Carrier VoIP

Gateway Controller Fault Management

NN10202-911

Document status: Standard
Document version: 08.02
Document date: 20 October 2006

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

Contents

Gateway Controller Fault Management

New in this release

The following sections detail what's new in *Gateway Controller Fault Management* (NN10202-911) for (I)SN09U:

- "Features" (page 5)
- "Other changes" (page 6)

Features

See the following sections for information about feature changes:

- "PKI on GWC (A00012334)" (page 5)
- "SESM Support for SIP Lines Part 2 (A00012217)" (page 5)
- "GWC Autonomous SWACT (A00011827)" (page 6)

PKI on GWC (A00012334)

This feature adds GWC logs and a GWC320 alarm (with various Specific Problems) to handle integration with the Certificate Manager. The following procedures are created or modified in this NTP:

- "IPSec and IKE security logs" (page 144) (new)
- IKE logs (removed)
- "View and troubleshoot GWC service alarms" (page 25)
- "Clear the GWC320 Phase 1 SA failure alarm" (page 46) (new)
- "Clear the GWC320 Phase 2 SA failure alarm" (page 50) (new)

For the description of log GWC320, see *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909).

SESM Support for SIP Lines Part 2 (A00012217)

This feature adds Session Server (SS) Manager database to the line data integrity audit. The following data stored in the SS Manger database is audited: the endpoints, group directory numbers (DN), member LEN information, DN to LEN mapping.

This feature modifies procedure "Perform a GWC line data integrity audit" (page 103).

GWC Autonomous SWACT (A00011827)

This feature allows you to enable or disable the autonomous switch-of-activity (SWACT) functionality on any trunk- or large line-type Gateway Controllers (GWC). This functionality allows the GWC to automatically invoke a warm SWACT after losing communication with all associated media gateways.

This feature introduces or modifies the following procedures in this NTP:

- "Clear the GWC318 critical alarm manually" (page 44) (new)
- "View and troubleshoot GWC service alarms" (page 25)

The following log report descriptions are added or modified in *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909):

- GWC318 (new)
- GWC319 (new)
- PM181

Other changes

See the following sections for information about changes that are not feature-related:

- "References to the Core" (page 6)
- "GWC log descriptions" (page 6)

References to the Core

Throughout this NTP, all generic references to the Core apply to both implementations of Core functionality:

- XA-Core, in a CS 2000 configuration environment
- Compact Call Agent (CCA), in a CS 2000 - Compact configuration environment

GWC log descriptions

All GWC log report descriptions, except Kerberos and IPSec/IKE logs, are removed from this NTP. For the GWC log descriptions, see *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909)

For this release, the following log descriptions are added to *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909):

- GWC321
- GWC322
- GWC601

- GWC603
- GWC604
- GWC605
- GWC606
- GWC702

The following log descriptions are updated in *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909):

- GWC501
- GWC502
- GWC503
- GWC600

Fault management strategy

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

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

GWC alarms

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

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

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

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

Alarm severity codes

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

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

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

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 (I)SN07, you can no longer acknowledge GWC alarms or view acknowledged GWC alarms using the CS 2000 GWC Manager. Procedures to perform this activities are removed from this NTP.

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

GWC logs

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

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

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

Alarm information is sent to:

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

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

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

Event log information is sent to:

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

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

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

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

For more information about how to access the GWC syslog logs, see procedure "View GWC logs in syslog files" (page 68) in this NTP.

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

Logs and alarms associated with IPSec

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

- logs GWC309, GWC320, GWC400

  For more information, see *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909).
- "Kerberos logs" (page 139)
- "IPSec and IKE security logs" (page 144)
- alarm SA_PERCENTAGE_USAGE (minor)
- GWC320 alarms (various specific problems)

For alarms information, see procedure "View and troubleshoot GWC service alarms" (page 25).

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 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 about how to access the CS 2000 GWC Manager and the CS 2000 SAM21 Manager, see CS 2000 Management Tools sections in *Nortel ATM/IP Solution-level Administration and Security* (NN10402-600).

Comparing the CS 2000 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 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

You can perform many FCAPS activities using the Integrated Element Management System (IEMS). In addition, you can use IEMS to access the CS 2000 GWC Manager and the CS 2000 SAM21 Manager. For more information, see *IEMS Overview* (NN10329-111).

To launch the CS 2000 GWC Manager or the CS 2000 SAM21 Manager, see the following procedures in *IEMS Overview* (NN10329-111):

- "Launching GWC Manager"
- "Launching SAM21 Manager"

If you wish to acknowledge alarms, see *IEMS Fault Management* (NN10334-911).

Use of ping and traceroute

A remote ping and traceroute functionality is provided through the IEMS GUI client. This allows users to launch ping and traceroute operations remotely on the GWC and SPFS platforms. Provision of this facility through IEMS avoids any potential problems caused by allowing non-root users access to these powerful commands.

Remote command launch allows users to troubleshoot network connectivity problems from a single location using the same user interface. It initiates an operation on a remote platform or device as if the user had logged on to the device and issued the command directly. Ping and traceroute are accessed from the drop-down menu available when a GWC (or SPFS) managed object is right-clicked in the IEMS GUI. The drop-down menu now includes two new items: Launch Remote Ping and Launch Remote TraceRoute.

For more information about how to launch ping and traceroute, see *IEMS Overview* (NN10329-111).

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.

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.

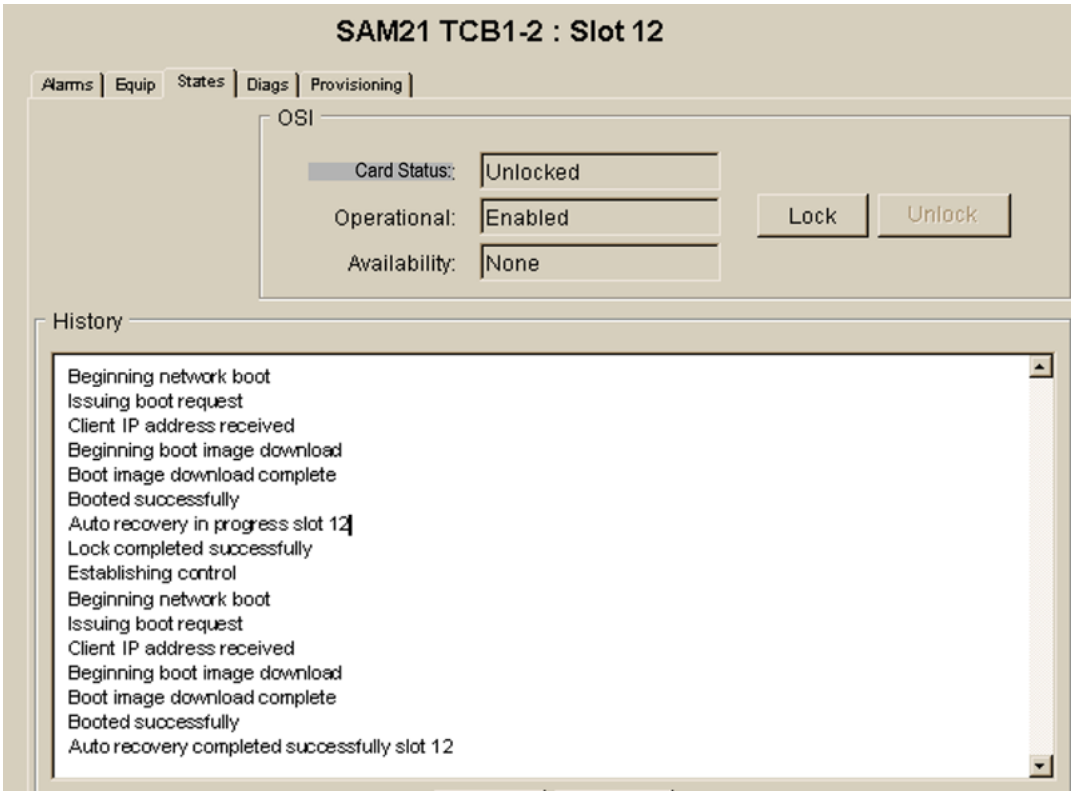
When an application failure occurs, the card is "unlocked-enabled" in the CS 2000 SAM21 Manager, but disabled at the card application level in the CS 2000 GWC Manager.

There are two stages of the recovery 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 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, see*SAM21 Shelf Controller Fault Management* (NN10089-911).

The following figure shows a sample of the auto-recovery progress text displayed in the "History" window.



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.

The GWC boot audit recovery sequence is also captured in the NSS_boot_audit logs on the shelf controller, for example:

```
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
```

GWC overload

GWC overload causes the system to generate log PM181. The system continues to output the log every 10 seconds while the GWC unit remains in overload.

When a GWC goes into overload, some trunks on that node must be busied to off load traffic. In (I)SN09, the post command at MAPCI TTP level is enhanced to provide the facility for manually busying a specific trunk group on an individual GWC.

The post command has a new post type I with meaning 'Post in existing set'. When a post command with type I is entered, it posts the trunks in the existing post set (see Example 1). If no post set exists when the post command with type I is used, the command returns an error message (see Example 2).

After the I option, the only valid options are G and D.

The D option used after the I option supports only the digital equipment GWC and SPM.

On the GWC, this feature supports trunk types ISUP, PRI, and PTS.

The following figures show examples of the post command using post type I.

Example 1: Post the members of group TRUNK_EXAMPLE on GWC32

```
                IOD          PM    CCS    Lns    Trks   Ext    APPL
                OCC  B       PMLOAD 3   RS  SYSB    42C..  2Crit   .
                *C*            *C*    *C*    *C*    *C*    *C*
TTP
 0 QUIT         POST       DELQ          BSYQ        DIG
 2 Post_        TTP 27-0102
 3 SEIZE        CKT TYPE    PM NO.        COM LANG    STA S R  DOT TE  RESULT
 4
 5 BSY
 6 RTS
 7 TST
 8
 9 CktInfo
10 CktLoc
11 Hold          NO CKT, SET IS EMPTY
12 NEXT          TTP:
13 RLS
14 Ckt_
15 TrnslVf_
16 StkSdr_
17 Pads
18 Level_
 TESTER
Time  15:32  >POST D GWC 32; POST I G TRUNK_EXAMPLE
```

Create a post set containing all the trunks on GWC32

Post only those trunks in the post set whose CLLI is TRUNK_EXAMPLE

Example 2: No existing post set for post command with type I

```
            IOD        PM   CCS   Lns   Trks  Ext   APPL
            OCC B      PMLOAD 3  RS SYSB   42C.. 2Crit  .
            *C*          *C*   *C*   *C*   *C*   *C*
TTP
 0 QUIT      POST     DELQ       BSYQ      DIG
 2 Post_     TTP 27-0102
 3 SEIZE     CKT TYPE   PM NO.      COM LANG   STA S R  DOT TE  RESULT
 4
 5 BSY
 6 RTS
 7 TST
 8
 9 CktInfo
10 CktLoc
11 Hold        POST I G TRUNK_EXAMPLE
12 NEXT        FAIL: EMPTY POST SET
13 RLS
14 Ckt_
15 TrnslVf_
16 StkSdr_
17 Pads
18 Level_
 TESTER
Time  15:32 >
```

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. See the following two figures for details.

  The following LEDs appear on the front of the GWC cards.
  - — SPD/LNK (green/yellow; MCPN905 only) - Ethernet link speed and status; lights green to show 1000 Mbit link, lights yellow to show 10/100 Mbit link, off if no valid link
  - — ACT (green; MCPN905 only) - Ethernet link activity; lights when the Ethernet link is active

— CPU (green) - CPU activity; lights when the card's processor is active

— BFL (yellow) - Board failure; lights when a system failure occurs on the card

— Hot swap status (blue; in handles of MCPN905 card) - 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 cards. 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.

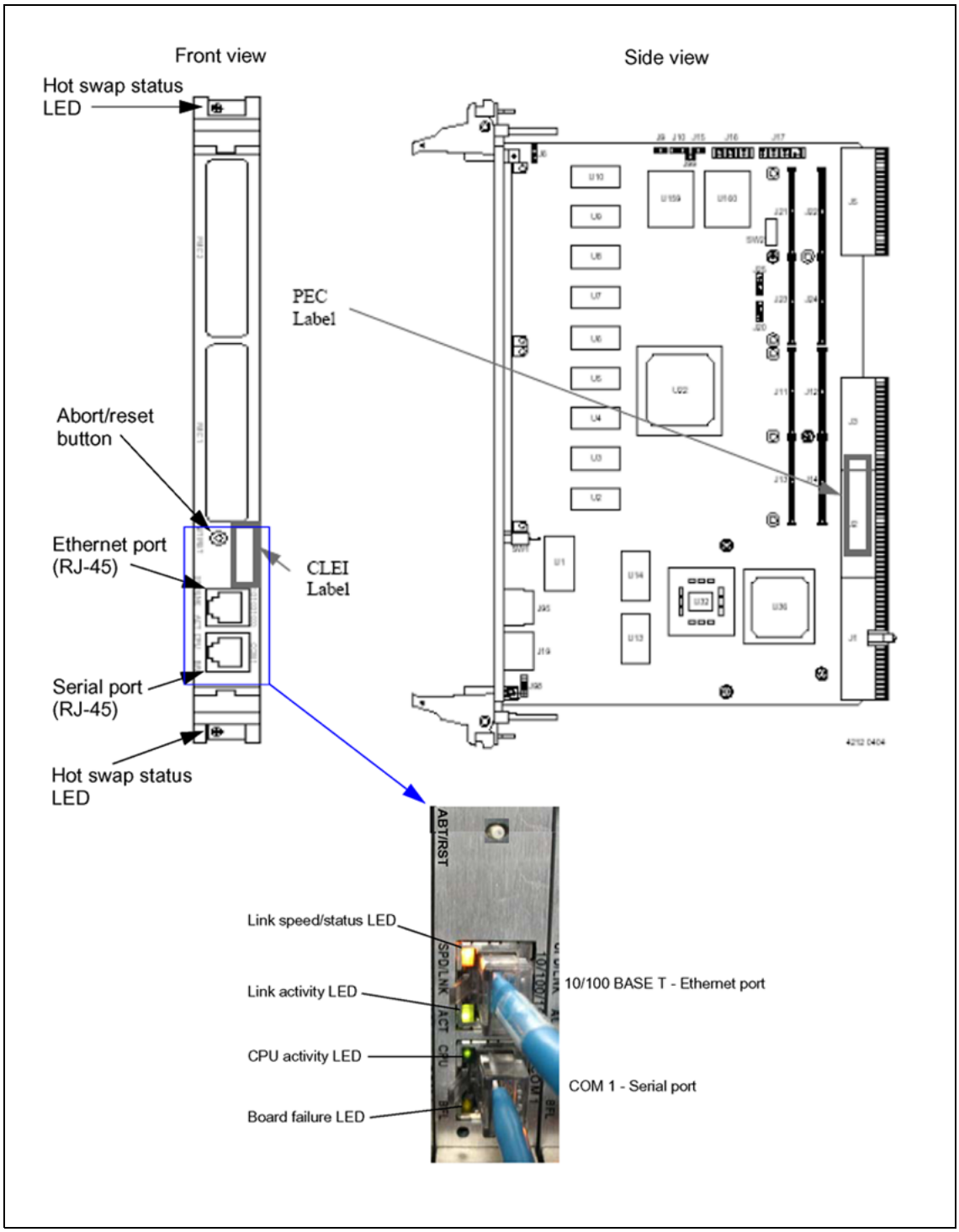
  — Ensure that the data and power cables are routed separately.

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

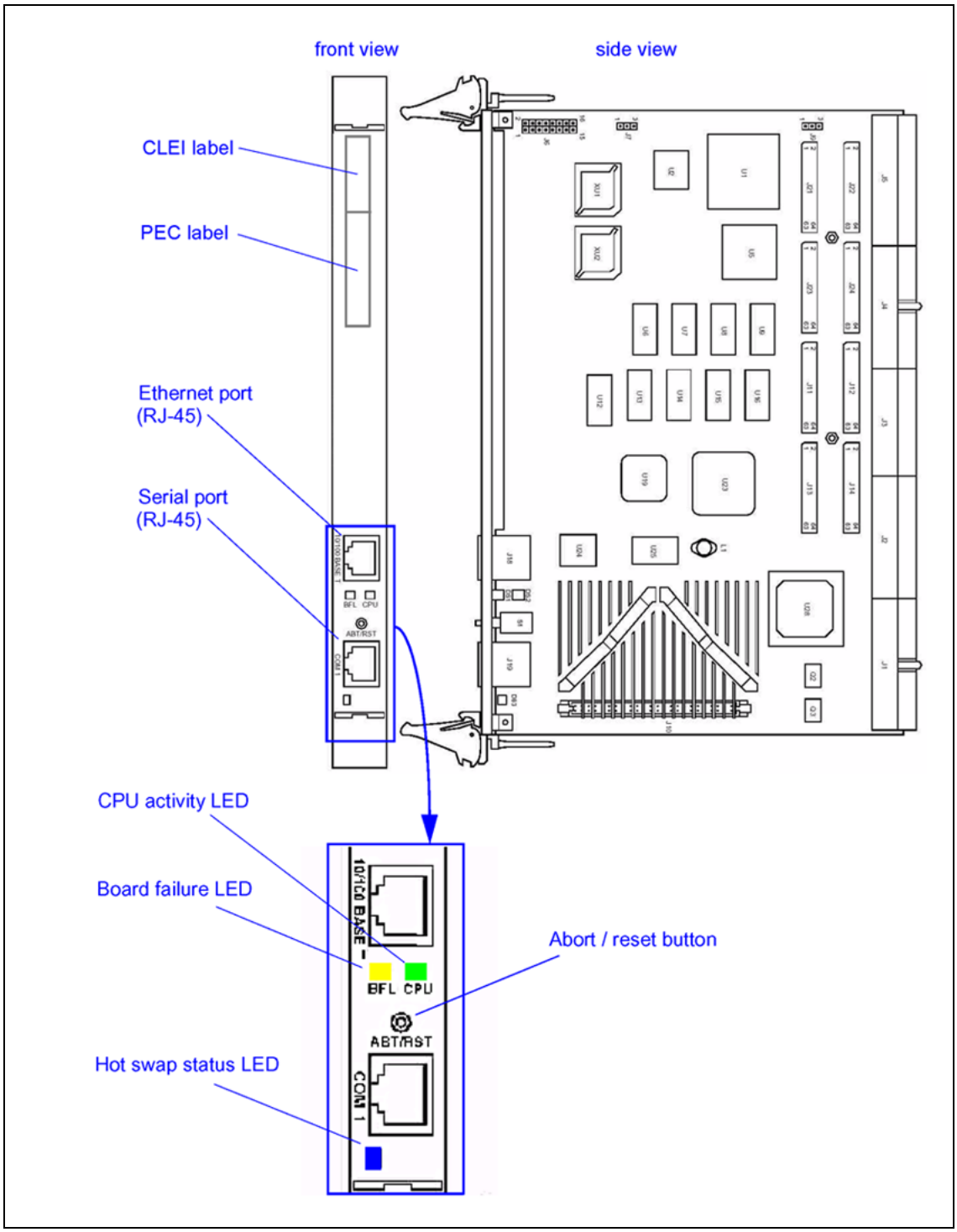
  The following two figures show the connectors and slots on the front of the GWC cards. The Ethernet port is the card's main network connection. The peripheral component interconnect (PCI) mezzanine card expansion slots are currently not used on a GWC card.

Consult your Nortel installation personnel for proper maintenance practices.

Details: Motorola N905 NSS board



Details: Motorola N750 NSS board



View GWC service alarm history

Purpose of this procedure

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

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

Access to platform-related alarms is provided in procedure "View GWC platform hardware alarms" (page 42).

When to use this procedure

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

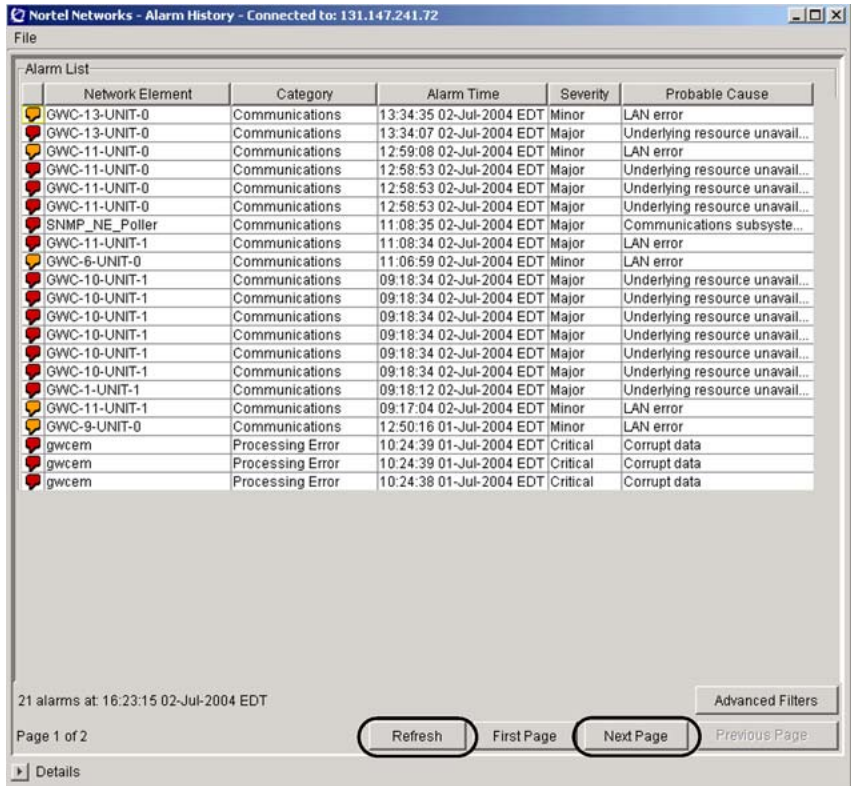
Prerequisites

This procedure has no prerequisites.

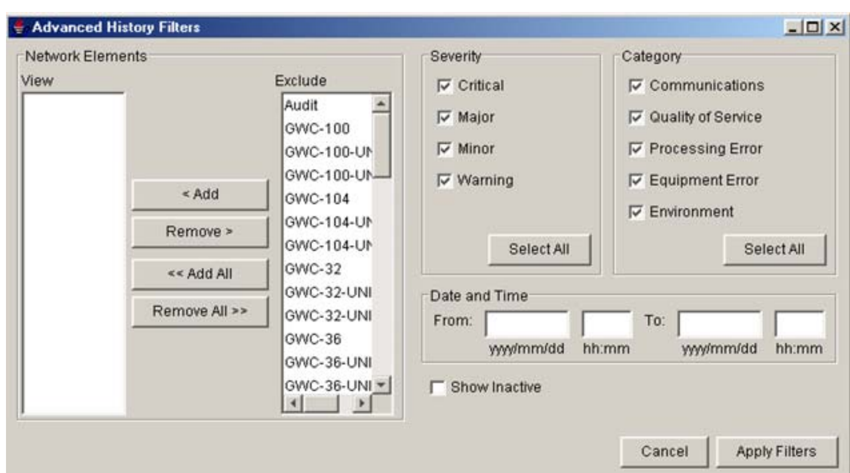
Action

Step	Action
	At the CS 2000 GWC Manager client
1	From the CS2000 Management Tools window menu, select the **Fault** menu and then **Alarm History**.
2	Review the alarms displayed. The colors to the left of the alarm display provide a visual indication of alarm severity: • yellow - warning • orange - minor • red - major and critical
3	Click **Refresh** to update the alarm list.

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



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



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

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

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

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

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

e. If you wish to filter according a specific range of dates, type the date range in the format, yyyy/mm/dd.

f. If you wish to filter according a specific time frame, type the time frame in the format, hh:mm.

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

6 If necessary, click the **Advanced Filters** button again to further modify the filter criteria, then click the **Apply Filters** button.

7 When you are finished with the Alarm History, click the **File** menu at the top of the screen and select **Close**.

8 This procedure is complete.

—End—

View and troubleshoot GWC service alarms

Purpose of this procedure

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

Access to platform-related alarms is provided in procedure "View GWC platform hardware alarms" (page 42).

When to use this procedure

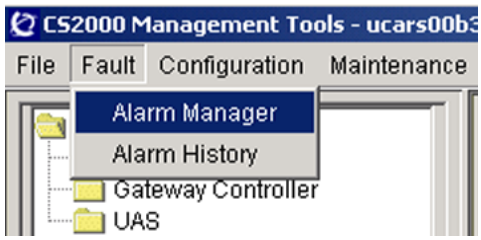
Use this procedure as a primary source for fault diagnostic information related to GWC services.

Prerequisites

This procedure has no prerequisites.

Action

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



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

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

- yellow - warning

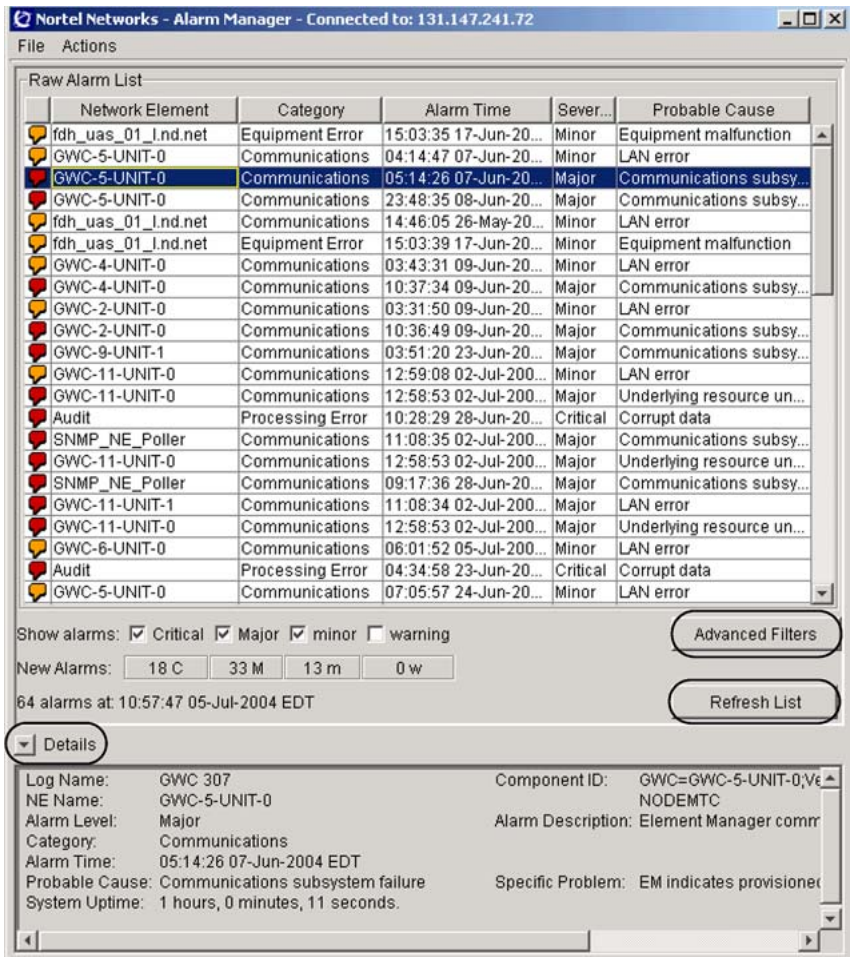
- orange - minor

- red - major and critical

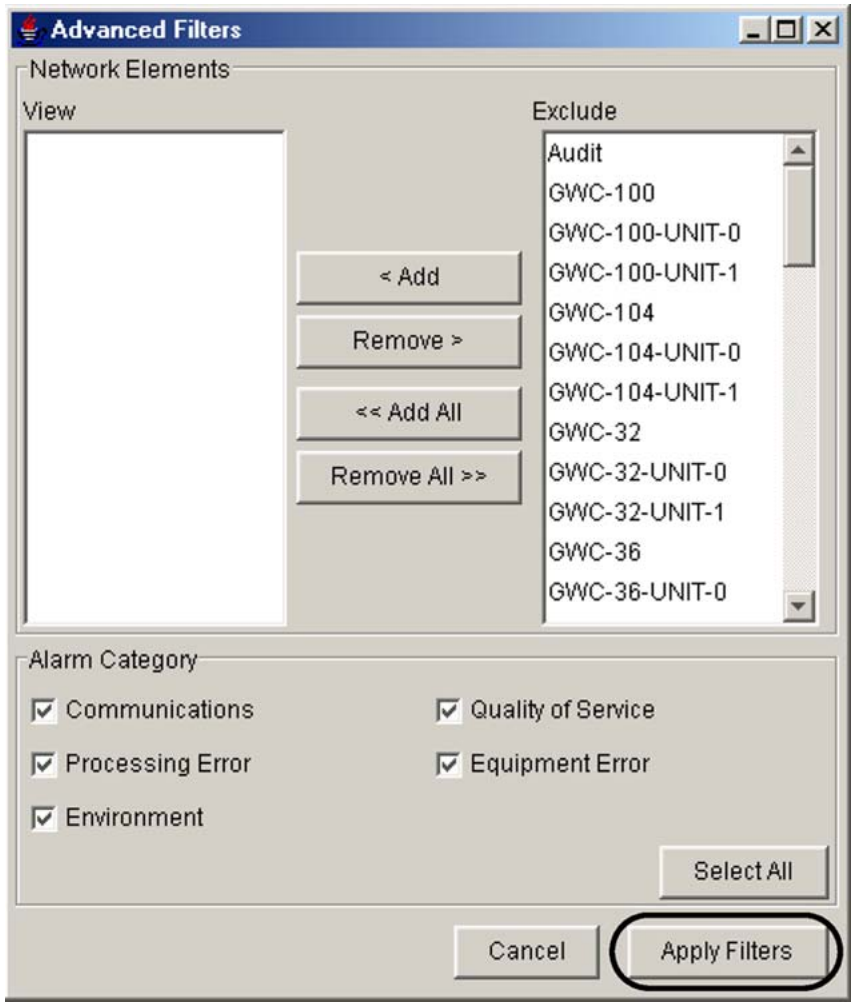
See section "Troubleshooting GWC service alarms" (page 28) at the end of this procedure for details about the alarm types displayed, including appropriate actions to diagnose and resolve the alarm condition. Table "Troubleshooting GWC service alarms" (page 29) specifically contains the alarm information.

3 Click **Refresh List** to update the alarm list.

4 Click the **Details** button to review specific details about an alarm.



5 To filter the alarm display for specific GWC units by excluding the display of certain alarm types, click the **Advanced Filters** button to filter alarms based on selected alarm categories.



Perform the following steps at the Advanced filters dialog box:

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

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

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

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

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

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

7 This procedure is complete.

—End—

Troubleshooting GWC service alarms

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

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

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

  For information about how to open these Syslog log files and search for alarm codes, see procedure "View GWC logs in syslog files" (page 68) in this NTP.

- These logs may also be available in syslog format in custlog files in the /var/adm directory on the CS 2000 Core Manager or Core and Billing Manager (CBM). The CS 2000 Management Tools server must be configured to send the syslog logs to the CS 2000 Core Manager or CBM.

- Switch Control Center (SCC2) or Nortel STD log formats available on the customer's Operations Support System (OSS) interface.

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

The following table lists GWC service alarms.

Troubleshooting GWC service alarms

Alarm description Alarm ID code Severity	Specific problem Probable cause	Action
Recovery alarm **GWCEM301** *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. When both units are out of service, the active unit must recover before the standby unit will. Check the following: • Whether the unit is manually locked out of service (Administrative state of "locked"). • Alarms that may indicate a problem on the unit preventing it from returning to service. • Other state indicators which may indicate problems, such as: — Isolation state of "isolated" — Availability state of "offLine" • 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.

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. When both units are out of service, the active unit must recover before the standby unit will. Check the following: • alarms that may indicate a problem on the unit preventing it from returning to service • other state indicators which may indicate problems, such as: — isolation state of "isolated" — for the standby unit, availability state of "degraded" — availability state of "offLine" • logs which may also indicate a failure of a step in the process of recovering the unit
Standby unit disable **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. When both units are out of service, the active unit must recover before the standby unit will. Check the following: • alarms that may indicate a problem on the unit preventing it from returning to service

Alarm description Alarm ID code Severity	Specific problem Probable cause	Action
		• other state indicators which may indicate problems, such as: — isolation state of "isolated" — for the standby unit, availability state of "degraded" — availability state of "offLine" • logs which may also indicate a failure of a step in the process of recovering the unit
	Specific problem: Unit out of service - invalid GWC Profile Data. Probable cause: Configuration or customization error.	Check the profile data for the unit and do one of the following: - Change to another profile. - Reconfigure the GWC unit software or CS 2000 GWC Manager software to remove the incompatibility. Then, RTS the unit.
Core communication lost **GWC302** *Major*	Specific problem: No response received to Core heartbeat messages from active GWC unit. Probable cause: LAN error.	Clears automatically after a Core or network outage clears. Otherwise, verify that the node number and Core Side IP address is correct for the GWC to communicate with the Core.
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.

Alarm description Alarm ID code Severity	Specific problem Probable cause	Action
Communication with a gateway is down **GWC304** *Major*	Specific problem: Communication with gateway <Gatewayname> is down. Probable cause: The underlying resource is not available. 'Gateway' is defined as large gateway or audio gateway (e.g. PVG, H.323 gateway with 64 or more endpoints, MG 9000, UAS).	Cleared by restoring communication to the managed gateway. Do this by verifying the availability of the gateway, and comparing the configuration data at the gateway and the CS 2000 GWC Manager (IP address, protocol/version, etc.).
This is a test alarm generated from pmdebug interface **GWC305** *Minor* This is a test alarm generated from pmdebug interface **GWC305** *Critical, Major, or Minor*	Specific problem: A test alarm generated to log in to notilog table - not sent to manager. Probable cause: Unspecified reason. 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 "GWC fault management in a DQoS network" (page 12) 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.

Alarm description Alarm ID code Severity	Specific problem Probable cause	Action
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 or disconnected, or both. Determine if the GWC has been setup to use the wrong IP address for the CS 2000 GWC Manager at the CS 2000 SAM21 Manager.
Flash memory error **GWC308** *Minor*	Specific problem: Erase of flash sector failed. Probable cause: Equipment malfunction. Flash life span exceeded; the number of writes to flash has exceeded the recommended or intended limit.	Cleared with hardware replacement.
SA_PERCENTAGE_USAGE **GWC309** *Minor* This alarm does not apply to the Wireline Universal Packet Access (UA-AAL1) solution.	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.

Alarm description Alarm ID code Severity	Specific problem Probable cause	Action
Provisioned GWC Profile not yet activated **GWC311** *Warning*	Specific problem: GWC profile loaded into Flash will activate on the next reload. A New GWC Profile has been loaded to GWC FLASH by the CS 2000 GWC Manager, but the GWC is still using the old Profile. Probable cause: Configuration or customization error.	Cleared with a GWC reload.
QoS collection application (QCA) connection failure **GWC312** *Major (partial outage)*	Specific problem: QCA connection <ConnName> has failed - attempting recovery. Probable cause: Communications subsystem failure.	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.
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.

Alarm description Alarm ID code Severity	Specific problem Probable cause	Action
		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.
External host interface signal loss **GWC315** *Critical* (>50% loss) *Major* (>20% loss) *Minor* (any signal loss)	Specific problem: Small GWs in disabled state Probable cause: Signal loss - alarm based on number of GWs out of service compared with number of GWs provisioned	Logs (GWC502) indicate a small line GW going out of service and coming back into service. GWs are considered to be out of service when heartbeat messages between the GW and GWC are lost. Use the new small gateway OMs to check how many small line GWs are out of service. Use the logs to identify which GWs need attention.

Alarm description Alarm ID code Severity	Specific problem Probable cause	Action
External host interface signal loss **GWC315** *Major* (both links down) *Minor* (one link down)	Specific problem: USP SS7 paths disabled Probable cause: Signal loss	This alarm is based on the number of USP connections that are out of service, compared with the number of paths (maximum two) checked in a 5-minute polling period. The link paths are considered to be out of service when heartbeat messages between the GWC and USP are lost. Check the USP connections.
External host interface signal loss **GWC315** *Critical* (>50% loss) *Major* (>20% loss) *Minor* (any signal loss)	Specific problem: Peer connections failed during interval Probable cause: Signal loss	This alarm is based on the number of call setups failed, compared with the number of calls attempted in a 5-minute polling period. Use the new peer messaging OMs to check the number of calls failed over a longer period. Check the Ethernet link between the GWC and the remote host or peer GWCs.
External host inter face configuration error **GWC315** *Warning*(non-service affecting)	Specific problem: DNS failed GW discovery Probable cause: Configuration or customization error	This alarm is based on the number of gateways that failed DNS lookup in a 5-minute polling period. Use the new DNS OMs to check the number of gateways not discovered, and the number of gateways discovered using RSIP. RSIP discovery does not survive a cold SwAct on the GWC, which may cause long outages. Check the DNS server entries for every gateway.
External host interface protocol error **GWC315** *Major* (both links not active) *Minor* (one link not active)	Specific problem: USP SS7 path not active Probable cause: Communications protocol error	This alarm is based on the number of USP connections that have heartbeat messages but are not active in a 5-minute polling period. A major alarm affects some call processing; a minor alarm causes a redundancy error. Check the USP configuration to the GWC.

Alarm description Alarm ID code Severity	Specific problem Probable cause	Action
External communic ation interface **GWC315** *Critical* (>50% proxies disabled) *Major* (>20% proxies disabled) *Minor* (any media proxies disabled)	Specific problem: Media proxies in disabled state Probable cause: Signal loss - alarm based on number of media proxies out of service compared with number of media proxies provisioned	Media proxies are considered to be out of service when they fail to respond to messages sent from the GWC, and returned to service when the GWC receives the regular RSIP message. The alarm is raised as a media proxy goes out of service, and cleared when it comes back into service. Use the media proxy OMs to check how many media proxies are out of service in any 5-minute polling period. Use the RTP Portal EM to identify which media proxies need attention. This alarm and the associated OMs give the GWC view of calls, as opposed to the media proxy view.
PreSwact audit failure **GWC317** *Major*	Specific problem: PreSwact audit failed for two consecutive cycles Probable cause: • monitored base resource reaches the threshold level • monitored application resource reaches the threshold level • data synchronization mismatch (SESM, GWC flash, GWC RAM) • standby unit is jammed and prevented from taking up the activity	Check the alarm text to see which component has failed. The alarm clears when you clear the error condition. If required, you can use Swact force to force a manual warm Swact.
The preSwact audit runs at a frequency of 40 seconds and with priority 6. A second occurrence of the same error condition does not raise an alarm. No alarm is raised if the preSwact audit fails while patching is in progress in the inactive unit.		

Alarm description Alarm ID code Severity	Specific problem Probable cause	Action
Autonomous SWACT initiated **GWC318** *Critical*	Specific problem: (Element Name>: No communication with associated media gateway(s) Probable cause: Underlying resource unavailable. This alarm indicates that the system attempts to restore communication with the associated media gateways.	Check the related network component managers to identify failures within the network. The alarm clears automatically when a manual SWACT back to the original active unit is performed. You can also manually clear this alarm once the problem on the original active unit is solved. Follow procedure "Clear the GWC318 critical alarm manually" (page 44).
GWC communi cation loss with associated media gateway(s) **GWC319** *Critical*	Specific problem: (Element Name>: No communication with associated media gateway(s) Probable cause: Underlying resource unavailable.	Check the related network component managers to identify failures within the network. This alarm clears when the GWC detects communication with at least one associated gateway. It also clears when the GWC automatically or manually switches activity, but it is raised again on the newly active unit if communication is still lost with all associated gateways.
IKE/IPSec **GWC320**	GWC320 alarms indicate an IKE/IPSec-related problems. See the Specific Problem: field to check the reason for generating this alarm. Each specific alarm may have an associated security log, which provides additional details about the problem. For the description of all IKE and IPSec security logs, see procedure "IPSec and IKE security logs" (page 144).	
GWC320 *Critical* - certificate expires within 5 days *Major* - certificate expires within 15 days *Minor* - certificate expires within 30 days	Specific problem: One or more certificates in set number <x> are expiring. An outage may occur if an IKE connection policy is using these certificates. At the GWCEM, please verify the expiry dates for certificates in set number <x> -- <GWC_IP_address> where **<x>** is the set number of the [IKE certificates] panel Probable cause: Key expired	This alarm indicates that an IKE certificate is expiring soon and the GWC Manager has not obtained a new certificate from the Certificate Manager. Service disruption may occur when the certificate expires. For information about how to clear this alarm, see procedure “Recovery of the GWC320 certificate expiry alarm” in *Nortel CVoIP IPSec Security Service Implementation Overview* (NN10453-100).

Alarm description Alarm ID code Severity	Specific problem Probable cause	Action
GWC320 *Critical*	Specific problem: One or more certificates in set number <x> are expired. An outage will occur if an IKE connection policy is using these certificates. At the GWCEM, please verify the expiry dates for certificates in set number <x> -- <GWC_IP_address> where **<x>** is the set number of the [IKE certificates] panel Probable cause: Key expired	This alarm indicates that an IKE certificate is expired and the GWC Manager has not obtained a new certificate from the Certificate Manager. Service disruption will occur when the certificate expires. For information about how to clear this alarm, see procedure “Recovery of the GWC320 certificate expiry alarm” in *Nortel CVoIP IPSec Security Service Implementation Overview* (NN10453-100).
GWC320 *Major*	Specific problem: Phase 1 SA failure -- <remote_gateway_IP _address> Probable cause: Underlying resource unavailable	This alarm indicates that a Phase 1 negotiation failed. This alarm is the result of an outage. To clear this alarm, complete procedure "Clear the GWC320 Phase 1 SA failure alarm" (page 46).
GWC320 *Major*	Specific problem: Phase 2 SA failure -- <remote_gateway_IP _address> Probable cause: Underlying resource unavailable	This alarm indicates that a Phase 2 negotiation failed. This alarm is the result of an outage. To clear this alarm, complete procedure "Clear the GWC320 Phase 2 SA failure alarm" (page 50).
GWC320 *Critical*	Specific problem: GWC certificate in set number <x> doesn’t match private key -- <GWC_IP_address> Probable cause: Unexpected Information	This alarm may indicate an outage. Contact your next level of support. There are no security logs associated with this specific problem.

Alarm description Alarm ID code Severity	Specific problem Probable cause	Action
GWC320 *Critical*	Specific problem: Invalid Subject Alternative Name in GWC certificate set number <x> -- <GWC_IP_address> where **<x>** - is the set number of the [IKE certificates] panel Probable cause: unexpectedInformation	This alarm indicates that the Subject Alternative Name in the GWC certificate does not match the provisioned IP address for the GWC certificate. This may indicate a data or communication problem between the GWC and the GWC Manager. Contact your next level of support.
Ethernet/IP Errors **GWC321** *Major*	Specific problem: Auto-negotiation disabled on ethernet link. Probable cause: Configuration or customization error	Enable the auto-negotiation capability on the Ethernet Routing Switch 8600. If required, see the Ethernet Routing Switch 8600 configuration documentation.
A subsystem overloaded **GWC322** *Minor* - SNMP message rate crossed the Panic Level *Warning* - SNMP message rate crossed the Warning Level	Specific problem: • for major alarms: SNMP message rate exceeded recommended maximum • for warning alarms: SNMP message rate is close to recommended maximums Probable cause: Threshold crossed	Reduce the SNMP traffic level.
Communication with a gateway is down	Specific problem: Gateway failed to respond to heartbeat/audit	Cleared by restoring communication to the managed gateway. Do this by verifying the availability of the gateway, and comparing

Alarm description Alarm ID code Severity	Specific problem Probable cause	Action
GWC501 *Major*	Probable cause: The underlying resource is not available. 'Gateway' is defined as small gateway (e.g. Askey/Mediatrix line gateway, Arris/Motorola gateway, H.323 gateway with less than 64 endpoints).	the configuration data at the gateway and the CS 2000 GWC Manager (IP address, protocol/version, etc.).
Data inconsistency between GWCEM and Session Server *Minor*	Specific problem: Data inconsistency between GWCEM and Session Server Probable cause: Depends on the condition that caused the alarm. Examples: "Data Audit run but data not fully synchronized", "Setting the Call Agent ID has resulted in data changes, which need to be propagated to the Session Server. Run the CS2KSS EM Data Integrity Audit", "Failed to rollback 'add zone' command from Database", "Failed to rollback 'delete zone' command.	For all cases other than when the Data Audit fails, run the CS2KSS Data Integrity Audit. If the data audit fails, investigate the reason (for example, connection failure, problem with the data on the CS2KSS EM, and so on) and manually correct the problem.

View GWC platform hardware alarms

Purpose of this procedure

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

When to use this procedure

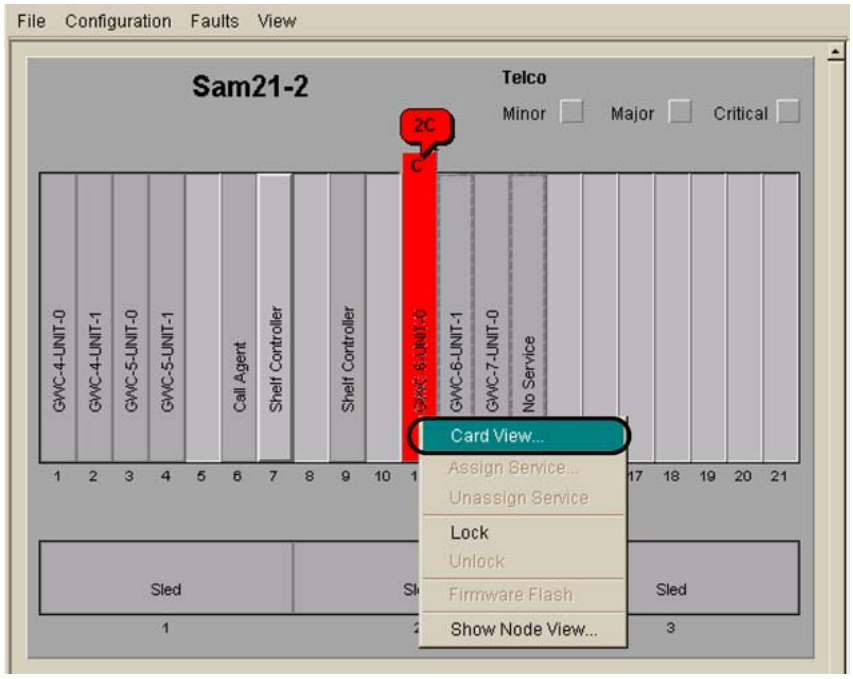
Use this procedure as a part of alarm clearing at the CS 2000 SAM21 Manager or as a secondary source of diagnostic information for GWC application (service) alarms.

Prerequisites

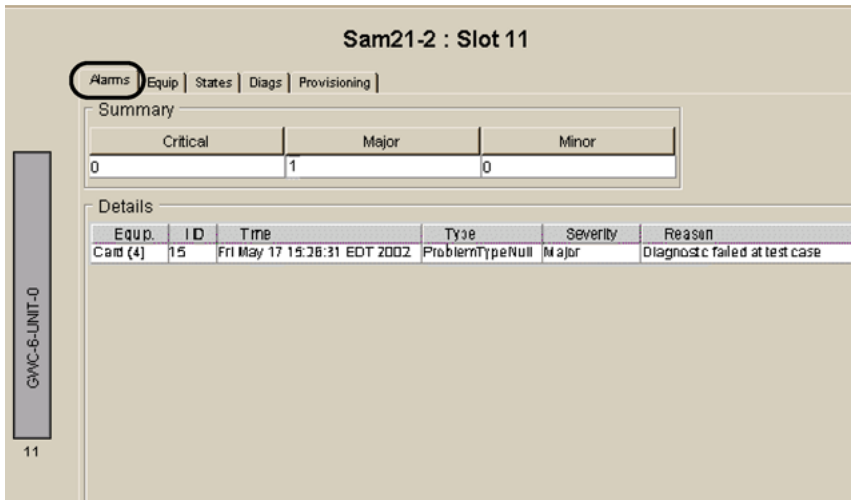
This procedure has no prerequisites.

Action

Step	Action
	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.



- For information about various alarms generated by the SAM21 platform, see *SAM21 Shelf Controller Fault Management* (NN10089-911).
- For information about individual alarms related to the NSS cards (including the GWC card) in the SAM21 Shelf, see the CS 2000 Management Tools sections in *Nortel ATM/IP Solution-level Fault Management* (NN10408-900).

  In wireless markets, see *Packet MSC Fault Management* (NN-20000-212).

3 This procedure is complete.

—End—

Clear the GWC318 critical alarm manually

Purpose of this procedure

This procedure describes how to manually clear the GWC318 critical alarm.

GWC318 critical alarm is raised when a GWC initiates an autonomous switch of activity (SWACT) in an attempt to restore communication with its associated media gateways.

For information about the GWC autonomous SWACT option, see procedure "Enable or disable GWC autonomous SWACT" in *Gateway Controller Configuration Management* (NN10205-511).

When to use this procedure

Use this procedure after the autonomous SWACT occurred and the problem on the original active unit is solved to manually clear the GWC318 critical alarm.

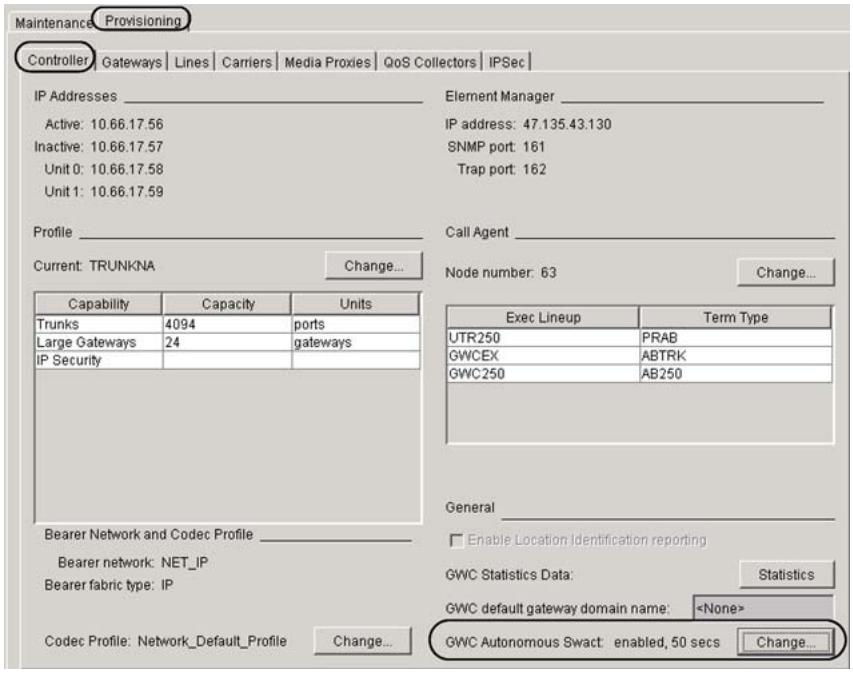
Prerequisites and guidelines

The following prerequisites apply to this procedure:

- The autonomous SWACT occurred and the GWC318 critical alarm is raised.
- The problem on the original active unit is solved.

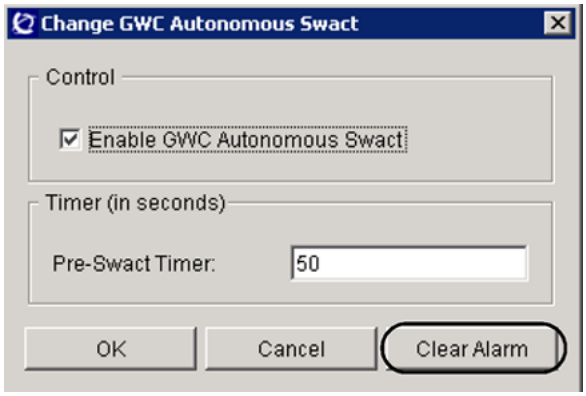
Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: Gateway Controller frame, select the GWC node on which the alarm is raised.
3	Click the **Provisioning** tab and the **Controller** tab.



4 Click the GWC Autonomous Swact: **Change** button. The Change GWC Autonomous Swact dialog box opens.

5 Click the **Clear Alarm** button.



6 At the confirmation window, click **OK** to confirm your request.

Click **No** and then **Cancel** if you wish to cancel the operation.

7 The procedure is complete.

—End—

Clear the GWC320 Phase 1 SA failure alarm

Purpose of this procedure

This procedure describes how to clear a GWC320 major alarm raised for the following specific problem: Phase 1 SA failure - <remote_gateway_IP_address>.

This alarm may have associated security logs, which provide additional details about the problem. For the description of all IKE/IPSec security logs, see procedure "IPSec and IKE security logs" (page 144).

When to use this procedure

Use this procedure to clear a GWC320 Phase 1 SA failure alarm.

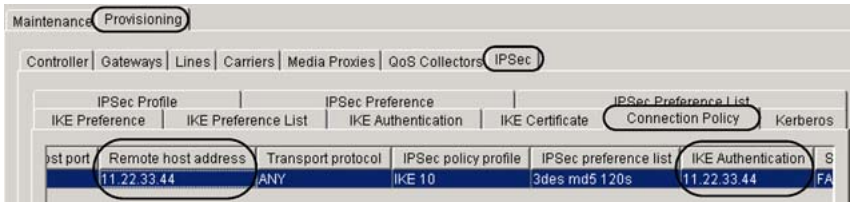
Prerequisites and guidelines

Complete the following tasks before starting this procedure:

- Verify whether any security logs associated with the alarm exist in the syslog file. Follow procedure "View GWC logs in syslog files" (page 68), searching for the text string ISAKMP_FAIL. An ISAKMP_FAIL log with the same date and time as the alarm may indicate the precise reason for the failure.
- Make sure that the remote media gateway is enabled and that the IPSec on the remote gateway is enabled.

Action

Step	Action
	At your workstation
1	Launch the CS 2000 Management Tools client application. If required, see procedure "Launching CS 2000 Management Tools and NPM client applications".
	At the CS 2000 GWC Manager client
2	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
3	From the Contents of: Gateway Controller frame, select the GWC node on which the alarm is raised.
4	Click the **Provisioning** tab, the **IPSec** tab, then the **Connection Policy** tab to display connection policies currently configured for the selected GWC node.



5 In the Remote host address column, find the IP address that matches the <remote_gateway_IP_address> in the alarm.

If there is more than one policy with the same Remote host address, select the one with the lowest policy ID. Click that row to highlight the policy.

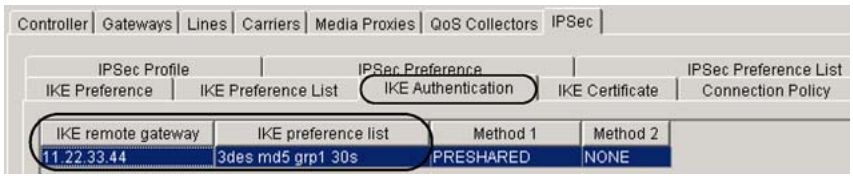
The policy with the lowest ID number has the highest priority and will be selected by the GWC.

If the highlighted policy is	Do
FLEX or SECURE	Continue the procedure.
BYPASS or DISCARD	Stop the procedure and contact your next level of support.

6 For the highlighted policy, verify that the IKE Authentication IP address matches the Remote host address.

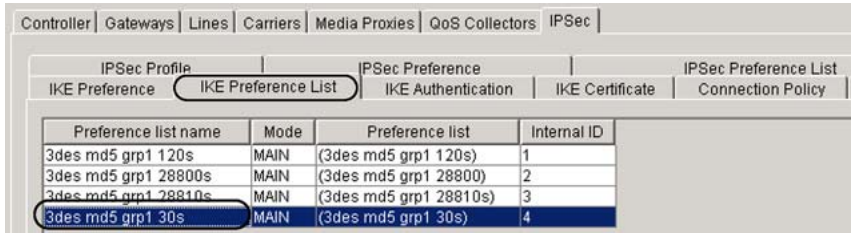
If these two addresses do not match, stop the procedure and re-configure the connection policy correctly. For full instructions, see *Nortel CVoIP IPSec Security Service Implementation Overview* (NN10453-100). Otherwise, continue the procedure.

7 Click the **IKE Authentication** tab.



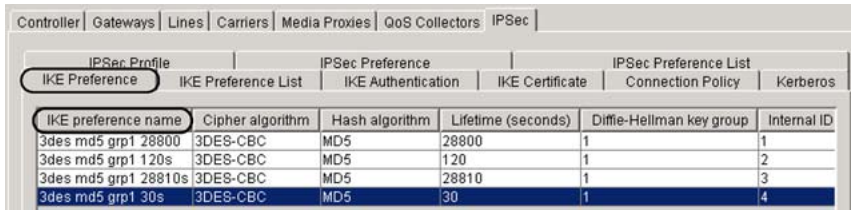
In the IKE remote gateway column, find the IP address that matches the <remote_gateway_IP_address> in the alarm. From the selected IKE authentication row, note the name of the IKE preference list.

8 Click the **IKE Preference List** tab. Find the preference list name that matches the name noted in step 6.



9 Note the names of all preferences included in the list (displayed in the Preference list column). Each preference list can include up to three preferences.

10 Click the **IKE Preference** tab.



Under IKE preference name heading, find the preferences noted in the previous step and verify that the configuration values for at least one preference match the values configured on the remote gateway.

If the remote gateway is a Media Gateway 9000, verify that one of the preferences has the following values:

- Cipher algorithm = 3DES-CBC
- Hash algorithm = SHA
- Lifetime = 86400
- Diffie-Hellman key group = 1

11 Use the following table to determine your next step.

If IKE preference values	Do
do not match	Go to the next step.
match	Stop the procedure and contact your next level of support.

12 Add a new IKE preference and IKE preference list with the configuration values that match the values configured on the remote gateway.

If required, see procedure "Configure IKE Preference and Preference List" in *Gateway Controller Security and Administration* (NN10213-611).

13 Modify the IKE authentication selected in step 6 by selecting the new IKE preference list.

If required, see procedure "Modify IKE authentication_change IKE preference list" in *Gateway Controller Security and Administration* (NN10213-611).

If the alarm clears within 5 minutes, the procedure is complete.

If the alarm does not clear within 5 minutes, contact your next level of support.

14 The procedure is complete.

—End—

Clear the GWC320 Phase 2 SA failure alarm

Purpose of this procedure

This procedure describes how to clear a GWC320 major alarm raised for the following specific problem: Phase 2 SA failure - <remote_gateway_IP_address>.

This alarm may have associated security logs, which provide additional details about the problem. For the description of all IKE/IPSec security logs, see procedure "IPSec and IKE security logs" (page 144).

When to use this procedure

Use this procedure to clear a GWC320 Phase 2 SA failure alarm.

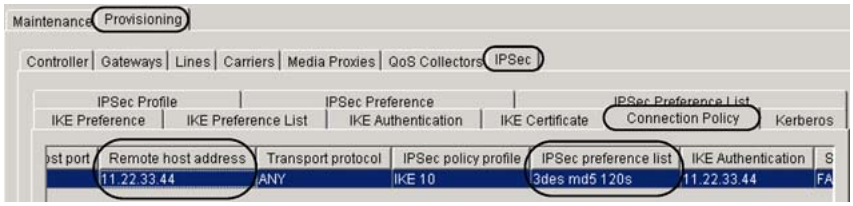
Prerequisites and guidelines

Complete the following tasks before starting this procedure:

- Verify whether any security logs associated with the alarm exist in the syslog file. Follow procedure "View GWC logs in syslog files" (page 68), searching for the text string ISAKMP_FAIL. An ISAKMP_FAIL log with the same date and time as the alarm may indicate the precise reason for the failure.
- Make sure that the remote media gateway is enabled and that the IPSec on the remote gateway is enabled.

Action

Step	Action
	At your workstation
1	Launch the CS 2000 Management Tools client application. If required, see procedure "Launching CS 2000 Management Tools and NPM client applications".
	At the CS 2000 GWC Manager client
2	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
3	From the Contents of: Gateway Controller frame, select the GWC node on which the alarm is raised.
4	Click the **Provisioning** tab, the **IPSec** tab, then the **Connection Policy** tab to display connection policies currently configured for the selected GWC node.



5 In the Remote host address column, find the IP address that matches the <remote_gateway_IP_address> in the alarm.

If there is more than one policy with the same Remote host address, select the one with the lowest policy ID. Click that row to highlight the policy.

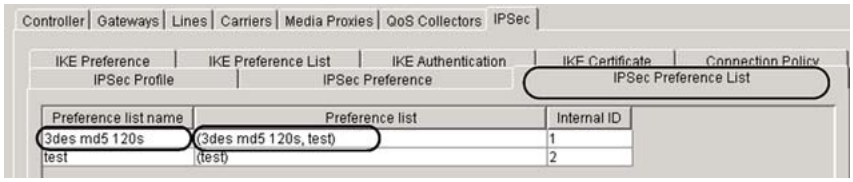
The policy with the lowest ID number has the highest priority and will be selected by the GWC.

The remote host IP address must match the IKE Authentication gateway IP address displayed in the same row.

If the highlighted policy is	Do
FLEX or SECURE	Continue the procedure.
BYPASS or DISCARD	Stop the procedure and contact your next level of support.

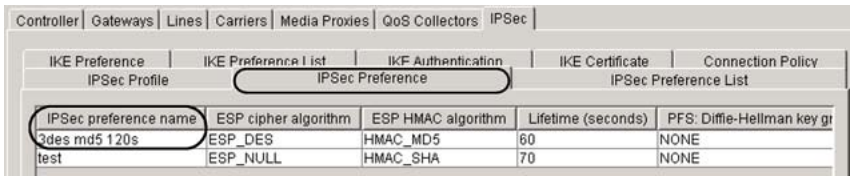
6 Note the name of the IPSec preference list configured for the selected connection policy.

7 Click the **IPSec Preference List** tab. Find the preference list name that matches the name noted in step 5.



8 Note the names of all preferences included in the list (displayed in the Preference list column). Each preference list can include up to five preferences.

9 Click the **IPSec Preference** tab.



Under IPSec preference name heading, find the preferences noted in the previous step and verify that the configuration values for at least one preference match the values configured on the remote gateway.

If the remote gateway is a Media Gateway 9000, verify that one of the preferences has the following values:

- ESP cipher algorithm = ESP_NULL
- ESP HMAC algorithm = SHA
- Lifetime = 57600
- PFS: Diffie-Hellman key group = 1

10 Use the following table to determine your next step.

If IPSec preference values	Do
do not match	Go to the next step.
match	Stop the procedure and contact your next level of support.

11 Add a new IPSec preference and IPSec preference list with the configuration values that match the values configured on the remote gateway.

If required, see procedure "Configure IPSec Preference and Preference List" in *Gateway Controller Security and Administration* (NN10213-611).

12 Change the connection policy selected in step 4 by selecting the new IPSec preference list.

If required, see the appropriate steps in procedure "Modify an existing IPSec connection policy" in the *Gateway Controller Security and Administration* (NN10213-611).

13 If the alarm does not clear within 5 minutes, contact your next level of support. Otherwise, go the next step.

14 The procedure is complete.

—End—

View and interpret the operational status of a GWC node

Purpose of this procedure

Use this procedure to determine the operational status of a selected Gateway Controller (GWC) node using the CS 2000 GWC Manager.

When to use this procedure

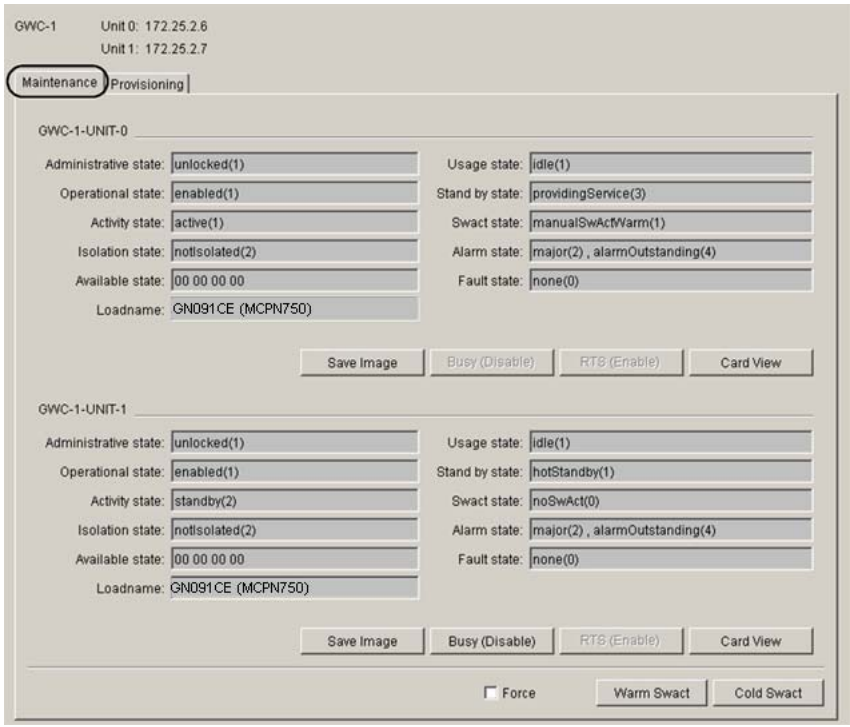
Use this procedure as a primary source of information about the operational status of a GWC card or GWC node.

Prerequisites or guidelines

This procedure has no prerequisites or guidelines.

Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.
3	Click the **Maintenance** tab. The GUI displays the Maintenance panel with two independent status views, one for each of the GWC cards in the node.



4 See table "CS 2000 GWC Manager status fields" (page 55) following this procedure to interpret the GWC card (unit) status fields.

If the selected GWC loses communication with the GWC Manager, the client does not provide an accurate status of the GWC node. You can verify the call processing status of a GWC node using the MAPCI interface. If required, follow procedure "Verify the call processing status of a GWC node" (page 54).

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

6 The procedure is complete.

—End—

Verify the call processing status of a GWC node

Step	Action
	At the MAPCI interface
1	Enter the peripheral module maintenance level by typing `>MAPCI;MTC;PM` and pressing the Enter key.

2 Post the desired GWC node in the control position by typing

>post GWC <node_number>

and pressing the Enter key.

where

node_number is the node number of the GWC that you selected

3 The system displays both GWC units and their current states. Verify the current state of the selected GWC node.

The GWC node can be in one of the following states:

- InSv (in service)

  If one or both units are in an InSv state, the GWC is capable of performing call processing.

- SysB (system busy) or ManB (manual busy)

  If both units are in SysB or ManB state, the GWC is not capable of performing call processing.

4 Go back to step 5 in the main procedure.

—End—

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

CS 2000 GWC Manager status fields

Status field	Possible values	Meaning
Administrative state:	locked	The unit is prohibited, administratively, from providing service to users.
	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.

Status field	Possible values	Meaning
	disabled	The unit is not operating or providing service to users. If the Administrative state for this unit is "locked", then the unit has been manually busied. If the Administrative state for this unit is "unlocked", then the unit has been busied by the system.
Activity state:	active	The unit is currently providing end user services. This is the state of the node as seen by other network elements.
	standby	The unit is not providing end user services but can be switched to Active at any time if the active (mate) unit fails.
Isolation state:	isolated	The unit is not communicating with the Core.
	notisolated	The unit is communicating with the Core.
Available state:	offLine(3)	The unit has not received its configuration data from the CS 2000 GWC Manager. The unit cannot provide service until it is booted and receives configuration data.
	degraded(6)	The unit does not have heartbeat communication with its mate and it is operating without fault-tolerant redundancy.
	offLine(3), degraded(6)	The unit has both: offline and degraded conditions.
	00 00 00 00	The unit does not have either of the preceding conditions.
Loadname:	<string_of_alphanumeric_ characters>	This is the name of the load file that the unit currently boots from. The file is located on the CS 2000 Core Manager or Core and Billing Manager (CBM) disk drive.
Usage state:	idle	The GWC maintenance system is not currently working on a request, such as a Return to Service (RTS). The unit is available for maintenance requests.
	busy	Maintenance is in progress on this unit and no further requests are accepted.
Stand by state:	providingService	The unit is the active unit and is providing service.
	hotStandby	The unit is the standby unit - ready to provide service.

Status field	Possible values	Meaning
	coldStandby	The unit is synchronizing with the active unit (not providing redundancy). After completion of synchronization, the status changes to hotStandby when the Operational state is enabled.
Swact state:		This field indicates the last switch of activity for the unit.
	manualSwActWarm	Last switch of activity was due to a manual warm SwAct. Requested by a user, a warm SwAct causes no service interruption to stable calls, but calls in the setup processes can be lost.
	manualSwActCold	Last switch of activity was due to a manual cold SwAct. Requested by a user, a cold SwAct temporarily takes both units out of service and takes down all calls.
	autonomousSwActWarm	Last switch of activity was due to a system warm SwAct. These SwActs are automatically performed by the device in response to faults or failures. Established calls are preserved. Calls in setup are lost.
	autonomousSwActCold	Last switch of activity was due to a system cold SwAct. These SwActs are automatically performed by the device in response to faults or failures. All calls are lost.
	noSwAct	No switch of activity has occurred.
Alarm state:		This field indicates the severity of the currently raised alarms.
	00 00 00 00	There are no alarms raised on the GWC card unit.
	critical(1)	If present, indicates that one or more critical alarms have been raised.
	major(2)	If present, indicates that one or more major alarms have been raised.
	minor(3)	If present, indicates that one or more minor alarms have been raised.
	alarmOutstanding(4)	If present, indicates that at least one or a combination of different alarms has been raised.
Fault state:	none(0)	This field is not used.

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

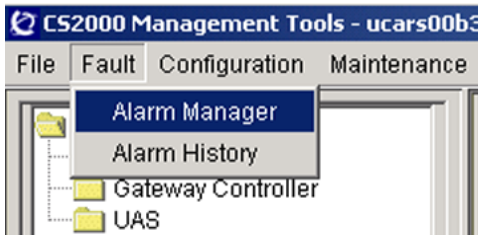
Use this procedure when implementing your fault management alarm strategy. You may also use this procedure to focus on specific alarms during alarm clearing or diagnostic activities.

Prerequisites

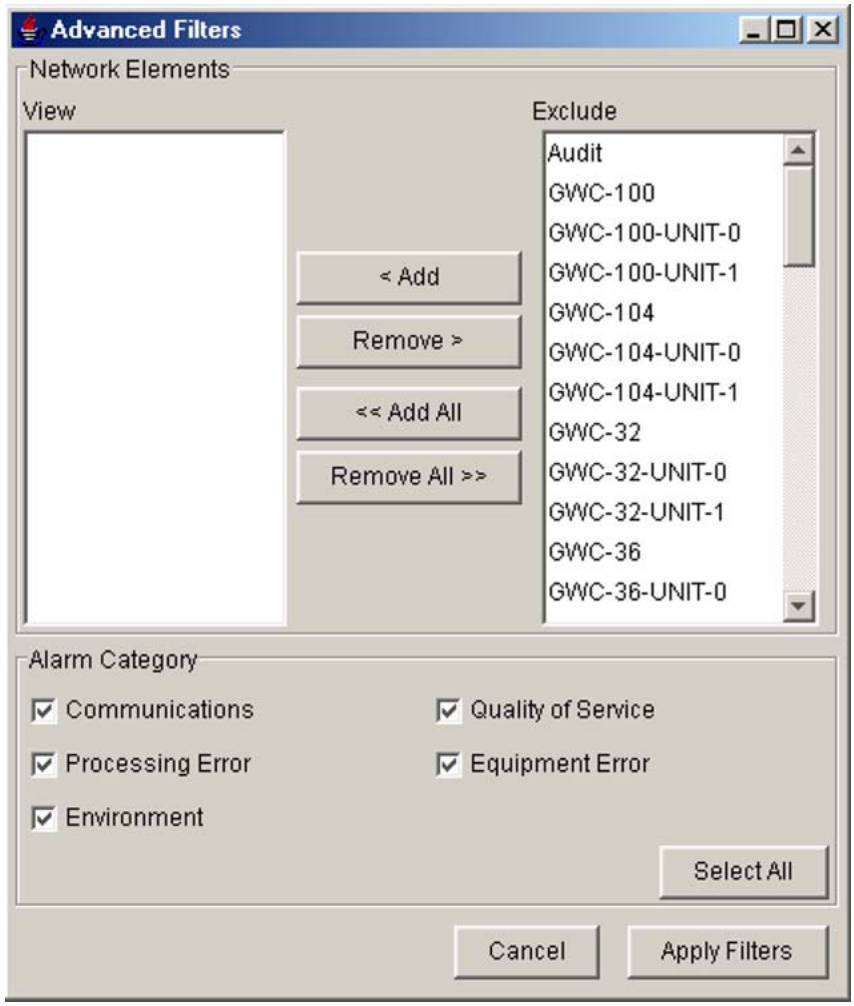
This procedure has no prerequisites.

Action

Step	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 at the bottom of the Alarm Manager window to open the Advanced Filters window.
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 in the upper left corner of the screen and select **Close**.

5 This procedure is complete.

—End—

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" (page 63)
- "Unlocking a card that has failed a diagnostic test" (page 64)

When to use this procedure

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

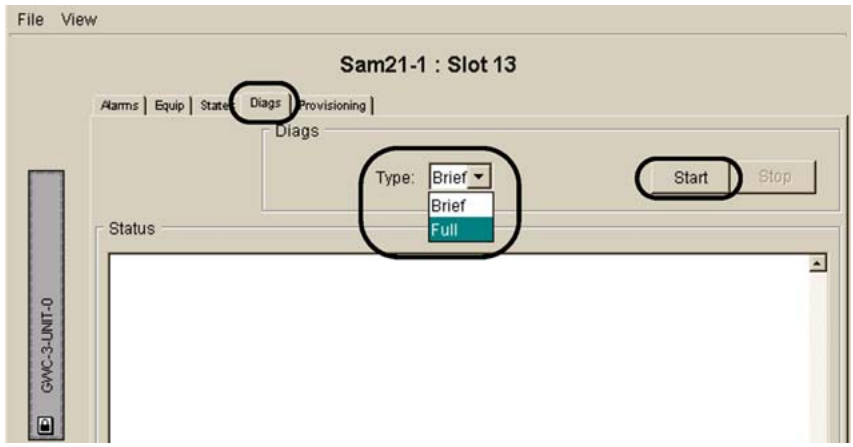
Prerequisites

The GWC card on which you wish to perform diagnostics must first be locked using the CS 2000 SAM21 Manager. Follow procedure "Lock a GWC card" in *Gateway Controller Security and Administration* (NN10213-611).

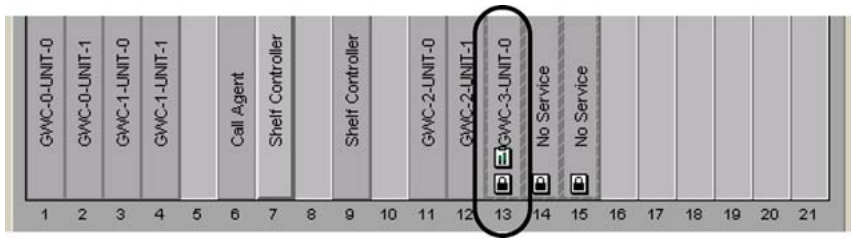
For additional information about GWC card states and diagnostics, see procedure "Interpret GWC card states" (page 86) in this NTP.

Action

Step	Action
	At the CS 2000 SAM21 Manager client
1	In the Card View window, click the **Diags** tab. 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.

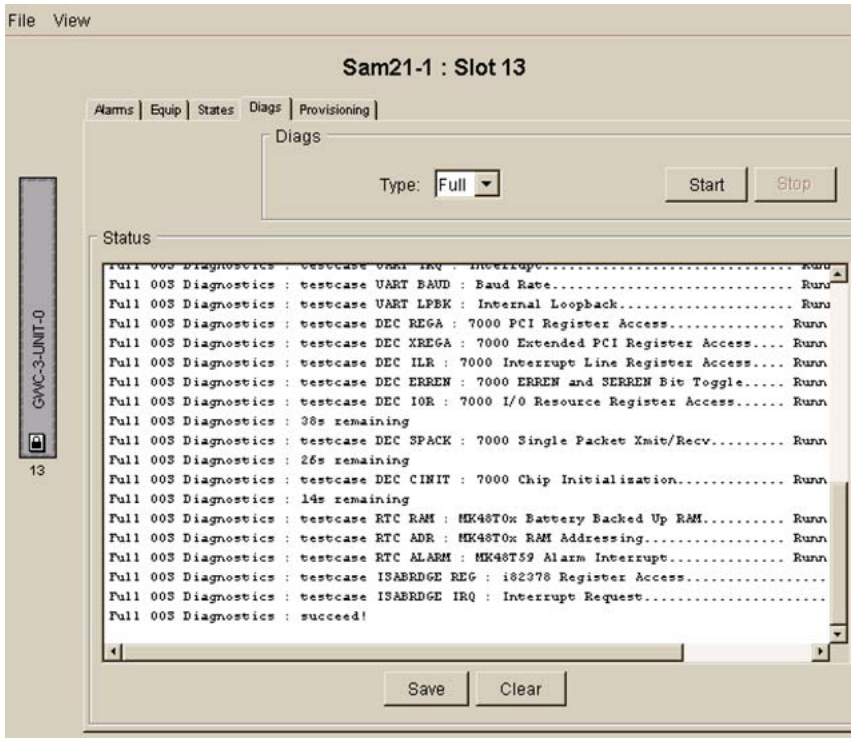


A diagnostics icon appears on the GWC card in the Shelf View.



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

If the diagnostic test indicates a hardware failure of any kind, see section "What to do if a diagnostic test fails" (page 63).



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.

5 This procedure is complete.

—End—

What to do if a diagnostic test fails

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

Step	Action
1	Rerun the diagnostics using the Brief test option.
2	If the Brief test passes, go to step 3. If the Brief test fails, go to step 5.
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.

5 Replace the card using the procedure "Replace and re-provision a GWC card" (page 97) in this NTP.

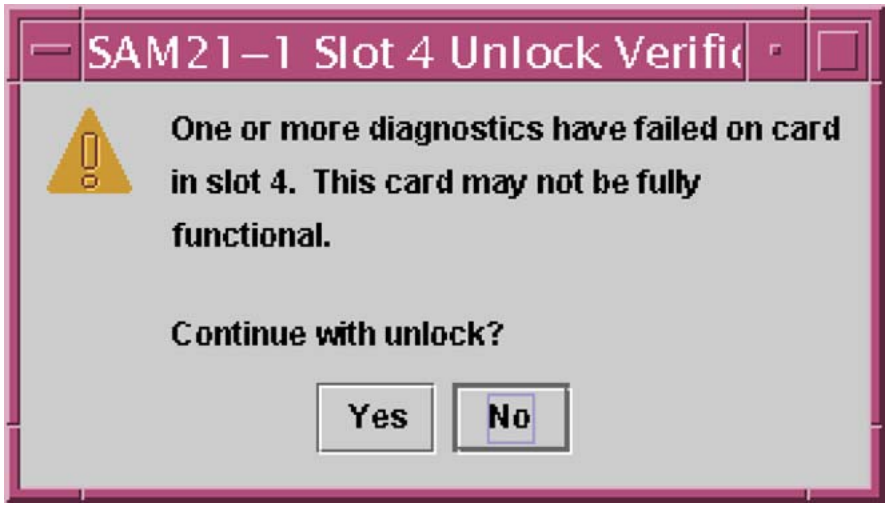
Return the defective card to Nortel according to the procedures of your service contract.

—End—

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 support personnel.



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" (page 61).

Prerequisites

Perform a diagnostics test.

Action

Step	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.

—End—

View GWC PM logs

Purpose of this procedure

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

For specific information about the logs, and any actions required, see the PM log descriptions in *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909).

When to use this procedure

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

Prerequisites

This procedure has no prerequisites.

Action

Step	Action
	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.
>
```

For information about PM logs related to GWC activities, see the appropriate PM log description in the *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909).

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

4 This procedure is complete.

—End—

View GWC logs in syslog files

Purpose of this procedure

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

For a list of GWC syslog logs, see section "Syslog files relevant to the GWC" (page 71).

This procedure describes how to access syslog files by logging into the CS 2000 Management Tools server using telnet or ssh. You can also access syslog files using the Integrated Element Management System (IEMS) GUI. If required, see the IEMS procedure “Viewing audit and security logs”.

When to use this procedure

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

Prerequisites

You need the root user ID and password to log in to the CS 2000 Management Tools server.

Action

Step	Action

At your workstation

1 Establish a login session to the CS 2000 Management Tools server using one of the following methods:

If using	Do
telnet (unsecure)	go to step 2
ssh (secure)	go to step 3

2 Complete the following sub-steps to log in using telnet.

a. Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the hostname or IP address of the server

b. When prompted, enter you user ID and password.

c. Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d. When prompted, enter the root password.

Continue with step 4.

3 Complete the following sub-steps to log in using ssh (secure).

Use the following command only if your workstation platform supports ssh. Otherwise, the command fails.

a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the hostname or IP address of the server

b. When prompted, enter the root password.

At the CS 2000 Management Tools client

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

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

and pressing the enter key.

5 List the directory content by typing

```
$ ls
```

and pressing the enter key.

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

6 If the file that you want to view is zipped (has an extention .gz), unzip it using the following command. Otherwise, go to the next step.

Unzip the file by typing

```
$ gunzip <log_filename.gz>
```

and pressing the enter key.

where

log_filename.gz is the name of the log file you want to unzip

Example
$ gunzip securitylog.1.gz
The file changes to a readable file securitylog.1.

7 Use the following table to determine your next step.

If you want to view	Do
the entire content of a log file	go to step 8
specific content of a log file	go to step 10

8 Display the entire content of a log file by typing

$ cat <log_filename> |more

and pressing the enter key.

where

log_filename is the name of the log file you want to display. For specific examples, see table "Syslog logs containing GWC entries" (page 71).

Example
$ cat customerlog.0 |more

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

9 Continue with step 11.

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

$ cat <log_filename> |grep <search_string>

and pressing the enter key.

where

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

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

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

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

12 This procedure is complete.

—End—

Syslog files relevant to the GWC

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

Syslog logs containing GWC entries

Log type	Description	Examples of log file names
Audit log	Records the actions taken by users on the system, including some of the parameters they used.	auditlog 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 Kerberos and IKE/IPSec security.	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 equired

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.

To view a summary of auto-image logs, see procedure "View and troubleshoot GWC auto-image error logs" (page 75).

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

Step	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] UBSnmpSimpleT
rap 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
```

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 to search for other entries of the same text in the debug log, or for different text.

6 This procedure is complete.

—End—

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.

The log recycles after recording 2000 lines of text.

The section "Interpreting auto-image logs" (page 76) contains some examples of auto-image logs and suggested actions.

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

Step	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.

—End—

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 or Core and Billing Manager (CBM). See procedure "Enable/disable GWC software auto-imaging" in *Gateway Controller Configuration Management* (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.

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. For more information, see *Gateway Controller Configuration Management* (NN10205-511).

Prerequisites

You must first busy the GWC node using the CS 2000 GWC Manager before automatically reprovisioning any card in the node. Follow procedure "Busy a GWC Node" in *Gateway Controller Configuration Management* (NN10205-511).

Action

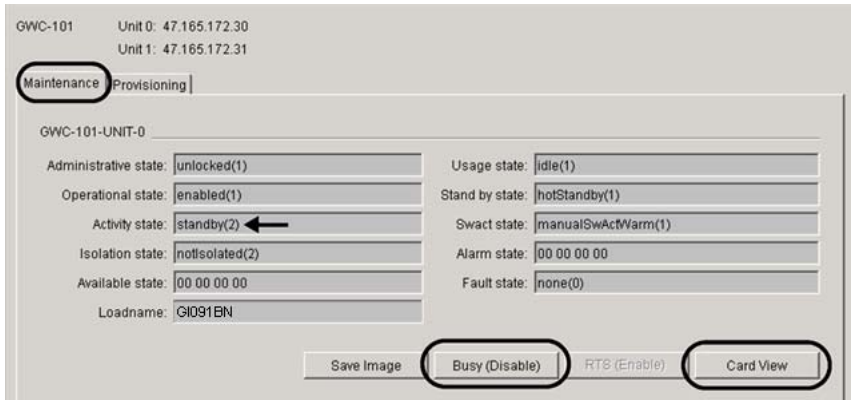
Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.
2	From the Contents of: Gateway Controller frame, select the GWC node that you wish to automatically reprovision, or type the name of the GWC node in the text field to the left of the **Go To** button.
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.

Follow procedure "Invoke a manual protection switch (warm SWACT)" in *Gateway Controller Security and Administration* (NN10213-611).

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

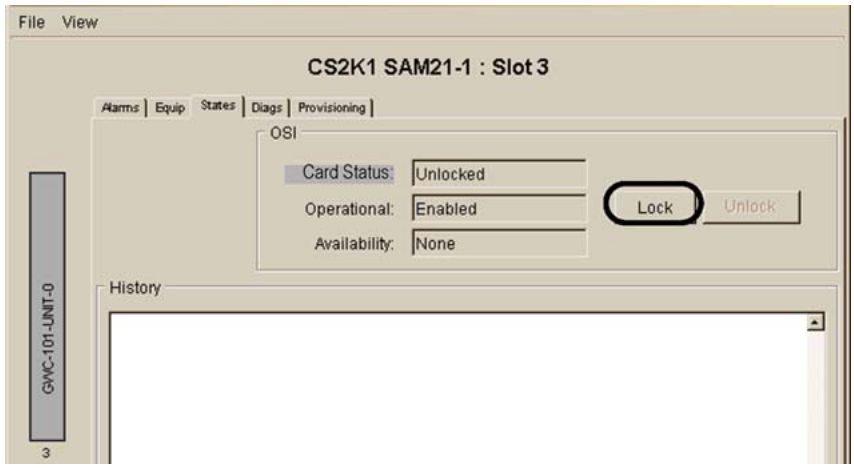
This would typically be the standby card in the node. Confirm this action at the prompt

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

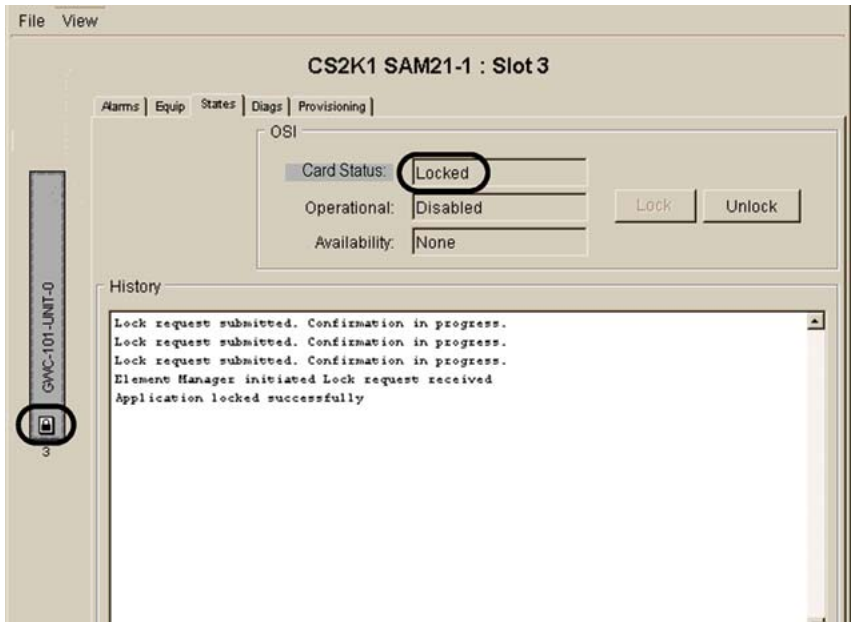


At the CS 2000 SAM21 Manager client

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



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 Card Status "Locked".



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.

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.

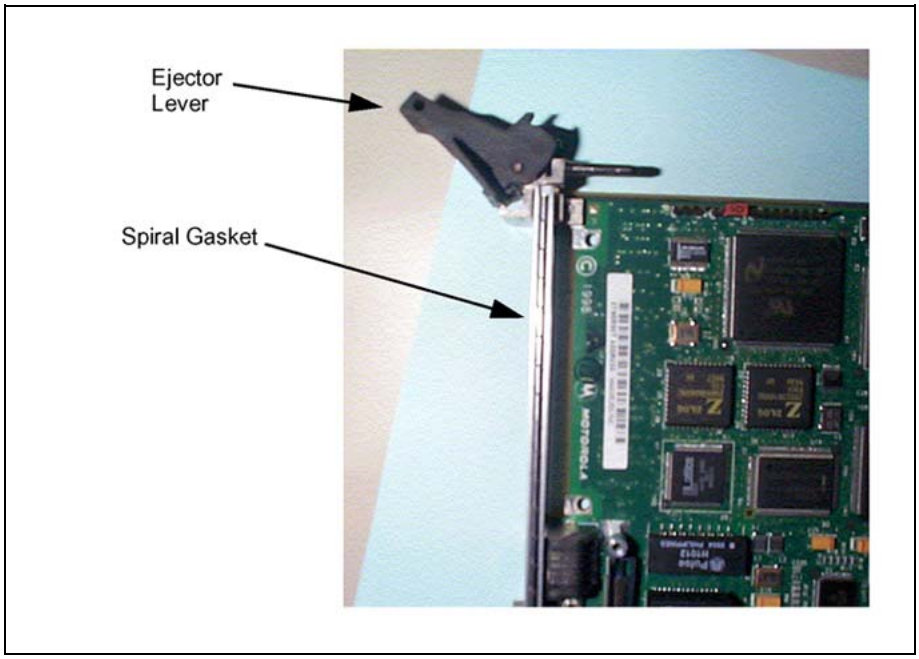
CAUTION

Static electricity damage

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

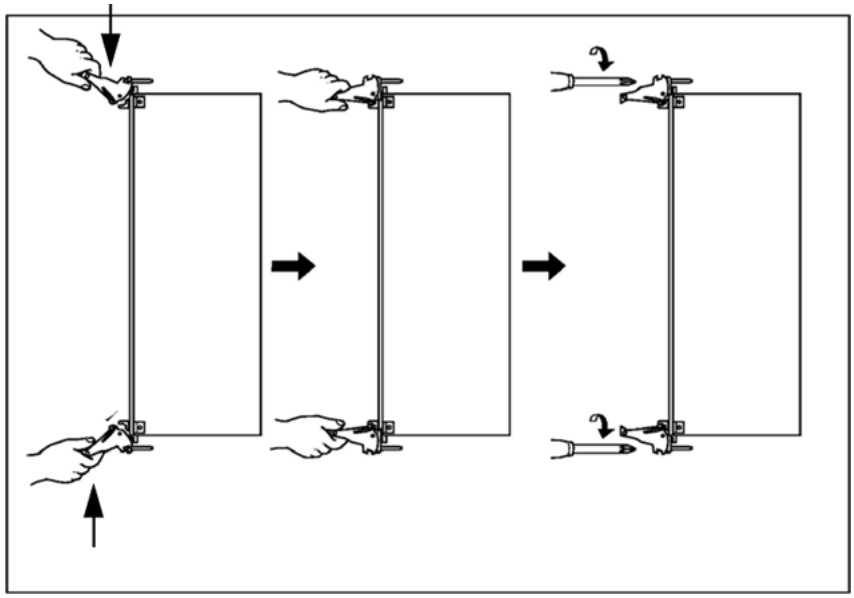
11 Hold the GWC card by the latches and remove the card from the shelf.

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.

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

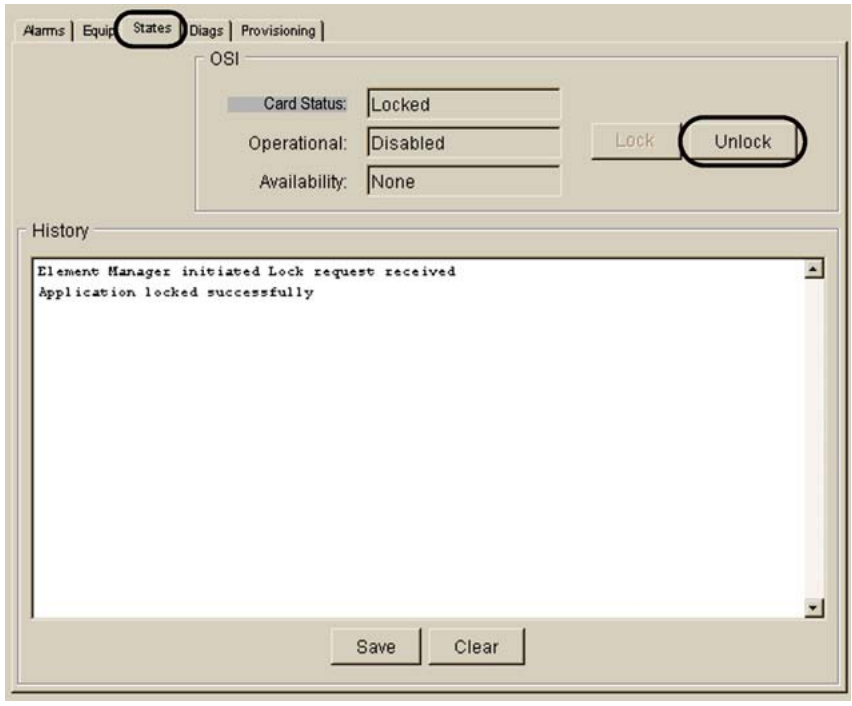
16 In the shelf view or card view window, wait until the GWC card you are reprovisioning appears as follows:

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.



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.

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.

20 Repeat this procedure for each GWC you need to automatically reprovision.

21 This procedure is complete.

—End—

Restart or reboot a GWC card

Purpose of this procedure

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

To restart software applications only, follow procedure "Restart GWC card services" (page 91).

When to use this procedure

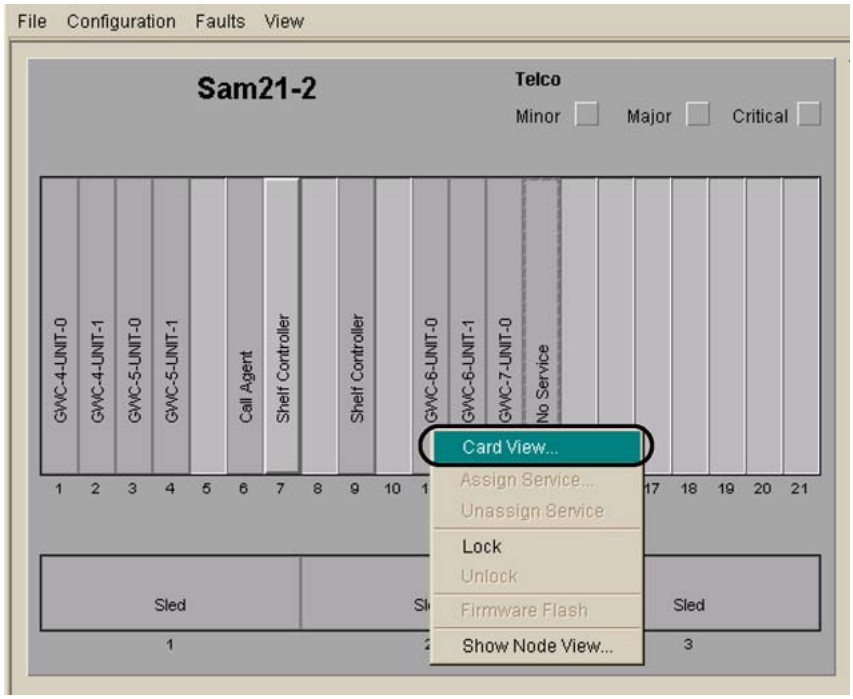
Use this procedure when you need to reboot a GWC card and force a GWC to download and execute a software load from the CS 2000 Core Manager or CBM.

Prerequisites

To reduce the risk of service interruption, you can first busy the GWC applications on specific GWC nodes using the CS 2000 GWC Manager. Follow procedure "Disable (Busy) GWC card services" in *Gateway Controller Security and Administration* (NN10213-611).

Action

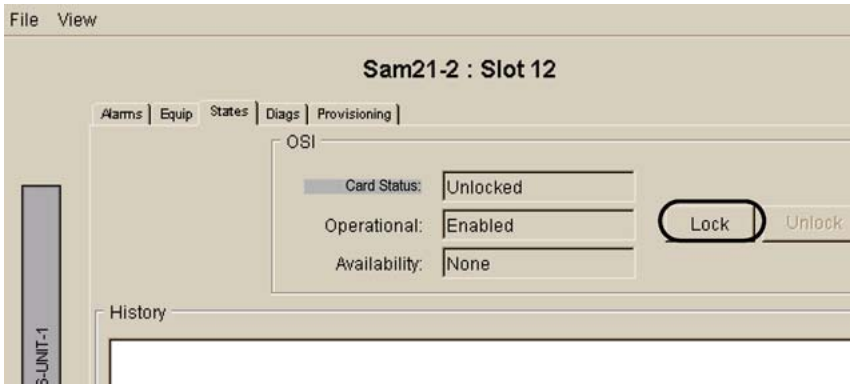
Step	Action
	At the CS 2000 SAM21 Manager client
1	From the Shelf View, right-click the GWC card you want to reboot and select **Card View** from the context menu.



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

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

The card must be busy (disabled) before you can lock it. If required, see procedure "Disable (Busy) GWC card services" in *Gateway Controller Security and Administration* (NN10213-611).



4 Wait until the Card Status is Locked and the History window indicates "Application locked successfully". Then, click the **Unlock** button.

5 Monitor the reboot process. Wait until the Card Status is "Unlocked" and the History window indicates "Bootloaded successfully".

6 This procedure is complete.

—End—

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" (page 87) suggests actions in response to different card states.

When to use this procedure

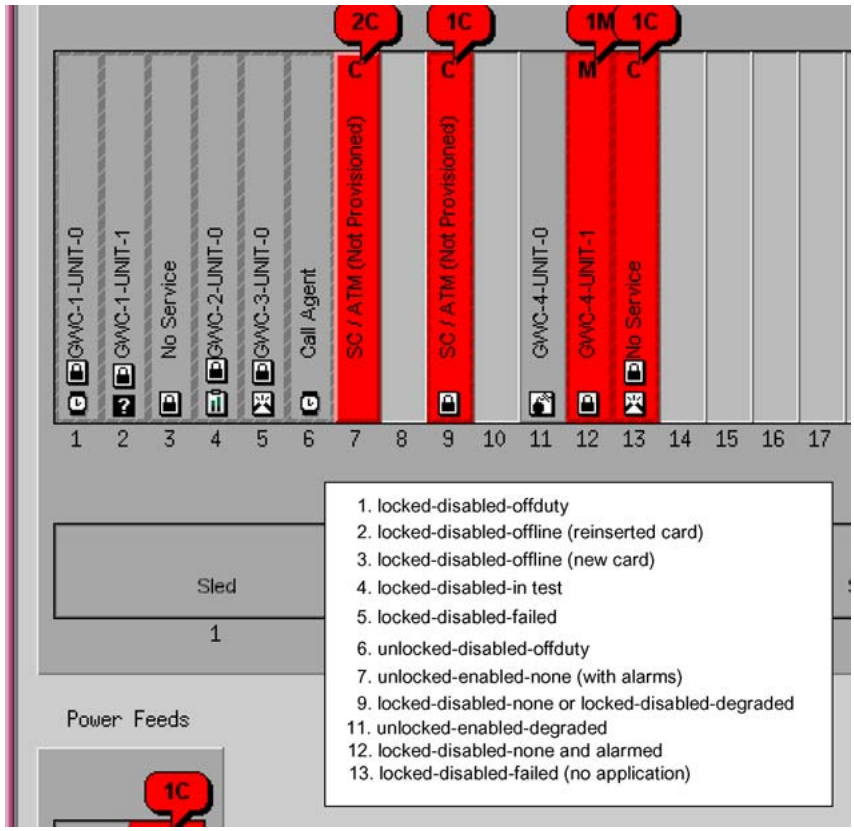
Use this procedure when you are encountering an unknown card state.

Prerequisites

There are no prerequisites for this procedure.

Action

Step	Action
	At the CS 2000 SAM21 Manager client
1	Review the following figure and determine the card icons that apply.



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 Use the following table to determine the next action.

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

State	Possible action
locked-disabled-offduty	Wait for the firmware flash to complete. Verify that the card changes to the locked-disabled-none state.

State	Possible action
  unlocked-disabled-offduty 	If the GWC card transitions to locked-disabled-degraded, follow the suggestions for that state. 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.
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.

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 support personnel. The active Shelf Controller generates two 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 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.
unlocked-enabled-degraded 	This card failed one or more diagnostics and was Unlocked. See "Unlocking a card that has failed a diagnostic test" (page 90) 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 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.

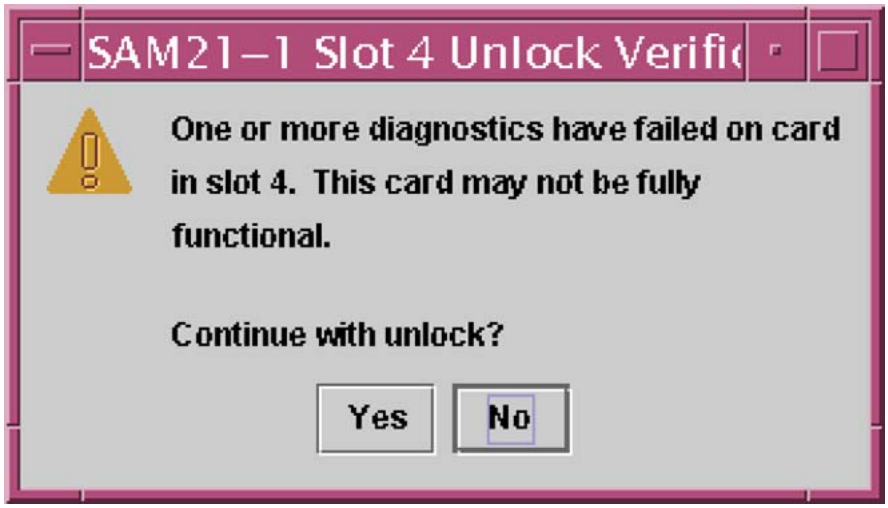
4 This procedure is complete.

—End—

Unlocking a card that has failed a diagnostic test

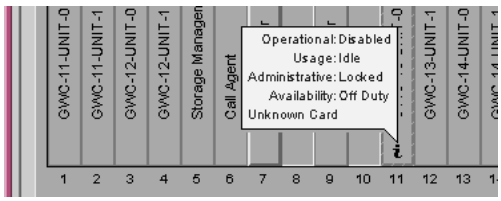
The following message appears on the CS 2000 SAM21 Manager if you attempt to unlock a card that has failed a diagnostic test.

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



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.



Restart GWC card services

Purpose of this procedure

Use this procedure to stop and restart call processing and network services on a standby GWC card.

To restart the hardware and software on an individual GWC card, follow procedure "Restart or reboot a GWC card" (page 83).

When to use this procedure

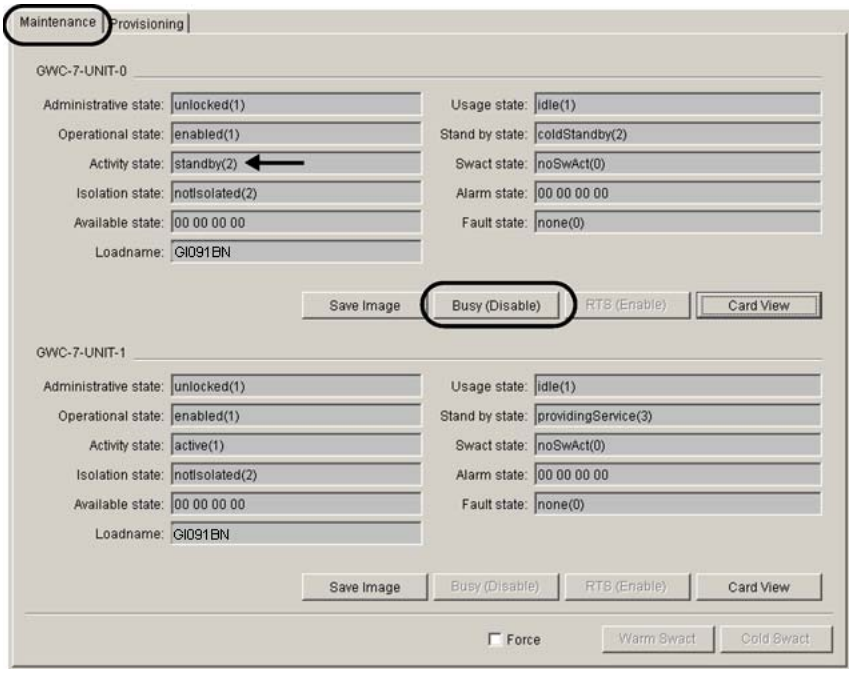
Use this procedure on a GWC card to determine if a known fault is temporary or persistent and if the fault is limited to the GWC card in question.

Prerequisites

To reduce the risk of service interruption, ensure that the card you are about to restart is in standby status. Otherwise, perform a call processing switch activity (SWACT) to change the card state from active to standby. If required, see procedure "Invoke a manual protection switch (warm SWACT)" in *Gateway Controller Security and Administration* (NN10213-611).

Action

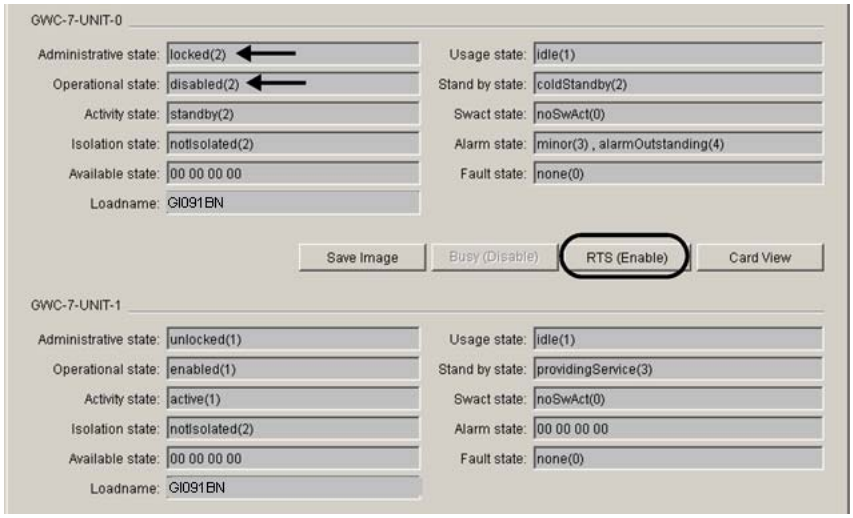
Step	Action
	At the CS 2000 GWC Manager client
1	At the main CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.
2	From the Contents of: Gateway Controller frame, select the appropriate GWC node you wish to restart.
3	Click the **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.



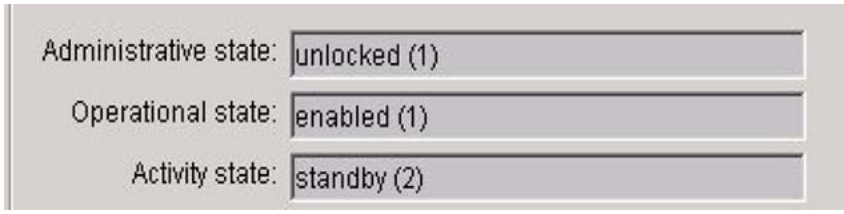
6 At the confirmation box, click **OK** to busy the standby GWC unit.

Wait for the CS 2000 GWC Manager screen to update the Operational state of the card to disabled(2).This indicates that the card has been busied

7 Click the **RTS (Enable)** button to return the card to service.



After 30 seconds, the Administrative state field changes to unlocked and the Operational state field changes to enabled.



The state change is automatic. However, if necessary, you can refresh the screen. At the top of the CS 2000 GWC Manager screen, click the **Windows** menu and select **Refresh GWC Status**.

8 This procedure is complete.

—End—

Diagnose problems with a GWC card that cannot be booted

Purpose of this procedure

Use this procedure to diagnose problems with a GWC card that cannot be booted and does not appear in the CS 2000 SAM21 Manager shelf view.

When to use this procedure

Use this procedure when a GWC card is installed in the SAM21 shelf but does not appear on the CS 2000 SAM21 Manager shelf view.

Prerequisites

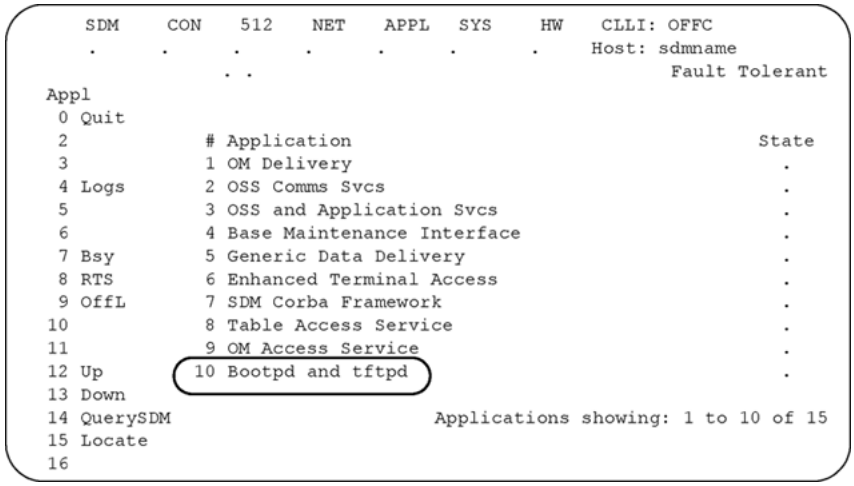
You must have root user access to the CS 2000 Core Manager or Core and Billing Manager (CBM) console.

Action

Step	Action
	At the CS 2000 Core Manager or Core and Billing Manager (CBM) console
1	Login to the CS 2000 Core Manager or CBM as the root user.

2	Start the CS 2000 Core Manager or CBM maintenance interface 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. *Example system response:*



In SDM, the application "Bootpd and tftpd" is an optional application and may not be installed on your system. In this case it would not be visible in the APPL level menu. In CBM, "Bootpd and tftpd" does not have a presence on the maintenance interface APPL level.

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

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

At the SAM21 frame

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

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

Use a standard straight through serial cable, rather than a null modem cable.

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

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

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

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

Error ID	Reason text
0500	TFTP retry time out. 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
8100	The load file on the CS 2000 Core Manager or CBM has the wrong path, the wrong permissions, or the wrong load name.
0020	Message CRC errors. The network could be busy and causing traffic errors.
0017	10baseT link failure. Verify that the Ethernet cable is fully seated in the faceplate and the router.

11 You have completed this procedure.

—End—

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 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.

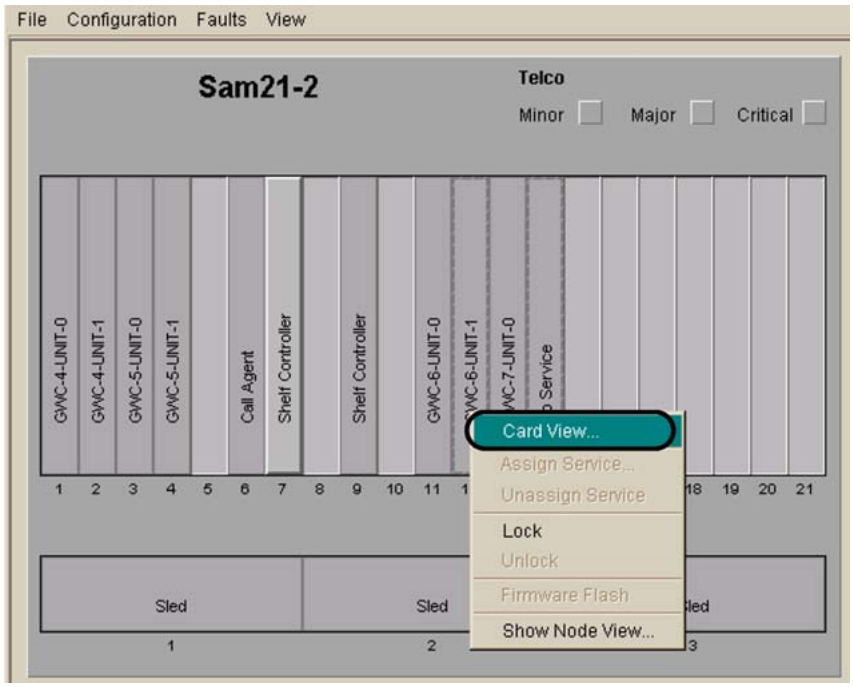
This procedure does not provide instructions to make services provisioning changes to a GWC card, such as changing the service profile type of a GWC node. If changes to the GWC node provisioning are necessary, use the CS 2000 GWC Manager to busy the cards and reprovision node information. For more information,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

Prerequisites

This procedure has no prerequisites.

Action

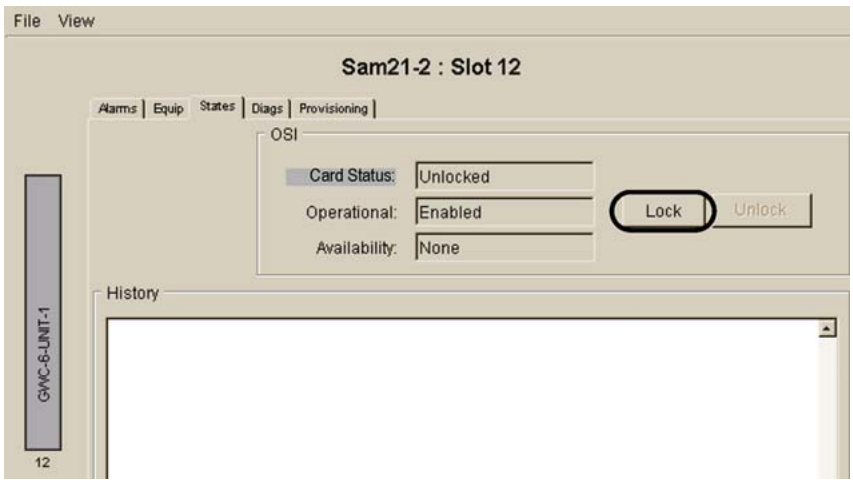
Step	Action
	At the CS 2000 SAM21 Manager client
1	Access the Card View for the card you want to replace by right-clicking the card and selecting **Card View**.



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

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

The card must be busy (disabled) before you can lock it. If required, see procedure "Busy a GWC node" in *Gateway Controller Configuration Management* (NN10205-511).



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.)

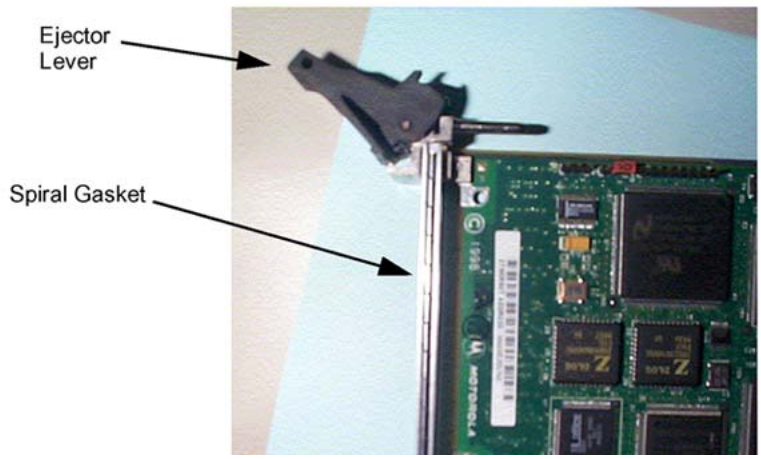
CAUTION
A service outage can occur if care is not taken while removing the GWC circuit packs.

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.

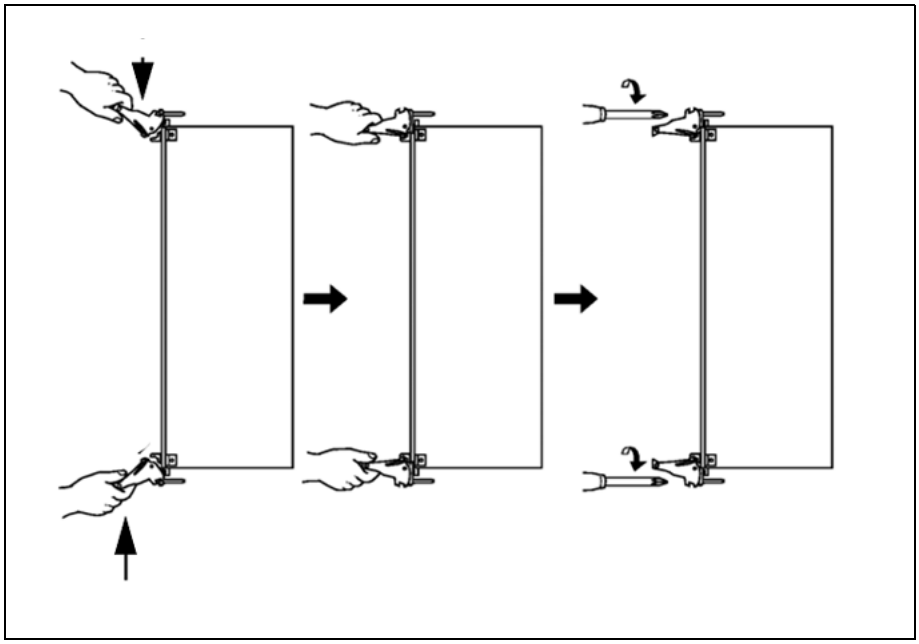
CAUTION
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the SAM21 Shelf Cabinet when handling a GWC card. The strap protects the card against damage caused by static electricity.

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

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. 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.

On insertion of the new card, the system automatically provisions the new card with the old card's provisioning information.

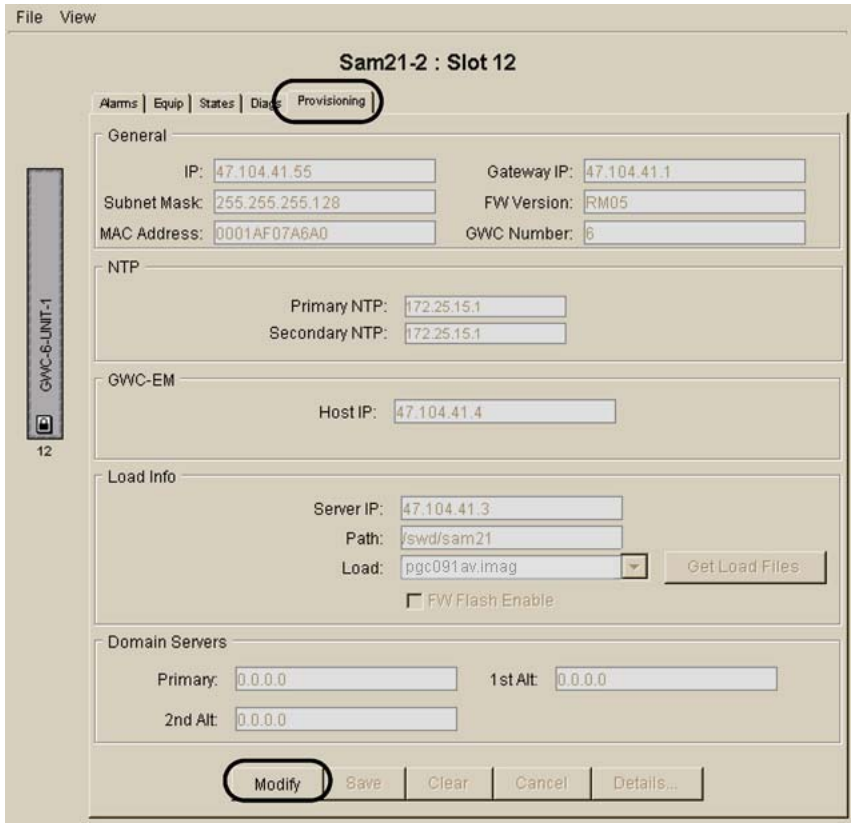
The system assigns a new MAC address to the new card.

The CS 2000 SAM21 Manager displays the card name (MCPN905, MCPN750) and the corresponding memory size in the Equip tab of the card view.

13 Determine the next action to take.

If	Do
the provisioning data is correct data for the replacement GWC	the procedure is complete
the provisioning data for the replacement GWC requires changes	continue with the next step

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

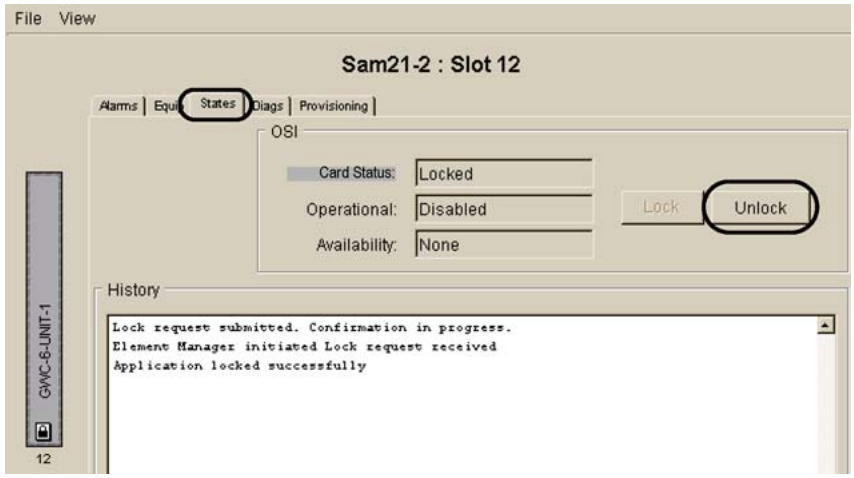


15 Click the **Modify** button to make changes to the provisioning datafill.

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

You do not need to type the load name. Click the **Get Load Files** button and select the required load from the drop-down list.

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



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

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

20 This procedure is complete.

—End—

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 (SESM), the Session Server (SS) Manager database (SIP lines), and the CS 2000 Core database.

The audit checks the information in these 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.

You can also use this tool to schedule a line data integrity audit. If required, see procedure "Configure a recurring data integrity audit" in *Gateway Controller Configuration Management* (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 Core database:

- DNINV
- LGRPINV
- LNINV
- HUNTMEM (if hunt groups have been provisioned)
- MDNMEM (if MADN groups have been provisioned)
- LTMAP (if ISDN BRI endpoints have been provisioned)

For SIP lines, the system audits and compares the following data stored in the SS Manager database:

- the endpoints - compares with the GWC Manager database
- group directory number (DN) and member (endpoint/line equipment number [LEN]) information - compares with CS 2000 Core
- DN to LEN mapping - compares with the CS 2000 Core

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.

Single-direction and double-direction audits

In a single-direction audit (SESM to Core), for each line in the SESM table, the system queries the Core tables for corresponding lines. You can request a single-direction audit by selecting individual elements at step 6 in the following procedure.

For a single GWC, LGRP, or gateway, only the single-direction line audit is implemented.

In a double-direction audit, SESM and Core independently query all the lines in their own tables, then the system compares the SESM and Core lines. You can request a double-direction audit by selecting the Select ALL check box at step 6 in the following procedure.

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.

Prerequisites and guidelines

Do not run an on-demand line data integrity audit while line provisioning is occurring.

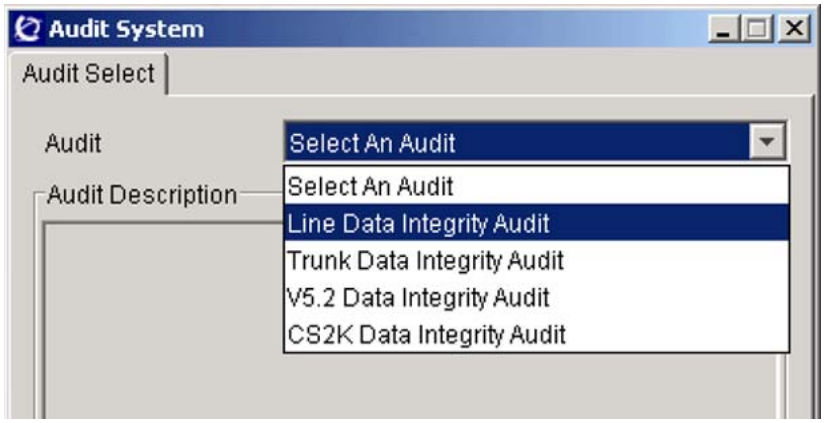
The audit application keeps no record of problems that caused the alarm. Therefore, if a problem is detected during an audit and it is not corrected, an alarm is generated for the same problem the next time the audit runs.

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. If you wish to view the currently running audits, see procedure "View or abort running audits" (page 133) in this NTP.

Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, select **Maintenance**, then **Audit System**.

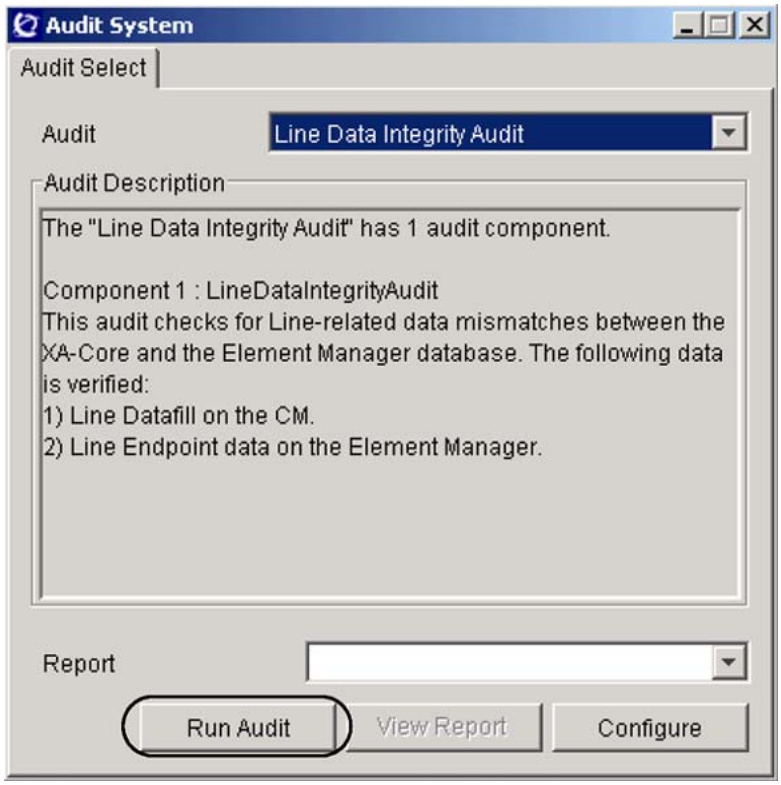
2 At the Audit System dialog box, select **Line Data Integrity Audit** from the list of audits displayed in the drop-down menu.



3 Use the following table to determine your next step.

If you want to	Do
perform an on-demand line audit	go to step 4
view a line audit report	go to step 13

4 At the Audit System dialog box, click the **Run Audit** button.



5 At this time, the system performs the following checks to ensure that it is ready for the audit:

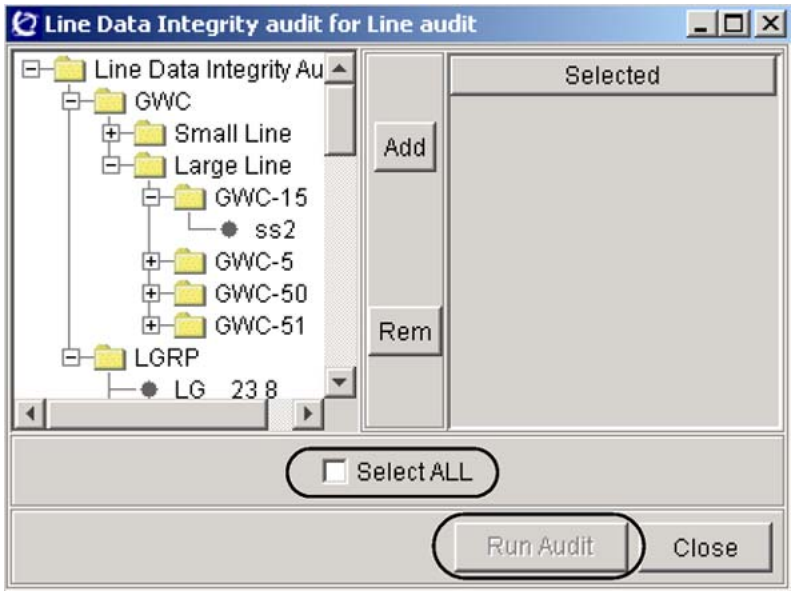
- Are there 10 or more non-query line provisioning operations running?
- Is the batch provisioning tool (BPT) running a lines batch operation?
- Is there any bulk query operation in progress?

After each check, if the condition is found, the system displays an appropriate warning message describing the condition and informing you that running an audit at this time will impact user response time.

After each warning, you can click the **Cancel** button to postpone the audit. Repeat this procedure at a later time.

If you wish to continue the audit, click the **Proceed** button on each displayed warning dialog box. Go to the next step to continue this procedure.

6 The system displays a Line Data Integrity selection window to allow you to select the elements that you wish to audit.



The Line Data Integrity Audit list on the left displays all the small and large line GWCs and the associated gateways, as well as the logical line groups of these small line or large line gateways. You can display or hide any of the sub-lists by clicking on the plus (+) or minus (-) sign.

From the list on the left,

- click and highlight the specific item that you want to audit (single-direction audit; for more information see "Single-direction and double-direction audits" (page 103)

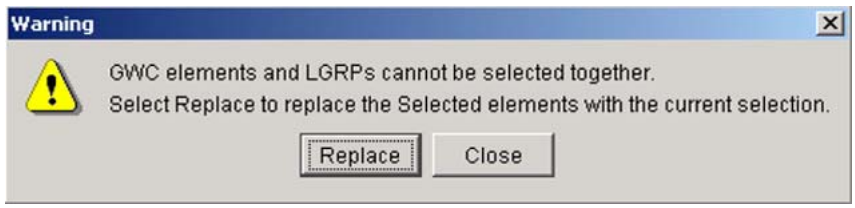
or

- click the Select ALL check box to select all GWCs and associated gateways or all logical groups (LGRP) - double-direction audit; for more information see "Single-direction and double-direction audits" (page 103)

Use the following guidelines:

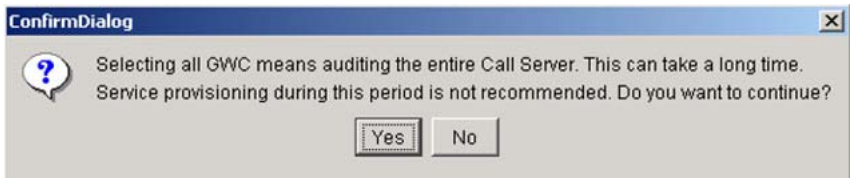
- You can click and select individual items (for example, ss2) or you can click a heading to select all items listed underneath (for example, Large Line).
- If you wish to select more than one item at the same time, press the Shift key and click each item that you want to select.
- You cannot select GWCs and LGRPs for the same audit. If you attempt to select both, the system displays the following warning:

If you try to select a GWC element and an LGRP is already selected (or the opposite), the system displays the following warning:



If you wish to continue your selection, click the **Replace** button. Otherwise, click the **Close** button.

- If you click the Select ALL check box, the system displays the following confirmation message:



Click **Yes** if you wish to continue. Otherwise, click **No**.

7 Click the **Add** button.

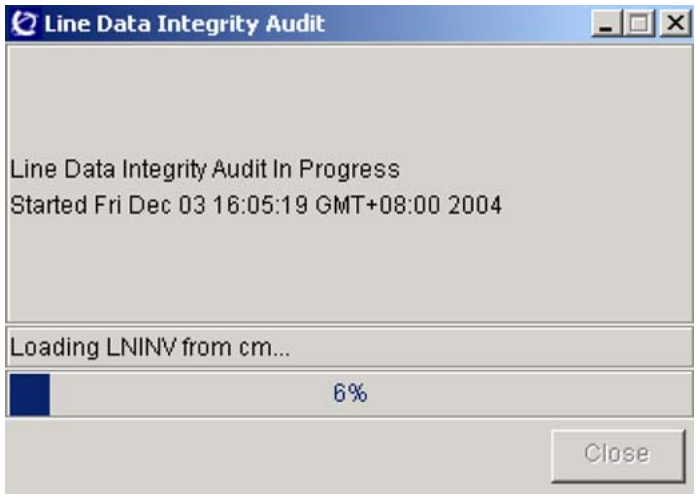
Your selection appears in the Selected box on the right.

8 If necessary, repeat the selection process until all the items that you want to audit appear in the Selected window.

If you need to remove an item from the Selected table, click the item to highlight it, then click the **Rem** button.

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

10 During a line audit, the system displays a progress window, which includes the progress bar and the current operation.



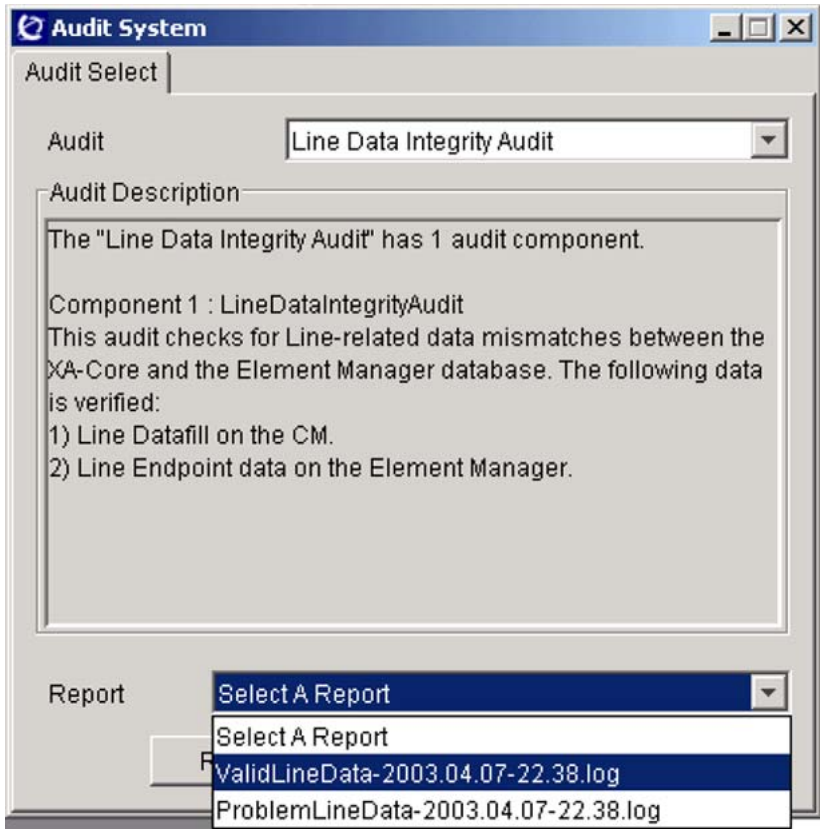
11 The audit may take a few minutes to complete. When the audit is successfully completed, the system displays the following message:

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.

12 Click the **Close** button to close the Audit Status window.

13 To view the line audit reports, complete the following sub-steps.

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



b. From the drop-down menu in the Report field at the bottom of the dialog box, select the **ValidLineData** or the **ProblemLineData** report that you want to view. If there is more than one 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 or ProblemLineData-<date>-<time>.log

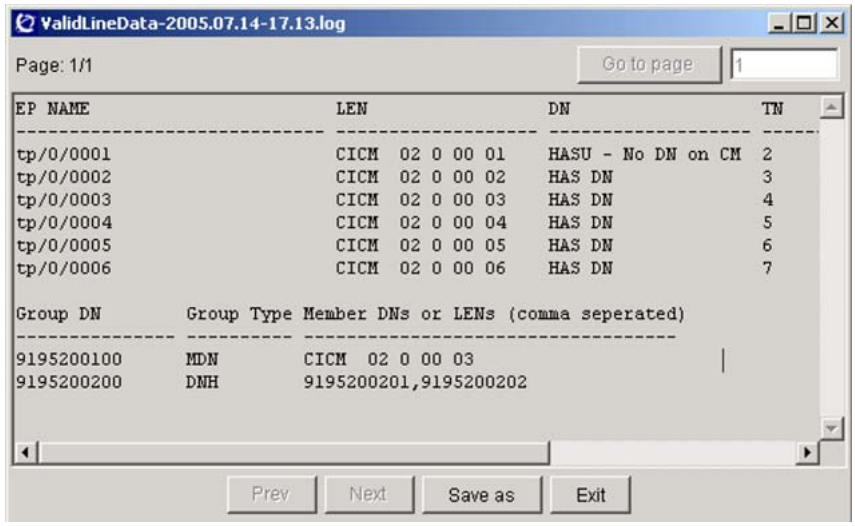
where

<date> is the date in yyyy.mm.dd format; for example, 2003.02.15.
<time> is the time in hh.mm format; for example 17.30.

c. Click the **View Report** button.

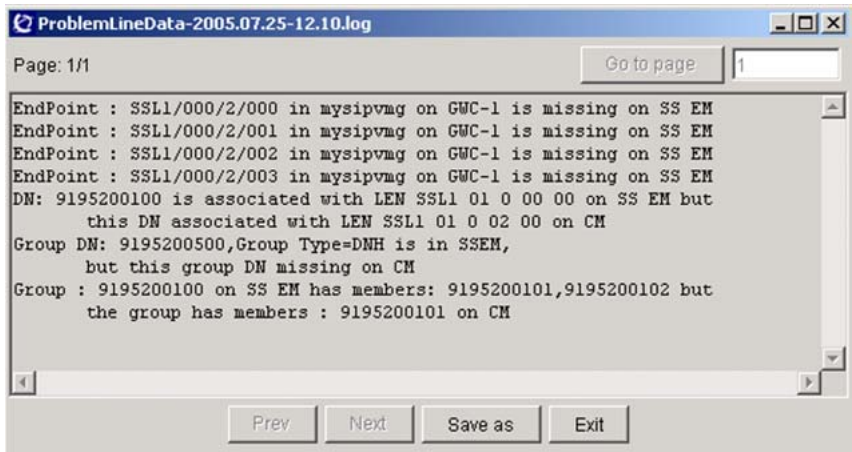
The system displays the selected report.

Example
The following is an example of a "ValidLineData" report.



Example
The following is an example of a "ProblemLineData" report.

If the audit found no problems, the "Problem" report contains a message stating that no problems were found.



You can configure the number of reports that the CS 2000 Management Tools server retains. The maximum default value is seven. When a new line audit occurs, the server deletes the oldest report.

The system places 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 to 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. For a description of each problem, see the printed copy of the ProblemLineData report. To correct the problems, you need to delete and reprovision the listed lines.

g. After viewing the report, click the **Exit** button at the bottom of the screen.

14 This procedure is complete.

—End—

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 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.

You can also use this tool to schedule a trunk data integrity audit. For instructions, see procedure "Configure a recurring data integrity audit" in the *Gateway Controller Configuration Management* (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 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.

Do not run an on-demand trunk data integrity audit while trunk provisioning is occurring.

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

ATTENTION

If you have scheduled data integrity audits, remember that a maximum of one 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

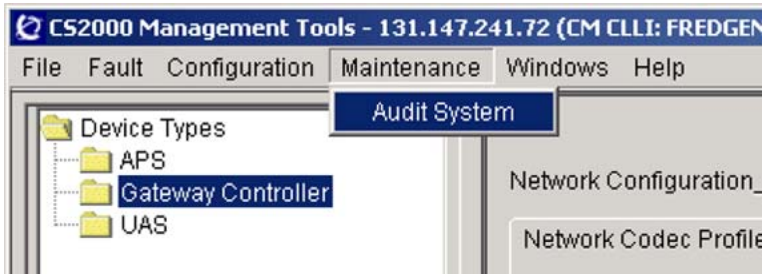
Ensure that there are no trunk audits scheduled to occur during a manual audit.

Action

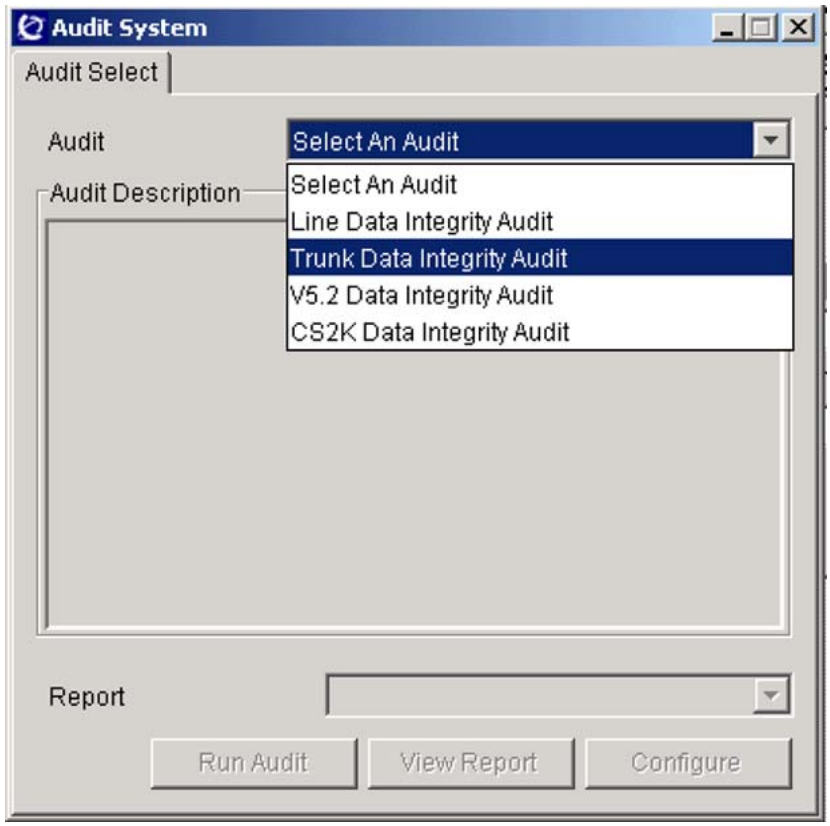
Step	Action

At the CS 2000 GWC Manager client

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



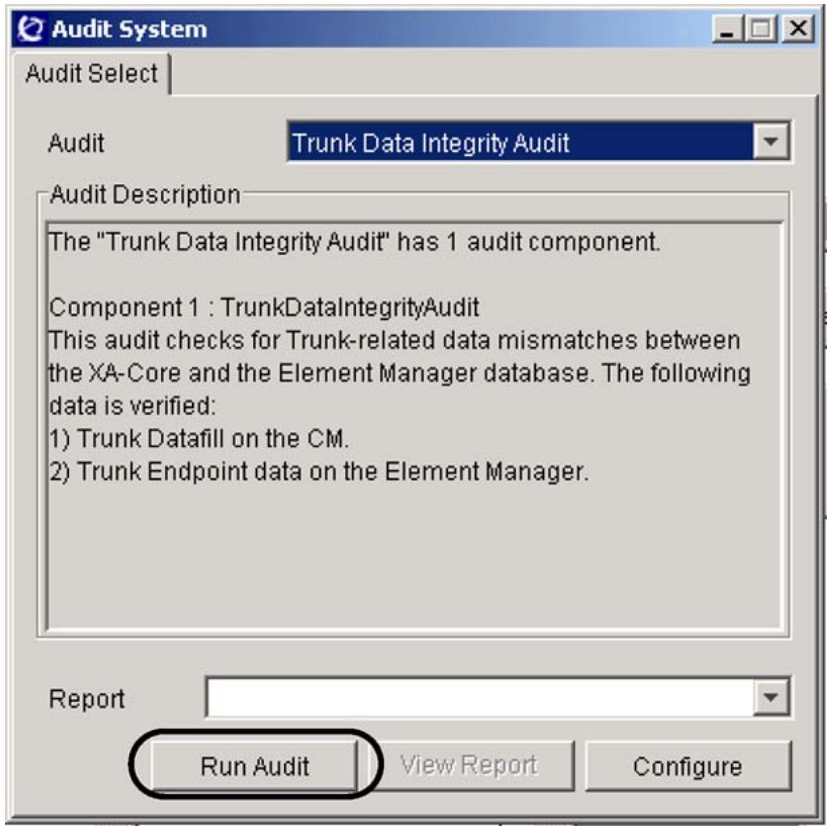
2 At the Audit System dialog box, select **Trunk Data Integrity Audit** from list of audits displayed in the drop-down menu.



3 Use the following table to determine your next step.

If you want to	Do
perform an on-demand trunk audit	go to step 4
view a trunk audit report	go to step 6

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



During a trunk audit, the system displays a progress window, which includes the progress bar and the current operation.

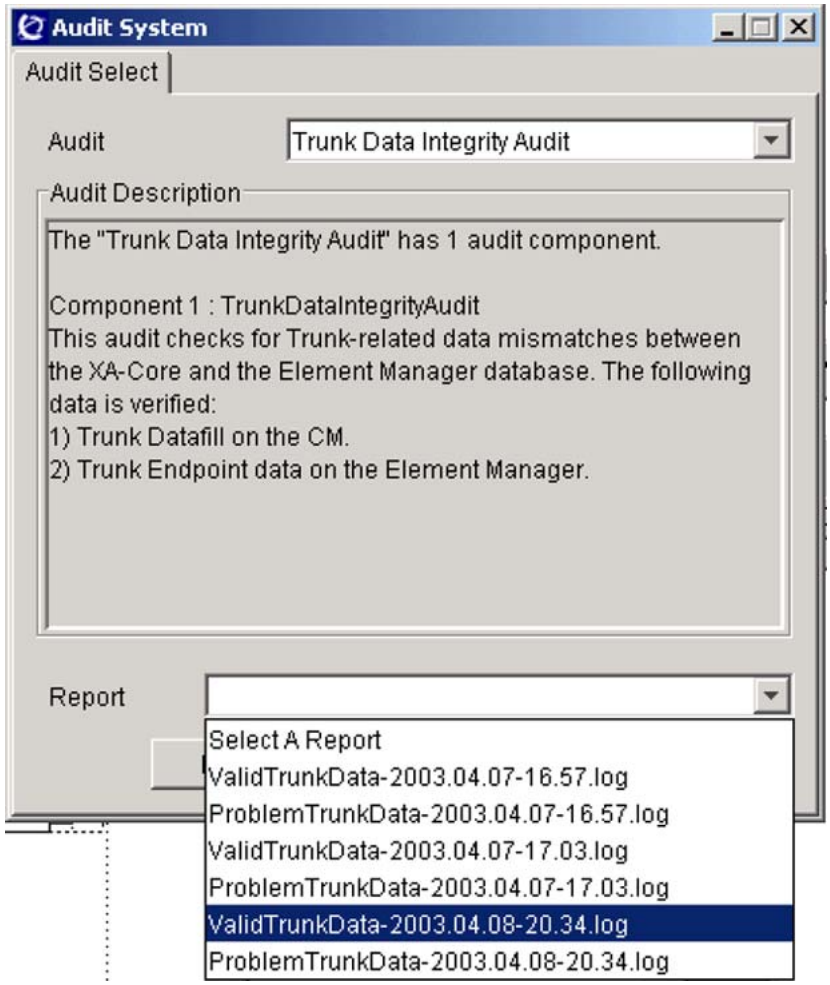
The audit may take a few minutes to complete. When the audit ends successfully, the system displays the following message:

If the audit does not execute successfully, the system displays the message "Trunk Data Integrity Audit Failed to Complete", 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 audit reports, complete the following sub-steps:

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. From the drop-down menu in the Report field at the bottom of the dialog box, select the **ValidTrunkData** or the **ProblemTrunkData** report that you want to view. If there is more than one 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 or ProblemLineData-<date>-<time>.log

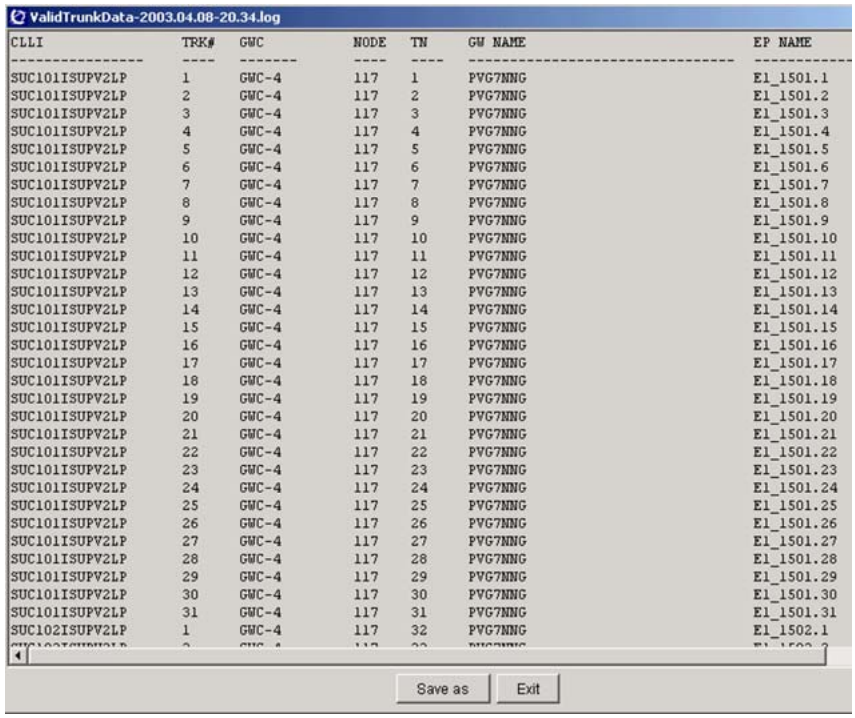
where

<date> is the date in yyyy.mm.dd format, for example, 2003.02.15.
<time> is the time in hh.mm format, for example 17.30.

c. Click the **View Report** button.

The system displays the selected report.

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

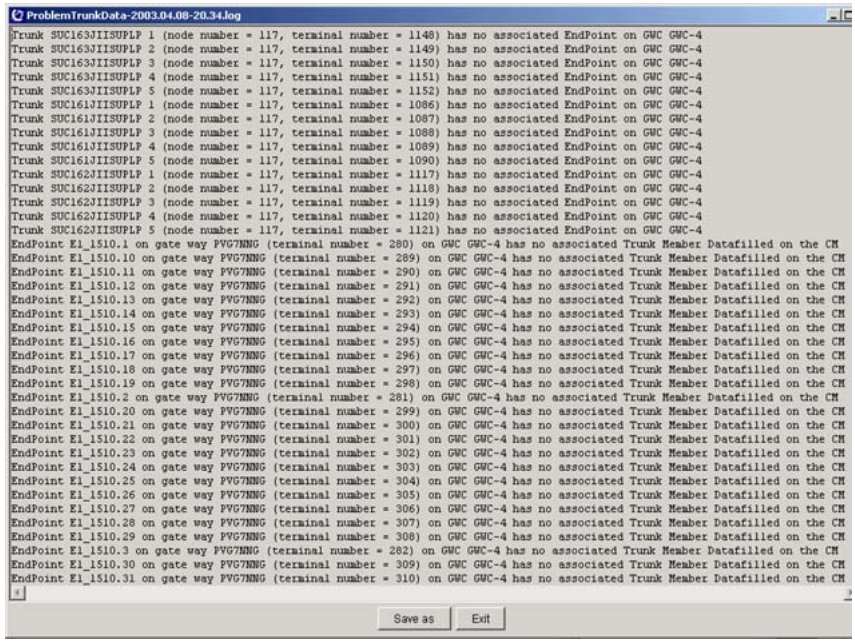
Example of a ProblemTrunkData report

If the audit found no problems, the report contains a message stating that no problems were found.

The ProblemTrunkAudit report can contain messages in the following formats:

- Trunk <trunk name> (node number = <NODE>, terminal number = <TID>) has no associated endpoint on GWC <GWC ID>.

- Endpoint <EP NAME> on gateway <GW NAME> (terminal number = <TID>) on GWC <GWC ID> has no associated trunk member datafilled on the CM.



The CS 2000 Management Tools server retains the six most recent reports. When a new trunk audit occurs, the server deletes the oldest report.

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

d. If you want to retain one of these reports for a longer time, or if you want to print a report, click the **Save as** button at the bottom of the screen and 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. For a description of each problem, see the printed copy of the ProblemTrunkData report. To correct the problems, delete and re-provision the listed trunks.

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

7 You have completed this procedure.

—End—

Perform a CS 2000 data integrity audit

Purpose of this procedure

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

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

You can also use this tool to schedule a CS 2000 data integrity audit. For instructions, see procedure "Configure a recurring data integrity audit" in *Gateway Controller Configuration Management* (NN10205-511).

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

Starting in (I)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 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.

If your network configuration includes a Session Server for SIP Lines functionality, the audit can also compare the IP-VPN(NAT) network zones configuration data in the GWC Manager and the Session Server Manager databases. This data must be consistent to allow the insertion of Media Proxies for SIP lines. For information about the Session Server Lines virtual gateway, see procedure "Associate a Session Server virtual gateway for SIP Lines" in *Gateway Controller Configuration Management* (NN10205-511).

For the Session Server Lines configuration information, see *Session Server Lines Fundamentals* (NN10437-111).

When to use this procedure

Use this procedure when you are receiving logs or alarms in the CS 2000 Core or at the CS 2000 SAM21 Manager client indicating a possible provisioning errors or data inconsistencies.

When the audit is running, suitable locks are in place that disable provisioning operations.

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

ATTENTION

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

Prerequisites

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

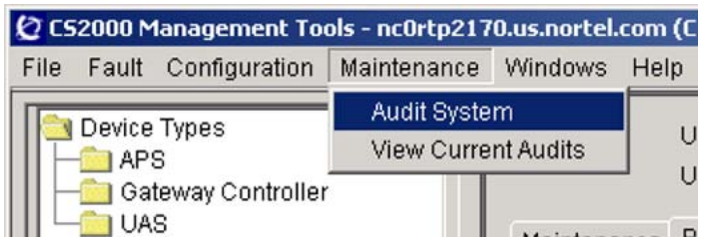
Unlike the line and trunk audits, the CS 2000 data integrity audit does not provide an option to save the audit report to a file on the local disk.

Action

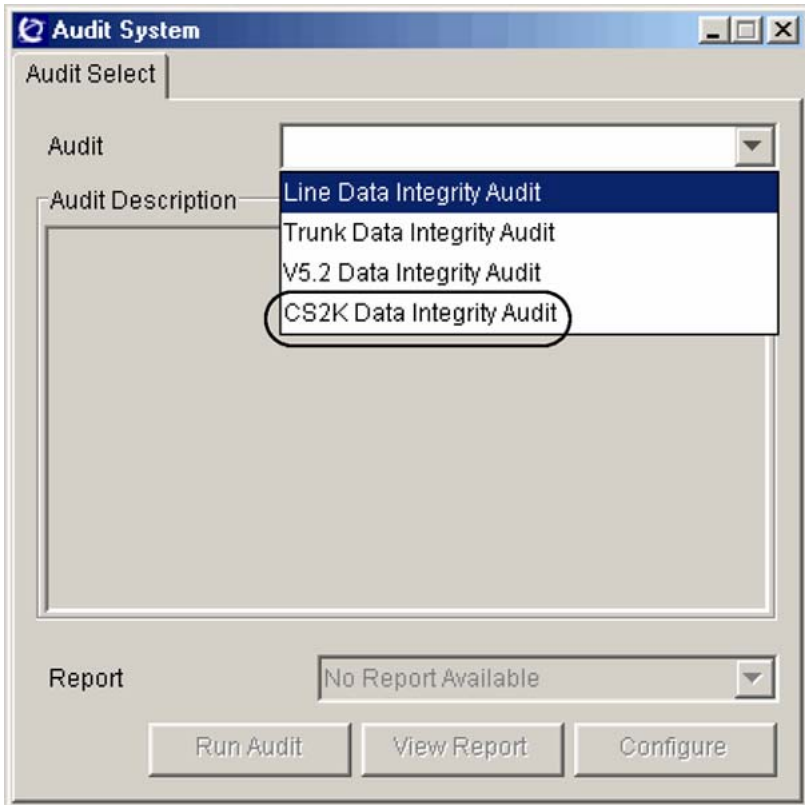
Step	Action

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 **CS2K Data Integrity Audit** from the list of audits displayed in the drop-down menu.



3 Use the following table to determine your next step.

If you want to	Do
perform an on-demand CS 2000 audit, then view the results of the audit	go to step 4
view the results of an audit that has finished running and resolve problems	go to step 8

4 At the Audit System dialog box, click the **Run Audit** button to display the CS2K Data Integrity Audit Configuration dialog box.

5 Select the CS 2000 component that you wish to audit:

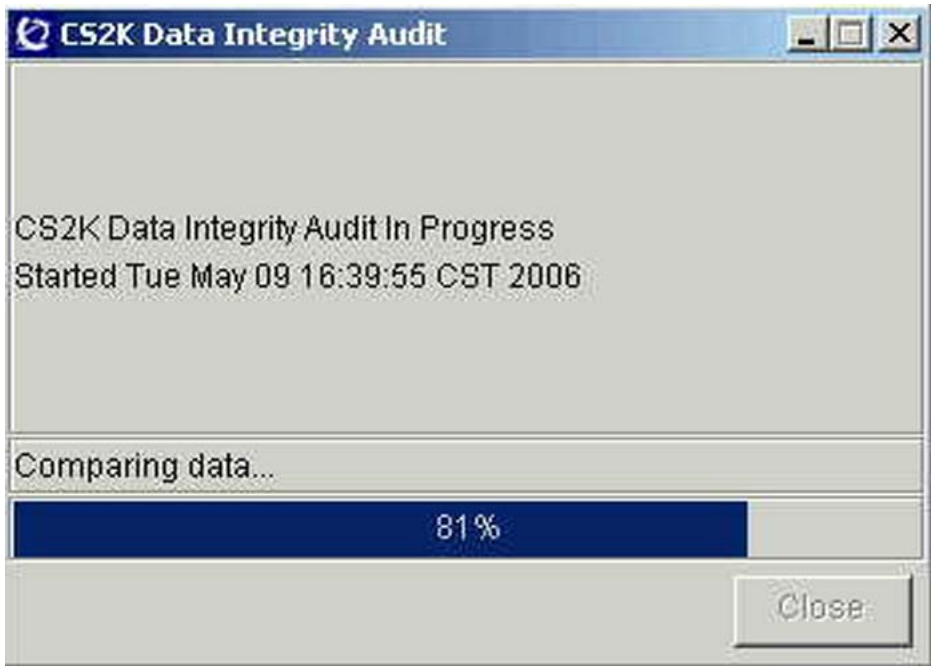
- Select the CS2KSS EM Data Integrity Audit check box - if you wish to verify that the network zones configuration data in the GWC Manager and the Session Server Manager databases match.
- Select the CS2K Call Server Data Integrity Audit check box - if you wish to verify that the data held by the GWC Manager database and the CS 2000 Call Server Core match.
- Select both check boxes - if you wish to audit both components.

  If there is no Session Server Manager configured on the CS 2000, the CS2KSS EM Data Integrity Audit check box is disabled.

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

If you wish to cancel the process, click the **Close** button.

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



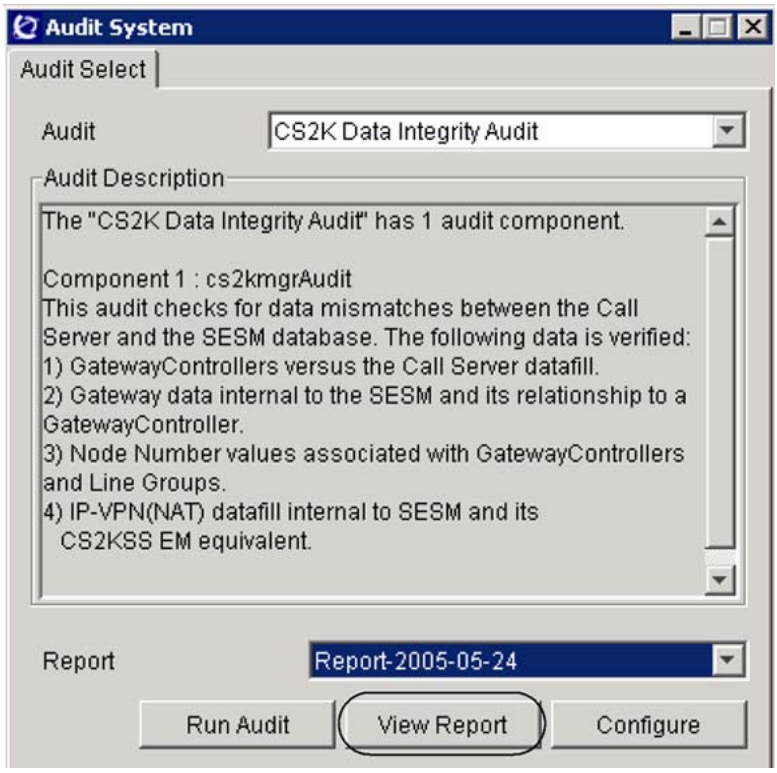
The audit may take a few minutes to complete. When the audit ends successfully, the system displays the following message:

If the audit does not execute successfully, the system displays the message "CS2K Data Integrity Audit Failed to Complete", with an error message indicating the reason. Contact your next level of support to resolve the problem.

7 Click the **Close** button to close the Audit Status window.

8 To view a CS 2000 audit report, complete the following sub-steps:

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



b. From the drop-down menu in the Report field at the bottom of the dialog box, select the report that you want to view.

   The file name has the following format:

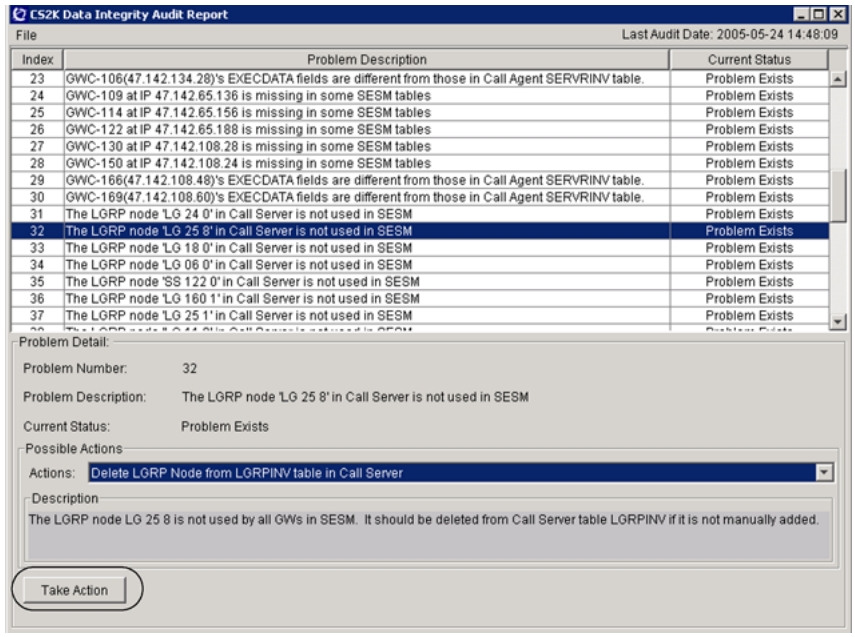
   Report-<date>

   where

   <date> is the date in yyyy-mm-dd format, for example, 2005-05-24.

c. Click the **View Report** button.

   The system displays the selected report. If no problems were discovered, the report is empty. The following example of a report lists various problems.



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

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

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

The CS2KSS EM Data Integrity Audit attempts to automatically correct all data mismatches found. The problems listed in the report are typically corrected and are displayed for information only. If any mismatch correction fails, manual action may be required or the system re-attempts the audit, or both.

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

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

10 Click the Actions: field and from the drop-down menu, select an appropriate action.

11 Read the description of the action and ensure that you observe any recommended steps or cautions.

12 Click the **Take Action** button.

If you see the message *Correction Failed*, contact your next level of support.

13 Return to step 9 if you wish to review another problem.

14 You have completed this procedure.

—End—

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 Core database

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

You can also use this tool to schedule a V5.2 data integrity audit. For instructions, see procedure "Configure a recurring data integrity audit" in *Gateway Controller Configuration Management* (NN10205-511).

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

When the audit is running, suitable locks are in place that disable provisioning operations.

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

ATTENTION

If you have scheduled data integrity audits, remember that a maximum of one 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.

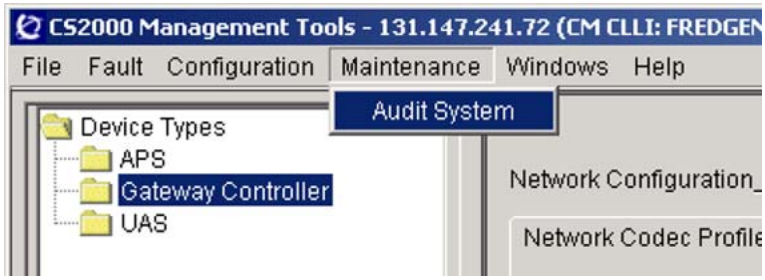
Unlike the line and trunk audits, the V5.2 data integrity audit does not provide an option to save the audit report to a file on the local disk.

Action

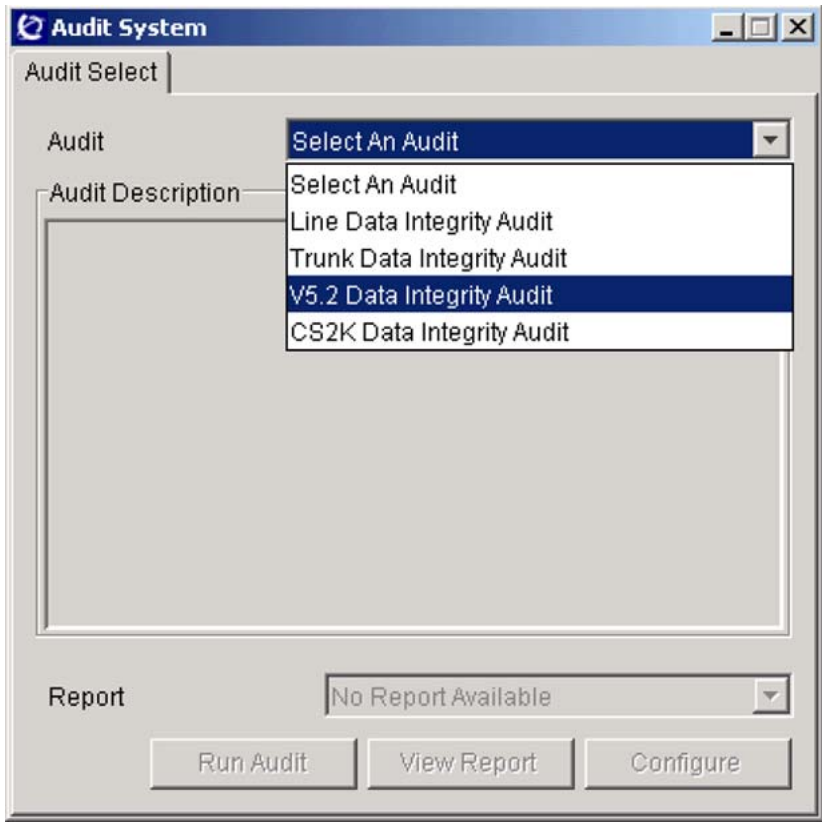
Step	Action

At the CS 2000 GWC Manager client

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



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

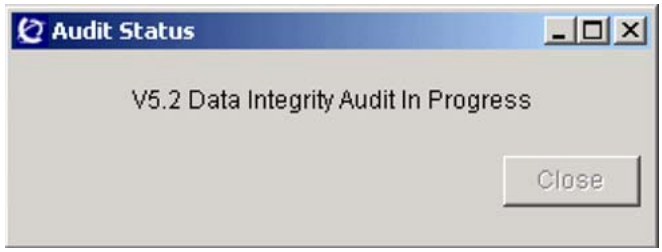


3 Select the next step as follows.

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.

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



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

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.

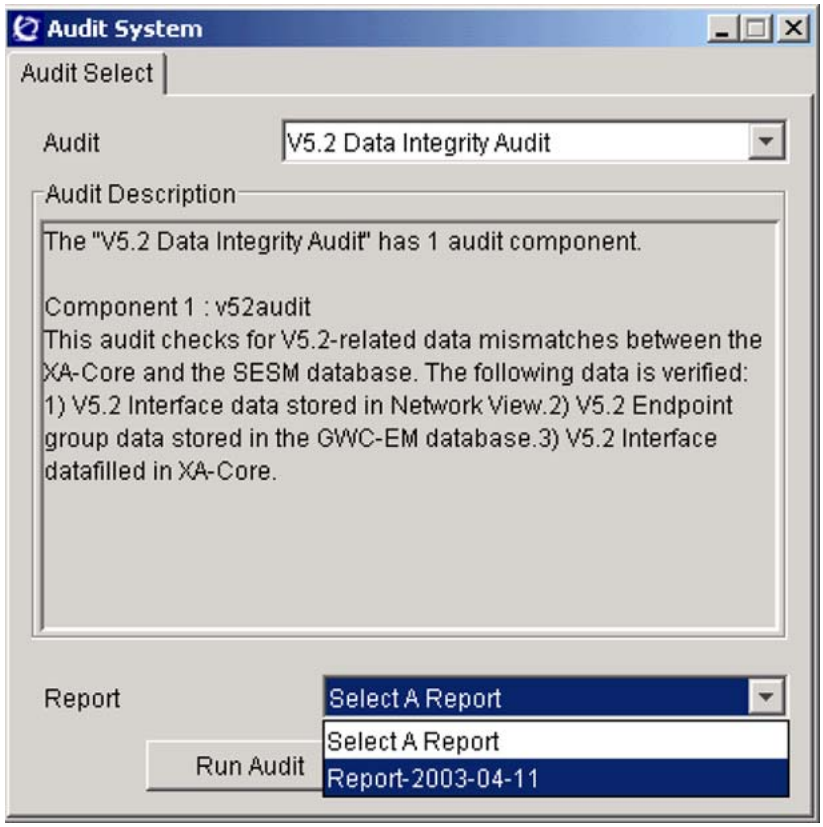
b. Select **Report** <date> from the drop-down menu in the Report field at the bottom of the dialog box.

The file name has the following format:

Report-<date>

where

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



c. Click the **View Report** button.

The system displays the selected report. If no problems were discovered, the report will be empty.

The CS 2000 Management Tools server retains the most recent V5.2 audit report. When a new audit occurs, the server deletes the previous report.

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

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

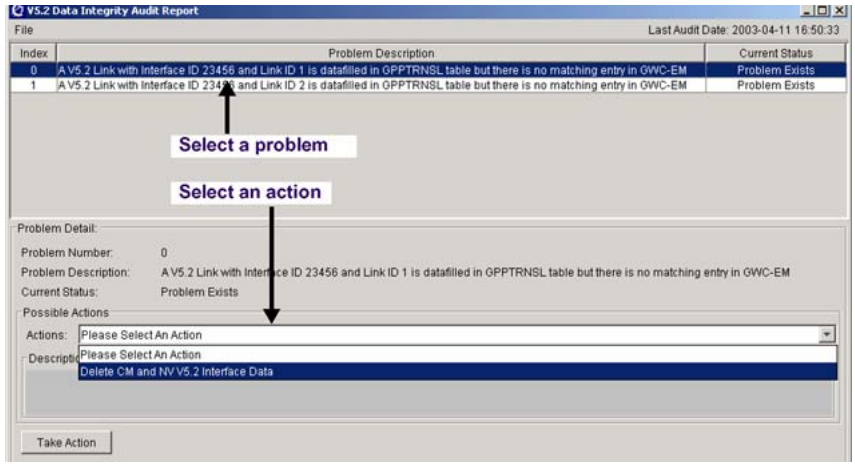
7 Review the results of the audit and select a problem to resolve.

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

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.



c. Click the **Take Action** button

If you see the message *Correction Failed*, contact your next level of support.

9 Return to step 7 to review another problem.

10 This procedure is complete.

—End—

View or abort running audits

Purpose of this procedure

Use this procedure to view and, if required, abort currently running audits. You can view and, if necessary, abort any of the following audits:

- line audit
- trunk audit
- V5.2 audit
- CS 2000 (CS2K) data integrity audits:
  - CS2K Call Server data integrity audit
  - CS 2000 Session Server (CS2KSS) Manager data integrity audit

For more information about each audit, see one of the following procedures:

- "Perform a CS 2000 data integrity audit" (page 119)
- "Perform a GWC line data integrity audit" (page 103)
- "Perform a GWC trunk data integrity audit" (page 112)
- "Perform a GWC V5.2 data integrity audit" (page 127)

For information about how to configure a recurring data integrity audit, see procedure "Configure a recurring data integrity audit" in *Gateway Controller Configuration Management* (NN10205-511).

When to use this procedure

Use this procedure when you need to view and abort the running audits.

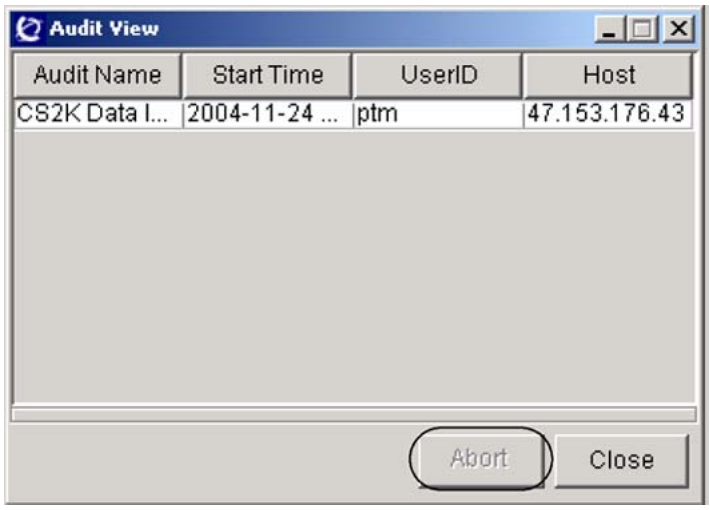
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click on the **Maintenance** menu and select **View Current Audits**.

2 At the Audit View window, you can view the currently running audits.



3 If you wish to abort one of them, click the appropriate row to select the audit. Your selection is highlighted.

4 Click the **Abort** button.

At the confirmation window, click **OK** to continue.

The audit originator receives an error message indicating that the audit has been aborted and identifying the user that aborted the audit.

5 The procedure is complete.

—End—

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" (page 66).

Action

Investigate problems using V5.2 audit logs.

Use table "V5.2 logs" (page 136) to review the details of the log type displayed by your log utility and formulate the appropriate actions to diagnose and repair the problem.

For more information about V5.2 logs, see the appropriate V5.2 log description in *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909).

V5.2 logs

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)
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.

Log type; Problem logged	Reason for failure	Details
		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.
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.

Log type; Problem logged	Reason for failure	Details
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.
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.

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" (page 68). 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 (IEMS). For more information, see *IEMS Fault Management* (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. 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.
<log description>	alphanumeric character string	A description of the conditions or reasons generating the log. The log can be static or variable. For log descriptions, causes, and associated actions, see section "Action" (page 140).
<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

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
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
Some log descriptions use variables such as %d or %s to indicate a numeric value is provided.		

Kerberos application log description	Cause or condition	Action
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		
IP mismatch: fqdn=%s, ip=%s		
Failed HMAC in SA_RECOVERED		
NULL session key parsing AP_REQ but no KRB ERROR		
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>. For the list of possible reasons and the associated actions, see table "Kerberos log reasons" (page 142).
<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

Kerberos application log description
<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.

IPSec and IKE security logs

This section describes how to access and understand IPSec and IKE security log reports associated with GWC nodes. These log reports are stored in the securitylog files in directory /var/log on the CS 2000 Management Tools server.

To access these security log reports, follow procedure "View GWC logs in syslog files" (page 68).

To display IPSec and IKE log reports, search for the text string ISAKMP within the securitylog files.

Format

The format for security log reports is as follows:

```
mmm dd hh:mm:ss [<IP address>] class_security.ver01 CMD="ISAKMP_<INFO or
FAIL> <log message>",STAT=<status> MID=<MID>
```

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. mmm means three first letters of the month, for example, Aug.
<IP address>	numeric	The IP address of the unit device from which the log originated.
<log type>	class_security.ver01	Common name for security logs.
ISAKMP_INFO or ISAKMP_FAIL	text string	Indicates an information-only or a problem-reporting log.
<log message>	alphanumeric character string	A description of the conditions or reasons generating the log. For log descriptions and associated actions, see section "Actions" (page 145).
<status>	success or failure	Indicates whether the operation succeeded or failed.
<MID>	MID=MID_Nortel_MGC_autho.<0016 or 0017>	0016 indicates an INFO log. 0017 indicates a FAIL log.

Actions

Required action depends on the log description. The following table lists security log messages and explanations, and the appropriate actions.

IPSec and IKE security logs

Log message	Explanation and Action
Logs associated with the "Phase 1 SA failure" GWC320 major alarm: **ATTENTION** **Service disruption** The following log reports and the associated alarms are the result of an outage. To clear these fault conditions, complete procedure "Clear the GWC320 Phase 1 SA failure alarm" (page 46).	
`ISAKMP_FAIL IKE phase 1 timeout exhausted (PHASE 1 <INITIATOR or RESPONDER>, init:<IP>, resp:<IP>)`	There is a problem during an IKE Phase 1 negotiation and multiple retransmission attempts fail.
`ISAKMP_FAIL IKE payload not formed correctly, possible preshared key mismatch (PHASE 1 INITIATOR, init:<IP>, resp:<IP>)`	The system cannot authenticate the remote gateway.
`ISAKMP_FAIL IKE payload validation failed, possible preshared key mismatch (PHASE 1 <INITIATOR or RESPONDER>, init:<IP>, resp:<IP>)`	The pre-shared key configured on the GWC does not match the pre-shared key configured on the remote gateway.
`ISAKMP_FAIL payload malformed, possible pre-shared key mismatch (resp:<IP>, init:<IP>)`	The pre-shared key configured on the GWC does not match the pre-shared key configured on the remote gateway.
`ISAKMP_FAIL payload malformed (resp:<IP>, init:<IP>)`	The system cannot authenticate the remote gateway.
`ISAKMP_FAIL No Preferences Match for IKE Phase 1 Negotiation (init:<IP>, resp:<IP>)`	IKE preferences configured on the GWC and on the remote gateway do not match.
`ISAKMP_FAIL invalid signature (init IP:<IP>, resp IP:<IP>)`	The GWC cannot authenticate the remote gateway.
`ISAKMP_FAIL IKE phase 1 signature or certificate check (PHASE 1 <INITIATOR or RESPONDER>, init:<IP>, resp:<IP>)`	There is a problem during an IKE Phase 1 negotiation and the GWC cannot verify or authenticate the certificate presented by the remote gateway.
Logs associated with the "Phase 2 SA failure" GWC320 major alarm: **ATTENTION** **Service disruption** The following log reports and the associated alarms are the result of an outage.	

Log message	Explanation and Action
To clear these fault conditions, complete procedure "Clear the GWC320 Phase 2 SA failure alarm" (page 50).	
`ISAKMP_FAIL No Preferences Match for IKE Phase 2 Negotiation (init IP:<IP>, resp IP:<IP>)`	IPSec preferences configured on the GWC and on the remote gateway do not match.
`ISAKMP_FAIL IKE phase 2 timeout exhausted (PHASE 2 <INITIATOR or RESPONDER>, init:<IP>, resp:<IP>)`	There is a problem during an IPSec Phase 2 negotiation and multiple retransmission attempts fail.
Logs associated with the "Certificate expiring" GWC320 minor, major, or critical alarm:	
`Certificate is expiring on Year=<yyyy> Month=<mm> Day=<dd>`	After an IKE Phase 1 negotiation, if any certificate in the chain (excluding the root CA) is expiring within 30 days, this failure log is generated. If the certificates are not replaced immediately, there may be a call processing outage. This log is associated a GWC320 alarm: • critical - certificate expires within 5 days • major - certificate expires within 15 days • minor - certificate expires within 30 days If the certificate is expired, this alarm remains, and if any connection policy and IKE authentication is using this certificate, a "Phase 1 SA failure" alarm is also raised. To clear the "Certificate expiring" alarm, complete procedure “Recovery of the GWC320 certificate expiry alarm” in *Nortel CVoIP IPSec Security Service Implementation Overview* (NN10453-100).
Logs associated with the "Certificate expired" GWC320 critical alarm:	
`One or more certificates in set number <x> are expired`	One or more certificates in a set is expired. An outage will occur if an IKE connection policy is using these certificates. To clear the "Certificate expired" alarm, complete procedure “Recovery of the GWC320 certificate expiry alarm” in *Nortel CVoIP IPSec Security Service Implementation Overview* (NN10453-100).
Logs indicating problems with the Diffie-Hellman (DH) exchange - no associated alarms:	

Log message	Explanation and Action
ATTENTION **Service disruption** The following log reports are the result of an outage.	
`ISAKMP_FAIL IKE Phase 1 key negotiation failed - DH is NULL (ini:<ip>, resp:<ip>)`	The GWC cannot allocate sufficient resources. Contact your next level of support
`ISAKMP_FAIL IKE Phase 1 key negotiation failed - unable to set peer's DH pub key (ini:<ip>, resp:<ip>)`	The GWC cannot allocate sufficient resources. Contact your next level of support
`ISAKMP_FAIL IKE Phase 1 key negotiation failed - unable to gen DH key pair (ini:<ip>, resp:<ip>)`	The GWC cannot allocate sufficient resources. Contact your next level of support
`ISAKMP_FAIL IKE Phase 1 key negotiation failed - unable to compute shared secret (ini:<ip>, resp:<ip>)`	The GWC cannot allocate sufficient resources. Contact your next level of support
`ISAKMP_FAIL DOI no supported (ini:<ip>, resp:<ip>)`	The GWC cannot negotiate a security association with the remote gateway. Contact your next level of support.
Logs indicating problems with the Phase 1 exchange - no associated alarms:	
ATTENTION **Service disruption** The following log reports are the result of an outage.	
To clear these fault conditions, complete procedure "Clear the GWC320 Phase 1 SA failure alarm" (page 46).	
`ISAKMP_FAIL invalid signature (ini:<ip>, resp:<ip>)`	The GWC cannot authenticate the remote gateway.
`ISAKMP_FAIL invalid payload (ini:<ip>, resp:<ip>)`	The GWC cannot authenticate the remote gateway.
`ISAKMP_FAIL invalid hash info (ini:<ip>, resp:<ip>)`	The GWC cannot authenticate the remote gateway.
Information-only logs:	

Log message	Explanation and Action
`Certificate provisioning - validity period checked: Certificate <effective or expire> Y/M/D H:M:S: <effective or expiry date and time>`	When a certificate is provisioned on the GWC, the GWC checks the certificate effective and expiry date and generates this log. When certificate provisioning fails, use this log to determine if the certificate is not effective or has expired. There is no associated alarm.
`Phase 1 SA Successfully Established (init IP:<IP>, resp IP:<IP>)`	This log confirms a successful IKE Phase 1 negotiation between the GWC and a remote gateway. If a GWC320 alarm is generated, it clears automatically. No action required.
`Phase 2 SA Successfully Established (init IP:<IP>, resp IP:<IP>`	This log confirms a successful IPSec Phase 2 negotiation between the GWC and a remote gateway. If a GWC320 alarm is generated, it clears automatically. No action required.

Associated OM registers

These log reports have no associated OM registers.

Additional information

None

Carrier VoIP

Gateway Controller Fault Management

Publication: NN10202-911
Document status: Standard
Document version: 08.02
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback .

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