then, RTS the unit.

Troubleshooting GWC service alarms (Sheet 2 of 8)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
Standby unit disabled GWC301	Major 💬	Specific problem: Unit is out of service - Service is not available. Probable cause: The lack of availability of the underlying resource.	This alarm reports that the unit is not in service (Operational state of “disabled” and Administrative state is “unlocked”). The unit is system busy (SysB). If the Administrative state is “unlocked” and the Usage state is “busy” this indicates the unit is trying to recover itself to an in service state. Note that when both units are out of service, the active unit must recover before the standby unit will. Check the following: 1 - Alarms that may indicate a problem on the unit preventing it from returning to service. 2 - Other state indicators which may indicate problems, such as - Isolation state of “isolated” - If it is the standby unit, Availability state of “degraded” - Availability state of “offLine” 3- Logs which may also indicate a failure of a step in the process of recovering the unit.

Troubleshooting GWC service alarms (Sheet 3 of 8)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
Standby unit disabled GWC301	Minor 🗨	• Specific problem: Unit is out of service - Service is not available. Probable cause: The lack of availability of the underlying resource.	This alarm reports that the unit is not in service (Operational state of “disabled” and Administrative state is “locked”). The unit is manually busy (ManB). If the Administrative state is “unlocked” and the Usage state is “busy” this indicates the unit is trying to recover itself to an in service state. Note that when both units are out of service, the active unit must recover before the standby unit will. Check the following: 1- Alarms that may indicate a problem on the unit preventing it from returning to service. 2- Other state indicators which may indicate problems, such as - Isolation state of “isolated” - If it is the standby unit, Availability state of “degraded” - Availability state of “offLine” 3- Logs which may also indicate a failure of a step in the process of recovering the unit.
		• Specific problem: Unit out of service - invalid GWC Profile Data. Probable cause: Configuration or customization error.	Check the profile data for the unit and do one of the following: - Change to another profile. - Reconfigure the GWC unit software or CS 2000 GWC Manager software to remove the incompatibility. Then, RTS the unit.

Troubleshooting GWC service alarms (Sheet 4 of 8)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
Core communication lost GWC302	Major 🟥	Specific problem: No response received to Core heartbeat messages from active GWC unit. Probable cause: LAN error.	Clears automatically after a Core or network outage clears. Otherwise, verify that the node number and Core Side IP address is correct for the GWC to communicate with the Core.
Core communication lost GWC302	Minor 🟧	Specific problem: No response received to Core heartbeat messages from inactive GWC unit. Probable cause: LAN error.	Clears automatically after a Core or network outage clears. Otherwise, verify that the node number and Core Side IP address is correct for the GWC to communicate with the Core.
Mate unit communication lost GWC303	Minor 🟧	Specific problem: No response received to mate unit heartbeat messages. Probable cause: LAN error.	Cleared by restoring communication from the CS 2000 GWC Manager to the GWC unit. Do this by unlocking the GWC at the CS 2000 SAM21 Manager. Also, verify that the Ethernet cable is connected, and that the GWC is setup to use the correct node number.
Communication with a gateway is down GWC304	Major 🟥	Specific problem: Communication with <Gatewayname> is down. Probable cause: The underlying resource is not available. ***Note:*** In the case of H.323 GWCs, this alarm is generated only for H.323 gateways that contain 64 endpoints or greater.	Cleared by restoring communication to the managed gateway. Do this by verifying the availability of the gateway, and comparing the configuration data at the gateway and the CS 2000 GWC Manager (IP address, protocol/version, etc.).
This is a test alarm generated from pmdebug interface GWC305	Minor 🟧	Specific problem: A test alarm generated to log in to notilog table - not sent to manager. Probable cause: Unspecified reason.	Cleared from pmdebug command (not a customer interface) or with a GWC reload.

Troubleshooting GWC service alarms (Sheet 5 of 8)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
This is a test alarm generated from pmdebug interface GWC305	Any (critical, major, or minor)	Specific problem: Alarms test from debug interface. Probable cause: Unspecified reason.	Cleared from pmdebug command (not a customer interface) or with a GWC reload.
DQoS/COPS connection failure GWC306	Major	Specific problem: A DQoS connection <ConnName> has failed - attempting recovery. Probable cause: Communications subsystem failure. See Note 2 on page 34 for details about what happens when a DQoS connection fails.	The DQoS connection loss alarm is cleared by DCCNXMGR (using DCALARM) when the connection is reestablished or the connection is deleted by provisioning.
Element Manager communication failure GWC307	Major	• Specific problem: CS 2000 GWC Manager indicates provisioned data mismatched in this unit. Probable cause: Communications subsystem failure	Cleared with a Busy/RTS of GWC unit.
		• Specific problem: CS 2000 GWC Manager not responding, provisioned data loaded from local Flash. Probable cause: Communications subsystem failure	Restore communication with the CS 2000 GWC Manager. Determine if the CS 2000 GWC Manager is down and or disconnected. Determine if the GWC has been setup to use the wrong IP address for the CS 2000 GWC Manager at the CS 2000 SAM21 Manager.
Flash memory error GWC308	Minor	Specific problem: Erase of flash sector failed. Probable cause: Equipment malfunction. Flash life span exceeded; the number of writes to flash has exceeded the recommended or intended limit.	Cleared with hardware replacement.

Troubleshooting GWC service alarms (Sheet 6 of 8)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
SA_PERCENTAGE_USAGE GWC309 **Note**: This alarm does not apply to the Wireline Universal Packet Access (UA-AAL1) solution.	Minor	Specific problem: The number of IPSec security associations (that is, secure connections) reached the maximum supported number. Probable cause: Resource at or nearing capacity	This is an information alarm. Report this alarm with details to your next level of support. Note that the alarm clears automatically as SA usage decreases.
Provisioned GWC Profile not yet activated GWC311	Warning	Specific problem: GWC profile loaded into Flash will activate on the next reload. A New GWC Profile has been loaded to GWC FLASH by the CS 2000 GWC Manager, but the GWC is still using the old Profile. Probable cause: Configuration or customization error.	Cleared with a GWC reload.
QoS collection application (QCA) connection failure GWC312	Major (partial outage)	Specific problem: QCA connection <ConnName> has failed - attempting recovery. Probable cause: Communications subsystem failure.	**Note**: No reports are lost since a back up server is collecting them. Check the following: 1- Ensure that the QCA contains the correct properties (port, IP address...). Check that the QCA is properly provisioned using the CS 2000 Management Tools. 2- Use the ping command to see if you can reach the QCA server. If you cannot reach the server, there may be a problem in the network. 3- Verify that there is no memory exhaustion on the QCA server. 4- Restart the QCA application on the server to bring up the links. 5- Try connecting to a QCA on another CS 2000 Management Tools server.

Troubleshooting GWC service alarms (Sheet 7 of 8)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action
QCA connection failure GWC312	Critical (total outage)	Specific problem: QCA connection <ConnName> has failed - attempting recovery. Probable cause: Communications subsystem failure.	Check the following: 1- Ensure that the QCA contains the correct properties (port, IP address...). Check that the QCA is properly provisioned using the CS 2000 Management Tools. 2- Use the ping command to see if you can reach the QCA server. If you cannot reach the server, there may be a problem in the network. 3- Verify that there is no memory exhaustion on the QCA server. 4- Restart the QCA application on the server to bring up the links. 5- Try connecting to a QCA on another CS 2000 Management Tools server.
RMGC overloaded GWC313	Major	Specific problem: RMGC can't process all incoming requests. Probable cause: Resource at or nearing capacity.	The RMGC is temporarily overloaded The alarm will clear itself once the RMGC is able to process requests again. Gateways keep sending requests until they get a response. So, once the overload clears, gateways will be able to register without any further intervention. If this alarm is seen regularly or does not clear, then this is an indication that there is insufficient RMGC processing capacity in the office. Consider commissioning another RMGC.
Location ID reporting connection failure GWC314	Major	Specific problem: Location ID reporting connection <IP address> has failed - attempting to recover. Probable cause: Communications subsystem failure - destination not available.	Clear the alarm condition using one of the following approaches: - Reestablish the connection to the location recipient. - Disable the location ID reporting application. - Busy/RTS the GWC unit.

Troubleshooting GWC service alarms (Sheet 8 of 8)

Alarm description Alarm ID code	Severity	Specific problem Probable cause	Action

Note 1: An alarm ID code for each alarm appears in the first column of the table under the alarm description. You can also find these logs with the alarm ID code in the following locations:

- The syslog Customerlog files in the /var/log directory on the CS 2000 Management Tools server. For example, see the file customerlog.1.

  For information on how to open these Syslog log files and search for alarm codes, refer to procedure View GWC logs in syslog files on page 54 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 (SDM) or Core and Billing Manager (CBM). The CS 2000 Management Tools server must be configured to send the syslog logs to the CS 2000 Core Manager or CBM.
- Switch Control Center (SCC2) or Nortel Networks STD log formats available on the customer's Operations Support System (OSS) interface.

  Conversion to these log formats must be activated at the CS 2000 Core Manager or CBM. For information on configuring log delivery to the customer's OSS, refer to the Fault Management NTP for the CS 2000 Core Manager (SDM) or CBM.

Note 2: When a dynamic quality of service (DQoS) connection is down between the CS 2000 and a CMTS, the CS 2000 will allow new calls hosted by that CMTS to proceed without DQoS. The behavior of the Multimedia Terminal Adapter (MTA) and CMTS determines whether new calls are attempted using best-effort service or whether they are torn down:

- Some MTA vendors allow calls to proceed as a data call (best-effort) and do not send a data-over-cable service interface specification (DOCSIS) authorization block to the CMTS. In this case, the CMTS cannot recognize the call as a voice call and so it proceeds without managed quality of service.
- Other MTA vendors send the DOCSIS authorization block to the CMTS with no authorization key or gate-id. When this happens, the CMTS decides whether or not to allow calls to proceed.

When the DQoS connection is up, but the CS 2000 does not receive a DQoS gate-id from the CMTS, the CS 2000 will tear down a call.

Troubleshooting faults in a DQoS network

Refer to section GWC fault management in a DQoS network on page 8 for information specific to troubleshooting faults in a dynamic quality of service (DQoS) network.

View GWC platform hardware alarms

Purpose of this procedure

This procedure provides access to platform related alarms such as communication over Ethernet, operating system resource availability, and hardware faults.

When to use this procedure

Use this procedure as a part of alarm clearing at the CS 2000 SAM21 Manager or as a secondary source of diagnostic information for GWC application (service) alarms.

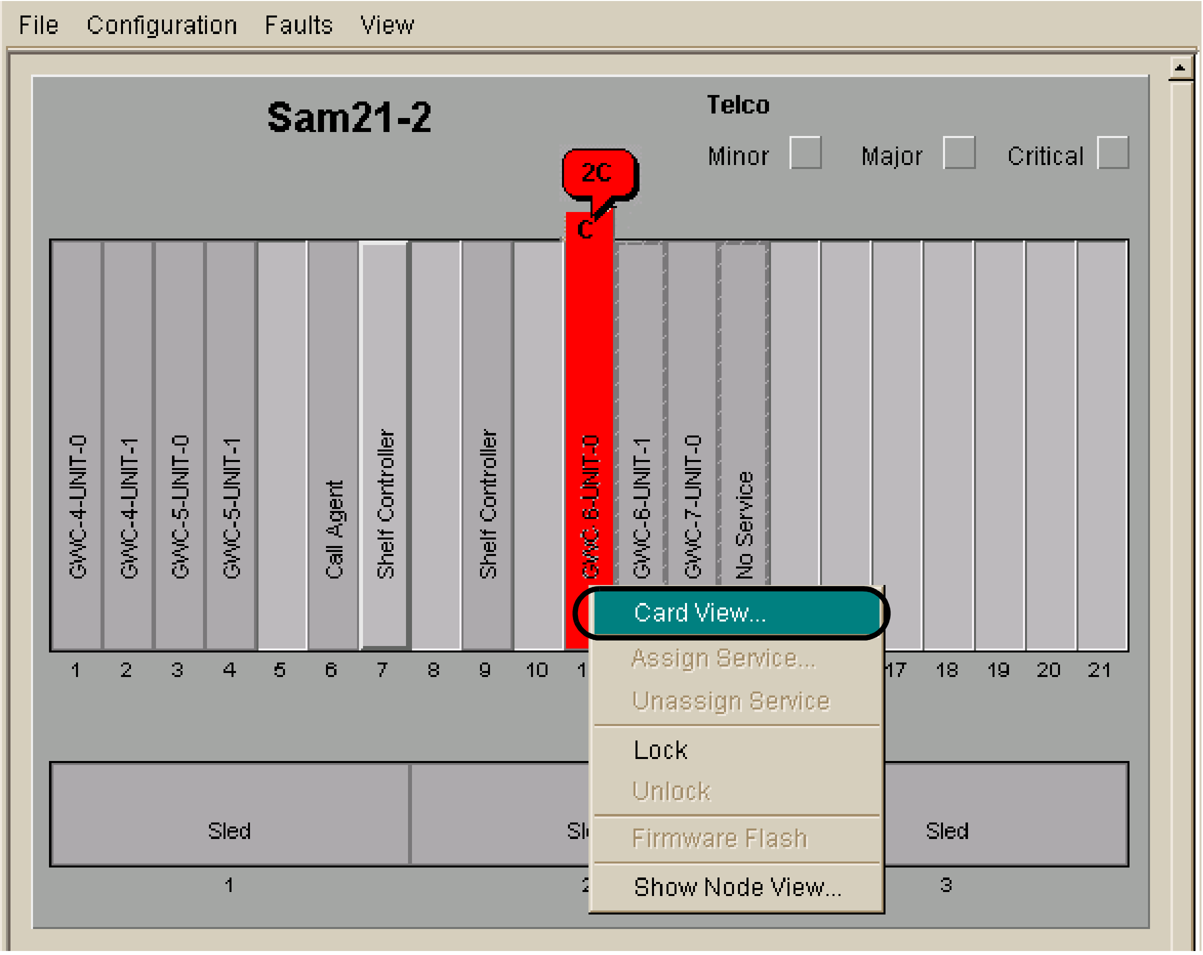
Prerequisites

This procedure has no prerequisites.

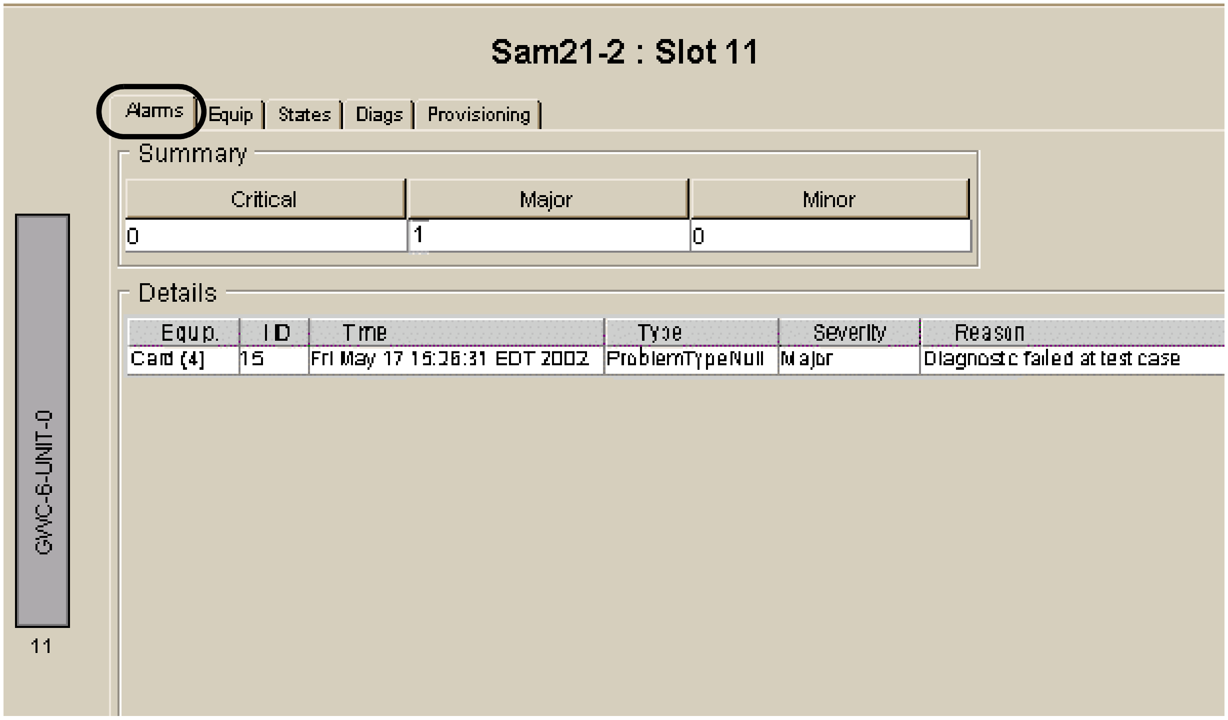
Action

At the CS 2000 SAM21 Manager client

1 Open the Card View for the card in an alarm condition by right-clicking the card and selecting **Card View** from the pop-up menu.



2 Select the **Alarms** tab in the Card View window.



Summary

Critical	Major	Minor
0	1	0

Details

Equip.	ID	Time	Type	Severity	Reason
Card (4)	15	Fri May 17 15:36:31 EDT 2002	ProblemTypeNull	Major	Diagnostic failed at test case

- Refer to the SAM21 Fault Management NTP, NN10089911 for details about the various alarms generated by the SAM21 platform.
- For details about individual alarms related to the NSS cards (including the GWC card) in the SAM21 Shelf, refer to CS 2000 Management Tools information in the ATM/IP Solution-level Fault Management NTP, NN10408-900.

3 This procedure is complete.

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.

> ***Note:*** Refer to table CS 2000 GWC Manager status fields on page 40 to interpret the GWC cards (units) status fields.

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.

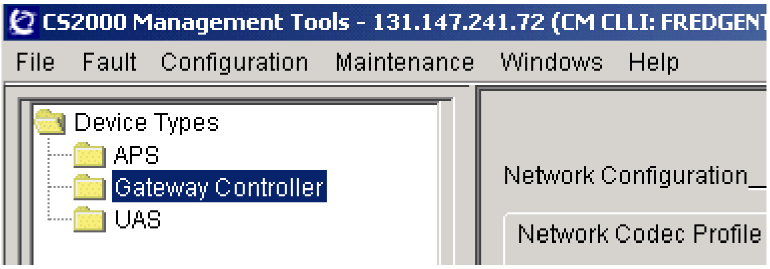
Prerequisites or guidelines

This procedure has no prerequisites or guidelines.

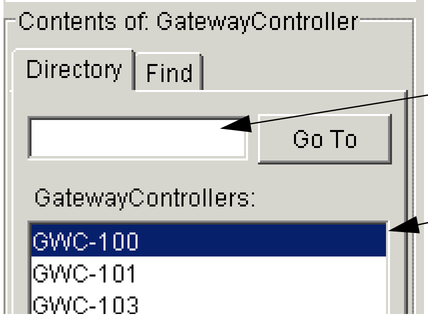
Action

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.


CS2000 Management Tools - 131.147.241.72 (CM CLLI: FREDGENT
File Fault Configuration Maintenance Windows Help
Device Types
APS
Gateway Controller
UAS
Network Configuration
Network Codec Profile

2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.



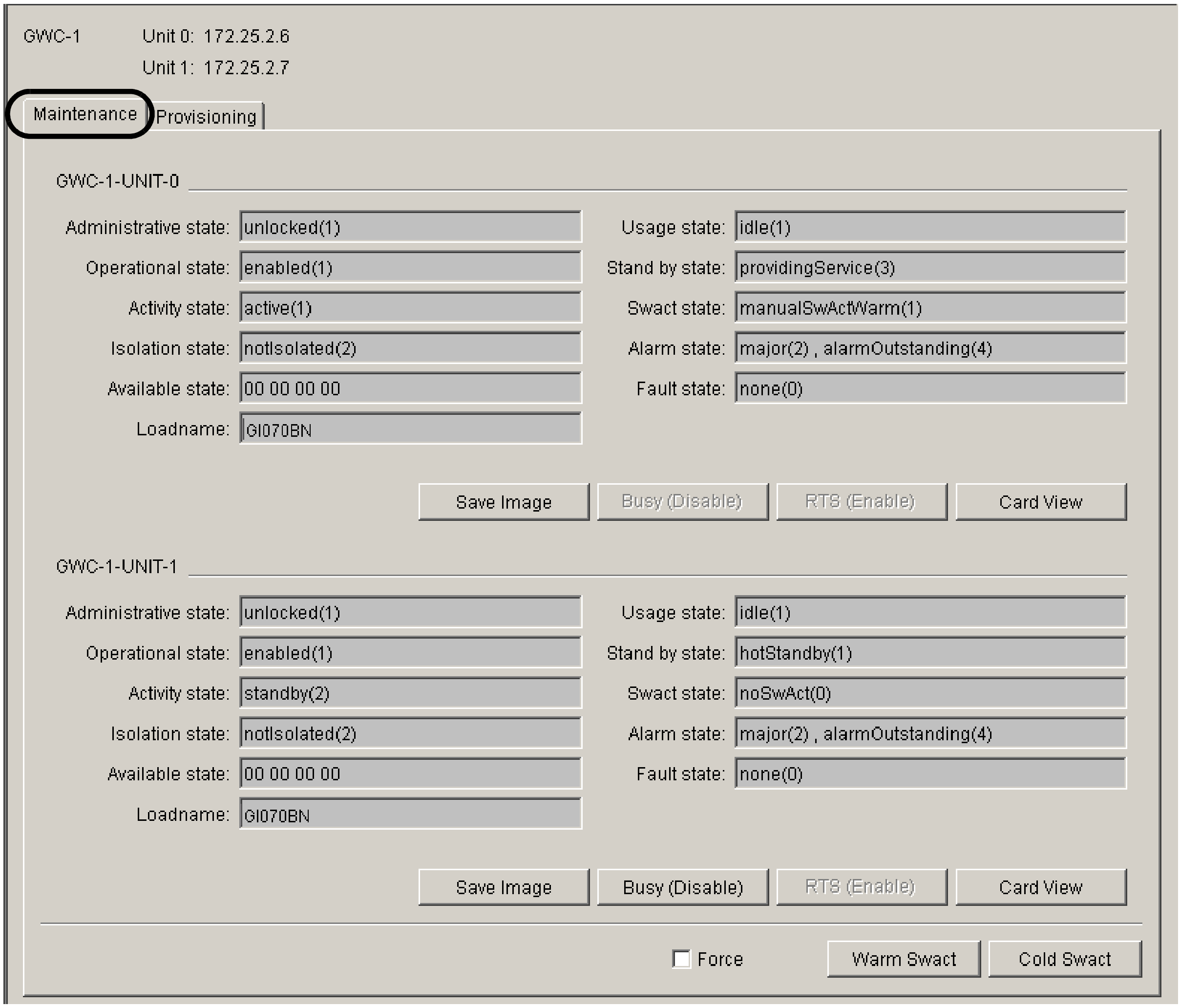
Type a GWC node number here

or

Select a GWC node from the list of provisioned GWC nodes.

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.



GWC-1 Unit 0: 172.25.2.6
Unit 1: 172.25.2.7

GWC-1-UNIT-0

Administrative state: unlocked(1)
Operational state: enabled(1)
Activity state: active(1)
Isolation state: notIsolated(2)
Available state: 00 00 00 00
Loadname: GI070BN
Usage state: idle(1)
Stand by state: providingService(3)
Swact state: manualSwActWarm(1)
Alarm state: major(2) , alarmOutstanding(4)
Fault state: none(0)

GWC-1-UNIT-1

Administrative state: unlocked(1)
Operational state: enabled(1)
Activity state: standby(2)
Isolation state: notIsolated(2)
Available state: 00 00 00 00
Loadname: GI070BN
Usage state: idle(1)
Stand by state: hotStandby(1)
Swact state: noSwAct(0)
Alarm state: major(2) , alarmOutstanding(4)
Fault state: none(0)

4 Refer to table CS 2000 GWC Manager status fields on page 40 following this procedure to interpret the GWC card (unit) status fields.

5 Repeat this procedure for other cards that you wish to view.

6 This procedure is complete.

The following table describes the GWC card (unit) status fields.

CS 2000 GWC Manager status fields (Sheet 1 of 3)

Status field	Possible values	Meaning
Administrative state:	locked	The unit is prohibited, administratively, from providing service to users.
	Note: 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.) 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.
	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 XA-Core.
	notisolated	The unit is communicating with the XA-Core.

CS 2000 GWC Manager status fields (Sheet 2 of 3)

Status field	Possible values	Meaning
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 above 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 (SDM) 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 will be 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.
	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.

CS 2000 GWC Manager status fields (Sheet 3 of 3)

Status field	Possible values	Meaning
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:	00 00 00 00	There are no alarms raised on the GWC card unit.
	critical(1), major(2), minor(3), alarmOutstanding(4)	This field indicates the severity of the currently raised alarms.
Fault state:	none(0)	This field is not used.

Filter GWC service alarms

Purpose of this procedure

Use this procedure to filter (exclude) GWC service related alarms so personnel are not distracted by alarms that are not relevant to their current fault management activities. Also, use this procedure to filter recurring alarms that you are currently addressing.

When to use this procedure

Use this procedure when implementing your fault management alarm strategy. You may also use this procedure to focus on specific alarms during alarm clearing or diagnostic activities.

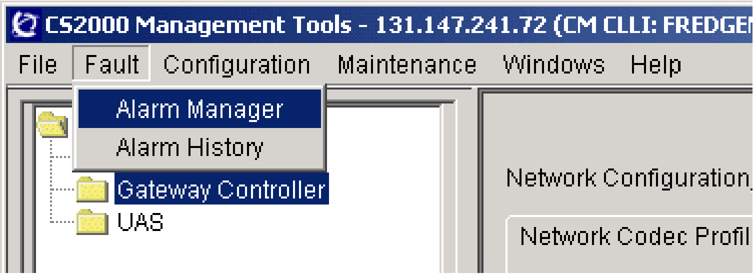
Prerequisites

This procedure has no prerequisites.

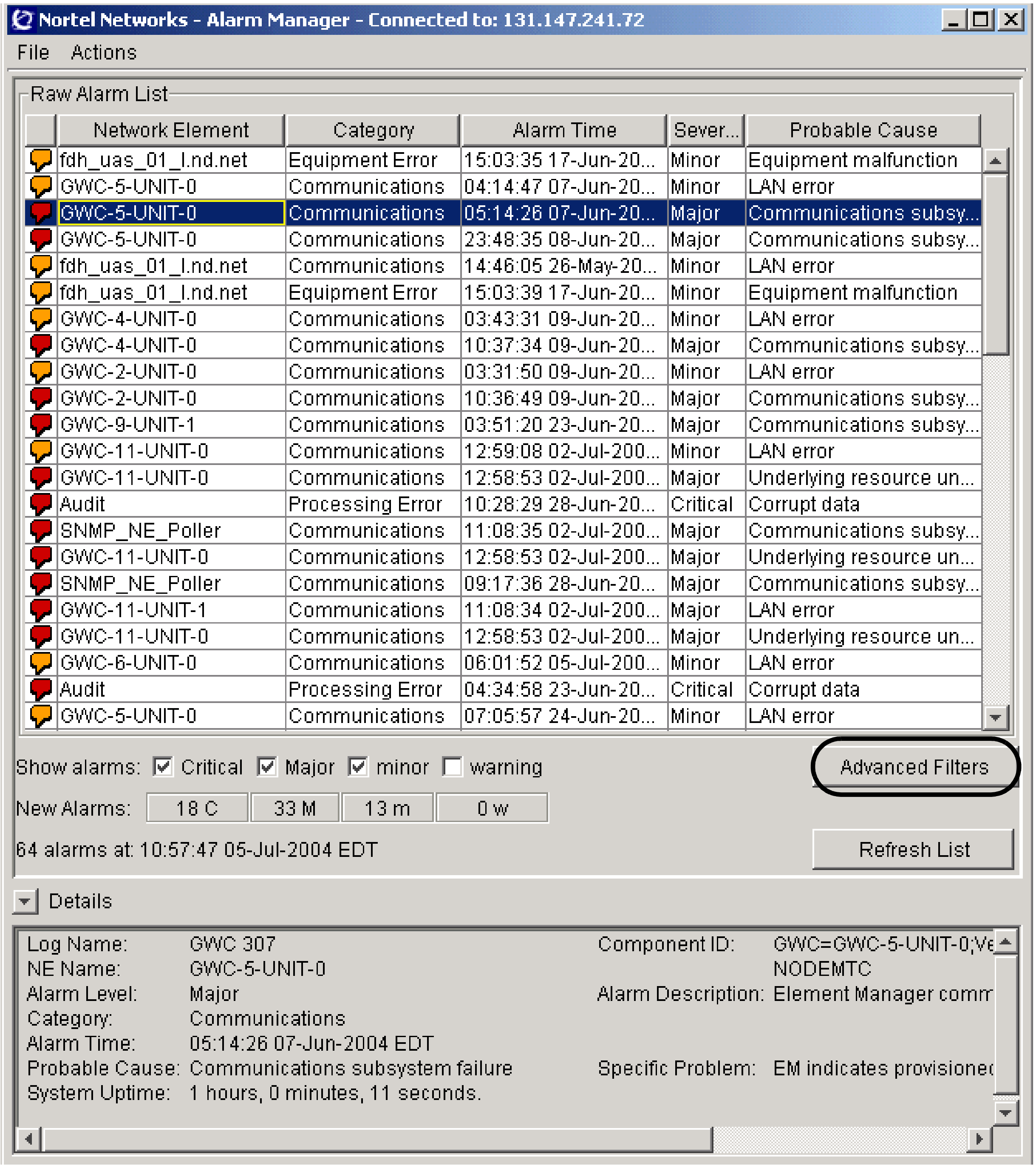
Action

At the CS 2000 GWC Manager client

1 From the CS 2000 Management Tools window, select **Alarm Manager** from the Fault menu to open the Alarm Manager window.



2 Click the **Advanced Filters** button on the Alarm Manager window to open the Advanced Filters window.



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 subsy...
🟥	GWC-5-UNIT-0	Communications	23:48:35 08-Jun-20...	Major	Communications subsy...
🟨	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 subsy...
🟨	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 subsy...
🟥	GWC-9-UNIT-1	Communications	03:51:20 23-Jun-20...	Major	Communications subsy...
🟨	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 subsy...
🟥	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 subsy...
🟥	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

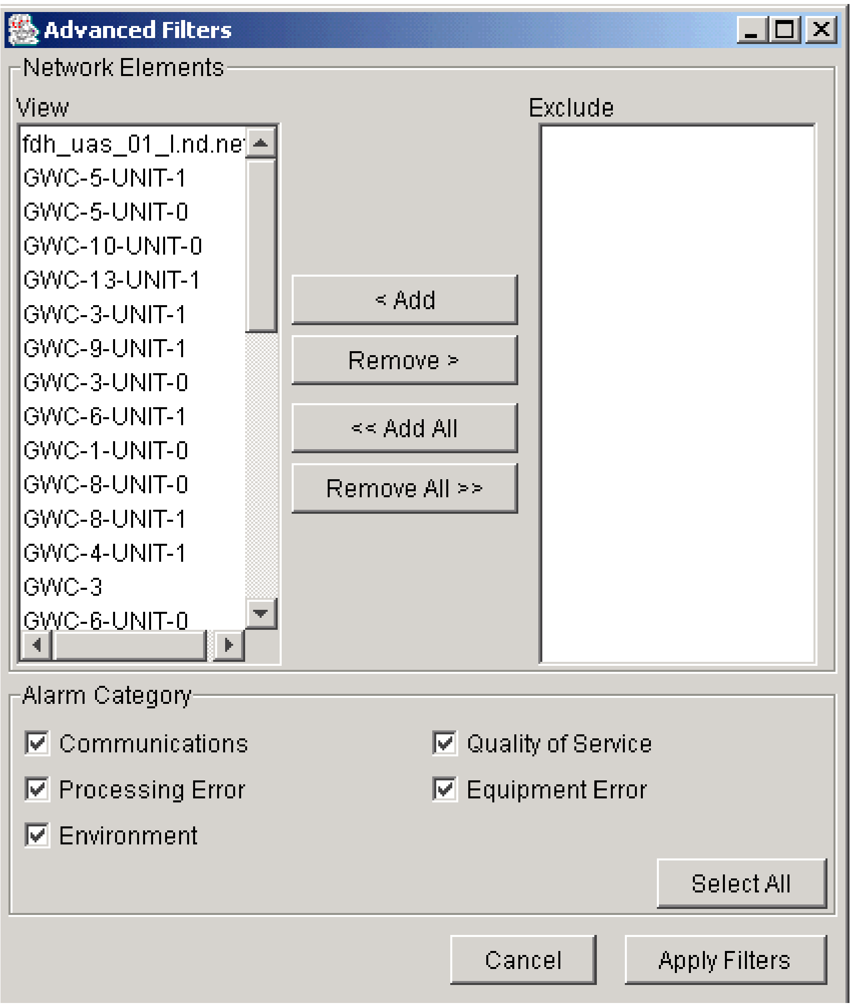
New Alarms: 18 C 33 M 13 m 0 w

64 alarms at: 10:57:47 05-Jul-2004 EDT

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 provisioned

3 To filter the alarm display for specific GWC units by excluding the display of certain alarm types, click the **Advanced Filters** button.



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.

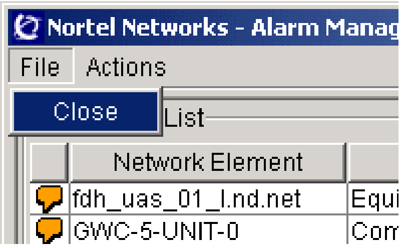
b Click the **Remove** > button to place the selected GWC units in the Exclude (filtered) list. Click the **Remove All** >> button to place all GWC units in the Exclude (filtered) list.

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.

4 When you are finished with the Alarm Manager, click the **File** menu and select **Close**.



5 This procedure is complete.

Perform GWC hardware diagnostics

Purpose of this procedure

Use this procedure to perform hardware diagnostics on the GWC card. Instructions are also provided to save the diagnostic results to an ASCII text file for later analysis.

This procedure also includes the following sections:

- What to do if a diagnostic test fails on page 51
- Unlocking a card that has failed a diagnostic test on page 51

When to use this procedure

Use this procedure as a secondary source of diagnostic information or when a hardware fault persists.

Prerequisites

The GWC card on which you wish to perform diagnostics must first be locked using the CS 2000 SAM21 Manager. Refer to procedure “Lock a GWC card” in the Gateway Controller Security and Administration NTP, NN10213-611.

For additional information about GWC card states and diagnostics, refer to the procedure Interpret GWC card states on page 64 in this NTP.

Action

At the CS 2000 SAM21 Manager client

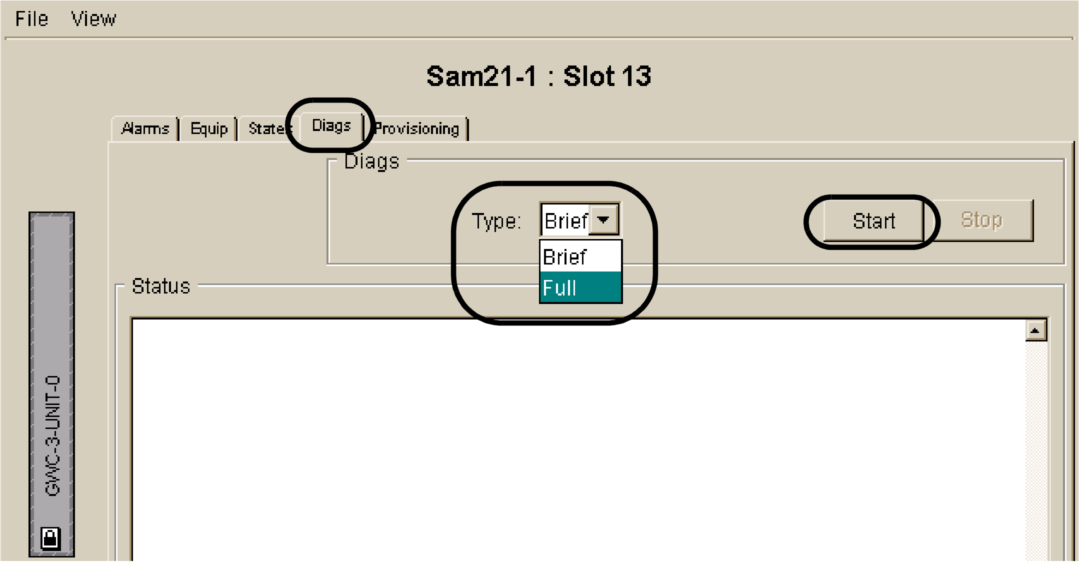
1 In the Card View window, click the **Diags** tab.

   Note: The GWC must be locked to perform diagnostics.

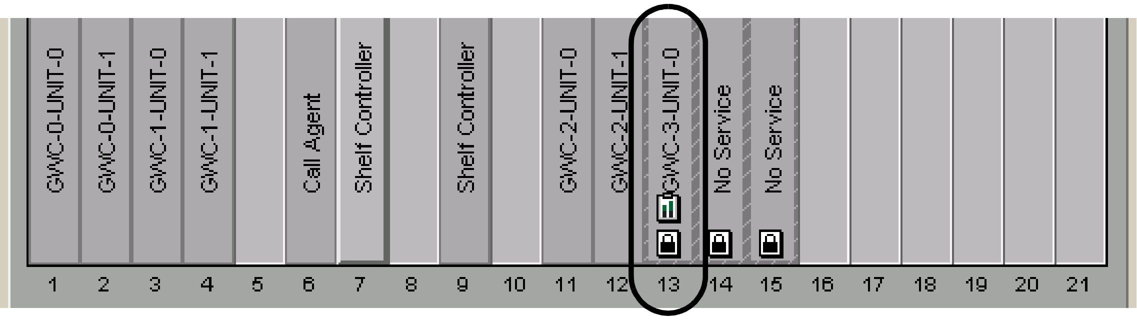
2 Select **Brief** or **Full** diagnostics using the drop-down menu.

3 Click the **Start** button.

   If necessary, you can stop a diagnostics test in progress by clicking the **Stop** button.

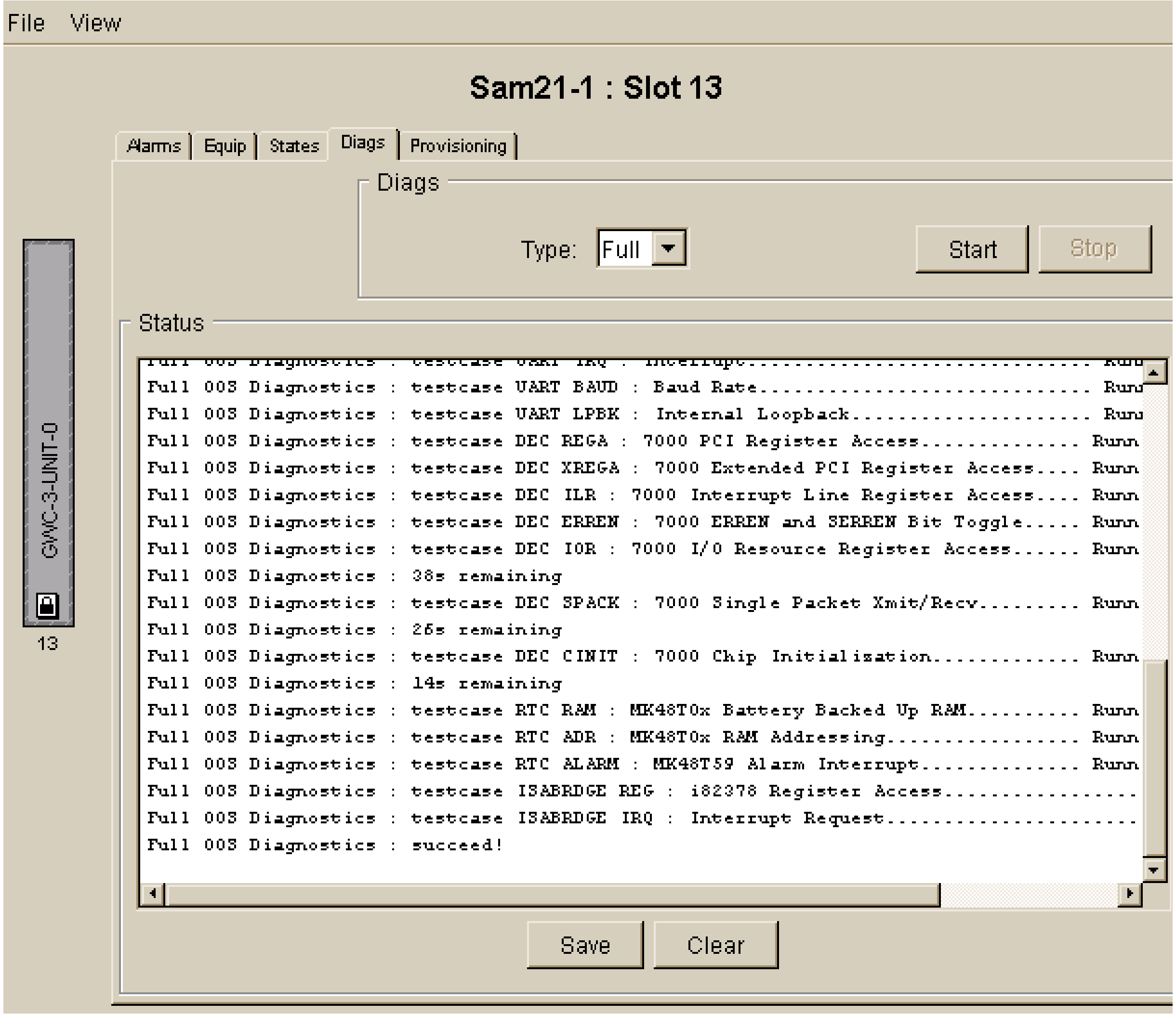


A diagnostics icon appears on the GWC card in the Shelf View.



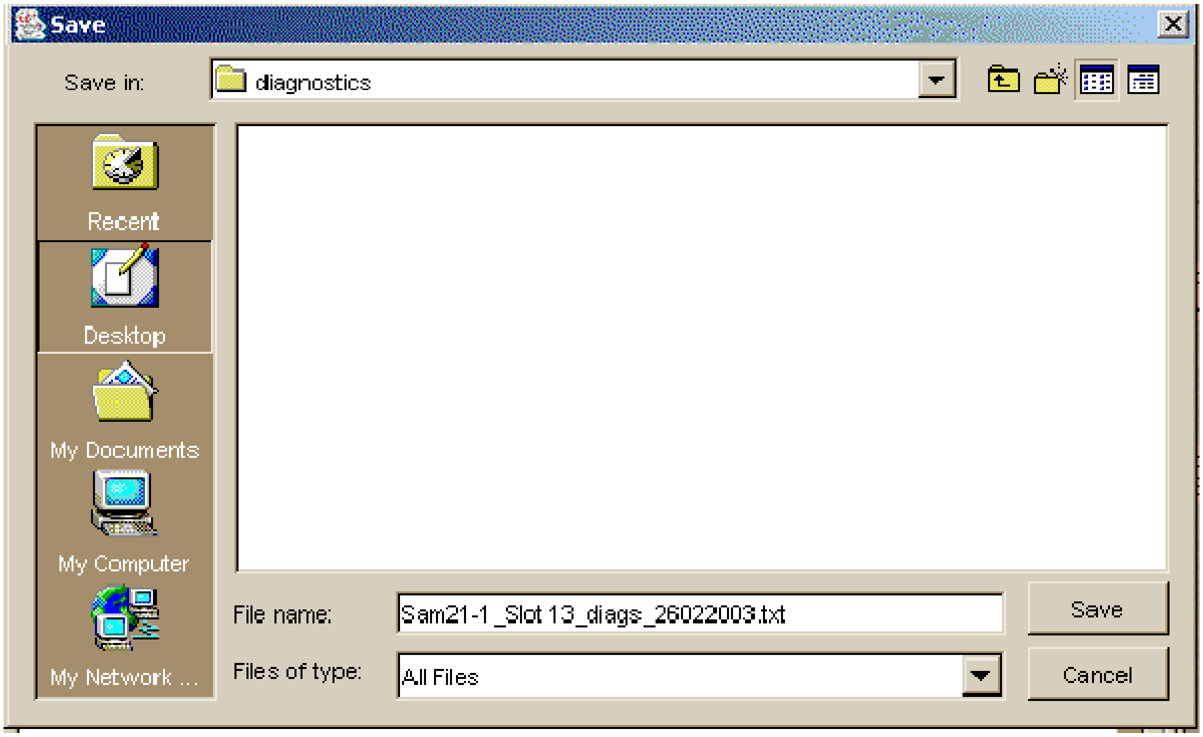
Diagnostic messages appear in the Status area of the Card View.

> ***Note:*** If the diagnostic test indicates a hardware failure of any kind, refer to section What to do if a diagnostic test fails on page 51.



```
Full 003 Diagnostics : testcase UART IRQ : Interrupt............................. Run
Full 003 Diagnostics : testcase UART BAUD : Baud Rate............................ Run
Full 003 Diagnostics : testcase UART LPBK : Internal Loopback.................... Run
Full 003 Diagnostics : testcase DEC REGA : 7000 PCI Register Access............. Runn
Full 003 Diagnostics : testcase DEC XREGA : 7000 Extended PCI Register Access.... Runn
Full 003 Diagnostics : testcase DEC ILR : 7000 Interrupt Line Register Access.... Runn
Full 003 Diagnostics : testcase DEC ERREN : 7000 ERREN and SERREN Bit Toggle..... Runn
Full 003 Diagnostics : testcase DEC IOR : 7000 I/O Resource Register Access...... Runn
Full 003 Diagnostics : 38s remaining
Full 003 Diagnostics : testcase DEC SPACK : 7000 Single Packet Xmit/Recv......... Runn
Full 003 Diagnostics : 26s remaining
Full 003 Diagnostics : testcase DEC CINIT : 7000 Chip Initialization............. Runn
Full 003 Diagnostics : 14s remaining
Full 003 Diagnostics : testcase RTC RAM : MK48T0x Battery Backed Up RAM.......... Runn
Full 003 Diagnostics : testcase RTC ADR : MK48T0x RAM Addressing................. Runn
Full 003 Diagnostics : testcase RTC ALARM : MK48T59 Alarm Interrupt.............. Runn
Full 003 Diagnostics : testcase ISABRDGE REG : i82378 Register Access.................
Full 003 Diagnostics : testcase ISABRDGE IRQ : Interrupt Request......................
Full 003 Diagnostics : succeed!
```

4 To save the diagnostics results to a file on the CS 2000 SAM21 Manager client, click the **Save** button at the bottom of the Card View window. Choose a name and location for the diagnostics file. Append the file with a “.txt” extension for easy identification.



Save in: diagnostics

File name: Sam21-1_Slot 13_diags_26022003.txt

Files of type: All Files

5 This procedure is complete.

What to do if a diagnostic test fails

If any part of the hardware diagnostic test fails, for any reason, do the following:

1. Rerun the diagnostics using the Brief test option.
2. If the Brief test passes, go to step 3 in this list.

   If the Brief test fails, go to step 5 in this list.
3. Rerun the diagnostics using the Full option.
4. If the Full test passes, you may unlock the card and return it to service.

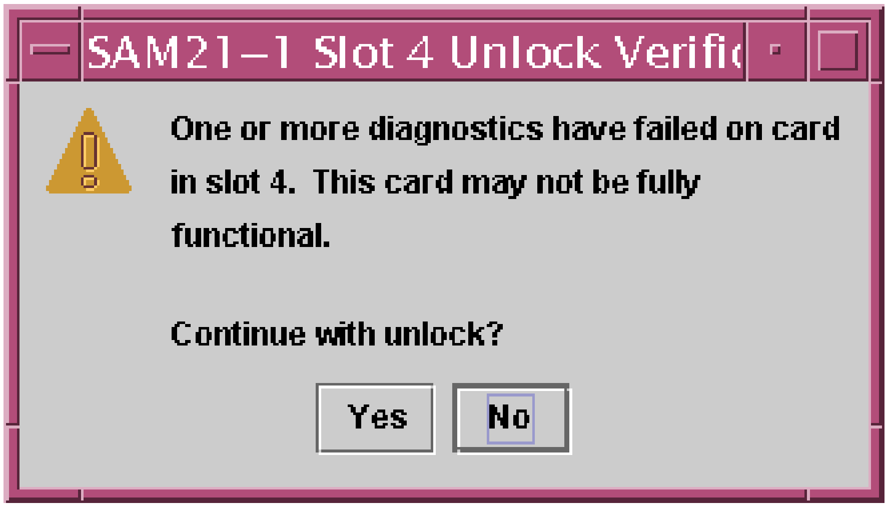
   If the Full test fails, then go to step 5 in this list
5. Replace the card using the procedure Replace and re-provision a GWC card on page 92 in this NTP.

   Return the defective card to Nortel according to the procedures of your service contract.

Unlocking a card that has failed a diagnostic test

The following message appears on the CS 2000 SAM21 Manager if you attempt to unlock a card that has failed a diagnostic test.

If this occurs, rerun the diagnostic test. If the card fails a second time, replace the card and contact Nortel Networks support personnel.



SAM21-1 Slot 4 Unlock Verifi

One or more diagnostics have failed on card in slot 4. This card may not be fully functional.

Continue with unlock?

Access and print GWC diagnostic results

Purpose of this procedure

Use this procedure to retrieve and print diagnostic results from a saved ASCII text file stored on the SAM21 client workstation.

When to use this procedure

Use this procedure after procedure Perform GWC hardware diagnostics on page 47.

Prerequisites

Perform a diagnostics test.

Action

At the CS 2000 SAM21 Manager client

1 Open a terminal session on the client workstation.

2 Type

```
$ cat </path/to/file/filename>
```

and press the enter key.

where

</path/to/file/filename>
is the directory location of the diagnostic file.

3 If a printer is available on the network, print a copy of the diagnostic results by typing

```
$ lp -c  </path/to/file/filename> <printername>
```

and pressing the enter key.

where

</path/to/file/filename>
is the directory location of the log file

<printername>
is the system name of the printer connected to or mounted to the CS 2000 SAM21 Manager (if available).

4 This procedure is complete.

View GWC PM logs

Purpose of this procedure

Use this procedure to access service-related Peripheral Module (PM) logs generated by the GWC and forwarded to the core.

> ***Note:*** For specific information about the logs, and any actions required, refer to the PM log descriptions in this NTP.

When to use this procedure

Use this procedure as a part of scheduled maintenance and as a secondary source of diagnostic information.

Prerequisites

This procedure has no prerequisites.

Action

At the MAPCI interface

1 Type **logutil** and press **Enter**.

2 Type **open pm** and press **Enter** to retrieve the latest PM log.

```
CI:
>logutil
Current MODE setting is: EXTENDED

LOGUTIL:
>open pm
Done.
RTPS03BD   *   PM185 SEP10 09:07:49 0000 TBL  PM TRAP
         GWC 21 Unit 1 : Act
         Trap message received from the XPM. But unable
        to get trap data because either LOGON not allowed
        or unable to talk to the XPM.
>
```

> ***Note:*** For reference information about PM logs related to GWC activities, refer to the appropriate PM log description in this NTP.

3 For more information about commands available in logutil, type **print logutildir** and press **Enter**.

4 This procedure is complete.

View GWC logs in syslog files

Purpose of this procedure

This procedure provides access to GWC logs stored in the syslog files on the CS 2000 Management Tools server. Instructions are also provided for searching specific entries in the syslog files. The logs mentioned in this procedure contain information on the GWC.

For a list of syslog logs that contain information on the GWC, refer to section Syslog files relevant to the GWC on page 56.

Note: This NTP contains descriptions of GWC series logs.

When to use this procedure

Use this procedure as a part of scheduled maintenance and as a secondary source of diagnostic information.

Prerequisites

This procedure has no prerequisites.

Action

At the CS 2000 Management Tools client

1 Access the directory level where the syslog files reside by typing

```
$ cd /var/log
```

and pressing the enter key.

2 List the directory content by typing

```
$ ls
```

and pressing the enter key.

The system displays a list of different log files, such as, customerlog, securitylog, and so on. These files are appended with numbers, for example “customerlog.0”. The files with the lower numbers are the newer files.

Note: For a list of files relevant to the GWC, refer to table Syslog logs containing GWC entries on page 56.

3 Use the following table to determine your next step.

If you want to view	Do
the entire content of a log file	step 4
specific content of a log file	step 6

4 Display the entire content of a log file by typing

```
$ cat <log_filename> |more
```

and pressing the enter key.

where

log_filename
is the name of the log file you want to display. See the first table below for specific examples.

Example
$ cat customerlog.0 lmore

Press the space bar to scroll through the file if it is larger than the screen can display.

5 Continue with step 7.

6 Search and display specific content of a log file by typing

```
$ cat <log_filename> |grep <search_string>
```

and pressing the enter key.

where

search_string
is the text you want to search for, for example KRB (to search for logs associated with the Kerberos application)

Example

```
cat customerlog.0 |grep GWC309
```

or

```
cat securitylog.1 |grep KRB_LOG
```

7 To print the contents of this file, contact your site system administrator for assistance with using UNIX print commands and with locating a printer connected to your network.

8 This procedure is complete.

Syslog files relevant to the GWC

The following table describes the syslog logs in the /var/log directory that contain entries relevant to the GWC.

Syslog logs containing GWC entries

Log type	Description	Examples of log file names
Audit log	Records the actions taken by users on the system, including some of the parameters they used.	auditlog auditlog.0 auditlog.1
Customer log	Records all alarms the system has received.	customerlog customerlog.0 customerlog.1
Debug log	Records debug information for CS 2000 Management Tools network components to help detect an underlying problem.	debuglog debuglog.0
PTM log	Contains a record of all the SNMP traps received by the system.	ptmlog ptmlog.1 ptmlog.2
Security log	Records failed actions taken by users on the system. Securitylog file also includes fault related logs for the Kerberos application.	securitylog securitylog.0

Use the following table to interpret the syslog application logs on the redirecting media gateway controller (RMGC).

GWC syslog application logs

Application log description	Cause or condition	Action
RMGC: Successful Count: x Failed Count: y	The RMGC application produces a syslog performance report once an hour. (See the debug log in /var/log.) It contains the counts of the number of RSIPs processed successfully (x) and the number failed (y). The counts are cumulative, so that to calculate the number of successful/failed RSIPs, it is not necessary to parse each and every log but just to subtract the counts from the previous log to derive the counts between the current log and the previous.	No action is required.

Access the debug log to view GWC auto-image events

Purpose of this procedure

Use this procedure to display the contents of the CS 2000 GWC Manager debug log and search for auto-image events in the log. The debug log resides on the CS 2000 Management Tools server.

> ***Note:*** To view a summary of auto-image logs, refer to View and troubleshoot GWC auto-image error logs on page 61.

To find out how auto-imaging works, refer to the description of GWC software imaging in Upgrading the Gateway Controller, NN10196-461.

When to use this procedure

Use this procedure if you are troubleshooting a problem with auto-imaging and you want to search for a specific auto-image entry in the debug log.

Prerequisites

You must have a user account on the CS 2000 Management Tools server. The error log is located on the CS 2000 Management Tools server in the following directory: /opt/nortel/NTsesm/admin/logs.

Action

At the CS 2000 Management Tools client

1 Log onto the server as the root user.

2 Change to the /opt/nortel/NTsesm/admin/logs directory by typing

```
>cd /opt/nortel/NTsesm/admin/logs
```

and pressing the enter key.

3 Open the debug log by typing

```
>less <debug_log_filename>
```

and pressing the enter key.

where

debug_log_filename
is the name of the debug log file. This file name can be configured. The default file name is ptmdebuglog<n>.mi2, where <n> is a number that increments as the log increases in size.

Example

```
less ptmdebuglog1.mi2
```

Example Response

```
03.01.28 13:30:28.697 VRB (ubsnmp) [PE-8]
UBSnmpSimpleTrap Notifying 1 listeners

03.01.28 13:30:28.697 VRB (MI2Server) [PE-8]
TrapLogger::trapNotification  #queue: 1
03.01.28 13:30:28.699 VRB (EM) [Thread-78]
GWCUtils: Attempting to convert gwcid
```

4 Search for auto-image events while in the debug log by typing

`/<text_to_search>`

and pressing the enter key.

where

text_to_search
can be any of the following search strings:

- /auto
- /Auto
- /AUTO

Example

```
/Auto
```

Note: The search string you enter is case sensitive. Each search yields different results. The text that you have searched is highlighted in the display.

Example Response

```
03.01.29 10:31:34.235 VRB (gwcem@1)
[RequestProcessor[1]] SesmSecureProxy::invoke
isAutoImagingEnabled

03.01.29 10:31:34.236 VRB (gwcem@1)
[RequestProcessor[1]]
AuthorizingHandler.authorize:
isAutoImagingEnabled ()

03.01.29 10:31:34.258 NOA (gwcem@1)
[RequestProcessor[1]] AUDIT:
isAutoImagingEnabled ()
```

5 Repeat step 4. You can search for other entries of the same text in the debug log, or you can search for different text as indicated in step 4.

6 You have completed the procedure.

View and troubleshoot GWC auto-image error logs

Purpose of this procedure

Use this procedure to display the contents of the auto-image error log. This log provides a summary of any errors that prevent auto-imaging from taking place. The error log resides on the CS 2000 Management Tools server.

> ***Note:*** The log recycles after recording 2000 lines of text.

The section Interpreting auto-image logs on page 62 contains some examples of auto-image logs and suggested actions.

To find out how auto-imaging works, refer to the description of GWC software imaging in Upgrading the Gateway Controller, NN10196-461.

When to use this procedure

Use this procedure when you want to determine if auto-imaging is working properly.

Prerequisites

You must have a user account on the CS 2000 Management Tools server. The error log is located on the CS 2000 Management Tools server in the following directory: /opt/nortel/NTsesm/admin/logs.

Action

At the CS 2000 Management Tools client

1 Log onto the server as the root user.

2 Change to the /opt/nortel/NTsesm/admin/logs directory by typing

```
>cd /opt/nortel/NTsesm/admin/logs
```

and pressing the enter key.

3 Display the contents of the auto-image error log by typing

>more AutoImagingErrorLog

and pressing the enter key.

Example Response

```
Auto Imaging Executed Tue Jan 28 02:00:01 EST
2003

An error occurred while auto imaging: Auto
imaging has not been enabled.

Auto Imaging Executed Wed Jan 29 02:00:01 EST
2003
An error occurred while auto imaging: Auto
imaging has not been enabled.
```

4 This procedure is complete.

Interpreting auto-image logs

Use the following table to interpret an example of the log. Auto-image logs are recorded in the format:

```
Auto Imaging Executed
<day><month><dd><hh:mm:ss><yyyy>
"log description"
```

where

day/month/dd/hh:mm:ss/yyyy
is the date and time stamp for the log

"log description"
is a description of the conditions or reasons for generating the log.

The following table provides examples of auto-image error logs.

Examples of auto-image error logs

Auto-image log description	Cause or condition	Action
An error occurred while auto imaging: Auto imaging has not been enabled.	An image of the software loads on your GWC devices was not taken automatically at the scheduled time because auto-imaging was not enabled.	Enable auto-imaging using the CS 2000 GWC Manager if you want to automatically save an up-to-date image of GWC software loads once daily on the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM). Refer to “Enable/disable GWC software auto-imaging” in the Gateway Controller Configuration management NTP, NN10205-511.
An error occurred while trying to connect to the GWC EM.	The CS 2000 Management Tools server is down.	Restart the CS 2000 Management Tools server.

Interpret GWC card states

Purpose of this procedure

Use this procedure to determine the state of a GWC card using the CS 2000 SAM21 Manager.

Table GWC card states and possible actions on page 66 suggests actions in response to different card states.

When to use this procedure

Use this procedure when you are encountering an unknown card state.

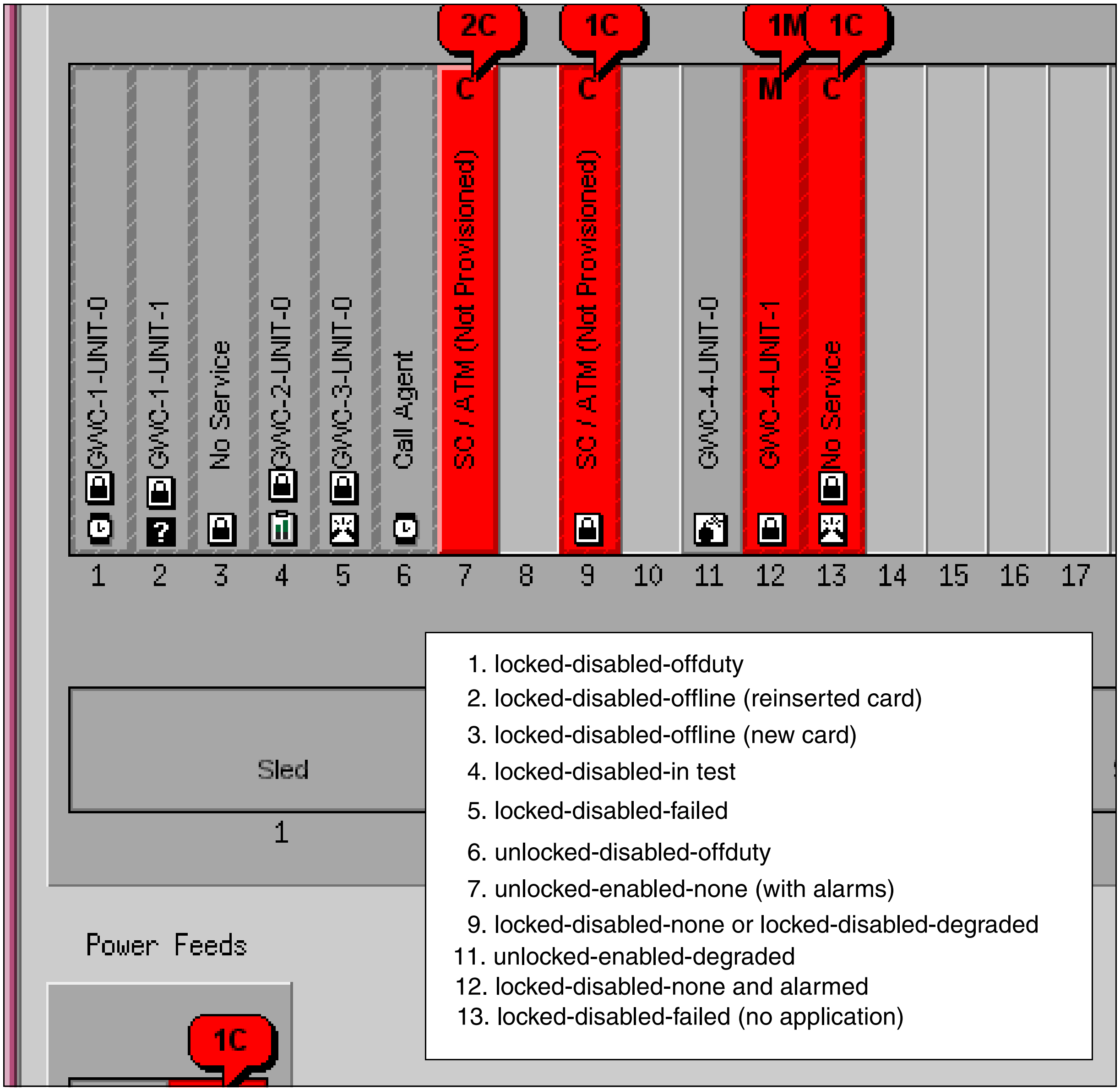
Prerequisites

There are no prerequisites for this procedure.

Action

At the CS 2000 SAM21 Manager client

1 Review the following figure and determine the card icons that apply.



1. locked-disabled-offduty
2. locked-disabled-offline (reinserted card)
3. locked-disabled-offline (new card)
4. locked-disabled-in test
5. locked-disabled-failed
6. unlocked-disabled-offduty
7. unlocked-enabled-none (with alarms)
9. locked-disabled-none or locked-disabled-degraded
11. unlocked-enabled-degraded
12. locked-disabled-none and alarmed
13. locked-disabled-failed (no application)

Note: These states also apply to Shelf Controllers.

2 To view the card state tab, right-click the card icon and select Card View from the card context menu. In the Card View window that opens, select the States tab.

3 Determine the next action.

> ***Note:*** 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.
>
> A status of “locked” on the CS 2000 GWC Manager indicates that the software application on the card is still running, but it is no longer performing its primary call processing function.

GWC card states and possible actions (Sheet 1 of 4)

State	Possible action
locked-disabled-offduty 🕒 🔒	Wait for the firmware flash to complete. Verify that the card changes to the locked-disabled-none state. For GWC cards, this state is entered during the SN04 to SN06 upgrade while the Shelf Controller configures the GWC card for the dead shelf recovery (DSR) feature. If the GWC card transitions to locked-disabled-degraded, follow the suggestions for that state.
unlocked-disabled-offduty 🕒	For Call Agent cards, this state also represents the restart and reload of the call processing application during a routine exercise test (RExTst). When the Shelf Controller performs it’s boot audit, any GWC card that is not running or booting is set to this state until the Shelf Controller recovers the card.

GWC card states and possible actions (Sheet 2 of 4)

State	Possible action
locked-disabled-offline (new card) ?	Right-click the card icon and select Assign Service from the card context menu. Select the correct service from the Assign Service window. If the question mark icon does not disappear, open the Card View and view the States tab. If the history text area indicates that service assignment failed because the service type is incompatible with the hardware, either replace the card with the correct hardware type, or unassign service from the shelf view and then assign the correct service type.
locked-disabled-offline (reinsertion) ? 🔒	Wait for Shelf Controller to recognize the card and reinstate the provisioning information. The question mark icon disappears and the card transitions to a new state. Refer to the suggestions for the new state. If the question mark icon does not disappear, open the Card View window and view the States tab. If the history text area indicates that service assignment failed because the service type is incompatible with the hardware, either replace the card with the correct hardware type, or unassign service from the shelf view and then re-assign with the correct service type. If the history text area indicates that the service assignment failed because the IP address is already reserved by another unit, contact network engineering to determine if another unit is misconfigured, or if this unit should be reconfigured.

GWC card states and possible actions (Sheet 3 of 4)

State	Possible action
locked-disabled-none or locked-disabled-degraded 🔒	Unlock the card by right-clicking on the card icon and select Unlock from the card context menu. Rerun diagnostics if the CS 2000 SAM21 Manager client generates a “Degraded state Unlock confirmation window”. If diagnostics fail a second time, replace the card and contact Nortel Networks support personnel. ***Note:*** The active Shelf Controller generates 2 critical alarms when the inactive Shelf Controller is locked. A locked-disabled-degraded state for non system slot (NSS) cards is also alarmed.
locked-disabled-failed 🔒	This card is inaccessible. Verify the following items: • Shelf Controllers are in service • If the Shelf Controllers are in service, replace the card. If the replacement card does not enter unlocked-enabled-none, contact Nortel Networks support personnel.
locked-disabled-in test 🔒	Wait for diagnostics to complete. Verify that the card changes to the locked-disabled-none state. Optionally monitor diagnostics progress from the Card View window.

GWC card states and possible actions (Sheet 4 of 4)

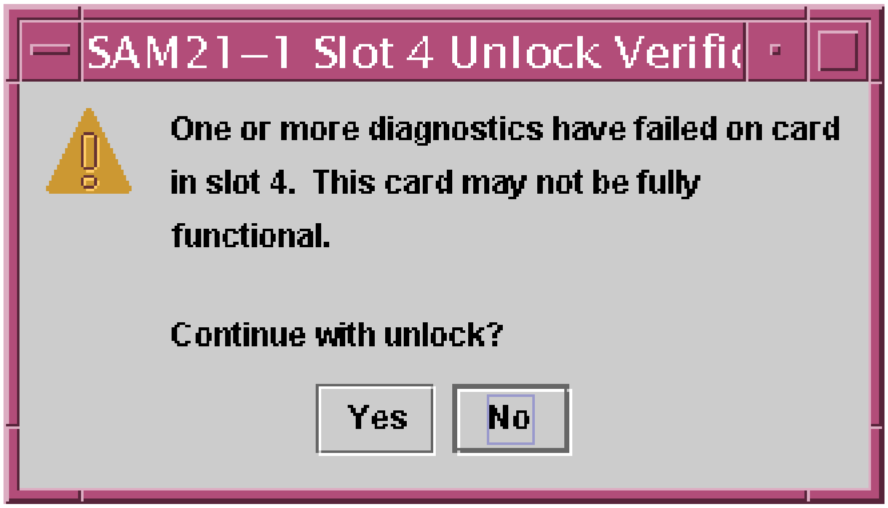
State	Possible action
unlocked-enabled-degraded 🔓	This card failed one or more diagnostics and was Unlocked. See Unlocking a card that has failed a diagnostic test at the end of this procedure. This card may not be providing service or may be unreliable. Lock and run diagnostics on this card. If the card fails diagnostics, replace this card and contact Nortel Networks support personnel.
locked-disabled-none and alarmed 🔒	This card has taken more than three minutes to complete a lock or unlock request. The alarm clears when the card completes the request or is removed from the shelf.
locked-disabled-failed (no application) ⚠ 🔒	The Shelf Controller detects a card in the slot, but cannot determine the MAC address for the card. Reinsert the card.

4 This procedure is complete.

Unlocking a card that has failed a diagnostic test

The following message appears on the CS 2000 SAM21 Manager if you attempt to unlock a card that has failed a diagnostic test.

If this occurs, rerun the diagnostic test. If the card fails a second time, replace the card and contact Nortel Networks support personnel.

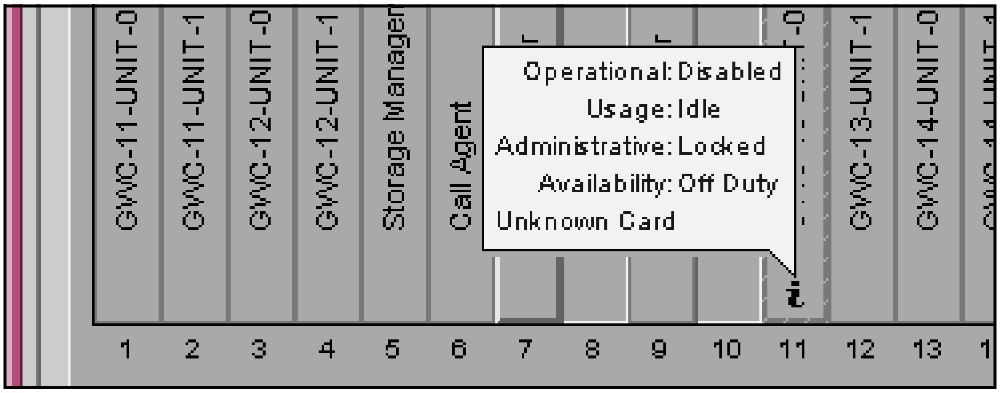


One or more diagnostics have failed on card in slot 4. This card may not be fully functional.

Continue with unlock?

Information card icon

An additional shelf view card icon indicates that the CS 2000 SAM21 Manager client cannot display all the card icons. Click this information icon to view the card state information in a balloon. This icon normally indicates that the card type is not supported for the current release of the CS 2000 SAM21 Manager software.



Operational: Disabled
Usage: Idle
Administrative: Locked
Availability: Off Duty
Unknown Card

Re-provision a GWC card automatically

Purpose of this procedure

Use this procedure to automatically reprovision a known good GWC card with a new media access control (MAC) address. All other card information including IP addresses, port addresses, gateway addresses, and load paths remain unchanged.

When to use this procedure

Use this procedure when you need to change the MAC address of a GWC card due to possible address conflicts or to ensure information in the CS 2000 SAM21 Manager database is correct.

This procedure does not provide instructions to make services provisioning changes to a GWC card, such as changing the service profile type of a GWC node. If changes to the GWC node provisioning are necessary, use the CS 2000 GWC Manager to busy the cards and reprovision node information. Refer to the Gateway Controller Configuration Management NTP, NN10205-511, for details.

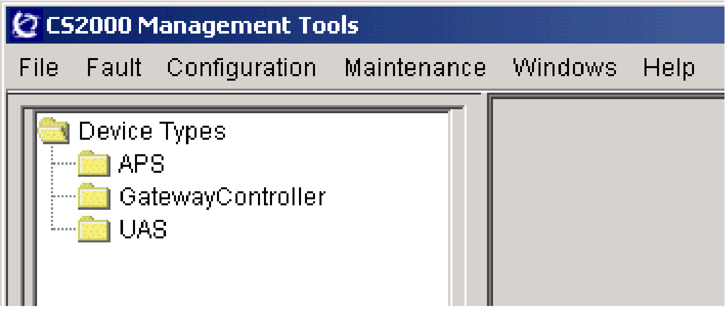
Prerequisites

You must first busy the GWC node using the CS 2000 GWC Manager before automatically reprovisioning any card in the node. Refer to procedure “Busy a GWC Node” in the Gateway Controller Configuration Management NTP, NN10205-511.

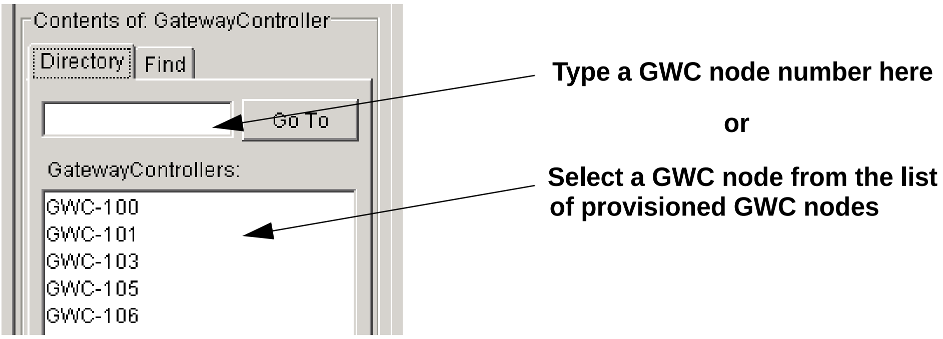
Action

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: Gateway Controller frame, select the GWC node that you wish to automatically reprovision, or type the name of the GWC node in the text field to the left of the **Go To** button.



Type a GWC node number here

or

Select a GWC node from the list of provisioned GWC nodes

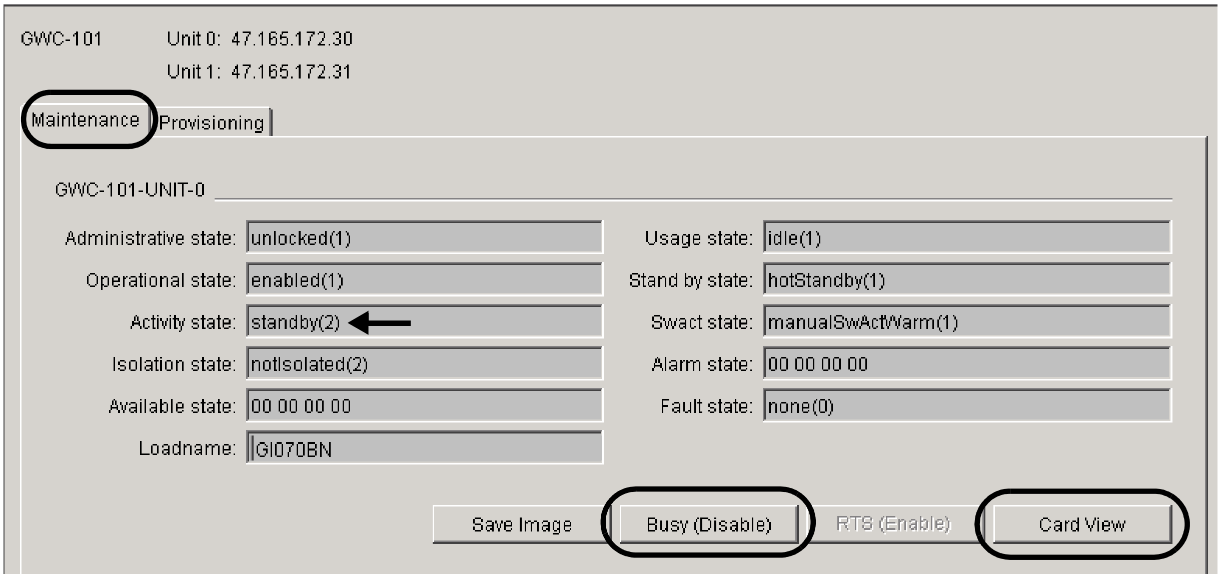
3 If the GWC card you need to automatically reprovision is currently providing service, you need to switch call processing between the two GWC units in the node in order to avoid affecting service.

Refer to procedure “Invoking a manual protection switch (warm swact)” in the Gateway Controller Security and Administration NTP, NN10213-611.

4 In the Maintenance panel, busy the GWC card you want to automatically reprovision by clicking the **Busy (Disable)** button.

This would typically be the standby card in the node. Confirm this action at the prompt

5 Click the **Card View** button for the card you busied in step 4. This opens the CS 2000 SAM21 Manager.



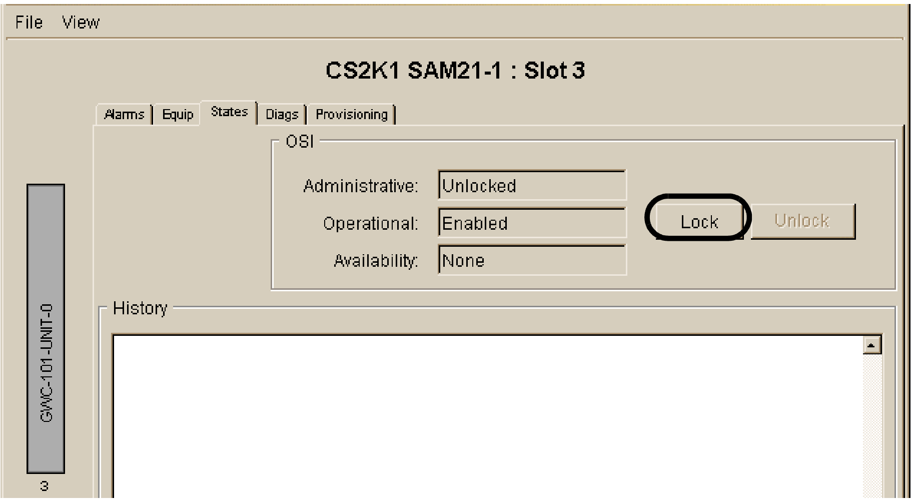
GWC-101 Unit 0: 47.165.172.30
Unit 1: 47.165.172.31

GWC-101-UNIT-0

Administrative state: unlocked(1)
Operational state: enabled(1)
Activity state: standby(2)
Isolation state: notIsolated(2)
Available state: 00 00 00 00
Loadname: GI070BN
Usage state: idle(1)
Stand by state: hotStandby(1)
Swact state: manualSwActWarm(1)
Alarm state: 00 00 00 00
Fault state: none(0)

At the CS 2000 SAM21 Manager client

6 Click the **Lock** button in the card view to lock the card.



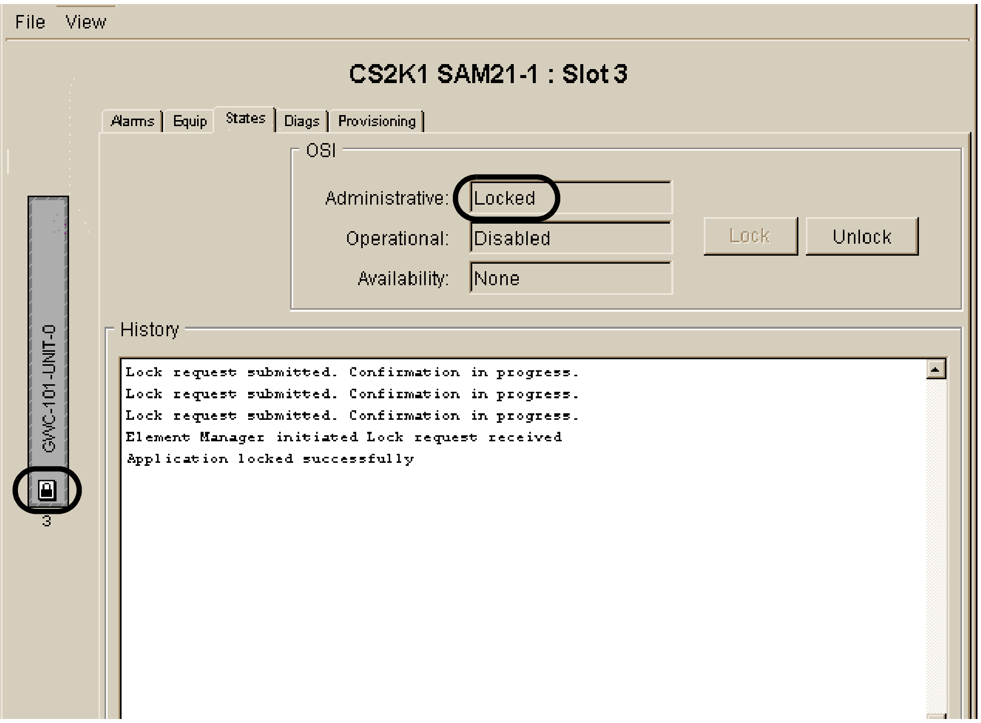
CS2K1 SAM21-1 : Slot 3

OSI

Administrative: Unlocked
Operational: Enabled
Availability: None

History

7 Observe the History display to confirm that the card has been locked. Look for the text “Application locked successfully”. Also, notice the lock icon on the card graphic at the left of the screen and the Administrative state “Locked”.



Administrative: Locked

Operational: Disabled

Availability: None

```
Lock request submitted. Confirmation in progress.
Lock request submitted. Confirmation in progress.
Lock request submitted. Confirmation in progress.
Element Manager initiated Lock request received
Application locked successfully
```

At the SAM21 shelf

8 Remove the Ethernet and serial cables (if present) from the GWC faceplate.

9 Open the ejector levers.

10 Wait for the green LED on the faceplate to extinguish and the blue LED to appear at the bottom of the faceplate.

11 Hold the GWC card by the latches and remove the card from the shelf.

CAUTION

A service outage can occur if care is not taken while removing the GWC circuit packs.

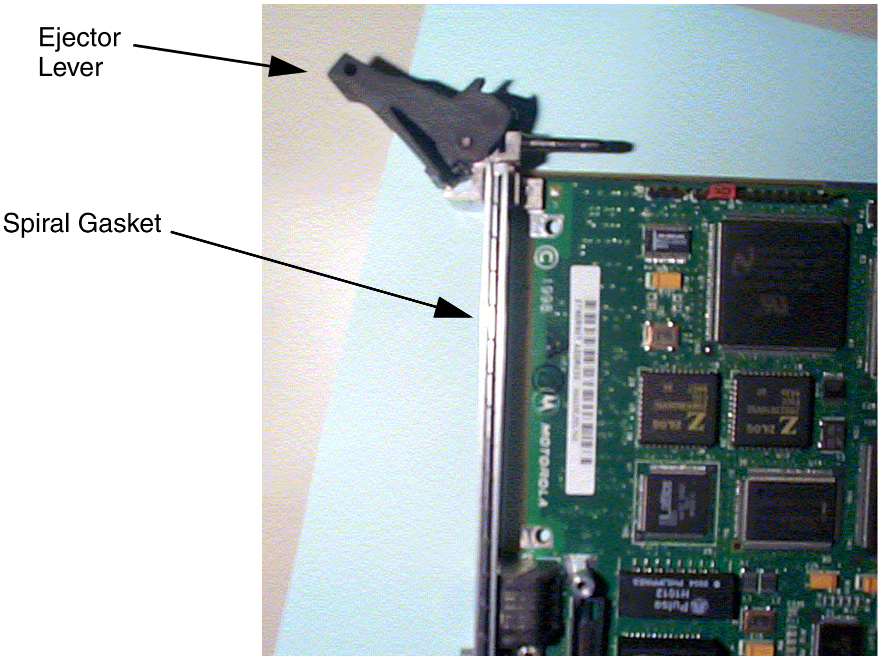
The spiral gasket, located on the faceplate of the circuit pack, can become caught on an adjacent card and ripped off of the faceplate. If the spiral gasket ends up making contact with the backplane inside the chassis, an electrical short circuit can result in a service outage.

WARNING

Static electricity damage

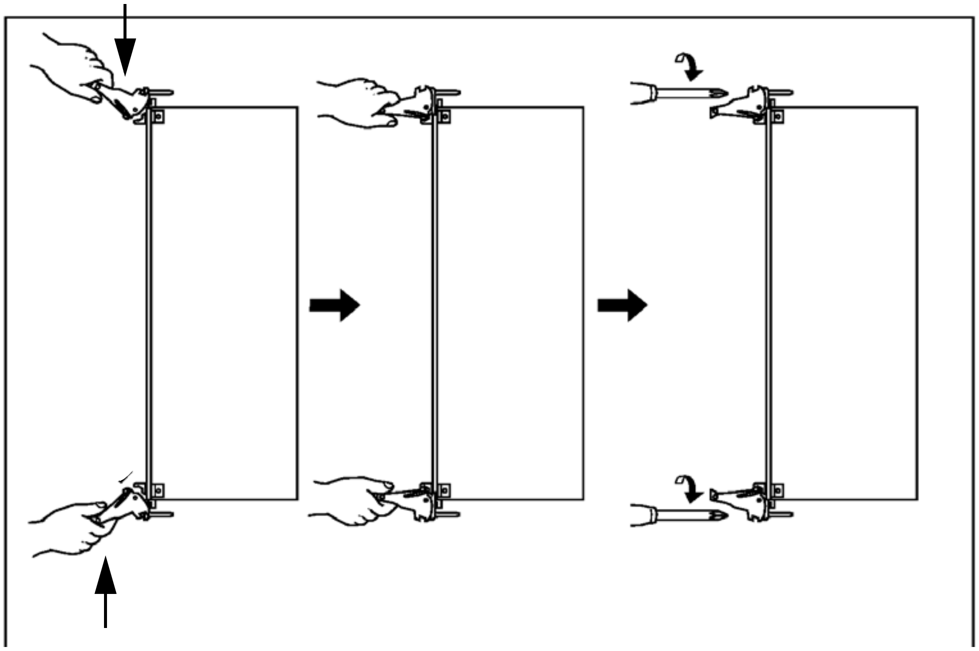
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the SAM21 Shelf Cabinet when handling a GWC card. This protects the card against damage caused by static electricity.

12 Examine the circuit pack before (re)inserting it into the SAM21 chassis to ensure that the spiral gasket is seated and not loose.



13 Hold the same GWC card by the latches and reinsert the card into the shelf.

> ***Note:*** Do not push on the faceplate to seat the card.

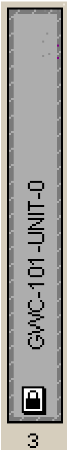


14 Secure the card by tightening the captive screws at the top and bottom of the panel.

15 Replace the cables on the GWC card faceplate.

At the CS 2000 SAM21 Manager client

16 In the shelf view or card view window, wait until the GWC card you are reprovisioning appears as follows:

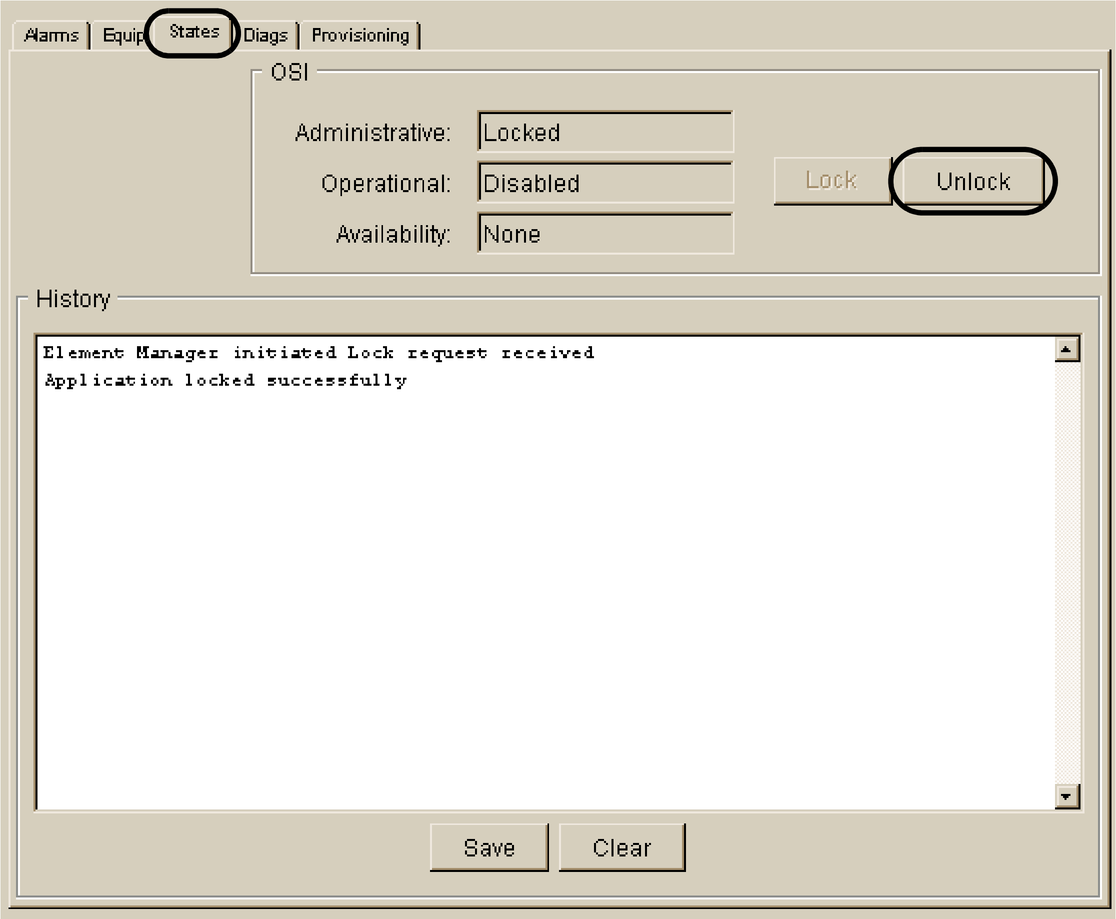


The card should appear with the correct text label (GWC-<x>-UNIT-<y>) and in a locked state (note the lock icon at the bottom).

After the card is inserted and connected, it passes through the following states, indicated in the shelf view or the card view:

- The card first appears with the text label "No Service" and locked.
- A short time afterwards, the CS 2000 GWC Manager determines if the newly inserted card can support the current provisioning. If a GWC card was inserted, the display then changes from “No Service” to "GWC-<x>-UNIT-<y>" with the "?" icon just above the lock icon.
- When the card is configured for GWC service, the “?” icon is removed from the display.
- At this point, the card is ready to be unlocked (reprovisioned).

17 Reprovisioning with the new MAC address does not take effect until the card is unlocked and rebooted. Click the **States** tab to display the status of the GWC card.



Administrative: Locked
Operational: Disabled
Availability: None

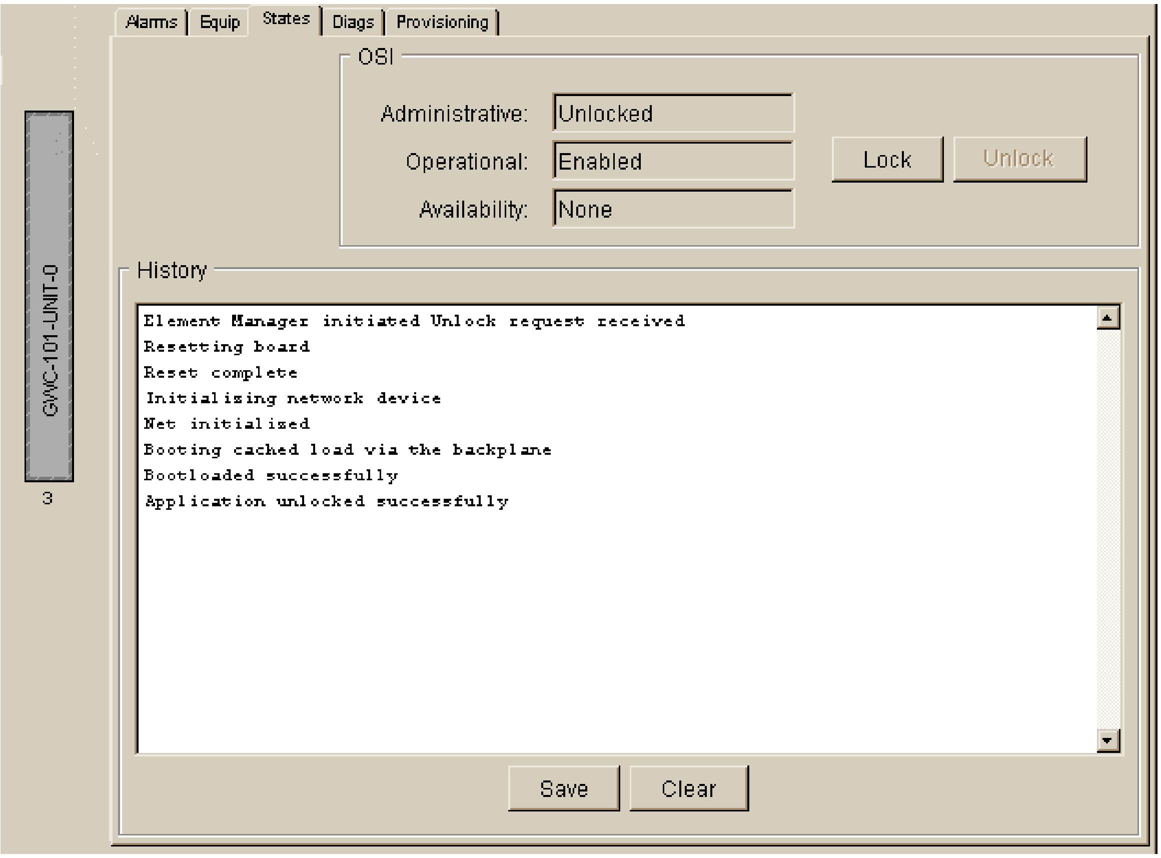
```
Element Manager initiated Lock request received
Application locked successfully
```

18 Click the **Unlock** button to unLock the GWC card. This causes the card to reboot and to be automatically reprovisioned.

19 Observe the History display until the screen message "Bootloaded successfully" appears.

Note: If the card status does not display "Application unlocked successfully", then click the **Lock** button in the card view and wait for the "Application locked successfully" message. Then, click the **Unlock** button again.

If you are still unable to successfully unlock a GWC card, contact your next level of support.



Administrative: Unlocked
Operational: Enabled
Availability: None

```
Element Manager initiated Unlock request received
Resetting board
Reset complete
Initialising network device
Net initialised
Booting cached load via the backplane
Bootloaded successfully
Application unlocked successfully
```

20 Return to step 2 and repeat this procedure for each GWC you need to automatically reprovision.

21 This procedure is complete.

Restart or reboot a GWC card

Purpose of this procedure

Use this procedure to stop all software processes on the GWC card, performs a hardware reset, and reloads the GWC card software from the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM).

To restart software applications only, refer to procedure Restart GWC card services on page 84 in this NTP.

When to use this procedure

Use this procedure when you need to reboot a GWC card and force a GWC to download and execute a software load from the The CS 2000 Core Manager (SDM) or CBM.

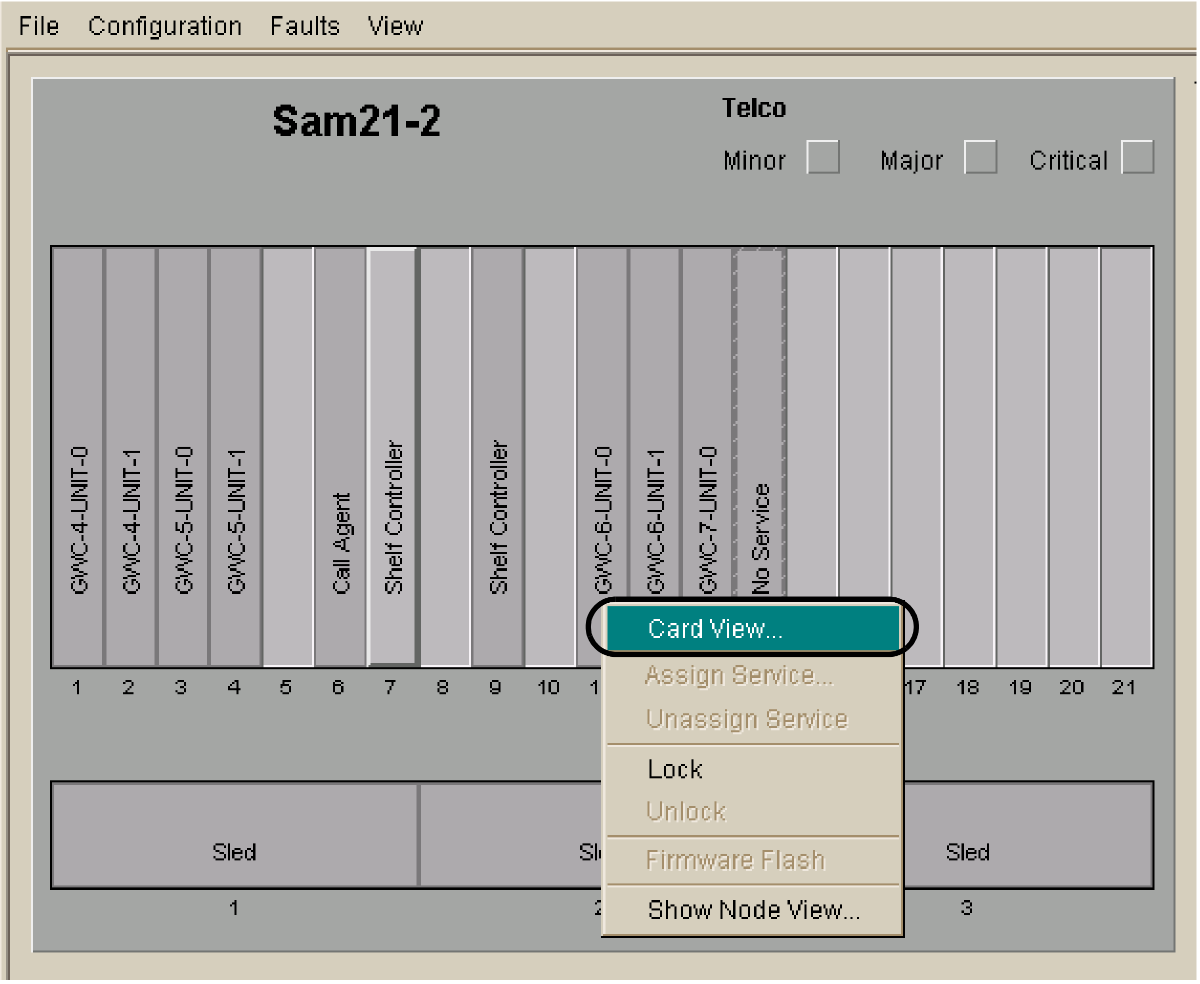
Prerequisites

To reduce the risk of service interruption, you can first busy the GWC applications on specific GWC nodes using the CS 2000 GWC Manager. Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for these procedures.

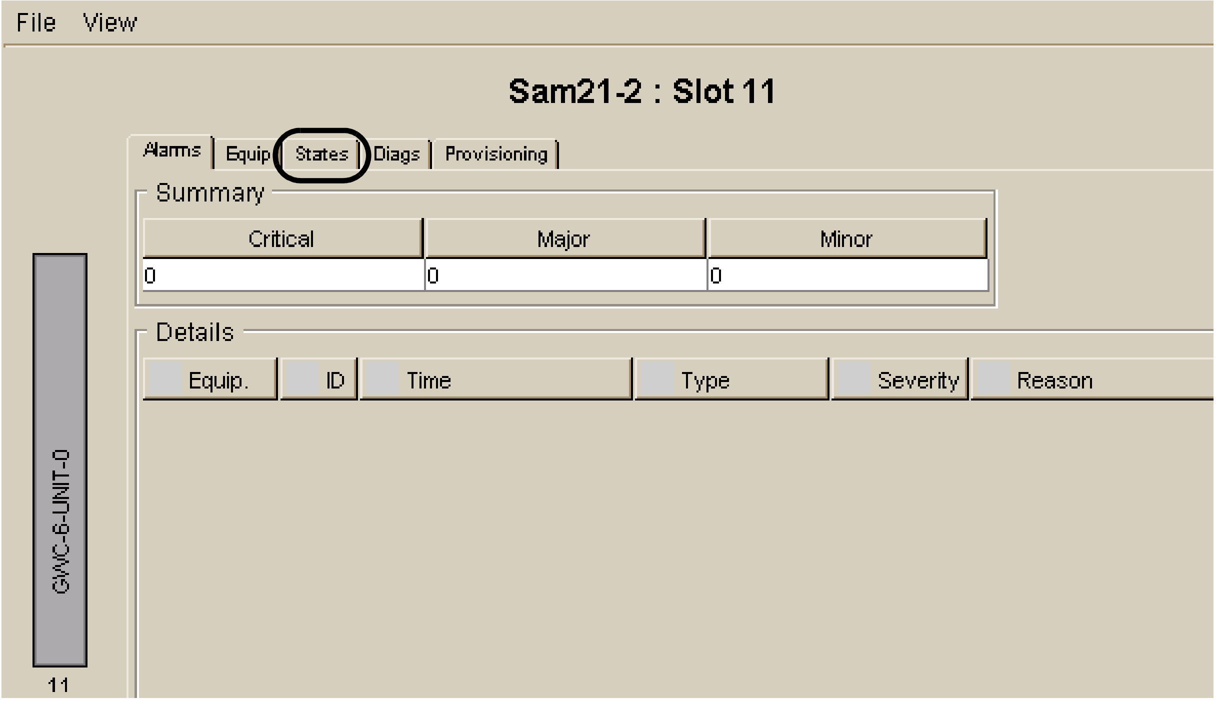
Action

At the CS 2000 SAM21 Manager client

1 From the Shelf View, right-click the GWC card you want to reboot and select **Card View** from the context menu.



2 At the Card View, select the **States** tab.



Sam21-2 : Slot 11

Summary

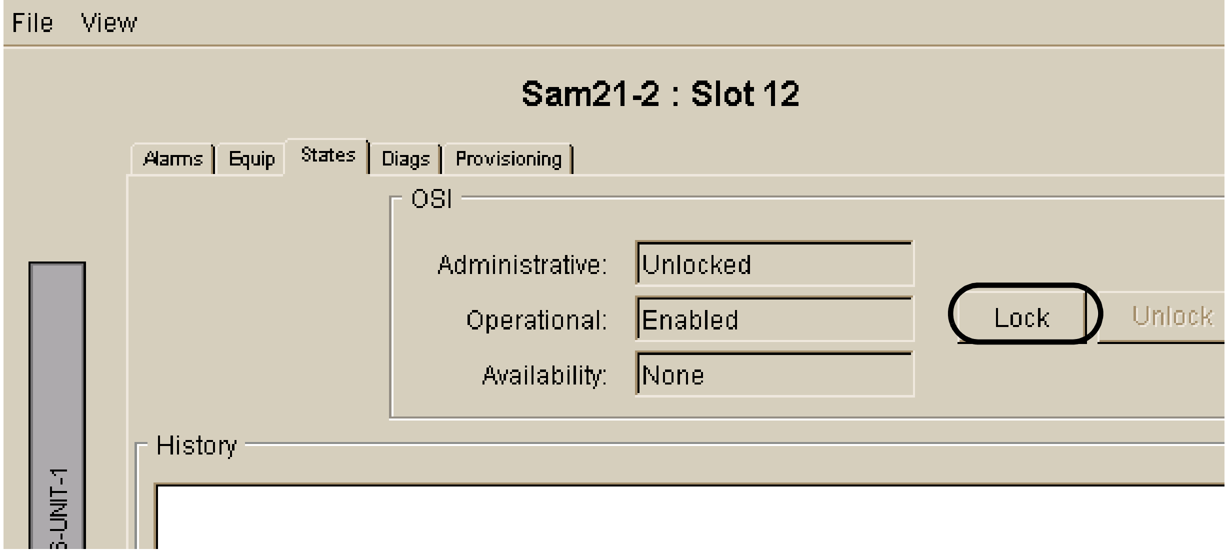
Critical	Major	Minor
0	0	0

Details

Equip.	ID	Time	Type	Severity	Reason

3 Click the **Lock** button to lock the card.

Note: The card must be busy (disabled) before you can lock it. Refer to the procedure “Disable (Busy) GWC card services” in the Gateway Controller Security and Administration NTP, NN10213-611.



Sam21-2 : Slot 12

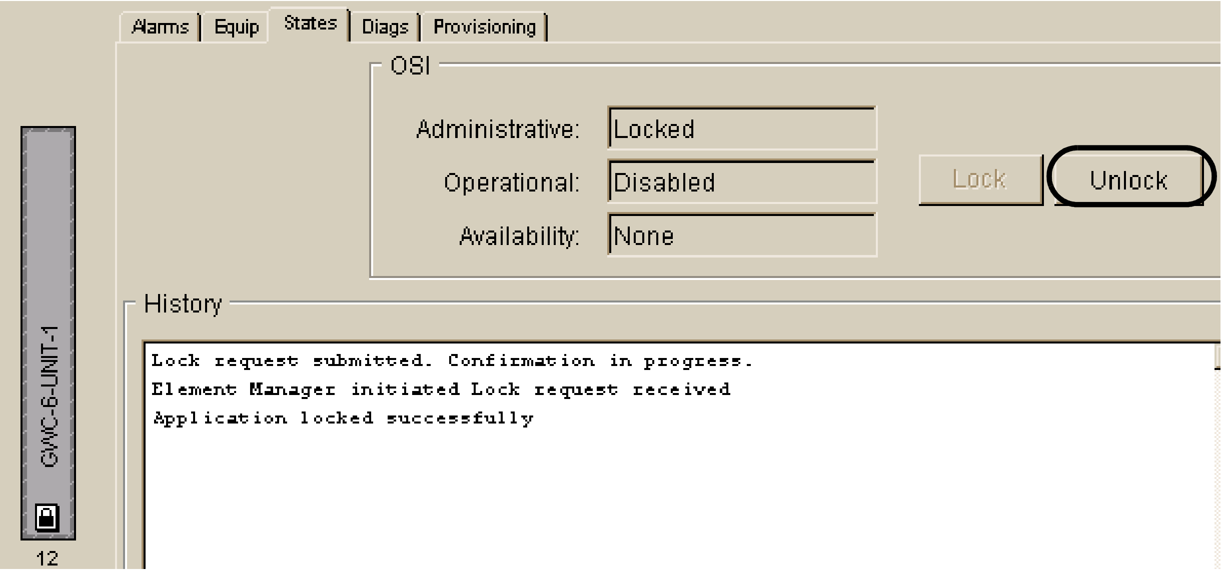
OSI

Administrative: Unlocked

Operational: Enabled

Availability: None

4 Wait until the Administrative state of the card is Locked and the History window indicates "Application locked successfully". Then, click the **Unlock** button.



OSI

Administrative: Locked

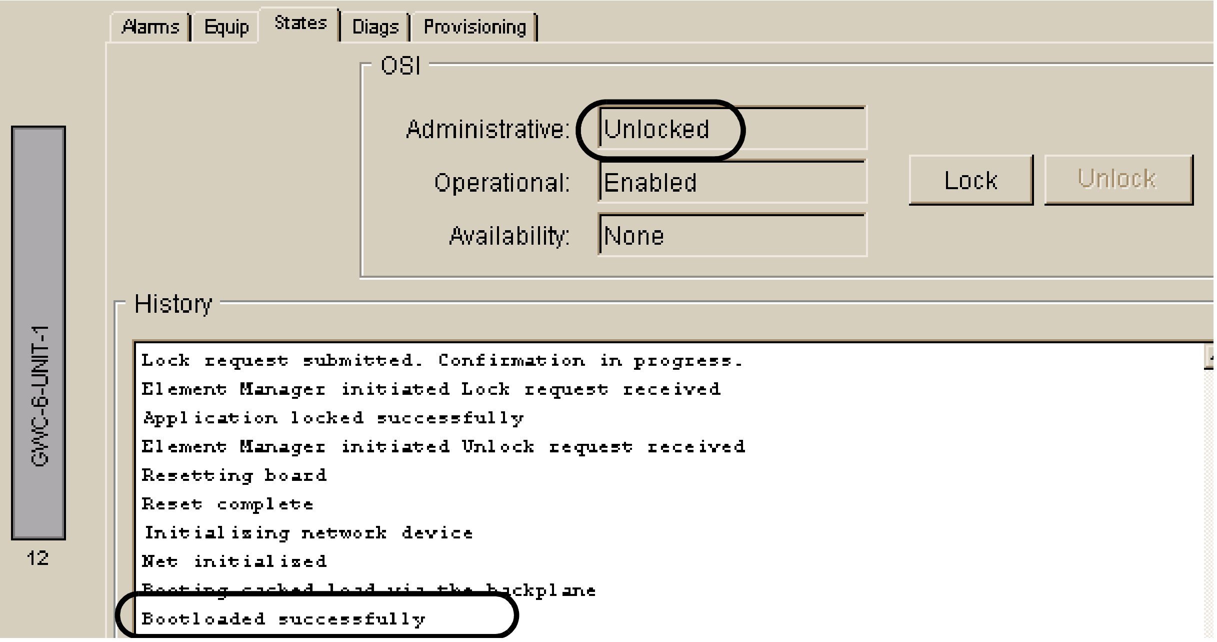
Operational: Disabled

Availability: None

History

```
Lock request submitted. Confirmation in progress.
Element Manager initiated Lock request received
Application locked successfully
```

5 Monitor the reboot process. Wait until the Administrative state of the card is "Unlocked" and the History window indicates "Bootloaded successfully".



OSI

Administrative: Unlocked

Operational: Enabled

Availability: None

History

```
Lock request submitted. Confirmation in progress.
Element Manager initiated Lock request received
Application locked successfully
Element Manager initiated Unlock request received
Resetting board
Reset complete
Initializing network device
Net initialized
Booting cached load via the backplane
Bootloaded successfully
```

6 This procedure is complete.

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, refer to procedure Restart or reboot a GWC card on page 80.

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.

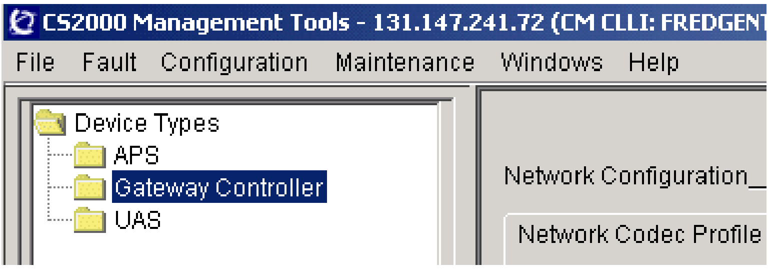
Prerequisites

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. Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for procedures to perform a SwAct.

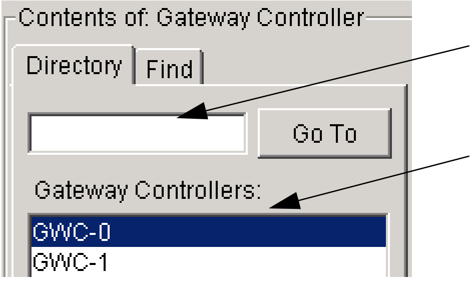
Action

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.



Type a GWC node number here,

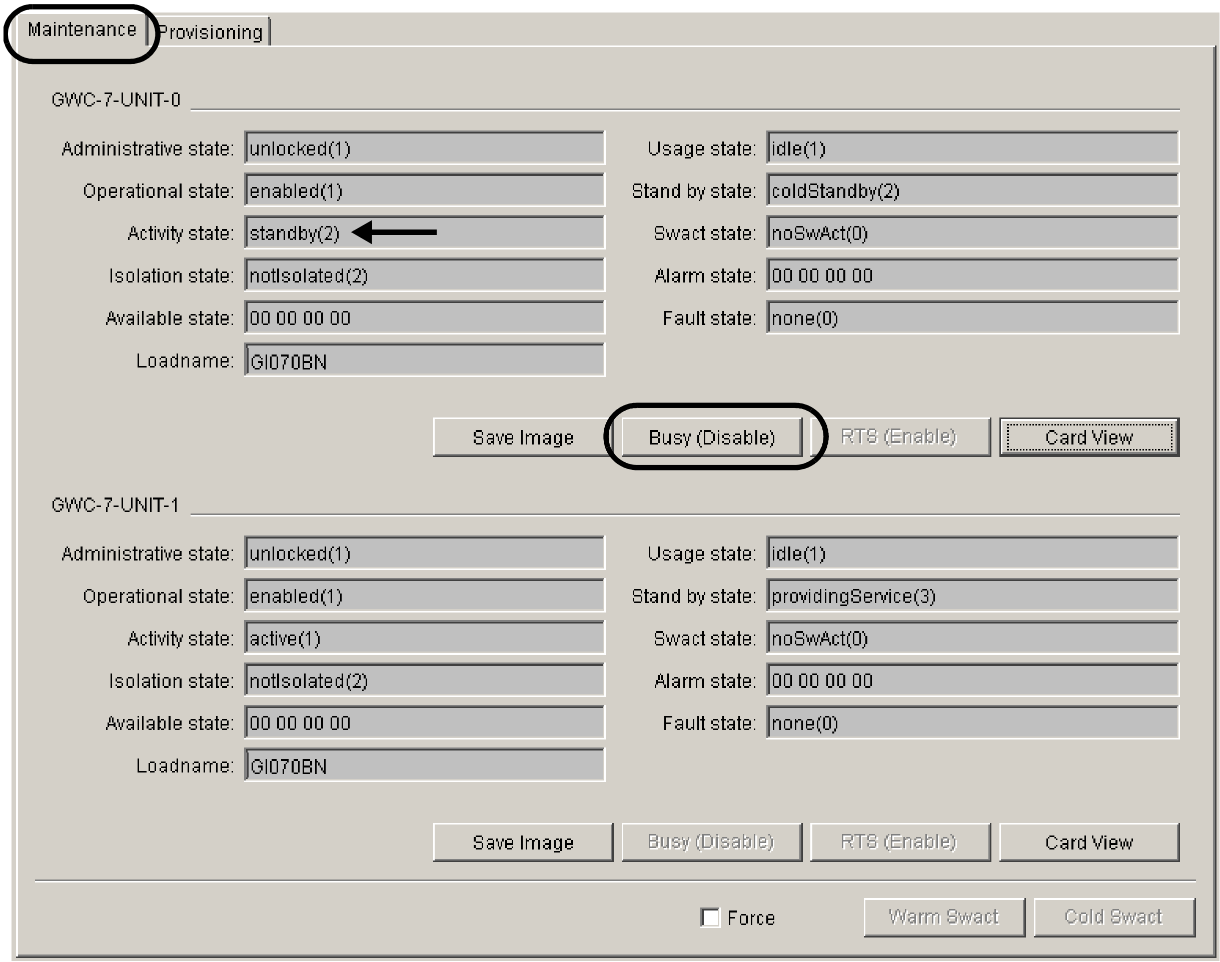
or

Select a GWC node from the list of provisioned GWC nodes.

3 Click the **Maintenance** 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 **Busy (Disable)** button for the GWC unit on standby.



GWC-7-UNIT-0

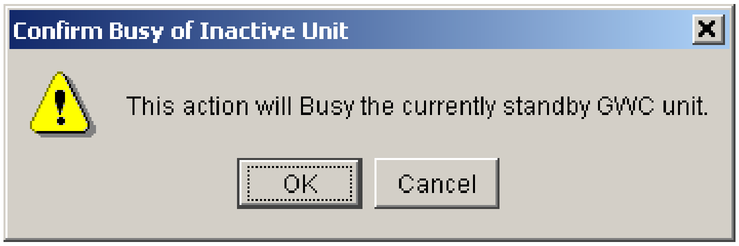
Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	coldStandby(2)
Activity state:	standby(2)	Swact state:	noSwAct(0)
Isolation state:	notIsolated(2)	Alarm state:	00 00 00 00
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	GI070BN		

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

6 At the confirmation box, click **OK** to busy the standby GWC unit.

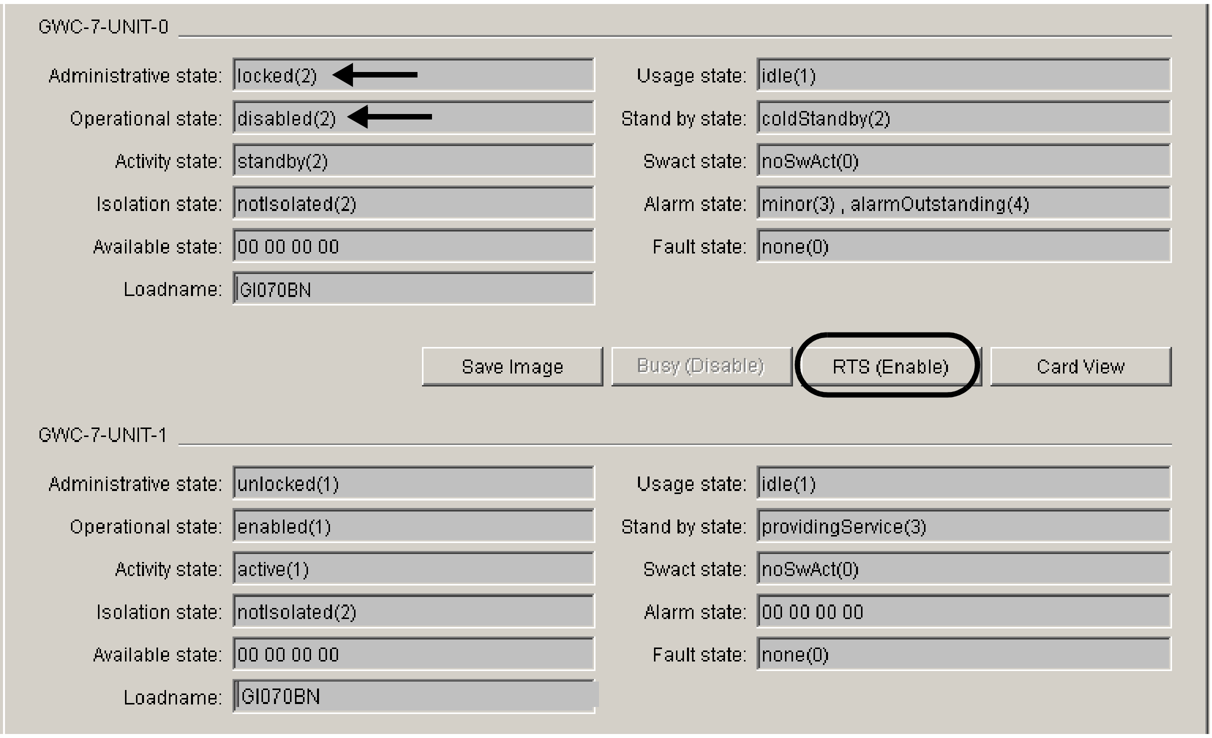


Confirm Busy of Inactive Unit

This action will Busy the currently 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.



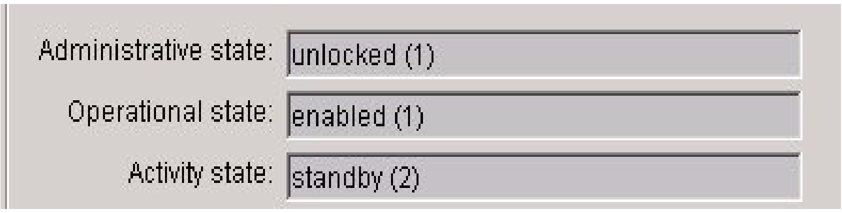
GWC-7-UNIT-0

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		

GWC-7-UNIT-1

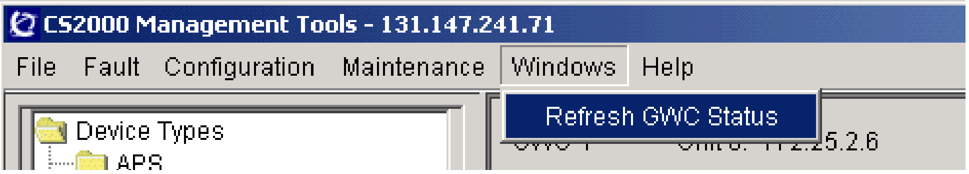
Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	providingService(3)
Activity state:	active(1)	Swact state:	noSwAct(0)
Isolation state:	notIsolated(2)	Alarm state:	00 00 00 00
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	GI070BN		

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)

Note: Normally 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.

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 (SDM) or Core and Billing Manager (CBM) console.

Action

At the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM) console

1 Login to the CS 2000 Core Manager or CBM as the root user.

2 Start the CS 2000 Core Manager or CBM maintenance interface application by typing

```
#sdmmtc
```

or

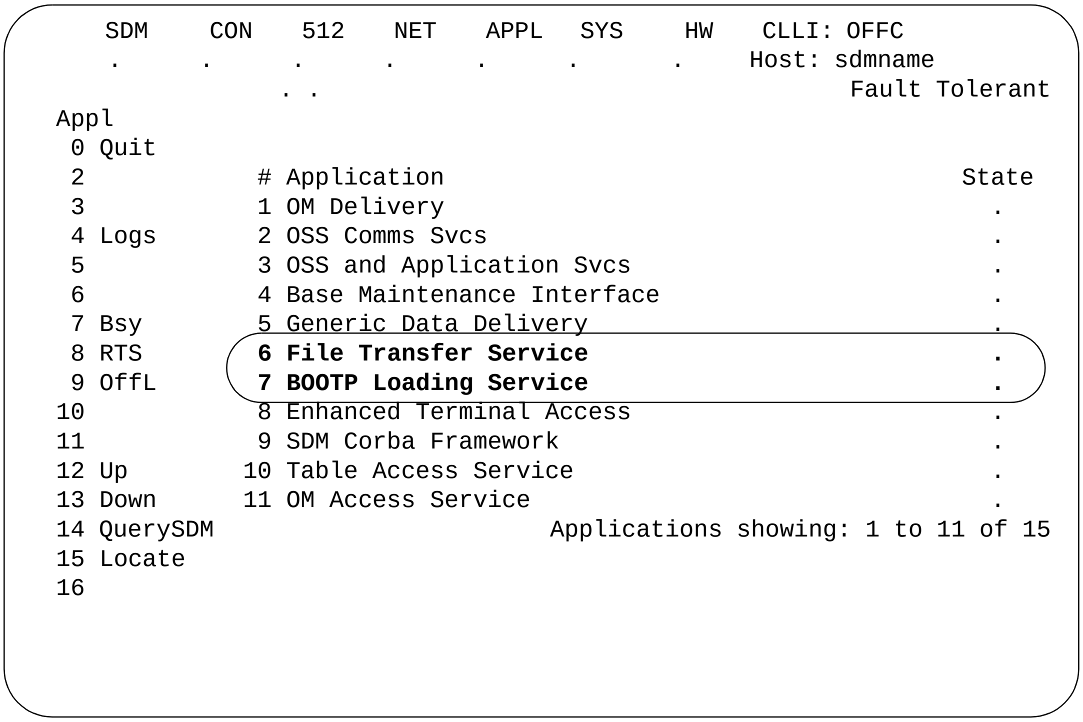
```
#cbmmtc
```

and pressing the enter key.

3 Access the applications (APPL) level of the CS 2000 Core Manager or CBM maintenance interface and verify that the Bootp Loading Service and File Transfer Service applications are in service (.) by typing

>appl

and pressing the enter key.



```
       SDM     CON    512    NET    APPL   SYS     HW    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 File Transfer Service                             .
    9 OffL       7 BOOTP Loading Service                             .
   10            8 Enhanced Terminal Access                          .
   11            9 SDM Corba Framework                               .
   12 Up        10 Table Access Service                              .
   13 Down      11 OM Access Service                                 .
   14 QuerySDM                    Applications showing: 1 to 11 of 15
   15 Locate
   16
```

4 If these applications are not in service, first BSY then RTS the applications. If these applications are in service (.), then check for bootpd and tftpd messages in the /var/adm/syslog and /var/adm/daemon.log. Refer to the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM) Security and Administration NTP for details on busying applications and returning them to service.

> ***Note:*** Unless log entries have been generated relating to application problems, no log file exists for daemon.log.

At the SAM21 frame

5 Verify that the GWC card has power by looking for the lighted yellow or green LEDs on its faceplate.

6 Use a VT100 terminal or a PC with terminal application software to connect to the DB9 serial port on the faceplate of the GWC card.

> ***Note:*** Use a standard straight through serial cable, rather than a null modem cable.

7 Configure the PC software to set the PC serial port to 9600 baud, 8 bits, no parity, 1 stop bit.

8 Start the terminal application and select a direct connection from COM1.

9 Press and hold the reset button on the faceplate of the GWC card for 5 seconds.

10 Monitor the boot process on the terminal. If the boot fails, check for the error number and reference it to the following list of error IDs.

(Sheet 1 of 2)

Error ID	Reason text
0500	TFTP retry time out. The following problems could exist: • network has too much traffic • the CS 2000 Core Manager or CBM is busy • the tftp daemon is not running • the load name was entered incorrectly
0600	BOOTP retry time out. The following problems could exist: • network has too much traffic • the CS 2000 Core Manager or CBM is busy • the bootp daemon is not running • the /etc/bootptab file is incorrectly configured

(Sheet 2 of 2)

Error ID	Reason text
8100	The load file on the CS 2000 Core Manager or CBM has the wrong path, the wrong permissions, or the wrong load name.
0020	Message CRC errors. The network could be busy and causing traffic errors.
0017	10baseT link failure. Verify that the Ethernet cable is fully seated in the faceplate and the router.

11 This procedure is complete.

Replace and re-provision a GWC card

Purpose of this procedure

Use this procedure to replace a faulty GWC card and automatically provision the replacement GWC card with the provisioning datafill of the previous card. A new media access control (MAC) address is assigned to the replacement card but all other card information, including IP addresses, port addresses, gateway addresses, and load paths, remain unchanged.

When to use this procedure

Use this procedure when Nortel Networks support personnel indicate that a GWC card should be replaced and you need to provision the replacement card with the provisioning datafill of the previous card.

This procedure does not provide instructions to make services provisioning changes to a GWC card, such as changing the service profile type of a GWC node. If changes to the GWC node provisioning are necessary, use the CS 2000 GWC Manager to busy the cards and reprovision node information. Refer to the Gateway Controller Configuration Management NTP, NN10205-511 for details.

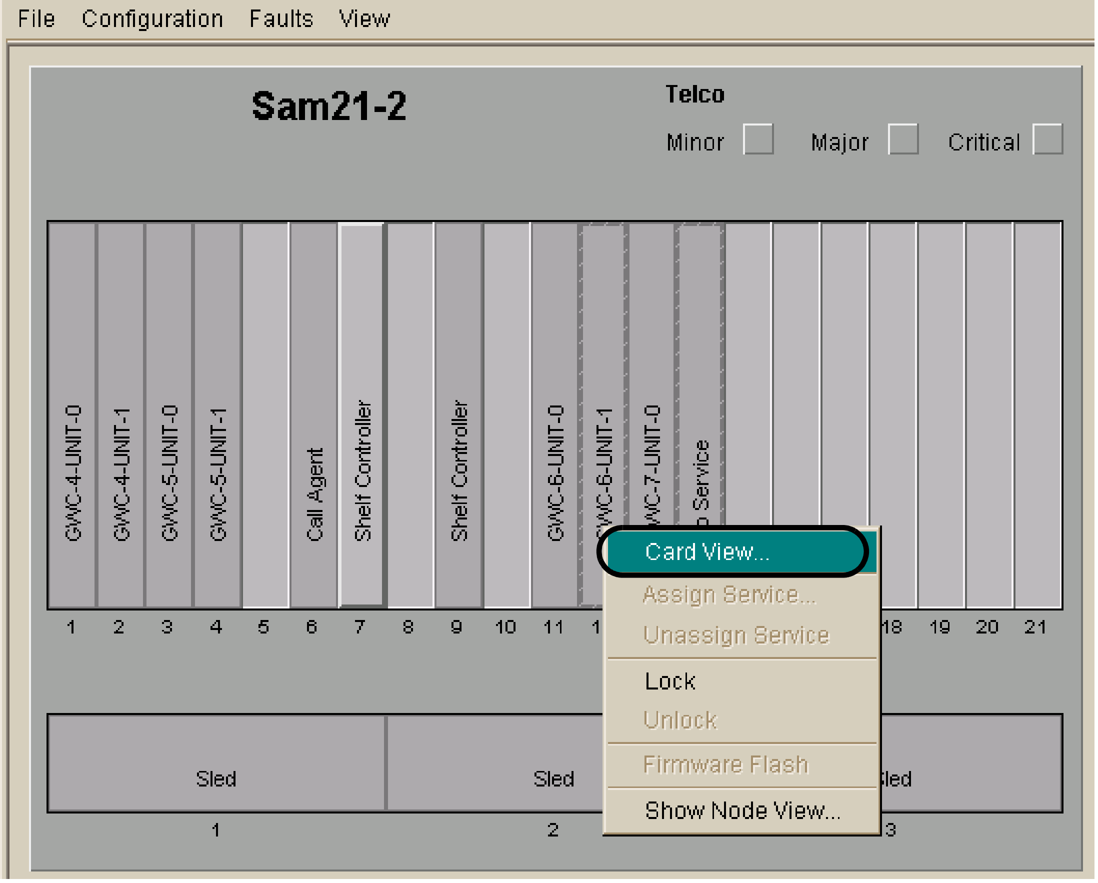
Prerequisites

This procedure has no prerequisites.

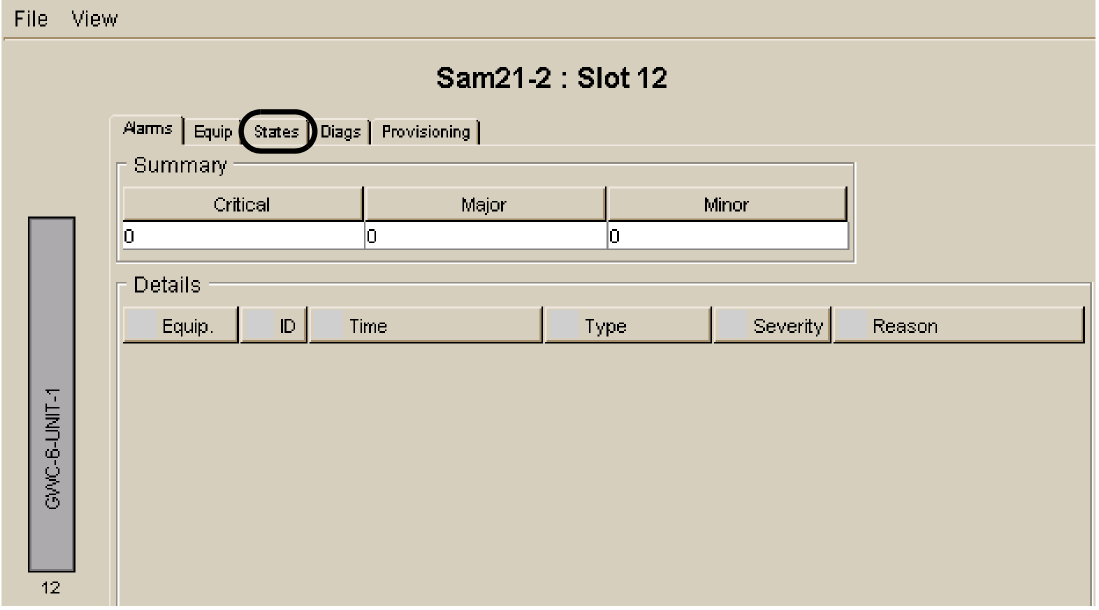
Action

At the CS 2000 SAM21 Manager client

1 Access the Card View for the card you want to replace by right-clicking the card and selecting **Card View**.

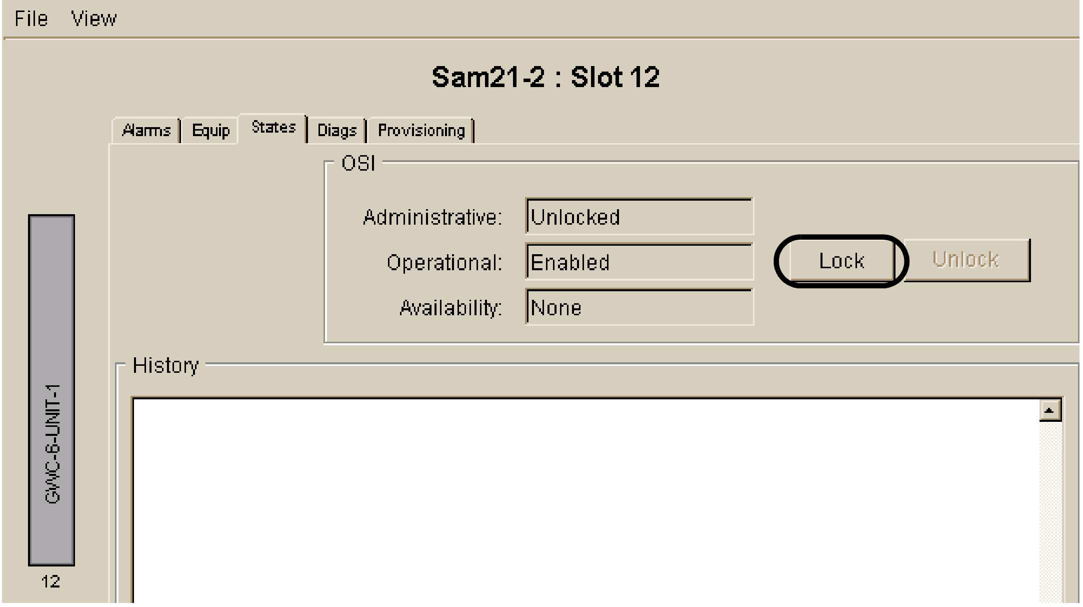


2 Click the **States** tab in the Card View.



3 Lock the card by clicking the **Lock** button.

Note: The card must be busy (disabled) before you can lock it. Refer to procedure “Busy a GWC Node” in the Gateway Controller Configuration Management NTP, NN10205-511.



Administrative: Unlocked
Operational: Enabled
Availability: None

At the SAM21 shelf

4 Remove the Ethernet and serial cables (if present) from the GWC faceplate.

5 Open the bottom ejector lever.

6 Wait for the blue LED at the bottom of the faceplate to turn on, and wait for the red LED above the card to extinguish. (The red LED indicates that the card is out of service.)

7 Press both ejector levers until card is ejected from the Shelf.

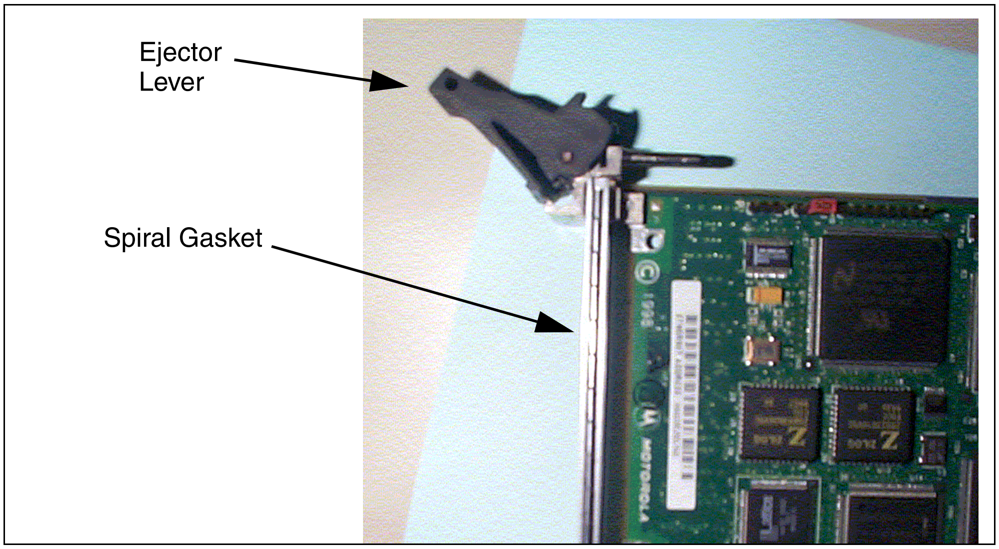
CAUTION

A service outage can occur if care is not taken while removing the GWC circuit packs.

The spiral gasket, located on the faceplate of the circuit pack, can become caught on an adjacent card and ripped off of the faceplate. If the spiral gasket ends up making contact with the backplane inside the chassis, an electrical short circuit can result in a service outage.

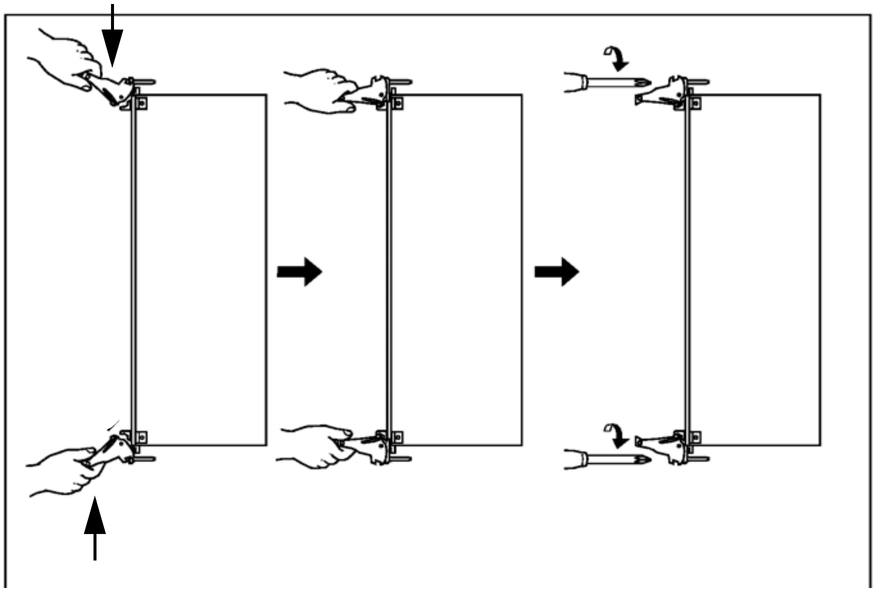
WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the SAM21 Shelf Cabinet when handling a GWC card. This protects the card against damage caused by static electricity.

8 Examine the new circuit pack before inserting it into the SAM21 chassis to ensure that the spiral gasket is seated and not loose.



9 Hold the replacement GWC card by the latches and insert the card into the shelf.

> ***Note:*** Do not push on the faceplate to seat the card.



10 Secure the card by tightening the captive screws at the top and bottom of the panel.

11 Replace the cables on the GWC card faceplate.

At the CS 2000 SAM21 Manager client

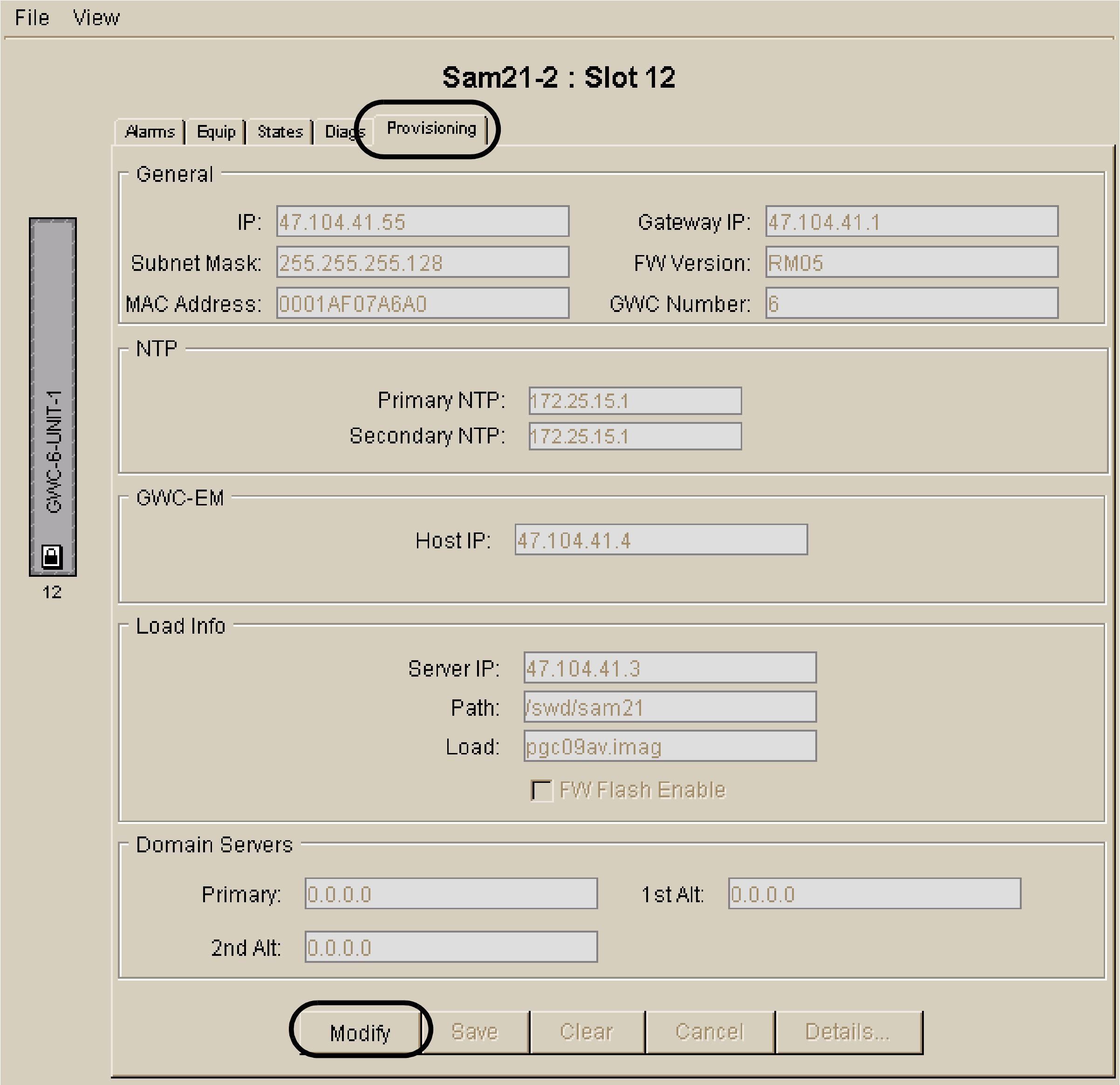
12 Wait for a card icon with a hashed outline to appear in the shelf view.

Upon insertion of the new card, the system will automatically provision the new card with the old card's provisioning information. Note that the system will assign a new MAC address to the new card.

13 Determine the next action to take.

If	Do
the provisioning data is correct data for the replacement GWC	step 20
the provisioning data for the replacement GWC requires changes	step 14

14 Open the Card View for the GWC card and click the **Provisioning** tab.



Sam21-2 : Slot 12

General

IP: 47.104.41.55

Gateway IP: 47.104.41.1

Subnet Mask: 255.255.255.128

FW Version: RM05

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/sam21

Load: pgc09av.imag

□ FW Flash Enable

Domain Servers

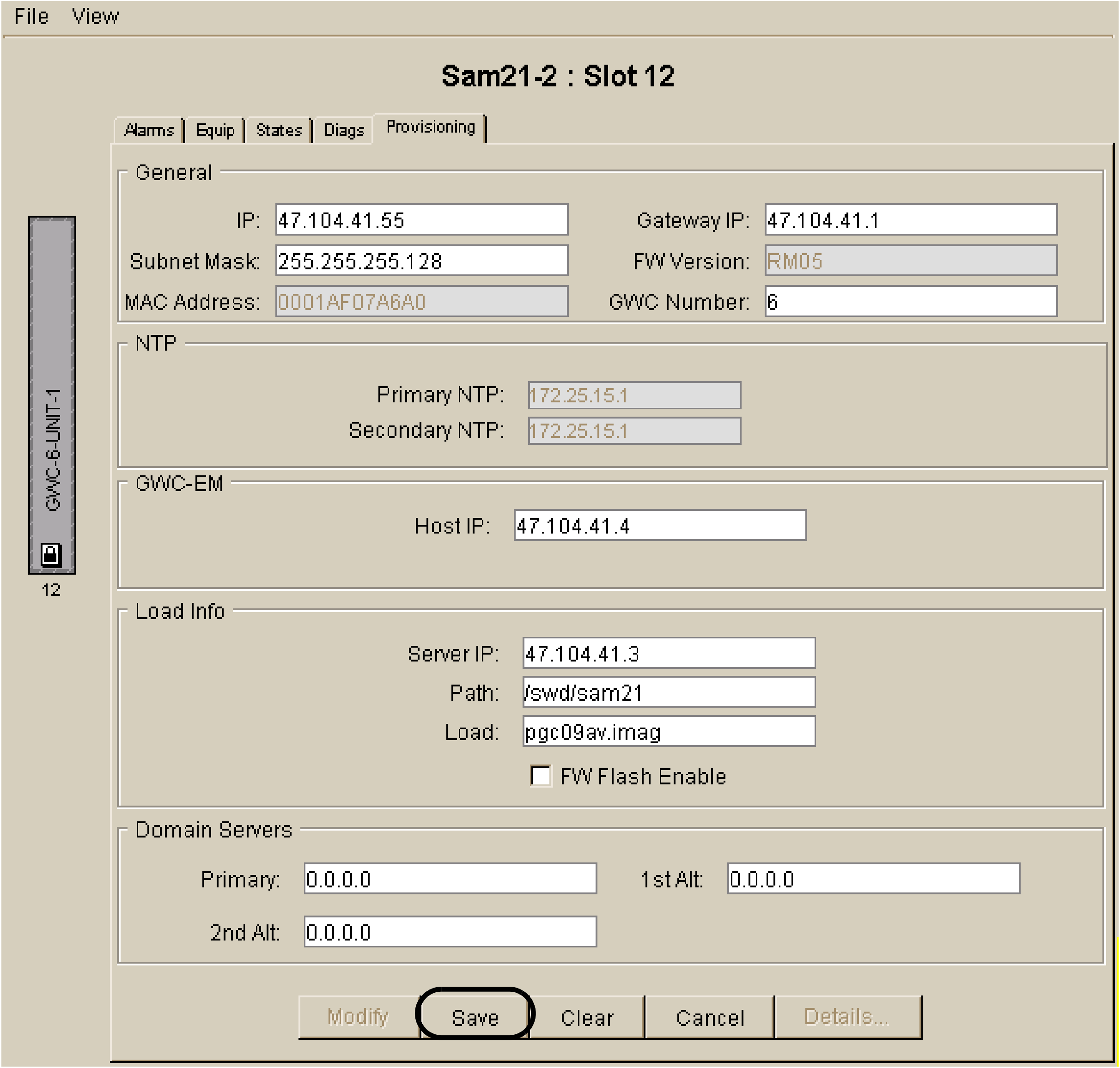
Primary: 0.0.0.0

1st Alt: 0.0.0.0

2nd Alt: 0.0.0.0

15 Click the **Modify** button to make changes to the provisioning datafill.

16 Enter the new or changed provisioning data on the window and click the **Save** button.



Sam21-2 : Slot 12

General

IP: 47.104.41.55

Gateway IP: 47.104.41.1

Subnet Mask: 255.255.255.128

FW Version: RM05

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/sam21

Load: pgc09av.imag

□ FW Flash Enable

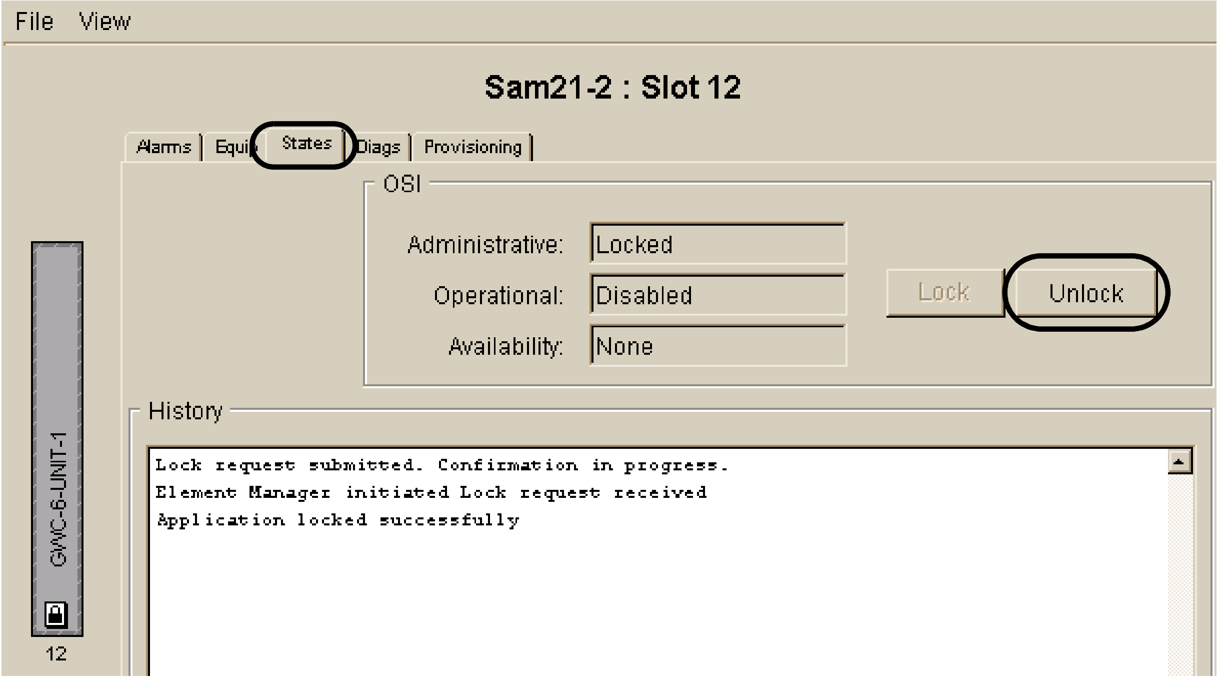
Domain Servers

Primary: 0.0.0.0

1st Alt: 0.0.0.0

2nd Alt: 0.0.0.0

17 Return to the States view by clicking the **States** tab.



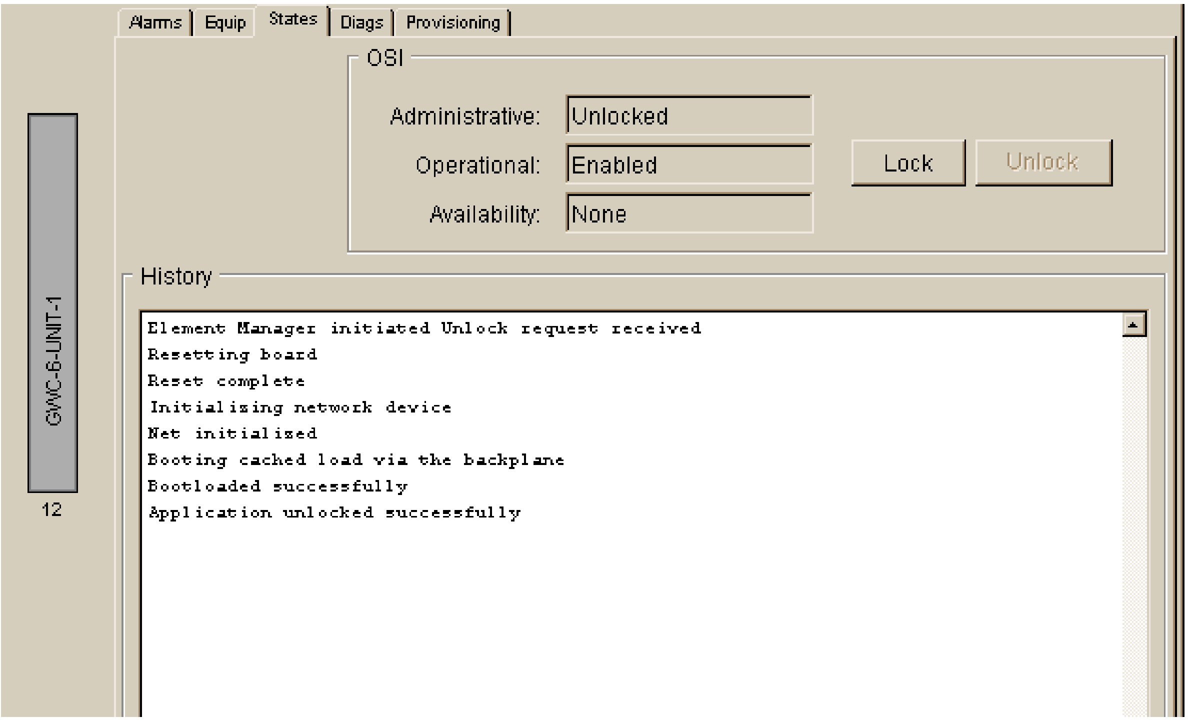
Administrative: Locked

Operational: Disabled

Availability: None

```
Lock request submitted. Confirmation in progress.
Element Manager initiated Lock request received
Application locked successfully
```

18 Unlock the card by clicking the **Unlock** button.



Administrative: Unlocked

Operational: Enabled

Availability: None

```
Element Manager initiated Unlock request received
Resetting board
Reset complete
Initializing network device
Net initialized
Booting cached load via the backplane
Bootloaded successfully
Application unlocked successfully
```

19 Observe the History window to ensure that the card boot loaded and unlocked successfully.

20 This procedure is complete.

Perform a GWC line data integrity audit

Purpose of this procedure

Use this procedure to perform an on-demand data integrity audit of line data stored in the CS 2000 GWC Manager database and the CS 2000 XA-Core database.

The audit compares the information in the two databases, flags any mismatches and displays the results of the audit. This procedure uses the audit system data integrity tool to perform the audit and view the results.

> ***Note:*** You can also schedule a line data integrity audit using this tool. Refer to procedure “Configure a recurring data integrity audit” in the Gateway Controller Configuration Management NTP, NN10205-511.

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
- 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.

When to use this procedure

Use this procedure to perform an on-demand audit to check for defective data after you have done line provisioning, or if you suspect there is a problem with line provisioning.

Use this procedure to view the results of completed audits as required.

> ***Note 1:*** Do not run an on-demand line data integrity audit while line provisioning is occurring.
>
> ***Note 2:*** The audit application keeps no record of problems that it has raised an alarm for. Therefore, if a problem is detected during an audit and not corrected, an alarm will be generated in the alarm manager for the same problem the next time the audit is run.

Note 3: If you have scheduled data integrity audits, remember that a maximum of one line audit can be in progress at any given time. An in-progress line audit blocks all attempts to run any subsequent line audit requests. If you run an on-demand line audit, and if that audit is still in progress at the start time of a scheduled line audit, the scheduled audit will not occur.

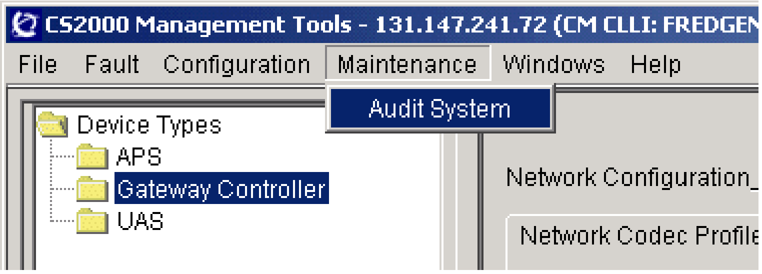
Prerequisites

Ensure that there are no line audits scheduled to occur during a manual audit.

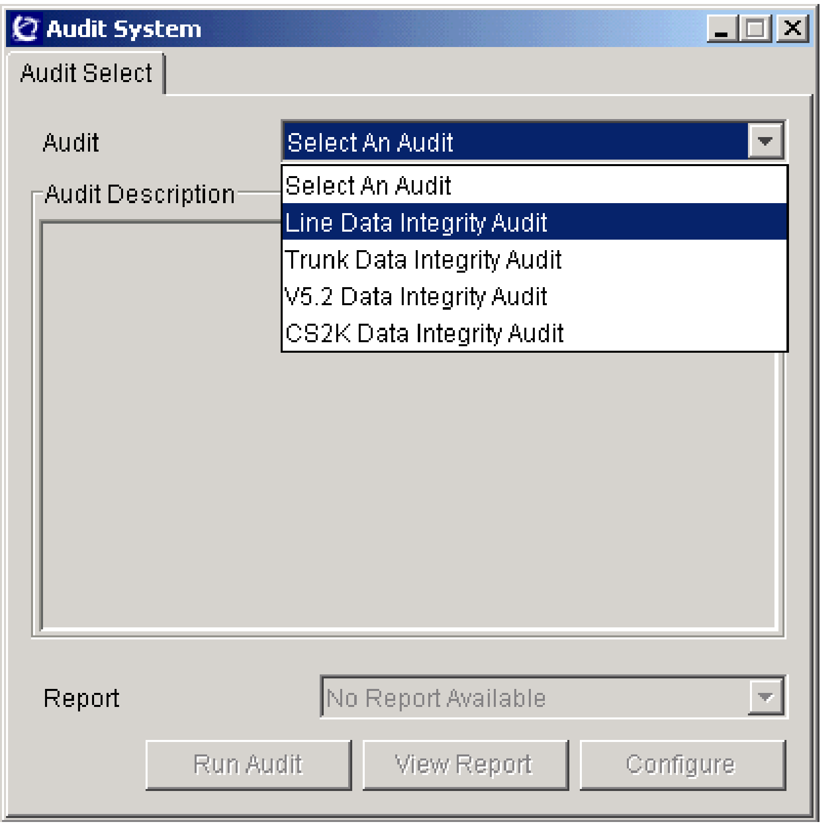
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, select **Maintenance**, then **Audit System**.



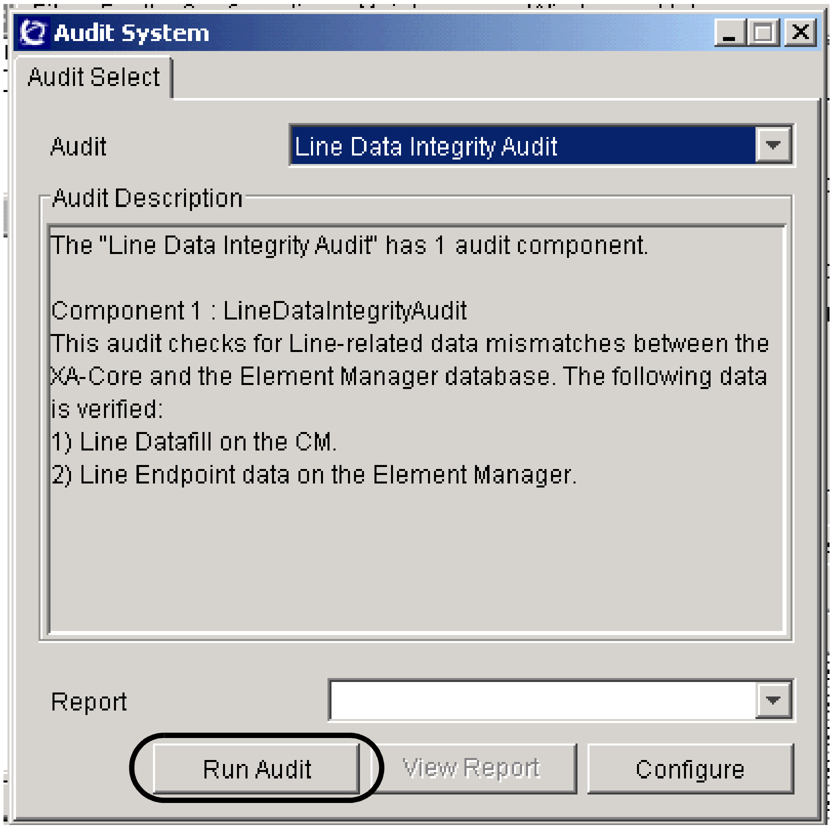
2 At the Audit System dialog box, select **Line Data Integrity Audit** from list of audits displayed in the drop-down menu.



3 Select the next step as follows.

If you want to	**Do**
perform an on-demand line audit and view the “valid data” and “problem data” results of the audit	step 4 and complete the procedure
perform an on-demand line audit and view only the “problem data” results of the audit	step 4, and then perform steps 5 and 7
view the “valid data” and “problem data” results of a trunk audit that has finished running	step 6 and complete the procedure
view only the “problem data” results of a trunk audit that has finished running	step 7 and complete the procedure

4 Click the **Run Audit** button to start the audit.



Audit System

Audit Select

Audit: Line Data Integrity Audit

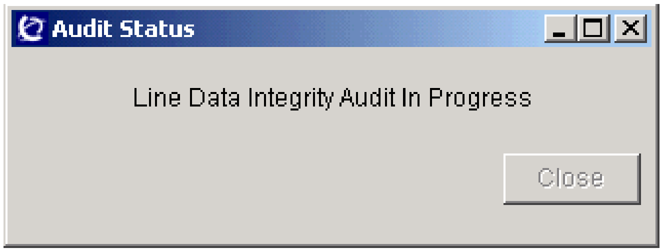
Audit Description

The "Line Data Integrity Audit" has 1 audit component.

Component 1 : LineDataIntegrityAudit
This audit checks for Line-related data mismatches between the XA-Core and the Element Manager database. The following data is verified:
1) Line Datafill on the CM.
2) Line Endpoint data on the Element Manager.

Report:

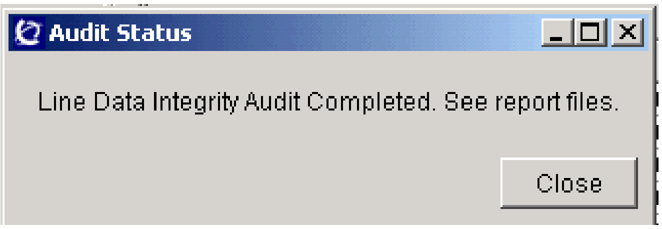
During a line audit, the system displays the following message:



Audit Status

Line Data Integrity Audit In Progress

The audit may take a few minutes to complete. When the audit is successfully completed, the system displays the following pop-up window message.



Line Data Integrity Audit Completed. See report files.

Note: If the audit does not execute successfully, the message “Line Data Integrity Audit Failed to Complete” is displayed with an error message indicating the reason. Contact your next level of support to resolve the problem.

5 Click the **Close** button to close the Audit Status pop-up window.

6 To view the line valid-data report, proceed as follows:

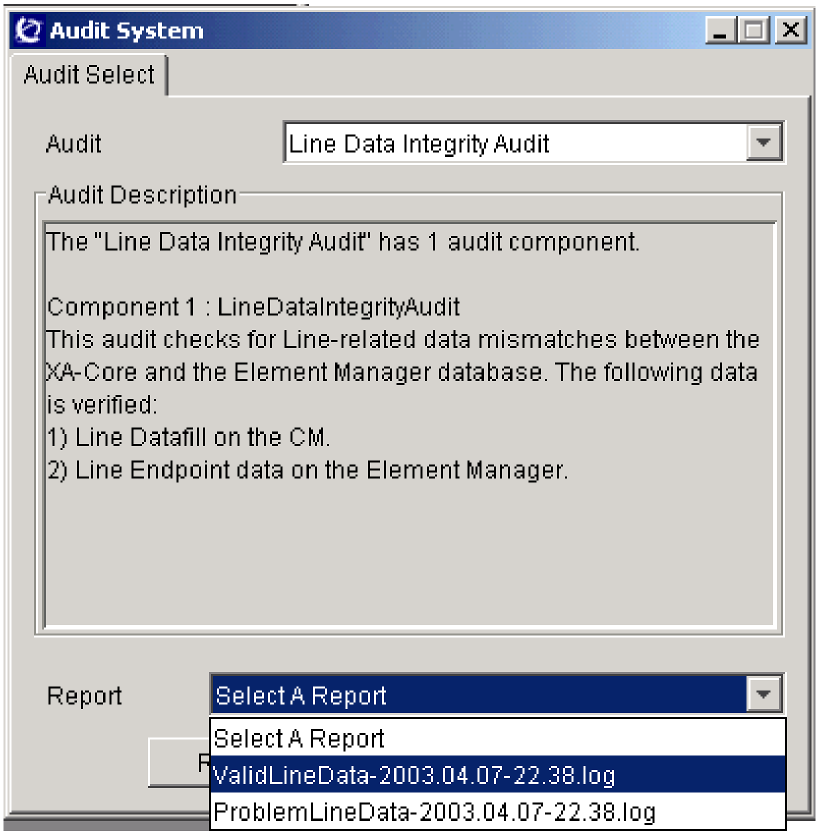
a Ensure that you have selected **Line Data Integrity Audit** from the Audit field drop-down menu at the top of the Audit System dialog box.

b Select **ValidLineData** from the drop-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.



Audit System

Audit Select

Audit: Line Data Integrity Audit

Audit Description

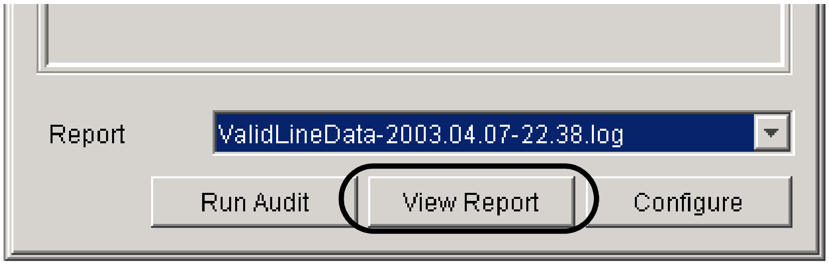
The "Line Data Integrity Audit" has 1 audit component.

Component 1 : LineDataIntegrityAudit
This audit checks for Line-related data mismatches between the XA-Core and the Element Manager database. The following data is verified:
1) Line Datafill on the CM.
2) Line Endpoint data on the Element Manager.

Report: Select A Report

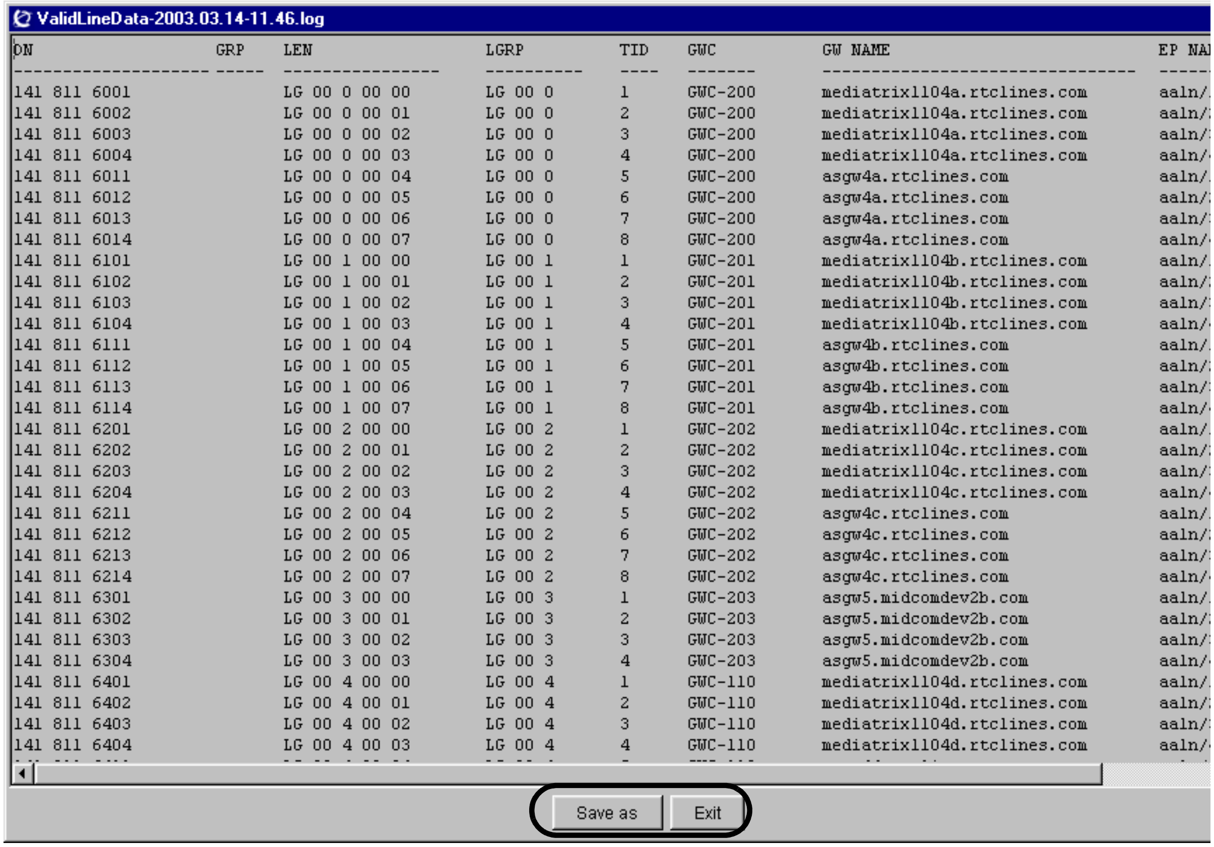
Select A Report
ValidLineData-2003.04.07-22.38.log
ProblemLineData-2003.04.07-22.38.log

c Click the **View Report** button.



Report ValidLineData-2003.04.07-22.38.log

The system displays the selected report. An example of a "ValidLineData" report is shown below.



ValidLineData-2003.03.14-11.46.log

```
DN                   GRP   LEN                  LGRP         TID    GWC           GW NAME                           EP NA
-------------------- ----- ----------------     ----------   ----   -------       --------------------------------  -----
141 811 6001               LG 00 0 00 00        LG 00 0      1      GWC-200       mediatrix1104a.rtclines.com       aaln/
141 811 6002               LG 00 0 00 01        LG 00 0      2      GWC-200       mediatrix1104a.rtclines.com       aaln/
141 811 6003               LG 00 0 00 02        LG 00 0      3      GWC-200       mediatrix1104a.rtclines.com       aaln/
141 811 6004               LG 00 0 00 03        LG 00 0      4      GWC-200       mediatrix1104a.rtclines.com       aaln/
141 811 6011               LG 00 0 00 04        LG 00 0      5      GWC-200       asgw4a.rtclines.com               aaln/
141 811 6012               LG 00 0 00 05        LG 00 0      6      GWC-200       asgw4a.rtclines.com               aaln/
141 811 6013               LG 00 0 00 06        LG 00 0      7      GWC-200       asgw4a.rtclines.com               aaln/
141 811 6014               LG 00 0 00 07        LG 00 0      8      GWC-200       asgw4a.rtclines.com               aaln/
141 811 6101               LG 00 1 00 00        LG 00 1      1      GWC-201       mediatrix1104b.rtclines.com       aaln/
141 811 6102               LG 00 1 00 01        LG 00 1      2      GWC-201       mediatrix1104b.rtclines.com       aaln/
141 811 6103               LG 00 1 00 02        LG 00 1      3      GWC-201       mediatrix1104b.rtclines.com       aaln/
141 811 6104               LG 00 1 00 03        LG 00 1      4      GWC-201       mediatrix1104b.rtclines.com       aaln/
141 811 6111               LG 00 1 00 04        LG 00 1      5      GWC-201       asgw4b.rtclines.com               aaln/
141 811 6112               LG 00 1 00 05        LG 00 1      6      GWC-201       asgw4b.rtclines.com               aaln/
141 811 6113               LG 00 1 00 06        LG 00 1      7      GWC-201       asgw4b.rtclines.com               aaln/
141 811 6114               LG 00 1 00 07        LG 00 1      8      GWC-201       asgw4b.rtclines.com               aaln/
141 811 6201               LG 00 2 00 00        LG 00 2      1      GWC-202       mediatrix1104c.rtclines.com       aaln/
141 811 6202               LG 00 2 00 01        LG 00 2      2      GWC-202       mediatrix1104c.rtclines.com       aaln/
141 811 6203               LG 00 2 00 02        LG 00 2      3      GWC-202       mediatrix1104c.rtclines.com       aaln/
141 811 6204               LG 00 2 00 03        LG 00 2      4      GWC-202       mediatrix1104c.rtclines.com       aaln/
141 811 6211               LG 00 2 00 04        LG 00 2      5      GWC-202       asgw4c.rtclines.com               aaln/
141 811 6212               LG 00 2 00 05        LG 00 2      6      GWC-202       asgw4c.rtclines.com               aaln/
141 811 6213               LG 00 2 00 06        LG 00 2      7      GWC-202       asgw4c.rtclines.com               aaln/
141 811 6214               LG 00 2 00 07        LG 00 2      8      GWC-202       asgw4c.rtclines.com               aaln/
141 811 6301               LG 00 3 00 00        LG 00 3      1      GWC-203       asgw5.midcomdev2b.com             aaln/
141 811 6302               LG 00 3 00 01        LG 00 3      2      GWC-203       asgw5.midcomdev2b.com             aaln/
141 811 6303               LG 00 3 00 02        LG 00 3      3      GWC-203       asgw5.midcomdev2b.com             aaln/
141 811 6304               LG 00 3 00 03        LG 00 3      4      GWC-203       asgw5.midcomdev2b.com             aaln/
141 811 6401               LG 00 4 00 00        LG 00 4      1      GWC-110       mediatrix1104d.rtclines.com       aaln/
141 811 6402               LG 00 4 00 01        LG 00 4      2      GWC-110       mediatrix1104d.rtclines.com       aaln/
141 811 6403               LG 00 4 00 02        LG 00 4      3      GWC-110       mediatrix1104d.rtclines.com       aaln/
141 811 6404               LG 00 4 00 03        LG 00 4      4      GWC-110       mediatrix1104d.rtclines.com       aaln/
```

Note 1: The CS 2000 Management Tools server retains the six most recent "ValidLineData" reports. When a new line audit occurs, the server deletes the oldest report.

Note 2: The system places valid data audit reports in the following directory on the CS 2000 Management Tools server: /opt/nortel/ptm/current/www/Audit/LineDataIntegrityAudit/.

d If you want to retain one of these reports for a longer time, or if you want to print a report, click the **Save as** button at the bottom of the screen. Then, save the report under a file name of your choice.

e To print a report you have saved, open the file using a text editor and print the file.

f After viewing the valid-data report, click the **Exit** button at the bottom of the screen.

7 To view the line problem-data report, proceed as follows:

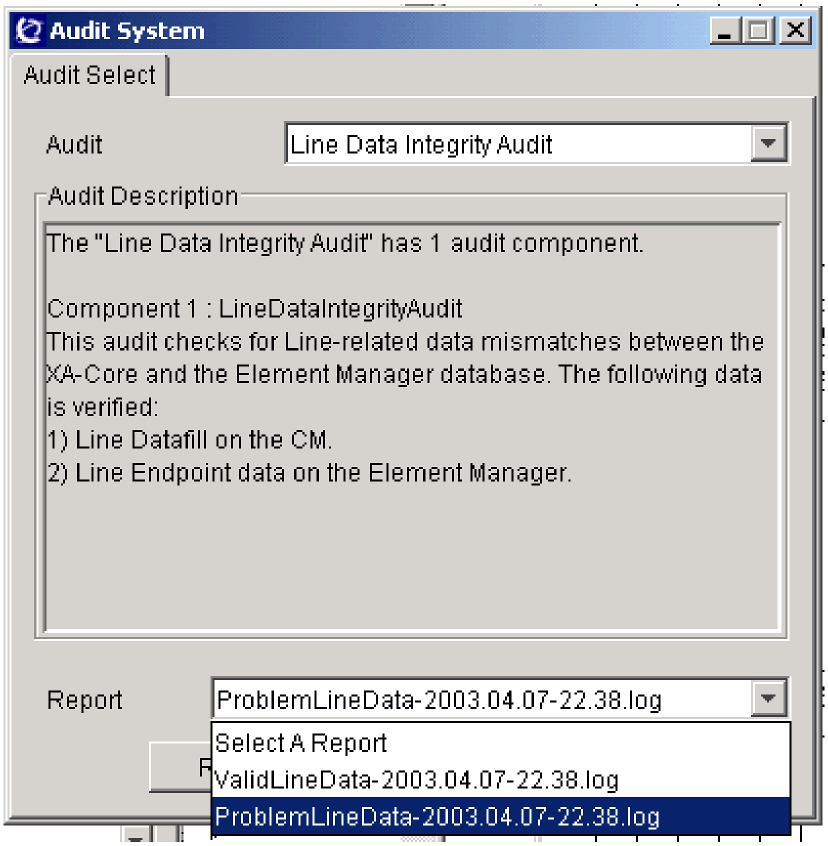
a Ensure that you have selected **Line Data Integrity Audit** from the Audit field drop-down menu at the top of the Audit System dialog box.

b Select **ProblemLineData** from the drop-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.



Audit: Line Data Integrity Audit

Audit Description

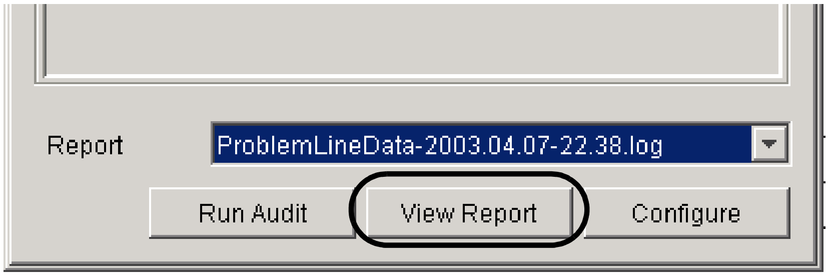
The "Line Data Integrity Audit" has 1 audit component.

Component 1 : LineDataIntegrityAudit
This audit checks for Line-related data mismatches between the XA-Core and the Element Manager database. The following data is verified:
1) Line Datafill on the CM.
2) Line Endpoint data on the Element Manager.

Report: ProblemLineData-2003.04.07-22.38.log

Select A Report
ValidLineData-2003.04.07-22.38.log
ProblemLineData-2003.04.07-22.38.log

c Click the **View Report** button.



Report ProblemLineData-2003.04.07-22.38.log

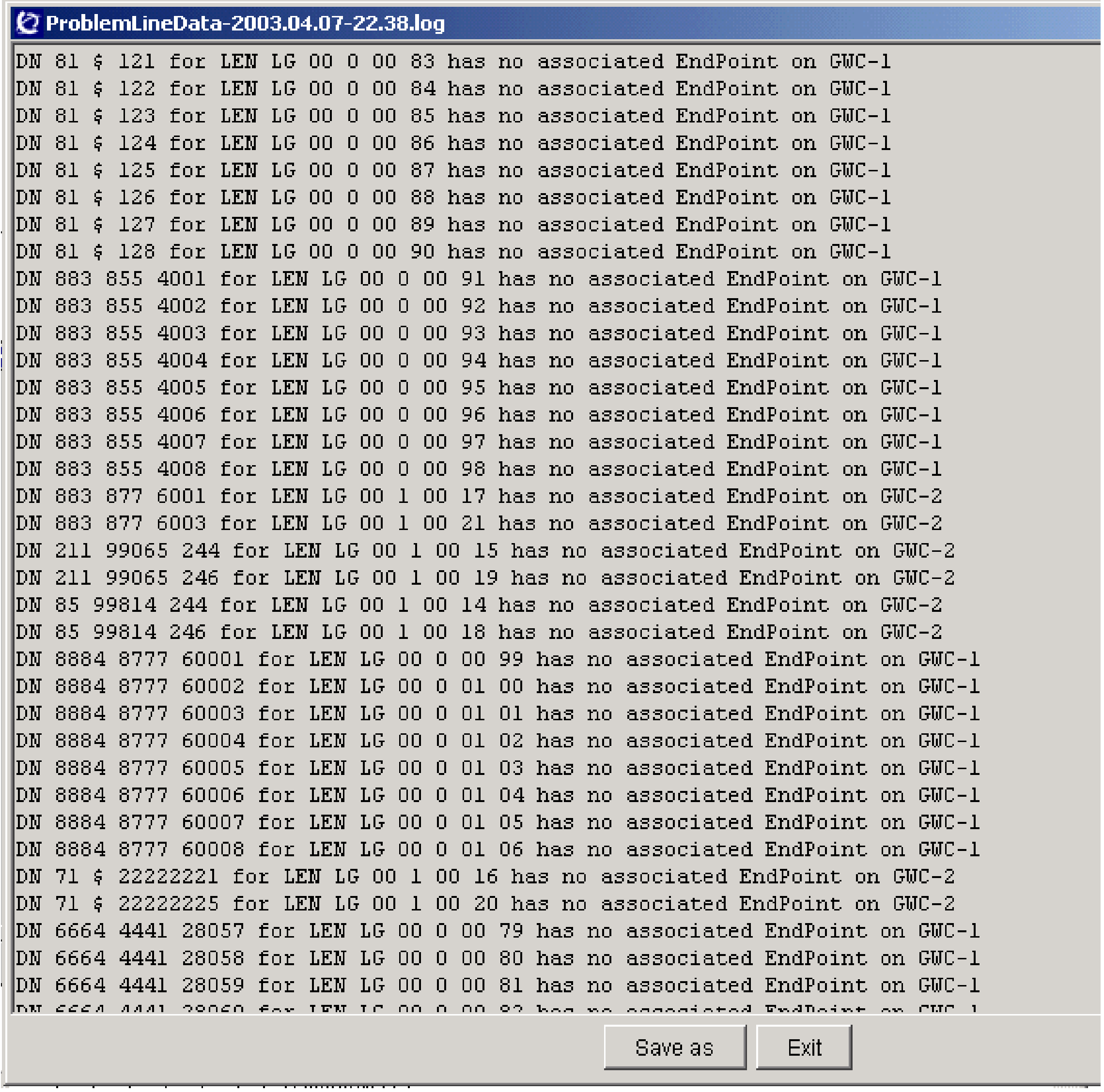
The system displays the selected report.

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 the CM.

Here is an example of a “ProblemLineData” report:



```
DN 81 $ 121 for LEN LG 00 0 00 83 has no associated EndPoint on GWC-1
DN 81 $ 122 for LEN LG 00 0 00 84 has no associated EndPoint on GWC-1
DN 81 $ 123 for LEN LG 00 0 00 85 has no associated EndPoint on GWC-1
DN 81 $ 124 for LEN LG 00 0 00 86 has no associated EndPoint on GWC-1
DN 81 $ 125 for LEN LG 00 0 00 87 has no associated EndPoint on GWC-1
DN 81 $ 126 for LEN LG 00 0 00 88 has no associated EndPoint on GWC-1
DN 81 $ 127 for LEN LG 00 0 00 89 has no associated EndPoint on GWC-1
DN 81 $ 128 for LEN LG 00 0 00 90 has no associated EndPoint on GWC-1
DN 883 855 4001 for LEN LG 00 0 00 91 has no associated EndPoint on GWC-1
DN 883 855 4002 for LEN LG 00 0 00 92 has no associated EndPoint on GWC-1
DN 883 855 4003 for LEN LG 00 0 00 93 has no associated EndPoint on GWC-1
DN 883 855 4004 for LEN LG 00 0 00 94 has no associated EndPoint on GWC-1
DN 883 855 4005 for LEN LG 00 0 00 95 has no associated EndPoint on GWC-1
DN 883 855 4006 for LEN LG 00 0 00 96 has no associated EndPoint on GWC-1
DN 883 855 4007 for LEN LG 00 0 00 97 has no associated EndPoint on GWC-1
DN 883 855 4008 for LEN LG 00 0 00 98 has no associated EndPoint on GWC-1
DN 883 877 6001 for LEN LG 00 1 00 17 has no associated EndPoint on GWC-2
DN 883 877 6003 for LEN LG 00 1 00 21 has no associated EndPoint on GWC-2
DN 211 99065 244 for LEN LG 00 1 00 15 has no associated EndPoint on GWC-2
DN 211 99065 246 for LEN LG 00 1 00 19 has no associated EndPoint on GWC-2
DN 85 99814 244 for LEN LG 00 1 00 14 has no associated EndPoint on GWC-2
DN 85 99814 246 for LEN LG 00 1 00 18 has no associated EndPoint on GWC-2
DN 8884 8777 60001 for LEN LG 00 0 00 99 has no associated EndPoint on GWC-1
DN 8884 8777 60002 for LEN LG 00 0 01 00 has no associated EndPoint on GWC-1
DN 8884 8777 60003 for LEN LG 00 0 01 01 has no associated EndPoint on GWC-1
DN 8884 8777 60004 for LEN LG 00 0 01 02 has no associated EndPoint on GWC-1
DN 8884 8777 60005 for LEN LG 00 0 01 03 has no associated EndPoint on GWC-1
DN 8884 8777 60006 for LEN LG 00 0 01 04 has no associated EndPoint on GWC-1
DN 8884 8777 60007 for LEN LG 00 0 01 05 has no associated EndPoint on GWC-1
DN 8884 8777 60008 for LEN LG 00 0 01 06 has no associated EndPoint on GWC-1
DN 71 $ 22222221 for LEN LG 00 1 00 16 has no associated EndPoint on GWC-2
DN 71 $ 22222225 for LEN LG 00 1 00 20 has no associated EndPoint on GWC-2
DN 6664 4441 28057 for LEN LG 00 0 00 79 has no associated EndPoint on GWC-1
DN 6664 4441 28058 for LEN LG 00 0 00 80 has no associated EndPoint on GWC-1
DN 6664 4441 28059 for LEN LG 00 0 00 81 has no associated EndPoint on GWC-1
DN 6664 4441 28060 for LEN LG 00 0 00 82 has no associated EndPoint on GWC-1
```

Note 1: The CS 2000 Management Tools server retains the six most recent “ProblemLineData” reports. When a new audit occurs, the server deletes the oldest report.

Note 2: The system places problem data audit reports in the following directory on the CS 2000 Management Tools server: /opt/nortel/ptm/current/www/Audit/LineDataIntegrityAudit/.

d If you want to retain one of these reports for a longer time, or print a report, click the **Save as** button at the bottom of the screen. Then, save the report under a new file name.

- **e** To print a report you have saved, open the file using a text editor and print the file.
- **f** To correct the problems, refer to the printed copy of the report. You will need to delete and then reprovision the listed lines.
- **g** After viewing the problem-data report, click the **Exit** button at the bottom of the viewer screen.

8 This procedure is complete.

Perform a GWC trunk data integrity audit

Purpose of this procedure

Use this procedure to perform an on-demand data integrity audit of trunk data stored in the CS 2000 GWC Manager database and the CS 2000 XA-Core database.

The audit compares the information in the two databases, flags any mismatches and displays the results of the audit. This procedure uses the audit system data integrity tool to perform the audit and view the results.

> ***Note:*** You can also schedule a trunk data integrity audit using this tool. Refer to procedure “Configure a recurring data integrity audit” in the Gateway Controller Configuration Management NTP, NN10205-511.

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.

When to use this procedure

Use this procedure to perform an on-demand audit to check for defective data after you have done trunk provisioning, or if you suspect there is a problem with trunk provisioning.

Use this procedure to view the results of completed audits as required.

> ***Note 1:*** Do not run an on-demand trunk data integrity audit while trunk provisioning is occurring.
>
> ***Note 2:*** The audit application keeps no record of problems that it has raised an alarm for. Therefore, if a problem is detected during an audit and not corrected, an alarm will be generated in the alarm manager for the same problem the next time the audit is run.

Note 3: If you have scheduled data integrity audits, remember that a maximum of one trunk audit can be in progress at a time. An in-progress trunk audit blocks all attempts to run trunk audits. If you run an on-demand trunk audit, and if that audit is still in progress at the start time of a scheduled trunk audit, the scheduled audit will not occur.

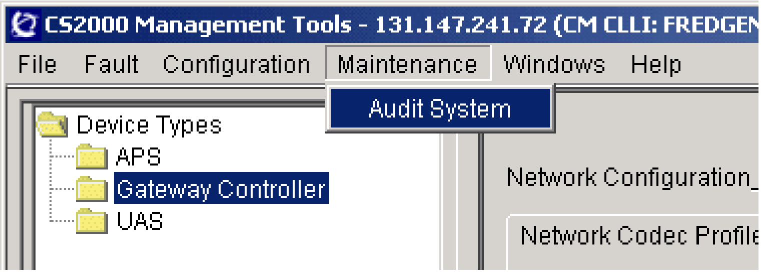
Prerequisites

Ensure that there are no trunk audits scheduled to occur during a manual audit.

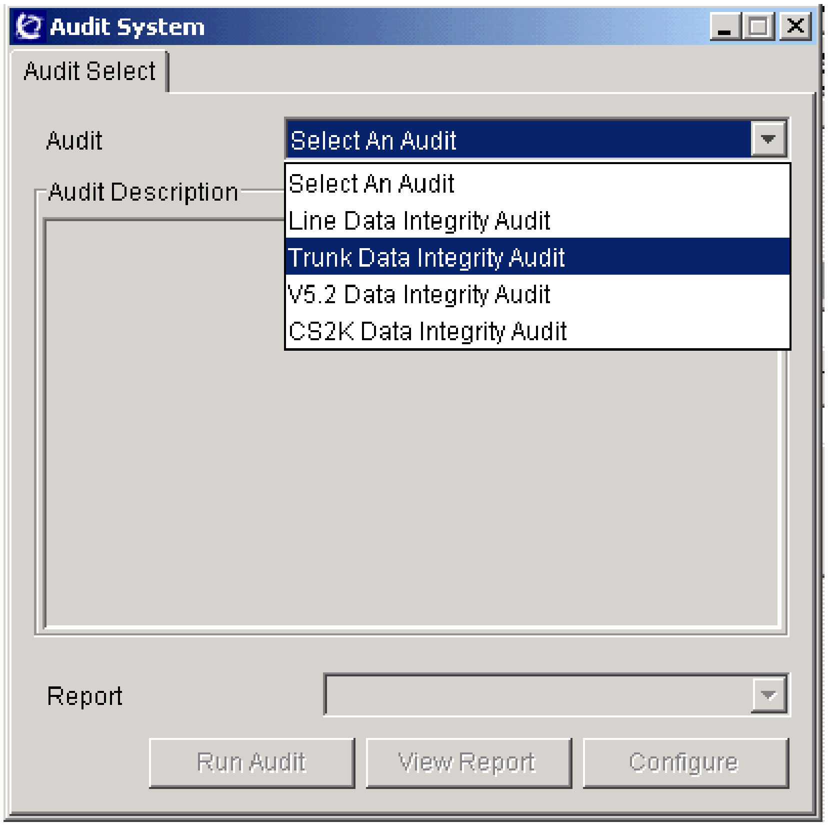
Action

At the CS 2000 GWC Manager client

1. At the CS 2000 Management Tools window, select **Maintenance**, then **Audit System**.



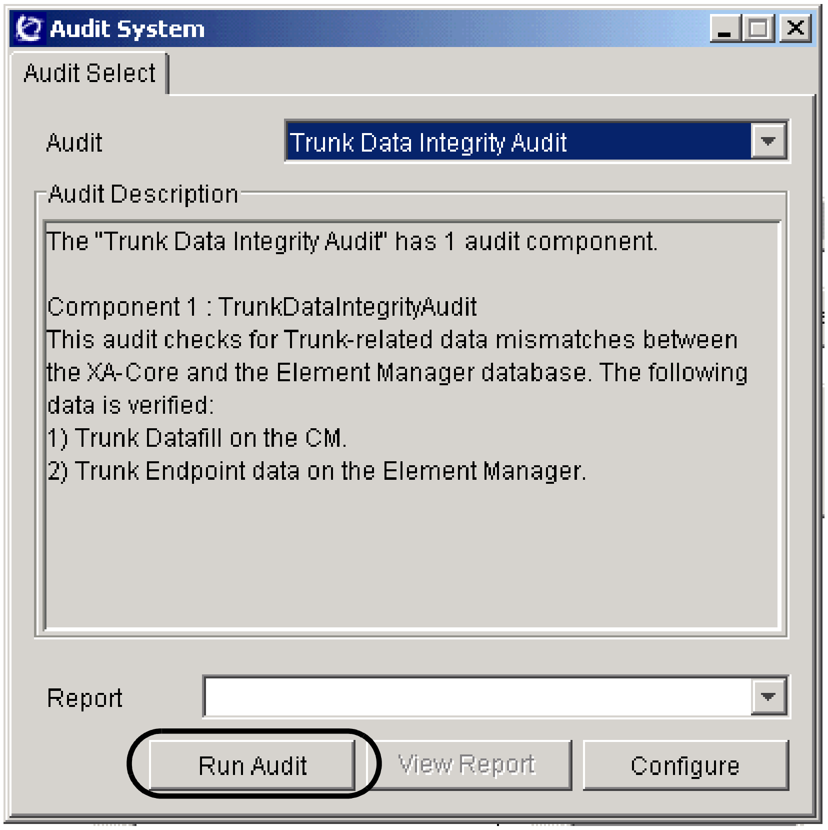
2 At the Audit System dialog box, select **Trunk Data Integrity Audit** from list of audits displayed in the drop-down menu.



3 Select the next step as follows.

If you want to	Do
perform an on-demand trunk audit and view the “valid data” and “problem data” results of the audit	step 4 and complete the procedure
perform an on-demand trunk audit and view only the “problem data” results of the audit	step 4, and then perform steps 5 and 7
view the “valid data” and “problem data” results of a trunk audit that has finished running	step 6 and complete the procedure
view only the “problem data” results of a trunk audit that has finished running	step 7 and complete the procedure

4 Click the **Run Audit** button to start the audit.



Audit: Trunk Data Integrity Audit

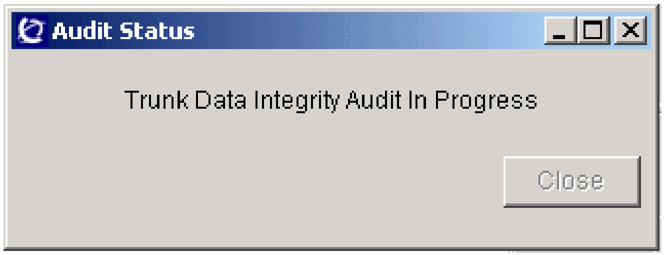
Audit Description

The "Trunk Data Integrity Audit" has 1 audit component.

Component 1 : TrunkDataIntegrityAudit
This audit checks for Trunk-related data mismatches between the XA-Core and the Element Manager database. The following data is verified:
1) Trunk Datafill on the CM.
2) Trunk Endpoint data on the Element Manager.

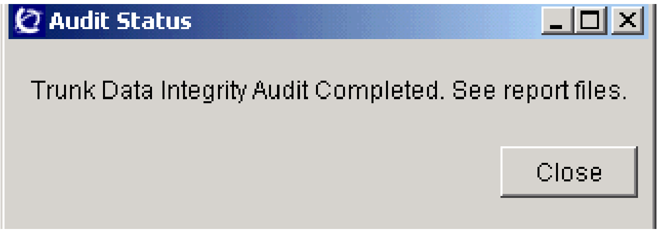
Report:

During a trunk audit, the system displays the following message:



Trunk Data Integrity Audit In Progress

The audit may take a few minutes to complete. When the audit is successfully completed, the system displays the following message.



Trunk Data Integrity Audit Completed. See report files.

Note: If the audit does not execute successfully, the message “Trunk Data Integrity Audit Failed to Complete” is displayed with an error message indicating the reason. Contact your next level of support to resolve the problem.

5 Click the **Close** button to close the Audit Status pop-up window.

6 To view the trunk valid-data report, proceed as follows:

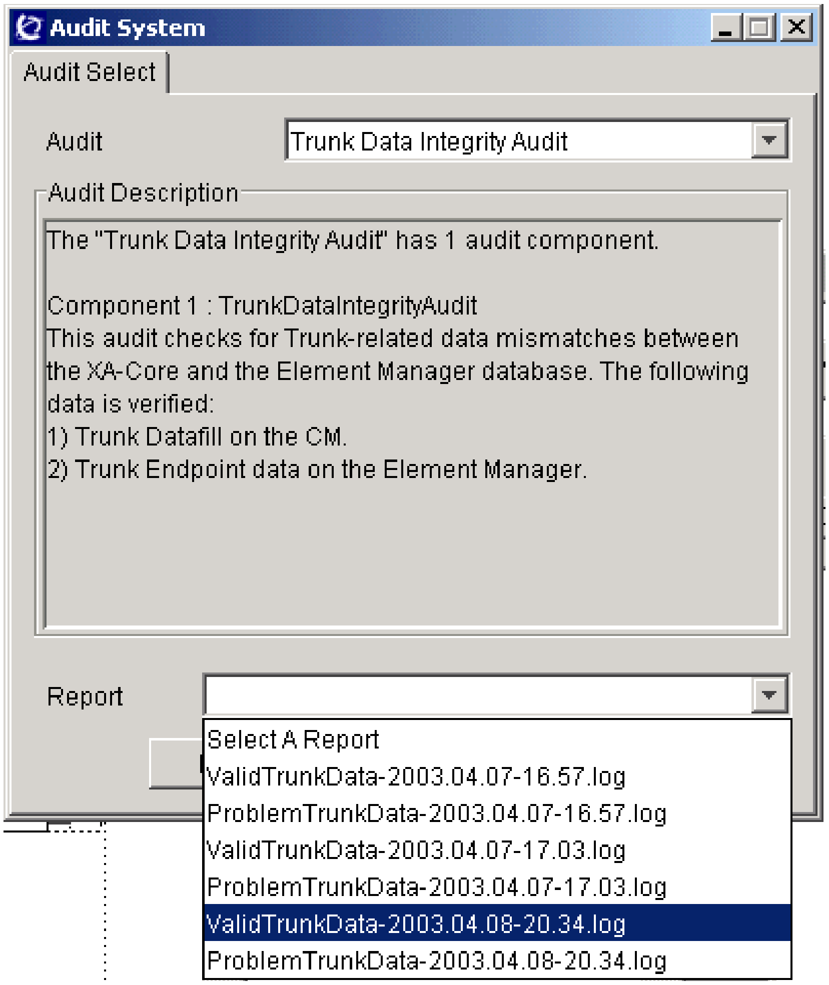
a Ensure that you have selected **Trunk Data Integrity Audit** from the Audit field drop-down menu at the top of the Audit System dialog box.

b Select **ValidTrunkData** from the drop-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.



Audit System
Audit Select

Audit: Trunk Data Integrity Audit

Audit Description

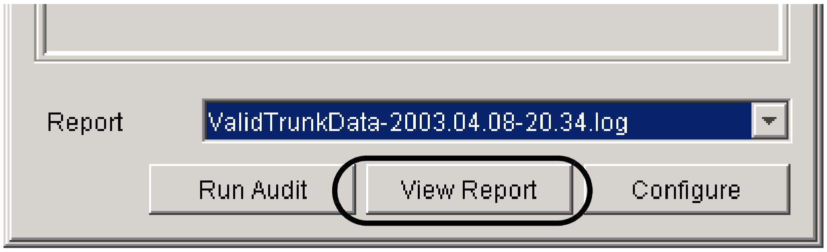
The "Trunk Data Integrity Audit" has 1 audit component.

Component 1 : TrunkDataIntegrityAudit
This audit checks for Trunk-related data mismatches between the XA-Core and the Element Manager database. The following data is verified:
1) Trunk Datafill on the CM.
2) Trunk Endpoint data on the Element Manager.

Report

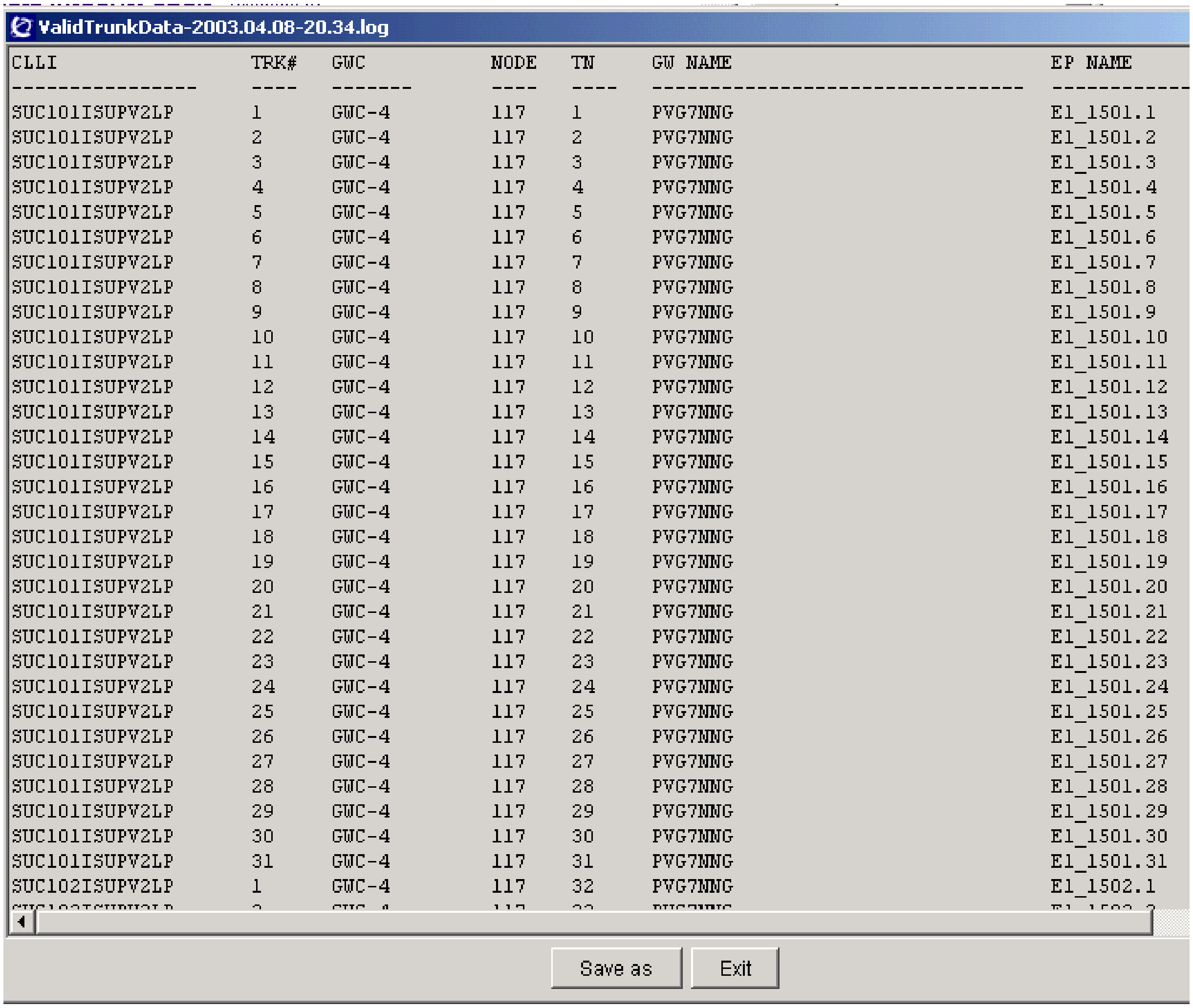
Select A Report
ValidTrunkData-2003.04.07-16.57.log
ProblemTrunkData-2003.04.07-16.57.log
ValidTrunkData-2003.04.07-17.03.log
ProblemTrunkData-2003.04.07-17.03.log
ValidTrunkData-2003.04.08-20.34.log
ProblemTrunkData-2003.04.08-20.34.log

c Click the **View Report** button.



Report ValidTrunkData-2003.04.08-20.34.log

The system displays the selected report. Here is an example of a “ValidTrunkData” report.



```
CLLI               TRK#   GWC          NODE   TN     GW NAME                                  EP NAME
----------------   ----   -------      ----   ----   ---------------------------------        ------------
SUC101ISUPV2LP     1      GWC-4        117    1      PVG7NNG                                  E1_1501.1
SUC101ISUPV2LP     2      GWC-4        117    2      PVG7NNG                                  E1_1501.2
SUC101ISUPV2LP     3      GWC-4        117    3      PVG7NNG                                  E1_1501.3
SUC101ISUPV2LP     4      GWC-4        117    4      PVG7NNG                                  E1_1501.4
SUC101ISUPV2LP     5      GWC-4        117    5      PVG7NNG                                  E1_1501.5
SUC101ISUPV2LP     6      GWC-4        117    6      PVG7NNG                                  E1_1501.6
SUC101ISUPV2LP     7      GWC-4        117    7      PVG7NNG                                  E1_1501.7
SUC101ISUPV2LP     8      GWC-4        117    8      PVG7NNG                                  E1_1501.8
SUC101ISUPV2LP     9      GWC-4        117    9      PVG7NNG                                  E1_1501.9
SUC101ISUPV2LP     10     GWC-4        117    10     PVG7NNG                                  E1_1501.10
SUC101ISUPV2LP     11     GWC-4        117    11     PVG7NNG                                  E1_1501.11
SUC101ISUPV2LP     12     GWC-4        117    12     PVG7NNG                                  E1_1501.12
SUC101ISUPV2LP     13     GWC-4        117    13     PVG7NNG                                  E1_1501.13
SUC101ISUPV2LP     14     GWC-4        117    14     PVG7NNG                                  E1_1501.14
SUC101ISUPV2LP     15     GWC-4        117    15     PVG7NNG                                  E1_1501.15
SUC101ISUPV2LP     16     GWC-4        117    16     PVG7NNG                                  E1_1501.16
SUC101ISUPV2LP     17     GWC-4        117    17     PVG7NNG                                  E1_1501.17
SUC101ISUPV2LP     18     GWC-4        117    18     PVG7NNG                                  E1_1501.18
SUC101ISUPV2LP     19     GWC-4        117    19     PVG7NNG                                  E1_1501.19
SUC101ISUPV2LP     20     GWC-4        117    20     PVG7NNG                                  E1_1501.20
SUC101ISUPV2LP     21     GWC-4        117    21     PVG7NNG                                  E1_1501.21
SUC101ISUPV2LP     22     GWC-4        117    22     PVG7NNG                                  E1_1501.22
SUC101ISUPV2LP     23     GWC-4        117    23     PVG7NNG                                  E1_1501.23
SUC101ISUPV2LP     24     GWC-4        117    24     PVG7NNG                                  E1_1501.24
SUC101ISUPV2LP     25     GWC-4        117    25     PVG7NNG                                  E1_1501.25
SUC101ISUPV2LP     26     GWC-4        117    26     PVG7NNG                                  E1_1501.26
SUC101ISUPV2LP     27     GWC-4        117    27     PVG7NNG                                  E1_1501.27
SUC101ISUPV2LP     28     GWC-4        117    28     PVG7NNG                                  E1_1501.28
SUC101ISUPV2LP     29     GWC-4        117    29     PVG7NNG                                  E1_1501.29
SUC101ISUPV2LP     30     GWC-4        117    30     PVG7NNG                                  E1_1501.30
SUC101ISUPV2LP     31     GWC-4        117    31     PVG7NNG                                  E1_1501.31
SUC102ISUPV2LP     1      GWC-4        117    32     PVG7NNG                                  E1_1502.1
```

Note 1: The CS 2000 Management Tools server retains the six most recent “ValidTrunkData” reports. When a new trunk audit occurs, the server deletes the oldest report.

Note 2: The system places trunk audit reports in the following directory on the CS 2000 Management Tools server: /opt/nortel/ptm/current/www/Audit/TrunkDataIntegrityAudit/.

d If you want to retain one of these reports for a longer time, or if you want to print a report, click 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.

7 To view the trunk problem-data report, proceed as follows:

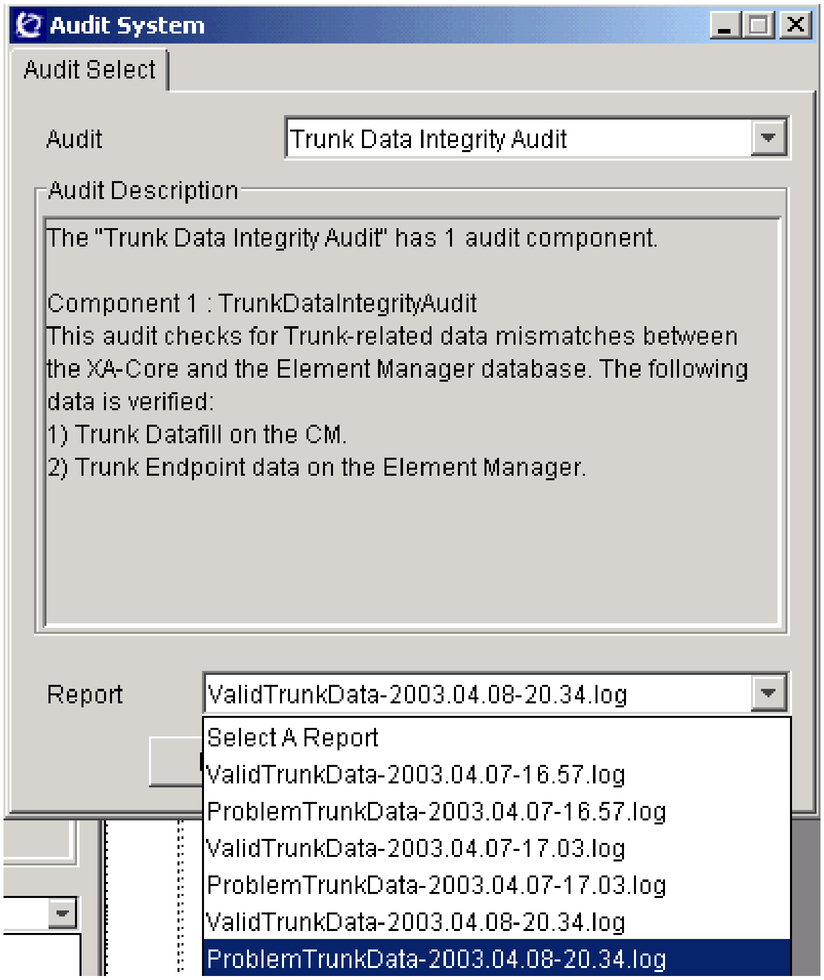
a Ensure that you have selected **Trunk Data Integrity Audit** from the Audit field drop-down menu at the top of the Audit system dialog box.

b Select **ProblemTrunkData** from the drop-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.



Audit: Trunk Data Integrity Audit

Audit Description

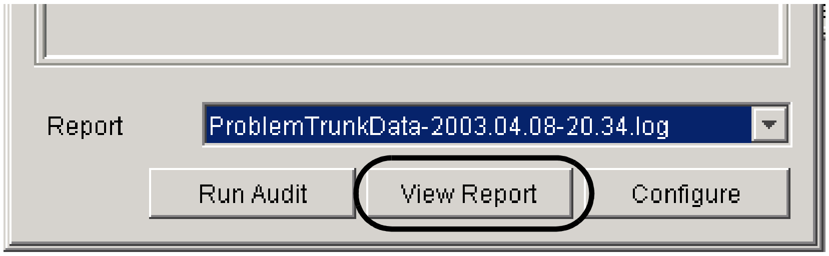
The "Trunk Data Integrity Audit" has 1 audit component.

Component 1 : TrunkDataIntegrityAudit
This audit checks for Trunk-related data mismatches between the XA-Core and the Element Manager database. The following data is verified:
1) Trunk Datafill on the CM.
2) Trunk Endpoint data on the Element Manager.

Report: ValidTrunkData-2003.04.08-20.34.log

```
Select A Report
ValidTrunkData-2003.04.07-16.57.log
ProblemTrunkData-2003.04.07-16.57.log
ValidTrunkData-2003.04.07-17.03.log
ProblemTrunkData-2003.04.07-17.03.log
ValidTrunkData-2003.04.08-20.34.log
ProblemTrunkData-2003.04.08-20.34.log
```

c Click the **View Report** button.



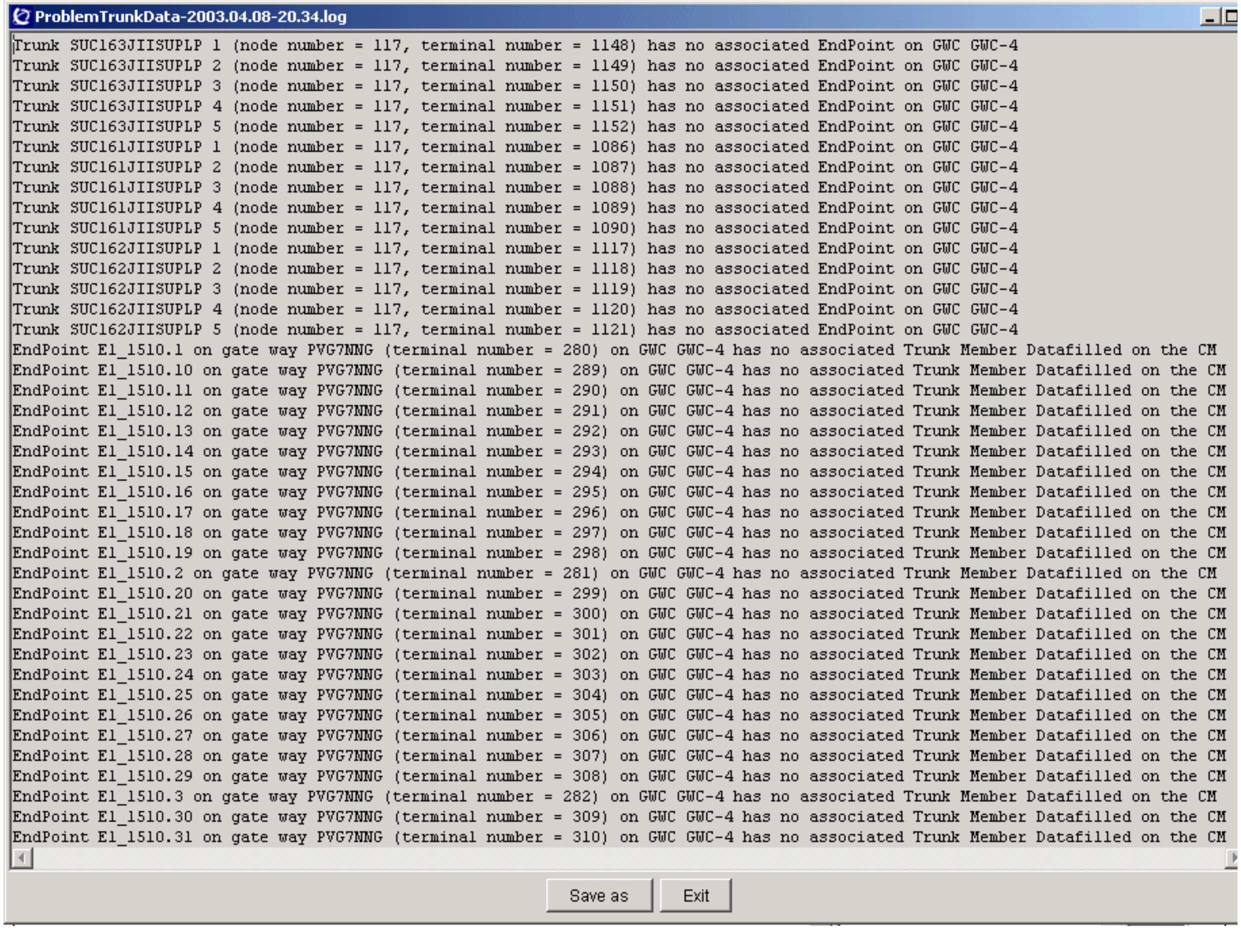
The system displays the selected report.

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 gate way <GW NAME> (terminal number = <TID>) on GWC <GWC ID> has no associated trunk member datafilled on the CM.

Here is an example of a “ProblemTrunkData” report:



```
Trunk SUC163JIISUPLP 1 (node number = 117, terminal number = 1148) has no associated EndPoint on GWC GWC-4
Trunk SUC163JIISUPLP 2 (node number = 117, terminal number = 1149) has no associated EndPoint on GWC GWC-4
Trunk SUC163JIISUPLP 3 (node number = 117, terminal number = 1150) has no associated EndPoint on GWC GWC-4
Trunk SUC163JIISUPLP 4 (node number = 117, terminal number = 1151) has no associated EndPoint on GWC GWC-4
Trunk SUC163JIISUPLP 5 (node number = 117, terminal number = 1152) has no associated EndPoint on GWC GWC-4
Trunk SUC161JIISUPLP 1 (node number = 117, terminal number = 1086) has no associated EndPoint on GWC GWC-4
Trunk SUC161JIISUPLP 2 (node number = 117, terminal number = 1087) has no associated EndPoint on GWC GWC-4
Trunk SUC161JIISUPLP 3 (node number = 117, terminal number = 1088) has no associated EndPoint on GWC GWC-4
Trunk SUC161JIISUPLP 4 (node number = 117, terminal number = 1089) has no associated EndPoint on GWC GWC-4
Trunk SUC161JIISUPLP 5 (node number = 117, terminal number = 1090) has no associated EndPoint on GWC GWC-4
Trunk SUC162JIISUPLP 1 (node number = 117, terminal number = 1117) has no associated EndPoint on GWC GWC-4
Trunk SUC162JIISUPLP 2 (node number = 117, terminal number = 1118) has no associated EndPoint on GWC GWC-4
Trunk SUC162JIISUPLP 3 (node number = 117, terminal number = 1119) has no associated EndPoint on GWC GWC-4
Trunk SUC162JIISUPLP 4 (node number = 117, terminal number = 1120) has no associated EndPoint on GWC GWC-4
Trunk SUC162JIISUPLP 5 (node number = 117, terminal number = 1121) has no associated EndPoint on GWC GWC-4
EndPoint E1_1510.1 on gate way PVG7NNG (terminal number = 280) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.10 on gate way PVG7NNG (terminal number = 289) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.11 on gate way PVG7NNG (terminal number = 290) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.12 on gate way PVG7NNG (terminal number = 291) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.13 on gate way PVG7NNG (terminal number = 292) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.14 on gate way PVG7NNG (terminal number = 293) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.15 on gate way PVG7NNG (terminal number = 294) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.16 on gate way PVG7NNG (terminal number = 295) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.17 on gate way PVG7NNG (terminal number = 296) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.18 on gate way PVG7NNG (terminal number = 297) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.19 on gate way PVG7NNG (terminal number = 298) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.2 on gate way PVG7NNG (terminal number = 281) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.20 on gate way PVG7NNG (terminal number = 299) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.21 on gate way PVG7NNG (terminal number = 300) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.22 on gate way PVG7NNG (terminal number = 301) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.23 on gate way PVG7NNG (terminal number = 302) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.24 on gate way PVG7NNG (terminal number = 303) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.25 on gate way PVG7NNG (terminal number = 304) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.26 on gate way PVG7NNG (terminal number = 305) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.27 on gate way PVG7NNG (terminal number = 306) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.28 on gate way PVG7NNG (terminal number = 307) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.29 on gate way PVG7NNG (terminal number = 308) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.3 on gate way PVG7NNG (terminal number = 282) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.30 on gate way PVG7NNG (terminal number = 309) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
EndPoint E1_1510.31 on gate way PVG7NNG (terminal number = 310) on GWC GWC-4 has no associated Trunk Member Datafilled on the CM
```

Note 1: The CS 2000 Management Tools server retains the six most recent “ProblemTrunkData” reports. When a new audit occurs, the server deletes the oldest report.

Note 2: The system places trunk audit reports in the following directory on the CS 2000 Management Tools server: /opt/nortel/ptm/current/www/Audit/TrunkDataIntegrityAudit/.

d If you want to retain one of these reports for a longer time, or print a report, click 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** 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 the **Exit** button at the bottom of the viewer screen.

8 This procedure is complete.

Perform a CS 2000 data integrity audit

Purpose of this procedure

Use this procedure to perform an on-demand data integrity audit of the CS 2000 GWC Manager database.

The audit compares the GWC Manager database with the CS 2000 XA Core database and flags any mismatches between the two databases. The XA Core is considered to hold the 'master' database. This procedure uses the audit system data integrity tool to perform the audit, view the results and take corrective action.

> ***Note:*** You can also schedule a CS 2000 data integrity audit using this tool. Refer to procedure "Configure a recurring data integrity audit" in the Gateway Controller Configuration Management NTP, NN10205-511.

Remedial actions offered are likely to involve deletion of inconsistent data. However, where possible the option to repair data inconsistencies will be given.

> ***Note:*** Starting in SN07, the CS 2000 data integrity audit compares the following data to highlight inconsistencies:
>
> - On the CS 2000 Management Tools server:
>   - Bearer network fabric type of each GWC node
>   - The network instance of each GWC node
> - On the XA-Core:
>   - The network instance and fabric type contained in the BEARNETS table
>   - The bearer network type for each GWC node contained in the SERVRINV table.
>
> If the audit detects any inconsistencies in this data, you will have the option to attempt to repair them.

When to use this procedure

Use this procedure when you are receiving logs or alarms in the CS 2000 XA Core or at the CS 2000 SAM21 Manager client indicating a possible provisioning error with a GWC card or node.

> ***Note 1:*** When the audit is running, suitable locks are in place that disable provisioning operations.

Note 2: The audit application keeps no record of problems that it has raised an alarm for. Therefore, if a problem is detected during an audit and not corrected, an alarm will be generated in the alarm manager for the same problem the next time the audit is run.

Note 3: If you have scheduled data integrity audits, remember that a maximum of one CS 2000 data integrity audit can be in progress at a time. An in-progress CS 2000 audit blocks all attempts to run CS 2000 audits. If you run an on-demand CS 2000 audit, and if that audit is still in progress at the start time of a scheduled CS 2000 audit, the scheduled audit will not occur.

Prerequisites

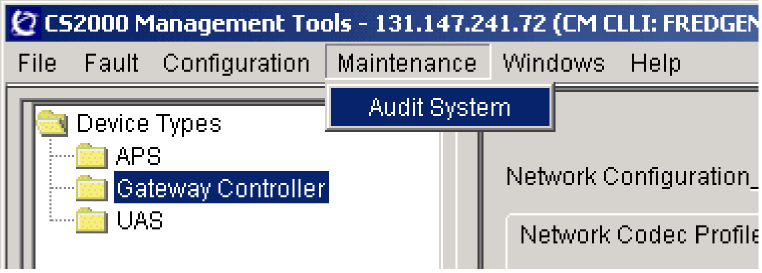
Ensure that no provisioning activities are scheduled to take place during the audit.

Unlike the line and trunk audits, the data integrity audit does not provide an option to save the audit report to a file on the local disk.

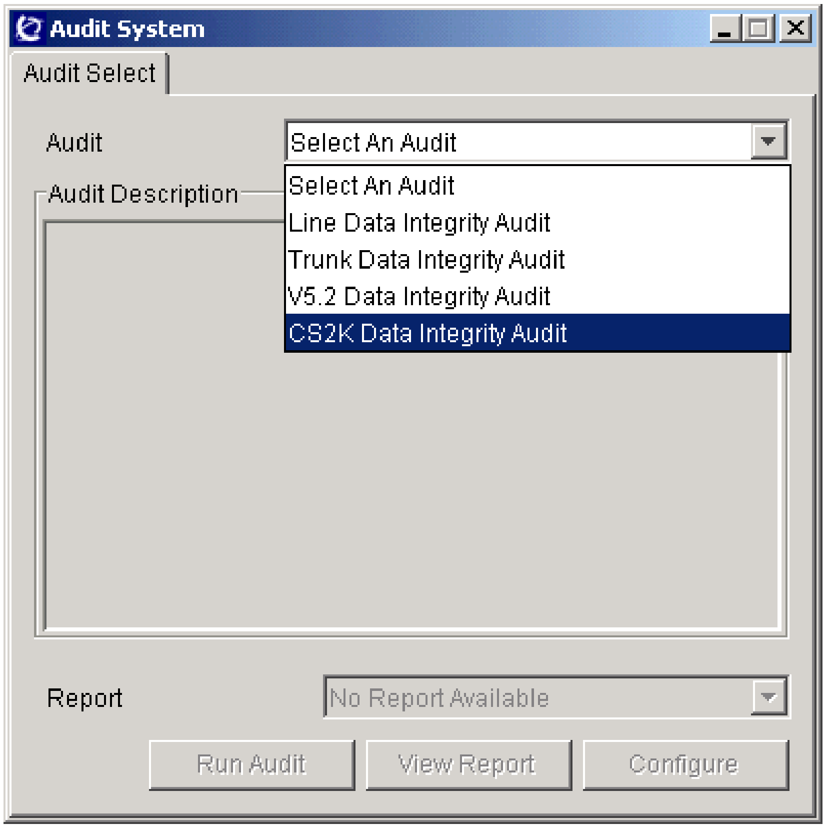
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, select **Maintenance**, and then **Audit System**.



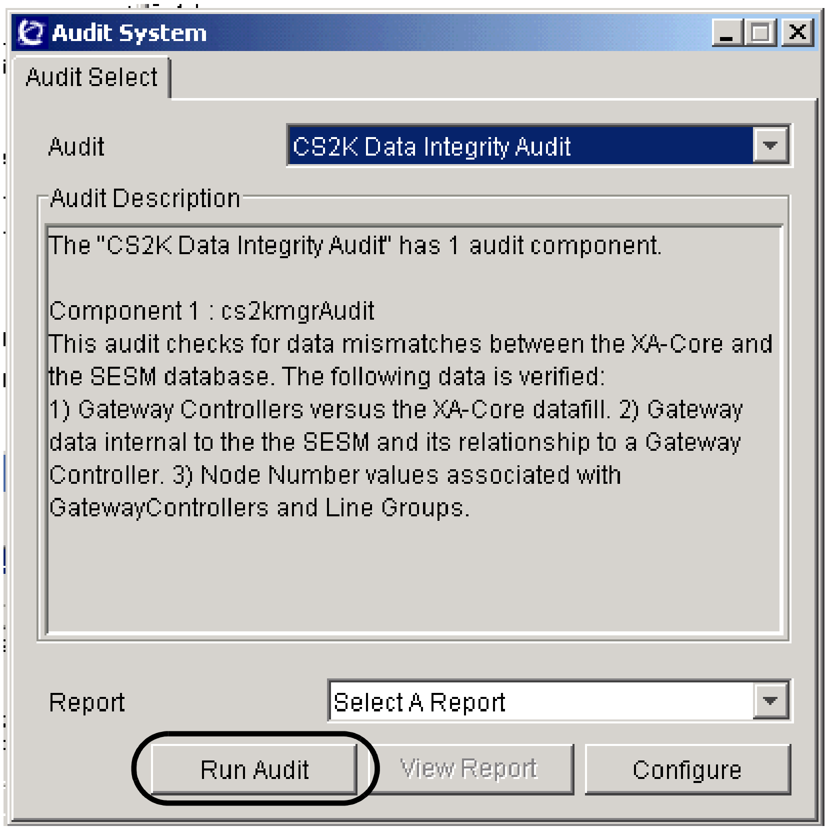
2 At the Audit System dialog box, select **CS2K Data Integrity Audit** from list of audits displayed in the drop-down menu.



3 Select the next step as follows.

If you want to	Do
perform a CS 2000 audit and view the results of the audit	step 4 and complete the procedure
view the results of a CS 2000 audit that has finished running and resolve problems	step 6 and complete the procedure

4 Click the **Run Audit** button to start the audit.



Audit: CS2K Data Integrity Audit

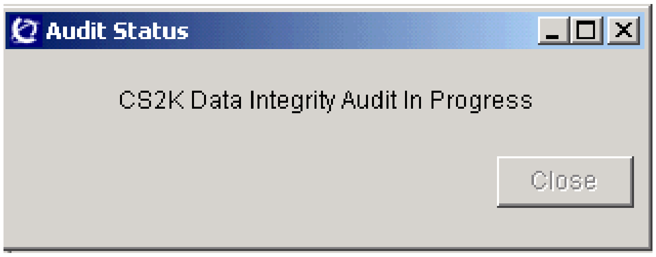
Audit Description

The "CS2K Data Integrity Audit" has 1 audit component.

Component 1 : cs2kmgrAudit
This audit checks for data mismatches between the XA-Core and the SESM database. The following data is verified:
1) Gateway Controllers versus the XA-Core datafill. 2) Gateway data internal to the the SESM and its relationship to a Gateway Controller. 3) Node Number values associated with GatewayControllers and Line Groups.

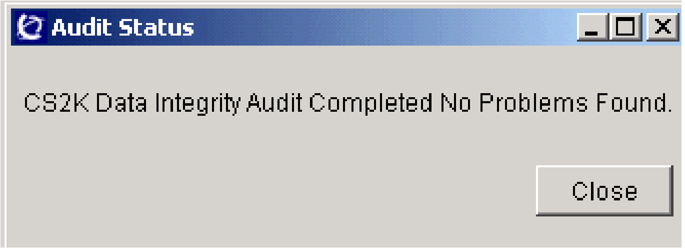
Report: Select A Report

During a CS 2000 audit, the system displays the following message:

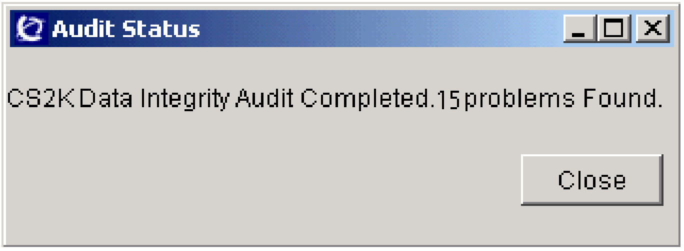


CS2K Data Integrity Audit In Progress

The audit may take a few minutes to complete. When the audit is successfully completed, the system displays one of two types of messages as follows:



CS2K Data Integrity Audit Completed No Problems Found.



CS2K Data Integrity Audit Completed.15problems Found.

> ***Note:*** If the audit does not execute successfully, the message “CS2K Data Integrity Audit Failed to Complete” is displayed with an error message indicating the reason. Contact your next level of support to resolve the problem.

5 Click the **Close** button to close the Audit Status pop-up window.

6 To view a CS 2000 audit report, proceed as follows:

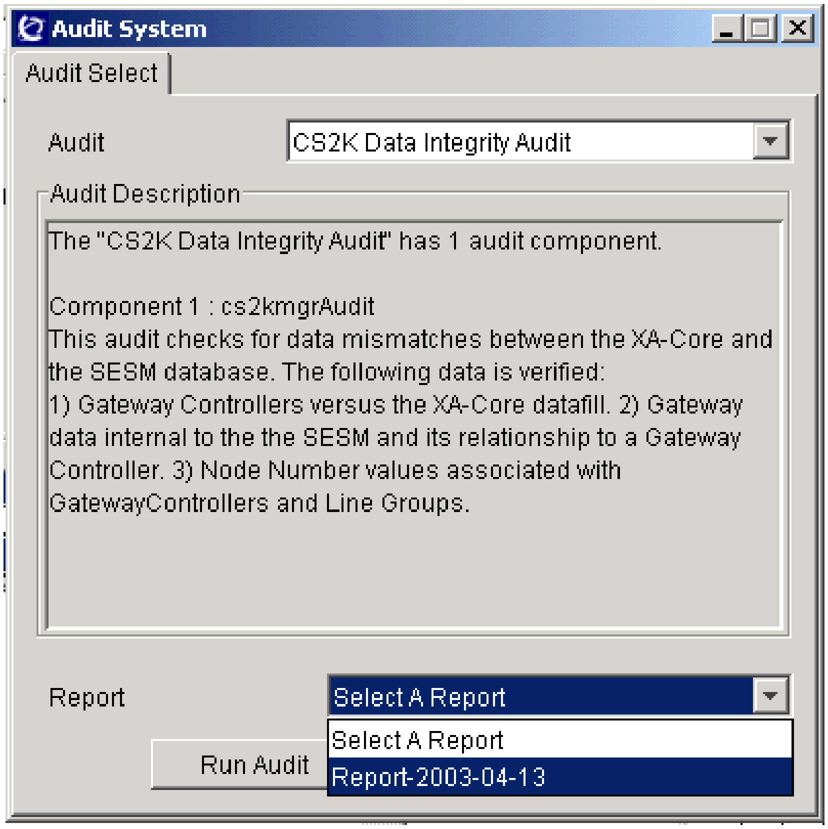
a Ensure that you have selected **CS2K Data Integrity Audit** from the Audit field drop-down menu at the top of the Audit System dialog box.

b Select **Report** <date> from the drop-down menu in the Report field at the bottom of the dialog box.

The file name has the following format:

Report-<date>

where
<date> is the date in yyyy-mm-dd format, for example, 2003-02-15.



Audit: CS2K Data Integrity Audit

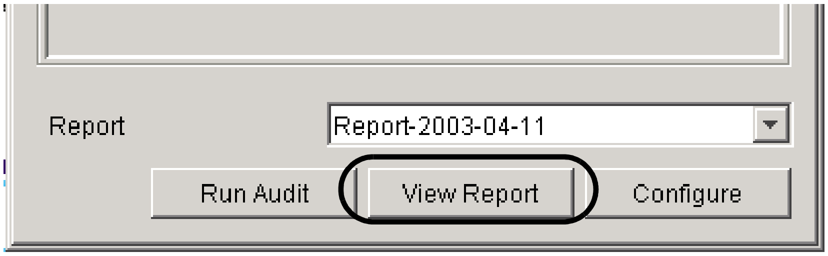
Audit Description

The "CS2K Data Integrity Audit" has 1 audit component.

Component 1 : cs2kmgrAudit
This audit checks for data mismatches between the XA-Core and the SESM database. The following data is verified:
1) Gateway Controllers versus the XA-Core datafill. 2) Gateway data internal to the the SESM and its relationship to a Gateway Controller. 3) Node Number values associated with GatewayControllers and Line Groups.

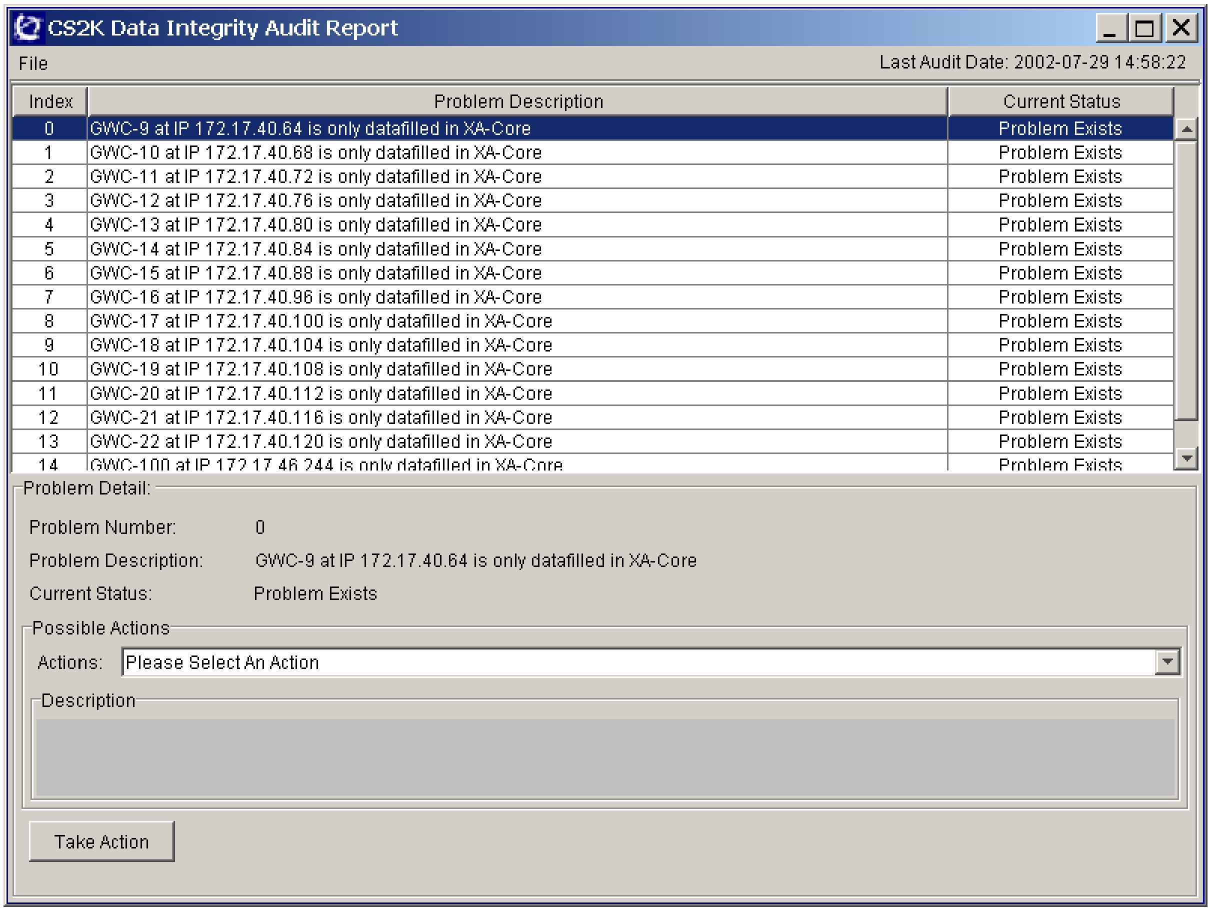
Report: Select A Report

c Click the **View Report** button.



Report: Report-2003-04-11

The system displays the selected report. If no problems were discovered, the report will be empty. Here is an example of a report containing problems:



CS2K Data Integrity Audit Report

Last Audit Date: 2002-07-29 14:58:22

Index	Problem Description	Current Status
0	GWC-9 at IP 172.17.40.64 is only datafilled in XA-Core	Problem Exists
1	GWC-10 at IP 172.17.40.68 is only datafilled in XA-Core	Problem Exists
2	GWC-11 at IP 172.17.40.72 is only datafilled in XA-Core	Problem Exists
3	GWC-12 at IP 172.17.40.76 is only datafilled in XA-Core	Problem Exists
4	GWC-13 at IP 172.17.40.80 is only datafilled in XA-Core	Problem Exists
5	GWC-14 at IP 172.17.40.84 is only datafilled in XA-Core	Problem Exists
6	GWC-15 at IP 172.17.40.88 is only datafilled in XA-Core	Problem Exists
7	GWC-16 at IP 172.17.40.96 is only datafilled in XA-Core	Problem Exists
8	GWC-17 at IP 172.17.40.100 is only datafilled in XA-Core	Problem Exists
9	GWC-18 at IP 172.17.40.104 is only datafilled in XA-Core	Problem Exists
10	GWC-19 at IP 172.17.40.108 is only datafilled in XA-Core	Problem Exists
11	GWC-20 at IP 172.17.40.112 is only datafilled in XA-Core	Problem Exists
12	GWC-21 at IP 172.17.40.116 is only datafilled in XA-Core	Problem Exists
13	GWC-22 at IP 172.17.40.120 is only datafilled in XA-Core	Problem Exists
14	GWC-100 at IP 172.17.46.244 is only datafilled in XA-Core	Problem Exists

Problem Detail:

Problem Number: 0

Problem Description: GWC-9 at IP 172.17.40.64 is only datafilled in XA-Core

Current Status: Problem Exists

Possible Actions

Actions: Please Select An Action

Description

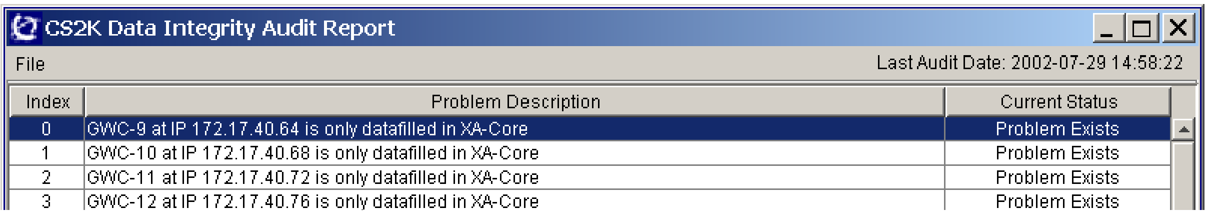
Note 1: The CS 2000 Management Tools server retains the most recent CS 2000 audit report. When a new audit occurs, the server deletes the previous report.

Note 2: The system places the audit report in the following directory on the CS 2000 Management Tools server: /opt/nortel/ptm/current/MI2/apps/Audit.

Note 3: The CS 2000 GWC Manager does not provide an option to save a CS 2000 data audit report to local disk.

7 Review the results of the audit and select a problem to resolve.

Note: If necessary, resize the entire window to completely view the Problem Description field.



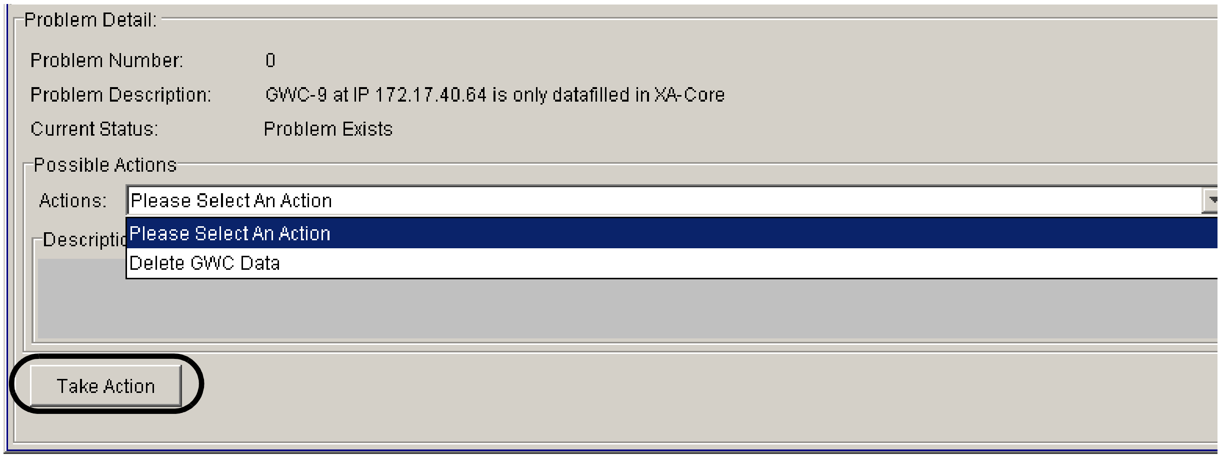
Last Audit Date: 2002-07-29 14:58:22

Index	Problem Description	Current Status
0	GWC-9 at IP 172.17.40.64 is only datafilled in XA-Core	Problem Exists
1	GWC-10 at IP 172.17.40.68 is only datafilled in XA-Core	Problem Exists
2	GWC-11 at IP 172.17.40.72 is only datafilled in XA-Core	Problem Exists
3	GWC-12 at IP 172.17.40.76 is only datafilled in XA-Core	Problem Exists

8 Evaluate actions to resolve a problem and take action.

a Click and hold on the Action drop-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.



Problem Number: 0
Problem Description: GWC-9 at IP 172.17.40.64 is only datafilled in XA-Core
Current Status: Problem Exists
Actions: Please Select An Action

c Click the **Take Action** button

Note: If you see the message "Correction Failed", please contact your next level of support.

9 Return to step 7 to review another problem.

10 This procedure is complete.

Perform a GWC V5.2 data integrity audit

Purpose of this procedure

Use this procedure to perform an on-demand data integrity audit of V5.2 interfaces.

A V5.2 data integrity audit 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 Manger database
- V5.2 interface data stored in the table GPPTRNSL in the CS 2000 XA-Core database

This procedure uses the audit system data integrity tool to perform the audit, view the results and take corrective action.

> ***Note:*** You can also schedule a V5.2 data integrity audit using this tool. Refer to procedure “Configure a recurring data integrity audit” in the Gateway Controller Configuration Management NTP, NN10205-511.

Remedial actions offered are likely to involve deletion of inconsistent data. However, where possible, the option to repair data inconsistencies will be offered.

When to use this procedure

Use this procedure to check for defective data after you have done V5.2 interface provisioning, or if you suspect there is a problem with V5.2 provisioning.

> ***Note 1:*** When the audit is running, suitable locks are in place that disable provisioning operations.
>
> ***Note 2:*** The audit application keeps no record of problems that it has raised an alarm for. Therefore, if a problem is detected during an audit and not corrected, an alarm will be generated in the alarm manager for the same problem the next time the audit is run.
>
> ***Note 3:*** If you have scheduled data integrity audits, remember that a maximum of one V5.2 interface audit can be in progress at a time. An in-progress V5.2 interface audit blocks all attempts to run V5.2 audits. If you run an on-demand V5.2 audit, and if that audit is still in progress at the start time of a scheduled V5.2 audit, the scheduled audit will not occur.

Prerequisites

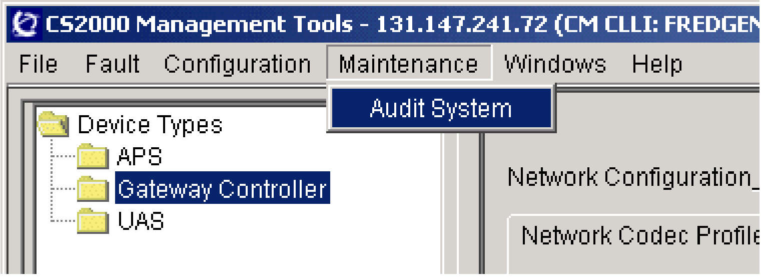
Ensure that no provisioning activities are scheduled to take place during the audit.

Unlike the line and trunk audits, the V5.2 data integrity audit does not provide an option to save the audit report to a file on the local disk.

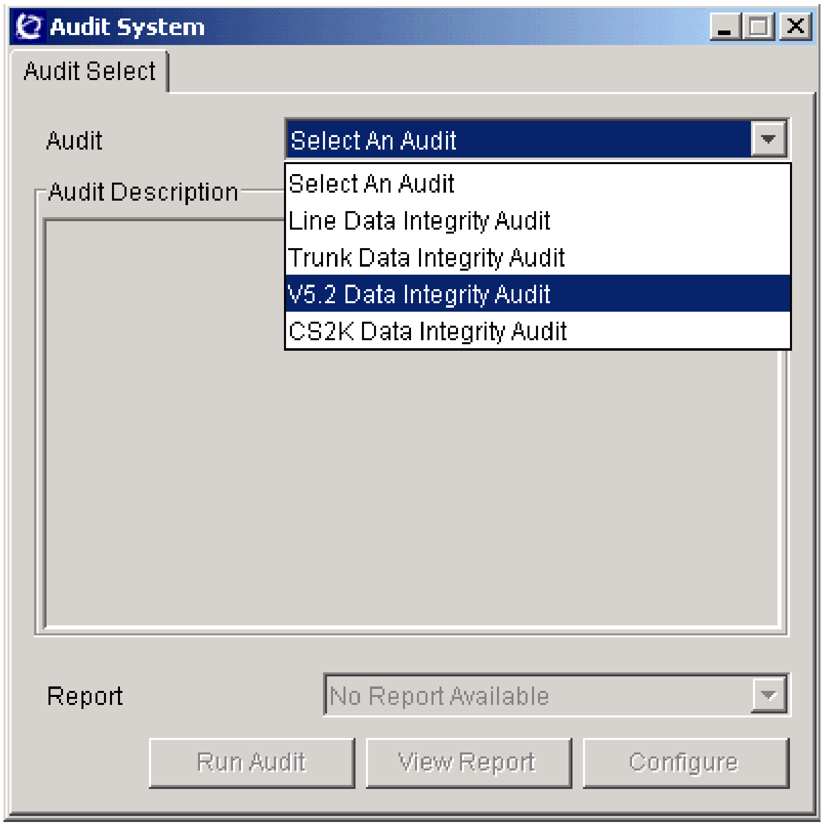
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, select **Audit System** from the Maintenance menu.


CS2000 Management Tools - 131.147.241.72 (CM CLLI: FREDGEN
File Fault Configuration Maintenance Windows Help
Audit System
Device Types
APS
Gateway Controller
UAS
Network Configuration_
Network Codec Profile

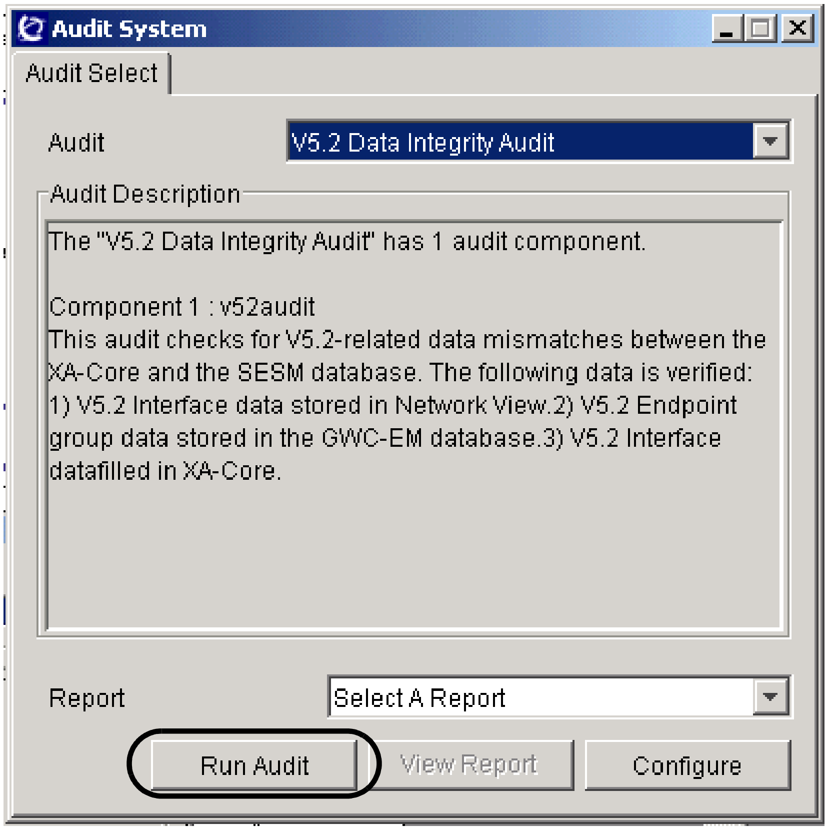
2 At the Audit System dialog box, select **V5.2 Data Integrity Audit** from list of audits displayed in the drop-down menu.



3 Select the next step as follows.

If you want to	Do
perform a V5.2 interface audit, view the results of the audit and resolve problems	step 4 and complete the procedure
view the results of a V5.2 interface audit that has finished running and resolve problems	step 6 and complete the procedure

4 Click the **Run Audit** button to start the audit.



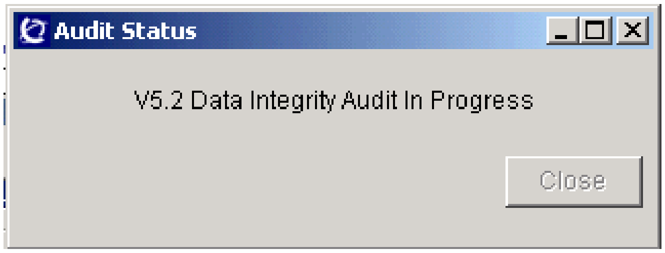
Audit: V5.2 Data Integrity Audit

The "V5.2 Data Integrity Audit" has 1 audit component.

Component 1 : v52audit
This audit checks for V5.2-related data mismatches between the XA-Core and the SESM database. The following data is verified: 1) V5.2 Interface data stored in Network View.2) V5.2 Endpoint group data stored in the GWC-EM database.3) V5.2 Interface datafilled in XA-Core.

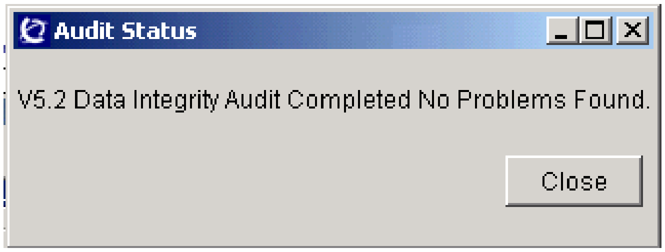
Report: Select A Report

During a V5.2 data integrity audit, the system displays the following message:

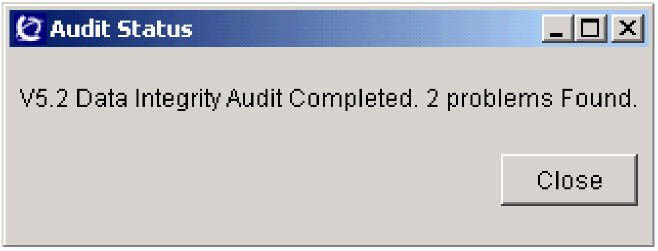


V5.2 Data Integrity Audit In Progress

The audit may take a few minutes to complete. When the audit is successfully completed, the system displays one of two types of messages as follows:



V5.2 Data Integrity Audit Completed No Problems Found.



V5.2 Data Integrity Audit Completed. 2 problems Found.

Note: If the audit does not execute successfully, the message “V5.2 Data Integrity Audit Failed to Complete” is displayed with an error message indicating the reason. Contact your next level of support to resolve the problem.

5 Click the **Close** button to close the Audit Status pop-up window.

6 To view a V5.2 audit report, proceed as follows:

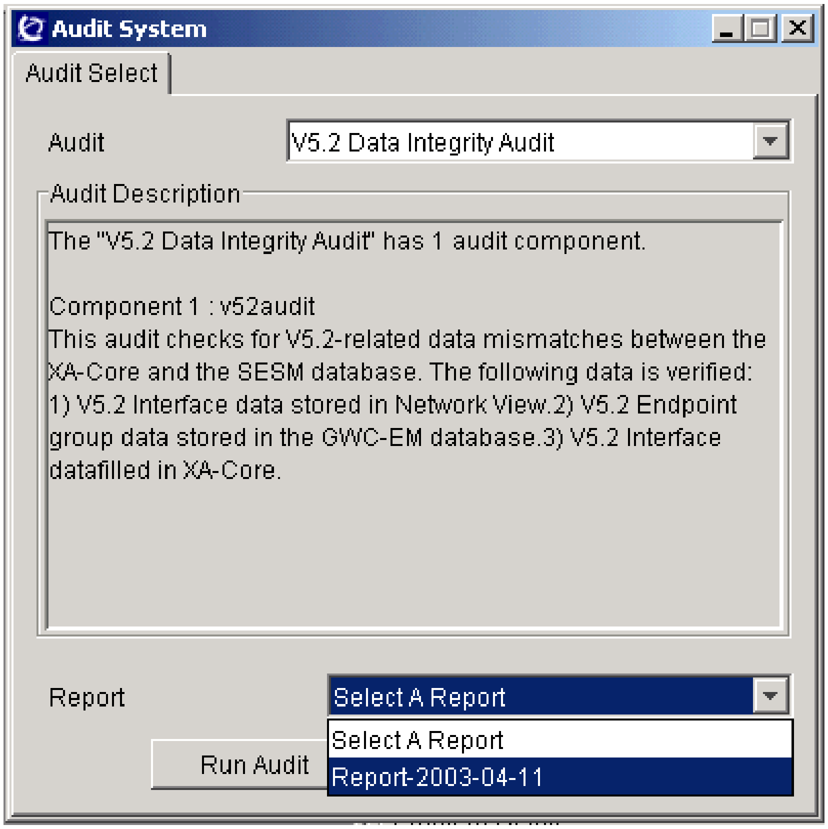
a Ensure that you have selected **V5.2 Data Integrity Audit** from the Audit field drop-down menu at the top of the Audit System dialog box.

b Select **Report** <date> from the drop-down menu in the Report field at the bottom of the dialog box.

The file name has the following format:

Report-<date>

where
<date> is the date in yyyy-mm-dd format, for example, 2003-02-15.



Audit: V5.2 Data Integrity Audit

Audit Description

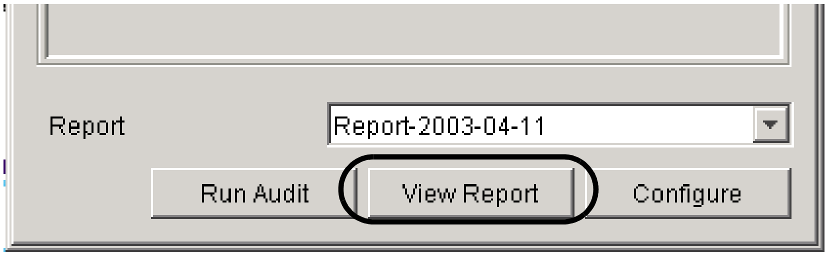
The "V5.2 Data Integrity Audit" has 1 audit component.

Component 1 : v52audit
This audit checks for V5.2-related data mismatches between the XA-Core and the SESM database. The following data is verified: 1) V5.2 Interface data stored in Network View.2) V5.2 Endpoint group data stored in the GWC-EM database.3) V5.2 Interface datafilled in XA-Core.

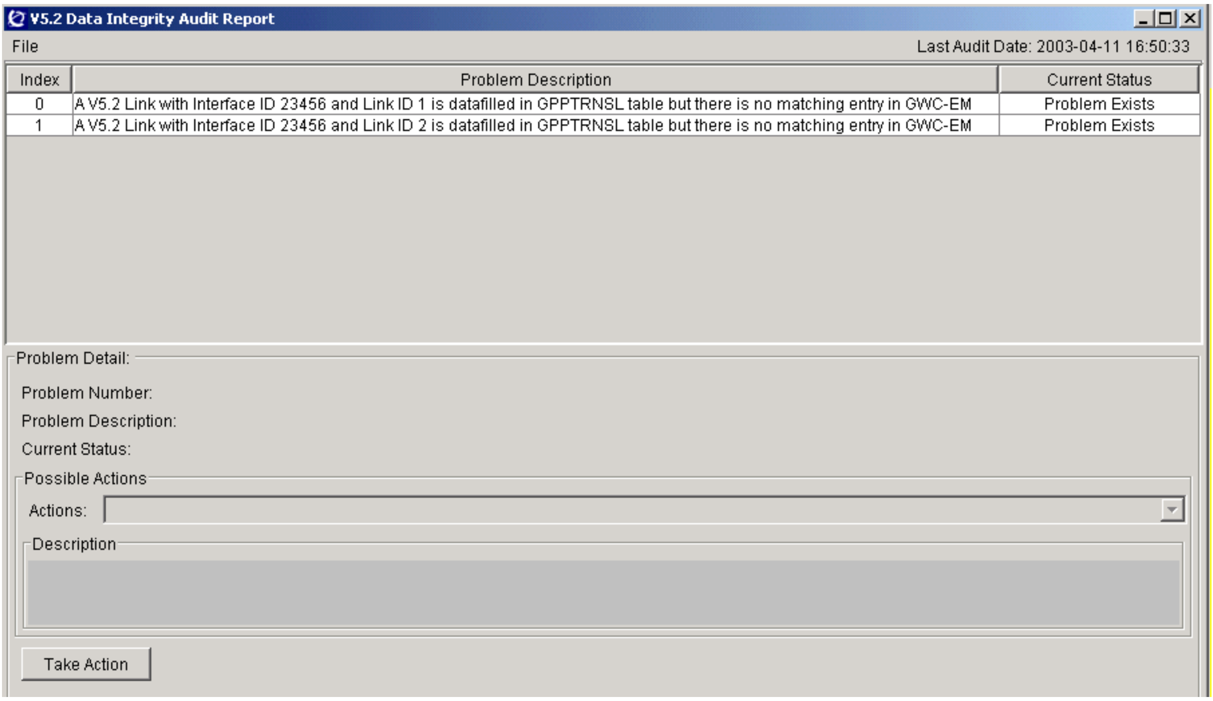
Report: Select A Report

Select A Report
Report-2003-04-11

c Click the **View Report** button.



The system displays the selected report. If no problems were discovered, the report will be empty. Here is an example of a report in which two problems were discovered:



Last Audit Date: 2003-04-11 16:50:33

Index	Problem Description	Current Status
0	A V5.2 Link with Interface ID 23456 and Link ID 1 is datafilled in GPPTRNSL table but there is no matching entry in GWC-EM	Problem Exists
1	A V5.2 Link with Interface ID 23456 and Link ID 2 is datafilled in GPPTRNSL table but there is no matching entry in GWC-EM	Problem Exists

Note 1: The CS 2000 Management Tools server retains the most recent CS 2000 audit report. When a new audit occurs, the server deletes the previous report.

Note 2: The system places the audit report in the following directory on the CS 2000 Management Tools server: /opt/nortel/ptm/current/MI2/apps/Audit.

Note 3: The CS 2000 GWC Manager does not provide an option to save a V5.2 audit report to local disk.

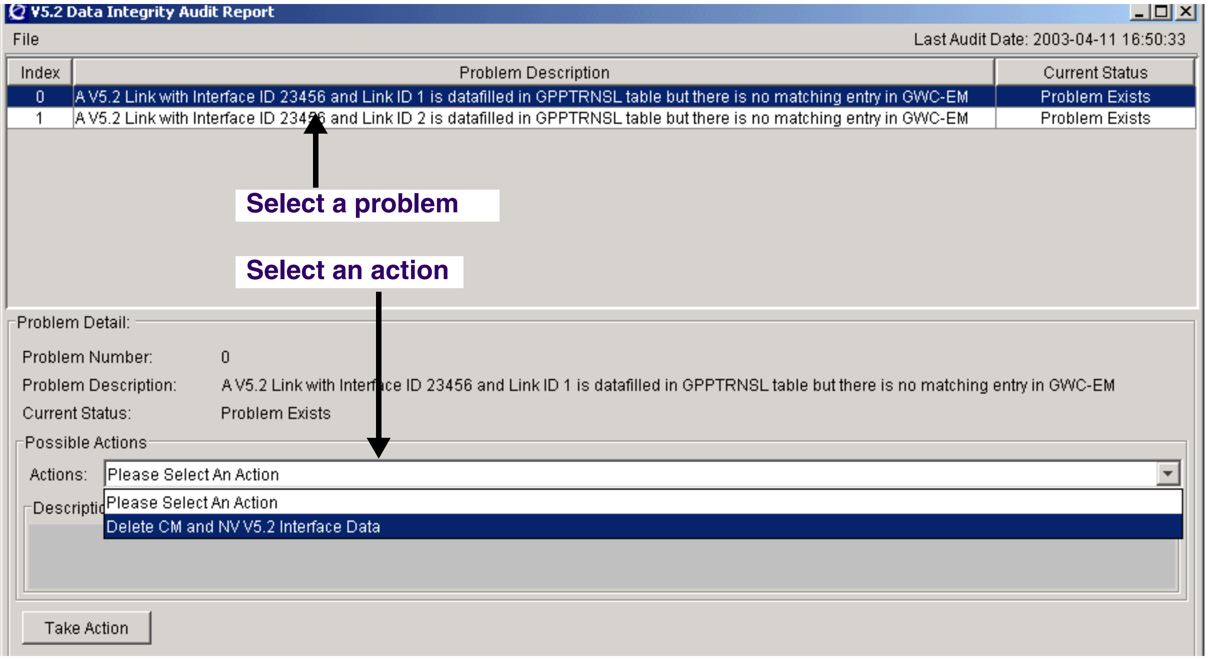
7 Review the results of the audit and select a problem to resolve.

Note: If necessary, resize the entire window to completely view the Problem Description field.

8 Evaluate actions to resolve a problem and take action.

a Click and hold on the Action drop-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.



V5.2 Data Integrity Audit Report

File

Last Audit Date: 2003-04-11 16:50:33

Index	Problem Description	Current Status
0	A V5.2 Link with Interface ID 23456 and Link ID 1 is datafilled in GPPTRNSL table but there is no matching entry in GWC-EM	Problem Exists
1	A V5.2 Link with Interface ID 23456 and Link ID 2 is datafilled in GPPTRNSL table but there is no matching entry in GWC-EM	Problem Exists

Select a problem

Select an action

Problem Detail:

Problem Number: 0

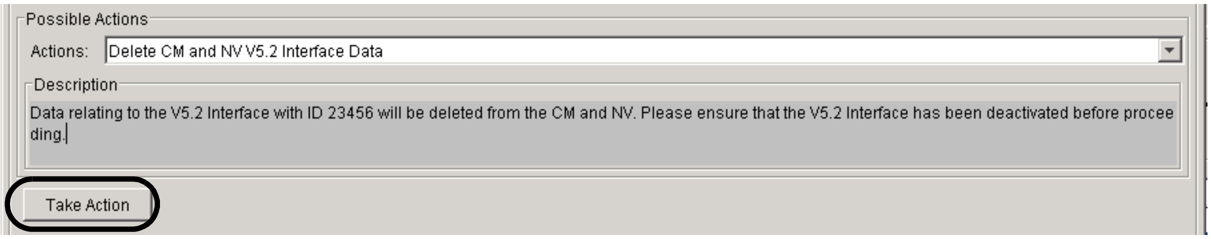
Problem Description: A V5.2 Link with Interface ID 23456 and Link ID 1 is datafilled in GPPTRNSL table but there is no matching entry in GWC-EM

Current Status: Problem Exists

Possible Actions

Actions: Please Select An Action

c Click the **Take Action** button



Possible Actions

Actions: Delete CM and NV V5.2 Interface Data

Description

Data relating to the V5.2 Interface with ID 23456 will be deleted from the CM and NV. Please ensure that the V5.2 Interface has been deactivated before proceeding.

Note: If you see the message “Correction Failed”, please contact your next level of support.

9 Return to step 7 to review another problem.

10 This procedure is complete.

Review GWC V5.2 audit logs and investigate problems

Purpose of this procedure

Use this procedure to perform troubleshooting activities on the GWC or a related component in response to a particular V5.2 fault log.

There are a number of GWC-related log types that are specific to V5.2 lines maintenance. V5.2 audit logs are generated to capture regular maintenance test results made to associated V5.2 media gateways and access nodes. The BCC audit verifies a possible mismatch between GWC and AN while the V5CC audits verify a possible mismatch CM and GWC. See the relationship as follows:

- V5 BCC Audit
- V5CC Audit
  - V5 Interface Audit
  - V5 Link Audit
  - V5 C-channels Audit
  - V5 Data Link Audit

When to use this procedure

Use this procedure when the log presented requires action to resolve, or when other faults with associated components are involved.

Prerequisites

Before executing this procedure ensure that you have executed procedure View GWC PM logs on page 53.

Action

Investigate problems using V5.2 audit logs.

Use table V5.2 logs to review the details of the log type displayed by your log utility and formulate the appropriate actions to diagnose and repair the problem.

> ***Note:*** For additional reference information about V5.2 logs, refer to the appropriate V5.2 log description in this NTP.

V5.2 logs (Sheet 1 of 4)

Log type; Problem logged	Reason for failure	Details
V5200 (BCC Audit fails) V5201 (BCC Audit message) V5202 (BCC Audit incomplete)	Generated when an AN (access node) does not respond to a BCC Audit message. Generated when an audit message is sent from the CM to an access node. Generated during a BCC (bearer channel control) audit, when the returned “Audit Complete” message includes the information element “Connection Incomplete”.	The BCC audit allows checking of a possible mismatch between GWC and access node (AN). It is executed when the AN sends a *BCC Reject* message to the GWC, upon receiving BCC Allocation. There are several reject causes, which are given in the BCC Reject message. Some of those reject causes will make the GWC send a BCC Audit to the AN. • Connection already present at the PSTN user port to a different V5 time slot (0x83) • Connection already present at the V5 time slot(s) to a different port or ISDN user port time slot (0x84) • Connection already present at the ISDN user port time slot(s) to a different V5 time slot(s) (0x85) • Deallocation cannot be completed due to V5 time slot(s) data incompatibility (0x88) • Deallocation cannot be completed due to port data incompatibility (0x89) • Deallocation cannot be completed - user port time slot(s) data incompatibility (0x8A)

V5.2 logs (Sheet 2 of 4)

Log type; Problem logged	Reason for failure	Details
V5400 (V5CC Audit)	Generated when there is no reply from the V5 interface for the V5 audit queries during V5CC audit.	V5CC interface audit is the only audit executed if an interface in the deactivated status. The V5CC (channel control) Audit performs consistency checks for various interface, link and line statuses. When the GWC is not in service, when a GWC startup/activation process takes place or when in a GWC is in a maintenance in-progress state, a V5CC audit will not be executed. V5 interfaces will be audited in the following order: • V5 interface audit • V5 link audit • V5 c-channel audit • V5 data link audit • V5 babbling lines audit • V5 line state audit An interface will receive audit queries every 10 minutes.
V5401 (V5 Interface Audit)	Generated when a mismatch is detected by the CM for a queried V5 interface on a GWC.	During a V5CC audit, the CM sends a V5 interface query to an interface on a GWC, the query message requests the status of the interface on the GWC. The GWC will send a response message upon receiving a V5 interface query message with the status of the corresponding interface (either ACT or DEACT). If a mismatch is detected, the CM will request the GWC to change the status of the interface to that held on the CM.

V5.2 logs (Sheet 3 of 4)

Log type; Problem logged	Reason for failure	Details
V5402 (V5 Link Audit)	Generated when a mismatch is detected by the CM for a queried V5 link on a GWC.	During a V5CC audit, a V5 link audit is performed. When the GWC sends a reply message, which contains the status of the links, the CM will check the status of the link carrier and compare it with the status of a carrier flag. In case of mismatch of carrier flag, the CM will send a message to GWC in order to open or close scanning on the given link, respectively.
V5403 (V5 C-channels Audit)	Generated when a mismatch occurs between the status of the C-channel as recorded in the GWC and in the CM.	The CM sends a V5 C-channel audit to a GWC to request the C-channel information on the GWC. No action is taken on the GWC side. After receiving the response message from GWC, the CM looks for the following: • C-channel status mismatch (INSV/OOS) • C-channel activity mismatch (ACT/STBY) • C-channel static data mismatch In all cases of mismatch, the C-channel status on the CM will be updated according to the status held on the GWC. No additional maintenance request is needed upon mismatch detection.

V5.2 logs (Sheet 4 of 4)

Log type; Problem logged	Reason for failure	Details
V5404 (Data Link Audit)	Generated when a mismatch occurs between the status of the data links as recorded in the GWC and in the CM.	The CM sends a V5 data link audit message to a GWC to request a data link status on the GWC. No action is taken on the GWC side. The GWC will send a response message which contains the current data link status. The data link status consists of CTRL, PSTN, BCC, LNK_CTRL, PROT1 and PROT2 statuses. After receiving a response message from GWC, the CM will look for a mismatch, In case of mismatch, the appropriate alarm status on the CM will be updated according to the status of the data link. Additional maintenance requests to reset (MANRTS) or block (MANBSY) all V5 lines is sent upon mismatch detection. Log V5404 will be generated in case of a mismatch.

PM180

Log report PM180 appears when the system encounters a software exception. A software exception occurs when software is not used correctly. Operating company personnel use log report PM180 to identify and correct software errors. A software exception that relates to hardware can also generate log report PM180.

The PM subsystem generates this report when a software condition occurs. This software condition affects normal operation of the DMS or the peripherals of the DMS. Formats 3 and 4 supply information on a PM EXCEPTION REPORT. Format 5 identifies software exceptions in the remote line concentrating module with extended distance capability (RLCM-EDC) and the universal edge 9000 (UE9000).

Format

The format for log report PM180 is as follows:

```
PM180 mmmdd hh:mm:ss ssdd TBL PM EXCEPTION REPORT
   pmid UNIT n: acttxt
   TASKID : taskid, TIME: hhhhhhhh, COMID: comid
   TEXT: swerrtxt hh hh hh hh hh hh hh
   CONTEXT TERMINAL: TID=(nodenum,termnum), EXTBYTE=n,
   AGENT=CKT trkid
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
TBL PM EXCEPTION REPORT	Constant	Indicates a PM exception report.
pmid	Symbolic text	Identifies the affected PM
UNIT	Integer (0 or 1)	Identifies the PM unit that generates the report
acttxt	Act	Indicates that the PM unit is active (Act). Not provided for digital line module (DLM).
	Inact	Indicates that the PM unit is inactive (Inact). Not provided for DLM.
TASKID	Symbolic text	Provides identification for suspect task

Field	Value	Description
TIME	Hex (0000-FFFF)	Indicates time that exception occurred
COMID	Hex (0000-FFFF), Character string	Provides communication port identification. Not provided for DLM.
swerrtxt	Character string	Provides the reason for the exception.
hhhh	Hex (0000-FFFF)	The 14 hexadecimal characters display contents of process status word for DLMs. The hexadecimal characters display more than 14 characters in the hhhh format to display the following: • contents of process status word • different registers • other information used in troubleshooting
CONTEXT TERMINAL	Constant	Indicates the information that follows applies to the terminal involved in the transaction that produced the exception condition. Not provided for DLM.
TID	Integers	Provides the node number and terminal number for terminal identification. Not provided for DLM.
EXTBYTE5000	0 or 1	Identifies the extension byte of the call involved in the exception condition. Electronic business sets use the extension byte to distinguish directory number (DN) keys. For 500 series and 2500 series sets and for trunks, the field does not apply and is set to zero. Not provided for DLM.
AGENT	Symbolic text	Provides identification for context terminal equipment. Not provided for DLM.
TEXT	CMR CARD TROUBLE	Indicates the system detected a problem on the CLASS modem resource (CMR) card. The system attempts to reset the card. Report that this log occurred.
	Character string or blank	Provides additional information for operating company personnel to isolate problems
hhhh	Hex (0000-FFFF)	Provides a dump of information for operating company personnel to use
Text string	Alphabetic	Provides the reason of the exception

Field	Value	Description
Software Exception	Character string	Provides the reason for the log
Processor ID	MP, CP, or PP	Indicates that the processor in the RLCM-EDC or the UE9000 that generates the report is one of the following: • master processor • control side (C-side) • peripheral processor (P-side)
Task ID	Symbolic text	Identifies the ID of the RLCM-EDC or the UE9000 task that generated the log
Time	00 00-2359	Indicates the RLCM-EDC or the UE9000 time of exception
Data	Hex (0000-FFFF)	Identifies the type of hardware exception
site	0000-ZZZZ	Identifies the site to the ILDR
frame	0 through 99	Identifies the line concentrating module (LCM) frame number
drawer	0 through19	Identifies the ILDR drawer number in the LCM
swerrdata	Character string	Provides the exception data from the software error text (swerrtxt)

Action

Attempt to interpret swerrdata character string to determine the cause of the exception. If you are not able to interpret swerrdata, contact the next level of support.

If the system indicates a hardware problem, perform diagnostic and maintenance procedures on the suspect equipment.

If the character string indicates a software error, retain the log report for trend analysis. There is no action required.

For formats 3 and 4, save all reports generated during the 5 min before the subsystem generated log report PM180 report. Contact the next level of support.

For format 5, save all reports generated during the 6 h before the subsystem generated log report PM180. Contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

PM181

Log report PM181 is generated when a specified step occurs in a PM function. This log also reports the occurrence of a PM exception.

This log report contains the following information:

- The section Examples on page 151 provides examples of events and fault conditions associated with log report PM181.
- The section Format on page 161 presents the different formats for log report PM181.
- The section Selected field descriptions on page 168 contains a table describing the selected fields applicable to the different log formats.
- The section Action on page 174 provides actions associated with the different fault conditions and log formats.
- The section Additional information on page 183 provides information, explanations and actions associated with different fault conditions and messages.

Examples

This section provides numbered examples of events and fault conditions associated with the different formats of log report PM181. To see each format referenced, refer to section Format on page 161.

Format 1 - The following conditions use format 1:

- Examples 1 and 2 use Format 1. The PM generates these examples when a request for diagnostics arrives from the host. The subsystem also generates these examples during a return to (RTS) procedure with diagnostics permitted. Format 1 specifies the unit (0 or 1) for a routine exercise (REX) test failure, if the failure is unit specific.
- Example 3 uses Format 1. The PM subsystem generates this example in the following condition. The call processing node status table is not the same as the current status of the line appearance on a digital trunk (LDT). The LDT node status table records the current status.
- Example 4 uses Format 1. The PM subsystem generates this example when one or more frame transport buses (F-bus) tap in a link interface module (LIM). The error occurs because the frame transport buses have changed to the in-service trouble (ISTb) state within the previous 3 s.

- Example 5 uses Format 1. The PM subsystem generates this example when an XMS-based peripheral module (XPM) facility audit detects a state change in an echo canceller module.
- Example 22 uses Format 1. The PM subsystem generates this example under the following conditions:
  - — a line concentrating module (LCM) REX test or LCM continuity and voltage (LCMCOV) REX test passes
  - — the LCM REX test or LCMCOV REX test has not occurred on a specified node for a fixed number of days

  In NA004 and up, feature AF5898 (LCM REX Controller Enhancement) migrates the LCM REX test from the LCM node audit process of the system REX (SREX) controller. Feature AF5898 also places the continuity and voltage (COV) part of the LCM REX test in a separate LCMCOV test.
- Example 24 uses Format 1. The PM subsystem generates this example when a return to service command fails on an external node entered in table EXNDINV.
- Example 25 uses Format 1. This example generates when a TEST command fails on an external node entered in table EXNDINV.
- Example 26 uses Format 1. The PM subsystem generates this example when a service processor with UNIX (SPX) is system busy. The log lists the possible causes for the system being busy, which can include faults in the following components:
  - — the single-shelf link peripheral processor (SSLPP)
  - — Ethernet interface unit (EIU)
  - — local area network (LAN) connections
  - — the LAN-BAY cards
  - — the SPX cards

Format 2 - The following conditions use Format 2:

- Example 6 uses Format 2. The PM subsystem generates this example for PMs when a PM exception occurs.
- Examples 7, 8, and 9 use Format 2. These examples provide the status of the intelligent peripheral equipment (IPE) load.
- Example 21 uses Format 2. The subsystem generates this example when a BSY PM command causes removal of an LCM node from

an in-service (InSv) state. The LCM node changes to an out-of-service (OOS) state.

- Example 28 uses Format 2. The PM subsystem generates this example when a digital subscriber loop (xDSL) line card is added to the LNINV table. The drawer for the table does not support the high speed data traffic of the 1 Meg Modem Service. The line installed functions as a standard voice line only.
- Example 29 uses Format 2. The PM subsystem generates this example when an xDSL line card is added to the LNINV table. The drawer for the table supports the high speed data traffic of the 1 Meg Modem Service. The line drawer contains more xDSL line cards than the xDSL engineering rules allow. The installed xDSL line card functions as an xDSL line. The whole line drawer is at risk of failure because the drawer is operating beyond its thermal and electrical limits. Operating company personnel receive warning of the xDSL engineering rules breach at the time of the addition. These personnel can perform the following actions to correct the condition:

  — use the QXNET EXPANDALL command to locate another LCM that supports xDSL and has room for expansion
  upgrade another LCM line drawer with a data-enhanced bus interface card (DBIC) and relocate this xDSL line card to that drawer

  — use the QXNET VERIFY <site> <frame> <unit> <drawer> command to verify the xDSL line card assignments

- Example 30 uses Format 2. The PM subsystem generates this example when an xDSL line card is added to the LNINV table. The drawer contains more xDSL line cards in a vertical row than the xDSL engineering rules allow. The installed xDSL line card functions as an xDSL line. The whole line drawer is at risk of failure because the drawer is operating beyond the thermal and electrical limits. Operating company personnel receive warning of the xDSL engineering rules breach at the time of the addition. These personnel can perform the following actions to correct the condition:

  — use the QXNET EXPAND<site> <frame> <unit> <drawer> command to locate another row in the same drawer for the xDSL line card

  — use the QXNET EXPANDALL command to locate another LCM that supports xDSL

Format 3 - The following conditions use Format 3:

- Example 10 uses Format 3. This example indicates the detection of a fault on an LIM during any InSv or OOS test. Refer to the MS200 and MS300 series of logs for the possible faults.
- Example 11 uses Format 3. The PM subsystem generates this example when the central control (CC) receives a report from an XPM. This report indicates the detection of a parity fault. The parity fault can be hard, soft or not continuous. If the XPM detects a hard parity fault, the system displays the card that has faults on the card list. Format 3 changes to include the user name and the message `Performed Override of SWACT Controller`. This change occurs when a user overrides the rejection by the switch of activity (SWACT) controller to perform a SWACT. The user assumes all responsibility for XPM SWACT operation when the user overrides the decision of the SWACT controller.
- Example 12 uses Format 3. The PM subsystem generates this example when an XPM diagnostic detects a fault in the echo canceller control card.
- Example 23 uses Format 3. The PM subsystem generates this example when the system detects an F-Bus composite clock fault on the LIM. The log also lists possible cause and possible action. Possible cause indicates all possible causes to the composite clock fault report. Possible action indicates the actions to take to resolve the composite clock fault and the CCS7 outage protection.
- Example 43 uses Format 3. The PM subsystem generates this example when an XPM unit reports a fault report message that is not requested. The XPM unit report this message to the computing module (CM). The log report contains the current degradation level in the XPM unit and a card list of any cards that have faults. The following list is a correct list of status messages that can appear in this occurrence of PM181 log:
  - No degradation of service in unit
  - Minor or potential service degradation in unit
  - Partial service degradation in unit
  - Severe service degradation in unit
- Example 45 uses Format 3. This format is generated when an XPM unit reports an unsolicited fault report message to the computing module (CM). Beginning in XPM09, the log report also identifies the

type of fault and the states in which the faults have been detected. Following is a list of the fault types:

- — Fault inferred by maintenance
- — Fault detected by diagnostics
- — Operational fault

Format 4 - The following conditions use Format 4:

- Examples 13 and 14 use Format 4. The PM subsystem generates these examples when the host sends a request for diagnostics. These examples also occur during a return to service (RTS) with diagnostics permitted.
- Example 15 uses Format 4. This example indicates if the broadcast patching function was successful and if the units passed or failed.
- Example 16 uses Format 4. The PM subsystem generates this example as a result of a PM diagnostic failure or as notification of test completion. The system also generates this log with the new system busy reason of XPM in emergency stand-alone (ESA). This generation occurs when a remote cluster controller (RCC) can return to service after the RCC enters a CC warm or cold restart.
- Example 17 uses Format 4. This example produces a message that indicates unified processor (UP) activity because of signaling processor (SIGP) clock failure or power failure.
- Example 18 uses Format 4. The PM subsystem generates this example when the enhanced ISDN-line concentrating module (LCME) does not load multipoint embedded operations channel (EOC) data from the CC. The LCME returns a failure code to the CC. The system also generates this log when the LCME does not load data from the CC that monitors performance.
- Example 19 uses Format 4. The message field indicates that the firmware name for LOADABLE EEPROM is different from the firmware name for EXECUTABLE EEPROM. During the initialization, an attempt to upgrade the EEPROM with the wrong firmware name can result in failure. This error is the reason for the mismatch.
- Example 20 uses Format 4. The PM subsystem generates this example when a user uses the SWACT Force MAP command to attempt an XPM SWACT. This attempt overrides the rejection of the SWACT controller to perform a SWACT. Format 4 changes with the text string `failed: XPM SWACT Back` to inform the user that a SWACT back occurred. Format 4 also changes to indicate if the aborted SWACT was an override of the SWACT controller. When the system generates this log with this text string, the active unit is

not indicated. The user assumes all responsibility for the XPM SWACT when the user overrides the decision of the SWACT controller.

The system suppresses PM181 log reports in Format 4 that indicate `Static Data Updated/Cleared for the following XPMs that run REX:`

- line trunk controller (LTC), LTC+, ISDN LTC (LTCI)
- line group controller (LGC), LGC+, ISDN LGC (LCDI)
- digital trunk controller (DTC), DTC7, DTC+, ISDN DTC (DTCI)
- remote cluster controller (RCC), RCC+, RCC2
- subscriber carrier module-100S (SMS), SM-100 rural (SMR), SM-100 urban (SMU), and SMS remote (SMSR)
- remote cluster controller (RCC), RCC+, RCC2
- subscriber carrier module-100S (SMS), SM-100 rural (SMR), SM-100 urban (SMU), and SMS remote (SMSR)

Several of the following formats apply to ISDN line drawer for remotes (ILDR). The ILDR is first available for remote switching center-SONET (RSC-S) and remote switching center (RSC) configurations in the NA007/XPM08 timeframe. The ILDR is first available for the following configurations in the NA008/XPM81 timeframe:

- remote line concentrating module (RLCM)
- outside plant module (OPM)
- outside plant access cabinet (OPAC)

Format 5 - The following condition uses Format 5:

- Example 31 uses Format 5. The PM subsystem generates this example when an ISDN line drawer for remotes (ILDR) state changes from InSv to SysB.

Format 6 - The following condition uses Format 6:

- Example 32 uses Format 6. The PM subsystem generates this example when an ILDR changes from InSv to ISTb.

Format 7 - The following condition uses Format 7:

- Example 33 uses Format 7. The PM subsystem generates this example when an ISTb reason is set or deleted (ILDR).

Format 8 - The following condition uses Format 8:

- Example 34 uses Format 8. The PM subsystem generates this example when a switch bank is complete. The system generates this log if the switch bank is successful or not successful.

Format 9 - The following condition uses Format 9:

- Example 35 uses Format 9. The PM subsystem generates this example when an ILDR test fails.

Format 10 - The following condition uses Format 10:

- Example 36 uses Format 10. The PM subsystem generates this example when a file is loaded to the ISDN drawer controller (IDC). The PM subsystem also generates this example when the load attempt fails.

Format 11 - The following conditions use Format 11:

- Examples 37 and 38 use Format 11. The PM subsystem generates these examples when a minimum of one LIS or FBus taps change state. The log indicates the LIS number and the tap number when these numbers apply. This format applies only to an LIM with triple FBus configuration. Tap number range is 0-11.

Format 12 - The following condition uses Format 12:

- Example 39 uses Format 12. The PM subsystem generates this example when the system detects a tap fault. This format applies only to an LIM with triple FBus configuration. Tap number range is 0-11.

Format 13 - The following condition uses Format 13:

- Example 40 uses Format 13. The PM subsystem generates this example when the system detects a bus fault. This format applies only to an LIM with triple FBus configuration.

Format 14 - The following conditions use Format 14:

- Example 41 uses Format 14. The PM subsystem generates this example when an ILDR enters the congestion state.
- Example 42 uses Format 14. The PM subsystem generates this example when an ILDR exits the congestion state.

Format 15 - The following condition uses Format 15:

- Example 44 uses Format 15 when a load containing MtcArb is present in only one unit. Beginning with CSP09, MtcArb will always be functional by the fact of its being part of the load. The operating company personnel will not be able to disable MtcArb. Therefore, log PM181 will not indicate if MtcArb is functional or disabled.

Format 16 - The following condition uses Format 16:

- Example 46 displays the EEPROM loading process log report in Format 16. One of the F/W loading processes is the erase step. After the erase step finishes, the system displays the log.

Format 17 - The following condition uses Format 17:

- Example 47 displays the recovery failure log report in Format 17. The SXO5 processor card could contain a flash memory (SX06) in one of it's internal slots. When the XPM image dump fails, the system displays the log.

Format 18 - The following condition uses Format 18:

- Example 48 uses Format 18. If the configuration data table (CDT) Audit finds a static data mismatch between the CM and the XPM configuration data, the system sets the XPM to ISTb. In the event of a configuration data manager (CDM) checksum mismatch, the PM subsystem generates a log. The log displays the table and the table ID of the CDT table that failed.

Format 19 - The following condition uses Format 19:

- Example 49 uses Format 19. An RTS of a unit that does not have the hardware associated with the extended messaging feature will fail. A log will be generated.

Format 20 - The following condition uses Format 20:

- Example 50 uses Format 20. If the CC and LCM do not indicate the same current generator for the LCM units, the system generates this example. During a one night process (ONP), the system initializes the CC to the default ring generator of the LCM. If there is a mismatch between the CC and LCM, on NORESTARTSWACT the system updates the CC to match the LCM. This log does not require action.

Format 21 - The following condition uses Format 21:

- Example 51 uses Format 21. The system generates this example in section VCPY (module XPMMASUI) when the configuration data management (CDM) dynamic tuple update fails.

Format 22 - The following condition uses Format 22:

- Example 52 uses Format 22. The system generates this example when the static data download fails.

Format 23 - The following condition uses Format 23:

- Example 53 uses Format 23. The system generates this example when the state of the entry `xpm_supports_dynamic_sd` is false.

Format 24 - The following condition uses Format 24:

- Example 54 uses Format 24. The system generates this example when a reload is finished.

Format 25 - The following condition uses Format 25:

- Example 55 uses Format 25. The system generates this example when the active unit, which is handling call processing, changes. The other unit is in standby mode and is ready to take over activities if there is a problem with the active unit. You can use the CS 2000 GWC Manager to manually change the active unit by performing a warm or cold swact.

Format 26 - The following condition uses Format 26:

- Example 56 uses Format 26. The system generates this example when the XA-Core detects irregular heartbeat messages coming from the GWC. This is likely due to a router problem.

Format 27 - The following condition uses Format 27:

- Example 57 uses Format 27. When a GWC is attempting to return to service and encounters a problem with the return to service sequence, any of the following logs may be seen to indicate a problem. Each log lines up sequentially with an XA-Core side step that must be completed to successfully return a GWC to service. A failure at any one of these steps can cause the GWC to fail to return to service.

Format 28 - The following condition uses Format 28:

- Example 58 uses Format 28. The GWC uses a heartbeat mechanism to detect communication loss between the GWC and the XA-Core. The heartbeat is sent periodically from the GWC to the Core, and is then acknowledged from the Core back to the GWC. This log is printed if a heart beat is not received from the GWC.

Format 29 - The following condition uses Format 29:

- Example 59 uses Format 29. If the heartbeat is not sent consistently then the XA-Core will determine that communication between the XA-Core and GWC has been lost and will create this log. If both units of the GWC suffer a loss of communication, then the XA-Core will also change the Core status of the GWC to SYSB. This will cause all call processing on the Core side to be cleared.

Format 30 - The following condition uses Format 30:

- Example 60 uses Format 30. The GWC uses a heartbeat mechanism to keep the XA-Core informed of its current state. If the XA-Core determines that the recorded state of the GWC node or GWC unit is not the same state as shown in the heartbeat message, then a state mismatch is detected.

Format 31 - The following condition uses Format 31:

- Example 61 uses Format 31. If a state mismatch has been consistently detected, then the XA-Core will take action to resolve the mismatch by synchronizing the GWC and Core states as well as any related call processing. This may involve sending the GWC a message which will cause the GWC to go out of service and then return to service, necessitating a call processing outage.

Format 32 - The following condition uses Format 32:

- Example 62 uses Format 32. There are a few logs that are specific to GWC recovery. These logs are primarily intended to make customers aware of GWCs that are datafilled, but these logs are not associated with the recovery of real hardware. Since this can negatively affect system recovery, the logs are produced so that customers can confirm that datafilled GWCs represent actual working hardware.

Format

This section contains the different formats for log report PM181.

The fields and entries associated with maintenance arbitrator are optional (apply only to XPMs). When a load containing MtcArb is present in both XPM units, the MtcArb state is indicated for each unit as either functional or disabled. In XPM81, when a load containing MtcArb is present in only one of the units, the MtcArb state is indicated for that unit only. The state of the of the second unit is not indicated. Beginning in TL09, MtcArb is always functional and the MtcArb state is not indicated in the logs.

> ***Note:*** Selected field descriptions for the following log report PM181 formats appear in section Selected field descriptions on page 168

The formats for log report PM181 are as follows:

Format 1

```
PM181 mmmdd hh:mm:ss ssdd INFO
spmid
opttxt
Unit0: MTCARB is <state>, Unit1: MTCARB is <state>
```

Format 2

```
PM181 mmmdd hh:mm:ss ssdd INFO
pmid
Node : statxt
opttxt
```

Format 3

```
PM181 mmmdd hh:mm:ss ssdd INFO
pmid Unit n
Unit0: MTCARB is <state>, Unit1: MTCARB is <state>
TEXT_STRING
Site Flr RPos Bay_id Shf Description Slot EqPec
site nn cn ccc 00 nn type :no :nn pec_id
```

Format 4

```
PM181 mmmdd hh:mm:ss ssdd INFO
pmid Unit n
Node: statxt, Unit0 actxt: statxt1, opttxt0 Unit1 actxt: statx
opttxt
Unit0: MTCARB is <state>, Unit1: MTCARB is <state>
```

Format 5

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
Node: <state>, Unit0: <state>, Unit1: <state>
Drawer <drawer>: <state> from <state>
Reason: <SysB_reason>
```

Format 6

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
Node: <state>, Unit0: <state>, Unit1: <state>
Drawer <drawer>: <state> from <state>
Reason: <SysB_reason>
```

Format 7

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
Node: <state>, Unit0: <state>, Unit1: <state>
Drawer <drawer>: <state>
Reason: <ISTb_reason>
(<Set/Delete>) <ISTb_reason>
```

Format 8

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
Node: <state>, Unit0: <state>, Unit1: <state>
Drawer <drawer>: ILD <C/W> switch bank <S/F> (<S/M> action).
Reason: <Switch_Bank_Failure_reason>
```

Note: In Format 8, the log report displays the “Reason” only when the switch bank fails.

Format 9

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
Node: <state>, Unit0: <state>, Unit1: <state>
Drawer <drawer>: Test <C/F>
Reason: <Test_Failure_reason>
```

Format 10

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
Node: <state>, Unit0: <state>, Unit1: <state>
ILD <drawer>
IDC bank <bank_no> load <load_result> from <srctxt> Load file:
<load_file>
Failure reason: <reasontxt>
ILD <drawer>
IDC bank <bank_no> load <load_result> from <srctxt> Load file:
<load_file>
Failure reason: <reasontxt>
```

Note 1: Format 10 applies to loading all ILDRs in the LCM. When loading a given ILDR, the log report shows only the results for that IDC.

Note 2: In format 10, the log report displays the “Failure reason” only if the loading fails.

Format 11

```
<node><Alarm_ind>PM181 mmmdd hh:mm:ss seqnbr INFO
LIM <LIM_number>
LIS <LIS_number>
FBus <FBus_number>
<Tap_header> <Tap_number>
From: <from_s>
To: <to_s> : <Tap_header> <Tap_number>
```

Note: Format 11 applies only to an LIM in the triple FBus configuration.

Format 12

```
<node><Alarm_ind>PM181 mmmdd hh:mm:ss seqnbr INFO
LIM <LIM_number>
LIS <LIS_number>
FBus <FBus_number>
<Tap_header> <Tap_number>

Service affecting faults. CODE: <Fault_code>
```

Note: Format 12 applies only to an LIM in the triple FBus configuration.

Format 13

```
<node><Alarm_ind>PM181 mmmdd hh:mm:ss seqnbr INFO
LIM <LIM_number>
LIS <LIS_number>
FBus <FBus_number>
<Tap_header> <Tap_number>

Fault found against LIS <LIS_number> (Shelf Pos <shelf_positic
```

Note: Format 13 applies only to an LIM in the triple FBus configuration.

Format 14

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
<text>
```

Format 15

```
PM181 mmmdd hh:mm:ss ssdd INFO
pmid
opttxt
Unit n: MTCARB is <state>
```

Format 16

```
PM181 mmmdd hh:mm:ss log no INFO PM no Unit no
Node: <state>, Unit n : <state>, Unit n : <state>
<string1>
```

Format 17

```
PM181 mmmdd hh:mm:ss ssdd INFO
Node: <state>, Unit n : <state>, Unit n : <state>
<string 1>
<string 2>
```

Format 18

```
PM181 mmmdd hh:mm:ss ssdd INFO pmid
Node: statxt, Unit0 actxt: statxt1, Unit1 actxt: statxt1
<ISTb_reason>: <TBL> <(tab_id)>
```

Format 19

```
PM181 mmmdd hh:mm:ss ssdd INFO pmid Unit <n>:actxt
Node: statxt, Unit0 actxt: statxt1, Unit1 actxt: statxt1
<Switch Bank Failure Reason>: Reason: <SysB_reason>
```

Format 20

```
PM181 mmmdd hh:mm:ss ssdd INFO LCM <site> <frame> <unit> Unit
Node: <state>, Unit0 : <state>, Unit1 : <state>
RGI Mismatch
```

Format 21

```
PM181 mmmdd hh:mm:ss ssdd INFO pmid Unit<n>:actxt
Node: <statxt>, Unit0 actxt: statxt1, Unit1 actxt: statxt1
Dynamic Tuple update failed tabID: <table ID) (Reason:
<Dynamic_Download_Failure_Reason>)
```

Format 22

```
PM181 <mmmdd> hh:mm:ss ssdd INFO <PM no.>
Node: <state> UNIT : <state> UNIT : <state>
<string l>
```

Format 23

```
PM181 <mmmdd> hh:mm:ss ssdd INFO pmid
Node: statxt, Unit0 actxt: statxt Unit1 actxt: statxt
<Reason>
```

Format 24

```
PM181 <mmmdd> hh:mm:ss ssd INFO pmid
PMTYPE loaded with LOADFILE, Elaspsed time: mm: ss
```

Format 25

```
<Clli> PM181 <Date> <Time> <Sequence #> INFO <GWC#> <Unit #>
   GWC activity gained.

<Clli> PM181 <Date> <Time> <Sequence #> INFO <GWC#> <Unit #>
   GWC activity dropped.
```

Note: Format 25 is outputted as a no alarm info log.

Format 26

```
<Clli> PM181 <Date> <Time> <Sequence #> INFO <GWC#> <Unit #>
   Unexpected heartbeat flooding (<Flood Count>)
```

Note: Format 26 is outputted as a no alarm info log.

Format 27

```
<Clli> * PM181 <Date> <Time> <Sequence #> INFO <GWC #><Unit#>
   <Return to service step being performed> failed
   <Reason for failure>
```

Format 28

```
<Clli> * PM181 <Date> <Time> <Sequence #> INFO <GWC #><Unit#>
    Detecting communication loss between core and GWC
```

Format 29

```
<Clli> * PM181 <Date> <Time> <Sequence #> INFO <GWC #><Unit#>
   Communication loss between core and GWC has been confirmed
```

Format 30

```
<Clli> * PM181 <Date> <Time> <Sequence #> INFO <GWC #><Unit#>
   A GWC state discrepancy has been detected
   CM recorded state: <State> <Activity>
   GWC reporting state: <State> <Activity>
```

Format 31

```
<Clli> * PM181 <Date> <Time> <Sequence #> INFO <GWC #><Unit#>
   The GWC state discrepancy is being resolved
   CM recorded state: <State> <Activity>
   GWC reporting state: <State> <Activity>
```

Format 32

```
<Clli> * PM181 <Date> <Time> <Sequence #> INFO <GWC #><Unit#>
    GWC node timed out on recovery.
    Ensure datafilled GWC is communicating with the core.
```

Selected field descriptions

The following table explains selected fields in the different log report formats:

Field	Value	Description
actxt	Act	Identifies the activity state of the PM unit as active (Act).
	Inact	Identifies the activity state of the PM unit as inactive (Inact).
alarm		Optional field. Indicates the type of alarm that accompanied the change of state.
	***	Indicates a critical alarm.
	**	Indicates a major alarm.
	*	Indicates a minor alarm.
	(blank)	Indicates no alarm.
bank_no	0 or 1	Indicates the bank number loaded.
C/F	completed or failed	Indicates the test result. The “Reason” line is populated only in the case of a failed result.
C/W	cold or warm	Indicates a cold or warm switch bank.
Dynamic_Download_Failure_reason	tblnacktimeout Wrong Message, UNIT OOS, or unknown	Indicates why dynamic tuple download failed.
drawer	0 through 19	Indicates the drawer number.
ISTb_reason	Incoming message overloaded One DMSX channel is unavailable Load name mismatch CDT Chksm mismatch Noncritical in-service test failed One or both Bd-channels are out of service Load in progress Invalid load file or Overload	Indicates the reason for the ISTb state.
load_result	succeeded or failed	Indicates if the load succeeded or failed. The log format changes according to this field.

Field	Value	Description
<link_mtc_action>	RTS Request ManB Request SysB Request Mtce Open Request Close Request Test Request or Abort Request	Indicates the maintenance action request made to link maintenance.
link_mtc_result	Failed to close link Fault found on link Failed to open link Failed to mtce open link or Failed to test link	Indicates the result of the maintenance action request sent to link maintenance.
<m>	6 to 21	Indicates the MS card.
opttxt	Character string	Optional field. Provides additional information to help software troubleshooting technicians isolate problems.
opttxt0	Character string	Optional field. Provides additional information to help software troubleshooting technicians isolate trouble.
	(8x46)	Indicates that the NT8X46 card on unit 0 failed pulse code modulation (PCM) or signaling tests.
	(swacting)	Indicates that unit 0 is switching activity in response to a SWACT Force MAP command. This action overrides the rejection by the SWACT controller to switch activity.
	(XPM in ESA)	Indicates that unit 0 became SysB because of an XPM in ESA mode.

Field	Value	Description
opttxt1	Character string	Optional field. Provides additional information to help software troubleshooting technicians isolate trouble.
	(8x46)	Indicates that the NT8X46 card on unit 1 failed PCM or signaling tests.
	(swacting)	Indicates that unit 1 is switching activity in response to a SWACT Force MAP command. This switch overrides the rejection by the SWACT controller to switch activity.
	(XPM in ESA)	Indicates that unit 1 is switching activity in response to a SWACT Force MAP command. This switch overrides the rejection by the SWACT controller to switch activity.
pmid	alphanumeric	Indicates the PM affected. **Note:** A change of state in the F-bus taps in an LIM can generate PM181. In this condition, the pmid field appears in the form: LIM nn FBus n TAP. The subfield “FBus n Tap” indicates the specific F-bus tap responsible.
reasontxt	Illegal S-record File incorrect Fail to erase bank Bad checksum Task aborted while loading Invalid load address Failed to write the record Sequence number error Fail to send query message Fail to load mate bank Fail to get route or Fail to establish connection	Indicates the reason for the failure.
S/F	succeeded or failed	Indicates the switch bank result. The “Reason” line is populated only in the case of a failed result.
S/M	system or manual	Indicates the action originator.
Set/Delete	set or deleted	Indicates if the reason for the ISTb is a new reason (Set) or if a reason was cleared (Deleted).

Field	Value	Description
Switch_Bank_Failure_reason	No reply from ILD Active bank not changed Invalid load Bsy failed or RTS failed	Indicates the reason for the switch bank failure.
SysB_reason	Incoming message overload Critical in-service test failed No response from ILD Active bank mismatch Call process activity mismatch LCM activity mismatch Unsolicited message limit exceeded S/W error message limit exceeded WAI received Cold switch bank in progress CC restart has occurred C-side node RTSILDR Bus interface card (BIC) loop failure Fault message received from ILD or Extended Messaging Hardware Mismatch	Indicates the reason for the SysB state.
state	functional or disabled	Indicates the state of MtcArb in the XPM unit at the time the log is formatted for display. This state can differ from the state of the log at the time the system generated the log. The possibility of this difference increases as the time between log generation and log formatting increases.

Field	Value	Description
statxt	InSv, ISTb, Cbsy, SysB, and ManB username: <userid> Performed Override of SWACT Controller username: <userid> Performed a BSY PM FROM: <state> (sq) TO: <statxt> (sq) TAP: <tap_number_set> Diag Failed: <TTTTTT> <CCCCCCn> <reason text> Loading of mp-eoc data failed Loading of Performance Monitoring Data Failed	Defines the current state of the PM node. Examples are: C-side busy (Cbsy), system busy (SysB), manual busy (ManB).
statxt1	ManB, InSv, ISTb, Cbsy, OffL, UnEq, SysB	Defines the current state of the PM unit. Off-line (OffL) is an example.
TBL	character string	Indicates the name of the table.
TEXT_STRING	Character string	Indicates the type of fault detected in the XPM. Beginning in XPM09, this field also indicates the states in which the faults were detected and how the faults were detected. This value is followed by a card list if the log indicates a hard fault. See the Parity audit faults table in the “Additional information” section of this log report. See the *Peripheral Modules Maintenance Guide* (Circuit location display) for details about the card list format.

Field	Value	Description
Test_Failure_reason	Flash memory bank Sanity timeout Active bank: Checksum Inactive bank: Checksum Timing MatrixB53 Application-specific integrated circuit (ASIC) 100VU-loop power supply or No reply from ILD	Indicates the reason for the switch bank failure.
tab_id	alphanumeric	Indicates the table identification number.
Unit n	0 or 1	Identifies the PM unit that generates the report. If the PM that generates the report is an ESA, there is no unit specified. When MtcArb is loaded in only one PM unit, this value identifies that unit.
Unit 0: MTCARB is	constant	Indicates that the current state of the maintenance arbitrator in XPM unit 0 follows. This field is optional and applies only to digital trunk controllers (DTC), line trunk controllers (LTC) and line group controllers (LGC). If the XPM maintenance arbitrator is not loaded in the unit, the field is blank. Beginning in TL09, this field is not present.
Unit 1: MTCARB is	constant	Indicates the current state of the maintenance arbitrator in XPM unit 1 follows. This field is optional and applies only to DTCs, LTCs, and LGCs. If the XPM maintenance arbitrator is not loaded in the unit, the field is blank. Beginning in TL09, this field is not present.

Action

This section describes additional action you can take to resolve problems indicated in the log report.

Take action as the report specifies. If you cannot resolve the problem, save all reports generated during the 5 min before the system generated PM181. Contact the next level of maintenance.

The following table suggests actions to take in response to the different failure conditions associated with log report PM181:

Actions for log report PM181 (Sheet 1 of 9)

Problem	Additional information	Action
Loading the IPE fails.	See log format 2, examples 7, 8, and 9.	Maintenance may be required. Contact the next level of maintenance.
PM nodes fail the patching function.	See log format 4, example 15.	Modify the nodeset (or create a new nodeset) that includes the failed units. Try to remove or apply the patch again
Failure involving an SPX.	See log format 1, example 26.	Perform fault diagnostics on the SPX. Access the SPX through the console port at the DMS ServiceBuilder LAN-BAY.
Failure involving an integrated digital terminal (IDT).	The IDT becomes ManB.	Take the correct maintenance steps. If the problem persists, contact the next level of support. A time-out can occur while the CC maintenance task waits for the busy request reply from the subscriber carrier module-100 access (SMA). If a time-out occurs, check the status of the SMA, the IDT, and the P-side message DS-1 links at the MAP display. If the SMA responds that the busy request failed, refer to log reports for additional information.

Actions for log report PM181 (Sheet 2 of 9)

Problem	Additional information	Action
Parity audit fault.	See log format 3, example 11.	Refer to the Parity audit faults table at the end of this log. The table contains information on the correct action to take.
XPM diagnostic detects a fault in the echo canceller control card.	See log format 3, example 12.	Replace the card.
XPM facility audit detects a state change in an echo canceller module.	See log format 1, example 5.	Replace the echo canceller module that has faults. Check the buses that connect the ring generator to the units.
A line card that has faults overloads the ring generator.	Log report PM179 is the current report for ring generator overload.	Determine the line card that causes the fault. Remove the cards and test the drawer that faults to check for the card that has faults. The test passes when more than one line card that has faults is installed. With all line cards unseated, test the drawer to clear the fault. Next, reseat the cards one at a time. The LCM sends a message that is not requested. This message reports the ring generator overload when you reseat the card that has faults. Remove the known card that has faults and replace the card.
ASU attempts SYSB recovery (autoloading of an ASU).	An error occurs if a mismatch between the processor card and the loadsize causes the loading to fail. The load continues to fail autoload until the load is compatible with the process size.	No action indicated.
Ring generator overload (that a line card that has faults does not cause).	None.	Replace the ring generator that has faults.

Actions for log report PM181 (Sheet 3 of 9)

Problem	Additional information	Action
The opttxt field indicates that the firmware name of the loadable EEPROM is different from that of the executable EEPROM.	See log format 4, example 19. In this condition, the action fails because the system cannot upgrade the EEPROM with the wrong firmware name.	Load the firmware to the EEPROM. If the log appears again, replace the card.
The opttxt field indicates that the unit is in ROMlevel.	None.	Perform the command PMRESET. If this command does not work, load the unit again and perform an RTS. After you perform the RTS, load the firmware to the EEPROM again.
The opttxt field indicates the programming was not successful.	The programming failed because of time-out open route.	Perform the LOADPM command again.
The opttxt field indicates that the query was not successful.	None.	Perform the LOADPM command again. If the system generates same log message is after you reissue the LOADPM command, replace the card.
The number of erases that erased more than one time is close to 3000, and the time of the load process increases.	None.	Replace the EEPROM in the unit with a newer one because the EEPROM is old.
The opttxt field indicates that the programming was not successful because of a file name that was not correct.	In this condition, the loadfile in the inventory table is not correct.	Change the file name in the inventory table.
The opttxt field indicates that the programming was not successful because of flags that were not correct.	In this condition, the loadfile in the inventory table is not correct.	Return the unit to service to upgrade the erased EEPROM. Change the firmware file that includes correct flags. Replace the loadfile.

Actions for log report PM181 (Sheet 4 of 9)

Problem	Additional information	Action
The opttxt field indicates that the programming was not successful because burning action failed.	None.	In this condition, issue the LOADPM command again. If the system generates the same log message after you reissue the LOADPM command, replace the EEPROM. If the system generates the same log message after the reissue, replace the card.
The opttxt field indicates that the programming was not successful because of address overlap.	The loadfile in the inventory table is not correct.	Change the file name in the inventory table.
The opttxt field indicates that the programming was not successful because of an S-record that was not legal.	The loadfile in the inventory table is not correct.	Change the file name in the inventory table.
The opttxt field indicates that the programming was not successful because of address range error.	The loadfile in the inventory table is not correct.	Change the file name in the inventory table.
The opttxt field indicates that the checksum of the EEPROM failed.	None.	Perform the LOADPM command again. If the system generates the same log, change the file name in the inventory table.
The opttxt field indicates that the switching action between the two EEPROMs failed.	None.	Perform the LOADPM command. If the system generates the same log again, replace the card.

Actions for log report PM181 (Sheet 5 of 9)

Problem	Additional information	Action
The opttxt field indicates that the ROM diagnostics failed.	None.	Perform the LOADPM command. If the system generates the same log, replace the card.
The opttxt field indicates that the running on the EEPROM that executes was not successful.	None.	Check for additional log messages and load the unit again with the previous firmware. Load the firmware to the EEPROM. If the log appears again, replace the card.
The opttxt field indicates one of the following: • `LCM REX test has not been performed on this node for nn days.` • `LCMCOV REX test has not been performed on this node for nn days.`	None.	The operating-company technician can determine why the test was not performed on the specified LCM. The TST REX OFF or TST COVREX OFF commands can cause the system to disable REX testing on the LCM. These commands are at the LCM level of the MAP display. The technician should make the correct entry changes to enable REX testing for the LCM.
The opttxt field indicates `LCM REX TEST PASSED` or `LCMCOV REX TEST PASSED.`	None.	No action required.
An NT8X46 card fails a PCM or signaling test.	A card that has faults affects voice and data calls until you replace the card.	Follow resolution recommendations in the PCM/Signaling test failures table. Refer to *Meridian SL-100 Digital Line Module Reference Manual* for additional information on the NT8X46 card.

Actions for log report PM181 (Sheet 6 of 9)

Problem	Additional information	Action
The system generates this log as a result of an override of the decision of the SWACT controller.	See log format 3, example 11. The system generates this log to inform the user that a SWACT back occurred. This log also informs the user if the SWACT back was an override of the decision of the SWACT controller. The system also generates this log to identify the user with the responsibility for the SWACT.	This condition does not require immediate action.
The state of the ILDR changes to ISTb, SysB, or switch bank failure.	See the following: • log format 5, example 31 • log format 6, example 32 • log format 8, example 34	Proceed according to the failure reason. If none of these changes are the reason, there is no action required.
The ILDR load operation fails.	None.	Check the reason for the failure and proceed as required. Notes: • If you correctly load the ILDR file, there is no action required • If the ILDR load operation fails, check the reason for the failure and proceed as required. • There is no action required if ILDR enters or exits the congestion state.

Actions for log report PM181 (Sheet 7 of 9)

Problem	Additional information	Action
The XPM maintenance arbitrator (MtcArb) diagnostic detects a card that has faults in the XPM unit.	None.	Replace the card.
RTS fails because of an Extended Messaging Hardware Mismatch	None.	Install the appropriate circuit packs to support extended messaging.
The CDT Audit detects a CDT Chksm Mismatch.	The log identifies the mismatched CDM table. The system sets the peripheral to ISTb. See log format 16, example 48.	To clear the ISTb, busy (BSY) and return the peripheral to service (RTS). This action sends a static data download to the PM and corrects the static data mismatch in the CDM table.
The system indicates `Could not configure NETPROT for unit 1 occurs`, reload static data.	None.	Use the LOADPM command to reload static data in the unit identified in the log (for example, LOADPM UNIT 1 CC DATA).
If the flag `xpm_supports_dynamic_sd` is false.	The 1 minute audit sets the boolean to 'True' and generates a log indicating the same.	No action required.
Log format 26, example 56.	None.	Contact Nortel Networks customer support.

Actions for log report PM181 (Sheet 8 of 9)

Problem	Additional information	Action
Log format 27, example 57.	There are many possible failure reasons that may be printed and, as a result, not all of them can be listed here. The failure reason will give some specific information to indicate the cause of the failure. The most common failure reason is “`NO reply from PM`” as shown in the example log. If this failure reason is given, then the communication path between the XA-Core and the GWC is probably faulty. Most commonly, recently datafilled GWCs may encounter this problem due to one of the following: • the SRVRADDR IP address is incorrect in table SRVRINV on the Core • the CS IP number or node number is incorrect on the GWC.	If the reason is “`NO reply from PM`” then verify that the GWC is datafilled correctly and that the ethernet links and Passport 8600 are connected and working properly.
Log format 28, example 58.	A number of reasons can cause the heartbeat to be missed: • A packet could have been intermittently lost. • There could be a problem with the GWC such that it is not sending a heartbeat message. • The communication link between the GWC and XA-Core could be broken.	If the log is printed only once then there was likely just an intermittent packet loss in the network and no action is required If the log is printed periodically then there is likely a problem with the network path between the GWC and the XA-Core and packets are being dropped periodically. In this case the network should be examined to reduce packet loss.

Actions for log report PM181 (Sheet 9 of 9)

Problem	Additional information	Action
Log format 29, example 59.	The GWC may have stopped sending heartbeat messages without notifying the XA-Core that it is going out of service. This may occur if the GWC is re-booted without first being taken out of service, or if an autonomous restart occurs due to sever failures on the GWC.	If the GWC is in service at the time these logs are printed, then there is likely a network fault and the network should be examined to locate the broken communication path.
Log format 30, example 60.	A state mismatch could occur if a state transition message sent from the GWC to the XA-Core is lost. This log report is not common and should rarely be seen.	A transient log seen once is of no concern. If these logs are seen periodically then there may be an internal software problem. There may be a problem with the network if communication loss logs are also seen.
Log format 31, example 61.	A state mismatch has occurred consistently. The XA-Core will resolve the mismatch automatically.	The circumstances surrounding the mismatch should be investigated by the design group. Please contact Nortel Networks customer support if this log is seen.
Log format 32, example 62.	The active GWC unit failed to respond within 30 seconds of receiving notification of an XA-Core restart. Therefore, the Core recovery of the GWC node has timed out.	Check the GWC to ensure it is functioning correctly. If the datafilled GWC does not represent actual GWC hardware, then the tuple should be deleted from table SERVRINV.

.

Associated OM registers

This log report has no associated OM registers.

Additional information

Host-requested diagnostics

The following table provides failure reasons for host-requested diagnostics.

Host-requested diagnostics - failure reasons (Sheet 1 of 2)

Failure reason	Explanation
CMR NT6X78AA OOS CMR Diagnostic Fail	Indicates the class modem resource card is out-of-service. This failure implies that the calling number delivery feature does not work for terminating lines on that peripheral.
Test Failed: CTRDIAG	Indicates the detection of an operational fault on the CX10. Call progress tone receiver (CTR) configured in the specified test access controller XPM (TAC) is not available for call progress tone reception.
Test Failed: CPADIAG	Indicates the detection of an operational fault on the CX09. Class protocol analyzer (CPA) configured in the specified TAC is not available for class message reception.
Diagnostic TestAll passed.	Indicates diagnostics ran and did not find faults.
Diagnostic TestAll failed.	Indicates the diagnostic failed but was not able to generate a card list.
Diagnostic TestAll failed, CardList: nXnn, nXnn	Indicates the diagnostic failed the cards listed in the card list. Table ROM test failures provide the text strings that reflect the failure of ROM tests run on the NT6X51AB board. Refer to the end of the log for the Table ROM test failures.
Diagnostic TestAll failed, Invalid Static Data.	Indicates the diagnostic failed because the requested diagnostics require static data in the peripheral module.
Diagnostic TestAll failed, a resource was unavailable	Indicates the request to run a diagnostic. The diagnostic system in the PM was not able to allocate all the resources that the diagnostic required.

Host-requested diagnostics - failure reasons (Sheet 2 of 2)

Failure reason	Explanation
Diagnostic TestAll was not run.	Indicates that for some reason, the diagnostic system in the PM was not able to run the requested diagnostic.
Diagnostic TestAll failed, PP has an invalid load.	Indicates the diagnostic system did not run the diagnostic because this system has a temporary overload.
Diagnostic TestAll not run, Diagnostic system is in overload	Indicates the diagnostic system did not run the diagnostic because this system has a temporary overload.
Software error in Diagnostic TestAll	Indicates the diagnostic system encountered a software error. The error occurred when the system tried to run the requested diagnostics.
Diagnostic Test All not present in PP load.	Indicates the requested diagnostic is not present in that given peripheral module.
Diagnostic TestAll - unknown return code.	Indicates the diagnostic system returned a reply to the host that the host cannot process.

The following table provides maintenance action explanations for host-requested diagnostics.

Host-requested diagnostics - maintenance actions

Maintenance action	Explanation
(Blank)	There is no action required.
Reload this unit	
BSY and RTS this unit.	
Diagnose this unit.	The audits in the PM discovered a fault. Use the TST command from the MAP display to isolate the fault in this unit.
Try diagnostics again later.	
Watch for and report PM180 logs.	The diagnostics can have triggered some PM180 logs. Record these PM180 logs on any problem report.

Host-requested diagnostics - maintenance actions

Maintenance action	Explanation
Replace cards on card list.	The card list presents cards in order of the most probable cause of the failure. Replace each card in order, testing with each replacement until a replacement clears the fault.
Report this log to your field support division. BSY and RTS C-Side PP LCM REMn n n	A C-side peripheral module is the most probable cause of the failure. The most possible state for this module is a system busy state. Perform the BSY and RTS commands on the peripheral module identified in the text section of the log.
Diagnose C-Side PP LCM REMn n n	A fault isolation in the PM determined the fault lies in the C-side peripheral. Perform the POST and TST commands on the peripheral identified in the log text.
Diagnose C-Side links:	Post the C-side peripheral of this unit and diagnose the P-side links of that peripheral module.
Reload Static Data:	Use the LOADPM command to reload static data in the unit identified in the log (for example, LOADPM UNIT 1 CC DATA).

DMPC faults

The format of the text string (opttxt) for digital port maintenance card (DMPC) faults is as follows:

Diag Failed: DPMC Fault - <fault reason>

The following table lists DPMC faults and actions.

DPMC faults and actions

DPMC fault reason	Action
Card Not Present	Insert a DPMC card completely in the DLM shelf in slot 13 or change customer data in table DLMINV. Change this data to indicate that the DLM is not equipped with a DPMC.
Card Not Accessible	The card was in use during the test. Start InSv tests on one of the units of the DLM to test the DPMC again.
Control Logic Defective	Replace the DPMC.
Relay Drivers Defective	Replace the DPMC.
Facility Sensors Defective	Replace the DPMC.
DSIC 30V Measurement Circuit Defective	Replace the DPMC.
Loop Voltage Sensor Defective	Replace the DPMC.
30V Source Defective	Replace the DPMC.
Defective DSIC Emulation Circuit	Replace the DPMC.
Prime DSIC 10V Measurement Circuit Defective	Replace the DPMC.
Mate DSIC 10V Measurement Circuit Defective	Replace the DPMC.

RLCM/RDLM-ESA messages

The following table provides RLCM/RDLM-ESA log messages and actions.

RLCM/RDLM-ESA messages and actions

RLCM/RDLM-ESA message	Explanation	Action
PM in ESA, communication restored, ready to be returned to service	The RLCM/RDLM runs in ESA and the office parameter RLCM_XPMESAEXIT is set to 0. This condition means that the system will issue a warning log for every audit cycle.	Manually return the RLCM/RDLM to service when problems with the links of the RLCM/RDLMs links are resolved.
ESAExit failed, Reason: no reply from PM	Indicates that the RLCM/RDLM did not perform a successful exit from the ESA	For information only.
LCM unit inhibiting ESA. Return to service or reload this PM.	The CC found an LCM unit that requests ESA while the LCM is InSv. The possible cause is a defective exit or an ESA REX test.	Busy and return the unit to service to clear the problem. If this action does not work, reload the unit from the mate and return the unit to service.
DLM unit inhibiting ESA. Return to service or reload this	The CC found a DLM unit that requests ESA while the DLM is InSv. The possible cause is a defective exit or an ESA REX test.	Busy and return the unit to service to clear the problem. If this action does not work, reload the unit from the mate and return the unit to service.
DLM unit inhibiting ESA. Return to service or reload this PM.	The CC found a DLM unit that requests ESA while the DLM is InSv. The possible cause is a defective exit or an ESA REX Test.	Busy and return the unit to service to clear the problem. If this action does not work, reload the unit from the mate and return the unit to service.

EIU failure messages

The following table lists EIU failure messages and actions.

EIU failure messages and actions (Sheet 1 of 4)

EIU failure message	Additional information	Action
ISTb condition	Indicates the EIU detects the following errors on the LAN: • rx framing errors • rx overflow errors • rx CRC errors • tx deferred errors • loss of carrier errors • late collision errors • retries exceeded errors	Perform external diagnostics. Retain all reports generated 5 min before and 5 min after this report and contact the next level of maintenance.
ISTb condition - lack of buftype	Indicates one of the following buffers caused the EIU to overload: • rx sw buffers • tx hw buffers	Retain all reports generated 5 min before and 5 min after this report and contact the next level of support.
In-service Test Failure Card: <cardtxt> < failure id>	Indicated a test failure occurred. Subfield cardtxt identifies the card. Subfield failure id indicates one of the following messages:	Follow the procedures as indicated for each failure id.
	EIC CARD LOCATE TEST	Verify that the product engineering code (PEC) of the card in the slot is a valid Ethernet interface card (EIC) PEC. Run the test again.
	EIP CARD LOCATE TEST	Verify that the Ethernet interface paddle board (EIP) card is in the correct shelf and slot. Run the test again.

EIU failure messages and actions (Sheet 2 of 4)

EIU failure message	Additional information	Action
	EIP CARD ID PROM TEST	Verify that the PEC of the paddle board in the EIP shelf and slot is a valid EIP PEC. Run the test again.
	EIC CARD TEST	Replace the EIC for the specified EIU and run the test again.
	EIP CARD TEST	Replace the EIP card for the specified EIU and run the test again.
	EIC AND EIP CARD TEST	Replace the EIC for the specified EIU and run the test again. If the second test fails for the same reason, replace the EIP card and run the test again.
	EIP AND EIC CARD TEST	Replace the EIP card for the specified EIU and run the test again. If the second test fails for the same reason, replace the EIC and run the test again.
Operation Affecting Fault: faultxt	Indicates the fault encountered affects the operation. One of the following messages generates:	Refer to the fault messages for any possible action to take.

EIU failure messages and actions (Sheet 3 of 4)

EIU failure message	Additional information	Action
	Local EIU mtce software error: rsntxt. Field rsntxt consists of one of the following messages: • Inconsistent local mtce state • Unexpected msg from EICM • Bad parms for EICM command • EICM in illegal state for command	The system automatically places the EIU in a system busy state. Save this report and all other reports generated in the past 5 min. Contact the next level of support.
	EIC mtce software error	The system automatically places the EIU in a system busy state. Save this report and all other reports generated in the past 5 min. Contact the next level of maintenance.
	• Excessive spurious interrupts • EIC card failure	The system automatically places the EIU in a system busy state. Save this report and all other reports generated in the past 5 min. Contact the next level of support.
	EIU fault: <rsntxt> - Subfield “rsntxt” consists of one of the following messages:	Refer to the correct reason for any possible action to take.
	Enable failed - EIC card not found	Verify that the EIC card is in the correct shelf and slot. Attempt to return the EIU to service.
	Enable failed - EIC PEC mismatch	Verify that the PEC of the card in the EIC shelf and slot is a valid EIC PEC. Return the EIU to service.

EIU failure messages and actions (Sheet 4 of 4)

EIU failure message	Additional information	Action
	Enable failed - EIP card not found	Verify that the EIP card is in the correct shelf and slot. Return the EIU to service.
	Enable failed - EIP PEC mismatch	Verify that the PEC of the card in the EIP shelf and slot is a valid EIP PEC. Return the EIU to service.
	Enable failed - EIC card failure	Replace the EIC card for the specified EIU. Return the EIU to service.
	Enable failed - EIP card failure	Replace the EIP card for the specified EIU. Return the EIU to service.
	Enable failed - EIC and EIP cards failed (EIC most probable)	Replace the EIC card for the specified EIU. Try to return the EIU to service. If the second attempt fails for the same reason, replace the EIP card. Return the EIU to service.
	Enable failed - EIP and EIC cards failed (EIP most probable)	Replace the EIP card for the specified EIU and return the EIU to service. If the second attempt fails for the same reason, replace the EIC card. Return the EIU to service.

NT8X46 PCM/signaling test failure

The following table lists NT8X46 PCM/signaling test failure messages and actions.

NT8X46 PCM/signaling test failure messages and actions

NT8X46 PCM/signaling test failure message	Action
For the following messages: • Unit 0 failed PCM testing. • Unit 0 failed signaling tests. • Unit 0 failed PCM and signaling tests.	If unit 1 is already in a SysB state, unit 0 becomes ISTb. Replace the NT8X46 card in unit 0 as soon as possible. If unit 1 is in an InSv state, unit 0 becomes SysB. Run an InSv test on unit 1. If unit 1 passes and all data packet controllers (DPC) remain InSv, replace the NT8X46 card for unit 0. If any DPCs become SysB during the unit 1 InSv testing, the unit 0 NT8X46 card can be safe. Replace the NT8X47 cards associated with the DPCs that are SysB. Return those cards to service and return to service unit 0. If unit 0 stays in service, the NT8X47 cards are defective and unit 0 NT8X46 card works. If unit 0 becomes SysB again, and the NT8X46 reports the same failure, replace the unit 0 NT8X46 card.
For the following messages: • Unit 1 failed PCM testing. • Unit 1 failed signaling tests. • Unit 1 failed PCM and signaling tests.	If unit 0 is already in a SysB state, the state of unit 1 becomes ISTb. Replace the NT8X46 card in unit 1 as soon as possible. If unit 0 is in an InSv state, the state of unit 1 becomes SysB. Run an InSv test on unit 0. If unit 0 passes and all DPCs remain in service, replace the NT8X46 card for unit 1. If any DPCs become SysB during the unit 0 in service testing, the unit 1 NT8X46 card can be working. Replace the NT8X47 cards associated with the DPCs that are SysB. Return those cards to service and return unit 1 to service. If unit 1 stays in service, the NT8X47 cards are defective. The unit 1 NT8X46 card works. If unit 1 becomes SysB again, and the NT8X46 reports the same failure, replace the unit 1 NT8X46 card.

ESA failure

The following table lists emergency stand-alone (ESA) failure messages and actions.

ESA failure messages and actions (Sheet 1 of 2)

ESA failure message	Additional information	Action
Preparation Failure: LCMREMn nn n Unit n failed to enter ESA	One of the C-side LCM units failed to enter ESA when the software requested this action.	Check the state of the LCM unit. If SysB, attempt to RTS the LCM unit.
Preparation Failure: DLMREMn nn n Unit n failed to enter ESA	One of the C-side DLM units failed to enter ESA when the software requested this action.	Check the state of the DLM unit. If SysB, attempt to return the DLM unit to service.
ESA REX preparation Failure: LCM REMn nn n Unit n failed to enter ESA	Maintenance already started on the LCM when the REX test was requested. This maintenance on the LCM prevents the entry of the LCM unit into the ESA and aborts the REX test.	There is no action required.
ESA REX preparation Failure: DLM REMn nn n Unit n failed to enter ESA	Maintenance already started on the DLM when the REX test was requested. This maintenance on the DLM prevents the entry of the DLM unit into the ESA and aborts the REX test.	There is no action required.
Test Failure: LCM REMn nn n Unit n failed to exit ESA	The ESA software placed a unit of the LCM in ESA. The system used this unit to run the REX test. When the test was complete, the LCM unit failed to return to service. This failure caused the REX test to abort. (A no resources message normally accompanies this occurrence at the MAP display.)	Attempt to RTS the LCM unit.

ESA failure messages and actions (Sheet 2 of 2)

ESA failure message	Additional information	Action
Test Failure: DLM REMn nn n Unit n failed to exit ESA	The ESA software placed a unit of the DLM in ESA. The system used this unit to run the REX test. When the test was complete, the DLM unit failed to return to service. This failure caused the REX test to abort. (A no resources message normally accompanies this occurrence at the MAP display.)	Attempt to RTS the DLM unit.
Preparation Failure: LCMREMn nn n Unit n failed C-side message test	The C-side LCM failed its C-side messaging test.	Post the PM 0 on the C-side of the LCM unit that reports the fault. Test the P-side link from the PM to that LCM unit.
Preparation Failure: DLMREMn nn n Unit n failed C-side message test	The C-side DLM failed its C-side messaging test.	Post the PM on the C-side of the DLM unit that reports the fault. Test the P-side link from the PM to that DLM unit.
ESA Test Preparation Failure: RMM n failed C-side message test	The remote maintenance module (RMM) failed the C-side messaging test. The ESA software module needs the RMM in order to perform a REX test.	Check the state of the RMM to make sure that the RMM is in service and can pass diagnostics.
ESA Test Preparation Failure: ESA failed C-side message test	The ESA software module failed the internal C-side messaging test for ESA.	Post the LCM/DLM that contains the ESA module. Attempt to return to service the system busy link to the ESA.

ROM test failure

The following is a list of ROM test failure messages, all of which require that you replace the NT6X51AB board:

- Config reg rw test
- Stack test
- Rom size test

- Manual bank switch test
- Common bank data test
- Code execution test
- Common bank exec test

RCU and SMU status

The following table lists remote carrier urban (RCU) and SMU status messages and actions.

RCU and SMU status messages and actions (Sheet 1 of 3)

RCU/SMU status message	Explanation	Action
Node Status Mismatch	A difference in status information between the SMU and the CC is present.	Contact your maintenance support group.
AST Line Testing Initiated from <MAP or RCU>	Automatic system testing initiated from the MAP level or from the faceplate of the maintenance card at the RCU. Automatic system testing includes testing and switchover of common equipment cards and line card testing.	There is no action required.
AST Line Testing Completed from <MAP or RCU>	The system initiated automatic system testing from the MAP level or faceplate of the maintenance card at the RCU. Then the system completed automatic system testing.	There is no action required.

RCU and SMU status messages and actions (Sheet 2 of 3)

RCU/SMU status message	Explanation	Action
AST Line Testing Aborted from <MAP or RCU>	One of the following reasons caused the automatic system testing to abort: • a user entered the TST command with the ABORTLNTST parameter at the MAP display • a user pressed the EXEC button at the faceplate of the maintenance card at the RCU • a user set the AUTOTEST field in Table RCUINV to N during a test	There is no action required.
Switchover Initiated	The system initiates 24 h switchover for each RCU.	There is no action required.
Switchover Completed	24 h switchover for each RCU is complete.	There is no action required
Switchover Timeout waiting for Reply	A task waiting for a reply on the completion of the 24 h switchover for a RCU has timed out.	There is no action required.
RCU node status flag cleared	The setting of the RCU node status flag was not correct. This flag setting is now clear.	There is no action required.

RCU and SMU status messages and actions (Sheet 3 of 3)

RCU/SMU status message	Explanation	Action
Status Mismatch: Call Processing; *STATUS*, RCU Node Status; *STATUS*	The call processing node status table does not agree with the current status of the RCU. The call processing node status table is a quick reference for call processing to check the status of a given node. The RCU node status table records the current status.	There is no action required. The system updates the call processing node status table to reflect the status from the RCU node status table.
PCM Loopback test failed on P-side link 5	The PCM loopback test failed on the specified link. A PM183 state change log always follows this log. The PM183 log indicates that the system placed the link in the SysB state.	Post the correct RCU from the PM level of the MAP display, and determine if any alarms are present. Run tests on the RCU or the links to determine the cause of the failure. Link tests can run with the SMU posted at the PM level, or with the links posted at the CARRIER level

TONES sample generation messages

The following table lists TONES sample generation messages and actions.

TONES sample generation messages and actions

TONES sample generation message	Explanation	Action
Maketone Passed	Indicates the tone samples generation facility in the XPM had successful completion.	There is no action required.
Maketone Failed	Indicates the tones samples generation facility in the XPM failed.	After posting the defective PM on the MAP display, ManB the unit. Run OOS tests and proceed depending on return code. If OOS test fails, reload and return the unit to service. If the RTS command is not successful, contact the next level of support.

CMR loading status messages

The following table lists CLASS modem resource (CMR) loading status messages and actions.

CMR loading status messages and actions

CMR status message	Explanation
Loaded CMR	Indicates the system loaded the CMR file.
Loaded CMR via Mate	Indicates the system loaded the CMR file through the mate.
Failed to Load the CMR	Indicates the system failed to load the CMR file.
Failed to load CMR via Mate	Indicates the system was not able to load the CMR file through the mate.
Task Aborted while Loading CMR	Indicates loading process. was aborted.

XPM loading status messages

The following table lists XPM loading status messages and actions.

XPM loading status messages and actions

XPM loading status message	Description
Loaded XPM	Indicates the system loaded the XPM file.
Loaded XPM via Mate	Indicates the system loaded the XPM through the mate.
Failed to Load the XPM	Indicates the system did not load the XPM.
Failed to load XPM via Mate	Indicates the system was not able to load the XPM through the mate.
Task Aborted while Loading XPM	Indicates the loading process was aborted.

The following table lists a summary of loading types.

Summary of loading types (Sheet 1 of 4)

Loading type	Description
Regular loading	Loaded with NDT28AU.
	Loaded CMR with CMR28AB.
	Failed to load with NDT28AU.
	Failed to load while loading with NDT28AU.
	Task aborted while loading with NDT28AU.
	Task aborted while loading CMR with CMR28AU.
Mate loading	Received NDT28AU and broadcasted to the inactive unit of the NDT28AU.
	Failed to receive NDT28AU and failed to broadcast to the inactive unit of the NDT28AU.
	Task aborted during reception of NDT28AU broadcasting to the inactive unit of the NDT28AU.

Summary of loading types (Sheet 2 of 4)

Loading type	Description
Enhanced RCC loading	Loaded with NRC28AU and broadcasted to the inactive unit of the NRC28AU. Loaded CMR with CMR28AU and broadcasted to the inactive unit of the CMR. Failed to load with NRC28AU and failed to broadcast to the inactive unit of the NRC28AU. Failed to load CMR with CMR28AU and failed to broadcast to the inactive unit of the CMR. Loaded with NRC28AU. Loaded CMR with CMR28AU. Failed to load with NRC28AU. Failed to load CMR with CMR28AU. Task aborted while loading with NRC28AU and broadcasting to the mate of NRC28AU. Task aborted while loading CMR with CMR28AU and broadcasting to the CMR mate. Task aborted while loading with NRC28AU. Task aborted while loading CMR with CMR28AU.

Summary of loading types (Sheet 3 of 4)

Loading type	Description
Broadcast loading	Loaded with NDT28AU and broadcasted to unit 0 of DTC 0, 1, 2, 3, 4. Loaded CMR with CMR28AU and broadcasted to unit 0 of DTC 0, 1, 2, 3, 4. Loaded with NDT28AU and broadcasted to the mate and both units of DTC 0, 1, 2, 3, 4. Loaded CMR with CMR28AU and broadcasted to the mate and both units of DTC 0, 1, 2, 3, 4. Failed to load with NDT28AU and failed to broadcast to unit 0 of DTC 0, 1, 2, 3, 4. Failed to load CMR with CMR28AU and failed to broadcast to unit 0 of DTC 0, 1, 2, 3, 4. Failed to load with NDT28AU. Failed to broadcast to the mate of NDT28AU and both units of DTC 0, 1, 2, 3, 4. Failed to load CMR with CMR28AU. Failed to broadcast to the CMR mate and both units of DTC 0, 1, 2, 3, 4. Task aborted while loading with NDT28AU and broadcasting to unit 0 of DTC 0, 1, 2, 3, 4. Task aborted while loading CMR with CMR28AU and broadcasting to unit 0 of DTC 0, 1, 2, 3, 4. Task aborted while loading with NDT28AU. Task aborted while broadcasting to the mate of NDT28AU and both units of DTC 0, 1, 2, 3, 4. Task aborted while loading CMR with CMR28AU and broadcasting to the CMR mate and both units of DTC 0, 1, 2, 3, 4.

Summary of loading types (Sheet 4 of 4)

Loading type	Description
Broadcast mate loading	Received NDT28AU and broadcasted to the inactive unit of DTC 0, 1, 2, 3, 4. Received CMR28AU and broadcasted to the inactive unit of DTC 0, 1, 2, 3, 4. Failed to receive NDT28AU and failed to broadcast to the inactive unit of DTC 0, 1, 2, 3, 4. Failed to receive CMR28AU and failed to broadcast to the inactive unit of DTC 0, 1, 2, 3, 4. Task aborted while receiving NDT28AU and broadcasting to the inactive unit of DTC 0, 1, 2, 3, 4. Task aborted while receiving CMR28AU and broadcasting to the inactive unit of DTC 0, 1, 2, 3, 4.
Broadcast LCM loading	Received LCM28A and broadcasted to unit 0 of LCM HOST 00 0, REM1 00 1, HOST 10 0. Received LCM28A and broadcasted to both units of LCM HOST 00 0, REM1 00 1, HOST 10 0. Failed to receive NDT28AU and failed to broadcast to unit 0 of LCM HOST 00 0, REM1 00 1, HOST 10 0 Task aborted while receiving NDT28AU and broadcasting to unit 0 of LCM HOST 00 0, REM1 00 1, HOST 10 0.

The following list provides a summary of loading results:

- failed to open link
- no reply from PM
- bad message received from PM
- fail message received from PM
- first get on file failed
- invalid I/P record length
- invalid first char

- invalid character
- load error message received
- failed to get checksum
- failed to open file
- C-side links unavailable
- bad checksum over load
- record count error
- PM reports bad load checksum
- load message error count
- no resources available - try again
- no system resources are available
- load ESA aborted: Nil ESA target
- failed to submit secondary process
- PM excluded from loading group
- timed out waiting to open file
- unexpected who am I (WAI) detected from PM

Operational message faults for DMSX protocols

The following table explain operational message faults for DMSX protocols.

Operational message faults for DMSX protocols (Sheet 1 of 2)

Operational message fault	Explanation
BACKPR	Back pressure time-out - no free receiver buffers.
BADCRC	Occurs when the cyclic redundancy check (CRC) code is not correct.
BADSUM	Occurs when the checksum for a message is not correct.
BCKDWN	Occurs when a slave process waits for a SEND message so that the process can transmit a message. Instead the slave process receives an MIS (may I send) message from the master process.
BUFOVF	Occurs when no buffers are available.

Operational message faults for DMSX protocols (Sheet 2 of 2)

Operational message fault	Explanation
FLSMIS	False MIS that occurs when only one MIS is on the link. A minimum of two MISs are needed on the link for the message to be valid.
MISTO	May I send Time Out.
MSGLEN	Message length error that occurs during reception of a message length that is not correct.
NACK1	Occurs during reception of the first negative acknowledgement (NACK) after a message transmission.
NACK2	Occurs during the reception of a second NACK after a message transmission.
NACKX	Occurs during NACK transmission after reception of a corrupted message.
RBNDMSG	Rebounded message error occurs when a message rebounds.
WACKTO	Wait for acknowledgement time-out error occurs when transmission of a SEND does not result in reception of a start of message (SOM).
WANRTO	Wait for Idle after acknowledging. A positive acknowledgement (PACK) or a NACK can acknowledge a message. A message time-out occurs when this acknowledgement does not result in reception of IDLE.
WANXTO	Wait for Idle after a PACK. A NACK time-out occurs when the reception of a NACK acknowledgement does not result in the reception of a PACK or NACK.
WASTO	Wait to send time-out occurs when the transmission of an MIS does not result in the reception of a filtered SEND.

Operational message faults for HDLC protocols

The following table explain operational message faults for HDLC protocols.

Operational message faults for HDLC protocols

Operational message fault	Explanation
INGLN	Occurs when the first alignment attempt of the protocol fails.
MSURX	The message signal unit (MSU) contains messages that UP tasks generate.
MSUTX	The number of MSUs transmitted on the link divided by 128.
NKRCV	Occurs during reception of NACK.
NTRSH	The number of MSUs retrieved from the transmission queue after reactivation occurred.
REACT	The number of reactivations on the link.
SGERR	Detects loops on the link, and occurs in two conditions: • the system receives on the link a bad backward sequence number (BSN) or bad forward indicator bit (FIB) detected in a signal unit (SU) • the system detects a looped signal
SGRCV	The system detects an error in a received SU.

Loopback status messages

The following is a list of loopback status messages:

- Local loopback enabled
- Local loopback cleared
- Remote loopback enabled
- Remote loopback cleared
- Remote loopback waiting enabled

PSAP test failure messages

The following table lists public-safety answering point (PSAP) messages and actions.

PSAP test failure messages and actions

PSAP test failure message	Explanation	Action
PM not responding	Identifies that the generated LDT fails to receive an expected message from the SMU. This message also can indicate that the CC and SMU do not agree on the status of an LDT node.	Try to determine reason for the failure of the SMU to respond.
LDT node status flag cleared	Indicates that the audit set and cleared the LDT node status flag by accident.	There is no action required.
LDT node status; ManB	Identifies that the generated call processing node status table is not the same as the correct status of the LDT. The LDT node status table records the correct status of the LDT.	There is no action required.
Node status mismatch	Indicates differences in information between the SMU node/link status table and the CC statue table.	There is no action required.

Parity audit fault messages

The following table lists parity audit fault messages and actions.

Parity audit fault messages and actions

Parity audit fault message	Explanation	Action
Parity audit detected hard parity fault	Indicates that the parity audit detected a parity fault that a hardware failure caused. The system generates a list of memory cards that have faults.	Perform the following steps: • Replace the card that has faults displayed in the cardlist. • Reload and RTS the unit that has faults. Refer to table XPM LOADING STATUS for loading information.
Parity audit detected soft parity fault in the program store.	Indicates that the parity audit detected a parity error that a software fault in the program store caused.	Reload and RTS the unit that has faults indicated in the log.
Parity audit detected soft parity fault in the data store.	Indicates that the parity audit detected a parity error that a software fault in the data store caused.	BUSY and RTS the unit that has faults indicated in the log.
Parity audit detected intermittent parity fault.	Indicates that the parity audit detected a parity error. The parity audit did not detect a parity error on the reread of the location at fault.	BUSY and RTS the unit that has faults.

RCC2 messages

A list of RCC2 messages follows:

- Mismatch of the firmware edition between the LOADABLE and EXECUTABLE EEPROM in unit
- Mismatch of the firmware edition between the inventory table and EEPROM # & in the unit
- FAIL TO LOAD EEPROM - UNIT FOUND IN FRM LEVEL
- FAIL TO LOAD EEPROM - TIME OUT OPEN ROUTE
- FAIL TO LOAD EEPROM - UNIT FOUND IN ROM LEVEL
- FAIL TO QUERY FOR EDITION OF EEPROM

- ERASE EEPROM #& COMPLETED SUCCESSFULLY # OF REERASES : &$ # OF REWRITES : &$
- FAIL TO ERASE EEPROM #& # OF REERASES : &$ # OF REWRITES : &$
- FAIL TO LOAD EEPROM # & - FILE INCORRECT
- FAIL TO LOAD EEPROM # & - FLAGS INCORRECT
- FAIL TO LOAD EEPROM # & - FAIL TO PROGRAM
- FAIL TO LOAD EEPROM # & - ADDRESS OVERLAP
- FAIL TO LOAD EEPROM # & - ILLEGAL S-RECORD
- FAIL TO LOAD EEPROM # & - ADDRESS RANGE VIOLATION
- BAD EEPROM # & CHECKSUM MS COUNT OF CC IS : N MSG COUNT OF XPM IS : N
- FAIL TO LOAD EEPROM # & - FAIL TO SWITCH BETWEEN EEPROMS
- FAIL TO LOAD EEPROM # & - ROM DIAGNOSTIC FAILED
- FAIL TO LOAD EEPROM #&-FAIL TO RUN FROM EEPROM # $
- FAIL TO LOAD EEPROM # & - FLAGS UPDATE FAIL
- UPDATE EEPROM #& WITH <file name> COMPLETED SUCCESSFULLY EEPROM # & EDITION WAS CHANGED FROM <edition> to <edition>
- UPDATE EEPROM #& INFO : # OF REWRITES :&$
- UPGRADE EEPROM #& WITH <file name> COMPLETED SUCCESSFULLY EEPROM #& EDITION WAS CHANGED FROM <edition> TO <edition>
- UPGRADE EEPROM # & INFO : # OF REERASES : &$ OF REWRITES : &$
- If the loading process is aborted the text field will read: TASK ABORTED WHILE LOADING EEPROM
- HDLC Cside msg link GAINED sync - link 0
- HDLC Cside msg link LOST sync - link 2

XLIU ISTb messages

When congestion causes an X.25/X.75 link interface unit (XLIU) to go ISTb, the system issues a PM181 log. The system issues PM181 to provide the reason for the congestion. The following table lists XLIU ISTb messages. These messages use the following acronyms:

- packet (PKT)
- buffer management system (BMS)
- dynamic window (DW)
- HDLC frame processor (HFP)
- HFP buffer management (HBM)
- receiver not ready (RNR)
- layer two (L2)

XLIU ISTb messages

XLIU message	Explanation	Action
PKT drop threshold reached.	ISTb condition	There is no action required.
BMS DW congestion threshold reached.	ISTb condition	There is no action required.
HBM DW congestion threshold reached.	ISTb condition	There is no action required.
BMS RNR@L2 threshold reached.	ISTb condition	There is no action required.

PM185

Log report PM185 gives the trace back of the last trap that caused a peripheral to start again.

Format

The format for log report PM185 is as follows:

```
PM185 date time seqnbr TBL PM TRAP pmtype pmnbr
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
pmtype	alphabetic	The peripheral module type.
pmnbr	0000-9999	The peripheral module number.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

PM720

This log report is produced whenever an unsolicited maintenance message is received in the Core from a GWC indicating that a certain number of service ports are to be placed in or out of service. These service ports represent the capability of the subtending UAS to process announcement and conference calls.

Format

The format for log report PM720 is as follows:

```
PM720 mmmdd hh:mm:ss ssdd INFO SERVICE CHANGE pmid
    Mtc Request: <request type>
    Service: <aaaa>  Ports: <nnnn>
    <warning text>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
INFO SERVICE CHANGE	Symbolic text	Information concerning service change request from GWC.
pmid	Symbolic text	Identifies the affected Audio Server node (subtending the GWC).
Mtc Request:	POOL INIT POOL BUSY POOL GRACEFUL BUSY POOL RTS or NODE GRACEFUL BUSY	Identifies the type of service change requested: POOL INIT - indicates that the pool of ports associated with the given service has been initialized. POOL BUSY - indicates that a number of ports associated with the given service are being taken out of service. Active calls involving any of the ports being taken out of service will also be taken down. POOL GRACEFUL BUSY - same as POOL BSY except that outstanding calls are not affected. POOL RTS - indicates that a number of ports associated with the given service are being returned to service. NODE GRACEFUL BUSY - indicates that all ports associated with all services on the node are being taken out of service. However, active calls involving these ports are not affected.
Service:	ANNC, CONF, BCT or ALL	Identifies the service for which the service change is being requested: ANNC - announcements CONF - conferencing BCT - Bearer Channel Tandeming ALL - all services (only applicable to the NODE GRACEFUL BUSY mtc request)
Ports:	Symbolic text	Indicates the number of ports affected for the given service.
<warning text>	Symbolic text	Optional field which applies to POOL INIT requests only. It identifies a mismatch between the data provided by the GWC and the values provisioned in table SERVSINV for the option(s) identified.

Action

Action is required whenever the following warning text is present:

Warning: SERVSINV mismatch detected

Do one of the following:

- Assign one or more of the options ANNC, 3PORT and/or 6PORT in table SERVSINV.
- Change the values of the options ANNC, 3PORT and/or 6PORT in table SERVSINV to correspond with the values which appear in the log report.

Associated OM registers

This log is associated with the following usage registers in OM group AUDSRVS:

- ANNCINSU - indicates the number of ANNC ports which are currently in an in-service state
- CNF3INSU - indicates the number of 3PORT conference circuit ports which are currently in an in-service state
- CNF6INSU - indicates the number of 6PORT conference circuit ports which are currently in an in-service state
- ANNCOOSU - indicates the number of ANNC ports which are currently in an out-of-service state
- CNF3OOSU - indicates the number of 3PORT conference circuit ports which are currently in an out-of-service state
- CNF6OOSU - indicates the number of 6PORT conference circuit ports which are currently in an out-of-service state

Additional information

This log report requires no additional information.

PM777

Log report PM777 is generated when the software detects a hardware defect. This log indicates the source of the defect.

Format

The format for log report PM777 is as follows:

```
PM777 mmmdd hh:mm:ss ssdd INFO SUSPECTED H/W FAULT pmid
   unit no.
   PP TIME: hh:mm:sshs
   ERROR STATE: xxxxxxxxxxxxxxxxx
   SUSPECTED CARD(S):
   SITE FLR RPOS BAY ID SHF DESCRIPTION SLOT EQPEC
   host fl# row# bay id sh# frame# slot# cardid
   DATA: xx xx xx xx xx xx xx
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
INFO SUSPECTED H/W FAULT	Symbolic text	Indicates the PM with the suspected hardware defect.
unit no.	Integers	Indicates the unit number.
PP TIME	Integers	Indicates the time of the defect.
ERROR STATE	Symbolic text	Indicates the error state.
SUSPECTED CARD(S)	Numeric	Indicates the suspect cards.
DATA	Alphanumeric	Indicates more information about the defect.

Action

Follow standard maintenance procedures.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC300

Log report GWC300 indicates an “Active unit disabled.” Unit Out of Service: Service is not available or Invalid GWC Profile Data. The alarm severity is Critical.

Format

The format for log report GWC300 is as follows:

```
COMPACT2 *** GWC300 JUN30 11:01:55 0580 TBL GWC Fault
      Location: GWC-0-UNIT-0
      NotificationID: 1
      State: Raise
      Category: Quality of Service
      Cause: Underlying resource unavailable
      Time: Jun 30 11:09:16 2003
      Component Id: GWC-0-UNIT-0
      Specific Problem: Unit Out of Service: Service is not available
      Description: Active unit disabled.
```

Selected field descriptions

This log report has no selected fields.

Action

See the following table:

Specific problem **Probable cause**	**Action**
Specific problem: Indicates that a unit is out of service: Service is not available. Probable cause: the lack of availability of the underlying resource.	This log reports that the unit is not in service (Operational state of "disabled"). If the Administrative state is “unlocked” and the Usage state is “busy” this indicates the unit is trying to recover itself to an in service state. Note that when both units are out of service, the active unit must recover before the standby unit will. Check the following: 1- Whether the unit is manually locked out of service (Administrative state of “locked”). 2- Alarms that may indicate a problem on the unit preventing it from returning to service. 3- Other state indicators which may indicate problems, such as - Isolation state of “isolated” - If it is the standby unit, Availability state of “degraded” - Availability state of “offLine” 4- Logs which may also indicate a failure of a step in the process of recovering the unit.
Specific problem: Indicates that a unit has invalid GWC Profile Data: Service is not available. Probable cause: A configuration or customization error	Check the profile data for the unit and do one of the following: - Change to another profile. - Reconfigure the GWC unit software or CS 2000 GWC Manager software to remove the incompatibility. Then, RTS the unit.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC301

Log report GWC301 indicates a "Standby unit disabled." Unit Out of Service: Service is not available or Invalid GWC Profile Data. The alarm severity is Minor or Major.

Format

The format for log report GWC301 is as follows:

```
COMPACT2 * GWC301 JUN30 11:02:44 0588 TBL GWC Fault
       Location: GWC-0-UNIT-1
       NotificationID: 1
       State: Raise
       Category: Quality of Service
       Cause: Underlying resource unavailable
       Time: Jun 30 10:54:34 2003
       Component Id: GWC-0-UNIT-1
       Specific Problem: Unit Out of Service: Service is not available
       Description: Standby unit disabled.
```

Selected field descriptions

This log report has no selected fields.

Action

See the following table:

Specific problem Probable cause	Action
Specific problem: Indicates that a unit is out of service: Service is not available. Probable cause: the lack of availability of the underlying resource.	This log reports that the unit is not in service (Operational state of "disabled"). If the Administrative state is “unlocked” and the Usage state is “busy” this indicates the unit is trying to recover itself to an in service state. Note that when both units are out of service, the active unit must recover before the standby unit will. If the Operational state “disabled” and Administrative state is “unlocked”, the unit is system busy (SysB) - the alarm is major. If the Operational state “disabled” and Administrative state is “locked”, the unit is manually busy (ManB) - the alarm is minor. Check the following: 1- Alarms that may indicate a problem on the unit preventing it from returning to service. 2- Other state indicators which may indicate problems, such as - Isolation state of “isolated” - Availability state of “offLine” 3- Logs which may also indicate a failure of a step in the process of recovering the unit.
Specific problem: Indicates that a unit has invalid GWC Profile Data: Service is not available. Probable cause: A configuration or customization error	Check the profile data for the unit and do one of the following: - Change to another profile. - Reconfigure the GWC unit software or CS 2000 GWC Manager software to remove the incompatibility. Then, RTS the unit.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC302

Log report GWC302 indicates a Major for active unit; Minor for inactive unit. "Core communication lost." No response received to Core heartbeat messages.

Format

The format for log report GWC302 is as follows:

```
COMPACT06BT * GWC302 JUL1 15:02:21 0055 TBL GWC Fault
        Location: GWC-2-UNIT-0
        NotificationID: 3
        State: Raise
        Category: Communications
        Cause: LAN error
        Time: Jul 01 15:02:27 2003
        Component Id: GWC=GWC-2-UNIT-0;Version=PGC91AQ;Unit=unit_0;
            Software=NODE MTC
        Specific Problem: No response received to Core heartbeat messages.
        Description: Core communication lost.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log clears automatically after a Core or network outage clears. Otherwise, verify that the node number and Core Side IP address is correct for the GWC to communicate with the Core.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC303

Log report GWC303 indicates a "Mate unit communication lost." No response received to mate heartbeat messages. The alarm severity is Minor.

Format

The format for log report GWC303 is as follows:

```
COMPACT2 * GWC303 JUN30 11:02:47 0589 TBL GWC Fault
      Location: GWC-0-UNIT-0
      NotificationID: 4
      State: Raise
      Category: Communications
      Cause: LAN error
      Time: Jun 30 11:10:08 2003
      Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
          Software=NODE MTC
      Specific Problem: No response received to mate heartbeat messages.
      Description: Mate unit communication lost.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by restoring communication from the CS 2000 GWC Manager to the GWC unit. Do this by unlocking the GWC at the CS 2000 SAM21 Manager. Also, verify that the Ethernet cable is connected, and that the GWC is setup to use the correct node number.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC304

Log report GWC304 indicates that communication with a gateway is down. The alarm severity is Major.

> ***Note:*** In the case of H.323 GWCs, this log report is generated only for H.323 gateways that contain 64 endpoints or greater.

Format

The format for log report GWC304 is as follows:

```
COMPACT2 ** GWC304 JUL2 01:25:58 0619 TBL GWC Fault
       Location: GWC-1-UNIT-1
       NotificationID: 78
       State: Raise
       Category: Communications
       Cause: Underlying resource unavailable
       Time: Jul 02 01:21:20 2003
       Component Id: GWC=GWC-1-UNIT-1;Version=PGT09BL;
             Unit=unit_1;Software=SSC
       Specific Problem: TESTPVG
       Description: Communication with a gateway is down.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by restoring communication to the managed gateway. Do this by verifying the availability of the gateway, and comparing the configuration data at the Gateway and the CS 2000 GWC Manager (IP address, protocol/version, etc).

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC305

Log report GWC305 indicates that a test alarm is generated from pmdebug interface to log in to the notilog table. May be any level.

Format

The format for log report GWC305 is as follows:

```
COMPACT2 *** GWC305 JUL10 09:56:30 0671 TBL GWC Fault
      Location: GWC-0-UNIT-0
      NotificationID: 12
      State: Raise
      Category: Communications
      Cause: Unspecified reason
      Time: Jul 10 10:07:23 2003
      Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
          Software=DEBUG
      Specific Problem: Alarms test from debug interface
      Description: This is a test alarm generated from pmdebug interface.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by using the pmdebug command (not a customer interface) or with a GWC reload.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC306

Log report GWC306 indicates a DQoS/COPS connection failure. The alarm severity is major.

Format

The format for log report GWC306 is as follows:

```
COMPACT2 ** GWC306 JUL10 09:56:31 0672 TBL GWC Fault
       Location: GWC-0-UNIT-0
       NotificationID: 13
       State: Raise
       Category: Communications
       Cause: Communications subsystem failure
       Time: Jul 10 10:07:24 2003
       Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
            Software=DQOS MTC
       Specific Problem: DQoS connection CMTS065 has failed - attempting
            rec overy.
       Description: DQoS/COPS connection failure.
```

Selected field descriptions

This log report has no selected fields.

Action

The DQoS connection loss alarm is cleared by DCCNXMGR (using DCALARM) when the connection is reestablished or the connection is deleted from provisioning.

Associated OM registers

This log report has no associated OM registers.

Additional information

When a dynamic quality of service (DQoS) connection is down between the CS 2000 and a CMTS, the CS 2000 will allow new calls hosted by that CMTS to proceed without DQoS. The behavior of the multimedia terminal adapter (MTA) and CMTS determines whether new calls are attempted using best-effort service or whether they are torn down:

- Some MTA vendors allow calls to proceed as data calls (best-effort) and do not send a data-over-cable service interface specification (DOCSIS) authorization block to the CMTS. In this case, the CMTS cannot recognize the call as a voice call and so it proceeds without managed quality of service.

- Other MTA vendors send the DOCSIS authorization block to the CMTS with no authorization key or gate-id. When this happens, the CMTS decides whether or not to allow calls to proceed.

When the DQoS connection is up, but the CS 2000 does not receive a DQoS gate-id from the CMTS, the CS 2000 will tear down a call.

GWC307

Log report GWC307 indicates an "Element Manager communication failure." EM indicates provisioned data mismatched in this unit, or EM is not responding, provisioned data loaded from local Flash. The alarm severity is Major.

Format

The format for log report GWC307 is as follows:

```
COMPACT06BT ** GWC307 JUL1 10:45:47 0028 TBL GWC Fault
        Location: GWC-3-UNIT-1
        NotificationID: 10
        State: Raise
        Category: Communications
        Cause: Communications subsystem failure
        Time: Jul 01 10:45:51 2003
        Component Id: GWC=GWC-3-UNIT-1;Version=PGC91AQ;Unit=unit_1;
            Software=NODE MTC
       Specific Problem: EM indicates provisioned data mismatched in this
            unit
        Description: Element Manager communication failure.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared with a Busy/RTS of GWC unit.

Restore communication with the CS 2000 GWC Manager. Determine if the CS 2000 GWC Manager is down and or disconnected. Determine if the GWC has been setup to use the wrong IP address for the CS 2000 GWC Manager at the CS 2000 SAM21 Manager.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC308

Log report GWC308 indicates a "Flash memory error." Erase of Flash sector failed. The alarm severity is Minor

Format

The format for log report GWC308 is as follows:

```
COMPACT2 * GWC308 JUL10 09:56:37 0675 TBL GWC Fault
       Location: GWC-0-UNIT-0
       NotificationID: 16
       State: Raise
       Category: Equipment
       Cause: Equipment Malfunction Time: Jul 10 10:07:23 2003
       Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
            Software=FLAS H
       Specific Problem: Erase of Flash sector failed
       Description: Flash memory error.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by replacing the hardware.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC309

Log report GWC309 indicates that the number of the security associations (SA) that the system can support has been exceeded. The associated alarm severity is Minor.

Format

The format for log report GWC309 is as follows:

```
GWC309 AUG10 14:15:09 0674 TBL GWC Fault
    Location: GWC-12-UNIT-0
    Component ID: GWC=GWC-12-UNIT-0;Version=GN070BV;Unit=unit_0;
                  Software=Signalling security
    Alarm Level: Minor
    Alarm Description: Security SAs are nearing capacity
    Category: Processing Error
    Alarm Time: 14:05:10 10-Aug-2004 EDT
    Probable Causes: Resource at or nearing capacity
    Specific Problem: SA nearing capacity
    System Uptime: 1 hours, 0 minutes, 45 seconds
```

Selected field descriptions

This log report has no selected fields.

Action

This log is associated with a minor information alarm. Report this alarm with details to your next level of support. Note that the alarm clears automatically as SA usage decreases.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC311

Log report GWC311 indicates a Warning. "Provisioned GWC Profile not yet activated." The GWC Profile loaded into Flash will activate on the next reload.

Format

The format for log report GWC311 is as follows:

```
COMPACT06BT GWC311 JUL1 10:39:56 0022 TBL GWC Fault
        Location: GWC-3-UNIT-0
        NotificationID: 12
        State: Raise
        Category: Quality of Service
        Cause: Configuration or customization error
        Time: Jul 01 10:40:03 2003
        Component Id: GWC=GWC-3-UNIT-0;Version=PGC91AQ;Unit=unit_0;
             Software=CONFIG
        Specific Problem: GWC Profile loaded into Flash will activate on
             next reload.
        Description: Provisioned GWC Profile not yet activated.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by reloading the GWC.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC312

Log report GWC312 indicates a QCA connection failure, either a major alarm (partial outage) or a critical alarm (total outage).

Format

The format for log report GWC312 is as follows:

```
COMPACT2 *** GWC312 JUN30 11:02:37 0586 TBL GWC Fault
       Location: GWC-0-UNIT-0
       NotificationID: 3
       State: Raise
       Category: Communications
       Cause: Communications subsystem failure
       Time: Jun 30 11:09:58 2003
       Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
            Software=QCAMTC
      Specific Problem: QCA connection <qca_47.142.130.70 Port # 20000> has
            failed - attempting recovery.
      Description: QCA connection failure
```

Selected field descriptions

This log report has no selected fields.

Action

No reports are lost since they are collected on a backup server.

- Ensure that the QCA contains the correct properties (port, IP address, etc). Check that the QCA is properly provisioned using the CS 2000 Management Tools.
- Use the ping command to see if you can reach the QCA server. If you cannot reach the server, there may be a problem in the network.
- Verify that there is no memory exhaustion on the QCA server.
- To bring up the links, restart the QCA application on the server.
- Try connecting to a QCA on another CS 2000 Management Tools server.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC313

Log report GWC313 indicates that "RMGC is overloaded." The corresponding alarm severity is Major.

> ***Note:*** RMGC stands for Redirecting Media Gateway Controller.

The specific problem is that RMGC cannot process all incoming requests. The probable cause is that the resource at or nearing capacity.

Format

The format for log report GWC313 is as follows:

```
COMPACT2 *** GWC313 JUN30 11:02:37 0586 TBL GWC Fault
       Location: GWC-0-UNIT-0
       NotificationID: 3
       State: Raise
       Category: Communications
       Cause: Communications subsystem failure
       Time: Jun 30 11:09:58 2003
       Component Id: GWC=GWC-0-UNIT-0;
       Version=PGT09BL;Unit=unit_0;Software=RMGC
       Specific Problem: RMGC can't process all the incoming requests.
       Description: RMGC overloaded
```

Selected field descriptions

This log report has no selected fields.

Action

The RMGC is temporarily overloaded. The alarm corresponding to this log 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 should be able to register without any further intervention.

If the alarm corresponding to this log 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.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC314

Log report GWC314 indicates a Major alarm (partial outage). The Centrex IP Client Manager (CICM) location identification reporting application fails to establish a TCP/IP connection to the location recipient, or the established connection is broken.

Format

The format for log report GWC314 is as follows:

```
CS2K1 *** GWC314 JUN30 11:02:37 0586 TBL GWC Fault
     Location: GWC-213-UNIT-0
     NotificationID: 3
     State: Raise
     Category: Processing Error
     Cause: Communications subsystem failure
     Time: Jun 30 11:09:58 2003
     Component Id: GWC=GWC-213-UNIT-0;Version=GI070BCD;Unit=unit_0;
          Software=LocIdRep
     Specific Problem: Location Id Reporting connection <47.30.178.20>
          has failed - attempting recover
     Description: Location Id Reporting connection failure
```

Selected field descriptions

This log report has no selected fields.

Action

Clear the alarm condition using one of the following approaches:

- Re-establish the connection to the location recipient.
- Disable the location ID reporting application.
- Busy/RTS the GWC unit.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC399

Log report GWC399 clears all other GWC logs.

> ***Note:*** In the case of H.323 GWCs, this log report is generated only for H.323 gateways that contain 64 endpoints or greater.

Format

The format for log report GWC399 is as follows:

```
MSH10_IO6BR      GWC399 MAY26 13:38:30 0529 INFO GWC Fault
        Location: GWC-2-UNIT-1
        NotificationID: 6
        State: Clear
        Time: May 26 13:38:40 2003
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC400

Log report GWC400 is an information-only log and there is no alarm associated with it. Log GWC400 provides IPSec-associated metrics, that is, the log reports how many times an event occurs within a 15-minutes interval. This log is generated every 15 minutes.

Format

The format for log report GWC400 is as follows:

```
GWC400 mmd/dd hh:mm:ss <sequence number> INFO SUMM Security Metrics Summary
Location: GWC-<node number>-UNIT-<unit_number>
AP_REQ: <numeric value>
WAKEUP: <numeric value>
SA_SUCCESS: <numeric value>
SA_FAIL: <numeric value>
SUSPICIOUS_FAIL: <numeric value>
```

Selected field descriptions

The following table explains selected fields in the log report.

Field	Value	Description
sequence number	0000-9999	Four digit sequence number identifying a specific log entry.
node number	numeric	Identifies the GWC node, for example, GWC-6.
unit number	0 or 1	Identifies the GWC unit, 0 or 1.
AP_REQ: <numeric value>	numeric	Identifies how many times the Kerberos application on the GWC received an AP_REQ message.
WAKEUP: <numeric value>	numeric	Identifies how many times the Kerberos application on the GWC sent a wake-up request.
SA_SUCCESS: <numeric value>	numeric	Identifies how many SAs have been successfully established on the GWC.

Field	Value	Description
SA_FAIL: <numeric value>	numeric	Identifies how many times an attempt to establish SAs on the GWC has failed.
SUSPICIOUS_FAIL: <numeric value>	numeric	Identifies how many times an attempt to establish SAs has failed under suspicious circumstances, such as, encryption failure. Contact your next level of support when this event is listed.

Action

This log report requires no action. You can use it for maintenance and diagnostic purposes.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC501

Log report GWC501 indicates that there has been a connection fault between the GWC and the gateway which requires investigation.

Format

The format for log report GWC501 is as follows:

```
RTP4 GWC34    GWC501 JUN21 09:36:02 4767 PBSY GWC34_OrigGW35.rtp4.net
Reason: GW failed to respond to HeartBeat/Audit
```

Selected field descriptions

This log report has no selected fields.

Action

Verify the availability of the gateway and compare the configuration data at the gateway and the CS 2000 GWC Manager (IP address, protocol/version, etc).

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC502

Log report GWC502 indicates that service has been restored to the referenced gateway.

Format

The format for log report GWC502 is as follows:

```
RTP4 GWC34    GWC502 JUN21 09:36:11 4852 RTS   GWC34_OrigGW27.rtp4.net
Connection to remote gateway restored: GWC34_OrigGW27.rtp4.net
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC503

Log report GWC503 indicates that the gateway has requested that service become interrupted because of a fault condition on the gateway.

Format

The format for log report GWC503 is as follows:

```
RTP4 GWC32    GWC503 JUN21 10:41:56 9371 OFFL GWC32_OrigGW99.rtp4.net
Connection drop initiated by remote gateway: GWC32_OrigGW99.rtp4.net
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC506

Log report GWC506 indicates that an H.323 GWC unit has lost the connection to an H.323 gateway. The log entry identifies the specific problem and describes the reason for the failure.

This log report recommends a set of actions that depend on the specific problem and reason for the problem.

> ***Note:*** This log report is generated only for H.323 gateways that contain less than 64 endpoints.

Format

The format for log report GWC506 is as follows:

```
RTPG GWC11 GWC600 MAY21 14:54:47 <sequence number> PBSY Gateway State Change
        Category: Communication
        Component Id: GWC=<GWC node/unit>;LINK=<gateway name>
        Specific Problem: H323 Connection lost to gateway <gateway name>
        Description: <reason for problem>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
sequence number	0000-9999	Four digit sequence number identifying a specific log entry.
GWC node / unit	Alpha-numeric text label	Identifies the GWC node and unit affected by the failure. Example: GWC-11-UNIT-0
gateway name	Alpha-numeric text label	Identifies the gateway connected to the GWC card affected by the failure condition. Example: BCM_RTPG1
reason for problem	Text description	Describes the specific reason for the failure.

Action

The following table describes the actions the user may take when a GWC experiences a loss of connection to an H.323 gateway.

Actions associated with a loss of connection to an H.323 gateway

Description	Action
Gateway Unregistration by CS2K Successful	No action required. The craftsperson has busied the D-channel for the H.323 gateway, or the CS 2000 has busied the D-channel for H.323 gateway due a maintenance action such as GWC cold SWACT, CS 2000 restart reload, etc.
Time to Live Expired	The H.323 gateway failed to refresh the 30 second keepalive timer in the CS 2000 GWC. Verify communication between the gateway and the GWC. If necessary, check the H.323 gateway itself since the CS 2000 GWC unregistered the H.323 gateway because the Time To Live value has expired.
Gateway Initiated Unregistration Successful	The H.323 gateway initiated the unregistration from the CS 2000 for some reason. Action on the H.323 gateway side may be warranted if the Unregistration was unplanned.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

GWC507

Log report GWC507 indicates that the connection between a GWC and an H.323 gateway has been restored.

> ***Note:*** This log report is generated only for H.323 gateways that contain less than 64 endpoints.

Format

The format for log report GWC507 is as follows:

```
RTPG GWC4  GWC507 AUG02 14:15:28 <sequence number> RTS Gateway State Change
        Category: Communication
        Component Id: GWC=<GWC node/unit>;LINK=<gateway name>
        Specific Problem: H323 Connection restored to gateway <gateway name>
        Description: Gateway Registration Successful
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
sequence number	0000-9999	Four digit sequence number identifying a specific log entry.
GWC node / unit	Alpha-numeric text label	Identifies the GWC node and unit affected by the failure. Example: GWC-11-UNIT-0
gateway name	Alpha-numeric text label	Identifies the gateway connected to the GWC card affected by the failure condition. Example: BCM_RTPG1

Action

No action is required.

You may verify that the D-channel has gone in service (INSV) at the MAPCI;MTC:TRKS; TTP; PRADCH; POST GD <trkname >. If any trunk members are provisioned and you wish to be able to make calls, then check the trunk members to see that they are also idle (IDL).

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

GWC600

Log report GWC600 is an information log for an H.323 failure. The log entry identifies the specific problem and describes the reason for the failure.

This log report recommends a set of actions that depend on the specific problem and reason for the problem.

Format

The format for log report GWC600 is as follows:

```
RTPG GWC11 GWC600 MAY21 14:54:47 <sequence number> INFO GWC Protocol Event
        Category: Communication
        Component Id: GWC=<GWC node/unit>;LINK=<gateway name>
        Specific Problem: <specific problem>
        Description: <reason for problem>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
sequence number	0000-9999	Four digit sequence number identifying a specific log entry.
GWC node / unit	Alpha-numeric text label	Identifies the GWC node and unit affected by the failure. Example: GWC-11-UNIT-0
gateway name	Alpha-numeric text label	Identifies the gateway connected to the GWC card affected by the failure condition. Example: BCM_RTPG1
specific problem	Text description	Identifies the H.323 failure condition.
reason for problem	Text description	Describes the specific reason for the failure.

Action

The following table describes the actions the user takes when an H.323 failure condition occurs.

Note:
GRQ = Gatekeeper request
RRQ = Registration request
ARQ = Admission request
URQ = Unregistration request
DRQ = Disengage request
RAS = Registration, admission and status

Actions associated with an H.323 failure (Sheet 1 of 4)

Specific problem	Description	Action
H323 GRQ rejected	Gateway Name Not Provisioned ***Note:*** A log with same description is generated for RRQ received with invalid GW name.	Ensure that the H.323 gateway name provisioned on the CS 2000 GWC Manager matches exactly with the gateway name provisioned using the H323 GW provisioning tool.
H323 GRQ rejected	Gateway IP Address Invalid ***Note:*** A log with same description is generated for RRQ received with an invalid source gateway IP address. In this case, the source IP address is the IP address in the ethernet frame. So, for gateways behind the NAT, the source IP address will be the NAT IP address. The RAS IP address is not part of the H.323 payload. If the H.323 gateway is not behind a NAT, the source IP will be the IP address of the H.323 gateway.	If the H.323 gateway is behind the NAT: • Ensure that the H.323 gateway IP address provisioned on the CS 2000 GWC Manager matches exactly the IP address of the NAT box. If the H.323 Gateway is not behind a NAT box: • Ensure that the H.323 gateway IP address provisioned on the CS 2000 GWC Manager matches exactly the IP address of the H323 gateway.

Actions associated with an H.323 failure (Sheet 2 of 4)

Specific problem	Description	Action
H323 GRQ rejected	Gateway Port Invalid ***Note:*** A log with same description is generated for an RRQ received with an invalid source gateway port. In this case, the source port is the source port address in the ethernet frame. So, for gateways behind a NAT, the source port is the port entry of the static bind at the enterprise NAT for the H323 gateway. It is not the RAS port which is part of the H323 payload. If the H323 Gateway is not behind a NAT, the source port will be the RAS port of the H323 gateway.	If the H.323 gateway is behind the NAT: • Ensure that the H.323 gateway port provisioned on the CS 2000 GWC Manager matches exactly the port entry of the static bind at the enterprise NAT for the H323 gateway. If the H.323 Gateway is not behind a NAT box: • Ensure that the H.323 gateway IP address provisioned on the CS 2000 GWC Manager matches exactly the IP address of the H323 gateway.
H323 GRQ rejected	Missing Mandatory RAS Address	No action needed. This log report is for information only.
H323 RRQ rejected	Incorrect Endpoint Identifier Syntax	No action needed. This log report is for information only.
H323 keepAlive RRQ rejected	Incorrect Endpoint Identifier Syntax	No action needed. This log report is for information only.
H323 RRQ rejected	Invalid Endpoint Identifier	No action needed. This log report is for information only.
H323 ARQ rejected	Invalid Endpoint Identifier	No action needed. This log report is for information only.
H323 RRQ rejected	D-Channel Not Provisioned	Ensure that the trunk datafill is provisioned correctly on the CS 2000 XA-Core and CS 2000 GWC Manager.

Actions associated with an H.323 failure (Sheet 3 of 4)

Specific problem	Description	Action
H323 RRQ rejected	D-Channel Out Of Service	Ensure that the D-channel associated with the H.323 gateway is in LO state at mapci, mtc, ttp, trks, pradch level on the CS 2000 Core before the H.323 gateway registers. This log can be cleared with a BSY/RTS of the D-channel associated with the H.323 gateway on the CS 2000 Core. ***Note:*** Trunk logs are also generated which are similar to PRI trunk logs. For example, H.323 gateway “BCM_RTPG” appears on the XA-Core as trunk name “RTPG_BCM_LOCAL” Refer to section Additional information on page 248 for examples of XA-Core logs.
H323 RRQ rejected	Table LTDATA Needs H323 Option	Check the datafill in Table LTDATA on the CS 2000 Core. The option PRI_IP_PROT H323 should be present for the D-channel associated with the H.323 gateway.
H323 RRQ rejected	Max Gateways Registered	No action needed. This log report is for information only. The CS 2000 GWC has reached the maximum limit for the number of H.323 gateways it can have registered simultaneously.
H323 ARQ rejected	B-Channel Resource Unavailable	Ensure that B-channels associated with the gateway are idle (IDL) at mapci, mtc, ttp, trks level on the CS 2000 XA-Core. This log can be cleared with a BSY/RTS of the B-channels associated with the H.323 gateway on the CS 2000 XA-Core. If all the B-channels associated with the H.323 gateway are call processing busy (CPB) at mapci, mtc, ttp, trks level on the CS 2000 XA-Core, then no action is needed. There is no B-channel available for the call. This log report is for information.

Actions associated with an H.323 failure (Sheet 4 of 4)

Specific problem	Description	Action
H323 RRQ rejected	No GWC Unit Active Running ***Note:*** A log with the same description will be generated if any RAS message (GRQ, RRQ, ARQ, URQ, DRQ) is received when the GWC unit is not active running. This log can be cleared with a BSY/RTS of GWC unit.	Ensure that the CS 2000 GWC is in active running state. This log can be cleared with a BSY/RTS of GWC unit.
H323 DRQ rejected	Request to Drop Non Existent Call	No action needed. This log report is for information only. This reports a disengage request for a call which is not active or non-existent.
H323 URQ rejected	Endpoint Not Registered	A RAS request is received from a H.323 gateway which is not registered on the CS 2000 GWC. Verify that the H.323 gateway is provisioned on the CS 2000 GWC.
H323 Call rejected	Codec Mismatch With CS2K	Ensure that at least one of the codecs provisioned on the H323 gateway matches the codec for the CS 2000 provisioned at the CS 2000 GWC Manager.
H323 Call rejected	Codec / Payload Mismatch With CS2K	Ensure that at least one of the codecs provisioned on the H323 gateway matches the codec for the CS 2000 provisioned at the CS 2000 GWC Manager. Ensure that the payload (packetization) time on the H323 gateway matches the payload (packetization) for the CS 2000 provisioned at the CS 2000 GWC Manager.
H323 Call rejected	H245 Tunneling Not Enabled On Gateway	Ensure that H.245 tunneling is enabled on the H.323 gateway.

Associated OM registers

This log report has no associated OM registers.

Additional information

This section provides examples of XA-Core logs relevant to

- Specific problem: H323 RRQ rejected
- Description: D-Channel Out Of Service.

Examples of XA-Core logs when the D-channel is manually busied (BSY):

```
RTPG * ISDN105 JUN16 21:45:44 2311 FLT PRA Sync Loss
    ISP = 0 GWC 11 PORT 0 CHNL 0

RTPG *** ISDN112 JUN16 21:45:44 2412 INFO PRA D-CHANNEL
   CRITICAL ALARM RTPG_BCM_LOCAL DCH=GWC 11 120 1 : OOS

RTPG *** TRK103 JUN16 21:45:49 2917 FLT GROUP_ALARM
    RTPG_BCM_LOCAL 100% BUSY
```

Examples of XA-Core logs when the D-channel is returned to service (RTS) and the gateway registers with GWC:

```
RTPG ISDN118 JUN16 21:46:52 6654 INFO PRA Sync Established
    ISP = 0 GWC 11 Port 0 Chnl 0

RTPG TRK104 JUN16 21:46:56 7462 INFO GROUP OK
    RTPG_BCM_LOCAL
```

Kerberos logs

This section describes how to access and understand log reports associated with the Kerberos application running on the GWC card. These log reports are stored in the securitylog files in directory /var/log on the CS 2000 Management Tools server.

To access the Kerberos log reports, follow procedure “View GWC logs in syslog files” in the Gateway Controller Fault Management NTP, NN10202-911.

> ***Note:*** To display Kerberos log reports, search for the text string KERBEROS (common name for all Kerberos logs).

You can also access the Kerberos log reports through the Integrated Element Management System (EMS). For more information, refer to the Integrated EMS Fault Management NTP, NN10334-911.

Format

The format for Kerberos log reports is as follows:

```
mmm dd hh:mm:ss [<host name>] KERBEROS <log description>, IP=<remote IP
address>
```

Selected field descriptions

The following table explains selected fields in the log report.

Field	Value	Description
mmm dd hh:mm:ss	alphanumeric	The date and time stamp for the log report. ***Note:*** mmm means three first letters of the month, for example, Aug.
<host name>	numeric	The IP address of the GWC.
KERBEROS	text string	Common name for all Kerberos log reports.

Field	Value	Description
<log description>	alphanumeric character string	A description of the conditions or reasons generating the log. The log can be static or variable. Refer to the Action section for the list of log descriptions, causes, and associated actions.
<remote IP address>	numeric	The IP address of the remote gateway.

Action

The following tables list the static and variable Kerberos logs. Use these tables to determine your action.

GWC Kerberos static logs (Sheet 1 of 3)

Kerberos application log description	Cause or condition	Action
WAKE_UP timeout after %d ms, exhausted after %d retries	gateway fails to respond to WAKE_UP request	verify connectivity between the GWC and the gateway
AP_REP timeout after %d ms, exhausted after %d retries	gateway fails to respond to AP_REP (a request for a security association)	verify connectivity between the GWC and the gateway
AP_REP timeout after %d ms, retry attempt is now %d	gateway fails to respond to AP_REP (a request for a security association)	verify connectivity between the GWC and the gateway
failed to get FQDN	gateway is not provisioned at the GWC	verify gateway's authenticity and provision gateway
Cannot exceed maximum of %d KM sessions	a large number of gateways try to recover or restore connectivity at once	information-only log
Received AP_REQ while waiting for SA_RECOVERED	race condition, or gateway did not receive AP_REP request	information-only log

GWC Kerberos static logs (Sheet 2 of 3)

Kerberos application log description	Cause or condition	Action
unsolicited SA_RECOVERED	gateway sends an SA_RECOVERED message. Possible cause is the gateway is responding to an old AP_REP (the session was deleted on the GWC).	information-only log
Received SA_RECOVERED while responder for existing key neg	gateway sends an SA_RECOVERED message whereas the server didn't ask for it.	information-only log
Received SA_RECOVERED out of order	gateway sends an SA_RECOVERED message whereas the server was not waiting for this message type	information-only log
CMS nonce is zero in AP_REQ reply to WAKE_UP	race condition, an AP_REQ was initiated by the GW at the same time that a WAKE_UP was sent from the GWC	information-only log
CMS nonce mismatch in AP_REQ reply to WAKE_UP	race condition, an AP_REQ was sent as a response to a previously initiated WAKE_UP	information-only log
Non-zero CMS nonce in initiator AP_REQ	race condition, an AP_REQ was sent by the GW as a response to a WAKE_UP after the WAKE_UP had already timed out	information-only log
For all the following static logs, contact your next level of support: MUTUAL REQUIRED not set in AP_REQ USE_SESSION_KEY (not supported) set in AP_REQ Sub-key in AP_REQ is not allowed		

GWC Kerberos static logs (Sheet 3 of 3)

Kerberos application log description	Cause or condition	Action
IP mismatch: fqdn=%s, ip=%s		
Failed HMAC in SA_RECOVERED		
NULL session key parsing AP_REQ but no KRB ERROR		
Note: Some log descriptions use variables such as %d or %s to indicate a numeric value is provided.		

GWC Kerberos variable logs

Kerberos application log description
The following log reports can be displayed with different <reasons>. Refer to table Kerberos log reasons for the list of possible reasons and the associated actions.
<reason> while making KRB_ERROR message
<reason> while checking AP_REQ proposal
<reason> while generating AP_REP sub-key
<reason> while adding pending incoming SA for AP_REQ
<reason> while adding pending outgoing SA for AP_REQ
<reason> while computing SA_RECOV HMAC
<reason> while committing SAs for AP_REQ
<reason> while parsing AP_REQ
<reason> while parsing KRB_AP_REQ
<reason> while verifying AP_REQ
<reason> while parsing SA RECOV
<reason> while verifying SA RECOV
<reason> while updating CLOCKSKEW
<reason> when parsing name \"%s\"
<reason> while updating server principal

Kerberos log reasons

Kerberos log reasons	Action
"No IPSEC policy match"	verify provisioning datafill; if required, configure an appropriate connection policy
"IPSEC ciphersuite is not supported"	verify encryption and authentication provisioning datafill
"No policy match for AP_REQ"	verify provisioning datafill
"Invalid SA lifetime"	verify provisioning datafill; make sure that the same values are configured on the GWC and the gateway
"Invalid ciphersuite"	verify provisioning datafill (encryption and authentication algorithms); make sure that the same values are configured on the GWC and the gateway
"No IPEC policy"	verify provisioning datafill
"Invalid IPSEC proposal"	verify provisioning datafill
"Invalid key length"	verify provisioning datafill
"Invalid renewal period"	verify provisioning datafill
"Ticket not yet valid"	synchronize the time between the GWC and KDC
"Clock skew too great"	synchronize the time between the GWC and the gateway
"Ticket expired"	no action required - gateway should automatically request a new ticket. If re-occurring, check the KDC status and configuration.
"Generic KRBKMP error'	information only
"Message out of order"	information only
"Generic error (see e-text)"	information only
For all other <reasons>, contact your next level of support.	

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

IKE logs

This section describes how to access and understand log reports associated with the Internet Key Exchange (IKE) system running on the GWC card. These log reports are stored in the securitylog files in directory /var/log on the CS 2000 Management Tools server.

To access the IKE log reports, follow procedure “View GWC logs in syslog files” in the Gateway Controller Fault Management NTP, NN10202-911.

> ***Note:*** To display IKE log reports, search for the text string ISAKMP_INFO or ISAKMP_FAIL (common names for all IKE logs).

You can also access the IKE log reports through the Integrated Element Management System (EMS). For more information, refer to the Integrated EMS Fault Management NTP, NN10334-911.

Format

The format for IKE log reports is as follows:

```
mmm dd hh:mm:ss [<host name>] ISAKMP_<INFO or FAIL> <log description>, (src
IP:<source_IP_address>, dst:<destination_IP_address>)
```

Selected field descriptions

The following table explains selected fields in the log report.

Field	Value	Description
mmm dd hh:mm:ss	alphanumeric	The date and time stamp for the log report. ***Note:*** mmm means three first letters of the month, for example, Aug.
<host name>	numeric	The IP address of the GWC.
ISAKMP_INFO or ISAKMP_FAIL	text string	Common names for all IKE log reports.

Field	Value	Description
<log description>	alphanumeric character string	A description of the conditions or reasons generating the log. Refer to the Action section for the list of log descriptions and associated actions.
<source IP address>	numeric	The IP address of the node initiating the negotiation.
<destination IP address>	numeric	The IP address of the destination node.

Action

The action depends on the log description. The following table lists the IKE log descriptions and associated actions.

GWC IKE logs

IKE log description	Action
No Preferences Match for IKE Phase 1 Negotiation	Ensure that the IPSec configuration values on the GWC and the gateway are the same.
No Preferences Match for IPSec Phase 2 Negotiation	Ensure that the IPSec configuration values on the GWC and the gateway are the same.
Phase 1 SA Successfully Established	Information-only log
Phase 2 SA Successfully Established	Information-only log

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

V5200

Log report V5200 generates this information report when the bearer channel connection (BCC) fails on a speech link.

Format

The format for log report V5200 is as follows:

```
V5200 mmmdd hh:mm:ss xxxx <log_type> <link_type> <pm_id>
   <interface_information>
   V5LINK No: <link_number> <chnl_number> V5ID: <ID>
   PORT: <pm_id> <P-side_link_number>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	FLT	Status. V5 link fault.
link_type	BCC	Fault occurred on BCC (speech) link.
pm _id	see subfields	Peripheral module (PM) identifier. Consists of subfields PM type and GPP PM number.
PM_type	GPP	V5 links always terminate on a GPP.
PM_number	0 to 255	Peripheral module number assigned to the GPP.
interface_information	alphanumeric string	Information. BCC failed on a speech link for one of the following reasons: • BCC allocation fails • BCC de-allocation fails • BCC audit fails
link_number	1 to 16	V5 AN C-side link number.
chnl number	0 to 31	channel number. PCM30 channel carrying BCC information on the V5.2 link.
V5ID	see subfields	V5 interface identifier. Equates to field AMCNO in table GPPTRNSL. composed of subfields; SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site designator.

Field	Value	Description
FRAME	0 to 511	Frame number of access node (AN) supplying the V5 interface. Entry can be unique within the site if office parameter, UNIQUE_BY_SITE_NUMBERING, in table OFCENG, is datafilled Y.
UNIT	0 to 9	Access node unit number
PORT	see subfields	GPP port of affected link. Consists of subfield pm_id.
pm _id	see subfields	Peripheral module (PM) identifier. Consists of subfields PM_type and PM_number.
PM_type	GPP	V5 links always terminate on a GPP.
PM_number	0 to 255	Peripheral module number assigned to the GPP.
P-side_link_number	0 to 47	GPP P-side PCM30 link number.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

V5201

Log report V5201 generates this information when a V5.2 link bearer channel control (BCC) request for a speech channel is rejected.

Format

The format for log report V5201 is as follows:

```
V5201 mmmdd hh:mm:ss xxxx <log_type> <link_type>
<interface_information>
Reason: <reason>
V5LINK No:<link_number> <chnl_number> <ID>
PORT: <GPP_number> <P-side_link_number>
 LEN: <line_equipment_number> DN: <directory number>
 <user_port_information>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	Status. Protection switching has occurred indicating a link with a C-channel has failed.
link_type	BCC	Fault occurred on BCC (speech) link.
interface_information	alphanumeric string	Information. BCC request rejected.

Field	Value	Description
Reason	alphanumeric string	Reason for failure. BCC request was rejected for one of the following reasons: • Connection already present on time slot to a different port. • Connection already present at PSTN user port to a different time slot. • User port not provisioned. • Invalid V5 time slot identification • Invalid V5 2048 Kbits/s link identification • V5 time slot(s) being used as physical C-channel(s). • Use port unavailable (blocked). • V5 link unavailable (blocked). • De-allocation cannot be completed due to incompatible data content. • De-allocation cannot be completed due to user port time slot(s) data incompatibility. • De-allocation cannot be completed due to port data incompatibility.
LINK_number	1 to 16	Number assigned to V5LINK at the access node (AN). Determined by order of datafill in table GPPTRNSL.
chnl_number	0 to 31	C-channel number. The bearer channel on the PCM30 V5.2 link.
ID	see subfields	V5 interface identifier. Equates to field AMCNO in table GPPTRNSL. composed of subfields; SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site designator.
FRAME	0 to 511	Frame number of access node (AN) supplying the V5 interface. Entry can be unique within the site if office parameter, UNIQUE_BY_SITE_NUMBERING, in table OFCENG, is datafilled Y.
UNIT	0 to 9	Access node unit number
PORT	see subfields	GPP port of affected link. Consists of subfields GPP PM number and P-side link number.
GPP_number	0 to 255	Peripheral module number assigned to the GPP.

Field	Value	Description
line_equipment_number	numeric	Virtual line equipment number from table LNINV assigned to line.
directory_number	numeric (up to 15 digits)	Directory number assigned to line.
user_port_information	alphanumeric string	Information. Failing user port or time slot identification.

Action

Determine the reason the V5 link has been blocked on the access node (AN) side.

Post the GPP P-side links.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

V5202

Log report V5202 generates this information report when a V5.2 link bearer channel control (BCC) audit request is incomplete.

Format

The format for log report V5202 is as follows:

```
V5202 mmmdd hh:mm:ss xxxx <log_type> <link_type>
<interface_information>.
Reason: <reason>
V5LINK No:<link_number> <chnl_number> <ID>
PORT: <GPP_number> <P-side_link_number>
 LEN: <line_equipment_number> DN: <directory_number>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	Status. Incomplete audit request occurred.
link_type	BCC	Fault occurred on BCC (speech) link.
interface_information	alphanumeric string	Information. BCC audit connection incomplete information element.
Reason	alphanumeric string	Reason for failure. BCC audit request was rejected for one of the following reasons: • Incomplete normal • Access network fault • User port not provisioned • Invalid V5 time slot identification • Invalid V5 2048 Kbits/s link identification • V5 time slot(s) being used as physical C-channel(s)
LINK_number	1 to 16	Number assigned to V5LINK at the access node (AN). Determined by order of datafill in table GPPTRNSL.
chnl_number	0 to 31	C-channel number. The bearer channel on the PCM30 V5.2 link.

Field	Value	Description
ID	see subfields	V5 interface identifier. Equates to field AMCNO in table GPPTRNSL. composed of subfields; SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site designator.
FRAME	0 to 511	Frame number of access node (AN) supplying the V5 interface. Entry can be unique within the site if office parameter, UNIQUE_BY_SITE_NUMBERING, in table OFCENG, is datafilled Y.
UNIT	0 to 9	Access node unit number
PORT	see subfields	GPP port of affected link. Consists of subfields GPP_PM_number and P-side_link_number.
GPP_number	0 to 255	Peripheral module number assigned to the GPP.
line_equipment_number	numeric	Virtual line equipment number assigned to line in table LNINV.
directory_number	numeric (up to 15 digits)	Directory number assigned to line.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

V5400

Log report V5400 generates this information report when the V5 CC Audit sends a V5 interface query message, and receives no reply message.

Format

The format for log report V5400 is as follows:

```
V5400 mmmdd hh:mm:ss xxxx <log_type> V5AUDIT GPP <gpp_no>
No reply from V5 Interface.
V5id: <ID>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	This field indicates V5 information that follows in field interface information.
gpp_no	0 to 255	Peripheral number assigned to GPP.
ID	see subfields	V5 interface identifier. Made of subfields SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site identifier.
FRAME	0 to 511	Frame number of the access node (AN) that supplies the V5 interface.
UNIT	0 to 9	AN node number.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

V5401

Log report V5401 generates this information report when a V5 Interface status mismatch occurs between the computing module (CM) and GPP.

Format

The format for log report V5401 is as follows:

```
V5401 mmmdd hh:mm:ss xxxx <log_type> V5AUDIT GPP <gpp_no>
V5 Interface activity status mismatch.
The interface status will be fixed to <status> on the LE.
V5id: <ID>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	This field indicates V5 information that follows in field interface information.
gpp_no	0 to 255	Peripheral number assigned to GPP.
status	ACTIVE, or DEACTIVE	Status of the V5 interface that will be fixed on the LE.
ID	see subfields	V5 interface identifier. Made of subfields SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site identifier.
FRAME	0 to 511	Frame number of the access node (AN) that supplies the V5 interface.
UNIT	0 to 9	AN node number.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

V5402

Log report V5402 generates this information report when a V5 link status mismatch occurs between the computing module (CM) and GPP.

Format

The format for log report V5402 is as follows:

```
V5402 mmmdd hh:mm:ss xxxx <log_type> V5AUDIT GPP <gpp_no>
V5 link status mismatch has been detected.
The link status has been fixed to <status>.
V5LINK No: 1 V5id: V5AN 0 2
PORT: GPP 1 P-Side Link 7
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	This field indicates V5 information that follows in field interface information.
gpp_no	0 to 255	Peripheral number assigned to GPP.
status	InService, or System Busy, or Remote Blocked	Status of the V5 link.
ID	see subfields	V5 interface identifier. Made of subfields SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site identifier.
FRAME	0 to 511	Frame number of the access node (AN) that supplies the V5 interface.
UNIT	0 to 9	AN node number.
P-Side_link_no	0 to 47	GPP P-side PCM30 link number.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

V5403

Log report V5403 generates this information report when a C-channel data mismatch occurs between the computing module (CM) and GPP.

Format

The format for log report V5403 is as follows:

```
V5403 mmmdd hh:mm:ss xxxx <log_type> V5AUDIT GPP <gpp_no>
V5 C-channel data mismatch has been detected.
<reason>
V5LINK No: <link_no> C-chnl <C_no> V5id: <ID>
PORT: GPP <gpp_no> P-Side Link <p-side_link_no>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	This field indicates V5 information that follows in field interface information.
gpp_no	0 to 255	Peripheral number assigned to GPP.
reason	C-channel definition C-channel activity mismatch (ACT/STBY)C-channel status mismatch (INSV/OOS)	The reason for the C-channel data mismatch.
link_no	0 to 15	V5 AN C-side link number.
C_no	15, 16, or 31	C-channel number. Note: C-channel links can only be located on PCM30 link channels 15, 16, and 31.
ID	see subfields	V5 interface identifier. Made of subfields SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site identifier.
FRAME	0 to 511	Frame number of the access node (AN) that supplies the V5 interface.
UNIT	0 to 9	AN node number.
P-side_link_no	0 to 47	GPP P-side PCM30 link number.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

V5404

Log report V5404 generates this information report when a data link status mismatch occurs between the computing module (CM) and GPP.

Format

The format for log report V5404 is as follows:

```
V5404 mmmdd hh:mm:ss xxxx <log_type> V5AUDIT GPP <gpp_no>
V5 Data link status mismatch has been detected.
Protocol: <text>
Protection group: <group_no>
V5id: <ID>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	This field indicates V5 information that follows in field interface information.
gpp_no	0 to 255	Peripheral number assigned to GPP.
text	CONTROL, or PSTN, or ISDN	Name of the V5.2 protocol.
group_no	1 to 2	Number assigned to the protection group.
ID	see subfields	V5 interface identifier. Made of subfields SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site identifier.
FRAME	0 to 511	Frame number of the access node (AN) that supplies the V5 interface.
UNIT	0 to 9	AN node number.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.